Lancaster University

Characterisation and Performance Analysis of Random Linear Network Coding for Reliable and Secure Communication

Author:

Amjad Saeed Khan

Supervisor:

Dr. Ioannis Chatzigeorgiou

A thesis submitted in partial fulfillment

for the degree of Doctor of Philosophy

Communication Systems Group

School of Computing and Communications

January 25, 2018

Declaration of Authorship

I, Amjad Saeed Khan, declare that this thesis titled, ‘Characterisation and Performance Analysis of Random Linear Network Coding for Reliable and Secure Communication’ and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: ____

Date: ____

Acknowledgements

First of all, I would like to thank Almighty God, the one, who bless me with the opportunity to pursue the journey towards a PhD.

I would like to express my sincere gratitude and very special thanks to Dr. Ioannis Chatzigeorgiou for being no less than a perfect supervisor I could ever possibly imagine. In fact, Ioannis has always impressed me by exceeding all my expectations. He is a real gentleman and excellent teacher: very supportive, encouraging, understanding, kind, sincere, honest and generous. Throughout my PhD, Ioannis was not only supporting me to improve my knowledge and writing expertise, but also seemed to have always a better thought and plan for my exposure and future development. Apart from the research, he has given me great advices from his life experience that added a lot of positivity in my personality, which is priceless to me. I will always be very grateful to Ioannis for making my graduate experience very productive, enjoyable and memorable.

I wish to thank the Lancaster University for their excellent resources. In particular, thanks to the School of Computing and Communications (InfoLab21) for providing the research environment and resources, and for their friendly and supporting faculty and staff members including: Prof. Zhiguo Ding, Prof. Qiang Ni, Vicky Waddington, Gillian Balderstone and Debbie Stubbs. Moreover, I am very grateful and thankful to the Faculty of Science and Technology (FST) for granting me a very precious PhD scholarship, and providing me support to attend the number of summer schools. The opportunity of studying in the Lancaster University will always be a remarkable experience in my life.

I specially thanks to my father and mother for their never-ending love, prayers, encouragements, support and showing confidence on me, without which it would be impossible for me to pursue my studies up to this stage. In addition, thanks to my sisters and brother for their love, prayers and encouragements throughout my studies. Furthermore, I wish to thank all my colleagues and sincere friends for helping me with their valuable discussions and guidance during my PhD. Last but not least, I would like to thank Andrew Wood and Elspeth Wood, the organizers of Friends International Lancaster, for beautifying my stay here at Lancaster, and for being a part of wonderful memories.

List of Publications

Most of the work documented in this thesis has been published or under preparation for publication in journals or conference proceedings, as listed below:

Journal

1. **A. S. Khan** and I. Chatzigeorgiou, "Non-Orthogonal Multiple Access Combined With Random Linear Network Coded Cooperation", IEEE Signal Processing Letters, vol. 24, no. 9, pp. 1298-1302, Sept. 2017.
2. **A. S. Khan** and I. Chatzigeorgiou, "Improved bounds on the decoding failure probability of linear NC over multi-source multi-relay networks", IEEE Communications Letters, vol. 20, no. 10, pp. 2035-2038, Oct. 2016.
3. **A. S. Khan**, A. Tassi and I. Chatzigeorgiou, "Rethinking the intercept probability of random linear network coding", IEEE Communications Letters, vol. 19, no. 10, pp. 1762-1765, October 2015.
4. **A. S. Khan** and I. Chatzigeorgiou, "Opportunistic relaying and random linear network coding for secure and reliable communication", IEEE Transactions on Wireless Communications, ***(accepted with minor revisions)***.
5. **A. S. Khan** and I. Chatzigeorgiou, "A Framework for the Analysis of Network-Coded Schemes Characterized by Random Block Matrices", IEEE Transactions on Wireless Communications, ***(in preparation)***.

Conference

1. **A. S. Khan** and I. Chatzigeorgiou, "Performance analysis of random linear network coding in two-source single-relay networks", in Proc. IEEE International Conference on Communications Workshops (ICC), Workshop on Cooperative and Cognitive Networks, London, United Kingdom, June 2015.

LANCASTER UNIVERSITY

Abstract

Faculty of Science and Technology
School of Computing and Communications

Doctor of Philosophy

Characterisation and Performance Analysis of Random Linear Network Coding for Reliable and Secure Communication

by Amjad Saeed Khan

In this thesis, we develop theoretical frameworks to characterize the performance of Random Linear Network Coding (RLNC), and propose novel communication schemes for the achievement of both reliability and security in wireless networks. In particular, (i) we present an analytical model to evaluate the performance of practical RLNC schemes suitable for low-complexity receivers, prioritized (i.e., layered) coding and multi-hop communications, (ii) investigate the performance of RLNC in relay assisted networks and propose a new cross-layer RLNC-aided cooperative scheme for reliable communication, (iii) characterize the secrecy feature of RLNC and propose a new physical-application layer security technique for the purpose of achieving security and reliability in multi-hope communications.

At first, we investigate random block matrices and derive mathematical expressions for the enumeration of full-rank matrices that contain blocks of random entries arranged in a diagonal, lower-triangular or tri-diagonal structure. The derived expressions are then used to model the probability that a receiver will successfully decode a source message or layers of a service, when RLNC based on non-overlapping, expanding or sliding generations is employed. Moreover, the design parameters of these schemes allow to adjust the desired decoding performance.

Next, we evaluate the performance of Random Linear Network Coded Cooperation (RLNCC) in relay assisted networks, and propose a cross-layer cooperative scheme which combines the emerging Non-Orthogonal Multiple Access (NOMA) technique and RLNCC. In this regard, we first consider the multiple-access relay channel in a setting where two source nodes transmit packets to a destination node, both directly and via a relay node. Secondly, we consider a multi-source multi-relay network, in which relay nodes employ RLNC on source packets and generate coded packets. For each network, we build our analysis on fundamental probability expressions for random matrices over finite fields and we derive theoretical expressions of the probability that the destination node will successfully decode the source packets. Finally, we consider a multi-relay network comprising of two groups of source nodes, where each group transmits packets to its own designated destination node over single-hop links and via a cluster of relay nodes shared by both groups. In an effort to boost reliability without sacrificing throughput, a scheme is proposed whereby packets at the relay nodes are combined using two methods; packets delivered by different groups are mixed using non-orthogonal multiple access principles, while packets originating from the same group are mixed using RLNC. An analytical framework that characterizes the performance of the proposed scheme is developed, and benchmarked against a counterpart scheme that is based on orthogonal multiple access.

Finally, we quantify and characterize the intrinsic security feature of RLNC and design a joint physical-application layer security technique. For this purpose, we first consider a network comprising a transmitter, which employs RLNC to encode a message, a legitimate receiver, and a passive eavesdropper. Closed-form analytical expressions are derived to evaluate the intercept probability of RLNC, and a resource allocation model is presented to further minimize the intercept probability. Afterward, we propose a joint RLNC and opportunistic relaying scheme in a multi relay network to transmit confidential data to a destination in the presence of an eavesdropper. Four relay selection protocols are studied covering a range of network capabilities, such as the availability of the eavesdropper's channel state information or the possibility to pair the selected relay with a jammer node that intentionally generates interference. For each case, expressions of the probability that a coded packet will not be decoded by a receiver, which can be either the destination or the eavesdropper, are derived. Based on those expressions, a framework is developed that characterizes the probability of the eavesdropper intercepting a sufficient number of coded packets and partially or fully decoding the confidential data. We observe that the field size over which RLNC is performed at the application layer as well as the adopted modulation and coding scheme at the physical layer can be modified to fine-tune the trade-off between security and reliability.

Contents

Declaration of Authorship **i**

Acknowledgements **ii**

List of Publications **iii**

Abstract **iv**

Contents **vii**

List of Figures **x**

Abbreviations **xiii**

1 Introduction **1**

1.1 Background and Motivations 1

1.2 Basic Examples of Network Coding 2

1.2.1 NC in a Butterfly Network 3

1.2.2 NC in a Wireless Network 4

1.3 Random Linear Network Coding 4

1.3.1 RLNC Encoding and Decoding 5

1.3.2 RLNC Example 6

1.3.3 RLNC Limitation and Literature Work 7

1.4 RLNC Applications 8

1.4.1 RLNC for Heterogeneous Devices and Broadcast Communication . 9

1.4.2 Random Linear Network Coded Cooperation 9

1.4.3 RLNC for Secure Communication 9

1.4.4 RLNC Integrated with Opportunistic Relaying and Intentional Jamming 10

1.5 Overview and Contributions of Thesis 12

1.5.1 Thesis Structure and Organization 13

2 A Framework for the Assessment of Network Coding Techniques Characterized by Random Block Matrices **16**

2.1 Fundamental Preliminary Expressions 17

2.2 Partitioning of Random Matrices . . . 18
2.3 Structures of Random Block Matrices . . . 20
2.3.1 Block Diagonal (BD) Matrices . . . 21
2.3.2 Block Lower-Triangular (BLT) Matrices . . . 22
2.3.3 Block Tri-Diagonal (BTD) Matrices . . . 23
2.4 Assessment of Network Coding Techniques . . . 26
2.4.1 Non-Overlapping Generations RLNC (NOG-RLNC) . . . 27
2.4.2 Expanding Generations RLNC (EG-RLNC) . . . 28
2.4.3 Sliding Generations RLNC (SG-RLNC) . . . 30
2.5 Results and Discussions . . . 31
2.5.1 Performance Comparison between NOG-RLNC, SG-RLNC and EG-RLNC over Non-erasure Channels . . . 32
2.5.2 Performance Comparison between SG-RLNC and EG-RLNC over Erasure Channels . . . 35
2.6 Summary . . . 36

3 Random Linear Network Coding for Coded Cooperation 38
3.1 Random Linear Network Coded Cooperation in Two Source Single Relay Networks . . . 39
3.1.1 System Model and Problem Statement . . . 39
3.1.2 Performance Analysis . . . 42
3.1.2.1 Preliminaries: fundamental probability expressions . . . 42
3.1.2.2 Decoding probability for non-systematic network coding . 43
3.1.2.3 Decoding probability for systematic network coding . . . 45
3.1.3 Results and Discussions . . . 47
3.2 Random Linear Network Coded Cooperation in Multi-source Multi-relay Networks . . . 49
3.2.1 System Model . . . 49
3.2.2 Preliminary Results and Former Bounds on the Probability of Decoding Failure . . . 50
3.2.3 Improved Bounds on the Probability of Decoding Failure . . . 52
3.2.3.1 Upper bound . . . 52
3.2.3.2 Lower bound . . . 54
3.2.4 Results and Discussions . . . 54
3.3 Random Linear Network Coded Cooperation Combined with Non-Orthogonal Multiple Access . . . 57
3.3.1 System Model . . . 57
3.3.2 Achievable Rate and Link Outage Probability . . . 59
3.3.3 Decoding Probability and Analysis . . . 61
3.3.4 Results and Discussions . . . 63
3.4 Summary . . . 65

4 Random Linear Network Coding for Secure Communication 67
4.1 The Intercept Probability of RLNC . . . 68
4.1.1 System Model . . . 69
4.1.2 Performance Analysis . . . 69
4.1.3 Optimization Model . . . 72
4.1.4 Results and Discussions . . . 73

4.2 Opportunistic Relaying and RLNC for Secure and Reliable Communication 75
4.2.1 System Model 75
4.2.2 Relay Selection and Outage Analysis 78
4.2.2.1 Relay selection protocols without jammer 79
4.2.2.2 Relay selection protocols with jammer 82
4.2.3 Secrecy Analysis 87
4.2.3.1 Preliminaries 87
4.2.3.2 Derivation of the τ-intercept probability 88
4.2.4 Results and Discussions 90
4.3 Summary 96

5 Conclusions and Future Research Directions 97
5.1 Summary and Conclusions of the Thesis 97
5.2 Future Directions 98

A Analytical proof of Lemma 2.1 100

B Reformulation of the intercept probability of FT 101

C Proof of Proposition 4.2 for the case of FT 102

Bibliography 103

List of Figures

1.1 Example of network coding in wired network 3

1.2 Example of network coding in wireless network 4

1.3 Structure of transmitted coded packet 6

1.4 Example of RLNC in multi-path network 6

1.5 Applications of RLNC 8

1.6 Thesis Flowchart 13

2.1 Examples of 25×20 random block matrices, which have been constructed by vertically concatenating three matrices. Random elements are depicted by '■', while zero-valued entries are represented by '□'. 21

2.2 Example of NOG-RLNC. The source packets $x_1, \ldots, x_m$ have been organized into L generations $\mathbf{G}_1, \ldots, \mathbf{G}_L$. Generation $\mathbf{G}_i$ contains k_i source packets. 28

2.3 Example of EG-RLNC. Each generation $\mathbf{G}_i$ is nested in generation $\mathbf{G}_{i+1}$. The number of source packets that belong to a generation $\mathbf{G}_i$ but not to lower-indexed generations is denoted by m_i. 29

2.4 Example of SG-RLNC. The m source packets are members of L contiguous generations $\mathbf{G}_1, \ldots, \mathbf{G}_L$. For $i > 1$, generations $\mathbf{G}_{i-1}$ and $\mathbf{G}_i$ have w_{i-1} source packets in common. 30

2.5 Comparison between theoretical results for SG-RLNC obtained from (2.25) and simulation results for $L = 2$ generations and different values of $\hat{n}_2$. The remaining parameters have been set as follows: $q = 2$, $m = 20$, $m_1 = m_2 = 10$, $n_1 = \hat{n}_1 = 10$, $n_2 = \hat{n}_2$ and $\epsilon = 0$. 32

2.6 Comparison between NOG-RLNC, SG-RLNC and EG-RLNC for $L = 3$, $m = 60$, $m_1 = m_2 = m_3 = 20$, $\hat{n}_1 = \hat{n}_2 = 20$ and $\hat{n}_3 = 20 + \delta_3$. Various percentages of overlap in the case of SG-RLNC have been considered. Furthermore, $n_i = \hat{n}_i$ for all values of i, $q = 2$ and $\epsilon = 0$. 33

2.7 Comparison between NOG-RLNC, SG-RLNC and EG-RLNC for $L = 3$, $m = 60$, $m_1 = m_2 = m_3 = 20$, $\hat{n}_1 = \hat{n}_2 = \hat{n}_3 = 20 + \kappa$, where κ represents overhead per generation. In addition, $q = 2$, $\epsilon = 0$ and the overlap in SG-RLNC is set to 9% 33

2.8 Theoretical predictions and simulation results for SG-RLNC and EG-RLNC, when the field size q is 2, 3, 5 or 7. The system parameters are $L = 3$, $m = 60$, $m_1 = m_2 = m_3 = 20$, $n_1 = \hat{n}_1 = 20$, $n_2 = \hat{n}_2 = 20$ and $\epsilon = 0$. The overlap in SG-RLNC is fixed at 9%. 34

2.9 Effect of the field size q on the decoding probability of SG-RLNC and EG-RLNC for $L = 3$, $m = 60$, $m_1 = m_2 = m_3 = 20$ and $\epsilon = 0.2$. If the overhead per generation is $\kappa = 0, 1, \ldots, 15$, the overall overhead is $\delta = 3\kappa$, i.e., $\delta = 0, 3, \ldots, 45$. 34

2.10 Performance comparison between SG-RLNC and EG-RLNC for $m = 60$, $m_1 = m_2 = m_3 = 20$, $n_1 = n_2 = 26$, $\epsilon \in \{0.1, 0.2, 0.3, 0.4\}$ and $q = 256$. Various percentages of overlap for SG-RLNC have been considered. 35

3.1 Block diagram of a network consisting of two source nodes S_1 and S_2, a relay node R and a destination node D. The packet erasure probability of each link as well as the number of transmitted and received coded packets at each node are also depicted. 41

3.2 Comparison between theoretical upper bounds obtained from (3.12) and simulation results for different values of m and n. The erasure probabilities have been set to $\epsilon_{\mathrm{SD}} = 0.3$, $\epsilon_{\mathrm{SR}} = 0.1$ and $\epsilon_{\mathrm{RD}} = 0.2$. 47

3.3 Comparison between theoretical upper bounds obtained from (3.12) and simulation results for different values of ϵ_{SD}. The remaining system parameters have been set to $m = 20$, $n = 30$, $\epsilon_{\mathrm{SR}} = 0.1$ and $\epsilon_{\mathrm{RD}} = 0.2$. . . . 47

3.4 Performance comparison of systematic and non-systematic network coding as a function of the excess coded packets $n - m$ transmitted by each source node for various values of ϵ_{SR}. The remaining system parameters have been set to $m = 20$, $n_{\mathrm{R}} = 15$, $\epsilon_{\mathrm{SD}} = 0.3$ and $\epsilon_{\mathrm{RD}} = 0.1$. 48

3.5 A network consisting of m source nodes, $n \geq m$ relay nodes and a destination D. The packet erasure probability of a source-to-relay link and a relay-to-destination link is represented by ϵ_{SR} and ϵ_{RD}, respectively. . . . 50

3.6 Comparison between simulation results and the theoretical upper bounds obtained from (3.24) and (3.28) for different values of m and n, when $q = 2$, $\epsilon_{\mathrm{RD}} = 0.1$ and $\epsilon_{\mathrm{SR}} \in [0.1, 0.9]$. 55

3.7 Effect of field size q on network performance and comparison between the proposed bounds and the old bounds for $\epsilon_{\mathrm{SR}} \in [0.1, 0.9]$, when $m = 20$, $n = 25$ and $\epsilon_{\mathrm{RD}} = 0.1$. 55

3.8 Performance of the network for an increasing number of relays n. The proposed bounds and the old bounds have been plotted for $m = 10$, $\epsilon_{\mathrm{SR}} = 0.7$, $\epsilon_{\mathrm{RD}} = 0.2$ and different values of field size q. 56

3.9 Network performance and comparison between the proposed bounds and the old bounds for $m = 10$, an increasing number of relays n, $\epsilon_{\mathrm{SR}} = 0.3$, $\epsilon_{\mathrm{RD}} = 0.1$ and different field size q. 56

3.10 Block diagram of the system model 58

3.11 Simulation results and performance comparison between NOMA-RLNC and OMA-RLNC, when $m = 20$, $n = 10$ and $q = 4$. 63

3.12 Effect of the field size q and the number of relay nodes n on the joint decoding probability, when $m = 20$. 64

3.13 Comparison between the two schemes in terms of the required average number of relay nodes and the SNR when $m = 20$ and $q = 4$. 65

3.14 Effect of target rates on the system throughput against the system SNR, when $m = 20$ and $q = 4$. 65

4.1 Block diagram of the system model, where ϵ_{B} and ϵ_{E} denote the erasure probabilities of the channels linking Alice to Bob and Alice to Eve, respectively. 69

4.2 Comparison between analytical and simulation results for FT and UT, when $\epsilon_{\mathrm{E}} \in [0.1, 0.5]$, $\epsilon_{\mathrm{B}} = \{0.01, 0.03, 0.05, 0.07, 0.09\}$, $m = 50$, $\dot{n} = 150$, $q = 2$ and $\dot{P} = 90\%$. 74

4.3 Contour map (solid lines) depicting the loss in intercept probability caused by the change from UT to FT, as a function of ϵ_{E} and ϵ_{B}. The value of n^* (dashed line) as a function of ϵ_{B} has been superimposed on the plot. . 74
4.4 Block diagram of the system model. 76
4.5 Comparison between simulation and theoretical results, and secrecy-reliability performance of the considered protocols for different values of m, when $q = 2$ and $\tau/m = 0.6$. 91
4.6 Effect of the field size q on the secrecy performance of both CSWJ and OSWJ, as a function of the SNR, when $\tau = 8$ and $m = 15$. 92
4.7 Performance comparison in terms of the amount of decoded data and the SNR value, for $q = 2$ and $m = 15$. 93
4.8 Delay performance as a function of SNR for $q = 2$ and $q = 64$, when $m = 15$ is considered. 94
4.9 Secrecy-reliability trade-off as a function of the SNR for two different transmission schemes, $m = 15$, $q = 2$ and $\tau = 8$. 94
4.10 Performance comparison based on the decoding probability and the zero-intercept probability at SNR=30 dB, for $m = 15$ and $q = 2$. 95

Abbreviations

ARQ	Automatic Repeat Request
BD	Block diagonal
BLT	Block Lower-Triangular
BTD	Block Tri-Diagonal
CSI	Channel State Information
CDF	Cumulative Distribution Function
CS	Conventional Selection
CSWJ	Conventional Selection with Jammer
EG	Expanding Generations
FT	Feedback-aided transmission
LTE	Long Term Evolution
NC	Network Coding
NOMA	Non-Orthogonal Multiple Access
NOG	Non-Overlapping Generations
OMA	Orthogonal Multiple Access
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OSWJ	Optimal Selection with Preset Jammer
OS	Optimal Selection
PMF	Probability Mass Function
PLS	Physical-Layer Security
RAM	Resource Allocation Model
RMT	Random Matrix Theory
RLNC	Random Linear Network Coding
RLNCC	Random Linear Network Coded Cooperation

SG	Sliding Generations
SNR	Signal-to-Noise Ratio
SINR	Signal-to-Interference-plus-Noise Ratio
SIC	Successive Interference Cancellation
UT	Unaided Transmissions
UEP	Unequal Error Protection
3GPP	3rd Generation Partnership Project

Chapter 1

Introduction

This thesis deals with RLNC based communication schemes which are suitable for the reliability and security in wireless networks. More specifically, the thesis focuses on sparse structures of random matrices over finite fields and makes design recommendations suitable for low-complexity receivers, prioritised coding for reliable multimedia content delivery, and multicast/broadcast communications. In addition, it exploits the use of RLNC in cooperative networks, and focuses on a cross layer design for attaining high reliability gains. Moreover, the thesis aims to quantify the secrecy features of RLNC, and design a cross-layer technique for the purpose of achieving a perfectly secure communication.

This chapter continues with the background and motivations of the thesis. Then overview and contributions are presented. Finally, the organization of the thesis is explained and linked with the list of author's publications to each contribution.

1.1 Background and Motivations

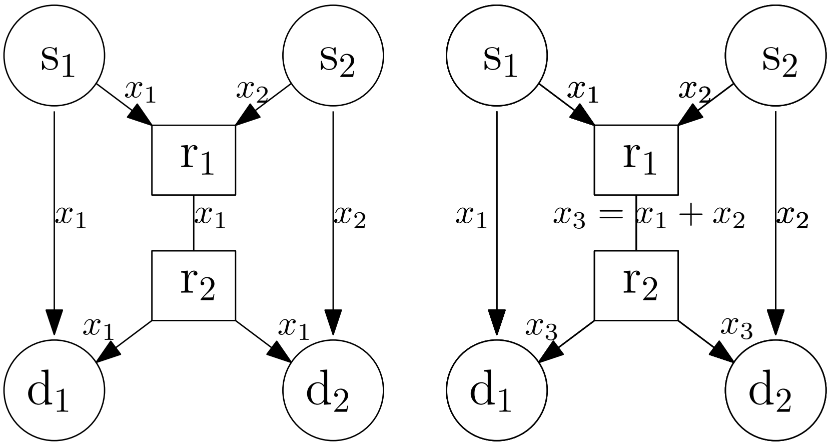
Network coding (NC) is a great breakthrough in the field of information theory. It was originally proposed by R. Ahlswede et al. [1] in 2000, and has since attracted an increasing interest of researchers in the area of both wired and wireless communication. We can broadly define network coding as allowing intermediate nodes to perform decoding and process the incoming information flows, as opposed to traditional store-and-forwarding routing techniques. Moreover, in contrast to traditional routing, network coding can exploit the full capacity of the network. For example, it has been demonstrated in [1] that network coding can be used to solve the bottleneck problem in wired networks and therefore can achieve the multicast capacity. The reliability benefits of network coding compared with Automatic Repeat Request (ARQ) baseline protocols has been exhibited in [2–4]. In addition, network coding is proposed in [5] and [6] for efficient multicast routing. Network coding has the inherent capability to achieve spatial diversity. It has been shown in [7] that network coding can improve the diversity gain of networks that either contain distributed antenna systems or support cooperative relaying. Research has revealed that NC offers a performance gain in terms of not only network reliability, throughput, transmission delay and robustness, but also in terms of energy consumption [8], scalability, routing complexity [9] and security. Furthermore, these benefits are not restricted to error free communication networks, but can also be exploited in sensor networks, device to device networks, industrial wireless networks, optical networks and heterogeneous networks. Thus, network coding is considered as one of the attractive solutions for integration into or combination with existing as well as future communication technologies. For example, it has been shown in [10] that by modifying the IEEE 802.11g frame structure, network coding combined with Orthogonal Frequency Division Multiplexing (OFDM) can significantly improve the network throughput. In addition, the importance of network coded cooperation has been demonstrated in [11], and a practical implementation of network-coded cooperation based on Orthogonal Frequency Division Multiple Access (OFDMA) has been presented in [12]. Recently, Non-Orthogonal Multiple Access (NOMA) has been recognized as a promising multiple access technique for 5G mobile networks [13, 14]. It has been shown in [15], [16] that combining NOMA with OFDM can improve the spectral efficiency and accommodate more users than the conventional OFDMA-based systems. Moreover, the usefulness of network coding for downlink NOMA-based transmissions has been studied in [17].

1.2 Basic Examples of Network Coding

The idea behind network coding is to combine several data packets and generate a coded packet, with length equal to the length of one of the original packets. These data packets could be data packets of the same flow or data packets from different flows. The former approach is known as *intra-session* NC and the later is known as *inter-session* NC [18]. Intra-session NC can be applied at any source node of a multi-source network or at any intermediate node of a single-source network. On the other hand, inter-session NC can be used at any intermediate node of a multi-source network. However, it is challenging to employ the inter-session NC for multimedia streaming. For example, in order to generate a coded packet by the inter-session network coding, an intermediate node is required to wait until the data packets of all the information flows are received which may induce delays in the system. These delays can increase the delivery time of video segments and is therefore critical in multimedia streaming session. Thus, in order to address this issue, a concept of opportunistic network coding [19, 20] and progressive decoding has been introduced in the literature [21–23]. According to the opportunistic network coding scheme, a node combines all the data packets that have been successfully received and stored in its buffer. Whereas, in the progressive decoding approach, a receiver can start decoding as soon as the first coded block is received, and progressively decodes the new incoming coded blocks as soon as they are received. In the rest of this section, we present two well known examples to demonstrate the basic principle of network coding, and its potential to improve throughput and achieve the capacity of a network.

1.2.1 NC in a Butterfly Network

Consider a butterfly network as shown in Fig. 1.1, where source nodes s_1 and s_2 want to transmit their data packets x_1 and x_2 respectively to destination nodes d_1 and d_2. Let us assume that the capacity of each link is equal to one packet. Without network coding, a possible transmission scheme is shown in Fig. 1.1a. The link connecting nodes r_1 and r_2 acts as a bottleneck, that is, r_1 can only transmit one packet at a time. Consequently, if r_1 transmits x_1 then d_1 cannot receive x_2, or, if r_1 transmits x_2 then d_2 cannot receive x_1. On the other hand as shown in Fig. 1.1b, network coding is employed at the bottleneck that is r_1 adds the received data packets x_1 and x_2 and transmits the coded packet $x_3 = x_1 + x_2$ towards the destinations. In this case, d_1 can easily retrieve x_2 by subtracting the packet x_1 from x_3, and similarly d_2 can retrieve x_1 by subtracting x_2 from x_3. Thus, network coding helps us in the delivery of the data packets to both destinations at the same time, and therefore multicast capacity of the network increases from 1 to 2.



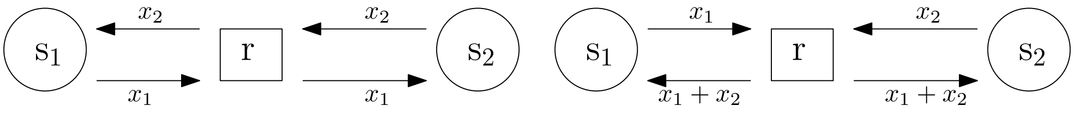
(A) without network coding

(B) with network coding

FIGURE 1.1: Example of network coding in wired network

1.2.2 NC in a Wireless Network

Consider a network as shown in Fig. 1.2a, where two source nodes s_1 and s_2 want to communicate with each other via a relay node r. There are no direct links available between the nodes s_1 and s_2. In addition, it is assumed that the network is operated in half duplex mode, whereby a node cannot transmit and receive at the same time. Therefore, nodes s_1 and s_2 need to transmit their packets to the relay node r. After the relay node receives both packets, it forwards the packet of s_1 to s_2 and the packet of s_2 to s_1. Thus, a total of 4 transmissions are needed for nodes s_1 and s_2 to exchange packets. In Fig. 1.2b, network coding is employed at the relay node r, such that, instead of the relay node transmitting x_1 and x_2 separately broadcasts a single packet x_1+x_2 to both s_1 and s_2. When node s_1 receives x_1+x_2, it extracts x_2 using the self-information x_1 as $(x_1+x_2)-x_1 = x_2$. Similarly s_2 extracts x_1 from $(x_1+x_2)-x_2$. Thus, in this example network coding helps in reducing the number of transmissions from 4 to 3. By reducing the number of transmissions from 4 to 3, network coding achieves a throughput improvement of 25% over the traditional forwarding scheme. Note that, in network coding all the arithmetic operations are carried out in a finite field $\mathbb{F}_q$, with size q. Note that, the idea of NC in a wireless network has also been proposed as a physical layer network coding scheme [24, 25], where where the natural superposition of electromagnetic waves is equivalent to the NC encoding operations.



(A) without network coding

(B) with network coding

FIGURE 1.2: Example of network coding in wireless network

1.3 Random Linear Network Coding

Random linear network coding (RLNC) is a class of network coding, first proposed in [6] for multicast communication, which does not require coordination between network nodes and therefore makes the transmission scheme simple and efficient. According to this scheme, a coded packet is generated by randomly selecting and linearly combining the data packets over some finite field. This random feature of coding technique incorporates the property of ratelessness, that is, it allows to generate an infinite number of coded packets. In addition, the coding feature of RLNC also minimizes the need for signaling in contrast to deterministic codes. The original packets can be decoded from any sufficient set of coded packets. Moreover, in contrast to other traditional coding schemes, RLNC is capable to adapt to any transmission rate on the fly. Because of these features, RLNC is easy to implement and is considered as a suitable technique for dynamic topologies and varying connections. Thus, RLNC is a powerful method for node cooperation, in particular for broadcast communication, and in distributed networks, where nodes cannot easily coordinate the routing of information through the network. Furthermore in [6], it has been proved that RLNC due to its inherent randomness achieves the multicast capacity in a distributed fashion. In energy-constraint wireless networks, such as sensor networks, the communicating nodes are typically battery powered and have a limited energy budget. The improvement of the network lifetime without a reduction in network reliability is a major challenge. RLNC can decrease the number of distinct packet transmissions in a network and minimize or eliminate packet retransmissions due to poor channel conditions [6]. Consequently, RLNC has the potential to both improve energy efficiency [26] and reduce the overall latency in a network [27], which effectively leads to an increase in the lifetime of the network.

1.3.1 RLNC Encoding and Decoding

The encoding process is employed on packets/symbols, where a packet could be composed of multiple symbols. These packets could be either obtained after dividing the information at the source node or could be packets of different information flows received at intermediate nodes. In order to understand the encoding process, let us assume that there are m packets $\{x_1, x_2, \ldots, x_m\}$ which need to be encoded using RLNC. A coded packet y_i can be obtained by simple vector multiplication, as follows

$$y_i = \begin{bmatrix} c_{1,i}, c_{2,i}, \ldots, c_{m,i} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} \tag{1.1}$$

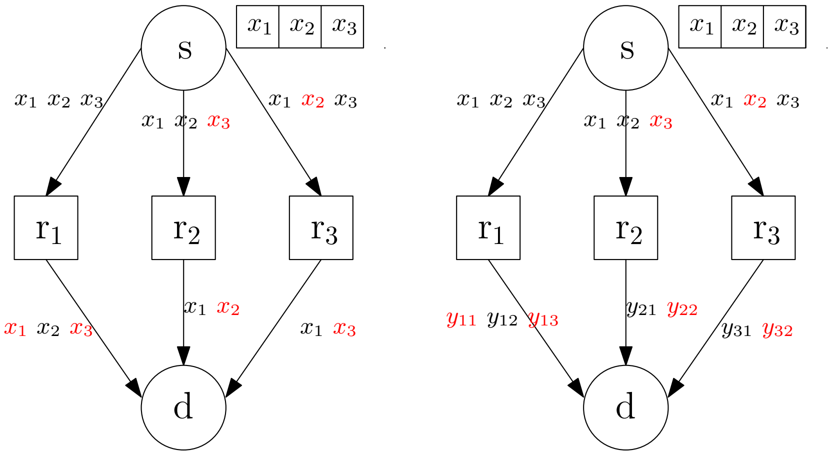
where, $[c_{1,i}, c_{2,i}, \ldots, c_{m,i}]$ is the coding vector whose elements (coding coefficients) are selected independently at random over the finite field $\mathbb{F}_q$ with size q. In this way, we can generate $m + \kappa$ coded packets and coding vectors, where κ is any number of redundant packets. Thus, the encoding process can, in theory, generate an infinite number of coded packets. However, due to the random selection of coding coefficients there is a non-zero probability that some of the coding vectors are linearly dependent and the corresponding coded packets cannot contribute to the decoding process. Before transmitting a coded packet into a network, the coding vector is appended to the associated coded packet, as described in [28] and shown in Fig 1.3. Where, the header may contain information or data associated to other layers of protocol stack, required for a packet to reach its intended destination. A sink node after receiving a transmitted packet, extracts both

Header	Coding vector	Coded packet

FIGURE 1.3: Structure of transmitted coded packet

the coded packet and the coding vector, and stores them into two separate matrices that could be termed as *payload matrix* and *decoding matrix* respectively, provided that the coding vector is linearly independent. In order for a sink to decode m original packets, it must collect at least m coded packets with linearly independent coding vectors. Finally, the sink node employs Gaussian elimination on the decoding matrix augmented with the payload matrix to decode the packets.

1.3.2 RLNC Example



(A) Without RLNC (B) With RLNC

FIGURE 1.4: Example of RLNC in multi-path network

In order to understand the benefits of RLNC in comparison to normal transmission scheme, let us consider a simple example of RLNC in a multi-path network, shown in Fig. 1.4. A source node s wants to transmit packets x_1, x_2 and x_3 to destination d through relay nodes r_1, r_2 and r_3. All the channels between the nodes are assumed to be packet erasure channels with erasure probabilities between source to relay and relay to destination nodes set as $\epsilon_{\mathrm{sr}} = 0.33$ and $\epsilon_{\mathrm{rd}} = 0.66$, respectively. The communication scheme is divided into two phases. In the first phase, the source s broadcasts all the packets simultaneously through orthogonal channel, while the relay nodes are operated in the receiving mode. Because of the erasure channels sometimes transmission failures occur, therefore consider that r_1 receives all three packets, but r_2 and r_3 fail to receive x_3 and x_2, respectively. In the second phase of the scheme that is devoid of RLNC, as shown in Fig. 1.4a, r_1 forwards all the packets x_1, x_2 and x_3, r_2 forwards x_1 and x_2, and r$_3$ forwards x_1 and x_3 to the destination d. Because of the transmission failures, we see that the destination d could only receive x_2 from r$_1$ and x_1 from both r$_2$ and r$_3$. On the other hand, as shown in Fig. 1.4b, all the relay nodes employ RLNC for transmitting the packets. By this strategy r$_1$ produces the output coded packets y_{11}, y_{12} and y_{13}, correspondingly y_{21} and y_{22} are produced by r$_2$, and y_{31} and y_{32} are produced by r$_3$. We see that because of the packet failures, at the end of second phase, the destination d receives y_{12}, y_{21} and y_{31}. The received coded packets can be represented by the following linear equations:

$$y_{12} = c_{1,1}x_1 + c_{1,2}x_2 + c_{1,3}x_3 \tag{1.2}$$

$$y_{21} = c_{2,1}x_1 + c_{2,2}x_2 \tag{1.3}$$

$$y_{31} = c_{3,1}x_1 + c_{3,3}x_3 \tag{1.4}$$

where $c_{1,j}$, $c_{2,j}$ and $c_{3,j}$ are the non-zero coding coefficients generated by the relay nodes r$_1$, r$_2$ and r$_3$, respectively. Thus, by solving these equations the destination d can recover all the packets x_1, x_2 and x_3, because the received coded packets are combinations of linear independent packets

1.3.3 RLNC Limitation and Literature Work

Decoding complexity is a main limitation of RLNC. For example, in order to decode m packets, each of size $\mathbb{L}$ symbols from a given finite field, the decoder employs the Gaussian elimination algorithm to invert an $m \times m$ matrix and needs $O(m^3 + m^2\mathbb{L})$ finite field operations in total [29]. Practical methods that aim to reduce the decoding complexity of RLNC include the adoption of Chunk Codes [30], the implementation of RLNC over non-overlapping windows [31] and the use of RLNC over disjoint generations [32]. These schemes first split a message into disjoint sub-messages and then encode each sub-message separately using RLNC. The decoding complexity, which is inversely proportional to the number of partitioned sub-messages, is reduced compared to that of conventional RLNC. However, this reduction in complexity comes at the cost of reduced performance (in terms of decoding probability) and increased overhead (in terms of transmitted coded packets). In an effort to fine-tune the trade-off between the performance advantage of conventional RLNC and the reduced decoding complexity of RLNC based on disjoint generations, the partitioned sub-messages can be allowed to overlap. This RLNC implementation is known as overlapping generations [32], overlapped chunk codes [33] and sliding window RLNC [34, 35]. The aforementioned schemes exploit a principle similar to that of message passing, which is used by fountain decoders [36]; packets of decoded generations can be back-substituted into undecoded generations that contain it, increase the probability of these generations being decoded and improve the overall throughput. In order to further reduce both the decoding complexity and the overhead while maintaining the delay performance, the concept of sparse RLNC within each generation as well as a feedback mechanism to control the amount of overlap between generations were proposed in [29, 37].

1.4 RLNC Applications

Today, RLNC has made its place from mathematical theories to practical implementations [38–41]. As shown in Fig. 1.5, RLNC has been demonstrated to be able to improve the performance of many applications, such as multimedia streaming [42], broadcasting [43, 44], cooperative communication, reliability in unreliable wireless networks, support heterogeneous devices [45], distributed storage [46], network monitoring and management [47, 48], memory management [49], on-chips communication [50], energy efficiency [51], and security [52]. Details of specific applications that this thesis has focused on are presented in the remainder of this section.

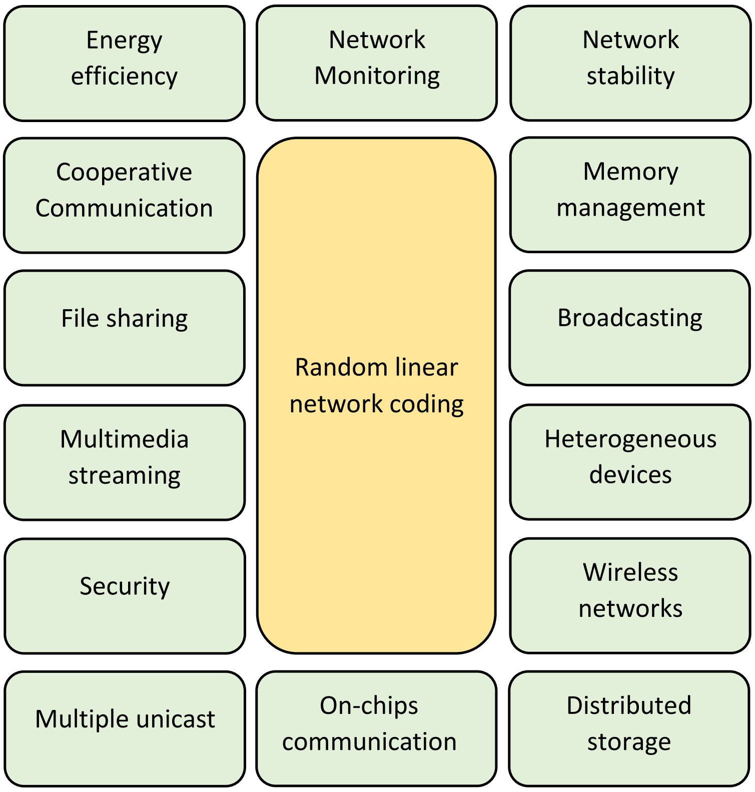


Figure 1.5: Applications of RLNC

1.4.1 RLNC for Heterogeneous Devices and Broadcast Communication

RLNC can be used to facilitate heterogeneous devices with different processing power, size and storage limitations. In order to accommodate a diverse set of receiving devices, the data that are about to be transmitted by a base station or access point can be divided into priority layers, which are encoded using RLNC that offers Unequal Error Protection (UEP) [31, 53]. The priority layers usually consist of a base layer and multiple enhancement layers. The base layer is responsible for providing a basic level of service, suitable for all types of devices with small storage and limited processing power. On the other hand, the enhancement layers contain data which can improve the quality of service. Thus, access to all or as many as possible layers offers a high quality of service. This layered structure of RLNC has fitted well into different applications. For example, in [54] as Prioritized Random Linear Coding (PRLC) for layered data delivery from multiple servers, in [44] as UEP RLNC for wireless layered video broadcasting and in [43] as Expanding Window-RLNC (EW-RLNC) for multimedia multicast services based on the H.264/SVC standard.

1.4.2 Random Linear Network Coded Cooperation

RLNC has attracted substantial research efforts due to its appealing benefits in cooperative communications. Several works in the literature have exploited Random Linear Network Coded Cooperation (RLNCC) for achieving reliability, energy efficiency,and diversity gain. For example in [55], RLNC-based cooperation was employed in cooperative compressed sensing for achieving energy efficiency and robustness against link failures. In [56, 57], network coded cooperation was employed to achieve maximum diversity gain. Cooperative communication with deterministic and random network coding schemes were studied in [58], where it has been demonstrated that both schemes outperform conventional cooperation in terms of diversity-multiplexing tradeoff. Moreover in [59] and [60], the authors proposed an analytical framework to characterize the performance of an RLNCC system in terms of bounds of decoding failure probability.

1.4.3 RLNC for Secure Communication

One of the elegant qualities of RLNC is its inherent nature of security. Therefore, the problem of achieving secure communication in systems employing network coding has recently attracted the attention of the research community in wireless networks. Ning and Yeung [61] first formulated the concept of secure network coding, which avoids information leakage to a wiretapper. They imposed a security requirement, that is, the mutual information between the source symbols and the symbols received by the wiretapper must be zero for secure communication. Based on a well-designed precoding matrix, Wang *et al.* [62] proposed a secure broadcasting scheme with network coding to obtain perfect secrecy. Probabilistic weak security for linear network coding was presented in [63], which devised network coding rules that can improve security depending on the adopted field size, the number of transmitted symbols and the ability of the attacker to eavesdrop on one or more independent channels. Moreover, the intercept probability of fountain coding, which is equivalent to random linear network coding for wireless broadcast applications, was formulated in [64] and exploited for industrial wireless sensor networks in [52].

1.4.4 RLNC Integrated with Opportunistic Relaying and Intentional Jamming

The dynamic nature of the wireless medium often introduces problems to the operation of wireless networks, which are related to node connectivity, communication reliability and robustness [65]. Methods that can ameliorate the side effects of wireless environments include *opportunistic relaying* and *node cooperation* [66]. For example, opportunistic relaying was proposed as an alternative to distributed space-time relaying; it achieves full diversity gain [67] but can also improve energy efficiency [68, 69]. Opportunistic routing based on cooperative forwarding was presented in [70] to combat errors and link failures in sensor networks. Multi-phase node cooperation for indoor industrial monitoring was described in [71] as a means to reduce energy consumption. Moreover, an experimental study of selective cooperative relaying was provided in [72]. Advantages from using opportunistic relaying with network coding in two-way relay communications have been reported in [73–75].

Even though opportunistic relaying and RLNC have the potential to improve energy efficiency and link reliability, the broadcast nature of the wireless medium renders data transmission to an authorized destination vulnerable to eavesdropping. The secure delivery of confidential data is important for many applications, for example, sharing of sensitive information or key distribution. In order to achieve secrecy and privacy, many cryptographic schemes are widely designed and adopted on the higher layers of the protocol stack, while assuming the error free communication at the physical layer. However, these methods usually require high computational power, and typically assume limited computing power for the eavesdroppers. Against this background, *Physical-layer security* (PLS) has emerged as a major research topic in recent years, and has been proposed as an alternative to achieve perfect resilience against eavesdropping attacks without requiring special key distribution and complex encryption/decryption algorithm [76, 77]. The core idea behind this paradigm is to exploit the dynamic nature of radio channel, such as fading and noise, for maximizing the uncertainty concerning the source messages at the eavesdropper [78, 79]. These properties are traditionally interpreted as impairments, but PLS take advantage of these properties for achieving secrecy in wireless transmission. PLS was first introduced in [80], where the wiretap channel was characterised as the fundamental element to protect information at the application layer. In this seminal work, the security is evaluated by establishing a metric called secrecy capacity as the maximum rate of transmission at which the information is considered to be secure without being interpreted by an eavesdropper. Later the subsequent result was employed to the broadcast channel in [79] and basic Gaussian channel in [81]. Moreover in the literature, several techniques are proposed for enhancing the PLS, including: secure on-off power allocation designs [82], secrecy enhancing channel coding scheme [83], and beamforming/precoding and artificial interference-aided techniques relying on multiple antennas [84]. Furthermore, PLS can be easily integrated into wireless networks that combine opportunistic relaying with cooperative communication [85–87]. For example in [85], a relay selection metric that utilizes knowledge of the relay-to-eavesdropper instantaneous channel conditions was presented and the network performance was evaluated in terms of the secrecy outage probability. Opportunistic relay selection protocols in the presence of multiple eavesdroppers were studied in [86]. The effect of single-relay and multi-relay selection on the performance of physical layer security in wireless networks was investigated in [87] and security-reliability tradeoffs were identified using comparisons between the intercept probability and the outage probability of direct transmission. On the other hand, jamming is a well-known PLS approach to enhance the quality of security in wireless transmissions [88, 89]. In this scheme, additional interference signals are transmitted to confuse the potential eavesdroppers or to degrade the channel's quality of unintentional receivers. These interference signals can be introduced by embedding them in the intended signals, which are also referred as artificial noise approach in the literature [90]. Moreover, *cooperative jamming* scheme has attained significant attention in the literature [91–94], and has become an effective way for improving the achievable secrecy rate. In this technique, a friendly jammer node aims to disturb the eavesdroppers and protect the legitimate users. For example, cooperative jamming strategy is provided in [91] for improving the secrecy rate. In addition, joint relay-and-jammer selection techniques were proposed in [92] to increase the secrecy capacity in wireless networks, whereas suboptimal relay selection and suboptimal joint relay-and-jammer selection protocols were compared in [93].

The main objective of PLS techniques is to increase the secrecy rate between the source and the destination, while ensuring that the transmitted information cannot be accessed by an eavesdropper. Strict information-theoretic security is achieved if and only if the mutual information between the packets available to an eavesdropper and the source packets is zero [61]. The performance of PLS schemes is often measured by the *secrecy capacity*, which is the maximum rate for reliable and perfectly secure communication, and the *secrecy outage probability*, which is the probability that secure communication will fail. However, these two metrics are used to optimize the transmission rate, so that the legitimate destination will fully recover the transmitted data with perfect secrecy. If information-theoretic secrecy cannot be achieved, the secrecy capacity and the secrecy outage probability do not provide any insight into the likelihood of an eavesdropper recovering only a *fraction* of the transmitted confidential information. To the best of our knowledge, only few studies that exploit the properties of RLNC in PLS are available. For example, fountain coding based secure wireless communication was analyzed in [64], and to enhance the secrecy of cooperative transmissions in sensor networks, fountain-coding aided cooperative relaying with jamming was proposed in [52].

1.5 Overview and Contributions of Thesis

This thesis is concerned with the development of probabilistic frameworks to evaluate and characterize the performance of RLNC based communications. More specifically, the problems which are considered in this thesis provide answers to the following main questions:

- **Research Question 1 (RQ1)**: How can we exploit random matrix theory over finite fields to formulate and characterize the performance of RLNC with layered structures and tunable sparsity?
- **Research Question 2 (RQ2)**: How can we develop probabilistic models to evaluate the performance of RLNCC and design a framework which integrates the benefits of physical layer multiplexing using the emerging NOMA and RLNCC?
- **Research Question 3 (RQ3)**: How can we evaluate and quantify the intrinsic security level provided by RLNC, and how can we design a cross layer security scheme which exploits the intrinsic security of RLNC on top of physical layer security techniques with minimum effect on reliability?

In particular, research question **RQ1** deals with the rank of random matrices over finite fields with adjustable tunable level of sparsity for the purpose of addressing the decoding complexity of RLNC, supporting heterogeneous devices and point-to-point or point-to-multipoint prioritized communication. On the other hand, **RQ2** mainly deals with tunable sparse RLNC and its applications for opportunistic coded cooperation. **RQ3** deals with the resilience of RLNC against eavesdropping, and also deals with the combination of RLNC, and relay and jammer selection techniques to discourage eavesdropping and support reliability.

1.5.1 Thesis Structure and Organization

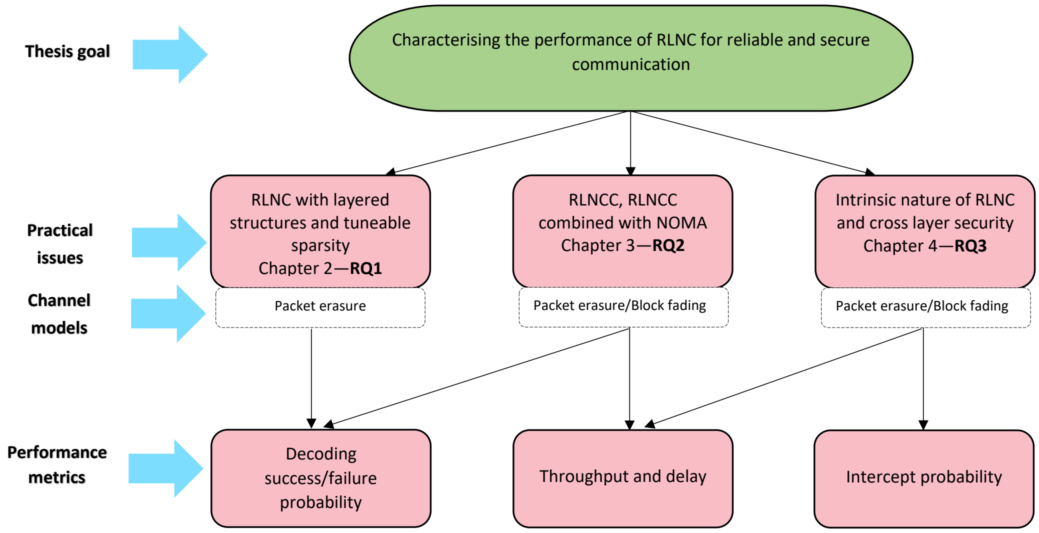

Thesis goal
Characterising the performance of RLNC for reliable and secure communication
Practical issues
RLNC with layered structures and tuneable sparsity Chapter 2—**RQ1**
RLNCC, RLNCC combined with NOMA Chapter 3—**RQ2**
Intrinsic nature of RLNC and cross layer security Chapter 4—**RQ3**
Channel models
Packet erasure
Packet erasure/Block fading
Packet erasure/Block fading
Performance metrics
Decoding success/failure probability
Throughput and delay
Intercept probability

FIGURE 1.6: Thesis Flowchart

Fig. 1.6 exhibits the flowchart of the thesis structure. Chapter 2 tackles the research question RQ1, by focusing on random block matrices over finite fields and investigating different matrix structures, which model the encoding process of layered structures of RNLC schemes. In order to address the decoding complexity of RLNC and support low power devices, these structures also allow to adjust the sparsity level of encoding. More specifically in this chapter, we employ fundamental expressions of random matrix theory over finite fields and develop a mathematical framework for the considered matrix structures. The proposed framework can be used to accurately characterize the probability that a receiver will successfully decode transmitted data or layers of a service. Numerical results and discussions are provided.

The results in this chapter have been presented in the following journal paper:
J1: **A. S. Khan** and I. Chatzigeorgiou, "A Framework for the Analysis of Network-Coded Schemes Characterized by Random Block Matrices", IEEE Transactions on Wireless Communications, under preparation.

Chapter 3 attempts to answer the research question RQ2, by studying three different network models. Here, we first consider a relay assisted network with two source nodes and a single destination node, where source nodes employ intra-session RLNC and the relay node employs inter-session RLNC for coded cooperation. The performance of the network is characterized by the probability of decoding success at the destination node. Closed form mathematical expressions are derived to evaluate the performance, and at the end, results and discussions are provided. Secondly, we consider a multi-source multi-relay network, where only relay nodes employ RLNC for coded cooperation. The performance of the network is characterized by the decoding failure probability. Exact theoretical expressions to evaluate this probability is still an open problem. However in this chapter, we derive mathematical closed form expressions to evaluate tighter upper and lower bounds to the failure probability. Simulation results and discussions are provided to exhibit the tightness of the derived expressions and characterize the network performance. Thirdly, we consider a multiple relay network with two source groups and two destination nodes, and propose a framework which integrates the advantages of RLNCC and NOMA based communication. Theoretical closed form expressions are derived to evaluate the network performance mainly in terms of throughput and successful decoding probability at the destination nodes. Simulation results and discussions are provided to demonstrate the benefits of NOMA based RLNCC as compared to the conventional OMA based communication.

The results in this chapter have been presented in the following conference and journal publications:
C1: **A. S. Khan** and I. Chatzigeorgiou, "Performance analysis of random linear network coding in two-source single-relay networks", in Proc. IEEE International Conference on Communications Workshops (ICC), Workshop on Cooperative and Cognitive Networks, London, United Kingdom, June 2015.
J2: **A. S. Khan** and I. Chatzigeorgiou, "Improved bounds on the decoding failure probability of linear NC over multi-source multi-relay networks", IEEE Communications Letters, vol. 20, no. 10, pp. 2035-2038, Oct. 2016.
J3: **A. S. Khan** and I. Chatzigeorgiou, "Non-Orthogonal Multiple Access Combined With Random Linear Network Coded Cooperation", IEEE Signal Processing Letters, vol. 24, no. 9, pp. 1298-1302, Sept. 2017.

Chapter 4 addresses the research question RQ3, by presenting two different network models where RLNC is employed for secure communications. In this chapter, we first consider a simple point-to-point network with conventional characters: Alice, Bob and a passive eavesdropper. Where, Alice exploits RLNC for secure communication to Bob. Feedback and without feedback protocols are considered, and the secrecy of communication is evaluated by deriving the exact close form expression of intercept probability corresponding to each protocol. Moreover, an optimization model is presented for further improving the network security. All the analyses are supported by simulation results and discussions. Secondly, a multi-relay network is considered to integrate the advantages of RLNC and physical layer security techniques. In particular, we consider relay/jammer selection techniques for physical layer security and RLNC at the application layer for self-encryption of data. Closed form outage expressions are derived corresponding to each relay/jammer selection technique. Furthermore, network security is accurately quantified by developing a framework which characterizes the probability of the eavesdropper intercepting a sufficient number of coded packets and partially or fully decoding the confidential data. Simulation results and discussions are presented to support the analysis and to exhibit a tradeoff between reliability and security corresponding to each relay/jammer selection technique.

The results in this chapter have been presented in the following journal publications:
J4: **A. S. Khan**, A. Tassi and I. Chatzigeorgiou, "Rethinking the intercept probability of random linear network coding", IEEE Communications Letters, vol. 19, no. 10, pp. 1762-1765, October 2015.
J5: **A. S. Khan** and I. Chatzigeorgiou, "Opportunistic relaying and random linear network coding for secure and reliable communication", IEEE Transactions on Wireless Communications, accepted with minor revisions.

Chapter 5 summarizes the thesis and provides the general conclusions drawn from each chapter. In addition, some possible research areas are also presented as an extension to the research presented in the thesis.

Chapter 2

A Framework for the Assessment of Network Coding Techniques Characterized by Random Block Matrices

Random matrix theory (RMT) was first introduced by Wishart [95] in 1928. From its inception, numerous fields of science, engineering and statistics have been heavily influenced. Nowadays it is a key subject in topics of information theory, wireless communications, graph theory, signal processing, probability, multivariate statistics, combinatorics, statistical physics and quantum communication. Two fundamental reasons for the ever growing success of RMT can be identified. Firstly, RMT techniques offer remarkably precise predictions of analytical computations that grow to infinity in the context they are modeling. Secondly, RMT outcomes can be applied on any kind of random matrix, as long as the entries are independent and can be formalized in a given environment [96, 97]. This implies that RMT does not depend on the probability distribution that defines the matrix entries, but depends only on the invariant properties of their distribution [98]. Thus, RMT is a valuable tool for modeling a large number of complex mathematical and physical problems.

The modeling and performance evaluation of information processing techniques, including random linear network coding RLNC, relies on RMT over the finite fields. Practical methods that are designed to reduce decoding complexity or introduce unequal error protection properties, add constraints to the entries of matrices that characterize RLNC schemes. These constraints permit only entries within particular blocks of an RLNC matrix to take random values from a finite field, while the remaining entries are set to zero.

This chapter considers random block matrices and presents a mathematical framework for the enumeration of full-rank matrices that contain blocks of random entries arranged in a diagonal, lower-triangular or tri-diagonal structure. The derived expressions are then used to model the probability that a receiver will successfully decode a source message or layers of a service, when RLNC based on non-overlapping, expanding or sliding generations is employed. In particular, this framework is suitable for the study of systems employing random linear network coding to broadcast or multicast information, including content streaming and data distribution.

This chapter has been organized as follows: Section 2.1 introduces fundamental expressions for the rank of random matrices over finite fields. Section 2.2 treats partitioned random matrices as a special case of random block matrices and derives an equivalent formula for the number of full-rank matrices. Section 2.3 investigates the aforementioned structures of random block matrices and obtains theoretical expressions for the full-rank of each matrix. Section 2.4 briefly describes three existing RLNC implementations and establishes links between the previously derived theoretical formulas and the decoding probability of each RLNC scheme. Results are discussed in Section 2.5, and finally the contributions in this chapter are summarized in Section 2.6.

2.1 Fundamental Preliminary Expressions

Finite or Galois fields have been receiving steady attention because of their applications in many cryptographic techniques and error correcting codes. Let $\mathbf{M} \in \mathbb{F}_q^{n \times m}$ be a matrix that has been sampled uniformly at random from the set of all $n \times m$ matrices with elements from $\mathbb{F}_q$, where q is a prime power $\mathbb{p}^{\mathbb{r}}$ (such that, $\mathbb{p}$ is a prime number and $\mathbb{r}$ is a positive integer) [99]. Matrix $\mathbf{M}$ is said to be a *full-rank* matrix if it has rank $\min(n, m)$ or, equivalently, $\min(n, m)$ rows of $\mathbf{M}$ are linearly independent. For $n \geq m$, the number of full-rank $n \times m$ matrices can be computed as follows [100]

$$\gamma(n, m) = \begin{cases} \prod_{i=0}^{m-1}(q^n - q^i), & \text{if } m \geq 1 \\ 1, & \text{if } m = 0. \end{cases} \tag{2.1}$$

The probability that a matrix $\mathbf{M}$ is a full-rank matrix can be obtained by dividing $\gamma(n, m)$ by q^{nm}, which represents the total number of matrices in $\mathbb{F}_q^{n \times m}$, that is,

$$P(n, m) = \frac{\gamma(n, m)}{q^{nm}}. \tag{2.2}$$

If the rank of $\mathbf{M}$ is r, where $0 \leq r \leq \min(n,m)$, the number of all matrices of rank r in $\mathbb{F}_q^{n\times m}$, is given by [101, 102]

$$\gamma_r(n,m) = \begin{bmatrix} n \\ r \end{bmatrix}_q \gamma(m,r) \tag{2.3}$$

where the term $\left[\begin{smallmatrix} n \\ r \end{smallmatrix}\right]_q$ specifies the number of r-dimensional subspaces of an n-dimensional vector space over the finite field $\mathbb{F}_q$. It is widely known as the Gaussian or q-binomial coefficient [103] and is defined as

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \begin{cases} \frac{(1-q^n)(1-q^{n-1})\dots(1-q^{n-r+1})}{(1-q)(1-q^2)\dots(1-q^r)}, & \text{if } r \leq n \\ 0, & \text{if } r > n. \end{cases} \tag{2.4}$$

The q-binomial coefficient can also be expressed as the ratio of the number of full-rank matrices in $\mathbb{F}_q^{n\times r}$ to the number of full-rank matrices in $\mathbb{F}_q^{r\times r}$ [102], that is,

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \frac{\gamma(n,r)}{\gamma(r,r)}. \tag{2.5}$$

The probability of $\mathbf{M}$ having rank r can be obtained by dividing $\gamma_r(n,m)$ by the total number of $n \times m$ matrices as follows

$$P_r(n,m) = \frac{\gamma_r(n,m)}{q^{nm}}. \tag{2.6}$$

The fundamental expressions presented in this section will be invoked in the derivation of proofs in the following sections.

2.2 Partitioning of Random Matrices

Even though the formula that computes the number of $n \times m$ full-rank random matrices is derived in [100] as presented in (2.1), an exact equivalent expression that treats a random matrix as the concatenation of sub-matrices is also of interest and will be derived in this section. The derived expression will then be adapted to specific structures of random block matrices, which can be used in the performance modelling of network-coded systems.

Before we proceed with the proof of a lemma, which will lead us to the main proposition of this section, we first introduce some additional notation. If $\mathbf{M}_1, \dots, \mathbf{M}_L$ are matrices having the same number of columns, then $(\mathbf{M}_1; \dots; \mathbf{M}_L)$ denotes the matrix obtained by the *vertical concatenation* of the L matrices or, equivalently, by appending $\mathbf{M}_{i+1}$ to the bottom of $\mathbf{M}_i$ for $i = 1, \dots, L-1$.

Lemma 2.1. *Let* $\mathbf{M} = (\mathbf{M}_1; \mathbf{M}_2) \in \mathbb{F}_q^{(n_1+n_2)\times m}$ *be a random matrix obtained by vertically concatenating* $\mathbf{M}_1 \in \mathbb{F}_q^{n_1\times m}$ *and* $\mathbf{M}_2 \in \mathbb{F}_q^{n_2\times m}$*, where* $n_1+n_2 \geq m$*. The number of combinations of all realisations of matrices* $\mathbf{M}_1$ *and* $\mathbf{M}_2$ *that result in a full-rank random matrix* $\mathbf{M}$ *is equal to*

$$\gamma(n_1+n_2,\, m) = \sum_{r_1} \gamma_{r_1}(n_1, m)\gamma(n_2,\, m-r_1)q^{n_2 r_1} \tag{2.7}$$

where $\max(0, m-n_2) \leq r_1 \leq \min(n_1, m)$*.*

Proof. Matrix $\mathbf{M}$ is a full-rank matrix iff it contains m linearly independent columns. Let r_1 columns of $\mathbf{M}_1$ be linearly independent. The corresponding columns of $\mathbf{M}_2$ can take $q^{n_2 r_1}$ possible values, while the remaining $m - r_1$ columns of $\mathbf{M}_2$ can be selected in $\gamma(n_2, m - r_1)$ possible ways to give a full-rank $n_2 \times (m - r_1)$ submatrix. Therefore, the number of matrices $\mathbf{M}$ having m linearly independent columns is equal to the number of all possible matrices $\mathbf{M}_1$ of rank r_1 given by $\gamma_{r_1}(n_1, m)$, multiplied by the number of all possible matrices $\mathbf{M}_2$ of rank $m - r_1$ given by $\gamma(n_2, m - r_1)q^{n_2 r_1}$, summed over all valid values of r_1. A proof, which analytically demonstrates that the right-hand side of (2.7) is equal to the right-hand side of (2.1) for $n = n_1 + n_2$, is presented in the Appendix A. □

Proposition 2.2. *Let* L *random matrices* $\mathbf{M}_1, \ldots, \mathbf{M}_L$*, where* $\mathbf{M}_i \in \mathbb{F}_q^{n_i\times m}$ *for* $1 \leq i \leq L$*, be vertically concatenated in order to generate* $\mathbf{M} = (\mathbf{M}_1; \mathbf{M}_2; \ldots; \mathbf{M}_L) \in \mathbb{F}_q^{n\times m}$*, where* $n = n_1 + \ldots + n_L$*. Equivalently, we can write*

$$\mathbf{M} = \begin{bmatrix} \mathbf{M}_1 \\ \mathbf{M}_2 \\ \vdots \\ \mathbf{M}_L \end{bmatrix}.$$

The number of all possible matrices $\mathbf{M}_1$*,* $\mathbf{M}_2, \ldots, \mathbf{M}_L$ *that result in a full-rank matrix* $\mathbf{M}$ *is equal to*

$$\gamma(n, m) = \sum_{r_1} \gamma_{r_1}(n_1, m)\, \gamma(n-n_1,\, m-r_1)\, q^{(n-n_1)r_1} \tag{2.8}$$

in recursive form, or

$$\gamma(n, m) = \sum_{r_1} \cdots \sum_{r_{L-1}} \prod_{i=1}^{L} \gamma_{r_i}(n_i, m-R_{i-1})\, q^{\sum_{k=1}^{L-1} n_{k+1} R_k} \tag{2.9}$$

in non-recursive form, where:

$R_k = r_1 + r_2 + \ldots + r_k$ *and* $R_0 = 0$ *for* $k = 0$*,*

$n = n_1 + n_2 + \ldots + n_L \geq m$

and r_i*, for* $i = 1, \ldots, L-1$*, takes values in the range*
$r_i \geq \max(0, m - R_{i-1} - \sum_{j=i+1}^{L} n_j)$ *and*
$r_i \leq \min(n_i, m - R_{i-1})$*, while* $r_L = m - R_{L-1}$ *for* $i = L$*.*

Proof. The expression (2.8) is a recursive formulation of $\gamma(n, m)$ in terms of $\gamma(n-n_1,\, m-r_1)$ given that the vertical concatenation of L matrices can be viewed as the concatenation of two matrices, that is, $\mathbf{M}_1$ and $(\mathbf{M}_2; \mathbf{M}_3; \ldots; \mathbf{M}_L)$ or, equivalently,

$$(\mathbf{M}_1; \mathbf{M}_2; \ldots; \mathbf{M}_L) \equiv (\mathbf{M}_1; (\mathbf{M}_2; \mathbf{M}_3; \ldots, \mathbf{M}_L)).$$

The non-recursive expression (2.9) can be derived from (2.8) if Lemma 2.1 is repeatedly applied on $\gamma(n - n_1,\, m - r_1)$ in (2.8), given that argument $n - n_1$ can be written as $n_2 + \ldots + n_L$. This process is equivalent to expressing the vertical concatenation of L matrices as follows

$$(\mathbf{M}_1;\ldots;\mathbf{M}_L)\equiv(\mathbf{M}_1;(\mathbf{M}_2;(\mathbf{M}_3;\ldots;(\mathbf{M}_{L-1};\mathbf{M}_L)))).$$

Note that (2.3) has been used to express the number of both full-rank and rank-deficient matrices because $\gamma_{r_i}(n_i, m - R_{i-1})$ in (2.9) reduces to $\gamma(n_i, m - R_{i-1})$ for $r_i = m - R_{i-1}$. □

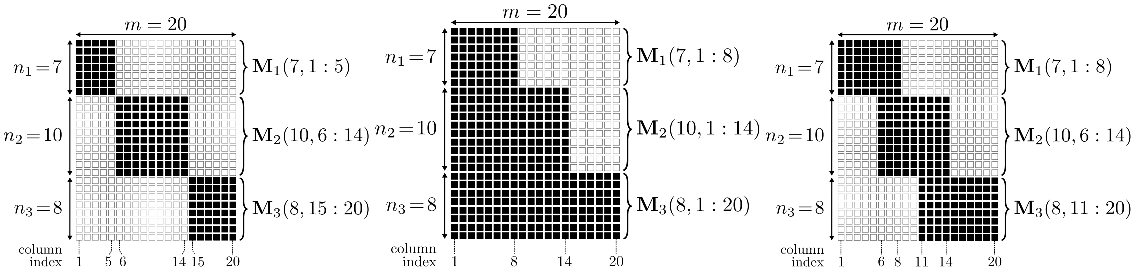
This section established that expression (2.1), which provides the number of full-rank $n \times m$ random matrices, can also take the form of (2.9), which partitions the random matrix into L sub-matrices and counts all possible combinations of each sub-matrix having a particular rank. The advantage of (2.9) over (2.1) is that it can be readily adapted to random block matrices, as will become evident in the following section.

2.3 Structures of Random Block Matrices

Whereas entries of a random matrix over a finite field $\mathbb{F}_q$ can take any of the q available values with equal probability, there exist cases where only a constrained number of entries can take values from $\mathbb{F}_q$ while the remaining entries are set to zero. We refer to matrices that contain blocks of random entries as *random block matrices* and we focus on the following general matrix structure in this chapter:

$$\mathbf{M} = \begin{bmatrix} \mathbf{M}_1(n_1, s_1 : e_1) \\ \mathbf{M}_2(n_2, s_2 : e_2) \\ \vdots \\ \mathbf{M}_L(n_L, s_L : e_L) \end{bmatrix}.$$

According to this structure, the $n \times m$ matrix $\mathbf{M}$ is the vertical concatenation of matrices $\mathbf{M}_i(n_i, s_i\!:\!e_i)$ of dimensions $n_i \times m$, for $i = 1, \ldots, L$. Parameters s_i and e_i signify the first and last columns of an $n_i \times (e_i - s_i + 1)$ random sub-matrix within $\mathbf{M}_i$. The remaining elements of $\mathbf{M}_i$ are equal to zero. Depending on the values of s_i and e_i, columns of $\mathbf{M}_i$ that contain random elements will be connected to columns of matrices above or below $\mathbf{M}_i$ that contain either random elements or zeros. This section will study three specific structures of random block matrices, namely Block Diagonal (BD) matrices, Block Lower-Triangular (BLT) matrices and Block Tri-Diagonal (BTD) matrices, and will derive exact expressions for the number of full-rank matrices in each case. The examples of random block matrices with the considered structures are exhibited in Fig. 2.1.



(A) Block diagonal (BD)

(B) Block lower-triangular (BLT)

(C) Block tri-diagonal (BTD)

FIGURE 2.1: Examples of 25 × 20 random block matrices, which have been constructed by vertically concatenating three matrices. Random elements are depicted by '■', while zero-valued entries are represented by '□'.

2.3.1 Block Diagonal (BD) Matrices

Consider an $n \times m$ matrix $\mathbf{M}$ with the following structure

$$\mathbf{M} = \begin{bmatrix} \mathbf{M}_1(n_1, 1:e_1) \\ \mathbf{M}_2(n_2, e_1+1:e_2) \\ \vdots \\ \mathbf{M}_L(n_L, e_{L-1}+1:m) \end{bmatrix}$$

where $n = n_1 + \ldots + n_L$, $s_i = e_{i-1} + 1$ for $i = 2, \ldots, L$, while $s_1 = 1$ and $e_L = m$. An example of a BD matrix for $L = 3$ is presented in Fig. 2.1a.

If $m_i = e_i - e_{i-1}$ denotes the number of columns in $\mathbf{M}_i$ that consist of random elements, we can infer that the $n \times m$ matrix $\mathbf{M}$ contains L random sub-matrices along its diagonal, each of dimensions $n_i \times m_i$, as shown in Fig. 2.1a. Observe that if a column of $\mathbf{M}_i$ consists of random elements, this column is connected to columns of matrices below or above $\mathbf{M}_i$ that always contain zeros. Consequently, the problem of computing the number of full-rank matrix realizations of $\mathbf{M}$ can be reduced to a set of independent problems, each associated to the number of full-rank $n_i \times m_i$ random sub-matrices. This implies that $\mathbf{M}$ is a full-rank matrix only if each $n_i \times m_i$ matrix $\mathbf{M}_i$, for $i = 1, \ldots, L$, has a full rank or, using mathematical notation, if $n_i \geq m_i$, $m_1 + \cdots + m_L = m$ and $r_i = m_i$. Substituting these conditions into (2.9) reduces the general expression of Proposition 2.2 into the following well-known relationship [43]

$$\gamma_{\mathrm{BD}}(\mathbf{M}) = \prod_{i=1}^{L} \gamma(n_i, m_i) \tag{2.10}$$

Therefore, the structure of BD matrices requires a reduced version of (2.9) to compute the number of full-rank matrices. Expression (2.9) can also be adjusted for the case of BLT matrices, as will be discussed in the following section.

2.3.2 Block Lower-Triangular (BLT) Matrices

The general structure of an $n \times m$ BLT matrix $\mathbf{M}$ is

$$\mathbf{M} = \begin{bmatrix} \mathbf{M}_1(n_1, 1:e_1) \\ \mathbf{M}_2(n_2, 1:e_2) \\ \vdots \\ \mathbf{M}_L(n_L, 1:m) \end{bmatrix}$$

where $s_i = 1$, $e_i \leq e_{i+1}$ and $e_L = m$. An example of a BLT matrix for $L = 3$ is depicted in Fig. 2.1b. The expression for the number of full-rank BLT matrices follows from Proposition 2.2 and will be presented as part of the following corollary:

Corollary 2.3. *Let* $\mathbf{M} = (\mathbf{M}_1; \ldots; \mathbf{M}_L) \in \mathbb{F}_q^{n \times m}$ *be a BLT matrix obtained by vertically concatenating* $\mathbf{M}_i \in \mathbb{F}_q^{n_i \times m}$ *for* $i = 1, \ldots, L$, *where* $n = n_1 + \ldots + n_L$. *Denote by* e_i *the number of the leftmost columns of* $\mathbf{M}_i$ *that contain elements from* $\mathbb{F}_q$ *while the remaining columns consist of zeros, where* $e_i \leq e_{i+1}$ *and* $e_L = m$. *The number of full-rank realizations of* $\mathbf{M}$ *is given by*

$$\gamma_{\mathrm{BLT}}(\mathbf{M}) = \sum_{r_1} \cdots \sum_{r_{L-1}} \prod_{i=1}^{L} \gamma_{r_i}(n_i, e_i - R_{i-1})\, q^{\sum_{k=1}^{L-1} n_{k+1} R_k} \tag{2.11}$$

where:

$R_k = r_1 + r_2 + \ldots + r_k$ *and* $R_0 = 0$ *for* $k = 0$,

$n = n_1 + n_2 + \ldots + n_L \geq m$

and r_i, *for* $i = 1, \ldots, L-1$, *takes values in the range*

$r_i \geq \max(0, m - R_{i-1} - \sum_{j=i+1}^{L} n_j)$ *and*
$r_i \leq \min(n_i, e_i - R_{i-1})$*, while* $r_L = m - R_{L-1}$ *for* $i = L$*.*

Proof. Whereas Proposition 2.2 is valid for constituent matrices $\mathbf{M}_i$, for $i = 1, \ldots, L$, which all comprise m columns that contain random elements from $\mathbb{F}_q$, this corollary considers the fact that only the first e_i columns of $\mathbf{M}_i$ contain random elements. Therefore, the maximum number of linearly independent columns that could remain in $\mathbf{M}_i$ depends on e_i rather than m. Expression (2.11) can thus be obtained from (2.9) if m is replaced by e_i in the second argument of γ_{r_i} and the upper limit of r_i. □

We note that Corollary 2.3 is not restricted to BLT matrices. It is valid for any matrix that can be transformed into a BLT matrix by swapping rows and columns, including rotated BLT structures such as block upper-triangular matrices.

2.3.3 Block Tri-Diagonal (BTD) Matrices

We refer to an $n \times m$ matrix $\mathbf{M}$ as a BTD matrix if it can be written in the following form

$$\mathbf{M} = \begin{bmatrix} \mathbf{M}_1(n_1, 1 : e_1) \\ \mathbf{M}_2(n_2, s_2 : e_2) \\ \vdots \\ \mathbf{M}_L(n_L, s_L : m) \end{bmatrix}$$

where $s_1 = 1$, $e_{i-2} < s_i \leq s_{i+1}$, $e_i \leq e_{i+1}$ and $e_L = m$. Fig. 2.1c shows an example of a BTD matrix for $L = 3$. In order to enumerate all full-rank BTD matrices for a given set of parameters, we will revisit and extend (2.2), so that the constraints of the BTD structure are incorporated. In an effort to facilitate the analysis, we will first discuss two relevant lemmata and introduce the notation $(\mathbf{\Phi}_1, \ldots, \mathbf{\Phi}_L)$ to represent the *horizontal concatenation* of L matrices.

Lemma 2.4. *Let* $\mathbf{M} = (\mathbf{\Phi}_1, \mathbf{\Phi}_2) \in \mathbb{F}_q^{n \times (m_1 + m_2)}$ *be a random matrix that has been constructed by horizontally concatenating* $\mathbf{\Phi}_1 \in \mathbb{F}_q^{n \times m_1}$ *and* $\mathbf{\Phi}_2 \in \mathbb{F}_q^{n \times m_2}$*. The number of full-rank matrix realizations of* $\mathbf{M}$ *can be expressed as*

$$\gamma(n,\, m_1 + m_2) = \gamma(n, m_1)\, \gamma(n - m_1,\, m_2)\, q^{m_1 m_2} \tag{2.12}$$

or

$$\gamma(n,\, m_1 + m_2) = \gamma(n - m_2,\, m_1)\, \gamma(n, m_2)\, q^{m_1 m_2} \tag{2.13}$$

where $n \geq m_1 + m_2$*.*

Proof. Matrix $\mathbf{M}$ has full rank if its $m_1 + m_2$ columns are linearly independent or, equivalently, $m_1 + m_2$ out of the n rows are linearly independent. This implies that $\boldsymbol{\Phi}_1$ and $\boldsymbol{\Phi}_2$ should be not only full-rank matrices but their columns should span non-overlapping vector subspaces. For $\boldsymbol{\Phi}_1$ to have full rank, m_1 of its rows should be linearly independent. As we have already seen, there exist $\gamma(n, m_1)$ full-rank random matrices of dimensions $n \times m_1$. For $\boldsymbol{\Phi}_2$ to have full rank, m_2 of its rows should also be linearly independent. However, the columns of $\boldsymbol{\Phi}_1$ and $\boldsymbol{\Phi}_2$ will span non-overlapping subspaces, only if the m_2 linearly independent rows of $\boldsymbol{\Phi}_2$ are connected not to the m_1 linearly independent rows of $\boldsymbol{\Phi}_1$ but to the remaining $n - m_1$ rows. Therefore, the number of full-rank realizations of $\boldsymbol{\Phi}_2$ is equal to the number of full-rank $(n - m_1) \times m_2$ random matrices multiplied by the number of arbitrarily defined elements in the remaining m_1 rows of $\boldsymbol{\Phi}_2$. The former quantity is given by $\gamma(n - m_1, m_2)$ and the latter quantity is equal to $q^{m_1 m_2}$. This concludes the proof of (2.12). The same line of reasoning can be followed to derive (2.13) if we first consider $\boldsymbol{\Phi}_2$ and then compute the number of possible realizations of $\boldsymbol{\Phi}_1$. □

Lemma 2.5. *Let* $\mathbf{M} = (\boldsymbol{\Phi}_1, \boldsymbol{\Phi}_2) \in \mathbb{F}_q^{n \times (m_1 + m_2)}$ *be a BTD matrix, where* $\boldsymbol{\Phi}_1 \in \mathbb{F}_q^{n \times m_1}$ *and* $\boldsymbol{\Phi}_2 \in \mathbb{F}_q^{n \times m_2}$*. The structure of* $\mathbf{M}$ *and the dimensions of its sub-matrices are as follows*

$$\begin{array}{c|cc|cc|c}
 & \multicolumn{2}{c}{\overbrace{\hspace{6em}}^{\boldsymbol{\Phi}_1}} & \multicolumn{2}{c}{\overbrace{\hspace{6em}}^{\boldsymbol{\Phi}_2}} & \\
 & \boldsymbol{\Phi}_1^{(1)} & \boldsymbol{\Phi}_1^{(2)} & \mathbf{0} & \mathbf{0} & n_1 \\
\mathbf{M} = & \mathbf{0} & \boldsymbol{\Phi}_1^{(3)} & \boldsymbol{\Phi}_2^{(1)} & \boldsymbol{\Phi}_2^{(2)} & n_2 \\
 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{\Phi}_2^{(3)} & n_3 \\
 & m_1 - w_1 & w_1 & m_2 - w_2 & w_2 &
\end{array}$$

and $n = n_1 + n_2 + n_3 \geq m_1 + m_2$*. The number of full-rank matrices that have the same structure as* $\mathbf{M}$ *is*

$$\gamma(\mathbf{M}) = \sum_{r_1} \sum_{r_2} \prod_{i=1}^{2} \gamma_{r_i}(n_{i+1}, w_i) \gamma(n_i - r_{i-1}, m_i - r_i) q^{\varphi_i} \tag{2.14}$$

where $\max(0, m_i - n_i + r_{i-1}) \leq r_i \leq \min(n_{i+1}, w_i)$ *and* $\varphi_i = (m_i - r_i) w_{i-1} + n_i r_i$ *for* $i = 1, 2$ *while* $w_0 = 0$*.*

Proof. As explained in Lemma 2.4, $\mathbf{M}$ will be a full-rank matrix if both $\boldsymbol{\Phi}_1$ and $\boldsymbol{\Phi}_2$ have full rank and their columns span non-overlapping subspaces. Observe that $\boldsymbol{\Phi}_1$ can be transformed into a BLT matrix and Corollary 2.3 can be invoked to compute the number of full-rank matrices that have the structure of $\boldsymbol{\Phi}_1$. If $\boldsymbol{\Phi}_1^{(3)}$ contains r_1 linearly independent columns, the remaining $m_1 - r_1$ columns of $(\boldsymbol{\Phi}_1^{(1)}, \boldsymbol{\Phi}_1^{(2)})$ should also be linearly independent for $\boldsymbol{\Phi}_1$ to have rank m_1. Using either (2.7) or (2.11), the number of full-rank realizations of $\boldsymbol{\Phi}_1$ can be obtained by

$$\gamma_{\boldsymbol{\Phi}_1} = \gamma_{r_1}(n_2, w_1)\, \gamma(n_1, m_1 - r_1)\, q^{n_1 r_1}$$

where $\max(0, m_1 - n_1) \leq r_1 \leq \min(n_2, w_1)$. When the rank of $\boldsymbol{\Phi}_1^{(3)}$ is r_1, the number of linearly independent rows of $\boldsymbol{\Phi}_1^{(3)}$ is also r_1. Therefore, as per Lemma 2.4, $n_2 - r_1$ rows of $(\boldsymbol{\Phi}_2^{(1)}, \boldsymbol{\Phi}_2^{(2)})$ should only be considered in the enumeration of all valid full-rank realizations of $\boldsymbol{\Phi}_2$ given by

$$\gamma_{\boldsymbol{\Phi}_2} = \gamma_{r_2}(n_3, w_2)\, \gamma(n_2 - r_1, m_2 - r_2)\, q^{(m_2 - r_2)w_1}\, q^{n_2 r_2}$$

where $\min(0, m_2 - n_2 + r_1) \leq r_2 \leq \max(n_3, w_2)$. If the product $\gamma_{\boldsymbol{\Phi}_1}\gamma_{\boldsymbol{\Phi}_2}$ is summed over all values of r_1 and r_2, expression (2.14) is obtained. □

Proposition 2.6. *A BTD matrix* $\mathbf{M} = (\mathbf{M}_1; \ldots; \mathbf{M}_L) \in \mathbb{F}_q^{n \times m}$ *has been built by vertically concatenating* $\mathbf{M}_i \in \mathbb{F}_q^{n_i \times m}$ *for* $i = 1, \ldots, L$*, where* $n = n_1 + \ldots + n_L$*. For* $s_i \leq e_i$*, let all elements of* $\mathbf{M}_i$ *in columns* s_i*,* e_i *and in-between take values from* $\mathbb{F}_q$ *while the remaining columns of* $\mathbf{M}_i$ *consist of zeros. As per the BTD structure requirements, we have* $s_1 = 1$*,* $e_{i-2} < s_i \leq s_{i+1}$*,* $e_i \leq e_{i+1}$ *and* $e_L = m$*. The number of full-rank realizations of* $\mathbf{M}$ *is given by*

$$\gamma_{\text{BTD}}(\mathbf{M}) = \sum_{r_1} \cdots \sum_{r_{L-1}} \prod_{i=1}^{L} \gamma_{r_i}(n_{i+1}, w_i)\gamma(n_i - r_{i-1}, m_i - r_i) q^{\varphi_i} \tag{2.15}$$

where:
$m_i = e_i - e_{i-1}$ *for* $i = 2, \ldots, L$ *and* $m_1 = e_1$ *for* $i = 1$*,*
$w_i = e_i - s_{i+1} + 1$ *for* $i = 1, \ldots, L-1$ *and* $w_L = 0$ *for* $i = L$*,* $\varphi_i = (m_i - r_i)w_{i-1} + n_i r_i$*,*
$n = n_1 + n_2 + \ldots + n_L \geq m$
and r_i*, for* $i = 1, \ldots, L-1$*, takes values in the range*
$r_i \geq \max(0, m_i - n_i + r_{i-1})$ *and*
$r_i \leq \min(n_{i+1}, w_i)$*, while* $r_0 = r_L = 0$*.*

Proof. The BTD matrix $\mathbf{M}$ can be rewritten as a horizontal concatenation of L matrices $(\boldsymbol{\Phi}_1, \ldots, \boldsymbol{\Phi}_L)$, where

$$\boldsymbol{\Phi}_i = \left(\overline{\mathbf{0}}_i \,;\, \left(\boldsymbol{\Phi}_i^{(1)}, \boldsymbol{\Phi}_i^{(2)} \right) ;\, \left(\mathbf{0}_i \,,\, \boldsymbol{\Phi}_i^{(3)} \right) ;\, \underline{\mathbf{0}}_i \right)$$

for $i = 1, \ldots, L-1$. Using the notation of Lemma 2.5, the dimensions of the random matrices $\boldsymbol{\Phi}_i^{(1)}$, $\boldsymbol{\Phi}_i^{(2)}$ and $\boldsymbol{\Phi}_i^{(3)}$ are $n_i \times (m_i - w_i)$, $n_i \times w_i$ and $n_{i+1} \times w_i$, respectively. On the other hand, the dimensions of the zero matrices $\overline{\mathbf{0}}_i$, $\mathbf{0}_i$ and $\underline{\mathbf{0}}_i$ are $(\sum_{k=1}^{i-1} n_k) \times m_i$, $n_{i+1} \times (m_i - w_i)$ and $(\sum_{k=i+2}^{L} n_k) \times m_i$, respectively. For $i = L$, $\boldsymbol{\Phi}_L$ has the following structure

$$\mathbf{\Phi}_L = \left(\overline{\mathbf{0}}_L \,;\, \mathbf{\Phi}_L^{(1)} \right)$$

where $\overline{\mathbf{0}}_L$ is the $(n - n_L) \times m_L$ zero matrix and $\mathbf{\Phi}_L^{(1)}$ is an $n_L \times m_L$ random matrix. If we consider the first $L-1$ sub-matrices only, the number of full-rank matrices with structure $(\mathbf{\Phi}_1, \ldots, \mathbf{\Phi}_{L-1})$ is

$$\gamma_{(\mathbf{\Phi}_1,\ldots,\mathbf{\Phi}_{L-1})} = \sum_{r_1} \cdots \sum_{r_{L-1}} \prod_{i=1}^{L-1} \gamma_{r_i}(n_{i+1}, w_i)\gamma(n_i - r_{i-1}, m_i - r_i) q^{\varphi_i} \tag{2.16}$$

as per Lemma 2.5. The inclusion of the last sub-matrix $\mathbf{\Phi}_L$ will increase the number of full-rank realisations of $\mathbf{M}$ by a factor of $\gamma_{\mathbf{\Phi}_L}$, where

$$\gamma_{\mathbf{\Phi}_L} = \gamma(n_L - r_{L-1},\, m_L)\, q^{m_L w_{L-1}}. \tag{2.17}$$

The product of (2.16) and (2.17) gives (2.15). Notice that (2.17) can be incorporated into (2.16) if we change the upper limit of the summation index i from $L-1$ to L and set $r_L = 0$. □

This section focused on random block matrices and demonstrated that Proposition 2.2 can be used to compute the number of full-rank BD matrices but, as Corollary 2.3 explained, it can also be extended to the case of BLT matrices. Proposition 2.6 was introduced for the enumeration of full-rank BTD matrices. The following section will discuss how the analysis of random block matrices can be used in the performance assessment of practical network coding techniques.

2.4 Assessment of Network Coding Techniques

In conventional network coding (NC), a source node segments a message into m source packets of equal length, linearly combines them over the finite field $\mathbb{F}_q$ and generates n coded packets. This implies that the i^{th} coded packet y_i, for $i = 1, \ldots, n$, can be expressed as follows

$$y_i = \sum_{j=1}^{m} c_{i,j} x_j \tag{2.18}$$

where x_j represents the j^{th} source packet of the message. As already described in Chapter 1, that the coefficients $c_{i,j}$ are selected uniformly at random over the finite field $\mathbb{F}_q$ in RLNC. For a given value of i, the sequence $c_{i,1}, c_{i,2}, \ldots, c_{i,m}$ forms a row vector, which is known as the coding vector of the output coded packet y_i, and is transmitted along with y_i in the packet header. Using matrix notation, expression (2.18) can be rewritten as

$$\mathbf{Y} = \mathbf{C}\mathbf{X} \tag{2.19}$$

where $\mathbf{Y} \in \mathbb{F}_q^{n\times 1}$, $\mathbf{C} \in \mathbb{F}_q^{n\times m}$ and $\mathbf{X} \in \mathbb{F}_q^{m\times 1}$ are the matrices whose elements are y_i, $c_{i,j}$ and x_j, respectively. Matrix $\mathbf{C}$ is also known as the coding matrix.

At a receiving node, when $\hat{n} \geq m$ coded packets have been received, the coding vectors of the received coded packets are stacked together to generate a decoding matrix $\mathbf{D}$ of dimensions $\hat{n} \times m$. A receiver can successfully decode the source message if and only if m linearly independent coded packets have been received or, equivalently, the rank of $\mathbf{D}$ is m. Therefore, the probability of successful decoding a source message, given that $\hat{n}$ coded packets have been received, is associated with the full-rank probability of $\mathbf{D}$, which is given by $P(\hat{n}, m)$ in (2.2).

If the transmission of the $n \geq \hat{n}$ coded packets is modeled as a sequence of n Bernoulli trials, whereby ϵ signifies the probability that a transmitted coded packet will be erased, the probability of a receiving node decoding the source message for a coding matrix $\mathbf{C}$ and all possible realizations of the decoding matrix $\mathbf{D}$ can be written as

$$P_{\text{dec}}(\mathbf{C}) = \sum_{\hat{n}=m}^{n} B(\hat{n}, n, \epsilon)\, P(\hat{n}, m) \tag{2.20}$$

where $B(\hat{n}, n, \epsilon)$ is the probability mass function of the binomial distribution, given by

$$B(\hat{n}, n, \epsilon) = \binom{n}{\hat{n}} (1-\epsilon)^{\hat{n}}\, \epsilon^{n-\hat{n}}. \tag{2.21}$$

Due to the fact that both the coding matrix $\mathbf{C}$ and the decoding matrix $\mathbf{D}$ can be very dense, RLNC is referred to as a *dense code* [104] and the decoding process can be computationally expensive. Various *layered* RLNC schemes have been considered in the literature as a means to reduce the complexity of conventional RLNC or introduce unequal error protection. These schemes organize the m source packets into L overlapping or non-overlapping groups, referred to as *generations* [105]. The remainder of this section is concerned with the characterization of the decoding probability of three widely-used layered RLNC schemes using expressions (2.10), (2.11) and (2.15).

2.4.1 Non-Overlapping Generations RLNC (NOG-RLNC)

Let the i^{th} generation, denoted by $\mathbf{G}_i$, contain k_i source packets. When each packet belongs to a single generation only, the generations are non-overlapping, i.e., $\mathbf{G}_i \cap \mathbf{G}_j = \varnothing$ for all $i \neq j$, as shown in Fig. 2.2. Similarly, if m_i denotes the number of source packets in $\mathbf{G}_i$ that are not shared with any other generation, we can write $m_i = k_i$ for any

$i = 1, \ldots, L$ while $m = \sum_{i=1}^{L} m_i$. During the encoding phase, n_i coded packets are generated by linearly combining the m_i source packets of generation $\mathbf{G}_i$, for $i = 1, \ldots, L$. Thus, each generation is associated with a coding matrix, which is a sub-matrix of the coding matrix $\mathbf{C}$ and does not overlap with the coding matrices of the other generations. Both matrices $\mathbf{C}$ and $\mathbf{D}$ have a BD structure, as described in Section 2.3.1.

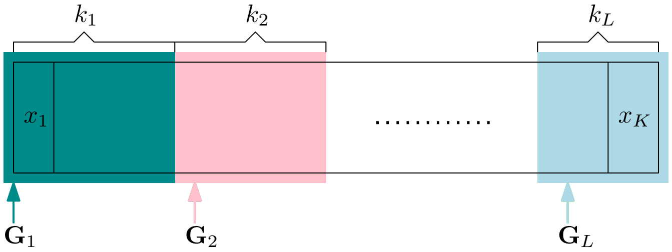


FIGURE 2.2: Example of NOG-RLNC. The source packets $x_1, \ldots, x_m$ have been organized into L generations $\mathbf{G}_1, \ldots, \mathbf{G}_L$. Generation $\mathbf{G}_i$ contains k_i source packets.

Unlike conventional RLNC, a receiver in Non-Overlapping Generations RLNC (NOG-RLNC) can attempt to decode generation $\mathbf{G}_i$ independently of the other generations, if $n_i \geq m_i$ coded packets from that generation have been received. The complete source message will be reconstructed if each $\hat{n}_i \times m_i$ sub-matrix of $\mathbf{D}$ has full rank. Dividing (2.10) by the number of all possible realizations of $\mathbf{D}$ and taking the average over all values of $n_1, \ldots, n_L$ leads to the probability of decoding the source message, that is,

$$P_{\text{dec}}^{\text{NOG}}(\mathbf{C}) = \sum_{\hat{n}_1 = m_1}^{n_1} B(\hat{n}_1, n_1, \epsilon) \cdots \sum_{\hat{n}_L = m_L}^{n_L} B(\hat{n}_L, n_L, \epsilon) \frac{\gamma_{\text{BD}}(\mathbf{D})}{q^{\sum_{j=1}^{L} \hat{n}_j m_j}}$$

which further reduces to

$$P_{\text{dec}}^{\text{NOG}}(\mathbf{C}) = \prod_{i=1}^{L} \sum_{\hat{n}_i = m_i}^{n_i} B(\hat{n}_i, n_i, \epsilon) \, \frac{\gamma(\hat{n}_i, m_i)}{q^{\hat{n}_i m_i}}. \tag{2.22}$$

Expression (2.22) has also been presented in [43, eq. (7)] but has been included in this chapter for completeness as is a special case of the proposed framework.

2.4.2 Expanding Generations RLNC (EG-RLNC)

Expanding Generations RLNC (EG-RLNC) [31] is considered to be a promising unequal error protection scheme for layered video streaming [43, 44, 106]. In this scheme, the m source packets are grouped into L generations $\mathbf{G}_1, \ldots, \mathbf{G}_L$ such that any generation $\mathbf{G}_i$ contains all previous generations, i.e., $\mathbf{G}_1, \ldots, \mathbf{G}_{i-1}$, as depicted in Fig. 2.3. Let k_i denote the total number of source packets in $\mathbf{G}_i$ and m_i represent the number of source packets in $\mathbf{G}_i$ that do not belong to any lower-indexed generations. We can write $|\mathbf{G}_i \setminus \mathbf{G}_{i-1}| = m_i$ and $m_i = k_i - k_{i-1}$ for $i = 2, \ldots, L$, while $m_1 = k_1$ for $i = 1$. Furthermore, $m = \sum_{i=1}^{L} m_i$. An $n_i \times k_i$ random coding matrix is used to encode generation $\mathbf{G}_i$. The vertical concatenation of the coding matrices of the L generations compose the $n \times m$ coding matrix $\mathbf{C}$. When transmitting over a packet erasure channel, $\hat{n}_i \leq n_i$ coded packets associated to $\mathbf{G}_i$ will be successfully received and will contribute to the construction of the $n \times m$ decoding matrix $\mathbf{D}$, which will consist of L sub-matrices of dimensions $n_i \times k_i$, for $i = 1, \ldots, L$. In EG-RLNC, both $\mathbf{C}$ and $\mathbf{D}$ have the BLT structure described in Section 2.3.2.

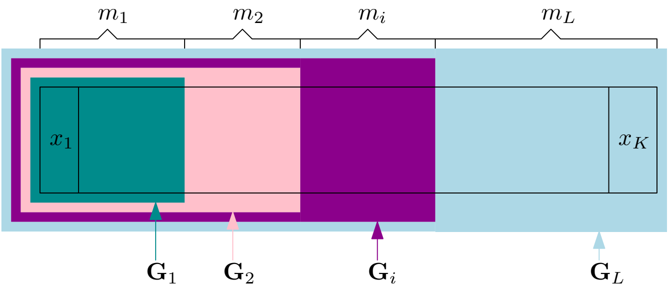


Figure 2.3: Example of EG-RLNC. Each generation $\mathbf{G}_i$ is nested in generation $\mathbf{G}_{i+1}$. The number of source packets that belong to a generation $\mathbf{G}_i$ but not to lower-indexed generations is denoted by m_i.

In contrast to NOG-RLNC, successful decoding of generation $\mathbf{G}_i$ in EG-RLNC implies that generations $\mathbf{G}_1, \ldots, \mathbf{G}_{i-1}$ have also been decoded, hence k_i source packets that belong to generations $\mathbf{G}_{i+1}, \ldots, \mathbf{G}_L$ have been decoded. Following the same reasoning as in Section 2.4.1, we find that the probability of obtaining a full-rank realization of the decoding matrix $\mathbf{D}$ from the random coding matrix $\mathbf{C}$, and thus decoding the L generations, is given by

$$P_{\text{dec}}^{\text{EG}}(\mathbf{C}) = \sum_{\substack{\hat{n}_1, \ldots, \hat{n}_L \\ \hat{n}_1 + \ldots + \hat{n}_L \geq m}} \left(\prod_{i=1}^{L} B(\hat{n}_i, n_i, \epsilon) \right) \frac{\gamma_{\text{BLT}}(\mathbf{D})}{q^{\sum_{j=1}^{L} \hat{n}_j k_j}} \tag{2.23}$$

where $\sum_{j=0}^{\ell} \hat{n}_j k_j$ enumerates the elements of $\mathbf{D}$ that take values from $\mathbb{F}_q$ and $\gamma_{\text{BLT}}(\mathbf{D})$ can be obtained from (2.11) for $e_i = k_i$. We note that (2.23) is equivalent to [31, eq. (13)] but employs (2.3) to compute the number of all random matrices of particular dimensions that have a specific rank as opposed to the more involved [31, eq. (11)]. Having established the generality of Proposition 2.2, which gave rise to (2.10) and (2.11) and encompasses specific RLNC designs, namely NOG-RLNC and EG-RLNC, we explore the applicability of Proposition 2.6 to another RLNC scheme in the following section.

2.4.3 Sliding Generations RLNC (SG-RLNC)

The use of a sliding window mechanism for the selection of a subset of source packets, based on which coded packets are generated, was proposed in [34] for random fountain codes and extended to Raptor codes in [107]. The concept of a window sliding over the source packets was later introduced into RLNC for wireless mesh networks [35] and networks compatible with the Transmission Control Protocol (TCP) [108]. Sliding window mechanisms are also being considered by the Network Coding Research Group of the Internet Research Task Force (IRTF) for the practical implementation of network coding in future Internet architectures [109].

In this scheme, which we refer to as Sliding Generations RLNC (SG-RLNC), the L generations overlap but are not nested as in EG-RLNC. Fig. 2.4 shows a particular implementation of SG-RLNC according to which generation $\mathbf{G}_i$ shares w_{i-1} of its k_i source packets with generation $\mathbf{G}_{i-1}$ only, that is, $|\mathbf{G}_{i-1} \cap \mathbf{G}_i| = w_{i-1}$. Note that, each source packet can belong to *at most* two generations, that is, $|\mathbf{G}_{i-2} \cap \mathbf{G}_i| = \varnothing$. If m_i is the number of packets in $\mathbf{G}_i$ that are not shared with $\mathbf{G}_{i-1}$, we can write $k_i = w_{i-1}+m_i$, where $k_1 = m_1$ for $i = 1$. The relationship $m = \sum_{i=1}^{L} m_i$ applies in this case too. The number of shared packets w_{i-1} between generations $\mathbf{G}_{i-1}$ and $\mathbf{G}_i$ can take values in the range $0 \leq w_{i-1} \leq m_{i-1}$, while the ratio

$$\frac{w_{i-1}}{k_i} = \frac{w_{i-1}}{w_{i-1}+m_i} \tag{2.24}$$

represents the amount of overlap between $\mathbf{G}_{i-1}$ and $\mathbf{G}_i$ in terms of the cardinality of $\mathbf{G}_i$. The design requirements of the considered SG-RLNC implementation impose constraints on matrices $\mathbf{C}$ and $\mathbf{D}$, which both comply with the BTD structure presented in Section 2.3.3.

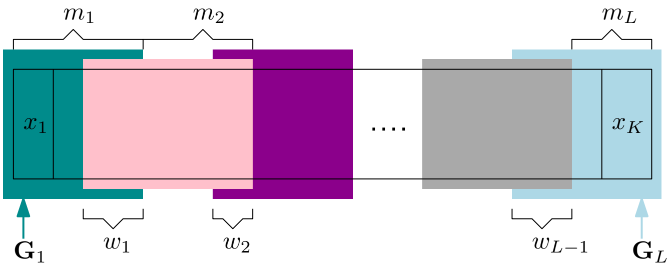


FIGURE 2.4: Example of SG-RLNC. The m source packets are members of L contiguous generations $\mathbf{G}_1, \ldots, \mathbf{G}_L$. For $i > 1$, generations $\mathbf{G}_{i-1}$ and $\mathbf{G}_i$ have w_{i-1} source packets in common.

Decoded source packets from $\mathbf{G}_i$ that are shared with $\mathbf{G}_{i-1}$ can assist in the decoding of additional source packets from $\mathbf{G}_{i-1}$ and vice versa. As a result, the decoding probability of each generation will be higher than that of NOG-RLNC but lower than that of EG-RLNC. If the coding matrix $\mathbf{C}$ dictates the transmission of n_i coded packets associated with generation $\mathbf{G}_i$ over a packet erasure channel and $\hat{n}_i$ of them are received, the probability that the decoding matrix $\mathbf{D}$ will have full rank assumes a similar expression to (2.23), i.e.,

$$P_{\text{dec}}^{\text{SG}}(\mathbf{C}) = \sum_{\substack{\hat{n}_1,\ldots,\hat{n}_L \\ \hat{n}_1+\ldots+\hat{n}_L \geq m}} \left(\prod_{i=1}^{L} B(\hat{n}_i, n_i, \epsilon) \right) \frac{\gamma_{\text{BTD}}(\mathbf{D})}{q^{\sum_{j=1}^{L} \hat{n}_j k_j}} \tag{2.25}$$

where $\gamma_{\text{BTD}}(\mathbf{D})$ can be obtained from (2.15) for $m_i = k_i - w_{i-1}$ when $i = 2, \ldots, L$ and $m_1 = k_1$ for $i = 1$.

It is important to emphasize that the requirement for $w_i \leq m_i$ in the considered SG-RLNC scheme stems from the constraint $e_{i-2} \leq s_{i+1}$ in Proposition 2.6, which implies that the overlap between two adjacent generations in the SG-RLNC implementation shown in Fig. 2.4 cannot exceed 50%, which is achieved for $w_{i-1} = m_i$ based on (2.24). Although each source packet could belong to more than two generations in the general case of SG-RLNC, Section 2.5 will demonstrate that an overlap smaller than 50% suffices for SG-RLNC to yield the same decoding probability as EG-RLNC for low erasure probabilities. Considering that RLNC is an Application Layer Forward Error Correction (AL-FEC) scheme, typical values of the erasure probability are $\epsilon \leq 0.2$ for TCP traffic [108] and $\epsilon \leq 0.1$ for Long Term Evolution (LTE) systems [110]. We can thus conclude that Proposition 2.6 can be used to characterize the decoding probability of a constrained, yet practical, class of SG-RLNC implementations.

2.5 Results and Discussions

The previous sections developed a mathematical framework for enumerating particular structures of full-rank random block matrices, which formed the basis for the performance evaluation of well-known RLNC schemes that use the concepts of non-overlapping, expanding and sliding generations. This section is concerned with the validation of the derived theoretical expressions and the performance comparison of the three considered RNLC schemes.

2.5.1 Performance Comparison between NOG-RLNC, SG-RLNC and EG-RLNC over Non-erasure Channels

In order to access the accuracy of the expressions derived in Section 2.3, we initially set $\epsilon = 0$ and $\hat{n}_i = n_i$ for $i = 1, \ldots, L$ in (2.22), (2.23) and (2.25) to pinpoint potential distortions that would have been flattened if averaging had been performed. The decoding probability of SG-RLNC for $m = 20$ source packets and $L = 2$ generations is first considered. Generation $\mathbf{G}_1$ consists of $k_1 = m_1 = 10$ source packets. Generation $\mathbf{G}_2$ comprises $k_2 = w_1 + m_2$ source packets, where w_1 varies from 0 to 10 and $m_2 = 10$. Note that SG-RLNC reduces to NOG-RLNC for $w_1 = 0$, and is equivalent to EG-RLNC for $w_1 = 10$.

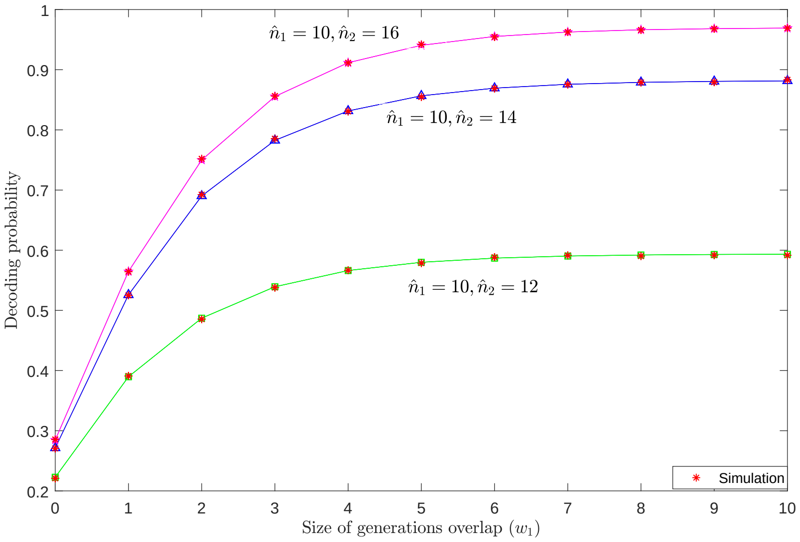


Figure 2.5: Comparison between theoretical results for SG-RLNC obtained from (2.25) and simulation results for $L = 2$ generations and different values of $\hat{n}_2$. The remaining parameters have been set as follows: $q = 2$, $m = 20$, $m_1 = m_2 = 10$, $n_1 = \hat{n}_1 = 10$, $n_2 = \hat{n}_2$ and $\epsilon = 0$.

Fig. 2.5 depicts the impact of the number of received coded packets from each generation on the decoding probability. Different values of $\hat{n}_1$ and $\hat{n}_2$, which represent the number of received coded packets that were generated from generations $\mathbf{G}_1$ and $\mathbf{G}_2$, respectively, were used in the simulations. Observe that the theoretical results exactly match the results obtained from Monte Carlo simulations. The effect of the number of shared source packets between the two generations, represented by w_1, is also illustrated. If we refer to the difference $\delta_2 = \hat{n}_2 - m_2$ as the *overhead*, Fig. 2.5 demonstrates the greater impact that the value of w_1 has on the decoding probability for an increasing overhead δ_2.

Fig. 2.6 and Fig. 2.7 consider all three RLNC schemes and compares simulation results to theoretical values when $m = 60$ source packets are organized into three generations,

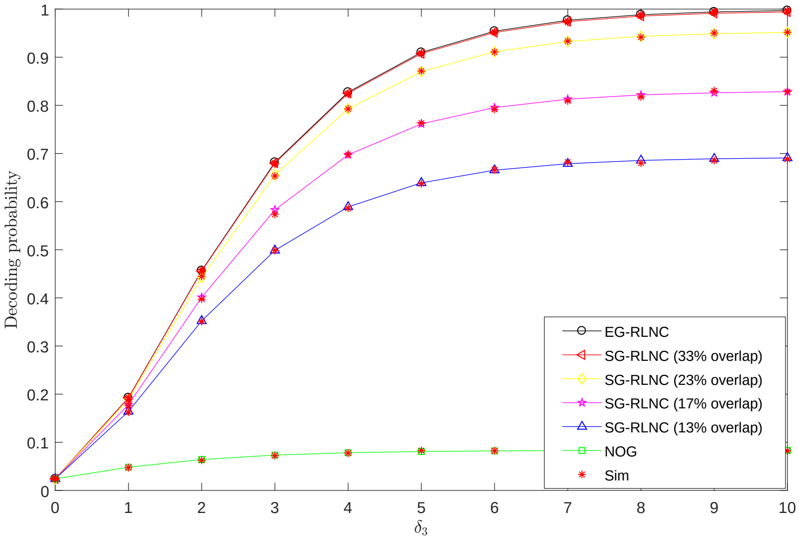


FIGURE 2.6: Comparison between NOG-RLNC, SG-RLNC and EG-RLNC for $L = 3$, $m = 60$, $m_1 = m_2 = m_3 = 20$, $\hat{n}_1 = \hat{n}_2 = 20$ and $\hat{n}_3 = 20 + \delta_3$. Various percentages of overlap in the case of SG-RLNC have been considered. Furthermore, $n_i = \hat{n}_i$ for all values of i, $q = 2$ and $\epsilon = 0$.

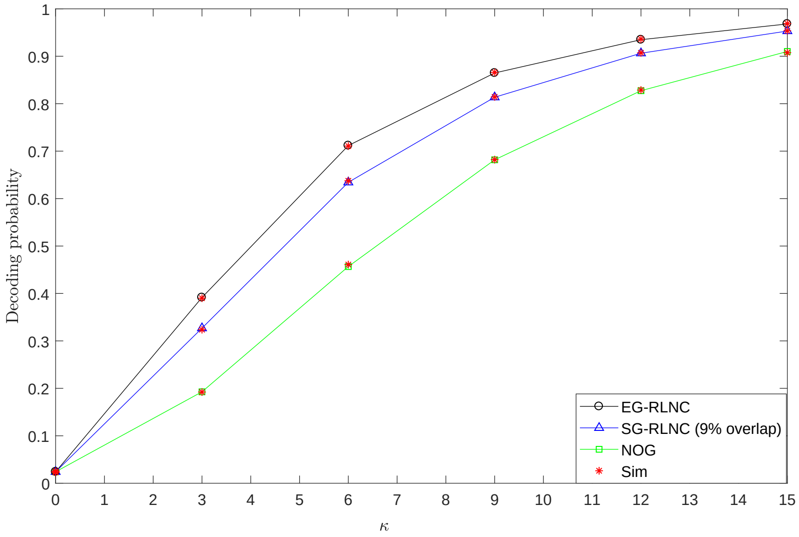


FIGURE 2.7: Comparison between NOG-RLNC, SG-RLNC and EG-RLNC for $L = 3$, $m = 60$, $m_1 = m_2 = m_3 = 20$, $\hat{n}_1 = \hat{n}_2 = \hat{n}_3 = 20 + \kappa$, where κ represents overhead per generation. In addition, $q = 2$, $\epsilon = 0$ and the overlap in SG-RLNC is set to 9%

.

$\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_3$, such that $m_1 = m_2 = m_3 = 20$. More specifically in Fig. 2.6, the number of received coded packets associated to each generation are $\hat{n}_1 = \hat{n}_2 = 20$ and $\hat{n}_3 = 20 + \delta_3$, where $\delta_3 = 0, \ldots, 10$ is the overhead of generation $\mathbf{G}_3$. As expected and confirmed in Fig. 2.6, an increasing overhead δ_3 can only increase the probability of decoding the source messages of $\mathbf{G}_3$ but does not notably improve the overall decoding probability. However, if we opt for an SG-RLNC configuration and allow adjacent generations to overlap, the decoding probability can significantly improve. Furthermore, if the generations are nested so that $k_1 = 20$, $k_2 = 40$ and $k_3 = 60$, the corresponding

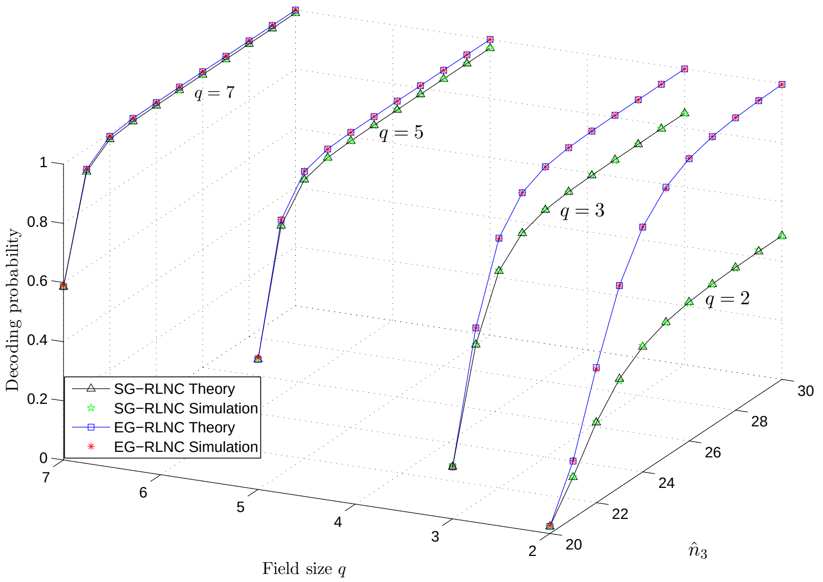


Figure 2.8: Theoretical predictions and simulation results for SG-RLNC and EG-RLNC, when the field size q is 2, 3, 5 or 7. The system parameters are $L = 3$, $m = 60$, $m_1 = m_2 = m_3 = 20$, $n_1 = \hat{n}_1 = 20$, $n_2 = \hat{n}_2 = 20$ and $\epsilon = 0$. The overlap in SG-RLNC is fixed at 9%.

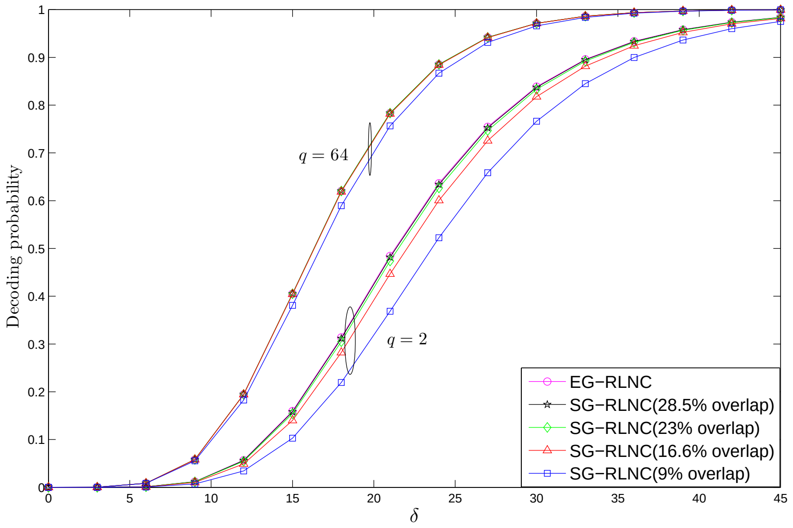


Figure 2.9: Effect of the field size q on the decoding probability of SG-RLNC and EG-RLNC for $L = 3$, $m = 60$, $m_1 = m_2 = m_3 = 20$ and $\epsilon = 0.2$. If the overhead per generation is $\kappa = 0, 1, \ldots, 15$, the overall overhead is $\delta = 3\kappa$, i.e., $\delta = 0, 3, \ldots, 45$.

EG-RLNC scheme should yield a higher decoding probability than both NOG-RLNC and SG-RLNC. Indeed, as Fig. 2.6 shows, EG-RLNC performs better than SG-RLNC for low percentages of overlap. However, when the overlap between generations is 33%, the more sparse and, thus, less computationally intensive SG-RLNC yields a similar performance to that of EG-RLNC. Moreover, the superiority of decoding performance of both the EG-RLNC and SG-RLNC over NOG-RLNC can also be seen in Fig 2.9. Where, the figure exhibits the relationship between the decoding performance of each coding scheme and the overall overhead i.e., $\delta = 3\kappa$, where κ denotes the overhead per generation. In all cases, the theoretical predictions match the simulation results.

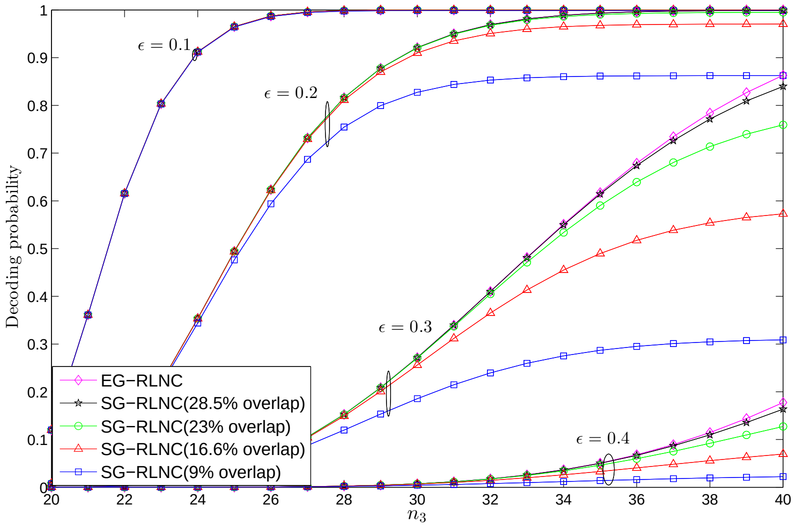


FIGURE 2.10: Performance comparison between SG-RLNC and EG-RLNC for $m = 60$, $m_1 = m_2 = m_3 = 20$, $n_1 = n_2 = 26$, $\epsilon \in \{0.1, 0.2, 0.3, 0.4\}$ and $q = 256$. Various percentages of overlap for SG-RLNC have been considered.

Whereas Fig. 2.5, Fig. 2.6 and Fig. 2.7 focused on obtaining results for RLNC schemes over $\mathbb{F}_2$ when $\epsilon = 0$, Fig. 2.8 uses the same setup but different values of field size q to compare the decoding probabilities of SG-RLNC and EG-RLNC. The percentage of overlap between generations in SG-RLNC has been fixed at 9%. As both the theoretical predictions and the simulation results confirm, the probability that the received coded packets are linearly independent improves as the field size increases from $q = 2$ to $q = 7$ and the performance gap between the decoding probabilities of SG-RLNC and EG-RLNC closes.

2.5.2 Performance Comparison between SG-RLNC and EG-RLNC over Erasure Channels

Having demonstrated the accuracy of the proposed theoretical framework for $\epsilon = 0$, we can now take a closer look at the performance of SG-RLNC and EG-RLNC for non-zero erasure probabilities. Fig. 2.9 presents the effect of the field size q on the decoding probability of SG-RLNC and EG-RLNC when $\epsilon = 0.2$. The $m = 60$ source packets are divided into generations $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_3$ such that $m_1 = m_2 = m_3 = 20$. The number of transmitted coded packets per generation is $n_i = 20 + \kappa$, for $i = 1, 2, 3$, where κ denotes the overhead per generation. The overall overhead is $\delta = 3\kappa$. For SG-RLNC employing a 9% overlap between generations, increasing the field size from $q = 2$ to $q = 64$ can cause an increase in the decoding probability by up to 39% (for $\delta = 21$). Higher amounts of overlap markedly improve the performance of SG-RLNC for $q = 2$. On the other hand, an increase in the overlap from 9% to 16.6% is sufficient for SG-RLNC to achieve a performance comparable to that of EG-RLNC for $q = 64$.

Fig. 2.10 compares the performance of SG-RLNC and EG-RLNC for $q = 256$ in various channel conditions represented by different erasure probabilities. Both schemes consider $m = 60$ source packets distributed among generations $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_3$, such that $m_1 = m_2 = m_3 = 20$. The number of transmitted coded packets per genetation are $n_1 = n_2 = 26$ and $n_3 = 20, \ldots, 40$. Fig. 2.10 shows that, when large finite fields are used, the decoding probabilities of the considered schemes are indistinguishable for erasure probabilities as low as 0.1. As the channel conditions deteriorate, low percentages of overlap can significantly degrade the performance of SG-RLNC. Nevertheless, a 28.5% overlap between generations is still sufficient for SG-RLNC to achieve a decoding probability similar to that of EG-RLNC, even for $\epsilon = 0.4$.

2.6 Summary

In this chapter, we focused on random block matrices and investigated three different matrix structures over finite fields. In particular, we presented a framework based on which exact analytical expressions were derived for the number of full-rank matrices complying with each structure. Furthermore, we mapped the three matrix structures onto RLNC schemes that are available in the literature and use the concepts of non-overlapping, expanding and sliding generations to either reduce the decoding complexity or incorporate unequal error protection features. The design parameters of these schemes allow to adjust the level of sparsity and the desired decoding performance. We observed the trade-off between the sparsity and the decoding performance, i.e., the higher the sparsity is, the lower the decoding performance will be. More importantly, the derived expressions for RLNC using sliding generations that can overlap by up to 50% demonstrated that a low amount of overlap between generations in practical settings can yield a similar decoding probability to that of the more computationally expensive RLNC based on expanding generations. In this chapter, specifically, we made the following contributions:

- We derived expressions for the enumeration of full-rank matrices that are constructed by the vertical (Lemma 2.1) or horizontal (Lemmata 2.4 and 2.5) concatenation of random matrices or random block matrices over finite fields.
- We revisited the formula that computes the number of full-rank random matrices and rewrote it for the case of partitioned random matrices (Proposition 2.2).

We then extended this formula to random block lower-triangular matrices (Corollary 2.3) and adjusted it for random block tri-diagonal matrices (Proposition 2.6).

- We demonstrated that the proposed framework offers a unified RMT-based approach for the analysis of practical RLNC schemes, which are described by random block matrices over finite fields of any size. In particular, we showed that our framework generates the well-known decoding probability of RLNC over non-overlapping windows and a more compact expression for the decoding probability of RLNC over expanding windows [31]. The proposed framework can also be used for the performance analysis of RLNC over sliding windows, which is often carried out based on simulations, e.g., [34].

Chapter 3

Random Linear Network Coding for Coded Cooperation

In the previous chapter, we developed a mathematical framework to evaluate and characterize the performance in terms of the decoding probability of RLNC techniques suitable for broadcast or multicast communication. In this chapter, we aim to study and evaluate the performance of RLNC in single-relay as well as multi-relay assisted cooperative networks. Finally, we propose and develop a novel framework which integrates the benefits of NOMA and RLNC based cooperative relaying.

Section 3.1 of this chapter focuses on a network configuration that encompasses both intra-session network coding at the source nodes, as in [111–113], and inter-session network coding at the relay node, as in [7, 114, 115]. In our study, we have looked at the *decode-and-forward* relaying scheme, that is, network-coded packets received by the relay node are decoded and re-encoded before they are forwarded to the destination node. The probability that the destination node will successfully decode the source packets of both source nodes is used as the performance measure of the system. The derived probability expressions could be adapted to other network-coded relaying strategies that incorporate both intra-session and inter-session network coding schemes, as in [116], or be used as benchmarks in performance comparisons.

Section 3.2 presents linear network coding over a multi-source multi-relay network, where m source nodes are supported by n relay nodes for the delivery of packets over packet erasure channels. To the best of our knowledge, an exact expression for the decoding failure probability that the destination will fail to decode the packets of all source nodes is not available but an effort has been made in [59], in which the author derives upper and lower bounds. However, the bounds presented in [59] are tight only for a certain range of parameters, including erasure probabilities, the values of m, n and the size of the finite field. As shown in Section 3.2.4, the existing upper bound is poor for a large number of source nodes and for large finite fields. Moreover, the existing lower bound is independent of the field size and is loose for small finite fields and low erasure probabilities. In this chapter our goal is to derive improved bounds on the probability of decoding failure and demonstrate the performance.

As identified in Chapter 1, RLNC has also the potential to address ever increasing number of users and devices in future cellular networks (5G and beyond 5G), and NOMA can efficiently utilize the bandwidth resources. After the performance characterisation of network coding based cooperation in Sections 3.1 and 3.2, Section 3.3 exploits the network-coded cooperation in a NOMA-based scenario with two groups of source nodes, where each group communicates with a different destination node via multiple relay nodes. In this work, using the fundamentals of RLNC and uplink/downlink NOMA, we derive closed-form expressions for the network performance, in terms of the decoding probability at each node, and the system throughput. To the best of our knowledge, this work represents the first attempt to characterise the performance of NOMA-based RLNC cooperation.

3.1 Random Linear Network Coded Cooperation in Two Source Single Relay Networks

This section considers the multiple-access relay channel in a setting where two source nodes transmit packets to a destination node, both directly and via a relay node, over packet erasure channels. Intra-session network coding is used at the source nodes and inter-session network coding is employed at the relay node to combine the successfully received source packets of both source nodes. In this work, we investigate the performance of the network-coded system in terms of the probability that the destination node will successfully decode the source packets of the two source nodes. We build our analysis on fundamental probability expressions for random matrices over finite fields and we derive upper bounds on the system performance for the case of systematic and non-systematic network coding.

3.1.1 System Model and Problem Statement

We consider a network comprising two source nodes S_1 and S_2 having different data contents, a relay node R and a destination node D, as shown in Fig. 3.1. Nodes S_1 and S_2 segment data into m_1 and m_2 equally-sized packets, respectively. Let $x_1, \ldots, x_{m_1}$ denote the source packets of node S_1 while $x_{m_1+1}, \ldots, x_{m_1+m_2}$ represent the source packets of node S_2. Each source node employs random linear network coding to combine source packets and generate coded packets. In *non-systematic* network coding, each source transmits $n_\ell \geq m_\ell$ coded packets, where $\ell = 1, 2$. In *systematic* network coding, the first m_ℓ transmitted packets are identical to the source packets, while the remaining $n_\ell - m_\ell$ packets are coded. As is customary in network coding, each coded packet is transmitted along with a coding vector, which contains the m_ℓ coefficients of the respective linear combination. In this work, we consider coefficients that are chosen uniformly at random from the elements of the finite field $\mathbb{F}_2$. Therefore, each coded packet is the bitwise sum of source packets.

Links between network nodes are modelled as packet erasure channels. We use $\epsilon_{\ell \mathrm{D}}$, $\epsilon_{\ell \mathrm{R}}$ and ϵ_{RD} to denote the packet erasure probabilities of the links connecting the ℓ-th source node with the destination node, the ℓ-th source node with the relay node and the relay node with the destination node, respectively. We assume that source nodes transmit on orthogonal channels enabling both the relay and the destination nodes to distinguish transmissions between the source nodes.

The communication process is split into two phases. In the first phase, nodes S_1 and S_2 transmit n_1 and n_2 coded packets, respectively, to node D. Node R overhears the transmissions of the source nodes, stores the successfully received coded packets and attempts to decode them. Let $\hat{n}_\ell$ and n'_ℓ be the number of coded packets from node S_ℓ that were received by the destination node D and the relay node R, respectively. The coding vectors of the received coded packets can be stacked together at the receiving nodes to form coding matrices. At the end of the first phase, the coding matrices at nodes D and R can be expressed in block diagonal form as follows

$$\mathbf{C}_{\mathrm{SD}} = \begin{bmatrix} \mathbf{C}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{C}_2 \end{bmatrix}, \quad \mathbf{C}_{\mathrm{SR}} = \begin{bmatrix} \mathbf{C}'_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{C}'_2 \end{bmatrix} \tag{3.1}$$

where $\mathbf{C}_\ell$ is a $\hat{n}_\ell \times m_\ell$ matrix constructed at node D using the received coding vectors from node S_ℓ, and $\mathbf{C}'_\ell$ is a $n'_\ell \times m_\ell$ matrix that consists of the received coding vectors from node S_ℓ at node R. The dimensions of $\mathbf{C}_{\mathrm{SD}}$ and $\mathbf{C}_{\mathrm{SR}}$ are $(\hat{n}_1 + \hat{n}_2) \times (m_1 + m_2)$ and $(n'_1 + n'_2) \times (m_1 + m_2)$, respectively.

Note that, in order to avoid the correlation between the coded packets generated by the source nodes and the relay nodes, the relay node is considered to support re-encoding operation instead of recoding the received coded packets. Therefore, in the second phase, if the relay node R successfully decoded the source packets of one or both source nodes, it linearly combines them in order to generate n_{R} coded packets. Thus, the coding vector that accompanies each relay-generated coded packet consists of $m_1 + m_2$ entries. If the relay node failed to decode the packets of either S_1 or S_2 then the first m_1 entries or

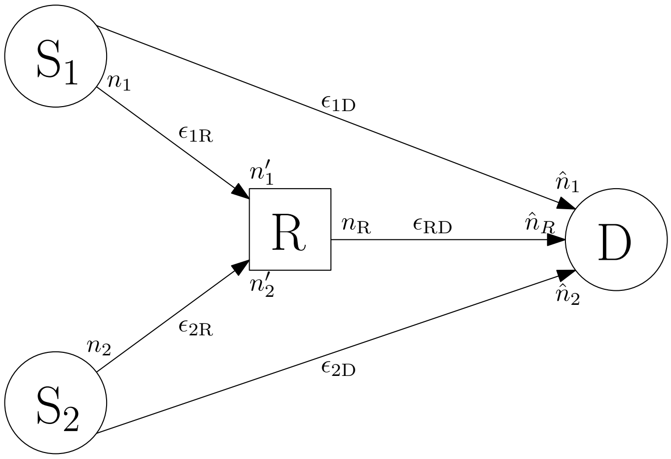


Figure 3.1: Block diagram of a network consisting of two source nodes S$_1$ and S$_2$, a relay node R and a destination node D. The packet erasure probability of each link as well as the number of transmitted and received coded packets at each node are also depicted.

the last m_2 entries of the coding vector, respectively, are set to zero. If $\hat{n}_\mathrm{R}$ of the n_R transmitted coded packets are received by the destination node D, a $\hat{n}_\mathrm{R} \times (m_1 + m_2)$ coding matrix $\mathbf{C}_\mathrm{RD}$ will be created and appended to $\mathbf{C}_\mathrm{SD}$. At the end of the second phase, the coding matrix at node D is

$$\mathbf{C}_\mathrm{D} = \begin{bmatrix} \mathbf{C}_\mathrm{SD} \\ \mathbf{C}_\mathrm{RD} \end{bmatrix} = \begin{bmatrix} \mathbf{C}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{C}_2 \\ \mathbf{C}_{\mathrm{R}1} & \mathbf{C}_{\mathrm{R}2} \end{bmatrix} \tag{3.2}$$

which is a $(\hat{n}_1 + \hat{n}_2 + \hat{n}_\mathrm{R}) \times (m_1 + m_2)$ block angular matrix. Note that $\mathbf{C}_\mathrm{RD}$ has been expressed as the concatenation of matrices $\mathbf{C}_{\mathrm{R}1}$ and $\mathbf{C}_{\mathrm{R}2}$, which were generated by node R and describe linear combinations of source packets originating from nodes S$_1$ and S$_2$, respectively. Note that, all coded packets in the network have the same size, which is customarily taken to be considerably larger than the size of the coding vectors.

The objective of this work is to characterise the system performance of the considered two-source relay-aided network. More specifically, we will carry out a performance analysis to determine the probability that the destination node D will decode the $m_1 + m_2$ source packets of both nodes S$_1$ and S$_2$, given that node D has successfully received at least $m_1 + m_2$ coded packets, that is, $(\hat{n}_1 + \hat{n}_2 + \hat{n}_\mathrm{R}) \geq m_1 + m_2$. The impact of the chosen values for n and n_R on the system performance will also be discussed.

3.1.2 Performance Analysis

Fundamental probabilities related to the rank of random matrices in $\mathbb{F}_2$ are summarised in this section and are subsequently used in the derivation of expressions for the probability that the destination node D will successfully decode the source packets of both source nodes, when they employ either non-systematic or systematic random linear network coding.

3.1.2.1 Preliminaries: fundamental probability expressions

Let $\mathbf{M}$ be a $n \times m$ binary random matrix with $n \geq m$. As discussed in Chapter 2, we say that $\mathbf{M}$ is a *full-rank* matrix if the rank of $\mathbf{M}$ is m or, equivalently, m of the n rows of $\mathbf{M}$ are linearly independent. The probability of $\mathbf{M}$ being a full-rank matrix can be obtained using (2.1) and (2.2) for $\mathbb{F}_2$, as follows

$$P(n,m) = \frac{\gamma(n,m)}{2^{nm}} \tag{3.3}$$

where 2^{nm} is the number of all $n \times m$ binary matrices and $\gamma(n,m)$ is the number of all full-rank $n \times m$ binary matrices, given as

$$\gamma(n,m) = \prod_{i=0}^{m-1} (2^n - 2^i).$$

Similarly, the probability of $\mathbf{M}$ having rank $r \leq m$ when $n \geq r$ can be obtained by employing (2.6) for $\mathbb{F}_2$, as follows

$$P_r(n,m) = 2^{-nm} \left(\frac{\gamma(n,r)\gamma(m,r)}{\gamma(r,r)} \right). \tag{3.4}$$

Let us now assume that matrix $\mathbf{M}$ has the following constrained structure

$$\mathbf{M} = \begin{bmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{bmatrix} \tag{3.5}$$

where the dimensions of submatrices $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ and $\mathbf{D}$ are $a \times a'$, $b \times b'$, $c \times a'$ and $c \times b'$, respectively. Matrices of this type, which are known as *block angular matrices*, were studied in [117]. It was proven that the probability of $\mathbf{M}$ being full-rank is given by

$$P(a,a',b,b',c) = \sum_{i+j \geq a'+b'-c} P_i(a,a')P_j(b,b')P(c, a'+b'-i-j). \tag{3.6}$$

As implied by (3.6), the rank of matrix $\mathbf{M}$ is $a'+b'$ if submatrix $\mathbf{A}$ has rank i, submatrix $\mathbf{B}$ has rank j and the remaining $a'+b'-i-j$ columns of $\mathbf{M}$ are linearly independent, for all valid values of i and j.

Expressions (3.3), (3.4) and (3.6) will be invoked in the subsequent performance analysis. Note that character P is used exclusively to denote probabilities associated with the rank of matrices but character $\mathcal{P}$ is used to refer to probabilities related to the system model under consideration.

3.1.2.2 Decoding probability for non-systematic network coding

In the general case of point-to-point communication over a channel with erasure probability ϵ, the probability of the receiving node decoding all of the m source packets when n coded packets have been transmitted can be obtained using (2.20), re-expressed as follows

$$\mathcal{P}(n,m,\epsilon)=\sum_{\hat{n}=m}^{n} B(\hat{n},n,\epsilon)\ P(\hat{n},m). \tag{3.7}$$

Where, $B(\hat{n},n,p)$ denotes the probability mass function of the binomial distribution, defined in (2.21). Expression (3.7) enumerates all possible scenarios of retrieving the m source packets when $\hat{n}\geq m$ coded packets have been successfully received and have formed a full-rank $\hat{n}\times m$ coding matrix.

In the particular case of the considered relay-aided network, the probability that the destination node D will decode the source packets of both source nodes can be decomposed into the following three components:

Unaided communication: Even though the relay node R has been deployed in the network, the destination node D could decode all of the source packets without the help of node R. The implies that both submatrices $\mathbf{C}_1$ and $\mathbf{C}_2$ in (3.1) are full-rank matrices and, consequently, $\mathbf{C}_{\text{SD}}$ is also a full-rank matrix. Therefore, the probability that node D will decode the m_1+m_2 source packets based solely on the n_1+n_2 transmitted coded packets can be obtained using (3.7) as follows

$$\mathcal{P}_{\text{S}}=\mathcal{P}(n_1,m_1,\epsilon_{1\text{D}})\ \mathcal{P}(n_2,m_2,\epsilon_{2\text{D}}). \tag{3.8}$$

Partially aided communication: In this mode, the destination node decodes the m_ℓ source packets of node S_ℓ based on coded packets transmitted both via the relay node and over the direct link between S_ℓ and D. The destination node retrieves the source packets of the other source node, denoted by $\text{S}_{\bar{\ell}}$ where $\bar{\ell}=1,2$ and $\bar{\ell}\neq\ell$, without the assistance of the relay node. The probability that node D will decode the m_1+m_2 source packets, when transmission from node S_ℓ is aided by the relay node R while transmission from node $\mathrm{S}_{\bar{\ell}}$ is unaided, can be upper-bound by the following product

$$\begin{aligned}\mathcal{P}_{\mathrm{S}_\ell\mathrm{RD}} \leq \mathcal{P}(n_{\bar{\ell}}, m_{\bar{\ell}}, \epsilon_{\bar{\ell}\mathrm{D}})\, \mathcal{P}(n_\ell, m_\ell, \epsilon_{\ell\mathrm{R}}) \sum_{\hat{n}_\ell=0}^{n_\ell} B(\hat{n}_\ell, n_\ell, \epsilon_{\ell\mathrm{D}}) \\ \cdot \sum_{i=0}^{\min(\hat{n}_\ell, m_\ell-1)} P_i(\hat{n}_\ell, m_\ell)\mathcal{P}(n_\mathrm{R}, m_\ell - i, \epsilon_{\mathrm{RD}}).\end{aligned} \tag{3.9}$$

The first two terms on the right-hand side of (3.9) represent the probability that nodes D and R will decode the source packets of nodes $\mathrm{S}_{\bar{\ell}}$ and S_ℓ, respectively, when the direct links are used. The remaining terms compute the probability that node D will construct a coding matrix of rank m_ℓ by obtaining i linearly independent coding vectors from node S_ℓ and $m_\ell - i$ linearly independent coding vectors from node R. Derivation of this probability invoked and extended a degraded version of the right-hand side of (3.6), where $\mathbf{M}$ in (3.5) was redefined as $\mathbf{M} = (\mathbf{A}\ \ \mathbf{C})^\intercal$.

The reason that the right-hand side of (3.9) is an upper bound and not the exact expression for $\mathcal{P}_{\mathrm{S}_\ell\mathrm{RD}}$ lies to the fact that the probability of the relay node decoding the packets of node S_ℓ is *not independent* of the probability that the destination node will decode the packets of the same node. For example, consider the case when $n_\ell = 10$ coded packets are transmitted to both D and R and $\epsilon_{\ell\mathrm{D}} = \epsilon_{\ell\mathrm{R}} = 0.1$. Given the fact that both R and D overhear the same transmissions over different channels, therefore, if each node successfully receives 9 coded packets then each node will have at least 8 of them in common. Therefore, if node D fails to decode the source packets of node S_ℓ, node R will most likely also fail to decode them and will not be in the position to assist node S_ℓ in its transmission. However, as the value of the product $n_\ell\, \epsilon_{\ell\mathrm{R}}$ or $n_\ell\, \epsilon_{\ell\mathrm{D}}$ increases, the upper bound gets tighter, as will become evident in Section 3.1.3.

Using (3.9), the probability that the destination node will decode the source packets of both S_1 and S_2, when either S_1 or S_2 is aided by the relay node R, is given by

$$\mathcal{P}_{\mathrm{SRD}} = \mathcal{P}_{\mathrm{S}_1\mathrm{RD}} + \mathcal{P}_{\mathrm{S}_2\mathrm{RD}}. \tag{3.10}$$

Fully aided communication: In this case, both S_1 and S_2 need the aid of the relay node R in order to deliver the necessary number of coded packets to the destination node. Node D successfully decodes the coded packets transmitted via node R and over the two direct links, and decodes all source packets. The probability that node D will decode the $m_1 + m_2$ source packets, when both source nodes are assisted by the relay node, can be upper-bound as follows

$$\begin{aligned}\mathcal{P}_{\mathrm{RD}} \leq & \mathcal{P}(n_1, m_1, \epsilon_{1\mathrm{R}})\, \mathcal{P}(n_2, m_2, \epsilon_{2\mathrm{R}}) \sum_{\hat{n}_1=0}^{n_1} B(\hat{n}_1, n_1, \epsilon_{1\mathrm{D}}) \sum_{\hat{n}_2=0}^{n_2} B(\hat{n}_2, n_2, \epsilon_{2\mathrm{D}}) \\ & \cdot \sum_{i=0}^{i_{\max}} \sum_{j=0}^{j_{\max}} P_i(\hat{n}_1, m_1) P_j(\hat{n}_2, m_2)\, \mathcal{P}(n_{\mathrm{R}},\ m_1{+}m_2{-}i{-}j,\ \epsilon_{\mathrm{RD}}).\end{aligned} \tag{3.11}$$

The first two terms on the right-hand side of (3.11) expresses the probability that node R will decode the source packets of both S_1 and S_2. The remaining terms compute the probability that node D will receive i, j and $m_1 + m_2 - i - j$ linearly independent coding vectors from S_1, S_2 and R, respectively, for all valid values of i and j. Similarly to (3.9), we set the upper limit of the third sum in (3.11) equal to $i_{\max} = \min(\hat{n}_1, m_1 - 1)$; this ensures that the number of linearly independent coded vectors i, which have been received directly from node S_1, is neither greater than the total number of received coded vectors $\hat{n}_1$, nor equal to or greater than the number of source packets m_1. The definition of $i_{\max}$ prevents i from taking the value m_1 because cases where node D can decode the m_1 source packets without the help of node R have already been considered in unaided and partially aided communication. Following a similar line of reasoning, we set $j_{\max} = \min(\hat{n}_2, m_2 - 1)$ in (3.11). Observe that the last two lines of (3.11) constitute a formula that is a constrained extension of (3.6).

The overall decoding probability at the destination node D can be obtained by adding the three constituent probabilities, that is,

$$\mathcal{P}_{\mathrm{D}} = \mathcal{P}_{\mathrm{S}} + \mathcal{P}_{\mathrm{SRD}} + \mathcal{P}_{\mathrm{RD}}. \tag{3.12}$$

We remark that if the right-hand side of (3.8), (3.9) and (3.11) are used in (3.12) to compute $\mathcal{P}_{\mathrm{S}}$, $\mathcal{P}_{\mathrm{SRD}}$ and $\mathcal{P}_{\mathrm{RD}}$, respectively, an upper bound on $\mathcal{P}_{\mathrm{D}}$ will be obtained.

3.1.2.3 Decoding probability for systematic network coding

In [118], systematic network coding for point-to-point communication was studied and it was proven that the probability of a receiving node decoding all of the m source packets, given that $m \leq \hat{n} \leq n$ packets have been successfully received, is

$$\mathcal{P}'(\hat{n}, m, n) = \frac{\displaystyle\sum_{h=h_{\min}}^{m} \binom{m}{h} \binom{n-m}{\hat{n}-h} P(\hat{n}{-}h, m{-}h)}{\displaystyle\binom{n}{\hat{n}}} \tag{3.13}$$

where $h_{\min} = \max(0, \hat{n}-n+m)$. Expression (3.13) considers the possibility of receiving h systematic and, hence, linearly independent packets out of the m transmitted systematic packets and computes the probability that there exist $m-h$ linearly independent coded packets among the remaining $\hat{n}-h$ packets, for all valid values of h. Following the same line of reasoning as in [118], we can express the probability of receiving $r \leq m$ linearly independent coded packets as

$$\mathcal{P}'_r(\hat{n}{,}m{,}n) = \frac{\displaystyle\sum_{h=h_{\min}}^{r} \binom{m}{h}\binom{n-m}{\hat{n}-h} P_{r-h}(\hat{n}-h, m-h)}{\displaystyle\binom{n}{\hat{n}}} \tag{3.14}$$

provided that $\hat{n} \geq r$. Similarly to the case of non-systematic network coding, the probability of the receiving node decoding all of the m source packets when n packets have been transmitted, denoted by $\mathcal{P}(n, m, \epsilon)$, can be obtained from (3.7) by replacing $P(\hat{n}, m)$ with $\mathcal{P}'(\hat{n}, m, n)$.

Taking into account (3.13) and (3.14) and using the same train of thought as in Section 3.1.2.2, we can obtain an expression for the performance of the considered two-source single-relay network for the case of systematic network coding. More specifically, the probability that the destination node will decode the source packets of both source nodes is given by

$$\mathcal{P}'_{\mathrm{D}} = \mathcal{P}'_{\mathrm{S}} + \left(\mathcal{P}'_{\mathrm{S_1RD}} + \mathcal{P}'_{\mathrm{S_2RD}}\right) + \mathcal{P}'_{\mathrm{RD}} \tag{3.15}$$

where

$$\mathcal{P}'_{\mathrm{S}} = \mathcal{P}'(n_1, m_1, \epsilon_{1\mathrm{D}})\, \mathcal{P}'(n_2, m_2, \epsilon_{2\mathrm{D}}), \tag{3.16}$$

$$\begin{aligned}\mathcal{P}'_{\mathrm{S}_\ell\mathrm{RD}} \leq \mathcal{P}'(n_{\bar{\ell}}, m_{\bar{\ell}}, \epsilon_{\bar{\ell}\mathrm{D}})\, \mathcal{P}'(n_\ell, m_\ell, \epsilon_{\ell\mathrm{R}}) \sum_{\hat{n}_\ell=0}^{n_\ell} B(\hat{n}_\ell, n_\ell, \epsilon_{\ell\mathrm{D}}) \\ \cdot \sum_{i=0}^{\min(\hat{n}_\ell, m_\ell-1)} \mathcal{P}'_i(\hat{n}_\ell, m_\ell, n_\ell)\, \mathcal{P}(n_{\mathrm{R}}, m_\ell - i, \epsilon_{\mathrm{RD}})\end{aligned} \tag{3.17}$$

for $\ell = 1, 2$, and

$$\begin{aligned}\mathcal{P}'_{\mathrm{RD}} \leq \mathcal{P}'(n_1, m_1, \epsilon_{1\mathrm{R}})\, \mathcal{P}'(n_2, m_2, \epsilon_{2\mathrm{R}}) \sum_{\hat{n}_1=0}^{n_1} B(\hat{n}_1, n_1, \epsilon_{1\mathrm{D}}) \sum_{\hat{n}_2=0}^{n_2} B(\hat{n}_2, n_2, \epsilon_{2\mathrm{D}}) \\ \cdot \sum_{i=0}^{i_{\max}} \sum_{j=0}^{j_{\max}} \mathcal{P}'_i(\hat{n}_1, m_1, n_1) \mathcal{P}'_j(\hat{n}_2, m_2, n_2) \mathcal{P}(n_{\mathrm{R}},\ m_1+m_2-i-j,\ \epsilon_{\mathrm{RD}}).\end{aligned} \tag{3.18}$$

The validity and tightness of the derived performance bounds will be investigated in the following section.

3.1.3 Results and Discussions

In this section, comparisons between the derived theoretical upper bounds and simulation results will be carried out for both systematic and non-systematic network coding. For convenience, a symmetric network configuration has been considered, according to which $m_1 = m_2 = m$, $n_1 = n_2 = n$, $\epsilon_{1\mathrm{D}} = \epsilon_{2\mathrm{D}} = \epsilon_{\mathrm{SD}}$ and $\epsilon_{1\mathrm{R}} = \epsilon_{2\mathrm{R}} = \epsilon_{\mathrm{SR}}$.

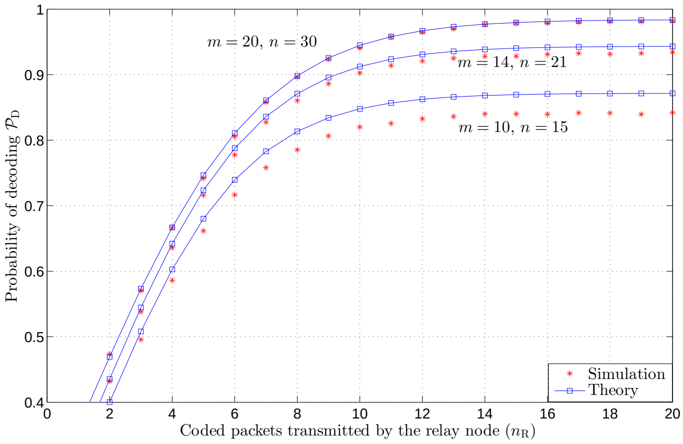


Figure 3.2: Comparison between theoretical upper bounds obtained from (3.12) and simulation results for different values of m and n. The erasure probabilities have been set to $\epsilon_{\mathrm{SD}} = 0.3$, $\epsilon_{\mathrm{SR}} = 0.1$ and $\epsilon_{\mathrm{RD}} = 0.2$.

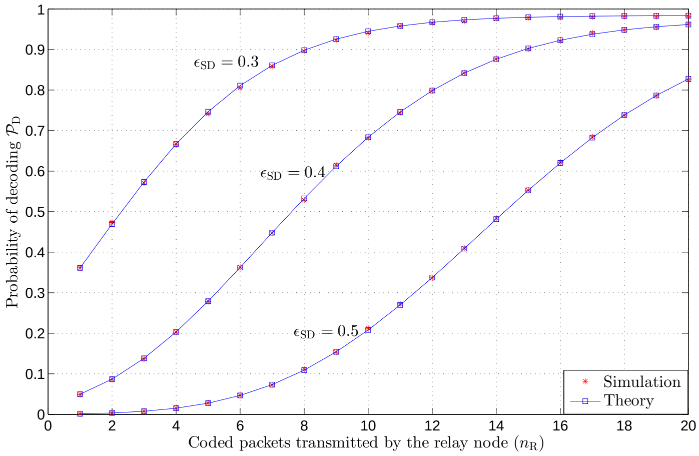


Figure 3.3: Comparison between theoretical upper bounds obtained from (3.12) and simulation results for different values of ϵ_{SD}. The remaining system parameters have been set to $m = 20$, $n = 30$, $\epsilon_{\mathrm{SR}} = 0.1$ and $\epsilon_{\mathrm{RD}} = 0.2$.

Fig. 3.2 compares simulation results with the theoretical expression in (3.12) as a function of n_{R}, for different values of m and n. As explained in Section 3.1.2.2, the interdependency between the decoding probability at node R and the decoding probability at node D is evident when $m = 10$ and $n = 15$; in this case, the upper bound yields a marginally higher decoding probability than that obtained via simulations. However, the interdependency becomes smaller and the upper bound gets tighter with an increasing number of source packets m and, consequently, an increasing number of transmitted packets n. We observe that for $m = 20$ and $n = 30$, the derived upper bound coincides with the simulation results.

The tightness of the proposed upper bound is also illustrated in Fig. 3.3, which depicts the impact of the source-to-destination channel quality, represented by ϵ_{SD}, and the number of coded packets n_{R} transmitted by the relay node on the system decoding probability $\mathcal{P}_{\mathrm{D}}$. As expected, aid by the relay is of key importance to the source nodes as the quality of the direct channel between each source node and the destination node deteriorates. The theoretical bounds accurately quantify the relationship between ϵ_{SD} and the number of coded packets n_{R} that need to be transmitted by the relay to achieve a target decoding probability.

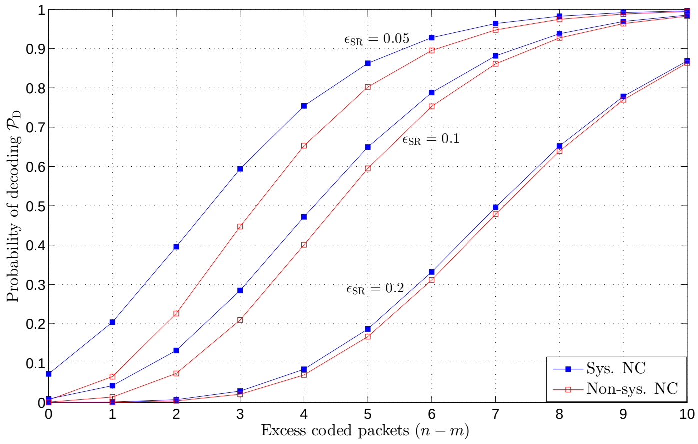


FIGURE 3.4: Performance comparison of systematic and non-systematic network coding as a function of the excess coded packets $n - m$ transmitted by each source node for various values of ϵ_{SR}. The remaining system parameters have been set to $m = 20$, $n_{\mathrm{R}} = 15$, $\epsilon_{\mathrm{SD}} = 0.3$ and $\epsilon_{\mathrm{RD}} = 0.1$.

Fig. 3.4 carries out a performance comparison between systematic and non-systematic RLNC for various values of ϵ_{SR}. As is evident from the figure, if systematic RLNC is used at the source nodes and the source-to-relay channel conditions are good, the destination node requires fewer excess coded packets $n - m$ from the source nodes to correctly decode all of the $m_1 + m_2$ source packets. This observation is in agreement with the findings in [118] for point-to-point communication. As the source-to-relay channel quality deteriorates, systematic RLNC performs similarly to non-systematic RLNC. Nevertheless, systematic RLNC still offers the benefits of progressive packet decoding and reduced decoding complexity, as detailed in [118].

3.2 Random Linear Network Coded Cooperation in Multi-source Multi-relay Networks

In this section, we consider a multi-source multi-relay network, in which relay nodes employ a coding scheme based on random linear network coding on source packets and generate coded packets. The links between source-to-relay nodes and relay-to-destination nodes are modeled as packet erasure channels. Both upper bound and lower bound on the probability of decoding failure are presented, which are markedly close to simulation results and notably better than previous bounds.

3.2.1 System Model

We consider a system with m source nodes and n relay nodes, $\{\mathrm{S}_1, \mathrm{S}_2, \ldots, \mathrm{S}_m\}$ and $\{\mathrm{R}_1, \mathrm{R}_2, \ldots, \mathrm{R}_n\}$, respectively, as shown in Fig. 3.5, where $n \geq m$. Each source node S_i has a packet x_i to transmit to a destination D via n relay nodes. No source-to-destination links are assumed. The links connecting source-to-relay and relay-to-destination nodes are modeled as independent packet erasure channels characterized by erasure probability ϵ_{SR} and ϵ_{RD}, respectively.

The communication process is split into two phases. In the first phase, all the source nodes transmit their information packets simultaneously to the relay nodes over orthogonal broadcast channels. In the second phase, each relay node instead of storing and forwarding the received packets, generates a single coded packet by randomly combining the successfully received packets from the m source nodes. Thus n coded packets are generated by n relay nodes. These n coded packets are then forwarded to the destination D over orthogonal channels. The coded packet z_i, which is transmitted by the i^{th} relay node, can be expressed as $z_i = \sum_{j=1}^{m} c_{i,j} x_j$, where $c_{i,j}$ is a coding coefficient selected independently at random over a finite field $\mathbb{F}_q$ of size q. Because of the link condition ϵ_{SR} between the source node S_j and the relay node R_i, each relay node receives packets from different source nodes. In contrast to [6] where coding coefficients are chosen uniformly at random, our system model imposes that the zero coefficient is assigned to erased packets and the remaining $q-1$ non-zero coefficients are selected uniformly at random by each relay for successfully received packets. Consequently, the coding coefficient distribution is given by

$$P[c_{i,j} = t] = \begin{cases} \epsilon_{\mathrm{SR}}, & \text{if } t = 0 \\ \dfrac{1-\epsilon_{\mathrm{SR}}}{q-1}, & \text{if } t \in \mathbb{F}_q \setminus \{0\} \end{cases} \tag{3.19}$$

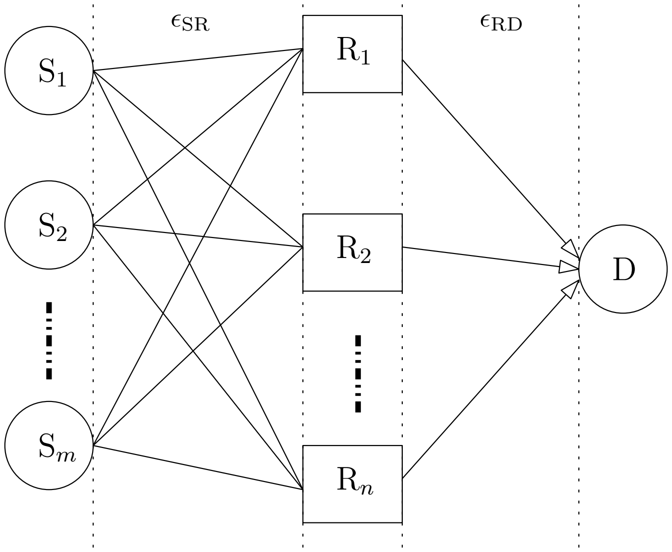


FIGURE 3.5: A network consisting of m source nodes, $n \geq m$ relay nodes and a destination D. The packet erasure probability of a source-to-relay link and a relay-to-destination link is represented by ϵ_{SR} and ϵ_{RD}, respectively.

where $0 \leq \epsilon_{\mathrm{SR}} \leq 1$. This implies that, the greater the value of erasure probability ϵ_{SR} is, the more likely that a coding coefficient is equal to zero. Thus, we observe that the average number of information packets participating in the generation of a coded packet is a function of ϵ_{SR}. For a given relay node i, the sequence $c_{i,1}, \ldots, c_{i,m}$ forms a row vector, which is known as the coding vector of the coded packet z_i. As is commonly assumed in network coding [28], coding vectors are transmitted along with the corresponding coded packets. When the destination D receives m linearly independent coded packets, the packets of all source nodes can be decoded. Transmission of source packets over erasure channels and random linear coding at relay nodes is analogous to sparse RLNC, which uses sparse random matrices [119, 120]. Based on the work of Blömer [119] and Cooper [120], this work derives improved upper and lower bounds on the probability that the destination will fail to decode the source packets.

3.2.2 Preliminary Results and Former Bounds on the Probability of Decoding Failure

Consider a matrix $\mathbf{A} \in \mathbb{F}_q^{n \times m}$, whose elements are the coding coefficients $c_{i,j}$ such that the i^{th} row of $\mathbf{A}$ represents the coding vector associated with the i^{th} coded packet received by the destination D. The destination can decode the packets of the m source nodes if and only if $rank(\mathbf{A}) = m$. Thus, the decoding failure probability at the destination D can be defined as $P_{\text{fail}} := \Pr\{rank(\mathbf{A}) < m\}$. It is related to the linear dependence of the vectors of matrix $\mathbf{A}$ and is defined as:

Definition 1. The vectors of matrix $\mathbf{A} \in \mathbb{F}_q^{n \times m}$ are said to be *linearly dependent* if and only if there exists a column vector $\mathbf{x} \in \mathbb{F}_q^{m \times 1} \backslash \{\mathbf{0}\}$ such that

$$\mathbf{A}\mathbf{x} = \mathbf{0}. \tag{3.20}$$

When there is no packet loss between the relay-to-destination channels, i.e., $\epsilon_{\text{RD}} = 0$, the probability that the elements of the i^{th} row of matrix $\mathbf{A}$ add up to zero, i.e., $c_{i,1} + c_{i,2} + \ldots + c_{i,m} = 0$, is given by [119]

$$\gamma_m = q^{-1} + (1 - q^{-1})(1 - \frac{1 - \epsilon_{\text{SR}}}{1 - q^{-1}})^m. \tag{3.21}$$

Taking into account that matrix $\mathbf{A}$ consists of n rows, the probability $\Pr(\mathbf{A}\mathbf{x} = \mathbf{0})$ can be obtained as

$$\Pr(\mathbf{A}\mathbf{x} = \mathbf{0}) = \gamma_m^n = \big(q^{-1} + (1 - q^{-1})(1 - \frac{1 - \epsilon_{\text{SR}}}{1 - q^{-1}})^m\big)^n. \tag{3.22}$$

The expected number of decoding failures at the destination D is given by the following theorem, which is a straightforward adaptation of [119, Theorem 3.3], [120, Theorem 3] to the system model under consideration.

Theorem 3.1. *For a linear network coding scheme over m source nodes, $n \geq m$ relay nodes and a single or multiple destinations, which are interconnected by links characterized by packet erasure probabilities $0 \leq \epsilon_{\text{SR}} \leq 1$ and $\epsilon_{\text{RD}} = 0$, the expectation of the decoding failures can be obtained as*

$$\mu_0(m, n) = E(\mathbf{A}\mathbf{x} = \mathbf{0}) = \frac{1}{q - 1} \sum_{w=1}^{m} \binom{m}{w} (q - 1)^w \gamma_w^n \tag{3.23}$$

where $\mathbf{A} \in \mathbb{F}_q^{n \times m}$ is the coding matrix at a destination.

Following the same line of reasoning, a direct extension of (3.23) for $\epsilon_{\text{RD}} \geq 0$ has been made in [59, Theorem 1] and was used to upper bound the probability of decoding failure.

Corollary 3.2. *The probability of decoding failure at a destination is bounded from above as:*

$$P_{\text{fail}} \leq \frac{1}{q - 1} \sum_{w=1}^{m} \binom{n}{w} (q - 1)^w \big[\epsilon_{\text{RD}} + (1 - \epsilon_{\text{RD}})\gamma_w\big]^n \tag{3.24}$$

where m is the number of source nodes, $n \geq m$ is the number of relay nodes and ϵ_{SR}, ϵ_{RD} represent the packet erasure probabilities between the network nodes.

However, (3.24) is only tight for limited values of erasures ϵ_{SR} and ϵ_{RD}, depending on m, n and q. In particular, the upper bound takes values greater than 1 when either the field size is big or the difference between the number of source and relay nodes is small. This disparity between the probability of decoding failure and the upper bound will be demonstrated in Section 3.2.4. In an effort to improve the tightness of (3.24), Seong *et al.* proposed the selection of the minimum value between the upper bound in (3.24) and 1 [60]. A lower bound on the probability of decoding failure has also been obtained by Seong in [59, Theorem 2]:

Theorem 3.3. *Consider a network comprising m source nodes and $n \geq m$ relay nodes, assume that links are modeled as packet erasure channels with erasure probabilities ϵ_{SR} and ϵ_{RD}, and let $\mathbf{A} \in \mathbb{F}_q^{n\times m}$ be the coding matrix at a destination node. The probability of decoding failure P_{fail} is lower bounded by*

$$P_{\text{fail}} \geq \sum_{k=1}^{m} \binom{m}{k} \Big((\epsilon_{\text{SR}} + \epsilon_{\text{RD}} - \epsilon_{\text{SR}}\epsilon_{\text{RD}})^n \Big)^k \big(1 - (\epsilon_{\text{SR}} + \epsilon_{\text{RD}} - \epsilon_{\text{SR}}\epsilon_{\text{RD}})^n\big)^{m-k}. \tag{3.25}$$

The bounds in (3.24) and (3.25) are used in [60] and [121]. For example, (3.24) is employed in [121] to evaluate the performance gains introduced by linear NC in a practical network architecture for emergency communications. However, the following section will derive new bounds, which are considerably tighter than the previous bounds and can significantly improve the quality and accuracy of results presented in the literature.

3.2.3 Improved Bounds on the Probability of Decoding Failure

3.2.3.1 Upper bound

For $\epsilon_{\text{RD}} = 0$, an upper bound on the decoding failure probability can be obtained by extending and adapting [119, Theorem 6.3] as follows:

Lemma 3.4. *Let $\mathbf{A} \in \mathbb{F}_q^{n\times m}$ be the coding matrix at a destination node of a network consisting of m source nodes and n relay nodes. If the internode erasure probabilities are $0 \leq \epsilon_{\text{SR}} \leq 1$ and $\epsilon_{\text{RD}} = 0$, the probability of decoding failure is upper bounded by*

$$\eta_{\max}(m,n) = 1 - \prod_{i=1}^{m} (1 - \beta_{\max}^{n-i+1}) \tag{3.26}$$

where $\beta_{\max} = \max(\epsilon_{\text{SR}}, \dfrac{1-\epsilon_{\text{SR}}}{q-1})$ represents the maximum probability of obtaining an element from $\mathbb{F}_q$.

Proof. Let us assume that the first $i-1$ columns of $\mathbf{A}$, denoted by $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_{i-1}$, are linearly independent. This implies that by using elementary column operations, matrix $\mathbf{A}$ can be transformed into a matrix that contains an $(i-1)\times(i-1)$ identity matrix. Without loss of generality, let us assume that the first $i-1$ rows form the identity matrix. The columns of this matrix represent the basis for the vector space spanned by $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_{i-1}$. Therefore, the probability that $\mathbf{A}_i$ is linearly independent from $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_{i-1}$ depends only on the last $n-i+1$ elements of $\mathbf{A}_i$. This probability is lower bounded by $1-\beta_{\text{max}}^{n-i+1}$, where β_{max} can be obtained by selecting the maximum between the erasure probability and the probability of choosing a non-zero element over the finite field $\mathbb{F}_q$. Hence, matrix $\mathbf{A}$ contains an $m \times n$ non-singular matrix with probability at least $\prod_{i=1}^{m}(1-\beta_{\text{max}}^{n-i+1})$. As a result, the probability that matrix $\mathbf{A}$ does not contain an invertible matrix and, consequently, a decoding failure will occur is upper bounded by subtracting this product from one, which completes the proof. □

Lemma 3.4 will be used to obtain a tighter upper bound on P_{fail}. Before we invoke it, we shall first revisit (3.24) and rewrite it as:

$$P_{\text{fail}} \leq \sum_{\hat{n}=0}^{n} \binom{n}{\hat{n}} \epsilon_{\text{RD}}^{n-\hat{n}} (1-\epsilon_{\text{RD}})^{\hat{n}} \mu_0(m,\hat{n}). \tag{3.27}$$

This change is possible if $[\epsilon_{\text{RD}} + (1-\epsilon_{\text{RD}})\gamma_w\ ]^n$ is expanded into a sum, as per the binomial theorem.

Theorem 3.5. *For a network coding scheme over multi-source multi-relay networks, composed of m source nodes and n relay nodes with packet erasures ϵ_{SR} and ϵ_{RD}, the probability of decoding failure is upper bounded by*

$$P_{\text{fail}} \leq \sum_{\hat{n}=0}^{n} \binom{n}{\hat{n}} \epsilon_{\text{RD}}^{n-\hat{n}} (1-\epsilon_{\text{RD}})^{\hat{n}} \min\{\eta_{\max}(m,\hat{n}), \mu_0(m,\hat{n})\}. \tag{3.28}$$

Proof. As inferred from (3.27), the number of packet deliveries by the relays follows the binomial distribution. If we employ Theorem 3.1 and Lemma 3.4 on the number of received coded packets $\hat{n}$, a tight upper bound can be obtained by taking the minimum of outcomes and multiply with the probability distribution of $\hat{n}$. Summing the resultant quantity gives (3.28), which concludes the proof. □

Remark 3.6. It is worth noting that the upper bound is not simply the minimum between two cumulative probability distributions (CDFs), that is, the right-hand of (3.24) and the CDF of (3.26) for *all* possible numbers of relay nodes. Instead, the right hand of (3.24) has been rewritten in the form of (3.27), which enabled us to identify the minimum between μ_0 and $\eta_{\max}$ for *each* possible number of relay nodes, and use it in the computation of the CDF shown in (3.27).

3.2.3.2 Lower bound

The bound that was derived in [119, Theorem 6.3] was extended to an upper bound on the probability that an $n \times m$ matrix $\mathbf{A}$ does not contain an invertible $m \times n$ matrix in Lemma 3.4. The same approach can be followed to obtain a lower bound as follows:

Lemma 3.7. *Let $\mathbf{A} \in \mathbb{F}_q^{n\times m}$ be the coding matrix at a destination of a network consisting of m source nodes and n relay nodes. If the internode erasure probabilities are $0 \leq \epsilon_{\text{SR}} \leq 1$ and $\epsilon_{\text{RD}} = 0$, the probability of decoding failure is lower bounded by*

$$\eta_{\min}(m,n) = 1 - \prod_{i=1}^{m}(1 - \beta_{\min}^{n-i+1}) \tag{3.29}$$

where $\beta_{\min} = \min(\epsilon_{\text{SR}}, \dfrac{1-\epsilon_{\text{SR}}}{q-1})$.

Proof. The proof follows exactly the same line of reasoning as that of Lemma 3.4. □

An improved lower bound on P_{fail} can be obtained if the right-hand side of (8) is denoted by $P_0(m,n)$ for $\epsilon_{\text{RD}} = 0$, that is

$$P_0(m,n) = \sum_{k=1}^{m}\binom{m}{k}(\epsilon_{\text{SR}}^{n})^{k}(1-\epsilon_{\text{SR}}^{n})^{m-k} \tag{3.30}$$

and then combined with (3.29) in Lemma 3.7. In particular:

Theorem 3.8. *For a linear network coding scheme over m source nodes and $n \geq m$ relay nodes, let ϵ_{SR} and ϵ_{RD} be the packet erasure probabilities of the internode links. The probability of decoding failure is lower bounded by*

$$P_{\text{fail}} \geq \sum_{\hat{n}=0}^{n}\binom{m}{\hat{n}}\epsilon_{\text{RD}}^{n-\hat{n}}(1-\epsilon_{\text{RD}})^{\hat{n}}\max\{\eta_{\min}(m,\hat{n}), P_0(m,\hat{n})\}. \tag{3.31}$$

Proof. In contrast to Theorem 3.5, here we employ Lemma 3.7 and (3.30) on the number of received coded packets $\hat{n}$, and we select the maximum of outcomes. The rest of the proof follows the same reasoning as that presented in the proof of Theorem 3.5. □

3.2.4 Results and Discussions

This section compares the analytical expressions of the proposed bounds to simulation results. In addition, the proposed upper bound and lower bound, which shall be referred to as UB-new and LB-new, are contrasted with the old bounds represented by (3.24) and (3.25), which shall be referred to as UB-old and LB-old. To obtain simulation results, each scenario was run over 10^4 realizations, failures by the destination to decode the packets of all source nodes were counted, and the decoding failure probability was measured.

Fig. 3.6 shows numerical results of the upper bounds obtained from (3.24) and (3.28) and labeled UB-old and UB-new, respectively. We observe that, in contrast to UB-old, UB-new is significantly tighter to the simulated performance. When the number of source nodes and the number of relay nodes increase to $m = 30$ and $n = 35$, respectively, it can be clearly seen that the UB-old curve moves far away from the simulated curve but the proposed UB-new expression still provides a tight bound. This reveals the fact that UB-old produces a worse approximation error for large values of m.

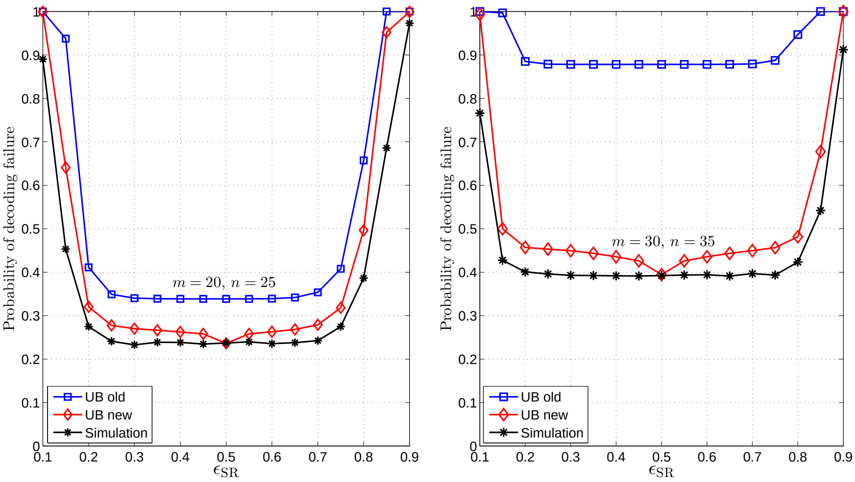


FIGURE 3.6: Comparison between simulation results and the theoretical upper bounds obtained from (3.24) and (3.28) for different values of m and n, when $q = 2$, $\epsilon_{RD} = 0.1$ and $\epsilon_{SR} \in [0.1, 0.9]$.

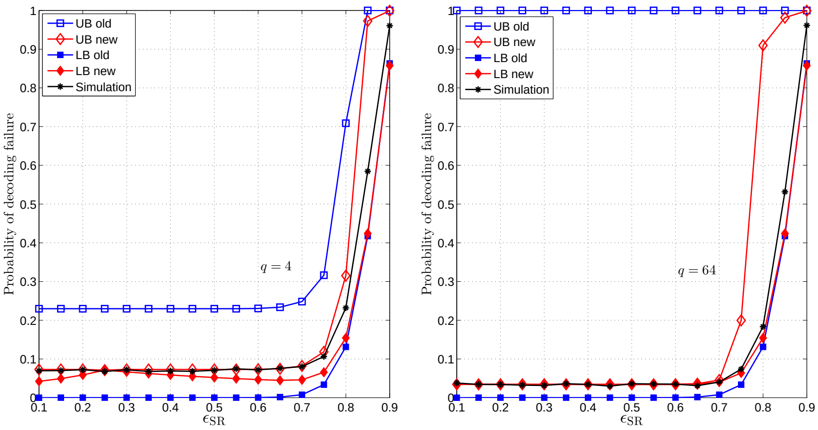


FIGURE 3.7: Effect of field size q on network performance and comparison between the proposed bounds and the old bounds for $\epsilon_{SR} \in [0.1, 0.9]$, when $m = 20$, $n = 25$ and $\epsilon_{RD} = 0.1$.

Fig. 3.7 evaluates the probability of decoding failure for $q = \{4, 64\}$, and contrasts the proposed bounds (UB-new and LB-new) with the old bounds (UB-old and LB-old). The

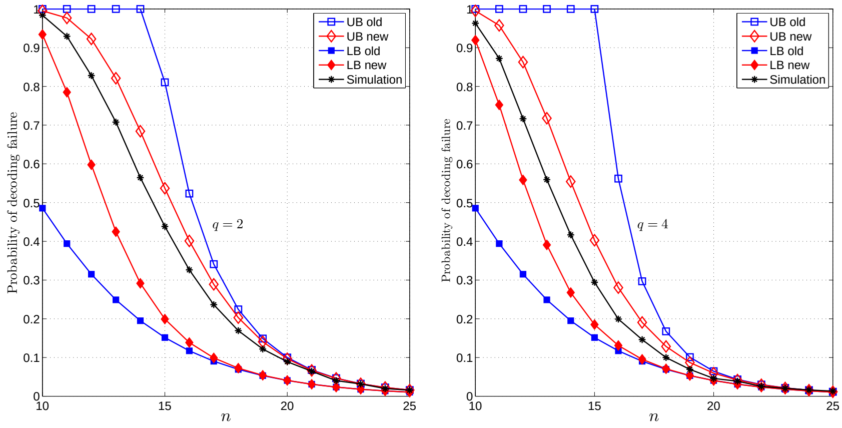


FIGURE 3.8: Performance of the network for an increasing number of relays n. The proposed bounds and the old bounds have been plotted for $m = 10$, $\epsilon_{\text{SR}} = 0.7$, $\epsilon_{\text{RD}} = 0.2$ and different values of field size q.

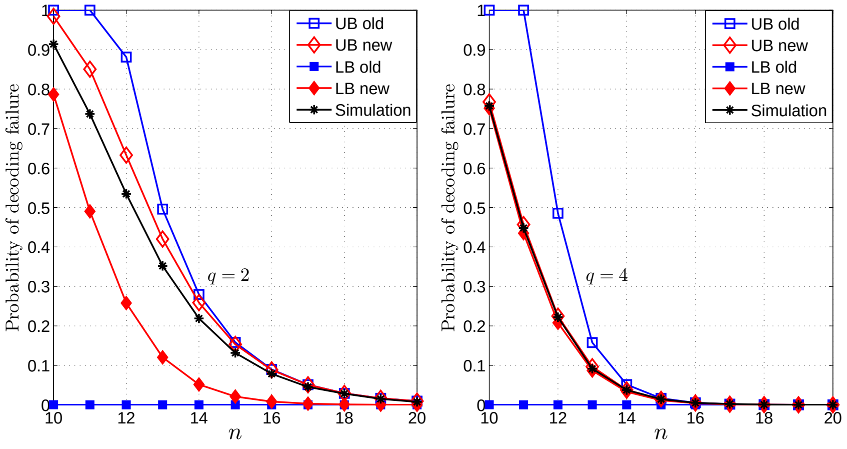


FIGURE 3.9: Network performance and comparison between the proposed bounds and the old bounds for $m = 10$, an increasing number of relays n, $\epsilon_{\text{SR}} = 0.3$, $\epsilon_{\text{RD}} = 0.1$ and different field size q.

figure demonstrates that for $\epsilon_{\text{SR}} \in [0.1, 0.7]$, the network experiences only a small probability of decoding failure. Furthermore, the figure shows that UB-new and LB-new are very close to the simulated performance and outperform UB-old and LB-old, respectively. In particular, when $q = 64$, UB-old and LB-old are markedly loose while UB-new and LB-new are very tight to the actual simulation results. Note that when $q = 64$, UB-old is always one, this is because for UB-old the minimum value between the upper bound in (3.24) and 1 is selected, as proposed by Seong *et al.* in [60]. The performance of the network deteriorates for values of ϵ_{SR} greater than 0.75. Moreover it is interesting to notice that, for large values of q, the upper bounds deviate from the simulation results and the simulations can be better approximated by the lower bounds.

Figs. 3.8 and 3.9 plot the probability of decoding failure versus the number of relays n with m=10 and q=$\{2, 4\}$. It is evident that the probability of decoding failure decreases with an increasing number of relays and field size. The figures also demonstrate that, when $n < 2m$, UB-new and LB-new are close to the simulated outcomes, compared to UB-old and LB-old, respectively. It follows from (3.25) that LB-old depends only on the erasures ϵ_{SR} and ϵ_{RD}, and does not depend on the field size q, thus shows no improvement for $q = 4$. However, LB-new approaches the simulation results, when q increases to 4. For example in Fig. 3.9, when $q = 4$ and $n \leq 14$, both UB-new and LB-new are very tight, while UB-old and LB-old are noticeably far from the simulated performance.

3.3 Random Linear Network Coded Cooperation Combined with Non-Orthogonal Multiple Access

This secion considers two groups of source nodes, where each group transmits packets to its own designated destination node over single-hop links and via a cluster of relay nodes shared by both groups. In an effort to boost reliability without sacrificing throughput, a scheme is proposed whereby packets at the relay nodes are combined using two methods; packets delivered by different groups are mixed using non-orthogonal multiple access principles, while packets originating from the same group are mixed using random linear network coding. An analytical framework that characterizes the performance of the proposed scheme is developed, compared to simulation results and benchmarked against a counterpart scheme that is based on orthogonal multiple access.

3.3.1 System Model

Consider a network with two source groups, two destination nodes and n commonly shared relay nodes $\mathrm{r}_1, \mathrm{r}_2, \ldots, \mathrm{r}_n$, as shown in Fig. 3.10. Each source group G_k contains m source nodes $\mathrm{s}_1^{(k)}, \mathrm{s}_2^{(k)}, \ldots, \mathrm{s}_m^{(k)}$ for $k = 1, 2$. The packets transmitted by source nodes in G_k are meant to be received by destination d_k either directly or via relay nodes. The acceptable transmission rate for G_1 is R_1^* and for G_2 is R_2^*. Without loss of generality, we assume that all the source nodes in G_1 require comparatively high quality of services with $R_1^* < R_2^*$. In practice, G_1 could be a group of sensors/devices associated to high risk applications which need to be connected quickly with low data rate, and G_2 could be a group of sensors/devices related to low risk applications which can afford opportunistic connectivity, as considered in [122, 123]. All the nodes operate in a half duplex mode. The links connecting the nodes are modeled as quasi static Rayleigh fading channels, where the channel gain between nodes i and j is represented by $|h_{ij}|$, has variance σ_{ij}^2 and mean zero. Before the communication process is initiated source nodes from the two groups are paired, such that $\mathrm{s}_i^{(1)}$ in group G_1 is paired with $\mathrm{s}_i^{(2)}$ in G_2. This

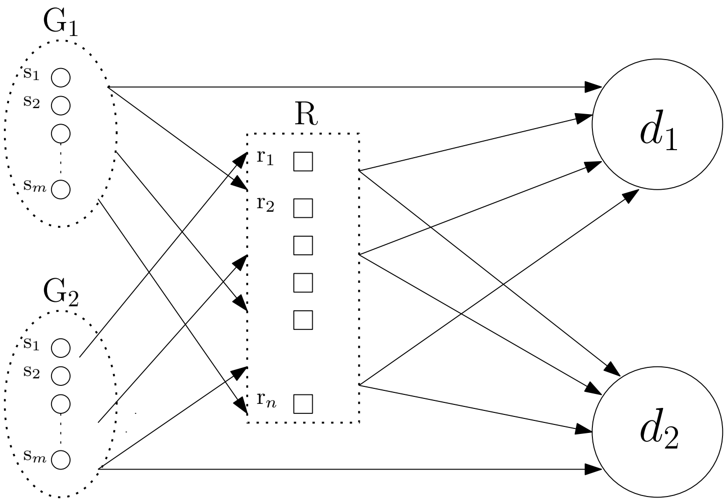


Figure 3.10: Block diagram of the system model

pairing is motivated by the fact that NOMA for two users has been recently proposed for 3GPP Long Term Evolution (LTE) advanced [124]. By exploiting the principle of superposition coding, only paired nodes are allowed to transmit simultaneously, over the same frequency band. Source nodes in different pairs transmit over orthogonal frequency bands, and therefore can be decoded independently. This approach is also known as OFDM-NOMA [15] but, for the sake of brevity, we shall simply refer it to as NOMA. We consider the worst case scenario, in which both source groups contain an equal (i.e., m) number of source nodes, such that relay nodes always receive superimposed signals. The proposed communication process is divided into two phases.

In the first phase, the source nodes broadcast their information-bearing signals to the relay and destination nodes. The signals transmitted by the i^{th} source pair $\mathrm{s}_i^{(1)}$ and $\mathrm{s}_i^{(2)}$ and received by relay node r_j and destination nodes $\{\mathrm{d}_1, \mathrm{d}_2\}$ are respectively given as

$$u^i_{\mathrm{r}_j} = \sqrt{\mathbb{a}_1 \varrho_\mathrm{s}}\, h_{\mathrm{s}_i^{(1)}\mathrm{r}_j} \tilde{x}_i + \sqrt{\mathbb{a}_2 \varrho_\mathrm{s}}\, h_{\mathrm{s}_i^{(2)}\mathrm{r}_j} \tilde{y}_i + w^i_{\mathrm{r}_j}$$

$$u^i_{\mathrm{d}_1} = \sqrt{\mathbb{a}_1 \varrho_\mathrm{s}}\, h_{\mathrm{s}_i^{(1)}\mathrm{d}_1} \tilde{x}_i + w^i_{\mathrm{d}_1}, \;\; z^i_{\mathrm{d}_2} = \sqrt{\mathbb{a}_2 \varrho_\mathrm{s}}\, h_{\mathrm{s}_i^{(2)}\mathrm{d}_2} \tilde{y}_i + w^i_{\mathrm{d}_2}$$

where ϱ_s is the total transmission power by the source pair, $\mathbb{a}_1$ and $\mathbb{a}_2$ are the proportions of ϱ_s transmitted by $\mathrm{s}_i^{(1)}$ and $\mathrm{s}_i^{(2)}$, respectively, and $\{\tilde{x}_i, \tilde{y}_i\}$ represent the modulated signals of data packets $\{x_i, y_i\}$. The additive white Gaussian noise components at the relay and destination nodes are represented by $w^i_{\mathrm{r}_j}$ and $w^i_{\mathrm{d}_k}$, respectively. All the relay nodes employ Successive Interference Cancellation (SIC) to recover the transmitted signals, demodulate and then store the correctly received data packets, disjointly.

In the second phase, each relay node r_j employs RLNC on the successfully received data packets of groups G$_1$ and G$_2$ independently, and generates coded packets $z_j^{(1)}$ and $z_j^{(2)}$, respectively. These coded packets can be represented as: $z_j^{(1)} = \sum_{i=1}^{m} c_{i,j}^{(1)} x_i$ and

$z_j^{(2)} = \sum_{i=1}^{m} c_{i,j}^{(2)} y_i$, where, $c_{i,j}^{(k)}$ represents the coding coefficients over the finite field $\mathbb{F}_q$ of size q. The value of a coefficient is zero if a received packet contains irrecoverable errors; otherwise, the value of that coefficient is selected uniformly at random from the remaining $q-1$ elements of $\mathbb{F}_q$. The probability mass function of $c_{i,j}^{(k)}$ is given as

$$g_{c_{i,j}^{(k)}}(0) = \epsilon_{\mathrm{s}_i^{(k)}\mathrm{r}_j}, \;\; g_{c_{i,j}^{(k)}}(t) = \frac{1-\epsilon_{\mathrm{s}_i^{(k)}\mathrm{r}_j}}{q-1}, \; t \in F_q \setminus \{0\} \tag{3.32}$$

where, $0 \leq \epsilon_{\mathrm{s}_i^{(k)}\mathrm{r}_j} \leq 1$ is the outage probability of the link connecting the source node $\mathrm{s}_i^{(k)}$with the relay node r_j. The closed form expression of $\epsilon_{\mathrm{s}_i^{(k)}\mathrm{r}_j}$will be presented in Section 3.3.2.

Each node, instead of transmitting two separate network-coded signals (one for each destination), generates a superimposed signal from the two network-coded signals and broadcasts it to both destinations. For example, the superimposed signals transmitted by relay r_j can be expressed as $(\sqrt{\varrho_{\mathrm{r}}\mathbb{b}_1}\tilde{z}_j^{(1)} + \sqrt{\varrho_{\mathrm{r}}\mathbb{b}_2}\tilde{z}_j^{(2)})$, where ϱ_{r} is the total transmitted power, and $\mathbb{b}_1$, $\mathbb{b}_2$ denote the power allocation coefficients, such that $\mathbb{b}_1 + \mathbb{b}_2 = 1$ with $\mathbb{b}_1 > \mathbb{b}_2$ in order to satisfy the quality of service requirement [122]. Thus, the received signal at destination d_k is given as

$$\hat{u}_{\mathrm{d}_k}^{j} = h_{\mathrm{r}_j\mathrm{d}_k}(\sqrt{\varrho_{\mathrm{r}}\mathbb{b}_1}\tilde{z}_j^{(1)} + \sqrt{\varrho_{\mathrm{r}}\mathbb{b}_2}\tilde{z}_j^{(2)}) + \hat{w}_{\mathrm{d}_k}^{j}$$

where $\hat{w}_{\mathrm{d}_k}^{j}$ is the Gaussian noise component. Each destination node employs SIC in order to separate the superimposed signals, demodulate and recover the relevant coded packets, and store them for future processing. Destination d_i will decode the data packets of source group G_i if it collects m linearly independent packets, either directly from that source group or via the relay nodes.

3.3.2 Achievable Rate and Link Outage Probability

This section describes the achievable transmission rate of source-to-destination, source-to-relay and relay-to-destination links. Transmission failure/outage occurs when the achievable rate is less than the target rate of transmission. Therefore, the outage probability of a link can be expressed in terms of the achievable rate and the target rate.

Let us consider the first phase, during which signals arrive at each destination node directly from the respective source group. The achievable rate of the $\mathrm{s}_i^{(k)}\mathrm{d}_k$ link corresponding to group G_k can be obtained as

$$R_{\mathrm{s}_i^{(k)}\mathrm{d}_k} = B_{\mathrm{s}} \log\big(1 + \frac{\varrho_{\mathrm{s}}\mathbb{a}_k |h_{\mathrm{s}_i^{(k)}\mathrm{d}_k}|^2}{B_s N_0}\big) \tag{3.33}$$

where $k \in \{1, 2\}$, $i \in \{1, 2, \ldots, m\}$, N_0 represents the noise power and B_s denotes the bandwidth of the sub-band allocated to each source pair for simultaneous transmissions as discussed in Section I. Based on the achievable rate, the outage probability of $\mathrm{s}_i^{(k)}\mathrm{d}_k$ link can be defined as

$$\epsilon_{\mathrm{s}_i^{(k)}\mathrm{d}_k} = Pr(R_{\mathrm{s}_i^{(k)}\mathrm{d}_k} < R_k^*) = 1 - \exp(-\frac{\Upsilon_k}{\rho_\mathrm{s}\mathbb{a}_k\sigma^2_{\mathrm{s}_i^{(k)}\mathrm{d}_k}})$$

where $\rho_\mathrm{s} = \frac{\varrho_\mathrm{s}}{B_\mathrm{s}N_0}$ and $\Upsilon_k = 2^{R_k^*/B_\mathrm{s}} - 1$. The achievable rate of the link between one of the nodes of a source pair and a relay node r_j depends on the channel conditions of both links that connect the nodes of the source pair with r_j. For example, assume that $\mathbb{a}_1|h_{\mathrm{s}_i^{(1)}\mathrm{r}_j}| > \mathbb{a}_2|h_{\mathrm{s}_i^{(2)}\mathrm{r}_j}|$. In that case, SIC at the relay node r_j will first recover the signal of the node from G_1 and treat the other signal as interference. Thus, the achievable rate of the links can be expressed as

$$R_{\mathrm{s}_i^{(1)}\mathrm{r}_j} = B_\mathrm{s}\log\big(1 + \frac{\mathbb{a}_1|h_{\mathrm{s}_i^{(1)}\mathrm{r}_j}|^2}{\mathbb{a}_2|h_{\mathrm{s}_i^{(2)}\mathrm{r}_j}|^2 + 1/\rho_\mathrm{s}}\big) \tag{3.34}$$

$$R_{\mathrm{s}_i^{(2)}\mathrm{r}_j} = B_\mathrm{s}\log\big(1 + \rho_\mathrm{s}\mathbb{a}_2|h_{\mathrm{s}_i^{(2)}\mathrm{r}_j}|^2\big). \tag{3.35}$$

The outage probability of the links $\mathrm{s}_i^{(1)}\mathrm{r}_j$ and $\mathrm{s}_i^{(2)}\mathrm{r}_j$ can be obtained as $\epsilon_{\mathrm{s}_i^{(1)}\mathrm{r}_j} = \Pr(R_{\mathrm{s}_i^{(1)}\mathrm{r}_j} < R_1^*)$, thus

$$\epsilon_{\mathrm{s}_i^{(1)}\mathrm{r}_j} = 1 - \frac{\mathbb{a}_1\sigma^2_{\mathrm{s}_i^{(1)}\mathrm{r}_j}}{\Upsilon_1\mathbb{a}_2\sigma^2_{\mathrm{s}_i^{(2)}\mathrm{r}_j} + \mathbb{a}_1\sigma^2_{\mathrm{s}_i^{(1)}\mathrm{r}_j}}\exp(-\frac{\Upsilon_1}{\rho_\mathrm{s}\mathbb{a}_1\sigma^2_{\mathrm{s}_i^{(1)}\mathrm{r}_j}})$$

$$\begin{aligned}\epsilon_{\mathrm{s}_i^{(2)}\mathrm{r}_j} &= 1 - \Pr(R_{\mathrm{s}_i^{(1)}\mathrm{r}_j} > R_1^* \cap R_{\mathrm{s}_i^{(2)}\mathrm{r}_j} > R_2^*)\\ &= 1 - \frac{\mathbb{a}_1\sigma^2_{\mathrm{s}_i^{(1)}\mathrm{r}_j}}{\Upsilon_1\mathbb{a}_2\sigma^2_{\mathrm{s}_i^{(2)}\mathrm{r}_j} + \mathbb{a}_1\sigma^2_{\mathrm{s}_i^{(1)}\mathrm{r}_j}}\exp(-\frac{\Upsilon_1(\Upsilon_2 + 1)}{\rho_\mathrm{s}\mathbb{a}_1\sigma^2_{\mathrm{s}_i^{(1)}\mathrm{r}_j}} - \frac{\Upsilon_2}{\rho_\mathrm{s}\mathbb{a}_2\sigma^2_{\mathrm{s}_i^{(2)}\mathrm{r}_j}}).\end{aligned}$$

During the second phase, the destination node d_2 can only successfully recover the coded signals corresponding to source group G_2, when $R_{\mathrm{r}_j\mathrm{d}_2} > R_2^*$ provided that $R_{\mathrm{r}_j\mathrm{d}_1} > R_1^*$. On the other hand, the destination d_1 can recover the coded signals of G_1, when $R_{\mathrm{r}_j\mathrm{d}_1} > R_1^*$. The achievable rates are given as

$$R_{\mathrm{r}_j\mathrm{d}_1} = B_\mathrm{s}\log\big(1 + \frac{\mathbb{b}_1|h_{\mathrm{r}_j\mathrm{d}_1}|^2}{\mathbb{b}_2|h_{\mathrm{r}_j\mathrm{d}_1}|^2 + 1/\rho_\mathrm{r}}\big) \tag{3.36}$$

$$R_{\mathrm{r}_j\mathrm{d}_2} = B_\mathrm{s}\log\big(1 + \rho_\mathrm{r}\mathbb{b}_2|h_{\mathrm{r}_j\mathrm{d}_2}|^2\big) \tag{3.37}$$

where B_s is the sub bandwidth allocated to each relay node, and $\rho_\mathrm{r} = \frac{\varrho_\mathrm{r}}{B_\mathrm{s}N_0}$. It is assumed that $\mathbb{b}_1 \geq \Upsilon_1\mathbb{b}_2$, otherwise the outage probability is always one [13]. The outage probability of links $\mathrm{r}_j\mathrm{d}_1$ and $\mathrm{r}_j\mathrm{d}_2$ can be respectively obtained as

$$\epsilon_{\mathrm{r}_j\mathrm{d}_1} = \Pr(\frac{\mathbb{b}_1|h_{\mathrm{r}_j\mathrm{d}_1}|^2}{\mathbb{b}_2|h_{\mathrm{r}_j\mathrm{d}_1}|^2 + 1/\rho_\mathrm{r}} \leq \Upsilon_1) = 1 - \exp(-\frac{\Upsilon_1}{(\rho_\mathrm{r}\mathbb{b}_1 - \Upsilon_1\rho_\mathrm{r}\mathbb{b}_2)\sigma^2_{\mathrm{r}_j\mathrm{d}_1}})$$

$$\begin{aligned}\epsilon_{\mathrm{r}_j\mathrm{d}_2} &= 1 - \Pr(\frac{\mathbb{b}_1|h_{\mathrm{r}_j\mathrm{d}_2}|^2}{\mathbb{b}_2|h_{\mathrm{r}_j\mathrm{d}_2}|^2 + 1/\rho_\mathrm{r}} > \Upsilon_1, \rho_\mathrm{r}\mathbb{b}_2|h_{\mathrm{r}_j\mathrm{d}_2}|^2 > \Upsilon_2)\\ &= 1 - \exp(-\frac{1}{\rho_\mathrm{r}\sigma^2_{\mathrm{r}_j\mathrm{d}_2}}\max(\frac{\Upsilon_1}{\mathbb{b}_1 - \Upsilon_1\mathbb{b}_2}, \frac{\Upsilon_2}{\mathbb{b}_2})).\end{aligned}$$

OMA based Benchmark scheme: In this work, we consider conventional OFDMA as the benchmark Orthogonal Multiple Access (OMA) scheme. According to this scheme, all the nodes $\mathrm{s}_i^{(k)}$ and r_j transmit over orthogonal frequency bands. As a result, likewise (3.33), the achievable rates of source-to-relay and source-to-destination links during the first phase, and the relay-to-destination links during the second phase can be respectively obtained as

$$R_{\mathrm{s}_i^{(k)}\bar{u}} = \frac{B_\mathrm{s}}{2}\log(1 + \frac{\varrho_\mathrm{s}\mathbb{a}_k|h_{\mathrm{s}_i^{(k)}\bar{u}}|^2}{0.5B_\mathrm{s}N_0}),\ R_{\mathrm{r}_j\mathrm{d}_k} = \frac{B_\mathrm{s}}{2}\log(1 + \frac{\varrho_r\mathbb{b}_k|h_{\mathrm{r}_j\mathrm{d}_k}|^2}{0.5B_\mathrm{s}N_0})$$

where $\bar{u} \in \{\mathrm{r}_j, \mathrm{d}_k\}$. The factor $1/2$ is due to the fact that, unlike NOMA, each sub-band is now further split between two transmitting nodes. Note that, using the achievable rates, we can derive the outage probabilities. These results can be further extended to RLNC based analysis, which will be presented in the next section, and can be used as benchmarks against the proposed NOMA based scheme.

In the remainder of the work, we consider the case where the channels between co-located transmitting nodes (e.g. source nodes or relay nodes) and receiving nodes are statistically similar, hence $\epsilon_{\mathrm{r}_j\mathrm{d}_k} = \epsilon_{\mathrm{rd}_k}$, $\epsilon_{\mathrm{s}_i^k\mathrm{r}_j} = \epsilon_{\mathrm{s}^k\mathrm{r}}$ and $\epsilon_{\mathrm{s}_i^k\mathrm{d}_k} = \epsilon_{\mathrm{s}^k\mathrm{d}_k}$.

3.3.3 Decoding Probability and Analysis

This section analyses the system performance in terms of the probability of a destination node successfully decoding the packets of all nodes in the corresponding source group. Furthermore, the system throughput is derived as a function of the number of packets transmitted by the source nodes and the relay nodes.

The destination node d_k can decode the packets of all source nodes in group G_k if and only if it collects packets which yield enough (m) degrees of freedoms (dofs). Note that dofs at a destination node represent successfully received linearly independent packets, which can be either source packets delivered during the first phase, or coded packets transmitted during the second phase. By exploiting (3.28), we can bound the probability that the $n \geq m$ coded packets, which have been transmitted by the n relay nodes, will yield m dofs as follows:

$$P'(m, n, \epsilon_{\mathrm{s}^{(l)}\mathrm{r}}, q) \geq \max\Big[\prod_{i=1}^{m} 1 - \Gamma_{\max}^{n-i+1}, 1 - \sum_{w=1}^{m} \binom{m}{w} (q-1)^{w-1} \{q^{-1} + (1-q^{-1})(1 - \frac{1-\epsilon_{\mathrm{s}^{(l)}\mathrm{r}}}{1-q^{-1}})^{w}\}^{n}\Big] \tag{3.38}$$

where $\Gamma_{\max} = \max(\epsilon_{\mathrm{s}^{(l)}\mathrm{r}}, \dfrac{1-\epsilon_{\mathrm{s}^{(l)}\mathrm{r}}}{q-1})$. The first term of the max function in (3.38) represents the probability that m out of n coded packets are linearly independent, and the second term provides the expectation that not all of the n coded packets are linearly dependent.

In order to formulate the decoding probability at each destination node, let us assume that the destination d_k successfully received $\hat{n}$ packets, given that $m + n$ packets were transmitted, i.e., m source packets during the first phase and n coded packets during the second phase. The probability that h of the $\hat{n}$ packets are source packets and the remaining $\hat{n} - h$ are coded packets, is given as

$$P_{h/\hat{n}}(\epsilon_{\mathrm{s}^{(k)}\mathrm{d}_k}, \epsilon_{\mathrm{rd}_k}) = f_h(m, \epsilon_{\mathrm{s}^{(k)}\mathrm{d}_k}) f_{\hat{n}-h}(n, \epsilon_{\mathrm{rd}_k}) \tag{3.39}$$

where the term $f_{n_{\mathrm{R}}}(n_{\mathrm{T}}, \epsilon)$ denotes the probability mass function of the binomial distribution, that is,

$$f_{n_{\mathrm{R}}}(n_{\mathrm{T}}, \epsilon) = \binom{n_{\mathrm{T}}}{n_{\mathrm{R}}} \epsilon^{n_{\mathrm{T}}-n_{\mathrm{R}}} (1-\epsilon)^{n_{\mathrm{R}}}. \tag{3.40}$$

The contribution of the h decoded source packets to the $\hat{n} - h$ coded packets can be removed, so that the $\hat{n} - h$ coded packets become linear combinations of the remaining $m - h$ source packets only. Thus, at this point of the decoding process, the destination node d_k can successfully decode the remaining data packets if and only if the modified $\hat{n} - h$ coded packets yield $m - h$ dofs. By employing (3.38), (3.39) and the law of total probability, the overall decoding probability at the destination d_k can be expressed as

$$P_{\mathrm{d_k}}(m, n) = \sum_{\hat{n}=m}^{n+m} \sum_{h=h_{\min}}^{m} P_{h/\hat{n}}(\epsilon_{\mathrm{s}^{(k)}\mathrm{d}_k}, \epsilon_{\mathrm{rd}_k}) P'(m-h, \hat{n}-h, \epsilon_{\mathrm{s}^{(k)}\mathrm{r}}, q) \tag{3.41}$$

where $h_{\min} = \max(0, \hat{n} - n)$.

Note that retransmissions are not allowed in case of packet failures during the first phase or the second phase. Therefore, by modifying the expression of the end-to-end throughput in [125], the average system throughput can be defined as

$$\bar{\eta} = \frac{m}{m + \max\{E_{\mathrm{d}_1}(n), E_{\mathrm{d}_2}(n)\}} \tag{3.42}$$

where $E_{\mathrm{d}_k}(n)$ is the average number of relay nodes needed by each destination node d_k to decode the entire source group G_k, and can be calculated using [126]

$$E_{\mathrm{d}_k}(n) = n - \sum_{v=0}^{n-1} P_{\mathrm{d_k}}(m, v). \tag{3.43}$$

Moreover, by following (3.43), the average number of relays required for both destinations to decode the packets of the respective source groups can be represented as $E_{\mathrm{T}}(n) = n - \sum_{v=0}^{n-1} P_{\mathrm{joint}}(m, v)$, where $P_{\mathrm{joint}}(m, v) = P_{\mathrm{d}_1}(m, v)P_{\mathrm{d}_2}(m, v)$.

3.3.4 Results and Discussions

In this section, the accuracy of the derived analytical bound in (3.38), when used in combination with the decoding probability in (3.41), is verified through simulations. In the considered system setup, the bandwidth of each sub-band is normalized to 1, i.e., $B_{\mathrm{s}} = 1$. The source nodes and relay nodes have been positioned such that $\sigma^2_{\mathrm{s}^{(1)}\mathrm{d}_1} = 0.1458$, $\sigma^2_{\mathrm{s}^{(2)}\mathrm{d}_2} = 0.1458$, $\sigma^2_{\mathrm{s}^{(1)}\mathrm{r}} = 2.9155$, $\sigma^2_{\mathrm{s}^{(2)}\mathrm{r}} = 1$, $\sigma^2_{\mathrm{rd}_1} = 1.3717$ and $\sigma^2_{\mathrm{rd}_2} = 1.9531$. We set $\mathbb{a}_1 = 0.6$ and $\mathbb{a}_2 = 0.4$, while exhaustive search has been used to identify the values of $\mathbb{b}_1$ and $\mathbb{b}_2$ that maximize the joint decoding probability mentioned in Section 3.3.3. The average system SNR is set equal to $\rho_{\mathrm{s}} = \rho_{\mathrm{r}} = \bar{\rho}$ and, unless otherwise stated, we consider $R_1^* = 1$, $R_2^* = 1.5$.

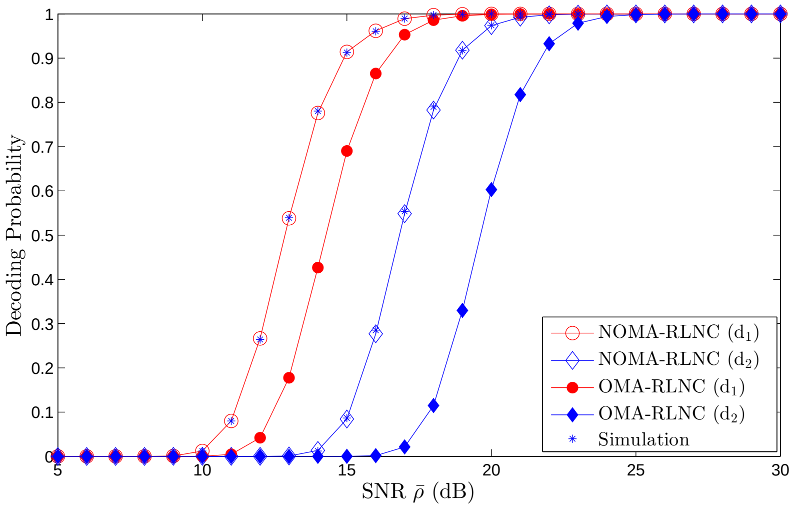


FIGURE 3.11: Simulation results and performance comparison between NOMA-RLNC and OMA-RLNC, when $m = 20$, $n = 10$ and $q = 4$.

Fig. 3.11 shows the decoding probabilities P_{d_1} and P_{d_2} at the two destination nodes in terms of the system SNR. The figure clearly demonstrates the tightness of the analytical curve to the simulation results. The decoding probability P_{d_1} is greater than P_{d_2} because node d_1 supports a lower target rate than node d_2, and d_1 is allocated more power than d$_2$ to ensure that the quality of service requirements are met. As expected, NOMA-RLNC outperforms OMA-RLNC because each source node in NOMA-RLNC benefits from being allocated twice the bandwidth that is allocated in OMA-RLNC.

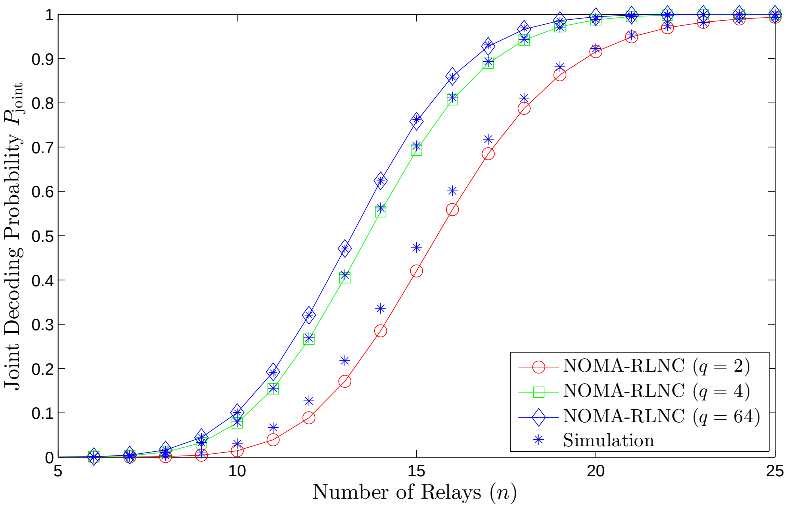


FIGURE 3.12: Effect of the field size q and the number of relay nodes n on the joint decoding probability, when $m = 20$.

Fig. 3.12 shows the joint decoding probability, for different values of field size q, as a function of the number of relays. The analytical bound is close to the simulation results for $q = 2$ and becomes tighter for greater values of q. A significant gain in performance can be observed when the field size increases from $q = 2$ to $q = 4$. However, the increase in gain is markedly smaller when q further increases from 4 to 64. This is because the certainty of linear independence between coded packets increases with the field size and approaches the highest possible degree even for relatively small values of q. We stress that the computational complexity of the decoder at the destination nodes also depends on the value of q. Thus, the choice of the field size over which RLNC is performed results in a trade-off between complexity and performance gain.

Fig. 3.13 illustrates the relationship between the system SNR and the average number of relays required for the successful decoding of the source packets of both source groups by the respective destination nodes. The plotted curves establish the diversity advantage offered by the combination of NOMA with RLNC as opposed to OMA with RLNC. For a fixed value of SNR, OMA-RLNC clearly needs more relays for cooperation than NOMA-RLNC. Alternatively, OMA-RLNC can achieve the same performance as NOMA-RLNC at the expense of a higher SNR.

Fig. 3.14 presents the system throughput as a function of the system SNR, for different target rates. The performance gap between NOMA-RLNC and OMA-RLNC is evident. We observe that, for a fixed SNR value, when the target rate increases from $R_2^* = 1.5$ to

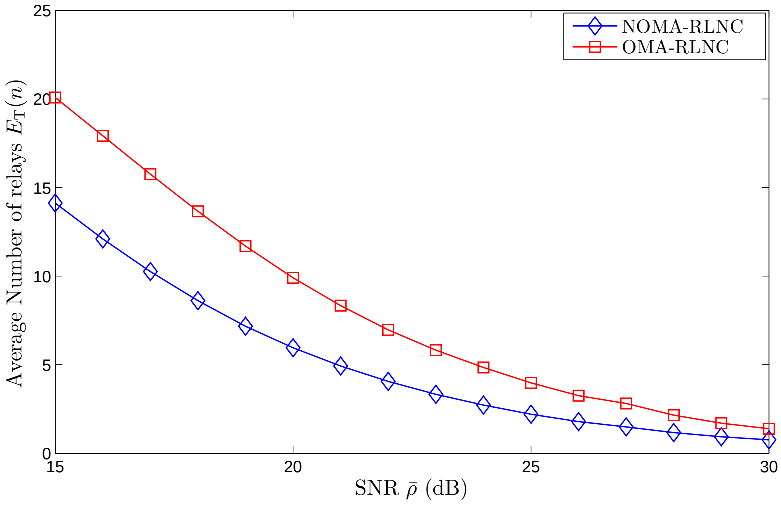


FIGURE 3.13: Comparison between the two schemes in terms of the required average number of relay nodes and the SNR when $m = 20$ and $q = 4$.

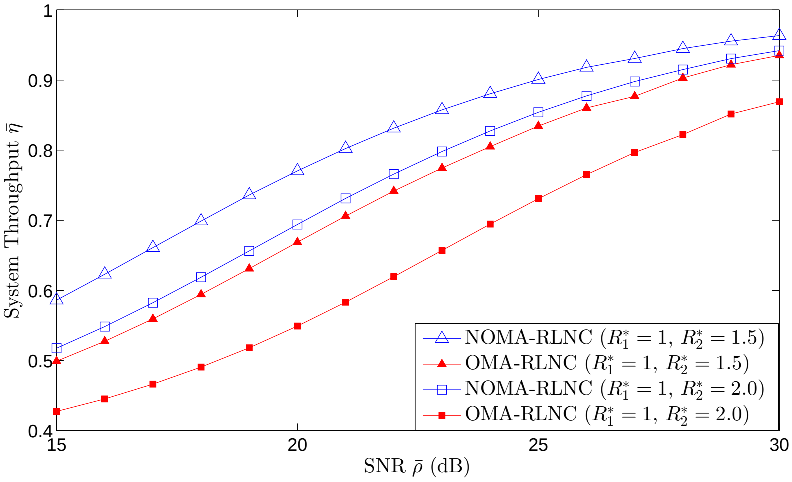


FIGURE 3.14: Effect of target rates on the system throughput against the system SNR, when $m = 20$ and $q = 4$.

$R_2^* = 2$, the outage probability increases and, therefore, the system throughput reduces. Interestingly, an increase in the target rate also increases the performance gap between NOMA-RLNC and OMA-RNC, that is, the throughput degradation of NOMA-RLNC is less severe than that of OMA-RLNC. An intuitive reason for this observation is that the 1/2 spectral loss in OMA dominates the system throughput.

3.4 Summary

In this chapter, we presented three different types of relay assisted networks and, in each network, RLNC based cooperation was exploited. Analytical closed form expressions were derived in order to evaluate and characterise the performance of RLNC based cooperation, for each network. Simulation results confirmed the accuracy of the expressions. The contributions made in this chapter can be summarised as follows:

- In Section 3.1, we studied the performance of a network comprising two source nodes transmitting to a destination node via a relay node, where random linear network coding is used both at the source nodes and the relay node. Upper bounds on the probability of the destination node successfully decoding the packets of both source nodes were derived for both systematic and non-systematic network coding. Simulation results confirmed the validity of our theoretical analysis and established that the upper bounds get tighter and accurately predict the system decoding probability for an increasing number of transmitted coded packets by the source nodes. Furthermore, we demonstrated that systematic network coding can yield a similar or better performance than non-systematic network coding depending on the quality of the uplink channels.

- In Section 3.2, we presented improved upper and lower bounds on the probability of decoding failure in a multi-source multi-relay network, which employs RLNC. The proposed analysis for counting failures provided significantly tighter bounds, which outperform existing bounds, derived in [59]. Several examples, which considered various numbers of source nodes and relay nodes, different field sizes and a range of erasure probabilities, established the shortcomings of the existing bounds and demonstrated the tightness of the proposed improved bounds. Finally, we asserted that the proposed bounds can also be used to better estimate the performance of systems employing sparse random linear network coding schemes, presented in the literature.

- In Section 3.3, we investigated the benefits of NOMA-based multiplexing and RLNC-based cooperative relaying in terms of decoding probability and system throughput. Simulation results established the tightness of the derived expressions. Comparisons emphasized the importance of network-coded cooperation and demonstrated the impact of the field size on network performance. This work showed that the combination of NOMA with RLNC can clearly provide a superior performance, in terms of diversity gain and system throughput, than the combination of conventional OMA with RLNC.

Chapter 4

Random Linear Network Coding for Secure Communication

Chapter 2 and Chapter 3 were focused on the development of mathematical frameworks for the evaluation and characterisation of RLNC performance in multicast communication as well as cooperative communication. We have studied the robustness and usefulness of RLNC against erasure channels, and exhibited the effect of the finite field and the number of cooperative relays on the overall decoding performance of networks. Finally, we have also demonstrated the effect of multiple access schemes on the performance of network coded cooperation.

In this chapter, we divert our attention from the reliability benefits of RLNC and instead focus on the study and application of the inherent feature of RLNC for secure communication. The chapter is mainly divided into two sections. Section 4.1 considers a basic secrecy problem with conventional characters: Alice (legitimate transmitter), Bob (legitimate receiver) and Eavesdropper (undesired receiver), where Alice employs RLNC for the delivery of confidential message to Bob. In this section, we assess and formulate the level of intrinsic secrecy provided by RLNC, in terms of intercept probability. This work has been inspired by the methodology in [64] but differs in two major points. Firstly, we have revisited the derivation of the intercept probability. More specifically, the decoding probability of a receiver has been taken into account in our calculations. Furthermore, key probability expressions have been revised to accurately reflect (i) the effect of the size of the finite field over which network coding is performed, (ii) the impact of a feedback link between the legitimate receiver and the transmitter, and (iii) the fact that the number of transmitted coded packets cannot be infinite in practice. The second difference is that [64] proposed an optimization model with respect to the number of source packets composing a message. However, the number of source packets and, by extension, their length are often dictated by the provided service. Our objective is to minimize the intercept probability by optimizing the number of transmitted coded packets, under delay and reliability constraints. As part of the optimization process, we prove that awareness of the existence of an eavesdropper is not required by the transmitter and the legitimate receiver.

Section 4.2 focuses to investigate the potential of relay-aided networks that combine RLNC with opportunistic relaying, with or without cooperative jamming, in securely and reliably delivering confidential messages. To this end, we consider four different relay selection protocols, we analyze their outage behaviour and we quantify the proportion of the message that could leak to the eavesdropper with a certain probability by the time the legitimate destination has decoded the entire message with a target probability. To the best of our knowledge, only few studies that exploit the properties of RLNC in PLS are available. For example, in order to enhance the secrecy of cooperative transmissions in sensor networks, fountain-coding aided cooperative relaying with jamming was proposed in [52]. Similarly to this work, we employ RLNC on the application layer. In contrast to [52], where only one relay has been considered for aiding the source in its transmission to the destination, we consider the complete problem of selecting a relay or a relay-jammer pair from the set of available nodes. Furthermore, relays do not only perform decode-and-forward, as in [52], but also linearly combine successfully received data packets. Other notable differences from [52] include the derivation of the probability that a fraction of data will leak to the eavesdropper, as opposed to the total amount of transmitted data, and the investigation of the impact of both the finite field size used by RLNC and the adopted forward error correction and modulation scheme on the security and reliability of the network.

4.1 The Intercept Probability of RLNC

This section considers a network comprising a transmitter, which employs random linear network coding to encode a message, a legitimate receiver, which can decode the message if it gathers a sufficient number of linearly independent coded packets, and an eavesdropper. Closed-form expressions for the probability of the eavesdropper intercepting enough coded packets to decode the message are derived. Transmission with and without feedback is studied. Furthermore, an optimization model that minimizes the intercept probability under delay and reliability constraints is presented.

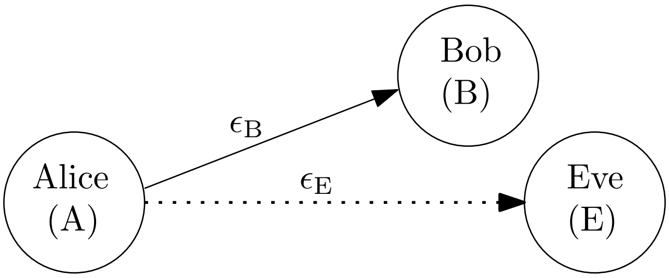


FIGURE 4.1: Block diagram of the system model, where ϵ_{B} and ϵ_{E} denote the erasure probabilities of the channels linking Alice to Bob and Alice to Eve, respectively.

4.1.1 System Model

We consider a network configuration whereby a source (Alice) wishes to transmit a message to a legitimate destination (Bob) in the presence of a passive eavesdropper (Eve), as shown in Fig. 4.1. Before initiating the communication process, Alice segments the message into m source packets and employs Random Linear Network Coding (RLNC) to generate and broadcast $n \geq m$ coded packets. The links connecting Alice to Bob and Alice to Eve are modeled as packet erasure channels characterized by erasure probabilities ϵ_{B} and ϵ_{E}, respectively. As per the RLNC requirements, Bob and Eve can decode the message only if they collect at least m linearly independent coded packets.

Based on this setup and the general condition that $\epsilon_{\mathrm{B}} < \epsilon_{\mathrm{E}}$ for physical layer security, we consider two network coded transmission modes, which we refer to as *Feedback-aided Transmission* (FT) and *Unaided Transmission* (UT). In the FT mode, Alice broadcasts up to n coded packets but ceases transmission as soon as Bob sends a notification over a perfect feedback channel acknowledging receipt of m linearly independent coded packets. In the case of UT, a feedback channel between Bob and Alice is not available, therefore Alice broadcasts exactly n coded packets anticipating Bob to successfully decode her message. In both modes, the communication process is considered to be secure if Eve fails to reconstruct Alice's message. In the rest of this work, we will investigate the resilience of FT and UT to the interception of m linearly independent coded packets by Eve.

4.1.2 Performance Analysis

The physical layer security offered by the two transmission modes will be quantified by the probability that Eve will manage to decode the message. To derive this probability, which is known as the *secrecy outage probability* or the *intercept probability*, we will first consider the general case of point-to-point communication between Alice and a receiver D over an erasure channel with erasure probability ϵ_D. Note that D can be either Bob or

Eve, i.e., $D \in \{\mathrm{B}, \mathrm{E}\}$. If Alice transmits $n \geq m$ coded packets and the receiver retrieves $\hat{n}$ coded packets, where $m \leq \hat{n} \leq n$, the probability that the receiver will successfully decode the m source packets can be obtained using (2.2), given as

$$P(\hat{n}, m) = \prod_{i=0}^{m-1} \left[1 - q^{-(\hat{n}-i)}\right],$$

where q is the size of the finite field over which network coding operations are performed. Let X be a random variable that represents the number of transmitted coded packets for which the receiver can decode the m source packets. The Cumulative Distribution Function (CDF) of X describes the probability that the receiver will decode the m source packets after n_{T} coded packets have been transmitted, where $m \leq n_{\mathrm{T}} \leq n$. This CDF can be obtained by employing (2.20) that is averaging $P(\hat{n}, m)$ over all valid values of $\hat{n}$, represented as

$$F_D(n_{\mathrm{T}}) = \Pr\{X \leq n_{\mathrm{T}}\} = \sum_{\hat{n}=m}^{n_{\mathrm{T}}} \binom{n_{\mathrm{T}}}{\hat{n}} (1-\epsilon_D)^{\hat{n}} \epsilon_D^{n_{\mathrm{T}}-\hat{n}}\, P(\hat{n}, m). \tag{4.1}$$

The probability that the receiver will decode the m source packets when the n_{T}-th coded packet has been transmitted, but not earlier, is given by the Probability Mass Function (PMF) of X, which can be derived as follows:

$$f_D(n_{\mathrm{T}}) = \Pr\{X = n_{\mathrm{T}}\} = \begin{cases} F_D(n_{\mathrm{T}}) - F_D(n_{\mathrm{T}} - 1), & \text{if } m < n_{\mathrm{T}} \leq n \\ F_D(m), & \text{if } n_{\mathrm{T}} = m. \end{cases} \tag{4.2}$$

Let us now return our focus to the considered network configuration operating in the FT mode. Recall that Bob sends an acknowledgment to Alice when he receives m linearly independent coded packets and can thus decode the source message. The intercept probability can be expressed as the sum of two constituent probabilities:

$$P_{\mathrm{int}}^{\mathrm{FT}}(n) = P_{\mathrm{BE}}(n) + P_{\mathrm{E}}(n). \tag{4.3}$$

The first term of the sum in (4.3), $P_{\mathrm{BE}}(n)$, denotes the probability that both Bob and Eve will decode the message. This can happen if Bob decodes the message only after the n_{T}-th coded packet has been transmitted, while Eve has already decoded the message or decodes it concurrently with Bob. Invoking the definitions in (4.1) and (4.2), and considering all possible values of n_{T}, we can express $P_{\mathrm{BE}}(n)$ as

$$P_{\mathrm{BE}}(n) = \sum_{n_{\mathrm{T}}=m}^{n} f_{\mathrm{B}}(n_{\mathrm{T}})\, F_{\mathrm{E}}(n_{\mathrm{T}}). \tag{4.4}$$

The second term of the sum in (4.3), $P_{\mathrm{E}}(n)$, represents the probability that Eve will be successful in decoding the message but Bob will fail to decode it after Alice has transmitted the complete sequence of n coded packets. Using the CDF of the number of coded packets delivered by Alice to Eve and Bob, respectively, we can write $P_{\mathrm{E}}(n)$ as follows:

$$P_{\mathrm{E}}(n) = F_{\mathrm{E}}(n)\, [\,1 - F_{\mathrm{B}}(n)\,]\,. \tag{4.5}$$

We should stress that (4.4) and (4.5) are exact only if the sequence of coded packets delivered over the Alice-to-Bob link is independent of the sequence delivered over the Alice-to-Eve link. This is a common hypothesis in the literature of broadcast networks, e.g., [64] and [113], and is valid for a non-vanishing product between the number of coded packets transmitted over a channel and the erasure probability of that channel. The accuracy of (4.3) will also be demonstrated in Section 4.1.4.

In the case of UT, a feedback channel is not available between Bob and Alice, therefore Alice transmits the complete sequence of n coded packets uninterruptedly. Therefore, the intercept probability is simply equal to the probability that Eve will decode the message after Alice has transmitted n coded packets. Using the definition of the CDF in (4.1), we obtain

$$P_{\mathrm{int}}^{\mathrm{UT}}(n) = F_{\mathrm{E}}(n). \tag{4.6}$$

Manipulation of the expression for $P_{\mathrm{int}}^{\mathrm{FT}}(n)$, as shown in Appendix B, and subtraction of $P_{\mathrm{int}}^{\mathrm{UT}}(n)$ from it, yields

$$P_{\mathrm{int}}^{\mathrm{FT}}(n) - P_{\mathrm{int}}^{\mathrm{UT}}(n) = -\sum_{n_{\mathrm{T}}=m+1}^{n} f_{\mathrm{E}}(n_{\mathrm{T}})\, F_{\mathrm{B}}(n_{\mathrm{T}} - 1). \tag{4.7}$$

Expression (4.7) measures the loss in the intercept capability of Eve or, equivalently, the gain in secrecy by Bob, if Bob can acknowledge the decoding of the source message to Alice using a feedback channel.

Remark 4.1. In this work, we assume that Alice has knowledge of the *average* channel conditions, characterized by the erasure probability, between her and Bob. If Alice could sense the *instantaneous* channel quality and transmitted coded packets only when the channel quality warranted their error-free delivery to Bob, as in [64], [127], the equivalent erasure probability of the link between Alice and Bob would be $\epsilon_{\mathrm{B}} = 0$. In that case, Alice could generate exactly m linearly independent coded packets in a deterministic manner, as opposed to random, and forward them to Bob. As a result, the intercept probability would reduce to $(1 - \epsilon_{\mathrm{E}})^m$ regardless the transmission mode. This remark concurs with the conclusion of [64] that an arbitrarily small intercept probability can be achieved by increasing the value of m, but at the cost of increased delay.

4.1.3 Optimization Model

This section aims to determine the optimum value of n, i.e., the number of coded packet transmissions, that minimizes the intercept probability, provided that a hard deadline is met. This hard deadline, denoted by $\dot{n}$, represents the number of coded packet transmissions that Alice is not allowed to exceed. In addition, the proposed optimization strategy permits Bob to decode the message with a target probability $\dot{P}$. In the rest of this work, both FT and UT will be optimized by the Resource Allocation Model (RAM), which is defined as follows:

$$\begin{aligned} \text{(RAM)} \quad & \min_{n} \; P_{\text{int}}(n) && (4.8) \\ \text{subject to} \quad & F_{\text{B}}(n) \geq \dot{P} && (4.9) \\ & n \leq \dot{n} && (4.10) \end{aligned}$$

where the objective function (4.8) represents the intercept probability when n coded packets have been scheduled for transmission. Constraint (4.9) ensures that the probability of Bob decoding the message is at least $\dot{P}$, while constraint (4.10) imposes that the number of planned coded packet transmissions is less than or equal to $\dot{n}$.

The proof of the following proposition will contribute to the solution of the RAM problem.

Proposition 4.2. *The intercept probability $P_{int}(n)$ is a non-decreasing function of n, i.e.,*

$$P_{int}(n_1) \leq P_{int}(n_2) \quad \textit{for all} \quad n_1 \leq n_2. \tag{4.11}$$

Proof. One of the properties of CDFs is that they are non-decreasing functions and, as per (4.6), the intercept probability of UT is equal to a CDF. In the case of FT, the subtraction of $P_{\text{int}}(n_1)$ from $P_{\text{int}}(n_2)$ for $n_2 \geq n_1$ gives a sum of non-negative terms, as shown in Appendix C. Therefore, $P_{\text{int}}(n_2) - P_{\text{int}}(n_1) \geq 0$, which concludes the proof. □

We can now proceed to Proposition 4.3 and provide a description of the solution to the RAM problem.

Proposition 4.3. *If the RAM problem admits a solution, the optimum solution is*

$$n^* = \arg\min \left\{ n \in [m, \dot{n}] \;\middle|\; F_{\text{B}}(n) \geq \dot{P} \right\}. \tag{4.12}$$

Proof. Let n^* denote the smallest value of n in the interval $[m, \dot{n}]$ for which constraint (4.9) holds. If an integer value smaller than n^* is selected, for example $n^* - 1$, the intercept probability will reduce, as per Proposition 4.2, but constraint (4.9) will not be met. We thus conclude that n^* is the optimum solution to the RAM problem. □

Root-finding algorithms, such as the bisection method, can be used on the right-hand side of (4.12) to determine if n^* exists and identify its value. Based on this analysis, we showed that minimization of the intercept probability under delay and reliability constraints can be achieved by minimizing the number of transmitted coded packets. Thus, Alice should know the erasure probability of the channel between her and Bob but knowledge of the presence of an eavesdropper *is not necessary.*

4.1.4 Results and Discussions

This section compares the derived analytical expressions with simulation results, establishes their validity and obtains solutions to the RAM problem for various channel conditions.

Fig. 4.2 depicts the relationship between the intercept probability and the quality of Bob's and Eve's channels, represented by ϵ_{B} and ϵ_{E}, respectively. For each point, the value of the n coded packet transmissions was optimized by RAM for $m = 50$ source packets, $\dot{n} = 150$ maximum allowable coded packet transmissions, a field size of $q = 2$ and a target probability of Bob decoding the source message equal to $\dot{P} = 90\%$. In simulations, Alice broadcasts the optimal number of coded packets determined by RAM. Instances where Eve successfully decodes m linearly independent coded packets are counted and averaged over 10^4 realizations to obtain the intercept probability. We observe the close agreement between analytical and simulation results, which confirms the tightness of (4.3) and (4.6). Fig. 4.2 also shows that when the channel quality between Alice and Eve is significantly worse than the channel quality between Alice and Bob, the intercept probability is close to zero for both FT and UT. As expected, the intercept probability increases when the two channels experience identical or relatively similar conditions but FT offers a clear advantage over UT. For example, for $\epsilon_{\mathrm{B}} = 0.09$ and $\epsilon_{\mathrm{E}} = 0.1$, the intercept probability will reduce from 68% to 45% if the mode of operation switches from UT to FT. The reduction in the intercept probability due to the adoption of FT becomes pronounced when ϵ_{E} drops below 0.25.

Fig. 4.3 exhibits the secrecy performance of FT over UT, and quantifies the loss in intercept probability or, equivalently, the gain in secrecy that occurs by changing the operational mode from UT to FT, as noted in (4.7). The optimum value of n, denoted by n^*, has also been plotted in Fig. 4.3 (secondary y-axis on the right-hand side of the plot). For instance, when $\epsilon_{\mathrm{B}} = 0.04$ and $\epsilon_{\mathrm{E}} = 0.14$, a reduction of 0.05 in the intercept

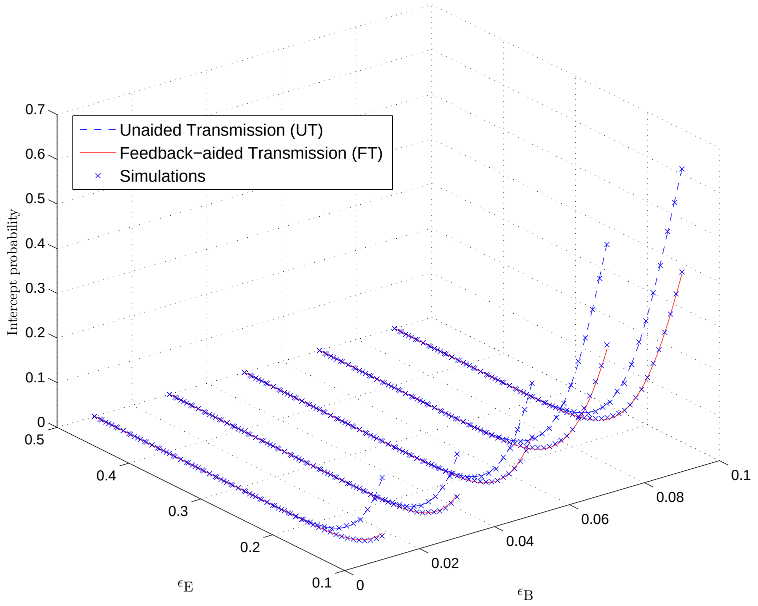


FIGURE 4.2: Comparison between analytical and simulation results for FT and UT, when $\epsilon_E \in [0.1, 0.5]$, $\epsilon_B = \{0.01, 0.03, 0.05, 0.07, 0.09\}$, $m = 50$, $\dot{n} = 150$, $q = 2$ and $\dot{P} = 90\%$.

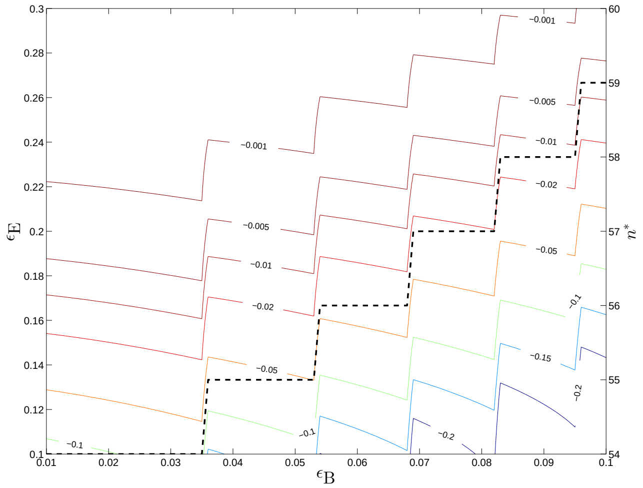


FIGURE 4.3: Contour map (solid lines) depicting the loss in intercept probability caused by the change from UT to FT, as a function of ϵ_E and ϵ_B. The value of n^* (dashed line) as a function of ϵ_B has been superimposed on the plot.

probability is observed, and optimal transmissions $n^* = 55$ are noticed. Moreover, when ϵ_B increases from 0.04 to 0.1, Alice increases the coded packet transmissions from 55 to 59 in an effort to maintain the probability of Bob decoding the source message at $\dot{P} = 90\%$. Notice the abrupt change in the intercept probability each time RAM generates a new optimum value for n, based on ϵ_B.

A way to reduce the intercept probability, especially in settings where the values of ϵ_B and ϵ_E are similar, has been hinted in the Remark. If Alice can measure the instantaneous quality of the channel between her and Bob and transmits coded packets only when the measured quality is above an acceptable threshold, the effective value of ϵ_{B} will be reduced and the intercept probability will drop at the expense of delay.

4.2 Opportunistic Relaying and RLNC for Secure and Reliable Communication

Opportunistic relaying has the potential to achieve full diversity gain, while RLNC can reduce latency and energy consumption. In recent years, there has been a growing interest in the integration of both schemes into wireless networks in order to reap their benefits while taking into account security concerns. This section considers a multi-relay network, where relay nodes employ RLNC to encode confidential data and transmit coded packets to a destination in the presence of an eavesdropper. Four relay selection protocols are studied covering a range of network capabilities, such as the availability of the eavesdropper's channel state information or the possibility to pair the selected relay with a node that intentionally generates interference. For each case, expressions for the probability that a coded packet will not be decoded by a receiver, which can be either the destination or the eavesdropper, are derived. Based on those expressions, a framework is developed that characterizes the probability of the eavesdropper intercepting a sufficient number of coded packets and partially or fully decoding the confidential data. Simulation results confirm the validity and accuracy of the theoretical framework and unveil the security-reliability trade-offs attained by each RLNC-enabled relay selection protocol.

4.2.1 System Model

As shown in Fig. 4.4, we consider a network that consists of a source S, a destination D and a set of $\mathbb{N}$ trusted nodes $\mathcal{S}_{\mathbb{N}} = \{1, \ldots, \mathbb{N}\}$. The source could be an independent node or an element of $\mathcal{S}_{\mathbb{N}}$. The main objective of the nodes in $\mathcal{S}_{\mathbb{N}}$ is to relay information from the source to the destination. However, they can also cause interference to overhearing attacks by a malicious eavesdropper, denoted by E. Links between the source and the destination as well as between the source and the eavesdropper are not considered; the direct links could be in deep shadowing or the destination and the eavesdropper could be outside the coverage area of the source. This is an assumption that is often made in the context of cooperative communications [128, 129], as well as in cooperative relaying for secure communications [93, 130, 131].

A centralized network topology has been used, whereby a control unit located in the source S or a dedicated controller node employs one of the following protocols in order to select a single node or a pair of nodes:

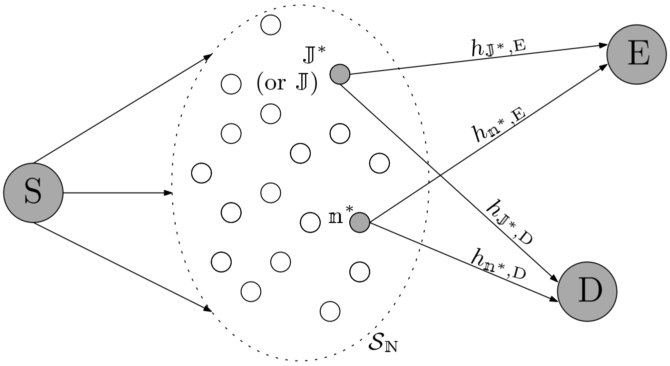

$h_{\mathbb{J}^*,\mathrm{E}}$
E
$\mathbb{J}^*$
(or $\mathbb{J}$)
$h_{\mathbb{n}^*,\mathrm{E}}$
S
$h_{\mathbb{J}^*,\mathrm{D}}$
$\mathbb{n}^*$
$h_{\mathbb{n}^*,\mathrm{D}}$
D
$\mathcal{S}_{\mathbb{N}}$

FIGURE 4.4: Block diagram of the system model.

1. *Conventional selection*: Similarly to [85], the relay that provides the best instantaneous relay-to-destination channel quality is selected.

2. *Optimal selection*: Selection of the optimal relay considers the instantaneous channel quality of both links that originate from each candidate node and terminate at the destination and the eavesdropper, respectively [85].

3. *Conventional selection with jammer*: The conventional selection protocol is first used to determine the node that will act as a relay. The worst instantaneous relay-to-destination link is then identified to determine the node that will transmit noise concurrently with the chosen relay in an effort to degrade the reception quality at the eavesdropper while causing the least interference for the destination.

4. *Optimal selection with preset jammer*: In this case, the node that acts as a jammer is fixed, while the node that acts as a relay is chosen from the remaining nodes in $\mathcal{S}_{\mathbb{N}}$ using the optimal selection protocol.

The relay selected by each of the four protocols is denoted by $\mathbb{n}^*$, the jammer selected by the third protocol in the list is represented by $\mathbb{J}^*$, and the preset jammer in the last protocol is denoted by $\mathbb{J}$. We have opted for optimal selection with a preset jammer in order to provide some insight into how the reliability and security offered by optimal relaying is affected by the introduction of a jammer. Specific techniques for the selection of the appropriate jammer that could further improve the secrecy performance of the network at the expense of reliability could be considered [92, 132] but this discussion is beyond the scope of this work.

In order to achieve optimal performance and to fully exploit spatial diversity, our analysis assumes that the control unit has knowledge of the channel state information (CSI) at the destination in all four protocols. This assumption could be justified by the possible scenario of a receiving node obtaining the downlink CSI and feeding it back to the control unit using an uplink feedback channel [133, 134]. The control unit also has knowledge of the CSI at the eavesdropper in the case of optimal selection with or without a jammer.

Note that this is a common assumption in the physical-layer security literature [86, 135]. For example, the eavesdropper's CSI can be known if the eavesdropper is part of the network of legitimate receivers when unclassified data are broadcast, but is treated as an unauthorized receiver when confidential data are transmitted. Even if an eavesdropper is never destined to receive any type of transmitted data, its presence can still be detected from power leaked via its antenna port while in receiving mode [136].

The delivery of a confidential message by the source to the destination using opportunistic relaying is divided into two phases. In the *first phase*, the source broadcasts the message and the candidate relay nodes operate in receiving mode. In this work, we study the impact that the RLNC-enabled relay selection schemes have on the leakage and reliability of information broadcast by the relay nodes. For this reason, we assume that at the end of the first phase all of the relays have successfully received the message. For example, the source could employ RLNC to segment the message into multiple packets and encode them. The source would then broadcast randomly generated coded packets until all receiving nodes in $\mathcal{S}_{\mathbb{N}}$ have reconstructed the message. Alternatively, the source could transmit coded packets until one of the nodes in $\mathcal{S}_{\mathbb{N}}$ has received the message; the nodes in $\mathcal{S}_{\mathbb{N}}$ could then use short-range communication to exchange packets until all nodes have knowledge of the message. Given that, all the nodes in $\mathcal{S}_{\mathbb{N}}$ are trusted nodes and there are no direct links available between the source and the eavesdropper node, delivery of the broadcast message is considered to be secure during the first phase of communication. In the *second phase*, each node in $\mathcal{S}_{\mathbb{N}}$ divides the message into m data packets. Based on the adopted relay selection protocol, the control unit instructs the chosen relay $\mathbb{n}^*$ to employ RLNC on the data packets and generate a coded packet. The coded packet is further processed by the transmission scheme at the physical layer of the relay. The transmission scheme, which involves forward error correction and modulation techniques, can be accurately characterized by a signal-to-noise ratio (SNR) threshold, denoted by ρ_{th}, as described in [137–139]. This process is repeated up to n times and, thus, up to n coded packets are transmitted; each time, the appropriate relay is selected from $\mathcal{S}_{\mathbb{N}}$, depending on the instantaneous channel conditions. Both the destination D and the eavesdropper E collect coded packets and use them to construct local decoding matrices. If m linearly independent coded packets are received, the rank of the decoding matrix will be m. This implies that the m data packets can be decoded and the entire message can be reconstructed. If the destination decodes the message before the set deadline of n transmissions, it sends a notification to the control unit to terminate the relay selection and packet transmission process.

The relay-to-destination links and the relay-to-eavesdropper links have been modeled as independent but not identically distributed (i.n.i.d) quasi-static Rayleigh fading channels. The channel gain between nodes i and j, denoted by $|h_{i,j}|$, remains constant for the duration of a coded packet but changes independently from packet to packet. The variance of the fading distribution is given by $\sigma_{i,j}^2 = \mathbb{E}\left\{|h_{i,j}|^2\right\} = d_{i,j}^{-\alpha_{i,j}}$, where $\mathbb{E}\left\{|h_{i,j}|^2\right\}$ represents the expected value of $|h_{i,j}|^2$, and $d_{i,j}$ and $\alpha_{i,j}$ are the Euclidean distance and the path loss exponent between the two nodes, respectively. Furthermore, links are impaired by additive white Gaussian noise with zero mean and variance N_0. The instantaneous SNR of the link between i and j is represented as $\rho_{i,j} = \varrho_i |h_{i,j}|^2/N_0$, where ϱ_i is the transmitted power of node i. The probability density function of $\rho_{i,j}$ is equal to [140]

$$\tilde{f}_{\rho_{i,j}}(\rho) = \Pr(\rho_{i,j} = \rho) = \lambda_{i,j} e^{-\rho\lambda_{i,j}} \tag{4.13}$$

where $\lambda_{i,j} = 1/\mathbb{E}\left\{\rho_{i,j}\right\}$. The cumulative density function of $\rho_{i,j}$ can be obtained as follows

$$\tilde{F}_{\rho_{i,j}}(\rho_{\text{th}}) = \Pr(\rho_{i,j} \leq \rho_{\text{th}}) = 1 - e^{-\rho_{\text{th}}\lambda_{i,j}}. \tag{4.14}$$

Both the destination and the eavesdropper in the considered system model apply the Gaussian elimination method on their respective decoding matrices to compute their rank and decode the source message. The objective of the destination is to decodes the entire message, i.e., all of the m data packets. Traditionally, the communication process is deemed to be secure if the eavesdropper fails to decodes the message [64]. By contrast, this work assumes that the probability of the eavesdropper decoding the received coded packets and recovering even a subset of the m data packets should be very small. We shall refer to the probability of the eavesdropper retrieving at least τ of the m data packets as τ-intercept probability and we will evaluate it in Section 4.2.3. However, we will first investigate the impact of the considered relay selection protocols on the capability of the system to reliably and securely relay confidential messages in Section 4.2.2.

4.2.2 Relay Selection and Outage Analysis

This section describes the relay selection protocols in greater detail, and characterizes their performance in terms of the outage probability at the destination D and the outage probability at the eavesdropper E. The outage probability is the probability that the instantaneous signal-to-interference-plus-noise ratio (SINR) at a receiving node, either D or E, will drop below a predefined threshold ρ_{th} due to an event, e.g., deep fading or interference. The outage probability at the destination D and the eavesdropper E, denoted by ϵ_{D} and ϵ_{E}, respectively, can be expressed as

$$\epsilon_{\text{D}} = \Pr(\text{SINR}_{\mathbb{n}^*,\text{D}} \leq \rho_{\text{th}}) \tag{4.15}$$

$$\epsilon_{\mathrm{E}} = \Pr(\mathrm{SINR}_{\mathbb{n}^*,\mathrm{E}} \leq \rho_{\mathrm{th}}) \tag{4.16}$$

where $\mathbb{n}^*$ represents the selected relay. As established in [137] for Rayleigh fading channels and extended in [138] and [139] for other channel models, the outage probability is a very tight approximation of the packet error probability, if the value of ρ_{th} accurately reflects the employed modulation and coding scheme. For example, $\rho_{\mathrm{th}} = 5.89$ dB for uncoded BPSK and $\rho_{\mathrm{th}} = -0.983$ dB for BPSK combined with a typical convolutional code [137] over Rayleigh fading channels. Analytical expressions of ϵ_{D} and ϵ_{E} are derived in this section, which first considers the protocols that only use opportunistic relaying and then focuses on the protocols that combine relaying with jamming.

4.2.2.1 Relay selection protocols without jammer

Conventional selection

This protocol only considers the channel quality of the relay-to-destination link. A relay $\mathbb{n}^*$ is selected from $\mathcal{S}_{\mathbb{N}}$, such that

$$\mathbb{n}^* = \arg\max_{\mathbb{n} \in \mathcal{S}_{\mathbb{N}}} \rho_{\mathbb{n},\mathrm{D}}. \tag{4.17}$$

Owing to the fact that no interference is introduced by a jammer, the SINR at the destination D and the SINR at the eavesdropper E are $\mathrm{SINR}_{\mathbb{n}^*,\mathrm{D}} = \rho_{\mathbb{n}^*,\mathrm{D}}$ and $\mathrm{SINR}_{\mathbb{n}^*,\mathrm{E}} = \rho_{\mathbb{n}^*,\mathrm{E}}$, respectively. The outage probability ϵ_{D} can be obtained by considering the joint probability of every node in $\mathcal{S}_{\mathbb{N}}$ being the selected relay and its link being in outage, that is,

$$\epsilon_{\mathrm{D}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \Pr\left[(\mathbb{n}^* = \mathbb{n}) \bigcap (\rho_{\mathbb{n},\mathrm{D}} \leq \rho_{\mathrm{th}})\right]. \tag{4.18}$$

If we take into account that the channels are statistically independent and that $\rho_{\mathbb{n},\mathrm{D}}$ follows the distribution given in (4.13), we can use order statistics [141] and obtain

$$\begin{aligned} \Pr(\mathbb{n}^* = \mathbb{n}) &= \int_0^\infty \prod_{i=1, i\neq \mathbb{n}}^{\mathbb{N}} \Pr(\rho_{i,\mathrm{D}} \leq x) \tilde{f}_{\rho_{\mathbb{n},\mathrm{D}}}(x)\, dx \\ &= \int_0^\infty \prod_{i=1, i\neq \mathbb{n}}^{\mathbb{N}} \left(1 - e^{-x\lambda_{i,\mathrm{D}}}\right) \tilde{f}_{\rho_{\mathbb{n},\mathrm{D}}}(x)\, dx. \end{aligned} \tag{4.19}$$

The joint probability in (4.18) can be obtained from (4.19) by setting the upper limit of the integral in (4.19) to ρ_{th}, resulting in

$$\epsilon_{\text{D}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \int_{0}^{\rho_{\text{th}}} \prod_{i \neq \mathbb{n}}^{\mathbb{N}} \left(1 - e^{-x\lambda_{i,\text{D}}}\right) \tilde{f}_{\rho_{\mathbb{n},\text{D}}}(x)\, dx. \tag{4.20}$$

Using the multinomial identity [142], the product of terms in (4.20) can be expanded as follows

$$\prod_{i \neq \mathbb{n}}^{\mathbb{N}} (1 - e^{-x\lambda_{i,\text{D}}}) = \sum_{\mathbb{m}=0}^{\mathbb{N}-1} \sum_{\substack{\mathcal{S}_{\mathbb{m}} \subseteq \mathcal{S}_{\mathbb{N}} \setminus \mathbb{n} \\ |\mathcal{S}_{\mathbb{m}}| = \mathbb{m}}} (-1)^{\mathbb{m}} e^{-x \sum_{i \in \mathcal{S}_{\mathbb{m}}} \lambda_{i,\text{D}}} \tag{4.21}$$

where the inner sum in (4.21) is over all possible sets $\mathcal{S}_{\mathbb{m}}$ of size $\mathbb{m}$ that are subsets of $\mathcal{S}_{\mathbb{N}}$ but exclude the node $\mathbb{n}$. Substituting (4.21) into (4.20) and solving the integral leads to

$$\epsilon_{\text{D}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \sum_{\mathbb{m}=0}^{\mathbb{N}-1} \sum_{\substack{\mathcal{S}_{\mathbb{m}} \subseteq \mathcal{S}_{\mathbb{N}} \setminus \mathbb{n} \\ |\mathcal{S}_{\mathbb{m}}| = \mathbb{m}}} (-1)^{\mathbb{m}} \frac{\lambda_{\mathbb{n},\text{D}}}{\sum\limits_{i \in \mathcal{S}_{\mathbb{m}}} \lambda_{i,\text{D}} + \lambda_{\mathbb{n},\text{D}}} \left[1 - e^{-\rho_{\text{th}}\left(\sum_{i \in \mathcal{S}_{\mathbb{m}}} \lambda_{i,\text{D}} + \lambda_{\mathbb{n},\text{D}}\right)}\right]. \tag{4.22}$$

Following the same line of thought, the outage probability at the eavesdropper E can be obtained as follows

$$\epsilon_{\text{E}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \Pr(\mathbb{n}^* = \mathbb{n}) \Pr(\rho_{\mathbb{n},\text{E}} \leq \rho_{\text{th}}) \tag{4.23}$$

because $\rho_{\mathbb{n},\text{D}}$, which determines $\Pr(\mathbb{n}^* = \mathbb{n})$ is independent of $\rho_{\mathbb{n},\text{E}}$. Based on (4.14), we have

$$Pr(\rho_{\mathbb{n},\text{E}} \leq \rho_{\text{th}}) = 1 - e^{-\rho_{\text{th}}\lambda_{\mathbb{n},\text{E}}} \tag{4.24}$$

therefore, expression (4.23) assumes the form

$$\epsilon_{\text{E}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \int_{0}^{\infty} \prod_{i \neq \mathbb{n},}^{\mathbb{N}} \left(1 - e^{-x\lambda_{i,\text{D}}}\right) \left(1 - e^{-\rho_{\text{th}}\lambda_{\mathbb{n},\text{E}}}\right) dx. \tag{4.25}$$

Invoking (4.21) and solving the integral gives the following closed form expression

$$\epsilon_{\text{E}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \sum_{\mathbb{m}=0}^{\mathbb{N}-1} \sum_{\substack{\mathcal{S}_{\mathbb{m}} \subseteq \mathcal{S}_{\mathbb{N}} \setminus \mathbb{n} \\ |\mathcal{S}_{\mathbb{m}}| = \mathbb{m}}} (-1)^{\mathbb{m}} \frac{\lambda_{\mathbb{n},\text{D}}}{\sum\limits_{i \in \mathcal{S}_{\mathbb{m}}} \lambda_{i,\text{D}} + \lambda_{\mathbb{n},\text{D}}} \left(1 - e^{-\rho_{\text{th}}\lambda_{\mathbb{n},\text{E}}}\right). \tag{4.26}$$

Optimal selection

This protocol is deemed 'optimal' because it exploits knowledge of the eavesdropper's CSI and achieves the maximum secrecy capacity [92]. Therefore, this work uses optimal selection as a benchmark protocol and compares its performance to that of the other three protocols. According to this protocol, the relay $\mathbb{n}^*$ is selected such that

$$\mathbb{n}^* = \arg\max_{\mathbb{n}\in\mathcal{S}_{\mathbb{N}}} \left(\frac{\rho_{\mathbb{n},\mathrm{D}}}{\rho_{\mathbb{n},\mathrm{E}}}\right). \tag{4.27}$$

The outage probability at the destination can be obtained from the general expression (4.18) if the probability of the selected relay being a particular node is expressed as

$$\Pr(\mathbb{n}^* = \mathbb{n}) = \int_0^\infty \int_0^\infty I_1(x,y)\tilde{f}_{\rho_{\mathbb{n},\mathrm{D}}}(x)\tilde{f}_{\rho_{\mathbb{n},\mathrm{E}}}(y)\,dx\,dy \tag{4.28}$$

where

$$I_1(x,y) = \prod_{\substack{i=1\\ i\neq\mathbb{n}}}^{\mathbb{N}} \Pr\left(\frac{\rho_{i,\mathrm{D}}}{\rho_{i,\mathrm{E}}} \leq \frac{x}{y}\right). \tag{4.29}$$

If we set $\Lambda_i = \frac{\lambda_{i,\mathrm{D}}}{\lambda_{i,\mathrm{E}}}$, expression (4.29) can be rewritten as [86]

$$I_1(x,y) = \prod_{\substack{i=1\\ i\neq\mathbb{n}}}^{\mathbb{N}} \frac{x\Lambda_i}{x\Lambda_i + y}. \tag{4.30}$$

Using partial fraction expansion and simplifying the resultant expression, (4.30) assumes the form

$$I_1(x,y) = 1 - \sum_{\substack{i=1\\ i\neq\mathbb{n}}}^{\mathbb{N}} \frac{y\Theta_i}{x\Lambda_i + y} \tag{4.31}$$

where Θ_i is the partial fraction coefficient and is equal to

$$\Theta_i = \prod_{k\notin\{\mathbb{n},i\}} \frac{-\Lambda_k}{\Lambda_i - \Lambda_k}, \quad \text{for } \Lambda_k \neq \Lambda_i. \tag{4.32}$$

Substituting (4.28) into (4.18) and taking into account that $\rho_{\mathbb{n},\mathrm{D}}$ should not exceed ρ_{th} gives

$$\epsilon_{\mathrm{D}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \int_0^\infty \int_0^{\rho_{\mathrm{th}}} I_1(x,y)\tilde{f}_{\rho_{\mathbb{n},\mathrm{D}}}(x)\tilde{f}_{\rho_{\mathbb{n},\mathrm{E}}}(y)\,dx\,dy. \tag{4.33}$$

Invoking [143, eq. (3.352.1)] and the relationships in [144, Section 4.2], we obtain

$$\begin{aligned}\epsilon_{\mathrm{D}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} 1 - e^{-\rho_{\mathrm{th}}\lambda_{\mathbb{n},\mathrm{D}}} + \sum_{j\neq\mathbb{n}} \Theta_j \lambda_{\mathbb{n},\mathrm{E}} e^{-\rho_{\mathrm{th}}(\lambda_{\mathbb{n},\mathrm{D}}-\Lambda_j\lambda_{\mathbb{n},\mathrm{E}})} \Bigg[\mathrm{E}_1\big((\alpha_2+1)\lambda_{\mathbb{n},\mathrm{D}}\rho_{\mathrm{th}}\big) \Bigg\{ \frac{\Lambda_j\rho_{\mathrm{th}}}{\alpha_2} - \\ \frac{\Lambda_j}{\lambda_{\mathbb{n},\mathrm{D}}\alpha_2^2} \Bigg\} + e^{-\rho_{\mathrm{th}}\alpha_2\lambda_{\mathbb{n},\mathrm{D}}} \mathrm{E}_1(\rho_{\mathrm{th}}\lambda_{\mathbb{n},\mathrm{D}}) \frac{\Lambda_j}{\lambda_{\mathbb{n},\mathrm{D}}\alpha_2^2} - \frac{\Lambda_j}{\lambda_{\mathbb{n},\mathrm{D}}\alpha_2(\alpha_2+1)} e^{-\rho_{\mathrm{th}}(\alpha_2+1)\lambda_{\mathbb{n},\mathrm{D}}} \Bigg] \\ - \frac{\Theta_j\lambda_{\mathbb{n},\mathrm{D}}\lambda_{\mathbb{n},\mathrm{E}}}{\Lambda_j\alpha_1^2} \Bigg\{ \ln\left(1+\frac{\alpha_1}{\beta_1}\right) - \frac{\alpha_1}{\lambda_{\mathbb{n},\mathrm{E}}} \Bigg\}\end{aligned} \tag{4.34}$$

where $\alpha_1 = \lambda_{\mathbb{n},\mathrm{E}} - \frac{\lambda_{\mathbb{n},\mathrm{D}}}{\Lambda_j}$, $\alpha_2 = \frac{\Lambda_j\lambda_{\mathbb{n},\mathrm{E}}}{\lambda_{\mathbb{n},\mathrm{D}}} - 1$, $\beta_1 = \frac{\lambda_{\mathbb{n},\mathrm{D}}}{\Lambda_j}$ and E_1 is the exponential integral, as defined in [143].

The value of $\rho_{\mathbb{n},\mathrm{E}}$ in optimal relay selection affects the probability that a node will be selected to act as a relay. As a result, and in contrast to (4.23), the outage probability at the eavesdropper has to be expressed as the summation of joint probabilities, as follows

$$\epsilon_{\mathrm{E}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \Pr\left[(\mathbb{n}^* = \mathbb{n}) \bigcap (\rho_{\mathbb{n},\mathrm{E}} \leq \rho_{\mathrm{th}})\right]. \tag{4.35}$$

Taking into account (4.28) and recalling that the value of $\rho_{\mathbb{n},\mathrm{E}}$ needs to be upper bounded by ρ_{th}, we obtain

$$\epsilon_{\mathrm{E}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \int_0^{\rho_{\mathrm{th}}} \int_0^{\infty} I_1(x,y) \tilde{f}_{\rho_{\mathbb{n},\mathrm{D}}}(x) \tilde{f}_{\rho_{\mathbb{n},\mathrm{E}}}(y)\, dx\, dy. \tag{4.36}$$

Derivation of an analytical expression for ϵ_{E} requires a similar approach to that in (4.34), and leads to

$$\begin{aligned}\epsilon_{\mathrm{E}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} 1 - e^{-\rho_{\mathrm{th}}\lambda_{\mathbb{n},\mathrm{E}}} + \sum_{j\neq\mathbb{n}} \frac{\Theta_j\lambda_{\mathbb{n},\mathrm{D}}\lambda_{\mathbb{n},\mathrm{E}}}{\Lambda_j\alpha_1^2} \Bigg[\mathrm{E}_1\big(\lambda_{\mathbb{n},\mathrm{E}}\rho_{\mathrm{th}}\big) - (1+\alpha_1\rho_{\mathrm{th}}) e^{-\alpha_1\rho_{\mathrm{th}}} \mathrm{E}_1(\beta_1\rho_{\mathrm{th}}) \\ - \frac{\alpha_1}{\lambda_{\mathbb{n},\mathrm{E}}}\big(1 - e^{-\rho_{\mathrm{th}}\lambda_{\mathbb{n},\mathrm{E}}}\big) + \ln\left(1+\frac{\alpha_1}{\beta_1}\right) \Bigg].\end{aligned} \tag{4.37}$$

4.2.2.2 Relay selection protocols with jammer

In an effort to increase the outage probability at the eavesdropper, a jammer can be employed by the two aforementioned protocols. The selection mechanism of the jammer and its impact on the outage probability at the destination and at the eavesdropper are investigated in this subsection.

Conventional selection with jammer

This protocol is based on a joint relay-jammer pair selection scheme. Similarly to conventional selection, this protocol first selects a relay $\mathbb{n}^*$ from $\mathcal{S}_{\mathbb{N}}$ that provides the best instantaneous SNR at the destination. Subsequently, one of the remaining nodes in $\mathcal{S}_{\mathbb{N}}$ is selected to act as a jammer, such that it causes the least interference to the destination. The pair selection scheme can be described by the following expressions

$$\mathbb{n}^* = \arg\max_{\mathbb{n}\in\mathcal{S}_{\mathbb{N}}} \rho_{\mathbb{n},\mathrm{D}} \tag{4.38}$$

$$J^* = \arg\min_{j\in\mathcal{S}_{\mathbb{N}}\backslash\mathbb{n}^*} \rho_{j,\mathrm{D}}. \tag{4.39}$$

The SINR at the destination and the SINR at the eavesdropper are given by

$$\mathrm{SINR}_{\mathbb{n}^*,\mathrm{D}} = \frac{\rho_{\mathbb{n}^*,\mathrm{D}}}{\rho_{\mathbb{J}^*,\mathrm{D}}+1} \tag{4.40}$$

$$\mathrm{SINR}_{\mathbb{n}^*,\mathrm{E}} = \frac{\rho_{\mathbb{n}^*,\mathrm{E}}}{\rho_{\mathbb{J}^*,\mathrm{E}}+1}. \tag{4.41}$$

respectively. Clearly, both $\mathrm{SINR}_{\mathbb{n}^*,\mathrm{D}}$ and $\mathrm{SINR}_{\mathbb{n}^*,\mathrm{E}}$ depend on the selected nodes $\mathbb{n}^*$ and $\mathbb{J}^*$.

The outage probability at the destination should consider the joint probability of a node $\mathbb{n}$ being the relay, a different node $\mathbb{m}$ being the jammer, and the SINR at the destination not exceeding the SNR threshold ρ_{th}, for all possible values of $\mathbb{n}$ and $\mathbb{m}$. Therefore, ϵ_{D} can be written as

$$\epsilon_{\mathrm{D}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \sum_{\mathbb{m}\neq\mathbb{n}}^{\mathbb{N}} \Pr\left[(\mathbb{n}^*=\mathbb{n})\bigcap(\mathbb{J}^*=\mathbb{m})\bigcap\left(\frac{\rho_{\mathbb{n},\mathrm{D}}}{\rho_{\mathbb{m},\mathrm{D}}+1}\leq\rho_{\mathrm{th}}\right)\right]. \tag{4.42}$$

Taking into account that the instantaneous SNR of the jammer-to-destination channel cannot be greater than the instantaneous SNR of the relay-to-destination channel, and that the two channels are independent, we can express the joint probability of selecting a relay-jammer pair as follows

$$\Pr\Big[(\mathbb{n}^*=\mathbb{n})\bigcap(\mathbb{J}^*=\mathbb{m})\Big] = \int_0^{\infty}\int_0^{\rho_{\mathbb{n},\mathrm{D}}} I_2(x,y)\tilde{f}_{\rho_{\mathbb{m},\mathrm{D}}}(y)\tilde{f}_{\rho_{\mathbb{n},\mathrm{D}}}(x)\,dy\,dx \tag{4.43}$$

where

$$I_2(x,y) = \prod_{i\neq\mathbb{n},i\neq\mathbb{m}}^{\mathbb{N}-2} \Pr(y\leq\rho_{i,\mathrm{D}}\leq x). \tag{4.44}$$

Invoking (4.14), $I_2(x, y)$ assumes the form

$$I_2(x,y) = \prod_{i \neq \mathbb{n}, i \neq \mathbb{m}}^{\mathbb{N}-2} \left(e^{-y\lambda_{i,\mathrm{D}}} - e^{-x\lambda_{i,\mathrm{D}}}\right) \tag{4.45}$$

which can be rewritten as

$$I_2(x,y) = \sum_{w=0}^{\mathbb{N}-2} \sum_{\substack{\mathcal{X}=\mathcal{S}_{\mathbb{N}} \setminus \{\mathbb{n},\mathbb{m}\} \\ \mathcal{S}_w \subseteq \mathcal{X}, \bar{\mathcal{S}}_w \subseteq \mathcal{X} \\ |\mathcal{S}_w|=w}} (-1)^w e^{-x\sum_{i\in\mathcal{S}_w}\lambda_{i,\mathrm{D}} - y\sum_{j\in\bar{\mathcal{S}}_w}\lambda_{j,\mathrm{D}}} \tag{4.46}$$

using the multinomial identity. Substituting (4.43) into (4.42) and properly setting the limits of the two integrals gives

$$\epsilon_{\mathrm{D}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \sum_{\mathbb{m}\neq\mathbb{n}}^{\mathbb{N}} \int_0^{\delta} \int_y^{(y+1)\rho_{\mathrm{th}}} I_2(x,y) \tilde{f}_{\rho_{\mathbb{n},\mathrm{D}}}(x) \tilde{f}_{\rho_{\mathbb{m},\mathrm{D}}}(y)\, dx\, dy \tag{4.47}$$

where $\delta = \infty$ for $\rho_{\mathrm{th}} \geq 1$, and $\delta = \frac{\rho_{\mathrm{th}}}{1-\rho_{\mathrm{th}}}$ otherwise. Solving the integrals, we obtain

$$\epsilon_{\mathrm{D}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \sum_{\mathbb{m}\neq\mathbb{n}}^{\mathbb{N}} \sum_{w=0}^{\mathbb{N}-2} \sum_{\substack{\mathcal{X}=\mathcal{S}_{\mathbb{N}} \setminus \{\mathbb{n},\mathbb{m}\} \\ \mathcal{S}_w \subseteq \mathcal{X}, \bar{\mathcal{S}}_w \subseteq \mathcal{X} \\ |\mathcal{S}_w|=w}} (-1)^w \lambda_{\mathbb{n},\mathrm{D}}\, \lambda_{\mathbb{m},\mathrm{D}}\, \delta_{\mathbb{n},\mathbb{m}} \tag{4.48}$$

where

$$\delta_{\mathbb{n},\mathbb{m}} = \begin{cases} \frac{1}{c_{\mathbb{n}}\lambda_{\mathrm{D}}} - \frac{e^{-\rho_{\mathrm{th}}c_{\mathbb{n}}}}{c_{\mathbb{n}}c_{\mathbb{n},\mathbb{m}}}, & \text{for } \rho_{\mathrm{th}} \geq 1 \\ \frac{1-e^{-\frac{\rho_{\mathrm{th}}\lambda_{\mathrm{D}}}{1-\rho_{\mathrm{th}}}}}{c_{\mathbb{n}}\lambda_{\mathrm{D}}} - e^{\rho_{\mathrm{th}}c_{\mathbb{n}}}\left[\frac{1-e^{-\frac{\rho_{\mathrm{th}}c_{\mathbb{n},\mathbb{m}}}{1-\rho_{\mathrm{th}}}}}{c_{\mathbb{n}}c_{\mathbb{n},\mathbb{m}}}\right], & \text{for } \rho_{\mathrm{th}} < 1 \end{cases}$$

and $c_{\mathbb{n}} = \left(\sum_{i\in\mathcal{S}_w}\lambda_{i,\mathrm{D}} + \lambda_{\mathbb{n},\mathrm{D}}\right)$, $c_{\mathbb{m}} = \left(\sum_{j\in\bar{\mathcal{S}}_w}\lambda_{j,\mathrm{D}} + \lambda_{\mathbb{m},\mathrm{D}}\right)$, $c_{\mathbb{n},\mathbb{m}} = (\rho_{\mathrm{th}}c_{\mathbb{n}} + c_{\mathbb{m}})$, $\lambda_{\mathrm{D}} = \sum_{k=1}^{\mathbb{N}} \lambda_{k,\mathrm{D}}$.

Due to the fact that the process of selecting the relay and the jammer is independent of the eavesdropper's CSI, the outage probability at the eavesdropper can be obtained as follows

$$\epsilon_{\mathrm{E}} = \sum_{\mathbb{n}=1}^{\mathbb{N}} \sum_{\mathbb{m}\neq\mathbb{n}}^{\mathbb{N}} \Pr\left[(\mathbb{n}^* = \mathbb{n}) \bigcap (\mathbb{J}^* = \mathbb{m})\right] \Pr\left(\frac{\rho_{\mathbb{n},\mathrm{E}}}{\rho_{\mathbb{m},\mathrm{E}}+1} \leq \rho_{\mathrm{th}}\right). \tag{4.49}$$

Using (4.43), we can express the joint probability of selecting the relay-jammer pair as

$$\Pr\left[(\mathbb{n}^* = \mathbb{n}) \bigcap (\mathbb{J}^* = \mathbb{m})\right] = \sum_{w=0}^{\mathbb{N}-2} \sum_{\substack{\mathcal{X}=\mathcal{S}_{\mathbb{N}} \setminus \{\mathbb{n},\mathbb{m}\} \\ \mathcal{S}_w \subseteq \mathcal{X}, \bar{\mathcal{S}}_w \subseteq \mathcal{X} \\ |\mathcal{S}_w|=w}} (-1)^w \frac{\lambda_{\mathbb{n},\mathrm{D}}\lambda_{\mathbb{m},\mathrm{D}}}{c_{\mathbb{m}}} \left[\frac{1}{c_{\mathbb{n}}} - \frac{1}{\lambda_{\mathrm{D}}}\right]$$

while the probability that the SINR at the eavesdropper will not be greater than the SNR threshold is given by

$$\begin{aligned}\Pr\left(\frac{\rho_{\mathbb{n},\mathrm{E}}}{\rho_{\mathbb{m},\mathrm{E}}+1} \le \rho_{\mathrm{th}}\right) &= \Pr\big(\rho_{\mathbb{n},\mathrm{E}} \le \rho_{\mathrm{th}}(\rho_{\mathbb{m},\mathrm{E}}+1)\big)\\ &= \int\limits_0^\infty \big(1-e^{-\rho_{\mathrm{th}}(y+1)}\big)\tilde{f}_{\rho_{\mathbb{m},\mathrm{E}}}(y)\,dy\\ &= 1-\frac{\lambda_{\mathbb{m},\mathrm{E}}\,e^{-\rho_{\mathrm{th}}\lambda_{\mathbb{n},\mathrm{E}}}}{\rho_{\mathrm{th}}\lambda_{\mathbb{n},\mathrm{E}}+\lambda_{\mathbb{m},\mathrm{E}}}.\end{aligned}$$

Optimal selection with preset jammer

According to this protocol, the control unit preselects a node $\mathbb{J}$ to act as a jammer and then employs optimal selection on the remaining nodes for each coded packet transmission. The identification of a suitable jammer could depend on the average quality of the link between the jammer and the destination. However, the selection process of the preset jammer is not further discussed in this work because it does not affect the outage analysis of this protocol. As in the case of optimal selection, a node is selected to act as a relay such that

$$\mathbb{n}^* = \arg\max_{\mathbb{n}\in\mathcal{S}_{\mathbb{N}}\setminus\mathbb{J}} \left(\frac{\rho_{\mathbb{n},\mathrm{D}}}{\rho_{\mathbb{n},\mathrm{E}}}\right). \tag{4.50}$$

Owing to the interference noise generated by $\mathbb{J}$, the SINR at the destination and the SINR at the eavesdropper are given by

$$\mathrm{SINR}_{\mathbb{n}^*,\mathrm{D}} = \frac{\rho_{\mathbb{n}^*,\mathrm{D}}}{\rho_{\mathbb{J},\mathrm{D}}+1} \tag{4.51}$$

$$\mathrm{SINR}_{\mathbb{n}^*,\mathrm{E}} = \frac{\rho_{\mathbb{n}^*,\mathrm{E}}}{\rho_{\mathbb{J},\mathrm{E}}+1}. \tag{4.52}$$

Using the law of total probability, as in the previous cases, the outage probability at the destination can be expressed as

$$\epsilon_{\mathrm{D}} = \sum_{\mathbb{n}=1}^{\mathbb{N}-1} \Pr\left[(\mathbb{n}^*=\mathbb{n}) \bigcap \left(\frac{\rho_{\mathbb{n},\mathrm{D}}}{\rho_{\mathbb{J},\mathrm{D}}+1} \le \rho_{\mathrm{th}}\right)\right]. \tag{4.53}$$

The probability that the selected relay $\mathbb{n}^*$ will be a particular node $\mathbb{n}$ can be obtained from (4.28) if the remaining $\mathbb{N}-1$ of the $\mathbb{N}$ nodes in $\mathcal{S}_{\mathbb{N}}$ are considered, that is,

$$\Pr(\mathbb{n}^*=\mathbb{n}) = \int\limits_0^\infty\int\limits_0^\infty \hat{I}_1(x,y)\tilde{f}_{\rho_{\mathbb{n},\mathrm{D}}}(x)\tilde{f}_{\rho_{\mathbb{n},\mathrm{E}}}(y)\,dx\,dy \tag{4.54}$$

where

$$\hat{I}_1(x,y) = 1 - \sum_{\substack{i=1\\ i\neq \mathbb{n}}}^{\mathbb{N}-1} \frac{\Theta_i y}{x\Lambda_i + y}. \tag{4.55}$$

Integrating (4.54) over all valid values of $\rho_{\mathbb{n},\mathrm{D}}$ and $\rho_{\mathbb{J},\mathrm{D}}$, as dictated by (4.53), gives

$$\epsilon_{\mathrm{D}} = \sum_{\mathbb{n}=1}^{\mathbb{N}-1} \int_0^\infty \int_0^\infty \int_0^{\upsilon} \hat{I}_1(x,y) \tilde{f}_{\rho_{\mathbb{n},\mathrm{D}}}(x) \tilde{f}_{\rho_{\mathbb{J},\mathrm{D}}}(z) \tilde{f}_{\rho_{\mathbb{n},\mathrm{E}}}(y)\, dx\, dz\, dy$$

where $\upsilon = (z+1)\rho_{\mathrm{th}}$. Evaluating the integrals and utilizing the relationships in [143, 144] leads to

$$\epsilon_{\mathrm{D}} = \sum_{\mathbb{n}=1}^{\mathbb{N}-1} 1 - \frac{\lambda_{\mathbb{J},\mathrm{D}} e^{-\rho_{\mathrm{th}}\lambda_{\mathbb{n},\mathrm{D}}}}{\rho_{\mathrm{th}}\lambda_{\mathbb{n},\mathrm{E}} + \lambda_{\mathbb{J},\mathrm{D}}} + \sum_{j\neq \mathbb{n}}^{\mathbb{N}-1} \Theta_j \frac{\lambda_{\mathbb{n},\mathrm{D}}\lambda_{\mathbb{n},\mathrm{E}}}{\Lambda_j} \Bigg\{ \frac{e^{\lambda_{\mathbb{J},\mathrm{D}}}}{\alpha_3} H_{\mathbb{n},j}(\alpha_3,\beta_2,\eta_2) - \frac{1}{\alpha_1} H_{\mathbb{n},j}(\alpha_1,\beta_1,\eta_1) \\ - \frac{1}{\alpha_1^2}\left[\ln\left(\frac{\lambda_{\mathbb{n},\mathrm{E}}}{\beta_1}\right) - \frac{\alpha_1}{\lambda_{\mathbb{n},\mathrm{E}}}\right]\Bigg\} \tag{4.56}$$

with

$$H_{\mathbb{n},j}(\alpha,\beta,\eta) = e^{\frac{\alpha\eta}{\beta}} \left(\frac{1}{\alpha} - \frac{\eta}{\beta}\right) \mathrm{E}_1\left(\frac{\alpha+\beta}{\beta}\eta\right) - \frac{1}{\alpha}\mathrm{E}_1(\eta) + \frac{1}{\alpha+\beta} e^{-\eta} \tag{4.57}$$

where $\alpha_3 = \alpha_1 - \frac{\lambda_{j,\mathrm{D}}}{\rho_{\mathrm{th}}\Lambda_j}$, $\beta_2 = \beta_1 + \frac{\lambda_{\mathbb{J},\mathrm{D}}}{\rho_{\mathrm{th}}\Lambda_j}$, $\eta_1 = \rho_{\mathrm{th}}\lambda_{\mathbb{n},\mathrm{D}}$ and $\eta_2 = \eta_1 + \lambda_{\mathbb{J},\mathrm{D}}$.

Similarly, the outage probability at the eavesdropper can be as written as

$$\epsilon_{\mathrm{E}} = \sum_{\mathbb{n}=1}^{\mathbb{N}-1} \Pr\left[(\mathbb{n}^* = \mathbb{n}) \bigcap \left(\frac{\rho_{\mathbb{n},\mathrm{E}}}{\rho_{\mathbb{J},\mathrm{E}} + 1} \leq \rho_{\mathrm{th}}\right)\right]. \tag{4.58}$$

Using (4.54), the joint probability in (4.58) can be obtained from

$$\Pr\left[(\mathbb{n}^* = \mathbb{n}) \bigcap \left(\frac{\rho_{\mathbb{n},\mathrm{E}}}{\rho_{\mathbb{J},\mathrm{E}} + 1} \leq \rho_{\mathrm{th}}\right)\right] = \int_0^\infty \int_0^{\upsilon} \int_0^\infty \hat{I}_1(x,y) \tilde{f}_{\rho_{\mathbb{n},\mathrm{D}}}(x) \tilde{f}_{\rho_{\mathbb{n},\mathrm{E}}}(y) \tilde{f}_{\rho_{\mathbb{J},\mathrm{E}}}(z)\, dx\, dy\, dz \tag{4.59}$$

which allows us to rewrite (4.58) as

$$\epsilon_{\mathrm{E}} = \sum_{\mathbb{n}=1}^{\mathbb{N}-1} \int_0^\infty \int_0^{\upsilon} \int_0^\infty \hat{I}_1(x,y) \tilde{f}_{\rho_{\mathbb{n},\mathrm{D}}}(x) \tilde{f}_{\rho_{\mathbb{n},\mathrm{E}}}(y) \tilde{f}_{\rho_{\mathbb{J},\mathrm{E}}}(z)\, dx\, dy\, dz. \tag{4.60}$$

Taking into account the formulas in [143, 144], we obtain the following expression for the outage probability at the eavesdropper:

$$
\begin{aligned}
\epsilon_{\mathrm{E}} = \sum_{\mathbb{n}=1}^{\mathbb{N}-1} 1 - \frac{\lambda_{\mathbb{J},\mathrm{E}} e^{-\rho_{\mathrm{th}} \lambda_{\mathbb{n},\mathrm{E}}}}{\rho_{\mathrm{th}} \lambda_{\mathbb{n},\mathrm{E}} + \lambda_{\mathbb{J},\mathrm{E}}} - \sum_{j \neq \mathbb{n}}^{\mathbb{N}-1} \Theta_j \frac{\lambda_{\mathbb{n},\mathrm{D}} \lambda_{\mathbb{n},\mathrm{E}}}{\Lambda_j \alpha_1^2} \Bigg[& \mathrm{E}_1\{\lambda_{\mathbb{n},\mathrm{E}} \rho_{\mathrm{th}}\} - e^{\lambda_{\mathbb{J},\mathrm{E}}} \mathrm{E}_1(\lambda_{\mathbb{n},\mathrm{E}} \rho_{\mathrm{th}} + \lambda_{\mathbb{J},\mathrm{E}}) \\
& - e^{-\alpha_1 \rho_{\mathrm{th}}} \frac{\lambda_{\mathbb{J},\mathrm{E}}(1 + \alpha_1 \rho_{\mathrm{th}})}{\alpha_1 \rho_{\mathrm{th}} + \lambda_{\mathbb{J},\mathrm{E}}} \Big\{ \mathrm{E}_1(\beta_1 \rho_{\mathrm{th}}) - e^{(\alpha_1 \rho_{\mathrm{th}} + \lambda_{\mathbb{J},\mathrm{E}})} \mathrm{E}_1(\lambda_{\mathbb{n},\mathrm{E}} \rho_{\mathrm{th}} + \lambda_{\mathbb{J},\mathrm{E}}) \Big\} \\
& + \frac{e^{-\alpha_1 \rho_{\mathrm{th}}} \lambda_{\mathbb{J},\mathrm{E}} \alpha_1 \rho_{\mathrm{th}}}{\alpha_4} H_{\mathbb{n},j}(\alpha_4, \beta_3, \eta_3) + \frac{\alpha_1 \lambda_{\mathbb{J},\mathrm{E}} e^{-\lambda_{\mathbb{n},\mathrm{E}} \rho_{\mathrm{th}}}}{\lambda_{\mathbb{n},\mathrm{E}} \{\rho_{\mathrm{th}} \lambda_{\mathbb{n},\mathrm{E}} + \lambda_{\mathbb{J},\mathrm{E}}\}} + \ln\left(\frac{\lambda_{\mathbb{n},\mathrm{E}}}{\beta_1}\right) - \frac{\alpha_1}{\lambda_{\mathbb{n},\mathrm{E}}} \Bigg]
\end{aligned}
$$

where $\alpha_4 = \alpha_1 \rho_{\mathrm{th}} + \lambda_{J,\mathrm{E}}$ and $\beta_3 = \eta_3 = \beta_1 \rho_{\mathrm{th}}$.

The expressions for ϵ_{D} and ϵ_{E} that were obtained in this section for the four considered protocols will be used in the following section for the evaluation of the secrecy performance of the system when the selected relay employs RLNC.

4.2.3 Secrecy Analysis

4.2.3.1 Preliminaries

In the literature work, when physical layer security over wireless fading channels is offered in the form of cooperative jamming, the secrecy outage probability is often the preferred metric for assessing the secrecy performance of the system [92, 93, 131, 132]. The secrecy outage probability assumes *strong* security, that is, the eavesdropper decoding the encoded message is as likely as guessing the message itself. In practice, the secrecy requirements can be less stringent and alternative metrics have been proposed in [145].

Secure transmission on a multicast or broadcast network can be guaranteed if RLNC is used to combine data packets with random keys [146]. In conventional RLNC for multicast or broadcast applications, as in this work, data packets are combined with other data packets in order to increase capacity or improve reliability without the need for retransmissions. As shown in [147], conventional RLNC can still offer strong security, if the entries of the decoding matrix are transmitted through a secure private channel to the intended destination, and source coding ensures that the zero element is not included in the data packets. Otherwise, RLNC offers *weak security*, as defined in [148], implying that a receiver (either D or E) may not be able to decode any meaningful information about the message without collecting a sufficient number of linearly independent coded packets. However, both [148] and [149] agree that strong security can be achieved if RLNC operations are over a large finite field.

The goal of Section 4.2.3 is to evaluate the inherent security of conventional RLNC for any size of finite field, when jamming may or may not be available at the physical layer. We consider the communication process to be secure when the destination decodes the message, while the eavesdropper is unable to decode even parts of the message without guessing. As explained in Section 4.2.1, the probability of the eavesdropper being successful in decoding at least τ of the m data packets using Gaussian elimination shall be referred to as the τ-intercept probability. We note that this metric can complement the algebraic security criterion presented in [149], which assumes that the number of decodable data packets is a readily available parameter and is not computed. The remainder of this section presents a framework for the calculation of the τ-intercept probability and the characterization of the secrecy performance of the system.

4.2.3.2 Derivation of the τ-intercept probability

A receiver is required to collect m linearly independent coded packets to decode the m data packets that compose the message. The probability of decoding the message can be obtained by employing (2.2), as follows

$$P(\hat{n}, m) = \prod_{i=0}^{m-1} \left[1 - q^{-(\hat{n}-i)}\right]$$

where $\hat{n}$ is the number of received coded packets and q represents the size of the finite field over which arithmetic operations are performed. The system of linear equations, which is represented by the decoding matrix, may be partially solved using the Gaussian elimination method and τ of the m data packets could be revealed based on a subset of $r \leq m$ linearly independent coded packets that have been received. The probability of decoding *exactly* $\tau \leq r$ data packets, given that r linearly independent coded packets have been collected, can be obtained from [150] as follows

$$P(\tau, m|r) = \frac{\binom{m}{\tau}}{\begin{bmatrix} m \\ r \end{bmatrix}_q} \sum_{j=0}^{m-\tau} (-1)^j \binom{m-\tau}{j} \begin{bmatrix} m-\tau-j \\ r-\tau-j \end{bmatrix}_q . \tag{4.61}$$

Therefore, the probability of decoding *at least* τ data packets can be obtained from

$$\mathbb{P}(\tau, \hat{n}) = \sum_{r=\tau}^{\min(\hat{n},m)} \sum_{i=\tau}^{r} P(i, m|r) P_r(\hat{n}, m) \tag{4.62}$$

where $P_r(m, \hat{n})$ is the probability that r out of the $\hat{n}$ received coded packets are linearly independent and is given by (2.6), but repeated here for convenience

$$P_r(\hat{n}, m) = \frac{1}{q^{\hat{n}m}} \begin{bmatrix} \hat{n} \\ r \end{bmatrix}_q \prod_{i=0}^{r-1} (q^m - q^i).$$

Using the aforementioned expressions, we can characterize the secrecy performance of the system. Let X_D and X_E be two random variables, representing the number of transmissions required by the destination D and the eavesdropper E, respectively, such that D can decode the entire message and E can decode at least τ data packets. Likewise (4.1), the cumulative distribution function of X_D and X_E can be expressed as

$$F_\mathrm{D}(n_\mathrm{T}) = \Pr\left\{X_\mathrm{D} \le n_\mathrm{T}\right\} = \sum_{\hat{n}=m}^{n_\mathrm{T}} \binom{n_\mathrm{T}}{\hat{n}} \epsilon_\mathrm{D}^{n_\mathrm{T}-\hat{n}} (1-\epsilon_\mathrm{D})^{\hat{n}} \; P(\hat{n}, m)$$

$$F_\mathrm{E}(\tau, n_\mathrm{T}) = \Pr\left\{X_\mathrm{E} \le n_\mathrm{T}\right\} = \sum_{\hat{n}=\tau}^{n_\mathrm{T}} \binom{n_\mathrm{T}}{\hat{n}} \epsilon_\mathrm{E}^{n_\mathrm{T}-\hat{n}} (1-\epsilon_\mathrm{E})^{\hat{n}} \mathbb{P}(\tau, \hat{n})$$

where ϵ_D and ϵ_E represent the probability that a transmitted coded packet will not be received by the destination and the eavesdropper, respectively. Both ϵ_D and ϵ_E can be evaluated using the outage probability expressions that have been derived in Section 4.2.2 for each relay selection protocol. Essentially, $F_\mathrm{D}(n_\mathrm{T})$ is the probability that the destination will reconstruct the entire confidential message, and $F_\mathrm{E}(\tau, n_\mathrm{T})$ is the probability that the eavesdropper will decode at least τ of the m data packets that compose the message, for n_T *or fewer* coded packet transmissions. The respective decoding probabilities for *exactly* n_T coded packet transmissions can be obtained from the probability mass functions, as follows

$$f_\mathrm{D}(n_\mathrm{T}) = \Pr\left\{X_\mathrm{D} = n_\mathrm{T}\right\} = \begin{cases} F_\mathrm{D}(n_\mathrm{T}) - F_\mathrm{D}(n_\mathrm{T}-1), & \text{if } m < n_\mathrm{T} \le n \\ F_\mathrm{D}(m), & \text{if } n_\mathrm{T} = m \end{cases}$$

$$f_\mathrm{E}(n_\mathrm{T}) = \Pr\left\{X_\mathrm{E} = n_\mathrm{T}\right\} = \begin{cases} F_\mathrm{E}(\tau, n_\mathrm{T}) - F_\mathrm{E}(\tau, n_\mathrm{T}-1), & \text{if } \tau < n_\mathrm{T} \le n \\ F_\mathrm{E}(\tau, n_\mathrm{T}), & \text{if } n_\mathrm{T} = \tau \end{cases}$$

where n represents the maximum permitted number of coded packet transmissions. In the event of the destination reconstructing the entire message before the deadline is reached, a feedback link is used to notify the control unit that additional coded packet transmissions are not required. Following the same line of reasoning as in Section 4.1.2, the τ-intercept probability assumes the form

$$P_{\text{int}}(\tau, n) = F_{\text{E}}(\tau, n) \left[1 - F_{\text{D}}(n) \right] + \sum_{n_{\text{T}}=m}^{n} f_{\text{D}}(n_{\text{T}}) \, F_{\text{E}}(\tau, n_{\text{T}}). \tag{4.63}$$

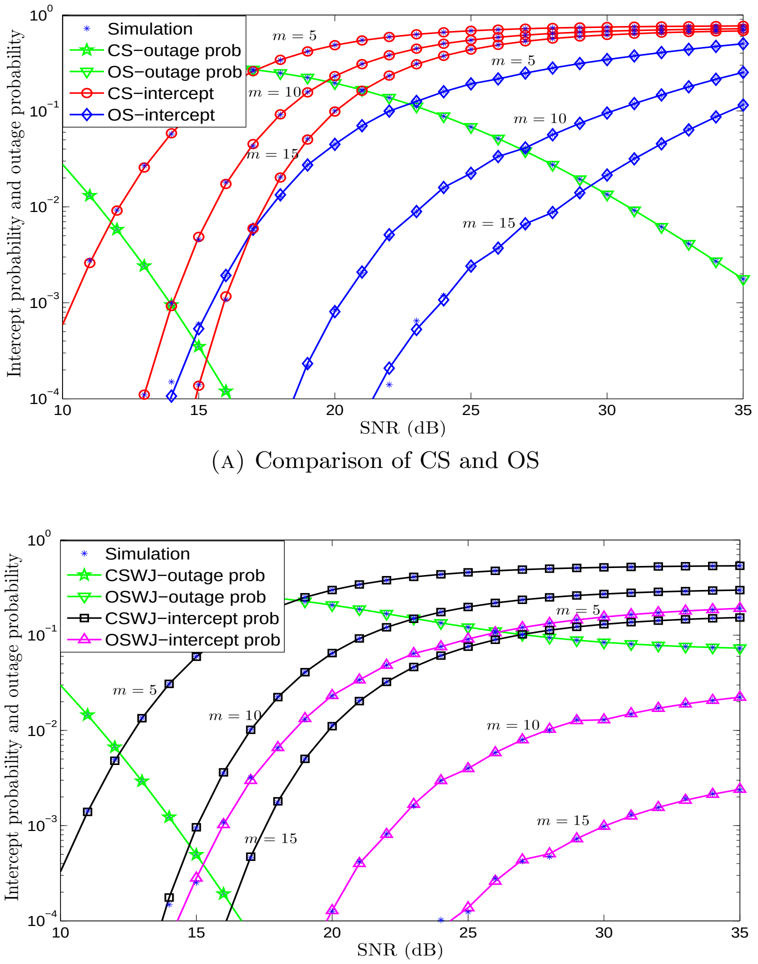
The first term in (4.63) is the probability that the eavesdropper will be successful in decoding at least τ data packets from the intercepted coded packets but the destination will fail to reconstruct the message after n coded packet transmissions. The second term represents the probability that the destination will decode the entire message after the n_{T}-th coded packet has been transmitted but the eavesdropper has already decoded at least τ data packets by that time.

The impact of the relay selection protocol on the outage probabilities ϵ_{D} and ϵ_{E}, and their effect on the intercept probability $P_{\text{int}}(\tau, n)$ and the decoding probability at the destination $F_{\text{D}}(n)$ will be explored in the following section.

4.2.4 Results and Discussions

This section presents simulation results and compares them with analytical results in order to validate the accuracy of the derived expressions. The secrecy performance of the system, which is reflected by the intercept probability at the eavesdropper, and the reliability performance of the system, which is associated with the outage probability of the link between the selected relay and the destination but also the decoding probability at the destination, are also discussed.

A Monte Carlo simulation platform representing the system model was developed in MATLAB. Instances where the eavesdropper successfully decoded at least τ data packets were counted and averaged over 10^4 realizations to compute the τ-intercept probability. The simulation environment considers $\mathbb{N} = 10$ relays. Let the pair $(d_{i,\text{D}}, d_{i,\text{E}})$ specify the distance of node i from the destination D and the eavesdropper E, for $i = 1, \ldots, 10$. The distance pairs in the simulation environment have been configured as follows: $(2, 2.3)$, $(3, 2)$, $(4, 6)$, $(3, 4)$, $(4, 5)$, $(1, 2)$, $(1, 2.1)$, $(1.3, 1.5)$, $(1.2, 1.9)$ and $(6, 6)$. In the case of optimal selection with preset jammer, we have configured the node with distance pair $(6, 6)$ to always act as a jammer. This node is equidistant from the destination and the eavesdropper, hence it causes the same levels of interference, on average, to both receivers. Pre-selection of this jammer yields a particular trade-off between secrecy performance and reliability but other schemes that trade reliability for secrecy are also available, e.g., [92, 132]. In all cases, the path loss exponents have been set to $\alpha_{i,j} = \alpha = 3$. Unless otherwise stated, the transmission scheme is uncoded BPSK, which is characterized by the SNR threshold $\rho_{\text{th}} = 5.89$ dB. As explained in Section 4.2.2, the



(A) Comparison of CS and OS

(B) Comparison of CSWJ and OSWJ

Figure 4.5: Comparison between simulation and theoretical results, and secrecy-reliability performance of the considered protocols for different values of m, when $q = 2$ and $\tau/m = 0.6$.

outage probability depends on the relay selection protocol and the transmission scheme but not on the RLNC parameters. The lowest number of transmitted coded packets, for which the destination can decode the entire message with 90% probability or greater, has been used in the measurement of the intercept probability. Equivalently, the theoretical value of $P_{\text{int}}(\tau, n)$ has been calculated from (4.63) for the smallest value of n that yields $F_{\text{D}}(n) \geq 0.90$. For simplicity, we assume that all nodes, including the jammer, transmit the same power, i.e. $\varrho_i = \varrho$. The term 'SNR' is used to refer to the ratio ϱ/N_0, as defined in Section 4.2.1. The four relay selection protocols, namely conventional selection, optimal selection, conventional selection with jammer and optimal selection with preset jammer, have been abbreviated to 'CS', 'OS', 'CSWJ' and 'OSWJ', respectively.

Fig. 4.5 demonstrates the agreement between simulation and analytical results, which confirms the correctness of our derivations. It also illustrates the effect of the transmitted SNR on the outage probability at the destination and compares the intercept probability of the four considered protocols. As expected, the CS scheme outperforms

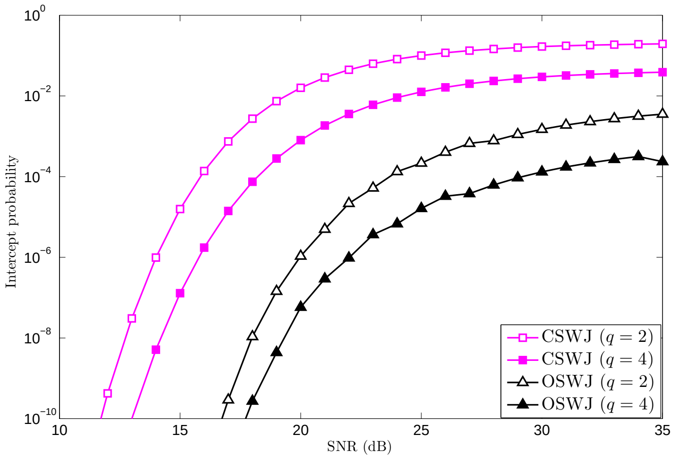


FIGURE 4.6: Effect of the field size q on the secrecy performance of both CSWJ and OSWJ, as a function of the SNR, when $\tau = 8$ and $m = 15$.

the other protocols in terms of reliable communication because it achieves the lowest outage probability. By contract, the CS protocol exhibits the worst performance in terms of secrecy. This is due to the fact that the CS protocol only considers the quality of relay-to-destination channels but does not take into account the relay-to-eavesdropper channels. For this reason, the OS and CSWJ protocols offer better secrecy performance than CS at the expense of reduced reliability. It can be noticed that the secrecy performance of both the CS and OS protocols deteriorates markedly at high SNR values because the intercept probability converges to one. On the other hand, the secrecy performance of the CSWJ and OSWJ protocols reveals that a jammer introduces a 'ceiling' to the intercept probability and, thus, a level of secrecy can be offered even at high SNR values. Fig. 4.5 also demonstrates that the secrecy-reliability tradeoff can be further improved if the message to be transmitted is segmented into a larger number of shorter data packets, that is, the value of m in RLNC is increased.

Fig. 4.6 investigates the effect that the field size q in RLNC has on the probability that the eavesdropper will reconstruct at least $\tau = 8$ data packets from the intercepted coded packets, for different SNR values, when $m = 15$ and either CSWJ or OSWJ is used. The figure shows that when the field size increases from $q = 2$ to $q = 4$, the intercept probability decreases notably. This is due to the fact that the larger the finite field is, the higher the probability of the received coded packets being linearly independent is. Consequently, if $q = 4$, the destination is required to collect fewer coded packets in order to reconstruct the entire message than if $q = 2$. On the other hand, if the finite field is large and the rank of the decoding matrix is smaller than m, the probability of partially reconstructing the transmitted message reduces significantly. For this reason, the fewer the linearly independent coded packets intercepted by the eavesdropper are, the smaller the probability of the eavesdropper decoding even a fraction of the message is. Fig. 4.5 and Fig. 4.6 reveal the impact of the number of data packets m and the field size q on

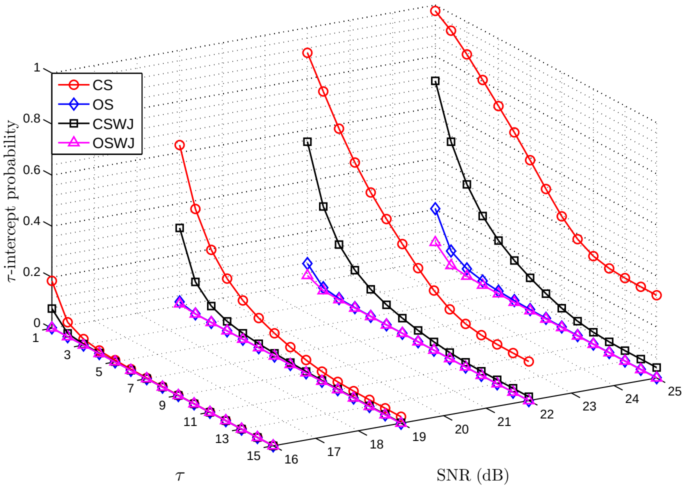


FIGURE 4.7: Performance comparison in terms of the amount of decoded data and the SNR value, for $q = 2$ and $m = 15$.

both reliability and security. Although the intercept probability decreases if the message is segmented into a larger number of data packets or if a larger field size is used, the values of m and q cannot increase unboundedly in practice. An increase in m or q also increases the overhead of RLNC and the decoding complexity of Gaussian elimination. Upper bounds for m and q due to practical limitations are discussed in [28].

Fig. 4.7 compares the τ-intercept probability offered by the considered protocols for all possible values of τ and different transmitted SNR values, when $q = 2$ and $m = 15$. At low SNR values, the probability of decoding data packets from intercepted coded packets is very small, regardless of the adopted protocol. For example, even when the CS protocol is employed, the probability of the eavesdropper decoding at least one data packet ($\tau = 1$) is 0.18 at SNR = 16 dB. However, for high SNR values, the CS scheme clearly yields the worst performance. For example, the performance curve of the CS protocol shows that even though the probability of decoding the entire data message ($\tau = 15$) is low, the eavesdropper can still decode a large portion of data with high probability. The other three protocols provide better performance even for $\tau = 1$.

Fig. 4.8 compares the delay performance of each protocol, in terms of the maximum permitted number of coded packet transmissions required by the destination to decode the entire data message. This delay metric also reflects the reliability of the network. The impact of the field size q on the secrecy-reliability tradeoff is depicted in this figure too. Both CS and CSWJ exhibit fixed and similar delay performance in the high SNR regime, even though CS offers higher link reliability than CSWJ, as established in Fig. 4.5. For $q = 64$, both CS and CSWJ achieve the minimum delay performance, i.e. $n = 15$. The worst-case delay is experienced when RLNC over fields of size $q = 2$ is combined with

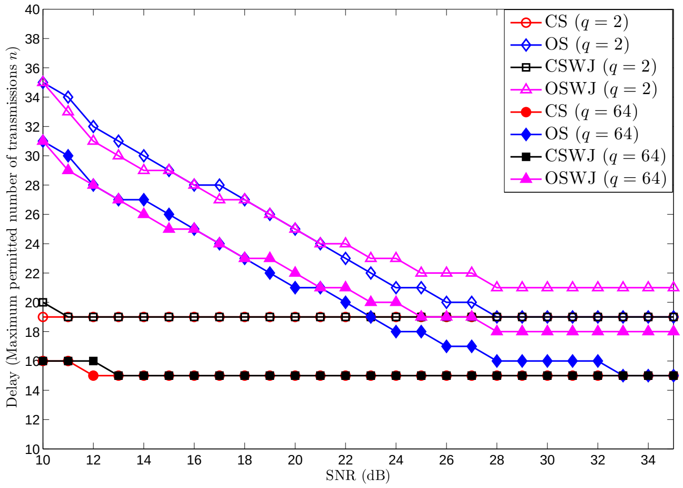


Figure 4.8: Delay performance as a function of SNR for $q = 2$ and $q = 64$, when $m = 15$ is considered.

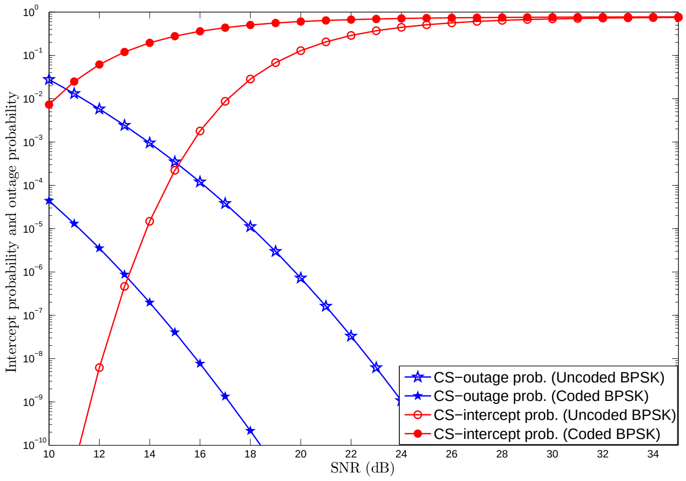


Figure 4.9: Secrecy-reliability trade-off as a function of the SNR for two different transmission schemes, $m = 15$, $q = 2$ and $\tau = 8$.

either OS or OSWJ. The delay of OS and OSWJ is reduced if the field size is increased to $q = 64$ and approaches the delay of CS and CSWJ for an increasing SNR value.

Fig. 4.9 focuses on the CS scheme and further investigates the reliability versus secrecy trade-off between uncoded BPSK and coded BPSK. The SNR threshold for coded BPSK, which employs convolutional coding, is set to $\rho_{\text{th}} = -0.983$ dB, as mentioned in Section 4.2.2. As expected, coded BPSK achieves a lower outage probability than uncoded BPSK at the expense of a notably higher intercept probability. This is due to the fact that the information redundancy introduced by convolutional coding assists not only the destination but also the eavesdropper in the error-free reception of coded packets and the decoding of at least τ data packets. Our proposed framework can thus be used to identify modulation and coding schemes that offer a required balance between security and reliability.

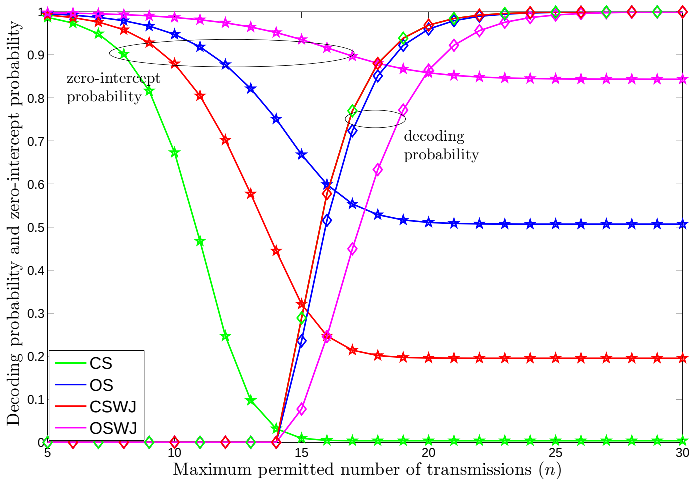


FIGURE 4.10: Performance comparison based on the decoding probability and the zero-intercept probability at SNR=30 dB, for $m = 15$ and $q = 2$.

For each point depicted in the previous figures, the maximum permitted number of transmitted coded packets n has been computed so that the probability of the destination decoding the entire message is at least 90%, i.e., $F_{\rm D}(n) \geq 0.9$. In contrast, Fig. 4.10 investigates the impact of n on both the decoding probability at the destination $F_{\rm D}(n)$ and the probability that the eavesdropper will be unable to decode any data packets. The latter probability is referred to as the *zero-intercept probability* and is given by $1 - P_{\rm int}(1, n)$. As expected, an increase in coded packet transmissions improves the decoding probability at the destination and decreases the zero-intercept probability. The benefit from using a feedback link to notify the control unit to cease the transmission of coded packets when the destination has decoded the entire message, can also be observed in Fig. 4.10. For a high value of n, the destination is more likely to decode the message when fewer than n coded packets have been transmitted. As a result, the transmission process will be terminated earlier than anticipated and the eavesdropper will be unable to collect more coded packets. For this reason, the zero-intercept probability gradually converges to a fixed value for an increasing value of n. We note that the CS protocol yields the highest decoding probability but provides no guarantees that the eavesdropper will decode no data packets. The selection of a jammer that causes the least interference to the transmitting relay gives CSWJ a security advantage over CS without a compromise on the decoding probability. Exploitation of the eavesdropper's CSI can further increase the zero-intercept probability and boost security, even when a jammer is not employed, as demonstrated by the OS protocol. On the other hand, OSWJ yields the highest zero-intercept probability at the expense of a lower decoding probability than the other protocols. The results reaffirm that the security advantage gained by opting for a protocol other than CS clearly outweighs the loss in reliability, when SNR = 30 dB.

4.3 Summary

The main contributions made in this chapter can be summarized as follows:

- In Section 4.1, we derived accurate expressions for the intercept probability of a network, where a transmitter uses random linear network coding to broadcast information. Both unaided transmission and feedback-aided transmission were investigated and the secrecy gain achieved by the latter approach was computed. Moreover, we presented a resource allocation model to minimize the intercept probability, while satisfying delay and reliability constraints, and showed that the legitimate receiver is not required to have knowledge of the presence of an eavesdropper.

- In Secction 4.2, we proposed a cross-layer security scheme, which combines the inherent secrecy features of RLNC at the application layer with physical-layer security mechanisms, based on relay selection with or without jamming. We derived analytical expressions of the outage probability at the destination and the eavesdropper. We introduced a novel secrecy metric, which is referred to as the $\tau-$intercept probability and is defined as the probability that a proportion of the transmitted information will be compromised. An exact expression of the τ-intercept probability is derived for systems that impose a deadline on coded packet transmissions but provide the destination with a feedback link, which can be used to terminate the transmission process before the deadline expires. Furthermore, we investigated the secrecy-reliability trade-offs of the considered RLNC-enabled relay selection protocols.

Chapter 5

Conclusions and Future Research Directions

In Chapters 2 to 4, we have studied several performance aspects of RLNC. In this chapter, we present general conclusions drawn from each chapter of this thesis. More detailed technical contributions can be found at the end of each chapter and are not repeated here. Finally, we also exhibit some possible future directions emerging from this work.

5.1 Summary and Conclusions of the Thesis

In Chapter 2, closed form analytical expressions have been derived to evaluate and characterize the performance of non-overlapping, expanding and sliding generations RLNC schemes. These schemes support point-to-point and point-to-multipoint communications, and are practically useful to exploit the sparsity and prioritization features of RLNC in order to provide unequal error protection and reduced decoding complexity. Moreover, the design parameters of these schemes allow to adjust the desired decoding performance. For instance, the derived expressions for RLNC using sliding generations that can overlap by up to 50% demonstrated that a low amount of overlap between generations in practical settings can yield a similar decoding probability to that of the more computationally expensive RLNC based on expanding generations. We note that if the system parameters impose an overlap bigger than 50% between generations, (e.g., when the field size is small, the number of source packets is high and the channel conditions are poor) the expressions of the decoding probability of expanding-generations RLNC and sliding-generations RLNC can be used as upper and lower bounds, respectively.

In Chapter 3, we primarily focused on the development of mathematical frameworks to evaluate and characterise the performance of RLNCC. In this respect, we first formulated the performance of single relay networks combining intra-session and inter-session RLNC. It has been shown that, depending on the channel qualities, systematic RLNC can provide equivalent or better decoding performance than non-systematic RLNC. Secondly, theoretical closed form expressions were derived to evaluate the performance of RLNC in multi-source multi-relay networks. We exhibited that the proposed framework can be employed to characterize the performance of opportunistic as well as sparse RLNC. Finally, we have proposed the use of RLNCC combined with NOMA for uplink multi-source multi-relay networks. In this work, we have demonstrated the gains in terms of decoding probability, diversity and throughput performance in comparison to conventional OMA based RLNCC.

In Chapter 4, we presented RLNC as a self encryption technique for secure communications. In this respect, we have formulated and characterized the inherent secrecy feature of RLNC, and demonstrated the importance of feedback based controlled transmissions and the finite field effect on network security. Moreover, we proposed a framework that combines RLNC at the application layer and physical-layer security in the form of relay selection with or without cooperative jamming. Four relay selection protocols were considered and analytical expressions of the outage probability at the intended destination and the eavesdropper were derived. In order to quantify the amount of information leakage to the eavesdropper, a novel metric called τ-intercept probability was proposed. This metric, which utilizes the outage probabilities associated to each relay selection protocol, characterizes the security that is jointly offered by the application and physical layers. Our analysis demonstrated that relay selection based on both the eavesdropper's CSI and the destination's CSI achieves a good balance between security and reliability, when a jammer is not employed. If a jammer is used, reliability can be traded for security. On the other hand, if the eavesdropper's CSI is not available, the selection of a relay and a jammer based solely on the destination's CSI favors reliability, while still providing some secrecy guarantees. We also noted that the field size over which RLNC is performed at the application layer as well as the adopted modulation and coding scheme at the physical layer can be modified to fine-tune the trade-off between security and reliability.

5.2 Future Directions

The following are proposed research directions that could be investigated as an extension to the research presented in this thesis.

- **Distributed Memory management and heterogeneous IoT devises**: The analysis and the work presented in Chapter 2 could be extended to design distributed storage schemes, and communication schemes to support heterogeneous IoT devices with different computation power.

- **Energy harvesting and software defined network environment**: The research work presented in Chapter 3 could be extended to design NOMA-RLNCC based energy harvesting techniques for green content delivery. Moreover, the advantages of RLNCC could be exploited in software defined network environment for data managements and low power receivers of limited computational capabilities.

- **Joint user pairing and RLNCC**: The research work presented in Chapter 4 can be extended by designing a joint user pairing and RLNCC scheme for improving the security and reliability performance of NOMA based communications.

Appendix A

Analytical proof of Lemma 2.1

The objective of this Appendix is to analytically prove that

$$\sum_{r_1} \gamma_{r_1}(n_1, m)\, \gamma(n_2, m{-}r_1) q^{n_2 r_1} = \gamma(n_1 + n_2,\, m) \tag{A.1}$$

for $\max(0, m-n_2) \leq r_1 \leq \min(n_1, m)$, and thus show that (2.1) and (2.7) are equivalent expressions. If we both divide and multiply the left-hand side of (A.1) by $\gamma(m, m)$ and use (2.3) and (2.5) to expand $\gamma_{r_1}(n_1, m)$ and $\gamma(n_2, m - r_1)$, respectively, we obtain

$$\sum_{r_1} \gamma_{r_1}(n_1, m)\gamma(n_2, m - r_1)q^{n_2 r_1} = \gamma(m, m) \sum_{r_1} \begin{bmatrix} n_1 \\ r_1 \end{bmatrix}_q \begin{bmatrix} n_2 \\ m - r_1 \end{bmatrix}_q \frac{\gamma(m, r_1)\, \gamma(m{-}r_1, m{-}r_1)}{\gamma(m, m)} q^{n_2 r_1}. \tag{A.2}$$

Expression (2.1) can be used to compute the ratio of the γ functions in the sum of (C.1) as follows

$$\frac{\gamma(m, r_1)\, \gamma(m{-}r_1, m{-}r_1)}{\gamma(m, m)} = \frac{\prod_{i=0}^{m-r_1-1}(q^{m-r_1} - q^i)}{\prod_{i=r_1}^{m-1}(q^m - q^i)} = q^{-r_1(m-r_1)}. \tag{A.3}$$

If we substitute (C.2) into (C.1) and invoke the following identity

$$\sum_{r_1} \begin{bmatrix} n_1 \\ r_1 \end{bmatrix}_q \begin{bmatrix} n_2 \\ m - r_1 \end{bmatrix}_q q^{r_1(n_2 - m + r_1)} = \begin{bmatrix} n_1 + n_2 \\ m \end{bmatrix}_q \tag{A.4}$$

which is known as the q-*Vandermonde identity*, expression (C.1) reduces to

$$\sum_{r_1} \gamma_{r_1}(n_1, m)\gamma(n_2, m - r_1)q^{n_2 r_1} = \gamma(m, m) \begin{bmatrix} n_1{+}n_2 \\ m \end{bmatrix}_q. \tag{A.5}$$

The right-hand side of (C.3) is equal to $\gamma(n_1{+}n_2, m)$ as per (2.5), which completes the proof.

Appendix B

Reformulation of the intercept probability of FT

Based on the definition of the PMF in (4.2), the expression for $P_{\mathrm{BE}}(n)$ in (4.4) can be expanded as follows:

$$\begin{aligned} P_{\mathrm{BE}}(n) = {} & F_{\mathrm{B}}(m)F_{\mathrm{E}}(m) - F_{\mathrm{B}}(m)F_{\mathrm{E}}(m+1) + F_{\mathrm{B}}(m+1)F_{\mathrm{E}}(m+1) \\ & - F_{\mathrm{B}}(n-1)F_{\mathrm{E}}(n) + F_{\mathrm{B}}(n)F_{\mathrm{E}}(n). \end{aligned}$$

If we create pairs from each two consecutive terms, with the exception of the last term, and invoke again the definition of the PMF, we obtain

$$P_{\mathrm{BE}}(n) = \left[- \sum_{n_{\mathrm{T}}=m+1}^{n} f_{\mathrm{E}}(n_{\mathrm{T}})\, F_{\mathrm{B}}(n_{\mathrm{T}}-1) \right] + F_{\mathrm{B}}(n)F_{\mathrm{E}}(n).$$

In (4.5), we established that $P_{\mathrm{E}}(n) = F_{\mathrm{E}}(n) - F_{\mathrm{B}}(n)F_{\mathrm{E}}(n)$. Using (4.3), the intercept probability of FT can be expressed as:

$$P_{\mathrm{int}}^{\mathrm{FT}}(n) = F_{\mathrm{E}}(n) - \sum_{n_{\mathrm{T}}=m+1}^{n} f_{\mathrm{E}}(n_{\mathrm{T}})\, F_{\mathrm{B}}(n_{\mathrm{T}}-1). \tag{B.1}$$

Appendix C

Proof of Proposition 4.2 for the case of FT

In order to prove Proposition 4.2 for the FT mode, it suffices to set $\Delta = P_{\text{int}}(n_2) - P_{\text{int}}(n_1)$ and show that $\Delta \geq 0$ for all $n_2 \geq n_1$. Using (B.1), we find that

$$\Delta = F_{\text{E}}(n_2) - F_{\text{E}}(n_1) - \sum_{n_{\text{T}}=n_1+1}^{n_2} f_{\text{E}}(n_{\text{T}})\, F_{\text{B}}(n_{\text{T}} - 1). \tag{C.1}$$

Terms $-F_{\text{E}}(i)$ and $F_{\text{E}}(i)$ for $i = n_1 + 1, \ldots, n_2 - 1$, which cancel each other out, are added to $F_{\text{E}}(n_2) - F_{\text{E}}(n_1)$ and give

$$\begin{aligned} F_{\text{E}}(n_2) - F_{\text{E}}(n_1) &= (F_{\text{E}}(n_2) - F_{\text{E}}(n_2 - 1)) + \ldots \\ &\quad \ldots + (F_{\text{E}}(n_1 + 1) - F_{\text{E}}(n_1)) \\ &= \sum_{n_{\text{T}}=n_1+1}^{n_2} f_{\text{E}}(n_{\text{T}}). \end{aligned} \tag{C.2}$$

If we substitute (C.2) into (C.1), we obtain

$$\Delta = \sum_{n_{\text{T}}=n_1+1}^{n_2} f_{\text{E}}(n_{\text{T}}) \big[1 - F_{\text{B}}(n_{\text{T}} - 1)\big]$$

which is a sum of non-negative terms and is, thus, $\Delta \geq 0$.

Bibliography

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[2] E. Ahmed, A. Eryilmaz, M. Medard, and A. E. Ozdaglar, "On the scaling law of network coding gains in wireless networks," in *Proc. IEEE Military Communications Conference*, Orlando, FL, USA, Oct. 2007.

[3] J. sang Park, M. Gerla, D. S. Lun, Y. yi, and M. Medard, "Codecast: a network-coding-based ad hoc multicast protocol," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 76–81, Oct. 2006.

[4] M. Ghaderi, D. Towsley, and J. Kurose, "Reliability gain of network coding in lossy wireless networks," in *Proc. IEEE Conference on Computer Communications (INFOCOM)*, Phoenix, AZ, USA, Apr. 2008.

[5] J. Zhang, P. Fan, and K. B. Letaief, "Network coding for efficient multicast routing in wireless ad-hoc networks," *IEEE Trans. Commun.*, vol. 56, no. 4, pp. 598–607, Apr. 2008.

[6] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[7] Y. Chen, S. Kishore, and J. Li, "Wireless diversity through network coding," in *IEEE Wireless Communications and Networking Conference*, Las Vegas, USA, Apr. 2006.

[8] R. Bassoli, H. Marques, J. Rodriguez, K. W. Shum, and R. Tafazolli, "Network coding theory: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 1950–1978, Fourth Quarter 2013.

[9] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Energy efficient reliable multi-path routing using network coding for sensor network," *Int. Journal of Comp. Science and Net. Sec.*, vol. 8, no. 12, pp. 329–338, Dec. 2008.

[10] X. Wang, Y. Xu, and Z. Feng, “Physical-layer network coding in OFDM system: Analysis and performance,” in *International Conference on Communications and Networking*, Kunming, China, Aug. 2012.

[11] S. T. Başaran, G. K. Kurt, M. Uysal, and İ. Altunbaş, “A tutorial on network coded cooperation,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2970–2990, Fourthquarter 2016.

[12] S. Gökceli, H. Alakoca, S. T. Başaran, and G. K. Kurt, “OFDMA-based network-coded cooperation: design and implementation using software-defined radio nodes,” *EURASIP Journal on Advances in Signal Processing*, vol. 2016, no. 1, p. 8, Jan. 2016.

[13] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, “On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users,” *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.

[14] S. Timotheou and I. Krikidis, “Fairness for non-orthogonal multiple access in 5G systems,” *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1647–1651, Oct. 2015.

[15] X. Li, C. Li, and Y. Jin, “Dynamic resource allocation for transmit power minimization in OFDM-based NOMA systems,” *IEEE Commun. Lett.*, vol. 20, no. 12, pp. 2558–2561, Dec. 2016.

[16] P. Parida and S. S. Das, “Power allocation in OFDM based NOMA systems: A DC programming approach,” in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Texas, USA, Dec. 2014.

[17] S. Park and D.-H. Cho, “Random linear network coding based on non-orthogonal multiple access in wireless networks,” *IEEE Commun. Lett.*, vol. 19, no. 7, pp. 1273–1276, Jul. 2015.

[18] H. Seferoglu, A. Markopoulou, and K. K. Ramakrishnan, “I^{2}NC: Intra- and inter-session network coding for unicast flows in wireless networks,” in *Proc. IEEE Conference on Computer Communications (INFOCOM)*, Shanghai, China, Apr. 2011.

[19] W. Chen, K. B. Letaief, and Z. Cao, “Opportunistic network coding for wireless networks,” in *Proc. IEEE Intern. Conf. on Commun. (ICC)*, Glasgow, UK, Jun. 2007.

[20] H. Seferoglu and A. Markopoulou, “Opportunistic network coding for video streaming over wireless,” in *Packet Video.* Lausanne, Switzerland: IEEE, Nov. 2007.

[21] M. Wang and B. Li, "Lava: A reality check of network coding in peer-to-peer live streaming," in *IEEE International Conference on Computer Communications (INFOCOM)*, Barcelona, Spain, May 2007.

[22] J. M. Walsh and S. Weber, "A concatenated network coding scheme for multimedia transmission," in *Network Coding, Theory and Applications (NetCod)*, Hong Kong, China, Jan. 2008.

[23] M. Wang and B. Li, "Network coding in live peer-to-peer streaming," *IEEE Transactions on Multimedia*, vol. 9, no. 8, pp. 1554–1567, 2007.

[24] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: Physical-layer network coding," in *International conference on Mobile computing and networking (MobiCom)*, Los Angeles, California, Sep. 2006.

[25] S. C. Liew, S. Zhang, and L. Lu, "Physical-layer network coding: Tutorial, survey, and beyond," *Physical Communication*, vol. 6, pp. 4–42, 2013.

[26] S. Deb, M. Effros, T. Ho, D. R. Karger, R. Koetter, D. S. Lun, M. Médard, and N. Ratnakar, "Network coding for wireless applications: A brief tutorial," in *Proc. Int. Workshop on Wireless Ad Hoc Networks*, London, UK, May 2005.

[27] D. Szabo, A. Gulyas, F. H. P. Fitzek, and D. E. Lucani, "Towards the tactile internet: Decreasing communication latency with network coding and software defined networking," in *Proc. European Wireless Conf.*, Budapest, Hungary, May 2015.

[28] J. Heide, M. V. Pedersen, F. H. Fitzek, and M. Médard, "On code parameters and coding vector representation for practical RLNC," in *Proc. IEEE Intern. Conf. on Commun. (ICC)*, Kyoto, Japan, Jun. 2011.

[29] C. W. Sørensen, D. E. Lucani, F. H. P. Fitzek, and M. Médard, "On-the-fly overlapping of sparse generations: A tunable sparse network coding perspective," in *Proc. IEEE Veh. Tech. Conf. (VTC Fall)*, Vancouver, BC, Sep. 2014.

[30] P. Maymounkov, N. J. A. Harvey, and D. S. Lun, "Methods for efficient network coding," in *Proc. Allerton Conf. on Commun., Control and Comp*, Monticello, IL, USA, Sep. 2006.

[31] D. Vukobratović and V. Stanković, "Unequal error protection random linear coding strategies for erasure channels," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1243–1252, May 2012.

[32] Y. Li, E. Soljanin, and P. Spasojević, “Effects of the generation size and overlap on throughput and complexity in randomized linear network coding,” *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1111–1123, Feb. 2011.

[33] A. Heidarzadeh and A. H. Banihashemi, “Overlapped chunked network coding,” in *Proc. IEEE Inform. Theory Workshop (ITW)*, Cairo, Egypt, Jan. 2010.

[34] M. C. Bogino, P. Cataldi, M. Grangetto, E. Magli, and G. Olmo, “Sliding-window digital fountain codes for streaming of multimedia contents,” in *Proc. IEEE Int. Symp. on Circ. and Systems (ISCAS)*, New Orleans, LA, May 2007.

[35] Y. Lin, B. Liang, and B. Li, “SlideOR: Online opportunistic network coding in wireless mesh networks,” in *Proc. IEEE Conference on Computer Communications (INFOCOM)*, San Diego, CA, Mar. 2010.

[36] D. J. C. MacKay, “Fountain codes,” *IEE Proc.-Communications*, vol. 152, no. 6, pp. 1062–1068, Dec. 2005.

[37] S. Feizi, D. E. Lucani, and M. Médard, “Tunable sparse network coding,” in *Proc. Int. Zurich Seminar on Commun. (IZS)*, Zurich, Switzerland, Feb. 2012.

[38] X. Chu, K. Zhao, and M. Wang, “Practical random linear network coding on GPUs,” *NETWORKING*, pp. 573–585, 2009.

[39] F. H. Fitzek, M. V. Pedersen, J. Heide, and M. Médard, “Network coding: applications and implementations on mobile devices,” in *Proc. ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, 2010, pp. 83–87.

[40] G. Angelopoulos, A. Paidimarri, A. P. Chandrakasan, and M. Médard, “Experimental study of the interplay of channel and network coding in low power sensor applications,” in *Proc. IEEE Intern. Conf. on Commun. (ICC)*, Budapest, Hungary, Jun. 2013.

[41] C. Khirallah, D. Vukobratovic, and J. Thompson, “Performance analysis and energy efficiency of random network coding in lte-advanced,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4275–4285, Dec. 2012.

[42] K. Nguyen, T. Nguyen, and S.-C. Cheung, “Video streaming with network coding,” *Journal of Signal Processing Systems*, vol. 59, no. 3, pp. 319–333, 2010.

[43] A. Tassi, I. Chatzigeorgiou, and D. Vukobratović, “Resource-allocation frameworks for network-coded layered multimedia multicast services,” *IEEE J. Sel. Areas Commun.*, vol. 33, no. 2, pp. 141–155, Feb. 2015.

[44] M. Esmaeilzadeh, P. Sadeghi, and N. Aboutorab, "Random linear network coding for wireless layered video broadcast: General design methods for adaptive feedback-free transmission," *IEEE Trans. Commun.*, pp. 790–805, Feb. 2017.

[45] N. J. H. Marcano, J. Heide, D. E. Lucani, and F. H. P. Fitzek, "On the overhead of telescopic codes in network coded cooperation," in *Proc. IEEE Vehicular Technology Conference (VTC)*, Boston, USA, Sep. 2015.

[46] C. Gkantsidis and P. R. Rodriguez, "Network coding for large scale content distribution," in *Proc. Joint Conference of the IEEE Computer and Communications Societies.*, Miami, FL, USA, Mar. 2005.

[47] C. Fragouli and A. Markopoulou, "A network coding approach to overlay network monitoring," in *Proc. Allerton Conf. on Commun., Control and Comp*, Illinois, USA, Sep. 2005.

[48] T. Ho, B. Leong, Y.-H. Chang, Y. Wen, and R. Koetter, "Network monitoring in multicast networks using network coding," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Adelaide, Australia, Sep. 2005.

[49] W. Guo, X. Shi, N. Cai, and M. Médard, "Localized dimension growth: a convolutional random network coding approach to managing memory and decoding delay," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3894–3905, 2013.

[50] S. Moriam, Y. Yan, E. Fischer, E. Franz, and G. P. Fettweis, "Resilient and efficient communication in many-core systems using network coding," in *Proc. International Performance Computing and Communications Conference (IPCCC)*, California, USA, Dec. 2015.

[51] D. Platz, D. H. Woldegebreal, and H. Karl, "Random network coding in wireless sensor networks: Energy efficiency via cross-layer approach," in *Proc. International Symposium on Spread Spectrum Techniques and Applications*, Bologna, Italy, Aug. 2008.

[52] L. Sun, P. Ren, Q. Du, and Y. Wang, "Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 291–300, Feb. 2016.

[53] Y. Lin, B. Liang, and B. Li, "Priority random linear codes in distributed storage systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1653–1667, Nov. 2009.

[54] N. Thomos, E. Kurdoglu, P. Frossard, and M. van der Schaar, "Adaptive prioritized random linear coding and scheduling for layered data delivery from multiple servers," *IEEE Trans. Multimedia*, vol. 17, no. 6, pp. 893–906, Jun. 2015.

[55] A. S. Lalos, A. Antonopoulos, E. Kartsakli, M. Di Renzo, S. Tennina, L. Alonso, and C. Verikoukis, "RLNC-aided cooperative compressed sensing for energy efficient vital signal telemonitoring," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3685–3699, 2015.

[56] A. Nasri, R. Schober, and M. Uysal, "Performance and optimization of network-coded cooperative diversity systems," *IEEE Trans. Commun.*, vol. 61, no. 3, pp. 1111–1122, 2013.

[57] T. Lv, S. Li, and W. Geng, "Combining cooperative diversity and network coding in uplink multi-source multi-relay networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, p. 241, Dec. 2013.

[58] H. Topakkaya and Z. Wang, "Wireless network code design and performance analysis using diversity-multiplexing tradeoff," *IEEE Trans. Commun.*, vol. 59, no. 2, pp. 488–496, Feb. 2011.

[59] J.-T. Seong, "Bounds on decoding failure probability in linear network coding schemes with erasure channels," *IEEE Commun. Lett.*, vol. 18, no. 4, pp. 648–651, Apr. 2014.

[60] J.-T. Seong and H.-N. Lee, "Predicting the performance of cooperative wireless networking schemes with random network coding," *IEEE Trans. Commun.*, vol. 62, no. 8, pp. 2951–2964, Aug. 2014.

[61] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, Lausanne, Switzerland, Jun. 2002.

[62] X. Wang, W. Guo, Y. Yang, and B. Wang, "A secure broadcasting scheme with network coding," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1435–1438, Jul. 2013.

[63] M. Adeli and H. Liu, "On the inherent security of linear network coding," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1668–1671, Aug. 2013.

[64] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting fountain codes for secure wireless delivery," *IEEE Commun. Lett.*, vol. 18, no. 5, pp. 777–780, May 2014.

[65] V. Ç. Güngör and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[66] W. Jiang, T. Kaiser, and A. J. H. Vinck, "A robust opportunistic relaying strategy for co-operative wireless communications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2642–2655, Apr. 2016.

[67] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 659–672, Mar. 2006.

[68] J. Luo, J. Hu, D. Wu, and R. Li, "Opportunistic routing algorithm for relay node selection in wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 11, no. 1, pp. 112–121, Feb. 2015.

[69] R. Madan, N. B. Mehta, A. F. Molisch, and J. Zhang, "Energy-efficient cooperative relaying over fading channels with simple relay selection," *IEEE Trans. Wireless Commun.*, vol. 7, no. 8, pp. 3013–3025, Aug. 2008.

[70] J. Niu, L. Cheng, Y. Gu, L. Shu, and S. K. Das, "R3E: Reliable reactive routing enhancement for wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 784–794, Feb. 2014.

[71] Z. Iqbal, K. Kim, and H. N. Lee, "A cooperative wireless sensor network for indoor industrial monitoring," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 482–491, Apr. 2017.

[72] N. Marchenko, T. Andre, G. Brandner, W. Masood, and C. Bettstetter, "An experimental study of selective cooperative relaying in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 3, pp. 1806–1816, Aug. 2014.

[73] Q. F. Zhou, Y. Li, F. C. Lau, and B. Vucetic, "Decode-and-forward two-way relaying with network coding and opportunistic relay selection," *IEEE Trans. Commun.*, vol. 58, no. 11, pp. 3070–3076, Nov. 2010.

[74] X. D. Jia, L. X. Yang, H. Y. Fu, B. M. Feng, and Y. F. Qi, "Two-way denoise-and-forward network coding opportunistic relaying with jointing adaptive modulation relay selection criterions," *IET Communications*, vol. 6, no. 2, pp. 194–202, Jan. 2012.

[75] Q. You, Y. Li, and Z. Chen, "Joint relay selection and network coding for error-prone two-way decode-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3420–3433, Oct. 2014.

[76] R. Liu and W. Trappe, *Securing wireless communications at the physical layer*. New york, USA: Springer, 2010, vol. 7.

[77] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE wireless Communications*, vol. 18, no. 2, Apr. 2011.

[78] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relay,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Dec. 2010.

[79] I. Csiszár and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[80] A. D. Wyner, “The wire-tap channel,” *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[81] S. Leung-Yan-Cheong and M. Hellman, “The gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[82] P. K. Gopala, L. Lai, and H. El Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Sep. 2008.

[83] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, “Coding for secrecy: An overview of error-control coding techniques for physical-layer security,” *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Aug. 2013.

[84] J. Huang and A. L. Swindlehurst, “Cooperative jamming for secure communications in MIMO relay networks,” *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, 2011.

[85] I. Krikidis, “Opportunistic relay selection for cooperative networks with secrecy constraints,” *IET Communications*, vol. 4, no. 15, pp. 1787–1791, Oct. 2010.

[86] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, “Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[87] J. Zhu, Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, “Security-reliability tradeoff analysis of multirelay-aided decode-and-forward cooperation systems,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5825–5831, Jul. 2016.

[88] E. Tekin and A. Yener, “The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, May 2008.

[89] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, “Improving physical layer secrecy using full-duplex jamming receivers,” *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[90] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[91] T.-N. Cho and C.-L. Wang, "An asymptotic secrecy rate analysis of a cooperative jamming strategy for physical-layer security," in *Proc. IEEE Intern. Conf. on Commun. (ICC)*, Budapest, Hungary, Jun. 2013.

[92] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[93] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259–6274, Aug. 2016.

[94] S. Huang, J. Wei, Y. Cao, and C. Liu, "Joint decode-and-forward and cooperative jamming for secure wireless communications," in *Proc. International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, Wuhan, China, Sep. 2011.

[95] J. Wishart, "The generalised product moment distribution in samples from a normal multivariate population," *Biometrika*, vol. 20A, pp. 32–52, Jul. 1928.

[96] A. Yellepeddi, "Applications of random matrix theory in wireless underwater communication or why signal processing and wireless communication need random matrix theory," 2013, MIT paper for course 18.338, unpublished. [Online]. Available: http://web.mit.edu/18.338/www/2013s/projects/ay_report.pdf

[97] A. Edelman and N. R. Rao, "Random matrix theory," *Acta Numerica*, vol. 14, pp. 233–297, Apr. 2005.

[98] F. Mezzadri, "How to generate random matrices from the classical compact groups," *Notices of the AMS*, vol. 54, no. 5, pp. 592–604, May 2007.

[99] R. Lidl and H. Niederreiter, *Finite fields.* Cambridge university press, 1997, vol. 20.

[100] X. Zhao, "Notes on "Exact decoding probability under random linear network coding"," *IEEE Commun. Lett.*, vol. 16, no. 5, pp. 720–721, May 2012.

[101] È. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems of Information Transmission*, vol. 21, no. 1, pp. 1–12, Jan. 1985.

[102] M. Gadouleau and Z. Yan, "Constant-rank codes and their connection to constant-dimension codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3207–3216, Jul. 2010.

[103] V. Kac and P. Cheung, *Quantum Calculus.* New York, NY: Springer-Verlag, 2002.

[104] A. Heidarzadeh, “Design and analysis of random linear network coding schemes: Dense codes, chunked codes and overlapped chunked codes,” Ph.D. dissertation, Carleton University, Ottawa, Canada, 2012.

[105] P. A. Chou, Y. Wu, and K. Jain, “Practical network coding,” in *Proc. Allerton Conf. on Commun., Control and Comp.*, Monticello, IL, Oct. 2003.

[106] C. Greco, I. D. Nemoianu, M. Cagnazzo, and B. Pesquet-Popescu, “Rate-distortion-optimized multi-view streaming in wireless environment using network coding,” *EURASIC J. Adv. Sig. Proc.*, vol. 2011, no. 1, pp. 1–20, Jan. 2016.

[107] P. Cataldi, M. Grangetto, T. Tillo, E. Magli, and G. Olmo, “Sliding-window raptor codes for efficient scalable wireless video broadcasting with unequal loss protection,” *IEEE Trans. Image Process.*, vol. 19, no. 6, pp. 1491–1503, Jun. 2010.

[108] J. K. Sundararajan, D. Shah, M. Médard, S. Jakubczak, M. Mitzenmacher, and J. Barros, “Network coding meets TCP: Theory and implementation,” *Proc. IEEE*, vol. 99, no. 3, pp. 490–512, Mar. 2011.

[109] (2013) The NWCRG website.

[110] S. Sesia, I. Toufik, and M. Baker, *LTE - The UMTS Long Term Evolution: From Theory to Practice.* John Wiley & Sons, 2011.

[111] A. F. Molisch, N. B. Mehta, J. S. Yedidia, and J. Zhang, “Performance of fountain codes in collaborative relay networks,” *IEEE Trans. on Wireless Commun.*, vol. 11, no. 6, pp. 4108–4119, Nov. 2007.

[112] A. Tarable and I. Chatzigeorgiou, “Randomly select and forward: Erasure probability analysis of a probabilistic relay channel model,” in *Proc. IEEE Inform. Theory Workshop (ITW)*, Taormina, Italy, Oct. 2009.

[113] E. Kurniawan, S. Sun, K. Yen, and K. F. E. Chong, “Network coded transmission of fountain codes over cooperative relay networks,” in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, Sydney, Apr. 2010.

[114] X. Bao and J. Li, “Matching code-on-graph with network-on-graph: Adaptive network coding for wireless relay networks,” in *Proc. Allerton Conf. on Commun., Control and Computing*, Monticello, USA, Sep. 2005.

[115] D. H. Woldegebreal and H. Karl, “Multiple-access relay channel with network coding and non-ideal source-relay channels,” in *Proc. Int. Symp. on Wireless Commun. Systems (ISWCS)*, Trondheim, Norway, Oct. 2007.

[116] J. Krigslund, J. Hansen, M. Hundeboll, D. Lucani, and F. Fitzek, "CORE: COPE with MORE in wireless meshed networks," in *Proc. IEEE Vehicular Technology Conference (VTC)*, Jun. 2013.

[117] P. J. S. G. Ferreira, B. Jesus, J. Vieira, and A. J. Pinho, "The rank of random binary matrices and distributed storage applications," *IEEE Commun. Lett.*, vol. 17, no. 1, pp. 151–154, Jan. 2013.

[118] A. L. Jones, I. Chatzigeorgiou, and A. Tassi, "Binary systematic network coding for progressive packet decoding," in *Proc. IEEE Intern. Conf. on Commun. (ICC)*, London, UK (to appear), Jun. 2015.

[119] J. Blömer, R. Karp, and E. Welzl, "The rank of sparse random matrices over finite fields," *Rand. Struct. Alg.*, vol. 10, no. 4, pp. 407–420, Jul. 1997.

[120] C. Cooper, "On the distribution of rank of a random matrix over a finite field," *Rand. Struct. Alg.*, vol. 17, no. 3-4, pp. 197–212, Oct. 2000.

[121] T. Do-Duy and M. A. Vázquez-Castro, "Efficient communication over cellular networks with network coding in emergency scenarios," in *Proc. International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, Rennes, France, Nov. 2015.

[122] Z. Ding, L. Dai, and H. V. Poor, "MIMO-NOMA design for small packet transmission in the internet of things," *IEEE Access*, vol. 4, pp. 1393–1405, Apr. 2016.

[123] Z. Ding, H. Dai, and H. V. Poor, "Relay selection for cooperative NOMA," *IEEE Wireless Communications Letters*, vol. 5, no. 4, pp. 416–419, Jun. 2016.

[124] 3rd Generation Partnership Project (3GPP), "Study on downlink multiuser superposition transmission for LTE," Shanghai, China, Mar. 2015.

[125] X. Wang, W. Chen, and Z. Cao, "SPARC: superposition-aided rateless coding in wireless relay systems," *IEEE Trans. Veh. Technol.*, vol. 60, no. 9, pp. 4427–4438, Nov. 2011.

[126] I. Chatzigeorgiou and A. Tassi, "Decoding delay performance of random linear network coding for broadcast," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, Feb. 2017.

[127] Z. Guan, T. Melodia, and G. Scutari, "To transmit or not to transmit? Distributed queueing games in infrastructureless wireless networks," *IEEE/ACM Trans. Netw.*, vol. 24, pp. 1153–1166, Apr 2016.

[128] K. R. Liu, *Cooperative communications and networking.* Cambridge University Press, 2009.

[129] K. B. Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," *Proc. IEEE*, vol. 97, no. 5, pp. 878–893, May 2009.

[130] K. Wang, L. Yuan, T. Miyazaki, D. Zeng, S. Guo, and Y. Sun, "Strategic anti-eavesdropping game for physical layer security in wireless cooperative networks," *IEEE Trans. Veh. Commun.*, vol. 66, pp. 9448–9457, May 2017.

[131] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Commun. Lett.*, vol. 6, no. 2, pp. 174–177, Apr. 2017.

[132] D. H. Ibrahim, E. S. Hassan, and S. A. El-Doli, "Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks," *Computers & Security*, vol. 50, pp. 47–59, May 2015.

[133] L. G. Krasny and K. C. Zangi, "Feedback of channel state information using the digital reverse link," in *IEEE Intern. Conf. on Commun. (ICC)*, Paris, France, 2004.

[134] D. Samardzija and N. Mandayam, "Unquantized and uncoded channel state information feedback in multiple-antenna multiuser systems," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1335–1345, Jul. 2006.

[135] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[136] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoustics, Speech and Sign. Proc. (ICASSP)*, Kyoto, Japan, Mar. 2012.

[137] I. Chatzigeorgiou, I. J. Wassell, and R. Carrasco, "On the frame error rate of transmission schemes on quasi-static fading channels," in *Proc. Conf. on Inform. Sciences and Systems (CISS)*, Princeton, USA, Mar. 2008.

[138] Y. Xi, A. Burr, J. Wei, and D. Grace, "A general upper bound to evaluate packet error rate over quasi-static fading channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 5, pp. 1373–1377, May 2011.

[139] T. Liu, Y. Li, Q. Huo, and B. Jiao, "Performance analysis of hybrid relay selection in cooperative wireless systems," *IEEE Trans. Commun.*, vol. 60, no. 3, pp. 779–788, Mar. 2012.

[140] A. Goldsmith, *Wireless communications.* Cambridge University Press, 2005.

[141] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes.* McGraw-Hill Education, 2002.

[142] A. Bletsas, A. G. Dimitriou, and J. N. Sahalos, "Interference-limited opportunistic relaying with reactive sensing," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 14–20, Jan. 2010.

[143] A. Jeffrey and D. Zwillinger, *Table of integrals, series, and products.* Academic Press, 2007.

[144] M. Geller and E. W. Ng, "A table of integrals of the exponential integral," *Journal of Research of the National Bureau of Standards*, vol. 71, pp. 1–20, 1969.

[145] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6913–6924, Oct. 2016.

[146] N. Cai and T. Chan, "Theory of secure network coding," *Proc. IEEE*, vol. 99, no. 3, pp. 421–437, Mar. 2011.

[147] L. Lima, J. P. Vilela, J. Barros, and M. Medard, "An information-theoretic cryptanalysis of network coding - Is protecting the code enough?" in *Proc. Int. Symp. on Inform. Theory and its Applications*, Dec. 2008, pp. 1–6.

[148] K. Bhattad and K. R. Narayanan, "Weakly secure network coding," in *Proc. Workshop on Network Coding, Theory and Applications (NetCod)*, Riva del Garda, Italy, Apr. 2005.

[149] L. Lima, M. Médard, and J. Barros, "Random linear network coding: A free cipher?" in *Proc. IEEE Int. Symp. on Inform. Theory*, Nice, France, Jun. 2007.

[150] J. Claridge and I. Chatzigeorgiou, "Probability of partially decoding network-coded messages," *IEEE Commun. Lett.*, vol. 21, pp. 1945–1948, May 2017.