

# COOPERATIVE COMMUNICATION IN WIRELESS NETWORKS: ALGORITHMS, PROTOCOLS AND SYSTEMS

A Thesis  
Presented to  
The Academic Faculty

by

Sriram Lakshmanan

In Partial Fulfillment  
of the Requirements for the Degree  
Doctor of Philosophy in the  
Electrical and Computer Engineering

Georgia Institute of Technology  
August 2011

# COOPERATIVE COMMUNICATION IN WIRELESS NETWORKS: ALGORITHMS, PROTOCOLS AND SYSTEMS

Approved by:

Professor Raghupathy Sivakumar,  
Committee Chair  
Electrical and Computer Engineering  
*Georgia Institute of Technology*

Professor Mary Ann Ingram  
Electrical and Computer Engineering  
*Georgia Institute of Technology*

Professor Nikil Jayant  
Electrical and Computer Engineering  
*Georgia Institute of Technology*

Professor George Riley  
Electrical and Computer Engineering  
*Georgia Institute of Technology*

Professor Mostafa Ammar  
College of Computing  
*Georgia Institute of Technology*

Date Approved: July 19, 2011

*To*  
*my parents Uma Lakshmanan and Lakshmanan Seetharaman*  
*and*  
*my grandfather (late) Pinnangudi S. Narayana Iyer.*

## ACKNOWLEDGEMENTS

Numerous individuals have directly or indirectly contributed to making this dissertation possible and I am very grateful to all of them.

To begin with, I would like to thank my parents, who in the first place encouraged me to embark on a Ph.D. I thank them for instilling in me a clear perspective about the importance of education and a global experience. More importantly, they have given me complete freedom at every stage of my life and have not placed any constraints on me either financially or otherwise. They have remained patient throughout the time it took to complete my Ph.D. (a not-so-short duration of six years!). Their sacrifices and support are the foundation of this dissertation.

I cannot express enough my thanks to my advisor, Prof. Raghupathy Sivakumar. He has been phenomenal from multiple standpoints. I thank him first for identifying my potential for research and recruiting me to the GNAN research group. He has been very patient with me. I remember vividly an incident from one of my first few meetings. Given my physical layer background, I told him that I might quit from GNAN if I did not like working on higher layer networking! He was very understanding and said he was fine as long as I invested the sincere effort and time on higher layer networking to see if it was interesting. Indeed his words were prophetic and I began to like networking very much. He has been ideal in terms of the freedom. In the early years he took a more pro-active approach which gradually gave way to more freedom in the later years. I have also learnt a good deal about breaking up complex problems into manageable ones by decoupling dependencies and managing multiple projects at a time. His emphasis on telling a story in every paper or presentation are an important reason why I was able to communicate ideas effectively in several

papers. His high standards for research and looking out for the most important and impactful problems will continue to guide me in my future endeavors. What surprises me most is his intense enthusiasm and drive. These qualities definitely enhanced my interest and accelerated research progress. My sincere thanks to him for the above and for other reasons that are too numerous to mention here.

I thank Prof. Ingram for all her help in collaborative research, writing joint proposals, clarifying several aspects of the wireless physical layer and her support for many of my works. Indeed, we had two successful NSF proposals related to my research and I am grateful that this collaboration has supported my research significantly. Several projects from her group have also helped validate assumptions about the physical layer that I have used for higher layer research. My sincere thanks to the other members of my dissertation committee as well. Prof. Jayant has always been a pleasure to work with. His feedback on both my proposal and dissertation have been very helpful. Prof. Riley's comments in my proposal have also helped significantly in shaping several parts of my dissertation. I thank Prof. Ammar for his comments and questions that have enabled a look at my research from a different perspective.

I thank my external collaborators: Allen from Ruckus Wireless was important in getting me started with real 802.11 beamforming systems. Sampath and Karthik from NEC laboratories, have played very important roles in enabling me to obtain a strong grasp of practical beamforming systems. I am grateful for the opportunity to work two summers and to publish several papers with them. Similarly, S. J. Lee, J. K. Lee, Raul and Sujata from HP laboratories have enabled me to work on really high performance wireless networks, an experience that I cherish.

I am also grateful to present and past members of the GNAN research group. One significant aspect of research at GNAN is the power of the group and the degree of collaboration. The discussions during the weekly meetings, presentations, ideas and

paper reviews have provided multiple independent perspectives on every problem. In this regard, past members such as Karthik, Ram, Tae-young, Yujie and Zhenyun have been very helpful. Cheng-Lin has helped significantly in different research projects and I am very thankful and glad about working with him. Sandeep has provided me guidance on many technical and non-technical aspects. His criticism of my research has always impelled me to investigate deeper and strengthened my research works. Shruti and Chao-Fang have also helped by providing feedback for my papers and presentations.

I would like to thank my friends both at Georgia Tech. and outside who have kept me good company and encouraged me particularly when research progress was slow. An additional word of thanks to all my relatives who have been very encouraging throughout the course of my Ph.D.

Finally, I thank my grandfather (late) Sri. P. S. Narayana Iyer. Before I left for the U.S. to pursue my Ph.D., he exclaimed that his wish was that I should successfully complete my Ph.D. Whenever I was dejected by rejection decisions at different conferences or contemplating whether a Ph.D. was indeed right for me, his words served to constantly motivate me. When he passed away a couple of years back, I really regret not being able to be by his side during his last moments. Till this date, I consider this as the most unbearable event during my Ph.D. I dedicate my dissertation to him and pray that he rests in peace and bliss.

# TABLE OF CONTENTS

DEDICATION . . . . .	ii
ACKNOWLEDGEMENTS . . . . .	iii
LIST OF TABLES . . . . .	x
LIST OF FIGURES . . . . .	xi
SUMMARY . . . . .	xiv
I INTRODUCTION . . . . .	1
II ORIGIN AND HISTORY OF THE PROBLEM . . . . .	6
2.1 Smart antennas in wireless networks . . . . .	6
2.2 Wireless network security . . . . .	7
2.3 Handling interference in wireless networks . . . . .	7
2.4 Cooperative communication in wireless networks . . . . .	9
III SECURING WIRELESS DATA NETWORKS AGAINST EAVESDROPPING USING SMART ANTENNAS . . . . .	11
3.1 Overview . . . . .	11
3.2 Scope and Background . . . . .	11
3.2.1 Scope . . . . .	11
3.2.2 Background . . . . .	13
3.3 Motivation . . . . .	14
3.3.1 A simple approach to enhancing security using smart antennas . . . . .	15
3.4 Aegis: Security using Virtual Arrays of Physical Arrays . . . . .	17
3.4.1 Information deprivation . . . . .	17
3.4.2 Information overloading . . . . .	20
3.4.3 Scalability of individual strategies . . . . .	25
3.5 Architecture and Algorithms . . . . .	26
3.5.1 Architectural model . . . . .	26
3.5.2 Integrated operations . . . . .	27

3.5.3	Problem formulation . . . . .	29
3.5.4	Idealized model and algorithms . . . . .	30
3.6	Practical Realization . . . . .	35
3.7	Performance Evaluation . . . . .	37
3.7.1	Simulation model . . . . .	37
3.7.2	Simulation results . . . . .	38
3.7.3	Proof of concept field trials . . . . .	43
3.8	Practical Beamforming . . . . .	45
3.8.1	Overview . . . . .	45
3.8.2	Power based beamforming solution . . . . .	45
3.8.3	Prototype setup . . . . .	49
3.8.4	Experimental results . . . . .	50
IV	SYMBIOTIC CODING FOR HIGH DENSITY WIRELESS LANS . . . . .	53
4.1	Overview . . . . .	53
4.2	Background . . . . .	53
4.3	Motivation . . . . .	55
4.4	Symbiotic Coding . . . . .	58
4.4.1	Concept and illustration . . . . .	58
4.4.2	Definition . . . . .	60
4.4.3	Proof of concept . . . . .	61
4.5	Design Considerations . . . . .	62
4.5.1	Channel impairments . . . . .	62
4.5.2	Modulations other than ASK . . . . .	65
4.5.3	Heterogeneous links . . . . .	68
4.5.4	Synchronizing transmissions . . . . .	70
4.5.5	Uplink communication . . . . .	72
4.6	Symbiotic Coded WLAN . . . . .	74
4.6.1	Code generation for templates . . . . .	76



4.6.2	Scheduling . . . . .	77
4.7	Performance Evaluation . . . . .	80
4.7.1	Testbed description . . . . .	80
4.7.2	How well does Symbiotic Coding work? . . . . .	82
4.7.3	The impact of varying SINR . . . . .	82
4.7.4	Many concurrent senders . . . . .	84
4.7.5	Synchronization . . . . .	85
4.7.6	Practical enterprise network benefits . . . . .	85
V	DIVERSITY ROUTING FOR WIRELESS NETWORKS WITH COOP- ERATIVE TRANSMISSIONS . . . . .	87
5.1	Overview . . . . .	87
5.2	VMISO Background . . . . .	87
5.3	Motivation . . . . .	90
5.3.1	Limitations of current routing . . . . .	90
5.3.2	Expected benefits of VMISO routing . . . . .	90
5.4	Theoretical Analysis . . . . .	95
5.4.1	Relation between interference and communication range with VMISO . . . . .	95
5.4.2	Capacity scaling with VMISO strategies . . . . .	98
5.4.3	Summary . . . . .	106
5.5	Algorithm Design . . . . .	106
5.5.1	Many or Few - Number of cooperating transmitters . . . . .	106
5.5.2	Farther or Faster - Strategy for cooperation . . . . .	107
5.5.3	Joint or Sequential - Ordering of decisions . . . . .	108
5.6	Solution Description . . . . .	109
5.6.1	Problem formulation . . . . .	109
5.6.2	Algorithm . . . . .	110
5.7	Distributed Realization . . . . .	114
5.7.1	Diversity routing protocol . . . . .	114

5.7.2	MAC layer support . . . . .	116
5.8	Performance Evaluation . . . . .	117
5.8.1	Evaluation platform . . . . .	117
5.8.2	Results . . . . .	118
VI	CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS . . . . .	123
VII	PUBLICATIONS . . . . .	127
	REFERENCES . . . . .	130
	VITA . . . . .	139

## LIST OF TABLES

1	Taxonomy of related work on concurrent transmissions . . . . .	8
2	Ordering of strategies . . . . .	25
3	Benefits over beamforming . . . . .	25
4	Field trials . . . . .	44
5	Success of transmissions . . . . .	59
6	Coding table at AP1 . . . . .	59
7	Coding table at AP2 . . . . .	60
8	Gains for different modulations . . . . .	69
9	Uplink coding table . . . . .	73
10	Decoding table at AP2 using C1 and C2 . . . . .	73
11	Average throughput across modulations . . . . .	81
12	Symbiotic Coding yields significant benefits in large networks . . . . .	85

## LIST OF FIGURES

1	Exposure region of beamforming with $k$ antenna elements shows sub-linear gains with increasing $k$ . . . . .	16
2	Illustration of secret sharing . . . . .	20
3	Illustration of controlled jamming . . . . .	22
4	Illustration of stream overwhelming . . . . .	24
5	Network model showing a high density of APs and a controller in an enterprise . . . . .	27
6	Definition of variables . . . . .	30
7	Throughput scheduler . . . . .	31
8	Security Scheduler . . . . .	32
9	Impact of $k$ . . . . .	39
10	Impact of $p$ . . . . .	39
11	Impact of rate parameter $S$ . . . . .	39
12	Throughput variation with $k$ . . . . .	41
13	Throughput variation with $p$ . . . . .	41
14	Eavesdropper collusion: Average case . . . . .	41
15	Eavesdropper collusion: Worst case . . . . .	42
16	Eavesdropper mobility . . . . .	42
17	Eavesdropper antenna capability . . . . .	42
18	Radiation pattern . . . . .	45
19	Channel estimation and beamforming. . . . .	46
20	Experimental testbed: The numbers indicate client locations. . . . .	49
21	RSSI gain . . . . .	50
22	Throughput gain . . . . .	51
23	CRC errors . . . . .	51
24	Channel gain magnitude . . . . .	51
25	Channel gain phase . . . . .	52

26	Operating regions of two contending links . . . . .	56
27	Measured scenarios in enterprise WLAN: Symmetric contention with high power separation: 190, asymmetric contention scenarios: 239 . .	57
28	Illustrative example . . . . .	58
29	The channel phase differences can be estimated accurately and retained for use over several minutes . . . . .	64
30	Same modulation at AP1 and AP2 . . . . .	65
31	Symbiotic Coding equal modulations: 4-QAM illustration and simulation	66
32	Different modulations at AP1 and AP2 . . . . .	69
33	Network model showing a high density of APs and a controller in an enterprise . . . . .	74
34	Example of input topology . . . . .	75
35	Pre-computed templates for three APs . . . . .	76
36	Flow chart of code scheduling algorithm . . . . .	78
37	Instances in Figure 34 . . . . .	78
38	Topology with 3 APs and 3 clients . . . . .	79
39	BER improvement: Symbiotic Coding outperforms time division scheduling. . . . .	81
40	SNR and SIR: Symbiotic Coding converts interfering transmission from AP2 to beneficial transmission . . . . .	81
41	Scalability and loss performance . . . . .	84
42	Rate and range improvements of a VMISO transmission . . . . .	88
43	VMISO benefits in arbitrary and random topologies . . . . .	92
44	Illustration for impact of cluster size . . . . .	94
45	Two phase VMISO communication . . . . .	98
46	Rate-Range trade-off for VMISO . . . . .	105
47	Illustration for sub-optimality of simple rate adaptation with range .	108
48	Algorithm for joint Routing, Cluster size and Strategy assignment . .	111
49	Throughput vs. Number of flows . . . . .	119
50	Throughput vs. Cluster size . . . . .	119

51	Throughput with grid size . . . . .	120
52	Throughput with hops and mobility . . . . .	120

## SUMMARY

Current wireless network solutions are based on a link abstraction where a single co-channel transmitter transmits in any time duration. This model severely limits the performance that can be obtained from the network. Being inherently an extension of a wired network model, this model is also incapable of handling the unique challenges that arise in a wireless medium. The prevailing theme of this research is to explore wireless link abstractions that incorporate the broadcast and space-time varying nature of the wireless channel. Recently, a new paradigm for wireless networks which uses the idea of ‘cooperative transmissions’ (CT) has garnered significant attention. Unlike current approaches where a single transmitter transmits at a time in any channel, with CT, multiple transmitters transmit concurrently after appropriately encoding their transmissions. While the physical layer mechanisms for CT have been well studied, the higher layer applicability of CT has been relatively unexplored. In this work, we show that when wireless links use CT, several network performance metrics such as aggregate throughput, security and spatial reuse can be improved significantly compared to the current state of the art. In this context, our first contribution is *Aegis*, a framework for securing wireless networks against eavesdropping which uses CT with intelligent scheduling and coding in Wireless Local Area networks. The second contribution is *Symbiotic Coding*, an approach to encode information such that successful reception is possible even upon collisions. The third contribution is *Proteus*, a routing protocol that improves aggregate throughput in multi-hop networks by leveraging CT to adapt the rate and range of links in a flow. Finally, we also explore the practical aspects of realizing CT using real systems.

# CHAPTER I

## INTRODUCTION

Wireless networks have proliferated considerably over the last few decades driven mainly by the advent of sophisticated consumer devices such as smartphones and tablets. Such rapid adoption of wireless technology is primarily due to its unique advantages of tetherless connectivity and mobility, which results from using air as the medium of transmission. In contrast to wired networks, which use a guided medium such as a fiber optic cable or wire, using air as the communication medium allows a communication device to access the medium irrespective of its location in the network and proximity to ports on walls. Despite this fundamental difference, current wireless networks are based on the point-to-point link abstraction, which is borrowed from wired networks. While such a link abstraction allows an easy extension of solutions developed for wired networks to wireless networks, it significantly limits the performance that can be obtained from a wireless network and is consequently a sub-optimal abstraction. As an illustration, it is well known that the IEEE 802.11 protocol, which separates the links in time, suffers from poor scalability. Given the increasing density of wireless devices, this is a serious problem.

The wireless medium has three fundamental characteristics that impact the problems and solutions in the context of networking: (1) signal radiation over a range of locations - while guided media allow signal reception only at specific locations (along the waveguide), in a wireless medium a signal is radiated across multiple dimensions in space. Thus, successful signal reception is possible at multiple locations in the network. This phenomenon leads to signal exposure in unintended locations, which affects the security performance and also causes unnecessary interference to other



wireless links in the vicinity; (2) interference among nearby co-channel users - when multiple wireless links operate in the same vicinity using a single channel (frequency), they cause interference to each other. This phenomenon affects several metrics such as throughput, loss rate, multi-hop routing performance. (3) space and time varying channel quality - the quality of the channel varies significantly depending on the spatial location and the time of the communication due to the multipath scattering effect of electromagnetic waves in a wireless medium. This variation in channel quality has a direct impact on higher layer metrics such as throughput and loss rate. Current networking solutions have attempted to tackle a subset of these problems using simple link abstractions and have consequently provided limited performance benefits.

In this work, we identify and explore a new link abstraction for wireless links, that leverages the wireless channel better. Conventionally, a link abstraction in a network containing  $M$  transmitters and  $N$  receivers is represented as  $MN$  point-to-point links. This model is quite representative of wired links where transmissions are guided and neither interfere nor have spatially varying link quality. However, in a wireless network, multiple spatially separated transmitters interfere and have varying channel characteristics to the receivers. Thus a set of wireless nodes is effectively one composite link that contains  $M$  transmitters and  $N$  receivers where any subset of the transmitters can communicate simultaneously with a subset of the receivers. This abstraction is motivated by a recent development in the physical layer, namely, cooperative communication. In contrast to traditional communication where a node with a single antenna transmits or receives information at a given time, cooperative communication involves multiple nodes actively transmitting or receiving different version of the same information at any given time. In this work, we consider a subclass of cooperative communication called cooperative transmission (CT) where the cooperation is among the transmitters. CT is a physical layer innovation in which multiple co-channel wireless transmitters transmit coded signals simultaneously. (We

use CT to refer to cooperative communication in its most generic form. This includes (i) physical arrays where multiple antenna elements on a single node transmit in a cooperative manner and (ii) virtual arrays where distinct nodes transmit in a cooperative manner.) Interestingly, CT has a significant potential for solving key wireless challenges because it can provide increased signal-to-noise-ratio (SNR) at the receiver, leading to higher reception range, higher throughput and increased spatial reuse.

This dissertation research falls into the broad category of works that utilize CT with certain key differences. Almost all existing work on CT has been at the physical layer of the protocol stack and has focused only on enabling concurrent transmissions, assuming highly idealized network conditions. As a consequence of the lack of higher layer research, there are several important questions left unanswered, such as: “what link layer abstractions are to be used for higher layer protocol development?”; “what kind and magnitude of benefits can be obtained using CT?”; “how can multi-flow routing be performed in a network with a CT capable physical layer?”, “how can CT be realized in a large network setting?”. The focus of this dissertation is to explore how fundamental challenges in wireless networking can be solved using algorithms at the higher layers of the protocol stack. The approach taken is to consider popular network performance metrics that are impacted by these challenges and develop algorithmic solutions to optimize these metrics using appropriate tools such as theory or simulation. An important consideration in the solution development is that each of the solutions be practically realizable. Hence, experiments with real-life systems are performed whenever appropriate, to highlight the practical feasibility of the proposed solutions.

In the rest of this thesis, we consider three popular networking problems that arise from the fundamental wireless characteristics identified previously, i.e, signal radiation to illegal eavesdroppers, signal interference to other clients in a single-hop and in a multi-hop network. We describe how higher-layer algorithms which leverage

CT can be used to significantly improve performance compared to state-of-the-art approaches in the above scenarios.

- First, we consider the problem of eavesdropping in wireless LANs. Since wireless transmissions are broadcast in nature, eavesdropping can be performed in a passive manner, unnoticed. Given the increasing use of WLANs to access sensitive information, we propose a new paradigm for securing wireless communication at a spatial level called “Physical-Space Security”. Using this paradigm, we propose a framework that uses an array of access points to increase the security performance in WLANs. We refer to this framework as “Aegis.” We identify the basic mechanisms developed from two primitives, namely, “information deprivation” and “information overloading.” With appropriate scheduling we show how the overall region of the network that is exposed to eavesdropping is reduced.
- Next, we present an approach called “Symbiotic Coding” that codes packets across transmitters such that information is successfully transferred despite collisions. We present the architecture and algorithms in the context of high density wireless LANs and address several challenges including coding algorithms, synchronization, channel impairments and uplink scenarios.
- Finally we present a diversity routing protocol that utilizes concurrent space-time coded transmissions to significantly improve the routing performance in a multi-hop network. We refer to this protocol as “Proteus”. While current routing protocols use point-to-point links to form paths, Proteus uses the “cooperative link abstraction” to alleviate the multi-hop burden. Further, Proteus works with multiple flows unlike current state-of-the-art cooperative routing solutions.

We evaluate the above solutions using a combination of analysis, simulation and real-world experiments.

## CHAPTER II

### ORIGIN AND HISTORY OF THE PROBLEM

#### *2.1 Smart antennas in wireless networks*

Smart antennas have been used popularly in wireless networks to combat multi-path fading using the diversity provided by the elements at the transmitter and/or receiver [18]. The physical layer benefits of smart antennas are well studied. However, higher-layer work has been relatively limited. The only higher layer works known currently are the design of stream controlled medium access [39] and MIMO routing [38] protocols. Considering lower layer research on smart antennas there have been both theoretical solutions [61] and practical solutions such as DIRC [63] using beamforming, SAM [54] enabling multiple access, IAC [50] using interference alignment and cancellation. These techniques require multiple antennas on the senders/receivers and provide gains only with rich scattering (full-rank) orthogonal channels across links. Physical layer cooperation (e.g., DSTBC, Cooperative MIMO [3, 55]) or multi-user detection techniques [61] require exchanging channel estimates and symbols across receivers. In a similar manner, sender diversity has been explored in [69]. The authors argue that diversity among access points can be used to improve performance of individual clients in wireless LANs. They present an architecture to synchronize transmissions across Access Points but focus only on improving single link throughput. Thus, their work motivates approaches which use synchronized transmissions across senders to improve aggregate capacity.

## *2.2 Wireless network security*

Both the security problems in WLANs [28] and higher layer solutions to specific problems [29, 30] have been well documented along with the standardization of security techniques in the form of IEEE 802.11i [31]. These solutions are purely higher-layer cryptographic mechanisms that do not specifically protect against problems unique to wireless links. Lower layer security has been considered in [32] and [33], where channel state and received signal information are used for identifying legal clients. In both the above examples, the authors do not consider smart antennas and hence the goals are different. In [34], the authors propose an authentication scheme that uses a beamforming antenna to identify and locate users. The focus of this related work is authentication and is orthogonal to the eavesdropping problem considered in this dissertation. In [35], the authors discuss spatial data striping techniques that increase the degree of security using a phased array antenna in 802.11 environments. In [36], the authors describe a theoretical communication scheme in which coding using multiple degrees of freedom is used to generate “artificial noise” which degrades only the eavesdropper’s channel quality. Neither of the above works provides a protocol or solution details. Also, while [35] does not define or evaluate metrics, [36] does not consider the eavesdropper equipped with smart antennas. Additionally, there are several information-theoretic works that identify the theoretical secrecy capacity [37], whereas the focus of the Aegis solution described in this dissertation is on practical algorithmic solutions.

## *2.3 Handling interference in wireless networks*

**Coding techniques:** Analog Network coding (ANC) [52] requires prior knowledge of one of the colliding transmissions at the receiver whereas Successive Interference cancellation (SIC) [48] requires the SNRs of the concurrent streams to be separated

**Table 1:** Taxonomy of related work on concurrent transmissions

Approach	Operation on multiple WLAN links	Does not require Tx. hardware modifications	Experimental verification	Handles Asymmetric contention	Realizable over digital symbols
LDPC based DPC [72]	X	X	X	✓	X
Turbo [70], Trellis [71] DPC	X	X	X	✓	X
Generic DPC [53, 58, 73, 74]	✓	X	X	✓	X
SIC [48], Zigzag [49]	✓	✓	✓	X	✓
ANC [52]	X	✓	✓	X	X

widely and also allow inefficient rates below the capacity of the links. Zigzag decoding [49] requires multiple retransmissions of the same colliding packets which reduces throughput. Superposition coding is used to handle SNR differences across receivers when broadcasting from a single sender [57] and does not improve capacity under interference. Finally, information theoretic approaches such as Dirty Paper Coding [53, 58] while holding promise, are infeasible in practice due to strict requirements on the radios. Although there have been several code designs proposed in related literature [72, 70, 71], the aim of these works is to consider optimal strategies for the simple one receiver scenario. None of these works consider the more general problem of coding for a wireless networks with many links. Further, these approaches assume specialized symbol transmissions from the transceiver whereas Symbiotic Coding works with existing modulation schemes and hence can be realized as a firmware/driver modification to existing designs. Additionally, these works have been evaluated using simulations for the Additive White Gaussian Noise channel(AWGN) and their performance in real, wireless scenarios has not been studied. We summarize these works along several dimensions in Table 1. A ✓ means that the work supports that point and an X means that the work does not support that point.

**Multiple Access techniques:** either *share* a wideband channel (e.g. CDMA [61]) or *avoid* collisions [51, 62] but do not improve capacity.

The Symbiotic Coding approach proposed in this dissertation differs from all these interference handling approaches. Specifically, Symbiotic Coding does not require

power separations, retransmissions or reduced rates. It also works with existing modulations, does not require sophisticated transceivers, considers multiple links and real wireless LAN conditions. More importantly, it uniquely targets asymmetric interference scenarios occurring in WLANs and provides capacity improvements that scale with the density of the network. Further, Symbiotic Coding delivers gains in real-life wireless experiments with software radios.

## ***2.4 Cooperative communication in wireless networks***

There has been significant research on cooperative communication in wireless networks. The works most relevant to the present work are [2, 4, 9, 13], which consider the use of cooperative transmit diversity for routing. In [2], the authors study the problem of choosing the modulation such that the cost of distribution to relays is much less than the benefit of cooperation in a three-node network. In [4], the authors describe a multi-layer protocol for exploiting transmit diversity in adhoc networks using Virtual Multiple Input Single Output (VMISO) routes constructed on Single Input Single Output (SISO) paths and an inter cluster medium access protocol similar to IEEE 802.11. Similarly, in [9], the authors present a forwarding protocol that uses transmit diversity to improve the reliability of acknowledgment(ACK) packets. Both these works focus on forwarding, not routing. In [13], the authors formulate the multi-source routing problem with cooperative communication and highlight the need for cooperative communication-aware routing but do not consider varying the strategy (rate,range) or its relation with cluster size. Cooperative transmit diversity has also been considered in the context of broadcasting protocols [5] and in [42] where energy efficient broadcasting is considered. However, these works do not consider the multi-flow unicast routing problem, which is important in multi-hop wireless networks. The information theory and physical layer formulations for cooperative communication



are well established, notably in [3, 40]. These works do not provide protocol or algorithmic solutions and consequently do not tackle the higher layer problems considered in this dissertation. There have been works that use cooperative communication for other networking problems such as network lifetime extension [77, 78] and energy efficiency [78, 79]. Similarly synchronization approaches have also been considered in [75]. Additionally, works on physical arrays [14, 38] have a fixed array size and different diversity gains and trade-offs than virtual arrays, whereas other forms of cooperative routing [15] do not consider the transmit diversity obtained by many concurrent transmitters.

## CHAPTER III

# SECURING WIRELESS DATA NETWORKS AGAINST EAVESDROPPING USING SMART ANTENNAS

### *3.1 Overview*

In this chapter, we focus on securing communication over wireless data networks from malicious eavesdroppers, using smart antennas. While conventional cryptography-based approaches focus on hiding the meaning of the information being communicated from the eavesdropper, we consider a complementary class of strategies that limits knowledge of the existence of the information from the eavesdropper. We profile the performance achievable using simple beamforming strategies using a newly defined metric called exposure region. We then present three strategies within the context of an approach called *Aegis*, which uses virtual arrays of physical arrays to significantly improve the exposure region performance of a wireless LAN environment. Using simulations, analysis, and field trials, we validate and evaluate the proposed strategies.

### *3.2 Scope and Background*

#### **3.2.1 Scope**

*Environment:* The wireless environment considered is that of a wireless local area network (WLAN), which consists of  $p$  wireless access points (APs), each equipped with a  $k$  element antenna array and one or more clients, each equipped with a single omni-directional antenna or an array of upto  $k$  elements. Channel parameters such as line of sight (LOS), the degree of fading, and the richness of scattering vary widely for different indoor environments. Thus, to begin, we consider a strong LOS path

between an AP and each client. Later, in Sections 3.4 and 3.7, we show how this assumption is relaxed. We assume that any frequency-selective fading is combatted by the use of schemes such as orthogonal frequency division multiplexing (OFDM) as in current WLAN devices. Further, since the mobility of indoor users is typically low, we do not consider the effect of fast-fading.

*Metric:* To quantify the security achieved against eavesdropping in a wireless network, we define a new security metric called the *the exposure region of the network*,  $ER_{Network}$ , defined as the union of the exposure regions of all the clients in the network.<sup>1</sup> The exposure region of the  $i^{th}$  client,  $ER(C_i)$ , is given by the region in which an eavesdropper can decode the information of client  $i$ .

$$ER_N = \bigcup_{i=1}^{N_c} ER(C_i) \quad (1)$$

where  $N_c$  is the total number of clients in the network.

Note that the above metric applies to both homogeneous and heterogeneous antenna capabilities (although we restrict our focus to a homogeneous network). Further, the exposure region of a client is also a function of the receiver's (or eavesdropper's) antenna gains. Thus, all references to the metric are for a fixed eavesdropper antenna capability.

*Eavesdropper:* Our eavesdropper model is captured by the following set of assumptions for the eavesdropper  $M$ : (i)  $M$  is a wireless node with  $k$  antenna elements (where  $k \leq$  the number of elements at each AP);<sup>2</sup> (ii)  $M$  has access to location information of all the clients and APs. (Such a scenario is typical in organizations and offices, where an eavesdropper could move freely within the network carrying a wireless device.); (iii)  $M$  can perform sophisticated antenna processing with its available elements; (iv) APs do not have any information about the position of  $M$  or its strategy. We initially consider the eavesdropper to operate in isolation, but later

---

<sup>1</sup>A similar but equivalent definition can be given in terms of exposure region of APs.

<sup>2</sup>Later we discuss the case when the eavesdropper has more antenna elements than the AP

consider the case of colluding eavesdroppers. We consider both *perimeter security* and *physical security* (*i.e.*, security against an eavesdropper situated just outside the physical perimeter of the network or inside the network, respectively).

### 3.2.2 Background

Adaptive array smart antennas employ an array of antenna elements coupled with both amplitude and phase weighting, thereby making it possible to tune and obtain a large set of angular and spatial patterns. Thus, with adaptive arrays, it is possible to manipulate the weights on the different elements to obtain a desired pattern. At the simplest level, the process of forming a beam or main lobe to a certain direction is called beamforming. More formally, it is the process of choosing antenna element weights such that the signal-to-noise-ratio (SNR) at the receiver is maximized. Also, when a strong LOS path is unavailable or multipath is rich, simple beam-steering is less effective and the pattern that maximizes the receiver's SNR does not necessarily have a main beam pointing toward the direction of the client [17]. This is particularly true in indoor environments and the beam has to be adapted based on the channel condition. With appropriately chosen weights, adaptive arrays can be used to maximize the signal quality at the receiver even in the presence of channel impairments. Also, depending on whether the weight adjustments are performed at the transmitter or receiver, the technique is called transmit beamforming or receive beamforming, respectively [18]. Another important feature of adaptive arrays is their *ability to place nulls in desired directions*. The number of elements on the array, typically called the degrees of freedom (DOF), bounds the number of nulls that can be placed. With a  $k$  element array, it is possible to place  $k - 1$  nulls in the pattern and use the remaining one DOF for the desired communication. The  $k - 1$  nulls can be used by a transmitter to restrict the transmitted signals from propagating along unwanted directions and

causing interference, while they can also be used by a receiver to nullify signals (interference) received in certain directions. Thus, when more than  $k$  streams are received at a receiver, the SNR of all these communication streams is degraded. Although the actual degradation will depend on the power levels, we assume that more than  $k$  received streams can cause enough interference to make the communication at the receiver unsuccessful.

Further, the best beam would need to be adapted due to the time-varying nature of the wireless channel. Since user mobility within a WLAN is typically limited we assume that the channel does not change within a packet duration. Hence the key properties of smart antennas that we leverage are as follows.

*Property 1* : A transmitter can control where it causes interference by the appropriate placement of nulls in its pattern.

*Property 2* : A receiver can null interference only from up to  $k - 1$  transmissions. Beyond that, it is unable to decode or resolve the transmissions.

*Property 3* : It is sufficient for either the interfering transmitter to suppress interference to an unintended receiver or for that receiver to suppress interference from an unintended transmitter.

*Property 4* : When more than  $k$  parallel transmissions happen within an interference range, all transmissions suffer a reduction in signal-to-interference and noise ratio (SINR) which will make the signal undecodable.

### ***3.3 Motivation***

*Wireless security:* While tapping the wired channel could require sophistication in device and physical manipulation of the medium, wiretapping can be done in a passive manner in the wireless channel. Consequently even a casual user could turn into an eavesdropper. Further, the actual security solutions are not as secure as the underlying cryptographic schemes due to practical difficulties such as improper key

management. In addition to this, the wireless medium introduces new security issues such as user fingerprinting [19] and passive security attacks [20], which are not directly addressed by cryptographic schemes. These attacks motivate another dimension of security on top of existing security techniques.

### 3.3.1 A simple approach to enhancing security using smart antennas

Smart antennas have been conventionally used for optimizing different communication parameters such as data rate, reliability, transmission power, range, etc. However, their use for security has been relatively limited. In the context of security, the direct relevance of smart antenna capabilities is their ability to beamform and achieve interference suppression to counteract jamming. Specifically, when the directions of arrival of the jammers are known, then it is possible to produce a null in the directions of the jammers. Again, the number of jammers that can be suppressed is at most  $k - 1$  for a  $k$  element array. Apart from jamming, to the best of our knowledge, smart antennas have thus far not been considered to tackle other security issues. A straightforward, simple technique to reduce the possibility of eavesdropping using smart antennas is to employ beamforming. Beamforming can be of two types, physical (based on the line-of-sight direction) or signal-space (channel matrix based). When a transmitter or receiver, or both, perform beamforming, the signal is contained in a specific region between them, depending on the beam patterns, the channel, and the eavesdropper's antenna capability. In the rest of this section, we study the benefits of such a simple strategy in terms of exposure region reduction and present approximations for the same.

*Benefits:* We now analyze how the security benefit (reduction of exposure region) of the simple beamforming mechanism compares to that of a scenario with omnidirectional antennas using simulations. The scenario we consider is that of a single AP communicating with a single client in the presence of an eavesdropper. To begin,

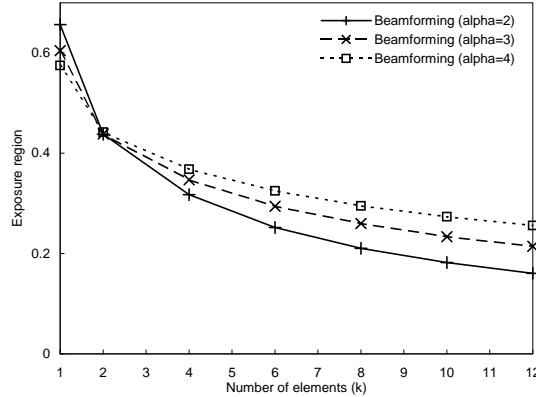
we consider that the AP has a  $k$  element array and both the client and eavesdropper have an omni-directional antenna.

Figure 1 shows the exposure region in a simulated setting with link shadow fading deviation of 3dB, four antenna elements, and a path loss exponent of 4.

The main observations are as follows: (1) The decrease rate with increasing number of elements is less than linear and we get diminishing returns for the exposure region with increasing antenna elements; (2) The path loss exponent also affects the exposure region.

Thus, the results clearly indicate the diminishing security benefits possible with simple beamforming, with an example *reduction in exposure region by a factor of half for a six-fold increase in antenna elements*.

While beamforming provides a first level security mechanism with a sub-linear  $k$  fold improvement, the key question we ask is whether *it is possible for a more intelligent scheme to achieve larger benefits*



**Figure 1:** Exposure region of beamforming with  $k$  antenna elements shows sub-linear gains with increasing  $k$ .

### ***3.4 Aegis: Security using Virtual Arrays of Physical Arrays***

In this section, we introduce two classes of strategies for improving security in wireless environments using smart antennas that rely on the use of a *virtual array of physical arrays* (VAPA). We call this approach of achieving security against eavesdropping, *Aegis*. Essentially, inspired by several recent studies about high density access point deployments [21], we exploit the availability of multiple access points (APs) in a single WLAN environment to form a virtual array. We then assume that each access point is equipped with a physical antenna array. We also assume that there are  $p$  APs, and they are connected to each other through a high-bandwidth distribution network such as Ethernet. Also, let  $c$  be the number of clients, each with 1 to  $k$  element arrays.

The strategies are based on two guiding principles to provide physical space security, namely, *prevent eavesdropper from getting access to the information signals* or *overwhelm eavesdropper with more signals than it can sustain such that the information signals cannot be decoded*. Interestingly, the techniques discussed below do apply to an environment with a *physical array of physical arrays* (a multi-radio smart antenna AP), but exploration of that dimension of the approaches is beyond the scope of this work. Also, while the techniques themselves can be applied to a virtual array of omni-directional antennas, our contention is that the efficacy of the schemes is minimal due to the lack of spatial/angular control with omni-directional antennas.

#### **3.4.1 Information deprivation**

The underlying principle of information deprivation is to ensure that the eavesdropper is rendered unable to receive information from separate transmissions occurring in the time, frequency, or spatial dimensions. Thus, the basic idea is to ensure that each piece of information is decodable only if multiple spatially separated transmissions



can be decoded successfully. We clarify the idea with an instance of this approach called “*secret sharing*”.

1) *Secret Sharing*:

(i) *Overview*: The basic idea of secret sharing is well established in the context of cryptography [22].

In a general *t-out-of-n* secret sharing scheme, a secret message  $x$  should be divided into  $n$  shares as

$x \Rightarrow (x_1, x_2, x_3 \dots x_n)$  such that the following properties are satisfied.

*Recoverability*: Given any  $t$  shares  $x$  can be recovered.

*Secrecy*: Given any  $t' < t$  shares, absolutely no information can be learned about  $x$ . More formally,  $\Pr(x \mid t' \text{ shares}) = \Pr(x)$  (ii)

*Mechanism*: The mechanism exploits the fact that when a single client is reachable from multiple access points, different shares of the message can be distributed to the clients through those access points.

An eavesdropper in any position in the vicinity of the client or access points would only be able to gain access to a fraction of the information due to the *spatially disjoint nature of the transmissions* that are possible with adaptive arrays unlike with omni

antennas. The multiple elements of the array are utilized to perform beamforming and the scheme is implemented in a time division manner. Thus, the exposure region

is the region of the network where all the shares (i.e, the packet fragments) of at least one data packet can be decoded successfully. Although several secret sharing

schemes exist, we are interested in those that do not significantly increase the traffic load on the network given the limited resources in wireless environments. In this

regard, we consider the *all or nothing encryption* (as proposed by Rivest [23],) which is a mechanism to prevent parts of a message from being recovered until the whole

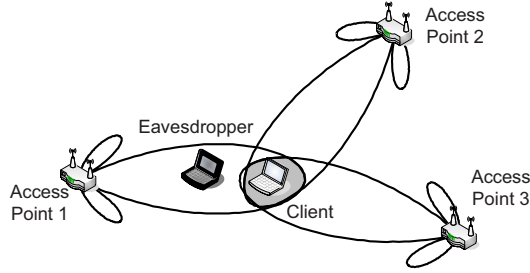
message is received in its entirety. This method involves encrypting the message with the key and the key with the message blocks, thus rendering each unusable until the

whole sequence (key and message) is correctly received.

A modified version of the above algorithm adapted for a WLAN scenario is presented here. The mechanism works as follows. Assume a secure Pseudo-Random Number Generator PRNG, which uses a key  $K$  of length  $\ell$  bits to generate a pseudo-random sequence  $\text{PRNG}(K)$ . The message that we require to be sent is a bit stream of length  $|M|$ . The message  $M$  undergoes the binary ‘XOR’ operation with the sequence generated by  $\text{PRNG}(K)$ , to create a cipher text  $C$  of length  $|C|$ , which is the same as  $|M|$ . This cipher text is now split into blocks of length  $\ell$  bits. Each of these blocks is made to undergo the ‘XOR’ operation with each other and then with the key  $K$ . The result is known as  $C_\ell$ . Now the controller divides the new packet formed by concatenating the above as  $C | C_\ell$  (where  $|$  denotes concatenation of packets) into fragments of length  $\ell$  bits. All these fragments must be received successfully at the intended client. When the receiver receives these fragments, it computes the XOR function of all the fragments to regenerate the  $\ell$ -bit encryption key. Once the key is regenerated, the receiver uses it to decrypt the fragments and aggregates them into a single packet based on the fragment numbers. The overhead of such a scheme is  $\ell$  bits (linear) for a message of length  $M$  bits and provides a strength of  $2^\ell$  (which means that the overhead increases linearly whereas the number of potential keys increases exponentially).

We illustrate the scheme. Figure 2 shows three APs, each possessing a share of the information they communicate to a client in consecutive time slots. Specifically, AP1 transmits its share to the client in slot 1, AP2 in slot 2, and AP3 in slot 3. At the end of the three slots, the client can process the fragments received to decode its packet. On the contrary, an eavesdropper who is positioned along the path between AP1 and the client would be able to obtain share 1 but not share 2. The eavesdropper cannot receive that share from AP2 being in that location.

The alternative is for the eavesdropper to move quickly and place himself in the



**Figure 2:** Illustration of secret sharing

path from AP2 to the client. In this case, the speed with which the eavesdropper must move to reposition himself in the direction of the new path within a time slot, is significantly high (close to signal propagation speeds). There are two main practical challenges with applying the proposed technique, namely, overheads and packet loss. Since each fragment has its own preamble, header, and error check bits in addition to the secret shared data, the payload size should be chosen to be large compared to the overheads. The other issue is the loss of fragments. If a fragment is lost, a conservative approach would require that all fragments be retransmitted in the next slot. While being acceptable for low loss scenarios, this would be inefficient when the losses are significant. We note that it is not necessary for all fragments of a datagram to arrive successfully at the receiver in the same slot. The transmissions of fragments of a datagram need not be synchronized. When a fragment is lost, that fragment alone can be retransmitted in the next slot by adjusting the AP's schedule. The client can then reconstruct the datagram in that slot. If the losses are very high, an additional optimization that can be employed to improve loss tolerance is to use a  $(t, n)$  scheme where  $t < n$  instead of  $t = n$ .

### 3.4.2 Information overloading

The core idea here is to overload/overwhelm the eavesdropper with multiple signals or information units so that the eavesdropper is unable to decode even a portion of the information. The main challenges here are (i) ensuring that the legitimate clients

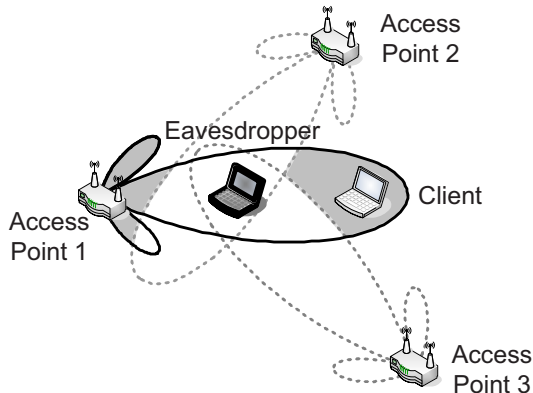
are unaffected and (ii) achieving this at a link/network level. We recall that interference suppression in an indoor setting (impaired by scattering) will now be pattern based rather than angle based, i.e., one can identify patterns that would cause power to be received or not at a nodes. This can be performed by obtaining and updating “radio frequency maps” at coarse time granularities (using schemes similar to those in [24]). When overloading of information is considered, one can use smart antenna strategies in different ways. However, there are two fundamental strategies that illustrate the range of strategies under this approach. These two flavors are called *controlled jamming* and *stream overwhelming*. For both strategies, we highlight the design principles and how the challenges can be overcome.

1) *Controlled Jamming:*

(i) *Overview:* The key concept is to generate interfering signals in a controlled manner such that those signals cause no (or negligible) interference at an intended receiver, but cause significant interference to eavesdroppers. When sufficient interference is generated the SINR at the eavesdropper is reduced significantly, thereby preventing the eavesdropper from obtaining access to the information itself. Thus, the exposure region for this technique is the region in the network where at least one data packet is received successfully (i.e., with sufficient SINR).

(ii) *Mechanism:* The scheme is illustrated in Figure 3, where a single AP attempts to convey a data packet to a client.

The other APs in the vicinity generate jamming signals with two constraints: (1) the intended receiver should suffer negligible interference, and (2) the eavesdropper (whose position is unknown) must suffer as much interference as possible. Recall that a  $k$  element array can be used to suppress interference of  $k - 1$  other nodes if it dedicates one DOF for communication. However, this technique differs from a conventional interference suppression technique in that a jamming AP does not serve



**Figure 3:** Illustration of controlled jamming

any client and therefore can use all its  $k$  DOFs for performing interference suppression and still jam several eavesdroppers. In the figure, AP1 communicates a data packet to the client. Simultaneously, AP2 and AP3 generate jamming signals by placing a null to the client. Then the maximum allowed power is used so that most of the region that is unoccupied by clients is filled with jamming signals. In this way, when multiple overlapping jamming signals are received, an eavesdropper in any of those locations would experience a poor SINR. The eavesdropper can attempt to use its  $k$  element array to suppress the interference along the directions of the jamming APs. However, if the number of APs that are in the vicinity times the number of antenna elements on them is higher than the number of antenna elements at the eavesdropper, it would still be unable to receive with a sufficient SINR. On the other hand, the client would be unaffected because the different jamming APs control their beam patterns to place a null in its direction.

The fine grained control that the  $k$  element array provides, enables successful reception at the client while jamming at the eavesdropper simultaneously. It is important to understand that, while increasing interfering transmissions in an omnidirectional communication environment leads to higher interference and less throughput, the interference suppression capability is what enables the adaptive arrays to generate jamming signals without affecting the throughput performance of existing

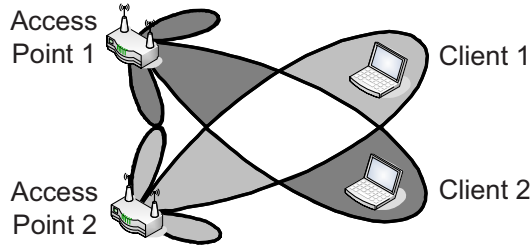
flows in the network. Further, the appropriate choice of the power to use depends on the antenna gain in the direction of a null, transmit power regulations and the currently existing flows in the vicinity. Additionally, when deploying controlled jamming, a high density of APs (as in the measurement study in [21]) is desirable, since it gives more opportunities to perform controlled jamming. However, we also note that, even in existing deployments multiple APs within carrier sense range do not transmit simultaneously. Such APs can be used for controlled jamming without incurring any throughput degradation.

2) *Stream Overwhelming:*

(i) *Overview:* This strategy exploits the fact that when a node receives more information than the resources possessed to handle it (overwhelmed node), the different information signals mutually interfere with each other resulting in insufficient SINR for each of these signals. (Here, we use the notion of a stream to indicate each independent data/information flow that a node receives.). Several valid data transmissions are coordinated such that every intended receiver has a sufficient SINR for its desired signal, whereas at other points in the network, the multiple signals interfere to prevent decodability. Thus, the exposure region for this technique is the region in the network where at least one data packet is received successfully (i.e with sufficient SINR).

(ii) *Mechanism:* Figure 4 shows an illustration of the idea, where two APs and two clients are considered. When each client chooses the nearest AP, then there is no stream overwhelming. However, as in Figure 4, if the AP client associations are performed in a suitable manner, the beams overlap, causing a larger region to be overwhelmed, thereby reducing the exposure area. We also note here that it is not necessary for the eavesdropper to be present in the overlap of transmission ranges,

rather, the eavesdropper would be left with poor SINR even if it is at a point in the overlap of interference ranges.



**Figure 4:** Illustration of stream overwhelming

Both the above techniques leverage two key principles.

*Principle 1: Transmit side interference suppression* is more beneficial for security than receive side interference suppression. Consider an AP with  $k$  elements transmitting to a client with an omni antenna. The AP can use just one DOF for suppressing interference to the client, since it is generating the interference. On the other hand, the eavesdropper, doing receive side interference suppression would need to suppress interference from the different transmitting elements of the jamming AP, since each of them would appear different to each of his elements. The central idea is that the number of DOFs needed for interference suppression depends also on the number of elements at the interferer (see for instance pages 229 and 231 of [18] for MISO interference cancellation). Hence the number of antenna elements required at the eavesdropper is proportional to  $p' * k$  where  $p'$  is the number of APs transmitting simultaneously within interference range of the eavesdropper and  $k$  is the number of elements on each AP. Thus interference from each interfering element must be managed by the eavesdropper.

*Principle 2: Beamforming with power adjustment:* While interference suppression reduces the power outside the main lobe, side-lobes may still have non-negligible gains in practice. To account for side-lobes and their gains affecting legitimate clients, the

APs employ beamforming with interference suppression in conjunction with transmit power adjustment. For instance, when side-lobes of a controlled Jamming AP transmitting at power  $P_1$  affect legitimate clients, the AP reduces its transmit power slightly to  $P_2 = P_1 - \delta$ , (where  $\delta$  is a small power decrement in dB) such that the legitimate clients are not affected.

### 3.4.3 Scalability of individual strategies

We evaluate the security improvement provided by each of the above techniques in isolation for varying number of access points ( $p$ ) and elements ( $k$ ) using simulations. The simulation parameters are described in section 3.7. The results are summarized in Tables 2, 3.

**Table 2:** Ordering of strategies

Reduction in ER over Omni		
Strategy	$k = 4, p = 12$	$k = 12, p = 4$
Secret sharing	37	117
Controlled Jamming	122	260
Stream Overwhelming	10	6

**Table 3:** Benefits over beamforming

Reduction in ER over Beamforming		
Strategy	$k = 2$	$k = 12$
Secret sharing	3	7
Controlled Jamming	40	54
Stream Overwhelming	2	4

Thus, the use of beamforming (in secret sharing) reduces received signal energy in several locations in the network where the eavesdropper would not know of the existence of any transmission. However, when controlled jamming and stream overwhelming are considered, although the signal energy would be high the eavesdropper would be unable to identify whether the signal is a WLAN signal or a signal not of interest such as a Zigbee or microwave signal, which AP the signal is transmitted

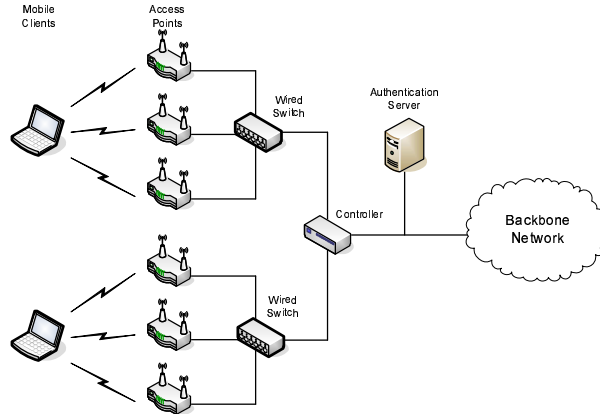


from, etc. In this sense, each of the strategies limit the knowledge of the existence of information itself.

## ***3.5 Architecture and Algorithms***

### **3.5.1 Architectural model**

The architectural model that we consider consists of a central controller connected to several access points as shown in Figure 5. The controller receives from the backbone a stream of packets to be transmitted over the wireless LAN to the clients. For such packets, it employs a combination of the schemes discussed in Section 3.4, and forwards the packets to the appropriate access points. We assume that the controller has strict synchronization and control over the access points. All transmissions by the APs are done at the granularity of *synchronized fragment slots*, where the length of a fragment slot is smaller than that of a *packet slot*. The controller controls both the downstream and upstream (we discuss upstream communication toward the end of the section) modes of communication, and the two modes alternate in epochs. For downstream communication, the controller divides packets into fragments, applies its security decisions, and provides the APs with a set of fragments to transmit. Additionally, the controller knows the locations of the APs in the network and also the approximate locations of the clients (using for instance [25]). Further, it also possesses a coverage map to identify how the actual transmissions could be affected by the scattering nature of the channel. This information is already in place, in commercial products and will be leveraged to make intelligent pattern adaptation taking into account the beamforming impairments due to multipath. Also, since some of the APs will be part of the controlled jamming strategy and the entire coverage map is known, the coverage of jamming signals is also known.



**Figure 5:** Network model showing a high density of APs and a controller in an enterprise

### 3.5.2 Integrated operations

While we discussed the three key strategies of secret sharing, controlled jamming, and stream overwhelming in Section 3.4, an important element of the operations is *how are the three techniques used in tandem to achieve the best performance possible?* While we present the details of the integrated operations in the description of the algorithms later in the section, we now briefly discuss the important constraints and trade-offs that form the basis of the algorithmic design. Briefly, two types of considerations need to be taken into account in deciding on the specific form of integration between the three techniques:

- **Security vs. throughput:** The primary trade-off in using the VAPA techniques outlined thus far for security is in the form of throughput. However, the three techniques differ in the extents of the trade-offs. Stream overwhelming provides its security benefits *without any degradation in throughput*. Controlled jamming, on the other hand, uses access points (other than the primary sender) purely for generating interference, and hence trades-off throughput the most. Finally, secret sharing can achieve certain levels of security without trading-off throughput, but can also trade-off throughput further to achieve a higher level of security. Hence, from a *security - throughput trade-off standpoint, controlled*

*jamming performs the best for security, but the worst for throughput. Stream overwhelming does exactly the opposite, while secret sharing lies in the middle.* Thus, for any set-up with security objectives with throughput constraints, the above trade-offs will have to be taken into account while determining the extent to which each of the three techniques will be used.

- Network resources and topology: Another important set of influencing factors includes the number of elements at the APs (and clients), the number of APs, and the specific topology. For example, if a client is accessible only through one AP, it cannot receive any secret sharing benefits. Stream overwhelming benefits can be achieved as long as AP-client pairs within interference range of each other are scheduled to transmit together. Finally, controlled jamming can be accomplished as long as there is one or more APs within interference range of a scheduled transmission. From a number of resources standpoint, secret sharing depends more on the number of APs, whereas controlled jamming and stream overwhelming depend more on the number of elements at the APs.

### ***Design Trends***

Based on the above considerations, it is clear that the desired throughput-security values and the available network resources and topology determine the right choice of strategies. Hence, the main guiding principles adopted for the algorithm design are as follows: (i) For a desired security, if capacity has to be maximized, then one must determine whether the security is achievable by purely stream overwhelming or secret sharing alone. If not, then the minimal number of APs necessary for controlled jamming needs to be used such that it will guarantee the desired level of security, and use the remaining APs for secret sharing or stream overwhelming to improve security while maximizing the capacity. (ii) Similarly, for a desired throughput constraint, if security has to be maximized, a combination of stream overwhelming and secret sharing (with preference to secret sharing) should be used for achieving the desired

throughput, and the remaining APs should be devoted to controlled jamming to maximize security.

In the rest of this chapter, we consider only the model where subject to a throughput constraint, security needs to be maximized. All discussions can be extended with minimal effort for the alternate model as well.

### 3.5.3 Problem formulation

In the model described thus far, the intelligence is concentrated at the controller and can be divided into two major components, *the throughput scheduler and the security scheduler*. The throughput scheduler takes as input a throughput constraint  $S$  (in the number of packets desired to be delivered) and determines the maximum number of packets  $j$  that are schedulable subject to a bound of  $S$ . This value  $j$  is then fed into the security scheduler that then determines the right strategies to use to maximize security while transmitting the  $j$  packets. Consider that the controller has an infinite stream of packets in its queue. We assume that any fairness mechanisms are implemented even before the packets reach the controller. In this fashion, the security algorithm works without affecting the fairness and is agnostic to the fairness mechanism used. The algorithm serves packets only in the order that they were queued to prevent potential starvation and out-of-order delivery problems .

The first part in the formulation is to determine the number of in-sequence packets  $j$  that can be scheduled out of the first  $S$  packets.  $S$  is thus a tunable knob which can be used to tune the desired levels of security in the network. For instance, if  $S = 1$ , then the problem reduces to maximizing security for this single packet's transmission. However, when  $S$  is larger (bound by the number of APs) then throughput is maximized, and any security achieved is opportunistic using unassigned resources. Note that, given a set of  $S$  packets, the number of in-sequence packets that are schedulable is not fixed but depends on the way APs are assigned. Thus the largest number of

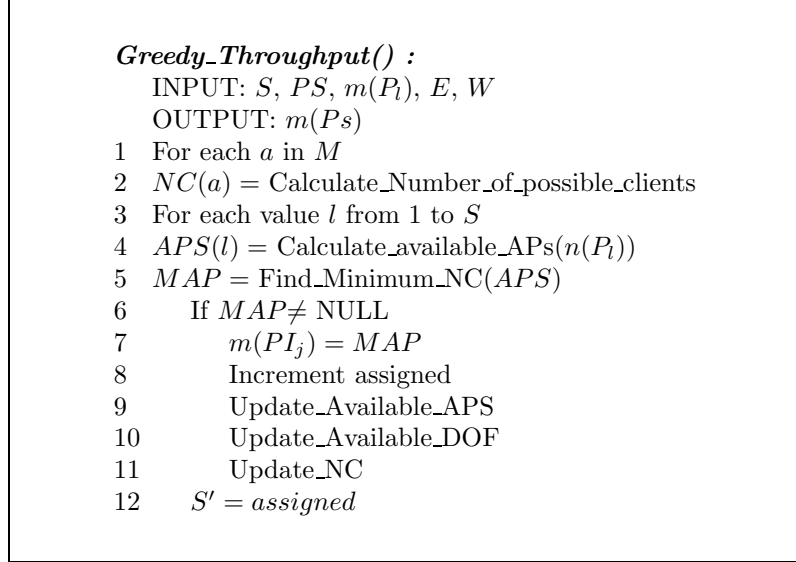
<p> <math>S'</math>: schedulable number of packets  <math>PS</math>: schedulable packet stream  <math>PS_s</math>: first <math>s</math> packets in the packet stream  <math>p_l</math>: <math>l^{th}</math> packet in <math>PS</math>  <math>F</math>: number of fragments  <math>r(a, b)</math>: available DOF of AP <math>a</math> for fragment <math>b</math>  <math>f</math>: fragment index, <math>m(p_l)</math>: AP to which packet <math>p_l</math> is to be sent  <math>E</math>: network Connectivity matrix  <math>AP(n)</math>: set of APs within communication range of client <math>n</math>  <math>n(p_i)</math>: destination(client) id of packet <math>P_i</math>,  <math>W_{ij}</math>: <math>(i, j)</math>-th element of link conflict matrix,  <math>W_{(ab)(cd)}</math>: link conflict indicator between links <math>ab</math> and <math>cd</math>,  <math>m(p, f)</math>: assigned AP id of packet <math>p</math> during fragment <math>f</math>  <math>Action(a, f)</math>: action of AP <math>a</math> for fragment duration <math>f</math>  <math>N</math>: set of clients for which packets are destined in <math>PS</math>  <math>M</math>: set of APs which are in range of clients in <math>N</math> </p>
---

**Figure 6:** Definition of variables

packets that can be scheduled will be achieved for the optimal scheduling algorithm. In the second part of the problem, the security mechanisms need to be applied to the  $j$  in-sequence packets such that those  $j$  packets are transmitted by the end of the slot but the security is maximized for these  $j$  packets (by appropriate choice of strategies for the APs during the fragment durations).

### 3.5.4 Idealized model and algorithms

The idealized model for the application of *Aegis*, consists of a central controller which controls the communication actions of each of the access points and comprises two cascaded schedulers. In such a case, the access points have a high degree of synchronization and do not take independent actions. Further, we assume that the access points act exactly as dictated by the controller and the controller has access to the head of line packet of the queue in each access point and also knows the positions of the access points and clients in the network (using for instance practical localization algorithms such as in [25]). We focus only on the downstream communication

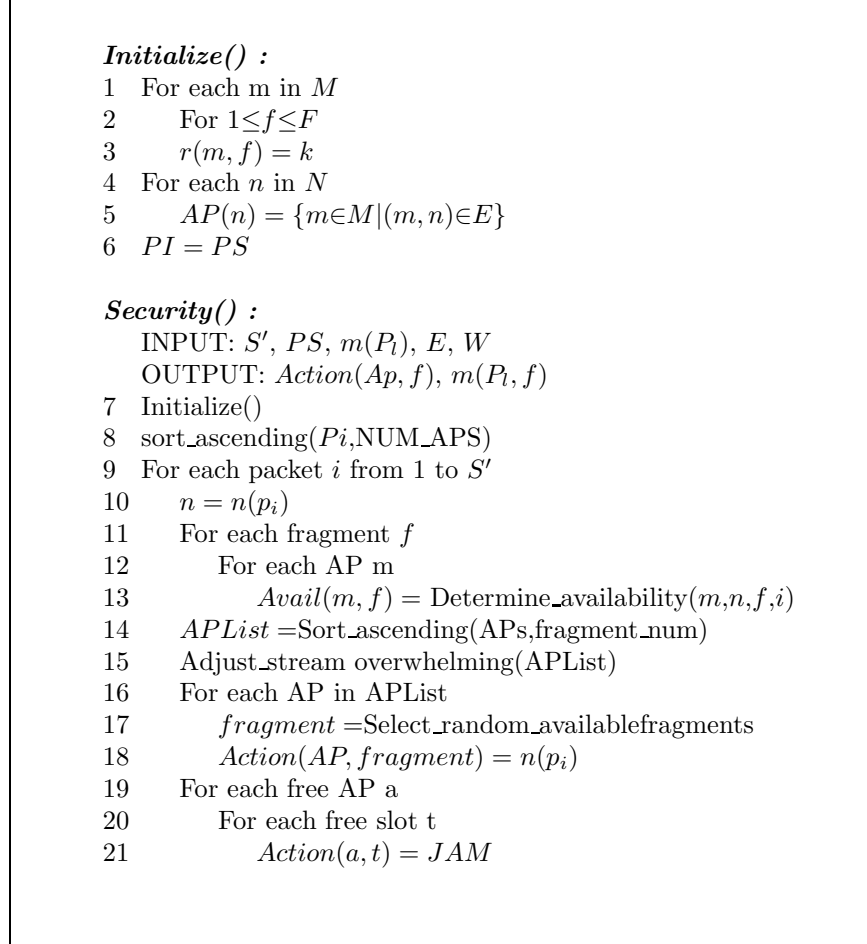


**Figure 7:** Throughput scheduler

here. We now present the details of the two cascaded schedulers at the controller.

#### *3.5.4.1 Throughput Scheduler*

The throughput scheduler takes as input the control parameter  $S$  and the first  $S$  packets in the input queue of the controller. It provides as output the set  $S'$  of the  $j$  schedulable in-sequence packets. The algorithm used is a greedy algorithm that attempts to maximize  $j$ , the number of in-sequence packets that would be served during this transmission slot considering the spatial reuse and the adaptive interference suppression capability. Note that while we use a greedy algorithm as a representative, any throughput scheduling algorithm designed for adaptive arrays is usable at this stage. The throughput scheduler first calculates how many clients for this packet stream can potentially use an AP, for each of the APs in the AP set  $M$  (lines 1-2). Then, for each packet starting from the first packet in the queue, the set of available APs is computed (line 4). Of this set, the one with minimum potential clients is chosen to be the one for this packet (line 5-7), as long as there is some such AP. Then the available APs, DOFs and the number of potential clients are updated at each AP. In this fashion, the number of in-sequence schedulable packets is given by the number



**Figure 8:** Security Scheduler

of packets that could be assigned.

### 3.5.4.2 Security Scheduler.

The objective of the security scheduler is to identify the assignment of actions of APs for different fragment durations such that all the packets handed down by the throughput scheduler are scheduled, while minimizing the exposure region. These are performed in a greedy manner, where secret sharing is the default strategy. However, when there is a tie between two choices of available APs for a fragment, both giving the same secret sharing benefit, then stream overwhelming is used as the strategy of choice. Once the possible fragments are scheduled (i.e. the throughput scheduler's constraint on number of packets is met), controlled jamming is attempted in the free

fragment durations. The free APs determine if the number of clients, for which to perform interference suppression, is less than  $k - 1$ . If so, that AP performs jamming for that fragment duration, otherwise, the next free fragment duration is checked. In the pseudocode, the edge connectivity matrix is given as  $E$ , where an entry of 1 in the  $(i, j)^{th}$  position indicates that node  $i$  and node  $j$  are within communication range of each other. The link conflict matrix is given as  $W$ , where  $W_{ij}$  is 1 if the links  $i$  and  $j$  are interfering links. Similarly  $W_{(ab)(cd)}$  represents whether links  $ab$  and  $cd$  interfere with each other. The algorithm takes as input the set of schedulable packets provided by the throughput scheduler, the connectivity and interference matrices of the network, and the set of client destination ids of the packets. As output, the algorithm provides the actions of the different APs for the different time-slots. This is indicated by  $Action(a, f)$  to indicate the action of AP  $a$  during fragment duration  $f$ . The action can either be a transmission of a fragment to a client  $c$  (indicated by  $Action = c$  in the pseudocode) or controlled jamming with care about clients (indicated by  $Action = JAM$ ) in the vicinity. Based on this, the APs to which each fragment of each packet is destined ( $m(p_i, f)$  in the pseudocode) can also be obtained. To begin with all the APs reachable from a client are included in the list of available APs for each client. Then the packets are arranged in ascending order of the number of APs (line 8). This is because clients with fewer number of APs should definitely be scheduled and must not lose their AP to other clients who may want to perform secret sharing. The next step is to identify the availability of each of the APs of the client under consideration for the different fragment durations (lines 11-13) i.e. the number of fragment durations that each AP is available and which of the fragment durations each AP is available. The availability of an AP during a fragment is decided by the number of already scheduled active clients in its vicinity and the number of DOF that it possesses. For instance, if there are already  $k - 1$  scheduled transmissions in the vicinity of this AP for that fragment



duration, then any additional transmission would surely cause interference. Next, the available APs are sorted in ascending order of the number of slots in which they are available. The AP with the fewest available fragments is scheduled first because, the allocation tries to greedily assign different APs for the fragment durations to obtain the secret sharing benefit. For instance, if an AP is available for only one fragment duration and another available AP is allocated during that fragment, then this AP would not be included (reducing the secret sharing benefit). The available APs are allocated (line 15 -18) in a round robin manner such that for each AP one of the available fragment durations is picked randomly. Such a technique has an advantage over randomly selecting one of the available APs for each fragment duration. This technique ensures that as many different APs are chosen as possible which improves secret sharing benefit over a random choice, whereas in selecting one of the available APs randomly for each fragment, there is a finite probability that a single AP is chosen for all fragments minimizing the secret sharing benefit. The algorithm thus ensures that the secret sharing benefit is maximized greedily. When there are more than one APs with same number of available fragment durations, the choice of AP is such that stream overwhelming is possible (line 15). Once the data schedules are completed, the controlled jamming strategy is applied (lines 19-21) taking the number of already active links and available DOFs into account. For all the free fragment durations, the number of scheduled clients in the vicinity of that particular AP for that duration is determined. If this value is lesser than  $k - 1$ , then it is possible to perform controlled jamming without interfering with clients and the AP is assigned a jamming action. However, if there are already enough clients in the vicinity, then controlled jamming would not be applied. In this way, the algorithm greedily applies the techniques according to the design guidelines presented in the previous section.

### ***3.6 Practical Realization***

We now briefly discuss an approach for practical realization of *Aegis* in the context of the 802.11 PCF (point coordination function) mode of operation. The 802.11 PCF is an access mechanism that operates in the infrastructure mode, where an access point of a cell acts as the central coordinator called the Point Coordinator(PC). The PC grants a contention free channel access to individual nodes by polling them for transmissions. On being polled, a node transmits a single frame. In the infrastructure mode, time is divided into periodic superframes which start with the beacon frames. At the beginning of a superframe, the PC waits for a PCF Inter Frame Spacing (PIFS) for the channel to be idle and then transmits the beacon frame which is a broadcast packet carrying special information. The PC, then consecutively polls each of the stations that operate in PCF mode, one at a time. At the end of the CFP, the PC sends a CF-END frame to signal the end of that CFP.

The PCF mode of operation is well-suited to the proposed solution in the context of a virtual array of physical arrays. The polling based mechanism endows the PC with the exact transmission slots for each client’s communication. The controller can assign the sequence to be used by each PC. Since the controller acts as a central decision maker, the exact assignment of actions to each AP in the network is possible and is accomplished within the current framework of the WLAN PCF mode of operation.

However, since transmissions are arranged always in an “AP first, client-next manner”, the actions of the APs for the durations of the client communication must also be determined. Specifically, since each AP listens for the reply from a client, it cannot be utilized to perform other actions such as counter jamming. Hence, when the clients talk, the counter-jamming APs must now perform interference suppression with respect to the APs and not the clients. In this fashion, the existing solution can be adapted to take the direction of information flow and the slotted access within the PCF mode of operation.

While the above realization has been presented in the context of downstream communication, it is relatively straightforward to extend the schemes to the *upstream communication* as well. To make correct decisions, it is necessary to obtain information about the time slot that different clients would use for their transmission. However, the use of a polling based mechanism, enables the AP to know what time duration a transmission can be expected from a client. This information is used along with the client positions to generate different communication patterns. More specifically, the controller performs centralized control to determine the actions of APs for the downlink, whereas the polling to cater to the clients and provide upstream security can be obtained by the APs controlling the polling sequence. This would enable the controlled jamming technique to be applied with the modification that nulls are placed by the jamming AP towards other APs in the vicinity as opposed to clients. However, stream overwhelming could be performed by adjusting the polling sequence. Also, the secret sharing approach can be applied by the client transmitting fragments to different APs consecutively. This will require that the client be able to obtain a dedicated fragment duration to transmit to each of the APs. In this manner, the basic schemes are applied with intelligent modifications of protocol parameters.

*Loss of fragments:* As discussed in the previous section, when a fragment is lost, all the fragments of that packet will be scheduled again in the next slot. While only the lost fragment needs to be transmitted, we use a retransmission of all fragments to keep loss recovery simple.

*Variable packet sizes:* When the packet size varies, the overhead of fragmentation could be high. Thus the size of the fragment relative to the ciphertext determines the efficiency of operation. Further, the efficiency would already be low because of other headers, fragmentation could reduce it further. In such cases, it must be ensured that the fragment size is greater than a threshold value. If not the secret sharing could be applied across packets with no fragmentation of small packets.

We add that, *Aegis* can also be realized by connecting multiple spatially disjoint beamforming antennas to a single AP using a cable (as recently introduced in [26]).

## 3.7 Performance Evaluation

### 3.7.1 Simulation model

We use a custom simulator written in C++ for the evaluation. The custom simulator incorporates the following modules: smart antennas pattern computation, ability to perform adaptive array processing [27] and indoor channel models. The details of the models are described below. *Beamforming*: Adaptive beamforming using the matrix inversion techniques described in [27]. *Channel model*: We use the ITU indoor attenuation model, which includes log-distance path loss with an exponent of 4 and a lognormal fading with a standard deviation of 2.5dB. We use a link margin of 3.2 dB (3dB with a 90% link reliability), an operating frequency of 2.4 GHz, an SNR threshold of 15 dB, a noise level of -100dBm (0.1pW), a sensitivity of -85dBm (3 pW) and a maximum transmission power of 20dBm (100mW) as used in standard 802.11 equipment. The default number of antennas is 4 and number of APs is 4. *Positions*: We generate the position of the client and APs randomly within the grid of points in a 100m \* 100m grid. We also select the eavesdropper's(s) position randomly within the grid. We consider 20 clients by default. *Traffic flow*: We consider downstream flows to a randomly chosen subset of clients. For each data point, we calculate the average of 20 simulation runs. *Metric*: The metric of interest is the average exposure area normalized to the area of the network. The network area is divided into ten thousand square grids. The number of grids in which the information from any of the APs is decodable divided by the total number of grids is plotted as the exposure region. For a single eavesdropper, a grid is exposed if the SINR in that grid is sufficient for decoding and all shares of a given packet are decodable. For the case of colluding eavesdroppers, if the eavesdroppers can together successfully decode all shares of a

given packet, then the grids occupied by them are exposed.

### 3.7.2 Simulation results

We present results for the integrated algorithm in this section.

#### 3.7.2.1 Varying number of elements $k$

We explore the effect of varying the number of antenna elements on the APs. From Figure 9 as the number of elements on the APs is increased, the exposure region is reduced significantly. We also observe that the exposure region is extremely small when the integrated algorithm operates. Further, and more importantly, the exposure region of simple beamforming is much larger compared to the integrated solution. This means that it is only the intelligent use of the mechanisms that gives large security gains and not just simple beamforming.

#### 3.7.2.2 Varying number of access points $p$

In Figure 10 we show how the average exposure region varies with the number of access points. We observe again that the exposure region reduces drastically as the number of APs is increased. Specifically, with 12 APs, a 2000x improvement compared to omni-directional communication.

#### 3.7.2.3 Varying values for parameter $S$

As we vary the value of  $S$  from low to high, the importance shifts from security to throughput. However, we observe from Figure 14 that while the throughput increases with increase in  $S$ , the security benefit does not degrade. This is counter-intuitive and means that the stream overwhelming benefit also increases when the number of scheduled transmissions increases. Specifically, when the number of transmissions is increased upto a certain value (3 in the Figure), the exposure region now increases since the eavesdropper can access more information than a single client's information.

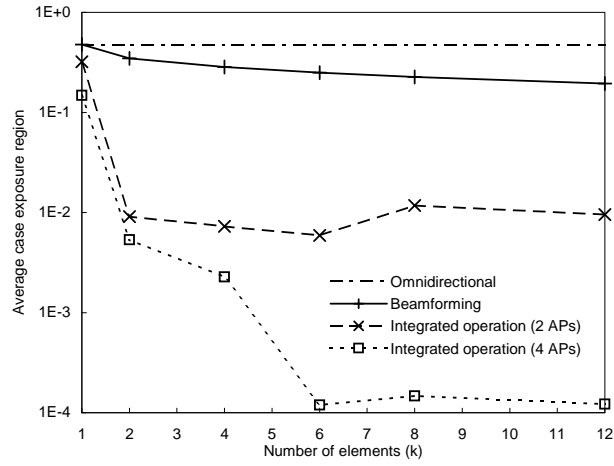


Figure 9: Impact of  $k$

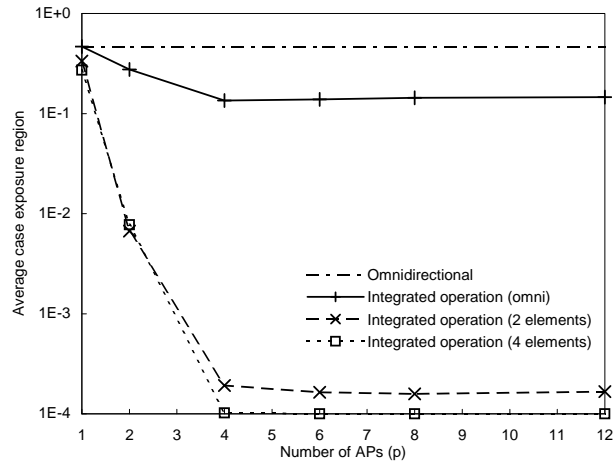


Figure 10: Impact of  $p$

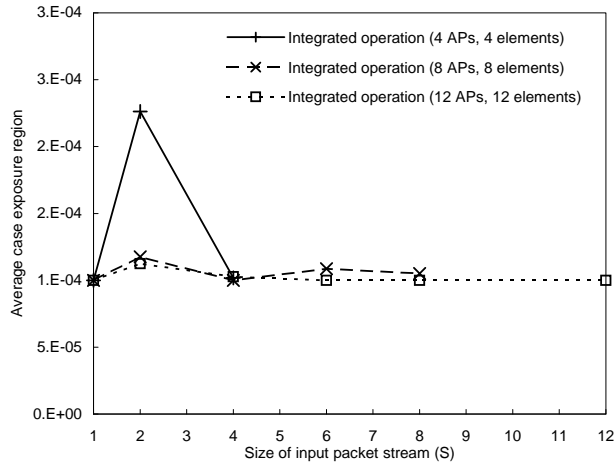


Figure 11: Impact of rate parameter  $S$

However, as  $S$  increases, the chances of applying stream overwhelming increases causing the exposure region to reduce. This suggests that the intelligent use of all the three techniques enables maximizing both throughput and security without any significant tradeoff for the given conditions.

#### 3.7.2.4 *Varying number of colluding eavesdroppers*

We simulate the effect of colluding eavesdroppers. For each packet destined to a client, we calculate if at the end of the slot duration, the eavesdroppers together have all the fragments for a client's packet. From Figure 14, one can observe that collusion increases the exposure area. Here the metric of exposure region by itself is not sufficient. Hence the metric used here is the packet exposure probability. Packet exposure probability for a given scenario is the number of packets that eavesdroppers can decode by collusion divided by the number of packets scheduled in a slot. This metric is shown in Figure 14. One can observe that with 4 Access points and with 4 element arrays each, the average packet exposure probability grows very gradually with increasing number of colluding eavesdroppers. Here we recall that collusion can only affect secret sharing, whereas controlled jamming and stream overwhelming would be unaffected by collusion. This is because, spatially separated eavesdroppers could decode different shares of the same message to compromise the security of an information packet. However, when the signals are jammed or overwhelmed at different parts of the network, they cannot be post-processed to improve the SINR since both the signal and noise would add together. Further, the channel gains would be different causing the signals to combine destructively if added as is. This explains why only with a large number of colluding eavesdroppers there is some increase in packet exposure probability. i.e even with 25 colluding eavesdroppers the packet exposure ratio is less than 20%.

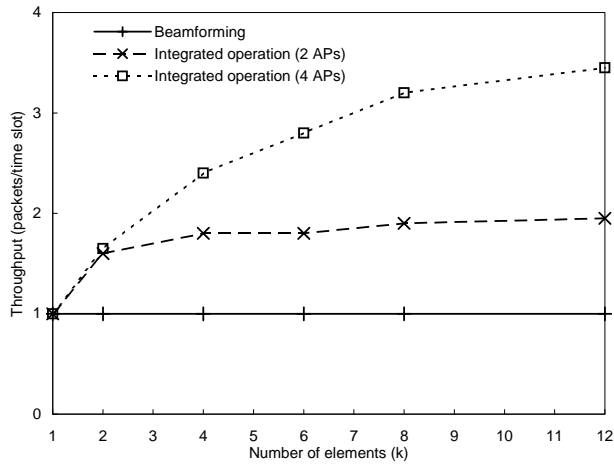


Figure 12: Throughput variation with  $k$

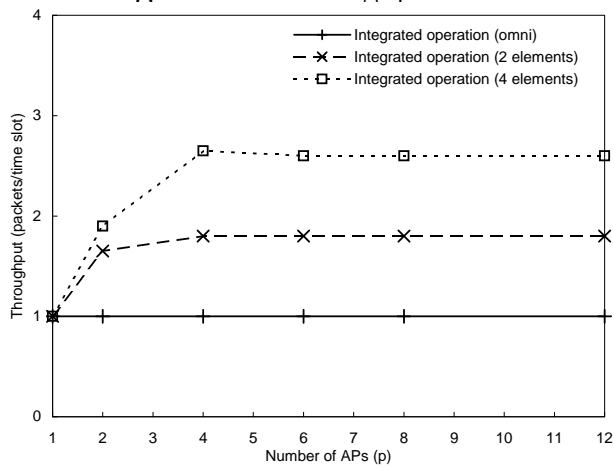


Figure 13: Throughput variation with  $p$

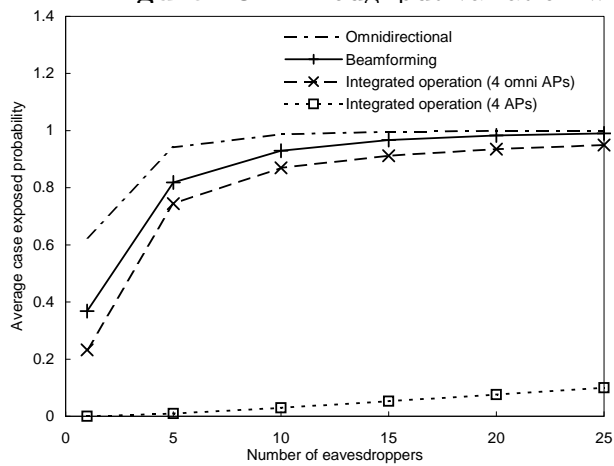


Figure 14: Eavesdropper collusion: Average case



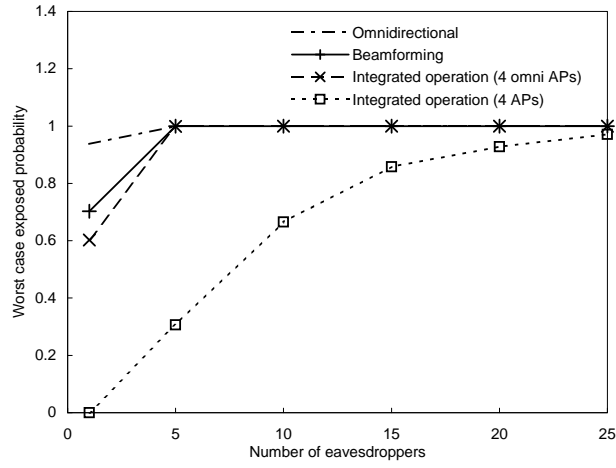


Figure 15: Eavesdropper collusion: Worst case

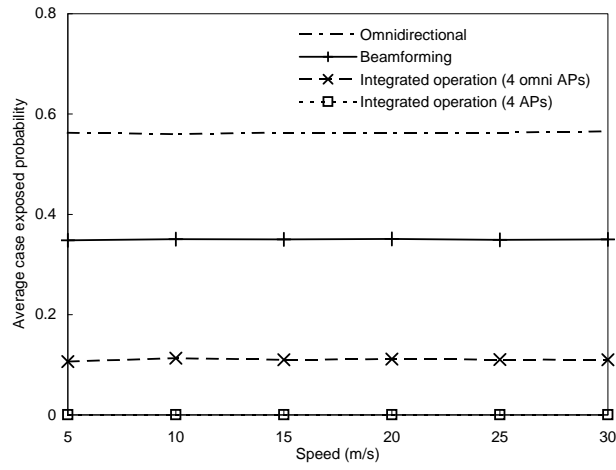


Figure 16: Eavesdropper mobility

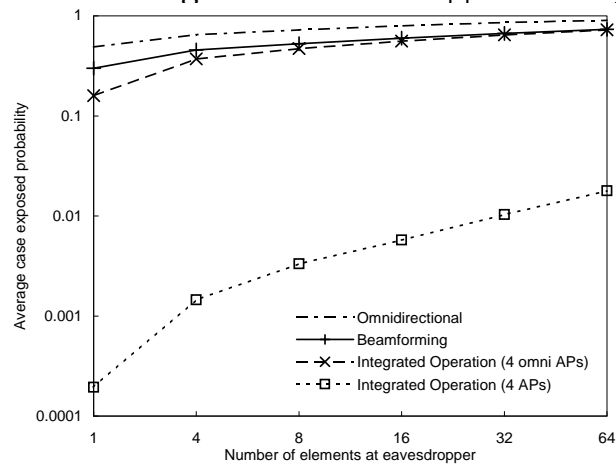


Figure 17: Eavesdropper antenna capability

### 3.7.2.5 Varying number of antennas at the eavesdropper

An eavesdropper with multiple antennas can use the antennas to beamform towards the clients or the AP. Since adaptive beamforming requires coordination between the sender and the receiver to estimate the correct beamforming weights [18], the best strategy for the eavesdropper is to use directional beamforming. While the beam direction could be arbitrarily chosen, the most insecure case happens when it 'magically' knows the direction of an AP which sends data. Hence, we simulate this strategy and plot the exposure region. As observed in Figure 17, Aegis results in an exposure region of 1.8% even for an eavesdropper with 64 antennas, which is significantly lower compared to using LOS beamforming (73.3%) and Omni-directional links (90.6%). The underlying reason is that, with increasing number of antennas, the signal gain at the eavesdropper is higher. However, the interference it perceives from the controlled jamming and stream overwhelming APs still leave it unable to decode all of the packets.

### 3.7.2.6 Varying mobility of eavesdroppers

As the eavesdroppers move, the algorithm still works in the same manner as when the eavesdropper did not move as illustrated in Figure 16. This is because, the algorithm does not assume any information about the mobility of the eavesdroppers. When the eavesdropper was allowed to move with a velocity from 5m/s to 30m/s, the security performance sees no significant change.

## 3.7.3 Proof of concept field trials

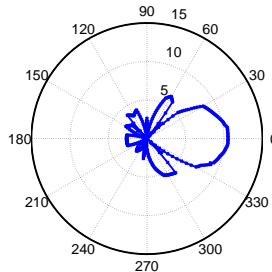
The objective of this section is to demonstrate that *Aegis* can be applied to indoor wireless settings to obtain security benefits using off the shelf components. The field trials are carried out in the fifth floor of a high rise building. The equipment used consists of three commercial 802.11g APs equipped with omni-directional antennas and a laptop. The effect of beamforming is demonstrated using a custom-built patch

**Table 4:** Field trials

Strategy	Insecure locations
OMNI	18
BF	14
BF+SS	4
BF+CJ	14
BF+SS+CJ	3

antenna for each AP to provide a beamwidth of 60 degrees and a mainlobe gain of 10 dB. 21 positions on the corridors of the building were identified for the experiment, with one client position and 20 as potential eavesdropper positions. The experiments conducted was the sending of ping packets between the laptop and each Access Point and measuring the ping responses. The successful reception at the receiver is determined by the success of the ping responses. The radiation pattern of the directional beamforming antenna is as shown in Figure 18. The antenna on each AP is (physically) positioned such that the client received a high power (main lobe) transmission from the desired AP and low power (null) transmissions from the other APs.

Table 4 shows the number of positions in this setup, where an eavesdropper can decode the communication of an AP for a given strategy. The second and third rows of the table show the number of points at which an eavesdropper can successfully decode the packets when the AP communicating to the client (AP1) uses an omni-directional antenna and a beamforming antenna respectively. The next three rows represent the number of points at which an eavesdropper can decode the packets when the strategy is just secret sharing or controlled jamming or secret sharing and controlled jamming, respectively. It can be observed that the number of insecure locations is progressively reduced as each technique is applied and the maximum benefit is obtained using the integrated solution of beamforming+secret sharing+controlled jamming. The results show that although practical impairments such as scattering exist, benefits are still obtainable in an indoor setting.



**Figure 18:** Radiation pattern

### ***3.8 Practical Beamforming***

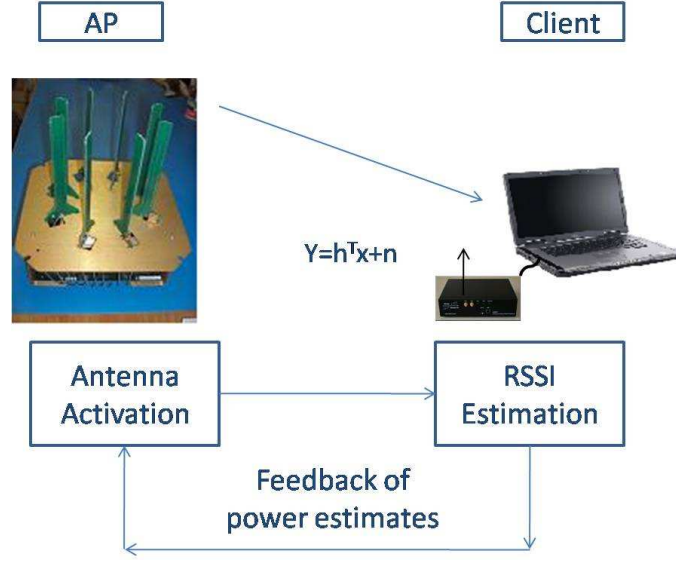
The goal of this section is to study the channel stationarity and to quantify the benefits of beamforming in practical indoor Wireless LAN scenarios.

#### **3.8.1 Overview**

Indoor environments are characterized by the phenomenon of “multipath” propagation of signals, where the signals transmitted from the transmitter get scattered, attenuated and delayed differently before combining at the receiver. Often times, the signals could combine destructively to make the effective signal at the receiver weak. *Beamforming* is a technique in which the signals fed to each of the antenna elements can be weighted in both amplitude and phase to produce a desired beam pattern that leverages the spatial variation optimally and increases the SNR at the receiver. Thus beamforming consists of two components (i) channel estimation and feedback from receiver and (ii) weight application at the transmitter as illustrated in Figure 19.

#### **3.8.2 Power based beamforming solution**

We provide a new beamforming solution that performs approximate channel estimation using signal power measurements at the receiver in conjunction with an intelligent antenna activation algorithm at the transmitter [43].



**Figure 19:** Channel estimation and beamforming.

### 3.8.2.1 Key idea

The algorithm is based on the idea of estimating differential channel phases by employing *tandem activation of more than one antenna* and using received power estimates. Thus, the estimation process is distributed across space (elements) instead of time. In conventional channel estimation, when a single antenna is activated at a time, the received power is dependent only on the channel magnitude and is given by  $P_i = |h_i|^2$  (assuming the transmitter power is unity). Hence the information about the channel phase  $\arg(h_i)$  is lost when the power is computed. In contrast, by the tandem activation of more than one antenna element, the effects of the channel phases are also reflected in the received power in a manner that depends on the relative channel phases. i.e. when two elements  $i$  and  $j$  are activated simultaneously with equal weights (such that the transmitted power still adds up to unity), the received power can be computed as  $P_{ij} = |h_i + h_j|^2$ . Thus, for tandem activation, the received power  $P_{ij}$  is given as

$$P_{ij} = P_i + P_j + 2 * \sqrt{P_i * P_j} * \cos(\theta_{ij}) \quad (2)$$

where  $\theta_{ij}$  is the *channel phase difference* between  $h_i$  and  $h_j$ . Depending on the relative channel phase  $\theta_{ij}$ , the two signals combine together to change the signal power at the receiver. When  $\theta_{ij} = 0$ , the signals combine constructively causing the powers of the individual elements to add up at the receiver. However, when  $\theta_{ij} = 180$  the signals combine destructively causing the received power to be the difference of the powers transmitted from the individual antennas. Hence, the change in the received power across a strategic set of activations can be used to identify the relative channel phase between the channel gains by rewriting Equation 2 as

$$\theta_{ij} = \cos^{-1} \frac{P_{ij} - P_i - P_j}{2 * \sqrt{P_i * P_j}} \quad (3)$$

By repeating this idea for pairs of antenna elements, the relative phases can be obtained. Since all the channel phases must be measured with respect to the same reference for estimates to be meaningful, we designate element 1 as the reference element. The channel gain magnitudes can be obtained directly from the power measurements by activating each antenna element individually as  $|h_i| = \sqrt{P_i}$ . When used along with the relative phases, the beamformer weights can be determined as  $w_i = \sqrt{P_i} e^{j\theta_{i1}}$  for  $i > 1$  and  $j = \sqrt{-1}$  with  $\theta_{11} = 0$ . We also note that, irrespective of the number of antennas used, we ensure that the total transmitted power remains constant by normalizing the weights.

**Algorithm steps:** The algorithm consists of the following steps and is performed at the transmitter and receiver consecutively.

*1. Single and tandem activation with equal weights:*

In the single antenna activation stage, each one of the  $K$  elements at the transmitter is activated in isolation, i.e. one at a time using  $S$  consecutive packets for each antenna element.  $S$  is a parameter that can be increased for more accurate estimates but is chosen to be small to keep the overhead of the estimation process low (we use  $S = 5$  in our experiments).  $S$  becomes specially important to perform right ambiguity resolution. This is followed by activating two antenna elements at a time. One of

the two antennas in each activation is the reference antenna element and the other is chosen successively from second to the  $K^{th}$  antenna.

*2. RSSI measurement and computation of channel magnitudes and phases:*

The  $K - 1$  received signal power values (we use RSSI as an approximation for the received power in our experiments) for each of the tandem activations is noted at the receiver along with the  $K$  average signal powers for the single activations. These  $2K - 1$  values are then used to compute the magnitudes  $|h_i| = \sqrt{P_i}, 1 \leq i \leq K$  and the relative phases  $\phi_{i1}, 1 < i \leq K$  from Equation 3. The  $K$  magnitudes  $|h_i|$  and the  $K - 1$  relative phases are then conveyed to the AP in a single packet.

*3. Ambiguity resolution through tandem activation with unequal weights:*

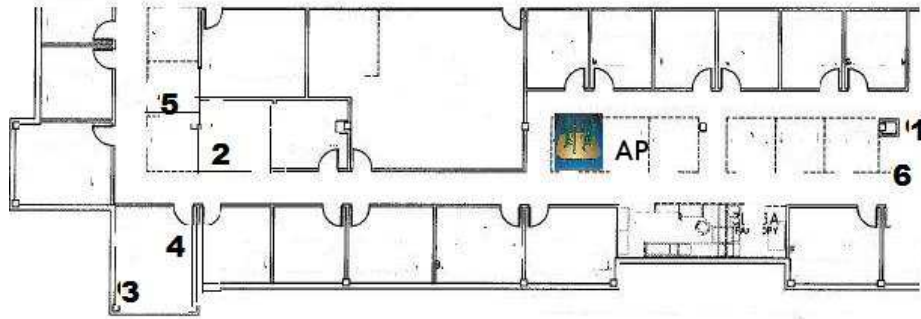
While the magnitudes are obtained correctly, the phases  $\phi_{ij}$  (in radians) have an ambiguity due to the use of the  $\cos^{-1}$  function in Equation 3. i.e. the correct  $\theta_{ij}$  can be either of  $\phi_{ij}, -\phi_{ij}, \pi - \phi_{ij}, -(\pi - \phi_{ij})$ . To resolve the ambiguity, the  $k - 1$  pairs activated in tandem in Stage 1 are again activated but with modified amplitude and phase weights<sup>3</sup>. i.e., element 1 is activated using the magnitude  $\sqrt{\frac{P_1}{P_1+P_i}}$  and phase '0', whereas element  $i, i > 1$  is activated with a magnitude  $\sqrt{\frac{P_i}{P_1+P_i}}$  and each of the phases  $\phi_{ij}, -\phi_{ij}, \pi - \phi_{ij}, -(\pi - \phi_{ij})$ . Hence, for each of the  $K - 1$  pairs, there are four activations corresponding to these four phases, which we call the quadruple.

*4. Accurate beam weight determination:*

Of the four choices in each quadruple, the receiver identifies the choice which yields the largest signal strength at the receiver and notes this as the unambiguous relative phase for each of the non-reference antenna elements i.e. element 2 to element  $K$ . The final beamforming weights for each antenna element  $i$  is given by the magnitude  $|w_i| = \sqrt{\frac{P_i}{\sum_{i=1}^K P_i}}$  and the phase  $\theta_{i1}$ .

---

<sup>3</sup>The relative magnitudes are chosen such that it is the same as what would eventually be used by the beamformer; only ambiguity in phase is being resolved at this point.



**Figure 20:** Experimental testbed: The numbers indicate client locations.

### 3.8.3 Prototype setup

To implement beamforming, we use a testbed consisting of an 802.11b/g access point with a phased array antenna from Fidelity-Comtech [44] and a laptop running Ubuntu 8.10 equipped with a D-Link 802.11b/g card in an indoor office environment as shown in Figure 19. The AP runs the open source Madwifi WLAN driver. It also consists of a set of 16 pre-computed directional antenna patterns that cover the entire 360 degrees and a command interface to set and write new beam patterns. In the AP, the pattern that is selected is used for both transmission and reception. The D-Link card uses the Atheros chipset and the Madwifi driver. We use Iperf as the traffic generating application and the *athstats* Madwifi utility on the laptop to obtain fine grained statistics from the card. The AP is placed at a fixed location on top of a cubicle and the laptop is placed at six different locations throughout the building as shown in Figure 20. The transmit power of the AP is fixed at 10dBm for all experiments. We use two main metrics: (1) the SNR (computed from the RSSI and the Noise Floor reported by the card) and (2) the throughput reported by the Iperf application on the receiver. We mainly highlight the benefits of the beamforming solution (Bf) in comparison to *Omni*(where the transmitter uses a single antenna element) and *Dir* where a directional pattern that points to the receiver is used. All experiments are conducted with 1500 byte packets by default and RTS/CTS is not used.



### 3.8.4 Experimental results

We vary the position of the client among the positions in Figure 20 and profile the performance of Omni, directional and beamformed links. We use Iperf to transmit UDP traffic to the client for one minute in the following scenarios. We then measure the SNR and throughput at the receiver in each of these cases. The results are plotted in Figures 21 and 22 for each of the six different locations. It is seen that beamforming performs better than directional and Omni at each of these locations. The average improvement of beamforming over Omni is 10.5 dB in SNR and 7.1X in throughput for the locations profiled. In addition, we also observe the loss rate at the MAC layer (CRC errors) and plot it in Figure 23. Beamforming shows a clear improvement in loss performance.

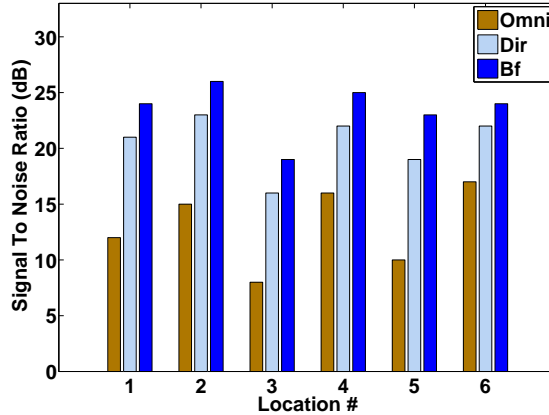


Figure 21: RSSI gain

Finally, we observe the variation of channel coefficients from this setup and plot the magnitude and the phase of the channel gains in Figures 24 and 25. The figures show the magnitude and phase of the channel gains for two successive one minute runs. It is clear that the indoor wireless channel provides short term stationarity that makes beamforming feasible in practice.

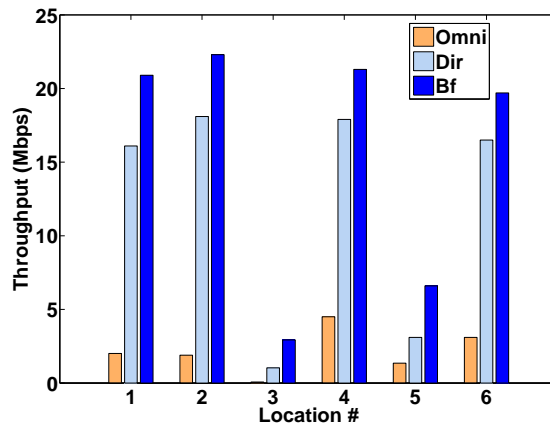


Figure 22: Throughput gain

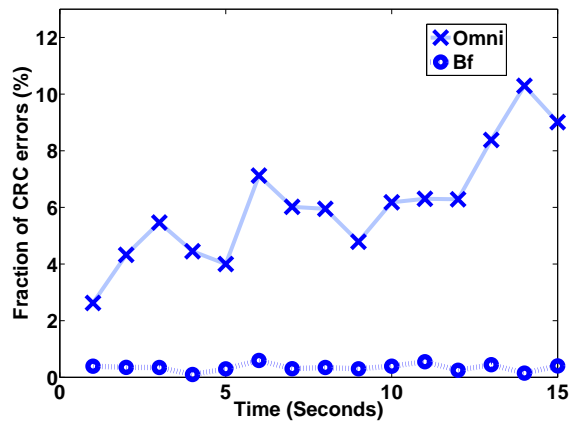


Figure 23: CRC errors

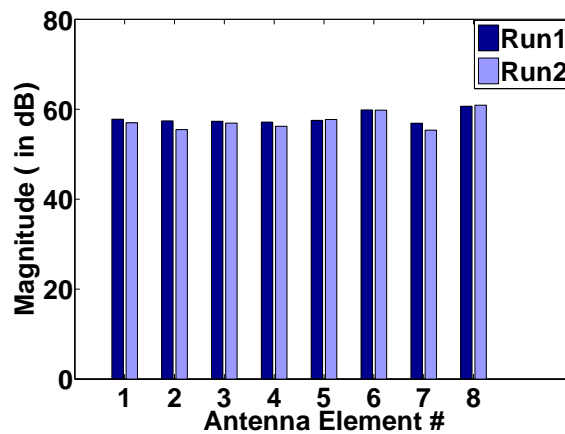


Figure 24: Channel gain magnitude

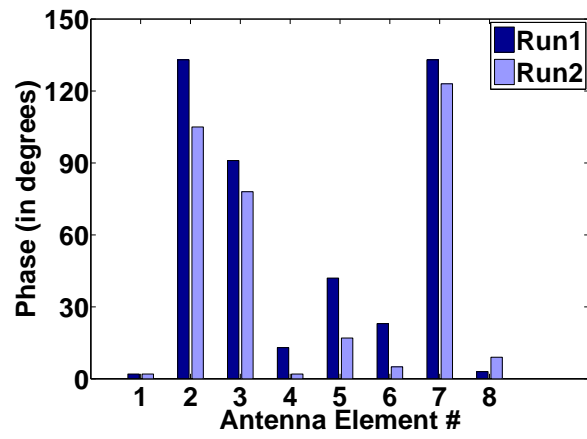


Figure 25: Channel gain phase

## CHAPTER IV

# SYMBIOTIC CODING FOR HIGH DENSITY WIRELESS LANs

### 4.1 *Overview*

Co-channel links in a Wireless LAN are separated across orthogonal time slots to avoid interference. With increasing density of links, time-sharing the channel leads to severe capacity problems. In this chapter, we identify a specific class of interference scenarios called *asymmetric interference scenarios* where the nature of interference is different at the receivers of the concurrent signals. We show that, with appropriate handling, asymmetric interference allows each receiver to decode its intended reception successfully. We represent the signal combination at the receiver as a function  $f_c$  and propose a solution called Symbiotic Coding (SC) such that  $f_c(E_1(d_1), E_2(d_2))$  is equal to  $E_1(d_1)$ , where  $d_1$  and  $d_2$  are the intended and interfering data symbol sequences and  $E_1$  is the encoder at sender 1 and  $E_2$  at sender 2 respectively. SC thus enables successful simultaneous co-channel transmissions even if they result in a collision. The performance of SC scales with the number of interfering links achieving improvements of 33% to 167% over time sharing with two to four interfering links. We address fundamental challenges in realizing SC including synchronization, coding algorithms, extensions to different modulations. We also implement SC on software defined radios and demonstrate its practical achievability.

### 4.2 *Background*

A wireless signal is typically represented as a stream of complex numbers which represents its values as a function of time [6]. To transmit a packet, a transmitter

first maps the bits into complex symbols. This process is called modulation. As an instance, in the Amplitude Shift Keying (ASK) modulation, a “0” bit is mapped to  $0 + j0$  whereas a “1” bit is mapped to  $1 + j0$ , whereas for Binary Phase Shift Keying (BPSK), a “1” bit is mapped to  $e^{j0} = 1 + j0$  and a “0” bit is mapped to  $e^{j\pi} = -1 + j0$ . The  $n^{\text{th}}$  received symbol  $\mathbf{y}[n]$  is related to the transmitted symbol  $\mathbf{x}[n]$  as:

$$\mathbf{y}[n] = \mathbf{H}\mathbf{x}[n] + w[n] \quad (4)$$

where  $\mathbf{H} = he^{j\gamma}$  is also a complex number whose magnitude  $h$  and phase  $\gamma$  are the attenuation and phase shift introduced by the channel respectively.  $\mathbf{w}[n]$  represents random complex noise.<sup>1</sup> The receiver uses  $\mathbf{y}[n]$  to estimate  $\mathbf{x}[n]$  and then maps it to the bit value (i.e., “0” or “1”). This process is called demodulation. The symbol  $\mathbf{y}[n]$  is also known as the ‘soft’ value that is used to decide whether the bit is a “0” or “1”. For instance, in ASK, the receiver checks if its estimate of  $\mathbf{x}[n]$  is greater than a threshold of 0.5 to decide a “1”.

When two senders A and B transmit their signals  $\mathbf{x}_A[n]$  and  $\mathbf{x}_B[n]$  concurrently, their signals add up in the channel and the received signal in this case can be expressed as :

$$\mathbf{y}[n] = \mathbf{H}_A\mathbf{x}_A[n] + \mathbf{H}_B\mathbf{x}_B[n] + \mathbf{w}[n] \quad (5)$$

Thus, the intended symbol is corrupted by the interfering symbol and prevents successful decoding. In practice, there are additional issues that complicate the process of estimating  $\mathbf{x}[n]$  such as frequency offsets, sampling offsets, inter-symbol interference and so on. Any practical decoder, has additional mechanisms to deal with these impairments. Every wireless radio contains oscillators that produce the clock and carrier signals. Since no two oscillators can be manufactured to produce the exact same frequency, there is always a frequency difference  $\delta f$  and a phase offset  $\delta\phi$  between the

---

<sup>1</sup>This models quasi-static flat fading channels.

transmitter and receiver. The received symbol is affected as follows:

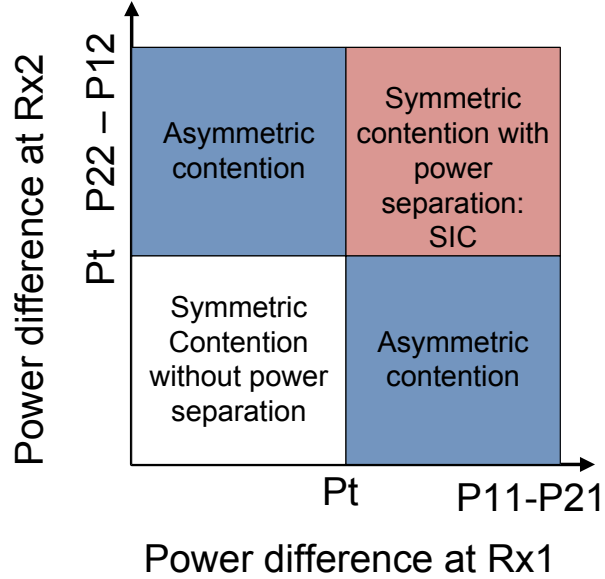
$$\mathbf{y}[n] = \mathbf{H}\mathbf{x}[n]e^{j2\pi\delta f T n + \delta\phi} + w[n] \quad (6)$$

With concurrent transmitters A and B, there are two frequency offsets  $\delta f_a$  and  $\delta f_B$  that must be estimated and corrected unless the clocks on the transmitters are perfectly synchronized.

### 4.3 *Motivation*

Wireless Local Area Networks provide tetherless connectivity and enable user mobility by using an unguided communication medium - air. However, the use of an unguided medium causes interference among co-channel signal transmissions when they arrive simultaneously at a receiver. Interference typically renders the intended signal non-decodable and hence lowers the performance of the communication network. Several medium access techniques exist to assign concurrent users to orthogonal time slots (e.g. Bit-Map protocol, Carrier Sense Multiple Access, TDMA [61]), or to orthogonal frequencies (e.g. channels 1, 6, 11 in IEEE 802.11g), or to orthogonal codes (e.g. CDMA). Given a certain spectrum, however, the performance obtained by an individual user degrades significantly with the number of co-channel users because of shared use of communication resources. The increasing user density of deployed wireless networks [21] and explosive increase of data traffic volumes over WiFi devices is hence problematic, and techniques that fundamentally enable concurrency of co-channel links are desirable.

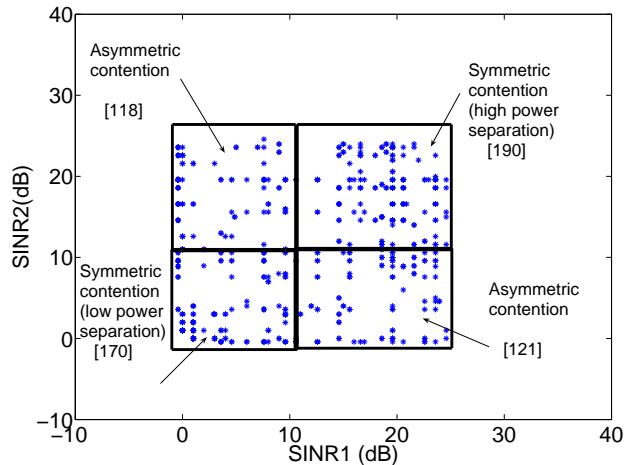
In this context, several approaches have tackled co-channel link concurrency in Wireless LANs (WLANs) recently. Such approaches rely on power separation among contending transmissions to extract interfering packets (e.g. SIC [48]), or leverage retransmissions (e.g. ZigZag [49]), or exploit the spatial separation of multiple antennas (e.g. DIRC [63], IAC [50], SAM [54]). All of the aforementioned approaches provide performance benefits provided some network conditions are satisfied. In the



**Figure 26:** Operating regions of two contending links

universal set of possible network scenarios, the approaches address distinct subsets of scenarios. In this dissertation, we consider one subset of scenarios where considerable power separation does not exist and multiple antenna elements are not available. We first show that such scenarios constitute a significant portion of real-life network scenarios, and then present a solution to enable concurrency of co-channel links under those conditions.

We now consider a network of two interfering links and specifically the power difference between interfering transmissions at each receiver. The operating region of the network can be classified into four regions as illustrated in Figure 26 depending on whether the power difference crosses a threshold at each receiver. We identify a class of scenarios in WLANs called *asymmetric contention* scenarios, where the *interference power ratios at the receivers are different*. i.e., receptions are separated by a large power difference at one receiver but not at the other receiver. We quantify the occurrence of such asymmetric interference scenarios by collecting signal strength traces from 120 locations in an enterprise WLAN consisting of approximately 120 802.11g Access Points (APs). We select only pairs of co-channel links that contend



**Figure 27:** Measured scenarios in enterprise WLAN: Symmetric contention with high power separation: 190, asymmetric contention scenarios: 239

with each other (i.e., if joint operation causes a Bit Error Rate  $> 10^{-5}$  at any receiver). We plot the resulting Signal to Interference and Noise Ratio (SINR) at the two clients of each of the above link pairs in Figure 27. The figure shows that around 190 scenarios are characterized by symmetric contention with sufficient signal power separation greater than 10 dB, whereas 239 scenarios involve asymmetric contention and around 170 scenarios involve symmetric contention with signal power separation less than 10 dB. This study, while brief, sheds light on a couple of insights: approaches such as SIC [48] and ZigZag[49] do have relevance in a significant portion of network scenarios; but at the same time there exist an equally significant set of scenarios where other solutions are necessitated. Thus, in this research we ask the following question: *Can multiple simultaneous co-channel transmissions be enabled to occur in spite of them causing (asymmetric) collisions and thereby increase the capacity performance of a wireless data network?*



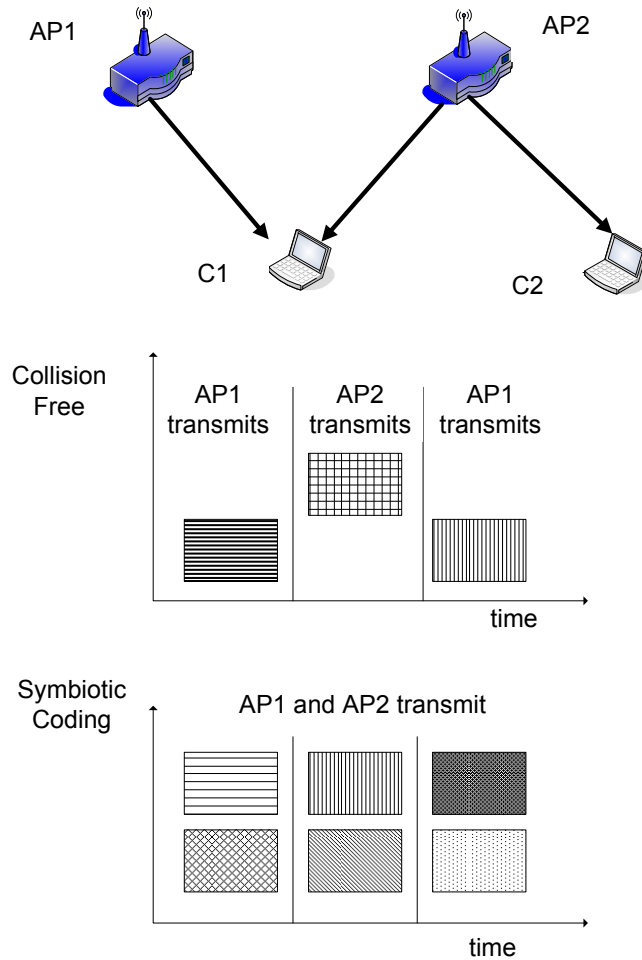


Figure 28: Illustrative example

## 4.4 Symbiotic Coding

### 4.4.1 Concept and illustration

When multiple senders transmit concurrently, the signals naturally combine in the channel after incurring channel impairments such as fading and attenuation. This signal superposition when translated to the bit level leads to the property that the decoded bit is a function of the transmitted bits depending on the modulation. We model the combination of symbols as a function called the *collision function*  $f_c$ . By characterizing this function and coding the transmitted symbols appropriately, concurrent links can be made to operate simultaneously.

Consider the network topology shown in Figure 28 where the access points AP1

**Table 5:** Success of transmissions

AP1	AP2	C1	C2	Successful ?
0	0	0	0	Yes
0	1	1	1	No
1	0	1	0	Yes
1	1	1	1	Yes

and AP2 operate on the same channel and two clients  $C1$  and  $C2$  associated to  $AP1$  and  $AP2$  respectively. When  $AP1$  and  $AP2$  both transmit simultaneously to  $C1$  and  $C2$ , the two transmissions collide at  $C1$ , but  $C2$  receives a clear signal from  $AP2$ . Considering Amplitude Shift Keying (ASK) Modulation a ‘1’ bit is represented by a high signal amplitude and a ‘0’ bit is represented by sending a low amplitude signal. Conventional collision free scheduling would require the transmissions for  $C1$  and  $C2$  to be separated in time, since  $AP2$ ’s transmission would cause a collision at  $C1$  rendering it unable to decode the packet sent by  $AP1$ . More specifically, the resulting bit decoded at  $C1$  for each of the four combination of bits transmitted from  $AP1$  and  $AP2$  is presented in Table 5. Clearly  $C1$  does not receive the intended bit from  $AP1$  always. But interestingly, it can be observed that except when  $AP1$  transmits a ‘0’ and  $AP2$  transmits a ‘1’, the receiver  $C1$  receives the correct bit (transmitted by its AP) even despite the collision. Overall, the bit error rate at  $C1$  is 0.25.

By analyzing the functional dependence between the transmitted and received bits, the collision function  $f_c$  at  $C1$  is a binary ‘OR’ function of the bits transmitted from  $AP1$  and  $AP2$ .

**Table 6:** Coding table at AP1

C1/C2	00	01	10	11
00	011	011	011	100
01	101	101	010	101
10	110	001	110	110
11	111	111	111	111

**Symbiotic coding:** In the above example, the ‘01’ bit combination (‘0’ from

**Table 7:** Coding table at AP2

C2	AP2
00	000
01	001
10	010
11	100

AP1 and ‘1’ from AP2) is the harmful combination, where the receiver C1 does not receive the intended information. Hence, *if this combination were to be avoided by appropriately coding the data bit sequences, simultaneous information transfer to both C1 and C2 is achievable.* Consider the following coding strategy. Instead of transmitting the data packets destined for clients C1 and C2 as-is, AP1 and AP2 transmit coded versions of the packet according to Tables 6 and 7 respectively. Thus every two bits of information in  $d_1$  and  $d_2$  are appropriately mapped to a three bit codeword.

When the channel executes the “OR” operation on the coded bits, all combinations of codewords are still successfully decoded at C1 (and trivially at C2). Hence, by avoiding the combination of bits that cause a failure due to collision, this approach allows the three-bit codewords to be transmitted concurrently from AP1 and AP2 conveying two data bits each for C1 and C2. Thus, this scheme provides a  $\frac{4}{3}$  i.e 1.33x improvement when compared to a collision free scheduler. We call this approach *Symbiotic Coding*.

#### 4.4.2 Definition

Generically, symbiotic coding refers to the use of an appropriate coding function  $e$  and decoding function  $g$  such that  $g(f_c(e(d_1), e(d_2))) = g(e(d_1))$ . We refer to the property of  $e(d_1)$  not being affected by a collision with  $e(d_2)$  as the *dominance* of the former over the latter and the codewords as ‘symbiotic’.

For  $N$  AP transmissions  $d_1, d_2, \dots, d_N$  interfering at a client  $j$ , the coding condition

can be given as,

$$g(f_c(e(d_1), e(d_2) \dots e(d_i) \dots e(d_N))) = g(e(d_j)) \quad (7)$$

where  $f_c$  is the collision function (i.e. binary addition operator for ASK or complex addition operator for other modulations),  $d_j$  is the data from the associated AP for client  $c_j$ , while  $e(d_j)$  is the encoded symbol and  $g$  is the decoding function. Thus, the coding problem is to design  $e$  and  $g$  such that the intended symbols are conveyed at the receiver  $j$ . In the previous example, the encoding and decoding functions  $e$  and  $g$  were presented in the form of Table 6 and Table 7.

While signal addition is a fundamental property of wireless transmission, the coding function depends on the modulation used, the topology considered, link Signal to Noise Ratio. We also note here that  $d_i$  and  $d_j$  need not be from the same modulation set (i.e. contending links can be operating at different rates) as we describe later.

#### 4.4.3 Proof of concept

We first experimentally verify that the above coding approach works in practice using software radios in a real-life setting. The USRP2 [45] hardware and default GNURadio [46] software modules for packet transmission are used by implementing non-coherent ASK modulator and demodulators. Two USRP2s act as the two APs and are connected by a cable from Ettus (called MIMO cable) which carries the clock and reset signals between them. This ensures that the clocks and the carrier frequencies on the two USRP2s are synchronized to within 10s of nanoseconds. The position of C1 and C2 are varied while maintaining the topology in Figure 28. The packet success rate at C1 averaged over 100 packets was observed to be around 0.5% without coding. But with the described coding scheme packet success improved to 98.1%. Clearly, symbiotic coding ensures that the Bit Error rate remains below the threshold of acceptance ( $10^{-3}$ ) thereby confirming its feasibility in real wireless channels.

## 4.5 Design Considerations

### 4.5.1 Channel impairments

When two senders AP1 and AP2 transmit their signals  $\mathbf{x}_1$  and  $\mathbf{x}_2$  concurrently, their signals add up in the channel after undergoing propagation losses and noise addition  $\mathbf{w}$ . The received signal at a receiver C1 can be expressed as [61] :

$$\mathbf{y}_1 = \mathbf{H}_{11}\mathbf{x}_1 + \mathbf{H}_{21}\mathbf{x}_2 + \mathbf{w} \quad (8)$$

where  $\mathbf{y}_1 = \mathbf{H}_{11}\mathbf{x}_1$  and  $\mathbf{y}_2 = \mathbf{H}_{21}\mathbf{x}_2$  represent the symbols transmitted by AP1 and AP2 after traversing the complex channels  $\mathbf{H}_{11}$  and  $\mathbf{H}_{21}$  from AP1 and AP2 to C1.

Similarly, the received signal at receiver C2 is given by:

$$\mathbf{y}_2 = \mathbf{H}_{12}\mathbf{x}_1 + \mathbf{H}_{22}\mathbf{x}_2 + \mathbf{w} \quad (9)$$

where the channels from AP1 and AP2 to C2 are given as  $\mathbf{H}_{12}$  and  $\mathbf{H}_{22}$  respectively.

#### 4.5.1.1 Channel Magnitude differences:

Since we consider an asymmetric contention scenario, the expected power from AP1 at C2 is smaller than that from AP2. i.e.  $E(|\mathbf{H}_{22}|^2) \gg E(|\mathbf{H}_{12}|^2)$ . Hence,  $\mathbf{y}_2$  can be decoded using known techniques (e.g. conventional detector or SIC [48]) depending on the separation  $E(|\mathbf{H}_{22}|^2) - E(|\mathbf{H}_{12}|^2)$  to yield  $\mathbf{x}_2$ . Thus, C2 can decode its intended packet successfully.

The power received from AP1 and AP2 at C1 are denoted as  $P_1 = 20 * \log(|\mathbf{H}_{11}|)$ ,  $P_2 = 20 * \log(|\mathbf{H}_{21}|)$  similar. If  $P_1$  and  $P_2$  are widely separated, they can be removed using SIC [48]. However, for our scenario of interest described in Figure 26, the powers are similar  $P_1 = P_2$  (and we cannot exploit conventional techniques such as SIC). Thus, each of  $\mathbf{H}_{11}$  and  $\mathbf{H}_{21}$  are complex channel gains with similar amplitude  $|\mathbf{H}_{11}| = |\mathbf{H}_{21}| = C_1$ . Interestingly, we note later that the channel gains need not be exactly same in magnitude and the proposed scheme works even when the signal magnitudes

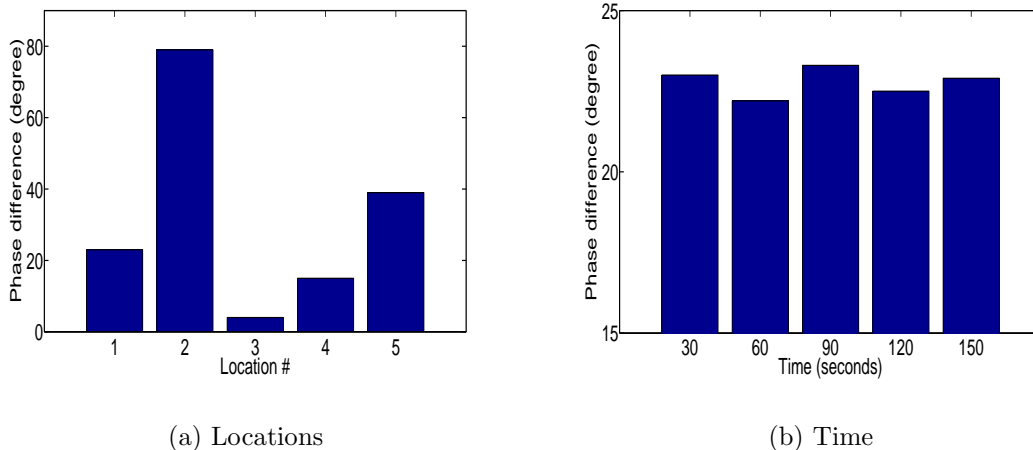
are different (by upto 10 dB) as illustrated by the results in Figure 40. Without loss of generality, we represent the channel gains in terms of the phase difference between the channel gains  $\theta_1$  as  $C_1$  and  $C_1 * e^{-j\theta_1}$ . Hence,  $\mathbf{y}_1 = C_1(\mathbf{x}_1 + \mathbf{x}_2.e^{-j\theta_1})$ . The only factor remaining to be handled is  $\theta_1$ .  $\theta_1$  can be estimated at the receiver and fed-back to the APs.

#### 4.5.1.2 Channel Phase differences

We first note that phase synchronization of signals from AP1 and AP2 is not needed but only the estimation of the phase difference perceived at the clients. This is a key difference of SC from several coordinated beamforming approaches which require the symbols to be synchronized in phase at the transmitters.

**Estimation methodology:** The phase difference of the transmissions from AP1 and AP2 must be known at the receivers to bootstrap the symbiotic coding approach. We first note that current 802.11n systems already estimate the channel phase difference between multiple transmit antennas and receive antennas. The procedure involves transmitting time-shifted versions of a common training sequence on each of the antennas and measuring the time shift between the correlation peaks at the receiver. The same procedure can be extended to the antennas of the APs to determine the channel phase difference accurately at the client.

**Practical results:** We perform baseline experiments to characterize the phase difference across clients in indoor WLAN settings. We use two software radio APs transmitting a constant tone of frequency 2.412 GHz to a software radio client. The power received at the client when AP1 and AP2 transmit in isolation is measured as  $P_1$  and  $P_2$  respectively. Next the power received at the client when both APs transmit together is measured as  $P_{12}$ . By applying Equation 8 and simplifying, we observe that  $P_{12}$  depends on the channel phase difference from AP1 and AP2 and is



**Figure 29:** The channel phase differences can be estimated accurately and retained for use over several minutes

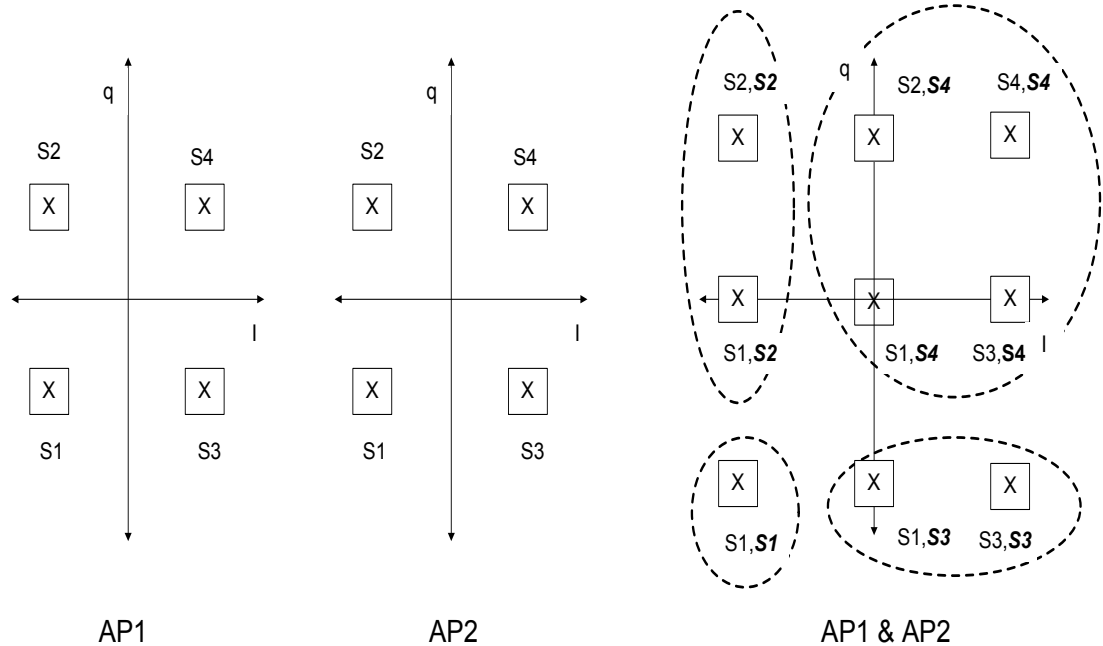
given by Equation 10.

$$P_{12} = P_1 + P_2 + 2\sqrt{P_1 \cdot P_2} \cdot \cos(\theta_{12}) \quad (10)$$

where  $\theta_{12}$  is the *channel phase difference* between the AP1–C1 and AP2–C1 channels. By inverting this relation, we obtain the channel phase difference.

Figure 29 a) plots the channel phase difference measured at different locations of C1. While Figure 29 b) plots the channel phase difference across time. The figures illustrate that the channel phase difference can be estimated accurately and also be used for several minutes without degradation in performance. Our experiments indicate that a resolution of eight bits is sufficient for the phase difference and that the estimates can be retained for several minutes, thereby keeping the overhead of the scheme very low.

After estimation, the channel phase effect can be pre-compensated at the transmitters by introducing phase delays or can be compensated at the receivers after passing through the channel. By extending the basic example illustrated before, the coding procedure can be adapted to the complex constellation formed by  $\mathbf{x}_1 + \mathbf{x}_2 \cdot e^{-j\theta_1}$ . It can be proved that capacity improvements are achieved by coding irrespective of



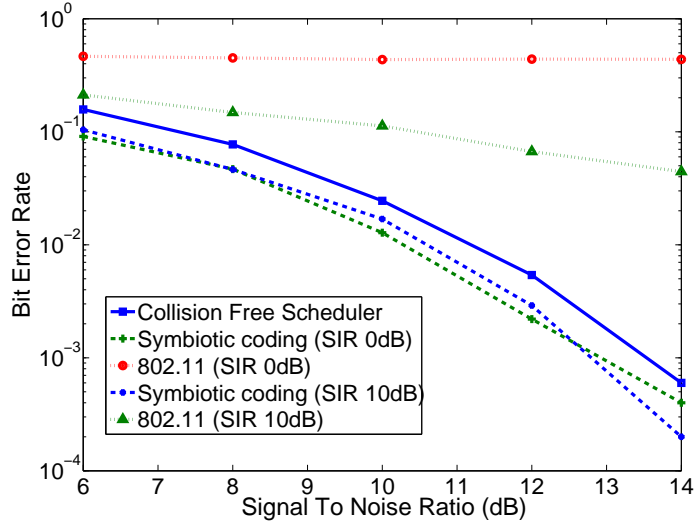
**Figure 30:** Same modulation at AP1 and AP2

the value of  $\theta$ . Hence, in the rest of this section, we describe the solution components with  $\theta_1 = 0$ . Thus, *channel conditions in asymmetric contention scenarios enable desired combination of symbols to be received successfully at the receivers.*

#### 4.5.2 Modulations other than ASK

**Applicability to modulations:** While we presented the basic idea using Amplitude Shift Keying as the modulation, Symbiotic Coding works with any modulation in principle. Symbiotic Coding leverages the fact that when senders transmit concurrently on the same frequency, some symbol combinations are resolvable and some that are not and appropriately codes for them. We note here that this model allows coding for all current modulation techniques including amplitude modulations like ASK, phase modulations like BPSK. Frequency modulations like FSK, OFDM would involve coding the transmitted symbols to be transmitted on the same sub-carriers together. The key requirements when applying to any modulation are: (1) coding must be adapted to prevent *error inducing* symbol combinations from occurring and (2) the demodulation should be adapted to leverage concurrent senders. To remain





**Figure 31:** Symbiotic Coding equal modulations: 4-QAM illustration and simulation

compatible with existing modulation mechanisms, we describe how symbiotic coding can be achieved using existing modulations with two key algorithms: (1) bit to symbol mapping at the transmitter and (2) the demodulation strategy at the receiver. We discuss the principles using Figure 28 as the illustrative scenario, where AP1 and AP2 transmit simultaneously to C1 and C2.

**Illustrative example:** Assume that both AP1 and AP2 use Quadrature Phase Shift Keying (QPSK) as the underlying modulation. QPSK (also called 4-QAM) is popularly used in the 802.11 standards (abgn). Depending on the bit pair to be encoded i.e. 00,01,10,11, the transmitted symbols are chosen from a set  $S = S_1, S_2, S_3, S_4$  where  $S_1 = -1 - j, S_2 = -1 + j, S_3 = 1 - j, S_4 = 1 + j$  for bits 00,01,10,11 respectively. The received symbols are shown pictorially using the constellation diagram in Figure 30 for both the single transmission case and for the concurrent transmission from AP1 and AP2. While there are 16 possible combinations, only nine of them are valid combinations which result in uniquely decodable (non overlapping) pairs. It can be observed that the concurrent symbol pairs that are allowed are given by the following nine pairs  $(S_1, S_1), (S_1, S_2), (S_1, S_3), (S_2, S_2), (S_3, S_3), (S_1, S_4), (S_2, S_4), (S_3, S_4), (S_4, S_4)$ . The demodulation regions are represented by dotted lines in the Figure 30.

The constellation diagram represents nine pairs with the property that (i) each of these pairs results in a unique constellation point at the receiver (ii) the distance between adjacent constellation points is not reduced compared to the original constellation. The minimum distance between valid constellation points determines the error performance under noise [6] and the larger this distance the better the decodability. Thus, the above nine pairs provide a larger number of states without reducing the error performance compared to a single transmission. Consequently, they can be used to improve the capacity of concurrent links.

***Bit-to-symbol mapping:*** The bit to symbol mapping is performed in the above manner, where adjacent constellation points are separated by only “1 bit-distance”. i.e. the symbol  $S_1$  and its adjacent symbols  $S_2, S_3$  represent bits 00 and 01, 10 which are only one bit different from 00. This is typically called a gray symbol mapping [6]. We recall that the coding scheme described in Table 6 and Table 7 has the property that the codewords from AP1 are unaffected by the codewords transmitted from AP2 (symbiotic codewords). When this mapping is used on bit streams encoded using the coding table described in Table 6 and 7, the resulting symbol streams are also symbiotic i.e. they do not have any harmful combinations. Thus, when data bits intended for C1 and C2 are encoded using symbiotic binary tables, they lead to two compatible bit streams at AP1 and AP2. When the resulting coded bit streams are mapped two bits at a time, using the gray mapping described above, the resulting 4-QAM symbol streams are also naturally compatible because the bit-to-symbol mapping assigns points separated by exactly 1 bit distance.

*Lemma 1:* If two bit streams are symbiotic, for any modulation, it is always possible to find a bit-to-symbol mapping such that their corresponding symbol streams are also symbiotic.

The proof follows from the construction presented previously.

Thus, *the basic symbiotic bit-level coding scheme naturally leads to a solution for*

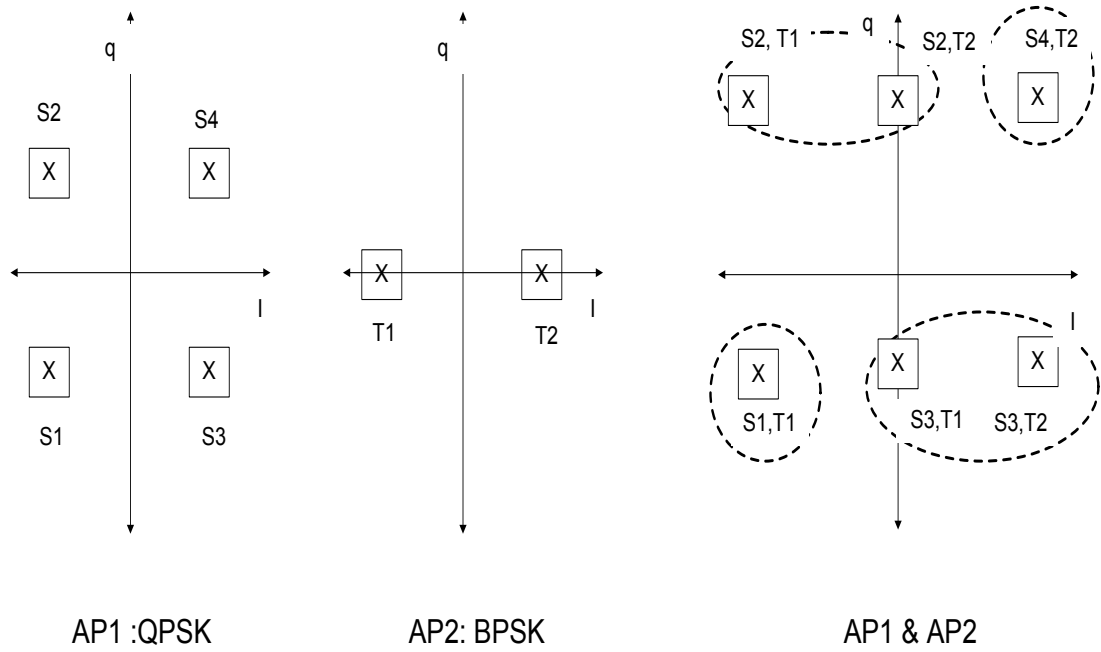
*higher modulations when appropriate symbol mapping and demodulation are used.*

**Benefits:** We evaluate the Bit Error Rate performance of the 4-QAM symbiotic coding scheme for the same two AP two client scenario using simulations based on an additive white Gaussian noise (AWGN) channel [6]. We present the evaluation in indoor fading channels in Section 4.7. Figure 31 plots the BER at C1 as a function of  $SNR_a$ , the SNR from AP1 to C1 for 4-QAM modulation. The figure shows that, Symbiotic Coding allows concurrent transmissions while achieving an error performance that is close to a collision free scheduler.

For a given pair of modulations, we determine the combined for each possible symbol in the modulation sets of AP1 and AP2. We then calculate the number of symbol pairs from AP1 and AP2 such that (1) they are uniquely resolvable symbols (i.e. given a symbol at C1, we know the corresponding transmitted symbols from AP1 and AP2 uniquely) (2) the minimum distance between the resulting combined symbols in the constellation is greater than or equal to the distance of the individual symbol constellations from AP1 and AP2. A summary of the rate improvement that can be achieved with the four popular modulations used in the IEEE 802.11 standard i.e. BPSK, QPSK, 16-QAM, 64-QAM is presented in the Table 8. We determine the number of uniquely decodable constellation points for each pair of modulations such that the minimum distance between constellation points is greater than or equal to that of the lower modulation in the pair considered. Thus, we note that unlike existing coordinated pre-coding approaches, symbiotic coding does not require coordination across clients and intelligently exploits symbol combinations to improve performance.

### 4.5.3 Heterogeneous links

We recall that Symbiotic Coding uses the fundamental signal combining properties of transmissions from multiple APs and thus does not require that the combining symbols be from the same modulation. When different modulations are used at AP1



**Figure 32:** Different modulations at AP1 and AP2

**Table 8:** Gains for different modulations

AP1,AP2	Time Sharing	Symbiotic coding	Improvement %
BPSK,BPSK	1.00	1.59	59
QPSK,BPSK	1.50	2.59	72
QPSK,QPSK	2.00	3.17	59
16-QAM, BPSK	2.50	4.32	73
16-QAM, QPSK	3.00	4.64	55
16-QAM, 16-QAM	4.00	5.61	40
64-QAM, BPSK	3.50	6.17	76
64-QAM, QPSK	4.00	6.34	59
64-QAM, 16-QAM	5.00	6.92	38
64-QAM, 64-QAM	6.00	7.81	30

and AP2, the superposed constellation depends on the pair of modulations used and would follow an appropriate demodulation strategy. We note that information about the pair of modulations used can be easily obtained using a common preamble before the payload. The common preamble would be uncoded and hence used by both clients to infer the modulations used. We illustrate this for the case of AP1 using QPSK modulation and AP2 using BPSK modulation in Figure 32. We also plot the superposed constellation at the receiver C1 when both APs transmit concurrently in the same figure. (We note here that the symbols for different modulations i.e. BPSK and QPSK are shown to be have energy at the receiver, since a fixed Bit error rate is desired. In contrast, if a fixed power constraint is used, the energy of a QPSK symbol would be scaled by 2. However, this scaling does not affect the approach itself nor its feasibility.) The dotted lines indicate the set of symbols which are demodulated into a single symbol. Thus, we observe that the pairs  $(S_1, T_1)$ ,  $(S_3, T_2)$ ,  $(S_3, T_1)$ ,  $(S_2, T_1)$ ,  $(S_2, T_2)$ ,  $(S_4, T_2)$  are allowed pairs. While time sharing across the two links would cause 1.5 bits/slot on the average, Symbiotic Coding leads to  $\log_2 6 = 2.58 \text{bits/slot}$ . Thus, significant capacity improvements are achieved even with heterogeneous modulations used by the contending links. We tabulate the rate improvements obtained using each pair of modulation in the Table 8. It is clear that *Symbiotic Coding provides capacity improvements from 30% to 76% for popular modulations across several heterogeneous two link scenarios.*

#### 4.5.4 Synchronizing transmissions

Symbiotic coding requires that the symbols received at the receiver C1 be synchronized. The time offset between the symbols from AP1 and AP2 measured at C1 depends on the difference between the transmission start times at AP1 and AP2, and the propagation delay differences from AP1 and AP2 to C1. In practice, since indoor ranges are limited and C1 must be located within the range of AP1 and AP2, the

maximum propagation delay difference can be shown to be less than a few tens of nanoseconds. Thus, if the transmissions are synchronized within tens of nanoseconds, the overall time difference can be ensured to be less than 100 nanoseconds in the worst case,. Since the Wifi technologies 802.11agn use a  $4\mu s$  symbol duration, the worst case offset is  $\frac{1}{40}$  of the symbol period, which is negligibly small. We describe two approaches that achieve transmissions synchronized to within tens of nanoseconds in practice, thereby making synchronization a non-issue.

**1. *Wireless triggering:*** When a short trigger packet is transmitted to both AP1 and AP2, they can use this as a trigger to start their transmissions in a synchronized manner. This approach is already successfully used in current 802.11 devices where an ACK packet is transmitted within  $10\mu s$  of a DATA packet transmission. This method was implemented in the context of two Wifi devices to achieve less than  $10\mu s$  synchronized transmissions in [55]. More recently, researchers have used this approach to synchronize four software radio transmitters and demonstrated a delay difference of 60 ns at the receiver [47]. Similarly, other researchers have also demonstrated 20ns synchronization using high performance software radios[76]. In practical WLANs, the control trigger can be transmitted from another AP in a high density deployment of APs or from a client which is in the range of both AP1 and AP2.

**2. *Wired clock sharing:*** An alternate approach is to synchronize the clocks of AP1 and AP2 by leveraging the wired ethernet backbone through which they are connected. This can be accomplished by the controller transmitting a short packet periodically. This type of approach was presented in [59] to achieve synchronization within few  $\mu s$ . This can also be realized by Network Time Protocol solutions with a precise time server connected to the ethernet backbone of the WLAN. We also note that it is sufficient if the adjacent APs in a large WLAN are synchronized and we do not need network wide synchronization. In practical WLANs, the synchronization

preamble of ethernet packets is used to determine the clock for decoding the ethernet packet. The same preamble can also be used to trigger transmissions on the wireless interface to achieve synchronized transmissions. We have realized this approach in a practical software radio testbed of USRP2s connected by a cable [45] and achieved transmissions synchronized to within 10 ns. Our prototype implementation of Symbiotic Coding using only common off-the-shelf hardware serves as a credible proof of concept for the feasibility of achieving synchronized transmissions needed for symbiotic coding.

#### 4.5.5 Uplink communication

While the basic coding scheme was designed for synchronized APs as transmitters (downlink), a modified version can be used to achieve symbiotic combining gains although with a reduced efficiency by exploiting joint decoding at the APs. Symbiotic Coding can also be applied to the uplink of the scenario (Figure 28) where C1 and C2 transmit to AP1 and AP2 respectively but cause collisions at AP1. In this case, the two main considerations are:

1. **Uplink synchronization:** The absence of a wired backbone between C1 and C2, requires the reception of a control or trigger packet on the wireless link from AP2 to trigger C1 and C2. Related work [47] has already demonstrated the feasibility of achieving synchronization to within 10s of nanoseconds using this approach. Thus AP2 transmits a control packet informing C1 and C2 to transmit after a preset time from the reception of the packet, thereby synchronizing their transmissions.

2. **Modified coding and joint decoding:** The second aspect of uplink operation is coding. Observe that C1 and C2 cannot jointly encode their information without wasting a time slot for wireless information exchange. Hence the strategy is for C1 and C2 to code independently and share the receptions of AP1 and AP2 and

decode all the transmitted bits together. Observe from Figure 28 that C1’s transmission is received successfully at AP1 whereas at AP2, packets of C1 and C2 collide. AP2 can use the correct bits of C1 from AP1 to decode the collided bits. However, without coding some of the bits are not be resolvable. As an example consider that the  $n^{th}$  collided bit at AP2 is a ‘1’ and the  $n^{th}$  bit at AP1 is also a ‘1’ i.e C1 transmitted a ‘1’. In this case, it is impossible to say using AP2’s received bit whether C2 transmitted a ‘1’ or ‘0’, because both  $1 + 0 = 1$  and  $1 + 1 = 1$ . Hence, the transmissions of C1 and C2 must be independently coded.

For the coordinated receive case, since one of the transmissions is received without any interference, the codewords must be designed such that the interfered codeword maps uniquely to each data bit transmitted as shown in Table 9.

**Table 9:** Uplink coding table

Data	C1-code	C2-code
00	000	010
01	001	100
10	010	001
11	100	111

**Table 10:** Decoding table at AP2 using C1 and C2

RX2/C1	00	01	10	11
001	10	10	-	-
010	00	-	00	-
011	-	00	10	-
100	01	-	-	01
101	-	01	-	10
110	-	-	01	00
111	11	11	11	11

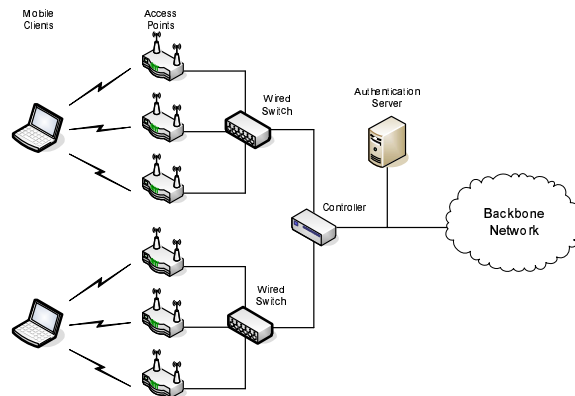
It can be observed that every possible data bit combination in Table 9 can be uniquely decoded using Table 10. In Table 10, a – indicates that such a pair of received codeword (RX2) and C1 is not possible under correct operation. Those states can be used for error detection or correction. Using this scheme C1 and C2



can convey two bits each in three bit-slots leading to a total throughput of  $\frac{4}{3} = 1.33$ . Thus, Symbiotic Coding can be applied to the upstream to yield benefits over collision free schedules.

## 4.6 Symbiotic Coded WLAN

**Model:** Given the benefits of symbiotic coding for several two link scenarios established in the previous section, we now consider how it can be applied to a large network consisting of several Access Points and clients distributed over a large geographical area. An example of such a network is an enterprise WLAN as shown in Figure 33 which consists of a controller that coordinates the actions of multiple Access Points.



**Figure 33:** Network model showing a high density of APs and a controller in an enterprise

**Solution overview:** While we presented the coding and decoding tables for the two link scenario, the key question that must be answered to enable a Symbiotic Coded WLAN is “How are the codes generated and applied for a topology consisting of more than two links?” Toward answering this question, we first note that not all topologies are amenable to coding and different topologies differ in the capacity benefits they provide. Specifically, we recall from Section 4.4.1 that the asymmetry in the interference topology enables symbiotic coding and symbiotic coding cannot

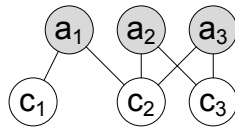
be directly applied to symmetric topologies. Thus, symmetric topologies must be decomposed into asymmetric topologies which are amenable to coding.

We model the network of APs and clients as a graph, where an edge between an AP and client represents that a transmission from an AP reaches the client with sufficient signal strength to cause interference. We use the granularity of bits for the design which can be extended to other modulations as described in 4.5.2. Throughout this section, we use the illustrative multi-link scenario of Figure 34 to explain the algorithms.

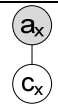
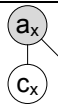
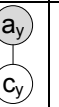


The useful topologies for any given graph are the acyclic, connected induced sub-graphs of a graph and are referred to here as ‘templates’. (Figure 35 shows all templates and their achievable capacity of the associated symbiotic code for degree three.) By designing codes for these templates, one can apply symbiotic coding to any topology by combining multiple templates and attain benefits without having to design a separate code for each topology.

Hence, we decompose the problem of symbiotic coding for a given network into two parts and solution includes

1. a code generation algorithm for a basic set of template topologies formed by the acyclic sub-graphs of the network graph (Section 4.6.1)
2. a scheduling algorithm that decides the subset of symbiotic coded topologies to activate and the time duration allotted to each of them to ensure that the network capacity is maximized subject to *max-min* fairness among clients (Section 4.6.2).



**Figure 34:** Example of input topology

Id	1	2	3	4	5
Template					
Number of Links	1	2	3	3	3
Per-link Capacity	1	0.67	0.67	0.67	0.5
Total Capacity	1	1.33	2	2	1.5

**Figure 35:** Pre-computed templates for three APs

#### 4.6.1 Code generation for templates

**Goal and heuristic:** The aim of the algorithm is to identify the codeword assignment to each data word combination for the APs in a template such that each client  $c_i$  successfully decodes its data as  $d_i = D_i(E_i(d))$ . Thus, the algorithm takes as input the connectivity graph of the topology  $G$  and produces the encoding functions  $E_i(m)$  at each AP  $a_i$ . To do this, the following key idea developed from Section 4.4.1 is used: *When the transmissions of multiple senders collides at a receiver, successful decoding can be achieved by assigning more 1's to the associated sender and 0's to the interfering sender(s)*. In other words a '1' dominates a '0' as far as coding is concerned. The algorithm is an iterative algorithm that attempts to greedily assign codewords for each data word  $d$  (i.e all possible data bit combinations of  $d_1, d_2, \dots, d_k$ ) for the given topology. To begin with, the algorithm first initializes the set of codewords for each dataword  $e(d, i)$  at each sender  $a_i$ , with all codewords of length  $W$  as possible codewords to use i.e  $|e(d, i)| = 2^W$ . Next, the following steps are performed sequentially until codewords have been assigned at each AP for all the dataword combinations or the codewords at any of the APs is exhausted.

**Step 1. AP and dataword selection:** The first step is to select the sender  $a_i$  and the dataword  $d$  for which number of available codewords  $|e(d, i)|$  is least among the senders in the topology and data pattern combinations. This step is important because a wrong order of assignment might lead to some codewords being eliminated at other APs before the assignment for all possible bit combinations is complete.

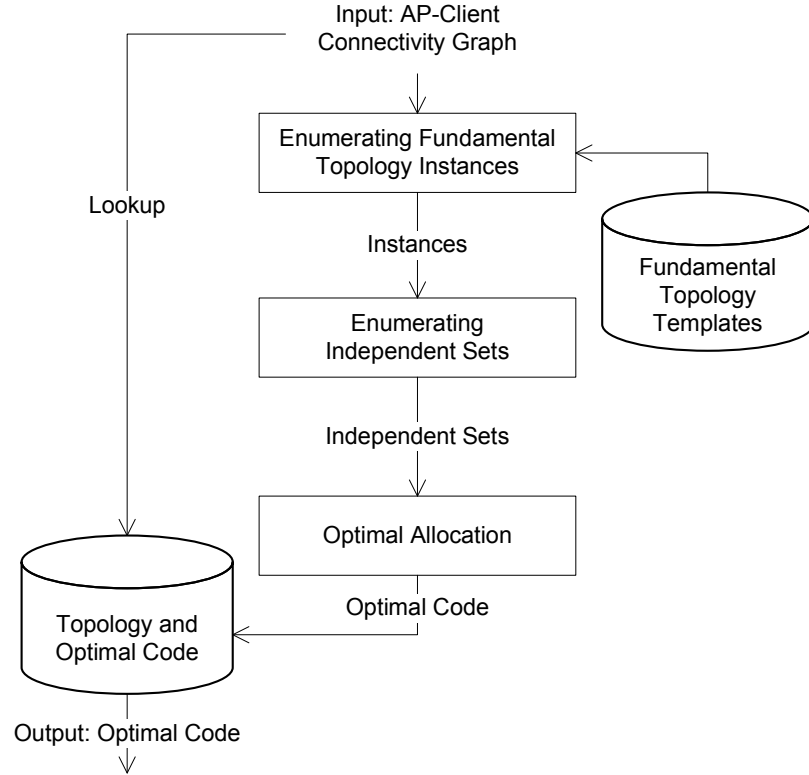
To understand this, we first note that an assignment of a codeword at an AP could eliminate one or more candidate codewords at other APs. For instance, in Figure 28 and Table 6, If AP1 transmits a '000', i.e  $e(d_1) = 000$ , then none of the codewords in  $e(d, 2)$  can satisfy Eqn. 7.

**Step 2. Codeword selection:** Once the AP is chosen based on the heuristic, the codewords containing more zeros is preferred for a dominated AP and a codeword containing more ones for a dominating AP (E.g. AP1 in Figure 28). If the assignment is not based on this heuristic, the codewords will not satisfy the symbiotic coding criterion expressed in Eqn. 7.

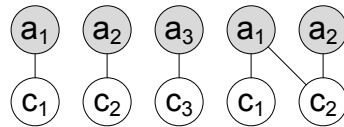
**Step 3. Update of Codeword set:** Every codeword assignment at an AP, can eliminate one or more codewords at other APs since only certain codeword pairs for two senders (or n-tuples for N APs) satisfy the condition in Eqn. 7. Hence, after assigning a codeword at an AP  $a_i$ , the unusable codewords at other APs ( $a_j \in [1, N]; j \neq i$ ) are removed from their respective codeword sets  $e(d, j)$ . For instance, if the dataword is 0000 and  $e(0000, 1) = \{000, 010, 101\}$ ,  $e(0000, 2) = \{010, 011\}$  are the corresponding codeword sets at  $a_1$  and  $a_2$ , we remove 011 from  $a_2$  since no codeword from  $a_1$  can dominate it. These steps are repeated until either the code table is obtained or there are no more unused codewords for this length.

#### 4.6.2 Scheduling

**Overview:** The goal of this algorithm is to apply the appropriate codes to be used for each scheduling epoch such that the throughput is optimized. In the context of downstream data to clients, the algorithm first obtains the packets from its stream such that there is one packet for each AP corresponding to exactly one of its associated clients. After identifying the clients to be served, the connectivity graph of the APs and the clients is used to identify the optimal schedule of codes across the APs for this slot. This is repeated for all the packets. The algorithm takes as *input* the



**Figure 36:** Flow chart of code scheduling algorithm



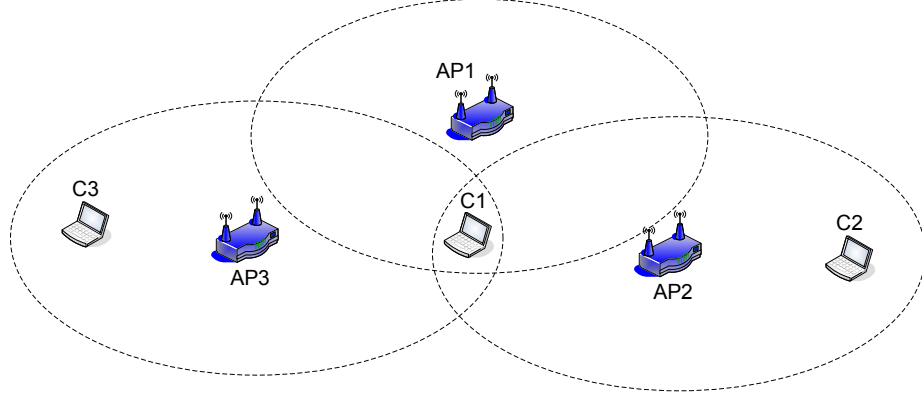
**Figure 37:** Instances in Figure 34

connectivity graph between APs and the clients under consideration for this slot and produces as *output* the code schedule for different APs that optimizes capacity. The algorithm has the following main steps, as shown in Figure 36.

**Key steps:**

**1. Identifying template instances:** Each of the templates in Figure 35 is used to generate multiple instances by replacing symbols with any permutation of AP/client index numbers. An instance is considered valid only if it is an ‘induced subgraph’ in the input topology. The generated instances are illustrated in Figure 37.

**2. Determining independent sets:** The next step is to generate the conflict



**Figure 38:** Topology with 3 APs and 3 clients

graph of instances and enumerate all independent sets. If two instances cannot operate simultaneously, i.e. any client in one instance is interfered by any AP in another, then they are connected with an edge in the conflict graph.

**3. Optimal allocation:** We formulate a linear problem to compute the optimal allocation of all independent sets to achieve max-min capacity, i.e. each client gets at least one unit of capacity.

$$\begin{aligned}
 \min \Lambda &= \sum_{S_i \in \mathcal{S}} \lambda_i \\
 \text{s.t.} \quad &\sum_{S_i \in \mathcal{S}} \lambda_i \sum_{I \in S^i, c_j \in I} F_I \geq 1, \forall c_j \in \mathcal{C}
 \end{aligned} \tag{11}$$

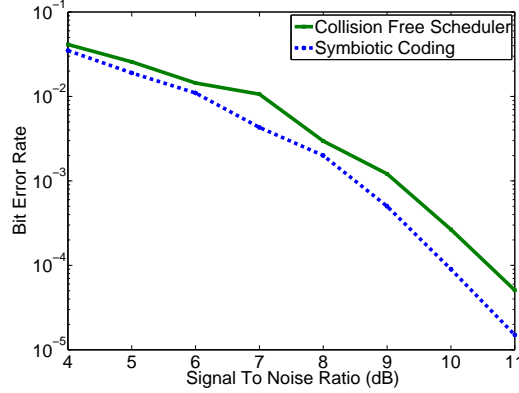
where  $\lambda_i$  is the time allocated to independent set  $S_i$ , and  $F_{I_j}$  is capacity of each client in instance  $I$ . When applied to the 3 AP scenario of Figure 38, a code rate of 2 bits/slot is achieved compared to 1.5 bits/slot with the best collision free scheduler.

## 4.7 Performance Evaluation

### 4.7.1 Testbed description

We evaluate Symbiotic Coding in a testbed of Software radios. Each node in the testbed is a laptop connected to a USRP2 GNURadio [45]. GNURadio [46] is a software defined radio where all communication operations are performed in software on the PC. At the transmitter side, the complex baseband samples are transported over

a Gigabit Ethernet connection to the USRP2 where the Digital to Analog converter produces the analog signal. The signal is then up-converted to 2.4GHz and transmitted over the wireless channel. At the receiver, the process is repeated in the reverse order. Our testbed allows 1 Mbps BPSK and 2 Mbps QPSK transmissions using a fixed bandwidth of 1 MHz. We use the default configuration parameters in GNURadio and implement packet transmitters and receivers using ASK, BPSK and QPSK modulations. **(i) Encoder and decoder** For the 2 topology implementation, the encoder takes 2 bits from each of the two streams and produces a 3 bit word. For the three topology case, each coding operation takes 2 bits from each of the 3 data streams and produces 4 bits as output. This is repeated until the maximum packet size of encoded bits is reached. The decoder does the reverse of this operation to find the dominant sequence. **(ii) The transmit trigger** is used to trigger the transmissions synchronously. The GNURadio software provides a timestamp field for each packet sent from the PC to the USRP2s so that the packets are sent out when the FPGA clock counter reaches the desired value. For our two AP experiments we connect the USRP2s with a cable (called MIMO cable, available from [45]) which ensures that the clocks of both USRP2s are perfectly synchronized to within 10ns. We use an ethernet cable based synchronization for more number of APs which achieves synchronization within few  $\mu s$ . **(iii) Enhanced Demodulators** We implement the demodulators described in Section 4.5.2 for ASK, BPSK and QPSK and perform experiments over multiple locations and times of the day for increased confidence. We compare Symbiotic Coding with CSMA and a collision free scheduler as an approximation of 802.11 since SDRs do not support timed ACK transmissions. We note that a collision free scheduler is an upper bound on the performance achievable with distributed MAC algorithms such as CSMA/CA.



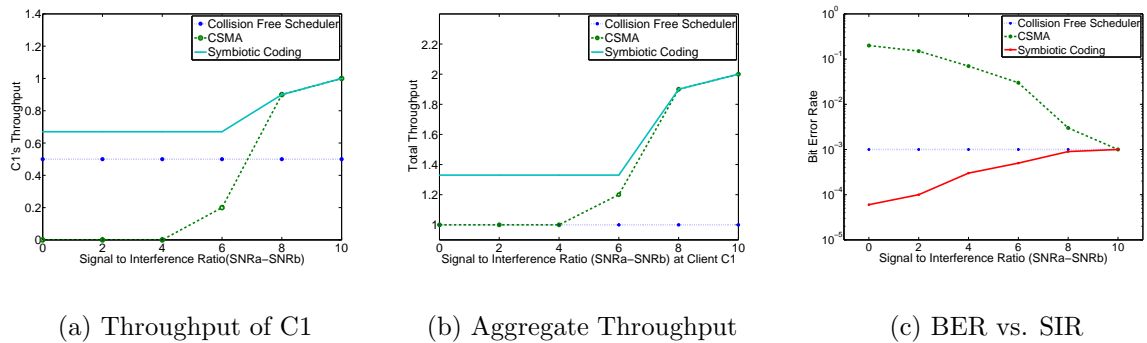
**Figure 39:** BER improvement: Symbiotic Coding outperforms time division scheduling.

**Table 11:** Average throughput across modulations

Modulation	CSMA/CA (Mbps)	Symbiotic Coding (Mbps)
BPSK	0.95 Mbps	1.30 Mbps
4-QAM	1.92 Mbps	2.60 Mbps

#### 4.7.2 How well does Symbiotic Coding work?

We first perform experiments to understand whether Symbiotic Coding leads to successful packet reception at the client C1 in the topology presented in Figure 28, where the powers from AP1 and AP2 to C1 are similar causing collisions. To do this, we observe the average Bit Error Rate (BER) with varying SNR for the case of two modulations BPSK and 4-QAM. This is a typical metric that determines the quality of a wireless receiver [61]. Figure 39 depicts the BER at client C1 versus the SNR



**Figure 40:** SNR and SIR: Symbiotic Coding converts interfering transmission from AP2 to beneficial transmission



( $SNR_a = SNR_b$ ). The plot consists of two curves, namely the performance of a collision free scheduler and the performance of Symbiotic Coding. Symbiotic Coding performs very close to a collision free scheduler within a few dB. (Similar curves are obtained for 4-QAM which we don't present due to lack of space). More importantly, Symbiotic Coding yields a BER curve which is better than the collision free scheduler. In summary,

(1) For all SNRs, Symbiotic Coding never degrades the error performance when compared to a collision free scheduler. On the contrary, it yields an improvement in BER due to the constructive combination of symbols from AP2 and AP1. The SNR required with Symbiotic Coding is only 63% of the SNR required by the collision free scheduler for a given BER of  $10^{-3}$ .

(2) The median throughput improves from 0.95 Mbps to 1.3 Mbps for BPSK, whereas it improves from 1.92 Mbps to 2.6 Mbps for 4-QAM as indicated in Table 11, indicating that even with ideal rate adaptation and higher modulations, Symbiotic Coding brings significant benefits.

### 4.7.3 The impact of varying SINR

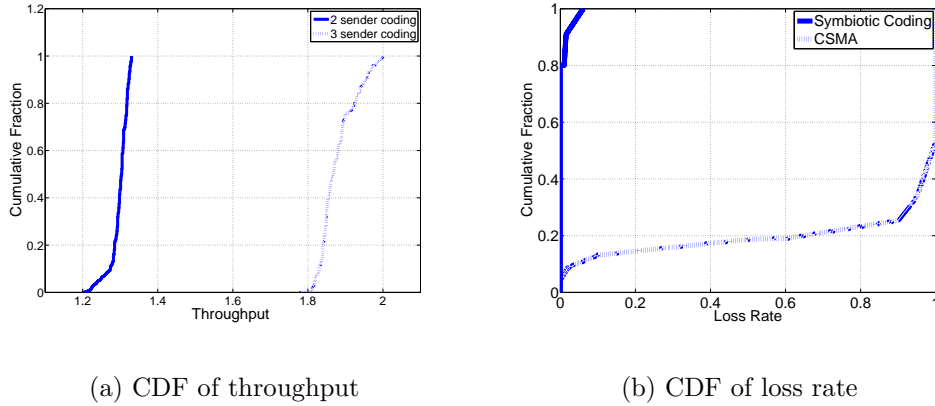
We evaluate Symbiotic Coding over a range of Signal to Interference and Noise Ratios ( $SINR = SNR_a - SNR_b$ ) to study different scenarios ranging from symmetric to asymmetric contentions at C1 and C2. We present the results for the case of BPSK.

**Throughput:** Contrary to the previous experiment where the two APs, AP1 and AP2 had the same SNR to client C1, here we consider the case when the SNRs are unequal. We begin with the case when the client C1 has an equal SNR from AP1 and AP2. Gradually we move C1 closer to AP1, thereby increasing the SNR of the transmission from AP1 with respect to AP2. Figure 40 a) presents the throughput of client C1 (normalized to the sending rate) as a function of the Signal to Interference Ratio ( $SIR = SNR_a - SNR_b$ ) for the collision free scheduler, CSMA and Symbiotic

Coding. The figure shows that Symbiotic Coding achieves a throughput for 0.67 whereas CSMA achieves a throughput close to zero for SIR from 0 to 6dB since AP1 and AP2 cannot ‘physically’ carrier sense each other. However, when the SIR is sufficiently high (greater than 6dB), AP1 starts to capture the channel and this causes its throughput to rise to 1. The total throughput of the two clients C1 and C2 is plotted in Figure 40 b) for the approaches considered previously. It can be observed that Symbiotic Coding outperforms both the collision free scheduler and CSMA for hidden terminal cases. When the capture effect occurs, Symbiotic Coding provides the throughput that CSMA achieves.

**Error performance:** Another aspect of performance is the BER as a function of the SIR. The BER measured at C1 for varying SIR is presented in Figure 40 c). The figure shows that CSMA suffers due to colliding transmissions since the competing transmission is treated as noise. Thus, while collision free scheduler achieves a BER close to  $10^{-3}$ , the BER of CSMA is very poor and becomes equal to that of the collision free scheduler for high SIRs, where the capture effect occurs. On the other hand, Symbiotic Coding begins with a much lower BER for an SIR of 0dB. This occurs due to the constructive addition that occurs when the two APs transmit a ”1”. However with increasing SIR, the error performance of Symbiotic Coding reduces and it becomes close to that of a collision free scheduler. This is a *counter-intuitive result and occurs because the contribution of AP2’s transmission is very small compared to AP1’s transmission.*

In summary, for all SIRs (i.e. all scenarios from hidden terminals to capture scenarios), Symbiotic Coding outperforms both collision free scheduler and CSMA in terms of both throughput and loss rate.



**Figure 41:** Scalability and loss performance

#### 4.7.4 Many concurrent senders

We evaluate the performance in a topology involving three senders and three receivers, where each AP is hidden from the others as shown in Figure 38.

**Throughput:** We plot the CDF of the total throughput achieved by all the clients for the case of Symbiotic Coding with 2 sender coding and 3 sender coding in Figure 41 a). Clearly, the benefits of Symbiotic Coding increase with the number of concurrent senders, with an average improvement upto 1.86x with 3 sender coding and 1.3x with two sender coding, when compared to a collision free scheduler. These values are quite close to the theoretical gains of 2 and 1.33.

**Loss performance:** We are also interested in determining the loss performance of Symbiotic Coding. For this, we use the same hidden terminal scenario as the previous experiment and conduct experiments for several time-spaced runs. We plot the results of the experiments in Figure 41 b) when using Symbiotic Coding and CSMA. It can be observed that Symbiotic Coding significantly improves the error performance of hidden terminals. Hence the average packet loss rate while using Symbiotic Coding is around 0.4% which is much smaller than the average loss rate when using CSMA which is around 86.5%.

**Table 12:** Symbiotic Coding yields significant benefits in large networks

Trace	Without coding (Mbps)	With coding (Mbps)	Improvement %
1	108	149.04	38
2	90	135	50
3	81	146.4	81

#### 4.7.5 Synchronization

Since we used a cable that carries the 100 MHz clock between two USRP2s, we measured that the transmit clocks are synchronized to within a sample clock (i.e. 10 ns). The computing power limitation at the receiver prevents us from sampling at a granularity lower than 250 nanoseconds. Hence, we sample at 250 nanoseconds at the receiver and observe that the transmissions from AP1 and AP2 are synchronized within this granularity. Thus, the synchronization achieved is a small fraction of the symbol duration of 1  $\mu$ s. Further, we observed the carrier frequencies from AP1 and AP2 to be perfectly coherent to within our sampling levels at C1 (250ns), thereby enabling existing frequency offset correction modules to be used as is, without any special treatment for concurrent transmissions. While the propagation induced phase difference varied for different locations, for each location they were estimated and overcome by pre-coding as described in Section 4.5.1. Thus the sampling interval, carrier frequency and start of packet are all synchronized successfully.

#### 4.7.6 Practical enterprise network benefits

We explore the benefits that our solution provides to a large enterprise WLAN over and above any natural spatial reuse that can be exploited simply by scheduling. We collect signal strength traces from a large enterprise network comprising around 30 Access Points distributed in the three 802.11g channels 1,6, and 11, operating in the 2.4GHz band. We perform trace-driven simulations of the algorithm described in Section 4.6.2 to determine the max-min fair network throughput. Our results are tabulated in Table 12 which shows that Symbiotic Coding improves the fair network

capacity by 38% to 81% compared to the existing state of the art communication and scheduling approach.

## CHAPTER V

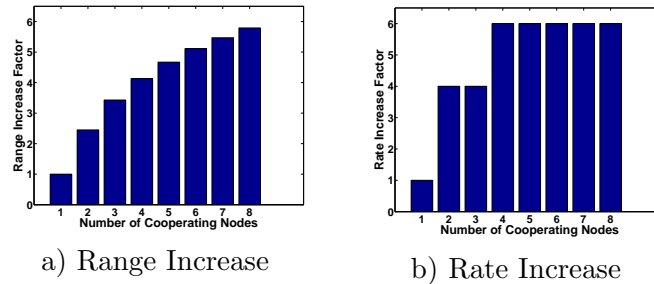
### DIVERSITY ROUTING FOR WIRELESS NETWORKS WITH COOPERATIVE TRANSMISSIONS

#### *5.1 Overview*

In this chapter, we consider the use of cooperative transmissions in multi-hop wireless networks to achieve Virtual Multiple Input Single Output (VMISO) links. Specifically, we investigate how the physical layer VMISO benefits translate into network level performance improvements. We show that the improvements are non-trivial (15% to 300% depending on the node density) but rely on two crucial algorithmic decisions: the number of cooperating transmitters for each link; and the cooperation strategy used by the transmitters. Finally, we present Proteus, an adaptive diversity routing protocol that includes algorithmic solutions to the above two decision problems and leverages VMISO links in multi-hop wireless network to achieve performance improvements. We evaluate Proteus using NS2 based simulations with an enhanced physical layer model that accurately captures the effect of VMISO transmissions.

#### *5.2 VMISO Background*

In a SISO link, a single transmitter sends one symbol in each symbol duration to its intended receiver. However, in a VMISO link,  $l$  ( $l \geq 1, l \leq n_c$ ) of the  $n_c$  transmitters transmit coded symbols to the (single) receiver in each symbol duration. The complex symbols transmitted by the  $l$  transmitters over a block of duration  $kT_s$  seconds are arranged to follow a certain structure which aids the decoding at the receiver in the presence of independent channel fading from each of the transmitters. This structure is called the Space Time Block Code (STBC) and is represented by a  $k * n_c$  matrix



**Figure 42:** Rate and range improvements of a VMISO transmission

which determines the symbols transmitted on each of the  $n_c$  transmitters for each of the  $k$  symbols periods. The bandwidth utilization of an STBC is determined by its rate  $R = \frac{l}{k}$  called the code rate, where  $R \leq 1$  [18].

**Benefits:** When spatially separated transmitters transmit encoded symbols across space and time, the receiver, with the knowledge of the channel fading coefficients, can process the signals to recover the symbols with much lesser bit error rate than otherwise. This spatial diversity benefit leads to a smaller SNR requirement (and  $E_b/N_o$  requirement, where  $E_b$  is the bit energy and  $N_o$  is the power spectral density of white noise). For instance, for a target BER of  $10^{-3}$ , the  $E_b/N_o$  required for uncoded BPSK modulation is 25 dB [6] whereas with a VMISO link, the required  $E_b/N_o$  is 10 dB (whereas it is around 15dB for MISO links which have a reduced SNR per branch). Thus with cooperation, the SNR required for decoding the signal is much lesser than without diversity.<sup>1</sup> For a specific target BER  $P_b$ , the reduced SNR requirement, can be translated into a longer transmission range for the same modulation rate or higher transmission rates by the use of higher order modulations for the same range or an intermediate rate, range pair. Consider BPSK modulation with diversity order  $n_c$  and a required bit error rate of  $P_b$ . Since the average SNR of a fading channel follows a path loss model, with exponent of  $\alpha$ , the range extension

---

<sup>1</sup>In a VMISO link where  $n_c$  transmitters transmit at a fixed power, the SNR per diversity branch is same as that of SISO link, unlike in MISO links, where the SNR per diversity branch is divided by  $n_c$ . Consequently, the diversity gains of transmit diversity are higher with VMISO link than with an equivalent MISO link.

factor can be obtained as

$$R_f(n_c) = \left( \frac{n_c * P_b^{\frac{1}{n_c} - 1}}{\binom{2n_c - 1}{n_c}^{\frac{1}{n_c}}} \right)^{\frac{1}{\alpha}} \quad (12)$$

The range extension factor is also a function of the modulation. The maximum range extension factor for the case of  $\alpha = 4$  is presented in Figure 42(a). Similarly, for a given range, the diversity gain can be used to obtain an increase in transmission rates. We consider a discrete set of modulations namely BPSK, QPSK, 16-QAM and 64-QAM which are popularly used in the 802.11 standard. The maximum rate improvement for the same range, with increasing number of transmitters is shown in Figure 42 (b) (where the code rate of the STBC (i.e 0.75) [18] is also considered. We consider the highest code rate for each  $n_c$  in this work). The values in the table represent the *maximum* range or rate that can be obtained independently.

Since the cooperating transmitters are not co-located, the signals could be received at the receiver with different delays and average received powers. Further, the clocks of the transmitters may not be synchronized. This leads to asynchronous reception and is similar to Inter-Symbol Interference in its effect. There have been several physical layer approaches to handle this problem, such as time-reversed space time codes and space time OFDM [7],[8].

**Feasibility:** There have been a few recent works which discuss the practical feasibility of cooperative transmissions. Specifically, [4] shows that the relative delays between signals from the transmitters are fairly small as compared to the symbol duration in 802.11 standard and in all cases the above physical layer approaches can be used to handle lack of synchronization. Also, [4] shows that due to spatial separation and consequent path loss differences, in more than 85%-90% of the cases, the relative power difference between two nodes is less than 5dB. These results and the related work indicate the existence of approaches to make cooperative transmissions feasible. Additionally, the feasibility has also been established recently in [9] with WLAN devices. All these works illustrate that cooperative transmissions are emerging close



to practice.

### 5.3 Motivation

In this section, we present the motivation for VMISO based strategies in improving routing performance. We first present the fundamental limitations of conventional (SISO) routing strategies in wireless multi-hop networks, followed by the benefits of VMISO based routing using a combination of illustrative scenarios, theoretical analysis and simulations.

#### 5.3.1 Limitations of current routing

The two basic factors that limit multi-hop throughput performance are as follows.

**1. Hop length effects:** While the number of hops that a flow traverses does not adversely affect throughput in wired networks, the number of hops has a significant impact on the end-to-end throughput of a flow. For a  $h$  hop flow, the end-to-end throughput is given by  $\frac{1}{h^\gamma}$  [64], where  $\gamma$  is an exponent between 1 and 2 for CSMA based networks with half-duplex radios.

**2. Inter-flow interference:** When multiple flows co-exist in a network, the resources have to be shared and the flows would interfere. Hence routing must also include the effects of interference across flows. This phenomenon has been analytically captured in [67]. As a result of the above factors, conventional routing techniques suffer severe degradation in practice. This has also been practically observed in wireless mesh network deployments [68]. We quantify the impact of these limitations on routing using simulations later in this section.

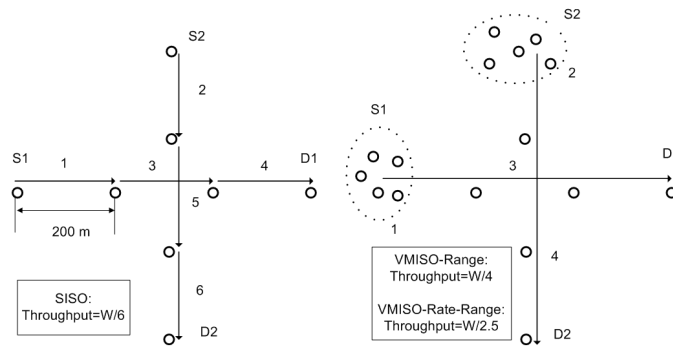
#### 5.3.2 Expected benefits of VMISO routing

While the physical layer data rate and range can be improved with cooperative transmissions as described in Section 5.2, the exact strategy for routing is non-trivial. A preliminary approach in related work [65] suggests the use of VMISO just for range

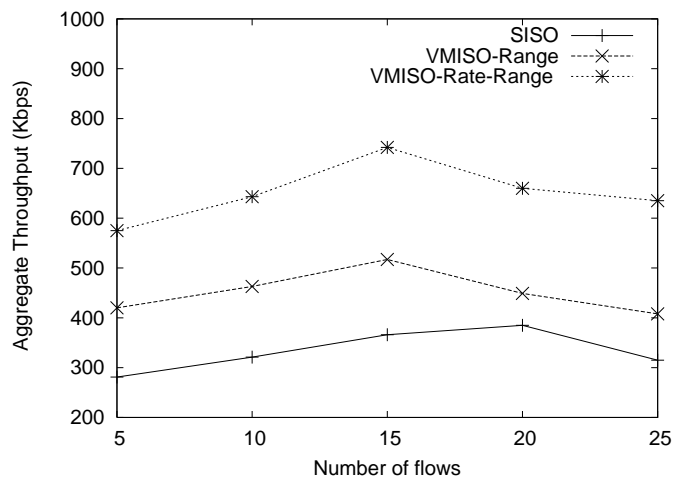
enhancement. However, different strategies using VMISO links provide different performance benefits and have inherent trade-offs. In the rest of this section, we highlight the fundamental trade-offs in using VMISO links and the need for intelligent mechanisms to leverage VMISO links. Throughout this discussion, the communication of each VMISO link involves two transmissions. One for distributing the packet to be sent, among its neighbors. The second transmission is the joint transmission of the source and all its neighbors together to the intended destination of the link. For the illustrations we consider a SISO transmission range of 250m. We refer to the number of simultaneous transmitters (including the source) as the cluster size. Similarly, we use cooperation gain and diversity gain interchangeably, (although cooperation gain includes both the diversity and power gain).

### 5.3.2.1 Illustrative scenarios

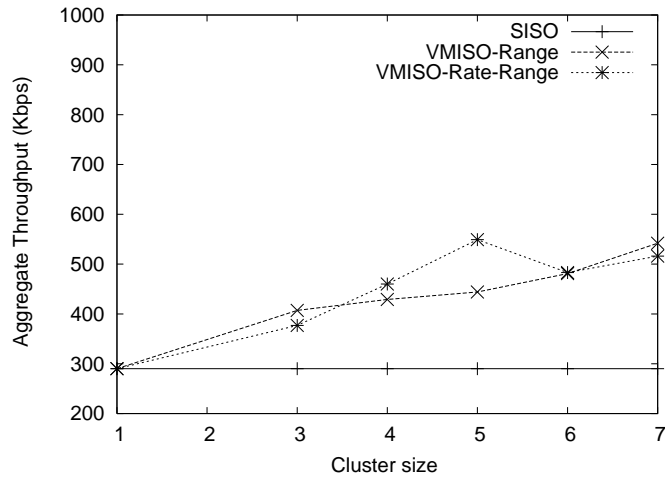
We use constructed topologies to highlight the impact of the cluster size and strategy on throughput with VMISO links. Figure 43 a) shows a topology with two flows, where nodes are separated by uniform distance of 200m. The end-to-end throughput of each flow obtained with SISO routing is then given as  $\frac{W}{6}$  where  $W$  is the bandwidth of the channel. First, we consider the use of cooperation gains for improving the rate of the VMISO link for the same number of hops. The rate strategy clearly performs worse than SISO achieving only 85% of the SISO throughput. This is due to the overhead of local transmission from the source to its neighbors. On the other hand, using VMISO gains for maximizing the range causes the throughput to be  $\frac{W}{4}$  since there are 4 contending transmissions, two for the local transmission (source to neighbors) and two for long-range all operating at the basic rate. When using an intermediate value of rate and range, the throughput is  $\frac{W}{2.5}$  since the cooperation gains (diversity and power gains) for 5 transmitting nodes to this destination, enable the VMISO links to operate at 4 times their basic rate (since the SINR requirement



(a) Illustrative topology for strategy



(b) Strategy in Random scenarios



(c) Cluster size in Random scenarios

**Figure 43:** VMISO benefits in arbitrary and random topologies

for this rate is about 10 dB higher than the basic rate).<sup>2</sup> Thus we observe that the benefits over SISO increase from (1.5x) with maximum range to (2.4x) with adaptive rate-range.

Next, we highlight the impact of cluster size through Figure 44 where two flows are depicted. With SISO routing, each flow achieves a throughput of  $\frac{W}{4}$ . Consider that cooperation gains are used with a fixed strategy namely to increase the transmission range. First, consider that a cluster size of 3 is used, where two neighbors transmit along with the source node. Now, the total power increases by 3 times, which with a path loss exponent of 4, gives a  $3^{\frac{1}{4}} = 1.31$  times increase in interference range compared to SISO. Since the nodes are out of interference range, the throughput of each flow is now increased to  $\frac{W}{2}$ . However, when a cluster size of 4 is used, the increase in interference range is  $4^{\frac{1}{4}} = 1.41$ . This causes non-interfering nodes to become interfering leading to a throughput of  $\frac{W}{3}$ . *Thus, we observe that the cluster size used affects throughput significantly and using all available neighbors for cooperation can degrade throughput(1.5x) compared to an intelligent choice of cluster size (2x).*

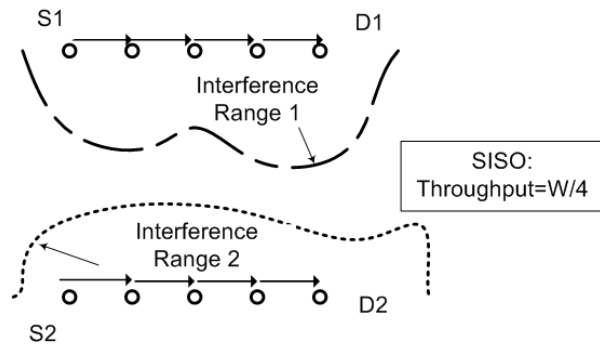
Thus, intelligent VMISO strategies substantially improve performance compared to both conventional routing (SISO) and naive VMISO (i.e. VMISO-Range [65]).

### 5.3.2.2 Simulations

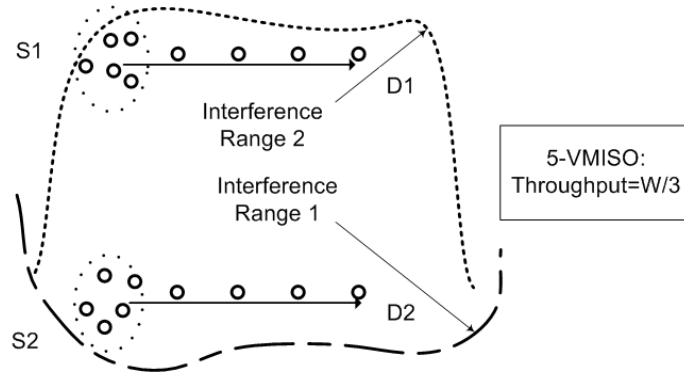
While it might appear that VMISO benefits are specific to the arbitrary scenarios presented in the illustrations, we highlight that significant benefits are obtained even in random scenarios using simulations. For the purpose of this discussion all nodes in the network use the same value of cluster size when strategy is varied and the same strategy when cluster size is varied. The simulation parameters are as described in

---

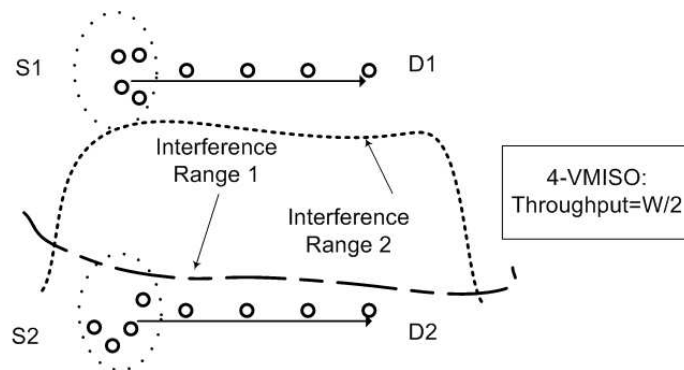
<sup>2</sup>In the above, when the bandwidth utilization of the space time code is also considered the achieved throughput change from  $\frac{W}{6}$  with SISO to  $\frac{W}{3.33}$  using range alone, to  $\frac{W}{2.67}$  using rate and range.



(a) SISO



(b) VMISO with cluster size 5



(c) VMISO with cluster size 4

**Figure 44:** Illustration for impact of cluster size

Section 5.8 with a default value of cluster size of 5 when not varied and the node degree is always higher than the cluster size under consideration. To begin with we consider the network throughput vs the number of flows, when the strategy is varied (plotted in Figure 43 b)). VMISO-Range is the strategy where every node utilizes all its available cooperation gain for range extension. VMISO-Rate-Range is the strategy when all nodes use a higher modulation (with 4 times higher data rate in this case). Among SISO and VMISO, VMISO schemes achieve a higher throughput compared to SISO for all values of number of flows. It can also be seen that the rate-range strategy where a higher rate than the base rate is used, provides significant benefits compared to SISO and using diversity gains for complete range extension. Thus, one can see that using diversity gains for rate and range in combination can yield significant benefits (2x) compared to SISO and (around 1.6x) compared to using the maximum range. Similarly, Figure 43 c) shows that the optimal cluster size is not the same for all strategies and is not always the maximum cluster size.

## 5.4 Theoretical Analysis

Since VMISO communication changes the physical layer parameters, the fundamental network parameters such as communication range and interference range must be appropriately modeled after taking into account the number of cooperating transmitters. To the best of our knowledge, the trade-offs and functional dependence of VMISO benefits have not been captured in related works. Hence, we first derive analytical relations for the communication range and interference range with and without VMISO. We then use these relations in determining the scaling of multi-hop throughput capacity with network parameters.

### 5.4.1 Relation between interference and communication range with VMISO

As described in the background section, for a given error performance (i.e. maximum allowable Bit Error Rate  $P_b$ ), the communication range of VMISO transmissions is

related to the cluster size  $n_c$  as described in Equation 12. Thus, for a given modulation, there is a clear improvement in communication range with increasing cluster size as plotted in Figure 42 a). However, this improvement is achieved only at the intended receiver which would perform channel estimation to benefit from the diversity gain. Since the other interfered clients would not perform channel estimation, the interference range does not increase by the same factor as the communication range. This is a profound result which makes VMISO a powerful strategy in overcoming interference related issues.

The wireless channel for a VMISO link with  $k$  transmitters is modeled by a vector of complex channel coefficients  $\mathbf{h} = [h_1 h_2 \dots h_K]^T$ . The received symbol  $y$  is then related to the transmitted symbol  $x$  as

$$y = \mathbf{h}^T \mathbf{x} + z \quad (13)$$

where  $z$  represents Additive White Gaussian Noise (AWGN) with zero mean and variance  $\sigma^2$ .

Without loss of generality let  $h_1$  represent the channel coefficient between the SISO transmitter and receiver and  $P$  be the transmit power. The expected receive power with SISO transmissions is then given as

$$S_1 = |h_1|^2.P.$$

Using a technique such as a space time code [18] to realize VMISO communication, the received power with  $k$  concurrent transmitters with corresponding channels  $h_1, h_2 \dots h_k$ , the received power can be given as

$$S_k = (|h_1|^2 + |h_2|^2 \dots |h_k|^2).P \quad (14)$$

Hence the received power gain is given by

$$G = \frac{P_k}{P_1}, \text{ i.e } G = \frac{(\sum_{i=1}^k |h_i|^2)^2}{|h_1|^2}$$

This power gain can be translated to an increase in communication range using the channel propagation and the threshold SNR required for achieving the desired

BER  $P_b$ . Let  $SNR_t$  be the threshold SNR required.

Since wireless channel propagation causes a power law dependence of the received power  $S$  with distance  $d$ , we have

$$S \propto \frac{1}{d^\alpha}$$

If  $d_1$  represents the communication range with SISO transmissions and  $d_k$  the range with VMISO transmissions, the previous relation can be inverted to yield

$$\frac{d_k}{d_1} = \left( \frac{(\sum_{i=1}^k |h_i|^2)^2}{|h_1|^2} \right)^{\frac{1}{\alpha}} \quad (15)$$

As a special case, when  $|h_1| = |h_2| \dots = |h_k|$ , the range improvement is  $k^{\frac{2}{\alpha}}$ . However, we note that the actual increase in communication range can be much greater than  $k$  depending on the channel distribution.

Similarly the interference range can be worked out by noting that Equation 14 is valid only at the intended receiver of the VMISO link as it performs channel estimation and DSTBC decoding. In contrast, for a receiver of another VMISO link whose channel signature would be different  $[w_1, w_2, \dots, w_k]$ , the received power is given by

$$I_k = E(|w_1 + w_2 \dots w_k|^2).P \quad (16)$$

Since the channel coefficients between each transmitter and the receiver are typically independent as long as the transmitters are separated by more than a quarter wavelength, The resulting interference power would depend on the channel distribution across transmitters 1 through  $k$ . Since the interference range is the range up to which another receiver can be interfered and the channels are typically independent and identically distributed, the equation can be simplified to yield

$$I_k = k.P \quad (17)$$

Similar to the preceding analysis, this power increase can be related to an increase in interference range by a factor

$$\frac{I_k}{I_1} = k^{\frac{1}{\alpha}} \quad (18)$$

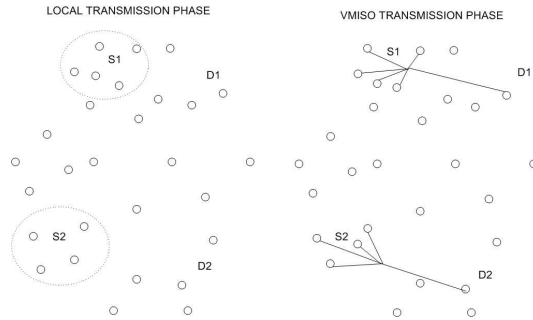


$$\frac{E(I_k)}{E(I_1)} < \frac{E(d_k)}{E(d_1)} \quad (19)$$

Thus Equations 15 and 18 represent the factors by which the communication and interference ranges are increased with VMISO links. Very importantly, we observe that the factors by which the communication and interference range increase is different which is the key leverage that VMISO transmissions enable to improve multi-hop interference performance.

### 5.4.2 Capacity scaling with VMISO strategies

We use the above derived relations to compute the throughput capacity bounds for different strategies as a function of the strategy and cluster size  $n_c$ . We use an approach similar to that in [67] to derive the order of benefits achievable with VMISO communication.



**Figure 45:** Two phase VMISO communication

#### 5.4.2.1 Model and Assumptions

*Network Model:* Consider  $n$  nodes deployed independently and uniformly at random on the surface of a disk of area  $A$ , in an environment characterized by a distance based signal reduction with path-loss exponent  $\alpha$  and Rayleigh fading. We use the protocol model of interference because of the simplicity of analysis and also because current MAC protocols like 802.11 readily support it. However, we corroborate our

insights using simulations based on the physical model of interference in Section 5.8. We clarify the notation that we use throughout this work. When we refer to network throughput we will use the notation  $NT$  and when referring to link throughput we will use the notation  $T$ . We will use  $R$  to represent the range for different strategies and transmit array sizes and indicate the range extension factor as  $R_f$ .  $D$  will represent the data rate and will be used with appropriate subscripts to indicate the link that we are talking about.

*Routing Model:* In a conventional multi-hop transmission, each source communicates to its intended destination through multiple intermediate nodes (hops). At each stage of the route, a node transmits a packet to its neighbor on the route which is within its (SISO) communication range. We consider a model for VMISO communication consisting of two transmission stages as illustrated in Figure 45. In the first stage, a source node of a VMISO link performs a local transmission at a rate  $D_L$  to a subset of its neighbors. This is followed by the simultaneous transmission of encoded versions of the same message by the cooperating neighbors including the source to the destination of the VMISO link.

To begin with consider nodes deployed independently and uniformly at random on the surface of a disk of area  $A$ . Let  $f$  be the number of flows each with an average hop length of  $h$  hops. If  $R$  is the (SISO) transmission range and  $R_i$  the corresponding interference range, the spatial reuse (number of simultaneously active links) in the network can be at most  $SR = \frac{A}{\pi * R_i^2}$

The total number of links that need to be scheduled to support the demand for all the  $f$  flows, is approximately  $f * h$ . In a manner similar to that in [67], the total throughput of the network can be bounded as

$$NT_{SISO} \leq \frac{A}{\pi * R_i^2 * f * h} \quad (20)$$

We will henceforth use this as the maximum SISO network throughput achievable

and present throughput for different cases normalized to this value.

#### 5.4.2.2 Throughput of VMISO-Rate

First consider the use of rate increase as the only strategy for exploiting VMISO links. The increased SNR on the VMISO transmission can be used to select higher modulations, but since the antennas are not co-located, some bandwidth must be spent in distributing the source symbols to the cooperating transmitters. Depending on the time consumed for this phase, the overall rate of the VMISO link including the local transmission can be much smaller than that with a SISO transmission. Typically, the cooperating transmitters must be in the vicinity of the source. The local transmission rate would be determined by the minimum rate required to provide the data successfully to the required number of cooperating neighbors. Specifically, the rate of the VMISO link can be given as

$$\frac{T_{VMISO}}{T_{SISO}} = \frac{\frac{1}{D(1)}}{\frac{1}{D(n_c)} + \frac{1}{D_L}} \quad (21)$$

where  $D(1)$  is the rate of a SISO transmission,  $D(n_c)$  is the rate of a transmission using  $n_c$  transmitters ( considering the diversity gain and code rate) and  $D_L$  is the data rate of the local transmission <sup>3</sup> . If  $D_L$  is the same as  $D(1)$  , then there is no benefit to using the rate strategy. Thus although, one would expect the rate increase provided by diversity gain to improve network performance it in fact reduces the network performance. *This is much unlike SISO or MIMO networks where using higher rates does not reduce the throughput!* Since the hop length is unchanged and only the effective link rate is decreased, the overall network throughput using only rate increase of VMISO is thus reduced by the same factor compared to SISO.

---

<sup>3</sup>While it is possible to adapt the local rate depending on the number of cooperating transmitters, a fixed rate is more generic and also allows for additional features like load balancing among cooperating nodes

### 5.4.2.3 Throughput of VMISO-Range

Consider the use of VMISO gains to increase the communication range of the links forming a multi-hop network. Compared to a network using SISO links, the use of longer ranges can reduce the number of hops required to reach the destination. This can cause an increase in end-to-end throughput for a flow. However, the interference range is also increased causing more links to interfere with each other. For this discussion, we consider that all VMISO transmissions happen with the same number of cooperating nodes  $n_c$ .

As discussed previously in Section 5.2,  $n_c$  transmitters can cooperate to obtain a range extension of  $R_f(n_c)$  given by equation 12. With the use of long range links, the number of hops to be scheduled in the network is reduced by this factor compared to the SISO case. Hence there are a smaller number of VMISO links instead of several SISO links which transport data between the same set of sources and destinations. Each of these VMISO links need to perform a local transmission before performing the long-range transmission to distribute the data to the cooperating neighbors. Hence the number of local SISO links that need to be scheduled is also the same as the number of VMISO links. Hence the throughput of the local phase normalized to that of a SISO network ( $NT_{LOCAL}$ ) can be written as

$$NT_{LOCAL} = R_f(n_c) \tag{22}$$

where  $R_f(n_c)$  is given by equation 12.

However, for the long range phase, the interference range of each VMISO link is higher than that of SISO by a factor  $n_c^{\frac{1}{\alpha}}$  since the factor of  $n_c$  increase in transmit power now causes more nodes to carrier sense the transmission. Since the spatial reuse decreases quadratically with interference range, the reduction in spatial reuse is by a factor  $n_c^{\frac{2}{\alpha}}$ . Thus the spatial reuse is reduced compared to SISO but the overall

number of links is also reduced by the factor  $R_f(n_c)$ <sup>4</sup>. Thus the network transport rate for this phase when compared to the SISO case is

$$NT_{VMISO} = \frac{R_f(n_c)}{n_c^{\frac{2}{\alpha}}} \quad (23)$$

Since we have two phases for the communication the total time required to convey the data to all the destinations is given by the sum of the durations of both phases. The inverse of this time gives the rate at which packets reach the destinations and represents the overall network throughput  $NT_{TOTAL}$ . Thus, The overall network throughput is then  $NT_{RANGE} = (\frac{1}{NT_{LOCAL}} + \frac{1}{NT_{VMISO}})^{-1}$

The network throughput with range extension can now be given as

$$NT_{RANGE} \leq \frac{R_f(n_c)}{1 + n_c^{\frac{2}{\alpha}}} \quad (24)$$

For a Bit error probability  $P_b$  of  $10^{-3}$ , the range extension function is almost linear. Assuming a path loss exponent of four lets us express the scaling with  $n_c$ , as

$$NT_{RANGE} = O\left(\frac{n_c}{c + n_c^{\frac{1}{2}}}\right) \quad (25)$$

Thus the total throughput depends on the range extension factor and number of transmitters used. This factor is greater than one and consequently we observe that the range improvement improves overall network rate. With an example value of  $P_b = 10^{-3}$  and  $n_c = 4$ , the value is 1.44, which represents a 44% improvement in network throughput when ideal routing is assumed. Further for all practical values of  $n_c$  i.e  $n_c < 8$ , this factor is greater than 1 and thus, throughput benefits occur with VMISO range links. To get an insight into the reason, we look at the relative impacts of the spatial reuse and multi-hop burden. The core idea is that the increase in transmission range is much more than an increase in interference range. Equivalently,

---

<sup>4</sup>Additionally, the code rate of the space time code for each  $n_c$ ,  $CR(n_c)$  will also enter the numerator of this expression, which we include at the end of this section

a large transmission range is obtained for a relatively small increase in interference range leading to improved spatial reuse.

#### 5.4.2.4 Throughput of VMISO- Rate-Range

For a specific cluster size  $n_c$  and rate, the communication range is also uniquely determined since the transmit power of each node is fixed. For a given error rate performance, the data rate of a link depends on the modulation used. Hence we need an index for the different rates (modulations) under consideration. Since the relation between error rate and SNR varies with different modulations we consider several modulations of the same class such as BPSK, QPSK, etc. indexed by the order  $m$  can capture the error performance relation. The scaling of achievable rate improvements with  $m$  depends on the modulation varying from  $m$  for a PSK constellation to  $2^m$  for QAM constellations [6]. In our model,  $m = 1$  represents the basic (lowest rate) modulation. Although we develop the analysis for a single family of modulations, we consider accurately the popular modulations of interest used in IEEE 802.11 standard, when quantifying the benefits later in this section. Thus the first step is to compute the range extension factor compared to SISO for different modulation orders  $m$  for a given  $n_c$ . To begin with consider  $n_c = 1$ . Assuming that the receivers are not noise limited and a channel path loss exponent of  $\alpha$ , if  $R(0)$  is the transmission range of the basic modulation, the transmission ranges of the higher modulations can be given as  $R(m) = R(0) * \frac{SNR_T(0)}{SNR_T(m)}^{\frac{1}{\alpha}}$ .

The relation between the modulation and its transmission range occurs through the SNR-threshold  $SNR_T(m)$  or equivalently the threshold SNR per bit ( $E_b/N_o$ ), related by the spectral efficiency of the modulation. This can be generalized to different cluster sizes  $n_c$  as follows.

Let  $R_f(n_c, 1)$  represents the communication range achieved using an average cluster size of  $n_c$  nodes and at the basic modulation indexed by  $m = 1$  (For BPSK, the

expression is given by Eqn. 12). When transmitting with a higher order modulation ( $m$ ), the effective range is now reduced to  $R_f(n_c, m)$ , with a modulation dependent rate increase.

$$R_f(n_c, m) = R_f(n_c, 1) * \left( \frac{SNR_T(1)}{SNR_T(m)} \right)^{\frac{1}{\alpha}} \quad (26)$$

having obtained the range extension factor with this rate, the throughput of the VMISO phase with modulation order  $m$ ,  $NT_{VMISO-m}$  can now be written as  $NT_{VMISO-m} = 2^m * \frac{R_f(n_c, m)}{n_c^{\frac{2}{\alpha}}}$  where we have used the fact that the rate is  $2^m$  times the basic rate. This when simplified becomes

$$NT_{VMISO-m} = 2^m * \frac{R_f(n_c, 0) * \left( \frac{SNR_T(0)}{SNR_T(m)} \right)^{\frac{1}{\alpha}}}{n_c^{\frac{2}{\alpha}}}$$

When compared to the throughput using only range we have

$$\frac{NT_{VMISO-m}}{NT_{VMISO-0}} = 2^m * \left( \frac{SNR_T(0)}{SNR_T(m)} \right)^{\frac{1}{\alpha}} \quad (27)$$

Considering both the local transmission stage and the cooperative transmission stage, the network throughput using Range and Rate can be given as

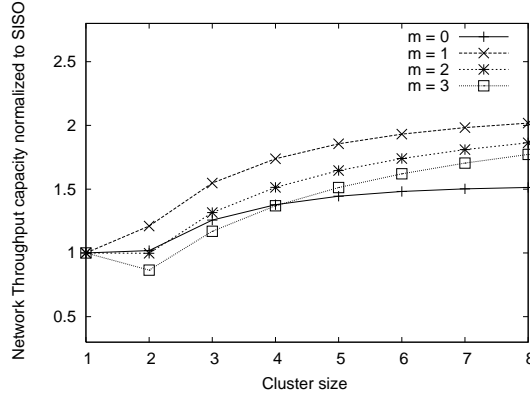
$$NT_{HYBRID}(n_c, m) \leq \frac{2^m * R_f(n_c, 0) * \left( \frac{SNR_T(0)}{SNR_T(m)} \right)^{\frac{1}{\alpha}}}{2^m + n_c^{\frac{2}{\alpha}}} \quad (28)$$

Since the range extension function is almost linear for a  $P_b = 10^{(-3)}$ , with  $\alpha = 4$  and assuming a PSK modulation class whose SNR requirement grows about 6 dB per additional bit per symbol [6], we can approximate the benefit as

$$NT_{HYBRID}(n_c, m) = O\left( \frac{2^{\frac{m}{2}} * n_c}{2^m + n_c^{\frac{1}{2}}} \right) \quad (29)$$

#### 5.4.2.5 Insights

The above expressions (valid for  $n_c \geq 2$ ) describe the dependence of network throughput on the rate and range. To gain additional insight, we evaluate the exact



**Figure 46:** Rate-Range trade-off for VMISO

expression numerically for different modulations and  $n_c$ , and the values obtained are as shown in Figure 46. Several interesting observations can be made.

1. The throughput improvement with VMISO range over SISO is between 1x to 1.5x for  $P_b = 10^{-3}$  and  $n_c \leq 8$ .
2. Using adaptive rate and range yields almost a 2x improvement compared to SISO.
3. The benefits are higher when the target BER  $P_b$  is lower ( $10^{-5}$  for instance).
4. The benefits are higher when the local transmission can be accomplished at a higher rate.
5. The results are a lower bound to the performance benefits achievable when the cluster size or strategy is varied at a finer granularity than on a network level.

The effect of the code rate of the space time code can be obtained by replacing  $2^m$  in the equation with  $2^m * CR(n_c)$ . This leads to a modest decrease in VMISO benefits over SISO, but preserves rate-range benefits over range. Thus, in this section ,we have showed that the overall network throughput using adaptive rate and range can be better than using a fixed rate alone under idealized conditions of balanced routing and simple scheduling. *The aim of the analysis is just to show that even*



*with a simple two phase scheduling, network benefits can be obtained by adaptive choice of strategies compared to SISO or using only a fixed strategy.* The analysis has also showed that the benefit obtainable with intelligent scheduling can be much higher since the transmission time required for the local transmissions is still the bottleneck. When the local phase and cooperative transmission phase are adjusted to be of different durations, it is possible to obtain larger benefits.

### **5.4.3 Summary**

In summary, both the simulations and the analysis confirm the following main observations:

1. Joint rate - range optimization offers the best possible performance when compared to optimizing one factor in isolation.
2. The optimal cluster size is not a fixed value (e.g. maximum) and varies with the strategy of operation.

## ***5.5 Algorithm Design***

In this section, we identify the key characteristics of VMISO links that determine network level benefits and explore how an algorithm can be developed to utilize the characteristics to adapt network layer choices.

In this section, we identify the key characteristics of VMISO links that determine network level benefits and explore how an algorithm can be developed to utilize the characteristics to adapt network layer choices.

### **5.5.1 Many or Few - Number of cooperating transmitters**

The cluster size directly determines the diversity gain and the total power transmitted by the VMISO link (cooperation gains). When translated to link level performance, the cluster size determines the data rate improvement or range improvement achievable for a specific reliability requirement. On the other hand, a larger cluster size

causes increased interference powers at other nodes. The increase in carrier sense range with cluster size was found in the previous sections as  $n_c^{\frac{2}{\alpha}}$ . Thus, the choice of cluster size must balance the benefits and the interference. Specifically, for isolated flows, the self interference among links of a flow impacts the spatial reuse. Using the arguments from Section 5.3, the number of contending links of a flow along a path  $P_j$ , is related to the interference range and transmissions range as

$$S_I(P_j, n_c, m) = \frac{2 * R_i * n_c^{\frac{2}{\alpha}}}{R(n_c, m)} \quad (30)$$

where  $R_i$  is the SISO interference range and  $R(n_c, m)$  is the communication range using modulation  $m$  and  $n_c$  cooperating nodes.

Since VMISO links allow long-range hops, the above expression must be modified to include the case when all hops of the flow are within the interference range. In that case, the self interference can be quantified as

$$S_I(P_j, n_c, m) = \min\left(\frac{h * S}{R(n_c, m)}, \frac{2 * R_i * n_c^{\frac{2}{\alpha}}}{R(n_c, m)}\right) \quad (31)$$

where the flow consists of  $h$  hops with average hop-length  $S$ .

### 5.5.2 Farther or Faster - Strategy for cooperation

The cooperation gains can be used for increasing the rate only or increasing the range alone or for obtaining an intermediate rate,range pair. For a given cluster size, the set of rate,range pairs achievable is fixed. A straightforward approach to using rate and range is to switch between the two strategies. However, as already seen in Section 5.3, such a switching is unlikely to yield benefits because of the performance degradation incurred by the cost of local transmissions. Thus, a hybrid of rate and range must be chosen for each case since only that allows fine grained usage of diversity gains to the maximum extent possible. Using a fixed strategy cannot utilize all the available diversity gain as seen in Section 5.3. For a given cluster size, the data rate of the local transmission affects the effective rate of the VMISO link. Hence, a higher VMISO

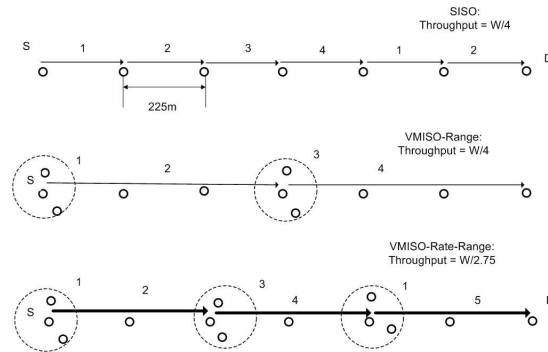
link rate can give benefits only when combined with range improvement. This must be factored in the strategy decision. The effective rate of a VMISO link (normalized to SISO) is thus

$$D = \frac{T(n_c) * 2^{m-1}}{T(n_c) * 2^{m-1} + 1} \quad (32)$$

where  $T(n_c)$  is the code rate for the STBC, (recall from [18] that it depends on  $n_c$ ) and the factor of 1 in the denominator denotes the local broadcast at the basic rate, before each VMISO transmission. Additionally, the cluster size of a VMISO link must be less than the node degree in the vicinity of the source node and the SINR must be satisfied at the receiving end-point for the VMISO link to be feasible.

### 5.5.3 Joint or Sequential - Ordering of decisions

Given the sub-optimality of using rate or range optimization in isolation (described in Section 5.3), the next question to explore is whether the rate and range optimization must be performed in a joint manner or sequentially (i.e maximize either the rate or range and use the excess diversity gains for the other strategy). We show that such a sequential maximization approach is not sufficient to achieve benefits and highlight the need for joint maximization over achievable rate-range pairs using an illustrative topology in Figure 47.



**Figure 47:** Illustration for sub-optimality of simple rate adaptation with range

The figure represents a single flow with 6 hops. The slot schedule is also depicted on the links along with the throughput. For the flow shown, using SISO, with a

transmission range of 250m, causes one in four hops to be inhibited with carrier sense protocols. A cluster size of 3 is available is available for cooperation. With this cluster size, the ranges for the basic rate, twice the rate and 4 times the basic rate are 3.43x, 2.88x, 1.88x respectively (using equations derived in Section 5.4), with x the SISO range being 250m. Thus, SISO achieves a throughput of  $\frac{W}{4}$  and VMISO with maximum range achieves a throughput of  $\frac{W}{4}$ , whereas adaptive rate-range yields a throughput of to  $\frac{W}{2.75}$ . This is because using the maximum possible range gives only 2.5dB of extra SNR over the threshold SNR for the basic rate whereas the adaptive strategy's rates are 4 times higher than the SISO rate. Thus joint decisions are required to prevent the throughput loss that occurs when using sequential decisions.

## ***5.6 Solution Description***

Since the nature of the links is changed fundamentally when VMISO transmissions are used, the routing must be performed in a manner which takes this into consideration. Hence the problem of utilizing VMISO links in a network can be formulated as a routing problem. However, even deciding the cluster size for different flows for fixed strategy is NP-HARD. The problem is complicated by the inter-dependence between the cluster-size, strategy and path characteristics on throughput (Section 5.4).

### **5.6.1 Problem formulation**

*VMISO-ROUTE*: Given a multi-hop network with  $f$  flows, the problem is to identify the routes to be taken for each flow i.e. the nodes that form the route and the strategy at each hop of the route with the constraint that only one-hop neighbors can participate in the cooperative transmission.

**Lemma 1: VMISO-ROUTE is NP-HARD:**

**Proof:** In general, the problem of determining the best path for a single flow, given a fixed cluster size and strategy is itself an NP-Hard problem as described in [66]. The problem of determining the best routes between a given source and destination can

be modeled as follows. Given a graph  $G$  of nodes in the network and a conflict graph  $H$  which contains an edge if two nodes interfere with each other, the problem of determining the maximum throughput route is the same as the problem of determining a maximum independent set of  $G$ . It can be shown that the problem of identifying a maximum independent set of the above graph can be reduced to the routing problem in the SISO case under the protocol model of interference. Hence, with the choice of cluster size and strategy leading to more possibilities and expanding the search options, the hardness of VMISO-ROUTE is greater than that of SISO routing. Even in the simplest case where the cluster size is unity, the problem is NP-HARD, which indicates that VMISO-ROUTE cannot be completed in polynomial complexity in general.

### 5.6.2 Algorithm

Since the routing problem is NP-HARD and we are interested in a distributed realization for the routing solution, we make decisions on a per-flow basis. We argue that this is a justifiable choice given the reduction in complexity compared to link level decisions. The key challenge here is *how to compute good VMISO routes with just SISO path information while taking into account the conflicting trends*. To do this, we model the dependencies carefully and also collect additional statistics from the intermediate nodes to capture the interactions in a single path metric. We first describe the derivation of the path metric and the identification of other constraints followed by the description of the algorithm.

#### 5.6.2.1 Derivation of Path Metric

Any path metric for routing in wireless networks must include three components, namely, self-interference, inter-flow interference and link data rate. All these three components change with VMISO links compared to SISO. The impact of self interference was captured already in Eqn. 31 and the link data rate in 32. Thus we need

**Variables:**

- 1  $f$ : Flow-id,  $P_j$ :  $j$ th shortest path,  $N$ : Maximum cluster size
- 2  $n_c$ : cluster size,  $n'_c$ : current best cluster size,  $m$ : modulation order
- 3  $m'$ : Current best modulation order,  $MAX_M$ : Current Maximum metric
- 4  $SNR_{TH}(m)$ : SNR Threshold of  $m$ ,  $l$ : Number of paths
- 5  $MAX_P$ : Current highest metric path-id,  $M$ : Highest modulation order,  $SNR(n)$ :  $SNR$  of node  $n$
- 6  $M(P_j, n_c, m)$ : Metric of path  $P_j$  with cluster size  $n_c$  and modulation order  $m$ ,  $D$ : VMISO link data rate
- 7  $I(n_c, n)$ : Interference value for node  $n$  and  $n_c$  neighbours,
- 8  $P_j(n_c, m)$ : Subset of  $P_j$  connected with links using rate  $m$  and cluster size  $n_c$ ,  $T(n_c)$ :  $n_c$  \*1 STBC rate
- 10  $F(P_j, n_c, m)$ : Bottleneck interference of path  $P_j$  with cluster size  $n_c$  and modulation order  $m$

**Compute-path-info ( $f$ )**INPUT: Source, Destination pair of flow  $f$ OUTPUT:  $l$  Paths  $P_j$  and  $I(n_c, n) \forall n \in P_j, n_c \leq N$ 

- 11 For  $j = 1$  to  $l$
- 12  $P_j = \text{Compute-SISO-shortest-path}(f)$
- 13 For each  $n \in P_j$
- 14 For each  $n_c \leq N$
- 15  $I(n_c, n) = \text{Interference-load}(n, n_c)$

**Compute-metric( $P_j, n_c, m$ )**INPUT:  $P_j, n_c, m, S$ OUTPUT:  $M(P_j, n_c, m)$ 

- 16  $F(P_j, n_c, m) = \max(I[n_c, n]) \forall n \in P_j(n_c, m)$
- 17 If  $n_c \geq \text{degree}(n) \forall n \in P_j(n_c, m)$  and  $SNR(n) > SNR_{TH}(m)$
- 18  $B = \max(F(P_j, n_c, m), \min(\frac{h(P_j)*S}{R(n_c, m)}, \frac{2*R_i(n_c)}{R(n_c, m)}))$
- 19 If  $n_c > 1$
- 20  $D = \frac{T(n_c)*2^{m-1}}{T(n_c)*2^{m-1}+1}$
- 21 Else
- 21  $D = 1$ , return ( $\frac{1}{B*D}$ )
- 22 Else
- 22 return(0)

**Execution Sequence**

- 23 For every unassigned flow  $f$
- 24 Compute-path-info ( $f$ )
- 25 For each path  $P_j, j = 1$  to  $l$
- 26  $MAX_M = 0, n'_c = 1, m' = 1$
- 27 For each  $n_c = 1$  to  $N$
- 28 For each  $m = 1$  to  $M$
- 29  $M(P_j, n_c, m) = \text{Compute-metric}(P_j, n_c, m)$
- 30 If  $M(P_j, n_c, m) > MAX_M$
- 31  $M(P_j, n_c, m) = MAX_M, n'_c = n_c$
- 32  $m' = m, MAX_P = j$
- 33  $P(f) = P_{MAX_P}$

**Figure 48:** Algorithm for joint Routing, Cluster size and Strategy assignment

to identify the impact of VMISO on the inter-flow interference.

When multiple flows are considered, the interference between links of different flows affects performance. Due to multiple concurrent transmissions, VMISO links can have increased interference effects if the cluster size and strategy are not controlled appropriately. In this sequel, we show how the bottleneck interference on each path  $P_i$  can be obtained to characterize the inter-flow interference. First consider the effective path  $P_i(n_c, m)$ , when a cluster size  $n_c$  and modulation order  $m$  are used. The set of nodes in  $P_i(n_c, m)$  is a subset of those in  $P_i$  since VMISO hops can skip over intermediate SISO nodes. Given a neighbor list, which consists of the number of links overheard by each of the neighbors, a source node of a VMISO link can determine how many links, it has to share the channel with. i.e to form a VMISO link of  $n_c$  neighbors the maximum of the interference activity overheard by any of its  $n_c$  neighbors would be the bottleneck which leads to sharing among links in the contention region. Since each flow can have multiple VMISO hops, the bottleneck contention for each hop can be obtained as the maximum of these values across the VMISO link sources ( i.e nodes in  $P_i(n_c, m)$ ).

$$F(P_i, n_c, m) = \max_{n \in P_i(n_c, m)} I(n_c, n) \quad (33)$$

where  $I(n_c, n)$  is the maximum interference perceived by any of the  $n_c$  neighbors of node  $n$ .

Combining expressions 31,32 and 33, the final throughput metric can be given as

$$M(P_i, n_c, m) = \max_{P_i, n_c, m} \frac{D(n_c, m)}{\max F(P_i, n_c, m), S_I(P_i, n_c, m)} \quad (34)$$

### 5.6.2.2 Constraints

With this we have the additional constraints that the links be bi-directional, the cluster size  $n_c$  for this path, is feasible at the VMISO end-points in the path and the

SINR requirements are satisfied at the receiver. Thus the algorithm computes the values of  $P_i$ ,  $n_c$  and  $m$  which maximize the metric subject to these constraints.

### 5.6.2.3 Algorithm

The details of the algorithm are presented in the pseudo code shown in Figure 48. The algorithm first determines the SISO shortest path information (line 26) along with the interference measure for each node in the path (lines 12-16). This is followed by identifying the bottleneck interference (line 17) for a given cluster size and modulation. Then, the feasibility of the VMISO link is checked to ensure that there is an end-to-end path for this  $n_c$  and  $m$  followed by determining the effective link rate of the VMISO links on the path (lines 20-22) and the path metric (lines 23-24). Then the expected path metric is computed for each of the available paths for different values of  $n_c$  and  $m$  and the values of  $P_j$ ,  $n_c$  and  $m$  with the highest metric is chosen as the solution (lines 31-35).

From Figure 48, one can observe how the algorithm takes into account the considerations identified in Section 5.5. Specifically, self-interference for VMISO links is captured in line 19, whereas the interference across flows is captured in line 17. The impact of the local transmission is also incorporated into the metric computation and the rate of the STBC code for different values of cluster size is also considered (lines 20-22).

### 5.6.2.4 Complexity and Correctness

While a brute force solution would involve  $n_c * f * m$  route computations for  $f$  flows, the proposed solution just requires  $f$  route computations, thereby significantly reducing the complexity of routing. Observe that the determination for cluster size, strategy combination is performed for the entire design space by computing the expected path metric using the available SISO path information. A critical feature of flow level assignment is that the bottleneck interference i.e the maximum number



of intersecting flows in any contention domain of the network decides the impact of inter-flow interference on the throughput of the flows. While adapting parameters such as  $n_c$  and  $m$  can be performed on a link or hop level in lieu of a flow level, this introduces a higher possibility of link asymmetry and increases the complexity of routing significantly.

## 5.7 *Distributed Realization*

In this section, we describe how the diversity routing algorithm presented in the previous section can be realized in a distributed manner with appropriate MAC layer support.

### 5.7.1 Diversity routing protocol

We present the distributed diversity routing protocol called Proteus. We focus only on the route discovery step of the routing protocol and use conventional route maintenance procedures for maintaining routes. Other components such as forwarding are similar to popular on-demand protocols such as the Dynamic Source Routing protocol (DSR) [10], except that the source route packet also includes the cluster sizes and strategies to be used in addition to the ids of intermediate nodes. This is needed since a given node which is part of multiple flows, can use different cluster sizes to support each of the flows.

#### 5.7.1.1 *Route Request*

The first step in the route discovery phase is the transmission of the Route Request (RREQ) by the source. As in conventional routing protocols, nodes stamp their IDs on the RREQ packet. In addition each node  $j$  stamp the following 4-tuple  $(S_j, I_j, NL_j, F_j)$  where  $S_j$  is the received signal strength from the previous hop,  $I_j$  is the ambient interference level (the fraction of time, the channel is busy) ,  $NL_j$ , the neighbor list consisting of the number of links (unique source addresses) that

each neighboring node has overheard and  $F_j$ , the number of flows already served by this node. The interference information is obtained by nodes monitoring the fraction of time that the channel is busy (the received signal crosses the carrier sense threshold). This is used to estimate the load on the channel. Similarly, the neighbor list consists of the number of active links overheard by each neighbor obtained when neighbors periodically broadcast HELLO messages conveying their IDs and the ambient interference information. The nodes also hear pilot tones to track the number of VMISO links in vicinity. Thus, the Route Request propagation proceeds using SISO transmissions as in popular source routing protocols, with modifications to provide information to the source that helps its decision making.

#### *5.7.1.2 Route Response*

When the destination receives the route request, it transmits the Route Response (RREP) after adding the information about its vicinity. Intermediate nodes forward the packet as usual, except that when any of their statistics has changed, they update it on the route response packet. When the source receives the route response (RREP), it uses the statistics available on the packet to compute the metric described in the algorithm in Figure 48. The source collects  $l$  paths received within a timeout duration (where  $l$  is a predetermined constant such as 4). The source computes the path metric for each path for different values of  $n_c, m$  and selects the value that provides the best metric. The algorithm in Figure 48 requires estimates for the following. (1) Approximate Interference powers for every node on the path (2) Number of flows already served by each node on the path (3) Node degree of each node on the path (3) Number of SISO hops in the path. The SISO hop length is also obtained as in conventional routing protocols, while the other information is available in the RREP. The number of flows already served by the node is directly read from the route response packet.

### 5.7.1.3 Route failures and Maintenance

While it is possible to design route maintenance approaches tailored to VMISO links, we use the default mechanisms for route failure detection and route re-computation. Thus, on a route failure a route re-computation is initiated and a new route is found.

## 5.7.2 MAC layer support

For a VMISO transmission to be successful, the receiver needs three key pieces of information, namely the cluster size used for the transmission, the strategy (modulation) and knowledge of channel coefficients. The best cluster size and modulation for a given flow (identified at the end of the routing process described in § 5.7.1) are conveyed to the receiver of each VMISO link along with channel estimation between the transmitters and the receiver as described below.

*Selection of transmitters* The first stage of every VMISO transmission is the local transmission of data from a source to its neighbors. The source node determines a subset of its neighbors for cooperation based on the results of the SISO path computation. Nodes that receive the transmission successfully, after identifying their IDs on the packet, transmit the pilot tone at an appropriate time, given by the order of nodes on the packet. If all nodes receive the local packet successfully, they transmit the pilot tones one after another in time. When the local transmission is not successful at any of the desired nodes, the desired number of pilot tones is not heard by the source and destination. Consequently, the VMISO transmission is suspended by the nodes when they do not overhear the correct number of pilot tones. The source then performs a random back-off before trying again. In this way, the unreliability of the local transmission is addressed.

*Pilot tone stage:* On hearing a single pilot tone, the receiver waits for a preset duration of time to receive pilot tones from the nodes of the VMISO cluster. Since the channel estimation duration required is very small ( $< 50\mu s$  [11]) compared to

the data durations, we allow a waiting time that is long enough to hear from  $\beta$  nodes (we use  $\beta = 8$  in our solution). As in related work [4], we assume that the pilot tones are detectable over a range longer than the VMISO transmission range. This is accomplished using lower order modulations that have a long range.

*VMISO transmission:* Once the pilot tones are successful, the (simultaneous) VMISO transmission begins with a preamble transmitted at the basic rate using the appropriate space time code, indicating the rate for the payload of the packet, so that the receiver can know the modulation to be used for decoding. With this information and that obtained in the previous stage, the receiver decides the number of transmitters and the appropriate space time code to be used. For each value of  $n_c$ , we use a fixed best rate space time code available and so this mapping is unique.

The MAC must also support medium access with asymmetric links (e.g [12]) and must also support the estimation of interference to be exposed to the routing layer.

## 5.8 Performance Evaluation

### 5.8.1 Evaluation platform

The NS2 simulator (ns-2.32) was used. Rayleigh fading was used through the CMU extensions over a path loss model with an exponent of four. All nodes use a single channel of operation at 2.4GHz. Further a cumulative SINR based decoding procedure was developed. The diversity gains at different SINRs for different number of cooperative transmitters was used with a table lookup. Further, the SINR threshold for the basic rate (uncoded BPSK) was set to 25dB with a rate of 2Mbps.

*Physical layer modeling:* We do not perform bit-level simulations but provide the required packet level abstractions to get reasonably accurate results without significantly increasing the simulation time. When  $n_c$  nodes transmit simultaneously, the received powers of the  $n_c$  nodes are added along with their path loss and fading effects. Specifically the receiver computes  $Pt * \sum_{i=1}^{n_c} \alpha_i^2 * d_i^{-4}$  and compares it with

a specific threshold  $SINR_T(n_c, m)$ . The SINR threshold for each  $n_c$  and modulation  $m$  are obtained from [6] based on the current receive SINR. We consider BPSK, QPSK, 16-QAM and 64-QAM as the modulation set.

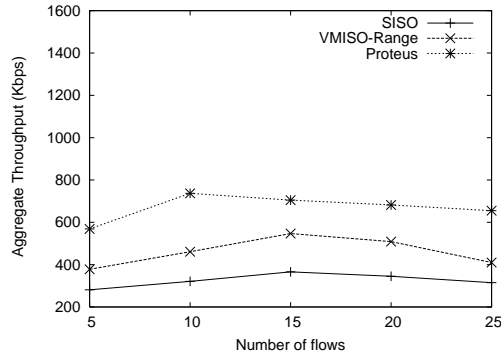
*Network parameters:* We use a 2500m by 2500m grid and deploy 200 nodes randomly in this region by default. The SISO transmission range is 250m for the basic rate. We setup random flows within the network using Constant Bit Traffic with UDP as the underlying transport protocol. We increase the sending rate to the maximum that the network can support. The default routing uses DSR. For the MAC, we use an idealized version of 802.11 which accommodates the presence of VMISO links using an approach similar to [4]. This MAC also handles the effects of differences in cluster sizes among nodes by allocating the channel fairly to different nodes. The local transmission rate of VMISO link is the same as the corresponding SISO rate. The aggregate end-to-end throughput of all the flows is the main metric. When cluster size is varied, the number of nodes in the network is set so that the average node degree is greater than the maximum cluster size. We use the random way-point mobility model with the ‘setdest’ utility in NS2. The mobility is varied between 0 m/s to 25 m/s with a pause time of 20s. For each data point, we average over 10 seeds with a simulation time of 100s per seed.

We compare Proteus with SISO (conventional routing) and the state of the art VMISO-Range [4].

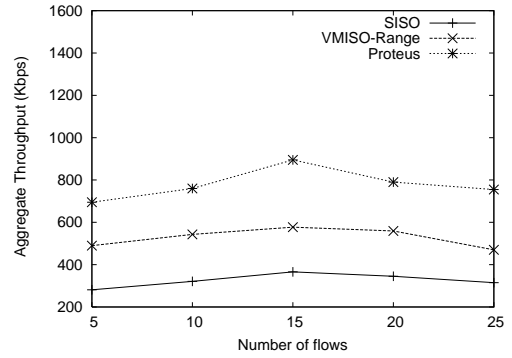
## 5.8.2 Results

### 5.8.2.1 Impact of number of nodes

Figures 49 a) and b) depict the impact of varying number of flows when the number of nodes deployed in the network is 150 and 200 respectively. From both figures, one can observe that the throughput increases up to a certain number of flows when the available spatial reuse in the network is fully utilized and beyond that it decreases. However, the throughput of Proteus is always much better than SISO. The magnitude

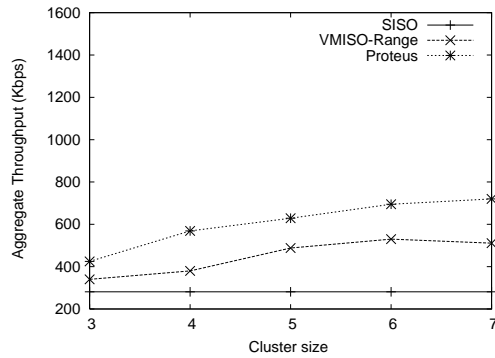


(a) Throughput with 150 nodes

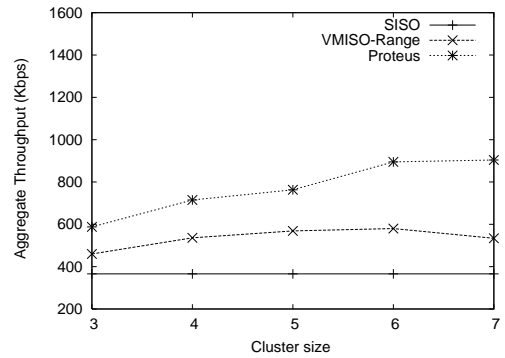


(b) Throughput with 200 nodes

**Figure 49:** Throughput vs. Number of flows



(a) Throughput with 5 flows



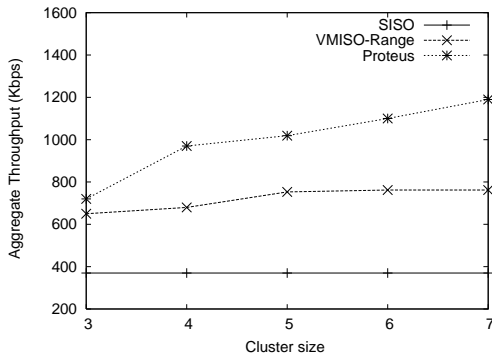
(b) Throughput with 15 flows

**Figure 50:** Throughput vs. Cluster size

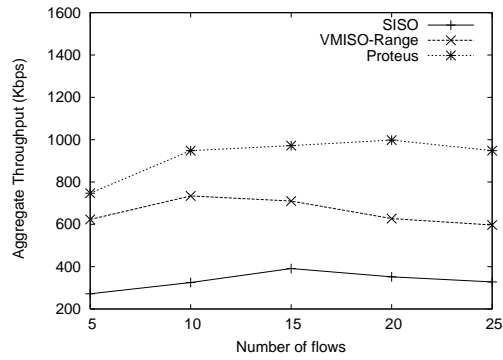
of the benefit is up to 2.1x for 150 nodes and 2.5x for 200 nodes. With 150 nodes, the average node degree being small, limits the cluster sizes that can be used. One can also observe that the throughput of using only range for routing although better than SISO (by about 1.3x and 1.6x), is still lesser than that of Proteus.

### 5.8.2.2 Impact of cluster size

The impact of varying cluster size is indicated in Figures 50 a) and 50 b) for 5 and 15 flows. One can observe that with increasing cluster size, the throughput of VMISO-range increases up to a certain point beyond which it decreases. This is because,

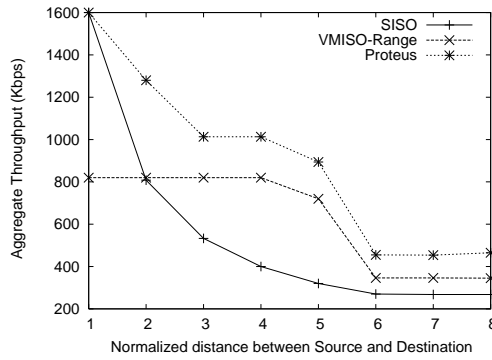


(a) Throughput vs cluster size with small grid size

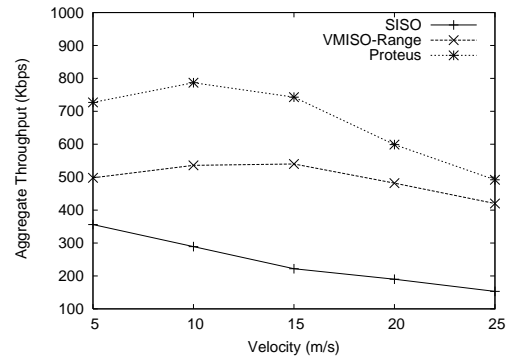


(b) Throughput vs flows with small grid size

**Figure 51:** Throughput with grid size



(a) Throughput with S-D distance



(b) Throughput with mobility

**Figure 52:** Throughput with hops and mobility

for any given flow pattern, indiscriminate increase of cluster size beyond a value, just contributes to increased interference without any range benefits. On the other hand, we observe that the throughput of Proteus does not decrease with increasing cluster size, since the best strategy that maximizes overall throughput is chosen and the increased gains from cluster size are utilized as much as the network allows to improve rate and/or range.

### 5.8.2.3 *Impact of grid size*

We study the effect of grid size using a ‘small’ network, where the grid size is 1500m \* 1500m. Since, the available spatial reuse itself is small the penalty of increased interference ranges due to VMISO transmission is lesser. Hence we observe an increase in throughput even with VMISO range (Figure 51). However, as the cluster size is increased, the benefits of VMISO range saturate because, the maximum range extension has been obtained. However, with Proteus, we observe that the throughput scales well with increasing cluster size since cooperation gains are also used for improving the rate. Thus, the throughput improves over SISO by a factor of 3x and less than 2x over VMISO range.

### 5.8.2.4 *Impact of mobility*

Figure 52 b) presents the aggregate throughput as a function of node mobility when the velocity of nodes is changed from 5 m/s to 25 m/s. It is clear that high mobility degrades performance for SISO. On the other hand, VMISO-Range is able to prevent route failures since nodes stay connected for longer durations due to the longer ranges. But, interestingly for the mobility considered here, Proteus has benefits over both SISO and VMISO. Only, when the velocity of the nodes is around 25 m/s Proteus has a slight degradation in its benefits due to its aim of achieving highest rate routes. Hence, the impact of mobility is significant only when the velocity is high. This is due to the longer range links (compared to SISO) available even when using a higher rate.

### 5.8.2.5 *Distance between source and destination*

The throughput of the flow when the source-destination distance is varied is presented in Figure 52 a) where the x-axis represents distance normalized to SISO transmission range. It is clear from the figure that the strategy that gives the best throughput depends also on the distance. Specifically, the SISO throughput falls with increasing



distance because of the number of hops within an interference region. VMISO-Range gives benefits when the number of hops is greater than 2. However, the best benefits are obtained with Proteus, when the source and destination are separated between 2 and 9 SISO hops. Thus, the results indicate that Proteus is likely to yield significant benefits for practical values of SISO hop lengths.

## CHAPTER VI

# CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

The focus of this dissertation has been to investigate the use of cooperative communication and smart antennas for addressing different challenges in wireless networks. The unique capabilities that cooperation provides to wireless links have been identified and their use for improving link quality, multi-hop throughput, spatial security and interference management have been described. This dissertation makes three main contributions: two in the context of single-hop wireless networks and one in the context of multi-hop wireless networks.

In the context of single-hop wireless networks, we first describe the need for new wireless security solutions by highlighting recent exploits on existing solutions. We then present an approach called physical space security that presents a new vision for secure information access in wireless networks. In this approach, secure information access is achieved by restricting the information to the desired spatial regions in the network by using smart antennas and node cooperation. While providing a first line of defense, this approach is also complementary to security approaches at other protocol layers. We then describe the challenges in realizing such a vision and novel techniques for information deprivation and information overloading to overcome these challenges. We presented “Aegis” a solution that includes the aforementioned techniques along with intelligent scheduling algorithms to achieve a fine balance between security and throughput in wireless LANs. Through simulations the gains of the proposed solution under different network conditions were illustrated. Prototype experiments using an 802.11g access point equipped with an antenna array were also conducted to

demonstrate the practical feasibility of beamforming in indoor wireless LAN scenarios.

Motivated by the rapidly growing density of wireless LAN deployments, we considered approaches to improve the capacity of dense wireless networks. We identified that a specific class of interference scenarios called asymmetric interference scenarios, allows successful information transfer upon collisions if the symbols are cooperatively coded. We proposed a coding solution called symbiotic coding whose capacity benefits scale with the number of interfered links. We presented coding tables for low density asymmetric interference scenarios and showed that significant capacity benefits can be achieved over collision-free scheduling approaches. We presented algorithms for applying the coding approach to large and dense wireless networks with appropriate scheduling. We also discussed several challenges including synchronization, modulations and handling channel impairments. We verified the experimental feasibility of the approach using software radios and used extensive traces from an enterprise wireless LAN to study network-level improvements.

In the context of multi-hop wireless networks, we considered the problem of achieving throughput scalability with increasing number of hops. We considered the use of cooperative transmissions in multi-hop wireless networks to achieve virtual MISO (Multiple Input Single Output) links. Specifically, we investigated how the physical layer VMISO benefits translate into network level performance improvements. We showed that the improvements are non-trivial (15% to 300% depending on the node density) but rely on two crucial algorithmic decisions: the number of co-operating transmitters for each link; and the cooperation strategy used by the transmitters. Finally, we presented Proteus, an adaptive diversity routing protocol that includes algorithmic solutions to the above two decision problems and leverages VMISO links in multi-hop wireless network to achieve performance improvements. We evaluated Proteus using NS2 based simulations with an enhanced physical layer model that accurately captures the effect of VMISO transmissions.

While the dissertation illustrates how smart antennas and cooperative communication can be used to achieve high performance and secure wireless networks through three specific problems, there exist several interesting open problems that are items for future research.

- ***Other wireless security attacks:*** While the dissertation has focused on the specific problem of eavesdropping in wireless LANs, there are several other security problems that are gaining significance in current wireless networks. These include privacy attacks such as user fingerprinting on end-users, the spread of malware and wireless denial of service. Given the increasing use of sensitive information over wireless networks and the limitations of wireless devices in terms of energy, computing power and storage, new security solutions are needed. Solutions developed for personal computers cannot be simply reused on smartphones, motivating a fresh look at wireless security problems. More importantly, the interference suppression capability of smart antennas and the potential for cooperation are becoming practical now. These unique capabilities offer a rich potential for novel security solutions.
- ***Multiple antenna receivers:*** The works in this dissertation have primarily considered receivers with single antenna and focused on adaptation, coding or beamforming at the transmitters. With the growth in technology client devices such as smartphones and tablets are becoming equipped with multiple antennas. In such scenarios, channel estimation, coding and adaptation solutions that were developed must be extended and modified to use the multiple antennas at the receiver intelligently. A careful consideration of how these approaches can be extended to multiple antenna receivers is an interesting direction for future research.
- ***Heterogeneous networks:*** While the dissertation focuses on homogeneous

networks where all access points are equipped with similar antenna capabilities, actual deployments are likely to be heterogeneous in the capabilities of nodes in the network. This heterogeneity makes distributed algorithms more challenging since resources are varied across the network. In practice, this may also lead to asymmetry induced problems such as deafness where different nodes perceive and understand the network condition differently. This is especially relevant in the design of medium access control solutions for wireless networks with smart antennas or node cooperation. Distributed carrier sensing, accounting for asymmetric link interference and appropriate link reliability mechanisms are important and non-trivial in such contexts.

- ***Handling mobility*** : The solutions developed in this dissertation have mainly focused on static and low mobility users. For such users, the frequency of adaptation of the strategies is low and justified due to the low doppler spread. However for highly mobile users, the feasibility of estimation and adaptation at fast time scales might be prohibitive. Investigating this line of research and developing solutions that explicitly handle user mobility is an interesting avenue for future research.
- ***Energy efficiency***: This dissertation considers capacity and security problems in wireless networks. However, devices such as smartphones and tablets are severely energy constrained. Beamforming and smart antennas can be used to reduce the overall energy expenditure of wireless devices by reducing transmit energy, transmit time and providing more opportunities for putting the radio in a low energy state. This line of research has been relatively unexplored and potentially significant in the near future.

## CHAPTER VII

### PUBLICATIONS

#### Journal Papers

1. **S. Lakshmanan**, K. Sundaresan and R. Sivakumar, “Multi-gateway association in wireless mesh networks,” *Elsevier Ad-hoc networks journal*, vol. 7, no. 3, pp. 622-637, May. 2009.
2. **S. Lakshmanan**, C.L. Tsao and R. Sivakumar, “Aegis: Physical-space security for wireless networks with smart antennas,” *IEEE/ACM Transactions on Networking*, vol.18, issue. 4, pp. 1105 - 1118, August. 2010.
3. Y.S.Jeong, **S.Lakshmanan**, K.Sandeep and R.Sivakumar, Cue-based networking , *Springer Wireless Networks journal*, vol. 17, Issue. 3, April 2011.
4. **S. Lakshmanan** and R. Sivakumar, “Diversity routing for multi-hop wireless networks with cooperative transmissions,” *under submission to IEEE/ACM Transactions on Networking*, Sep. 2009.
5. **S. Lakshmanan**, C.L. Tsao and R. Sivakumar, “Symbiotic Coding for high density wireless LANs,” *under submission to IEEE/ACM Transactions on Networking*, May. 2011.

#### Conference Papers

1. **S. Lakshmanan**, J.K. Lee, R. Etkin, S. J. Lee and R. Sivakumar, “Realizing High Performance Multi-radio 802.11n wireless networks,” to appear in the *IEEE Communications Society Conference on Sensor, Mesh and Ad hoc Communications and Networks (SECON)*, Salt Lake City, Utah, USA, June 27 - 30,

2011.

2. **S.Lakshmanan**, S. Sanadhya and R. Sivakumar, “On link rate adaptation in 802.11n WLANs,” in *IEEE International Conference on Computer Communications (INFOCOM)(Mini-conference)* Shanghai, China, April 10-15, 2011.
3. **S.Lakshmanan**, K.Sundaresan, A. Khojesteppour, and S.Rangarajan, “Practical Multi-link spatial reuse in wireless LANs,” in *ICST International Conference on Broadband Communications, Networks and Systems (BROADNETS)*, Athens, Greece, October 25-27, 2010.
4. **S.Lakshmanan**, K.Sundaresan, S.Rangarajan and R.Sivakumar, “The myth of spatial reuse with directional antennas in Indoor Wireless Networks,” in *Passive and Active Measurement Conference, Zurich (PAM)*, Switzerland, April 7-9, 2010.
5. **S.Lakshmanan**, K.Sundaresan, S.Rangarajan and R.Sivakumar, “Practical Beamforming based on RSSI measurements using Off-The-Shelf wireless clients,” in the *ACM SIGCOMM Internet Measurement Conference (IMC)*, Chicago, IL, USA, November 4-6, 2009.
6. **S. Lakshmanan**, C.L. Tsao and R. Sivakumar, “On coding concurrent transmissions in wireless networks,” Poster paper in Proceedings of *ACM Conference on Mobile Computing and Networking (MobiCom)*, Sep. 2009 (Extended abstract to appear in the ACM Mobile Computing and Communication Review).
7. **S.Lakshmanan** and R.Sivakumar, “Diversity routing for multi-hop wireless networks using cooperative transmissions,” in Proceedings of the *IEEE Communication society conference on Sensor, Mesh and Adhoc communication and networks, (SECON)*, Rome, Italy, June 22-26, 2009.

8. **S.Lakshmanan**, K. Sundaresan, R.Kokku, A.Khojestapour and S.Rangarajan, “Towards adaptive beamforming in indoor wireless networks,” in the *IEEE conference on computer communications (INFOCOM)*(Mini-conference), Rio de Janeiro, Brazil, April 19-25, 2009.
9. **S.Lakshmanan**, C.L.Tsao, R.Sivakumar and K.Sundaresan, “Securing Wireless Networks against eavesdropping using smart antennas,” in the *IEEE conference on Distributed Computing Systems (ICDCS)*, Beijing, China, June 17-20, 2008.
10. K.Sundaresan, **S.Lakshmanan** and R.Sivakumar, “On the use of Smart Antennas in Multihop wireless Networks,” in the *ICST conference on Broadband Communications, Networks and Systems (BROADNETS)*, San Jose, CA, USA, October 1-5, 2006.
11. R.Vedantham, S.Kakumanu, **S.Lakshmanan** and R.Sivakumar, “Component Based Channel Assignment in Single Radio, Multi channel adhoc networks”, in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, Los Angeles, CA, USA, September 24-29, 2006.



## REFERENCES

- [1] S. Lakshmanan and R. Sivakumar. (2008) Diversity routing for wireless networks with cooperative transmissions: Gnan technical report. [Online]. Available: <http://www.ece.gatech.edu/research/GNAN/archive/tr-proteus.pdf>
- [2] S. Barbarosa and G. Scutari, "Distributed space-time coding for multihop networks," in *IEEE ICC*, 2004.
- [3] J. N. Laneman and G. W. Wornell, "Distributed space-time coded protocols for exploiting cooperative diversity in wireless networks," *IEEE Transactions on Information Theory*, pp. 2415–2525, 2003.
- [4] G. Jakllari et al, "A cross layer framework for exploiting virtual miso links in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, 2007.
- [5] G. Jakllari et al, "Cooperative diversity in wireless networks: efficient protocols and outage behaviour," *IEEE Journal On Selected Areas in Communication*, 2007.
- [6] J. Proakis and M. Salehi, *Digital Communications*. McGraw-Hill Science/Engineering/Math, 2007.
- [7] G. Barriac, R. Mudumbai, and U. Madhow, "Distributed beamforming for information transfer in sensor networks," in *IEEE IPSN*, 2004.
- [8] D. R. B. III, G. B. Prince, and J. A. McNeill, "A method for carrier frequency and phase synchronization of two autonomous cooperative transmitters," in *IEEE SPAWC*, 2005.

- [9] M. Kurth and et al, “Cooperative oportunistic routing using transmit diversity in wireless mesh networks,” in *IEEE INFOCOM*, 2008.
- [10] D. Johnson, D. Maltz, and J. Broch, *DSR : The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks*. Addison-Wesley, 2001, ch. 5, pp. 139–172.
- [11] B. Daneshrad and B. Hochwald, “How much training is needed in multiple antenna wireless links?” *IEEE Transactions on Information Theory*, pp. 951–963, 2003.
- [12] G. Wang and et al, “A mac layer protocol for wireless networks with asymmetric links,” *Elseveier Adhoc Networks Journal*, pp. 424–440, 2008.
- [13] J. Zhang and Q. Zhang, “Cooperative routing in multi-source multi-destination multi-hop wireless networks,” in *IEEE INFOCOM*, 2008, pp. 2369–2377.
- [14] E. Gelal, G. Jakllari, and S. Krishnamurthy, “Exploiting diversity gain in mimo equipped ad hoc networks,” in *Asilomar Conference on Signals, Systems and Computers*, 2006.
- [15] L. Z. J. A. Amir Khandani, Eytan Modiano, *Cooperative Routing in Wireless Networks*. Kluwer Academic Publishers, 2004.
- [16] S. Lakshmanan *et al.*, “Securing wireless networks against eavesdropping using smart antennas,” in *IEEE ICDCS*, Jun 2008.
- [17] M. Buettner *et al.*, “A phased array antenna testbed for evaluating directionality in wireless networks,” in *MobiEval '07*. San Juan, Puerto Rico, USA: ACM, June 2007.
- [18] A.Paulraj, R.Nabar, and D.Gore, “Introduction to space-time wireless communications,” *Cambridge University Press*, May 2003.

- [19] J. Pang *et al.*, “802.11 user fingerprinting,” in *ACM International Conference on Mobile Computing and Networking (MOBICOM)*, Sep. 2007.
- [20] J. Franklin *et al.*, “Passive data link layer 802.11 wireless device driver fingerprinting,” in *USENIX Security Symposium*, Jul. 2006.
- [21] A. Akella *et al.*, “Self management in chaotic wireless deployments,” in *ACM Conference on Mobile Computing and Networking (MOBICOM)*, Sep. 2005.
- [22] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [23] R. L. Rivest, “All-or-nothing encryption and the package transform,” *Lecture Notes in Computer Science*, vol. 1267, p. 210, 1997. [Online]. Available: [cite-seer.ist.psu.edu/rivest97allornothing.html](http://citeseer.ist.psu.edu/rivest97allornothing.html)
- [24] Cisco wireless control system. [Online]. Available: <http://www.cisco.com/en/US/products/ps6305>
- [25] A. Haeberlen *et al.*, “Practical robust localization over large-scale 802.11 wireless networks,” in *ACM MOBICOM*, 2002.
- [26] Meru networks press release, July 28 2008. [Online]. Available: <http://www.merunetworks.com/>
- [27] M. Richards, *Fundamentals of Radar Signal Processing*. McGraw Hill inc., 2005.
- [28] N. Borisov, I. Goldberg, and D. Wagner, “Intercepting mobile communications: the insecurity of 802.11,” in *ACM Conference on Mobile Computing and Networking (MOBICOM)*, Jul. 2001, pp. 180–189.
- [29] P. Bahl, *et al.*, “Enhancing the security of corporate wi-fi networks using dair,” in *ACM MOBISYS*, 2006, pp. 1–14.

- [30] J. Yeo, M. Youssef, and A. Agrawala, "A framework for wireless lan monitoring and its applications," in *ACM Wireless Security Workshop (Wise)*, Sep. 2004, pp. 70–79.
- [31] J.-C. Chen, M.-C. Jiang, and Y.-W. Liu, "Wireless lan security and ieee 802.11i," *IEEE Wireless Communications*, vol. 12, no. 1, pp. 27–36, Feb. 2005.
- [32] Z. Li *et al.*, "Securing wireless systems via lower layer enforcements," in *ACM Wireless Security Workshop, WiSe*, Sep. 2006, pp. 33–42.
- [33] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *ACM Wireless Security Workshop, WiSe*, Sep. 2006, pp. 43–52.
- [34] Z. Sun and J. Lu, "Improving the security performance in mobile wireless computing network using smart directional antenna," in *IEEE Asia-Pacific Conference on Environmental Electromagnetics (CEEM)*, Nov. 2003, pp. 47–50.
- [35] J. M. Carey and D. Grunwald, "Enhancing wlan security with smart antennas: A physical layer response for information assurance," in *IEEE Vehicular Technology Conference (VTC)*, vol. 1, Sep. 2004, pp. 318–320.
- [36] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference (VTC)*, vol. 3, Sep. 2005, pp. 1906–1910.
- [37] N. L. S. Shafiee and S. Ulukus, "Secrecy capacity of the 2-2-1 gaussian mimo wire-tap channel," in *International Symposium on Communications, Control and Signal Processing*, Mar 2008.
- [38] K. Sundaresan and R. Sivakumar, "Routing in adhoc networks with MIMO links," in *IEEE ICNP*, 2005.

- [39] K. Sundaresan, R. Sivakumar and M. Ingram, “A Fair Medium Access Control protocol for wireless networks with MIMO links ,” in *IEEE INFOCOM*, 2003.
- [40] A. Sendonaris, E. Erkip, and B. Aazhang, “User Cooperation – part i: System Description, part ii: Implementation Aspects and Performance Analysis,” *IEEE Transactions on Communication*, vol. 51, no. 11, pp. 1927–48, Nov. 2003.
- [41] A. Scaglione and Y. W. Hong, “Opportunistic large arrays: Cooperative Transmission in Wireless Multi-hop Ad hoc Networks to Reach Far Distances,” *IEEE Transactions on Signal Processing*, vol. 51, no. 8, pp. 2082–92, Aug. 2003.
- [42] A. Kailas, L. Thanayankizil, and M. A. Ingram, “A Simple Cooperative Transmission Protocol for Energy-Efficient Broadcasting Over Multi-Hop Wireless Networks,” *Journal of Communications and Networks (Special Issue on Wireless Cooperative Transmission and Its Applications)*, vol. 10, no. 2, Jun. 2008.
- [43] Sriram Lakshmanan, Karthik Sundaresan, Sampath Rangarajan, and Raghupathy Sivakumar, “Practical beamforming using rssi measurements on off the shelf wireless clients,” in *ACM Internet Measurement Conference*, Nov. 2009.
- [44] “Fidelity-comtech inc, <http://www.fidelity-comtech.com>,” .
- [45] Ettus Inc., <http://www.ettus.com>.
- [46] The GnuRadio Project, <http://www.gnuradio.org/trac>.
- [47] Y. J. Chang and M. A. Ingram. Cluster transmission time synchronization for cooperative transmission using software defined radio. In *IEEE Workshop on Cooperative and Cognitive Mobile Networks (CoCoNet3)*, 2010.
- [48] Daniel Halperin et al. Taking the sting out of carrier sense: Interference cancellation for wireless lans. In *ACM MOBICOM*, 2008.

- [49] S. Gollakota and D. Katabi. Zigzag decoding: combating hidden terminals in wireless networks. In *ACM SIGCOMM*, pages 159–170, 2008.
- [50] S. Gollakota, S. D. Perli, and D. Katabi. Interference alignment and cancellation. In *ACM SIGCOMM*, 2009.
- [51] Jing Zhu et al. Cdma self-adaptation based on interference differentiation. In *IEEE Globecom*, 2007.
- [52] S. Katti, S. Gollakota, and D. Katabi. Embracing wireless interference: Analog network coding. In *Proc. of the ACM SIGCOMM*, pages 397–408. MIT, 2007.
- [53] A. Khina and U. Erez. On robust dirty paper coding. In *Proc. of IEEE ITW*, 2008.
- [54] Kun Tan et al. Sam: Enabling practical spatial multiple access in wireless lan. In *ACM MobiCom*, 2009.
- [55] M. Kurth, A. Zubow, and J.-P. Redlich. Cooperative opportunistic routing using transmit diversity in wireless mesh networks. In *Proc. of the IEEE INFOCOM*, 2008.
- [56] S. Lakshmanan, C. Tsao, and R. Sivakumar. Symbiotic coding for wireless networks: Available:, <http://www.ece.gatech.edu/research/gnan/archive/tr-sc.pdf>.
- [57] Li Li et al. Superposition coding for wireless mesh networks (extended abstract). In *ACM MOBICOM*, 2007.
- [58] T. Liu and P. Viswanath. Opportunistic orthogonal writing on dirty paper. *IEEE Transactions on Information Theory*, 52:1828–1846, 2006.
- [59] Nabeel Ahmed et al. Online estimation of rf interference. In *Proc. of the ACM Conext*, 2008.

- [60] Sriram Lakshmanan *et al.* Towards adaptive beamforming in indoor wireless networks: An experimental approach. In *IEEE Infocom (Miniconference)*, Apr 2009.
- [61] D. Tse and P. Vishwanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.
- [62] Vaduvur Bhargavan *et al.* Macaw: A media access protocol for wireless lans. In *ACM SIGCOMM*, 1994.
- [63] Xi Liu *et al.* . Dirc: Increasing indoor wireless capacity using directional antennas. In *ACM SIGCOMM*, 2009.
- [64] P. C. Ng and S. C. Liew, “Throughput analysis of ieee802.11 multi-hop ad hoc networks,” *IEEE/ACM Transactions on Networking (TON)*, pp. 309–322, 2007.
- [65] G. Jakllari, S. V. Krishnamurthy, M. Faloutsos, and P. V. Krishnamurthy, “Cooperative diversity in wireless networks: efficient protocols and outage behaviour,” *IEEE Journal On Selected Areas in Communication*, 2007.
- [66] K. Jain, J. Padhye, V. Padmanabhan, and L. Qiu, “Impact of interference on multi-hop wireless network performance,” in *ACM MobiCom*, Sep 2003.
- [67] P. Gupta and P.R.Kumar, “The capacity of wireless networks,” *IEEE Transactions on information theory*, vol. 46, no. 2, pp. 388–404, Mar. 2000.
- [68] Tropos networks inc. [Online]. Available: <http://www.tropos.com>
- [69] H. Rahul, H. Hassanieh, and D. Katabi. SourceSync: A Distributed Wireless Architecture for Exploiting Sender Diversity. In *ACM SIGCOMM 2010*, August 2010.

- [70] Y. Sun, M. Uppal, A. Liveris, S. Cheng, V. Stankovic, and Z. Xiong. Nested turbo codes for the costa problem. *IEEE Transactions on Communications*, pages 388–399, 2008.
- [71] Y. Sun, Y. Yang, A. Liveris, V. Stankovic, and Z. Xiong. Near-capacity dirty-paper code design: A source-channel coding approach. *IEEE Transactions on Information Theory*, pages 3013–3031, 2009.
- [72] Q. Wang and C. He. Practical dirty paper coding with nested binary ldgm-ldpc codes. In *IEEE ICC*, 2009.
- [73] U. Erez, S. Shamai, and R. Zamir. Capacity and lattice strategies for canceling known interference. *IEEE Transactions on Information Theory*, 51:3820–3833, 2005.
- [74] C. Ng, N. Jindal, A. Goldsmith, and U. Mitra. Capacity gain from two-transmitter and two receiver cooperation. *IEEE Transactions on Information Theory*, 53:3822–3827, 2007.
- [75] Z. Gao, Y. Chang, and M. A. Ingram, Synchronization for Cascaded Distributed MIMO Communications, MILCOM, San Jose, CA, November 2010.
- [76] H. Rahul, H. Hassanieh and D. Katabi, SourceSync: A Distributed Wireless Architecture for Exploiting Sender Diversity, ACM SIGCOMM, New Delhi, India, August 2010.
- [77] A. Kailas and M. A. Ingram, Alternating Opportunistic Large Arrays in Broadcasting for Network Lifetime Extension, *IEEE Transactions on Wireless Communication*, 8:2831–2835, June 2009.



- [78] L. V. Thanayankizil and M.A. Ingram, Reactive robust routing with opportunistic large arrays, IEEE International Conference on Communications (ICC), June 2009.
- [79] J.W.Jung and M.A. Ingram, Residual-Energy-Activated Cooperative Transmission (REACT) to Avoid the Energy Hole, Proceedings IEEE International Conference on Communications (ICC) Workshop on Cooperative and Cognitive Mobile Networks (CoCoNet3), May 2010.

## VITA

Sriram Lakshmanan was born in Palayamkottai, a small town in the south Indian state of Tamilnadu. He went to school in Chennai, the capital of Tamilnadu. He received his Bachelor of Engineering degree in Electronics and Communication from the College of Engineering at Guindy, Anna University in 2005.

From Fall 2005, he was a doctoral student in the Electrical and Computer Engineering department at the Georgia Institute of Technology working under Prof. Raghupathy Sivakumar. His research focus was on networked wireless systems that leverage smart antennas and cooperative communication. His thesis research builds algorithms and systems for several networking problems including achieving spatial security, improving capacity of interfered links and achieving scalable multi-hop routing in wireless networks.

Sriram received his M.S. degree in Electrical and Computer Engineering from the Georgia Institute of Technology in 2007. During internships at Ruckus Wireless, NEC Laboratories and Hewlett Packard Laboratories, he has worked on various high-performance networked wireless systems. His work on wireless security has won awards at the Cyber Security Awareness Week 2009 held at New York University and at the Georgia Tech Graduate Technical Symposium 2010. He has been a reviewer for the IEEE Transactions on Mobile Computing, the IEEE Transactions on Parallel and Distributed Systems, the Springer Wireless Networks journal and the Elsevier Computer Networks journal. His works at Georgia Tech. and at NEC have lead to multiple patents in wireless networking.

In his spare time, Sriram likes to listen to Indian classical music. He also likes to play Tennis and Volleyball.