INDIAN INSTITUTE OF TECHNOLOGY BOMBAY

Referee's Evaluation Report on Ph.D. Thesis

Name of the Candidate:	Mr. Iyer Krishnamoorthy Vasudevan
Department :	Electrical Engineering
Title of Thesis :	Distributed Systems for Multiple Access and Relay Broadcast under Secrecy
Name of Referee & Address :	Prof. Sumit Kundu Professor, Department of ECE, NIT Durgapur, Durgapur-713209. Phone: (+91) 9434788127

SECTION A
(Referee's Overall Recommendation)

	Recommendation of the Referee	Mark (√) in the appropriate box
(a)	The thesis be accepted.	√
(b)	The thesis be accepted after clarification of the minor points listed in my report, at the time of viva-voce.	
(c)	The thesis be accepted after minor modifications in the thesis, as suggested in my report. The thesis need not be referred to an external referee again.*	
(d)	The thesis requires major revisions. The nature of the revisions are indicated in my report. It is recommended that the revised thesis be examined again by an external referee.	
(e)	The thesis is rejected.	

Section B (Referee's Detailed Comments) : Please provide the following as an attachment.

1. General comments on the thesis, including a critical survey and evaluation of the quality and quantity of the work reported in thesis.
2. Points which require clarification, and suggested amendments or revisions (if any).
3. Questions to be asked at the time of the viva voce.
4. 4. If the thesis is recommended for an IIT-Bombay "Best Thesis Award", please provide suitable justification. You may base your recommendation on a comparison with other thesis in a similar area, with which you are familiar.

Date: 16/05/18 Referee's Signature: Sumit Kundu

Dr. Sumit Kundu
Professor
Department of Electronics & Communication Engg.
National Institute of Technology Durgapur
Durgapur - 713209, India

NATIONAL INSTITUTE OF TECHNOLOGY DURGAPUR

MAHATMA GANDHI AVENUE, DURGAPUR-713209, WEST BENGAL, INDIA

Website : www.nitdgp.ac.in, E-mail : sumit.kundu@ece.nitdgp.ac.in / sumitkundu@yahoo.com

Tel. + 91 343 2754385 (O), Mob + 91 9434788127, + 91 9232668406, Fax + 91 343 2547375

Dr. Sumit Kundu

PhD (IIT KGP), SMIEEE

Professor

Dept. of Electronics & Communication Engineering

Report on PhD Thesis "Distributed Systems for Multiple Access and Relay Broadcast under Secrecy" submitted by Krishnamoorthy Iyer

Reviewer: Prof. Sumit Kundu

The present thesis investigates communication rates and schemes for some fundamental wireless network model such as Multiple Access Channel (MAC), broadcast channel (BC) and Relay channel (RC) which are commonly and widely employed in distributed networks.

More precisely, a distributed MAC, two receiver broadcast channel, Relay eavesdropper channel and Relay broadcast channel under mutual secrecy are studied respectively from information theory perspective under four contributory chapters.

The thesis has four contributory chapters with one Introductory Chapter.

Chapter wise reviews are given below:

Chapter 1 presents a compact but useful literature review on concepts of relay broadcast channel, sliding window decoding, Compress and forward relay and relay eavesdropper channel. Proper linking with literature reviewed and problem solved in subsequent chapters is nicely established. Critical remarks and justifications are made regarding choice of relaying schemes and derivation of bounds, choice of sliding window decoding is compared to backward decoding.

Chapter 2 discusses power controlled adaptive sum capacity of popular fading MAC channel considering identical statistics across the users and distributed CSI. A novel rate allocation policy "alpha midpoint" strategy for Gaussian multiple access block fading channel is introduced which achieves the power controlled adaptive sum capacity under a water filling power allocation. A novel low complexity optimal rate splitting successive decoding scheme is also proposed and shown to achieve near optimal rate. The proposed schemes are shown to achieve better performance over conventional centralized scheduling scheme, saving the overhead of coordination. Further, the superiority is demonstrated with an example of Fading W channel. The proposed midpoint scheme is shown to outperform conventional TDMA in terms of sum rate which is demonstrated for a Fading W channel.

In Chapter-3, a discrete memoryless channel (DM-BC) with two receivers is studied where the transmitter sends separate messages to each receiver maintaining secrecy from each other. An inner bound as well as an outer bound for the problem is provided. A novel encoding scheme using one-time pad (OTP) in common sequence is proposed. Typically, four achievable schemes are proposed which use melding of double random binding and code based on multiple key dependent code books, double encryption on time sharing. Code construction, encoding, decoding schemes of all cases are presented with detail mathematics and error probability analysis. Several important lemmas are stated and proved. Inner bound and outer bounds are stated with necessary mathematical proofs under different scenarios.

Sumit Kundu

Dr. Sumit Kundu 6/05/18
Professor
Department of Electronics & Communication Engg.
National Institute of Technology Durgapur
Durgapur - 713209, India

NATIONAL INSTITUTE OF TECHNOLOGY DURGAPUR

MAHATMA GANDHI AVENUE, DURGAPUR-713209, WEST BENGAL, INDIA

Website : www.nitdgp.ac.in, E-mail : sumit.kundu@ece.nitdgp.ac.in / sumitkundu@yahoo.com

Tel. + 91 343 2754385 (O), Mob. + 91 9434788127, + 91 9232668406, Fax. + 91 343 2547375

Dr. Sumit Kundu

PhD (IIT KGP), SMIEEE

Professor

Dept. of Electronics & Communication Engineering

Chapter-4, investigates a DF relay based wiretap channel in presence of an eavesdropper. An achievable scheme using a multi-block encoding and sliding window based forward decoding is analysed in contrast to existing regular encoding and backward decoding. The proposed scheme incurs less decoding delay while achieving same rate.

Achievable rate, probability of decoding error are analysed with detail and necessary mathematical formulation. Bounds on equivocation is calculated using an exhaustive mathematical derivation. The secrecy requirement at Eve is shown to be satisfying.

In Chapter-5, a Relay broadcast channel is analysed under mutual secrecy requirements for a four node network. A novel achievable scheme is presented to simultaneously assist in creating mutual secrecy between two receivers using a block Markov encoding and sliding window decoding which is an important contribution. Several new theorems, Lemmas are proposed and proved in context of deriving rate region, probability of encoding and decoding error calculation. Further rigorous mathematics have been done towards equivocation calculation and bounds are calculated.

Several new and challenging problems are also highlighted as future work such as avoiding conventional Noise Forwarding (NF) step for scenarios of week relay in relay eavesdropper channel. A novel idea of combining peeling off of the transmitted code words with compress and forward for the scenario of Relay broadcast channel where relay is weak with respect to one receiver is indicated. Multiple relays with all relays trusted by both the destination, maintaining a constraint on mutual secrecy is hinted as another problem.

Good level of publications based on the thesis such as [61,62,63,64,65] are noted.

However, the following points may be noted:

Section 2.8 talks of a current paper. Either the paper ref no. is to be given or the presentation mode should be changed from paper to thesis. The author says "the paper is organized as follows" in Introduction section of Chapter-3 to describe the chapter organization, which should perhaps be 'thesis' instead of 'paper'. Such mistakes are found in other places also, e.g. Chapter -2. In Chapter-5, as the author says that their achievable scheme uses elements from mode of [73,66,77] , a comparison of their scheme with any of these would have been of interest. A separate list of publication of author based on the thesis is desired.

The thesis is an excellent piece of work with significant novel contribution, detail mathematical treatment and provides many interesting and novel results on the topic explored. Several new theorems and lemmas are proposed and proved. **The contribution is sufficient and satisfies the requirement for award of PhD degree.**

Sumit Kundu

Prof. Sumit Kundu 16/05/18
Professor, ECE Dept
NIT Durgapur

Dr. Sumit Kundu
Professor
Department of Electronics & Communication Engg.
National Institute of Technology Durgapur
Durgapur - 713209, India

INDIAN INSTITUTE OF TECHNOLOGY BOMBAY

Referee's Evaluation Report on Ph.D. Thesis

Name of the Candidate: Mr. Iyer Krishnamoorthy Vasudevan

Department : Electrical Engineering

Title of Thesis : Distributed Systems for Multiple Access and Relay Broadcast under Secrecy

Name of Referee & Address : Prof. Andrew Thangaraj
Professor, Electrical Engineering Department, IIT Madras, Chennai-600036. Phone: (+91) 9940489032

SECTION A
(Referee's Overall Recommendation)

	Recommendation of the Referee	Mark (√)) in the appropriate box
(a)	The thesis be accepted.	
(b)	The thesis be accepted after clarification of the minor points listed in my report, at the time of viva-voce.	X
(c)	The thesis be accepted after minor modifications in the thesis, as suggested in my report. The thesis need not be referred to an external referee again.*	
(d)	The thesis requires major revisions. The nature of the revisions are indicated in my report. It is recommended that the revised thesis be examined again by an external referee.	
(e)	The thesis is rejected.	

Section B (Referee's Detailed Comments) : Please provide the following as an attachment.

1. General comments on the thesis, including a critical survey and evaluation of the quality and quantity of the work reported in thesis.
2. Points which require clarification, and suggested amendments or revisions (if any).
3. Questions to be asked at the time of the viva voce.
4. 4. If the thesis is recommended for an IIT-Bombay "Best Thesis Award", please provide suitable justification . You may base your recommendation on a comparison with other thesis in a similar area, with which you are familiar.

Date: May 10, 2018 Referee's Signature: ___

SECTION B
(Referee's Detailed Comments)

Name of the Candidate : Mr. Iyer Krishnamoorthy Vasudevan

Referee's Name : Prof. Andrew Thangaraj

Detailed Comments :

This thesis is mainly concerned with multiterminal communication problems from an information-theoretic point of view. Several interesting situations have been considered - distributed settings, secrecy settings, relay settings. The main agenda is computing bounds on achievable rates. The overall quality of the work is acceptable as a PhD thesis. I do not have any major comments. I have added a few questions on the content of the individual chapters below:

Chapter 2: This chapter is concerned with sum capacity of a MAC under the assumption of distributed CSI. I found this chapter to be very interesting and the results have wide utility in operational scenarios. Can the author comment on the multi-antenna setting for the same problem?

Chapter 3: This chapter is concerned with broadcast channels with a secrecy requirement. The interesting twist is the presence of secret keys. There are a lot of derivations in this chapter. I would have liked to see a rate region plot that brings out the difference because of the shared key.

Chapter 4: This chapter is concerned with yet another model where there is a relay eavesdropper and secrecy requirements. This is a problem primarily of theoretical interest. Once again, will it be possible to include rate vs secrecy plots?

Chapter 5: The final chapter combines the previous two chapters to consider a relay scenario in a broadcast channel with secrecy. The scenario itself is more abstract now. However, my repeated requirement of a rate region vs. secrecy plot will be interesting to see.

The writing overall is very good, and I could understand most of the arguments that I read well. Though I did not check all the derivations closely, I have high confidence that they are correct.

Referee's Signature: _

(Please provide your signature on each additional sheets)