Self-supported and Cooperative Networking for Wireless Networks

July 2013

Biao Han

Self-supported and Cooperative Networking for Wireless Networks

Graduate School of Systems and Information Engineering

University of Tsukuba

July 2013

Biao Han

Abstract

Over the past half-decade, relaying and cooperation have emerged as effective solutions to satisfy the stringent requirements of advanced wireless communication applications. This dissertation studies the relaying mechanisms and potential benefits of node cooperation in wireless networks. Specifically, we propose two categories of networking schemes, namely self-supported networking and cooperative networking, to coordinate the network and enhance wireless communications. Overall system performance (e.g., throughput, end-to-end delay, secrecy capacity, capacity) is improved by applying our proposed networking schemes over wireless networks.

First, we investigate the problems of congestion mitigation and non-cooperation avoidance in packet forwarding wireless ad hoc networks (WANETs). To formulate the problem, we reflect the dependency relation among nodes in a connected WANET by constructing a dependency graph. According to the dependency graph, we observe that wireless network congestion and non-cooperative behaviors are usually caused by some potential selfish and busy nodes. Then we propose an energy-efficient congestion-aware routing protocol, which is the fundamental component of the networking strategy. Two self-supported novel movement procedures are designed for the urgent sources to support themselves and to avoid congestion and non-cooperation: Direct Movement to potential selfish/busy Relays (DMR) scheme to reduce the end-to-end delay, and Iterative Movement to potential selfish/busy Relays (IMR) scheme to ensure the network connectivity. Through extensive simulation results, we validate that our proposed self-supported networking scheme significantly improve the network performance in terms of throughput, packet drop ratio, and end-to-end delay, comparing with the Ad-hoc On-demand Distance Vector (AODV) routing protocol based networking scheme.

Second, motivated by the benefits of cooperative wireless networking, we investigate the potential issues in deploying cooperative communication (CC) to traditional multi-hop wireless networks. We propose a novel cross-layer design which jointly considers the problems of routing selection at the network layer, congestion and non-cooperation avoidance among multiple links at the Medium Access Control (MAC) layer under cooperative multi-hop wireless environments. Our objective is to maximize the minimum flow rate while minimizing the aggregate routing cost, by allocating the link activeness and relay selection for all links. We formulate the multi-hop cooperative flow routing and relay node selection process as a mixed integer linear programming (MILP) problem, which is an NP-hard combinatorial optimization problem. Based on the modeling and formulations, we first reduce the considered problem and relax some of the constraints to support multi-session cooperative transmission. Then we propose a Self-supported based Cooperative Networking (SCooN) scheme which includes three novel components: 1) dependency graph construction, captures the nodes' dependency relations in wireless multi-hop communication; 2) CC-aware routing, establishes the available routes for cooperative transmission; and 3) novel movement of source or relay, avoids potential collisions among multiple sessions hence reduce the flow cost. Extensive experimental results demonstrate that the proposed SCooN scheme makes the solution procedure of multi-hop cooperative transmission highly efficient and significantly achieves better network performance.

Third, to further exploit the capacity gain brought by cooperative communication, we study the optimal relay placement problem for multi-pair cooperative communication in wireless networks. A limited number of relay nodes can be placed into the network to help the transmission of multiple source-destination pairs. Our objective is to maximize the system capacity. After formulating the relay node placement problem, we comprehensively discuss the effect of relay location on cooperative link capacity and show several attractive properties of the considered problem. As the main contribution, we develop a geographic-aware relay node placement algorithm which optimally solves the relay node placement problem in polynomial time. The basic idea is to place a set of relay nodes to the optimum locations so as the maximize the system capacity. The efficiency of our proposed algorithm is evaluated by the results of series experimental studies.

Fourth, the problem of physical-layer security based cooperative communication in wireless networks is investigated. After characterizing the security performance of the system by secrecy capacity, we study the secrecy capacity maximization problem in cooperative ad hoc networks with the involvement of multiple malicious eavesdroppers. Specifically, we propose a system model where a set of relay nodes can be exploited by multiple source-destination pairs to achieve physical layer security. We theoretically present a corresponding formulation for the secrecy capacity maximization problem. Then we develop an optimal relay assignment algorithm which solves the problem in polynomial time. The basic idea behind our proposed algorithm is to boost the capacity of the primary channel by simultaneously decreasing the capacity of the eavesdropping channel. To further increase the system secrecy capacity, we exploit the jamming technique and propose a smart jamming algorithm to interfere the eavesdropping channels. Through extensive experiments, we validate that our proposed algorithms significantly increase the system secrecy capacity under various network settings.

Acknowledgements

First and foremost, I would like to thank my advisor, Prof. Jie Li, for his excellent guidance without which it would have been impossible for me to do the high quality of research I did during my PhD period. He has been extremely critical, helpful, encouraging, patient, and supportive of my study through all my years at University of Tsukuba. His high standards of research have inspired me to challenge myself much more than I would have otherwise. There is no doubt in my mind that my own research and writing style is greatly influenced by how Prof. Li conducts his research, and I hope that I can continue to live up to his high standards.

It is my great honor to thank Prof. Jiro Tanaka, Prof. Kazuhiko Kato, Prof. Daisuke Takahashi, and Prof. Shigetomo Kimura for being my dissertation committee members and providing valuable advices and comments on evaluating this dissertation in its final form. I would like to thank the Department of Computer Science, the Graduate School of Systems and Information Engineering at University of Tsukuba, for their continuous supports on my study in Japan.

I cannot thank my advisor during my postgraduate study, Prof. Jinshu Su enough for his supervision, guidance, and valuable help, without which it would have been difficult for me to have an opportunity to pursue the PhD degree in Japan. I would also like to thank the China Scholarship Council (CSC) Foundation, for offering the scholarship to support my study in University of Tsukuba.

I would like to acknowledge the memorable helps from the members of the Operating System and Distributed Processing (OSDP) lab, Prof. Hisao Kameda, Dr. Ghada Ahmed Abdel Monaim Khoriba, Dr. Yu Gu, Dr. Xiaofei Xing, Dr. Yongsheng Liu, Huang Lu, Xiaoyan Wang, Xiucai Ye, Shuai Fu, Li Qiang, Atsushi Nagashima, Zhongping Dong, Liwen Xu, Ou Wang, Yajun Tian, Kei Ebana, Zichen Jin, Yujie Hu, Zhengxu Li, Cheng Sun, Ke Tang, Naoto Ishiduka, and Serigne Mbacke Ndiaye. It has been my great honor to work with them. I would also like to express my gratitude to Prof. Yuguang Fang, and the members in the Wireless Networks Laboratory (WINET) at University of Florida, where I had a nice and fruitful 3-months internship. I would also like to thank Prof. Jiannong Cao (Hong Kong Polytechnic University), Dr. Corinne Touati (INRIA-LIG, France), Prof. Lasheng Yu (Central South University, China), Prof. Li Xu (Fujian Normal University,

China), Prof. Jianping Pan (University of Victoria, Canada) and Prof. Wenzhong Guo (Fuzhou University, China) for their kind suggestions and comments on my work.

Finally, and most importantly, I would like to acknowledge the immeasurable support given to me by my parents and my family. Words cannot describe my gratitude towards them.

My apologies if I have inadvertently omitted anyone to whom acknowledge is due.

Contents

List of Figures

List of Tables

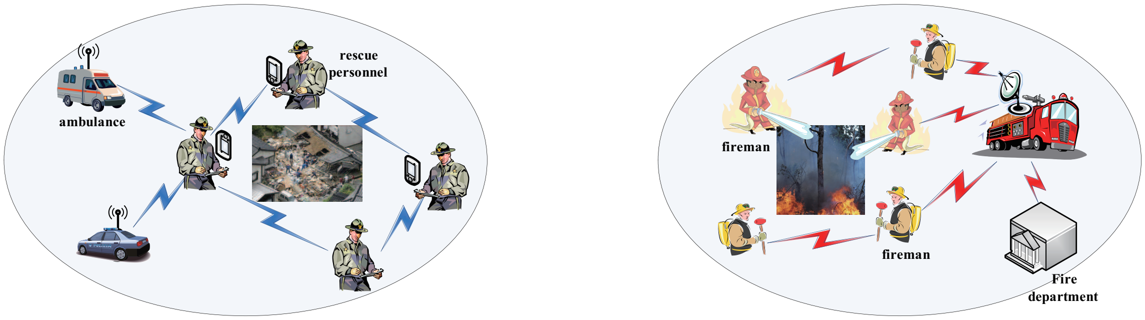
Chapter 1

Introduction

This chapter begins with introducing the motivation and the overview of our research work. We will provide the main objectives and contributions of this dissertation in the following of this chapter.

1.1 Motivation

Earthquakes, forest fires, and other natural disasters often devastate communications infrastructures just when they are most needed to save lives. With the advancement of telecommunication technology, public safety organizations increasingly rely on wireless networks to provide effective communications during emergency operations such as earthquake reliefs, fire rescues and medical assistance, etc. Wireless networking technology is an appropriate foundation to support communications among different individuals in an emergency situation. However, due to the energy constraints, radio-frequency regulations and potential interference in wireless networks, it imposes challenging problems for information routing, topology control and channel allocation while supporting emergency services. On one side, the demand of using communication services increases rapidly after an event of emergency. Without effective networking coordinations, it may lead to inefficient use of network resources by increasing congestion. On the other side, within a disaster area, it is of vital importance for rescue personnel to obtain an accurate and consistent picture of the situation, and to regain control and coordination on the shortest notice as soon as possible.



(a) An earthquake relief scenario

(b) A fire rescue scenario

FIGURE 1.1: Two examples when wireless networks are deployed to support various emergency services in disaster areas.

In recent wireless applications, relaying and cooperation have emerged as effective solutions to satisfy the the tremendously increasing demands of communication services. Relaying technique is first introduced into wireless networks to deliver data over longer distances, possibly through multiple hops data forwarding, and to ensure network connectivity. Due to the self-organized capabilities of wireless ad hoc network (WANET), it has been admitted as one of promising architecture to provide flexible data transmission for emergency services. However, in wireless ad hoc networks, autonomous nodes may be reluctant to forward others' packets because of the nodes' limited energy. Such selfishness and noncooperation will severely deteriorate the system efficiency and nodes' performances. Moreover, the distributed wireless nodes with only local information may not know the cooperation point, even if they are willing to cooperate. Hence, it is crucial to design effective networking strategy to avoid non-cooperative behaviors and to incentive node cooperation.

Cooperative communication (CC), which exploits the wireless broadcast advantage and the relaying capability of other cooperative nodes, is potential to provide significant performance enhancement in terms of spatial diversity, increased capacity and improved reliability in wireless networks. Networking over cooperative wireless networks has received significant attentions recently as an emerging network design strategy for future wireless networks. In cooperative networking, individual network nodes can cooperate to achieve network goals in a coordinated way, and the cooperation can take place in a cross-layer fashion. Successful cooperative networking can prompt the development of advanced wireless networks to cost-effectively provide multimedia services and applications such as telecommuting, video conferencing, interactive media, real-time Internet games, etc., anytime, anywhere. The uprising benefits of cooperative networking inspire us to investigate the potential issues in using the cooperative communication paradigm to supporting emergency services in wireless networks. However, the impact and challenges of cooperative networking on cross-layer design beyond cooperative transmissions have not been well investigated yet. Some fundamental aspects requiring immediate studies include: theoretical tools to guide the design of cooperative networking systems, effective incentive mechanisms for cooperation, new cooperative protocol design, compatible deployment of cooperative networking over existing wireless network infrastructures, innovative security enhancement and the state-of-art cooperative wireless application implementation.

1.2 Dissertation Objectives

Motivated by the critical requirements of emergency-oriented wireless applications, the goal of this dissertation is to understand the potential benefits of relaying and node cooperation in wireless networks, and provide effective networking mechanisms to support emergency services. Inspired by the idea of Do-It-Yourself, we propose the **self-supported** networking schemes for urgent sources and relays to support themselves by cognitive movements, with the objectives to mitigate network congestion and to avoid non-cooperation. Motivated by the benefits of **cooperative networking**, we focus on the problems of relay placement and secrecy capacity maximization, and propose efficient cooperative networking schemes to improve the network performance. Specifically, the objectives of this dissertation are summarized as follows.

1.2.1 Congestion Mitigation and Non-cooperation Avoidance in WANETs

In recent years, application domains of WANETs gain more and more attentions in military and non-military organizations. For an end-to-end transmission in WANET, packets are often delivered through multiple hops. During the packet forwarding process, it may not be in the best interest of an individual node to always accept the relay requests from other nodes. Because forwarding other's packets consumes its limited battery energy and might induce to intolerable congestion while transmitting its own packets. The congestion and non-cooperative problems become extremely critical while using WANETs to support the emergency operations within a disaster area.

Started from reflecting the relying relations of a connected WANET, we intend to model the potential network congestion and non-cooperative behaviors of the selfish users by dependency relations construction. A new routing protocol which is aware of network congestion and non-cooperation is the fundamental component of the networking strategy. Besides, the experience of surfing in an indoor wireless local area network (WLAN) environment motivates us to seek for better network performance based on the idea of Do-It-Yourself.

1.2.2 Cross-layer Optimization for Cooperative Multi-hop Wireless Networks

Cooperative communication creates a virtual Multiple-Input Multiple-Output (MIMO) environment where individual network nodes collaborate and share their antennas to form a distributed MIMO system. Specifically, cooperation performs in a cross-layer fashion. On one hand, CC can provide potential capacity improvement which is extremely important for advanced wireless applications. On the other hand, CC can reduce the end-to-end transmission delay and improve the probability of information reception by implementing in a set of coordinated cooperative nodes.

Based on the study in wireless networking for WANETs, we aim at applying cooperative communication over existing wireless infrastructures and design theoretical tools to guide the design of cooperative networking systems. First, the design of cooperative networking should be in a cross-layer fashion. Second, the performance gain from cooperative communication largely depends on the cross-layer design. Third, both the benefits and costs while applying CC in traditional multi-hop wireless network should be jointly considered. The objectives of our networking strategy in cooperative communication aware multi-hop wireless networks are twofold: 1) at the network layer, through optimal relay node selection to minimize the cost of multi-hop cooperative flow routing; 2) at the Medium Access Control (MAC) layer, maximize the minimum flow rate (or throughput) among all active sessions, as well as avoid congestion and non-cooperation behaviors.

1.2.3 Cooperative Relay Placement for Capacity Maximization in Wireless Networks

The increasing demands of high throughput, low transmission delay and cost-effective wireless communication applications motivate the development of Multi-hop Cellular Networks (MCNs), Wireless Ad-hoc NETworks (WANETs) and Worldwide Interoperability for Microwave Access networks (WiMAX). One of the most challenging problems in advanced wireless networking is the lack of compatible deployment of cooperative networking over existing wireless network infrastructures. Consider the limited network resources (e.g., a limited number of relay stations), the interaction between traditional wireless networking and cooperative networking has not been well understood yet. One critical issue involves the cooperative relay placement problem.

During cooperative communication (CC), spatial diversity can be achieved by exploiting the relaying capabilities of the involved relay nodes, which may vastly enhance the achieved system capacity. Although CC promises to enhance capacity, an improper placement of relay node can result in an even smaller capacity than that under direct transmission (DT). Therefore, the potential gains in capacity enhancement largely depend on the location of the involved relay nodes. The cooperative relay placement problem for capacity maximization in multi-session cooperative wireless networks is very challenging due to two facts: 1) the potential space for the relay placement is continuous; 2) multiple sessions exploiting the limited candidate relay set and the maximization of system capacity have to be jointly considered. For this research topic, our objective is to fully exploit the potential benefits of cooperative communication, theoretically formulate the relay placement problem, strive to obtain a comprehensive understanding of the problem and design simple yet provably good algorithms for finding a solution.

1.2.4 Physical-layer Security Enhancement for Cooperative Wireless Networks

The issues of security and privacy in wireless networks have taken on increasingly important roles in practice, especially in military and homeland security applications. Secure communications in wireless networks are traditionally achieved with cryptographic algorithm based protocols at higher layers of the network protocol stack, e.g., link, network, application or transport layer. The emergence of large-scale, dynamic, and decentralized wireless networks imposes new challenges on classical cryptographic measurements.

To this end, researchers have sought novel information theoretic techniques that can guarantee wireless network security without the need for secret keys. One of the most promising ideas is to exploit the wireless channel physical layer characteristics for improving the reliability of wireless transmission against eavesdropping attacks, named as *physical layer security*. Although physical layer security has attracted much attention recently, the issue of secure cooperative communication has not been well studied yet.

We aim to provide secure communication in cooperative ad-hoc networks by investigating the techniques of cooperative relaying and cooperative jamming. Through cooperative relaying, one can enhance the system security against eavesdroppers by boosting the capacity of primary channel (transmission channel from specific sources to respective destinations), and simultaneously decreasing the eavesdropping channel (transmission channel from specific sources to malicious eavesdroppers) by relay assignment procedure. Through cooperative jamming, one or several friendly jammers are able to cooperatively generate intentional interference towards the eavesdroppers.

1.3 A Roadmap and Summary of Contributions

The goal of this dissertation is to investigate the relaying mechanisms and potential benefits of node cooperation in wireless relay networks, and provide effective networking schemes to support emergency services. For this purpose, we analyze specific problems in both non-cooperative and cooperative wireless networks (especially, in wireless ad-hoc networks), present practical networking schemes, and derive comprehensive results to validate the efficiency of our proposed networking schemes. We depict a roadmap of the work performed in this dissertation in Fig. 1.2. The main contributions of this dissertation can be summarized in the following four aspects.

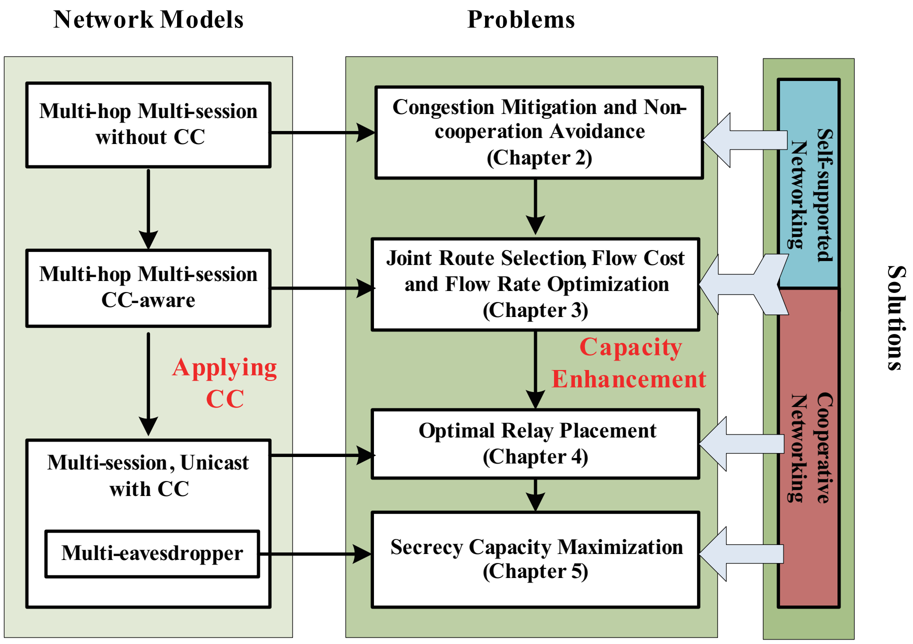

Network Models
Problems
Multi-hop Multi-session without CC
Multi-hop Multi-session CC-aware
Applying CC
Multi-session, Unicast with CC
Multi-eavesdropper
Congestion Mitigation and Non-cooperation Avoidance (Chapter 2)
Joint Route Selection, Flow Cost and Flow Rate Optimization (Chapter 3)
Capacity Enhancement
Optimal Relay Placement (Chapter 4)
Secrecy Capacity Maximization (Chapter 5)
Self-supported Networking
Cooperative Networking
Solutions

FIGURE 1.2: A roadmap of the work performed in this dissertation.

1.3.1 Self-supported Congestion-aware Networking for Non-cooperative WANETs

In **Chapter** 2, we focus on promoting energy-efficient and congestion-aware communication for emergency services in wireless ad hoc networks (WANETs) using self-supported schemes. To formulate the problem, we reflect a connected network by *dependency graph* and classify the nodes into principal nodes and subordinate nodes. Then we model network congestion and non-cooperation behaviors according to the relations between nodes in the constructed dependency graph. Then we propose an energy-efficient and congestion-aware routing protocol for the emergency services in WANETs.

Based on the proposed model and routing protocol, we design two novel movement schemes, called Direct Movement to potential selfish/busy Relays (DMR) scheme and Iterative Movement to potential selfish/busy Relays (IMR) scheme for urgent sources to support themselves and to avoid congestion and non-cooperation. Analysis and simulation results reveal that our proposed networking schemes significantly achieve better network performance and typically satisfy the requirements for emergency services in WANETs.

1.3.2 Self-supported Networking for Cooperative Multi-hop Wireless Networks

In **Chapter 3**, we investigate the potential issues in using cooperative communication (CC) paradigm to support emergency services in multi-hop wireless networks. We propose a novel cross-layer design which jointly consider the problems of routing selection in the network layer, congestion and non-cooperation avoidance among multiple links in the MAC layer under cooperative multi-hop wireless environments. Our objective is to maximize the minimum flow rate while minimizing the aggregate routing cost, by allocating the link activeness and relay selection for all links.

We formulate the multi-hop cooperative flow routing and relay node selection process as a mixed integer linear programming (MILP) problem, which is an NP-hard combinatorial optimization problem. Based on the modeling and formulations, we propose a self-supported networking scheme including three novel components that make the solution procedure highly efficient. Through extensive simulation results, we show that the proposed networking scheme performs well while supporting emergency services in multi-hop wireless networks.

1.3.3 Optimal Relay Placement for Multi-pair Cooperative Communication in Wireless Networks

In **Chapter 4**, to further improve the system performance of cooperative wireless networks, we study the relay node placement problem for multi-pair cooperative communication, where a limited number of candidate relay nodes can be placed to help the transmission of multiple source-destination pairs. Our objective is to maximize the system capacity.

After formulating the relay node placement problem, we comprehensively discuss the effect of relay location on cooperative link capacity and show several attractive properties of the considered problem. As the main contribution, we develop a geographic aware relay node placement algorithm which optimally solves the relay node placement problem in polynomial time. The basic idea is to place a set of relay nodes to the optimum locations so as the maximize the system capacity. The efficiency of our proposed algorithm is evaluated by the results of series experimental studies.

1.3.4 Secrecy Capacity Maximization for Secure Cooperative Wireless Networks

In **Chapter 5**, we exploit physical layer security to provide secure cooperative networking for emergency services in CC-aware wireless networks where involve multiple malicious eavesdroppers. By characterizing the security performance of the system by secrecy capacity, our objective is to maximize the system secrecy capacity.

Specifically, we propose a system model where secrecy capacity enhancement is achieved by the assignment of cooperative relays. After theoretically presenting a corresponding formulation for the problem, we make comprehensive investigations on the security gain brought by the relay assignment procedure. Then we develop an optimal relay assignment algorithm which is able to solve it in polynomial time. The basic idea behind our proposed relay assignment algorithm is to boost the capacity of the primary channel by simultaneously decreasing the capacity of the eavesdropping channel. To further increase the system secrecy capacity, we exploit the jamming technique and propose a smart jamming algorithm to interfere the eavesdropping channels. Through extensive experiments, we validate that our proposed algorithms can significantly increase the system secrecy capacity and satisfy the security requirements under various network settings.

1.4 Dissertation Organization

This dissertation is organized as follows. In Chapter 1, we introduce the motivation of our research, give a brief overview of the research topics and outline the main contributions in this dissertation. Self-supported congestion-aware networking is presented in Chapter 2. In Chapter 3, we propose the self-supported based cooperative networking for multi-hop wireless networks. Chapter 4 presents optimal relay node placement for multi-pair cooperative communication. In Chapter 5 we study the secrecy capacity maximization problem for cooperative ad-hoc networks. Finally we conclude this dissertation and points out the future work in Chapter 6.

Chapter 2

Self-supported Congestion-aware Networking for Non-cooperative WANETs

This chapter studies the problems of network congestion mitigation and non-cooperation avoidance in non-cooperative wireless networks. We focus on promoting self-supported and congestion-aware networking for emergency services in WANETs based on the idea of Do-It-Yourself. We model network congestion and non-cooperation behaviors according to the relations between nodes in the constructed dependency graph. Then, we propose an energy-efficient and congestion-aware routing protocol for the emergency services of WANETs. Based on the proposed model and routing protocol, we design two novel movement schemes, called Direct Movement to potential selfish/busy Relays (DMR) scheme and Iterative Movement to potential selfish/busy Relays (IMR) scheme for urgent sources to supported themselves and to avoid congestion and non-cooperation. Analysis and simulation results show that our approaches significantly achieve better network performance and typically satisfy the requirements for emergency services in WANETs.

This chapter is organized as follows. Section 2.1 introduces the motivation of our work and the emerging problems in using wireless networking to support emergency services. In Section 2.2, we briefly survey the related work. In Section 2.3, we describe the network model and give the problem formulation. In Section 2.4, we propose the self-supported congestion-aware networking scheme, prove some of its key properties, and describe how to apply it for emergency services in WANETs. In Section 2.5, we develop the proposed networking scheme to ensure network connectivity. In Section 2.6, we evaluate the performance of our proposed networking schemes through extensive simulations. Section 2.7 summarizes this chapter.

2.1 Introduction

Communication systems play an essential role in emergency situations such as fire rescues, traffic accidents or building collapses. In an emergency case, it is of vital importance for rescue personnel to obtain an accurate and consistent picture of the situation, and to regain control and coordination on the shortest possible notice as soon as possible. One promising method for providing real-time communication in emergency situations involves the use of wireless ad hoc networks (WANETs).

The main requirements for emergency services including: (1) real-time communication, (2) low-delay transmission, and (3) high priority of emergency information. The lack of infrastructure and the limited battery power in WANETs require new technologies for mobility management, topology control, and energy-efficient information routing in supporting emergency services. One challenging problem involves the coordination of network under emergency situations. It is often noticed that, without coordination between users, this may lead to inefficient use of the network resources by increasing congestion and affect the network connectivity because of the non-cooperation behaviors of some selfish users. As pointed out in [2], network demand can be up to 5 times of normal when emergency events happen. Network performance could be deteriorated because of congestion. On the other hand, in a multi-hop packet forwarding WANET, it may not be in the best interest of a selfish or busy node to always accept relay requests. Because forwarding of others' packets consumes its limited battery energy and might induce to intolerable delay while transmitting its own packets. These uncooperative activities will severely affect the network efficiency, at best, and network connectivity, at worst [5], [7].

This chapter focuses on promoting energy-efficient and congestion-aware communication for emergency services in WANETs using self-supported schemes. To formulate the problem, we reflect a connected network by dependency graph and classify network nodes into principal nodes and subordinate nodes. Then we model network congestion and non-cooperation behaviors according to the relations between principal and subordinate nodes in the constructed dependency graph. We design an energy-efficient and congestion-aware routing protocol based on the Ad-hoc On-demand Distance Vector (AODV) routing protocol [14]. Thirdly, after investigating the locations of congestion and non-cooperation, urgent sources support themselves by cognitive replacing some of their selfish and busy relays. We propose the Direct Movement to potential selfish/busy Relays (DMR) scheme to support instantaneous communication for emergency services. In order to ensure network connectivity, we design the Iterative Movement to potential selfish/busy Relays (IMR) scheme as an improvement of DMR scheme.

Our idea is from the experience of surfing in an indoor wireless local area network (WLAN) environment, wireless signals could be strengthened by moving the laptop closer to a wireless router. It motivates us to search for better network performance through self-supported networking scheme based on the idea of Do-It-Yourself [1]. The main contributions of this chapter can be listed as follows:

- We model network congestion and non-cooperation behaviors according to the relations between nodes in the constructed dependency graph.
- We propose an energy-efficient and congestion-aware routing protocol for emergency services in WANETs.
- We propose two novel movement schemes, called DMR and IMR for urgent sources to supported themselves and to avoid congestion and non-cooperation.

2.2 Related Work

This section briefly surveys related work in using WANETs for emergency services and the problems of network congestion and non-cooperation in supporting emergency services with WANETs.

[1] Do-It-Yourself (or DIY) is a term used to describe building, modifying, or repairing of something without the aid of experts or professionals [1]. In this chapter, we use it to represent the concept of our self-supported networking schemes.

Many research and applications exist in using wireless networks for emergency services. Harvard Sensor Networks Lab develops a wireless communication infrastructure for emergency medical care called *CodeBlue* [26]. Saikat Ray *et al.* [25] propose a new framework providing robust location detection in emergency response systems. Braunstein *et al.* [27] apply wireless mesh network to support emergency services and develop it to provide simulated disaster response activity. Tseng *et al.* [28] propose a distributed navigation algorithm for wireless sensor networks in emergency situations. Maurits *et al.* [4] address a broadband ad-hoc networking application for emergency services called *Easy Wireless* which pays more attention on supporting multimedia applications. To the best of our knowledge, there is not any related work comprehensively consider the problem of network congestion and non-cooperation while using WANETs for emergency services.

The problem of network congestion in wireless environment has draw significant scientific attentions [29]-[31]. Bret [3] address the congestion problem in WANETs and solve it from hop-by-hop flow control to medium access control (MAC). Wan and Eisenman [29] propose an energy-efficient congestion control scheme. On the basis of their work, Chen [30] and Lin [31] study cross-layer design for congestion control in WANETs. As far as we know, few of related work focuses on distributed congestion control methods as well as the probability that congestion could be avoided by the effort of network nodes themselves.

Recently, the problem of stimulating cooperation in WANETs has attracted much scientific attention. The related work are based on enforcement mechanisms [5]-[6] or on virtual currency [7]-[9]. Recent developments have also shown that there are potential cases in which selfish users can cooperate to forward packets without incentive mechanisms and cooperation may emerge [10], [35]. Saad and Han [37] introduce coalition games to solve the cooperation problem. However, it may lead to intolerable routing overload while applying these methods to support emergency services in WANETs. As far as we know, most of the recent literatures did not consider the critical requirements of emergency services.

2.3 Model Description and Problem Formulation

We model a WANET for emergency services with a graph $G = (V, E)$. Here V is a set of network nodes and E is a set of all directed links $\langle v_i, v_j \rangle$ where $v_i, v_j \in V$. The link $\langle v_i, v_j \rangle$ exists if the transmission power of node i to node j, P_{ij} in watt, is more than or equal to

$\beta \cdot d_{ij}^{\alpha}$ (i.e., $P_{ij} \geq \beta \cdot d_{ij}^{\alpha}$), where β is the transmission quality parameter, d_{ij} is the Euclidean distance between node i and node j, and α is the distance-power gradient [12]. There are M source nodes forming the source set $\mathrm{S} = \{s_1, s_2,...,s_M\}$ and the corresponding destination set is $\mathrm{D} = \{d_1, ...,d_i,...,d_M\}$. Denote a path connecting the ordered pair $\omega = (s_i, d_i)$ a sequence of links $\langle v_1, v_2 \rangle, \langle v_2, v_3 \rangle, ..., \langle v_{n-1}, v_n \rangle$ where $v_1, v_2, ..., v_n$ are distinct nodes, $v_1 = s_i$ and $v_n = d_i$. For all nodes $i \in V$, let the initial energy be E_i and residual energy be $\bar{E}_i$ in joule. An emergency case is denoted by $Emg_i(t)$, where i is the wireless node detecting the emergency case and t is the time when it happens. The system model of a sample WANET for emergency services is shown in Fig. 2.1.

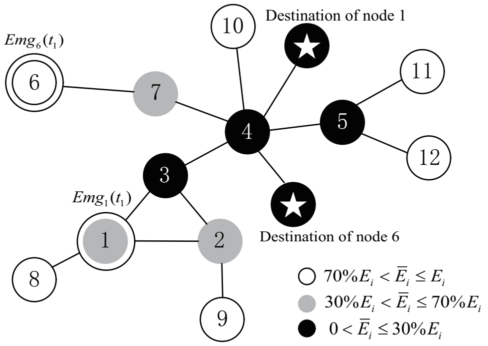

10
Destination of node 1
$Emg_6(t_1)$
6
7
11
4
5
12
3
$Emg_1(t_1)$
1
2
Destination of node 6
8
9
○ $70\%E_i < \bar{E}_i \leq E_i$
● $30\%E_i < \bar{E}_i \leq 70\%E_i$
● $0 < \bar{E}_i \leq 30\%E_i$

Figure 2.1: System model of a sample WANET for emergency services.

As an example shown in Fig. 2.1, nodes which are in emergency situations (double circles) want to communicate with their destinations (solid nodes with stars) respectively. Notice that there might be several emergency cases simultaneously (e.g. Emergency cases Emg_1 and Emg_2 occur at time t_1). The color of the nodes represents their residual energy levels, the hollow nodes are in high energy level, which have more than 70% of their initial energy, the gray nodes's residual energy are between 30% to 70% of their initial energy. The solid nodes are in low energy level, which have less than 30% of their initial energy.

In order to analyze the directed communication between distinct nodes in the interactive topology during a certain time period Δt, we describe it by a directed graph [32]. Connections appear in the directed graph as lines with arrows indicate the direction of wireless communication between nodes. The directed graph of our sample network is illustrated in Fig. 2.2, in which source node $s_i (i = 1, 2, ..., 7)$ communicates to its destination $d_i (i = 1, 2, ..., 7)$ respectively. Notice that certain nodes are denoted as source nodes in the diagram (e.g. s_1,...,s_5), but they act as relays as well.

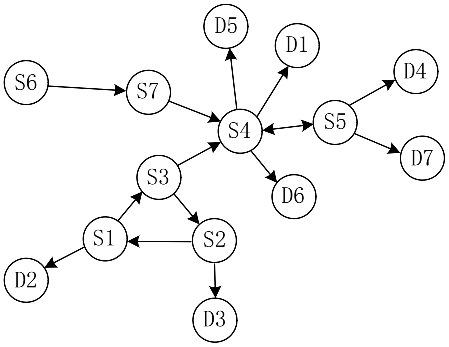


Figure 2.2: Directed graph of the sample network during Δt.

This example might correspond to a snapshot of a multi-hop packet forwarding WANET in which each node is acting on its own interest, transmitting more packets to its respective destination but consuming less energy in forwarding others' packets. We will use this example to explain the interactive relations for emergency services of WANET in the remainder of this chapter.

2.3.1 Dependency Graph Construction

In a defined WANET, each source node might depend on many intermediate nodes while transmitting to its destination. In order to formulate network congestion and non-cooperation behaviors, we represent the dependency relations in the network and classify the nodes in the dependency graph into different categories.

A *dependency graph* $G' = (N, L)$ is a diagram of the set of vertexes and edges. Each vertex v_i in set N corresponds to a node and L is the set of all directed edges. There is a directed edge from vertex v_i to v_j, denoted by the ordered pair $\langle v_i, v_j \rangle$, if there exists a route where v_i is the relay node of source node v_j. Intuitively, an edge $\langle v_i, v_j \rangle$ means that node v_j depends on node v_i while forwarding packets to its destination.

Notice that the dependency between nodes can be mutual, especially for the nodes at the center of the network, this mutual dependency is common. We define such mutual dependency as *dependency loop*.

A *dependency loop* is a sequence of edges $\langle v_1, v_2\rangle, \langle v_2, v_3\rangle, ..., \langle v_{j-1}, v_j\rangle$ in the dependency graph, where $v_1, v_2, ..., v_j$ are distinct nodes and the first node v_1 is same as the last node v_j, $v_1 = v_j$.

In the dependency loop, all nodes are mutually rely on others. There are also nodes do not have mutual dependency in the dependency graph, which depend on others but others do not depend on them.

2.3.2 Nodes Classification

As discussed before, in the dependency graph G' of a network, there are nodes in dependency loops and nodes that are not in dependency loops. According to the dependency graph with dependency loops, we have the following notations and assumptions:

- ON_i, IN_i: the outside and inside nodes sets of node $v_i \in N$ in the dependency graph. They denote the nodes set that v_i relies on and rely on v_i.

- OD_i, ID_i: the outdegree and indegree of node $v_i \in N$. They are the number of edges come out from node v_i and go into node v_i in the dependency graph. They represent the number of nodes v_i relies on and rely on v_i.

- $ON(L_i)$, $IN(L_i)$: the outside and inside nodes sets of dependency loop $L_i \in L$ in the dependency graph. They denote the nodes set that L_i relies on and rely on L_i.

- $OD(L_i)$, $ID(L_i)$: the outdegree and indegree of dependency loop $L_i \in L$ in the dependency graph. They are the number of edges come out from dependency loop L_i and go into L_i in the dependency graph. They represent the number of nodes L_i relies on and rely on L_i.

- $|V|$: the number of nodes in the network.

- $|L_i|$: the number of nodes in dependency loop L_i.

- N_p: principal nodes set.

- N_s: subordinate nodes set.

- We assume for the moment that each node is the source of only one route and they act selfishly.

We give the definitions of *principal nodes* and *subordinate nodes* as follows.

Definition of *principal nodes*: In a dependency graph, node v_i is a principal node if and only if it is in a dependency loop L_i and satisfies one of the following conditions:

$$\underset{v_i \in L_i}{|L_i|} \geq \sqrt{|V|}, \tag{2.1}$$

$$\underset{v_i \in L_i}{OD(L_i)} \geq \underset{v_i \in L_i}{|L_i|}\ . \tag{2.2}$$

The two conditions in the above definition imply the principal nodes should in a dependency loop, the number of nodes in this dependency loop should be large enough or this loop should have a sufficient amount of nodes that rely on it. Some of the principal nodes are potential to be busy and might consume more energy than others as they always act as relays for others, they are also prone to act selfishly to the nodes that are not in the same dependency loop with them, which might induce to non-cooperation.

Definition of *subordinate nodes*: In a dependency graph, subordinate nodes are the rest nodes except of principal nodes. In a dependency graph $G' = (N, L)$ of a network, all nodes are classified into two sets: the set of principal nodes N_p and the set of subordinate nodes N_s. They satisfy the following conditions:

$$N_p \cup N_s = N \quad \text{and} \quad N_p \cap N_s = \emptyset. \tag{2.3}$$

The above definition represents that subordinate nodes are neither in dependency loops or in a loop with only a small number of nodes. Intuitively, in a multi-hop WANET, nodes in the center of the network are potential to be critical as there are more mutual interaction among them. For the nodes which are at the boundary of the network, this mutual dependency is not common, they depend on others but others might not depend on them. These nodes are subordinate nodes, compared with the principal ones. From the definitions of principal nodes and subordinate nodes, we find that a node is either a principal node or a subordinate node in the dependency graph.

As an example shown in Fig. 2.3, we classify the nodes in the dependency graph into principal nodes and subordinate nodes. The solid nodes represent the principal nodes and the hollow ones represent the subordinate nodes. Notice that the principal and subordinate

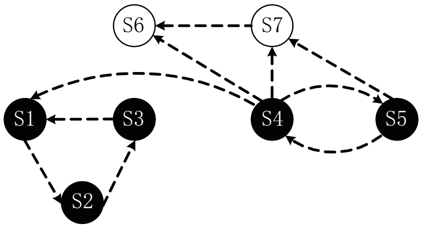


FIGURE 2.3: Dependency graph of the sample network with node category.

nodes are classified periodically as the interactive relation between nodes in the dependency graph might be dynamic. We will give the detail of constructing a dependency graph and classifying the node category in the next section.

2.3.3 Congestion and Non-cooperation Modeling

In the last subsection, we explain how to classify a node in a dependency graph into principal or subordinate node. Now we model congestion and non-cooperation behaviors by analyzing the relations between these nodes. According to [13], the data flow transmitted from node i to node j in bits per second is denoted by f_{ij}. At any node i, which is neither source nor destination, the flow-in should equal to the flow-out. For node $i \in S$, the flow-out should equal to the flow-in plus the throughput requirement Q_i. For node $i \in D$, the flow-out should equal to the flow-in minus Q_i. The conservative relation of data flow is defined formally as follows.

$$\sum_{\langle v_i,v_j\rangle \in E} f_{ij} - \sum_{\langle v_k,v_i\rangle \in E} f_{ki} = \begin{cases} Q_i & \text{if} \quad i \in S, \\ -Q_i & \text{if} \quad i \in D, \\ 0 & \text{otherwise.} \end{cases} \tag{2.4}$$

As in a multi-hop WANET, if there are more nodes rely on a node than it relies on, congestion may occur. According to the dependency graph, while the outdegree OD_i of a node v_i is larger than its indegree ID_i, node v_i might be in congestion status. This situation can be expressed as the following expression:

$$OD_i - ID_i > 0, \; if \;\; v_i \in N_s. \tag{2.5}$$

For the nodes in dependency loops, they are more potential to be in congestion status. The conservative relation of congestion is defined formally as follows:

$$\sum_{L_i \in L} OD(L_i) - \sum_{L_i \in L} ID(L_i) > |L_i| \ , \ if \ v_i \in N_p. \tag{2.6}$$

The cooperation problems between nodes with mutual dependency has been solved using repeated game theory [36]. We mainly focus on the non-cooperation behaviors between principal nodes and subordinate nodes as the latter are not in dependency loops. As we addressed before, in a dependency graph, if node v_i relies on v_j but v_j does not rely on v_i, non-cooperation may occur. The conservative of non-cooperation is defined as follows.

$$\begin{cases} v_i \in ON_j \quad \text{but} \quad v_j \notin ON_i, \\ v_i \in ON(L_j) \ \ \text{but} \quad v_i \notin IN(L_j). \end{cases} \tag{2.7}$$

2.4 Proposed Self-supported Congestion-Aware Networking (SCAN) Scheme

In the previous section, we model the network congestion and non-cooperation that are affecting the network efficiency. In order to support emergency services and meet the other critical requirements, we propose the self-supported congestion-aware networking (SCAN) scheme in this section. The SCAN scheme includes three parts. In the first subsection, we describe the initialization phase which constructs the dependency graph and classifies the nodes into principal nodes and subordinate nodes. We design an energy-efficient and congestion-aware routing protocol in the second subsection. Thirdly, we propose the Direct Movement to potential selfish/busy Relays (DMR) scheme to support instantaneous communication for emergency services in WANETs.

2.4.1 Initialization

At the initialization phase, we construct the dependency graph of a WANET during a set up time period Δt, classify the node category (principal/subordinate) for each node.

During the set up time period Δt, each node may act as source or relay. As a source node, it keeps all its relay nodes' identification and calculate how many nodes it relies on. As a relay node, it stores the request information containing the sender nodes' identification and calculate how many nodes rely on it. After the end of Δt, each node has a picture of the dependency relations of itself. Take our sample network in Fig. 2.2 as an example, the dependency relations and outdegree/indegree of each node are illustrated in Table 2.1. With these information of all nodes, a whole dependency graph of the network is constructed. We describe the initialization phase of constructing a dependency graph in Algorithm 1.

```
Algorithm 1: Construction steps of a dependency graph
Input: Network graph $G = (V, E)$ and set up time duration $\Delta t$
Output: Dependency graph $G' = (N, L)$
Start time $t = T$;
for $i = 1; i \leq N, t < T + \Delta t$ do
    $ON_i = \{\emptyset\}, ON_i = \{\emptyset\}$; $OD_i = 0, ID_i = 0$;
    if node $i$ generate a message then
        while node $j$ receives the message from $i$ do
            check the packet and keeps the identification of the sender:
            add $i$ to $ON_j$;
            add $j$ to $IN_i$;
            compute $OD_j$ and $ID_i$:
            $OD_j = OD_j + 1$;
            $ID_j = ID_i + 1$;
            if node $j$ is the destination then
                $ON_j = ON_j; IN_j = IN_j$
                $OD_j = OD_j; ID_j = ID_j$
            end
        end
    end
    return $ON_i, IN_i, OD_i, ID_i$
end
return Dependency Graph $G' = (N, L)$;
```

According to Algorithm 1, we can have the outside and inside nodes set for each node, the outdegree and indegree of each node can be calculated as well. Meanwhile, the dependency loops could also be identified based on the outside and inside nodes sets, as shown in Table 2.2. Each node could identify its category (principal/subordinate) according the degree information and dependency relations in the dependency graph. The corresponding dependency graph with node category is illustrated in Fig. 2.3.

Table 2.1: The table of nodes dependency relation and outdegree/indegree of the sample network.

Node	**Outside/Inside nodes set and degree**			
	ON_i	IN_i	OD_i	ID_i
s_1	$\{s_2\}$	$\{s_3,s_4\}$	1	2
s_2	$\{s_3\}$	$\{s_1\}$	1	1
s_3	$\{s_1\}$	$\{s_2\}$	1	1
s_4	$\{s_1,s_5,s_6,s_7\}$	$\{s_5\}$	4	1
s_5	$\{s_4,s_7\}$	$\{s_6\}$	2	1
s_6	$\{\emptyset\}$	$\{s_4,s_7\}$	0	2
s_7	$\{s_6\}$	$\{s_4,s_5\}$	1	2

Table 2.2: The table of dependency loops and outdegree/indegree of the sample network.

Loop	**Outside/Inside nodes and degree**			
	ON_i	IN_i	OD_i	ID_i
$L\{s_1,s_2,s_3\}$	$\{\emptyset\}$	$\{s_4\}$	0	1
$L\{s_4,s_5\}$	$\{s_1,s_6,s_7\}$	$\{\emptyset\}$	3	0

2.4.2 Route Selection

In addition to maximize the network lifetime and be aware of congestion and non-cooperation behaviors, an energy-efficient and congestion-aware routing protocol is required.

We design the proposed routing protocol of our networking framework based on the Ad-hoc On-demand Distance Vector (AODV) routing protocol [14]. In the AODV routing protocol, a route request message (RREQ) is used to send a route request from the source node by broadcasting it. When the desired destination node receives the RREQ messages, it chooses the best route, i.e., the shortest-hop route, then uses it to send route reply RREP to the source node. The source node then uses this route to send the data. As the shortest-hop route is used in AODV, some particular nodes may be used as intermediate nodes frequently and consume battery power much faster than others. Those hot spot nodes are easily running out of power much easier than the rest nodes in the network. Obviously, this will affect the network efficiency and network lifetime. Moreover, there may be competition between nodes to take those hot spot nodes as relays in terms of delay.

In the proposed protocol, we use the control message of the AODV routing protocol to avoid extra message overhead. The RREQ message triggers the received nodes to adjust their node category (principal/subordinate) before forwarding it to other nodes. Then each relay node calculates and adds in this RREQ message its residual living value V_i according to Eqn. (2.8):

$$V_i = \bar{E}_i / OD_i, \tag{2.8}$$

where V_i is proportional to the residual energy $\bar{E}_i$ and inversely proportional to the outdegree OD_i of a node. The nodes which have less V_i are acting as relays for more nodes or their residual energy are lower. V_i also reflects the possibility that a node is potential to be selfish and busy node.

We define a route from source s to destination d as follows:

$$R = \{(i_0, i_1), ..., (i_{h-1}, i_h)\}, \quad \forall (i_k, i_{k+1}) \ \in E, \tag{2.9}$$

where $i_0, i_1, ..., i_h$ are distinct nodes, $i_0 = s$, $i_h = d$, and h is the number of hops between source node s and destination node d. Consider there is a number of m available routes between source node $s \in S$ and destination node $d \in D$. The residual living value of route r_i, with nodes $i_0^{r_i}, i_1^{r_i}, ..., i_h^{r_i}$ is defined as follows:

$$V_{r_i} = Min(V_{i_0^{r_i}}, V_{i_1^{r_i}}, ..., V_{i_h^{r_i}}). \tag{2.10}$$

Then, the destination node receives the RREQ messages with their minimum residual living value V_{r_i} from each of the m available routes according to Eqn. (2.10). We define the utility U_{r_i} of each route r_i as in Eqn. (2.11), where $C_{hops}^{r_i}$ is the number of hops along r_i and $C_p^{r_i}$ is the number of principal nodes in r_i. The destination node calculates the hop-count utility of each route according to Eqn. (2.11).

$$U_{r_i} = V_{r_i} \Big/ (C_{hops}^{r_i} + C_p^{r_i}). \tag{2.11}$$

The best route $r_{\max}$ is the route with the maximum residual living energy, containing shortest hops and least principal nodes:

$$r_{\max} = Max(U_{r_1}, U_{r_2}, ...U_{r_m}). \tag{2.12}$$

Finally, the destination node uses the maximum one to send the RREP message as in Eqn. (2.12). Meanwhile, the destination node adds in this RREP message the identification number of the node which has the minimum residual living value V_{r_i} along the selected route. The RREP message also triggers this node to add its location information in it and then send back to the source node. The used route will change each time the source node sends to the same destination node as it depends on the residual living value which is dynamically changing.

2.4.3 Direct Movement to Potential Selfish/Busy Relays (DMR) Scheme

The key idea of our proposed networking scheme is to promote the source nodes to support themselves by their own efforts. In this subsection, we propose the Direct Movement to potential selfish/busy Relays (DMR) scheme by explaining how the source node move and replace their potential selfish/busy relays according to the feedback information received from the RREP message.

After receiving the RREP message from the destination containing the information of the potential selfish/busy relay nodes along the route, the source node notices the location of this relay node. We set a moving constraint value M_S for all source nodes. When the minimum residual living value V_{r_i} of its selected route r_i is less than M_S, our proposed DMR scheme triggers the source node to replace the relay node i ($V_i = V_{r_i}$) directly.

For some emergency services, response time is the most important requirement, it expects the destination could receive the emergency information as soon as possible and could have continuous communication with the source. DMR scheme satisfies these requirements because the movement of source node ensures the emergency information transmitting at a desired direction. On the other hand, the purpose of movement is to replace the potential selfish/busy relay, it ensures the communication could be maintained without considering the energy consumption of the relays with low energy. Furthermore, it avoids potential network congestion because the conscious movement of source node.

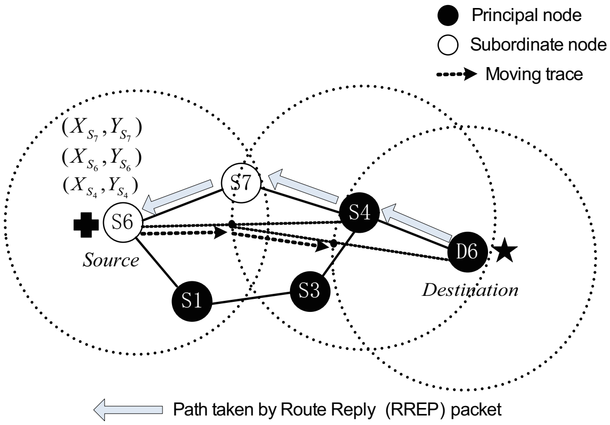


Figure 2.4: Direct Movement to potential selfish/busy Relays (DMR) scheme.

In Fig. 2.4, we take part of our sample network as an example to explain how the DMR scheme works. In this example, an emergency case occurs at node s_6. After receiving the RREP message, s_6 realizes the location of its most potential selfish/busy relay s_4 is (x_{s_6}, y_{s_6}). The dash line with arrow represents the moving trace of s_6. It indicates that s_6 directly moves to s_4 while sending its emergency messages at the same time.

2.5 Improvement of the Proposed SCAN Scheme

For some emergency services, connectivity and consistency of transmission are more critical. The DMR scheme we proposed in the SCAN networking scheme is simple and novel. However, it cannot ensure network connectivity during transmission. In this section, we propose the Iterative Movement to potential selfish/busy Relays (IMR) scheme as an improvement to our proposed SCAN scheme.

The first part of the Improved-SCAN (ISCAN) networking scheme is same as the SCAN scheme. At the route selection phase, the RREP message triggers all the relay nodes between source and the most potential selfish/busy relay to append their location information in it. At the last phase, IMR scheme maintains the source nodes to replace their potential selfish/busy relays iteratively.

We denote the source node S_0 and its most potential selfish/busy relay R_k, the relay nodes along the selected route between source to its most potential selfish/busy relay as $\{R_1, R_2, ..., R_{k-1}\}$, where k is the number of hops between S_0 and R_k. The locations of these relays are denoted as $\{(x_{R_1}, y_{R_1}), (x_{R_2}, y_{R_2}), ...(x_{R_{k-1}}, y_{R_{k-1}})\}$. In IMR scheme, the moving trace passes a sequence of points $\{S_0, I_1, ...I_{k-1}\}$, where S_0 is the starting point and I_i is the intersection from the $(i-1)_{th}$ point to the $(i+1)_{th}$ relay's transmission range. The moving trace is a sequence of coordinates: $(x_{S_0}, y_{S_0}), (x_{I_1}, y_{I_1}), ..., (x_{I_{k-1}}, y_{I_{k-1}})$, where (x_{I_i}, y_{I_i}) is the coordinate of the i_{th} intersection. After realizing the coordinates of the source node (x_{S_0}, y_{S_0}) and all the relays $\{(x_{R_1}, y_{R_1}), (x_{R_2}, y_{R_2}), ...(x_{R_{k-1}}, y_{R_{k-1}})\}$, (x_{I_i}, y_{I_i}) can be calculated according to Eqn. (2.13) and Eqn. (2.14), where $\overline{S_0R_2}$ is the distance between S_0 and R_2, and r is the transmission range.

$$\begin{cases} x_{I_1} = x_{R_2} - \frac{(x_{R_2} - x_{S_0}) \cdot r}{\overline{S_0R_2}}, \\ y_{I_1} = \frac{x_{I_1} \cdot (x_{R_2} - x_{S_0}) + x_{R_2} \cdot y_{S_0} - x_{S_0} \cdot y_{R_2}}{x_{R_2} - x_{S_0}}. \end{cases} \tag{2.13}$$

$$\begin{cases} x_{I_i} = x_{R_{i+1}} - \frac{(x_{R_{i+1}} - x_{I_{i-1}}) \cdot r}{\overline{I_{i-1}R_{i+1}}}, \\ y_{I_i} = \frac{x_{I_i} \cdot (x_{R_{i+1}} - x_{I_{i-1}}) + x_{R_{i+1}} \cdot y_{I_{i-1}} - x_{I_{i-1}} \cdot y_{R_{i+1}}}{x_{R_{i+1}} - x_{I_{i-1}}}. \end{cases} \tag{2.14}$$

Fig. 2.5 depicts the moving trace returned by the IMR scheme, in which source node S_0 move to its potential selfish/busy relay R_5 iteratively. Next, we also explain why the DMR scheme cannot ensure connectivity. If S_0 moves to R_5 directly, on the way between A to B, it will lose connectivity due to the disconnection with all the nodes in the network. The proposed IMR scheme ensures the source node could be connected to at least one relay node.

Intuitively, the most simple moving trace that ensures connectivity is the trace along the selected route from a source to its destination, but the distance of this moving trace is longer than the trace returned by the IMR scheme. We denote the moving distance of IMR scheme as D_{IMR} and the moving distance of the trace along selected route as D_R. The following process explains D_{IMR} is shorter than D_R ($D_{IMR} < D_R$).

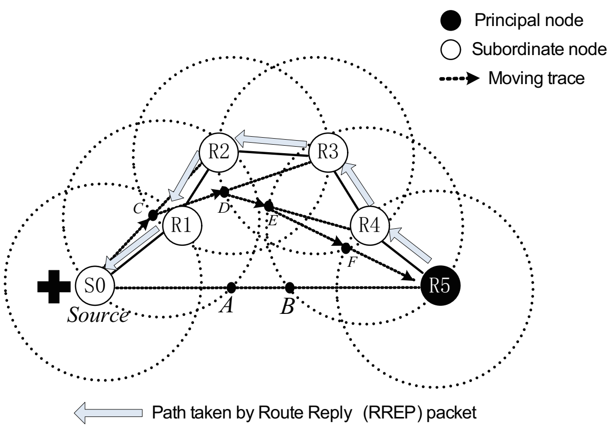


FIGURE 2.5: Iterative Movement to potential selfish/busy Relays (IMR) scheme.

According to our definitions and the *Triangle's Law*, we have the following expression:

$$\begin{cases} \overline{S_0 I_1} + \overline{I_1 R_2} = \overline{S_0 R_2}, \\ \overline{I_i I_{i+1}} + \overline{I_{i+1} R_{i+2}} = \overline{I_i R_{i+2}}. \end{cases}$$
$$\Rightarrow \begin{cases} \overline{S_0 R_2} < \overline{S_0 R_1} + \overline{R_1 R_2}, \\ \overline{I_i R_{i+2}} < \overline{I_i R_{i+1}} + \overline{R_{i+1} R_{i+2}}. \end{cases} \tag{2.15}$$

As the distance between the i_{th} intersection to the $(i+1)_{th}$ relay is equal to the transmission range r, $\overline{I_i R_{i+1}} = r$, we have Eqn. (2.16) from Eqn. (2.15).

$$\begin{cases} \overline{S_0 I_1} + r < \overline{S_0 R_1} + \overline{R_1 R_2} \\ \overline{I_i I_{i+1}} < \overline{R_{i+1} R_{i+2}} \end{cases} \tag{2.16}$$

Furthermore, we have Eqn. (2.17), as the distance between the $(k-1)_{th}$ relay to the k_{th} relay is no more than r, that is $\overline{R_{k-1} R_k} \leq r$.

$$\begin{aligned} &\overline{S_0 I_1} + r + \sum_{i=1}^{k-1} \overline{I_i I_{i+1}} \\ &< \overline{S_0 R_1} + \overline{R_1 R_2} + \sum_{i=1}^{k-1} \overline{R_{i+1} R_{i+2}} \\ &\Rightarrow D_{IMR} < D_R. \end{aligned} \tag{2.17}$$

The difference between the SCAN scheme and the ISCAN scheme is the moving trace of the source node in the last phase. In the ISCAN scheme, it ensures network connectivity by iterative and conscious movement of the source node. However, it takes time to convergence and the overhead of IMR scheme is more than DMR scheme as it needs more location information.

2.6 Performance Evaluation

We firstly consider typical wireless ad hoc networks with 50 to 350 wireless nodes randomly or grid located over a $1200m \times 300m$ rectangular flat space. We firstly evaluate the efficiency of our constructed dependency graph. Then we conduct a performance evaluation and make a comprehensive comparison with the well-known AODV protocol using a computer simulation. Emergency cases are randomly emerged among all nodes. Lastly, we compare our proposed SCAN and ISCAN networking schemes in the purpose of supporting different emergency services. The simulation is implemented using ns-2.33 [15].

2.6.1 Performance Metrics

To evaluate the generality of our classification in node category in a randomly deployed WANET, we calculate the percentage of subordinate nodes. To evaluate the efficiency of our model in investigating congestion and non-cooperation, we calculate the success ratio when applying our constructed dependency graph to detect the potential selfish/busy nodes compared with the real cases in simulation.

According to [25], packet drop ratio and average end-to-end delay are the main metrics to evaluate the WANETs for emergency services. Furthermore, we calculate the throughput and network lifetime to evaluate the network performance while applying our networking schemes.

To evaluate the advantages of each networking scheme, we compare our proposed SCAN and ISCAN schemes by calculating the probability of unconnectivity and average routing load for each of them.

The scenarios is repeated twenty times and the average result was presented with a 95% confidence interval.

2.6.2 Experimental Results

- **Efficiency of the Constructed Dependency Graph**

In Fig. 2.6, we calculate the percentage of subordinate nodes in randomly and grid located scenarios. From our analysis and simulation results, we find that the ratio of subordinate nodes is decreasing with the growth of network size, as there are more mutual dependency relations in a large scale network and the number of nodes without mutual dependency becomes less and less.

In Fig. 2.7, we calculate the success ratio when applying our dependency graph construction process to detect the potential selfish/busy nodes compared with the real cases in simulations. The set up time of constructing the dependency graph differs from 5s to 100s. Our model presents more than 80% correctness when the set up time is large enough (100s).

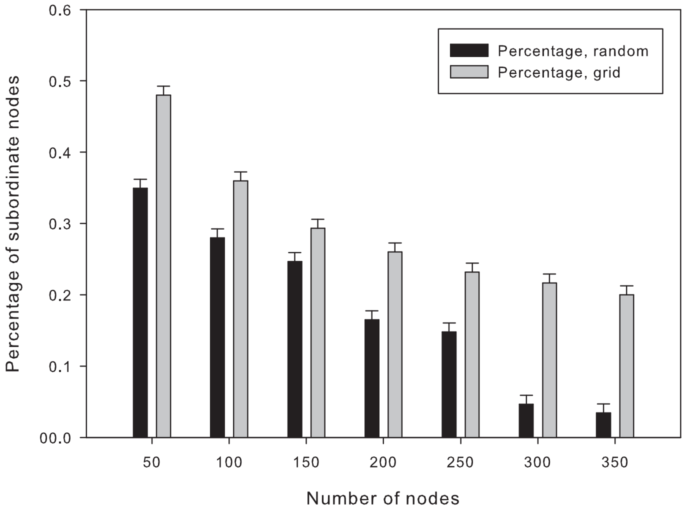


Figure 2.6: Percentage of subordinate nodes in randomly deployed scenarios.

- **Efficiency of the Proposed Networking Schemes**

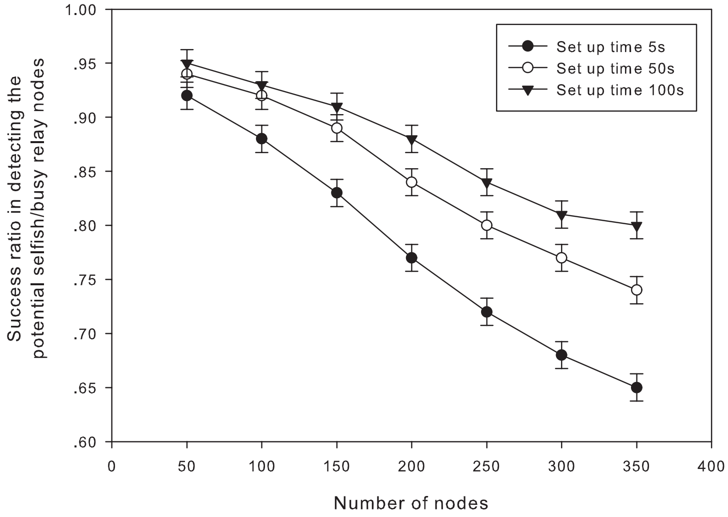


Figure 2.7: Success ratio in detecting congestion and noncooperation.

Table 2.3: Simulation parameters for the evaluated WANETs

Simulator	NS-2.33
Number of nodes	30
Simulation area	$1200 \times 300m^2$
Simulation time	900 seconds
Emergency cases	10 cases, randomly locate
Transmission range	200 meters
Traffic	30 CBR connections, 8 packets/second

Table 2.3 shows the simulation parameters in this subsection. In Fig. 2.8, we show the different performance comparison of the variations of the proposed networking schemes (i.e., SCAN and ISCAN) with the AODV protocol. This figure presents the simulation results in which the moving nodes' average speed changes. As AODV does not consider the movement of emergency nodes, we take the average results of AODV protocol and it is shown as constant values in the figures.

From Fig. 2.8(a)-2.8(c), we find that the proposed SCAN and ISCAN schemes achieve higher throughput, less packet drop ratio and less end-to-end delay comparing with the AODV routing protocol. SCAN performs better than ISCAN and AODV. As the moving node's speed increases, it can replace the selfish/busy relay more quickly, the advantages of SCAN scheme is obvious in such cases.

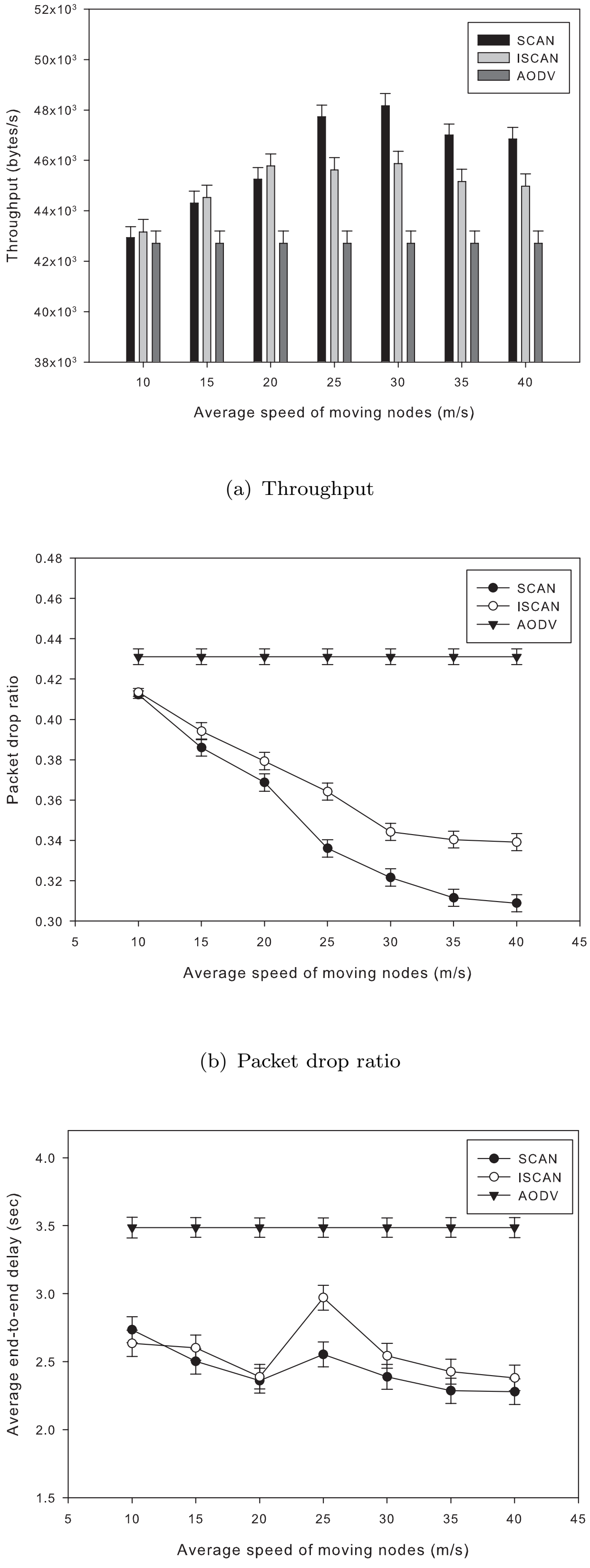
In Fig. 2.9(a), we compare the proposed SCAN and ISCAN networking schemes with AODV by calculating the network lifetime over different number of nodes. In our proposed frameworks, we take the average speed of moving nodes as $20m/s$ and the stay time in selfish/busy nodes as 300sec. Notice that our simulation time is $900sec$, the network lasts to the end of simulation when the amount of nodes is 50. The network lifetime of SCAN and ISCAN schemes is longer than AODV when the number of nodes is large, which indicates good performance with a higher network load.

In Fig. 2.9(b), we compare the probability of unconnectivity for SCAN and ISCAN. ISCAN scheme is better than SCAN scheme as it ensures connectivity by iterative movements. We also compare the routing load of SCAN and ISCAN schemes in Fig. 2.9(c), the routing overhead of SCAN is less than ISCAN as IMR scheme contains more location information than DMR scheme.

The simulation results reveal that our proposed SCAN and ISCAN networking schemes significantly improve the network performance by the cognitive movement of emergency nodes themselves and they are more efficient than the well-known AODV protocol for the emergency services in WANETs.

2.7 Summary

This chapter focuses on promoting energy-efficient and congestion-aware communication for emergency services in WANETs using self-supported schemes. The main contribution of this chapter is addressing self-supported and congestion-aware networking (SCAN) scheme for emergency services in WANETs. We model network congestion and non-cooperation behaviors according to the relations between nodes in the constructed dependency graph. Then we propose an energy-efficient and congestion-aware routing protocol for emergency services in WANETs. Based on the model and routing protocol, we design cognitive movement schemes for urgent sources to supported themselves and to avoid congestion and non-cooperation. Through analysis and simulation, we show that our approaches significantly achieve better network performance and typically satisfy the requirements for emergency services in WANETs. As the future work, we will consider more mobile scenarios and promote efficient networking schemes for emergency services.

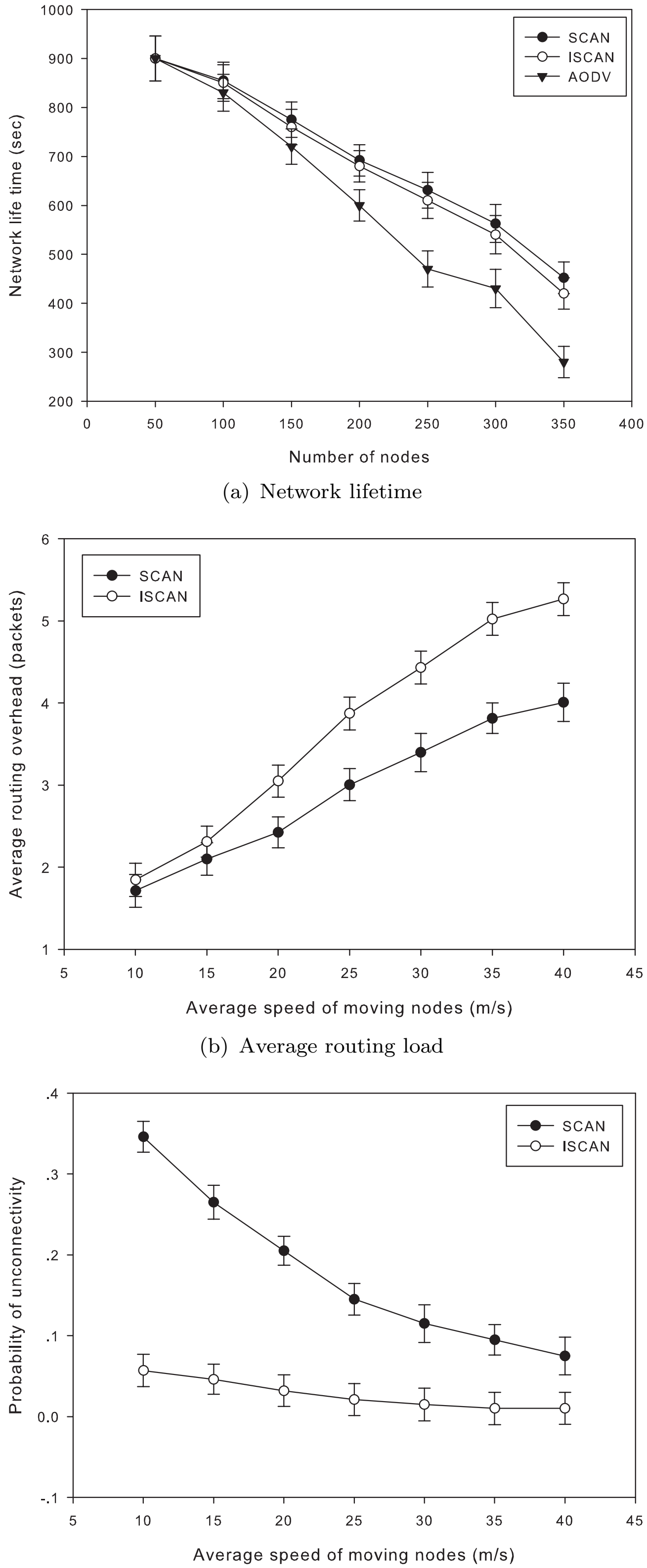


(a) Throughput

(b) Packet drop ratio

(c) Average end-to-end delay

Figure 2.8: Efficiency of the proposed networking schemes.



(a) Network lifetime

(b) Average routing load

(c) Probability of unconnectivity

Figure 2.9: Comparison of the proposed SCAN and ISCAN networking schemes.

Chapter 3

Self-supported Networking for Cooperative Multi-hop Wireless Networks

Cooperative communication (CC) is a promising approach which can offer significant enhancements in multi-hop wireless communications. This chapter investigates the potential issues in using this communication paradigm to support emergency services. We focus on promoting energy-efficient and congestion-aware cooperative networking for emergency services based on the idea of Do-It-Yourself. We propose a novel cross-layer design which jointly considers the problems of route selection in network layer, congestion and non-cooperation avoidance among multiple links in MAC layer under cooperative multi-hop wireless environments. We formulate the multi-hop cooperative flow routing and relay node selection process as an optimization problem. Based on the formulations and models, we propose a self-supported networking scheme including three novel components that make the solution procedure highly efficient. Analysis and simulation results show that our approaches significantly achieve better network performance and typically satisfy the requirements for emergency services in multi-hop wireless networks.

This chapter is organized as follows. Section 3.1 introduces the motivation of the self-supported networking for cooperative multi-hop wireless networks. Section 3.2 briefly surveys the related work. In Section 3.3, we describe our system model and introduce the basic concepts of cooperative communication. We formulate the multi-hop cooperative flow routing and relay node selection problem, characterize our cross-layer optimization in Section 3.4. We propose our self-supported based solution procedure in Section 3.5. In Section 3.6, we evaluate the performance of our proposed approaches through simulations. Section 3.7 concludes this chapter.

3.1 Introduction

Public safety organizations increasingly rely on wireless technology to provide effective communications during emergency operations such as earthquake reliefs, fire rescues or traffic accidents. One of the challenging issues for supporting emergency services in wireless networks is coordinating the network under emergency situations. It is often noticed that, without coordination between users, this may lead to inefficient use of the network resources by increasing congestion, as well as affect the network connectivity because of the noncooperative behaviors of some selfish users.

Cooperative Communication (CC), which exploits the wireless broadcast advantage and the relaying capability of other cooperative nodes, could provide significant performance enhancements in terms of spatial diversity, increased capacity and improved reliability in wireless networks. The uprising benefits of CC motivate us to investigate the potential issues in using this communication paradigm to support emergency services. On one hand, CC could provide potential capacity improvement which is critical to emergency communications. On the other hand, CC can reduce the end-to-end transmission delay and improve the probability of emergent information reception by implementing in a set of coordinated cooperative nodes.

In this chapter, we study the potential issues in using cooperative communication paradigm to support emergency services. We design a novel cross-layer networking scheme which focuses on promoting energy-efficient and congestion-aware cooperative networking based on the idea of **Do-It-Yourself**. The objectives of our networking scheme are twofold: (1) at the network layer, through optimal relay node selection to minimize the cost of multi-hop cooperative flow routing; (2) at the MAC layer, maximize the minimum flow rate (or throughput) among all active emergency sessions, as well as avoid congestion and non-cooperation behaviors. To formulate the problem, we introduce the concept of *dependency* *graph* to reflect a connected network. Then we develop a mathematical characterization for multi-hop flow routing and relay node selection process. For the first objective, we formulate the cost of data links and traffic flows in a CC aware network as a minimization problem. For the second objective, we formulate the flow rate problem based on multi-hop cooperative routing and relay node selection. Then we model network congestion and non-cooperation behaviors according to the formulations. To solve the formulated problems, we combine the two subproblems into a *mixed integer linear programming* (MILP) problem. Then we develop a self-supported based solution procedure to reduce the solution space. Our proposed Self-supported Cooperative Networking (SCooN) scheme includes three novel components which make the solution procedure highly efficient. First, we construct the dependency graph and complete the nodes classification. Then we design an energy-efficient cooperative routing protocol. Thirdly, after investigating the locations of congestion and non-cooperation, sources and relays support themselves by cognitive movements. Simulation results show that our approaches significantly achieve better network performance and typically satisfy the requirements for emergency services in multi-hop wireless networks.

The main contributions of this chapter are summarized as follows:

- The concept of self-supported networking introduced in this chapter is the first to investigate the problem of CC aware networking for emergency services in multi-hop wireless networks.
- We jointly consider the problems of route selection in network layer, congestion and non-cooperation avoidance among multiple links in MAC layer under cooperative aware environments.
- We formulate the multi-hop flow routing and relay node selection process into an optimization problem, develop a self-supported based cooperative networking scheme that make the solution procedure highly efficient.

3.2 Related work

Mainly, recent research on cooperative protocols could be classified into two categories: (1) CC protocols at the physical layer [17], [18], [19], [20]; (2) route selection and relay node assignment related cooperative protocols at the network layer [21], [22], [23], [24]. At the physical layer, various cooperative diversity protocols were proposed to exploit the wireless broadcast advantage and the relaying capability of other cooperative nodes. Authors in [17] and [18] make an in-depth investigation on the practical issues of implementing user cooperation in a conventional CDMA system, which have significant influence to the later research. Gurewitz [19] and Savazzi [20] study multi-hop cooperative protocols which involve cooperation among multiple transmitting nodes along the path. The physical layer property significantly affects the cooperative routing process at the network layer, i.e., route selection problem and relay assignment problem under CC aware environments. At the network layer, the cooperative routing makes use of two facts: the Wireless Broadcast Advantage (WBA) in the broadcast mode and the Wireless Cooperative Advantage (WCA) in the cooperative mode. In the broadcast mode each node sends its data to more than one node, while in the cooperative mode many nodes send the same data to the same destination. Scaglione *et al.* [21] propose two cooperative architectures for multi-hop mobile ad hoc networks. However, there still exists many problems in their work such as optimal routing and relay node assignment. Khandani *et al.* [22] study minimum energy routing problem for a single message by exploiting both wireless broadcast advantage and cooperative advantage. Sharma *et al.* [24] studies the relay node assignment problem in a cooperative ad hoc network environment with multiple source-destination pairs and they propose an optimal algorithm for relay node assignment.

J. Zhang and Q. Zhang [23] firstly investigate the problem of CC aware routing in multi-source multi-destination multi-hop wireless networks and address an optimal routing selection protocol called MFCR (Multi-Flow Cooperative Routing). MFCR takes the advantages of CC, both reduces the total transmission power and increases the network performance. However, the MFCR approaches to non-cooperative protocol when the network congestion emerges (e.g. when emergency cases happen). We illustrate the problems in traditional cooperative routing strategies which do not consider the link congestion among multiple flows in multi-hop wireless networks in Fig. 3.1, where source node S_1 and S_2 transmit to their respective destinations D_1 and D_2 simultaneously. The routes between S_1 and D_1 are $S_1 \rightarrow (R_1, R_4) \rightarrow (R_2, R_3) \rightarrow (R_3, D_1) \rightarrow D_1$. The routes between S_2 and D_2 are $S_2 \rightarrow (R_4, R_6) \rightarrow (R_5, R_7) \rightarrow D_2$. These two data flows will interfere with each other in R_4 as it cannot receive message from two individual data flows simultaneously and decode it correctly. In this chapter, we will compare with the MFCR scheme to show the efficiency of our proposed networking scheme to support emergency services.

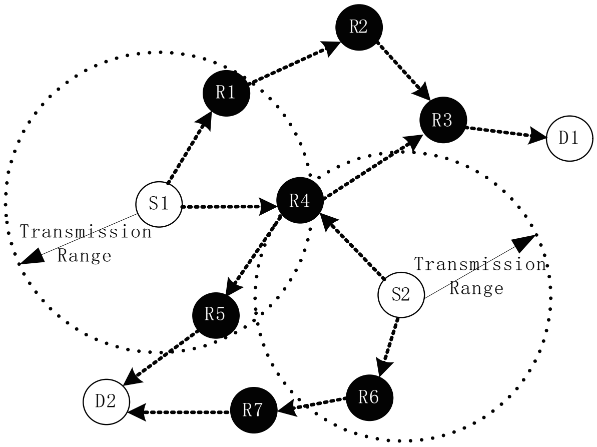


FIGURE 3.1: Illustrative example of traditional cooperative routing strategies.

A large body of applications exist in using wireless networks for emergency services [25], [26], [27] [28]. To the best of our knowledge, our work is the first to study the problems in using cooperative networking for emergency services. Furthermore, there is not any related work comprehensively considering the problems of network congestion and non-cooperation while exploiting wireless networking under emergent situations. Many congestion control methods have been proposed from single-layer to cross-layer prospect [29], [30], [31]. However, as far as we know, few of them focuses on distributed congestion control mechanisms as well as the probability that congestion could be avoided by the effort of network components themselves. Recent research in cooperation problems of wireless networks mainly focus on developing incentive based mechanisms [32], [33], [34], as well as investigating the potentiality of natural cooperation [35], [36], [37]. Most of them do not consider the requirements of emergency services under cooperative aware environments.

3.3 System Model and Preliminaries

Consider a wireless ad hoc network (WANET) consisting arbitrarily distributed nodes where each node is equipped with a single omnidirectional antenna and could use multi-hop cooperative transmission to communicate. We model a WANET for emergency services with a graph $G = (V, E)$. Here V is a set of network nodes and E is a set of all directed links $\langle v_i, v_j \rangle$ where $v_i, v_j \in V$. The link $\langle v_i, v_j \rangle$ exists if the transmission power of node i to node

j, P_{ij} in watt, is more than or equal to $\beta \cdot d_{ij}^{\alpha}$ (i.e., $P_{ij} \geq \beta \cdot d_{ij}^{\alpha}$), where β is the transmission quality parameter, d_{ij} is the Euclidean distance between node i and node j, and α is the distance-power gradient [13]. There are n source nodes forming the source set S = {s_1, s_2,..., s_n} and the corresponding destination nodes set is D = {d_1, d_2,..., d_n}. Denote a path connecting the ordered pair $\omega = (s_i, d_i)$ a sequence of links $\langle v_1, v_2 \rangle, \langle v_2, v_3 \rangle, ..., \langle v_{n-1}, v_n \rangle$ where $v_1, v_2, ..., v_n$ are distinct nodes, $v_1 = s_i$ and $v_n = d_i$. The ordered pair $\omega = (s_i, d_i)$ is also called a flow along a route from source node s_i to destination node d_i. We denote a link $\langle v_i, v_{i+1} \rangle$ serves a flow ω as $\langle v_i, v_{i+1} \rangle \in \omega$.

For all nodes $i \in V$, let the initial energy be E_i and residual energy be $\bar{E_i}$ in joule. An emergency case is denoted by $Emg_i(t)$, where i is the wireless node detecting the emergency case and t is the time when it happens. We assume that each emergency session have different priority level, denoted by PL_j.

3.3.1 Physical Layer Model

Consider the wireless channel between transmitter node i and receiver node j, we denote α_{ij} as the power attenuation factor of the channel, and φ_{ij} as the channel phase delay which is estimated by the receiver node j and send back to the transmitter node i. It is assumed that a free space propagation model is applied, under which the power attenuation α_{ij}^2 is proportional to the inverse of the square of d_{ij}. For the physical layer transmission mechanism, according to [24], any solution procedure designed for **Amplify-and-Forward (AF)** can be readily extended for **Decode-and-Forward (DF)**. In this chapter, we choose DF mode as the physical layer transmission mechanism. For the receiver model under CC environment, we assume that the received information can be decoded with no errors if the received SNR level is greater than the minimum threshold SNR_{th}. Otherwise, no information is received.

It is assumed that the information is encoded in a signal $\delta(t)$ which has the unit power $P_\delta = 1$. We also assume that we can control the phase and magnitude of the signal by multiplying it by a complex scaling factor γ_i before transmission. As a result, the transmitted power by node i is $|\gamma_i|^2$. We denote the noise signal at the receiver as $\eta(t)$ and the power of noise as P_η. Without loss of generality, we also assume the noise at the receiver is to be additive.

3.3.2 The Concept of Dependency Graph

In order to analyze the directed communication between distinct nodes in the interactive topology during a set up period Δt, we describe it by a directed graph [32]. In a defined WANET, each source node might depend on many intermediate nodes while transmitting to its destination. We represent the dependency relations in the network by **Dependency Graph** (DG).

Definition 3.3.1 (**Dependency Graph**). A dependency graph $G' = (N, L)$ is a diagram of the set of vertexes and edges. Each vertex v_i in set N corresponds to a node and L is the set of all directed edges. There is a directed edge from vertex v_i to v_j, denoted by the ordered pair $\langle v_i, v_j \rangle$, if there exists a route where v_i is the relay node of source node v_j. Intuitively, an edge $\langle v_i, v_j \rangle$ means that node v_j depends on node v_i while forwarding packets to its destination.

Notice that the dependency between nodes can be mutual. Especially for the nodes at the center of the network, this mutual dependency is common. We define such mutual dependency as *dependency loop*.

Definition 3.3.2 (**Dependency Loop**). A dependency loop is a sequence of edges $\langle v_1, v_2 \rangle$, $\langle v_2, v_3 \rangle$, ..., $\langle v_{j-1}, v_j \rangle$ in the dependency graph, where $v_1, v_2, ..., v_j$ are distinct nodes and the first node v_1 is same as the last node v_j, $v_1 = v_j$.

As discussed in Chapter 2, in the dependency graph G' of a network, there are nodes in dependency loops and nodes that are not in dependency loops. According to the dependency graph with dependency loops, we classify the nodes into *principal* nodes and *subordinate* nodes. Details of the definitions of these two types of nodes can be found in the last chapter or in our previous work [38].

3.3.3 Transmission Model

In a cooperative communication (CC) aware WANET, there are typically three types of transmission mode: (a) **ordinary mode**: information is transmitted from a single node and received by a single receiver; (b) **broadcast mode**: information is transmitted from a single node and received by multiple receivers; (c) **cooperative mode**: multiple intermediate nodes cooperatively transmit the information to a single receiver. In the next section, we will develop mathematical characterizations for the link cost, flow cost and flow rate under cooperative environments. In a CC-aware WANET, there are two types of relay nodes: Cooperative Relay (CR) for CC purpose and Traditional Relay (TR) for traditional multi-hop relaying. Due to the physical limitations of CC, a relay can serve as either CR or TR based on the system purpose but not both at the same time. Similar as [24], we only consider at most one relay node for CC between each link (transmitter and receiver pair). Furthermore, a source node (or a destination node) cannot be selected as a CR but can be selected as a TR.

Table 3.1 lists the frequently used notations in this chapter. Besides, we have the following assumptions:

- We assume for the moment that each node is the source of only one route.
- We assume all the nodes have the same relaying capability and a relay cannot generate its own traffic flow while acting as CR or TR.
- A source node (or a destination node) can be selected as a TR but cannot be selected as a CR.
- Multiple nodes cooperating in sending the information to a single destination can accurately time their transmitted signal to achieve perfect phase synchronization at the destination.

3.4 Problem Formulation and Cross-layer Optimization

In this section, we propose a novel cross-layer design which jointly considers the problems of route selection in network layer, congestion and non-cooperation avoidance among multiple links in MAC layer under cooperative multi-hop wireless environments. First we will formulate the relay node selection process and flow routing which affect the achievable flow rate as an optimization problem.

3.4.1 Link Cost, Flow Cost and Flow Rate Formulation

- **Link Cost Formulation**

Table 3.1: List of notations in Chapter 3.

Symbol	**Definitions**
E_i	initial energy of node v_i
$\bar{E}_i$	residual energy of node v_i
$Emg_i(t)$	event detected by node v_i
PL_i	priority level of $Emg_i(t)$
OD_i,ID_i	out-degree and In-degree of node v_i
ON_i,IN_i	outside and Inside nodes set of nodev_i
$OD(L_i)$,$ID(L_i)$	out-degree and In-degree of L_i
$ON(L_i)$,$IN(L_i)$	outside and Inside nodes set of L_i
$\|N\|$	number of nodes in DG $G' = (N, L)$
$\|L_i\|$	number of nodes in L_i
N_p	principal nodes set in DG
N_s	subordinate nodes set in DG
$LC(T_i, R_i)$	link cost from T_i to R_i
$FC(S_i, D_i)$	flow cost from S_i to D_i
$f_{kl}(s_i)$	flow rate on link $\langle v_k, v_l \rangle$
$FR(s_i, d_i)$	end-to-end flow rate of pair (s_i, d_i)
$C_{DF}(v_k, \Upsilon_p, v_l)$	capacity of link $\langle v_k, v_l \rangle$
$C_D(v_k, v_l)$	capacity of link $\langle v_k, v_l \rangle$
$\mathbb{U}_{ij}^k$	binary variable
$\mathbb{V}_{ij}$	binary variable
V_i	living value of node v_i
U_{r_k}	utility of route r_k
$C_{hops}^{r_k}$	number of hops along r_k
$C_p^{r_k}$	number of principal nodes in r_k

In this subsection, we first specify the link cost (LC) for transmitting in a certain link i, denoted by $LC(T_i, R_i)$, which is defined as the minimum power for transmitting from the a node in transmitter set $T_i = \{t_1, t_2,...,t_n\}$ to a node in receiver set $R_i = \{r_1, r_2,...,r_n\}$ of link i. According to [22], the value of LC is derived from the three distinct transmission modes.

Ordinary mode: point-to-point link. In this case, $T_i = \{t_1\}$ and $R_i = \{r_1\}$. The received signal at the receiver node is expressed as $\gamma(t) = \alpha\gamma e^{j\varphi}\delta(t) + \eta(t)$. The transmitted power by the transmitting node is $P_t = |\gamma_i|^2$. The SNR ratio at the receiver is $\frac{P_t\alpha^2}{P_\eta}$. In order to accurately decode the signal, the SNR ratio at the receiver must be no less than

SNR_{th}. Therefore, the link cost is given by:

$$LC(T_i, R_i) = LC(t_1, r_1) = \frac{P_\eta SNR_{th}}{\alpha^2}. \tag{3.1}$$

Broadcast mode: point-to-multipoint link. Under the broadcast mode, $T_i = \{t_1\}$ and $R_i = \{r_1,\ r_2,...,r_m\}$, where $m < n$. In this case, m simultaneous SNR constraints must be satisfied at the receiver. Hence, the cost of the power needed for transmitting from T_i to R_i is the maximum over the cost for reaching each of the nodes in the receiver set. LC is given as follows.

$$\begin{aligned} &LC(T_i, R_i) = LC(t_1, r_i) \\ &= \max\left\{LC(t_1, r_1), LC(t_1, r_2), ..., LC(t_1, r_m)\right\}, \end{aligned} \tag{3.2}$$

where $LC(t_1, r_i)$ $(i = 1, 2, ...m)$ is given by Eqn. (3.1).

Cooperative mode: multipoint-to-point link. Under the cooperative mode, T_i $= \{r_1,\ t_2,...,t_m\}$ and $R_i = \{r_1\}$. In this case, m sources cooperatively transmit the same information to a single receiver. According to our assumptions, the signals simply add up at the receiver. Hence, the signal at the receiver is $\gamma(t) = \sum\limits_{i=1}^{m} \alpha_{i1} \left|\gamma_i\right| \delta(t) + \eta(t)$. The transmitted power by the transmitting nodes is $\sum_{i=1}^{m} \left|\gamma_i\right|^2$. The SNR ratio at the receiver is $\frac{\left|\sum_{i=1}^{m} \alpha_{i1}\gamma_i\right|^2}{P_\eta}$. To calculate the minimum power for transmitting from T_i to R_i equals solving the following optimization problem.

$$\begin{aligned} &\min \textstyle\sum_{i=1}^{m} \left|\gamma_i\right|^2 \\ &\text{subject to } \frac{\left|\sum_{i=1}^{m} \alpha_{i1}\gamma_i\right|^2}{P_\eta} \geq SNR_{th}. \end{aligned} \tag{3.3}$$

According to [22], the Lagrangian multiplier techniques could be used to solve the above optimization problem. The optimal transmitting power for each node i is $\left|\gamma_i\right| = \frac{\alpha_{i1}}{\sum_{i=1}^{m} \alpha_{i1}{}^2} \sqrt{P_\eta SNR_{th}}$. The resulting link cost under cooperative mode is given by:

$$LC\left(T_i, R_i\right) = \sum\nolimits_{i=1}^{m} \left|\gamma_i\right|^2 = \frac{1}{\sum_{i=1}^{m} \frac{\alpha_{i,1}{}^2}{P_\eta SNR_{th}}} = \frac{1}{\frac{1}{LC(t_1,r_1)} + \frac{1}{LC(t_2,r_1)} + ... + \frac{1}{LC(t_m,r_1)}}. \tag{3.4}$$

- **Flow Cost Formulation**

We introduce the flow cost (FC) to specify the cost along a route from the source to the destination of a flow. It is defined as the minimum power needed for transmitting information along any route from the source to the destination of the flow, which is given by:

$$\begin{aligned} &FC(S_j, D_j) = \min_{\langle T_i, R_i\rangle \in \omega_j} \textstyle\sum_{i=1}^{r} LC(T_i, R_i) \\ &\forall R, T_1 = S_j, R_r = D_j, \end{aligned} \tag{3.5}$$

where $FC(S_j, D_j)$ is the flow cost of flow j, ω_j is any path such that the source of the path equals to S_j and the destination equals to D_j. Notice that the calculation of FC has no relations with the transmission modes. As the flow cost is the sum of link cost which is calculated under different transmitting modes.

- **Flow Rate Formulation**

In the following, we consider the achievable flow rate between s_i and d_i in CC environment. Under the Decode-and-Forward (DF) mode, relay nodes first decode and estimate the received signal from source node, and then transmit the estimated data to the destination node. The maximum average mutual information for DF can be readily shown in Eqn. (3.6):

$$\begin{aligned} I_{DF}(s_i, \Upsilon_j, d_i) = 1/2 \min\{&\log_2(1 + SNR_{s\Upsilon}), \\ &\log_2(1 + SNR_{sd} + SNR_{\Upsilon d})\}, \end{aligned} \tag{3.6}$$

where $SNR_{s\Upsilon} = \frac{P_s|\alpha_{s\Upsilon}|^2}{P_\eta}$, $SNR_{sd} = \frac{P_s|\alpha_{sd}|^2}{P_\eta}$, $SNR_{\Upsilon d} = \frac{P_\Upsilon|\alpha_{\Upsilon d}|^2}{P_\eta}$. Specifically, we require the relay to fully decode the source message, the first term in Eqn. (3.6) represents the maximum rate at which the relay can reliably decode the source message. Also, we require the destination to perfectly decode the message from the source and relay, the second term in Eqn. (3.6) represents the maximum rate at which the destination can reliably decode the source message given repeated transmissions both from the source and relay. Given B as the available bandwidth of channels at nodes s_i and d_i, the achievable rate under DF mode could be given by:

$$FR_{DF}(s_i, \Upsilon_j, d_i) = B \cdot I_{DF}(s_i, \Upsilon_j, d_i). \tag{3.7}$$

3.4.2 Route Selection and Relay Node Assignment at the Network Layer

According to our system model, there are $|N| - 2n$ nodes forming the relay nodes set $R = \{\Upsilon_1, \Upsilon_2, ...\Upsilon_{|N|-2n}\}$. We introduce a binary variable $\mathbb{U}_{ij}^k$ to characterize whether an available relay node k is used as CR on link $\langle v_i, v_j \rangle$ or not:

$$\mathbb{U}_{ij}^k = \begin{cases} 1, & if\ node\ k\ is\ used\ as\ CR\ on\ link\ \langle v_i, v_j \rangle \\ 0, & otherwise \end{cases} \tag{3.8}$$

We also introduce another binary variable $\mathbb{V}_{ij}$ to characterize whether the link between node i and node j exists or not:

$$\mathbb{V}_{ij} = \begin{cases} 1, & if\ link\ \langle v_i, v_j \rangle\ exists \\ 0, & otherwise \end{cases} \tag{3.9}$$

Either a relay node k is used as TR or CR, the number of data links entering node k should be equals to the number of data links exiting it. This constraint is given by **Constraint (1)**, as expressed in Eqn. (3.10):

$$\sum\nolimits_{v_i \in V}^{i \neq k} \mathbb{V}_{ik} = \sum\nolimits_{v_j \in V}^{k \neq j} \mathbb{V}_{kj}, \gamma_k \in R. \tag{3.10}$$

For a relay node k, it could be assigned to link $\langle v_i, v_j \rangle$ only if this link exists. This constraint is given by **Constraint (2)**, as expressed in Eqn. (3.11):

$$\mathbb{V}_{ij} - \sum\nolimits_{v_k \in V}^{i \neq k, j \neq k} \mathbb{U}_{ij}^k \geq 0, v_i, v_j \in V (i \neq j). \tag{3.11}$$

3.4.3 Flow Routing at the MAC Layer

According to our assumptions, we limit the source (or destination) of a flow to be a single node. Furthermore, we assume that there is at most one CR for each link. These two statements could be specified by the following **Constraint (3)**, as expressed in Eqn. (3.12) and Eqn. (3.13):

$$\sum\nolimits_{v_j \in V}^{s_i \neq v_j} \mathbb{V}_{ij} = 1, s_i \in S \quad \sum\nolimits_{v_i \in V}^{d_j \neq v_i} \mathbb{V}_{ij} = 1, d_j \in D, \tag{3.12}$$

$$\sum\nolimits_{v_k \in V}^{i \neq k, j \neq k} \mathbb{U}_{ij}^{k} \leq 1, v_i, v_j \in V (i \neq j). \tag{3.13}$$

The data flow transmitted from node i to node j in bits per second is denoted by f_{ij}. At any node i, which is neither source nor destination, the flow-in should equal to the flow-out. For node $i \in S$, the flow-out should equal to the flow-in plus the throughput requirement Q_i. For node $i \in D$, the flow-out should equal to the flow-in minus Q_i. The conservative relation of data flow is defined formally as **Constraint (4)**, as expressed in Eqn. (3.14):

$$\sum_{\langle v_i, v_j \rangle \in E} f_{ij} - \sum_{\langle v_k, v_i \rangle \in E} f_{ki} = \begin{cases} Q_i & \text{if } \ v_i \in S, \\ -Q_i & \text{if } \ v_i \in D, \\ 0 & \text{otherwise.} \end{cases} \tag{3.14}$$

For a given communication session (s_i, d_i), denote $f_{kl}(s_i)$ as the flow rate on link $\langle v_k, v_l \rangle$ that is attributed to the source-destination pair (s_i, d_i), denote the end-to-end flow rate (or throughput) as $FR(s_i, d_i)$, where $FR(s_i, d_i) = \sum_{v_k, v_l \in V}^{v_k \neq v_l} f_{kl}(s_i)$. We denote the minimum flow rate among all sessions as $FR_{\min}$, then we have $FR_{\min} \leq \sum_{v_k, v_l \in V}^{v_k \neq v_l} f_{kl}(s_i), (s_i \in S)$. Our objective is to maximize the minimum flow rate among all sessions, which is given by:

$$\text{maximize} \quad FR_{\min} = \underset{s_i \in S}{\text{maximize}} \quad \min \sum\nolimits_{v_k, v_l \in V}^{v_k \neq v_l} f_{kl}(s_i). \tag{3.15}$$

We should also consider the capacity constraint on each hop in the network, i.e. the flow rates on link $\langle v_k, v_l \rangle$ must not exceed the link capacity. This constraint is given by **Constraint (5)**, as expressed in Eqn. (3.16):

$$\sum\nolimits_{s_i \in S}^{v_k \neq s_i} f_{kl}(s_i) \leq C_{DF}(v_k, \Upsilon_p, v_l) + C_D(v_k, v_l), \tag{3.16}$$

where $C_{DF}(v_k, \Upsilon_p, v_l)$ is the link capacity under Cooperative Mode (using DF physical mechanism) and $C_D(v_k, v_l)$ is the link capacity under Ordinary Mode (using Direct Transmission mechanism), $FR_D(v_k, v_l)$ is the achievable flow rate under direct transmission and $FR_D(v_k, v_l) = B \cdot \log_2(1 + SNR_{kl})$. The relations between them are can be expressed as follows:

$$\begin{aligned} C_{DF}(v_k, \Upsilon_p, v_l) &= FR_{DF}(v_k, \Upsilon_p, v_l) \sum\nolimits_{\Upsilon_p \in R}^{v_k \neq \Upsilon_p, v_l \neq \Upsilon_p} U_{kl}^{p} V_{kl}, \\ C_D(v_k, v_l) &= FR_D(v_k, v_l)(1 - \sum\nolimits_{\Upsilon_p \in R}^{v_k \neq \Upsilon_p, v_l \neq \Upsilon_p} U_{kl}^{p}) V_{kl}. \end{aligned} \tag{3.17}$$

3.4.4 Congestion and Non-cooperation Modeling

In a multi-hop WANET, if there are more nodes rely on a node than it relies on, congestion may occur. According to the dependency graph, while the outdegree OD_i of a node v_i is larger than its indegree ID_i, node v_i might be in congestion status:

$$OD_i - ID_i > 0,\ if\ v_i \in N_s. \tag{3.18}$$

For the nodes in dependency loops, they are more potential to be in congestion status. The conservative relation of congestion is defined formally as follows:

$$\sum_{L_i \in L, v_i \in L_i} OD(L_i) - \sum_{L_i \in L, v_i \in L_i} ID(L_i) > |L_i|\ ,\ if\ v_i \in N_p. \tag{3.19}$$

To avoid network congestion, there should be constrains in selecting TR nodes. Furthermore, according to our discussion in the previous section, a single CR which serves more than one transmitter and receiver pair might cost contention. Hence, the constrains in selecting TR and CR nodes are given as the following **Constraint (6)**:

$$\textstyle\sum_{v_j \in V}^{v_i \neq v_j} \mathbb{V}_{ij} \leq 1, v_i \notin S, \textstyle\sum_{v_i \in V}^{v_i \neq v_j} \mathbb{V}_{ij} \leq 1, v_j \notin D, \tag{3.20}$$

$$OD_i - ID_i \leq 0, v_i \in N_s, \tag{3.21}$$

$$\sum_{L_i \in L, v_i \in L_i} OD(L_i) - \sum_{L_i \in L, v_i \in L_i} ID(L_i) \leq |L_i|\ , v_i \in N_p. \tag{3.22}$$

The cooperation problems between nodes with mutual dependency has been solved using repeated game theory [36]. We mainly focus on the non-cooperation behaviors between principal nodes and subordinate nodes as the latter are not in dependency loops. As we addressed before, in a dependency graph, if node v_i relies on v_j but v_j does not rely on v_i, non-cooperation may occur. The conservative of non-cooperation is defined as follow. Therefore, the constrain that serves for avoiding non-cooperation in the relay selection process is given by **Constraint (7)**:

$$\mathbb{V}_{ij} = 1, v_i \notin ON_j, v_j \in ON_i, \tag{3.23}$$

$$\sum\nolimits_{v_i,v_j\in\mathbb{V}}^{j=i+|L_j|}\mathbb{V}_{ij}=|L_j|\,,v_i\notin ON(L_j),v_i\in IN(L_i). \tag{3.24}$$

The above constraints specify the relay node selection process, as well as the congestion and non-cooperation avoidance, which are the main subjects of the following joint optimization formulation.

3.4.5 A Novel Cross-layer Optimization

As we consider supporting emergency services in CC aware multi-hop wireless networks, our objectives of the optimization problem are twofold:

(1) Minimize the sum of link cost and flow cost of the links within two constraints: a) for each flow, select one link to transmit at a certain time slot; b) the links selected for different flows should not interfere with each other. As we choose one cooperative relay for each transmitter-receiver pair, the link cost changes after each relay selection process. Hence, the flow cost of each flow is the power needed in a direct transmission route from the source and destination, which is consisted of point-to-point links. In order to count the cost of all active links using cooperative transmission and the cost of the active flow using other transmissions, we define the objectives as the sum of both costs. This sub-problem could be formulated as the following **minimization** problem:

$$\begin{array}{l}\min\sum\nolimits_{S_j,D_j\in S}^{\langle T_i,R_i\rangle\in(S_j,D_j)}\{LC(T_i,R_i)+FC(S_j,D_j)\}\\ s.t.\quad \text{Constraint}\ \ (1),(2)\end{array} \tag{3.25}$$

(2) Maximize the minimum flow rate (or throughput) among all active sessions via multi-hop cooperative routing and relay node selection within two constraints: a) for each flow, a relay node is selected either as a TR or CR but could not acts both at the same time; b) the selected relay nodes should avoid potential congestion and non-cooperation behaviors in the network. This sub-problem could be formulated as the following **maximization** problem:

$$\begin{array}{l}\max FR_{\min}=\max\limits_{s_i\in S}\min\sum\nolimits_{v_k,v_l\in V}^{v_k\neq v_l}f_{kl}(s_i)\\ s.t.\quad \text{Constraint}\ \ (2),(3),(4),(5),(6),(7)\end{array} \tag{3.26}$$

We combine the two sub-problems together and have the following mixed optimization formulation:

$$\begin{aligned}
&\text{maximize :} \quad \frac{FR_{\min}}{\sum_{S_j,D_j\in S}^{\langle T_i,R_i\rangle\in(S_j,D_j)}\{LC(T_i,R_i)+FC(S_j,D_j)\}} \\
&s.t. \qquad \text{Constraints} \;\; (1)-(7)
\end{aligned} \tag{3.27}$$

It is not hard to notice that this optimization formulation is the form of *mixed integer linear program* (MILP) problem, which is NP-hard. Our objective is to maximize the minimum flow rate while minimizing aggregate routing cost, by allocating the link activeness and relay selection for all links, together with scheduling the flow rate for each link.

3.5 Proposed Self-supported Cooperative Networking (SCooN) Scheme

In the previous section, we formulate the flow routing and relay node selection process under a CC aware multi-hop wireless environment. In order to support emergency services and meet the other critical requirements, we propose our self-supported cooperative networking (SCooN) scheme in this section. The SCooN scheme includes three novel components. In the first subsection, we describe the initialization phase which constructs the dependency graph and completes the nodes classification. We design an energy-efficient and congestion-aware cooperative routing protocol in the second subsection. Thirdly, we propose the *relay-first serve* and *source-first serve* procedures to support multiple instantaneous sessions for emergency services in WANETs.

3.5.1 Initialization

At the initialization phase, we construct the dependency graph of a network during a set up time period Δt, classify the node category (principal/subordinate) for each node.

During the set up time period Δt, each node may act as source or relay. As a source node, it keeps all its relay nodes' identification and calculate how many nodes it relies on. As a relay node, it stores the request information containing the sender nodes' identification and calculate how many nodes rely on it. After the end of Δt, each node has a picture of the dependency relations of itself. With these information of all the nodes, a whole dependency graph of the network is constructed. The algorithm of constructing a dependency graph could be found in the previous chapter. Hence, each node could identify its category (principal/subordinate) according the degree information and dependency relations in the constructed dependency graph.

3.5.2 Route Selection

This subsection introduces our proposed routing protocol and relay node selection process according to the formulations in the last section. Our objective is to maximizing minimum flow rate while minimizing aggregate routing cost, by allocating the link activeness and relay selection for all links, together with scheduling the flow rate for each link.

Our proposed CC aware routing protocol inherits the concepts of Ad-hoc On-demand Distance Vector (AODV) routing protocol [14]. In AODV, a route request message (RREQ) is used to send a route request from the source node by broadcasting it. When the desired destination node receives the RREQ messages, it chooses the best route, i.e. the shortest-hop route, then uses it to send route reply RREP to the source node. The source node then uses this route to send the data.

In the proposed protocol, we use the control message (RREQ and RREP) to avoid extra message overhead. The RREQ message triggers the received nodes to add their node category (principal/subordinate) into the message before forwarding it to other nodes. Then each relay node calculates and adds in this RREQ message its residual living value $V_i = \bar{E}_i/OD_i$, where V_i is proportional to the residual energy $\bar{E}_i$ and inversely proportional to the outdegree OD_i of a node. V_i reflects the possibility that a node is potential to be selfish and busy node.

We define a route from source s to destination d as $R = \{(i_0, i_1), ..., (i_{h-1}, i_h)\}, \forall(i_k, i_{k+1}) \in E$, where $i_0, i_1, ..., i_h$ are distinct nodes, $i_0 = s$, $i_h = d$, and h is the number of hops between source node s and destination node d. Under cooperative transmission, consider a number of m available routes between source node $s \in S$ and destination node $d \in D$. We define U_{r_k} to be a utility value for each route r_k, which considers the living value of the nodes along the route, the hops of the route, the number of selected cooperative relays in the route. The utility of route r_k, with nodes $i_0^{r_k}, i_1^{r_k}, ..., i_h^{r_k}$ is defined as follows.

$$\begin{aligned} U_{r_k} = & \frac{\underset{i_0,i_1,\dots i_h \in r_k}{Min}(V_{i_0},V_{i_1},\dots,V_{i_h})}{(C_{hops}^{r_k}+C_p^{r_k})} \cdot FC_{r_k}(s,d) \\ & \cdot (\tfrac{1}{2} - \textstyle\sum_{l=1}^{l=C_{hops}^{r_k}} \displaystyle\sum_{<v_i,v_j>\in r_k} \mathbb{U}_{ij}^{l}), \end{aligned} \tag{3.28}$$

where $C_{hops}^{r_k}$ is the number of hops along r_k and $C_p^{r_k}$ is the number of principal nodes among r_k. The destination node receives the RREQ messages with these information and calculates the utility value for each of the m available routes according to Eqn. (3.28).

Notice that the value of Eqn. (3.28) can have three cases. It is intuitive to observe that this equation is consisted of three terms. When the first term is 0, it is the first case that U_{r_k} equals to 0. When the third term is greater or less than 0, it falls into the other two cases.

- (1) If $U_{r_k} = 0$, the route r_k contains at least one relay node whose residual energy equals to 0. Hence, this route could not be selected as a cooperative transmission route.
- (2) If $U_{r_k} < 0$, the route r_k contains at least one relay node which has been selected as cooperative relays by other flows. So this route could not be selected as a cooperative transmission route.
- (3) Otherwise, if $U_{r_k} > 0$, all the selected relay nodes among the route r_k have not been selected as cooperative relays by other flows. It also do not contain any relays running out of energy. As a result, this is a normal route and it can be selected as a cooperative transmission route.

After the destination node receives all the RREQ messages from m available routes, it will send back the RREP messages according to the utility value of each route and select the available routes for cooperative transmission. In our proposed schemes, the flow rate is assigned when the transmission mode of each link is determined. The flow rate is assigned according to the capacity **Constraint (5)** under different transmission mode. The destination node also send back a RREP message and triggers those relays which have been running out of their energy or have been used to attach their location information in the RREP message. The following steps describe the core of our SCooN scheme, in which the relays and sources support cooperative transmission through their cognitive movements. Fig. 3.2 describes the main concepts of the relay-first serve procedure and the source-first serve procedure.

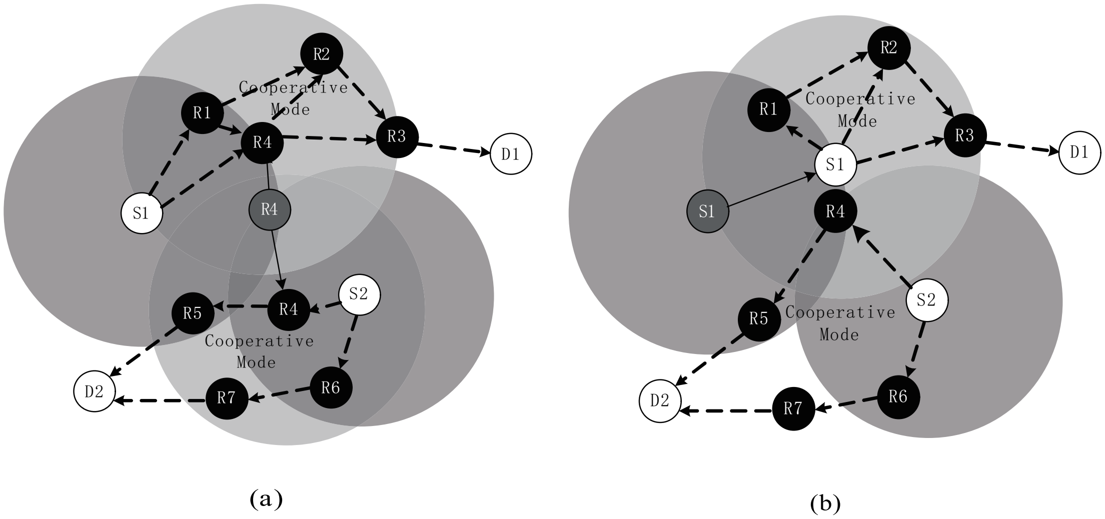


FIGURE 3.2: Illustrative examples: (a) relay-first serve procedure; and (b) source-first serve procedure.

3.5.3 Relay-First Serve: Novel Movement of Relays

The first key idea of our proposed networking scheme is to promote the relay nodes to support themselves by their own efforts. In this subsection, we propose the relay-first serve method according to the priority of different emergency sessions.

We use the sample network in Fig. 3.2(a) to explain the main idea. Suppose there are two emergency sessions in the network: $(S_1 \rightarrow D_1)$ and $(S_2 \rightarrow D_2)$. The priority level of the first session is greater than the second session. After relay node R_4 receives the RREP message from destination D_1, it realizes that the current session has a higher priority than the session it serving. So it moves out of the transmission of S_2 and only act as cooperative relays for session 1. Session 2, as cooperative transmission could not be applied, it only uses ordinary mode for transmission $(S_2 \rightarrow R_6 \rightarrow R_7 \rightarrow D_2)$. In the relay-first serve mechanism, R_4 moves to serve for two different flows and act as cooperative relay each time. Notice that when R_4 serves for the first flow $(S_1 \rightarrow D_1)$, it should move out of the transmission range of S_2 so as to avoid interference.

For a route r_k whose utility value is less than 0, the destination node send back a RREP message along this route containing the priority level of the current session. As r_k contains at least one relay node which has been selected by other flows, we denote this relay as r_{i_p}. After r_{i_p} receives the RREP message, it compares the priority level of the current session PL_j with the session it serving, e.g. PL_i. If $PL_j > PL_i$, r_{i_p} moves to a proper location and serve for the current session. Otherwise, it continues serving as the cooperative relay for its original session. The example in Fig. 3.3 explains the procedure of this method.

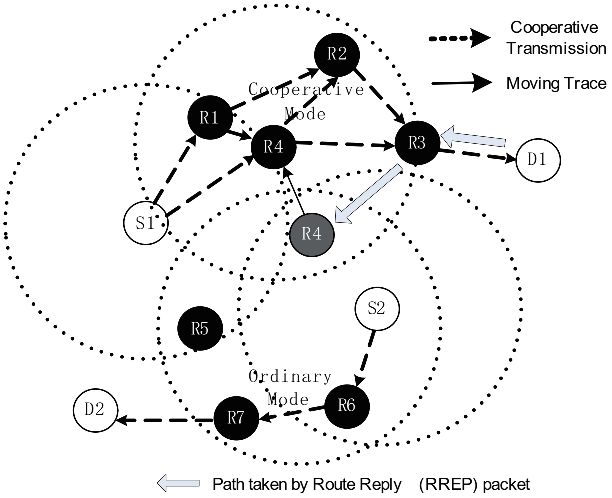


FIGURE 3.3: Relay-first serve procedure: novel movement of the relay node.

3.5.4 Source-First Serve: Novel Movement of Sources

According to Eqn. (3.28), if the utility value of a route r_k equals to 0, r_k contains at least one relay node which is running out of its energy. In order to exploit cooperative communication to supported the emergency sessions, we develop the source-first serve method. This method aims at promoting the sources to novelly replace their potential busy/selfish relay nodes by their movements.

Take the sample network in Fig. 3.2(b) as an example, the source node (i.e. S_1) moves to replace the bottleneck relay (i.e. R_4) and then use cooperative transmission to transmit its data. Hence, the second data flow ($S_2 \rightarrow D_2$) can use R_4 as its relay node and this two flows will not interfere each other.

We firstly propose the Direct Movement to potential selfish/busy Relays (DMR) scheme by explaining how the source node move and replace their potential selfish/busy relays according to the feedback information received from the RREP message.

For a route r_k whose utility value equals to 0, the destination node sends back a RREP message along this route. As r_k contains at least one relay node which has been running out of its residual energy, we denote this relay as r_{i_q}. After r_{i_q} receives the RREP message, it adds the location information of itself in the RREP message and then send back along the route. For simplify, we assume that each route at most contains one node that will exhaust its energy.

After receiving the RREP message from the destination and relay nodes containing the location information of the potential selfish/busy relay nodes along the route, the source node notices the location of this relay node. We set a moving constraint value M_S for all source nodes. When the utility value U_{r_k} of its selected route r_k is less than M_S, our proposed DMR scheme triggers the source node to replace the relay node r_{i_q} directly.

For some emergency services, connectivity and consistency of transmission are more critical. The DMR scheme we proposed is simple and novel. However, it cannot ensure network connectivity during transmission. As a result, we propose another Iterative Movement to potential selfish/busy Relays (IMR) approach as an improvement to the DMR approach. In IMR approach, the RREP message triggers all the relay nodes between source and the most potential selfish/busy relay to append their location information in it. Then the IMR scheme maintains the source nodes to replace their potential selfish/busy relays iteratively.

Details of both the DMR and the IMR scheme have been discussed in Chapter 2 already. Here we exploit them in CC-aware wireless networks to seek for cooperative transmission opportunities. The difference between SCooN-DMR and SCooN-IMR is the moving trace of the source node in the last phase. IMR scheme achieves connectivity by iterative and conscious movement of the source node. However, it takes time to convergence and the overhead of IMR scheme is more than DMR scheme as it needs more location information.

3.6 Performance evaluation

In this section, we will evaluate the performance of our proposed self-supported cooperative networking (SCooN) scheme.

We firstly consider typical wireless ad hoc networks with nodes randomly or grid located over a $1200m \times 300m$ rectangular flat space. We evaluate the efficiency of our constructed dependency graph. Then we conduct a performance evaluation and make a comprehensive comparison with the existing cooperative routing scheme MFCR (Multi-Flow Cooperative Routing) in [23] and Non-Cooperative Routing protocol AODV (NCR-AODV) using a computer simulation. Emergency cases are randomly emerged among all nodes. At last, we compare our proposed SCooN-DMR and SCooN-IMR networking schemes in the purpose of supporting different emergency services. The simulation is implemented using ns-2.33 [15].

3.6.1 Performance Metrics

To evaluate the generality of our classification in node category in a randomly deployed WANET, we calculate the percentage of subordinate nodes. To evaluate the efficiency of our model in investigating congestion and non-cooperation, we calculate the success ratio when applying our networking scheme to detect the potential selfish/busy nodes compared with the real cases in simulation.

Packet drop ratio is computed as the ratio between the dropped packets to total packets sent during the simulation time. End-to-end delay is defined as the time that a packet takes to be transmitted across a network from source to destination. We computed the average delay for all received packets. In this chapter, they are the main metrics to evaluate the WANETs for emergency services. Furthermore, we calculate the throughput to evaluate the network performance while applying our self-supported cooperative networking scheme.

To evaluate the advantages of each networking scheme, we compare our proposed SCooN-DMR and SCooN-IMR schemes by calculating the probability of unconnectivity and average routing load for each of them.

The scenarios is repeated twenty times and the average result was presented with a 95% confidence interval.

TABLE 3.2: Simulation parameters for the evaluated cooperative multi-hop wireless networks

Simulator	NS-2.33
Number of nodes	30
Simulation area	$1200 \times 300m^2$
Simulation time	900sec
Emergency cases	10 cases, randomly locate
Priority Level of Emergency cases	10
Transmission range	200m
Traffic	30 CBR connections, 8 packets/sec

3.6.2 Simulation results

3.6.2.1 Efficiency of the constructed dependency graph

In Fig. 3.4, we calculate the percentage of subordinate nodes in randomly and grid located scenarios. From our analysis and simulation results, we find that the ratio of subordinate nodes is decreasing with the growth of network size, as there are more mutual dependency relations in a large scale network and the number of nodes without mutual dependency becomes less and less.

In Fig. 3.5, we calculate the success ratio when applying the constructed dependency graph to detect the potential selfish/busy nodes compared with the real cases in simulation. The set up time of constructing the dependency graph differs from 5 seconds to 100 seconds. Our model presents more than 80% correctness when the set up time is large enough ($100s$).

3.6.2.2 Efficiency of the proposed networking schemes

Table 3.2 shows the simulation parameters in this subsection. From Fig. 3.6 to Fig. 3.8, we show the performance comparison of the variations of our proposed SCooN scheme with the MFCR and NCR-AODV. These results present the simulation results in which the

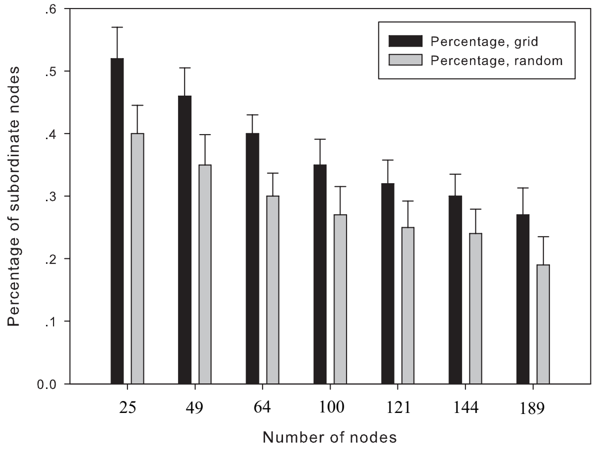


FIGURE 3.4: Percentage of subordinate nodes in grid and randomly deployed scenarios vs. number of nodes.

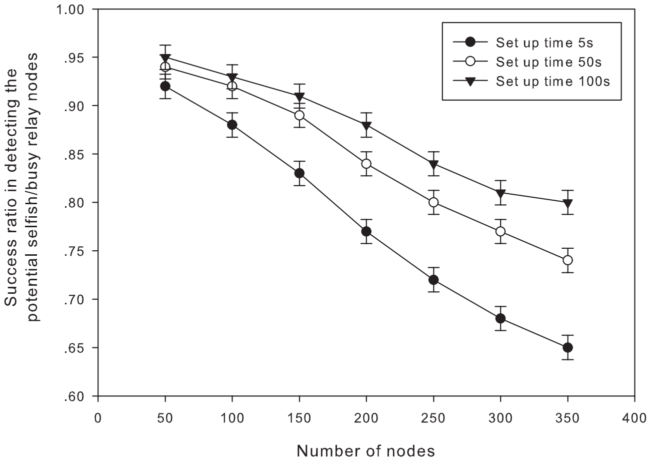


FIGURE 3.5: Success ratio in detecting congestion and noncooperation vs. number of nodes.

moving nodes' average speed change. As NCR-AODV does not consider the movement of emergency nodes, the performance values change very little in the figures.

As Fig. 3.6 shows, our proposed SCooN scheme performs better than MFCR and NCR-AODV at all speed levels. It is because our novel networking scheme properly selects the optimal relays to perform the cooperative transmission. Meanwhile, the speed of nodes influence the performance of our SCooN scheme. When the speed of moving nodes equals to 25 meters/second, it performs the best throughput. On the other hand, as both MFCR

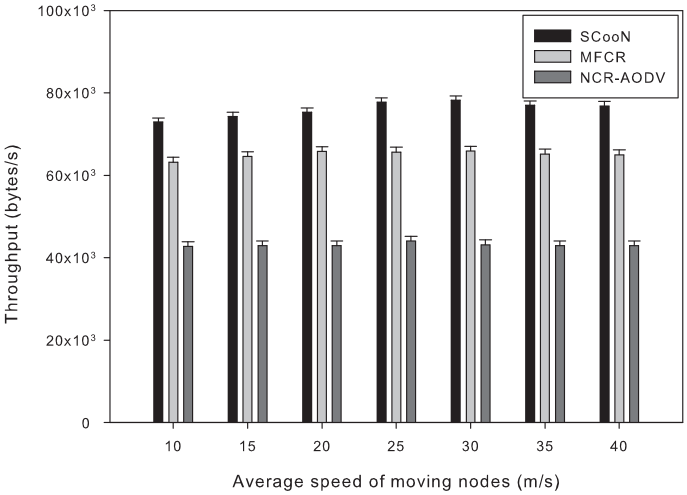


FIGURE 3.6: Efficiency of the proposed networking schemes: throughput vs. average speed of moving nodes.

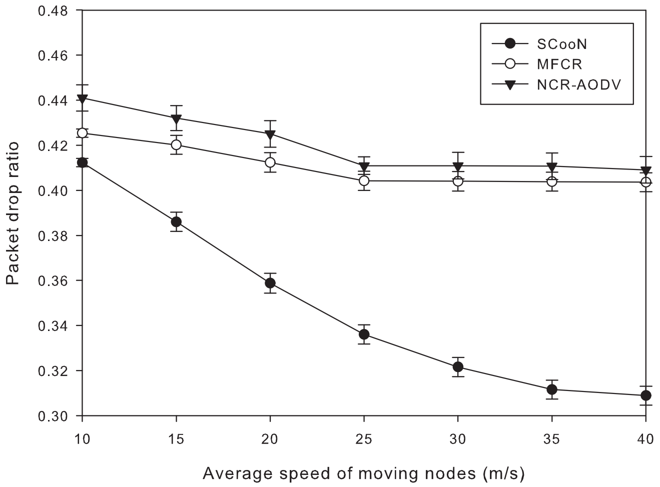


FIGURE 3.7: Efficiency of the proposed networking schemes: packet drop ratio vs. average speed of moving nodes.

and NCR-AODV schemes do not consider the movements of nodes, their throughput change little with as the average speed of moving nodes change.

In Fig. 3.7, we calculate the packet drop ratio of our SCooN scheme and compare with the other two referenced schemes. SCooN scheme also performs better than MFCR and NCR-AODV. It is because the SCooN scheme takes the advantages of cooperative

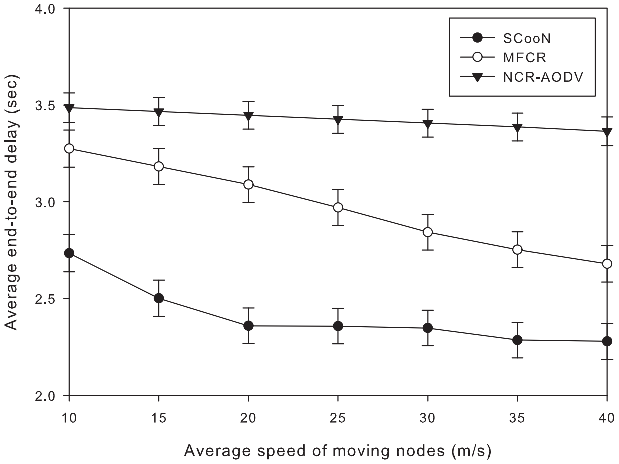


FIGURE 3.8: Efficiency of the proposed networking schemes: packet drop ratio vs. average speed of moving nodes.

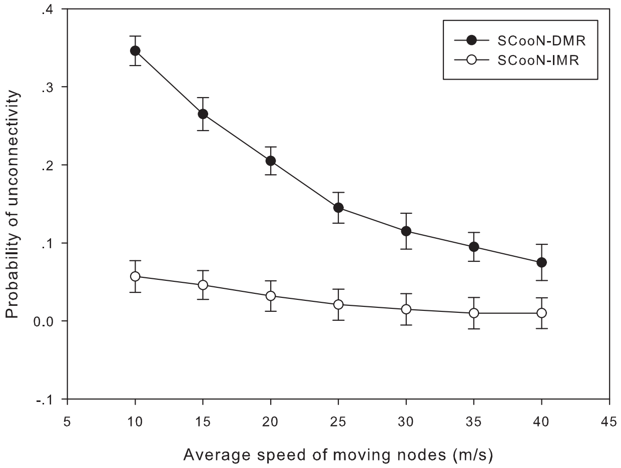


FIGURE 3.9: Comparison of the proposed networking schemes: probability of unconnectivity vs. average speed of moving nodes.

communication and dynamically select the proper relays for transmission. As a result, the optimal routes under cooperative mode are selected. The MFCR scheme owns better packet drop ratio than NCR-AODV as it is also a cooperative routing protocol which selects relay nodes to act as cooperative relays. However, these two schemes are quite close as when the emergency sessions emerged, the MFCR scheme only selects the route to act in ordinary

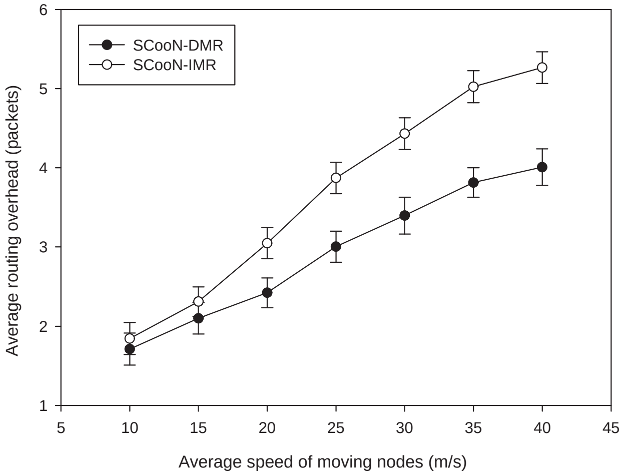


FIGURE 3.10: Comparison of the proposed networking schemes: average routing overhead vs. average speed of moving nodes.

mode. It is also because when the contention problem of the network is serious, the MFCR is similar to a non-cooperative routing protocol.

From Fig. 3.8, we obverse that the proposed SCooN scheme achieves less end-to-end delay comparing with the existing cooperative routing protocol MFCR and the non-cooperative routing protocol AODV. As the moving node's speed increases, it can replace the selfish/busy relay more quickly, the advantages of SCooN scheme is obvious in such cases.

In Fig. 3.9, we compare the probability of unconnectivity for SCooN-DMR and SCooN-IMR. ISCooN-IMR is better than SCooN-DMR as it ensures connectivity by iterative movement. We also compare the routing load of these two schemes in Fig. 3.10, the routing overhead of SCooN-DMR is less than ISCooN-IMR as IMR scheme contains more location information than DMR scheme.

The simulation results reveal that our proposed SCooN scheme significantly improves the network performance by the cognitive movement of emergency sources or relays themselves and they are more efficient than the MFCR and NCR-AODV for emergency services in WANETs.

3.7 Summary

This chapter focuses on promoting self-supported cooperative networking for emergency services in multi-hop wireless networks. We propose a novel cross-layer design which jointly considers the problems of route selection in network layer, congestion and non-cooperation avoidance among multiple links in MAC layer under cooperative multi-hop wireless environments. We formulate the multi-hop cooperative flow routing and relay node selection process as an optimization problem. Based on the formulations and models, we propose a self-supported based networking scheme including three novel components that make the solution procedure highly efficient. Analysis and simulation results show that our approaches significantly achieve better network performance. As a future work, we will consider the general mobile patterns in Mobile Ad-hoc Networks (MANETs) and promote efficient networking schemes to support emergency services.

Chapter 4

Optimal Relay Placement for Multi-Pair Cooperative Communication in Wireless Networks

This chapter studies the relay placement problem for multi-pair cooperative communication in wireless networks, where a finite number of candidate relay nodes can be placed to help the transmission of multiple source-destination pairs. Our objective is to maximize the system capacity. After formulating the relay node placement problem, we comprehensively investigate the effect of relay node location on cooperative link capacity and show several attractive properties of the problem under consideration. As the main contribution, we develop a geographic aware relay node placement algorithm which optimally solves the relay node placement problem in polynomial time. The basic idea is to place a set of relay nodes to the optimum locations so as to maximize the system capacity. The efficiency of our proposed algorithm is evaluated by the results of series experimental studies.

This chapter is organized as follows. Section 4.1 introduces the motivation of the relay placement problem for multi-pair cooperative communication in wireless networks. In Section 4.2, we describe the architecture of our system model and formulate the problem. We study the properties of our formulated problem in Section 4.3. In Section 4.4, we propose a polynomial time algorithm to optimally solve the problem. Performance evaluation is carried out in Section 4.5. Finally, Section 4.6 concludes this chapter and points out the future work.

4.1 Introduction

With the advancement of telecommunication technology, devices with wireless functionalities are ubiquitous nowadays. As a result, networking among such devices has become increasing critical in both theory and practice. Cooperative communication (CC), which exploits the nature of wireless broadcast and the relaying capabilities of other involved wireless devices to achieve spatial diversity, has been shown to have great potential to enhance the channel capacity between two wireless devices [64], [39]-[40], [66]. Although CC promises to enhance the capacity, an improper placement of relay node can result in an even smaller capacity than that under direct transmission (DT). Therefore, the potential gains in capacity enhancement largely depends on the placement of the involved relays, which is one of the most important issues in cooperative networking [68].

The problem of determining the locations of the relay nodes for wireless coverage maintenance or network performance optimization is usually referred to as the *relay node placement (RNP)* problem [41], which was originally emerged in the field of wireless sensor networks [42]. With the emergence of large-scale, dynamic and decentralized wireless networks, such problems are often encountered in WiMAX netwoks, wireless ad hoc networks (WANETs) and multi-hop cellular networks (MCNs). For example, in the IEEE 802.16 standard based WiMAX networks, RNP problem has been used to determine the locations of base stations, relay stations and subscriber stations for different purposes [39], [43], [45], [46]. Among the existing literatures, the signal-to-noise ratio (SNR) based model is often applied for RNP problem formulation, where the received signal strength is estimated according to the distance, and then the link capacity is decided by Shannon's channel capacity formula [48]. The RNP problem is then converted into an optimization problem which usually focuses on capacity enhancement and energy efficiency. This modeling approach yields a more flexible network topology and performance indexes which are continuous with respect to the locations of relays, hence is more suitable in practice. Depending on the placement space used for RNP problem formulation, the existing relay placement methodologies can be roughly classified into three categories: *discrete* placement, *continuous* placement, and *hybrid* placement (see e.g., in [50] for an overview). RNP problem for capacity maximization purpose in cooperative wireless networks has also drawn extensive attentions recently [44], [46], [47]. However, as far as we know, most of the prior works have considered different network model and objective comparing with the relay placement problem we considered here. Besides, with the same objective as our work, only heuristic algorithms with near-optimal solutions are proposed [44].

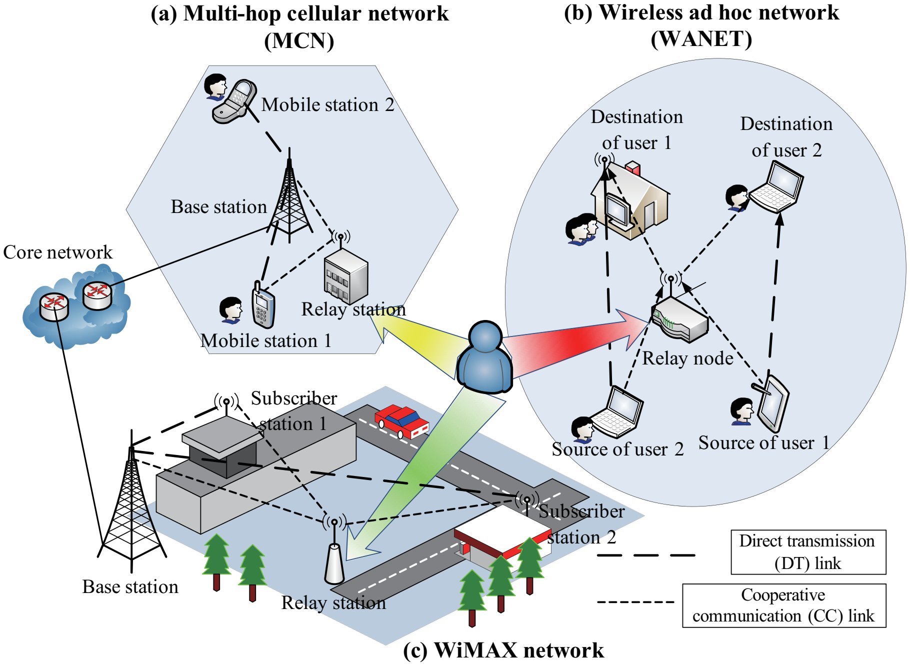


FIGURE 4.1: Relay placement in cooperative communication aware wireless networks.

We consider the continuous placement methodology and study the relay node placement problem for multi-pair cooperative communication (RNP-MPCC) in this chapter, where a finite number of wireless devices functioning as candidate relay nodes can be placed anywhere in the network and cooperatively help multiple source-destination pairs to achieve cooperative communication. The objective of our work is to maximize the system capacity. This problem has many applications. For example, in case of all sources share the same destination, it can be extended to the relay station placement problem in WiMAX networks or be developed to the relay station scheduling problem in multi-hop cellular network (MCN), as shown in Fig. 4.1. However, this problem is very challenging due to two facts: 1) the potential space for the relay node location is continuous; and 2) multiple source-destination pairs exploiting the limited number of relays and the maximization of system capacity have to be jointly considered. Our main contributions are summarized as follows:

- By applying the SNR-based capacity model, we theoretically formulate the relay node placement problem under consideration, named as RNP-MPCC, which seeks for a relay placement profile such that the system capacity is maximized.
- Due to the continuous nature of placement space, we carry out comprehensive studies on the effect of relay location on cooperative link capacity, and determine the optimum relay location site for each source-destination pair.
- We develop a geographic aware polynomial time algorithm to optimally solve RNP-MPCC, which maximizes the system capacity by placing a subset of the candidate relay nodes on the optimum relay location sites.
- Analytical and experimental results are carried out to evaluate the efficiency of our proposed algorithm.

4.2 System Description and Problem Formulation

4.2.1 Network Model

We consider a 2-Dimensional static wireless network with area $\mathcal{A}$, which is consisting of a set of n source nodes $S = \{s_1, s_2, ...s_n\}$ and a set of n destination nodes $D = \{d_1, d_2, ...d_n\}$. Transmission performs as a number of unicast sessions where each source node s_i is paired with a destination node d_i.[1] Besides, m relay nodes $R = \{r_1, r_2, ...r_m\}$ form the candidate relay nodes set, in which no more than m relay nodes can be placed into the network to help the s-d pairs achieve cooperative communication. All relay nodes are assumed to have equal relaying capability, i.e., the transmission power of all relay nodes are same. Besides, we assume that the distance between any *s-d* pair is less than the transmission range of source node so that each s-d pair can use direct transmission (DT) or cooperative communication (CC) with the help of the placed relay node. Following the investigation in [79], which has

[1] The terms source-destination pair s_i and d_i, s-d pair s_i and d_i, and $\langle s_i, d_i \rangle$ will be used interchangeably throughout this chapter.

showed that it is sufficient for an *s*-*d* pair to exploit the best relay node even when multiple relays are available to achieve full diversity. Therefore, it is reasonable to assume that each *s*-*d* pair will use at most one relay node for CC.

A slow, flat, block Rayleigh fading environment is applied, i.e., the channel remains static for one coherence interval and changes independently in different coherence intervals with a variance $\sigma_{i,j}^2 = d_{i,j}^{-\alpha}$, where $d_{i,j}$ is the Euclidean distance between node i and j, and α is the pass loss exponent. The channel gain between node i and j is denoted as $h_{i,j}$, which is modeled as a zero-mean, independent, circularly-symmetric complex Gaussian random variable with variance $\sigma_{i,j}^2$. Furthermore, additive white Gaussian noise (AWGN) with power spectral density N_0 is assumed. Thus, when node i transmits a signal to node j with power P_i, the instantaneous signal-to-noise ratio (SNR) seen by node j, denoted by $\gamma_{i,j}$, is $\gamma_{i,j} \triangleq \frac{P_i|h_{i,j}|^2}{N_0} = \frac{P_i d_{i,j}^{-\alpha}}{N_0}$. We assume that the transmission power for all source nodes and relay nodes are P_s and P_r in *Watt*, respectively. The bandwidth of all channels is assumed to be W in *MHz*. In order to mitigate interference, we make the same assumption as in [40] and [66], where the orthogonal channels are available in the network, e.g., using orthogonal frequency division multiple access (OFDMA) technique [78].

Table 4.1 lists the frequently used notations in this chapter.

4.2.2 Transmission Model

For a specified *s*-*d* pair $\langle s_i, d_i \rangle$, when DT is applied, s_i directly transmits data to d_i, the achievable capacity between s_i and d_i can be calculated by the SNR-based Shannon's capacity formula [48]:

$$C_{DT}(s_i, d_i) = W \log_2 (1 + \gamma_{s_i,d_i}) . \tag{4.1}$$

When a relay node involves to achieve CC, we adopt the model proposed in [64] where transmission proceeds in a frame-by-frame basis and each frame is divided into two time slots: the first slot for broadcast phase, and the second slot for cooperative phase. During the broadcast phase, source s_i transmits the signal to its corresponding destination d_i. Due to the broadcast nature of wireless communication, this transmission can also be overheard by the involved relay node. During the cooperative phase, the relay node forwards the overheard signal to d_i using different techniques depending on different CC modes. There

Table 4.1: Frequently used notations in Chapter 4.

Notation	Description
$S = \{s_1, s_2, ...s_n\}$	set of source nodes
$D = \{d_1, d_2, ...d_n\}$	set of destination nodes
$R = \{r_1, r_2, ...r_m\}$	set of candidate relay nodes
$\langle s_i, d_i \rangle$	s-d pair s_i and d_i
$\gamma_{i,j}$	signal-to-noise ratio (SNR) from node i to i
α, P_s, P_r	path loss exponent, transmission power of source and relay
$C_{DT}(s_i, d_i)$	channel capacity between s_i and d_i under direct transmission
$\mathcal{R}(s_i)$	relay node that helps $\langle s_i, d_i \rangle$ in the cooperative phase
$C_{AF}(\mathcal{R}(s_i))$	channel capacity between s_i and d_i under AF mode cooperative communication with relay $\mathcal{R}(s_i)$
$C_{DF}(\mathcal{R}(s_i))$	channel capacity between s_i and d_i under DF mode cooperative communication with relay $\mathcal{R}(s_i)$
$\lvert X \rvert$	cardinality of set X
$\delta_i \in \{0, 1\}$	binary variable to characterize whether a relay node is placed to serve for $\langle s_i, d_i \rangle$

are mainly two cooperative communication modes: Amplify-and-Forward (AF) and Decode-and-Forward (DF). Denote the relay node which helps *s*-*d* pair $\langle s_i, d_i \rangle$ in the cooperative phase by $\mathcal{R}(s_i)$. The achievable capacity from s_i to d_i under AF and DF mode can be expressed as Eqn. (4.2) and Eqn. (4.3), respectively [47]:

$$C_{AF}(\mathcal{R}(s_i)) = \frac{W}{2} \log_2 \left(1 + \gamma_{s_i,d_i} + \frac{\gamma_{s_i,\mathcal{R}(s_i)} \gamma_{s_i,d_i}}{\gamma_{s_i,\mathcal{R}(s_i)} + \gamma_{\mathcal{R}(s_i),d_i} + 1} \right), \tag{4.2}$$

$$\begin{aligned} C_{DF}(\mathcal{R}(s_i)) = \tfrac{W}{2} \min \big\{ & \log_2 \left(1 + \gamma_{s_i,\mathcal{R}(s_i)}\right), \\ & \log_2 \left(1 + \gamma_{s_i,d_i} + \gamma_{\mathcal{R}(s_i),d_i}\right) \big\}. \end{aligned} \tag{4.3}$$

For our predefined network model, a finite number of relay nodes are to place into the network for multiple *s*-*d* pairs to achieve CC, we call it multi-pair cooperative communication (MPCC) throughout this chapter. Specifically, we consider the situation where a relay node can be shared by multiple *s*-*d* pairs. Let $\mathcal{S}(\mathcal{R}(s_i))$ denote the set of source nodes $\mathcal{R}(s_i)$ serves for. For the case when multiple *s*-*d* pairs share one relay node, i.e., $|\mathcal{S}(\mathcal{R}(s_i))| > 1$ ($|X|$ is the cardinality of set X), we assume that the relay node equally provides service to all the *s*-*d* pairs employing it. This can be achieved by using a reservation-based TDMA scheduling and the shared relay node serves each s-d pair in a round-robin fashion [40]. Take the WANET in Fig. 4.1 as an example, relay node serves user 1 in the first two time slots and switches to serve user 2 in the following two time slots, etc. The achievable capacity from s_i to d_i under MPCC can be expressed as:

$$C\left(\mathcal{R}\left(s_i\right)\right)=\begin{cases}\frac{C_{AF}(\mathcal{R}(s_i))}{|\mathcal{S}(\mathcal{R}(s_i))|}, \text{if} \quad \mathcal{R}\left(s_i\right)\neq\emptyset, \quad \text{AF mode},\\ \frac{C_{DF}(\mathcal{R}(s_i))}{|\mathcal{S}(\mathcal{R}(s_i))|}, \text{if} \quad \mathcal{R}\left(s_i\right)\neq\emptyset, \quad \text{DF mode},\\ C_{DT}\left(s_i,d_i\right), \text{if} \quad \mathcal{R}\left(s_i\right)=\emptyset.\end{cases} \tag{4.4}$$

4.2.3 Problem Formulation

Following the previous definitions,, we introduce a binary variable $\delta_i\in\{0,1\}$ to characterize whether a relay node is placed to serve for $\langle s_{i,}d_i\rangle$. Thus, the capacity expression in Eqn. (4.4) can be formulated as:

$$C\left(\mathcal{R}\left(s_i\right)\right)=\delta_i\cdot C_{CC}\left(\mathcal{R}(s_i)\right)+(1-\delta_i)\cdot C_{DT}\left(s_i,d_i\right), \tag{4.5}$$

where $C_{CC}\left(\mathcal{R}(s_i)\right)$ is the achievable capacity from s_i to d_i under AF or DF mode; $\delta_i=1$, if $\mathcal{R}\left(s_i\right)\neq\emptyset$, otherwise, $\delta_i=0$.

As orthogonal channels are used to mitigate interference between different *s-d* pairs and relays, the system capacity can be defined as the summation of the achievable capacity of all pairs. Denote the relay nodes which are already placed into the network as $\mathbb{R}$. Notice that $\mathbb{R}\subseteq R$, i.e., $\mathbb{R}=R$ if all candidate relay nodes are placed, and $\mathbb{R}\subset R$ if only a subset of R is placed. In the rest of this chapter, we call it *complete placement* when $\mathbb{R}=R$, and *incomplete placement* when $\mathbb{R}\subset R$. Thus, the system capacity for the predefined network consisting of n s-d pairs and $|\mathbb{R}|$ ($|\mathbb{R}|\leq m$) placed relay nodes can be expressed as:

$$C_{sum}\left((S,D),\mathbb{R}\subseteq R\right)=\sum\nolimits_{s_i\in S}C\left(\mathcal{R}\left(s_i\right)\right). \tag{4.6}$$

Next we address the relay node placement problem for multi-pair cooperative communication (RNP-MPCC) as follows.

Definition 4.2.1 (**RNP-MPCC**). Given a set of source-destination pairs (S,D) within network area $\mathcal{A}$, no more than m relay nodes in R can be placed into $\mathcal{A}$ to achieve multi-pair cooperative communication, RNP-MPCC seeks for a relay placement profile such that the system capacity $C_{sum}\left((S, D), \mathbb{R} \subseteq R\right)$ is maximized among all the possible relay placement profiles.

More specifically, we define a relay node placement profile as a $m \times 2$ matrix where each of the m columns is a 2-Dimensional vector representing the location (coordinate) of the involved relay node in $\mathcal{A}$, i.e., $\left(x_{r_j}, y_{r_j}\right)$ is the placement profile for relay node r_j. We denote that a relay node r_j is placed into the network $\mathcal{A}$ as $\left(x_{r_j}, y_{r_j}\right) \in \mathcal{A}$. In case of incomplete placement ($\mathbb{R} \subset R$), the placement profile for the relay nodes which are not placed into the network is set to (∞, ∞). According to the above definitions, we theoretically formulate RNP-MPCC as the following optimization problem.

$$(\mathbf{RNP\text{-}MPCC}) \quad \text{Maximize} \quad C_{sum}\left((S, D), \mathbb{R} \subseteq R\right) \tag{4.7}$$

subject to

$$\delta_i = \begin{cases} 1, & \text{if } \mathcal{R}\left(s_i\right) \neq \emptyset, \\ 0, & \text{otherwise.} \end{cases} \tag{4.8a}$$

$$\left|\mathcal{R}\left(s_i\right)\right| \leq 1 \quad \left(s_i \in S, \quad \mathcal{R}(s_i) \in R\right), \tag{4.8b}$$

$$\left|\mathcal{S}\left(\mathcal{R}\left(s_i\right)\right)\right| \geq 1 \quad \left(s_i \in S, \quad \mathcal{R}(s_i) \in \mathbb{R}\right), \tag{4.8c}$$

$$\sum_{i=1}^{n} \delta_i \leq m \quad \left(s_i \in S, \quad \mathcal{R}(s_i) \in R\right), \tag{4.8d}$$

$$\begin{cases} \left(x_{r_j}, y_{r_j}\right) \in \mathcal{A}, & \text{if} \quad \mathrm{r}_j \in \mathbb{R}, \\ \left(x_{r_j}, y_{r_j}\right) = (\infty, \infty), & \text{otherwise,} \end{cases} \tag{4.8e}$$

where Eqn. (4.8a) specifies the binary variable δ_i, Eqn. (4.8b) specifies that each *s*-*d* pair can use at most one relay node for CC, Eqn. (4.8c) specifies that each placed relay node can be shared by multiple *s*-*d* pairs, Eqn. (4.8d) indicates the number of placed relay nodes can not exceed the cardinality of the relay nodes set, Eqn. (4.8e) indicates the continuous placement space for the relay nodes and the value of elements in the relay placement profile.

Notice that the solution of RNP-MPCC is a $m \times 2$ matrix consisting of one placement profile for each of the m candidate relay nodes. The value of the binary variable δ_i can be obtained according to the resulting placement profile. Due to the continuous nature of the placement space and the possibility of sharing a placed relay node by multiple *s*-*d* pairs, it is hard to observe how to reduce the formulated RNP-MPCC into an integer linear programming problem, let alone giving any heuristic algorithms to solve it.

4.3 Problem Analysis and Reduction

Ahead of solving the formulated problem, we first analyze it by studying the effect of relay node location on cooperative link capacity for the predefined network model. Then we exploit the reduction of the original formulated problem.

4.3.1 Effect of Relay Location on Cooperative Link Capacity

Although CC promises to enhance the capacity, an improper placement of relay node can result in an even smaller capacity than that under DT. This deterioration can not be obviously observed by comparing the capacity expressions in Eqn. (4.1) and Eqn. (4.2) (or Eqn. (4.3)). On the other hand, according to the SNR-based capacity formula, both $C_{AF}\left(\mathcal{R}(s_i)\right)$ and $C_{DF}\left(\mathcal{R}(s_i)\right)$ are functions of P_r, d_{s_i,r_j} and d_{r_j,d_i}. For constant P_r, the achievable cooperative link capacity is quite related to the location of the involved relay. For a dedicated *s-d* pair, we are particularly interested in seeking for an optimum relay location, on which the maximum link capacity can be achieved. The following lemma indicates the optimum cooperative relay node location can be obtained and the link capacity maximization problem can be solved optimally.

Lemma 4.1 (Optimum cooperative relay node location)**.** *Under the predefined network model, if the transmission power of relay is constant, the optimum cooperative relay node location can be obtained by solving the following optimization problems, through which the cooperative link capacity between s-d pair s_i and d_i is maximized.*

$$\text{AF mode}: \qquad r_j^* = \arg\max \left\{ \frac{\gamma_{s_i,r_j}\gamma_{r_j,d_i}}{\gamma_{s_i,r_j}+\gamma_{r_j,d_i}+1} \right\} \tag{4.9}$$

$$\text{DF mode}: r_j^* = \arg\max \left\{ \min\left\{\gamma_{s_i,r_j}, \gamma_{s_i,d_i}+\gamma_{r_j,d_i}\right\}\right\} \tag{4.10}$$

subject to

$$d_{s_i,r_j} + d_{r_j,d_i} = d_{s_i,d_i}. \tag{4.11}$$

Proof. It is not hard to notice that the above objective formulations is derived from the capacity expressions of the primary channel in Eqn. (4.2) and Eqn. (4.3). We proof the lemma by proving the constraint in Eqn. (4.11). Notice that Eqn. (4.11) indicates that the involved cooperative relay node is placed on the line passing between s_i and d_i. Considering the three-node example illustrated in Fig. 4.2, we prove the constraint by contradiction. We assume that the location of the involved cooperative relay is out of the line passing through s_i and d_i, with which resulting in the maximum capacity of the primary channel. Denote the involved relay as r_l, the proof process falls into the following four cases:

1) Case 1: $d_{s_i,r_l}, d_{r_l,d_i} > d_{s_i,d_i}$. Under this case, place another relay on the line passing through s_i and d_i, say r_j. Notice that γ_{s_i,d_i}, P_s and P_r are constant, $d_{s_i,r_j} < d_{s_i,d_i} < d_{s_i,r_l}$ and $d_{r_j,d_i} < d_{s_i,d_i} < d_{r_l,d_i}$. According to Eqn. (4.9) and Eqn. (4.10), the achievable capacity when relay r_j involves is greater than that when r_l involves.

2) Case 2: $d_{s_i,r_l}, d_{r_l,d_i} < d_{s_i,d_i}$. Under this case, as $d_{s_i,r_l} < d_{s_i,d_i}$, we could place another relay, say r_j, on the line passing through s_i and d_i where the distance between s_i and r_j equals to the distance between s_i and r_l, i.e., $d_{s_i,r_j} = d_{s_i,r_l}$, as illustrated in Fig. 4.2. Such that $d_{r_j,d_i} = d_{s_i,d_i} - d_{s_i,r_j} = d_{s_i,d_i} - d_{s_i,r_l} < d_{r_l,d_i}$. Therefore, we could have $d_{s_i,r_j} = d_{s_i,r_l}$ and $d_{r_j,d_i} < d_{r_l,d_i}$. Thus the capacity when r_j involves is greater than that when r_l involves.

3) Case 3 & 4: $d_{s_i,r_l} < d_{s_i,d_i}, d_{r_l,d_i} > d_{s_i,d_i}$ and $d_{s_i,r_l} > d_{s_i,d_i}, d_{r_l,d_i} < d_{s_i,d_i}$. As the proof process for these two cases are quite similar, we provide them together. Under these two cases, as either $d_{s,r_l} < d_{s_i,d_i}$ or $d_{r_l,d_i} < d_{s_i,d_i}$, we can place another relay node r_j on the line passing through s_i and d_i where $d_{s_i,r_j} = d_{s_i,r_l}$ (Case 3) or $d_{r_j,d_i} = d_{r_l,d_i}$ (Case 4), as shown in Fig. 4.2. Similar as the analysis under Case 2, we could have $d_{s_i,r_j} = d_{s_i,r_l}$ and $d_{r_j,d_i} < d_{r_l,d_i}$ under Case 3, $d_{r_j,d_i} = d_{r_l,d_i}$ and $d_{s_i,r_j} < d_{s_i,r_l}$ under Case 4. Thus the capacity when r_j involves, both under Case 3 and 4, is greater than that when r_l involves.

For the above four cases, we can always find a relay that locates on the line passing between s_i and d_i and the achievable capacity when r_j involves is greater than that when r_l involves. As illustrated in Fig. 4.2, the "=" symbol on the links represents the equal distance between the nodes in the marked link, e.g., under Case 2, $d_{s_i,r_l} = d_{s_i,r_j}$, which stands for the location of the involved relay r_j thus $C^P_{CC}(s_i, r_j, d_i) > C^P_{CC}(s_i, r_l, d_i)$.

Therefore, for a relay node r_l that is out of the line passing through s_i and d_i, we could always place another relay r_j which locates on the line passing s_i and d_i and have a greater

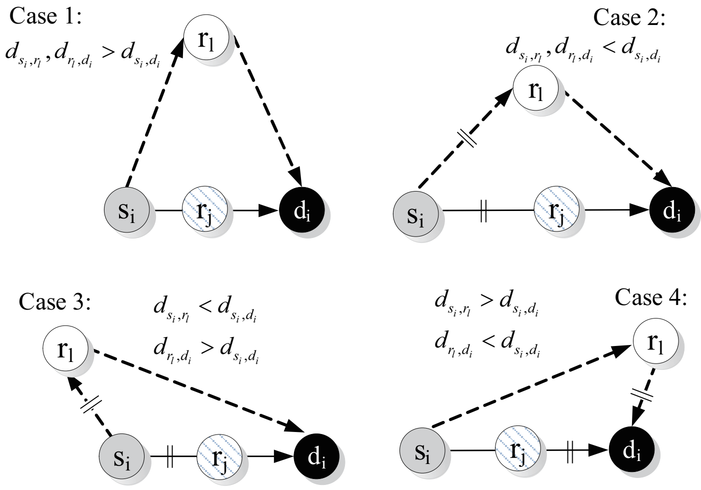

Case 1:
$d_{s_i,r_l}, d_{r_l,d_i} > d_{s_i,d_i}$
Case 2:
$d_{s_i,r_l}, d_{r_l,d_i} < d_{s_i,d_i}$
Case 3:
$d_{s_i,r_l} < d_{s_i,d_i}$
$d_{r_l,d_i} > d_{s_i,d_i}$
Case 4:
$d_{s_i,r_l} > d_{s_i,d_i}$
$d_{r_l,d_i} < d_{s_i,d_i}$
r_l
s_i
r_j
d_i

FIGURE 4.2: Illustrative examples for optimum cooperative relay node locations under four different cases.

capacity. It contradicts the fact that the best relay is out of the line passing through s_i and d_i. Thus, we complete the proof. □

According to the above lemma, we can obtain the optimum relay location for each s-d pair so as the maximize the cooperative link capacity. The above analytical result greatly reduces the placement space for RNP-MPCC and a set of n candidate optimum relay locations are determined. The optimum relay locations for all s-d pairs form a reduced placement space, denoted by $\mathbb{A}(\mathbb{A} \subset \mathcal{A})$. However, as the number of candidate relay nodes is finite, it may be infeasible to place each optimum location a cooperative relay. Specifically, when the number of candidate relay nodes is less then the number of s-d pairs, i.e., $m < n$.

4.3.2 Incomplete and Complete Placement

4.3.2.1 Incomplete placement

If the placed relay nodes set is a proper subset of the candidate relay nodes set, $\mathbb{R} \subset R$, such a placement profile is called an ***incomplete*** placement. The following lemma indicates the condition when an incomplete placement exists.

Lemma 4.2. *The solution for our predefined RNP-MPCC is an incomplete placement only if $n < m$. Moreover, an incomplete placement ensures to place a cooperative relay for each s-d pair.*

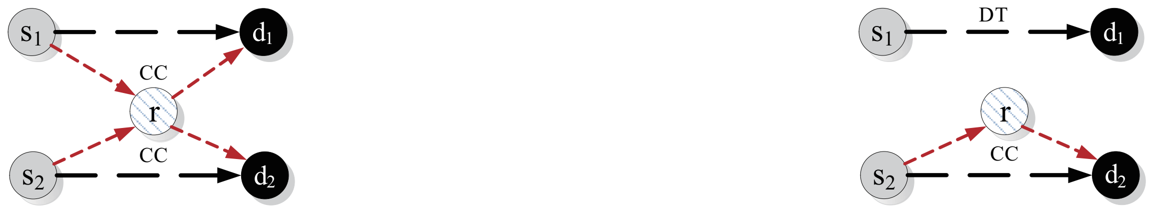
Proof. Suppose the solution for RNP-MPCC is an incomplete placement and $n \geq m$, according to Lemma 4.1 and the system capacity formulation in Eqn. (4.6), one can always increase the system capacity by placing the left relay nodes in R $(R \backslash \mathbb{R})$ to the unplaced $(n - m)$ s-d pairs, which will result in a complete placement in the end. It contradicts the fact that the solution is an incomplete placement. Therefore, as we have $n < m$ in an incomplete placement, we can always place a relay node on the optimum location for each s-d pair such that the system capacity is maximized. Hence, we complete the proof. □

According to Lemma 4.2, if the number of candidate relay nodes is no less than the number of s-d pairs, there is no incentive for the s-d pairs to share a placed relay node as each s-d pair exploits an optimum placed relay node will result in a global maximization of the system capacity. Thus, the solution for incomplete placement is equivalent to solving the optimization problem in Lemma 4.1 for each s-d pair.

4.3.2.2 Complete placement

On the other hand, if all the candidate relay nodes are placed into the network, $\mathbb{R} = R$, it is called a ***complete*** placement. From Lemma 4.2, it is not hard to observe that the complete placement exists when $n \geq m$. Specifically, complete placement is potential to involves the case of MPCC with a common relay, as shown in Fig. 4.3. As a result, we are more interested in how to increase the system capacity by cooperative networking. To this end, we switch to focus on the situation when MPCC with a common relay occurs in a complete placement.

Fortunately, a recent work by Yang *et al.* [40] has shown that if a common relay node is shared by multiple s-d pairs, one can increase the system capacity by separating multi-pair CC into several direct transmissions and single-pair CC. More specifically, if a placed relay node r_j is shared by multiple s-d pairs, we can always improve the system capacity by applying the following *double-step* adjustment: i) let the s-d pair with the minimum capacity among all the pairs sharing r_j transmit under DT; ii) keep other s-d pairs' relay



(a) Before adjustment

(b) After adjustment

FIGURE 4.3: Double-step adjustment for multi-pair cooperative communication with a common relay node.

placement profile the same. Consider the sample cooperative ad hoc network in Fig. 4.1, the multi-pair cooperative communication with a common relay before and after adjustment are illustrated in Fig. 4.3(a) and Fig. 4.3(b). During the adjustment, the s-d pair with the minimum capacity, say $\langle s_1, d_1 \rangle$, is adjusted from sharing cooperative relay node r to using direct transmission.

4.3.3 Reduced RNP-MPCC

To this point, we can reduce the formulated RNP-MPCC by relaxing the constraints in (4.8c) and (4.8e) and use the following (4.12a) and (4.12b) to replace them.

$$|\mathcal{S}\left(\mathcal{R}\left(s_i\right)\right)| \leq 1 \quad \left(s_i \in S, \quad \mathcal{R}(s_i) \in R\right), \tag{4.12a}$$

$$\begin{cases} \left(x_{r_j}, y_{r_j}\right) \in \mathbb{A}, & \text{if} \quad \mathrm{r}_j \in \mathbb{R}, \\ \left(x_{r_j}, y_{r_j}\right) = \left(\infty, \infty\right), \text{otherwise}, \end{cases} \tag{4.12b}$$

where Eqn. (4.12a) specifies that each relay node will be placed to act as cooperative relay for at most one s-d pair, in order to achieve maximum system capacity. Eqn. (4.12b) restricts the candidate relay locations to a number of optimum sites. Notice that $\mathbb{A}$ consisting of n 2-D vectors is the set of optimum relay location sites for all s-d pair. Therefore, $\mathbb{A}$ is a superset of the optimum relay placement profile and a subset of $\mathcal{A}$.

4.4 An Optimal Relay Node Placement Algorithm

Based on the analysis in the previous section, any optimal solutions for RNP-MPCC indicates putting at most m relay nodes on n optimum candidate sites. Besides, each site can be placed at most one relay node and each relay node can be used for at most one s-d pair. For incomplete placement ($n < m$), the optimum relay placement profile is the determined optimum candidate site. For complete placement ($n \geq m$), the one-to-one matching relation implies that we can map any instance of RNP-MPCC into that of the *Maximum Weighted Bipartite Matching* (MWBM) problem [81] and use corresponding algorithms to solve. We present our proposed optimal relay placement algorithm for MPCC, named ORNP, as described in the Algorithm 2.

4.4.1 Algorithm Details

The optimum relay placement profile for incomplete placement can be readily obtained by solving the optimization problem in Eqn. (4.9) or Eqn. (4.10). Next we give detailed descriptions for the complete placement. For any instance $((S, D), R)$ of RNP-MPCC, we construct an instance $G = (U, V, w)$ of the MWBM problem as follows. Let a set U of vertices represents the source nodes set S, and a set V of vertices represents $R \cup R'$, where R' is a set of $n - m$ virtual relay nodes. The edge between $s_i\,(s_i \in S)$ and $r_j\,(r_j \in R)$ represents cooperative communication from s_i to d_i with the connected relay node r_j. The edge between $s_i\,(s_i \in S)$ and ${r_j}'\,({r_j}' \in R')$ represents direct transmission from s_i to d_i. Then we set $w(s_i, r_j) = \max\limits_{d_{s_i,r_j} + d_{r_j,d_i} = d_{s_i,d_i}} \{C_{CC}(r_j)\}\,(r_j = \mathcal{R}(s_i))$, and set $w(s_i, {r_j}') = C_{DT}(s_i, d_i)$ for all $s_i \in U$, r_j,${r_j}' \in V$. The corresponding MWBM instance for the sample network in Fig. 4.1 is shown in Fig. 4.4. For clarity purpose, we only label some of the connected edges in the figure.

4.4.2 Optimality and Complexity Analysis

Next we prove the correctness and analyze the computational complexity of our proposed algorithm by the following theorem.

Theorem 4.4.1. The proposed ORNP algorithm guarantees to find an optimal cooperative relay placement profile for RNP-MPCC in time bounded by $O(n^3)$.

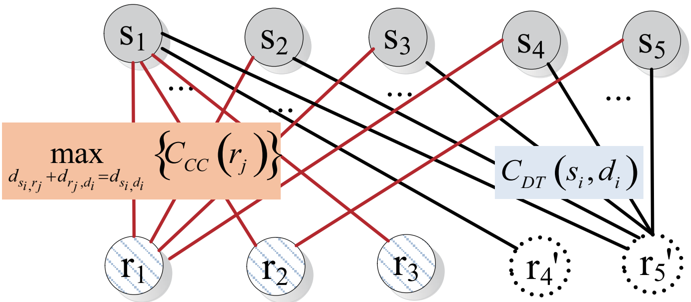


FIGURE 4.4: Mapping RNP-MPCC into the MWBM problem, in which red line represents CC with the connected relay node and black line represents DT.

Proof. The correctness of incomplete placement in ORNP (from Line 4 to 6) can be easily observed. We prove the correctness of complete placement in ORNP by contradiction. Following the formulated RNP-MPCC and our previous discussions, each optimal relay placement profile for RNP-MPCC can be mapped to a matching in the graph $G = (U, V, w)$, as described from Line 8 to 12. Assume there exists another relay placement profile which resulting in a higher system capacity than that returned by ORNP. In other words, there exists another matching M' for G, which has a higher weight than that of M^*. It contradicts the fact that M^* is a maximum weight matching for G. Therefore, ORNP is an optimal relay placement algorithm.

For the computational time of ORNP, it is consisted of two parts: computational time of obtaining the optimum relay location for all s-d pairs (from Line 1 to 3), and running time of placement profile calculation (incomplete placement from Line 4 to 6, or complete placement from Line 7 to 17). For the first part, it is bounded by $O(n)$. For the incomplete placement, it is bounded by $O(1)$. For the complete placement, it is bounded by the running time of the corresponding MWBM algorithm (Line 13). If the Kuhn-Munkres algorithm is used, the running time of complete placement is bounded by $O\left(n^3\right)$ [81]. Therefore, the running time of ORNP is bounded by $O\left(n^3\right)$. □

4.5 Performance Evaluation

In this section, we first conduct numerical results to study the effect of relay node location on link capacity in a cooperative wireless network. We calculate the achievable capacity between a pair of fixed source and destination when a cooperative relay is placed arbitrarily

Algorithm 2: Optimal relay node placement for multi-pair cooperative communication (ORNP)

Input: Source nodes set S, destination nodes set D, the number of candidate relay nodes m.

Output: A $m \times 2$ matrix consisting of one placement profile for each of the m candidate relay nodes.

```
for $i = 1; i \leq n$ do
    Compute the optimum relay location for $\langle s_i, d_i \rangle$;
end
if $n < m$ then
    Place a relay node on each optimum location and return the resulting relay placement profile;
end
else
    Construct a set $U$ of $n$ vertices corresponding to $S$;
    Construct a set $V$ of $n$ vertices corresponding to $R \cup R'$;
    for $i = 1, j = 1; i \leq n, j \leq n$ do
        Connect the vertices $u_i$ in $U$ and $v_j$ in $V$ and label the weight;
    end
    Apply an MWBM algorithm to find a maximum weighted matching $M^*$ for graph $G = (U, V, w)$;
    for $(u, v) \in M^*$ do
        Return the resulting relay placement profile;
    end
end
```

within a $1000m \times 1000m$ area, as illustrated in Fig. 4.5. Under this scenario, the path loss exponent α is 4, abient noise N_0 is 10^{-10} and transmission power of source and relay $P_s = P_r = 1Watt$. Notice that the capacity when the source directly transmits to the destination is 7.066 *Mbps*. From the results, we can observe that CC is not always better than DT, especially when the cooperative relay is placed improperly.

By varying the transmission power of relay node, we study the effect of transmission power of relay node on link capacity and the results are shown in Fig. 4.6. We make comprehensive comparisons with direct transmission, CC-AF x:y:z and CC-AF Upper bound, where x:y:z stands for the distance relationship $d_{s,r}$:$d_{r,d}$:$d_{s,d}$. We obtain CC-AF Upper bound by solving Eqn. (4.9) through the C-Plex optimizer [85]. From the results, we can also observe that an improper placement of cooperative relay node can result in an even

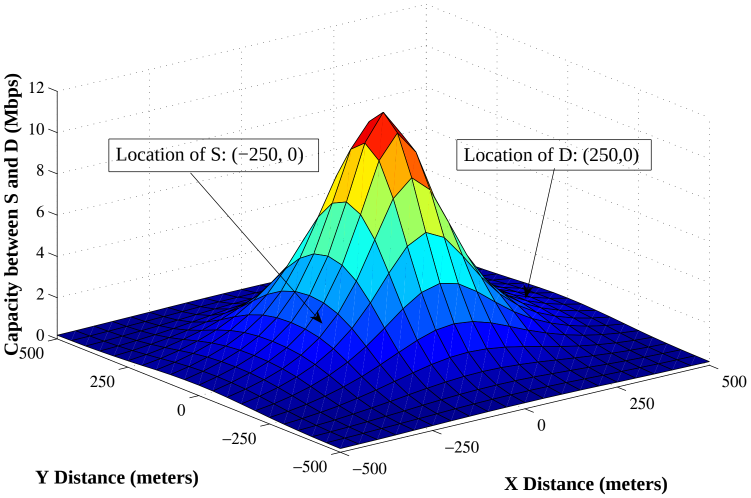


FIGURE 4.5: Effect of cooperative relay node location on link capacity.

smaller capacity than that under DT. For example, CC-AF 1:1:1 is a poor relay placement profile.

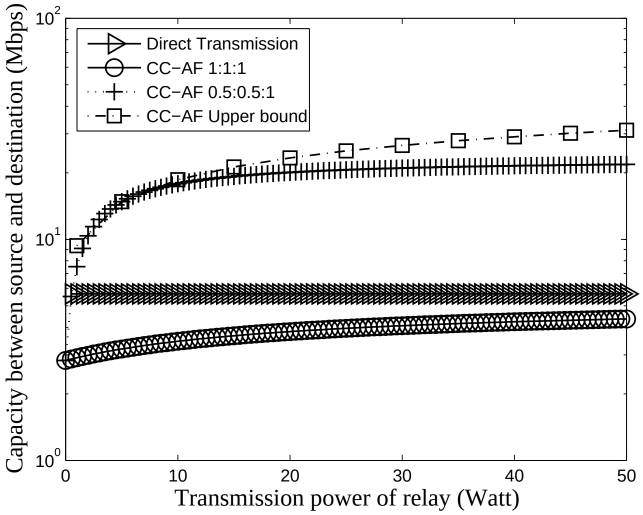


FIGURE 4.6: Effect of transmission power of relay node on link capacity.

Then we evaluate the efficiency of our proposed relay placement algorithm ORNP by conducting comprehensive experiments. Experiments are carried out by comparing our proposed ORNP with direct transmission, a heuristic algorithm proposed in [44] named CMRP.

Besides, we also compare ORNP with an optimal relay assignment algorithm (ORA) proposed in [66]. Although it is a relay assignment algorithm which has different methodology as relay placement, the capacity gain of ORNP can be observed as well. Experiment is first conducted in a static wireless network consisting of 30 s-d pairs. We set the bandwidth W to be 22 MHz for all channels and the transmission power of sources and relays are the same $P_s = P_r = 1Watt$ as the previous experiments. We first fix the number of candidate relay nodes m to 30 and run the corresponding algorithms, the results are shown in Fig. 4.7. As there are sufficient relay nodes, ORNP achieves the optimum capacity for each s-d pair and outperforms the other algorithms obviously. For the case of complete placement, we fix the number of relay nodes $m = 30$ and run the algorithms in a network of $n = 40$ s-d pairs, the results are shown in Fig. 4.8. As there are finite number of relay nodes, ORNP place the relay nodes on the optimum candidate sites or place no relay to specific s-d pairs. From the results, we can see that ORNP also achieves the best performance.

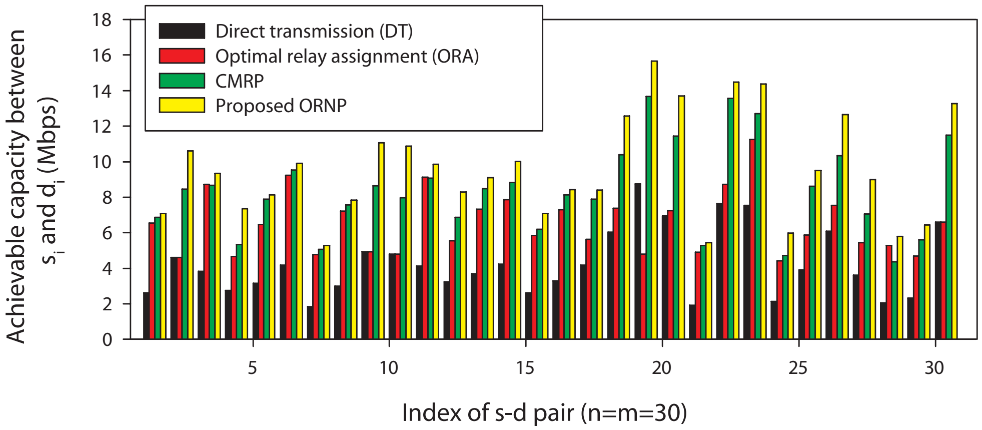


FIGURE 4.7: Achievable capacity in a multi-pair cooperative network when $n = m$.

4.6 Summary

Relaying and cooperation have emerged as important research topics in wireless communication over the past half-decade. During cooperative communication, spatial diversity can be achieved by exploiting the relaying capabilities of the involved relay nodes, which may

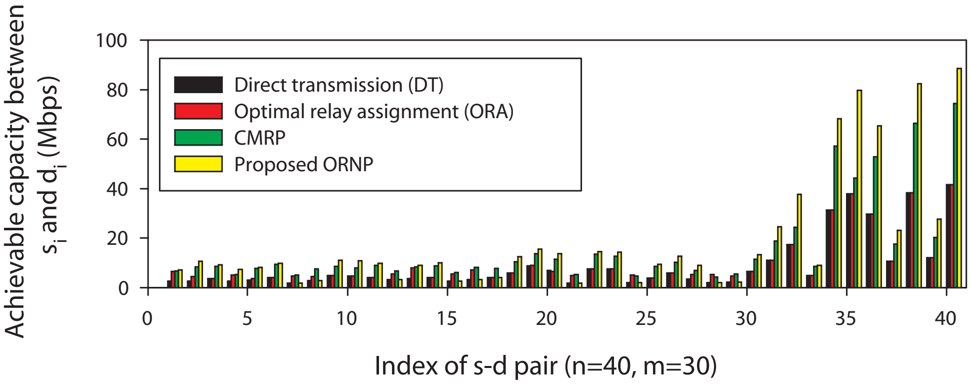


FIGURE 4.8: Achievable capacity in a multi-pair cooperative network when $n > m$.

vastly enhance the achieved system capacity. The potential gains largely depend on the location of relay nodes.

In this chapter, we study the relay node placement problem for multi-pair cooperative communication in wireless networks, where a finite number of candidate relay nodes can be placed to help the transmission of multiple source-destination pairs. Our objective is to maximize the system capacity. After formulating the relay node placement problem, we comprehensively study the effect of relay location on cooperative link capacity and show several attractive properties of the considered problem. As the main contribution, we develop a geographic aware relay node placement algorithm which optimally solves the relay node placement problem in polynomial time. The basic idea is to place a set of relay nodes to the optimum locations so as to maximize the system capacity. The efficiency of our proposed algorithm is evaluated by the results of series experimental studies. For a future work, we will consider the cooperative relay placement problem with per-user fairness consideration.

Chapter 5

Secrecy Capacity Maximization for Secure Cooperative Wireless Networks

This chapter investigates secure cooperative communication issue based on the idea of physical layer security. We aim at improving the physical layer security through the techniques of cooperative relaying and cooperative jamming. By characterizing the security performance of the system by secrecy capacity, we study the secrecy capacity maximization problem in cooperative wireless networks with the involvement of multiple malicious eavesdroppers. Specifically, we propose a system model where a set of relay nodes can be exploited by multiple source-destination pairs to achieve physical layer security. We theoretically present a corresponding formulation for the secrecy capacity maximization problem. Then we develop an optimal relay assignment algorithm to solve the problem in polynomial time. To further increase the system secrecy capacity, we exploit the cooperative jamming technique and propose a smart jamming algorithm to interfere the eavesdropping channels. Analysis and experimental results show that our proposed algorithms can significantly improve the system secrecy capacity under various network settings.

This chapter is organized as follows. Section 5.1 introduces the background of physical layer security and the motivation of secrecy capacity maximization for cooperative wireless networks. In Section 5.2, we briefly survey the related work. In Section 5.3, we describe the architecture of our system model and formulate the problem under consideration. We exploit the opportunities of secrecy capacity enhancement brought by relay assignment in Section 5.4. We develop an optimal relay assignment algorithm in Section 5.5. A smart jamming algorithm is presented in Section 5.6. In Section 5.7, we evaluate the efficiency of our proposed algorithms through extensive experiments. Finally, Section 5.8 concludes this chapter and points out the future work.

5.1 Introduction

Earthquakes, forest fires, and other natural disasters often devastate communication infrastructures just when they are most needed to save lives. Wireless networking technology is an appropriate foundation to support communications among different individuals in an emergency situation. However, due to the specific requirements of emergency services and regulations in wireless networks, it imposes many challenges for wireless networks to support emergency communications. On one side, the demand of using communication services increases rapidly after an event of emergency [51]. On the other side, within a disaster area, it is of vital importance for rescue personnel to obtain an accurate and consistent picture of the situation, and to regain control and coordination on the shortest notice. Cooperative networking, which exploits the relaying capability of other wireless devices, has received significant attentions recently as an emerging network design strategy for future wireless networks. Successful cooperative networking is potential to prompt the development of advanced emergency-oriented wireless applications such as disaster recovery, connectivity maintain, interactive multimedia communication, real-time rescue, etc. [52]. Although cooperative networking promises to provide performance enhancements in terms of spatial diversity, increased capacity and improved reliability, it also brings potential security crisis while exploiting the benefits of cooperative communication (CC).

One of the most significant vulnerabilities of cooperative communication is the disclosure of messages while transmission performs cooperatively. It becomes extremely critical for the environments where involve undesired receivers with eavesdropping capabilities. Take the illustrative toy network in Fig. 5.1 as an example, where the eavesdropper can overhear the cooperative transmitting signals generated from the source and forwarded by the relay. Secure communication can be achieved by using classical measurements, such as the cryptographic methods at higher layers [55]. However, the emergence of large-scale, dynamic, and decentralized cooperative wireless networks imposes new challenges on classical security measurements [86, 87]. Besides, due to the additional computational overhead associated with the key distribution and management process, it may be impractical for the energy-limited wireless users to handle while suffering in emergency situations. To this end, researchers have sought novel information theoretic techniques that can secure wireless networks *without* the need for secret keys. One of the most promising ideas is to exploit the wireless channel physical layer characteristics for improving the reliability of wireless transmission against eavesdropping attacks, named as *physical layer security* [54], [56]. Recently, physical layer security has emerged as a key technique for providing trustworthy and reliable future wireless networks and has witnessed a significant growth in the past few years.

This line of work is pioneered by Wyner [57], who introduced the wire-tap channel and established fundamental results of creating perfectly secure communications without relying on secret keys. Wyner showed that when the eavesdropper's channel is a degraded version of the main source-destination channel, the source and destination can exchange perfectly secure messages at a non-zero rate, while the eavesdropper is unable to decode any information. The maximum transmission rate of reliable information secretly sent from the source to the intended destination in the presence of eavesdroppers is termed as *secrecy capacity*. Following Wyner's work, Leung-Yan-Cheong and Hellman in [58] studied the secrecy capacity of the Gaussian wiretap channel. Csiszar and Korner in [59] extended Wyner's approach to the transmission of confidential messages over broadcast channels, which showed that when the destination and the eavesdropper have separate channels, secret communication is possible if the source-eavesdropper channel has a smaller capacity than the source-destination channel. There have been considerable efforts devoted to generalizing physical layer security to the wireless fading channel and to various multi-user scenarios (see e.g., in [54] ch. 6-8 for an overview). Among these literatures, secrecy capacity can be computed by $\max\{(\mathcal{C}_{\mathcal{P}} - \mathcal{C}_{\mathcal{E}}), 0\}$, where $\mathcal{C}_{\mathcal{P}}$ denotes the capacity of the primary channel between source and destination, $\mathcal{C}_{\mathcal{E}}$ denotes the capacity of the eavesdropping channel between source and eavesdropper. Notice that if the eavesdropping channel happens to be better than the primary channel, e.g., $\mathcal{C}_{\mathcal{E}} \geq \mathcal{C}_{\mathcal{P}}$, positive secrecy capacity cannot be achieved. In order words, secret communication cannot be guaranteed.

Recently, the interaction of cooperative diversity concept [64], [65] with secret communication opens opportunity for overcoming this limitation by cooperation, mainly *cooperative relaying* and *cooperative jamming*. By cooperative relaying, a relay node locates closer to the destination provides a higher capacity to the primary channel than the eavesdropping one, which boosts the capacity of the primary channel and decreases the capacity of the eavesdropping channel simultaneously by the assignment of cooperative relays [61], [62], [63]. However, most of the prior works are from the information theory point of view and the relationship between secrecy capacity enhancement and relay assignment process has not been well investigated yet. On the other hand, cooperative jamming technique which introduces intentional interference to the eavesdropping node in order to increase the secrecy capacity has also been developed as an interesting approach for recent secure applications [75], [76], [77]. Unfortunately, these literatures are considering simple models with single source-destination pair or single eavesdropper. Besides, as far as we know, joint cooperative relaying and jamming techniques with the presence of multiple eavesdroppers under cooperative communication aware wireless ad hoc networks (WANETs) have not been well exploited yet.

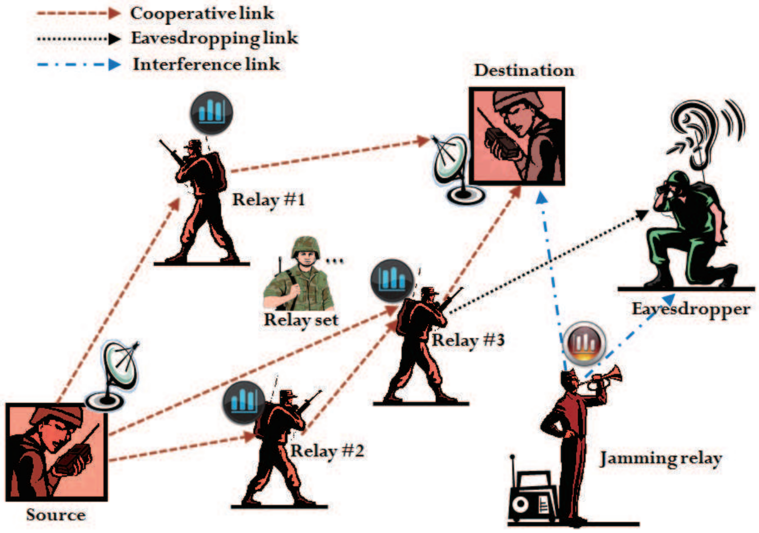


FIGURE 5.1: Illustrative toy topology for a cooperative ad hoc network with a malicious eavesdropper.

In this chapter, we aim at providing secure cooperative networking to support emergency services in CC-aware WANETs where involves multiple unicast sessions and eavesdroppers. The objective of our system design is to maximize the system secrecy capacity through cooperative relaying and jamming techniques. Our motivation is from the cooperative communication scenario in Fig. 5.1. In order to protect the broadcast message and achieve secure cooperative communication, source node can exploit the relay nodes set and choose one or more relays to cooperatively beam-form towards the destination and enable a greater capacity gain in the primary channel than the eavesdropping channel. Thus, the relays that are assigned to help the source-destination pairs have a great impact on the system security performance. One can enhance the system security against eavesdroppers by boosting the capacity of the primary channel and simultaneously decreasing the capacity of the eavesdropping one with an efficient relay assignment procedure. Besides, for the relays which are not assigned to help the transmission between sources and destinations, they can act as friendly jammer to the sources and generate intentional interference to the eavesdroppers. Therefore, the secrecy capacity can be further increased. Motivated by this scenario, we characterize the security performance of the system by secrecy capacity and study the secrecy capacity maximization problem.

This chapter also offers an extension of our previous work [88] for emergency-oriented cooperative ad-hoc environments. In contrast to [88], in which one relay node is assigned to at most one source-destination pair to ensure security, here, we propose a more general model where a relay node can be shared by multiple source-destination pairs and the secrecy capacity enhancement is achieved by the assignment of cooperative relays. Specifically, we present a corresponding formulation for the secrecy capacity maximization problem. After investigating the benefits brought by the cooperative relay assignment procedure, we develop an optimal relay assignment algorithm which solves the problem in polynomial time. Based on the relay assignment results, we exploit the advantages of jamming technique and propose a smart jamming algorithm to further increase the secrecy capacity. In the end, we validate the efficiency of our proposed algorithms by extensive experimental results. The main contributions of this chapter are summarized as follows:

- To the best of our knowledge, we are the *first* to exploit the secure cooperative networking issue for emergency services in CC-aware WANETs with the presence of *multiple eavesdroppers*. We address the system architecture and propose a system model where security enhancement is achieved by the assignment of relays.

- We model the relay assignment problem for secrecy capacity maximization, named RAP-SCAN. Then make comprehensive investigations on the security gain brought by the relay assignment procedure.
- We develop an optimal relay assignment algorithm, called ORA-SCAN, which solves RAP-SCAN in polynomial time.
- We exploit the advantages of jamming technique and propose a smart jamming algorithm to further increase the system secrecy capacity.
- Through extensive experiments, we validate our proposed relay assignment algorithm and jamming algorithm significantly improve the system secrecy capacity, which satisfy the critical security requirements of emergency services under various network settings.

5.2 Related Work

Cooperative networking with the objective to improve the system capacity have attracted extensive attentions during the past half-decade. For instance, in [66]-[68], authors tended to maximize the system capacity through effective cooperative relay assignment. With the objective to support emergency services in WANETs, Han *et al.* proposed two novel networking framework for non-cooperative and cooperative WANETs in [38] and [68], respectively. For cooperative networking methodologies and applications, interested readers can refer to the previous two special issues in [52] and [53]. Most of the prior work failed to provide secure cooperative communication, e.g., in environments where involve undesired receivers with eavesdropping capabilities. Recently, there have been considerable efforts devoted to generalizing physical layer security to the wireless fading channel and to various multi-user scenarios.

In order to provide secure cooperative communication, Dong *et al.* proposed effective decode-and-forward (DF) and amplify-and-forward (AF) based cooperative relaying protocols for physical layer security in [70] and [71], respectively. Aggarwal *et al.* studied the secrecy capacity of a class of orthogonal relay eavesdropper channels in [72]. In their scenario, relay and destination receive the source signals on two orthogonal channels, the destination also receives signals from the relay on its channel, and the eavesdropper overhears either one or both of the orthogonal channels. Tekin *et al.* in [73] considered the scenario where multiple users communicate with a common receiver in the presence of an eavesdropper, and the optimal transmission power allocation policy is chosen to maximize the secrecy sum-rate. Dong *et al.* in [74] used cooperative relays to improve wireless physical layer security in the presence of multiple eavesdroppers, in which they both considered the transmission power minimization problem and secrecy capacity maximization problem. Literature [75] and [77] investigated the joint relay and jammer selection problem for one-way and two-way cooperative relay networks with secrecy constraints, where one or more jammer nodes transmitting simultaneously with the relaying link in order to create artificial interference to degrade the eavesdropper links was analyzed.

Our work in this chapter is different from the aforementioned works in the following aspects: 1) The system models are different. Existing works have mainly focused on the case of single source-destination pair and single eavesdropper, while in this work a more general case with multiple source-destination pairs and multiple eavesdroppers is considered. 2) The problems to be addressed are different. Existing works have primarily concentrated on the analysis of secrecy capacity from an information theoretic point of view. While in this chapter, we focus on improving the system secrecy capacity through a novel cooperative relay assignment process and a smart jamming procedure as well. 3) Our work in this chapter is application-driven. We investigate the potential issues in using secure cooperative networking to support emergency services, which is attracting extensive attentions in practice.

5.3 System Description and Problem Formulation

5.3.1 Emergency-oriented WANET Model

In this chapter, we investigate the secure cooperative networking issue for emergency services in cooperative communication (CC) aware wireless ad-hoc networks (WANETs) with the presence of multiple malicious eavesdroppers. Specifically, we consider a WANET consisting of N individual nodes, with each node being either a source node, a destination node, a potential relay node or an eavesdropping node. We assume that there are N_s

source nodes forming the source set $S = \{s_1, s_2, ...s_{N_s}\}$. Each source node is monitoring under emergency situations and is required to transmit packets to its respective destination. Denote $D = \{d_1, d_2, ...d_{N_d}\}$ as the set of destination nodes. We consider the traffic in the WANET performs as a number of unicast sessions and each source node s_i is paired with a destination node d_i.[1] Thus, we have $N_s = N_d$. Besides, there are N_r relay nodes forming the relay set $R = \{r_1, r_2, ...r_{N_r}\}$ and N_e eavesdropping nodes $E = \{e_1, e_2, ...e_{N_e}\}$ forming the eavesdropper set.[2] We assume that each node is equipped with a single transceiver and can transmit/receive within one channel at a time. In addition, each node can only serve a unique role of source, destination, relay, or eavesdropper at a time, i.e., $N = 2N_s + N_r + N_e$. The eavesdropping nodes are assumed to be *passive* so they do not transmit any signal with the intention of jamming the destinations and only eavesdrops the information transmitted by the sources and relays. We assume that the WANET is cooperative communication aware, that is, the distance between any two nodes in the network is less than the transmission range so that each s-d pair can use direct transmission or cooperative communication. In other words, each transmission can be overheard by all the eavesdropping nodes. An example of a cooperative ad hoc network is shown in Fig. 5.2, which will be used for investigation throughout this chapter. For clarity purpose, we only indicate some of the eavesdropping links in the figure.

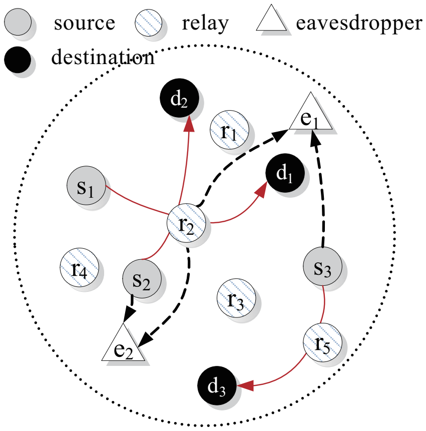


FIGURE 5.2: An example of a cooperative ad hoc network consisting of 3 s-d pairs, 5 relay nodes and 2 eavesdropping nodes, where solid line represents the cooperative link and dash line is the eavesdropping link.

[1] The terms source-destination pair s_i and d_i, s-d pair s_i and d_i, and $\langle s_i, d_i\rangle$ will be used interchangeably throughout this chapter.

[2] In [88], we assume $N_r > N_e$ to guarantee there are sufficient relays for all the sessions. Here, we relax this constraint and allow multiple source-destination pairs can share a common relay node. Besides, the spare relays can act as friendly jammers, which will be discussed in Section 5.6.

A slow, flat, block Rayleigh fading environment is applied [61]. That is, the wireless channel remains static for one coherence interval and changes independently in different coherence intervals with a variance $\sigma_{i,j}^2 = d_{i,j}^{-\alpha}$, where $d_{i,j}$ is the Euclidean distance between node i and j, and α is the pass loss exponent. The channel gain between node i and j is denoted as $h_{i,j}$, which is modeled as a zero-mean, independent, circularly-symmetric complex Gaussian random variable with variance $\sigma_{i,j}^2$. Furthermore, additive white Gaussian noise (AWGN) with power spectral density N_0 is assumed [75]. Thus, when node i transmits a signal to node j with power P_i, the instantaneous signal-to-noise ratio (SNR) seen by node j, denoted by $\gamma_{i,j}$, is $\gamma_{i,j} \triangleq \frac{P_i |h_{i,j}|^2}{N_0} = \frac{P_i d_{i,j}^{-\alpha}}{N_0}$. We assume that the transmission power for all source nodes and relay nodes are P_s and P_r in *Watt*, respectively. The bandwidth of all channels is assume to W in *MHz*. In order to mitigate interference, we make the same assumption as in [66]-[40], where the orthogonal channels are available in the network, e.g., different sources can communicate with their respective destinations at their assigned channels with orthogonal frequency division multiple access (OFDMA) technique, which is proposed for cooperative communication [78].

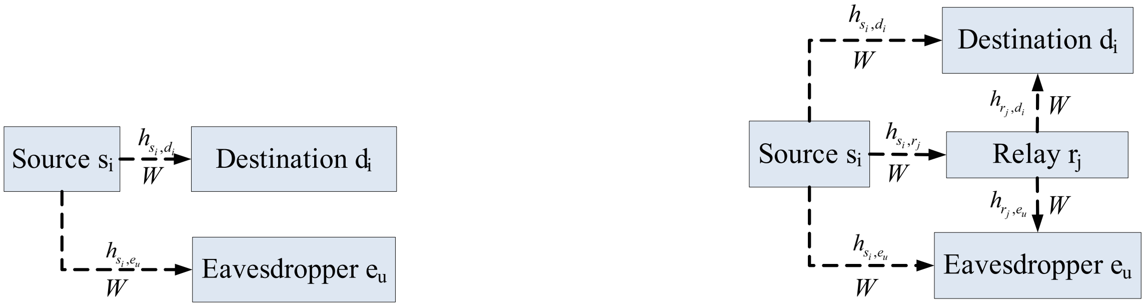
5.3.2 Transmission Model

Following our network model and the discussions in [66] and [79], each source-destination pair can use either direct transmission or cooperative communication with the help of the best relay to achieve full diversity. We define the channel between s_i and d_i (with or without cooperative relay) as *primary channel*, and the channel between s_i and e_u (with or without cooperative relay) as *eavesdropping channel*. When the direct transmission (DT) is applied, the transmission between s_i and d_i can also be overheard by the eavesdroppers, as illustrated in Fig. 5.3(a). The capacity of the primary channel from s_i to d_i and that of the eavesdropping channel from s_i to e_u under DT can be computed by:

$$C_{DT}^{P}\left(s_i, d_i\right) = W \log_2\left(1 + \gamma_{s_i,d_i}\right), \tag{5.1}$$

$$C_{DT}^{E}\left(s_i, e_u\right) = W \log_2\left(1 + \gamma_{s_i,e_u}\right). \tag{5.2}$$

When the cooperative communication (CC) is applied, we adopt the model proposed in [64] where transmission proceeds in a frame-by-frame basis and each frame is divided



(a) Direct transmission

(b) Cooperative communication

FIGURE 5.3: Wireless channels with the presence of eavesdropping node.

into two phases: (a) broadcast phase, and (b) cooperative phase. During the broadcast phase, source s_i transmits the signal to its dedicated destination d_i. Due to the broadcast nature of wireless communication, this transmission can also be overheard by the relay nodes in R and eavesdropping nodes in E. During the cooperative phase, at most one relay node is assigned to source-destination pair $\langle s_i, d_i \rangle$. In contrast to [88], where we assume that each source-destination pair is assigned a different relay. Here, we extend the model and analyze the situation when multiple source-destination pairs share a same relay. Depending on how the relay node processes the overheard signal, there are mainly two cooperative communication modes: Amplify-and-Forward (AF) and Decode-and-Forward (DF). We say that relay node r_j is *assigned* to source-destination pair $\langle s_i, d_i \rangle$ if r_j helps s_i to achieve cooperative communication from s_i to d_i. Denote the relay node assigned to source-destination pair $\langle s_i, d_i \rangle$ in the cooperative phase by $\mathcal{R}(s_i)$. Let $\mathcal{S}(\mathcal{R}(s_i))$ denote the set of s-d pairs to which $\mathcal{R}(s_i)$ is assigned for cooperative communication. For the case when multiple s-d pairs share one relay node, i.e., $|\mathcal{S}(\mathcal{R}(s_i))| > 1$, where $|X|$ is the cardinality of set X, we assume that each relay node equally provides service to all the s-d pairs employing it. This can be achieved, for example, by using a reservation-based TDMA scheduling and the shared relay node serves each s-d pair in a round-robin fashion [67]. According to [61] and [75], the achievable capacity of the primary channel between s_i and d_i with an assigned AF or DF relay $\mathcal{R}(s_i)$ can be expressed as Eqn. (5.3) and Eqn. (5.5). During cooperative communication, the eavesdropping nodes can also overhear the transmitting signals in both of the two phases. Similarly, the achievable capacity of the eavesdropping channel between s_i and e_u with an assigned AF or DF relay $\mathcal{R}(s_i)$ can be expressed as Eqn. (5.4) and Eqn. (5.6).

$$C_{AF}^{P}\left(\mathcal{R}(s_i)\right)=\frac{1}{|\mathcal{S}(\mathcal{R}(s_i))|}\frac{W}{2}\log_2\left(1+\gamma_{s_i,d_i}+\frac{\gamma_{s_i,\mathcal{R}(s_i)}\gamma_{s_i,d_i}}{\gamma_{s_i,\mathcal{R}(s_i)}+\gamma_{\mathcal{R}(s_i),d_i}+1}\right), \tag{5.3}$$

$$C_{AF}^{E}\left(\mathcal{R}(s_i),e_u\right)=\frac{1}{|\mathcal{S}(\mathcal{R}(s_i))|}\frac{W}{2}\log_2\left(1+\gamma_{s_i,e_u}+\frac{\gamma_{s_i,\mathcal{R}(s_i)}\gamma_{s_i,e_u}}{\gamma_{s_i,\mathcal{R}(s_i)}+\gamma_{\mathcal{R}(s_i),e_u}+1}\right), \tag{5.4}$$

$$C_{DF}^{P}\left(\mathcal{R}(s_i)\right)=\frac{1}{|\mathcal{S}(\mathcal{R}(s_i))|}\frac{W}{2}\min\left\{\log_2\left(1+\gamma_{s_i,\mathcal{R}(s_i)}\right),\ \log_2\left(1+\gamma_{s_i,d_i}+\gamma_{\mathcal{R}(s_i),d_i}\right)\right\}, \tag{5.5}$$

$$C_{DF}^{E}\left(\mathcal{R}(s_i),e_u\right)=\frac{1}{|\mathcal{S}(\mathcal{R}(s_i))|}\frac{W}{2}\min\left\{\log_2\left(1+\gamma_{s_i,\mathcal{R}(s_i)}\right),\ \log_2\left(1+\gamma_{s_i,e_u}+\gamma_{\mathcal{R}(s_i),e_u}\right)\right\}. \tag{5.6}$$

Secrecy capacity is defined as the maximum transmission rate of the involved s-d pair at which the eavesdropper is unable to decode any information. For our predefined model, secrecy capacity can be computed by the differences between the Shannon capacity of primary channel and that of the eavesdropping channel [60]. Let $C_{DT}^{S}(s_i,e_u)$ denote the secrecy capacity between s-d pair $\langle s_{i,}d_i\rangle$ and eavesdropping node e_u under direct transmission, it can be computed by:

$$C_{DT}^{S}(s_i,e_u)=\left[C_{DT}^{P}\left(s_i,d_i\right)-C_{DT}^{E}\left(s_i,e_u\right)\right]^{+}, \tag{5.7}$$

where $[x]^{+}\triangleq\max\{0,x\}$. Similarly, the secrecy capacity between s-d pair $\langle s_{i,}d_i\rangle$ and eavesdropping node e_u with an assigned AF or DF relay $\mathcal{R}(s_i)$ can be expressed as:

$$C_{AF}^{S}(\mathcal{R}(s_i),e_u)=\left[C_{AF}^{P}\left(\mathcal{R}(s_i)\right)-C_{AF}^{E}\left(\mathcal{R}(s_i),e_u\right)\right]^{+}, \tag{5.8}$$

$$C_{DF}^{S}(\mathcal{R}(s_i),e_u)=\left[C_{DF}^{P}\left(\mathcal{R}(s_i)\right)-C_{DF}^{E}\left(\mathcal{R}(s_i),e_u\right)\right]^{+}. \tag{5.9}$$

Take the network in Fig. 5.2 as an example, if the achievable transmission rate of the primary channel from s_1 to d_1 under direct transmission is 8 $Mbps$, and that of the eavesdropping channel from s_1 to eavesdropping node e_1 is 9 $Mbps$, the secrecy capacity between $\langle s_{1,}d_1\rangle$ and eavesdropping node e_1 under direct transmission is $[8-9]^{+}=0$. In other words, with the presence of eavesdropper e_1, reliable information can not be directly sent from s_1 to d_1 under a nonzero rate. For the same s-d pair, consider the involvement of cooperative relay node r_2 under AF mode, if $C_{AF}^{P}(r_2)=13Mbps$ and $C_{AF}^{E}(r_2,e_1)=10Mbps$, then the secrecy capacity between $\langle s_{1,}d_1\rangle$ and e_1 with relay r_2 under AF mode $C_{AF}^{S}(r_2,e_1)$ is $[13-10]^{+}=3Mbps$. Hence, with the presence of e_1 and involvement of r_2, the maximum transmission rate of reliable information sent from s_1 to d_1 is 3 $Mbps$.

5.3.3 Problem Formulation

Following the previous definitions, we first give the secrecy capacity expression between an *s*-*d* pair $\langle s_{i,} d_i \rangle$ and an eavesdropper e_u, denoted by $C^S\left(s_i, e_u\right)$:

$$C^S\left(s_i, e_u\right) = \delta_{i,j} \cdot C^S_{CC}\left(\mathcal{R}(s_i), e_u\right) + \left(1 - \delta_{i,j}\right) \cdot C^S_{DT}\left(s_i, e_u\right), \tag{5.10}$$

where $\delta_{i,j} \in \{0, 1\}$ is a binary variable to characterize whether a cooperative relay r_j is assigned to $\langle s_{i,} d_i \rangle$, i.e., if $\mathcal{R}(s_i) = r_j$, $\delta_{i,j} = 1$, otherwise, $\delta_{i,j} = 0$, and $C^S_{CC}\left(\mathcal{R}(s_i), e_u\right)$ is the secrecy capacity between $\langle s_{i,} d_i \rangle$ and e_u under AF or DF mode, i.e., $C^S_{CC}\left(\mathcal{R}(s_i), e_u\right) = C^S_{AF}\left(\mathcal{R}(s_i), e_u\right)$ if AF is used and $C^S_{CC}\left(\mathcal{R}(s_i), e_u\right) = C^S_{DF}\left(\mathcal{R}(s_i), e_u\right)$ if DF is used.

As there are multiple eavesdroppers in the network, the transmission rate between an *s*-*d* pair is restricted by the minimum secrecy capacity among all eavesdroppers. It is reasonable to focus on the *minimum* secrecy capacity between the dedicated *s*-*d* pair and all the eavesdroppers.

Definition 5.3.1 (Secrecy capacity for a single pair). The secrecy capacity for *s*-*d* pair $\langle s_{i,} d_i \rangle$ is the minimum secrecy capacity between $\langle s_{i,} d_i \rangle$ and all eavesdroppers, which is the maximum transmission rate at which all eavesdroppers are unable to decode any transmitting information from s_i to d_i:

$$C^S\left(s_i\right) = \min_{e_u \in E} \left\{ C^S\left(s_i, e_u\right) \right\}. \tag{5.11}$$

Therefore, the secrecy capacity for the predefined ad-hoc network consisting of N_s *s*-*d* pairs, N_r relay nodes and N_e eavesdropping nodes, is defined as the total secrecy capacity of all *s*-*d* pairs:

$$C^S_{sum}\left(\left(S, D\right), R, E\right) = \sum\nolimits_{s_i \in S} C^S\left(s_i\right). \tag{5.12}$$

Next we address the **R**elay **A**ssignment **P**roblem for secrecy capacity maximization in **S**ecure **C**ooperative **A**d-hoc **N**etworks (**RAP-SCAN**) as follows.

Definition 5.3.2 (RAP-SCAN). Given a set of source-destination pairs (S, D), a set of relay nodes R and a set of eavesdropping nodes E, RAP-SCAN seeks for a relay assignment profile such that the system secrecy capacity $C^S_{sum}\left(\left(S, D\right), R, E\right) = \sum_{s_i \in S} C^S\left(s_i\right)$ is maximized among all the possible relay assignment profiles.

According to the above definitions and discussions, we theoretically formulate RAP-SCAN as the following optimization problem:

$$(\textbf{RAP-SCAN}) \;\; \text{Maximize} \;\; C_{sum}^{S}\left(\left(S, D\right), R, E\right) \tag{5.13}$$

subject to:

$$\delta_{i,j} = \begin{cases} 1, & \text{if } \mathcal{R}(s_i) = r_j, \\ 0, & \text{otherwise.} \end{cases} \tag{5.14a}$$

$$\sum_{i=1}^{N_s} \delta_{i,j} = |\mathcal{S}(\mathcal{R}(s_i))| \quad \left(s_i \in S, r_j \in R\right), \tag{5.14b}$$

$$\sum_{j=1}^{N_r} \delta_{i,j} \leq 1 \quad \left(s_i \in S, r_j \in R\right), \tag{5.14c}$$

$$\begin{aligned} \Phi_{CSI} = & \left\{\gamma_{s_i,d_i}, \gamma_{s_i,r_j}, \gamma_{r_j,d_i}, \gamma_{s_i,e_u}, \gamma_{r_j,e_u}\right\} \\ & \left(\forall s_i \in S, d_i \in D, r_j \in R, e_u \in E\right). \end{aligned} \tag{5.14d}$$

where Eqn. (5.14a) specifies the binary variable $\delta_{i,j}$, Eqn. (5.14b) specifies that each relay node can be assigned to multiple s-d pairs, Eqn. (5.14c) specifies that each s-d pair can only choose at most one relay node for cooperative communication, Eqn. (5.14d) indicates that the global Channel State Information (CSI) is available [75] and [77]. Φ_{CSI} includes all channel information between sources and destinations, sources and relays, relays and destinations, sources and eavesdroppers, and relays and eavesdroppers.

Notice that the solution of RAP-SCAN is a matrix consisting of $n \times m$ decision variables $\delta_{i,j}$. Due to the possibility that sharing a common relay node among multiple s-d pairs, it is not clear how to reduce the formulated RAP-SCAN into an integer linear programming problem. Ahead of solving the formulated problem, we first study the properties of it by exploiting the conditions when the relay assignment procedure can benefit the system secrecy capacity.

5.4 Secrecy Capacity Gain from Cooperative Relay Assignment

The basic idea of secure cooperative communication (CC) is that after amplifying or decoding the signals, the cooperative relay and source can *beam-form* towards the destination to enable a greater capacity gain in the primary channel than the eavesdropping one. According to the previous formulations, it is not easy to observe whether cooperative relay assignment can benefit the secrecy capacity. In this section, we analyze the secrecy capacity gain brought by cooperative relay assignment and exploit the opportunities of secrecy capacity enhancement.

5.4.1 Maximum Primary Channel Capacity Under CC

As the secrecy capacity is defined as the difference between the capacity of the primary channel and that of the eavesdropping channel, intuitively, who want to obtain the maximum secrecy capacity can exploit maximizing the achievable capacity of the primary channel and minimizing that of the eavesdropping channel at the same time. Here, we first derive the achievable upper bound of the primary channel under cooperative AF and DF mode.

Lemma 5.1 (Maximum capacity of the primary channel)**.** *The maximum capacity of the primary channel between* s-d *pair s_i and d_i can be achieved by solving the following optimization problems:*

$$\text{AF mode}: \qquad r_j^{*}{=}\arg\max\left\{\frac{\gamma_{s_i,r_j}\gamma_{r_j,d_i}}{\gamma_{s_i,r_j}+\gamma_{r_j,d_i}+1}\right\} \tag{5.15}$$

$$\text{DF mode}: r_j^{*}{=}\arg\max\left\{\min\left\{\gamma_{s_i,r_j},\gamma_{s_i,d_i}{+}\gamma_{r_j,d_i}\right\}\right\} \tag{5.16}$$

subject to:

$$d_{s_i,r_j}+d_{r_j,d_i}=d_{s_i,d_i}. \tag{5.17}$$

Proof. See the proof of Lemma 4.1 in Chapter 4. □

According to the above Lemma, we can obtain the maximum capacity of the primary channel be solving the formulated sub-problems. Unfortunately, as the relay nodes are randomly distributed in the network, a source node can not always exploit the*best located* relay to assist its transmission towards the dedicated destination in order to achieve maximum cooperative link capacity. On the other hand, one can observe that the capacity formulations of the eavesdropping channel under cooperative communication have the similar form as that of the primary channel. It is hard to obtain the maximum secrecy capacity by maximizing Eqn. (5.3) and (5.5), and minimizing Eqn. (5.4) and (5.6) at the same time. Therefore, an efficient relay assignment procedure is quite needed and the secrecy capacity gain brought by the cooperative relays should be well investigated.

5.4.2 Secrecy Capacity Gain Under CC-AF Mode

Under AF mode, the relay node first amplifies the received signals from the source and then cooperates with the source to transmit the secret information to the destination. According our previous discussions, the secrecy capacity between *s*-*d* pair $\langle s_i, d_i \rangle$ and eavesdropping node e_u with an assigned AF relay is expressed in Eqn. (5.8). It is not obvious to observe the benefits brought by the involved AF relay. We first consider the case when the secrecy capacity between *s*-*d* pair $\langle s_i, d_i \rangle$ and eavesdropping node e_u under direct transmission is zero, i.e., the eavesdropping channel is better than the primary channel ($\gamma_{s_i,e_u} > \gamma_{s_i,d_i}$). The following lemma indicates the opportunities of secrecy capacity enhancement brought by the assigned AF relay node $\mathcal{R}(s_i) = r_j$.

Lemma 5.2. *In the case when the secrecy capacity between* s-d *pair* $\langle s_i, d_i \rangle$ *and eavesdropping node* e_u *under direct transmission is zero, i.e.,* $C^S_{DT}(s_i, e_u) = 0$*,* positive *secrecy capacity can be achieved if the involved AF relay node satisfies the following channel condition:*

$$\frac{\gamma_{s_i,r}\left(1+\gamma_{s_i,r}\right)\left(\gamma_{r,d}-\gamma_{r,e_u}\right)}{\left(1+\gamma_{s_i,r}+\gamma_{r,d}\right)\left(1+\gamma_{s_i,r}+\gamma_{r,e_u}\right)} > \gamma_{s_i,e_u} - \gamma_{s_i,r}. \tag{5.18}$$

Proof. The proof of the above lemma can be obtained by calculating $C^S_{AF}(\mathcal{R}(s_i), e_u) > 0$ in Eqn. (5.8). □

The above lemma indicates that the involved AF relay not only provides additional channel to transmit the secret information, but it also compensates the secret information loss at the source [80]. We can achieve nonzero secrecy capacity under AF mode with large γ_{s_i,r_j} and enough secret information compensation, i.e., $\gamma_{r_j,d_i} - \gamma_{r_j,e_u} \gg \gamma_{s_i,e_u} - \gamma_{s_i,d_i}$.

5.4.3 Secrecy Capacity Gain Under CC-DF Mode

Under DF mode, the relay first decodes the received signals from the source and then cooperates with the source to transmit the secret information to the destination. Similar as the analysis under AF mode, we consider the secrecy capacity brought by the involvement of DF relay when $\gamma_{s_i,e_u} > \gamma_{s_i,d_i}$.

Lemma 5.3. *In the case when the secrecy capacity between* s-d *pair* $\langle s_i, d_i\rangle$ *and eavesdropping node* e_u *under direct transmission is zero, i.e.,* $C^S_{DT}(s_i, e_u) = 0$*,* positive *secrecy capacity can be achieved if the involved DF relay node* r_j *satisfies the following channel conditions:*

$$\begin{cases} \gamma_{r_j,d_i} - \gamma_{r_j,e_u} > \gamma_{s_i,e_u} - \gamma_{s_i,d_i} \\ \gamma_{s_i,r_j} > \gamma_{s_i,e_u} + \gamma_{r_j,e_u} \end{cases} \tag{5.19}$$

Proof. The proof of the above lemma can be obtained by extending the secrecy capacity formula in Eqn. (5.9) into the following four cases:

1) $\gamma_{s_i,r_j} > \gamma_{s_i,d_i} + \gamma_{r_j,d_i}$, $\gamma_{s_i,r_j} > \gamma_{s_i,e_u} + \gamma_{r_j,e_u}$. From Eqn. (5.9), it is not hard to observe that $C^S_{DF}(\mathcal{R}(s_i), e_u)>0$ can be achieved if $\gamma_{r_j,d_i}-\gamma_{r_j,e_u}>\gamma_{s_i,e_u}-\gamma_{s_i,d_i}$.

2) $\gamma_{s_i,r_j} < \gamma_{s_i,d_i} + \gamma_{r_j,d_i}$, $\gamma_{s_i,r_j} > \gamma_{s_i,e_u} + \gamma_{r_j,e_u}$. Similar with the previous case, $C^S_{DF}(\mathcal{R}(s_i), e_u) > 0$ can be achieved if $\gamma_{s_i,r_j} > \gamma_{s_i,e_u} + \gamma_{r_j,e_u}$.

3) $\gamma_{s_i,r_j} > \gamma_{s_i,d_i} + \gamma_{r_j,d_i}$, $\gamma_{s_i,r_j} < \gamma_{s_i,e_u} + \gamma_{r_j,e_u}$. Under this case, the capacity of the primary channel $C^P_{DF}(\mathcal{R}(s_i))$ is $\frac{W}{2}\log_2\left(1 + \gamma_{s_i,d_i} + \gamma_{r_j,d_i}\right)$, and the capacity of the eavesdropping channel $C^E_{DF}(\mathcal{R}(s_i), e_u)$ is $\frac{W}{2}\log_2\left(1 + \gamma_{s_i,r_j}\right)$. It is clear that nonzero rate can not be achieved under the assumption that $\gamma_{s_i,r_j} > \gamma_{s_i,d_i} + \gamma_{r_j,d_i}$.

4) $\gamma_{s_i,r_j} < \gamma_{s_i,d_i}+\gamma_{r_j,d_i}$, $\gamma_{s_i,r_j} < \gamma_{s_i,e_u}+\gamma_{r_j,e_u}$. Similar with Case 3, the secrecy capacity $C^S_{DF}(\mathcal{R}(s_i), e_u) = 0$ under these assumptions.

To this end, we derive the channel conditions under which positive secrecy capacity can be achieved (under Case 1 and 2). Therefore, we complete the proof. □

To this end, let us look back into the formulated problem. From the above two lemmas, we observe that whether cooperative relay assignment benefits the secrecy capacity greatly depends on the involved relay nodes.

5.5 An Optimal Relay Assignment Algorithm

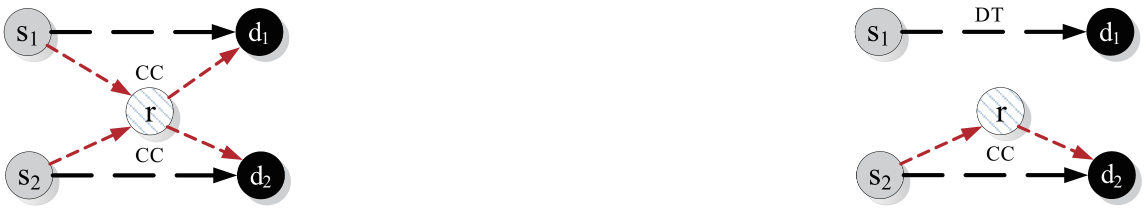
In the previous section, we have discussed the secrecy capacity gain brought by the cooperative relay assignment process and exploit the opportunities of secrecy capacity enhancement by the relay assignment. Although it is not hard to assign a relay to a dedicated *s*-*d* pair with secrecy consideration, relay assignment with a great amount of *s*-*d* pairs and multiple eavesdroppers is a challenging issue. Besides, advanced emergency-oriented wireless applications calls for time-efficient and effective networking strategies to improve the system operation efficiency and reliability. In this section, by discussing with the multi-pair cooperative communication, we develop an optimal relay assignment algorithm named ORA-SCAN, which is able to solve RAP-SCAN in polynomial time.

5.5.1 Multi-pair Cooperative Communication

For the case when multiple *s*-*d* pairs share a common relay, we are more interested in whether this sharing will deteriorate the system secrecy capacity [69]. The following lemma indicates us how we can improve the system secrecy capacity if there exists a relay node shared by multiple *s*-*d* pairs.

Lemma 5.4. *If a relay node r_j is shared by multiple* s-d *pairs, we can improve the system secrecy capacity by the following* double-step *adjustment: i) let the* s-d *pair with the minimum secrecy capacity among all the pairs sharing r_j use direct transmission; ii) keep other* s-d *pairs' relay assignment profile the same.*

Proof. Let $C^S_{sum}(\delta)$ and $C^S_{sum}(\delta')$ denote the system secrecy capacity before and after applying the above adjustment, respectively. Let $\langle s_i, d_i\rangle$ denote the *s*-*d* pair with the minimum secrecy capacity among the *s*-*d* pairs sharing r_j. $\mathcal{S}$ and $\mathcal{S}'$ denote the set of source nodes sharing the relay node r_j before and after applying the above adjustment. Notice that



(a) Before adjustment

(b) After adjustment

FIGURE 5.4: Multi-pair cooperative communication with a common relay node.

$\mathcal{S}' = \mathcal{S} \backslash \{s_i\}$. Comparing the system secrecy capacity, we have:

$$\begin{aligned}
&C^S_{sum}\left(\delta'\right) - C^S_{sum}\left(\delta\right) \\
&= C^S_{DT}\left(s_i, e_u\right) + \sum_{s_k \in \mathcal{S}'} \frac{C^S_{CC}(\mathcal{R}(s_k),e_u)}{|\mathcal{S}'|} - \sum_{s_k \in \mathcal{S}} \frac{C^S_{CC}(\mathcal{R}(s_k),e_u)}{|\mathcal{S}|} \\
&= C^S_{DT}\left(s_i, e_u\right) + \sum_{s_k \in \mathcal{S}'} \frac{C^S_{CC}(\mathcal{R}(s_k),e_u)}{|\mathcal{S}|-1} \\
&\quad - \left(\sum_{s_k \in \mathcal{S}'} \frac{C^S_{CC}(\mathcal{R}(s_k),e_u)}{|\mathcal{S}|} + \frac{C^S_{CC}(\mathcal{R}(s_i),e_u)}{|\mathcal{S}|} \right) \\
&= C^S_{DT}\left(s_i, e_u\right) + \left(\frac{\sum\limits_{s_k \in \mathcal{S}'} C^S_{CC}(\mathcal{R}(s_k),e_u)}{|\mathcal{S}| \cdot (|\mathcal{S}|-1)} - \frac{C^S_{CC}(\mathcal{R}(s_i),e_u)}{|\mathcal{S}|} \right) \\
&= C^S_{DT}\left(s_i, e_u\right) + \left(\frac{\sum\limits_{s_k \in \mathcal{S}'} C^S_{CC}(\mathcal{R}(s_k),e_u) - (|\mathcal{S}|-1) \cdot C^S_{CC}(\mathcal{R}(s_i),e_u)}{|\mathcal{S}| \cdot (|\mathcal{S}|-1)} \right) \\
&> C^S_{DT}\left(s_i, e_u\right) \geq 0
\end{aligned}$$

For the last second step of the above derivation, as $\langle s_i, d_i \rangle$ is the s-d pair with the minimum secrecy capacity before adjustment, we have

$$\sum_{s_k \in \mathcal{S}'} C^S_{CC}\left(\mathcal{R}\left(s_k\right), e_u\right) - \left(|\mathcal{S}| - 1\right) \cdot C^S_{CC}\left(\mathcal{R}\left(s_i\right), e_u\right) > 0.$$

Moreover, based on the definition of secrecy capacity, we have $C^S_{DT}\left(s_i, e_u\right) \geq 0$, as expressed in the last step of the above derivation. Therefore, the right side of the above equation is greater than 0. In other words, the secrecy capacity after adjustment $C^S_{sum}\left(\delta'\right)$ is greater than that before adjustment $C^S_{sum}\left(\delta\right)$. Thus, we complete the proof. □

Consider the sample cooperative ad hoc network in Fig. 5.2, the multi-pair cooperative communication before and after adjustment are illustrated in Fig. 5.4(a) and Fig. 5.4(b). During the adjustment, the *s*-*d* pair with the minimum secrecy capacity, say $\langle s_1, d_1 \rangle$, is adjusted from sharing cooperative relay node r_2 to using direct transmission.

Following our predefined system model, each source node will be either assigned a relay node for cooperative transmission or transmit to the destination directly. On the other hand, based on Lemma 5.4, we can always improve the system secrecy capacity by applying the double-step adjustment. Thus, each relay node will be assigned to at most one s-d pair in order to achieve maximum total secrecy capacity. This one-to-one matching relation indicates that we can relaxed the constraint in Eqn. (5.14b) to:

$$\sum_{i=1}^{N} \delta_{i,j} \leq 1 \quad (s_i \in S, r_j \in R)\,. \tag{5.20}$$

5.5.2 Motivating Example

Consider the cooperative ad hoc network in Fig. 5.2, the secrecy capacity between each *s*-*d* pair and eavesdropping node e_1 under the direct transmission and the cooperative communication are illustrated in TABLE 5.1 and TABLE 5.2, respectively. Under direct transmission, the secrecy capacity between $\langle s_{1,} d_1 \rangle$ and e_1 is 0, between $\langle s_{3,} d_3 \rangle$ and e_1 is 1. After a random relay assignment, e.g., $\mathcal{R}(s_1) = r_2$, $\mathcal{R}(s_2) = r_1$ and $\mathcal{R}(s_3) = r_5$, the secrecy capacity between $\langle s_{1,} d_1 \rangle$ and e_1 increases to 3, between $\langle s_{3,} d_3 \rangle$ and e_1 increases to 7. However, the secrecy capacity between $\langle s_{2,} d_2 \rangle$ and e_1 decreases from 2 to 0. In other words, this relay assignment profile benefits *s*-*d* pair $\langle s_{1,} d_1 \rangle$ and $\langle s_{3,} d_3 \rangle$, but harms $\langle s_{2,} d_2 \rangle$. Although it is hard to evaluate whether such an assignment profile is good or not, it inspires us to seek for an optimal relay assignment profile that the system secrecy capacity can be maximized.

In TABLE 5.3, we list the secrecy capacity between all *s*-*d* pairs and eavesdropping nodes for the sample network in Fig. 5.2. Secrecy capacity is denoted as a two dimensional vector, $(C^S(s_i, e_1), C^S(s_i, e_2),)$ $(1 \leq i \leq 3)$. Notice that the dimension of the vector here is the number of eavesdropping nodes k. Each highlighted cell represents the secrecy capacity under the current assignment, which is the minimum one among all of the k results. For example, $C^S(s_1, e_1) = 0$ (under direction transmission) and $C^S(s_1, e_1) = 2$ (with assigned relay r_1). With the secrecy capacity for each s-d pair in mind, any relay assignment algorithms with the objective to maximize the system secrecy capacity seek for a proper assignment profile for each s-d pair. Following our predefined system model and Lemma 5.4, each source node will be either assigned a relay node for cooperative transmission or transmit to the destination directly. This one-to-one matching relation indicates that we can map any instance of RAP-SCAN into that of the *Maximum Weighted Bipartite Matching* (MWBM) problem [81] and use corresponding algorithms to solve it.

Table 5.1: Secrecy capacity under direct transmission (*Mbps*).

	$C^P_{DT}(s_i, d_i)$	$C^E_{DT}(s_i, e_1)$	$C^S_{DT}(s_i, e_1)$
$< s_1, d_1 >$	8	9	0
$< s_2, d_2 >$	10	8	2
$< s_3, d_3 >$	10	9	1

Table 5.2: Secrecy capacity with an assigned cooperative relay (*Mbps*).

	$\mathcal{R}(s_i)$	$C^P_{CC}(\mathcal{R}(s_i))$	$C^E_{CC}(\mathcal{R}(s_i), e_1)$	$C^S_{CC}(\mathcal{R}(s_i), e_1)$
$< s_1, d_1 >$	r_2	13	10	$\boxed{3}$
$< s_2, d_2 >$	r_1	14	15	0
$< s_3, d_3 >$	r_5	15	8	$\boxed{7}$

Table 5.3: Secrecy capacity under cooperative communication (*Mbps*).

s-d pair	$\mathcal{R}(s_i)$					
	$\emptyset$	r_1	r_2	r_3	r_4	r_5
$< s_1, d_1 >$	(0, 2)	(2, 4)	(3, 3)	(0, 0)	(1, 0)	(0, 0)
$< s_2, d_2 >$	(2, 1)	(0, 0)	(3, 2)	(0, 0)	(4, 0)	(0, 0)
$< s_3, d_3 >$	(1, 4)	(0, 0)	(0, 0)	(2, 3)	(0, 0)	(7, 5)

5.5.3 Algorithm Details

For any instance $((S, D), R, E)$ of RAP-SCAN, we construct an instance $G = (U, V, w)$ of the MWBM problem as follows. Let a set U of vertices represents the source nodes set S,

TABLE 5.4: Optimum assignment profiles for Fig. 5.2.

(a) $C^S_{sum} = 3 + 1 + 5 = 9Mbps$

s_i	$\mathcal{R}(s_i)$					
	$\emptyset$	r_1	r_2	r_3	r_4	r_5
s_1	0	2	3	0	0	0
s_2	1	0	2	0	0	0
s_3	1	0	0	2	0	5

(b) $C^S_{sum} = 2 + 2 + 5 = 9Mbps$

s_i	$\mathcal{R}(s_i)$					
	$\emptyset$	r_1	r_2	r_3	r_4	r_5
s_1	0	2	3	0	0	0
s_2	1	0	2	0	0	0
s_3	1	0	0	2	0	5

and a set V of vertices represents $D \cup R$. Then we set $w(s_i, r_j) = \min_{e_u \in E} \{C^S_{CC}(s_i, e_u)\}$ $(r_j = \mathcal{R}(s_i))$, and set $w(s_i, d_i) = \min_{e_u \in E} \{C^S_{DT}(s_i, e_u)\}$ for all $s_i \in U$, $d_i \in V$. The corresponding MWBM instance for Fig. 5.2 is shown in Fig. 5.5. In order to have a clear view of the conversion, we also label the involved eavesdropping node with the minimum secrecy capacity together with the weight on the edge, e.g., e^*_u is the labeled eavesdropping node and $e^*_u = \arg\min_{e_u \in E} \{C^S(s_i, e_u)\}$.

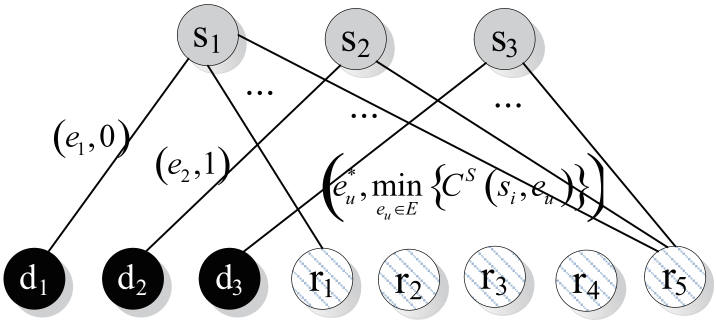


FIGURE 5.5: Mapping RAP-SCAN into the MWBM problem.

We present our proposed **O**ptimal **R**elay **A**ssignment algorithm for **S**ecure **C**ooperative **A**d-hoc **N**etworks, named **ORA-SCAN**, as illustrated in Algorithm 3. Next we prove the correctness and analyze the computational complexity of our proposed algorithm by the following theorem.

Theorem 5.5.1. The proposed ORA-SCAN algorithm guarantees to find an optimal cooperative relay assignment profile for RAP-SCAN in time bounded by $O(N_s^2 N_r)$.

Proof. We prove the correctness of ORA-SCAN by contradiction. Following the formulated

```
Algorithm 3: Optimal Relay Assignment for Secrecy Capacity Maximization (ORA-SCAN)
Input: Source nodes set $S$, destination nodes set $D$, relay nodes set $R$ and eavesdropping
       nodes set $E$.
Output: A relay assignment matrix $\delta_{n\times m}$ consisting of decision variables
        $\delta_{i,j}\,(1 \le i \le n, 1 \le j \le m)$.
1  Construct a set $U$ of $n$ vertices corresponding to $S$;
2  Construct a set $V$ of $n+m$ vertices corresponding to $D \cup R$;
3  for $i=0, j=0; i<n, j<m$ do
4      $\delta_{i,j}=0$;
5  end
6  for $i=1; i \le n$ do
7      Connect the vertices $s_i$ in $U$ and $d_i$ in $V$ and label the weight
       $w\,(s_i, d_i) = \min\limits_{e_u \in E} \left\{C_{DT}^{S}\,(s_i, e_u)\right\}$;
8  end
9  for $\forall s_i \in U$ and $\forall r_j \in V$ do
10     Connect the vertices $s_i$ in $U$ and $r_j$ in $V$ and label the weight
       $w\,(s_i, r_j) = \min\limits_{e_u \in E} \left\{C_{CC}^{S}\,(s_i, e_u)\right\}\,(r_j = \mathcal{R}(s_i))$;
11 end
12 Apply an MWBM algorithm to find a maximum weighted matching $M^*$ for graph
   $G=(U,V,w)$;
13 for $(s_i, v) \in M^*$ do
14     Reset the resulting assignment profile;
15 end
16 Return $\delta^*_{n\times m}$;
```

RAP-SCAN and our previous discussions, each optimal relay assignment profile for RAP-SCAN can be mapped to a matching in the graph $G=(U,V,w)$, as described from Line 1 to Line 11. Assume that there exists another relay assignment profile δ' which resulting in a higher secrecy capacity than δ^* returned by ORA-SCAN. In other words, there exists another matching M' for G, which has a higher weight than that of M^*. It contradicts the fact that M^* is a maximum weight matching for G. Therefore, it is an optimal relay assignment algorithm.

For the computational time of ORA-SCAN, it is consisted of three parts: mapping time from RAP-SCAN to MWBM (from Line 1 to 11), the running time of the corresponding MWBM algorithm (Line 12) and the resulting variable resetting (from Line 13 to 20). For the first part, the computational time of the secrecy capacity for all s-d pairs is $O\left(N_s N_r N_e\right)$. For the second part, many algorithms have been developed to solve the MWBM problem in polynomial time, such as Dijkstra algorithm with Fibonacci heap and Kuhn-Munkres algorithm [81]. If the Dijkstra algorithm with Fibonacci heap is used, the running time is bounded by $O\left(N_s^2 N_r\right)$. For the third part, the running time is bounded by $O\left(N_s N_r\right)$. Therefore, the running time of ORA-SCAN is bounded by $O\left(N_s N_r N_e + N_s^2 N_r + N_s N_r\right)$. For our system model, as we assume that $N_e \leq N_s$, the running time of ORA-SCAN is bounded by $O(N_s^2 N_r)$. □

One should also notice that there may be multiple optimal relay assignment profiles. For example, two optimal relay assignment profiles for our sample network are illustrated in TABLE 5.4, each of them has the maximum total secrecy capacity, $C_{sum}^S = 9Mbps$.

5.6 Proposed Smart Jamming Algorithm

In order to reduce the capacity of eavesdropping channel, jamming technique which encourages one or more involved nodes to generate artificial interference to the eavesdropping links is drawing extensive interests [76]-[77]. It has been shown that, by carefully scheduling the interaction between relay nodes and jamming nodes, critical secrecy requirements can be achieved. In this section, we exploit the advantages of jamming technique and propose a smart jamming algorithm to further increase the system secrecy capacity.

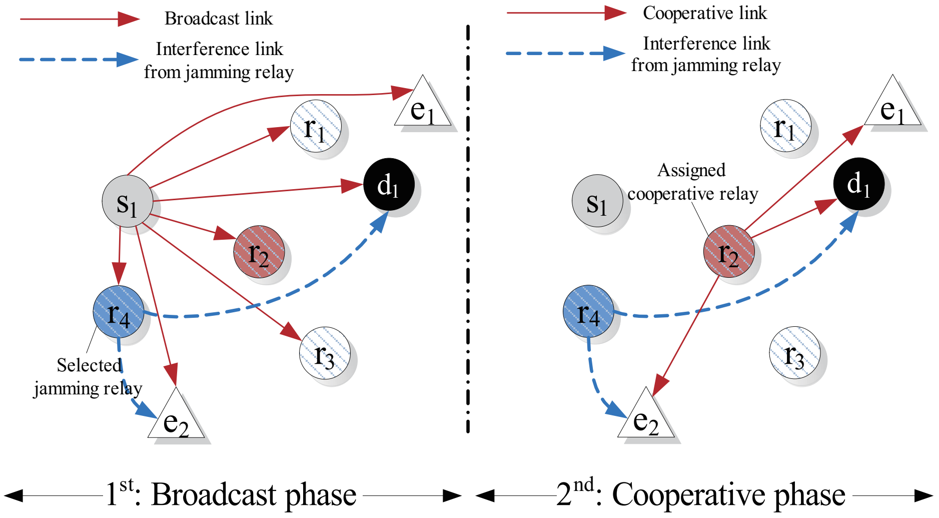


FIGURE 5.6: Cooperative communication phases with a selected friendly jammer.

5.6.1 Transmission Model with Jamming

We modify the two-phase cooperative communication transmission model presented in Section 5.3 and the communication phases are shown in Fig. 5.6. Under the modified model, one or more relays that were not assigned to any s-d pairs during the assignment procedure can be selected to act as friendly jammer(s) to further increase the system secrecy capacity. During the broadcast phase, in order to protect the source's broadcast message, a relay node is selected to act as the friendly jammer, which generates intentional interference towards the eavesdropping nodes. During the cooperative phase, the assigned cooperative relay transmit the source's message towards the destination. The selected jamming relay node acts as a friendly jammer to the s-d pair it is serving, and continues to generate intentional interference towards the eavesdropping nodes. Take the network in Fig. 5.2 as an example, relay node r_4 is not assigned to any s-d pairs after the relay assignment procedure, so it can be selected to serve as a friendly jammer for $\langle s_1, d_1 \rangle$. During the cooperative phase, the assigned cooperative relay node r_2 transmits the data from s_1 to d_1. r_4 acts as a friendly jammer to $\langle s_1, d_1 \rangle$ and generates intentional interference towards eavesdropper e_2. One should also notice that the interference signal generated by the selected jamming relay node can also affect the cooperative links, for example, there is interference from r_4 to d_1 during both phases.

Following our system model, orthogonal channels are applied to all s-d pairs, the selected friendly jammer can use the same channel as the s-d pair it is serving but just generating artificial interference. Thus, the interference signal generated by the friendly jammer will not affect the transmission of other s-d pairs. Furthermore, we assume that the friendly jammer selected in the two communication phases is the same, the selection methodology with involvement of two different jamming nodes in two phases is out of the scope of this chapter.

5.6.2 Algorithm Description

Under the predefined cooperative Decode-and-Forward (DF) mode, if the maximum ratio combiner (MRC) technique [84] is used to combine the two-phase transmissions at the destination, the instantaneous secrecy capacity between $\langle s_i, d_i \rangle$ and e_u with a jamming relay j_v can be expressed as [75]:

$$\begin{aligned} C_{DF}^{S}\left(s_i, e_u, j_v\right) = \Big[& \log_2\left(1+\frac{\gamma_{s_i,d_i}}{1+\beta^{(1)}\gamma_{j_v,d_i}} + \frac{\gamma_{\mathcal{R}(s_i),d_i}}{1+\beta^{(2)}\gamma_{j_v,d_i}}\right) \\ & -\log_2\left(1+\frac{\gamma_{s_i,e_u}}{1+\beta^{(2)}\gamma_{j_v,e_u}} + \frac{\gamma_{\mathcal{R}(s_i),d_i}}{1+\beta^{(2)}\gamma_{j_v,e_u}}\right)\Big]^{+} \end{aligned}, \tag{5.21}$$

where $\beta^{(t)} \in \{0,1\}$ is a binary variable to indicate whether the jamming relay is activated during the t-th phase, t=1 denotes the broadcast phase and t=2 is the cooperative phase, respectively.

Algorithm 4: Friendly jammer selection algorithm

```
Input: An optimal relay assignment profile $\delta^*_{n\times m}$.
Output: A jamming relay selection profile.
$R_J = \emptyset$;
for $i = 0, j = 0; i < n, j < m$ do
    $\lambda^*_{i,j} = 0$;
end
for $j = 1; j \leq m$ do
    if $\sum_{i=1}^{n} \delta_{i,j} = 0$ then
        $R_J = R_J \cup r_j$;
    end
end
while $R_J \neq \emptyset$ do
    Select each $r_j$ from $R_J$;
    for $i = 1, u = 1; i \leq n, u \leq k$ do
        if $\gamma_{r_j,e_u} > \gamma_{r_j,d_i}$ then
            $\lambda^*_{i-1,j-1} = 1$;
        end
    end
    $R_J = R_J - r_j$;
end
Return $\lambda^*_{n\times m}$;
```

As all relay nodes have the global channel state information, the following lemma indicates the condition for an *s*-*d* pair to select an unassigned relay as friendly jammer.

Lemma 5.5. *A relay node that was not assigned to any* s-d *pairs, denoted by r_v, can be selected to act as a friendly jammer for $\langle s_i, d_i\rangle$ if $\gamma_{r_v,e_u} > \gamma_{r_v,d_i}$.*

Proof. It can be derived from comparing Eqn. (5.21) and Eqn. (5.9). The improvement on secrecy capacity when jamming relay involves can be expressed as $C_{DF}^{S}(s_i, e_u, r_v) - C_{DF}^{S}(\mathcal{R}(s_i), e_u) > 0$. Hence, we have $\gamma_{r_v,e_u} > \gamma_{r_v,d_i}$. □

The above lemma implies whether an unassigned relay can be selected to act as a friendly jammer for an s-d pair. Obviously, each s-d pair exploiting the friendly jammer to protect their transmissions will result in a global secrecy capacity enhancement. The friendly jammer selection procedure is presented in Algorithm 4. After running the proposed algorithm, a friendly jammer selection profile is obtained, in which the selected relay nodes are associated with different s-d pairs. As the smart jamming procedure follows with the the optimal relay assignment process, an efficient transmission scheduling is necessary.

5.7 Performance Evaluation

5.7.1 Experiment Setup

In this section, we evaluate our analysis and algorithms through extensive experiments under various network settings.

To evaluate the effect of relay location on the primary channel capacity, we conduct experiments on a topology consisting of one source, one destination. A relay node is placed into the network and cooperatively help the transmission from the source to the destination. We compare the achievable capacity between source and destination under direct transmission and cooperative Amplify-and-Forward mode (CC-AF). We also obtain the capacity upper bound under cooperative AF mode (CC-AF Upper bound).

To evaluate the secrecy capacity gain brought by the cooperative relay assignment, experiments are first conducted in four sub-scenarios where the location of relay and eavesdropper varies, corresponding to different assignment choices, as shown in Fig. 5.7(a). The distance from source and destination is 1000 meters and the location of relay and eavesdropper varies in different scenarios, e.g., d_{s_1,e_1}=d_{r_1,e_1}=$500m$, d_{s_1,r_1}=d_{r_1,d_1}=$707m$ in Scenario A, d_{s_1,e_1}=d_{s_1,r_1}=d_{r_1,d_1}=$500m$, d_{r_1,e_1}=$707m$ in Scenario B, etc. In the experiments, we set W=22 MHz for the channel. We vary the path loss exponent, the transmission power of

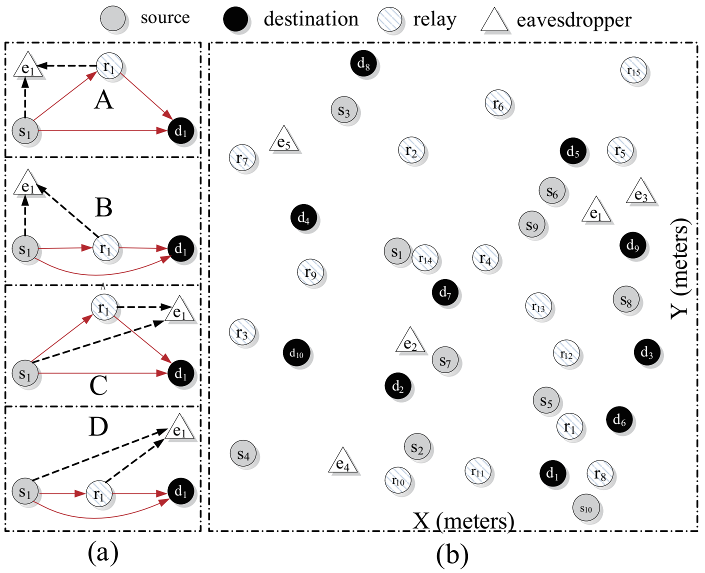


FIGURE 5.7: Experimental scenarios: (a) Four secure cooperative ad-hoc network scenarios each with one s-d pair, one relay node and one eavesdropping node. (b) Topology for a 40-node cooperative ad hoc network where N_s=10, N_r=15 and N_e=5.

relay, and the transmission power of source to compare the secrecy capacity under different scenarios.

To evaluate the efficiency of our proposed relay assignment algorithm and the smart jamming algorithm, we carry out comprehensive experiments by studying various cooperative ad hoc network scenarios. We varied the number of source-destination pairs n, the number of relay nodes m and the number of eavesdropping nodes k to evaluate the efficiency of our proposed relay assignment algorithm. Nodes are randomly distributed in a $500m \times 500m$ square. For each setting, we randomly generate 10 instances and the average result is presented with a 95% confidence interval. Since we are the first work on the problem of relay assignment in cooperative ad hoc networks with the objective to maximize the total secrecy capacity, experiments are conducted by comparing the total secrecy capacity under direct transmission, random cooperative relay assignment, and our proposed relay assignment algorithm ORA-SCAN. We run the random assignment algorithm and the proposed ORA-SCAN on a C++ based simulator. Besides, we set 22 *MHz* as the bandwidth for the channels. The transmission power for all sources and relays is set to 1 *Watt* and the ambient noise is 10^{-9}.

Lastly, we evaluate our proposed algorithms by studying a 40-node cooperative ad hoc network as shown in Fig. 5.7(b). Nodes are randomly distributed in a $500m \times 500m$ square. There are 10 source-destination pairs which represent the unicast emergency services, 15 relay nodes and 5 eavesdroppers. Experiments are conducted by comparing the total secrecy capacity under direct transmission, cooperative communication with ORA-SCAN, and cooperative communication with ORA-SACN and smart jamming.

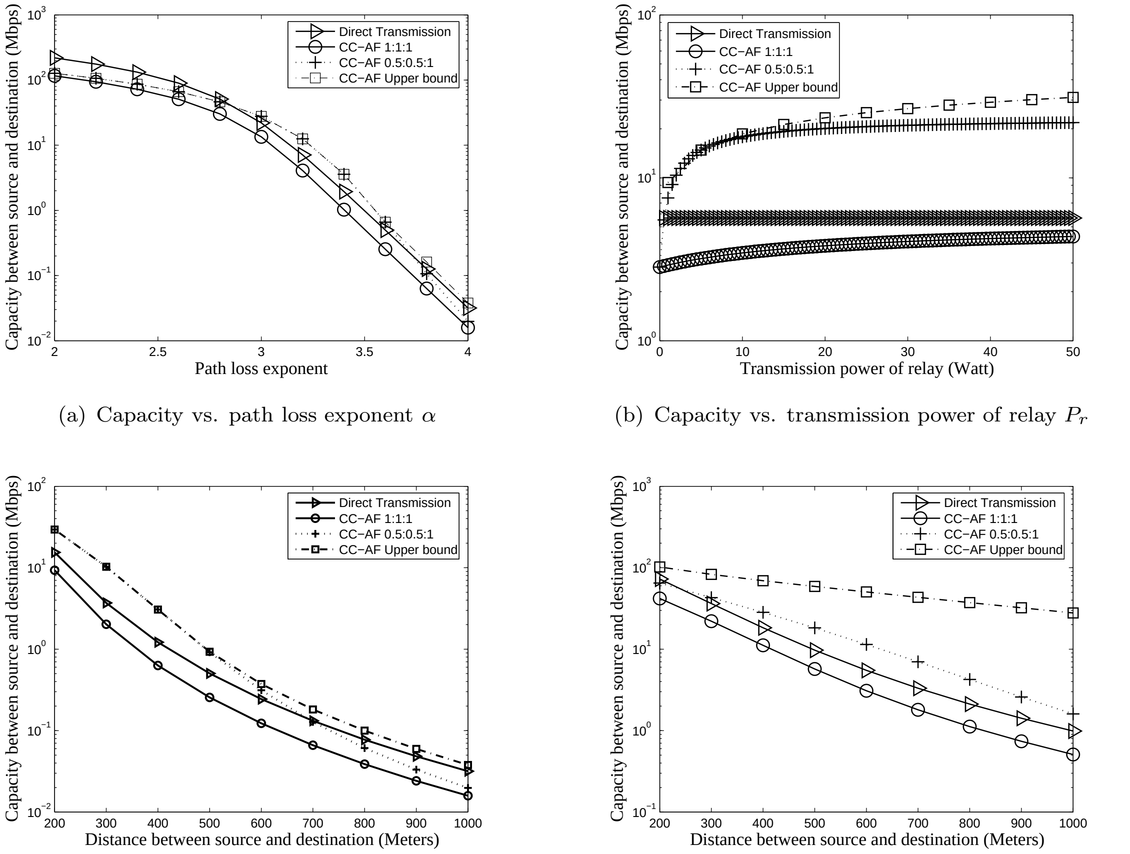
5.7.2 Numerical Results

5.7.2.1 Effect of relay location on the primary channel capacity

We compare the achievable capacity between a source and destination under direct transmission, CC-AF x:y:z and CC-AF Upper bound, where x:y:z represents the distance relationship $d_{s,r}$:$d_{r,d}$:$d_{s,d}$. When the distance between source and destination is constant, we study the effect on different path loss exponent and transmission power of relay, as illustrated in Fig. 5.8(a)-5.8(b). We obtain CC-AF Upper bound through the C-Plex optimizer [85]. When the distance between source and destination changes, we compute the capacity under different schemes as shown in Fig. 5.8(d). We can observe that CC is not always better than direct transmission in terms of link capacity, especially when the relay is placed improperly, for example, the relay locates as CC-AF 1:1:1.

5.7.2.2 Secrecy capacity gain from relay assignment

We evaluate the secrecy capacity under four different scenarios in Fig. 5.7(a) by varying the network settings, as shown in Fig. 5.10(a)-5.10(c). Secrecy capacity is computed by the capacity difference between the primary channel and the eavesdropping channel. For clarify purpose, we also give the secrecy capacity that is below zero. From the three sub-figures, we observe that the network settings (e.g., path loss exponent and the transmission power of source and relay) have less impact on the secrecy capacity than the assignment of relays. For example, sub-scenario-D always achieves nonzero secrecy capacity as the involvement of relay improve the capacity of the primary channel and simultaneously decrease the capacity of the eavesdropping one. Another observation is that the location of cooperative relay and



(a) Capacity vs. path loss exponent α

(b) Capacity vs. transmission power of relay P_r

(c) Capacity vs. distance between *s*-*d* pair d_{s_i,d_i}, $\alpha = 4$

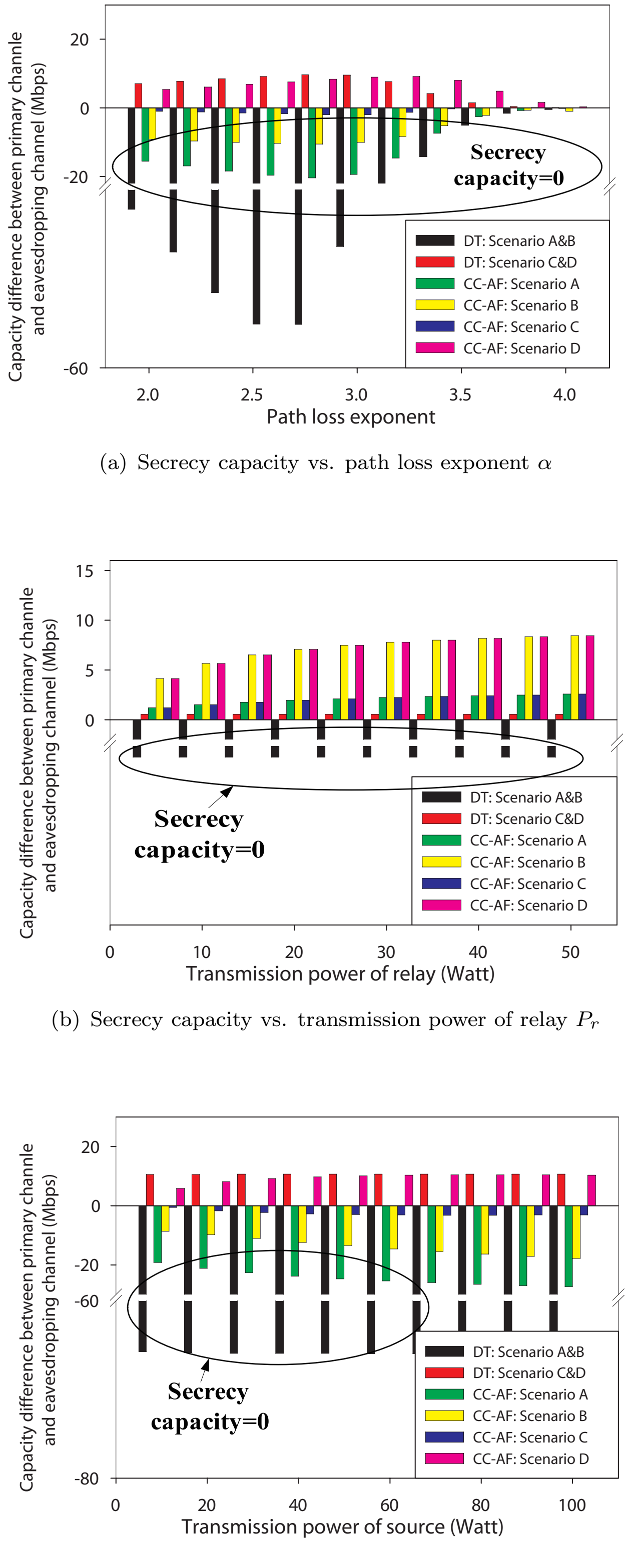
(d) Capacity vs. distance between *s*-*d* pair d_{s_i,d_i}, $\alpha = 3$

FIGURE 5.8: Effect of relay location on the primary channel capacity.

eavesdropper has great impact on the secrecy capacity. The reason is that when an eavesdropper locates near the source or relay can induce to enhancement on the eavesdropping channel so that decrease the corresponding secrecy capacity.

5.7.2.3 Efficiency of the proposed algorithms

We compare the performance of our proposed relay assignment algorithm (ORA-SCAN) with direct transmission and random assignment algorithm, by varying the number of relay nodes, *s*-*d* pairs and eavesdropping nodes, as shown in Fig. 5.10(a)-Fig. 5.10(c). In Fig. 5.10(a), we fix the number of *s*-*d* pairs to 20 and the number of eavesdropping nodes to 5. ORA-SCAN achieves a much greater secrecy capacity gain than the random assignment

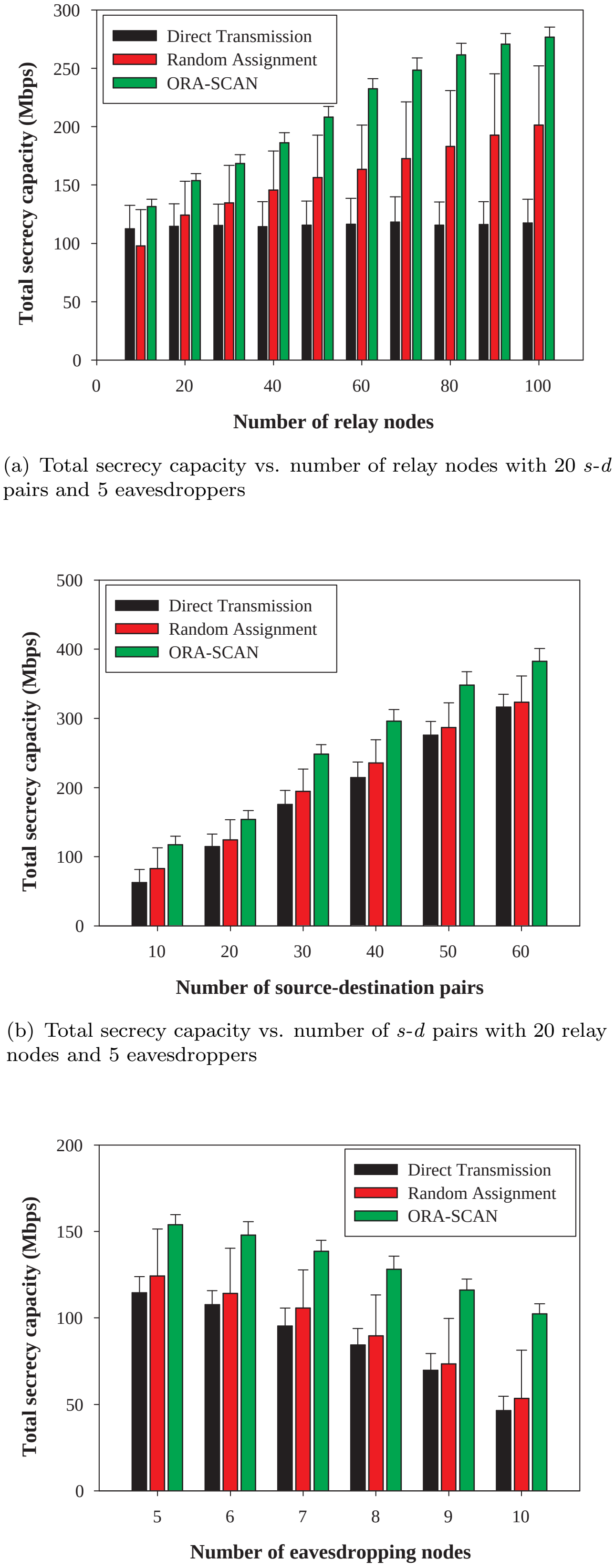


(a) Secrecy capacity vs. path loss exponent α

(b) Secrecy capacity vs. transmission power of relay P_r

(c) Secrecy capacity vs. transmission power of source P_s

FIGURE 5.9: Secrecy capacity under four different scenarios in Fig. 5.7(a).

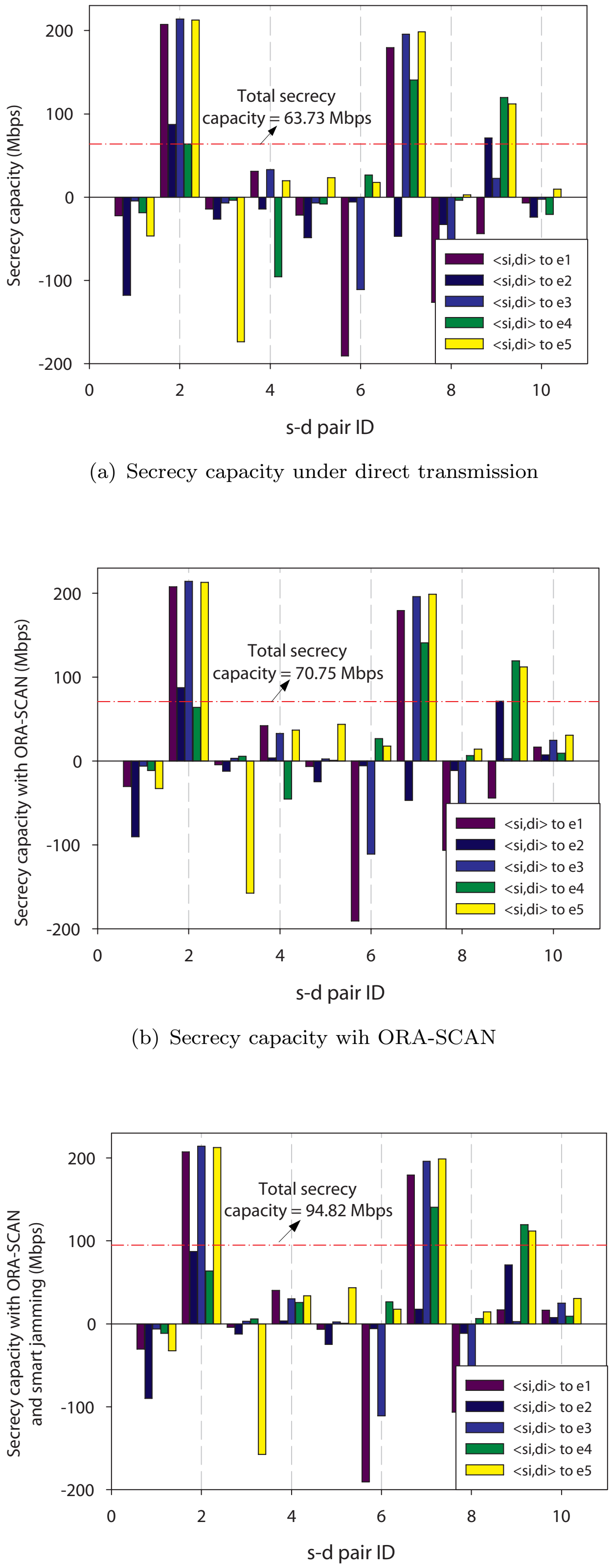


(a) Total secrecy capacity vs. number of relay nodes with 20 s-d pairs and 5 eavesdroppers

(b) Total secrecy capacity vs. number of s-d pairs with 20 relay nodes and 5 eavesdroppers

(c) Total secrecy capacity vs. number of eavesdropping nodes with 20 s-d pairs and 20 relay nodes

FIGURE 5.10: Efficiency of the proposed relay assignment algorithm.



(a) Secrecy capacity under direct transmission

(b) Secrecy capacity wih ORA-SCAN

(c) Secrecy capacity with ORA-SCAN and smart jamming

FIGURE 5.11: Secrecy capacity of different *s*-*d* pair in Fig. 5.7(b).

when the number of relay nodes increases. Then we fix the number of relay nodes to 20 and the number of eavesdropping nodes to 5, we calculate the total secrecy capacity by varying the number of *s*-*d* pairs, as shown in Fig. 5.10(b). Although ORA-SCAN still outperforms the other two algorithms, the secrecy capacity gain increase much slower as there are limited set of relay nodes to be exploited. In Fig. 5.10(c), we vary the number of eavesdropping nodes which indicates for different security requirements. For each of the algorithms under consideration, the total secrecy capacity significantly decrease with the number of eavesdropping nodes increases. However, the secrecy capacity gain from ORA-SCAN is much better than the other two algorithms.

Consider the network topology in Fig. 5.7(b), we generate the secrecy capacity for each *s*-*d* pair under our proposed ORA-SCAN algorithm, as shown in Fig. 5.11(b), and compare it with the secrecy capacity under direct transmission in Fig. 5.11(a). The total secrecy capacity increases from **63.73** *Mbps* to **70.75** *Mbps*. This benefit is from the optimal relay assignment process. Further, we exploit the jamming technique and select one or more unassigned relay nodes to act as friendly jammer for some of the *s*-*d* pairs. We compute the secrecy capacity after running ORA-SCAN and the smart jamming algorithm altogether, which receives considerable improvement on the total secrecy capacity from **70.75** *Mbps* to **94.82** *Mbps*, as shown in Fig. 5.11(c). The reason is that some spare relays can act as friendly jammer and serve for some transmitting sessions, e.g., jamming relay is selected to serve $\langle s_4, d_4 \rangle$, $\langle s_7, d_7 \rangle$ and $\langle s_9, d_9 \rangle$ and to combat the dedicated eavesdropping nodes, which increase the corresponding secrecy capacity for each of the above *s*-*d* pairs.

Through extensive experiments, we validate that our proposed relay assignment algorithm and jamming algorithm can significantly increase the system secrecy capacity. Besides, as the network setting changes, the proposed networking scheme is able to satisfy the critical requirements for unicast emergency services.

5.7.3 Discussions

The networking scheme we proposed in this chapter consists of an optimal relay assignment algorithm and a smart jamming algorithm. The proposed algorithms can work in a dynamic wireless ad-hoc network where the location of each node may vary as time progresses. The only consideration is the overhead in distributing the channel-state information (CSI) in the network. It is also the most challenging issue while implementing our networking scheme in the real wireless communication scenarios. We acknowledge that in some environments, the overhead could be large if CSI in the network varies on a smaller time scale. Under such scenarios, fast and efficient dissemination of CSI remains an open problem. Nevertheless, the analytical results and methodologies we proposed in this chapter can be used as a performance benchmark for future solutions in practice.

5.8 Summary

This chapter aims at improving the physical layer security in secure cooperative ad hoc networks with the presence of multiple eavesdroppers. We theoretically formulate the secrecy capacity maximization problem and develop an optimal relay assignment algorithm to solve it in polynomial time. Then we propose a smart jamming algorithm to further increase the system secrecy capacity. Extensive experimental results reveal that our proposed algorithms can achieve high secrecy capacity under various network settings.

Although we offered a possible implementation for the proposed algorithms, a number of issues remain challenging in practice. Specifically, efficient methodologies for collecting and disseminating CSI in large-scale and dynamic networks remain an open problem. Nevertheless, the theoretical results presented here can be used as a performance benchmark for future solutions in practice. For a future work, we will exploit the relay assignment problem with security and interference constraints in secure cooperative wireless networks.

Chapter 6

Conclusions and Future Work

With the advancement of telecommunication technology, devices with wireless functionalities are ubiquitous nowadays. As a result, networking among such devices has become increasingly critical in both theory and practice. This dissertation focuses on fundamental issues in wireless networking: congestion mitigation and non-cooperation avoidance, route selection and cross-layer optimization, cooperative relay placement, and physical layer security. We propose two categories of networking schemes, namely self-supported networking and cooperative networking, to coordinate the network and enhance wireless communications. Overall system performance (e.g., throughput, end-to-end delay, security, capacity) is improved by applying our proposed networking schemes over wireless networks. This dissertation is concluded as follows.

6.1 Self-supported Congestion-aware Networking for Non-cooperative WANETs

In Chapter 2, we investigated the issue of coordinating wireless ad-hoc networks (WANETs) to support emergency services. We focus on promoting self-supported and congestion-aware networking for emergency services in WANETs based on the idea of Do-It-Yourself. We model network congestion and non-cooperation behaviors according to the relations between nodes in the constructed dependency graph. Then we propose an energy-efficient and congestion-aware routing protocol for the emergency services of WANETs. Based on the proposed model and routing protocol, we design two novel movement schemes, called Direct Movement to potential selfish/busy Relays (DMR) scheme and Iterative Movement to potential selfish/busy Relays (IMR) scheme for urgent sources to supported themselves and to avoid congestion and non-cooperation. Analysis and simulation results show that our approaches significantly achieve better network performance and typically satisfy the requirements for emergency services in WANETs.

The main advantages of our proposed networking schemes are summarized as follows. 1) We model network congestion and non-cooperation behaviors according to the relations among the autonomous nodes in the constructed dependency graph. 2) The proposed routing protocol is energy-efficient and congestion-aware, which captures the dependency relations in the network and provides better routing solutions for the transmitting sessions. 3) We propose two novel movement schemes, called DMR and IMR for urgent sources to supported themselves and to avoid congestion and non-cooperation. 4) The proposed DMR scheme is simple and novel in improving the network performance in terms of increasing the throughput and reducing the end-to-end delay. 5) As an improvement of the DMR scheme, the proposed IMR scheme is superior in improving the network connectivity. 6) We implement the proposed networking schemes in a computer simulator. The simulation results reveal that our approaches significantly achieve better network performance.

6.2 Self-supported Networking for Cooperative Multi-hop Wireless Networks

In Chapter 3, we studied the potential issues in using cooperative communication paradigm to support emergency services. We design a novel cross-layer networking scheme which focuses on promoting energy-efficient and congestion-aware cooperative networking based on the idea of Do-It-Yourself. The objectives of our networking scheme are twofold: (1) at the network layer, through optimal relay node selection to minimize the cost of multi-hop cooperative flow routing; (2) at the MAC layer, maximize the minimum flow rate (or throughput) among all active emergency sessions, as well as avoid congestion and non-cooperation behaviors. To formulate the problem, we introduce the concept of *dependency graph* to reflect a connected network. Then we develop a mathematical characterization for multi-hop flow routing and relay node selection process. For the first objective, we formulate the cost of data links and traffic flows in a CC aware network as a minimization problem. For the second objective, we formulate the flow rate problem based on multi-hop cooperative routing and relay node selection. Then we model network congestion and non-cooperation behaviors according to the formulations. To solve the formulated problems, we combine the two subproblems into a *mixed integer linear programming* (MILP) problem. Then we develop a self-supported based solution procedure to reduce the solution space. Our proposed Self-supported Cooperative Networking (SCooN) scheme includes three novel components which make the solution procedure highly efficient. First, we construct the dependency graph and complete the nodes classification. Then we design an energy-efficient cooperative routing protocol. Thirdly, after investigating the locations of congestion and non-cooperation, sources and relays support themselves by cognitive movements. Simulation results show that our approaches significantly achieve better network performance and typically satisfy the requirements for emergency services in multi-hop wireless networks.

6.3 Optimal Relay Placement for Capacity Maximization in Wireless Networks

In Chapter 4, we studied the relay node placement problem for multi-pair cooperative communication in wireless networks. Currently, relaying and cooperation have emerged as important research topics in wireless communication. During cooperative communication, spatial diversity can be achieved by exploiting the relaying capabilities of the involved relay nodes, which may vastly enhance the achieved system capacity. The potential gains largely depend on the location of relay nodes. We studied the problem by exploiting a finite number of candidate relay nodes which can be placed to help the transmission of multiple source-destination pairs. Our objective is to maximize the system capacity. After formulating the relay node placement problem, we comprehensively study the effect of relay location on cooperative link capacity and show several attractive properties of the considered problem. Thus, we develop a geographic aware relay node placement algorithm which optimally solves the relay node placement problem in polynomial time. Compared with existing works, the main contributions of our work are summarized as follows.

- 1. By applying the SNR-based capacity model, we theoretically formulate the relay node placement problem under consideration, named as RNP-MPCC, which seeks for a relay placement profile such that the system capacity is maximized.
- 2. Due to the continuous nature of placement space, we carry out comprehensive studies on the effect of relay location on cooperative link capacity, and determine the optimum relay location site for each source-destination pair.
- 3. We develop a geographic aware polynomial time algorithm to optimally solve RNP-MPCC, which maximizes the system capacity by placing a subset of the candidate relay nodes on the optimum relay location sites.
- 4. Analytical and experimental results are carried out to evaluate the efficiency of our proposed algorithm.

6.4 Secrecy Capacity Maximization for Cooperative Wireless Networks

Physical layer security has emerged as a key technique for providing trustworthy and reliable future wireless networks and has witnessed a significant growth in the past few years. In Chapter 5, we aimed at improving the physical layer security and provide secure cooperative communication through cooperative relaying and cooperative jamming. We investigated secure cooperative communication with the involvement of multiple malicious eavesdroppers. By characterizing the security performance of the system by secrecy capacity, we study the secrecy capacity maximization problem in cooperative communication aware ad hoc networks. Specifically, we propose a system model where secrecy capacity enhancement is achieved by the assignment of cooperative relays. We theoretically present a corresponding formulation for the problem and discuss the security gain brought by the relay assignment process. Then, we develop an optimal relay assignment algorithm to solve the secrecy capacity maximization problem in polynomial time. The basic idea behind our proposed algorithm is to boost the capacity of the primary channel by simultaneously decreasing the capacity of the eavesdropping channel. To further increase the system secrecy capacity, we exploit the jamming technique and propose a smart jamming algorithm to interfere the eavesdropping channels. Analysis and experimental results show that our proposed algorithms can achieve high secrecy capacity under various network settings. The main contributions of this chapter can be summarized as follows.

- 1. To the best of our knowledge, we are the *first* to exploit the physical layer security based cooperative communication issue in wireless networks. We address the system architecture and propose a system model where security enhancement is achieved by the assignment of relays.
- 2. We model the relay assignment problem for secrecy capacity maximization, named RAP-SCAN. Then make comprehensive investigations on the security gain brought by the relay assignment procedure.
- 3. We develop an optimal relay assignment algorithm, called ORA-SCAN, which solves RAP-SCAN in polynomial time.
- 4. We exploit the advantages of jamming technique and propose a smart jamming algorithm to further increase the system secrecy capacity.
- 5. Through extensive experiments, we validate our proposed relay assignment algorithm and jamming algorithm significantly improve the system secrecy capacity, which satisfy the critical security requirements under various network settings.

6.5 Future Work

Our future work are two-fold: First, we will make surveys and investigate cooperative sensing technique with cooperative relays employed for spectrum sensing and secondary user transmission under primary user QoS constraints in cognitive radio networks (CRNs). Second, we will proceed our recent study in wireless physical layer security and consider more complicated and practical system models, for instance, multicast and broadcast sessions in cooperative wireless networks.

Bibliography

[1] DIY in wikipedia. [Online]. Available: http://en.wikipedia.org/wiki/DIY

[2] Federal Emergency Management Agency, “Technology applications by the federal emergency management agency in response, recovery, and mitigation operations”, in *the 27th Joint Meeting of the U.S./Japanese Panel on Wind and Seismic Effects*, Tokyo/Osaka, Japan, May, 1995.

[3] Bret Hull, Kyle Jamieson, and Hari Balakrishnan, “Mitigating congestion in wireless sensor networks”, in *Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys)*, November 2004.

[4] Maurits de Graaf et al. “Easy Wireless: broadband ad hoc networking for emergency services”, *MedHoc Conference on ad-hoc networking (MedHoc 2007)*, June 12-15, 2007.

[5] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker, “Mitigating routing misbehavior in mobile ad hoc networks”, in *Proceeding of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom)*, pp. 255-265, August 6-11, 2000, Boston, Massachusetts.

[6] S. Buchegger and J.-Y. L. Boudec, “Performance analysis of the CONFIDANT protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks)”, in *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*, June 2002.

[7] L. Buttyan and J. Hubaux, “Enforcing service availability in mobile ad-Hoc WANs”, in *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networkind and Computing (MobiHOC)*, Boston, August 2000.

[8] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J-P. Hubaux, and J-Y. Le Boudec, “Self-organization in mobile ad hoc networks: The approach of Terminodes”, *IEEE Comm. Magazine*, pp. 166-175, June 2001.

[9] S. Zhong, J. Chen, and Y. R. Yang, “Sprite, a simple, cheat-proof, credit-based system for mobile ad-hoc networks”, in *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, San Francisco, March 30 - April 3, 2003.

[10] V. Srinivasan, P. Nuggehalli, C.-F. Chiasserini and R. Rao, “Cooperation in wireless ad hoc networks”, in *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, pp. 808-817, San Francisco, March 30 - April 3, 2003.

[11] V. Srinivasan, P. Nuggehalli, C-F. Chiasserini, and R.R. Rao, “An analytical approach to the study of cooperation in wireless ad hoc networks”, *IEEE Transsactions on Communications*, 4(2): pp. 722-733, March 2005.

[12] T. Rappaport, *Wireless Communications: Principles and Practice.* IEEE Press Piscataway, NJ, USA, 1996.

[13] K. Ghada, J. Li, Y. Ji, and G. Wang, “Cross-layer Approach for Energy Efficient Routing in WANETs”, *IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, pp. 392-402, 2009.

[14] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing”, *Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pp. 90-100, February 1999.

[15] The network simulator ns-2. [Online]. Availavle: http://www.isi.edu/nsnam/ns/, 2011.

[16] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, “Cooperative diversity in wireless networks: Efficient protocols and outage behavior,” *IEEE Transactions on Information Theory*, Vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[17] A. Sendonaris, E. Erkip, and B. Aazhang, “User cooperation diversity part I: System description”, *IEEE Transactions on Information Theory*, vol. 51, no. 11, pp. 1927-1938, Nov. 2003.

[18] A. Sendonaris, E. Erkip, and B. Aazhang, “User cooperation diversity part II: Implementation aspects and performance analysis”, *IEEE Transactions on Communication*, vol. 51, no. 11, pp. 1939-1948, Nov. 2003.

[19] O. Gurewitz, A. de Baynast, and E. W. Knightly, “Cooperative strategies and achievable rate for tree networks with optimal spatial reuse”, *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3596-3614, Oct. 2007.

[20] S. Savazzi, and U. Spagnolini, “Energy aware power allocation strategies for multihop-cooperative transmission schemes”, *IEEE Journal on Selected Areas in Communications*, vol. 25, pp. 318-327, Feb. 2007.

[21] A. Scaglione, D. L. Goeckel, and J. N. Laneman, “Cooperative communications in mobile ad hoc networks”, *IEEE Signal Processing Magazine*, vol. 23, no. 5, pp. 18-29, Sept. 2006.

[22] A.E. Khandani, J. Abounadi, E. Modiano, and L. Zheng, “Cooperative Routing in Static Wireless Networks”, *IEEE Transactions on Communications*, vol. 55, no. 11, pp. 2185-2192, Nov. 2007.

[23] J. Zhang and Q. Zhang, “Cooperative Routing in Multi-Source Multi-Destination Multi-hop Wireless Networks”, in in *Proceedings of the 27th IEEE International Conference on Computer Communication (INFOCOM), mini-symposium*, 2008.

[24] S. Sharma, Y. Shi, Y.T. Hou, and S. Kompella, “An optimal algorithm for relay node assignment in cooperative ad hoc networks”, *IEEE/ACM Transactions on Networking*, vol. 18, issue 6, Nov. 2010.

[25] S. Ray, R. Ungrangsi, F. D. Pellegrini, A. Trachtenberg, and D. Starobinski, “Robust location detection in emergency sensor networks”, in *Proceedings of the 22nd IEEE International Conference on Computer Communication (INFOCOM)*, 2003.

[26] Malan D, Fulford-Jones TRF, Welsh M, and Moulton S, “CodeBlue: an ad Hoc sensor network infrastructure for emergency medical care”, in *Proceeding of the MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES)*, June 2004.

[27] B. Braunstein, T. Trimble, R. Mishra, B. S. Manoj, L. Lenert, and R. R. Rao, “Challenges in using of distributed wireless mesh networks in emergency response”, in *Proceedings of the 3rd International ISCRAM Conference*, pp. 30-38, May 2006.

[28] Y.C. Tseng, M.S. Pan, and Y.Y. Tsai, "Wireless sensor networks for emergency navigation", *IEEE Computers*, 39(7): 55-62, 2006.

[29] C.Y. Wan, S. B. Eisenman, and A.T. Campbell, "CODA: congestion detection and avoidance in sensor networks", in *Proceeding of the First ACM Conference on Embedded Networked Sensor Systems (SenSys 2003)*, pp. 266-279, Nov. 2003.

[30] L. Chen, S. H. Low, M. Chiang, and J. C. Doyle, "Cross-layer congestion control, routing and scheduling design in ad hoc wireless networks", in *Proceeding of the 25th IEEE International Conference on Computer Communication (INFOCOM)*, Apr. 2006.

[31] X. Lin and N. B. Shroff, "The impact of imperfect scheduling on cross-layer congestion control in wireless networks", *IEEE/ACM Transactions on Networking*, vol. 14, no. 2, pp. 302-315, Apr. 2006.

[32] M. Felegyhazi, J. P. Hubaux, and L. Buttyan, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks", *IEEE Transactions on Mobile Computing*, vol. 5, no. 5, pp. 463-476, Apr. 2006.

[33] L. Lai and H. El Gamal, "On cooperation in energy efficient wireless networks: the role of altruistic nodes", *IEEE Transaction on Wireless Communication.*, vol. 7, no. 5, pp. 1868-1878, May 2008.

[34] C. Pandana, Z. Han, and K. J. R. Liu, "Cooperation enforcement and learning for optimizing packet forwarding in autonomous wireless networks", *IEEE Transaction on Wireless Communication*, vol. 7, no. 8, pp. 3150-3163, Aug. 2008.

[35] J. Yang, A.G. Klein, and D.R. Brown III, "Natural Cooperation in wireless Networks", *IEEE Signal Processing Magazine*, pp. 98-106, Sept. 2009.

[36] Z. Han and V. Poor, "Coalition games with cooperative transmission: a cure for the curse of boundary nodes in selfish packet-forwarding wireless networks", *IEEE Transactions on Communication*, vol. 57, pp. 203-213, Jan. 2009.

[37] W. Saad, Z. Han, M. Debbah, A. Hjorungnes, and T. Basar, "Coalitional games for distributed collaborative spectrum sensing in cognitive radio networks", in *Proceedings of the 28th IEEE International Conference on Computer Communication (INFOCOM)*, PP. 2114-2122, Apr. 2009.

[38] B. Han, J. Li, and J. Su, “Self-supported Congestion-aware Networking for Emergency Services in WANETs”, in *Proceeding of the 30th IEEE International Conference on Computer Communication (INFOCOM)*, pp. 891-899, Apr. 2011.

[39] D. Yang, X. Fang and G. Xue, “Near-Optimal Relay Station Placement for Power Minimization in WiMAX Networks”, in *Proc.of IEEE Globecom*, December, 2011.

[40] D. Yang, X. Fang and G. Xue, “HERA: An Optimal Relay Assignment Scheme for Cooperative Networks”, *IEEE J. Sel. Areas Commun.*, Vol. 30, No. 2, pp. 245-253, Feb. 2012.

[41] E. Lloyd and G. Xue, “Relay node placement in wireless sensor networks”, *IEEE Transactions on Computers*, vol. 56, no. 1, pp. 134-138, Jan. 2007.

[42] X. Cheng, D. Du, L. Wang, and B. Xu, “Relay sensor placement in wireless sensor networks”, *Wireless Networks*, vol. 14, no. 3, pp. 347-355, 2008.

[43] B. Lin, P.-H. Ho, L.-L. Xie and X. Shen, “Optimal Relay Station Placement in IEEE 802.16j Networks”, in *Proc. of ACM IWCMC*, 2007.

[44] B. Lin, P.-H. Ho, L.-L. Xie, X. Shen and J. Tapolcai, “Optimal Relay Station Placement in Broadband Wireless Access Networks”, *IEEE Trans. Mobile Comput.*, Vol. 9, No. 2, pp. 259-269, Feb. 2010.

[45] W. Zhang, S. Bai, G. Xue, J. Tang and C. Wang, “DARP: Distance-Aware Relay Placement in WiMAX Mesh Networks”, in *Proc.of IEEE INFOCOM*, April 11-15, 2011.

[46] H.-C. Lu, W. Liao and F. Lin, “Relay Station Placement Strategy in IEEE 802.16j WiMAX Networks”, *IEEE Trans. Commun.*, Vol. 59, No. 1, pp. 151-158, Jan. 2011.

[47] Y.-W P. Hong, W.-J. Huang, and C.-C. J. Kuo, “Cooperative Communications and Networking:Technologies and System Design”, New York, USA: Springer, 2010.

[48] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: John Wiley and Sons, 2005.

[49] B. Han, J. Li, and J. Su, “Optimal Relay Node Placement for Multi-pair Cooperative Communication in Wireless Networks”, in *Proceeding of IEEE WCNC*, pp. 4771-4776, Shanghai, China, April 7-10, 2013.

[50] B. Han, and J. Li, "On relay placement for cooperative communication in wireless networks", *Technical report*, Available: http://www.osdp.cs.tsukuba.ac.jp/ han/-doc/ORNP12.pdf, Oct. 2012.

[51] R. Yamada, "DOCOMO's actions for new growth", *IEEE ICC Keynote*, NTT DOCOMO Inc., 2011.

[52] X. Shen, A. Hjrungnes, Q. Zhang, P.R. Kumar, and Z. Han, "Guest editorial: cooperative networking - challenges and applications (Part 1)", *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 241-244, Feb. 2012.

[53] X. Shen, A. Hjrungnes, Q. Zhang, P.R. Kumar, and Z. Han, "Guest editorial: cooperative networking - challenges and applications (Part 2)", *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1593-1596, Sept. 2012.

[54] Y. Liang, H.V. Poor, and S. Shamai, *Information Theoretic Security*, Delft, The Netherlands: Now Publishers, 2009.

[55] Y. Sun, W. Trappe, and K.J.R. Liu, *Network-aware security for group communications.* Springer, 2007.

[56] Y. Liang, H.V. Poor, and L. Ying, "Wireless broadcast networks: reliability, security, and stability", in *Proc. IEEE Inf. Theory Appl. Work.*, pp. 249-255, Feb. 2008.

[57] A.D. Wyner, "The wire-tap channel", *Bell Syst. Technical J.*, vol. 54, no. 8, pp. 1355-1387, 1975.

[58] S.K. Leung-Yan-Cheong and M.E. Hellman, "The Gaussian wiretap channel", *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451-456, July 1978.

[59] I. Csiszar and J. Korner, "Broadcast channel with confidential messages", *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[60] J. Barros and M.R.D. Rodrigues, "Secrecy capacity of wireless channels", in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 356-360, July 2006.

[61] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy", *IEEE Trans. Inform. Theory*, vol. 54, pp. 4005-4019, Sept. 2008.

[62] L. Dong, Z. Han, A.P. Petropulu, and H.V. Poor, “Improving wireless physical layer security via cooperative relays”, *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[63] J. Zhang, L. Fu, and X. Wang, “Impact of secrecy on capacity in large-scale wireless networks”, in *Proc. of IEEE INFOCOM*, pp. 3051-3055, Apr. 2012.

[64] J.N. Laneman, D.N.C. Tse and G.W. Wornell, “Cooperative diversity in wireless networks: efficient protocols and outage behavior”, *IEEE Trans. Inform. Theory*, vol.50, pp. 3062-3080, 2004.

[65] A. Bletsas, H. Shin, and M. Z. Win, “Cooperative communications with outage-optimal opportunistic relaying”, *IEEE Trans. Wireless Commun.*, vol. 6, pp. 3450-3460, Sept. 2007.

[66] S. Sharma, Y. Shi, Y.T. Hou and S. Kompella, “An optimal algorithm for relay node assignment in cooperative ad hoc networks”, *IEEE/ACM Trans. Netw.*, vol. 19, no. 3, pp. 879-892, June 2011.

[67] D. Yang, X. Fang and G. Xue, “OPRA: Optimal relay assignment for capacity maximization in cooperative networks”, in *Proc. of IEEE ICC*, June, 2011.

[68] B. Han, J. Li, J. Su and J. Cao, “Self-supported cooperative networking for emergency services in multi-hop wireless networks”, *IEEE J. Sel. Areas Commun.,*, vol. 30, no. 2, pp. 450-457, Feb. 2012.

[69] B. Han, J. Li, and J. Su, “Optimal relay assignment for secrecy capacity maximization in cooperative ad hoc networks”, in *Proc. of IEEE ICC*, accepted, June 2013.

[70] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Secure wireless communications via cooperation”,in *Proc. of 46th Annual Allerton Conference on Communication, Control, and Computing*, UIUC, Illinois, USA, Sept. 2008.

[71] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Amplify-and-forward based cooperation for secure wireless communications”, in *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing*, Taipei, Taiwan, Apr. 2009.

[72] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, “Secrecy capacity of a class of orthogonal relay eavesdropper channels”, EURASIP J. Wireless Commun. Netw., vol. 2009, Article ID 494696, 14 pages, 2009.

[73] E. Tekin and A. Yener, “The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jam- ming”, *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735-2751, Jun. 2008.

[74] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperative relays”, *IEEE Trans. Sign. Proc.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[75] 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.

[76] T. Wang and G. B. Giannakis, “Mutual information jammer-relay games”, *IEEE Trans. Inform. Foren. Sec.*, vol. 3, pp. 290-303, June 2008.

[77] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, “Joint relay and jammer selection for secure two-way relay networks”, *IEEE Trans. Inform. Foren. Sec.*, vol. 7, pp. 310-320, Feb. 2012.

[78] H. Liu and G. Li, *OFDM-based Broadband Wireless Networks: Design and Optimization*, Hobken, New Jersey: Wiley-Interscience, 2005.

[79] Y. Zhao, R.S. Adve, and T.J. Lim, “Improving amplify-and-forward relay networks: optimal power allocation versus selection”, *IEEE International Symposium on Information Theory*, pp. 1234-1238, 2006.

[80] P. Zhang, J. Yuan, J. Chen, J. Wang, and J. Yang, “Analyzing amplifyand-forward and decode-and-forward cooperative strategies in Wyner’s channel model”, in *Proc. of IEEE WCNC*, 2009.

[81] D.B. West, *Introduction to Graph Theory*, Prentice Hall, 2nd Edition, 2001.

[82] Z. Ding, K.K. Leung, D.L. Goeckel and D. Towsley, “On the application of cooperative transmission to secrecy communications”, *IEEE J. Sel. Areas Commun.,*, vol. 30, no. 2, pp. 359-368, Feb. 2012.

[83] Z. Gao, Y. Yang and K.J.R. Liu, “Anti-eavesdropping space-time network coding for cooperative communications”, *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3898-3908, Nov. 2011.

[84] Y.-W P.Hong, W.-J Huang and C.-C. J. Kuo, *Cooperative communications and networking: technologies and system design*, New York, USA: Springer, 2010.

[85] IBM ILOG CPLEX Optimizer. [Online]. Available: http://www-01.ibm.com/software/integration/optimization/cplex-optimizer/, 2012.

[86] Q. Wang, H. Su, K. Ren and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks", in *Proc. of IEEE INFOCOM*, 2011.

[87] K. Ren, H. Su and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications", *IEEE Wireless Commun. Magazine*, 18(4), 2011.

[88] B. Han and J. Li, "Secrecy capacity maximization for secure cooperative ad-hoc networks", in *Proc. of IEEE INFOCOM*, pp. 2896-2904, Turin, Italy, April 14-19, 2013.

List of Publications

1. **Biao Han**, Jie Li, Jinshu Su, and Jiannong Cao, “Self-supported cooperative networking for emergency services in multi-hop wireless networks”, *IEEE Journal on Selected Areas in Communications (IEEE JSAC)*, vol. 30, no. 2, pp. 450-457, February 2012.

2. **Biao Han**, and Jie Li, “Secrecy Capacity Maximization for Secure Cooperative Adhoc Networks”, in *Proceeding of the 32nd IEEE International Conference on Computer Communications (IEEE INFOCOM)*, pp. 2896-2904, Turin, Italy, April 14-19, 2013.

3. **Biao Han**, Jie Li, Yuguang Fang, and Jinshu Su, “GATORS: Geographical-Aware Transmission Relay Placement Schemes for Capacity Maximization in Cooperative Networks”, *The 31st IEEE International Conference on Computer Communications (IEEE INFOCOM)*, Demo/Poster Session, Orlando, USA, March 25-30, 2012.

4. **Biao Han**, Jie Li, and Jinshu Su, “Self-supported Congestion-aware Networking for Emergency Services in WANETs”, in *Proceeding of the 30th IEEE International Conference on Computer Communication (IEEE INFOCOM)*, pp. 891-899, Shanghai, China, April 10-15, 2011.

5. **Biao Han**, Jie Li, and Jinshu Su, “Optimal Relay Assignment for Secrecy Capacity Maximization in Cooperative Ad-hoc Networks”, in *Proceeding of the IEEE International Conference on Communications (IEEE ICC)*, pp. 4721-4725, Budapest, Hungary, June 9-13, 2013.

6. **Biao Han**, Jie Li, and Jinshu Su, “Optimal Relay Node Placement for Multi-pair Cooperative Communication in Wireless Networks”, in *Proceeding of the IEEE Wireless

Communication and Networking Conference (IEEE WCNC), pp. 4771-4776, Shanghai, China, April 7-10, 2013.

7. Yu Gu, Yusheng Ji, Jie Li, **Biao Han**, and Baohua Zhao, “Delay-bounded Sink Mobility in Wireless Sensor Networks”, in *Proceeding of the IEEE International Conference on Communications (IEEE ICC)*, pp.740-744, Ottawa, Canada, June 10-15, 2012.