PHYSICAL LAYER SECURITY IN ENERGY HARVESTING COOPERATIVE NETWORKS

KIRTI KANT SHARMA

BHARTI SCHOOL OF TELECOMMUNICATION
TECHNOLOGY AND MANAGEMENT
INDIAN INSTITUTE OF TECHNOLOGY DELHI

JULY 2023

© Indian Institute of Technology Delhi (IITD), New Delhi, 2023

PHYSICAL LAYER SECURITY IN ENERGY HARVESTING COOPERATIVE NETWORKS

by

KIRTI KANT SHARMA

BHARTI SCHOOL OF TELECOMMUNICATION
TECHNOLOGY AND MANAGEMENT

Submitted
in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

JULY 2023

Dedicated to

Maa and Papa

Certificate

This is to certify that the thesis entitled **"Physical Layer Security in Energy Harvesting Cooperative Networks"** being submitted by **Mr. Kirti Kant Sharma** to the Bharti School Of Telecommunication Technology And Management, Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy** is the record of bonafide research work carried out by him under my supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted either in part or in full to any other University or Institute for the award of any degree or diploma.

Dr. Ranjan Bose
Professor
Department of Electrical Engineering
Indian Institute of Technology Delhi
Hauz Khas, New Delhi, 110016, India

Date:
Place: New Delhi

Acknowledgements

First of all, I express my gratitude to my supervisor, **Prof. Ranjan Bose**, for taking me under his guidance and constantly supporting me during all the years of my Ph.D. He has always kept motivating me in the ups and downs of these years. He has been thoughtful in allowing me to handle my research work with ease. This entire process contributed immensely to my self-development, for which I will always be grateful to my supervisor.

I wish to express my gratitude to my research committee members Prof. Shankar Prakriya, Prof. Saif K. Mohammed, and Prof. Kolin Paul, for their helpful criticism and feedback during this period. A special thanks to Prof. Seshan Srirangarajan for being my caretaker supervisor and providing easy transit with institutional operations. Most importantly, I wish to thank Dr. Sonam Jain and Dr. Sasi Vinay Pechetti for their informative discussions and consistent help. I also want to thank my senior Dr. Sandeep Kumar Singh, and lab friends Ms. Srishti Kulshrestha and Ms. Monika Rajan.

Finally, and most significantly, I want to express my gratitude to my parents and family members for being continuous, selfless supporters always in my life.

Kirti Kant Sharma

Abstract

Telecommunication networks of the future will connect a vast number of heterogeneous devices wirelessly in the Internet of Things and machine-to-machine communications. Most of these applications require devices with a small size, low cost, and low energy consumption. Energy harvesting mechanisms will be a recommended feature in some of these devices due to the difficulty of charging and battery replacement due to device location and economic feasibility. Secure communications and energy efficiency for this large number of resource-limited devices are crucial due to the broadcast nature of the wireless medium and the severe repercussions of information leakage. Usually, cryptographic techniques are used for information security while assuming that the decryption will be difficult and take longer for an intruder without knowing secret keys. These schemes have challenges regarding key management, and the reliance on the eavesdropper's limited computing capabilities. Physical layer security techniques have been proposed as a low-complexity alternative for secure communications by utilizing the inherent random characteristics of wireless channels. These physical layer security techniques employ multiple antennas, carriers, artificial noise, and node cooperation to secure information transfer.

In this thesis, we first study the cost of secure transmission in terms of secure energy efficiency with relaying and jamming. We consider two cooperative scenarios in wireless networks to analyze secure energy efficiency. We propose a simple relay and jammer selection scheme for a decode-and-forward relaying network with friendly jamming in the first problem. Here, we study power allocation among selected nodes considering global channel state information to maximize secure energy efficiency. It is observed that the friendly jammer can improve energy efficiency with security compared to the relay-only

scheme. In the second scenario, we analyze the secure energy efficiency of a direct link in the presence of an unknown eavesdropper with the help of multiple spatially-distributed friendly jammers. We propose a practical uncoordinated cooperative jamming with less system overhead. Jammers are selected according to the source-to-destination channel quality within a finite region surrounding the source to limit energy consumption. We have considered a more realistic power consumption model with the transmit power of various nodes as well as their circuit consumption power. This analysis shows that some optimal value of selection parameters exists at which secure energy efficiency achieves maximum value.

Next, we analyze the importance of RF energy harvesting in cases of using a jammer and then an incremental relay to improve secrecy performance without the knowledge of the eavesdropper's channel state information. In these cases, we first utilize an RF energy harvesting cooperative jammer and analyze secrecy improvement in the presence of an unknown passive eavesdropper. By considering artificial noise transmission from a friendly multiantenna jammer with finite and infinite energy storage, the analytical expressions for secrecy outage probability are obtained considering the finite and infinite size energy buffer. This analysis shows that always-on jamming performs better than on-off jamming for the same buffer size. Results show the existence of an optimal secrecy rate to maximize secure throughput for a given source SNR. It is observed that the availability of jamming power has a more pronounced effect on secrecy outage than a larger number of antennas at the jammer. Further, we study the improvement in secrecy using a self-sustainable incremental relay and transmit antenna selection at both source and relay to reduce the feedback overhead. We propose a threshold-based incremental relaying scheme while considering both the direct and relaying links to the destination and eavesdropper. We have also considered the effect of outdated channel state information on secrecy performance. We model the energy present in the buffer as a discrete-time discrete-state Markov chain and derive a closed-form expression for secrecy outage probability. This analysis shows that the proposed scheme performs better than direct communication and conventional decode-and-forward relaying. Results show that secrecy performance can be further improved by choosing a proper value of the signal-to-noise ratio and energy threshold for relaying. These analyses show the adequacy of a finite buffer for RF energy harvesting at the cooperative node.

सार

भविष्य के दूरसंचार नेटवर्क इंटरनेट ऑफ थिंग्स और मशीन-टू-मशीन संचार में बड़ी संख्या में विविध उपकरणों को वायरलेस तरीके से जोड़ देंगे। इनमें से अधिकांश अनुप्रयोगों के लिए छोटे आकार, कम लागत और कम ऊर्जा खपत वाले उपकरणों की आवश्यकता होती है। डिवाइस के स्थान और आर्थिक व्यवहार्यता के कारण चार्जिंग और बैटरी प्रतिस्थापन की कठिनाई के कारण इनमें से कुछ उपकरणों में ऊर्जा संचयन तंत्र एक अनुशंसित सुविधा होगी। वायरलेस माध्यम की प्रसारण प्रकृति और सूचना रिसाव के गंभीर नतीजों के कारण बड़ी संख्या में संसाधन-सीमित उपकरणों के लिए सुरक्षित संचार और ऊर्जा दक्षता महत्वपूर्ण हैं। आमतौर पर, क्रिप्टोग्राफ़िक तकनीकों का उपयोग सूचना सुरक्षा के लिए किया जाता है, जबकि यह मानते हुए कि गुप्त कुंजियों को जाने बिना घुसपैठिए के लिए डिक्रिप्शन कठिन होगा और इसमें अधिक समय लगेगा। इन योजनाओं में प्रमुख प्रबंधन और गुप्तचर की सीमित कंप्यूटिंग क्षमताओं पर निर्भरता के संबंध में चुनौतियाँ हैं। वायरलेस चैनलों की अंतर्निहित यादृच्छिक विशेषताओं का उपयोग करके सुरक्षित संचार के लिए भौतिक परत सुरक्षा तकनीकों को कम जटिलता वाले विकल्प के रूप में प्रस्तावित किया गया है। ये भौतिक परत सुरक्षा तकनीकें सूचना हस्तांतरण को सुरक्षित करने के लिए कई एंटेना, वाहक, कृत्रिम नॉइज़ और नोड सहयोग का उपयोग करती हैं।

इस थीसिस में, हम सबसे पहले रिलेइंग और जैमिंग के साथ सुरक्षित ऊर्जा दक्षता के संदर्भ में सुरक्षित ट्रांसमिशन की लागत का अध्ययन करते हैं। सुरक्षित ऊर्जा दक्षता का विश्लेषण करने के लिए हम वायरलेस नेटवर्क में दो सहयोगी परिदृश्यों पर विचार करते हैं। हम पहली समस्या में अनुकूल जैमिंग के साथ डिकोड-एंड-फॉरवर्ड रिलेइंग नेटवर्क के लिए एक सरल रिले और जैमर चयन योजना का प्रस्ताव करते हैं। यहां, हम सुरक्षित ऊर्जा दक्षता को अधिकतम करने के लिए वैश्विक चैनल स्थिति की जानकारी पर विचार करते हुए चयनित नोड्स के बीच ऊर्जा आवंटन का अध्ययन करते हैं। यह देखा गया है कि रिले-ओनली स्कीम की तुलना में फ्रेंडली जैमर सुरक्षा के साथ ऊर्जा दक्षता में सुधार कर सकता है। दूसरे परिदृश्य में, हम कई स्थानिक रूप से वितरित मैत्रीपूर्ण जैमर की सहायता से एक अज्ञात गुप्तचर की उपस्थिति में एक सीधे लिंक की सुरक्षित ऊर्जा दक्षता का विश्लेषण करते हैं। हम कम सिस्टम ओवरहेड के साथ एक व्यावहारिक असंगठित सहकारी जैमिंग का प्रस्ताव करते हैं। ऊर्जा खपत को सीमित करने के लिए स्रोत के आसपास के एक सीमित क्षेत्र के भीतर स्रोत-से-गंतव्य चैनल की गुणवत्ता के अनुसार जैमर का चयन किया जाता है। हमने विभिन्न नोड्स की संचारित शक्ति के साथ-साथ उनकी सर्किट खपत शक्ति के साथ अधिक यथार्थवादी ऊर्जा खपत मॉडल पर विचार किया

है। इस विश्लेषण से पता चलता है कि चयन मापदंडों के कुछ इष्टतम मूल्य मौजूद हैं जिन पर सुरक्षित ऊर्जा दक्षता अधिकतम मूल्य प्राप्त करती है।

इसके बाद, हम एक जैमर का उपयोग करने के मामलों में आर एफ ऊर्जा संचयन के महत्व का विश्लेषण करते हैं और फिर ईव्सड्रॉपर के चैनल की स्थिति की जानकारी के बिना गोपनीयता प्रदर्शन में सुधार करने के लिए एक वृद्धिशील रिले का उपयोग करते हैं। इन मामलों में, हम पहले एक आरएफ ऊर्जा संचयन सहकारी जैमर का उपयोग करते हैं और एक अज्ञात निष्क्रिय ईव्सड्रॉपर की उपस्थिति में गोपनीयता सुधार का विश्लेषण करते हैं। परिमित और अनंत ऊर्जा भंडारण के साथ एक अनुकूल मल्टीएंटीना जैमर से कृत्रिम शोर संचरण पर विचार करके, परिमित और अनंत आकार के ऊर्जा बफर पर विचार करते हुए गोपनीयता आउटेज संभावना के लिए विश्लेषणात्मक अभिव्यक्ति प्राप्त की जाती है। इस विश्लेषण से पता चलता है कि समान बफ़र आकार के लिए ऑलवेज-ऑन जैमिंग, ऑन-ऑफ जैमिंग से बेहतर प्रदर्शन करती है। परिणाम किसी दिए गए स्रोत एसएनआर के लिए सुरक्षित थ्रूपुट को अधिकतम करने के लिए एक इष्टतम गोपनीयता दर के अस्तित्व को दर्शाते हैं। यह देखा गया है कि जैमर पर बड़ी संख्या में एंटेना की तुलना में जैमिंग पावर की उपलब्धता का गोपनीयता आउटेज पर अधिक स्पष्ट प्रभाव पड़ता है। इसके अलावा, हम एक स्व-टिकाऊ वृद्धिशील रिले का उपयोग करके गोपनीयता में सुधार का अध्ययन करते हैं और फीडबैक ओवरहेड को कम करने के लिए स्रोत और रिले दोनों पर एंटीना चयन प्रसारित करते हैं। हम गंतव्य और ईव्सड्रॉपर के लिए सीधे और रिलेइंग लिंक दोनों पर विचार करते हुए एक सीमा-आधारित वृद्धिशील रिलेइंग योजना का प्रस्ताव करते हैं। हमने गोपनीयता प्रदर्शन पर पुरानी चैनल स्थिति जानकारी के प्रभाव पर भी विचार किया है। हम बफर में मौजूद ऊर्जा को असतत-समय असतत-अवस्था मार्कोव श्रृंखला के रूप में मॉडल करते हैं और गोपनीयता आउटेज संभावना के लिए एक बंद-रूप अभिव्यक्ति प्राप्त करते हैं। इस विश्लेषण से पता चलता है कि प्रस्तावित योजना प्रत्यक्ष संचार और पारंपरिक डिकोड-एंड-फॉरवर्ड रिलेइंग से बेहतर प्रदर्शन करती है। नतीजे बताते हैं कि सिग्नल-टू-नॉइज़ अनुपात और रिलेइंग के लिए ऊर्जा सीमा का उचित मूल्य चुनकर गोपनीयता प्रदर्शन में और सुधार किया जा सकता है। ये विश्लेषण सहकारी नोड पर आर एफ ऊर्जा संचयन के लिए एक सीमित बफर की पर्याप्तता दिखाते हैं।

Contents

Certificate **i**

Acknowledgements **ii**

Abstract **iii**

List of Figures **viii**

List of Tables **xi**

List of Abbreviations **xii**

1 Introduction **1**

1.1 Background 1

1.2 Security in Wireless Communications 2

1.3 Physical Layer Security 3

1.4 Cooperative Communications 6

1.5 Energy Conservation and RF Energy Harvesting 7

1.6 Motivation and Thesis Organization 8

2 Literature Review **11**

2.1 Artificial Noise and Cooperative Jamming 11

2.2 Cooperative Relaying 13

2.3 Secure Energy Efficiency and RF Energy Harvesting 14

2.4 Thesis Objectives 16

3 Regulating the Energy Consumption **17**

3.1 Jammer Assisted Secure Energy Efficiency Maximization in Decode-and-Forward Relay Network 18

3.1.1 Motivation and Problem Description 18

3.1.2 System Model 19

3.1.3 SEE Problem Formulation 22

3.1.4 SEE Maximization Scheme 23

3.1.5 Simulation Results 28

3.2 Secure Energy Efficiency with Poisson Point Process Distributed Jammers 31

3.2.1 Motivation and Problem Description 31

3.2.2 System Model 33

3.2.3 Distance Distribution 36

3.2.4 Secrecy Performance Analysis 37

3.2.5 Simulation Results 39

3.3 Applications to Wireless Sensor Networks for Smart Infrastructures . . 42

3.4 Summary 43

4 Secure Communication with Energy-Harvesting Buffer-Aided Jammer 44

4.1 Motivation and Problem Description 45

4.2 System Model 48

4.3 Secrecy Performance Analysis 51

4.4 Simulation Results 60

4.5 EH-based Cooperative Jamming in Practical Networks 65

4.6 Summary 66

5 Secure Communication with Buffer-aided Energy-Harvesting Incremental Relay 68

5.1 Motivation and Problem Description 69

5.2 System Model 72

5.3 Markov Model of Energy Buffer at Relay 79

5.4 Secrecy Performance Analysis 82

5.5 Simulation Results 88

5.6 Information Security in Future Wireless Networks 95

5.7 Summary 96

6 Conclusions and Future Work **97**

6.1 Summary of the Contributions 97

6.2 Scope of Future Work 99

Bibliography **100**

Appendices **109**

A Proofs for Chapter 5 **110**

A.1 Evaluation of $P_r\{\mathcal{E}_1\}$ 110

A.2 Evaluation of $P_r\{\mathcal{E}_2\}$ and $P_r\{\mathcal{E}_3\}$ 111

A.3 Evaluation of $P_r\{\mathcal{E}_4\}$ 112

List of Publications **114**

Technical Biography of Author **115**

List of Figures

1.1 Wyner's wiretap model [3] 4

3.1 System model 19

3.2 Average SEE versus d_{sr}: $R_o = 1\ bit/s/Hz$. 29

3.3 Average SEE versus d_{se}: $R_o = 1\ bit/s/Hz$. 30

3.4 System model 34

3.5 Geometrical cases for $f_R(r)$ 36

3.6 The coverage probability P_{cov} and secure communication probability P_{sec} as a function of R_w 40

3.7 The coverage probability P_{cov} and secure communication probability P_{sec} as a function of ϵ 40

3.8 The SEE as a function of (a) R_w and (b) ϵ 41

4.1 Secure communication with EH jammer 48

4.2 Secrecy outage probability vs. δ for $\frac{1}{\lambda} = -20$ dB, $M = 2, 4, 8, \infty$, and $N_{\mathrm{j}} = 4$ 61

4.3 Secrecy outage probability vs. source SNR P_{s}/σ^2 for $M = 2, 4, 8, \infty$, and $N_{\mathrm{j}} = 4$ 62

4.4 Secrecy outage probability Throughput vs. source SNR P_{s}/σ^2 for $\frac{1}{\lambda} = -10$ dB, $M = 8, \infty$, and $N_{\mathrm{j}} = 4$ 62

4.5 Secrecy outage probability vs. source SNR P_{s}/σ^2 for $\frac{1}{\lambda} = -20$ dB, $M = 8, \infty$ and $N_{\mathrm{j}} = 2, 4, 6$ 63

4.6 Throughput vs. secrecy rate for $\frac{1}{\lambda} = -20$ dB, $M = 2, 4, 8, \infty$, and $N_{\mathrm{j}} = 4$ 64

4.7 Throughput vs. secrecy rate comparison of finite size buffer continuous-state space Markov model ($M = 8$) with the corresponding discrete-state Markov model ($L = 250$, 500) for $\frac{1}{\lambda} = -20$ dB, $N_{\mathrm{j}} = 4$ 64

5.1 Secure communication with EH relay 72

5.2 Secrecy outage probability vs γ_{sd} for $\gamma_\tau = 16$ dB, $\alpha = 0.2$ and $L = 200$, 500, 1500 88

5.3 Secrecy outage probability vs γ_{sd} for $\gamma_\tau = 12$, 14, 16 dB at $\gamma_{se} = 2$, 4 dB and $\alpha = 0.2$, ... 89

5.4 Secrecy outage probability vs γ_{sd} for $\gamma_\tau = 16$ dB, $\gamma_{se} = 2$, 4 dB and $\alpha = 0.15$, 0.2, 0.3 90

5.5 (a) Secrecy outage probability vs γ_τ for $\alpha = 0.2$, (b) Secrecy outage probability vs α for $\gamma_\tau = 16$, $\gamma_{sd} = 16$, 18 dB, $\gamma_{se} = 2$ dB, $\rho = 0.3, 0.7, 1$ 90

5.6 Secrecy outage probability vs γ_{sd} for $M = 2$, 4, 8, ∞ and powered relay at $\alpha = 0.2$ and $\gamma_{se} = 2$ dB 92

5.7 Secrecy outage probability vs γ_{sd} for $\gamma_\tau = 16$ dB, $\gamma_{se} = 2$ dB, $R_s = 1$ bps/Hz and $\rho = 0.3$, 0.7, 1 (channel error) 93

5.8 Secrecy outage probability vs γ_{sd} for (a) $N_s = 1, 2, 4$, (b) $N_r = 1, 2, 4$, (c) $N_d = 1, 2, 4$, (d) $N_e = 1, 2, 4$ 94

List of Tables

3.1 Simulation parameters 29

3.2 Simulation parameters 39

4.1 Simulation parameters 60

List of Abbreviations

AF	Amplify-and-forward
AN	Artificial noise
AO	Always-on
AWGN	Additive white Gaussian noise
CSI	Channel state information
DF	Decode-and-forward
EH	Energy harvesting
GSVD	Generalized singular value decomposition
HSU	Harvest, store, and use
IDF	Incremental decode-and-forward
IHDAF	Incremental hybrid decode-amplify-forward
IoT	Internet of Things
M2M	Machine-to-machine
MIMO	Multiple-input and multiple-output
MISO	Multiple-input and single-output
OCT	Opportunistic cooperative transmission
OFDMA	Orthogonal frequency division multiple access
OO	On-off
PLS	Physical layer security
PPP	Poisson point process
QoS	Quality of service
RF	Radio frequency
SDF	Selective decode-and-forward
SEE	Secure energy efficiency

SIMO	Single-input and multiple-output
SISO	Single-input and single-output
SNR	Signal-to-noise ratio
SOP	Secrecy outage probability
SWIPT	Simultaneous wireless information and power transfer
TAS	Transmit antenna selection
TEIR	TAS-based buffer-aided energy-harvesting incremental relaying
UCJ	Uncoordinated cooperative jamming
WC	Wireless charging
WPCCN	Wireless powered cooperative communication network
WSN	Wireless sensor networks