INTERFERENCE MANAGEMENT IN WIRELESS NETWORKS: A CROSS LAYER APPROACH

JUNMEI YAO

Ph.D

The Hong Kong Polytechnic University

2016

The Hong Kong Polytechnic University

Department of Computing

Interference Management in Wireless Networks: A Cross Layer Approach

Junmei Yao

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

October 2015

Certificate of Originality

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it reproduces no material previously published or written, nor material that has been accepted for the award of any other degree or diploma, except where due acknowledgement has been made in the text.

_____ (Signature)

Junmei Yao (Name of Student)

Abstract

Wireless local area networks (WLANs) have become an important communication infrastructure for internet access in the past decade because of the popularity of laptops, smartphones, and so on. They are propelled to improve the network throughput effectively to face the challenge of sustaining the rapid growth of data traffic and the high density of wireless nodes. Interference is well known to degrade the wireless network performance, and it is inevitable due to the broadcasting characteristics of wireless signals and the coexistence of various wireless nodes working at the shared channel, which makes interference management be an everlasting research topic over the years. Current 802.11 standard utilizes the carrier sense multiple access (CSMA) mechanism to make nodes access the channel to avoid interferences. However, this mechanism is inefficient because of prohibiting effective concurrent transmissions, inducing interference and existing the coordination overhead, all of the aspects will degrade the network performance. Therefore, a more efficient mechanism needs to be proposed to improve the network performance.

In wireless networks, interference management always needs nodes to exchange the coordination information with adjacent nodes, so that they can obtain the requisite information to permit effective concurrent transmissions and avoid interference. However, the exchange of control frames always induce a large amount of transmission overhead; meanwhile, they may in turn make the wireless nodes waste some concurrent transmission opportunities because of avoiding the collisions induced by control frames. In this

dissertation, I propose to improve the wireless network performance through designing a cross layer approach, which contains interference resistance mechanism in the physical layer to make control frames conveyed in a more efficient way, and also contains the MAC layer mechanisms that utilize the information obtained from the physical layer for effective interference management.

Firstly, this dissertation proposes Interference Resistant Multiple Access (IRMA) to combat the exposed terminal problem and exploit transmission opportunities in wireless networks. Observations on the 802.11 standard reveal that nodes degrade the network throughput from two aspects, including the so-called *CA-CF problem* and *varied-IR problem*, and the problems will make nodes around both the transmitter and receiver of the ongoing link waste concurrencies. IRMA proposes to exploit transmission opportunities from solving the two problems through utilizing a physical layer mechanism that can combat the control frames' collisions. Secondly, this dissertation proposes Interference Cancellation Multiple Reception (ICMR) to further exploit reception opportunities also from solving both the problems, through utilizing another physical layer mechanism that can successfully detect data frames when collided by control frames. Thirdly, this dissertation proposes concurrency-based coordination mechanism (CCM) that can coordinate among nodes effectively in a centralized way to maximize concurrency and avoid data packet interference in WLANs. This protocol is also based on an interference resistance mechanism in the physical layer to make the control message and data packets transmitted concurrently to avoid the coordination overhead. Experimental results based on USRP2 demonstrate the feasibility of the physical layer mechanisms, and simulations based on ns-2 show that the three protocols can outperform the other current protocols significantly.

As a conclusion, this dissertation proposes a cross layer approach that benefits from both the physical layer and the upper layer design to maximize concurrent transmissions,

avoid interference and decrease the coordination overhead in current wireless networks, so as to improve the network performance.

Publications

Journal Articles

1. **Junmei Yao**, Tao Xiong, and Wei Lou, Beyond the Limit: A Fast Tag Identification Protocol for RFID Systems. *Elsevier Pervasive and Mobile Computing*, 21:1-18, Aug. 2015.

2. **Junmei Yao**, Tao Xiong, Jin Zhang and Wei Lou, On Eliminating the Exposed Terminal Problem Using Signature Detection. *IEEE Transactions on Mobile Computing*, doi:10.1109/TMC.2015.2478459.

3. **Junmei Yao** and Wei Lou, On Exploiting Concurrent Transmissions through Discernible Interference Cancellation. *IEEE Transactions on Networking*, under review.

4. **Junmei Yao**, Chao Yang and Wei Lou, Efficient Interference-Aware Power Control in Wireless Ad Hoc Networks. *IEEE Communications Letters*, resubmission allowed.

5. Junchao Ma, Wei Lou and **Junmei Yao**, On Providing Interference-aware Spatio-Temporal Link Scheduling for Long Delay Underwater Sensor Networks. *IEEE Transactions on Mobile Computing*, major revision.

6. Chao Yang, **Junmei Yao**, and Wei Lou, On Demand Response Management Performance Optimization for Microgrids under Communication Unreliability Constraints. *IEEE Transactions on Communications*, under review.

Conference Papers

1. **Junmei Yao**, Tao Xiong, and Wei Lou, Eliminate the Exposed Terminal Problem Using Signature Detection. *Proc. of the 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (**SECON**)*, Seoul, Korea, June 18-21, 2012.

2. **Junmei Yao**, Wei Lou and Chao Yang, Efficient Power Control Based on Interference Range in Wireless Ad Hoc Networks. *Proc. of the International Conference on Embedded Wireless Systems and Networks (**EWSN**)*, TU Graz, Austria, Feb 15-17, 2016.

3. **Junmei Yao**, Chao Yang and Wei Lou, Towards Centralized Transmission Coordination in WLANs: A Cross-Layer Approach. Submitted to *the 25th International Conference on Computer Communication and Networks (**ICCCN**)*.

4. Tao Xiong, Jin Zhang, **Junmei Yao**, and Wei Lou, Symbol-Level Detection: A New Approach to Silencing Hidden Terminals. *Proc. of the 20th IEEE International Conference on Network Protocols (**ICNP**)*, Austin, Texas, USA, October 30 - November 2, 2012.

5. Chao Yang, Wei Lou and **Junmei Yao**, Energy-Efficient Gateway On-Off Switching Scheme in Cognitive Radio Based Smart Grid Networks. *To appear in Proc. of the IEEE International Conference on Communications (**ICC**)*, Kuala Lumpur, Malaysia, May 23-27, 2016.

Acknowledgements

First and foremost, I would like to express my sincere appreciation to my chief supervisor, Dr. LOU Wei, for giving me continues encouragement and rigorous supervision during my whole Ph.D. research. He discussed every research problem and idea with me in detail. Without his vision, advices, extensive knowledge and commitment to the excellence, this thesis would not be completed. Dr. LOU Wei supported me for not only the study but also my personal life. I would like to especially thank him for his comprehension and pardon when my pregnancy affected the progress of research. What I have learned and experienced from him will benefit me much in the future, including the study and life.

I would also like to thank my co-supervisor, Dr. CHANG Kow Chuen Rocky, and the coexaminers of my guided study, Dr. XIAO Bin and Dr. WANG Qixin. They provided me with a lot of constructive advises and insightful comments for my research.

I would like to thank Dr. XIONG Tao for giving me help in learning the USRP platform by sharing his valuable experience. I also want to thank my colleagues Dr. ZHANG Jin, Dr. MA Junchao, Dr. CHEN Honglong, Dr. YANG Libin and Dr. YANG Chao for their interesting discussions and suggestions.

Finally, I would like to gratefully and sincerely thank my parents and brother for giving me unwavering faith and confidence in my study and life. I would also like to thank my husband XU Xiaogeng, for encouraging me to accept this student life and

giving me continuous support through the years. At last, I would like to thank my son XU Tianji, and my daughter XU Xiyue, for bringing me so much fun, they are the amazing gifts in my life!

Shen Zhen, China Junmei Yao

October 16, 2015

Table of Contents

Abstract **i**

Publications **v**

Acknowledgements **ix**

Table of Contents **xi**

List of Figures **xv**

List of Tables **xviii**

1 Introduction **1**

1.1 Motivation 1

1.1.1 Background 1

1.1.2 Two Problems in the 802.11 Standard 3

1.1.3 Benefits from Centralized Coordination 5

1.2 Thesis Contributions 7

1.2.1 The Architecture Contributions 7

1.2.2 The Protocol Design Contributions 8

1.2.3 Summary 12

1.3 Thesis Outline 13

2 Literature Review and Background **15**

2.1 Avoid Interferences 15
2.1.1 Using Control Frames Effectively 16
2.1.2 Using Extra Resources 17
2.1.3 Reducing Coordination Overhead 18
2.2 Exploit Concurrent Transmissions 20
2.2.1 Using Control Frames More Efficiently 20
2.2.2 Considering the Varied Interference Range 21
2.3 Recover Signals under Interferences 22
2.4 Introduce SDN to WLAN 25
2.5 Summary of Literature and My Work 26
2.6 Background of Cross Correlation 28

3 Exploit Transmission Opportunities Using Signature Detection 31
3.1 Overview 32
3.2 Overview of IRMA 37
3.2.1 IRMA Architecture 38
3.2.2 Overview of IRMA Behavior 39
3.3 IRMA Design 41
3.3.1 Control Frame Design 42
3.3.2 Signature Attachment 46
3.3.3 Signature Detection Method 47
3.3.4 Channel Access Scheme 49
3.3.5 Differentiated NAV State Update 50
3.3.6 Signature Detection Range Analysis 51
3.3.7 Address Conflict Analysis 53
3.4 Experiment Evaluation 55
3.4.1 Experiment Setup 55
3.4.2 Threshold β_{Corr} 56
3.4.3 Signature Detection Evaluation 57

3.5 Performance Evaluation . . . 60
3.5.1 Linear Topology . . . 62
3.5.2 Random Topology . . . 70
3.6 Summary . . . 73

4 Exploit Reception Opportunities through Discernible Interference Cancellation 75
4.1 Overview . . . 76
4.2 Overview of ICMR . . . 80
4.2.1 Control Frame Design . . . 83
4.3 Discernible Interference Cancellation Design . . . 83
4.3.1 Overview of DIC . . . 84
4.3.2 Preamble Synchronization and Signature Discernment . . . 86
4.3.3 Control Signal Reconstruction and Detachment . . . 86
4.3.4 Refined Channel Estimation . . . 91
4.4 Theoretical Analysis . . . 92
4.4.1 Formulation . . . 92
4.4.2 Opportunity Quantification . . . 98
4.5 Feasibility Evaluation . . . 104
4.5.1 Experiment Setup . . . 104
4.5.2 Evaluation of Blind Estimation Algorithm . . . 105
4.5.3 Data Frame Detection . . . 106
4.6 Performance Evaluation . . . 107
4.6.1 Linear Topology . . . 108
4.6.2 Random Topology . . . 112
4.7 Summary . . . 115

5 Coordinate Transmissions Centrally Based on Interference Resistance 117
5.1 Overview . . . 118
5.2 Design of CCM PHY . . . 123

5.2.1 REQ Message Design 123
5.2.2 Description of CCM PHY 124
5.2.3 Design of Power Control 127
5.3 Design of OpenCCM 128
5.3.1 Overview of OpenCCM Process 128
5.3.2 REQ_transmit Clients Determination 130
5.3.3 Interfering Lists Construction 131
5.3.4 Polling Lists Update 133
5.3.5 Link Admission Control 134
5.4 Performance Evaluation 137
5.4.1 The Single-AP Topology 138
5.4.2 The Multiple-APs Topology 142
5.5 Summary 146

6 Conclusions and Future Work **147**
6.1 Conclusions 147
6.2 Suggestions for Future Work 149
6.2.1 Evaluate the Performance under Current 802.11 Standards 149
6.2.2 Some Other Suggestions 152

Bibliography **157**

List of Figures

1.1 An example of the influence range of the 802.11 standard. 4

1.2 The cross layer design. 8

1.3 The thesis architecture. 12

1.4 The thesis outline. 13

2.1 Correlation threshold β_{Corr}. 29

3.1 Two scenarios that nodes waste transmission opportunities and one scenario that nodes induce collisions. 33

3.2 System architecture of IRMA. Comparing with the 802.11 standard, IRMA needs additional grey blocks to accomplish the protocol. 38

3.3 A scenario of IRMA, where $S1$ and $S2$ are exposed terminals when they transmit data to $R1$ and $R2$ respectively. IRMA permits their concurrent transmissions. Note that $S3$ is out of the interference range d_{IR} of $R1$, but in the interference range d_{IR} of $R2$. 40

3.4 The format of new RTS/CTS/ACK frames. 42

3.5 The signature detection method that discerns a known signature s_i from the incoming samples and recovers the original information. The signature set here is $\{s_1 \dots s_l\}$. 48

3.6 An example of the signature detection method. 49

3.7 A potential address conflict scenario. The two circles indicate the transmission range of $R1$ and $R2$, respectively. 54

3.8 Normalized correlation value vs. SINR. 57

3.9 False negative error rate. 58

3.10 False positive/negative error rates for signatures with 160 bits. 59

3.11 A linear topology, where four nodes $R1$, $S1$, $S2$ and $R2$ form a line. The distance between $S1$ and $R1$ as well as that between $S2$ and $R2$ are both set to $d_{link}(v_b)$. The distance between $S1$ and $S2$, denoted by d, is varied from $50m$ to $700m$. 63

3.12 Average throughput in terms of d under three transmission rates in the linear topology. 64

3.13 Average throughput in terms of packet length under three transmission rates in the linear topology. Concurrent transmissions are exploited in this scenario. 69

3.14 Average throughput in terms of packet delivery rate in the random topology, under three transmission rates and two packet lengths. 71

3.15 The throughput of each link when $l = 2000bytes$ and $v_b = 48Mbits/s$. . . 74

4.1 Two scenarios of *the CA-CF problem*. 78

4.2 Two scenarios of *the varied-IR problem*. 78

4.3 The time sequence diagram of nodes in a sample scenario of ICMR. . . . 81

4.4 The format of new CTS/ACK frames. 83

4.5 The process of DIC. 84

4.6 An example of the central phase offset in a received control frame. 89

4.7 An illustration of the limitations of reception opportunity. 97

4.8 Opportunity comparison among ICMR, IRMA and 802.11 standard. . . . 99

4.9 Opportunity quantification among three protocols. 103

4.10 Opportunity gain of ICMR over IRMA. 103

4.11 The CDF of phase estimation error under different SINR environments when the signature length is $160bits$. 106

4.12 The packet error rate under different SINR environments. 107

4.13 A linear network topology with four nodes $R1$, $S1$, $S2$ and $R2$. 109

4.14 Average throughput in terms of d_1. 110

4.15 A grid topology, where the distances of adjacent nodes d are set to be 100m, 200m and 400m, respectively. 112

4.16 Average throughput in terms of packet delivery rate in the random topology, under three transmission rates and two packet lengths. 114

5.1 The CCM architecture. 120

5.2 The CCM transmissions. 121

5.3 The format of REQ message. 124

5.4 Architecture of CCM PHY. 125

5.5 An overview of the OpenCCM process. 129

5.6 An example of the multiple-APs scenario. 133

5.7 The overall throughput in terms of the number of clients with traffic under two packet lengths in the single-AP scenario. 140

5.8 The overall throughput in terms of packet delivery rate under two packet lengths in the single-AP scenario. 141

5.9 The throughput of the high priority flow in terms of packet delivery rate under two packet lengths in the single-AP scenario. 142

5.10 The average delay of the high priority flow in terms of packet delivery rate under two packet lengths in the single-AP scenario. 143

5.11 The throughput of the high priority flow in terms of packet delivery rate under two packet lengths in the multiple-APs scenario. 144

5.12 The throughput and average delay of the high priority flow in terms of packet delivery rate when $l_p = 1500bytes$ in the multiple-APs scenario. . 145

6.1 A scenario of the control message and data packets collided in MIMO communication systems. 150

List of Tables

2.1 Summary of literature review. 27

3.1 False positive error rates when SINR$=-10dB$. 60
3.2 Simulation parameters. 61
3.3 Three transmission rates selected in the simulation. 62

4.1 The summary of opportunities among three protocols. 103
4.2 Simulation parameters. 108

5.1 Simulation parameters. 138

Chapter 1

Introduction

1.1 Motivation

1.1.1 Background

Wireless local area networks (WLANs) have become an important communication infrastructure for internet access in the past decade because of the popularity of laptops, smartphones, and so on. They are propelled to improve the network throughput effectively to face the challenge of sustaining the rapid growth of data traffic and the high density of wireless nodes. As interferences in wireless networks are inevitable due to the broadcasting characteristics of wireless signals and the coexistence of various wireless nodes working at the shared channel, interference management is an everlasting research topic over the years to increase concurrent transmissions and avoid interferences, thus improve the network performance.

Currently, one widely-deployed mechanism to manage interference in wireless networks is the 802.11 standard, in which nodes use the carrier sense multiple access (CSMA) to avoid interferences: Before transmitting, a sender senses the medium to determine if a nearby node is transmitting. If the channel is determined idle, the node proceeds

the transmission after a backoff time; otherwise, the sender will defer until the end of the ongoing transmission. This mechanism is also called physical carrier sense and it is well known to have a low performance as it uses the situation at the transmitter side to determine whether there is an interference at the receiver side, which induces a serious hidden terminal problem. The 802.11 standard utilizes a virtual carrier sense mechanism (also called RTS/CTS mechanism) to coordinate among nodes and combat the hidden terminal problem. The virtual carrier sense uses the exchange of RTS and CTS frames to reserve the medium for the actual data transmission. The RTS and CTS frames contain a NAV field that defines the period of time that the medium is to be reserved for the transmission of the actual data frame and returned ACK. All nodes that receive the RTS or CTS frames will keep silence during the NAV time to avoid interferences. However, the RTS/CTS mechanism also has some overhead that causes performance degradation, such as the exposed terminal problem that prevents effective data transmissions, the backoff time in the channel access contention, and so on. Although The IEEE community has improved the data transmission rate in the physical layer from $2Mbits/s$ ((802.11b)) [24] to $54Mbits/s$ ((802.11a/g)) [24], and $600Mbits/s$ (802.11n) or even $> 1Gbits/s$ (802.11ac), to improve the network performance, the overhead existed in the channel access scheme impede their effectiveness significantly.

This thesis has the motivation to analyze the drawbacks of the channel access in the 802.11 standard, and designs new protocols to improve the network performance.

1.1.2 Two Problems in the 802.11 Standard

Our work starts from analyzing the RTS/CTS mechanism in the 802.11 standard. In a wireless network, a transmission is successful if and only if the received Signal to Interference plus Noise Ratio (SINR) is above a threshold [77]. Thus, the basic requirement that two transmission links can proceed concurrently is, there is no mutual interference affecting their data frame receptions at receivers (the SINR at both data receivers are above a threshold). The basic requirement can also be expressed using the interference range: As only nodes which are within the interference range will interfere with the ongoing link, two links can proceed concurrently if both transmitters are outside the interference range of the other link. However, the 802.11 standard does not conform to this basic requirement and will degrade the network performance from two aspects.

The first is called *the CA-CF problem* (the excessive Collision Avoidance problem induced by Control Frames). The 802.11 standard uses the RTS/CTS/ACK control frames to help nodes get proper information. Nodes that receive the control frames will decide that they are within the interference range of a transmission link and should keep silence to avoid interference. However, this mechanism should also avoid collisions introduced by CTS/ACK frames, leading to the *CA-CF problem* which occurs in two scenarios: (1) The collisions with the CTS/ACK frames should be avoided at the transmitter side of the link, as the transmitter needs to detect the CTS/ACK frames correctly to get the coordination information. As shown in Fig. 1.1, when there is an ongoing transmission link $T \rightarrow R$, T_1 is prohibited to transmit packet, in order to avoid collisions with the CTS/ACK frames at T. (2) The data frame being collided by control frames should be avoided at the receiver side of the ongoing link. As shown in Fig. 1.1, R_1 is prohibited to

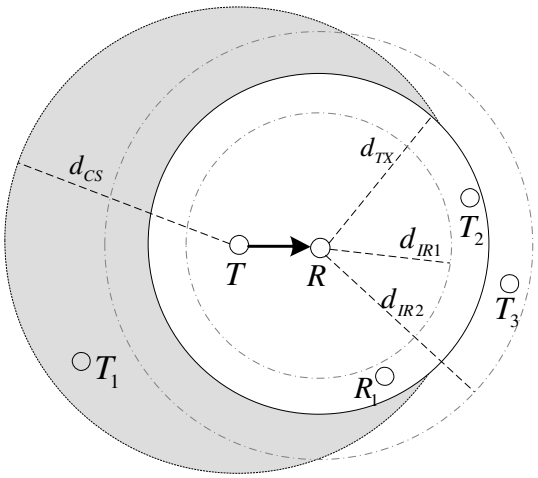


Figure 1.1: An example of the influence range of the 802.11 standard.

receive packets, in order to avoid its CTS/ACK transmissions to interfere with R's data reception.

The second is called *the varied-IR problem* (the varied Interference Range problem). Based on the 802.11 standard, nodes received CTS will determine that they are within the interference range of the ongoing link and should keep silence. This mechanism simply fixes the interference range to be the transmission range of CTS, although the interference range is variable and determined by the distance of the ongoing link [32,61]. As shown in Fig. 1.1, although the CTS transmission range d_{TX} is fixed, the interference range may be d_{IR1} which is smaller than d_{TX}, or may be d_{IR2} which is larger than d_{TX}. This situation will lead to *the varied-IR problem* that occurs in two scenarios: (1) It may cause excessive restriction of effective transmissions when the interference range is smaller than the transmission range (such as T_2 in Fig. 1.1 when the interference range is d_{IR1}, the node is wrongly prohibited to transmit packet). (2) It may bring false permissions of ineffective transmissions which lead to collisions when the interference range is larger than the transmission range (such as T_3 in Fig. 1.1 when the interference range is d_{IR2},

the node is wrongly permitted to transmit packet). Both scenarios will degrade the network performance through prohibiting concurrent transmissions or inducing collisions in wireless networks.

Recent studies that focus on exploiting concurrency and avoiding interferences mainly fall into solving one or two of the above problems. For example, Attached-RTS [79] and FAST [80] propose to make control information and data packet transmitted concurrently, thus solve *the CA-CF problem*; RTSS/CTSS [51], SDN [32] and TRACK [23] propose to solve *the varied-IR problem*; CMAP [78] proposes to solve parts of both problems. However, no protocol so far can exploit all the concurrent transmissions from solving the two problems.

Thus, this dissertation has the motivation to design efficient protocols to maximize concurrent transmissions and avoid interferences through solving both problems, which will result in exploiting concurrent transmission opportunities in wireless networks. As one node has different activities when transmitting or receiving a packet, we consider the analysis should be divided into two parts: the transmitter's transmission opportunity and the receiver's reception opportunity. In this dissertation, I design protocols to increase the two kinds of opportunities from solving the two problems, so as to improve the network performance.

1.1.3 Benefits from Centralized Coordination

As discussed before, the 802.11 standard utilizes CSMA and the RTS/CTS mechanism to coordinate among nodes to avoid interferences. However, besides the *CA-CF problem* and *varied-IR problem* induced overhead that prohibits concurrent transmissions or

induces collisions, this mechanism has a large amount of other coordination overhead that degrades the network performance, such as backoffs, DIFS (the distributed coordination function interframe space), the transmission of control frames and so on. All the overheads will dominate the communication resources in large scale networks [75]. Some current related works intend to design protocols in a distributed manner to mitigate the overheads and improve the network performance. However, mitigating one or some overhead may increase others, making these protocols not eliminate all the coordination overhead.

Nowadays, the concept of software defined network (SDN) for WLAN management using a centralized controller is an emerging method to improve the throughput of WLAN [74]. Based on this concept, data transmissions can be coordinated efficiently through utilizing the WLAN infrastructure, where multiple APs are connected by wired networks and can be treated as one virtual AP, which plays the role of coordination. This centralized coordination manner can largely mitigate the overhead induced by *the CA-CF problem*, *the varied-IR problem*, the backoff time and DIFS in the distributed mechanisms. Some recent research [4, 23, 57, 90] designs different mechanisms by utilizing the architecture of SDN to mitigate the coordination overhead and improve the network performance. However, these works have no effective way to coordinate the transmissions from clients to APs, and may induce some extra overhead because of unknowing the client side information.

Thus, we have the motivation to design a centralized coordination mechanism based on the concept of SDN, and utilize control frames to convey coordination information more efficiently to further improve the network performance.

1.2 Thesis Contributions

The main contributions of this thesis can be summarized into two aspects: the architecture contributions and the protocol design contributions.

1.2.1 The Architecture Contributions

Interferences in wireless networks are inevitable when there are various wireless nodes working at the shared channel. Improving the performance of wireless networks through interference management is a well-known concept, which always needs nodes to exchange the coordination information carried in control frames, so that they can obtain the requisite information of adjacent nodes and make proper channel access decisions. However, the exchange of control frames always induce a large amount of transmission overhead; meanwhile, they may in turn make the wireless nodes waste some concurrent transmission opportunities because of avoiding the collisions induced by control frames. In this dissertation, I propose to design cross layer protocols to manage interferences and improve the network performance through benefiting from both the physical layer and the upper layer design.

As shown in Fig. 1.2, the cross layer design in this dissertation contains the PHY layer and the upper layer design. The PHY layer design intends to make the coordination information in the control message transmitted concurrently with the other data or control message transmissions, so as to reduce its transmission overhead. This can be achieved through designing interference resistant mechanisms, based on which the control message can be detected correctly under interferences, and the control message transmissions will not degrade the effectiveness of data transmissions if needed. The upper layer design

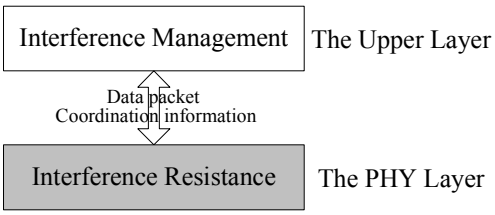


Figure 1.2: The cross layer design.

focuses on interference management, and intends to make nodes utilize the collected coordination information in the control messages to make proper channel access decisions, so as to increase the concurrent transmissions and avoid interferences to improve the wireless network performance.

1.2.2 The Protocol Design Contributions

Starts from solving different problems in current wireless networks, this thesis proposes three cross-layer protocols to increase the network performance. The detailed contributions of the three protocols are listed as follows:

1.2.2.1 Exploit Transmission Opportunities Using Signature Detection

Nowadays, most wireless networks are organized with the 802.11 standard [24], in which nodes use CSMA and the RTS/CTS mechanism to avoid collisions. However, theses mechanisms degrade the network performance because of two problems, including *the CA-CF problem* and *the varied-IR problem*, both problems will make nodes waste transmission and reception opportunities.

In this dissertation, I propose interference resistant multiple access (IRMA), a novel cross layer protocol, to solve the exposed terminal problem and exploit transmission opportunities to improve the throughput of wireless networks. IRMA can exploit transmis-

sion opportunities from solving the *the CA-CF problem* through permitting the control frame collision at the transmitter side by using a signature detection method (SDM), in which nodes use known symbol sequences, called as *signatures*, to convey information. When transmitting a control frame, nodes need to map the control information to dedicated signatures, attach the signatures to the frame at the physical layer and send the frame out. When receiving a control frame, nodes discern the signatures from the incoming signals and convert the signatures to the original control information. As signatures can be discerned in the presence of strong interferences, IRMA can exploit concurrent transmissions by using the signature detection method to tolerate control frame collisions at the transmitter side. IRMA can also exploit transmission opportunities from solving *the varied-IR problem*, through differentiating between the interfering and non-interfering links in an easy way. IRMA allows the receiver to use the CTS frame to reserve the medium for the transmitter's data transmission for the NAV time. Only the nodes in the interference range of the receiver will update the NAV state for keeping silence. IRMA further uses a new channel access scheme for nodes to determine whether to initiate a transmission or not when they intend to send a data frame. I conduct experiments based on USRP2 to demonstrate the feasibility of the signature detection method, and conduct simulations based on ns-2 to show the performance improvement of IRMA comparing with the 802.11 standard and other protocols. Specially, in a four-node scenario, IRMA has 2× throughput over current protocols.

1.2.2.2 Exploit Reception Opportunities through Discernible Interference Cancellation

Interference is a critical issue that will degrade the system performance in wireless networks. Although the 802.11 standard is widely deployed currently to avoid interferences, it has both *the CA-CF problem* and *the varied-IR problem* that degrade the network performance. IRMA is proposed to eliminate exposed terminals and exploit transmission opportunities from solving both problems. However, it leaves reception opportunities unexploited.

In this dissertation, I propose interference cancellation multiple reception (ICMR), a cross layer protocol, to further exploit the reception opportunities and improve the network performance. ICMR permits the reception of a data frame to be collided by control frames, and detects the collided data frame through a novel discernible interference cancellation (DIC) mechanism in the physical layer. In this mechanism, nodes also use signatures to convey the control information. When detecting a collided data frame, nodes first estimate the arrival and positions of control frames in the received signal, then discern signatures carried in the control frames, reconstruct the received control signal through proper channel estimations, and finally detach the control signal to recover the original data signal. I will also analyze the concurrent transmission opportunities of a link from the transmitter's transmission opportunities and the receiver's reception opportunities, then formulate the opportunities that can be exploited in the 802.11-based wireless networks from solving both *the CA-CF problem* and *the varied-IR problem*. I use hardware experiments based on USRP2 to demonstrate the feasibility of the discernible interference cancellation mechanism, and use simulations based on ns-2 to show

the performance improvement of ICMR comparing with IRMA and the 802.11 standard. Specially, in a four-node scenario, IRMA has 2× throughput over these protocols.

1.2.2.3 Coordinate Transmissions Centrally Based on Interference Resistance

Besides solving *the CA-CF problem* and *the varied-IR problem* to increase concurrent transmissions in wireless networks through designing distributed mechanisms, the concept of software defined network (SDN) for WLAN management inspires us to design a centralized coordination mechanism to further mitigate all the coordination overhead in current 802.11 standard, such as backoffs, DIFS and the transmissions of control frames.

In this dissertation, I propose concurrency-based coordination mechanism (CCM), a cross layer protocol, to maximize concurrent transmissions and eliminate the coordination overhead in WLANs, so as to increase the network performance. The main idea of CCM is based on the concept of SDN for WLAN management in a centralized manner, and also based on an observation that nodes only need to convey a small amount of information in the control message for the use of coordination. Therefore, through carefully design, the centralized controller can schedule the transmissions in both the uplink and downlink directions efficiently to maximize concurrency. It also makes the control message transmitted with the data packet simultaneously to eliminate the coordination overhead, through leveraging two interference resistance mechanisms in the physical layer, the signature detection method (SDM) and discernible interference cancellation (DIC), to detect both mutual interfered control messages and data packets successfully. Hardware experiments based on USRP2 can demonstrate the feasibility of the interference resistant mechanism in the physical layer. I use simulations based on ns-2 to show that

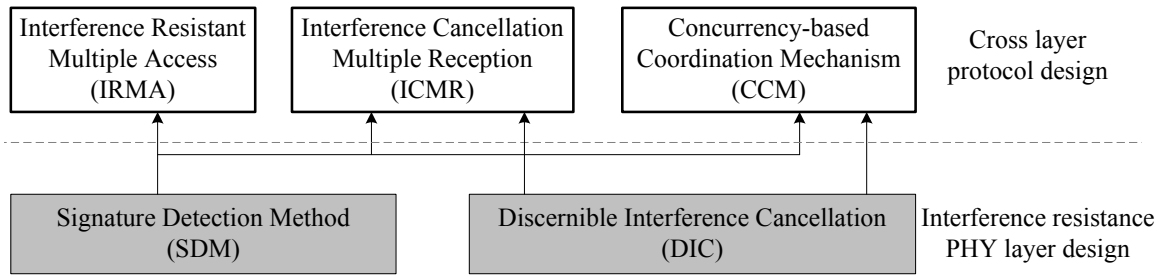


Figure 1.3: The thesis architecture.

CCM can outperform the 802.11 standard and other protocols significantly. Specially, in a multiple-AP scenario, CCM has about 151.6% throughput improvement over the 802.11 standard and about 45.5% over another current protocol.

1.2.3 Summary

As a conclusion, this dissertation proposes three cross layer protocols based on two physical layer mechanisms, as shown in Fig. 1.3. Interference resistant multiple access (IRMA) is proposed to exploit the transmission opportunities, it benefits from the signature detection method (SDM) in the physical layer. Interference cancellation multiple reception (ICMR) is proposed to further exploit the reception opportunities, it benefits from both SDM and the discernible interference cancellation (DIC) mechanism in the physical layer. Besides the two distributed mechanisms, concurrency-based coordination mechanism (CCM) is proposed to schedule transmissions centrally to maximize concurrent transmissions, it also benefits from both SDM and DIC mechanisms in the physical layer.

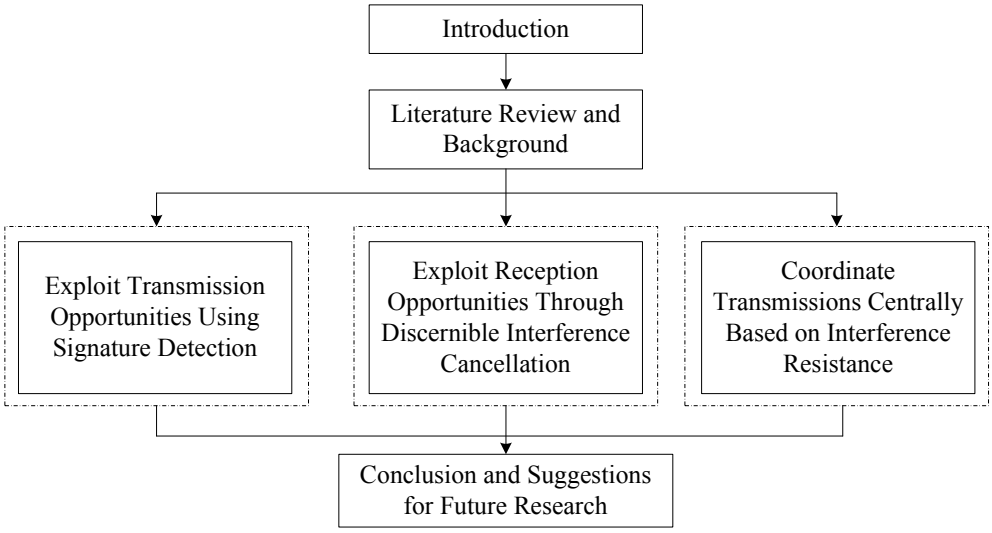


Figure 1.4: The thesis outline.

1.3 Thesis Outline

The structure of this thesis is organized as in Fig. 1.4. Chapter 1 is the introduction to this thesis. Chapter 2 briefly presents the literature review on interference management in wireless networks and gives some background of this thesis. The main body of this thesis is from Chapter 3 to Chapter 5. Chapter 3 proposes interference resistant multiple access (IRMA) protocol to exploit the transmission opportunities through using signature detection method in the physical layer. Chapter 4 proposes interference cancellation multiple reception (ICMR) protocol to exploit the reception opportunities and further improve the network performance through using the discernible interference cancellation mechanism in the physical layer. Chapter 5 proposes concurrency-based coordination mechanism (CCM) to improve the performance of WLANs through maximizing concurrent transmissions and eliminating the coordination overhead in a centralized way. Chapter 6 summarizes this thesis and puts forward future works.

Chapter 2

Literature Review and Background

Interferences in wireless networks are inevitable due to the broadcasting characteristics of wireless signals. Interference management is one of the fundamental challenges in the design of wireless systems to improve the network performance. Current related works mainly fall into four categories: avoiding interferences, exploiting concurrent transmissions, recovering signals under interferences, and introducing SDN to WLANs to schedule transmissions in a centralized way. In this chapter, I will first review the related work from the four categories in Section 2.1 to 2.4, then summarize the literature and give the position of my work in Section 2.5. I will finally introduce some background about the cross correlation technology which is related to my research in Section 2.6.

2.1 Avoid Interferences

The CSMA (physical carrier sense) is widely used in wireless networks to avoid interferences. However, this mechanism is well known to have a very low performance, as it may be wrong in many cases due to the different noise and interference conditions experienced between the transmitter and receiver. Brodsky and Morris in [8] recently presented a

theoretical model to analyze a two-sender carrier sense performance and concluded that this performance is close to optimal for radios with an adaptive bit rate. However, this model only considers situations with two contending senders, and it ignores MAC-level mechanisms such as the ACK and backoff. The result may not reflect practical network conditions.

Many research works [5,12–15,26,31,33,34,49,53,54,64,65,73,80,81,88,89] have been proposed to avoid interferences to improve the network performance.

2.1.1 Using Control Frames Effectively

Avoiding interference through utilizing control frames has been proposed since 1990's.

MACA [34] proposes to use the RTS/CTS handshake without the carrier sense to reserve a wireless channel. This mechanism can partially solve the hidden terminal problem to avoid interference. MACAW [5] revises MACA by introducing an ACK to acknowledge the successful reception of data transmission at the MAC layer. FAMA family MAC protocols [13–15] combine CSMA with RTS/CTS handshake to achieve better performances. Hardware experiments have been conducted to evaluate the performance of the 802.11 standard [54]. However, all these schemes work under the assumption that the interference range is the same as the data transmission range. However, this assumption cannot hold as the power needed for interrupting a packet's reception is much lower than that for delivering a packet successfully [89]. One solution to this problem in [89] is to let a node only response to RTS requests whose energy level is larger than a threshold, so as to make the interference nodes be within the receiver's data transmission range, but as a consequence it reduces more than half of the effective data transmission range.

RTS/S-CTS [88] presents a symbol-level detection mechanism to combat both the CTS collision problem and the remote hidden terminal problem, as the symbol sequences that carry useful information in the new S-CTS packet can be detected in very low SINR and SNR environments. It can improve the network throughput through avoiding collisions without sacrificing effective data transmission range.

Some research utilizes control frames to avoid interferences in power control mechanisms, where the interference range is varied due to the controlled transmission power of the sender [58,69,94,95,97,103]. In [94,103], authors utilize CTS to prevent interferences from possible senders. The transmission of CTS needs a power level larger than the data transmission power, so as to obtain a larger interference range to avoid data interference. Authors in [22] derive the optimal transmission power based on the location of each node in a centralized scheme. In [69], authors analyze the relationships among the transmission range, the carrier-sensing range, and the interference range in case power control is adopted, and propose four mechanisms to achieve power control and avoid interferences based on the analyzed results, then further propose an adaptive range-based power control (ARPC) MAC protocol to make use of the advantages of the four mechanisms to optimize the performance.

2.1.2 Using Extra Resources

Physical carrier sense is always ineffective as transmitters cannot get the condition at the receiver side in time. DBTMA [19] uses a separate control channel to send busy tone so that all nodes around a receiver can get its channel condition. DBTMA uses the RTS packet to initiate channel request, and use the transmit busy tone which is set up by

the RTS transmitter to protect the RTS packets, and use the receive busy tone which is set up by the receiver to acknowledge the RTS packet and provide continuous protection for the in-coming data packets. Nodes sensing any busy tone defer from sending their RTS packets on the channel. PCDC [53] also uses a separate control channel to send the RTS/CTS control packets and uses another channel to send data packets, so as to dynamically adjust the data transmission power to an optimal value. Some other research works such as [89] and [72] utilize directional antennas to avoid interference, they also need extra resources to combat the hidden terminal problem. Recently, FAST [80] is proposed to solve the hidden terminal problem through utilizing a full duplex paradigm [26] in wireless networks. It needs two antennas to be configured at each node to accomplish the duplex communications, one antenna is used for data packet transmissions, while the other antenna is used to broadcast control information by the receiver when it is receiving data packets, so that all the nodes around the receiver can keep silence to avoid interference.

2.1.3 Reducing Coordination Overhead

Avoiding interference always leads to coordination overheads, such as the back-offs, DIFS, and transmissions of control frames in current 802.11 standard. Some recent studies attempt to mitigate the coordination overhead through getting benefit from a physical layer mechanism.

802.11ec [49] exploits the cross correlation to accomplish the control frames' transmissions. Comparing with the 802.11 standard, this protocol uses three kinds of primitives to convey the RTS, CTS and ACK information. As the primitives can tolerate strong inter-

ferences, and the duration of these sequences is much less than that of the corresponding packets, this protocol can improve the network throughput through both avoiding collisions and reducing the transmission overhead of the control frames.

Backoff is a serious problem that degrades the wireless network performance, especially in the scenario of high node density and intensive traffic load [6]. T2F [64] and Back2F [65], which are based on OFDM wireless channels, migrate the random backoff from time domain to frequency domain to limit the backoff time in a few OFDM symbols, substantially decreasing the overhead induced by backoff. However, they need two antennas to be configured in each node, one for data transmissions, and the other for listening to all the subcarriers in the network.

REPICK [12] utilizes the OFDM subcarriers in the frequency domain for channel contention and ACK, thus enhances the MAC efficiency. Comparing with T2F [64] and Back2F [65] which only use subcarriers to reduce the backoff time, REPICK can reduce three overheads induced by 802.11 MAC, including DIFS, backoff and ACK, thus can dramatically improve the network performance. However, this mechanism needs symbol level synchronization among nodes, and also needs two antennas for transmitting data and listening to the channel at the same time.

The semi-distributed backoff (SDB) algorithm in [73] is proposed to make nodes perform the receiver-side backoff. Using SDB algorithm, they design a MAC protocol Semi-DCF, which exploits the collision detection capability of receivers for disseminating information on optimal backoffs to the contenders using signature vectors, so as to migrate backoff from random to deterministic, and largely reduce the backoff time in 802.11 standard. CWM [102] exploits collision tolerance mechanism to reduce the backoff time

and improve the channel utilization in the wireless networks. Upon detecting a collided signal from multiple senders, the receiver obtains the senders' IDs through exploiting the correlatable preamble in the physical layer, then allocates each sender a different timeslot so that the senders can transmit their data packets one after another in the following time, without mutual interference.

2.2 Exploit Concurrent Transmissions

Some research works [1, 9, 10, 21, 23, 30, 32, 38, 39, 46, 47, 51, 78–80, 93] focus on maximizing the number of successful concurrent transmissions to improve the network performance.

2.2.1 Using Control Frames More Efficiently

Some approaches are proposed to improve the network throughput through utilizing control frames in a more efficient way.

MACA-P [1] tries to avoid the control frames' collisions by scheduling them properly. Based on the exchanges of RTS/CTS, it schedules multiple transmissions in parallel to increase concurrent transmissions as well as avoiding their collisions. However, besides introducing a significant protocol overhead for information exchanges, it does not differentiate the interference ranges of different transmission links.

Attached-RTS [79] proposes Attachment Coding to allow the control information and data packet to be transmitted simultaneously, so as to reduce the overhead induced by the control information. Nodes then utilize the attached control information in the channel access decision to increase concurrent transmissions. However, this protocol has serious flaws as the control information is from the transmitter side, nodes around the receiver

side cannot obtain correct control information to make proper channel access decisions.

To solve the problem existed in Attached-RTS, the authors propose FAST [80] to combat both the hidden and exposed terminal problems. FAST utilizes a full duplex paradigm [26] in wireless networks, thus the control information will be transmitted by the transmitter with the data packet and be transmitted by the receiver at the same time. Nodes can obtain control information around both the transmitter and receiver side to make proper channel access decisions. However, FAST needs two antennas to be configured at each node because of the duplex communication, and the stringent requirement of full duplex communications seems hardly accomplishable with low cost in a near future.

2.2.2 Considering the Varied Interference Range

Many approaches are proposed to exploit concurrent transmissions which have no mutual interference but are prohibited because of not considering the varied interference range.

RTSS/CTSS [51] lets nodes differentiate between interfering and non-interfering links through an offline training, which is just applicable to the line topology.

Some research [46, 93] studies the physical carrier sense mechanism in the 802.11 standard, and proposes to tune the carrier sense threshold to an optimal value based on empirical probability analysis, so as to avoid interference and increase concurrent transmissions.

SDN [32] exploits non-interfering links that have no interference at both the transmitter and receiver sides for concurrent transmissions. Each node constructs an interference graph by periodically exchanging power-exchange packets with nearby nodes. The node

may transmit its own frame if there is no interference between its transmission link and any of current transmission links.

CMAP [78] builds a conflict map for each node using empirical observations of packet loss and uses the map to differentiate between interfering and non-interfering links. By listening to the ongoing transmissions and consulting the map, nodes can decide whether to transmit data immediately or not.

TRACK [23] harnesses the rate-adaptive exposed terminals in enterprise WLANs to make concurrent transmissions proceed successfully at a certain bit rate when the senders are prevented from transmitting by CSMA. TRACK tunes the bit rate of transmissions based on online channel measurements that account for SINRs, so as to maximize concurrency.

2.3 Recover Signals under Interferences

Instead of avoiding interference, some recent studies [17,20,28,29,35–37,40,43,44,49,56,59, 63,76,84,85,87,88,96,98,99,101] exploit strategies to recover signals under interferences, so as to improve the network performance.

Many current strategies leverage the technology of cross correlation to recover the control information under interferences so as to coordinate between nodes, such as CSMA/CN [63, 66], RTS/S-CTS [88] and 802.11ec [49]. In these protocols, authors carefully design some known symbol sequences to convey the control information, and conduct the cross correlation between the received signal and the known sequences to determine which sequence is received, so as to obtain the control information under interferences.

Some strategies intend to improve the network performance through improving the retransmission efficiency. PPR [27, 28] proposes a partial packet recovery mechanism to recover the whole packet via SoftPHY. The SoftPHY interface can analyze the symbol level information at the physical layer to identify the corrupted bits in the collided packet so that only the corrupted bits need to be retransmitted. MISC [56] is a packet retransmission scheme that merges incorrect symbols from multiple transmissions to produce correct ones. It exploits constellation diversity by rearranging the constellation maps in retransmissions, so as to improve the combining and decoding efficiency at the receiver side.

Some strategies try to reconstruct the collided packets by some known information. ANC [35] provides an algorithm for canonical 2-way relay transmission; it doubles the capacity of typical 2-way network by designing an analog network coding algorithm. The algorithm is based on the assumption that the receiver has already known one of the two collided packets; hence, the receiver can calculate the other collided packet. ZigZag [17] works for WiFi that has different transmission rates, and can deal with general collisions or hidden terminals. It uses the same idea as ANC but a novel approach to recover the collided packets. If the system has n packets collided, ZigZag requires each packet be retransmitted n times to fully decode the collided packets. DAC [99] and Chorus [98] utilize the similar decoding process in cooperative relay and efficient broadcast, respectively. mZig [40] can resolve one m-packet collision by this collision itself through utilizing the known shaping feature of the ZigBee physical layer design, so that it can achieve m-fold throughput improvement comparing with Zigzag.

Some strategies try to recover the collided signal through exploiting the well-known

capture effect [20, 42, 48, 83]. SIC [20, 67, 71] recovers the collided signal through receiving a stronger interfered signal first and then recovers the other interfered signal if its SINR after subtracting the stronger one is above the threshold. The idea of SIC has also been employed in [7, 52, 82] to improve the network performance through Aloha based random access. k-SIC [62] extends SIC to make a receiver capable of canceling up to k strongly interfering signals. Flash flooding [48] is proposed for rapid network flooding in wireless sensor networks. It avoids neighborhood contention by allowing concurrent transmissions among neighboring nodes, and exploits capture effect to ensure that each node can receive one flood from its neighbors. Coco [29] advocates simultaneous accesses from multiple senders to a sheared channel, optimistically allowing collisions instead of simply avoiding them, through both utilizing the capture effect and exploiting the ability to tolerate collisions because of redundancy in the physical layer implementations.

Some other strategies intend to transmit intended patterns (which carry the control information) with data packets simultaneously, through utilizing the redundancy in communication systems. Side Channel [85, 87] utilizes Direct-Sequence Spread Spectrum (DSSS) systems which have the ability to resist interferences to a certain extent [86]. The authors carefully design some "intended patterns" which carry the control information, and the "intended patterns" can be transmitted with the original data packet simultaneously, without degrading the effective throughput of data transmissions. hJam [84], Attached-RTS [79] and FAST [80] utilize a few of "clean" subcarriers which have no signal except noise in the packet preamble in current OFDM systems to carry the control information. They propose Attachment Coding to make the control information transmitted in some "clean" subcarriers of the data packet. The receiver can decide there

is an attached signal on a subcarrier if it detects a relatively high level energy on that subcarrier. After detecting the attached signals, node can obtain corresponding control messages. Meanwhile, the data signal can be recovered through detaching the attached control signal from the received signal.

2.4 Introduce SDN to WLAN

The concept of software defined network (SDN) for WLAN management using a centralized controller is an emerging method to improve the throughput of WLAN [2–4, 23, 41, 57, 70, 74, 90]. Based on this concept, transmissions can be coordinated efficiently through utilizing the WLAN infrastructure, where multiple APs are connected by wired networks and can be treated as one virtual AP in the protocol design.

CENTAUR [70] proposes to solve the downlink exposed and hidden terminal problems in enterprise WLANs through centralized scheduling. By periodical measuring the conflicts in the wireless environment according to the observation on the previously scheduled downlink traffic, a controller would have a fair estimate on when to transmit a new downlink packet for interference-free reception. However, it leaves the uplink transmissions unscheduled, leading to a poor performance when the uplink traffic increases. TRACK [23] harnesses the rate-adaptive exposed terminals in enterprise WLANs through centralized scheduling. It tunes the bit rate of concurrent transmissions based on online channel measurements that account for SINRs, and jointly schedule the transmissions of downlink exposed terminals through multiple APs connected by wired LAN. This protocol also cannot schedule the uplink transmissions, and may have poor performance when the uplink traffic increases and the CSMA-based contention mechanism is triggered.

OpenTDMF [90] builds an architecture that enables TDMA for enterprise WLANs, and combats the inefficiency of CENTAUR and TRACK. It contains a centralized controller that coordinates the whole WLAN jointly with APs. Uplink transmissions from clients are triggered by APs through the polling mechanism. Thus, OpenTDMF can achieve a higher performance in enterprise WLANs because of the lower overhead induced by control frames. COAP [57] is a cloud-based centralized frame work that can coordinate and manage individual home APs using an open API. It can lead to significant management improvement through effect efficient channel assignment and co-operative transmission schedules for interference mitigation.

Comparing with the works that exploit the WLAN architecture to schedule transmissions and avoid interference, some strategies benefit from the interference cancellation mechanism in the physical layer [4, 41]. Symphony [4] encourages collision of packets among transmitters at APs and cooperatively decode all the packets by utilizing a Zigzag-like [17] decoding process and the coordination information among APs. OpenRF [41] presents a cross layer architecture for MIMO interference management. It enables APs to perform three physical layer MIMO techniques: interference nulling [18], coherent beamforming [60] and interference alignment [45]. It then dynamically applies the right set of these MIMO techniques to suit any topology or traffic pattern.

2.5 Summary of Literature and My Work

Table. 2.1 gives a summary of the literature review. The interference management mechanisms are divided into two parts: those are in the distributed manner or in the centralized manner, while the physical layer mechanisms are mainly divided into three categories:

Table 2.1: Summary of literature review.

Interference management / Physical layer design	Distributed manner			Centralized manner	
	Recover interfered data signal	**Avoid data interference**		**Recover interfered data signal**	**Efficient coordination**
		Avoid interference	**Exploit concurrent transmissions**		
×		MACA[34], MACAW[5], FAMA[13-15], DBTMA[19], PCDC[52]	MACA-P[1], RTSS/CTSS[50], SDN[32], CMAP[77]		TRACK[23], CENTAUR[69], OpenTDMF[89], COAP[56],
Exploit cross correlation	PPR[27], ANC[35], Zigzag[17], DAC[97], Chorus[96], mZig[40]	CSMA/CN[65], RTS/S-CTS[88], 802.11ec[49], Semi-DCF[72], CWM[100] **IRMA&ICMR**	**IRMA&ICMR**	Symphony[4]	**CCM**
Exploit capture effect	SIC[20,66,70,71], *k*-SIC[61], Flash flooding[48], Coco[29]				
Utilize known feature in physical design	mZig[40], MISC[55]	Side Channel[84], REPICK[12], FAST[79], T2F[63], Back2F[64]	Attached-RTS[78], FAST[79]		OpenRF[41]

exploit cross correlation, exploit capture effect and utilize some known features in the physical design. Some related works are filled in the corresponding positions.

This thesis designs three cross layer protocols to manage interference, while the Interference Resistance Multiple Access (IRMA) and Interference Cancellation Multiple Reception (ICMR) are designed from both avoiding interference and increasing concurrent transmissions to improve the network performance, and Concurrency-based Coordination Mechanism (CCM) is designed from coordinating transmissions centrally based on the architecture of SDN. The three protocols are based on two interference resistance mechanisms in the physical layer to combat the control frame induced collisions, as described in section 1.2.3. The two mechanisms are based on the cross correlation technology. Comparing with existed works which exploit the cross correlation technology to recover collided control signal and avoid interference [49, 63, 88], this thesis first exploits this

technology to recover both the collided control message and data packets in the physical layer, based on which to further increase concurrent transmissions in the network.

2.6 Background of Cross Correlation

As described in section 1.2.1, this thesis contains a PHY layer interference resistance mechanism design that makes the coordination information in the control message transmitted concurrently with the other data or control message transmissions. According to the design, control messages can be detected correctly under interferences, while their transmissions will not degrade the effectiveness of data transmissions if needed. The interference resistance mechanisms are based on the cross correlation technology, which is commonly used for searching for a known feature in a long duration signal [77]. Cross correlation has already been used in preamble synchronization to accomplish the physical carrier sense mechanism in the 802.11 standard [24]. It also has some applications in recent works such as [4, 17, 49, 63, 88, 100]. In this section, I will give some details of cross correlation as a background of this thesis.

A wireless signal is typically described as a stream of complex numbers, and the bit sequence of the signal should be mapped into a series of complex samples in the digital modulation process. At the receiver, after RF down-converter and sampler in the demodulation process, the signal is represented as a series of complex samples, which may differ from the transmitted sample sequence in amplitude, phase, and frequency. Suppose $x[n]$ is the complex number that represents the n^{th} transmitted sample, the corresponding received sample $y[n]$ can be denoted as:

$$y[n] = Hx[n]e^{j2\pi n\delta_f T} + w[n],$$

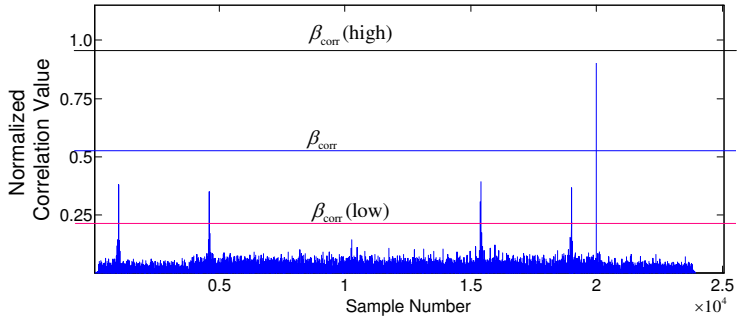


Figure 2.1: Correlation threshold β_{Corr}.

where H is the channel attenuation factor, δ_f is the frequency difference between the sender and receiver, T is the sampling period, and $w[n]$ is the background noise, which contains the thermal noise and interferences from other concurrent transmissions.

Suppose two nodes $S1$ and $S2$ transmit signals simultaneously, and are both received at node R. Suppose the transmitted sample is $x_1[n]$ in $S1$, and $x_2[n]$ in $S2$, then the received signal at R is

$$y[n] = H_1 x_1[n] e^{j2\pi n \delta_{f1} T} + H_2 x_2[n] e^{j2\pi n \delta_{f2} T} + w[n].$$

Let the samples $s[k]$, $1 \leq k \leq L$, refer to a known sequence, and $\overline{s[k]}$ be the complex conjugate[1] of $s[k]$. We can define the cross correlation of signals s and y at the position Δ as:

$$\begin{aligned} R_x(\Delta) &= \sum_{k=1}^{L} \overline{s[k]} y[\Delta + k] \\ &= \sum_{k=1}^{L} \overline{s[k]} (H_1 x_1[\Delta + k] e^{j2\pi(\Delta+k)\delta_{f1} T} + H_2 x_2[\Delta + k] e^{j2\pi(\Delta+k)\delta_{f2} T} + w[\Delta + k]). \end{aligned} \tag{2.1}$$

When the transmitted signal x_2 from $S2$ matches s at the position Δ', while x_1 and

[1]The conjugate transpose of a complex number is to negate its imaginary part but remain its real part unchanged.

w are independent of s at this position, we can get:

$$\begin{aligned} R_x(\Delta') &= \sum_{k=1}^{L} \overline{s[k]}(H_2 x_2[k+\Delta'] e^{j2\pi(k+\Delta')\delta_{f2}T}) \\ &= H_2 \sum_{k=1}^{L} |s[k]|^2 e^{j2\pi(k+\Delta')\delta_{f2}T}. \end{aligned} \tag{2.2}$$

Then we have:

$$|R_x(\Delta')| = H_2 \sum_{k=1}^{L} |s[k]|^2. \tag{2.3}$$

The correlation value $|R_x(\Delta')|$ is the sum of energy of this segment of signal, and it reaches a peak value if the known sequence appears in the received signal. If not, $|R_x(\Delta')|$ would be close to zero as the received signal is independent of the known sequence. The value $|R_x(\Delta')|$ can be normalized by the signal strength of s, as $|R_N(\Delta')| = \frac{|R_x(\Delta')|}{H\sum_{k=1}^{L}|s[k]|^2}$ [63]. Practically, the value $|R_N(\Delta')|$ is compared with a constant threshold β_{Corr} to detect the known sequence: If $|R_N(\Delta')|$ is above β_{Corr}, the known sequence is detected in the received signal at position Δ'.

Thus, the coordination information can be conveyed by some known sequences and be detected even under interferences through utilizing the cross correlation technology. Different thresholds may lead to different detection results. As shown in Fig. 2.1, a higher threshold $\beta_{Corr}(high)$ increases the probability of a false negative error (a sequence that is in the received signal is missed), and a lower threshold $\beta_{Corr}(low)$ increases the probability of a false positive error (a sequence that is not in the received signal is mistakenly detected). Both errors should be mitigated in the mechanism design.

Chapter 3

Exploit Transmission Opportunities Using Signature Detection

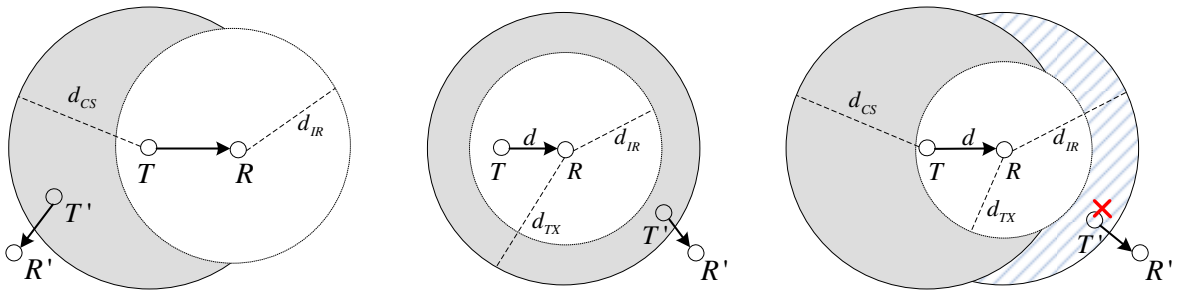
Wireless networks are propelled to improve the network throughput effectively to face the challenge of sustaining the rapid growth of data traffic and the high density of wireless nodes. Exposed terminals are a main source in wireless networks that degrades the network throughput as nodes are prevented from transmitting data frames concurrently even when their transmissions have no mutual interference. In this chapter, I propose the design of Interference Resistant Multiple Access (IRMA), a cross layer protocol, to solve the exposed terminal problem and exploit transmission opportunities. Observations on the 802.11 standard reveal that nodes degrade the network throughput from two aspects, including the so-called *CA-CF problem* and *varied-IR problem*, both problems will make nodes around both the transmitter and receiver of the ongoing link waste concurrencies. IRMA proposes to exploit transmission opportunities from solving the two problems. It proposes a signature detection method in the physical layer to combat control frames' collisions, thus solves the *CA-CF problem* and exploits the transmission opportunities at the transmitter side. It also designs a new NAV update scheme in

the MAC layer to differentiate the interference ranges of different transmission links, and designs a new channel access scheme for nodes to solve the *varied-IR problem* and exploits the transmission opportunities at the receiver side. Experimental results based on USRP2 demonstrate the feasibility of the signature detection method, and simulations based on ns-2 show that IRMA outperforms the 802.11 standard and other protocols significantly.

This chapter is organized as follows. Section 3.1 gives an introduction of IRMA. Section 3.2 gives an overview of the IRMA architecture and mechanism. Section 3.3 describes the design of IRMA in detail. Section 3.4 demonstrates the feasibility of the signature detection through hardware experiments. Section 3.5 evaluates the performance improvement of IRMA through simulations. Section 3.6 summarizes this chapter.

3.1 Overview

Nowadays, most wireless local area networks are organized with the 802.11 standard [24], in which nodes use the carrier sense multiple access (CSMA) to avoid collisions: Before transmitting, a sender senses the medium to determine if a nearby node is transmitting. If the channel is determined idle, the node proceeds the transmission; otherwise, the sender will defer until the end of the ongoing transmission. The CSMA can also be performed through a virtual mechanism. The virtual carrier sense uses the exchange of RTS and CTS frames to reserve the medium for the actual data transmission. The RTS and CTS frames contain a NAV field that defines the period of time that the medium is to be reserved for the transmission of the actual data frame and returned ACK. All nodes that receive the RTS or CTS frames will keep silence during the NAV time to avoid collisions. However, CSMA introduces the exposed terminal problem that causes performance degradation,



(a) *The CA-CF problem*: Nodes in the grey area are prohibited to transmit data.

(b) *The varied-IR problem*: Nodes in the grey area are prohibited to transmit data.

(c) *The varied-IR problem*: Nodes in the slash area permitted to transmit data.

Figure 3.1: Two scenarios that nodes waste transmission opportunities and one scenario that nodes induce collisions.

as senders are prevented from transmitting data frames concurrently even when their transmissions have no mutual interference [78].

This problem has attracted much attention as wireless networks should improve the performance effectively to face the challenge of sustaining the rapid growth of data traffic and the high density of wireless nodes. Although the transmission rate in the physical layer has been increased through advancing new technologies [24,25], the wasted transmission opportunities or collisions induced by CSMA impede their effectiveness remarkably.

As described in Section 1.2.1, in wireless networks, the basic requirement that two transmission links can proceed concurrently is, both transmitters are outside the interference range of the other link. However, the 802.11 standard does not conform to this basic requirement and has two problems that make nodes waste transmission opportunities.

The first is *the CA-CF problem* (the excessive Collision Avoidance problem induced by Control Frames). The 802.11 standard uses the RTS/CTS/ACK control frames to help nodes get proper information. Nodes that receive the control frames will decide that they are within the interference range of a transmission link and should keep silence to avoid

interference. However, this mechanism make nodes waste transmission opportunities because of avoiding the control frame collisions at the transmitter side. As shown in Fig. 3.1(a), although the data frame collision only exists at the receiver R, nodes that are in the carrier sense range d_{CS} of the transmitter T should also be prohibited to transmit concurrently, in order to avoid the CTS/ACK frame collision at T. Nodes in the grey area waste their transmission opportunities, as their concurrent transmissions will not interfere with R's reception of ongoing data.

The second is *the varied-IR problem* (the varied Interference Range problem). Based on the 802.11 standard, nodes received CTS will determine that they are within the interference range d_{IR} of the ongoing link and should keep silence. This mechanism simply fixes d_{IR} to be the transmission range d_{TX} of CTS, although the d_{IR} is variable and determined by the distance d of the ongoing link [32,61], that is, $d_{IR} \propto d$. As shown in Fig. 3.1(b), if d is fairly small, d_{IR} can be shorter than the transmission range d_{TX} [89]. However, under the 802.11 standard, nodes in the grey area are prohibited to transmit concurrently although they are more than d_{IR} from the receiver and will not interfere with the ongoing transmission link $T \rightarrow R$. Nodes waste transmission opportunities as the medium around the receiver has been simply reserved through the CTS frame.

Meanwhile, *the varied-IR problem* may induce unnecessary collisions as nodes wrongly have the transmission opportunities. As shown in Fig. 3.1(c), if d is relatively large, d_{IR} will be larger than the transmission range d_{TX}. However, under the 802.11 standard, nodes in the slash area are permitted to transmit packets although they are less than d_{IR} from the receiver and will definitely interfere with the ongoing transmission link $T \rightarrow R$. Nodes induce collisions as they cannot receive the CTS frame correctly. Ref. [89] intends

to solve this problem through reducing the effective transmission range so as to make d_{IR} smaller than the real transmission range d_{TX}. However, this mechanism will obviously prohibit more concurrent transmissions and degrade the network throughput.

Recent studies that address the exposed terminal problem and exploit the transmission opportunities fall into solving one or two of the above problems. SDN [32] exploits non-interfering links that have no interference at both the transmitter and receiver sides for concurrent transmissions, and can partially solve *the varied-IR problem*. In SDN, each node constructs an interference graph by periodically exchanging power-exchange packets with nearby nodes. The node may transmit its own frame if there is no interference between its transmission link and any of current transmission links. However, SDN cannot determine interfering links effectively when d_{IR} is larger than d_{TX}, thus may induce collisions in the scenario of Fig. 3.1(c). Meanwhile, it does not exploit transmission opportunities in the scenario of Fig. 3.1(a).

CMAP [78] considers two scenarios in Fig. 3.1(a) and Fig. 3.1(b). It builds a conflict map for each node using empirical observations of packet loss and uses the map to differentiate between interfering and non-interfering links. By listening to the ongoing transmissions and consulting the map, nodes can decide whether to transmit data immediately or not. CMAP also exploits transmission opportunities around the transmitter side, and tries to mitigate the ACK collision at the transmitter through a window-sized ACK and retransmission protocol. However, in the scenario of Fig. 3.1(a), concurrent transmissions have a high ACK loss rate, which causes many redundant retransmissions and degrades the network throughput. Meanwhile, collisions cannot be prevented in the scenario of Fig. 3.1(c).

In this chapter, I propose Interference Resistant Multiple Access (IRMA), a novel cross layer protocol, to exploit transmission opportunities and improve the throughput of wireless networks. IRMA combats the control frame collision at the transmitter side by using a signature detection method, in which nodes use known symbol sequences, called as *signatures*, to convey information. When transmitting a control frame, nodes need to map the control information to dedicated signatures, attach the signatures to the frame at the physical layer and send the frame out. When receiving a control frame, nodes discern the signatures from the incoming signals and convert the signatures to the original control information. As signatures can be discerned in the presence of strong interferences, IRMA can exploit concurrent transmissions by using signature detection method to tolerate control frame collisions at the transmitter side. Thus, it can exploit transmission opportunities in the scenario of Fig. 3.1(a).

IRMA also exploits transmission opportunities in the scenario of Fig. 3.1(b) through solving *the varied-IR problem* in an easy way. IRMA allows the receiver to use the CTS frame to reserve the medium for the transmitter's data transmission for the NAV time. Only the nodes in the interference range of the receiver will update the NAV state for keeping silence. IRMA further uses a new channel access scheme for nodes to determine whether to initiate a transmission or not when they intend to send a data frame. IRMA can differentiate between interfering and non-interfering links even when the interference range is larger than the transmission range, as the new designed CTS frame can be detected correctly in very low SINR environments. Thus, it can avoid collisions effectively in the scenario of Fig. 3.1(c).

This chapter makes the following key contributions:

- IRMA is the first protocol that can exploit transmission opportunities in the two scenarios shown in Fig. 3.1(a) and Fig. 3.1(b), and avoid collisions in the scenario shown in Fig. 3.1(c). IRMA can exploit transmission opportunities through solving *the CA-CF problem* as collided control frames can be detected correctly using the signature detection method. It also solves *the varied-IR problem* and exploits concurrency through differentiating between interfering and non-interfering links according to the ongoing transmission link, no matter the interference range is larger or smaller than the transmission range.

- I quantify the signature detection method through hardware experiments. The results demonstrate the feasibility of the signature design as the control frames' signatures can be detected correctly in the presence of strong interferences.

- I demonstrate IRMA's significant throughput improvement through simulations. The results show that IRMA can outperform both 802.11 standard protocols under different network topologies and different transmission rates.

3.2 Overview of IRMA

In this section, I will introduce the architecture of IRMA protocol and overview the IRMA mechanism through an example for ease of understanding. Based on that, I summarize the key information that should be detected using signature detection method (SDM) in the case of collisions for the IRMA design.

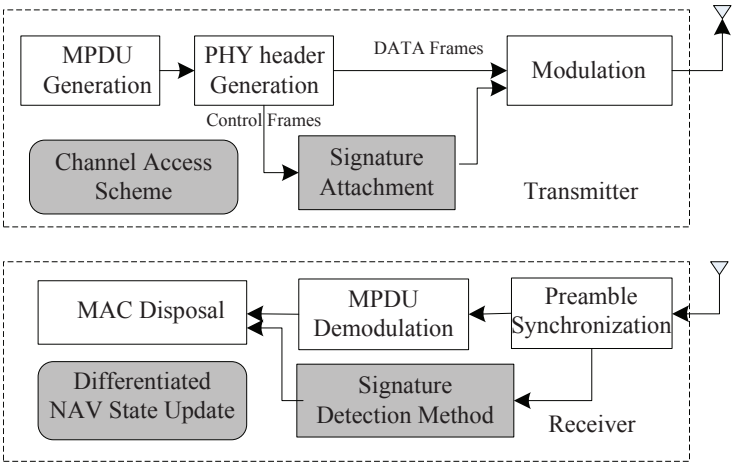


Figure 3.2: System architecture of IRMA. Comparing with the 802.11 standard, IRMA needs additional grey blocks to accomplish the protocol.

3.2.1 IRMA Architecture

Fig. 3.2 briefly illustrates the architecture of IRMA. Compared with the 802.11 standard, IRMA needs new blocks to accomplish the protocol.

Under the 802.11 standard, when a transmitter begins to transmit a frame, it first generates a MAC protocol data unit (MPDU), then adds a physical layer header, finally transmits the frame out after modulation. For a control frame to be transmitted, IRMA will attach signatures, which represent specific control information, to the standard frame before modulation. A new channel access scheme in the MAC layer is designed to achieve more concurrent transmissions and avoid data collisions.

In the receiving process, after completing the preamble synchronization, the receiver begins to demodulate the samples in the MPDU field. At this time, IRMA lets the receiver perform a signature detection method (SDM) to detect the control information. The outputs of MPDU demodulation and signature detection are both used for the MAC disposal. A new differentiated NAV state update scheme in the MAC layer is designed

to distinguish the interfering and non-interfering links around a node, while the results can assist the channel access scheme to make proper decisions.

3.2.2 Overview of IRMA Behavior

IRMA uses RTS/CTS/DATA/ACK four-way handshake mechanism for the medium access and data transmission. Physical carrier sense is disabled by IRMA as the interfered control frames at the transmitter side can be detected correctly using SDM. Moreover, all the new components in Fig. 3.2 work collaboratively to increase concurrent transmissions.

For ease of understanding, I illustrate the IRMA mechanism in a typical scenario with the time sequence diagram of each node, as shown in Fig. 3.3: $S1$ and $S2$ are exposed terminals as they intend to transmit data to $R1$ and $R2$, respectively. Their concurrent transmissions are permitted by IRMA. $S3$ can interfere with $R2$'s data reception, but it cannot interfere with $R1$'s reception. $S4$ may also interfere with $R2$'s data reception. Comparing to the 802.11 standard, IRMA works differently, which is illustrated as follows:

- If $S1$ wants to transmit data to $R1$, the transmission can be permitted by the channel access scheme as $S1$'s NAV state is zero. It then sends a RTS frame after a backoff time to initiate the transmission, and begins to transmit data frame after receiving the CTS feedback from $R1$ successfully. Although $S3$ (which acts as T' in Fig. 3.1(b)) is in the transmission range d_{TX} of $R1$ and can receive this CTS message, it should not update its NAV state, as it is outside the interference range d_{IR} of $R1$. Note that although $S2$ is out of d_{TX} of $R1$, it can also detect this CTS message correctly using SDM. It should not update its NAV state as it is also outside d_{IR} of $R1$.

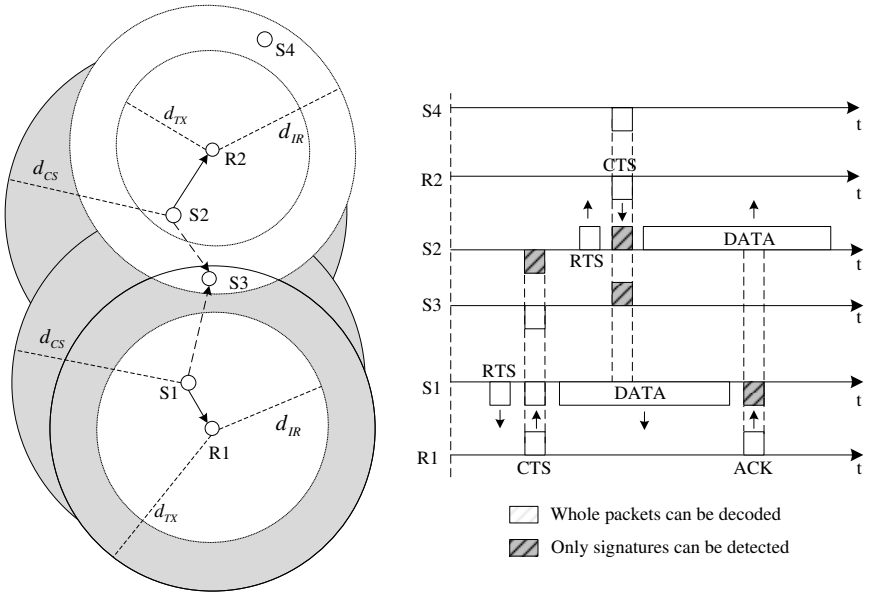


Figure 3.3: A scenario of IRMA, where $S1$ and $S2$ are exposed terminals when they transmit data to $R1$ and $R2$ respectively. IRMA permits their concurrent transmissions. Note that $S3$ is out of the interference range d_{IR} of $R1$, but in the interference range d_{IR} of $R2$.

- During the data transmission from $S1$ to $R1$, although $S2$ (which acts as T' in Fig. 3.1(a)) is in the carrier sense range d_{CS} of $S1$ and determines the channel to be busy, it can be permitted to transmit data to $R2$ by the channel access scheme as its NAV state is zero. $S2$ then sends a RTS frame after a backoff time to initiate its transmission. The corresponding CTS feedback from $R2$ will be interfered at $S2$ by the data transmission from $S1$. However, this interfered CTS can be detected correctly using SDM. Therefore, $S2$ can continue the data transmission to $R2$ accordingly. Note that $S3$ and $S4$ (both act as T' in Fig. 3.1(c) here) can also detect the CTS frame correctly using SDM and get the NAV information, although they are out of the transmission range of $R2$. They should update their NAV states to keep silence, as they are both in the interference range d_{IR} of $R2$.

- After finishing the reception of the data frame, $R1$ will reply an ACK to $S1$. The ACK frame would be interfered at $S1$ by the data transmission from $S2$. This interfered ACK can be detected by $S1$ using SDM, completing the transmission successfully.

From this scenario, we can see that three key control information should be detected correctly from the CTS/ACK frames even when they are under collisions. The first one is the receiver address (RA) of the CTS/ACK frames. The nodes (such as $S1$ and $S2$ in Fig. 3.3) should be able to obtain the RA information in the CTS frame to check if it is the target of this frame even when the CTS frame is interfered by other transmissions. Meanwhile, the RA information in the ACK frame notifies the node that its data frame has been received correctly. The second one is the NAV information in the CTS frame, with which nodes that do not involve in the RTS/CTS handshake (such as $S3$ in Fig. 3.3) can update their NAV state to keep silence. The third one is the interference range of the ongoing transmission link, which should be obtained by the nearby nodes as an input to the channel access scheme so that they can make a proper decision on accessing the channel concurrently while avoiding interferences.

3.3 IRMA Design

This section describes the design of the IRMA protocol. I first accomplish the control frame design according to the analysis in Section 3.2.2, then discuss the new blocks of IRMA (gray-color blocks shown in Fig. 3.2), including signature attachment, signature detection method (SDM), channel access scheme, and differentiated NAV state update. In the end, I analyze the signature detection range, and discuss an address conflict problem

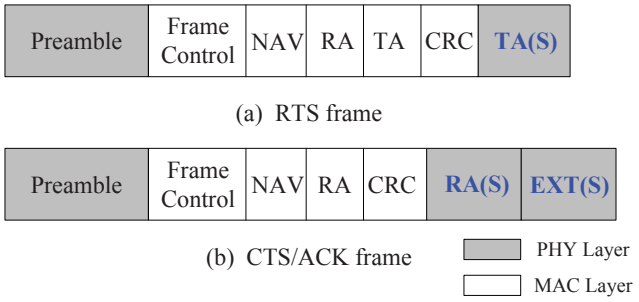


Figure 3.4: The format of new RTS/CTS/ACK frames.

when multiple nodes choose the same signature as their own addresses.

3.3.1 Control Frame Design

In Section 3.2.2, I have summarized three key control information that should be detected correctly when a collision occurs: the receiver address (RA), the NAV information and the interference range. Therefore, I design new control frames to make these control information detectable using SDM. I add some new fields to the 802.11 standard control frames, as shown in Fig. 3.4. In the transmitting process, these new fields are filled with signatures that carry specific control information. In the receiving process, nodes can recover the information after discerning signatures in corresponding fields.

For the new RTS frame, I attach a new field called TA(S) to the tail of the frame in the physical layer, as shown in Fig. 3.4(a). A transmitter will assign a signature, which represents its own address, in the TA(S) field of the RTS frame. For the new CTS or ACK frame, two new fields RA(S) and EXT(S), which are also filled with signatures, are attached to the tail of the frame, as shown in Fig. 3.4(b). RA(S) indicates the receiver address of the frame, which will be filled directly with the TA(S) signature derived from the received RTS frame. EXT(S) carries the combined information of both the NAV time

and interference range (IR) of the ongoing transmission link[1].

Each of the TA(S)/RA(S) and EXT(S) needs a group of global-unique signatures to represent their information. I design a signature set $S_{Addr} = \{s_1, \ldots, s_p\}$ for TA(S)/RA(S). A node can randomly select a signature $s_i (i = 1, 2, ..., p)$ from the set as its own signature, and put it in the TA(S) field when sending a RTS frame.

I then design a signature set $S_{EXT} = \{S_{m\times n}, s_{ACK}\}$ for EXT(S), where s_{ACK} is a unique signature specially used to differentiate the CTS and ACK frames. With the s_{ACK}, the node, such as $S3$ in Fig. 3.3, will not misinterpret the $R1$'s ACK feedback as a CTS frame when a collision occurs. I use a matrix $S_{m\times n}$ to represent the combination of the NAV time and interference range:

$$\mathbf{S_{m\times n}} = \begin{pmatrix} s_{11} & s_{12} & \ldots & s_{1n} \\ s_{21} & s_{22} & \ldots & s_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m1} & s_{m2} & \ldots & s_{mn} \end{pmatrix},$$

where s_{ij} is a signature, the NAV indicator i represents a data transmission time, and the IR indicator j represents an interference range. Here, m and n denote the maximal values of i and j, respectively.

I next illustrate the design of the NAV indicator and IR indicator in detail. To simplify the description of the system, we assume that all the frames are transmitted at the same rate v_b, the corresponding transmission range as $d_{TX}(v_b)$, and the corresponding SINR threshold as $\beta_{SINR}(v_b)$, respectively.

[1]Though we can use two different signatures to carry both information, we use one EXT(S) signature here to reduce the introduced transmission overhead of signatures.

3.3.1.1 NAV Indicator Design

I design a set of signatures to represent different transmission durations (the NAV time). As the length of MPDUs cannot exceed a threshold l_{max} according to the 802.11 standard, the MPDU transmission time is upper-bounded by $l_{max} \cdot 8/v_b$. We define the maximum data frame transmission time as $t_{max} = l_{max} \cdot 8/v_b + t_{PHY}$, where t_{PHY} is a constant time for transmitting the preamble. We divide t_{max} into m segments, each of which lasts for $L_{NAV} = \lceil \frac{t_{max}}{m} \rceil$. Therefore, each NAV time t_{NAV} can be mapped to a specific NAV indicator $i = round(\frac{t_{NAV}}{L_{NAV}})$.

3.3.1.2 IR Indicator Design

The IR indicator j represents the interference range of a receiver of the ongoing transmission link, with which each node around the receiver can make a proper decision about whether its transmission will interfere with the ongoing transmission link.

In this thesis, I use the two-ray ground propagation model [61], which is widely adopted in wireless network research studies (such as [32, 89]) as well as the network simulators (such as ns-2 [55]). Based on this model, the receiving power P_r of a signal is inversely proportional to the distance d between the transmitter and receiver, i.e., $P_r = P_t G_t G_r \frac{h_t^2 h_r^2}{d^\alpha}$, where P_t is the transmission power, G_t and G_r are antenna gains of the transmitter and receiver respectively, h_t and h_r are the heights of both antennas, α is a factor larger than 2 and reflects the attenuation degree of the signal. Here, we assume all the nodes in the network are homogeneous, i.e., all the radio parameters are the same at each node, all the antenna heights are the same, and all the nodes have the same fixed transmission power P_t. Thus, we can simplify the equation to calculate P_r as $P_r = c\frac{P_t}{d^\alpha}$,

where c is a constant. We also assume the radio channel is symmetric, i.e., the signal has the same propagation attenuation in both directions. Here we should admit that if the assumptions do not hold, the calculated interference range in the following parts may be deviated from the real one, thus either leading to collisions or losing some concurrent transmission opportunities, both of which will pull down IRMA's performance.

If a node receives a RTS frame, the receiving power P_r is obtained. The node first uses P_r to compute its distance d from the sender. Then, according to the physical interference model, it computes the interference range d_{IR} of this transmission link using the formula below:

$$SINR = \frac{c\frac{P_t}{d^\alpha}}{c\frac{P_t}{d_{IR}^\alpha} + P_I + P_N} \geq \beta_{SINR}(v_b),$$

where P_I indicates the cumulated interference power from other concurrent transmissions, P_N is the thermal noise power and it can be ignored. Suppose P_I is negligible comparing with $c\frac{P_t}{d_{IR}^\alpha}$, we have:

$$SINR \approx \frac{c\frac{P_t}{d^\alpha}}{c\frac{P_t}{d_{IR}^\alpha}} = (\frac{d_{IR}}{d})^\alpha \geq \beta_{SINR}(v_b),$$

which means only nodes that are at least $d_{IR} = d \cdot \sqrt[\alpha]{\beta_{SINR}(v_b)}$ away from the receiver are permitted to transmit concurrently. Note that the threshold $\beta_{SINR}(v_b)$ is related to the data rate v_b. Generally, the transmission link with higher v_b has a larger interference range.

Once v_b is determined, the transmission range $d_{TX}(v_b)$ is also fixed[2]. Then, the maximum interference range is

$$d_{IR\_max} = d_{TX}(v_b) \cdot \sqrt[\alpha]{\beta_{SINR}(v_b)}. \tag{3.1}$$

[2]The transmission range d_{TX} is related to the transmission power P_t and the receiver's sensitivity P_{RXthd}. It can be calculated through $P_{RXthd} = c \cdot \frac{P_t}{d_{TX}^\alpha}$, that is, $d_{TX} = \sqrt[\alpha]{\frac{c \cdot P_t}{P_{RXthd}}}$.

We divide d_{IR_max} into n segments, each of which has a length $L_{IR} = \lceil \frac{d_{IR\_max}}{n} \rceil$, then each interference range d_{IR} can be mapped to a specific IR indicator $j = \lceil \frac{d_{IR}}{L_{IR}} \rceil$.

It is noted that in certain real scenarios, the real interference range may be larger than the calculated d_{IR}, which is $d \cdot \sqrt[\alpha]{\beta_{SINR}(v_b)}$, due to multiple nodes' concurrent transmissions (P_I is not negligible). This problem can be partially mitigated since the interference range information carried by j is generally larger than d_{IR}. Moreover, the problem can also be mitigated by using a higher $\beta_{SINR}(v_b)$ when calculating d_{IR}, which makes the transmitter convey a larger interference range information in the CTS. The value of $\beta_{SINR}(v_b)$ that can maximize the performance should be determined by the real network scenarios.

3.3.2 Signature Attachment

Fig. 3.2 shows that when a transmitter/receiver intends to transmit a control frame RTS/CTS/ACK, it will generate specific signatures and put them in the corresponding fields according to the format of these frames shown in Fig. 3.4.

When a transmitter intends to send a RTS frame for initiating a transmission, it randomly selects a signature from the signature set S_{Addr} as the TA(S), trying to make the signature unique in the vicinity of the transmitter/reciever each time.

Upon receiving a RTS frame, a node first checks if it is the designated receiver. If the node is the designated receiver, it will generate a CTS frame with required signatures. It fills the RA(S) field of the CTS frame with the TA(S) that is directly obtained from the received RTS frame.

For the EXT(S) field of the CTS frame, the node first calculates its NAV time t_{NAV}

according to the NAV time set in the RTS frame, by subtracting the SIFS and the transmission time of the CTS frame. It then calculates L_{NAV} to be $\lceil \frac{t_{max}}{m} \rceil$. The resultant time duration is mapped to a NAV indicator $i = \lceil \frac{t_{NAV}}{L_{NAV}} \rceil$. The node also calculates the interference range d_{IR} through the receiving power of the RTS frame and v_b, then maps d_{IR} to an IR indicator $j = \lceil \frac{d_{IR}}{L_{IR}} \rceil$. The signature s_{ij} of $S_{m \times n}$ is put in the EXT(S) field. The node finally replies this CTS frame to the transmitter.

Similarly, when the node intends to reply an ACK frame after a successful data reception, besides the RA(S) field, it puts the s_{ACK} signature in the EXT(S) field and then broadcasts it.

3.3.3 Signature Detection Method

Since signatures that carry useful information are attached in control frames when they are transmitted, nodes can use the SDM to discern these signatures from incoming control frame's samples and recover the original information.

Note that the process of discerning signatures is based on the cross correlation technology, which has already been described as a preliminary of this thesis in Section 2.6. When conducting cross correlation between the incoming signal and a known signature, one node can determine the presence or absence of this signature in the received signal according to whether the correlation result is above or below a threshold β_{Corr}.

We construct two signature sets S_{Addr} and S_{EXT}, containing p and $m \times n+1$ signatures, respectively. To illustrate the SDM in general, we assume the number of signatures in a signature set is l. The SDM first discerns which signature can be found in the incoming samples. As shown in Fig. 3.5, the cross correlation is conducted between the incoming

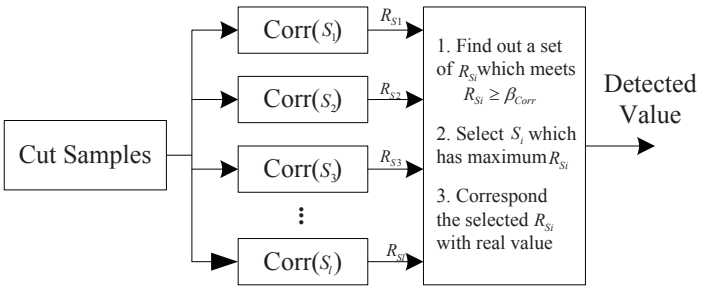


Figure 3.5: The signature detection method that discerns a known signature s_i from the incoming samples and recovers the original information. The signature set here is $\{s_1 \ldots s_l\}$.

samples and each of the l known signatures, the outputs of l correlation values $R_{s_1}, \ldots, R_{s_l}$ are compared with the threshold β_{Corr}. We select the s_i which has the maximum value R_{s_i} among those ones that exceed β_{Corr}. Fig. 3.6 demonstrates an example of SDM in which l equals to 16. Although both R_{s_5} and R_{s_8} are over the threshold β_{Corr}, we decide s_5, whose correlation result is maximum, is in the received signal. This method can largely mitigate the false positive error rate in the detection process.

As all the signatures have their fixed positions after the preamble field in the control frames, as shown in Fig. 3.4, nodes can easily obtain the positions of signatures by offsetting the fixed number of samples after the position of the preamble is determined. Thus, the SDM only needs to cross-correlate the "cut samples" (i.e., the fixed-length samples at certain positions) of the incoming signal with the known signatures. This mechanism makes the computational complexity of the SDM in the order of the size of the signature set.

For the TA(S), since IRMA does not permit the RTS frame to be collided at the receiver, TA(S) can be easily decoded by the receiver.

For the detection of the RA(S), the correlation process should just be performed one

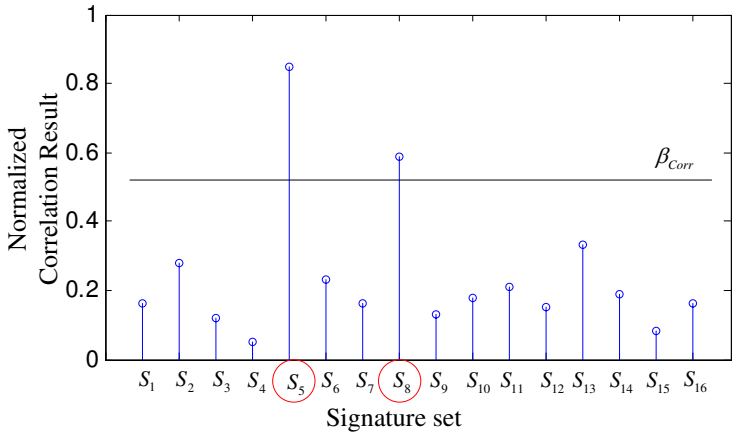


Figure 3.6: An example of the signature detection method.

time between the incoming cut samples at the RA(S) field and its own signature. The node simply determines itself to be the designated receiver of the frame if the correlation value exceeds β_{Corr}.

For the detection of the EXT(S), the node should perform the correlation process $m \times n + 1$ times between the incoming cut samples at the EXT(S) field and each signature in S_{EXT}. If the discerned signature is s_{ACK}, the node determines the received frame to be an ACK. If the signature is a signature s_{ij} of $S_{m \times n}$, the node determines the received frame to be a CTS, then calculates L_{NAV} to be $\lceil \frac{t_{max}}{m} \rceil$ and converts the NAV time to be $i \cdot L_{NAV}$, finally calculates the L_{IR} to be $\lceil \frac{d_{IR\_max}}{n} \rceil$ and converts the interference range to be $j \cdot L_{IR}$.

3.3.4 Channel Access Scheme

IRMA disables the physical carrier sense and only relies on the NAV state, which is set by the virtual carrier sense, to avoid the interference caused by data transmissions. When a node intends to send a data frame, it just checks the NAV state, and initiates a

RTS transmission after the NAV state becomes zero. It will not check if the channel is confirmed idle or not any more. Meanwhile, when a node receives a RTS and detects the frame correctly, it should also check the NAV state, and respond a CTS after SIFS if the NAV state is zero.

The NAV state in IRMA is merely updated by the NAV or EXT(S) field in the CTS frame, which is different from the mechanism used in the 802.11 standard, where the NAV state is updated by the NAV field in either the RTS or CTS frame. Since IRMA permits concurrent transmissions at the transmitter side, the NAV field in the RTS frame is not used to update the NAV state. It is also conditional in IRMA to use the detected NAV or EXT(S) value in the CTS frame to update the NAV state, as it may make nodes miss transmission opportunities. As shown in Fig. 3.3, when $R1$ replies a CTS to $S1$, $S2$ also detects the EXT(S) correctly. As $S2$ does not interfere with $R1$'s data reception, it will miss a transmission opportunity if its NAV state is updated by the EXT(S) field of the received CTS. To make a proper channel access decision, we propose the following differentiated NAV state update scheme to solve this problem.

3.3.5 Differentiated NAV State Update

In this scheme, upon receiving a CTS frame, nodes that are in the interference range of the ongoing transmission link should update their NAV states, while other nodes do not update the NAV states so that they do not waste transmission opportunities.

When the EXT(S) field in the CTS frame is detected to be s_{ij}, the interference range is determined to be $j \cdot L_{IR}$. We use a threshold β_{rCTS} to represent the signal strength at a position which is d_{IR} away from the CTS transmitter, that is, $\beta_{rCTS} = c\frac{P_t}{d_{IR}^{\alpha}}$. By

comparing the signal strength of the received CTS frame with β_{rCTS}, a node can decide whether its concurrent transmission would interfere with the ongoing transmission link or not. The signal strength of the CTS frame in the presence of an interference can be obtained through an easy way: As a sharp change appears in the amplitude variation of the received signal when a new frame arrives [20], together with the signal strength before and after the sharp change, we can determine what the frame's power level is.

For the scenario shown in Fig. 3.3, both $S1$ and $S3$ can receive the CTS from $R2$, but the signal strength of this frame is above β_{rCTS} at $S3$, and below β_{rCTS} at $S1$. Thus, $S3$ concludes that it should update its NAV state, while $S1$ would not yet.

The NAV state of each node can be updated by the control information carried in a CTS frame in two different ways: It can be updated by the NAV field of the frame at the MAC layer; it can also be updated by the EXT(S) field of the frame at the physical layer. As the NAV field carries more precise NAV time information than the EXT(S) field, the former has a higher priority in the NAV state update process. If the frame can be correctly decoded at the MAC layer, the node's NAV state will be updated by the decoded NAV value; otherwise, it will be updated by the NAV time determined by the EXT(S) field, that is, $i \cdot L_{NAV}$, where s_{ij} is the discerned signature in the EXT(S) field, and $L_{NAV} = \lceil \frac{t_{max}}{m} \rceil$.

3.3.6 Signature Detection Range Analysis

IRMA prohibits nodes that are within the interference range but outside the transmission range of the ongoing link from transmitting data, so as to avoid collisions, as shown in Fig. 3.1(c). Thus, nodes within the interference range d_{IR} should have the ability to

detect the CTS frame correctly to keep silent. In this part, I will give the theoretical analysis about it.

To simplify the analysis, we define the signature detection range d_S as the maximum range within which signatures can be detected correctly. Here I first formulate d_S, then compare it with the maximum interference range d_{IR_max}, which has been discussed in Section 3.3.1.2.

According to the physical interference model, a data frame can be detected correctly if the SINR of the received signal power is above a threshold β_{SINR}, that is:

$$SINR = \frac{P_r(data)}{P_I^1 + P_N} = \frac{c\frac{P_t}{d^\alpha}}{P_I^1 + P_N} \geq \beta_{SINR},$$

where P_I^1 indicates the cumulated interference power at the data frame's receiver side. When $d = d_{TX}$, we set $SINR = \beta_{SINR}$, then we have:

$$d_{TX} = \sqrt[\alpha]{\frac{c \cdot P_t}{(P_I^1 + P_N) \cdot \beta_{SINR}}}. \tag{3.2}$$

We define the signature detection threshold β_{SINR_S} as the threshold that, a signature can be detected correctly through SDM if its SINR is above β_{SINR_S}, that is:

$$SINR = \frac{P_r(signature)}{P_I^2 + P_N} = \frac{c\frac{P_t}{d^\alpha}}{P_I^2 + P_N} \geq \beta_{SINR\_S},$$

where P_I^2 indicates the cumulated interference power at the signature's receiver side. When $d = d_S$, we set $SINR = \beta_{SINR\_S}$, then we have:

$$d_S = \sqrt[\alpha]{\frac{c \cdot P_t}{(P_I^2 + P_N) \cdot \beta_{SINR\_S}}}. \tag{3.3}$$

Suppose $P_I^1 = P_I^2$. Combining Ineq. (3.2) and Ineq. (3.3), we get:

$$d_S = \sqrt[\alpha]{\frac{\beta_{SINR}}{\beta_{SINR\_S}} \cdot \frac{P_I^1}{P_I^2}} \cdot d_{TX} = \sqrt[\alpha]{\frac{\beta_{SINR}}{\beta_{SINR\_S}}} \cdot d_{TX}. \tag{3.4}$$

According to the experiment results in Section 3.4, the signatures can be detected correctly with the probability of about 100% when the signature length is 160bits and the SINR is above -10dB, thus we set $\beta_{SINR\_S} = -10dB = 0.1$. Through Ineq. (3.1) and Ineq. (3.4), we get:

$$d_S = \sqrt[\alpha]{\frac{\beta_{SINR}}{0.1}} \cdot d_{TX} > \sqrt[\alpha]{\beta_{SINR}} \cdot d_{TX} = d_{IR\_max}.$$

Therefore, we can conclude that the signature detection range is always larger than the interference range, and the nodes within the interference range can detect the CTS frame correctly to keep silent. Note that P_I^1 may not equal to P_I^2 because of the different environments at the data frame's receiver side and the signature's receiver side in the real network, if $P_I^1 \gg P_I^2$ (e.g. , $P_I^1 > 10 \cdot P_I^2$), the signature detection range may be smaller than the interference range, leading to a collision to the ongoing link. However, we consider this case is rare since it does not appear in the simulations.

3.3.7 Address Conflict Analysis

Though each transmitter independently chooses its signature TA(S) from S_{Addr} each time when it transmits a RTS frame, it still has a small probability to pick up the same signature used by other nearby nodes, leading to a potential address conflict problem. Fortunately, this address conflict can be naturally resolved in our protocol due to the CTS timeout mechanism that has already been specified in 802.11 standard [24].

I illustrate this mechanism through a scenario shown in Fig. 3.7. Suppose $S2$ sends a RTS frame to $R2$ using a signature s_i in the TA(S) field, this RTS is collided at $R2$ with a data frame sent from $S3$, leading to no CTS feedback from $R2$ to $S2$. $S2$ will wait for the CTS feedback only for a CTS timeout interval, then it can initiate a retry if it fails to

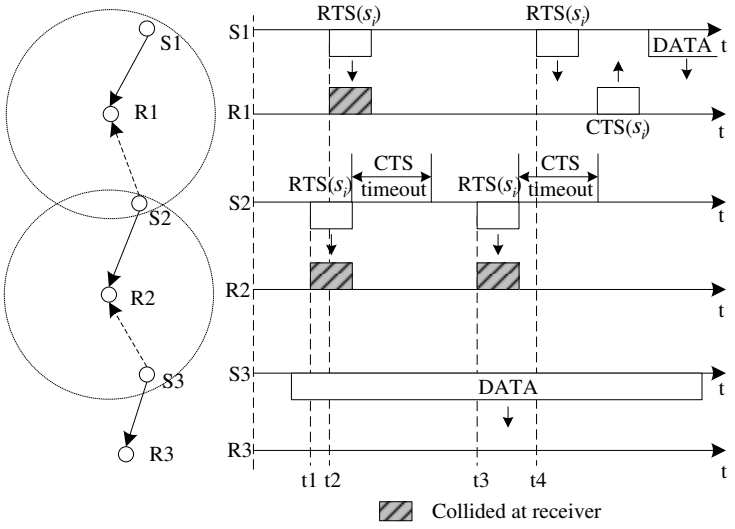


Figure 3.7: A potential address conflict scenario. The two circles indicate the transmission range of $R1$ and $R2$, respectively.

receive the CTS. The CTS timeout interval is always set to be SIFS plus the transmission time of CTS [24]. Suppose $S1$ intends to send a data frame to $R1$, and it also selects the same signature s_i in the TA(S) field of the corresponding RTS frame. However, $S2$ will not misinterpret $R1$'s CTS as its own feedback although this CTS's RA(S) field has the same value s_i as the one used in $S2$'s RTS. We consider there are two possible situations in this scenario. The first one is that both RTS frames are collided. As shown in Fig. 3.7, when $S2$ sends a RTS at $t1$, and $S1$ sends a RTS at $t2$, there is no CTS feedback as the two RTS frames are both collided. The second situation is that $S2$ experiences a CTS timeout before receiving a CTS frame. As shown in Fig. 3.7, when $S2$ initiates a retry and sends a RTS at $t3$, and $S1$ sends a RTS at $t4$, $S2$ will not misinterpret $R1$'s CTS as its own feedback as this CTS is not within its CTS timeout interval. $S1$ then transmits its data frame after receiving the CTS, without any collision at $R1$.

Meanwhile, since the medium has been reserved by the RTS/CTS handshake before

an actual data transmission, no conflict will appear in the ACK frame transmission.

3.4 Experiment Evaluation

In this section, I evaluate the feasibility of using the SDM to detect control frames' signatures in the presence of interference through hardware experiments.

3.4.1 Experiment Setup

The experiments are conducted with Universal Software Radio Peripheral 2 (USRP2) platform [11] and use the GNURadio [16] for the signal processing blocks. USRP2 is a RF front-end that converts the baseband digital samples into analog waves centered at a specific carrier frequency according to the configured RF daughter-board. It can also down-convert the RF signal into digital samples in the receiving process. In the experiments we use the RXF2400 daughter-board, which makes each USRP2 operate at about 2.4GHz. GNURadio is an open-source software development toolkit that provides signal processing blocks to implement software radios. The physical layer modulation and demodulation processes are divided into modules and implemented by GNURadio blocks, which are connected using Python files to complete the signal process. We implement IRMA on an 8-node USRP2 testbed and the topology is randomly set up in our labs. Each node is a USRP2 connected to a commodity PC that configured GNU Radio, and each USRP2 operates at 2.4GHz with a sample rate of 2M samples/sec. We choose DBPSK as the modulation method in the experiment.

A real time performance evaluation based on USRPs is difficult because of the hardware delays in obtaining samples from the RF front-end to the connected PC, and also

the artificial software delays induced by GNU Radio. Therefore, we also resort to trace-based evaluation that is used in [17, 49, 63, 88]. Each node saves all the incoming samples for off-line processing.

For each experiment, we pick up four nodes to form two links, each of which has a sender and a receiver. The two selected senders should be exposed terminals and IRMA permits their concurrent transmissions, so as to generate control frame collisions at the sender side. Different SINR environments are tested for SDM by adjusting the transmission power of one sender and fixing that of the other.

Similar to CSMA/CN [63], we also use two metrics, the false negative error rate and false positive error rate, to measure the performance of SDM in this part. The difference from CSMA/CN is that, we focus on designing the signature set that will be used in this protocol. Thus, we need to strike a balance among the ability of combating interferences, the signature length and the size of signature set through this experiment.

3.4.2 Threshold β_{Corr}

The SDM determines if a known signature is found in the incoming samples by performing the cross correlation between the two signals. In the correlation process, the normalized correlation peak is always detected by comparing the peak value with a threshold β_{Corr}, as described in Section 2.6. A higher threshold $\beta_{Corr}(high)$ can lead to more false negative errors, and a lower threshold $\beta_{Corr}(low)$ can lead to more false positive errors. Both errors will make the CTS or ACK receivers get wrong information, leading to either collisions in data packet transmissions or failure to exploit concurrent transmissions, thus degrading the network throughput. To make a tradeoff between the two errors, we adjust

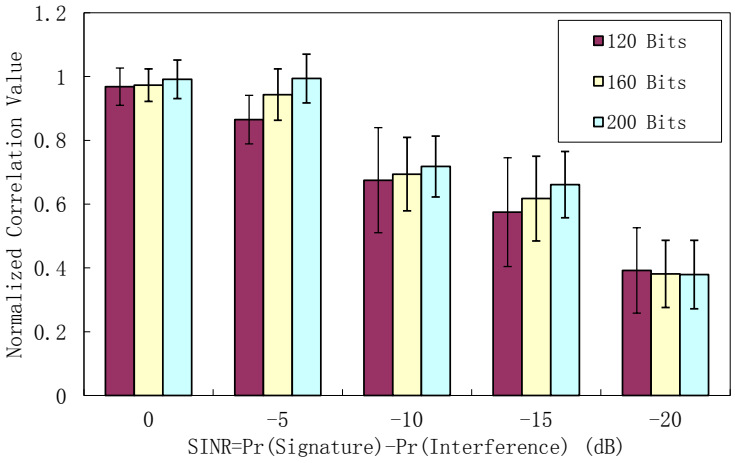


Figure 3.8: Normalized correlation value vs. SINR.

the threshold β_{Corr} of the normalized correlation process to be ψ, where ψ is set to be 0.55 in the experiment.

Empirically, the false negative error rate is closely related to L and SINR, as a shorter L or lower SINR would lead to a lower correlation peak. The false positive error rate is more affected by the Hamming distance between the signature and the correlated incoming samples, as a shorter distance would lead to a higher false correlation peak. In the experiment, we try to mitigate both error rates from the two aspects.

3.4.3 Signature Detection Evaluation

In this part, I quantify SDM's ability to detect signatures at the presence of strong interferences. I also demonstrate that the size of the signature set is large enough to meet the protocol's requirements. The experiment starts from mitigating the two errors in the correlation process.

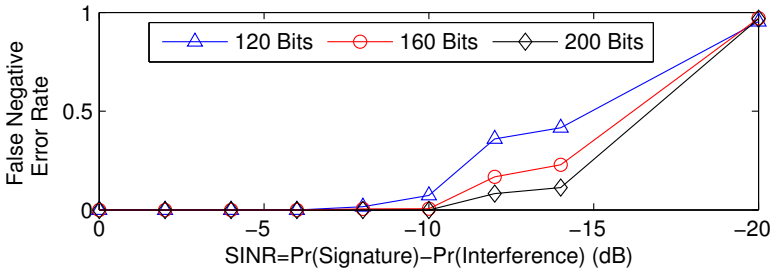


Figure 3.9: False negative error rate.

3.4.3.1 False Negative Error

In order to quantify how the false negative error can be affected by the signature length L and SINR, we test three sets of data with three signature lengths L under different SINR environments and channel conditions. For each L, we conduct the experiment for ten times in two places, and each time we select four different nodes from the testbed to form the two links. As shown in Fig. 3.8, the results clearly show that the correlation spike appears even under strong interferences where SINR is $-20dB$. The longer the signature is, the easier the signature is to be detected. Moreover, when both the SINR value and L are fixed, the correlation value has a variance in a certain range, which is induced by various channel environments. In the following parts, we will use the average correlation results to calculate the false negative and false positive error rates.

Fig. 3.9 demonstrates the false negative error of the three sets of data. The result shows that a longer signature (such as 200 bits) can have a lower false negative error under the same SINR, and the error decreases significantly when the SINR increases.

We use the SDM to detect signatures in the presence of interferences. The lower SINR the SDM can support, the more transmission opportunities the nodes can explore. Here we make a tradeoff between the SDM's detection ability and the signature length L. We

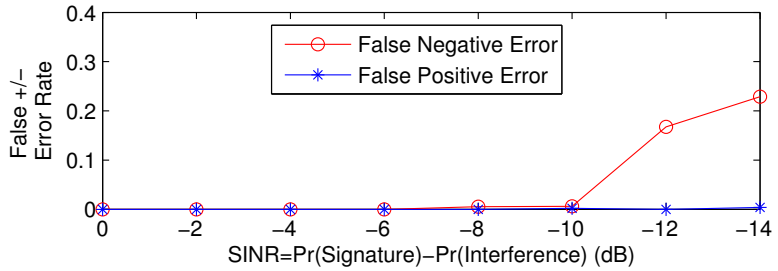


Figure 3.10: False positive/negative error rates for signatures with 160 bits.

set the minimum SINR that the SDM can support to be $-10dB$. To minimize the false positive error, we select the L to be 160 bits, then the error rate is below 0.3% when the SINR is above $-10dB$.

Note that when L is 160 bits and SINR is below $-10dB$, the false negative error rate is a little more than that was tested by CSMA/CN, that's because the correlation result has a wider fluctuation range when SINR is lower (as shown in Fig. 3.8), thus the calculated positive/negative error rates will be more affected by the channel characteristics in the experiment.

3.4.3.2 False Positive Error

Here we explore how to mitigate the false positive error in the correlation process. Fig. 3.10 shows both false positive error rate and false negative error rate when L is 160 bits. The result indicates that the SINR has almost no effect on the false positive error when the SINR is above $-14dB$, as there is enough Hamming distance between the signature and the correlated samples. As shown in Fig. 3.10, when the Hamming distance is 52, the false positive error rate is below 0.5% when the SINR is $-14dB$.

Table 3.1 shows the false positive error rates under various Hamming distances when the SINR is $-10dB$, which indicates that the false positive error rate decreases when the

Hamming distance increases.

Table 3.1: False positive error rates when SINR=$-10dB$.

Hamming distance	34	40	46	52
False positive error rate	0.170	0.047	0.008	0.002

When we set the signature length to be 160 bits and the minimum Hamming distance between any two signatures to be 52, the SDM can achieve a very low signature detection error rate (less than 1%) even when the SINR is $-10dB$. I use the pseudo-noise code in this thesis to accomplish the signature design. I have more than 200 signatures with 160 bits and the Hamming distance between any pairs of them is above 52.

3.5 Performance Evaluation

In this section I evaluate IRMA's throughput improvement in wireless networks compared with 802.11 standard and three recent protocols under two topology scenarios, a linear topology and a random topology. The two mechanisms of CSMA in the 802.11 standard that we choose to compare are (1) PCS, which uses the standard's physical carrier sense mechanism to access a wireless channel, (2) PCS+VCS, which uses both the physical and virtual carrier sense mechanisms to access a wireless channel. The three protocols we choose to compare are CMAP [78], SDN [32] and 802.11ec [49]. CMAP and SDN are two typical recent protocols that solve the exposed terminal problem, as described in Section 1, and 802.11ec is a recent protocol that exploits cross correlation to avoid collisions and improve the network throughput. I implement all the protocols in ns-2.

Table 5.1 lists the basic configuring parameters used in our simulation.

For IRMA, I do not implement the signature detection process in ns-2, but utilize the

Table 3.2: Simulation parameters.

Parameter	**Value**	**Parameter**	**Value**
Preamble	$20\mu s$	SIFS	$16\mu s$
Time slot	$9\mu s$	DIFS	$34\mu s$
Signature	$13.3\mu s$	CWmax	$1023\mu s$
p	20	CWmin	$15\mu s$
m	20	n	8

experiment results and the SINR of the received signal to determine whether the control frames can be detected or not. I implement it as follows: If $SINR > -5dB$, the signatures can be obtained correctly with the probability of 100%; if $-10dB < SINR \leq -5dB$, the probability is 99%; otherwise, if $SINR \leq -10dB$, the signatures will be ignored. Note that the strength of interference used to calculate the SINR is measured as the accumulated signal strengths from all other transmitting nodes, which has already been implemented by ns-2.

The aim of the simulations is to discover how each protocol can exploit concurrency and avoid collisions to improve the network performance in different transmission rates. Hence, I select three values of v_b defined in the 802.11a standard to evaluate the performance of each protocol in the two simulation scenarios, the corresponding transmission ranges $d_{TX}(v_b)$, carrier sense ranges $d_{CS}(v_b)$ and the SINR thresholds $\beta_{SINR}(v_b)$ are all listed in Table 3.3. I let the preamble in the physical layer be transmitted using basic modulation (BPSK), that means, the transmission rate for these fields are fixed to $6Mbits/s$, all the transmission rate of control frames and the data frames in the MAC layer will be changed to the configured rate.

Table 3.3: Three transmission rates selected in the simulation.

v_b	$d_{TX}(v_b)$	$d_{CS}(v_b)$	$\beta_{SINR}(v_b)$
$6Mbits/s$	$500m$	$600m$	$5.0dB$
$24Mbits/s$	$150m$	$600m$	$15.0dB$
$48Mbits/s$	$50m$	$600m$	$25.0dB$

3.5.1 Linear Topology

I first conduct the simulation under a four-node linear topology to evaluate the effectiveness of IRMA compared with the other five protocols and also their constraints. As shown in Fig. 3.11, the network contains two link pairs $S1 \rightarrow R1$ and $S2 \rightarrow R2$. The sender-receiver distances of both links $d_{link}(v_b)$ are fixed to $250m$, $80m$ and $30m$ when the transmission rate v_b is set to be $6Mbits/s$, $24Mbits/s$ and $48Mbits/s$, respectively. The distance between $S1$ and $S2$ is denoted by d, which will be varied from $50m$ to $700m$. Each link pair has a CBR (Constant Bit Rate) flow set up at the sender to be transmitted to the receiver. We evaluate the network throughput by adjusting the distance d. The packet delivery rate (flow rate) and packet length will also be changed in the simulation to get more detailed evaluation. Note that the packet length here means the length in the upper layer; obviously, the frame length should be a little longer as additional headers will be attached in the MAC layer and physical layer.

3.5.1.1 The impact of distance d

The IRMA protocol can exploit concurrent transmissions when there is no mutual interference in their data frame receptions, and can avoid collisions when mutual interferences exist. Therefore, we first evaluate the impact of the distance d in the following simulation. The simulation is conducted for three times, each with a different transmission rate

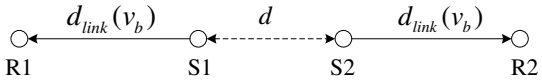


Figure 3.11: A linear topology, where four nodes $R1$, $S1$, $S2$ and $R2$ form a line. The distance between $S1$ and $R1$ as well as that between $S2$ and $R2$ are both set to $d_{link}(v_b)$. The distance between $S1$ and $S2$, denoted by d, is varied from $50m$ to $700m$.

listed in Table 3.3, according to which the sender-receiver distance $d_{link}(v_b)$ should also be adjusted. The packet length is fixed to 1500 bytes.

Fig. 3.12 shows the aggregate throughput of the network with three transmission rates. The simulation results can be summarized into six cases:

Case 1: Only one transmission is permitted by all protocols when the following conditions hold:

$$d < d_{link}(v_b) \cdot (\sqrt[k]{\beta_{SINR}(v_b)} - 1),$$

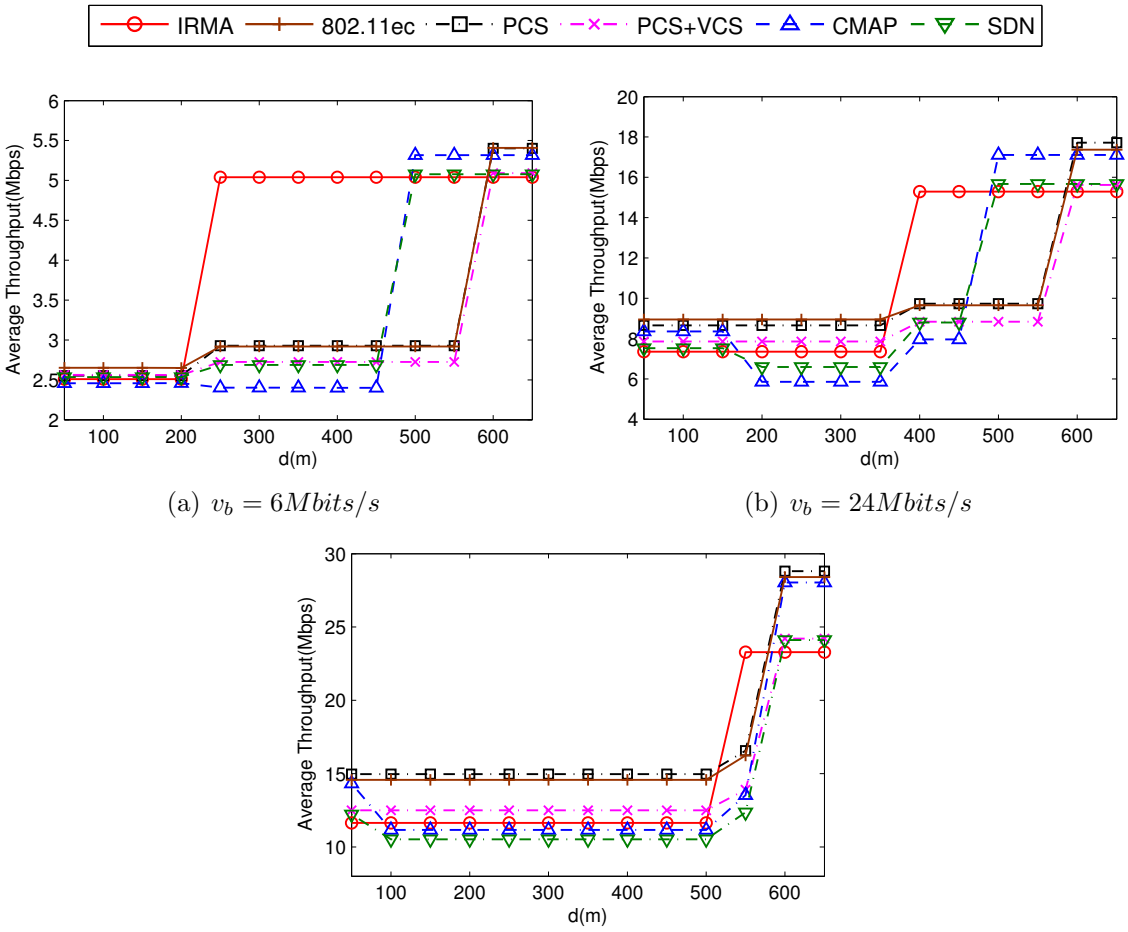
$$d \leq d_{TX}(v_b).$$

In this case, each sender is in the interference range of the other transmission link, and it is in the transmission range of the other sender, concurrent transmissions can be prohibited successfully by all protocols to avoid the interferences to the reception of the data frame, such as the scenario when $d \leq 250m$ in Fig. 3.12(a), the scenario when $d \leq 150m$ in Fig. 3.12(b) and the scenario when $d \leq 50m$ in Fig. 3.12(c).

Case 2: Only one transmission should be permitted but CMAP and SDN induce collisions when the following conditions hold:

$$d < d_{link}(v_b) \cdot (\sqrt[k]{\beta_{SINR}(v_b)} - 1),$$

$$d > d_{TX}(v_b).$$



(a) $v_b = 6Mbits/s$

(b) $v_b = 24Mbits/s$

(c) $v_b = 48Mbits/s$

Figure 3.12: Average throughput in terms of d under three transmission rates in the linear topology.

In this case, each sender is in the interference range of the other transmission link and concurrency should be prohibited. As each sender is out of the transmission range of the other sender, it cannot decode the packets from the other link correctly. IRMA and 802.11ec can avoid collisions successfully as the CTS information , which is carried by signatures in IRMA and by primitives in 802.1ec, can be obtained correctly in very low SINR environment. PCS and PCS+VCS can also avoid collisions through physical carrier sense. However, as both CMAP and SDN disable physical carrier sense, when a sender

cannot detect the packets from the other transmission link correctly, it will decide there is no conflict and initiate transmissions, leading to mutual interferences. The corresponding scenarios are $200 \leq d \leq 350m$ in Fig. 3.12(b) and $100 \leq d \leq 500m$ in Fig. 3.12(c).

Case 3: Concurrent transmissions are permitted by IRMA and CMAP but prohibited by other protocols when both the following conditions hold:

$$d_{link}(v_b) \cdot (\sqrt[k]{\beta_{SINR}(v_b)} - 1) < d < d_{link}(v_b) \cdot (\sqrt[k]{\beta_{SINR}(v_b)}),$$

$$d < d_{TX}(v_b).$$

As the two transmission links have no mutual interferences to their data frame receptions, both IRMA and CMAP can exploit concurrent transmissions under this case, such as the scenarios when $250 \leq d \leq 400m$ in Fig. 3.12(a). However, the performance of CMAP in this scenario is even lower than that in Case 1, because of spurious retransmissions due to ACK collisions. Although CMAP design a windowed-ACK mechanism to reduce the ACK collisions, and this mechanism really can increase the throughput from about $1.6Mbits/s$ to about $2.4Mbits/s$, it cannot reach the approximately $2\times$ performance improvement as IRMA. For the other protocols, PCS, PCS+VCS and 802.11ec can only permit one link's transmission as the sender will determine the channel to be busy after physical carrier sense; SDN also only permit one link's transmission to avoid control frame collisions at the transmitter side.

Case 4: Concurrent transmissions are permitted by IRMA, CMAP and SDN but prohibited by other protocols when both the following conditions hold:

$$d_{link}(v_b) \cdot (\sqrt[k]{\beta_{SINR}(v_b)} - 1) < d < d_{link}(v_b) \cdot (\sqrt[k]{\beta_{SINR}(v_b)}),$$

$$d_{TX}(v_b) < d < d_{CS}(v_b).$$

In this case, IRMA can exploit concurrency as each sender is out of the interference range of the other link. However, CMAP and SDN permit concurrency just because one node cannot correctly decode the packets from the other link and determine there is no conflict, such as the scenario of $400m \leq d \leq 500m$ in Fig. 3.12(b) and $d = 550m$ in Fig. 3.12(c). The performance of these two protocols in this case is lower than that of IRMA as both protocols face control frame collisions. PCS, PCS+VCS and 802.11ec also can only permit one link's transmission due to physical carrier sense.

Case 5: Concurrent transmissions are exploited by IRMA, CMAP and SDN successfully but prohibited by other protocols when both the following conditions hold:

$$d > d_{link}(v_b) \cdot (\sqrt[k]{\beta_{SINR}(v_b)}),$$

$$d < d_{CS}(v_b).$$

In this case, IRMA, CMAP and SDN can exploit concurrency as there is no mutual interferences for both data frame and control frame receptions, such as the scenario of $500 \leq d < 600m$ in Fig. 3.12(a) and Fig. 3.12(b). The performance of CMAP is a little higher than IRMA and SDN because of no overhead in transmitting RTS and CTS frames. PCS, PCS+VCS and 802.11ec can only permit one link's transmission due to physical carrier sense.

Case 6: Two links can transmit independently when the following condition holds:

$$d > d_{CS}(v_b).$$

In this case, the two transmission links are independent from each other. They can transmit simultaneously without any interferences.

We should note that Fig. 3.12 just shows the throughput of this scenario when the sender-receiver distance d_{link} is about one-half of the transmission range $d_{TX}(v_b)$ in each transmission rate. Obviously, if d_{link} is set to be a smaller value, concurrent transmissions can be exploited in a larger area because of the shorter interference range.

3.5.1.2 The impact of transmission rates

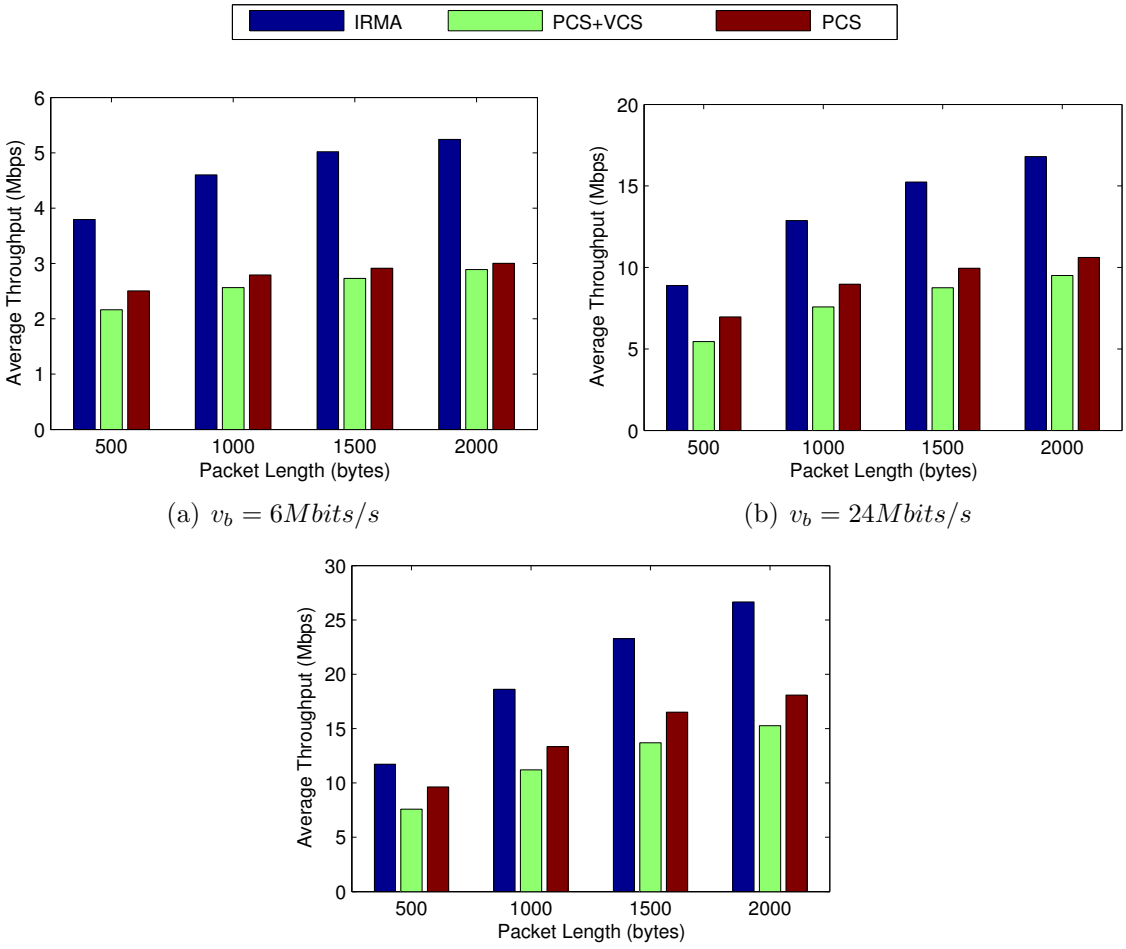
As the interference range of a transmission link with distance $d_{link}(v_b)$ can be calculated as $d > d_{link}(v_b) \cdot (\sqrt[k]{\beta_{SINR}(v_b)})$, a higher transmission rate that corresponds to a higher β_{SINR} value may lead to a larger interference range. Thus, the situation of the interference range larger than the transmission range (as described in Fig. 3.1(c)) will more easily occur at a higher transmission rate. For example, it will happen even when $d_{link}(v_b) = 3m$ and $v_b = 48Mbits/s$. CMAP and SDN are more vulnerable to this situation, leading to a performance degradation due to collisions. On the contrary, IRMA and 802.11ec can combat this problem successfully as their CTS and ACK information can be detected in very low SINR environments. PCS and VCS+PCS can also partially handle this problem as the carrier sense range is always much larger than the transmission range, collisions may be avoided due to the physical carrier sense mechanism.

Meanwhile, I should admit that the throughput improvement of IRMA decreases along with the increases of the transmission rate. As shown in Fig. 3.12(c), when the rate is $48Mbits/s$, the performance improvement of IRMA is significantly lower than twice over PCS or PCS+VCS due to the reason that the overhead induced by signatures is much larger in a higher transmission rate.

3.5.1.3 The Impact of Signatures

IRMA adds signatures in the control frames to convey the information that can be detected when a collision occurs, as shown in Fig. 3.4. Introducing the signatures into control frames will cause throughput degradation. To evaluate the overhead induced by signatures, we conduct three simulations with three transmission rates shown in Table 3.3, and the packet lengths are 500, 1000, 1500 and 2000$bytes$, respectively. We set the distance d to a specific value so that the conditions of Case 2 or Case 3 can hold. Under these conditions, the throughput gain of IRMA can theoretically be up to twice over PCS+VCS as concurrent transmissions of two links are exploited. However, IRMA's throughput cannot reach the expected value due to the overhead induced by transmitting signatures. The simulation results are shown in Fig. 3.13.

Fig. 3.13 indicates that the throughput gain of IRMA over 802.11 standard decreases while the transmission rate increases. For example, when the packet length is 2000$bytes$, the throughput gain is about twice when the data rate is $6Mbits/s$, but this value decreases to 74% when the data rate is $24Mbits/s$, and decreases to 47% when the data rate is $48Mbits/s$. Fig. 3.13 also indicates that the throughput gain increases along with increases of the packet length. For example, when the transmission rate is $6Mbits/s$, the throughput gain is about 51% when the packet length is 500$bytes$, much lower than that of 100% when the packet length is 2000$bytes$. That is because the time proportion in transmitting the control frames increases with the data rate, and decreases with the packet length.



(a) $v_b = 6Mbits/s$

(b) $v_b = 24Mbits/s$

(c) $v_b = 48Mbits/s$

Figure 3.13: Average throughput in terms of packet length under three transmission rates in the linear topology. Concurrent transmissions are exploited in this scenario.

3.5.1.4 Constrains of protocols

IRMA, SDN and CMAP will have no throughput improvement in a sparse network where there is no exposed terminal problem and no additional concurrent transmission can be exploited. In Fig. 3.11, when the distance d is larger (such as $700m$) and the two links have no mutual interference, PCS can have the best performance among all protocols due to the overhead induced by transmitting control frames in other protocols. We should

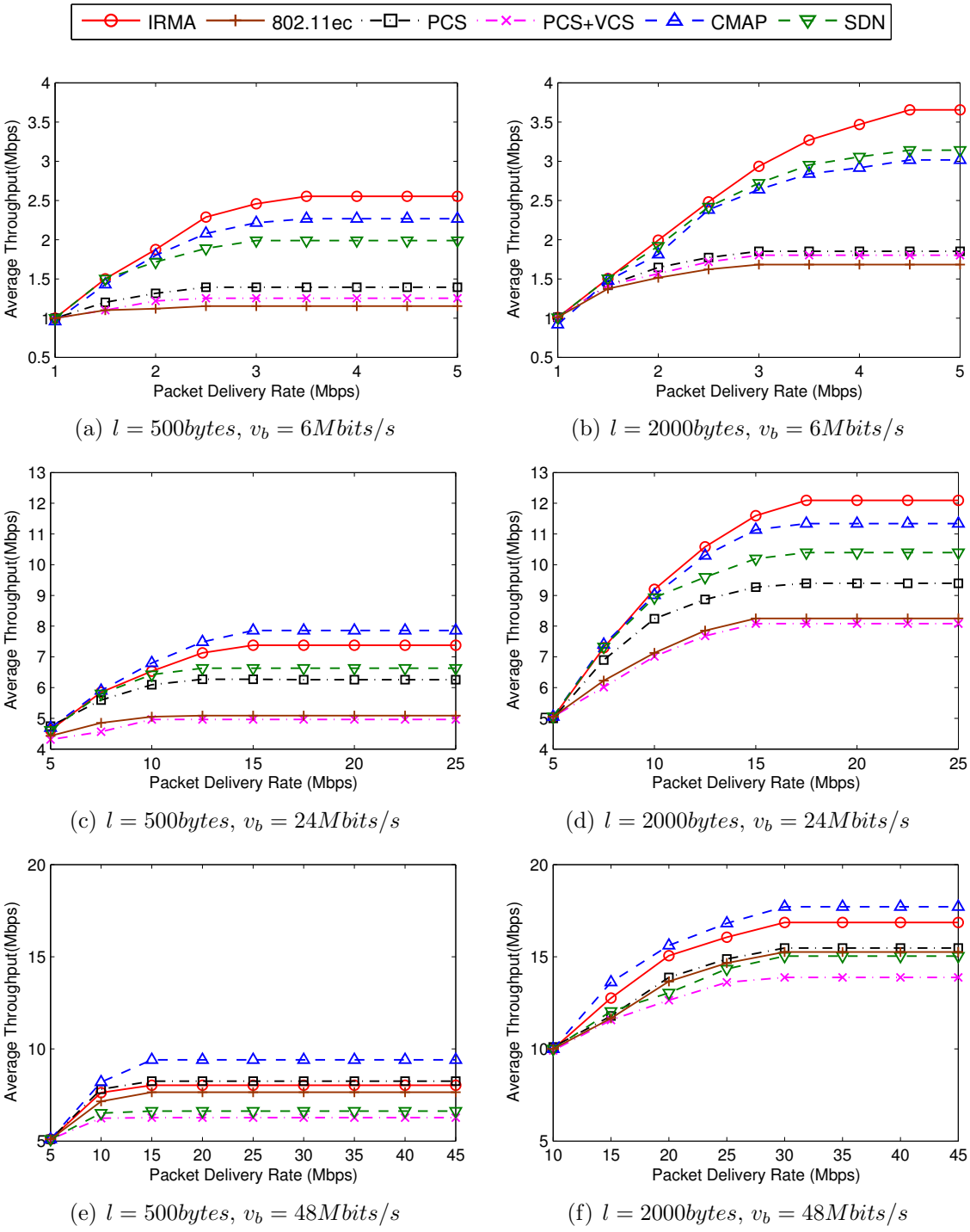
admit that IRMA has the lowest performance in this scenario because of the overhead induce by signatures. The simulation results indicate that IRMA, SDN and CMAP are not suitable for sparse networks, where they will even reduce the network throughput.

802.11ec can tolerate control frame collisions and reduce the duration of the control frame transmissions, but it cannot exploit concurrent transmissions. Furthermore, comparing with PCS and PCS+VCS, more concurrent transmissions will be prohibited by this protocol due to the high detection ability of the CTS primitive. Thus, 802.11ec is not suitable for intensive networks.

3.5.2 Random Topology

In this experiment I evaluate the performance of IRMA compared with other protocols in a general scenario where the network topology is randomly generated. I set up 10 transmitter-receiver link pairs in a $1000m \times 1000m$ area for three times to derive three configurations. For each configuration, nodes will use one transmission rate v_b listed in Table 3.3 to transmit packets. To set up the 10 link pairs, I first randomly generate one link (two nodes) in the area, calculate their distance and compare with the transmission range $d_{TX}(v_b)$, the link will be reserved if the distance is shorter than $d_{TX}(v_b)$; otherwise, it will be dropped. This process will be repeated for 10 times to generate 10 links in the network.

Fig. 3.14 shows the average throughput of IRMA comparing with the other five protocols for different packet delivery rates when the packet length is $500bytes$ and $2000bytes$, respectively. The figure indicates that the average throughput of all protocols increases along with the increases of the packet delivery rate and packet length, and the throughput



(a) $l = 500bytes$, $v_b = 6Mbits/s$

(b) $l = 2000bytes$, $v_b = 6Mbits/s$

(c) $l = 500bytes$, $v_b = 24Mbits/s$

(d) $l = 2000bytes$, $v_b = 24Mbits/s$

(e) $l = 500bytes$, $v_b = 48Mbits/s$

(f) $l = 2000bytes$, $v_b = 48Mbits/s$

Figure 3.14: Average throughput in terms of packet delivery rate in the random topology, under three transmission rates and two packet lengths.

is always up-bounded when the packet delivery rate reaches a specific value.

Fig. 3.14 also shows that PCS+VCS has the lowest performance in all the configurations, even comparing with the PCS protocol. The reason is that the hidden terminal problem is not so serious in dense networks, where PCS can avoid collisions in most cases through the physical carrier sense. 802.11ec also has low performance especially at a lower transmission rate, because, although it can tolerate control frame collisions and reduce transmission durations of control frames, it may prohibit more concurrent transmissions even comparing with PCS and PCS+VCS due to the high detection ability of the CTS primitive.

We can see that IRMA, CMAP and SDN can improve the network performance through exploiting concurrent transmissions comparing with both PCS and PCS+VCS, and IRMA can outperform other protocols in most cases, but the throughput gain decreases along with the increase of transmission rate and increases along with the increase of packet length. As shown in Figs. 3.14(a) and 3.14(d), when the transmission rate is $6Mbits/s$, IRMA's throughput gain is about 83% over PCS and 103% over PCS+VCS when the packet length is $500bytes$. These values increase to 98% and 112% respectively when the packet length is $2000bytes$. When the transmission rate increases to $24Mbits/s$, as shown in Figs. 3.14(b) and 3.14(e), the throughput gain decreases to about 17.9% over PCS and 48.7% over PCS+VCS when the packet length is $500bytes$, and about 31.5% over PCS and 50.7% over PCS+VCS when the packet length is $2000bytes$. We can also see from Figs. 3.14(b) that CMAP can even outperform IRMA a little at this situation. The reason is that the overhead induced by signatures in IRMA is much larger when shorter packet lengths and higher transmission rates are configured.

According to the analysis in Section 3.3.1.2, the interference range is more likely larger than the transmission range at a higher transmission rate scenario because of the higher SINR threshold, making CMAP and SDN face a high probability of collisions. In this random topology scenario, when the transmission rate increases to $48Mbits/s$, the throughput gain of SDN really decreases, but that of CMAP surprisingly increases on the contrary, as shown in Figs. 3.14(c) and 3.14(f). After analyzing the throughput of each link, we find that CMAP faces a more serious unfairness issue in this scenario, even comparing with PCS and PCS+VCS. Fig. 3.15 shows a snapshot of the throughput of ten links for each protocol when the transmission rate is $48Mbits/s$ and the packet length is $2000bytes$. We see that CMAP makes five links have very high throughputs and three links have close-to-zero throughputs. This unfairness situation largely avoids collisions in the network, and allows the network to achieve a higher average throughput. We also see from Fig. 3.15 that IRMA, SDN and 802.11ec are relative fair among all the links.

Generally speaking, IRMA can outperform the other protocols in most cases, as concurrent transmissions exploited by this protocol lead to significant performance improvement, despite the overhead induced by signatures and control frames. Meanwhile, IRMA has a high fairness performance as it can avoid collisions successfully.

3.6 Summary

In this chapter, I observe that nodes in the 802.11 standard degrade the network performance because of two problems. Based on analyzing the two problems, I identify that nodes waste transmission opportunities in two scenarios and induce collisions in one scenario, and then propose IRMA to exploit transmission concurrency and avoid inter-

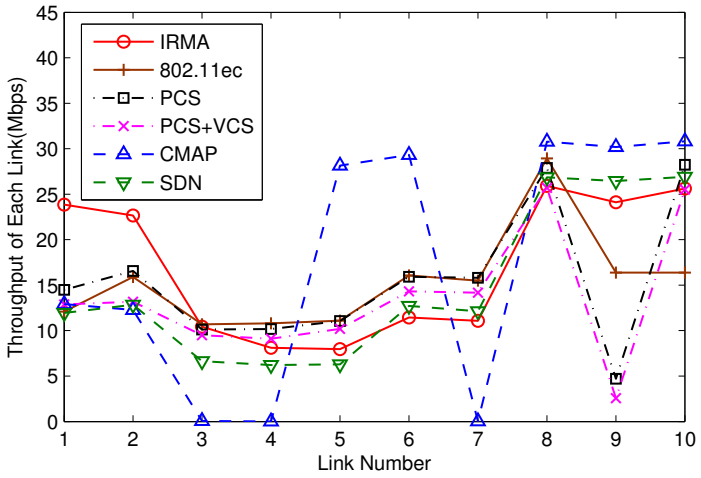


Figure 3.15: The throughput of each link when $l = 2000bytes$ and $v_b = 48Mbits/s$.

ferences in all the scenarios. IRMA employs new components to work collaboratively to increase network's transmission opportunities. I propose the signature detection method in the physical layer to combat control frame's collisions at the transmitter side. I propose a channel access scheme to permit concurrent transmissions while avoid data reception interferences. I show the feasibility of signature detection method via hardware experiments. I also show the significant throughput improvement over the two 802.11 standard and three recent protocols by ns-2.

Chapter 4

Exploit Reception Opportunities through Discernible Interference Cancellation

Since IRMA is proposed to exploit transmission opportunities and improve the network throughput from solving the *varied-IR problem* and the *CA-CF problem*, this chapter proposes ICMR to further exploit reception opportunities also from solving the two problems, through discernible interference cancellation, a physical layer mechanism that can successfully detect data frames when collided by control frames. I analyze the concurrent transmission opportunities of one link from the transmitter's transmission opportunities and the receiver's reception opportunities, then formulate the opportunities, and give theoretical analysis to indicate that ICMR will have a higher opportunity gain over other protocols. Hardware experiments based on USRP2 demonstrate the feasibility of the discernible interference cancellation mechanism, and simulations based on ns-2 confirm that ICMR outperforms the 802.11 standard and other protocols under different network scenarios.

This chapter is organized as follows. Section 4.1 gives an introduction of ICMR. Sec-

tion 4.2 shows an overview of ICMR. Section 4.3 describes the design of the discernible interference cancellation mechanism in detail. Section 4.4 first formulates the concurrent transmission opportunities, and then gives theoretical analysis to quantify the opportunities. Section 4.5 demonstrates the feasibility of discernable interference cancellation through hardware experiments. Section 4.6 evaluates the performance improvement of ICMR through simulations. Section 4.7 summarizes this chapter.

4.1 Overview

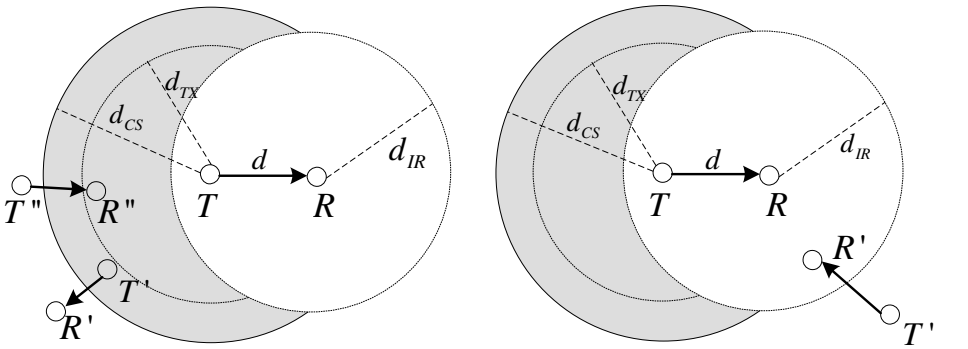
Interference is a critical issue that will degrade the system performance in wireless networks. The widely-deployed 802.11 standard uses the carrier sense multiple access (CSMA) to avoid interferences. However, this mechanism is well known to have low performance as it uses the situation at the transmitter side to decide whether there is an interference at the receiver side, which induces a serious hidden terminal problem. To combat this problem, the 802.11 standard proposes a virtual CSMA mechanism, which uses the exchange of RTS and CTS control frames to coordinate between nodes. The RTS and CTS frames contain a NAV field that represents the duration of data and ACK transmissions, and all nodes that receive the RTS or CTS frames should keep silence during the NAV time to avoid interference. This mechanism still has a low system performance because of two problems, including *the CA-CF problem* and *the varied-IR problem*. Chapter 3 gives the analysis of the two problems from the aspect of wasting transmission opportunities. In this chapter, I will give more detailed analysis of them from the aspect of wasting the reception opportunities.

The CA-CF problem occurs because of avoiding the CTS/ACK control frame induced

collisions. It has two scenarios: (1) The collisions with the CTS/ACK frames should be avoided at the transmitter side of the link, as the transmitter needs to detect the CTS/ACK frames correctly to get the coordination information. The 802.11 standard uses the physical carrier sense and the NAV field in the RTS frame to avoid the collision at the transmitter side. As shown in Fig. 4.1(a), nodes in the grey area are prohibited to transmit data packets or CTS/ACK control frames, so as to avoid collisions with the CTS/ACK frames at node T. (2) The data frame being collided by control frames should be avoided at the receiver side of the ongoing link. The 802.11 standard uses the NAV field in the CTS frame to avoid the collision at the receiver side. As shown in Fig. 4.1(b), nodes in the grey area are prohibited to initiate packet receptions, so as to avoid their CTS/ACK transmissions to interfere with R's data reception.

The varied-IR problem occurs due to fixing the varied interference range d_{IR} to be the transmission range d_{TX}. It also has two scenarios: (1) It may cause excessive restriction of effective transmissions when $d_{IR} < d_{TX}$ (such as the transmission of $T' \rightarrow R'$ or $T'' \rightarrow R''$ in Fig. 4.2(a)). (2) It may bring false permissions of ineffective transmissions which lead to collisions when $d_{IR} > d_{TX}$ (such as the transmission of $T' \rightarrow R'$ or $T'' \rightarrow R''$ in Fig. 4.2(b), where the sign "$\times$" indicates a false permission of a node's data frame transmission or reception).

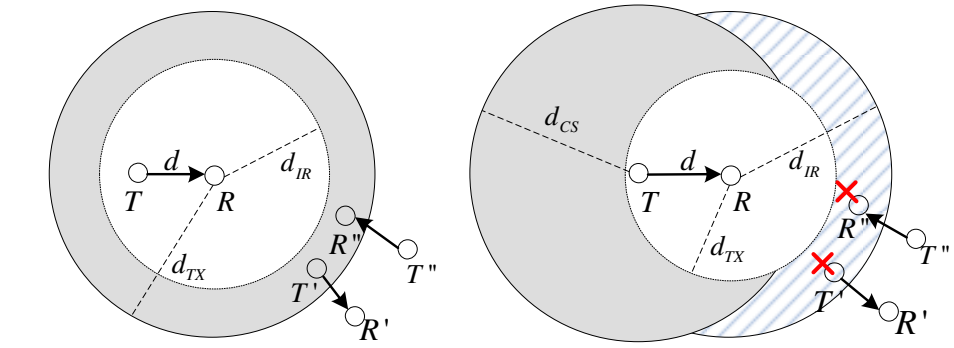
IRMA combats the control frame collision at the transmitter side by using a signature detection method, so as to exploit transmission opportunities through solving *the CA-CF problem* in the scenario of Fig. 4.1(a). IRMA also exploits transmission opportunities through solving *the varied IR problem*, by differentiating between the interfering and non-interfering links, as only nodes that are in the interference range d_{IR} will update the NAV



(a) Nodes in the grey area are prohibited to transmit data or control frames.

(b) Nodes in the white area are prohibited to receive data frames.

Figure 4.1: Two scenarios of *the CA-CF problem*.



(a) Nodes in the grey area are prohibited to transmit data or control frames.

(b) Nodes in the slash area are permitted to transmit data or control frames.

Figure 4.2: Two scenarios of *the varied-IR problem*.

state to keep silence, while the other nodes should not update the NAV state so that they can initiate data transmissions. Thus, IRMA can exploit the transmission opportunities in the scenario of Fig. 4.2(a) and avoid collisions in the scenario of Fig. 4.2(b).

In this chapter, I propose Interference Cancellation Multiple Reception (ICMR), a novel cross layer protocol, to further exploit the reception opportunities and improve the network performance. ICMR permits the reception of a data frame be collided by control frames, and detects the collided data frame through a discernible interference cancellation mechanism in the physical layer. In this mechanism, nodes use signatures (certain known

sequences) to convey the control information. When detecting a collided data frame, nodes first estimate the arrival and positions of control frames in the received signal, then discern signatures carried in the control frames, reconstruct the received control signal through proper channel estimations, and finally detach the control signal to recover the original data signal. According to the ICMR design, all the links which have no mutual interference in their data frame receptions can be permitted to proceed concurrently. For example, the node R' in Fig. 4.1(b) may have the opportunity to initiate data receptions, as long as the transmission of $T' \rightarrow R'$ will not interfere with R's data reception.

I also analyze the concurrent transmission opportunities of a link from the transmitter's transmission opportunities and the receiver's reception opportunities, then formulate the opportunities that can be exploited in the 802.11-based wireless networks from solving both the *CA-CF problem* and the *varied-IR problem*, and finally give theoretical analysis to quantify how ICMR can exploit concurrent transmission opportunities comparing with IRMA and the 802.11 standard.

This chapter makes the following key contributions:

- I design ICMR to exploit reception opportunities in wireless networks through permitting the data frame being collided by control frames.
- I design a DIC mechanism in the physical layer to detect the data frame correctly when it is collided by control frames.
- I analyze the concurrent transmission opportunities of a link from the transmitter's transmission opportunities and the receiver's reception opportunities, then formulate the two kinds of opportunities from solving both the *CA-CF problem* and the

varied-IR problem.

- I quantify the concurrent transmission opportunities which can be exploited theoretically, the results indicate that ICMR can have a higher opportunity gain comparing with IRMA and 802.11 standard.

- I verify the discernible interference cancellation mechanism through hardware experiments. The results demonstrate the feasibility of this mechanism as the data frame can be detected correctly with a high probability when collided by control frames.

- I demonstrate ICMR's significant throughput improvement through simulations. The results show that ICMR can outperform IRMA and the 802.11 standard under different network topologies.

4.2 Overview of ICMR

Based on the RTS/CTS mechanism in the 802.11 standard, IRMA disables the physical carrier sense and lets one node only rely on its NAV state to decide whether it can initiate a data transmission. This protocol can increase concurrency through exploiting transmission opportunities from solving both the *CA-CF problem* and *varied-IR problem*.

In this chapter, I propose ICMR to further increase concurrency through exploiting the reception opportunities in wireless networks. ICMR enhances IRMA, which also adopts RTS/CTS/DATA/ACK handshake mechanism to determine data transmissions and receptions. It can exploit reception opportunities from solving the *CA-CF problem* as the collided control frames can be detected correctly using the same signature detection

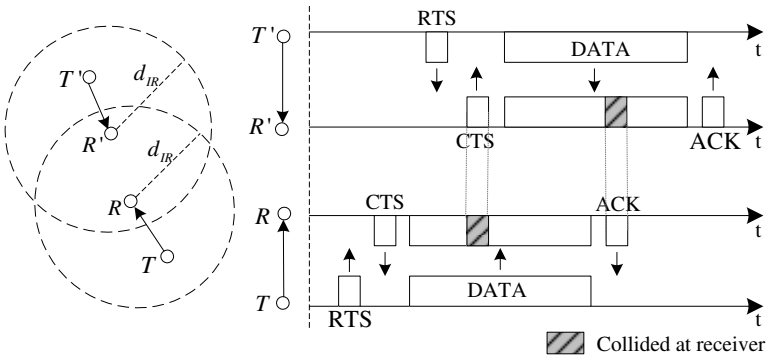


Figure 4.3: The time sequence diagram of nodes in a sample scenario of ICMR.

method as that in IRMA, and the collided data frames can be detected correctly using a DIC mechanism. Based on DIC, concurrent transmissions in the scenario of Fig. 4.1(b) can be exploited successfully. Here I just give an overview of ICMR, and remain the details of DIC in Section 4.3.

To explain how ICMR is designed to exploit reception opportunities, I illustrate this protocol in a simple scenario with the time sequence diagram of each node, as shown in Fig. 4.3. There are two links $T \rightarrow R$ and $T' \rightarrow R'$ in the network. The transmitters T and T' are out of the interference range of the other link, while the receivers R and R' are in the interference range of the other link. ICMR permits the two links' concurrent transmissions. Comparing with the 802.11 and IRMA protocols, the process of ICMR is illustrated as follows:

- If T intends to transmit data to R, the transmission can be permitted by the channel access scheme as its NAV state is zero. T then sends a RTS frame after a backoff time to initiate the transmission, and begins to transmit data frame after receiving the CTS feedback successfully. R' will update its NAV state based on the received CTS as it is in the interference range d_{IR} of R, while T' will not update its NAV

state as it is outside d_{IR} of R. These operations are the same as those in IRMA.

- During the data transmission from T to R, T' has the transmission opportunity as its NAV state is zero, it can send a RTS frame after a backoff time to initiate the transmission. After receiving the RTS frame, R' can decide that its data frame reception will not be interfered by the other link's data frame transmission as it can detect the RTS frame correctly. It has the reception opportunity and will respond a CTS frame to initiate the data reception. Note that the CTS feedback from R' will interfere with R's data reception, this interfered data frame can be detected correctly by using DIC.

- After finishing the reception of the data frame, R will reply an ACK to T to complete the transmission. The ACK frame will also interfere with R''s data reception. The interfered data frame can also be detected using DIC. Therefore, the two concurrent transmissions can be completed successfully.

Note that ICMR has the same channel access scheme and NAV state update mechanism as those in IRMA. Only nodes that are outside the interference range of the ongoing link will update the NAV states, and one node can transmit a data frame only when its NAV state is zero. Thus, nodes adopt ICMR or IRMA have the same transmission opportunities. Meanwhile, nodes in ICMR have different reception opportunities from IRMA. Based on ICMR, one node can respond a CTS feedback when it receives a RTS frame correctly, no matter its NAV state is zero or not, the data frame interfered by control frames will be detected correctly by DIC.

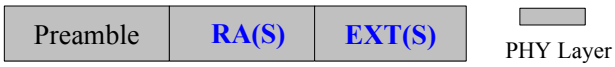


Figure 4.4: The format of new CTS/ACK frames.

4.2.1 Control Frame Design

I make some changes to the IRMA control frames to complete the ICMR control frame design. The RTS frame of this protocol has the same format as that of IRMA (shown in Fig. 3.4(a)), while the CTS/ACK frame only remains the fields in the physical layer.

Based on the idea of DIC, when receiving a collided signal containing the CTS/ACK control signal and data signal, one node should first detect the control signal so as to detach them and recover the original data signal. As the fields in the MAC layer cannot be detected correctly under interferences, we remove all the fields in the MAC layer in the new ICMR CTS/ACK frame design.

As shown in Fig. 4.4, the new CTS/ACK control frame has three fields, including the preamble, RA(S) and EXT(S), which are the same as those in the physical layer of the IRMA CTS/ACK control frame (shown in Fig. 3.4(b)), and the detailed signature design for both RA(S) and EXT(S) fields are the same as that in the IRMA protocol.

4.3 Discernible Interference Cancellation Design

ICMR uses the Discernible Interference Cancellation (DIC) mechanism to detect data frames when they are interfered by CTS or ACK control frames. In this section, I first introduce the process of DIC as an overview, then give the detailed process of data signal recovery, including the preamble synchronization, signature discernment, control signal reconstruction and detachment, and a refined control channel estimation mechanism.

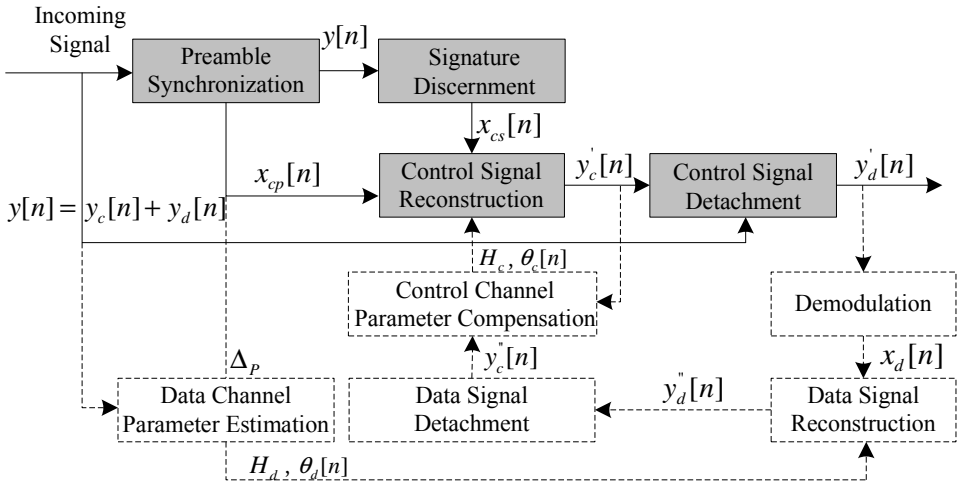


Figure 4.5: The process of DIC.

4.3.1 Overview of DIC

Before describing the process of DIC, I first formulate the signal at the transmitter and receiver sides.

A wireless signal is typically described as a stream of complex samples, and a received signal may differ from the transmitted one in amplitude, phase and frequency due to the wireless channel distortion.

Suppose $x_c[n]$ is the complex number that represents the nth transmitted control sample, the corresponding received control signal $y_c[n]$ can be denoted as:

$$y_c[n] = H_c x_c[n] e^{j(2\pi n \delta_{f_c} T + \theta_{c0})}, \tag{4.1}$$

where H_c refers to the control signal's amplitude attenuation, δ_{f_c} and θ_{c0} refer to the frequency offset and phase offset respectively, and T is the sample period.

Similarly, if $x_d[n]$ is the nth transmitted data sample, the received data signal $y_d[n]$

can be denoted as:

$$y_d[n] = H_d x_d[n] e^{j(2\pi n \delta_{f_d} T + \theta_{d0})}, \tag{4.2}$$

where H_d is the the amplitude attenuation between the data signal's transmitter and receiver, δ_{f_d} and θ_{d0} refer to the frequency offset and phase offset, respectively.

When a node receives a collided signal containing a data signal and a CTS/ACK control signal, the collided signal $y[n]$ is represented as:

$$y[n] = y_c[n] + y_d[n] + w[n], \tag{4.3}$$

where $w[n]$ is the random noise.

The process of DIC is described as follows (Fig. 4.5): The node continuously conducts the preamble synchronization to determine the arrival and position of the control frame. It will conduct the following modules only if this module indicates the arrival of a control frame. From preamble synchronization, the node also gets the transmitted control samples $x_{cp}[n]$ in the preamble field. It then performs the signature discernment at the estimated positions to discern the signatures, so as to get the transmitted control samples $x_{cs}[n]$ in the corresponding field filled with signatures. With the information of $x_{cp}[n]$ and $x_{cs}[n]$, the node gets all the transmitted control signal $x_c[n]$. It can reconstruct the received control signal based on Ineq. (4.1), where the channel parameters H_c, δ_{f_c} and θ_{c0} should be estimated properly. The output $y'_c[n]$ may be a little different from the original received control signal $y_c[n]$ because of the error introduced in channel parameter estimations. The node can finally detach the control signal $y'_c[n]$ from the received signal $y[n]$ to recover the data signal $y'_d[n]$, which is transformed into bits after demodulation and passed to the MAC layer to complete the protocol disposal. The white blocks are used to refine the control channel estimation, which will be discussed in Section 4.3.4.

Note that DIC should only be performed when a receiving data packet is collided by an incoming signal, it should be disabled in other circumstances when the data packet can be decoded successfully through normal demodulation process.

4.3.2 Preamble Synchronization and Signature Discernment

After receiving a data frame collided by CTS or ACK frames, a node should first use the preamble synchronization module to determine the positions of control frames, and use the signature discernment module to determine the signatures in each field of the control frames.

Note that the preamble can be treated as a specific signature s_P, it can be discerned through doing cross correlation between s_P and the received signal $y[n]$. If the correlation result at position Δ_P is above the threshold β_{Corr}, s_P is determined to be in $y[n]$. Meanwhile, Δ_P also represents the position of the control signal in $y[n]$, the obtained position information will be further used in the control signal detachment module in Section 4.3.3.

The process of signature discernment here is the same as that in the signature detection method (SDM), as described in Section 3.3.3. Cross correlation is conducted between the incoming signal and all the known signatures in the signature set S_{Addr} or S_{EXT}. The signature, which has the maximum correlation result among those ones that exceed β_{Corr}, is determined to be in the received signal in the corresponding position.

4.3.3 Control Signal Reconstruction and Detachment

After passing the received collided signal through the preamble synchronization and signature discernment modules, the node can only obtain the control signal at the transmitter

side (denoted by $x_c[n]$), it should then reconstruct the control signal at the receiver side (denoted by $y_c[n]$), so as to detach it and recover the original data signal. To reconstruct $y_c[n]$, we should accurately estimate three key parameters, H_c, δ_{f_c} and θ_{c0} in Ineq. 4.1.

4.3.3.1 Amplitude Estimation

The parameter H_c can be estimated in a simple way: As a sharp change appears in the amplitude variation of the received signal when a new control signal arrives, together with the signal strength before and after the sharp change, we can easily get the amplitude A_c of the received control signal, then the parameter H_c can be calculated as:

$$H_c = \frac{A_c}{\frac{1}{L}\sum_{k=1}^{L}|x_c[k]|}.$$

4.3.3.2 Frequency and Phase Offsets Estimation

As the effect of wireless channels can be approximated by amplitude attenuation and phase shift [77], the frequency offset δ_{f_c} will finally affect the overall phase offset $\theta_c[n]$ of the received signal. Hence, we make $\theta_c[n]$ as one parameter to estimate.

Different from Zigzag [17] or DAC [99] that use clean samples to estimate the frequency and phase offsets of the following collided samples, ICMR cannot use clean samples to estimate these parameters of the control frame as the control samples may be fully collided by data samples. In this thesis, I propose a *Blind Estimation Algorithm* to estimate the phase offset of control samples by further exploiting cross correlation, which is described as follows.

Suppose the received collided signal $y[n]$ contains a data signal $y_d[n]$ and a control signal $y_c[n]$, as described in Ineq. 4.3, and suppose a signature $s_i[k]$ $(1 \leq k \leq L)$ in the

received signal is at position Δ. According to Ineq. 2.2, the correlation result between $y[n]$ and s_i at Δ is described as:

$$R(\Delta) = H_c \sum_{k=1}^{L} |s_i[k]|^2 e^{j(2\pi k \delta_{f_c} T + \theta_{c0})},$$

We set overall phase offset of the nth control sample as $\theta_c[n] = 2\pi n \delta_{f_c} T + \theta_{c0}$, then we have:

$$R(\Delta) = H_c \sum_{k=1}^{L} |s_i[k]|^2 e^{j\theta_c[k]}.$$

As δ_{f_c} can be compensated based on history information, this value can be very small. That means, within the L samples of the signature s_i that we do cross correlation, the overall phase offset of each sample $\theta_c[k]$ can be approximately equal to a constant value Θ. Here we denote Θ as the central phase offset of this signature, then the correlation result can be simplified as:

$$R(\Delta) \approx e^{j\Theta} H_c \sum_{k=1}^{L} |s_i[k]|^2.$$

The central phase offset of this signature can be calculated as:

$$\Theta = arctan\left(\frac{Imag(R(\Delta))}{Real(R(\Delta))}\right). \tag{4.4}$$

According to the format of the CTS/ACK frame (Fig. 4.4), there are one preamble and two signatures in a CTS or ACK frame. We let the sample length L of the control frame's three fields be L_P, L_1 and L_2, and let the calculated central phase offsets in the corresponding fields be Θ_P, Θ_1 and Θ_2. Note that the preamble can be treated as a specific signature and its central phase offset Θ_P can also be calculated by Ineq. (4.4). Fig. 4.6 gives an example of the three values in a control frame. The three different marks

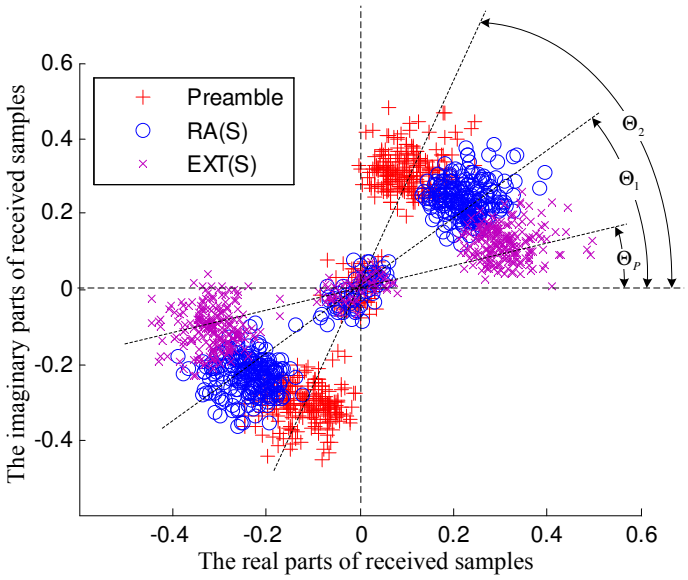


Figure 4.6: An example of the central phase offset in a received control frame.

are used to represent the constellation positions of the received samples in the three fields, respectively.

Upon calculating Θ_P, Θ_1 and Θ_2, the receiver just gets a rough estimation about the phase offset of each field, it should then recover the phase offset of each sample in the control frame, so that each received control sample can be reconstructed and detached from the collided samples. Suppose the jitter of δ_{f_c} is small, that means, the change of phase at each sample is approximately uniform. Then we recover the phase offset of each sample in preamble as:

$$\theta_P(k) = \Theta_P - \frac{\Theta_1 - \Theta_P}{2} + \frac{\Theta_1 - \Theta_P}{L_P} \cdot k, \ \ k \in [1, L_P], \tag{4.5}$$

and the phase offset of each sample in the following two fields as:

$$\theta_1(k) = \Theta_1 - \frac{\Theta_1 - \Theta_P}{2} + \frac{\Theta_2 - \Theta_P}{L_p + L_1} \cdot k, \ \ k \in [1, L_1], \tag{4.6}$$

$$\theta_2(k) = \Theta_2 - \frac{\Theta_2 - \Theta_1}{2} + \frac{\Theta_2 - \Theta_1}{L_2} \cdot k, \ \ k \in [1, L_2]. \tag{4.7}$$

The Blind Estimation Algorithm is listed as Algorithm 4.1, based on which we can estimate the phase of each received control sample even when there is no clean control signal in the received signal.

Algorithm 4.1 Blind Estimation Algorithm

Input: y, s; Δ_p, Δ_{sRA} and Δ_{sEXT}; L_p, L_1 and L_2.
Output: $\theta_p(k)$, $\theta_1(k)$, $\theta_2(k)$.

1: Calculate $R(\Delta_p)$, $R(\Delta_{sRA})$ and $R(\Delta_{sEXT})$ using Ineq. (2.1);
2: Calculate Θ_p, Θ_1 and Θ_2 using Ineq. (4.4);
3: **for** $k = 1 : L_p$ **do**
4: Calculate $\theta_p(k)$ using Ineq. (4.5);
5: **end for**
6: **for** $k = 1 : L_1$ **do**
7: Calculate $\theta_1(k)$ using Ineq. (4.6);
8: **end for**
9: **for** $k = 1 : L_2$ **do**
10: Calculate $\theta_2(k)$ using Ineq. (4.7);
11: **end for**

After the preamble synchronization and the signature discernment module, one node has the transmitted control signal to be $x_c[n]$ at position Δ_P; combining with the estimated control channel parameters H_c and $\theta[n]$, the node can reconstruct the received control samples as $y'_c[n]$. It will then detach $y'_c[n]$ from the received signal at the position Δ_P, and get the original data samples $y'_d[n]$, which will be finally transformed into bits after the normal demodulation process. Note that the control signal reconstruction and detachment process can be conducted for multiple times during a data frame reception, as the data frame may be collided by several CTS or ACK frames. The module will be triggered when the preamble synchronization module indicates an arrival of a control frame.

4.3.4 Refined Channel Estimation

We let Θ calculated by Ineq. (4.4) as the central phase offset of the received signature. However, this value is just an estimated value and may deviate from the real central phase offset. The deviation of Θ will affect the calculated phase offset of each control sample, and finally affect the recovered data samples $y'_d[n]$, introducing more errors to the demodulated bits of the data frame. Meanwhile, the amplitude distortion H_c may also have some deviation when estimated using the method in Section 4.3.3.

To mitigate the deviation of control channel parameters, we design a simple feedback algorithm to refine the channel estimation during the process of control signal reconstruction and detachment, as shown in the white blocks of Fig. 4.5. The data signal always has clean samples as the data frame is longer than the control frame, these clean data samples can be utilized to refine the control channel estimation. After recovering the original data samples $y'_d[n]$, one node will obtain the bits of the data packet $x_d[n]$ after passing $y'_d[n]$ through the normal demodulation process. As the data samples are clean when $n < \Delta_P$, the node can calculate the amplitude distortion H_d and phase offset $\theta_d[n]$ during this period, according to which it then reconstructs the collided data samples as $y''_d[n]$, and gets a new estimation of the control samples as $y''_c[n] = y[n] - y''_d[n]$. The new channel parameters H'_c and $\theta'_c[n]$ in the control samples $y''_d[n]$ can be calculated and will be used to compensate the values estimated in the control signal reconstruction module.

4.4 Theoretical Analysis

In this section, I intend to quantify the opportunities ICMR can exploit theoretically. To this end, I will first formulate the concurrent transmission opportunities, then give the quantified opportunity comparison among ICMR, IRMA and the 802.11 standard.

4.4.1 Formulation

Determining whether a link $T' \rightarrow R'$ can have concurrent transmission opportunities with an ongoing link $T \rightarrow R$ in a wireless network is equivalent to determining both the two conditions: (1) whether T' can be permitted to send a data frame and (2) whether R' can be permitted to receive a data frame. To make the analysis clear, we introduce two concepts, *transmission opportunity*, which is the opportunity that a node can send a RTS frame to initiate a data transmission, and *reception opportunity*, which is the opportunity that a node can response a CTS frame to grant a data reception.

The concurrent transmission of the link $T' \rightarrow R'$ can proceed only if the transmitter T' has the transmission opportunity and the receiver R' has the reception opportunity. In the following parts, I will give detailed analysis about the two opportunities in the 802.11-based wireless networks. All the opportunity analysis will start from solving the *CA-CF problem* and the *varied-IR problem*. In the analysis, we use $D(A, B)$ to denote the distance between nodes A and B.

4.4.1.1 Transmission Opportunity

According to the basic requirement of concurrent transmissions, one node has the transmission opportunity if its data transmission will not interfere with the ongoing link's

data reception. I will discuss this opportunity from solving both the *CA-CF problem* and *varied-IR problem* in the current 802.11 standard.

A) Solving the CA-CF problem

According to *the CA-CF problem* shown in Fig. 4.1(a), when a node T', which is a neighbor of the transmitter T of the link $T \rightarrow R$, intends to initiate a transmission, it should not interfere with T's reception of the CTS/ACK control frames, so that T can get the proper control information. The 802.11 standard uses the physical carrier sense to avoid this collision, therefore, nodes within the carrier sense range d_{CS} of T will be prohibited to transmit a packet. We call this as the *Tx transmitter-side data-excessive-restriction*, which is formulated as:

$$D(T', T) < d_{CS}. \tag{4.8}$$

B) Solving the varied-IR problem

According to the *varied-IR problem*, the 802.11 standard uses the NAV field in the CTS frame to reserve the medium around the receiver side, thus fixing the interference range d_{IR} of the receiver to be the transmission range d_{TX} of CTS. That means, T' is prohibited to transmit a packet if $D(T', R) < d_{TX}$. This problem occurs in two scenarios:

1) As shown in Fig. 4.2(a), T' is prohibited to initiate a transmission although it will not interfere with R's data reception if:

$$d_{IR} < D(T', R) < d_{TX}. \tag{4.9}$$

Ineq. (4.9) is referred as the *Tx receiver-side data-excessive-restriction* in the 802.11 standard.

2) As shown in Fig. 4.2(b), T' is permitted to initiate a transmission although it will definitely interfere with R's data reception if:

$$d_{TX} < D(T', R) < d_{IR}. \tag{4.10}$$

Ineq. (4.10) is referred as the *Tx receiver-side data-false-permission* in the 802.11 standard. In this condition, nodes will bring some "threat" to the ongoing link because of improperly using this transmission opportunity. The threat can be regarded as a negative opportunity.

As a conclusion, considering both problems, with an ongoing link $T \rightarrow R$, a node T' may exploit the transmission opportunity if the condition of Ineq. (4.8) or Ineq. (4.9) is satisfied, and may suppress the threat if the condition of Ineq. (4.10) is satisfied.

4.4.1.2 Reception Opportunity

According to the basic requirement of concurrent transmissions, one node has the reception opportunity if its data reception will have no mutual interference with the data reception of the ongoing link. I will also discuss this opportunity in the 802.11 standard from solving both the *CA-CF problem* and the *varied-IR problem*.

A) Solving the CA-CF problem

According to *the CA-CF problem* shown in Fig. 4.1(a), when a node R' around the link $T \rightarrow R$ receives a RTS frame and determines whether to response a CTS frame to initiate a data reception, its CTS/ACK transmission should not interfere with T's CTS/ACK reception. The 802.11 standard uses the NAV field in the RTS frame to avoid this collision. R' cannot be permitted to receive a data frame if it has updated its NAV state

according to the received RTS frame from T. The constraint that R' will be prohibited to receive a packet is:

$$D(R', T) < d_{TX}. \tag{4.11}$$

Ineq. (4.11) is referred as the *Rx transmitter-side control-excessive-restriction* in the 802.11 standard.

Meanwhile, according to *the CA-CF problem* shown in Fig. 4.1(b), the node R''s CTS/ACK transmission should also not interfere with the receiver R's data reception, that means, R' is prohibited to receive a packet if it is within the interference range d_{IR} of R. We formulate it as:

$$D(R', R) < d_{IR}. \tag{4.12}$$

Ineq. (4.12) is referred as the *Rx receiver-side data-excessive-restriction*.

B) Solving the varied-IR problem

To avoid collisions under the condition of Ineq. (4.12), the 802.11 standard uses the NAV field in the CTS frame to reserve the medium. R' cannot be permitted to receive a data frame if it has updated its NAV state according to the received CTS frame from R. However, this mechanism itself also has the *varied-IR problem* as d_{TX} of CTS is fixed but d_{IR} of the ongoing link $T \rightarrow R$ is variable. This problem occurs in two scenarios:

1) As shown in Fig. 4.2(a), R' is prohibited to initiate a data frame reception although its CTS/ACK frame transmission will not interfere with $T \rightarrow R$'s data reception if:

$$d_{IR} < D(R', R) < d_{TX}. \tag{4.13}$$

Ineq. (4.13) is referred as the *Rx receiver-side control-excessive-restriction* in the

802.11 standard.

2) As shown in Fig. 4.2(b), R' is permitted to initiate a data frame reception although its CTS/ACK frame transmission will interfere with $T \rightarrow R$'s data reception if:

$$d_{TX} < D(R', R) < d_{IR}. \tag{4.14}$$

Ineq. (4.14) is referred as the *Rx receiver-side control-false-permission* in the 802.11 standard.

Similar to Ineq. (4.13) and Ineq. (4.14), we can see that when d_{IR} varies, Ineq. (4.12) also has two conditions:

$$D(R', R) < d_{IR} < d_{TX} \tag{4.15}$$

or

$$D(R', R) < d_{TX} < d_{IR}. \tag{4.16}$$

For the analysis simplification, we refer Ineq. (4.15) and Ineq. (4.16) as the *Rx receiver-side data-excessive-restriction 1* and *Rx receiver-side data-excessive-restriction 2*.

As a conclusion, considering both problems, with an ongoing link $T \rightarrow R$, a node R' may exploit the reception opportunity if the condition of Ineq. (4.11), Ineq. (4.13), Ineq. (4.15) or Ineq. (4.16) is satisfied, and may suppress the threat if the condition of Ineq. (4.14) is satisfied.

C) Limitations of reception opportunity

The concurrent transmissions of one link with the ongoing link is permitted if and only if its transmitter has the transmission opportunity and its receiver has the reception opportunity. With this limitation, one node that satisfies Ineq. (4.15) and Ineq. (4.16)

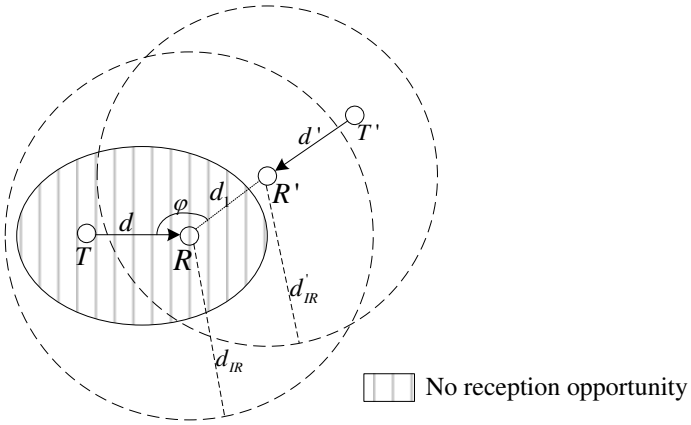


Figure 4.7: An illustration of the limitations of reception opportunity.

may still have no reception opportunity if any of its transmitters has no transmission opportunity (its transmitters cannot be out of the interference range of the ongoing link). Here we will quantify how many reception opportunities that satisfy Ineq. (4.15) and Ineq. (4.16) cannot be exploited.

As shown in Fig. 4.7, there is an ongoing transmission link $T \rightarrow R$ with the distance d. Its interference range is $d_{IR} = \rho \cdot d$, where $\rho = \sqrt[\alpha]{\beta_{SINR}}$ is a constant. If a node R' within the interference range has the reception opportunity from any other node T', that means, T should be out of the interference range of R', that is:

$$D(T, R') = d^2 - 2cos\varphi \cdot d \cdot d_1 + d_1^2 > d'^2_{IR},$$

where $d_1 = D(R, R')$ and $d' = D(T', R')$, φ is the intersection angle of $T \rightarrow R$ and $R \rightarrow R'$, $d'_{IR} = \rho \cdot d'$. We have:

$$d_1^2 - 2cos\varphi \cdot d \cdot d_1 + d^2 - \rho^2 d'^2 > 0,$$

that is:

$$d_1 > d \cdot cos\varphi + \sqrt{\rho^2 d'^2 - d^2 sin^2\varphi}. \tag{4.17}$$

There is another limitation that, for any transmitter T', it should be out of the interference range of R, which means:

$$d' + d_1 > d_{IR}. \tag{4.18}$$

With Ineq. (4.17) and Ineq. (4.18), we get:

$$d_1 > \frac{d}{\rho^2 - 1}\left(\rho^3 - cos\varphi - \sqrt{cos^2\varphi - 2\rho^3 cos\varphi + \rho^4 + \rho^2 - 1}\right). \tag{4.19}$$

According to Ineq. (4.19), when φ rotates from 0 to 2π, there is an ellipse region within which nodes have no reception opportunity. We denote the right-side expression of Ineq. (4.19) to be $f(d, \varphi)$ and simplify Ineq. (4.19) to be $d_1 > f(d, \varphi)$, then the two *Rx receiver-side data-excessive-restriction* conditions in Ineq. (4.15) and Ineq. (4.16) can be updated as:

$$f(d, \varphi) < D(R', R) < d_{IR} < d_{TX} \tag{4.20}$$

and

$$f(d, \varphi) < D(R', R) < d_{TX} < d_{IR}. \tag{4.21}$$

4.4.2 Opportunity Quantification

In this part, I first quantify the transmission and reception opportunities of 802.11, IRMA and ICMR, then give an overall opportunity comparison among the three protocols.

To simplify the analysis, we let $C(A, r)$ represent the area of a disk whose center is A and radius is r. We let $E(d)$ represent the area of an ellipse formed by Ineq. (4.19). We also let $O_T(\cdot)$ and $O_R(\cdot)$ represent the transmission and reception opportunity area of each protocol, respectively. I will analyze the opportunities in the scenario that there is an

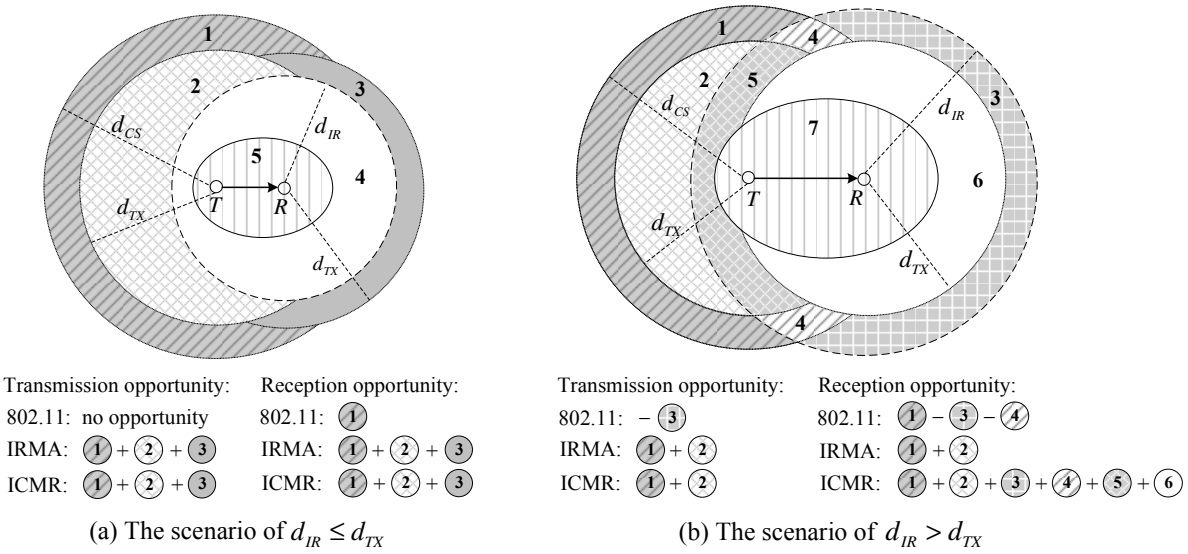


Figure 4.8: Opportunity comparison among ICMR, IRMA and 802.11 standard.

ongoing link $T \rightarrow R$ in the network, and let both the overall transmission opportunity area $O_T(All)$ and reception opportunity area $O_R(All)$ in the vicinity of the link be the influence region of T and R. Then the transmission and reception opportunities of each protocol are calculated as $\frac{O_T(\cdot)}{O_T(All)}$ and $\frac{O_R(\cdot)}{O_R(All)}$, respectively. I will analyze both opportunities from two cases: $d_{IR} \le d_{TX}$ and $d_{IR} > d_{TX}$.

4.4.2.1 Transmission Opportunity

Case 1.1: $d_{IR} \le d_{TX}$. As shown in Fig. 4.8(a), the transmission opportunity area of each protocol in this case is listed as follows:

$$\begin{aligned} O_T(All) &= C(T, d_{CS}) \cup C(R, d_{TX}), \\ O_T(802.11) &= \phi, \\ O_T(IRMA) &= C(T, d_{CS}) \cup C(R, d_{TX}) \setminus C(R, d_{IR}), \\ O_T(ICMR) &= C(T, d_{CS}) \cup C(R, d_{TX}) \setminus C(R, d_{IR}). \end{aligned} \tag{4.22}$$

The 802.11 has no transmission opportunity in this case, while IRMA and ICMR

can exploit the transmission opportunities formulated in Ineq. (4.8) and Ineq. (4.9), as collided CTS/ACK control frames can be detected correctly through the signature detection method, and channel access is determined according to the real interference range in these two protocols. Thus, nodes in the areas ① + ② + ③ in Fig. 4.8(a) can exploit transmission opportunities.

Case 1.2: $d_{IR} > d_{TX}$. As shown in Fig. 4.8(b), the transmission opportunity area of each protocol in this case is listed as follows:

$$\begin{aligned} &O_T(All) = C(T, d_{CS}) \cup C(R, d_{IR}), \\ &O_T(802.11) = -C(R, d_{IR}) \setminus C(R, d_{TX}) \setminus C(T, d_{CS}), \\ &O_T(IRMA) = C(T, d_{CS}) \setminus C(R, d_{IR}), \\ &O_T(ICMR) = C(T, d_{CS}) \setminus C(R, d_{IR}). \end{aligned} \tag{4.23}$$

From Fig. 4.8(b), we can see that for the 802.11 standard, nodes in the area ③ satisfy Ineq. (4.10), so their transmissions will bring some "threat" to the ongoing link $T \rightarrow R$. We regard the threat as the negative opportunity since the nodes' transmission opportunity in this area will be negatively affected. We use the label " $-$ " to denote it. On the contrary, nodes adopted IRMA or ICMR in this area can detect the CTS frame through the signature detection method, and keep silence to suppress the threat successfully. Meanwhile, IRMA and ICMR can also exploit transmission opportunities formulated in Ineq. (4.8), which corresponds to the areas ① + ② in Fig. 4.8(b).

4.4.2.2 Reception Opportunity

Case 2.1: $d_{IR} \leq d_{TX}$. As shown in Fig. 4.8(a), the reception opportunity area of each protocol in this case is listed as follows:

$$\begin{aligned} O_R(All) &= C(T, d_{CS}) \cup C(R, d_{TX}), \\ O_R(802.11) &= C(T, d_{CS}) \setminus C(T, d_{TX}) \setminus C(R, d_{TX}), \\ O_R(IRMA) &= C(T, d_{CS}) \cup C(R, d_{TX}) \setminus C(R, d_{IR}), \\ O_R(ICMR) &= C(T, d_{CS}) \cup C(R, d_{TX}) \setminus E(d). \end{aligned} \tag{4.24}$$

For the 802.11 standard, one node that is within the carrier sense range but outside the transmission range of T may have the reception opportunity if its NAV state is zero and the received signal's SINR is over the threshold β_{SINR}, which corresponds to the area ① in Fig. 4.8(a). IRMA can exploit the reception opportunity formulated in Ineq. (4.11) and Ineq. (4.13), which corresponds to the areas ①+②+③ in Fig. 4.8(a), while ICMR can further exploit the reception opportunities formulated in Ineq. (4.20), which corresponds to the area ④ in Fig. 4.8(a).

Case 2.2: $d_{IR} > d_{TX}$. As shown in Fig. 4.8(b), the reception opportunity area of each protocol in this case is listed as follows:

$$\begin{aligned} O_R(All) &= C(T, d_{CS}) \cup C(R, d_{IR}), \\ O_R(802.11) &= C(T, d_{CS}) \setminus C(T, d_{TX}) \setminus C(R, d_{TX}) \\ &\quad - C(R, d_{IR}) \setminus C(R, d_{TX}) \setminus C(T, d_{CS}), \\ O_R(IRMA) &= C(T, d_{CS}) \setminus C(R, d_{IR}), \\ O_R(ICMR) &= C(T, d_{CS}) \cup C(R, d_{IR}) \setminus E(d). \end{aligned} \tag{4.25}$$

For the 802.11 standard, nodes in the areas ③+④ of Fig. 4.8(b) satisfy Ineq. (4.14) and may bring some threats when they receive packets. Both IRMA and ICMR can

suppress these threats. Moreover, IRMA and ICMR can exploit the reception opportunity formulated in Ineq. (4.11) (corresponding to area ②), while ICMR can further exploit the reception opportunities formulated in Ineq. (4.16) (corresponding to areas ③+④+⑤) and Ineq. (4.21) (corresponding to area ⑥), all shown in Fig. 4.8(b).

4.4.2.3 Comparison

The overall opportunity of each protocol can be calculated as $\frac{O_T(\cdot)+O_R(\cdot)}{O_T(All)+O_R(All)}$, whose value depends on the values of d_{CS}, d_{TX}, d and β_{SINR} (which determines the value of d_{IR}). Fig. 4.9 shows an example of the overall opportunity of each protocol varying with d, when $d_{CS} = 700m$, $d_{TX} = 500m$ and $\beta_{SINR} = 3.16$ (using the BPSK modulation). It shows that, along with the increase of d, 802.11 standard will bring more threats to the network, and ICMR will introduce more opportunities comparing with that of IRMA. Fig. 4.10 shows the opportunity gain of ICMR over IRMA. We can see that ICMR will have around 50% opportunity gain over IRMA when d is about $0.65 \times d_{TX}$, and this value increases to more than 200% when $d = d_{TX}$. From this analysis, we can conclude that ICMR will have a higher performance improvement over IRMA in a relatively sparse network where the transmitter-receiver distance is large.

I summarize the opportunities of three protocols in Table 4.1. I use the letters "O" or "T" to indicate whether there exists the opportunity can be exploited or the threat can be suppressed in each condition, respectively. "/" indicates the opportunity cannot be exploited or no threat is induced in this condition. "$-$" indicates a threat is induced and "$+$" indicates an opportunity can be exploited. I ignore the situations when no opportunity or no threat exists in each condition, such as threats in Ineq. (4.8). The table

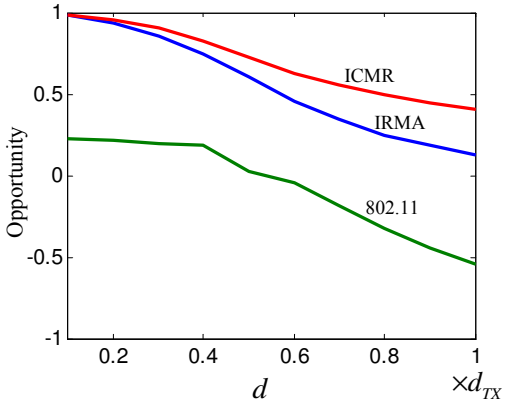


Figure 4.9: Opportunity quantification among three protocols.

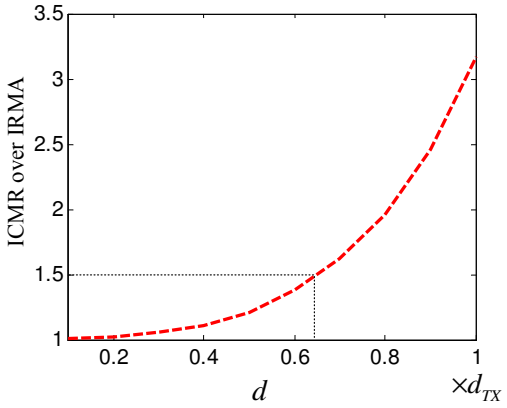


Figure 4.10: Opportunity gain of ICMR over IRMA.

indicates that IRMA has already exploited four kinds of opportunities and suppressed the two kinds of threats, while ICMR can further exploit the remaining three kinds of opportunities, which are marked with red "+" signs.

Table 4.1: The summary of opportunities among three protocols.

Condition			**O/T**	**802.11**	**IRMA**	**ICMR**
Transmission Opportunity	*Tx transmitter-side data-excessive-restriction*	Eq. (12)	O	/	+	+
	Tx receiver-side data-excessive-restriction	Eq. (13)	O	/	+	+
	Tx receiver-side data-false-permission	Eq. (14)	T	—	/	/
Reception Opportunity	*Rx transmitter-side data-excessive-restriction*	Eq. (15)	O	/	+	+
	Rx receiver-side control-excessive-restriction	Eq. (17)	O	/	+	+
	Rx receiver-side control-false-permission	Eq. (18)	O	/	/	+
			T	—	/	/
	Rx receiver-side data-excessive-restriction1	Eq. (24)	O	/	/	+
	Rx receiver-side data-excessive-restriction2	Eq. (25)	O	/	/	+

4.5 Feasibility Evaluation

In this section, I quantify the feasibility of using the DIC mechanism to detect data frames when they are collided by control frames through hardware experiments.

4.5.1 Experiment Setup

The experiments are conducted on Universal Software Radio Peripheral 2 (USRP2) platform and use the GNURadio for the signal processing blocks. We use the RXF2400 daughter-board which makes each USRP2 operate at about 2.4GHz. GNURadio has already implemented the physical layer modulation and demodulation processes. For the receiving process of DIC, we will first restore the received collided samples and make trace-based off-line analysis for the modules in Fig. 4.5. After that, the recovered data samples will be fed into the GNURadio receiving process to be transformed into bits. We choose DBPSK as the constellation method. The bit rate is $1Mbits/s$ and the number of samples per symbol is 2.

The experimental network consists of eight USRP2 nodes, and the topology is randomly set up. For each experiment, we choose four nodes to form two links like the topology shown in Fig. 4.3. Each link has a sender and a receiver, ICMR permits the two links' concurrent transmissions. The CTS/ACK transmissions from each receiver may potentially interfere with the other one's data frame reception. As the signals from different nodes may have different signal strength in the real network, we test different $P_r(Signature)$ and $P_r(Data)$ environments by adjusting the transmission power of the two receivers while fixing that of the senders, where $P_r(Signature)$ and $P_r(Data)$ are the received signal strengths of the signature and data frame, respectively.

As IRMA has given thorough evaluation of signature detection from two aspects: the false negative error rate and false positive error rate, as described in Section 3.4, here I focus on the evaluation of the data signal recovery.

4.5.2 Evaluation of Blind Estimation Algorithm

To recover the data signal from the received collided signal, one node will first reconstruct the control signal. It should conduct both amplitude estimation and phase offset estimation to get the control channel parameters. As the amplitude estimation is relatively simple and accurate, in the experiment we focus on the Blind Estimation Algorithm in the phase offset estimation process.

I intend to quantify this algorithm through estimating the phase difference between the recovered control samples and the original clean control samples. As the phase offset of the clean control signal cannot be obtained correctly when it is collided by another data signal, here we use the mimetic collision as that was used in [44] to conduct this experiment. We first separately generate and log the CTS/ACK control frames and data frames without collisions, and then add them up to mimic a collided signal. For the collided signal, I estimate the phase offset of control samples through the Blind Estimation Algorithm, and then compare the phase offset obtained from the clean control samples to get the phase estimation error.

As shown in Fig. 4.11, the phase estimation error increases along with the decrease of $SINR(Signature)$. When $SINR(Signature)$ is above -4dB, more than 90% phase estimation errors are below $\pi/6$, and when $SINR(Signature)$ decreases to $-10dB$, only 80% phase estimation errors are below this value. We should note that when

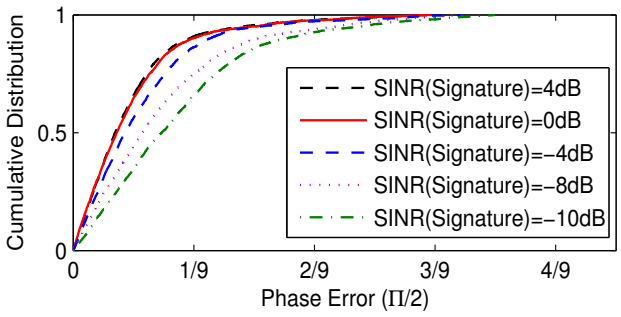


Figure 4.11: The CDF of phase estimation error under different SINR environments when the signature length is $160bits$.

$SINR(Signature)$ is above $0dB$, the phase estimation error has little change with the increase of $SINR(Signature)$, which means that the *blind estimation algorithm* can obtain its best performance when $SINR(Signature)$ is $0dB$.

4.5.3 Data Frame Detection

In this part, I evaluate the effectiveness of data transmissions when interfered by CTS/ACK transmissions. I intend to measure this by comparing the packet error rate (PER) of the data frame transmissions collided by control frames with or without DIC under different $SINR(Data) = P_r(Data) - P_r(Signature)$ environments. Note that I make two links proceed concurrently in this experiment. I set the payload of data frame to be $300bytes$, and evaluate PER when the signature length is $160bytes$.

As shown in Fig. 4.12, without DIC, the PER of data frames increases from 0 to 100% when the value of $SINR(Data)$ increases to about $2dB$. The PER is about 0 when the $SINR(Data)$ is above $8dB$, under which environment the normal DBPSK decoding always works.

The figure also demonstrates that, with DIC, the data frames have a high probability

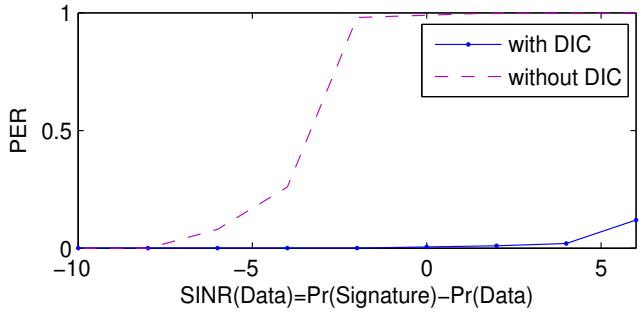


Figure 4.12: The packet error rate under different SINR environments.

to be detected when the value of $SINR(Data)$ is above $-4dB$, the PER is below 5%, which increases to about 12% when $SINR(Data)$ decreases to $-6dB$. We consider that is because the jitter of frequency offset exists in the real networks, which induces errors in the control channel estimation, and the impact of these errors will become larger when the signal strength of signatures increases comparing with that of data frames. When $SINR(Data)$ is lower than $-8dB$, DIC will have a comparative higher PER value. However, we consider the technique of SIC [20] can be exploited in this scenario to reduce the PER as the control frames can be detected through normal demodulation at first.

4.6 Performance Evaluation

In this section, I evaluate ICMR's performance improvement comparing with IRMA and the 802.11 standard. The two mechanisms in the 802.11 standard that we choose to compare are (1) PCS, which only uses the physical carrier sense mechanism to avoid interferences, (2) PCS+VCS, which uses RTS/CTS control frames to coordinate between nodes. All the protocols are implemented in the ns-2 simulator.

The basic parameters used in the simulations are listed in Table 4.2.

I do not implement the physical layer processes of the signature detection and dis-

Table 4.2: Simulation parameters.

Parameter	**Value**	**Parameter**	**Value**
Preamble	$20\mu s$	SIFS	$16\mu s$
Time slot	$9\mu s$	DIFS	$34\mu s$
Signature	$13.3\mu s$	CWmax	$1023\mu s$
p/q	20/150	CWmin	$15\mu s$
m	8	n	16

cernible interference cancellation in the simulation, and just simplify them based on the calculated $Pr(Signature)$ and $Pr(Data)$. The signature detection of the control frames is implemented as follows: If $SINR = Pr(Signature) - Pr(Data) > -5dB$, the signatures can be obtained correctly with the probability of 100%; if $-10dB < SINR \leq -5dB$, the probability is 99%; otherwise, if $SINR \leq -10dB$, the signatures will be ignored. The discernible interference cancellation mechanism is implemented as follows: If $Pr(Data) - Pr(Signature) > -6dB$, the data frame can be detected correctly with the probability of 100%; Otherwise, the data frame will be discarded. We set the transmission rate be $6Mbps$, the transmission range be $500m$, and the carrier sense range be $700m$ in the following simulations.

4.6.1 Linear Topology

I first use a simple four-node linear topology to evaluate the effectiveness of ICMR comparing with other protocols, as shown in Fig. 4.13. The network has two links $S1 \rightarrow R1$ and $S2 \rightarrow R2$, the transmitter-receiver distances of both links are the same and are denoted by d, the receiver-receiver distance is denoted by d_1. We conduct the simulation under three scenarios: (1) $d = 100m$, which is much smaller than the transmission range of $500m$; (2) $d = 200m$, which is about one-half of the transmission range; (3) $d = 400m$,

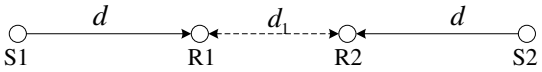
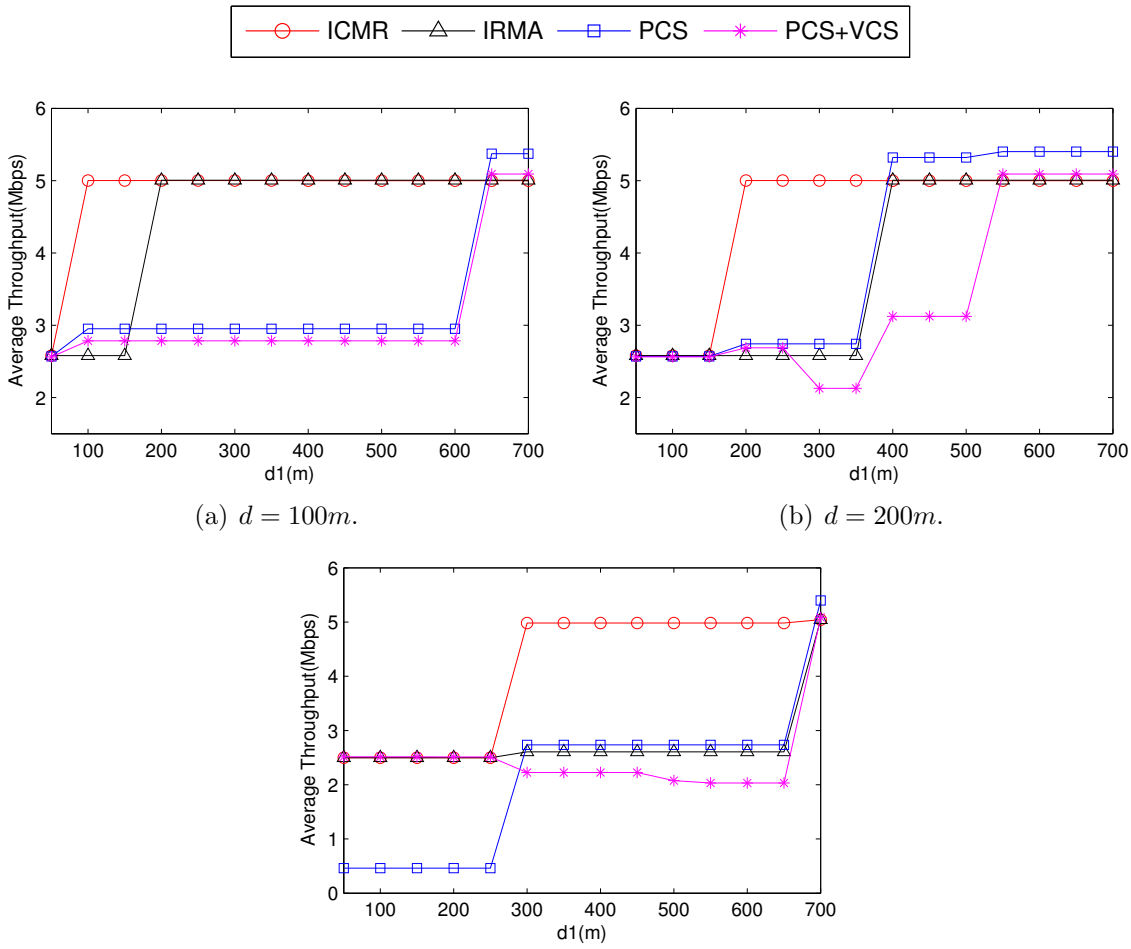


Figure 4.13: A linear network topology with four nodes $R1$, $S1$, $S2$ and $R2$.

which is about the transmission range. For each scenario, we change d_1 from $50m$ to $700m$ to evaluate how d can affect the performance of each protocol. Each link has a constant bit rate (CBR) flow set up at the sender to be transmitted to the receiver. The packet length is fixed to be $1500bytes$ in the simulation.

Fig. 4.16 shows the aggregate throughput of the network with different d_1 when d is set to be $100m$, $200m$ and $400m$, respectively. The simulation results can be summarized into three main cases:

Case 1: $d + d_1 < d_{IR}$. The corresponding scenarios are $d_1 < 100m$ in Fig. 4.14(a), $d_1 < 200m$ in Fig. 4.14(b) and $d_1 < 300m$ in Fig. 4.14(c), where all the senders and receivers are in the interference range of the other link, concurrent transmissions are prohibited by all the protocols to avoid interferences. Note that two scenarios should be discussed separately in this case. When $2 \cdot d + d_1 < d_{CS}$, which means the two senders are in the carrier sense range of each other, the four protocols has similar performance, as shown in Fig. 4.14(a) when $d_1 < 100m$ and Fig. 4.14(b) when $d_1 < 200m$. However, when $2 \cdot d + d_1 > d_{CS}$, the two senders cannot carrier sense each other, the performance of PCS degrades dramatically. As shown in Fig. 4.14(c), the average throughput of PCS is nearly zero when $d_1 < 300m$, as the two links will "threaten" each other but cannot utilize the physical carrier sense to avoid the interference. This is a typical hidden terminal problem. On the contrary, ICMR, IRMA and PCS+VCS can combat this problem and has similar performance through coordinating among nodes using control frames.



(a) $d = 100m$. (b) $d = 200m$.

(c) $d = 400m$.

Figure 4.14: Average throughput in terms of d_1.

Case 2: $d_1 < d_{IR} \leq d + d_1$. The corresponding scenarios are $100m \leq d_1 < 200m$ in Fig. 4.14(a), $200m \leq d_1 < 400m$ in Fig. 4.14(b) and $300m \leq d_1 < 700m$ in Fig. 4.14(c), where the senders are out of the interference range but the receivers are within the interference range of the other link. Concurrent transmissions are prohibited by IRMA, PCS and PCS+VCS because of the *R-orient receiver extra-collision-avoidance*, but they can be exploited by ICMR, leading to a 2× throughput comparing with the other protocols. There are also two scenarios that should be discussed separately in this case. When $2 \cdot d + d_1 < d_{CS}$, such as $100m \leq d_1 < 200m$ in Fig. 4.14(a) and $200m \leq d_1 < 300m$ in

Fig. 4.14(b), PCS+VCS only has a little performance degradation (about 3%) comparing with PCS, because of the overhead induced by RTS and CTS control frame transmissions. However, when $2 \cdot d + d_1 > d_{CS}$, such as $300m \leq d_1 < 400m$ in Fig. 4.14(b) and $300m \leq d_1 < 700m$ in Fig. 4.14(c), as the two senders are out of carrier sense of each other, the exchange of RTS and CTS may worse affect the other link's data reception, leading to about 22.4% performance degradation comparing with PCS.

Case 3: $d_1 \geq d_{IR}$. The corresponding scenarios are $d_1 \geq 200$ in Fig. 4.14(a), $d_1 \geq 400m$ in Fig. 4.14(b) and $d_1 \geq 700$ in Fig. 4.14(c), where all the senders and receivers are out of the interference range of the other link. When $2 \cdot d + d_1 < d_{CS}$, such as $200m \leq d_1 \leq 600m$ in Fig. 4.14(a), concurrent transmissions are permitted by ICMR and IRMA, but prohibited by PCS and PCS+VCS because of the physical carrier sense. When $2 \cdot d + d_1 > d_{CS}$, such as $d_1 > 600m$ in Fig. 4.14(a), $d_1 \geq 400m$ in Fig. 4.14(b) and $d_1 \geq 700m$ in Fig. 4.14(c), the two senders cannot carrier sense each other, concurrent transmissions are permitted by ICMR, IRMA and PCS. Both ICMR and IRMA have a little performance degradation (about 6%) comparing with PCS, because of the overhead induced by transmitting control frames and signatures. For PCS+VCS, two scenarios should be discussed separately. When $d_1 < d_{TX}$, such as $400m \leq d_1 \leq 500m$ in Fig. 4.14(b), the two receivers $R1$ and $R2$ can get the CTS from the other link correctly to update their NAV states, making PCS+VCS prohibit the concurrent transmissions. When $d_1 > d_{TX}$, such as $d_1 > 500m$ in Fig. 4.14(b) and $d_1 > 700m$ in Fig. 4.14(c), PCS+VCS permits the concurrent transmissions and it has the similar performance as the other protocols.

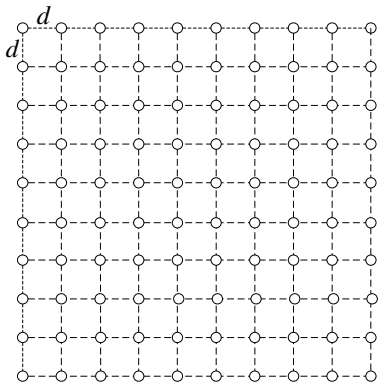


Figure 4.15: A grid topology, where the distances of adjacent nodes d are set to be 100m, 200m and 400m, respectively.

4.6.2 Random Topology

In this experiment I evaluate the performance of ICMR compared with other protocols in a more general scenario where networks have different densities.

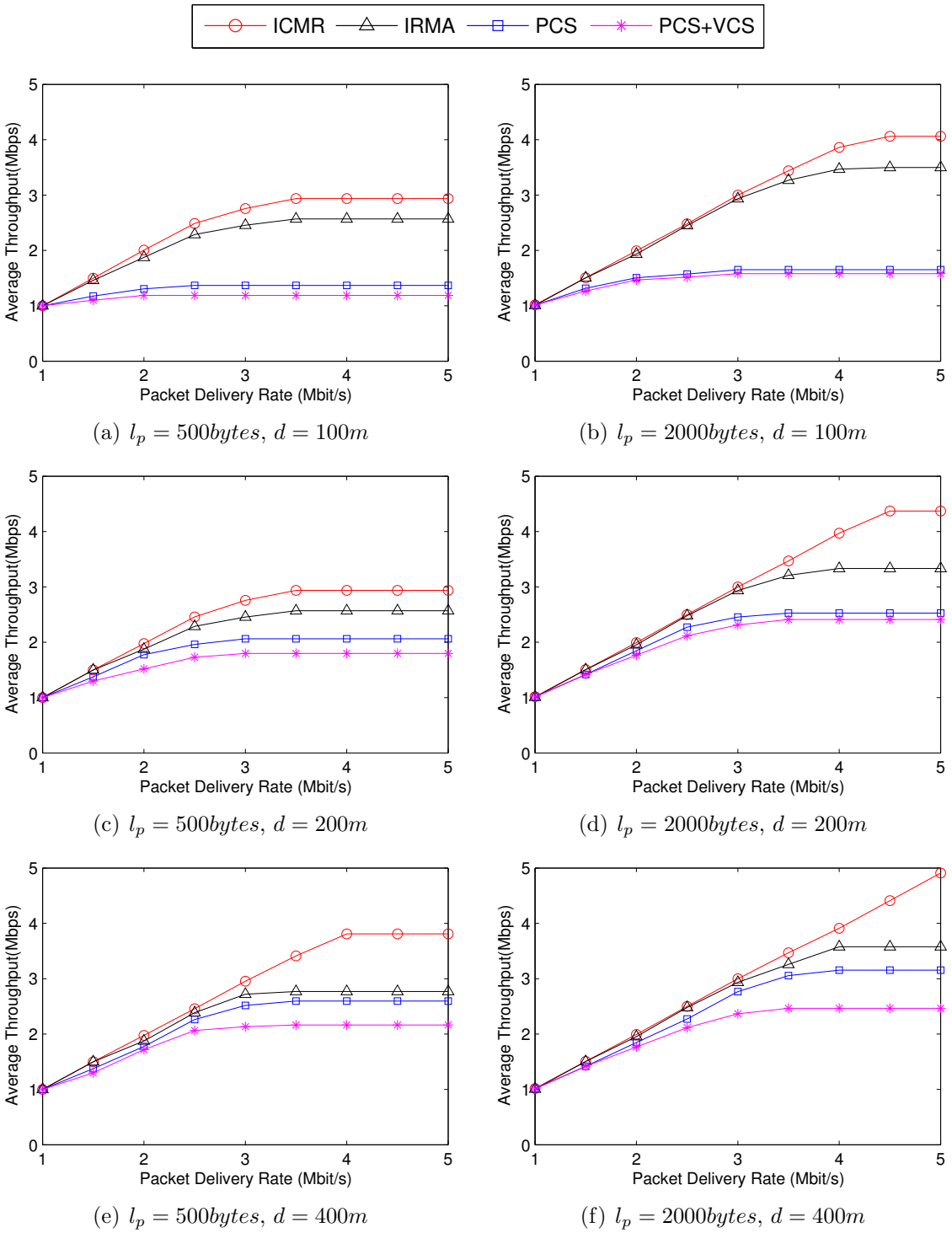
I set up three networks, each of which has 100 nodes deployed in a 10×10 grid, as shown in Fig. 4.15. We set the distances of adjacent nodes d to be $100m$, $200m$ and $400m$, making the networks have three different densities. For each network, I randomly select 10 transmitter-receiver links: I first randomly select one node as a transmitter, then select an adjacent node as its receiver. This process will be repeated for 10 times to generate 10 links in each network.

Fig. 4.16 shows the average throughput of ICMR comparing with the other three protocols for different packet delivery rates when the packet length l_p is $500bytes$ and $2000bytes$, respectively. The figure indicates that the average throughput of all protocols increases along with the increases of the packet delivery rate and packet length. The figure also indicates that PCS+VCS has the lowest performance in all the scenarios. Although PCS nearly has the lowest performance in the line topology when $d = 400m$ because

of the hidden terminal problem, as shown in Fig. 4.14(c), it has a better performance than PCS+VCS in the random topology even when $d = 400m$, as shown in Fig. 4.16(e) and Fig. 4.16(f), the reason is that PCS faces a more serious unfairness issue, which largely avoids collisions and allows the network to achieve a higher average throughput. Fig. 4.16 also indicates that the performance of the four protocols increases along with the increases of the packet length l_p. This is because the overhead induced by control frames are much larger when the packet length is shorter, leading to a lower performance.

We can see from Fig. 4.16 that both ICMR and IRMA can improve the network performance through exploiting concurrent transmissions and avoiding collisions, comparing with PCS and PCS+VCS, and ICMR can outperform the other protocols in all cases. The throughput gain of ICMR over IRMA increases along with the increases of d, that means the throughput gain increases along with the deceases of network density. As shown in Fig. 4.16, when the packet length is $l_p = 2000bytes$, ICMR's throughput gain is about 16.1% over IRMA when $d = 100m$. This value increases to 31.2% when $d = 200m$, and it increases to 37.3% when $d = 400m$. The situation is similar when $l_p = 500bytes$. These results coincide with the theoretical analysis in Section 4.4. However, the throughput gain of both ICMR and IRMA over PCS or PCS+VCS decreases along with the increases of d. As shown in Fig. 4.16, when $l_p = 2000bytes$, ICMR's throughput gain is about 146.2% over PCS and 157.8% over PCS+VCS when $d = 100m$. These values decrease to 55.6% and 99.1% respectively when $d = 400m$.

In summary, ICMR can outperform other protocols in all cases because concurrent transmission opportunities are effectively exploited by this protocol. The throughput gain over PCS or PCS+VCS will be larger in a denser network, and the throughput gain



(a) $l_p = 500bytes$, $d = 100m$

(b) $l_p = 2000bytes$, $d = 100m$

(c) $l_p = 500bytes$, $d = 200m$

(d) $l_p = 2000bytes$, $d = 200m$

(e) $l_p = 500bytes$, $d = 400m$

(f) $l_p = 2000bytes$, $d = 400m$

Figure 4.16: Average throughput in terms of packet delivery rate in the random topology, under three transmission rates and two packet lengths.

over IRMA will be larger in a sparser network.

4.7 Summary

In this chapter, I conclude that the 802.11 standard waste transmission and reception opportunities from two aspects, including the *CA-CF problem* and the *varied-IR problem*. To enhance the IRMA protocol, I propose ICMR to further exploit reception opportunities through permitting the data frame being collided by the control frames, and propose a discernible interference cancellation mechanism to detect the data frame in this situation, so as to maximize the network performance. I define a link to have the concurrent transmission opportunity when its transmitter has the transmission opportunity and its receiver has the reception opportunity, and formulate both two opportunities from solving the two problems, then quantify and compare the opportunities among ICMR, IRMA and the 802.11 standard theoretically. I show the feasibility of the discernible interference cancellation mechanism through hardware experiments, and demonstrate ICMR's significant throughput improvement over IRMA and the 802.11 standard by ns-2.

Chapter 5

Coordinate Transmissions Centrally Based on Interference Resistance

In this chapter, I propose concurrency-based coordination mechanism (CCM), a cross layer protocol that can coordinate among nodes effectively in a centralized way to maximize concurrency and avoid data packet interference in WLANs. The design of CCM contains OpenCCM which is based on the architecture of software defined network to schedule the transmissions in both the uplink and downlink directions centrally to maximize transmission concurrency. It also contains an interference-resistant mechanism in the physical layer that can make the control message transmitted with the data packet simultaneously to eliminate the coordination overhead. Experiment results with USRP2 demonstrate the feasibility of the interference-resistant mechanism, and simulations based on ns-2 demonstrate the performance improvement of CCM comparing with other protocols.

This chapter is organized as follows. Section 5.1 gives an introduction of CCM. Section 5.2 describes the design and implementation of the interference resistance mechanism in the physical layer. Section 5.3 shows how OpenCCM can coordinate the downlink and

uplink transmissions efficiently to increase the network performance, based on the CCM PHY. Section 5.4 evaluates the performance improvement of CCM through simulations. Section 5.5 concludes this chapter.

5.1 Overview

Due to the inevitable interferences existed in WLANs, improving the network performance through interference management is a well-known concept and attracts much research interest, which mainly falls into two categories. Exploiting concurrent transmissions and avoiding interference [24,32,78] emphasize on coordinating among nodes to reduce mutual interferences of simultaneous data transmissions. On the contrary, interference cancellation [17, 20, 76] attempts to propose a physical layer strategy to recover the interfered data packet from interferences instead of avoiding them.

Chapter 3 and Chapter 4 analyze the CSMA and RTS/CTS mechanism in the 802.11 standard, and conclude that the mechanisms degrade the network performance because of two problems, including the *CA-CF problem* and *varied-IR problem*. The two chapters then propose two distributed protocols, IRMA and ICMR, to exploit the transmission and reception opportunities respectively from solving the two problems, so as to improve the network performance. However, both protocols cannot reduce some coordination overhead existed in the 802.11 standard, such as backoffs, DIFS and the transmission of control frames.

Nowadays, the concept of software defined network (SDN) for WLAN management using a centralized controller is an emerging method to improve the throughput of WLAN [74]. Based on this concept, data transmissions can be coordinated efficiently

through utilizing the WLAN infrastructure, where multiple APs connected by wired networks are treated as one virtual AP in the protocol design. Current related work also falls into two classes. TRACK [23], OpenTDMF [90] and COAP [57] focus on the upper layer design. They utilize APs to allocate data transmissions and avoid interferences, but transmissions from clients cannot be coordinated in an efficient way. Symphony [4] focuses on the physical layer design. It encourages interferences of data packets at APs and then lets APs cooperatively recover the collided packets by utilizing a Zigzag-like [17] decoding process, but it lacks an effective mechanism in the MAC layer. The lack of protocol design from both the physical layer and upper layers motivates us to design a cross-layer protocol to benefit from both aspects, so as to further improve the network performance.

In this chapter, I propose the concurrency-based coordination mechanism (CCM), a novel cross-layer protocol, to maximize concurrent transmissions and eliminate the coordination overhead in WLANs, so as to increase the network performance. The architecture of CCM inherits from the SDN design, as shown in Fig. 5.1. The control plane, which is called OpenCCM in this protocol, is separated from the data plane. The OpenCCM controller is responsible to manage all the APs through the OpenCCM interface that resides at APs. Besides OpenCCM, CCM designs an interference resistant mechanism in the PHY layer to make the coordination information transmitted concurrently with data packets, and make both the interfered information decoded successfully, thus eliminate the coordination overhead. By utilizing the received coordination information from the CCM PHY, the OpenCCM can well coordinate all APs and clients in the network, so as to maximize concurrent transmissions to improve the network performance.

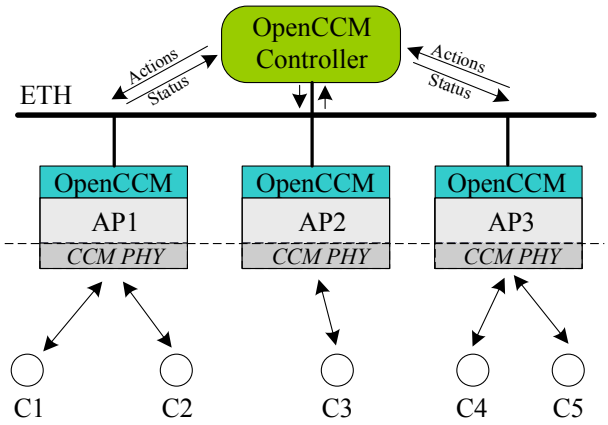
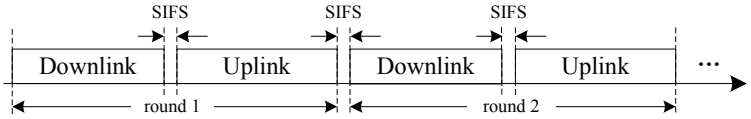


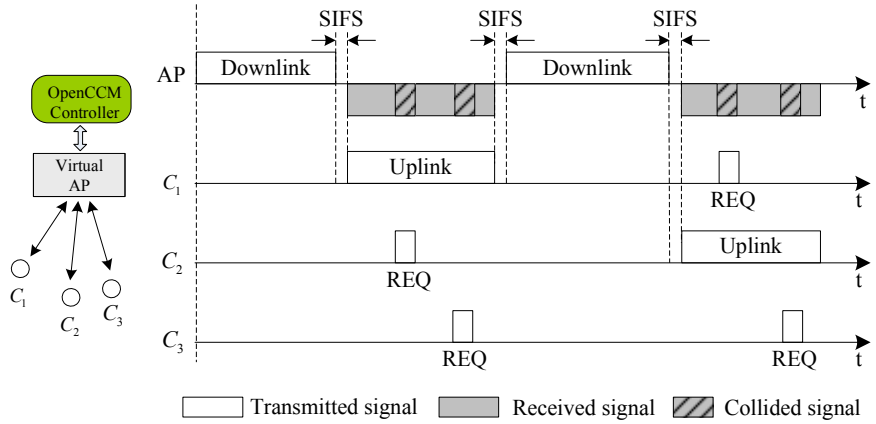
Figure 5.1: The CCM architecture.

Fig. 5.2(a) shows an overview of the CCM transmissions. The transmissions are divided into rounds. Each round contains a downlink semi-slot, which is from APs to clients, and an uplink semi-slot, which is from clients to APs. The downlink semi-slot may contain multiple downlink data transmissions from different APs, and the uplink semi-slot may contain multiple uplink data transmissions from different clients. The coordination information, which is carried by a REQ (REQuest-to-send) control message in CCM, can be transmitted concurrently with data packets in the uplink direction.

To illustrate the CCM protocol more clearly, I give a simple network scenario with one virtual AP and three clients, as shown in Fig. 5.2(b). Note that the virtual AP can be either one AP or multiple APs connected with each other by wired networks. In CCM, the OpenCCM controller schedules all the APs' and clients' transmissions. It maintains a list of APs and clients that have data packets to send out and makes AP exchange data with the clients according to the list. AP can transmit downlink data packets together with the control information, which allocates the clients which can transmit their data packets in the next uplink transmission. Upon the completion of the downlink transmission, after a SIFS, the polled client (node C_1 in Fig. 5.2(b)) can transmit its data



(a) The overview of CCM transmissions.



(b) The time sequence diagram of nodes in a scenario of CCM

Figure 5.2: The CCM transmissions.

packet, while some other clients (nodes C_2 and C_3 in Fig. 5.2(b)) can transmit their on-demand REQ messages simultaneously. Thus, AP will receive a mixed signal composed of both the data packet from C_1 and the REQ messages from C_2 and C_3. It conducts an interference-resistant mechanism in the physical layer to decode both the REQ messages and the data packet. According to the received REQ messages, the controller will update the scheduler (a polling list) adaptively to arrange the next clients for the next round uplink transmission.

One key issue in CCM is to design an interference resistance mechanism in the physical layer to make the REQ messages transmitted with the data packet concurrently to reduce the coordination overhead. As clients only need to convey a small amount of information for the use of coordination, each information can be represented as a signature (a known sequence), which can be decoded correctly by using the signature detection

method (SDM) in Section 3.3.3. Meanwhile, when an AP receives a mixed signal containing the coordination information and a data packet, the data packet can also be recovered correctly after detaching the signatures from the mixed signal, using the discernible interference cancellation (DIC) process in Section 4.3. Thus, through this mechanism, the REQ message can be transmitted concurrently with data packets without harming the effectiveness of original data transmissions.

Another key issue in CCM is to design OpenCCM to make the data transmissions coordinated centrally and efficiently. The OpenCCM controller should determine the downlink and uplink transmissions in each round, and make them scheduled simultaneously to increase transmission concurrency and avoid mutual interferences in both directions. Meanwhile, high priority links should be scheduled headmost to minimize the packet delivery delay. Thus, I make the OpenCCM controller maintain both uplink and downlink polling lists, which contain the information of the data packets to be sent out. I also make the controller construct a set of interfering lists through empirical observations on the packet losses. Based on the polling lists and the interfering lists, besides maximizing concurrent transmissions, OpenCCM makes high priority links scheduled at first and also makes other links have fair transmission opportunities.

The main contributions in this chapter are summarized as follows:

- I exploit the interference resistance mechanism in the physical layer, which allows REQ messages to be transmitted concurrently with the data packet and both types of information can be decoded correctly. This mechanism makes CCM eliminate the coordination overhead.

- With the support from the CCM PHY, I exploit OpenCCM to coordinate the downlink and uplink transmissions centrally, so as to maximize transmission concurrency, minimize packet delivery delay, and avoid mutual interferences of data packets.
- I demonstrate CCM's throughput improvement through simulations. The results show that CCM can outperform the 802.11 standard and other state-of-the-art protocols significantly.

5.2 Design of CCM PHY

In this section, I will first accomplish the REQ message design, then illustrate the architecture of CCM PHY. Finally, a power control mechanism is proposed to optimize the performance of CCM PHY.

5.2.1 REQ Message Design

To accomplish the interference resistance uplink transmission in CCM, the REQ message should be carefully designed so that it can carry effective coordination information, and can be transmitted concurrently with a data packet from another client.

As shown in Fig. 5.3, the REQ message is designed to contain three fields, including Preamble, S-TA and S-EXT, each of which is filled with a known signature. I design the Preamble to indicate the arrival of a REQ message in the received signal, which will be filled with a global-unique known signature s_P. I design S-TA field to carry the client's own address, and design a set of sequences, $S_{TA} = \{s_1, \ldots, s_N\}$, to represent the addresses of clients, where N indicates the maximum number of clients in the network. The controller that manages all the APs will allocate a unique $s_k (s_k \in S_{TA})$ to each client

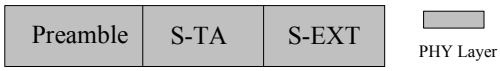


Figure 5.3: The format of REQ message.

when the client is associated to a specific AP. The client then preserves this s_k as its own address and fills it in the S-TA field when transmitting the REQ message. We also design S-EXT field to carry the length and priority of a packet that will be transmitted from the client, and design a set of signatures, $S_{EXT} = \{S_{u\times v}\}$, to represent the combination of the two information:

$$\mathbf{S_{u\times v}} = \begin{pmatrix} s_{11} & s_{12} & \dots & s_{1v} \\ s_{21} & s_{22} & \dots & s_{2v} \\ \vdots & \vdots & \ddots & \vdots \\ s_{u1} & s_{u2} & \dots & s_{uv} \end{pmatrix},$$

where s_{ij} is a signature, the length indicator i represents a maximum packet length, and the priority indicator j represents a priority of the data packet. Here, u and v denote the maximal values of i and j, respectively.

As the length of MPDUs cannot exceed a threshold l_{max} according to the 802.11 standard, we divide l_{max} into u segments, each of which has a length of $L_{seg} = \lceil \frac{l_{max}}{u} \rceil$. Therefore, each packet length l_p can be mapped to a specific length indicator $i = \lceil \frac{l_p}{L_{seq}} \rceil$. In this thesis, I set $u = 8$ to represent eight packet lengths. I then set $v = 2$, that means, the priority indicator j with the values of 0 and 1 represents a low priority and a high priority, respectively.

5.2.2 Description of CCM PHY

In CCM, the downlink transmission is interference-free while the uplink is interference-resistant. The physical layer processes of APs and clients in the downlink transmission are exactly the same as 802.11 standard. Here we focus on the mechanism in the uplink

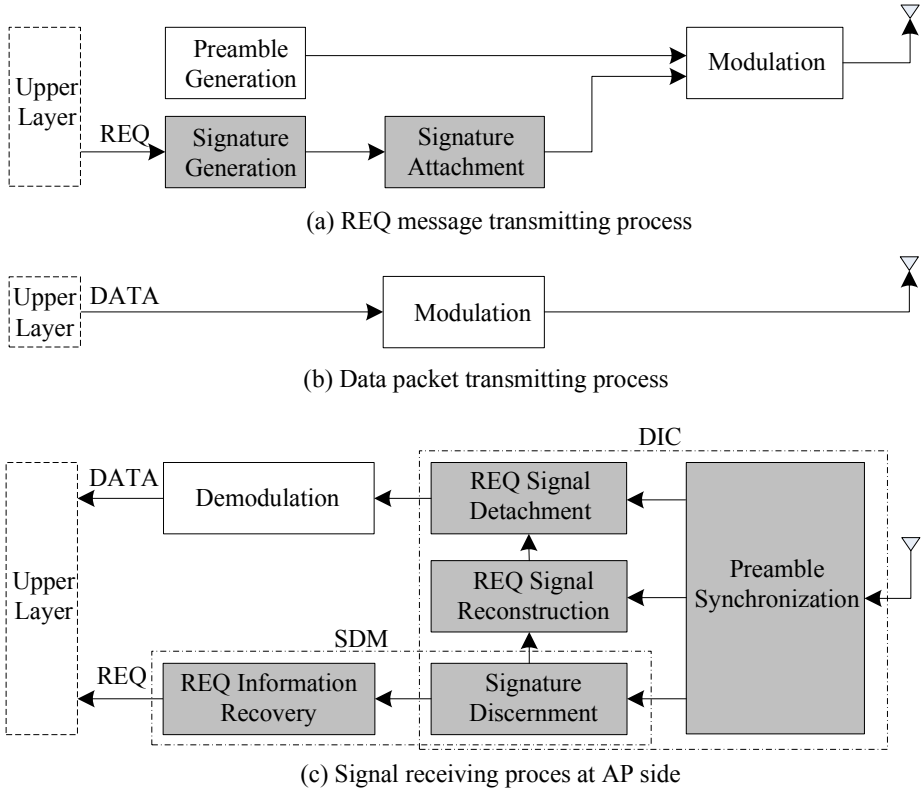


Figure 5.4: Architecture of CCM PHY.

transmission.

Fig. 5.4 illustrates the architecture of CCM PHY. White blocks indicate the processes of the 802.11 standard. Comparing with the 802.11 standard, CCM PHY adds some new components to accomplish the interference-resistant uplink transmission, shown as the grey blocks in Fig. 5.4.

In the transmitting process, the bit stream of a packet from the upper layer is mapped into complex samples after the digital modulation.

When transmitting a REQ message, as shown in Fig. 5.4(a), a client first generates known signatures to represent the coordination information. Each signature is filled in the corresponding field of REQ, then transformed into sample sequences and broadcast

after the modulation.

The process of transmitting a data packet is the same as the 802.11 standard, as shown in Fig. 5.4(b). The bits of a data packet are mapped into complex samples and broadcast after the modulation.

As shown in Fig. 5.4(c), after receiving a mixed signal containing a data packet and some REQ messages, one AP begins to detect both kinds of information. The AP continuously conducts the preamble synchronization process to determine the arrival of REQ message and their positions, then the REQ detection process is to discern signatures carried in the REQ message and recover the original information, including the client's address, the packet length and the packet priority. The process is similar as IRMA's CTS/ACK detection through the signature detection method (SDM). Meanwhile, the processes of data signal recovery is estimating the channel parameters to reconstruct the REQ signals and detaching them from the mixed signal to recover the original data samples, which will be transformed into bits after demodulation. This process is similar as ICMR's data signal recovery process through discernible interference cancellation (DIC). As the basic process of CCM PHY is the combination of SDM and DIC, which have been discussed thoroughly in Section 3.3.3 and Section 4.3, respectively, I will omit the detailed process of CCM PHY in this chapter, including the preamble synchronization, signature discernment, REQ signal reconstruction and detachment.

Meanwhile, the feasibility of CCM PHY has also been naturally evaluated in the previous works based on the USRP2 platform: the signature detection has been evaluated in Section 3.4, while the control signal reconstruction and data packet detection have been evaluated in Section 4.5. In this chapter, I will use these experiment results directly.

5.2.3 Design of Power Control

The performance of the CCM PHY is not always acceptable according to the experiment results in Section 4.5. As shown in Fig. 4.12, the packet error rate is comparatively high when the received signal strength of the data packet is around $4dB$ higher than that of the REQ message. This will obviously degrade the throughput of CCM due to a large number of retransmissions of data packets. To combat this problem, I further design a power control mechanism in CCM to make the data packet and REQ messages have comparable received signal power at AP.

Suppose the transmitted downlink's signal power at AP is denoted by $P_t(downlink)$, the corresponding received signal power at one client is denoted by $P_r(downlink)$, we have $P_r(downlink) = \lambda\frac{P_t(downlink)}{d^\alpha}$ [32], where λ and α are constant values, d is the distance between the AP and the client. Suppose $P_t(downlink)$ is fixed, after obtaining $P_t(downlink)$ and $P_r(downlink)$, the client can simply calculate its distance from AP to be $d = \sqrt[\alpha]{\frac{\lambda \cdot P_t(downlink)}{P_r(downlink)}}$. It will then determine the transmitted signal power of the uplink, denoted by $P_t(uplink)$, to make the received signal power of this link at AP, denoted by $P_r(uplink)$, have a constant value P_c. As $P_c = P_r(uplink) = \lambda\frac{P_t(uplink)}{d^\alpha}$, the client can calculate $P_t(uplink) = \frac{P_c \cdot P_t(downlink)}{P_r(downlink)}$. When all the clients transmit data packets or REQ messages using the calculated signal power $P_t(uplink)$, the collided data packet and REQ messages at each AP will have comparable values, that means, P_r(Data)-P_r(REQ)$\approx 0dB$, which can make both the data packet and REQ messages have high detection rate of about 100%.

5.3 Design of OpenCCM

In this chapter, I design OpenCCM to make the transmissions of data packets and REQ messages coordinated centrally and efficiently. The OpenCCM controller manages each AP through the OpenCCM interface which resides at APs. Similar with the OpenFlow interface defined in some previous works [50,90], OpenCCM interface also operates over a set of $\{FlowID, Actions\}$ tuples. Meanwhile, OpenCCM needs APs to be synchronized on μs level, so that the APs can execute the controller's instructions accurately. This issue has already been settled by OpenTDMF [90] currently. In this section, I will just give detailed discussion about how OpenCCM can leverage the coordination information obtained from CCM PHY to maximize concurrent transmissions and increase the network performance.

5.3.1 Overview of OpenCCM Process

In CCM, OpenCCM is responsible for coordinating the transmissions in both directions, as illustrated in Fig. 5.5.

In the downlink direction, the OpenCCM controller selects downlinks which have no mutual interference according to a set of *interfering lists* and a *DLink polling list*, and makes the selected APs transmit packets concurrently. Besides the data packet that one AP should transmit to a designated client, each downlink packet may further append three more parts if necessary: (1) an ACK to indicate the successful reception of a previous uplink data packet from that client; (2) the polled client that can send a data packet in the following uplink transmission; (3) the REQ_transmit clients and their REQ timeslot assignment information. All the information will be encapsulated into one

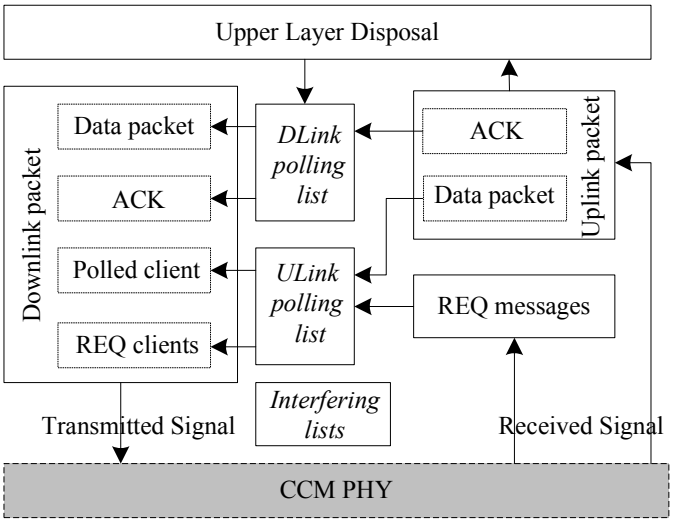


Figure 5.5: An overview of the OpenCCM process.

downlink packet and broadcast by an AP.

Upon receiving the downlink packet from APs, after a SIFS time, all the clients switch to the transmit mode. The polled client transmits a data packet, together with an ACK, if necessary, to indicate the successful reception of a previous downlink data packet to this client. Other clients should first check whether they have been assigned a REQ timeslot in this round, according to the appended third part information in the received downlink packet. If confirmed, the client will transmit a REQ message in the corresponding timeslot if it has data packets to be transmitted. Otherwise, it will keep silence and wait for an opportunity in the next round.

In the uplink direction, each AP that has just transmitted a downlink packet will obtain the received uplink data packet and REQ messages from the physical layer, while the data packet may contain an ACK to indicate a successful downlink data packet reception at the client. The data information will be used to complete the process in the upper layer, and all the information will be reported to the OpenCCM controller to

update the *ULink polling list*, the *DLink polling list* and the *interfering lists*.

Thus, the key issues in the OpenCCM process are concluded as follows: How to decide and make the clients to transmit REQ messages? How to construct the *interfering lists*? How to construct the *polling lists*? How to decide the downlink and uplink data packets? We will give detailed design of the four issues in the following part.

5.3.2 REQ_transmit Clients Determination

One key issue in CCM is to let clients send data packets and REQ messages concurrently in the interference-resistant uplink transmissions, so that the OpenCCM controller can update the *ULink polling list* and coordinate the clients' transmissions effectively. Although it is possible to detect all the information using the CCM PHY even when multiple REQ messages from different clients are overlapped in the channel, this mechanism will obviously increase the decoding error rate and make the design of CCM PHY more complicated. To simplify the system design, we adopt a time division multiplexing algorithm for sending REQ messages. The uplink transmission time is divided into several REQ timeslots, each of which will be assigned to one client by AP in the downlink transmission.

The number of REQ timeslots N_{ts} represents the number of clients that can send REQ messages during an uplink peroid. We set $N_{ts} = \lfloor \frac{t_{max}}{t_{REQ}+\sigma} \rfloor$, where t_{max} and t_{REQ} represents the duration of the maximum data packet and the REQ message, respectively, σ is the interval between two REQ messages to combat the time offset among clients. In this thesis, I set $\sigma = 10\mu s$ according to the experiment result in OpenTDMF [90].

Suppose the client set in the network is $\{C_1, C_2, \ldots, C_M\}$, and the number of clients

M is always larger than N_{ts}. To guarantee the fairness in the scheduling of uplink transmissions, we set a *flag* for each client C_i and denote it by $flag_i$ ($i \in [1, M]$), then utilize them to determine the REQ_transmitted clients in each round to make all the clients have comparable REQ transmission opportunities. The *flag* of each client is initiated to be zero and will be updated at the end of each uplink transmission according to the received REQ messages. The clients whose REQ messages are received in each round are preserved in a temporary set REQ_CLIENT. The update process is relatively simple and described in Algorithm 5.1.

Algorithm 5.1 The client's *flag* update algorithm

Input: $\{flag_i\}, i \in [1, M]$;REQ_CLIENT.
Output: The updated $\{flag_i\}, i \in [1, M]$;

```
1: for i = 1 : M do
2:     if C_i ∈REQ_CLIENT then
3:         flag_i = 0;
4:     else
5:         flag_i = flag_i + Num(REQ_CLIENT);
6:     end if
7: end for
```

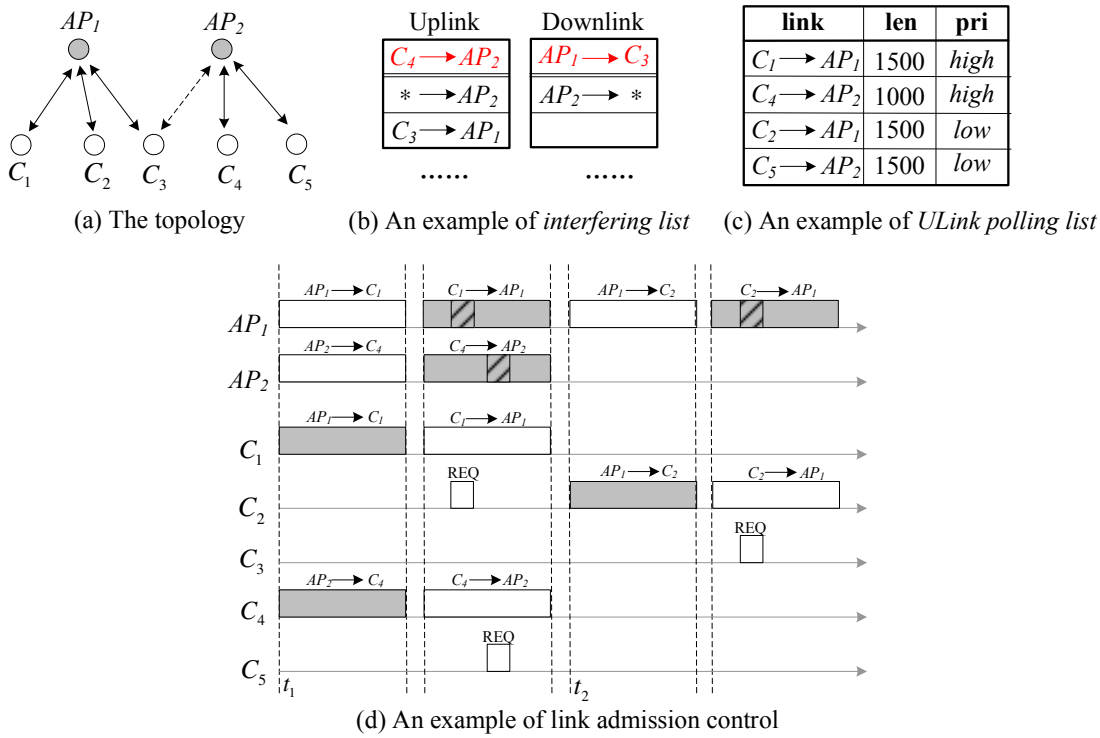
The client with a larger value in *flag* will have a higher opportunity to send a REQ message in the following round. Especially, when $flag_i$ is larger than a threshold γ ($\gamma = 2M$ in this thesis), the controller should set the client C_i as the REQ_transmit client soon as it has not been permitted to transmit REQ for a long time. This criterion will be considered in the link admission control in Section 5.3.5.

5.3.3 Interfering Lists Construction

The OpenCCM controller constructs a set of *interfering lists* through empirical observations, based on which it can maximize the concurrent transmissions in the scheduling.

To illustrate the *interfering lists* clearly, I use a multiple-APs scenario shown in Fig. 5.6(a) as an example. The network has two APs and five clients. Client C_1, C_2 and C_3 are associated to AP_1, C_4 and C_5 are associated to AP_2. For each link, the controller maintains an *interfering list* through a table whose entry is this link and contains the information of all the links that will interfere with this link's data transmissions. As shown in Fig. 5.6(b), the controller has constructed a table for the link $C_4 \rightarrow AP_2$. Its entry is $C_4 \rightarrow AP_2$, it maintains the links $* \rightarrow AP_2$ and $C_3 \rightarrow AP_1$ as the *interfering list* because they can interfere with $C_4 \rightarrow AP_2$'s data transmissions, where $* \rightarrow AP_2$ indicates all the uplinks whose destinations are AP_2. In Fig. 5.6(a), $* \rightarrow AP_2$ is specified to be $C_5 \rightarrow AP_2$. Similarly, for the link $AP_1 \rightarrow C_3$, a table is also constructed with the entry of $AP_1 \rightarrow C_3$, and the *interfering list* is $AP_2 \rightarrow *$, where $AP_2 \rightarrow *$ indicates all the downlinks whose sources are AP_2, and it can be specified to be $AP_2 \rightarrow C_4$ and $AP_2 \rightarrow C_5$ in this scenario. The *interfering lists* for all the other links can be constructed in the same way.

At the beginning of each round, when the controller determines the downlink and uplink transmissions, it will refer to the *interfering lists* to avoid interferences. All the links in each *interfering list* are prohibited to proceed concurrently with the entry link. For the search convenience, the *interfering lists* are divided into two groups, the uplink and downlink directions, through the entry of each list. As shown in Fig. 5.6(b), the interfering list of $C_4 \rightarrow AP_2$ is located in the uplink group, while that of $AP_1 \rightarrow C_3$ is located in the downlink group. Note that the two transactions in the uplink and downlink directions are interleaved in the CCM design, thus, the interfering lists in the uplink direction cannot contain downlinks, and vise versa.



(a) The topology (b) An example of *interfering list* (c) An example of *ULink polling list*

(d) An example of link admission control

Figure 5.6: An example of the multiple-APs scenario.

The initial interfering lists are empty, the controller permits concurrent uplink or downlink transmissions associated to different APs as it determines there is no mutual interference among the links. Collisions will occur and APs will collect the conflict information about which links have mutual interferences through packet losses, then report to the controller to update the *interfering lists*.

5.3.4 Polling Lists Update

In the OpenCCM process, the *DLink polling list* is updated by the information from the upper layer, and the *ULink polling list* is updated by the received REQ messages. Both *polling lists* have a set of data packet's information, each of which contains three kinds of information: the source and destination of the data packet, its packet length

and its priority. In this thesis, we suppose the data packet has two priority: *high* and *low*. All the packets with *high* priority will be in the superior location of the polling list, comparing with those with the *low* priority. The new incoming packet's information will be added to the *polling list* at the bottom of the packet set which has the same priority with the incoming one. Here we use the scenario in Fig. 5.6(a) as an example to illustrate the *ULink polling list* more clearly. As shown in Fig. 5.6(c), suppose the polling list has already contained two links' information, $C_1 \rightarrow AP_1$ and $C_2 \rightarrow AP_1$. After receiving two REQ messages from C_4 and C_5, whose packets' priorities are *high* and *low*, respectively, the controller will insert $C_4 \rightarrow AP_2$ after $C_1 \rightarrow AP_1$, and insert $C_5 \rightarrow AP_2$ after $C_2 \rightarrow AP_1$. The packet's information obtained from the upper layer will also be updated to the *DLink polling list* in the same way.

Upon sending a downlink data packet and receiving an ACK from the destination client, the AP will report this packet's information to the OpenCCM controller, so that the controller can remove it from the *DLink polling list*. Meanwhile, upon receiving an uplink data packet successfully, the AP will also report it to the controller to make it removed from the *ULink polling list*.

In principle, OpenCCM will make the *high* priority packets in the *polling lists* proceeded at first; within the same priority, it will apply a first-in-first-out method for the packet process.

5.3.5 Link Admission Control

Before the downlink and uplink transmissions of each round, the OpenCCM controller should determine the downlink data packets, the polled clients and the REQ_transmit

clients.

Based on the OpenCCM design, when determining the link admission in each round, the controller should guarantee that: (1) the admitted downlinks and uplinks have no mutual interference so that they can proceed concurrently, (2) the polled clients can detect the downlink packets successfully to get the polling information, (3) the REQ_transmit clients can also detect the downlink packets successfully to get the REQ timeslot information, (4) all clients have comparable packet transmission opportunity to guarantee the fairness.

The pseudocode of Algorithm 5.2 gives the details of link admission control in each round. I use two matrices, ULINK and DLINK, to restore the admitted uplinks and downlinks, and use a matrix REQ_TX_TEMP to restore the clients those have the opportunity to transmit REQ messages in this round. To simplify the description, I first denote some symbols to convey specific information. I suppose the controller has known all the association information between APs and clients, and use $C_i \propto AP_j$ to indicate the client C_i is associated to AP_j. We use $link1 \Leftrightarrow link2$ to indicate the two links have no mutual interference, and use $INV(A \rightarrow B)$ to indicate the inversion of link $A \rightarrow B$, that is $B \rightarrow A$. I use $link$.SA, $link$.DA and $link$.pri to indicate the source, destination and priority of $link$, respectively.

Note that the number of clients in REQ_TX_TEMP may be more than the REQ timeslots N_{ts}, the controller should select the clients whose *flag* are larger than the remaining ones' in REQ_TX_TEMP as the REQ_transmit clients in this round.

Fig. 5.6(c) gives an example of the link admission control in the multiple-APs scenario shown in Fig. 5.6(a). At the first round beginning from time t_1, the controller first

Algorithm 5.2 The link admission control in CCM

Input: $\{AP_1, AP_2, \ldots, AP_K\}$,$\{C_1, C_2, \ldots, C_M\}$;
The *DLink polling list*; The *ULink polling list*; The *interfering lists*.
Output: (1) The admitted downlinks and uplinks in DLINK and ULINK;
(2) The potential REQ_transmit clients in REQ_TX_TEMP;

$m := 0$; $n := 0$;
if find $AP_k \rightarrow C_i$ from *DLink polling list* $\bigwedge$ $(AP_k \rightarrow C_i)$.pri=high **then**
  $m := m + 1$; $AP_{temp} := AP_k$; DLINK(m) := $AP_k \rightarrow C_i$;
else if find $C_i \rightarrow AP_k$ from *ULink polling list* $\bigwedge$ $(C_i \rightarrow AP_k)$.pri=high **then**
  $n := n + 1$; $AP_{temp} := AP_k$; ULINK(n) := $C_i \rightarrow AP_k$;
else if find C_i whose $flag_i = max\{flag_j\ (j = 1, \ldots, M)\}$ $\bigwedge$ $flag_i > \gamma$ $\bigwedge$ $C_i \propto AP_k$ **then**
  Add C_i to REQ_TX_TEMP; $AP_{temp} := AP_k$; REQ_LINK:=$AP_{temp} \rightarrow C_i$;
  if find $AP_{temp} \rightarrow C_j$ from *DLink polling list* **then**
    $m := m + 1$; DLINK(m) := $AP_{temp} \rightarrow C_j$.
  end if
  if find $C_l \rightarrow AP_{temp}$ from *ULink polling list* **then**
    $n := n + 1$; ULINK(n) := $C_l \rightarrow AP_{temp}$.
  end if
else

  if get $AP_k \rightarrow C_i$ from the top of *DLink polling list* **then**
    $m := m + 1$; $AP_{temp} := AP_k$; set DLINK(m) = $AP_{temp} \rightarrow C_i$.
    if find $C_j \rightarrow AP_{temp}$ from *ULink polling list* **then**
      $n := n + 1$; ULINK(n) := $C_j \rightarrow AP_{temp}$.
    end if
  end if
end if
for $k = 1 : K$ **do**
  if find $AP_k \rightarrow C_i$ from *DLink polling list* $\bigwedge$ $AP_k \rightarrow C_i$ $\Leftrightarrow$\{REQ_LINK,DLINK(l)\}($l \in [1, m]$) **then**
    $m := m + 1$; $AP_{temp} := AP_k$; DLINK(m) := $AP_{temp} \rightarrow C_i$;
    if find $C_j \rightarrow AP_{temp}$ from *ULink polling list* $\bigwedge$ $C_j \rightarrow AP_{temp}$ $\Leftrightarrow$\{ULINK(l)\}($l \in [1, n]$) $\bigwedge$ $AP_{temp} \rightarrow C_j$ $\Leftrightarrow$\{DLINK(l)\}($l \in [1, m]$) **then**
      $n := n + 1$; ULINK(n) := $C_j \rightarrow AP_{temp}$.
    end if
  end if
end for
for $l = 1 : m$ **do**
  repeat
    if DLINK(l).SA$\rightarrow C_i$ $\Leftrightarrow$\{REQ_LINK,DLINK(l_1),$INV(DLINK(l_2))$\}, $l_1 \in [1, m], l_2 \in [1, n]$ **then**
      Add C_i to REQ_TX_TEMP.
    end if
  until All the $C_i \in \{C_1, \ldots, C_M\}$ $\bigwedge$ $C_i \propto DLINK(l).SA$
end for

gets a downlink $AP_1 \rightarrow C_1$ from the top of *DLink polling list*, assigns C_1 as the polled client according to the *ULink polling list*, then sets the link $AP_2 \rightarrow C_4$ that has no interference with $AP_1 \rightarrow C_1$ as another downlink, and assigns C_4 as another polled client as $C_4 \rightarrow AP_2$ has no mutual interference with $C_1 \rightarrow AP_1$. Finally, it sets C_2 and C_5 as the REQ_transmit clients and allocates two REQ timeslots to them. At the second round beginning from time t_2, the controller finds $C_3.flag$ is larger than γ, it sets C_3 as the REQ_transmit client since this client has not been permitted to transmit REQ for a long time. Meanwhile, C_3 should detect the downlink packet successfully so as to obtain its allocated timeslot in the uplink direction. The controller then allocates $AP_1 \rightarrow C_2$ as the downlink and C_2 as the polled client. The process of Algorithm 5.2 will be conducted at the beginning of each round to maximize the concurrent transmissions in the network.

5.4 Performance Evaluation

The goal of this section is to measure CCM's ability to improve the throughput in WLANs comparing with the 802.11 standard and another state-of-the-art protocol under two scenarios, a single-AP topology and a multiple-APs topology. The 802.11 standard recommends two kinds of coordination functions: DCF (Distributed Coordination Function) which is a distributed mechanism and is widely deployed in current networks, and PCF (Point Coordination Function) which is a centralized method and makes clients coordinated by AP through polling. Meanwhile, DCF contains two mechanisms: PCS which uses physical carrier sense to access a wireless channel, and PCS+VCS which uses both the physical and virtual carrier sense to access the channel. In this section, I intend to compare CCM with the three mechanisms in the 802.11 standard, including PCF, PCS

Table 5.1: Simulation parameters.

Parameter	**Value**	**Parameter**	**Value**
Preamble	$20\mu s$	SIFS	$10\mu s$
PIFS	$19\mu s$	DIFS	$34\mu s$
Time slot	$9\mu s$	CWmax	$1023\mu s$
u/v	8/2	CWmin	$15\mu s$

and PCS+VCS. I also compare CCM with OpenTDMF [90], a state-of-the-art protocol that utilizes the architecture of SDN to enable TDMA in WLANs. I implement all protocols in ns-2.

For the CCM protocol, I do not implement the interference resistance mechanism in the physical layer, but simplify it based on the received signal strength of REQ and data packet. We enable the power control mechanism in the simulation, thus the two signal strengths are comparable, and both the REQ message and the data packet can be detected successfully. The OpenTDMF divides time into slots and the slot size is fixed to be $2ms \sim 10ms$; it uses polling based method to control the uplink traffic, and designs group polling period for clients to contend for their uplink transmissions. Here I set the slot size to be $5ms$, and set the group polling period to be 10 time slots, that means, the APs trigger one group polling every 10 time slots.

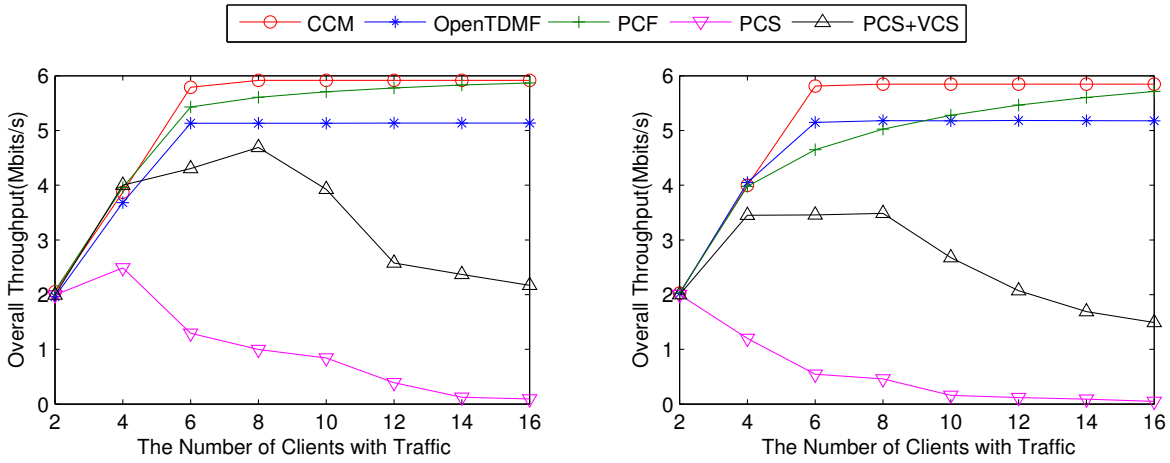
Table 5.1 lists the configuring parameters in our simulations.

5.4.1 The Single-AP Topology

5.4.1.1 Throughput Analysis

I first conduct the simulation under a single-AP topology where there are one AP and multiple clients in the network, and each client is randomly located around the AP. The

transmission rate is set to be $6Mbits/s$. We change the number of clients with traffic, which indicates the number of clients that have packets to send out, to observe the effectiveness of CCM. Each client has been configured a variable bit rate (VBR) flow, whose average packet delivery rate is $1Mbits/s$. Each flow has the same priority. The results in Fig. 5.7 demonstrates that CCM can outperform OpenTDMF and the three mechanisms in the 802.11 standard nearly in all cases. No matter the packet length l_p is $1500bytes$ or $500bytes$, when the number of clients with traffic increases, the throughput of PCS decreases dramatically due to the high probability of collisions in the hidden terminal scenarios, and the throughput of PCS+VCS also decreases because of the the increased collision probability of RTS/CTS frames, although the RTS/CTS mechanism can mitigate the hidden terminal problem and make the throughput relatively high comparing with PCS. On the contrary, CCM, OpenTDMF and PCF have higher throughput comparing with the two distributed 802.11 mechanisms, as the overhead of collisions, backoff and DIFS in both mechanisms can all be mitigated. Especially, when the number of clients is larger than 6, CCM has about 48.7% throughput improvement over PCS+VCS when $l_p = 1500bytes$, and this value increases to 114.8% when $l_p = 500bytes$, that's because the transmission overhead in PCS+VCS and PCS increases when l_p decreases. However, l_p has little effect to the throughput of CCM and OpenTDMF. CCM has about 16.1% throughput improvement comparing with OpenTDMF, as the group polling in OpenTDMF will degrade its throughput, while CCM permits the control message to be transmitted with the data packet concurrently, leading to a higher throughput in the network. The throughput of PCF increases along with the increase of the number of clients with traffic, as the overhead induced by null polling decreases in this situation. Especially, when the number of clients with traffic increases to about 16, PCF has the



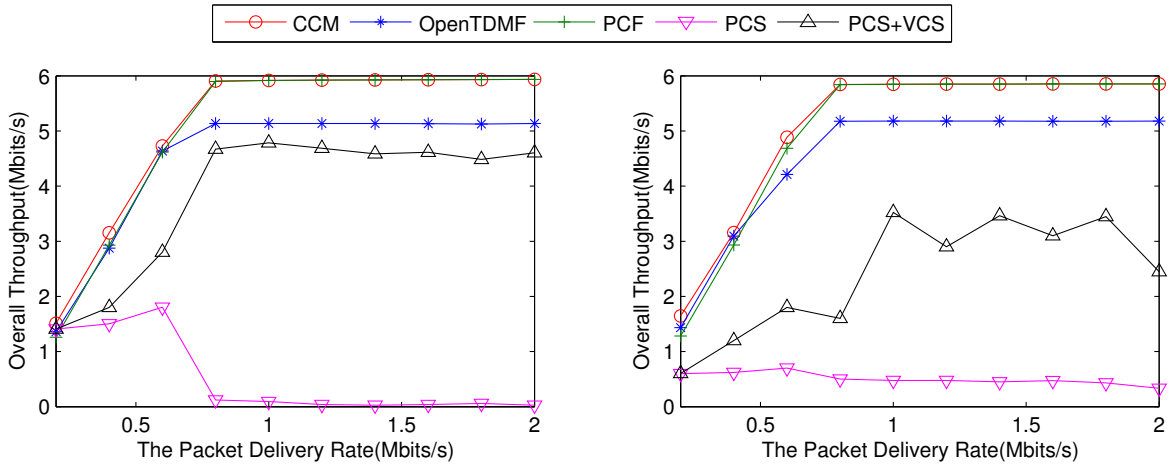
(a) $l_p = 1500bytes$ (b) $l_p = 500bytes$

Figure 5.7: The overall throughput in terms of the number of clients with traffic under two packet lengths in the single-AP scenario.

comparable performance with CCM.

As a conclusion, in this scenario, CCM outperforms OpenTDMF and PCF due to reducing the overhead induced by group polling and null polling, it outperforms PCS and PCS+VCS mainly due to avoiding collisions.

I also conduct a simulation to compare the throughput where the number of clients in the network is fixed to 8, but the average packet delivery rate of each client varies from $200Kbits/s$ to $2.0Mbits/s$, as shown in Fig. 5.8. We can see that the throughput of PCS maintains in a lower value, and the throughput of PCS+VCS decreases from about $4.6Mbits/s$ when $l_p = 500bytes$ (shown in Fig. 5.8(a)) to about $3.1Mbits/s$ when $l_p = 500bytes$ (shown in Fig. 5.8(b)). When the packet delivery rate is below $0.8Mbits/s$, CCM has comparable throughput with OpenTDMF; when the value is above $0.8Mbits/s$, CCM always has about 16.1% throughput improvement over OpenTDMF because of the overhead induced by group polling. As the null polling of PCF in this situation is very



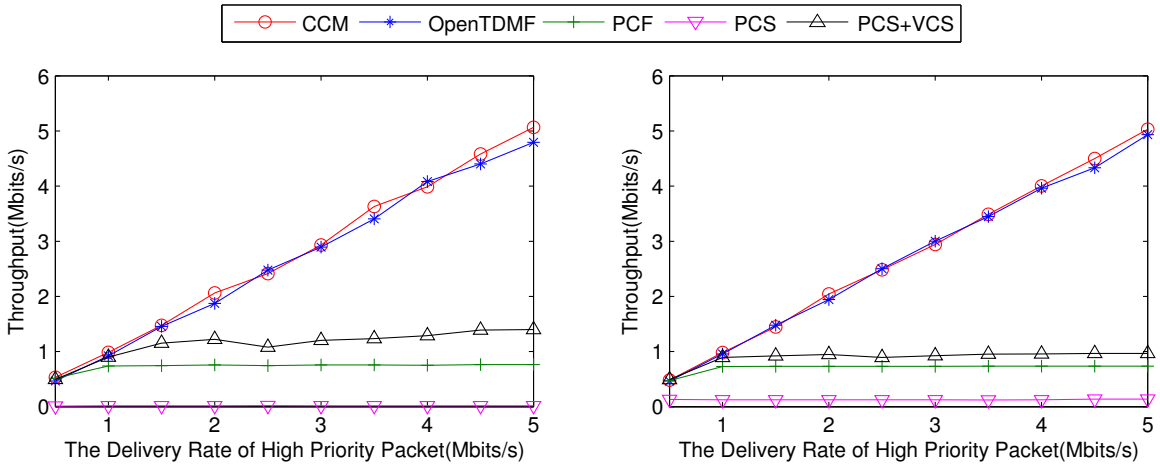
(a) $l_p = 1500bytes$ (b) $l_p = 500bytes$

Figure 5.8: The overall throughput in terms of packet delivery rate under two packet lengths in the single-AP scenario.

few, making PCF have comparable throughput with CCM nearly in all cases.

5.4.1.2 Delay Analysis

I then conduct a simulation under this single-AP topology to analyze the packet delivery delay when there are high priority flows in the network. Here we define the packet delivery delay to be the duration from the time that one packet is generated to the time that this packet is successfully received. The transmission rate is also set to be $6Mbits/s$, and the number of clients in the network is fixed to 8. We let 7 clients transmit low priority packets with a fixed packet delivery rate of $1.0Mbits/s$, and let one client transmit high priority packets, whose rate is varied from $0.5Mbits/s$ to $5.0Mbits/s$. Fig. 5.9 indicates that CCM and OpenTDMF have comparable throughput of the high priority flow, and they can outperform PCF, PCS and PCS+VCS dramatically, no matter l_p is 1500 or 500 bytes. Meanwhile, Fig. 5.10 indicates that CCM and OpenTDMF can process the



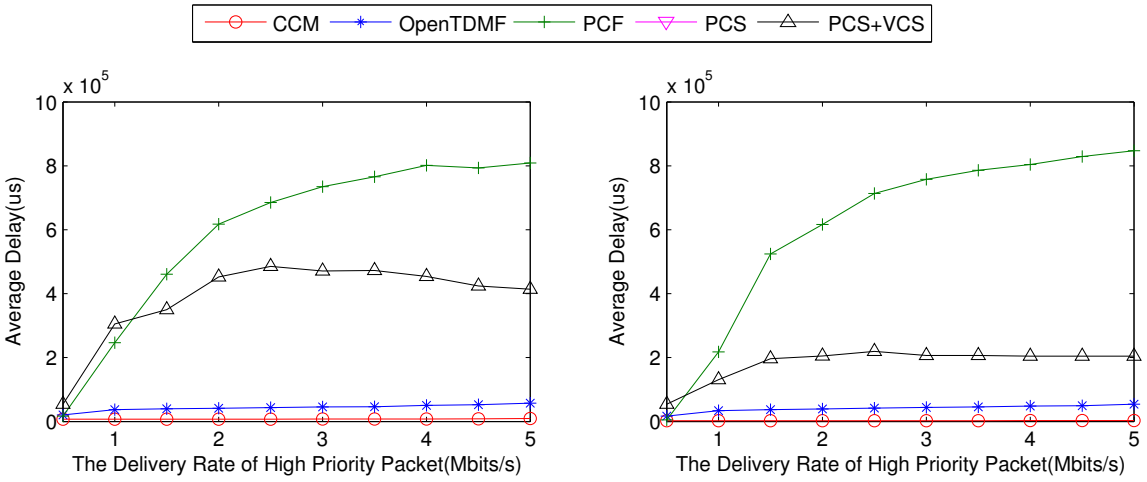
(a) $l_p = 1500bytes$ (b) $l_p = 500bytes$

Figure 5.9: The throughput of the high priority flow in terms of packet delivery rate under two packet lengths in the single-AP scenario.

high priority flow more rapidly than the other mechanisms. When $l_p = 1500bytes$, the average delay in CCM is about $6ms$, the value increases to about $50ms$ in OpenTDMF, about $400ms$ in PCS+VCS, and even about $800ms$ in PCF. CCM has the lowest delay as AP can make the clients with high priority packets transmit immediately through the REQ message, while OpenTDMF will make the client wait until the next group polling. When $l_p = 500bytes$, the performance is similar as that when $l_p = 1500bytes$, although the delay of each protocol decreases correspondingly. Note that we do not display the delay in PCS, as the throughput is very low and the delay is meaningless in this scenario.

5.4.2 The Multiple-APs Topology

In this simulation, I evaluate the performance comparison of CCM, OpenTDMF, PCS and PCS+VCS in a multiple-APs scenario. I do not take PCF into account as it cannot work in this multiple-AP scenario.

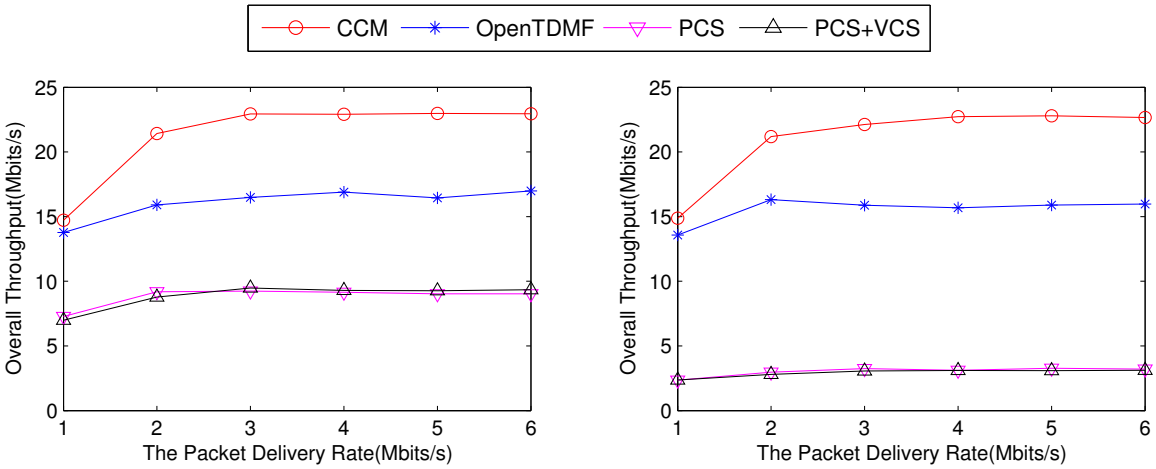


(a) $l_p = 1500bytes$ (b) $l_p = 500bytes$

Figure 5.10: The average delay of the high priority flow in terms of packet delivery rate under two packet lengths in the single-AP scenario.

5.4.2.1 Throughput Analysis

I randomly set up 5 nodes which act as APs in the network. Four clients are associated with one AP and are randomly located around it. I configure a VBR flow from each client to its AP, and also configure a VBR flow from each AP to a selected client. I change the average packet delivery rate of each flow from $1Mbits/s$ to $6Mbits/s$, and change the packet length to be 1500 bytes and 500 bytes, to get the simulation results. As shown in Fig. 5.11, although PCS has the lowest performance in the single-AP scenario, it has comparable throughput with PCS+VCS in the multiple-APs topology, that's because PCS faces a serious unfairness issue in this scenario, thus presents a higher throughput due to the collision avoidance. Fig. 5.11 also shows that CCM has about 151.6% and OpenTDMF has about 75.6% throughput improvement over PCS and PCS+VCS when $l_p = 1500bytes$, and the values increase to about 510.6% and 341.1% when $l_p = 500bytes$, because the overhead induced by collisions, backoff, DIFS and control frame transmissions



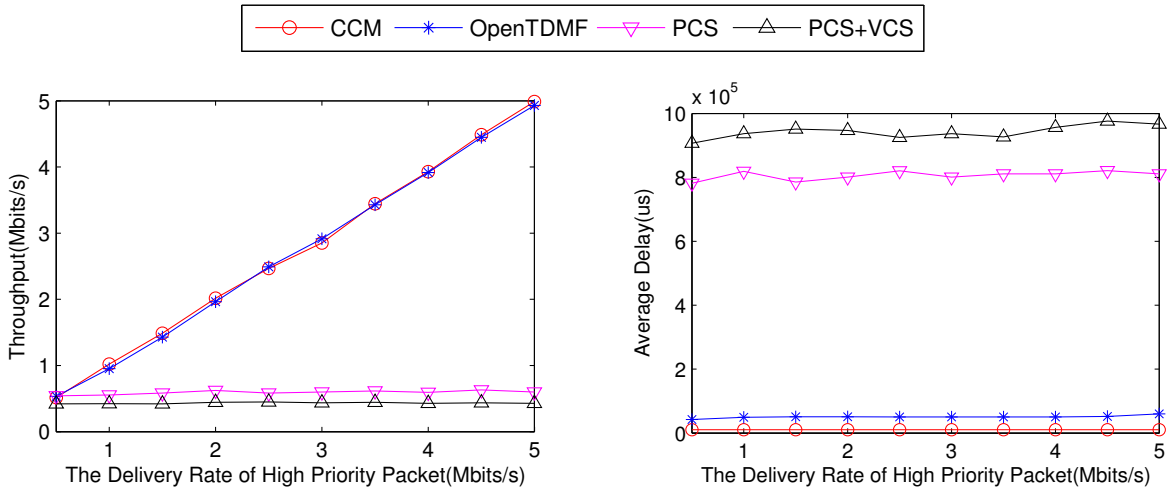
(a) $l_p = 1500bytes$ (b) $l_p = 500bytes$

Figure 5.11: The throughput of the high priority flow in terms of packet delivery rate under two packet lengths in the multiple-APs scenario.

increases when the packet length decreases in PCS and PCS+VCS mechanisms, but the overhead has little effect on CCM and OpenTDMF.

CCM further has the throughput improvement of about 45.5% over OpenTDMF when $l_p = 1500bytes$, and about 41.3% when $l_p = 500bytes$, which is larger than that in the single-AP scenario. That's because, besides the overhead induced by group polling, OpenTDMF coordinates channel access in the flow level, and two flows can proceed concurrently only if they have no mutual interference in both the uplink and downlink transmissions. This design prohibits some concurrent transmissions that have interference in one direction but have no mutual interference in the opposite direction.

As a conclusion, in this scenario, CCM outperforms OpenTDMF due to both increasing concurrent transmissions and reducing the overhead induced by group polling, while it outperforms PCS+VCS due to exploiting concurrency and reducing the overhead induced by backoff, DIFS and control frame transmissions.



(a) The throughput

(b) The average delay

Figure 5.12: The throughput and average delay of the high priority flow in terms of packet delivery rate when $l_p = 1500bytes$ in the multiple-APs scenario.

5.4.2.2 Delay Analysis

I also conduct a simulation under this multiple-APs topology to analyze the packet delivery delay of four protocols when there are high priority flows in the network. We let one client transmit high priority packets, whose rate is varied from $0.5Mbits/s$ to $5.0Mbits/s$, and let all the other links have low priority packets. Fig. 5.12 shows the throughput and average delay of the high priority flow when $l_p = 1500bytes$. The figure indicates that CCM and OpenTDMF have comparable throughput of the high priority flow, and they can outperform PCS and PCS+VCS dramatically. Meanwhile, CCM and OpenTDMF can process the high priority flow more rapidly than PCS and PCS+VCS. The average delay in CCM is about $10ms$, the value increases to about $70ms$ in OpenTDMF, and about 800-$900ms$ in PCS and PCS+VCS.

5.5 Summary

In this chapter, I propose CCM that can coordinate among nodes centrally in WLANs through both utilizing OpenCCM design that is based on the architecture of SDN and utilizing an interference-resistant mechanism in the physical layer, so as to mitigate the coordination overhead and maximize concurrent transmissions, achieving a higher throughput in the network. I also show CCM's significant throughput improvement over the other protocols by ns-2.

Chapter 6

Conclusions and Future Work

In this chapter, I first conclude this thesis by summarizing the original contributions, then give some suggestions for the future work.

6.1 Conclusions

In this dissertation, I study the interference problem in current wireless networks from analyzing the CSMA and RTS/CTS mechanisms in the widely-deployed 802.11 standard, and conclude that the 802.11 standard prohibits concurrency because of two problems, including the *CA-CF problem* and the *varied-IR problem*. Both problems will make nodes waste the transmission and reception opportunities. Meanwhile, besides the overhead induced by the two problems, these mechanisms also have some coordination overhead such as back-offs, DIFS and the transmissions of control frames. All the overheads will degrade the network performance. In this dissertation, I propose a cross layer approach that benefits from both the physical layer and the upper layer design to decrease the overhead in current wireless networks and improve the network performance. The physical layer design focuses on making the control information transmitted with data packets

successfully to eliminate its transmission overhead. The upper layer design is based on the physical layer design, and focuses on design different interference management protocols to maximize concurrency, avoid interference and reduce coordination overhead.

I first propose Interference Resistant Multiple Access (IRMA) to combat the exposed terminal problem and exploit transmission opportunities in wireless networks from solving the two problems. I propose a signature detection method in the physical layer to combat control frames' collisions, thus solves the *CA-CF problem* and exploits the transmission opportunities at the transmitter side. I also design a new NAV update scheme in the MAC layer to differentiate the interference ranges of different transmission links, and designs a new channel access scheme for nodes to solve the *varied-IR problem* and exploits the transmission opportunities at the receiver side. Experimental results based on USRP2 demonstrate the feasibility of the signature detection method, and simulations based on ns-2 show that IRMA outperforms the 802.11 standard and other protocols significantly.

I then proposes Interference Cancellation Multiple Reception (ICMR) to further exploit reception opportunities also from solving both the problems, through discernible interference cancellation, a physical layer mechanism that can successfully detect data frames when collided by control frames. I analyze the concurrent transmission opportunities of one link from the transmitter's transmission opportunities and the receiver's reception opportunities, then formulate the opportunities, and give theoretical analysis to indicate that ICMR will have a higher opportunity gain over other protocols. Hardware experiments based on USRP2 demonstrate the feasibility of the discernible interference cancellation mechanism, and simulations based on ns-2 confirm that ICMR outperforms the 802.11 standard and other protocols under different network scenarios.

I finally propose concurrency-based coordination mechanism (CCM) that can coordinate among nodes effectively in a centralized way to maximize concurrency and avoid data packet interference in WLANs. I propose an interference-resistant mechanism in the physical layer to make both the control message and data packets be detected correctly when they are transmitted simultaneously. I also propose the OpenCCM design which is based on the concept of SDN for WLAN management, to schedule the transmissions in both the uplink and downlink directions in a centralized manner, so as to maximize concurrency in WLANs. Experiment results in USRP2 demonstrate the feasibility of the interference-resistant mechanism in the physical layer, and simulations based on ns-2 demonstrate the performance improvement of CCM comparing with other protocols.

6.2 Suggestions for Future Work

In this part, I will give some suggestions for future work.

6.2.1 Evaluate the Performance under Current 802.11 Standards

Currently, most wireless nodes have been deployed some new 802.11 standards, such as 802.11n and 802.11ac, which increase the physical data rate to about $600Mbps$ and $> 1Gbps$ respectively, through wider bandwidth, higher-order modulations, MIMO technology, and so on. The protocol design in this thesis can also be applied to improve the performance of current networks which deploy the new 802.11 standards.

At first, the two physical layer mechanisms in this thesis, including the signature detection method (SDM) and the discernible interference cancellation (DIC), are mod-

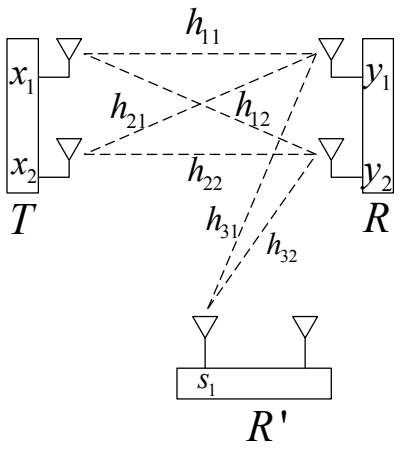


Figure 6.1: A scenario of the control message and data packets collided in MIMO communication systems.

ulation independent theoretically, as their design is in the sample level, and it has no relationship with the signal's modulation method. We have conduct experiments for SDM under different modulations and bit rates, the detection error rate is only related with the signature's sample length, but is not related with the modulation method and bit rate. For DIC, I consider it may have a higher PER (packet error rate) in the case of a higher-order modulation, as the small errors in control signal reconstruction may have more impact to the higher-order modulated signal. I leave the performance of DIC under higher-order modulation methods as one of my future work.

At second, as both 802.11n and 802.11ac are based on the MIMO technology, here I want to use a simple scenario to illustrate both SDM and DIC still work in MIMO wireless communication systems. For ease of description, we use the 2×2 MIMO system as an example. As shown in Fig. 6.1, consider a standard MIMO example that there are two packets x_1 and x_2 transmitted from T to R through the antenna array. x_1 is transmitted from T's first antenna while x_2 is from the second one. The received signal

y_1 and y_2 at the two antennas of R are illustrated as follows:

$$\begin{aligned} y_1 &= h_{11}x_1 + h_{21}x_2, \\ y_2 &= h_{12}x_1 + h_{22}x_2. \end{aligned} \tag{6.1}$$

where h_{ij} is the channel coefficient, it is a complex number and can be obtained in the training phase. R can calculate x_1 and x_2 through solving this two-dimensional linear equations.

According to the protocol design, a control message CTS or ACK from another node R' can be transmitted concurrently during this data transmission of $T \rightarrow R$. As shown in Fig. 6.1, we suppose the control message is transmitted through the first antenna and a signature s_1 is in the control message, then the received signal at R is:

$$\begin{aligned} y_1 &= h_{11}x_1 + h_{21}x_2 + h_{31}s_1, \\ y_2 &= h_{12}x_1 + h_{22}x_2 + h_{32}s_1. \end{aligned} \tag{6.2}$$

The receiver R will first conduct the DIC process on the separate signal y_1 and y_2. After detecting s_1 in the received signal through SDM, R will reconstruct the received signal $h_{31}s_1$ and $h_{32}s_2$ in y_1 and y_2 respectively, detach them to recover the original data signal as represented in Ineq. (6.1), and finally calculate x_1 and x_2 through the standard MIMO process. I consider this 2×2 MIMO example can be easily extended to a more general $m \times n$ system. However, the performance of SDM and DIC in this situation needs further study, I also leave it as my future work.

Based on the performance of SDM and DIC under both higher-order modulation methods and the MIMO technology, I will further evaluate the performance improvement of the cross layer protocols (IRMA, ICMR and CCM) in these situations.

6.2.2 Some Other Suggestions

The research that has been completed in this thesis can also be extended in some directions.

- For the fields that are filled by signatures in the control messages, I use the pseudo-noise code to accomplish the signature design, and obtain the hardware experiment results using the designed signatures, as described in Section 3.4. I consider more efficient codes may be exploited in the signature design to reduce the value of $SINR(Signature)$ that a signature can be detected correctly, and to reduce the Hamming distance of pair-wise signatures, such as the Zadoff-Chu sequence [68] and so on. This manner may reduce the length of designed signatures, and consequently improve the performance of current mechanisms further.

- Based on the simulation results in section 3.5, I get the conclusion that "the performance improvement of IRMA decreases along with the increases of the transmission rate". That is because the signature's transmission rate is fixed to be $6Mbps$ when the data transmission rate is varied from $6Mbps$ to $48Mbps$, leading to more overhead under higher data rate. When the signature transmission rate is set to be the same with the data transmission rate, the performance improvement of IRMA can still remain a high value under higher data rate. I leave it as my future work to test the performance of IRMA when signatures are transmitted under higher-order modulations.

- In the DIC design described in Section 4.3, I propose a *blind estimation algorithm* to estimate the phase offset of the control channel, so as to reconstruct the control

samples and detach them to recover the original data signal. However, this algorithm may induce some errors to the recovered control signal because of the jitter of frequency offset in the real networks, leading to a high packet error rate when the signal strength of signatures increases comparing with that of the data packets. For example, when $SINR(Signature) > 4dB$, the packet error rate is larger than 12%. Inspired by [40], we may utilize the known shaping of each symbol to improve the performance of channel estimation. In WLANs, every symbol is also over-sampled by multiple samples, and the waveform of each symbol can be known based on the modulation scheme. When receiving a collided signal containing a data packet and a control message, one node first detects the position Δ of the control message through preamble synchronization, then gets some clean data samples before Δ. Using the clean data samples and known shaping of this symbol, it can estimate the following collided data samples of this symbol, and then can subtract the estimated data samples from the collided signal to get the control samples, which can be used to refine the control channel estimation.

- As the performance of data packet detection in DIC is high when $SINR(Signature) = 0dB$ based on current design (the packet error rate is about zero in this scenario), I design a power control mechanism in CCM to make the received signal strength of signatures and data packets be comparable, so as to achieve a better performance, as described in Section 5.2.3. I consider this power control mechanism can be extended to a distributed manner to minimize the data packet detection errors in ICMR.

- In this thesis, I propose two interference resistance mechanisms in the physical layer,

including SDM that can detect control messages successfully during interferences, and DIC that can detect the data packet successfully when it is collided by the control messages. I utilize the two mechanisms to design interference management cross layer protocols in wireless networks to improve the network performance. I consider these physical layer mechanisms can be utilized in other scenarios, such as RFID, radio cognitive networks, and so on. For example, we have exploited the SDM in RFID systems to improve the performance of tag identification [92], this mechanism can be extended to improve the performance of missing tag identification.

- I also try to exploit SDM to combat the POINT (power control induced hidden terminal) problem in wireless ad hoc networks. Based on the basic power control mechanism, the POINT problem is caused by the varied interference range induced by the adjusted transmission power. I intend to design new CTS message to make it carry the information of the interference range of ongoing link. Nodes utilize SDM to detect the CTS, obtain the interference range and finally make proper decisions. Some of this work has been published in [91].

- As described in Section 5.3.5, in the link admission control of CCM MAC, I make the two transactions in the uplink and downlink directions interleaved. I consider this design still make nodes miss some concurrent transmission opportunities, as some uplinks may proceed concurrently during the downlink transmissions, and vice versa. For example, as shown in Fig. 5.6(d), during the downlink transmission of $AP_1 \rightarrow C_2$, an uplink transmission $C_5 \rightarrow AP_2$ can be permitted to proceed concurrently, as it will have no mutual interference with the transmission of $AP_1 \rightarrow C_2$.

However, permitting concurrent transmissions in the two directions will complicate the protocol design, which would be a problem to solve in the future research.

- All the protocol design is based on an assumption that all the nodes access a single channel. As the 802.11 standard recommends that nodes can access different channels in the network to avoid interference and increase concurrent transmissions, I intend to extend the protocols proposed in this thesis to multiple-channel scenarios, thus to further increase the network performance.

Bibliography

[1] A. Acharya, A. Misra, and S. Bansal. Design and analysis of a cooperative medium access scheme for wireless mesh networks. In *Proc. of ICST BROADNETS*, 2004.

[2] N. Ahmed, S. Keshav, and K. Papagiannaki. Order matters: Transmission reordering in wireless networks. In *Proc. of ACM MOBICOM*, 2009.

[3] N. Ahmed, S. Keshav, and K. Papagiannaki. OmniVoice: A mobile voice solution for small-scale enterprises. In *Proc. of ACM MOBIHOC*, 2011.

[4] T. Bansal, B. Chen, P. Sinha, and K. Srinivasan. Symphony: Cooperative packet recovery over the wired backbone in enterprise WLANs. In *Proc. of ACM MOBICOM*, 2013.

[5] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang. MACAW: A media access protocol for wireless LANs. In *Proc. of ACM SIGCOMM*, 1994.

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

[7] J. Blomer and N. Jindal. Transmission capacity of wireless ad hoc networks: Successive interference cancellation vs. joint detection. In *Proc. of IEEE ICC*, 2009.

[8] M. Z. Brodsky and R. T. Morris. In defense of wireless carrier sense. In *Proc. of ACM SIGCOMM*, 2009.

[9] M. Cesana, D. Maniezao, and M. Gerla. Interference aware (IA) MAC: An enhancement to IEEE 802.11b DCF. In *Proc. of IEEE VTC*, 2003.

[10] S. B. Eisenman and A. T. Campbell. E-CSMA: Supporting enhanced CSMA performance in experimental sensor networks using per-neighbor transmission probability thresholds. In *Proc. of IEEE INFOCOM*, 2007.

[11] Ettus Inc. Universal software radio peripheral.

[12] X. Feng, J. Zhang, Q. Zhang, and B. Li. Use your frequency wisely: explore frequency domain for channel contention and ACK. In *Proc. of IEEE INFOCOM*, 2012.

[13] C. L. Fullmer and J. J. Garcia-Luna-Aceves. FAMA-PJ: A channel access protocol for wireless LANs. In *Proc. of ACM MOBICOM*, 1995.

[14] C. L. Fullmer and J. J. Garcia-Luna-Aceves. Floor acquisition multiple access (FAMA) for packet-radio networks. In *Proc. of ACM SIGCOMM*, 1995.

[15] C. L. Fullmer and J. J. Garcia-Luna-Aceves. Solutions to hidden terminal problems in wireless networks. In *Proc. of ACM MOBICOM*, 1997.

[16] GNU Radio. GNU Radio - the open source software radio project.

[17] S. Gollakota and D. Katabi. Zigzag decoding: Combating hidden terminals in wireless networks. In *Proc. of ACM SIGCOMM*, 2008.

[18] S. Gollakota, S. Perli, and D. Katabi. Interference alignment and cancellation. In *Proc. of ACM SIGCOMM*, 2009.

[19] Z. Haas and J. Deng. Dual busy tone multiple access (DBTMA) C a multiple access control scheme for ad hoc networks communications. *IEEE Transactions on Communications*, 50(6):975–985, Jun. 2002.

[20] D. Halperin, T. Anderson, and D. Wetherall. Taking the sting out of carrier sense: Interference cancellation for wireless LANs. In *Proc. of ACM MOBICOM*, 2008.

[21] M. Heusse, F. Rousseau, R. Guillier, and A. Duda. Idle sense: An optimal access method for high throughput and fairness in rate diverse wireless lans. In *Proc. of ACM SIGCOMM*, 2005.

[22] I.-H. Ho and S. C. Liew. Impact of power control on performance of IEEE 802.11 wireless networks. *IEEE Transactions on Mobile Computing*, 6(11):1245–1258, Nov. 2006.

[23] J. Huang, G. Xing, and G. Zhou. Unleashing exposed terminals in enterprise WLANs: a rate adaptation approach. In *Proc. of IEEE INFOCOM*, 2014.

[24] IEEE Computer Society. 802.11. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. 2007.

[25] IEEE Computer Society. 802.11. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 5: Enhancements for higher throughput. 2009.

[26] M. Jain, J. I. Choi, T. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha. Practical, real-time, full duplex wireless. In *Proc. of ACM MOBICOM*, 2011.

[27] K. Jamieson. The SoftPHY abstraction: From packets to symbols in wireless network design. Ph.D thesis, MIT. 2008.

[28] K. Jamieson and H. Balakrishnan. PPR: Partial packet recovery for wireless networks. In *Proc. of ACM SIGCOMM*, 2007.

[29] X. Ji, Y. He, J. Wang, K. Wu, K. Yi, and Y. Liu. Voice over the dins: Improving wireless channel utilization with collision tolerance. In *Proc. of IEEE ICNP*, 2013.

[30] C. Jiang, Y. Shi, Y. T. Hou, W. Lou, S. Kompella, and S. F. Midkiff. Toward simple criteria to establish capacity scaling laws for wireless networks. In *Proc. of IEEE INFOCOM*, 2012.

[31] L. B. Jiang and S. C. Liew. Removing hidden node Problem in IEEE 802.11 wireless networks. In *Proc. of IEEE VTC*, 2005.

[32] L. B. Jiang and S. C. Liew. Improving throughput and fairness by reducing exposed and hidden nodes in 802.11 networks. *IEEE Transactions on Mobile Computing*, 7(1):34–49, Jan. 2008.

[33] G. Judd and P. Steenkiste. Using emulation to understand and improve wireless networks and applications. In *Proc. of ACM NSDI*, 2005.

[34] P. Karn. MACA - a new channel access method for packet radio. In *Proc. of the 9th ARRL Computer Networking*, 1990.

[35] S. Katti, S. Gollakota, and D. Katabi. Embracing wireless interference: Analog network coding. In *Proc. of ACM SIGCOMM*, 2007.

[36] S. Katti, D. Katabi, H. Balakrishnan, and M. Medard. Symbol-level network coding for wireless mesh networks. In *Proc. of ACM SIGCOMM*, 2008.

[37] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft. XORs in the air: Practical wireless network coding. In *Proc. of ACM SIGCOMM*, 2008.

[38] S. Kim, R. Fonseca, P. Dutta, A. Tavakoli, D. Culler, P. Levis, S. Shenker, and L. Stoica. Flush: A reliable bulk transport protocol for multihop wireless networks. In *Proc. of ACM SENSYS*, 2007.

[39] L. Kong and X. Liu. C-MAC: Model-driven concurrent medium access control for wireless sensor networks. In *Proc. of IEEE INFOCOM*, 2009.

[40] L. Kong and X. Liu. mZig: Enabling multi-packet reception in ZigBee. In *Proc. of ACM MOBICOM*, 2015.

[41] S. Kumar, D. Cifuentes, S. Gollakota, and D. Katabi. Bringing cross-layer MIMO to todays wireless LANs. In *Proc. of ACM SIGCOMM*, 2013.

[42] K. Leentvaar and J. Flint. The capture effect in fm receivers. *IEEE Transactions on Communications*, 24(5):531–539, May. 1976.

[43] L. Li, K. Tan, H. Viswanathan, Y. Xu, and Y. Yang. Retransmission $\neq$ Repeat: Simple retransmission permutation can resolve overlapping channel collisions. In *Proc. of ACM MOBICOM*, 2010.

[44] T. Li, M. K. Han, A. Bhartia, L. Qiu, and E. Rozner. CRMA: Collision-resistant multiple access. In *Proc. of ACM MOBICOM*, 2011.

[45] K. Lin, S. Gollakota, and D. Katabi. Random access heterogeneous mimo networks. In *Proc. of ACM SIGCOMM*, 2011.

[46] T. Lin and J. C. Hou. Interplay of spatial reuse and SINR-determined data rates in CSMA/CA-based, multi-hop, multi-rate wireless networks. In *Proc. of IEEE INFOCOM*, 2007.

[47] P. Liu, C. Nie, E. Erkip, and S. Panwar. Robust cooperative relaying in a wireless LAN: Cross-layer design and performance analysis. In *Proc. of IEEE GLOBECOM*, 2009.

[48] J. Lu and K. Whitehouse. Flash flooding: Exploiting the capture effect for rapid flooding in wireless sensor networks. In *Proc. of IEEE INFOCOM*, 2009.

[49] E. Magistretti, O. Gurewitz, and E. W. Knightly. 802.11ec: Collision avoidance without control messages. In *Proc. of ACM MOBICOM*, 2012.

[50] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. OpenFlow: Enabling Innovation in Campus Networks. *ACM SIGCOMM Computer Communication Review*, 38(2):69–74, 2008.

[51] K. Mittal and E. Belding. RTSS/CTSS: Mitigation of exposed terminals in static 802.11-based mesh networks. In *Proc. of IEEE WIMESH*, 2006.

[52] M. Mollanoori and M. Ghaderi. On the performance of successive interference cancellation in random access networks. In *Proc. of IEEE SECON*, 2012.

[53] A. Muqattash and M. Krunz. Power controlled dual channel (PCDC) medium access protocol for wireless ad hoc networks. In *Proc. of IEEE INFOCOM*, 2003.

[54] P. Ng, S. C. Liew, K. Sha, and W. To. Experimental study of hidden node problem in IEEE 802.11 wireless networks. In *Proc. of ACM SIGCOMM Poster*, 2005.

[55] ns-2. The Network Simulator - Version 2.

[56] J. Ou, Y. Zheng, and M. Li. MISC: merging incorrect symbols using constellation diversity for 802.11 retransmissions. In *Proc. of IEEE INFOCOM*, 2014.

[57] A. Patro and S. Banerjee. Outsourcing coordination and management of home wireless access points through an open API. In *Proc. of IEEE INFOCOM*, 2015.

[58] D. Qiao, S. Choi, A. Jain, and K. Shin. Miser: An optimal low-energy transmission strategy for IEEE 802.11a/h. In *Proc. of ACM MOBICOM*, 2003.

[59] C. Qin, N. Santhapuri, S. Sen, and S. Nelakuditi. Known interference cancellation: Resolving collisions due to repeated transmissions. In *Proc. of IEEE WiMesh*, 2010.

[60] H. Rahul, S. S. Kumar, and D. Katabi. Megamimo: Scaling wireless capacity with user demand. In *Proc. of ACM SIGCOMM*, 2012.

[61] T. Rappaport. *Wireless communications: Principles and practice*. Prentice Hall, 2002.

[62] A. Sankararaman and F. Baccelli. CSMA k-sic - A class of distributed mac protocols and their performance evaluation. In *Proc. of IEEE INFOCOM*, 2015.

[63] S. Sen, R. R. Choudhury, and S. Nelakuditi. CSMA/CN: Carrier sense multiple access with collision notification. In *Proc. of ACM MOBICOM*, 2010.

[64] S. Sen, R. R. Choudhury, and S. Nelakuditi. Listen (on the frequency domain) before you talk. In *Proc. of ACM HotNets*, 2010.

[65] S. Sen, R. R. Choudhury, and S. Nelakuditi. No time to countdown: migration backoff to frequency domain. In *Proc. of ACM MOBICOM*, 2011.

[66] S. Sen and N.Santhapuri. Moving away from collision avoidance: towards collision detection in wireless networks. In *Proc. of ACM HotNets*, 2009.

[67] S. Sen, N. Santhapuri, R. Choudhury, and S. Nelakuditi. Successive interference cancellation: A back-of-the-envelope perspective. In *Proc. of HotNets*, 2010.

[68] S. Sesia, L. Toufik, and M. Baker. *LTE - The UMTS long term evolution: from theory to practive*. Wiley, 2009.

[69] K. Shih, Y. Chen, and C. Chang. A physical/virtual carrier-sense-based power control MAC protocol for collision avoidance in wireless ad hoc networks. *IEEE Transactions on Parallel and Distributed Systems*, 22(2):193 – 207, Feb. 2011.

[70] V. Shrivastava, N. Ahmed, S. Rayanchu, S. Banerjee, S. Keshav, K. Papagiannaki, and A. Mishra. CENTAUR: Realizing the full potential of centralized wlans through a hybrid data path. In *Proc. of ACM MOBICOM*, 2009.

[71] N. Singh, D. Gunawardena, A. Proutiere, B. Radunovie, H. V. Balan, and P. Key. Efficient and fair MAC for wireless networks with self-interference cancellation. In *Proc. of IEEE WiOpt*, 2011.

[72] A. P. Subramanian and S. R. Das. Addressing deafness and hidden terminal problem in directional antenna based wireless multi-hop networks. *ACM/Kluwer Wireless Networks Journal*, 16(6):1557–1567, Aug. 2010.

[73] A. P. Subramanian and S. R. Das. Semi-distributed backoff: Collision-aware migration from random to deterministic backoff. *IEEE Transactions on Mobile Computing*, 14(5):1071–1084, May. 2014.

[74] L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, and T. Vazao. Towards programmable enterprise WLANs with Odin. In *Proc. of ACM HotSDN*, 2012.

[75] K. Tan, J. Fang, Y. Zhang, S. Chen, L. Shi, J. Zhang, and Y. Zhang. Fine grained channel access in wireless LAN. In *Proc. of ACM SIGCOMM*, 2010.

[76] A. S. Tehrani, A. G. Dimakis, and M. J. Neely. SigSag: iterative detection through soft message-passing. In *Proc. of IEEE INFOCOM*, 2011.

[77] D. Tse and P. Viswanath. *Fundamentals of wireless communication*. Cambridge University Press, 2005.

[78] M. Vutukuru, K. Jamieson, and H. Balakrishnan. Harnessing exposed terminals in wireless networks. In *Proc. of ACM NSDI*, 2008.

[79] L. Wang and K. Wu. Attached-RTS: Eliminating exposed terminal problem in wireless networks. *IEEE Transactions on Parallel and Distribution Systems*, 24(7):1289–1299, Jul. 2012.

[80] L. Wang, K. Wu, and M. Hamdi. Combating hidden and exposed terminal problems in wireless networks. *IEEE Transactions on Wireless communications*, 11(11):4204–4213, Nov. 2012.

[81] C. Ware, J. Judge, J. Chicharo, and E. Dutkiewicz. Unfairness and capture behavior in 802.11 ad hoc networks. In *Proc. of IEEE ICC*, 2000.

[82] S. P. Weber, J. Andrews, X. Yang, and G. de Veciana. Transmission capacity of wireless ad hoc networks with successive interference cancellation. *IEEE Transactions on Information Theory*, 53(8):2799C2814, Aug. 2007.

[83] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler. Exploiting the capture effect for collision detection and recovery. In *Proc. of IEEE workshop on Embedded Networked Sensors*, 2005.

[84] K. Wu, H. Li, L. Wang, Y. Yi, Y. Liu, D. Chen, X. Luo, Q. Zhang, and L. M. Ni. hJam: Attachment transmission in WLANs. In *Proc. of IEEE INFOCOM*, 2012.

[85] K. Wu, H. Tan, Y. Liu, J. Zhang, Q. Zhang, and L. M. Ni. Side channel: Bits over interference. In *Proc. of ACM MOBICOM*, 2010.

[86] K. Wu, H. Tan, H.-L. Ngan, Y. Liu, and L. M. Ni. Chip error pattern analysis in IEEE 802.15.4. *IEEE Transactions on Mobile Computing*, 11(4):543 – 552, Apr. 2012.

[87] K. Wu, H. Tan, H.-L. Ngan, Y. Liu, and L. M. Ni. Side channel: Bits over interference. *IEEE Transactions on Mobile Computing*, 11(8):1317–1330, Aug. 2012.

[88] T. Xiong, J. Zhang, J. Yao, and W. Lou. Symbol-level detection: A new approach to silencing hidden terminals. In *Proc. of IEEE ICNP*, 2012.

[89] K. Xu, M. Gerla, and S. Bae. Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks. *ELSEVIER on Ad Hoc Networks*, 1(1):107–123, Jul. 2003.

[90] Z. Yang, J. Zhang, K. Tan, Q. Zhang, and Y. Zhang. Enabling TDMA for Today's Wireless LANs. In *Proc. of IEEE INFOCOM*, 2015.

[91] J. Yao, W. Lou, and C. Yang. Efficient Power Control Based on Interference Range in Wireless Ad Hoc Networks. In *Proc. of IEEE EWSN*, 2016.

[92] J. Yao, T. Xiong, and W. Lou. Beyond the limit: A fast tag identification protocol for RFID systems. *ELSEVIER on Pervasive and Mobile Computing*, 21:1–18, Aug. 2015.

[93] H. Zhai and Y. Wang. Physical carrier sensing and spatial reuse in multirate and multihop wireless ad hoc networks. In *Proc. of IEEE INFOCOM*, 2006.

[94] J. Zhang and B. Bensaou. Core-PC: A class of correlative power control algorithms for single channel mobile ad hoc networks. *IEEE Transactions on Wireless Communications*, 6(9):3410–3417, Sep. 2007.

[95] J. Zhang, Z. Fang, and B. Brahim. Adaptive power control for single channel ad hoc networks. In *Proc. of IEEE ICC*, 2005.

[96] S. Zhang, S. Liew, and P. Lam. Physical-layer network coding. In *Proc. of ACM MOBICOM*, 2006.

[97] X. Zhang, H. Gong, M. Liu, S. Lu, and J. Wu. Quantitative analysis of the effect of transmitting power on the capacity of wireless ad hoc networks. In *Proc. of ACM MOBIHOC*, 2010.

[98] X. Zhang and K. G. Shin. Chorus: Collision resolution for efficient wireless broadcast. In *Proc. of IEEE INFOCOM*, 2010.

[99] X. Zhang and K. G. Shin. DAC: distributed asynchronous cooperation for wireless relay networks. In *Proc. of IEEE INFOCOM*, 2010.

[100] X. Zhang and K. G. Shin. E-MiLi: Energy-minimizing idle listening in wireless networks. In *Proc. of ACM MOBICOM*, 2011.

[101] X. Zhang and K. G. Shin. Efficient network flooding and time synchronization with glossy. In *Proc. of ACM/IEEE IPSN*, 2011.

[102] J. Zhao, S. Fan, D. Li, and B. Zhao. Collision tolerance: Improving channel utilization with correlatable symbol sequences in wireless networks. *International Journal of Distributed Sensor Networks*, 2015, http://dx.doi.org/10.1155/2015/678735.

[103] Y. Zhou and S. M. Nettles. Balancing the hidden and exposed node problems with power control in CSMA/CA-based wireless networks. In *Proc. of IEEE WCNC*, 2005.