中文摘要

摘要：近年来，网络编码、协作通信、认知无线电等技术由于能大幅提高无线网络性能而成为了无线通信领域的研究热点。与传统通信技术不同的是，这些新技术更多地依赖于无线网络节点间的协作与认知行为。但是，由于受到自身处理能力、存储空间、电池容量等各种资源的限制，网络节点在没有激励机制的情况下往往表现出自私行为，从而影响无线网络性能；此外，以认知无线电技术为代表的相关技术要求无线网络节点可以动态地、不受任何约束地接入主用户的授权频段，在提高网络性能的同时也使得网络节点可以方便地实施窃听、干扰等恶意行为，为无线通信带来了新的安全问题。因此，研究无线网络中节点的行为，对提高网络性能、增强网络安全具有重要意义。

本文利用博弈理论，对无线网络中节点的自私行为和恶意行为进行了研究，主要工作包括以下两个方面：

(1) 从提高网络性能的角度，结合网络编码技术研究了无线网络中节点的自私行为。通过建立链路节点的重复博弈模型，在考虑链路节点自私行为的基础上，提出了一种促进流量均衡分配的策略。

(2) 分析了 MIMO 窃听信道模型中无线网络节点的行为并建立了博弈模型，进而针对博弈模型中攻击者位置、天线数量、发射功率及友好中继节点不同策略等情况给出了相应的博弈结果及保密率。

关键词：无线网络；博弈论；纳什均衡；网络编码；自私行为；MIMO；窃听信道；保密率

分类号：TP393.0

ABSTRACT

ABSTRACT: In recent years, the new technologies such as network coding, cooperative communication and cognitive radio are becoming the hot points in the field of wireless communications, which are proved to improve the network performance greatly. Compared with the traditional communication technology, these new technologies more dependent on the cooperation and cognitive of network nodes. However, some network nodes show the selfish behaviors without motivation mechanism of which the resources (energy, memory, bandwidth etc) are limited, and it has a direct impact on network performance. Moreover, the relevant technology such as cognitive radio requires that the CR user can use the corresponding band freely, so it is easy for the network nodes to wiretap information and jam communication, which has brought new safety problems for wireless communications. Therefore, the research on node behaviors in wireless network has significances to the performance and security of wireless network.

In this paper, the node behaviors in wireless network are analyzed and researched using the game theory. The main works can be summarized as follows:

(1) In order to improve the network performance, this paper analyses the selfish behaviors of node in wireless network based on network coding. A model of the repeated game for link nodes is established, and on the basis of the selfish behaviors of link node, we propose a strategy to balance the distribution of network flows.

(2) This paper analyses the behaviors of node in MIMO Wiretap channel, and establishes a mode of game. Then the game result and secrecy rate are given for when the attacker in the mode has different strategies such as location, the number of antenna and the power or when there is a friendly relay in the mode.

KEYWORDS: Wireless network; Game theory; Nash equilibrium; Network Coding; Selfish Behaviors; MIMO; Wiretap channel; Secrecy rate.

CLASSNO: TP393.0

致谢

本论文的工作是在我的导师王升辉老师的悉心指导下完成的，王升辉老师严谨的治学态度和科学的工作方法给了我极大的帮助和影响。在此衷心感谢两年来王老师对我的关心和指导。

王老师悉心指导我们完成了实验室的科研工作，在学习上和生活上都给予了我很大的关心和帮助，在此向王老师表示衷心的谢意。

熊柯老师对于我的科研工作和论文都提出了许多的宝贵意见，在此表示衷心的感谢。

在实验室工作及撰写论文期间，付秀花、刘振兆等同学对我论文中的研究工作给予了热情帮助，在此向他们表达我的感激之情。

另外也感谢我的家人，他们的理解和支持使我能够在学校专心完成我的学业。

1 绪论

1.1研究背景

无线通信网络按照其组网控制方式可以分为集中式和分布式两类。集中式网络要求在无线网络中布置基础设施，比如依靠基站和移动交换中心等基础设施支持的蜂窝移动通信网络、基于接入点(Access Point)和有线骨干网模式工作的无线局域网等；与之对应，分布式无线网络不依赖固定基础设施，具有动态变化的拓扑结构，能快速构建网络，可广泛应用于国防战备、灾难援助等特殊场合，主要包括移动自组织（Ad-hoc）网络、传感器网络、Mesh 网络等。无论哪种组网方式，无线网络中节点的行为方式都直接影响着网络性能。无线网络节点间最常见的行为方式是竞争，由于网络节点共用开放式的无线信道，同一空间中的不同通信节点对之间会产生干扰，这种干扰最直接的后果就是导致通信数据包的丢失，继而使网络性能下降；除竞争外，无线网络节点还存在着协作与认知行为[29]，在无线自组织网络（Ad hoc）中，两个无法直接通信的节点必须借助其他节点的分组转发才能进行通信，在这种场景下，节点间的协作行为是网络正常运行的基础；而建立在节点认知行为基础上的认知无线电技术可以显著改善频谱利用率，也得到了越来越广泛的关注[30]。

无线网络节点间的竞争、协作、认知行为相互作用、相互依赖，并受网络环境的限制和约束。传统无线通信技术主要关注无线网络节点间的竞争关系，比如无线局域网中 MAC 层的 CSMA/CA 机制，网络层的 IP 技术等，其目标是在保证网络通信节点传输公平性的基础上，尽力提高网络吞吐量、延时及抖动等性能指标。近年来，随着无线通信技术的发展，以网络编码、协作中继等技术为代表的新理论新技术不断出现，这些新技术更多地依赖于无线节点间的协作与认知行为，由于能大幅提高无线网络性能而成为了研究热点。

需要注意的是，协作通信、认知无线电等相关技术的实现是建立在网络节点的无条件协作和认知基础上的。一方面，建立在协作行为基础上的协作通信、网络编码等通信理论要求无线网络节点是无私的，即每个节点都愿意为其他节点提供网络服务。在一些如军事、救灾等特殊场景中，可以认为节点具有这种无私的协作意愿和行为，节点协作行为的无私性假设可以成立。而在一些商业性的民用化网络中，由于受到自身处理能力、存储空间、电池容量等各种资源的限制，网络节点为了节省自身的资源消耗，在没有激励机制的情况下，往往不参与路由寻

路或不对传递给其他节点的数据包进行转发，比如 P2P 网络中的“搭便车”（free-riding）现象等。这种节点的自私性行为势必会破坏节点之间的协作，从而影响无线网络性能；另一方面，建立在认知行为基础上的认知无线电技术要求无线网络节点可以动态地、不受任何约束地接入主用户的授权频段，尽管这种技术可以通过认知寻找空闲频谱资源，从而提高网络频谱资源利用率，但同时也为窃听、干扰等恶意行为带来了便利条件。由于无线网络的广播特性，在物理层认证机制不完善的情况下，一些处于合法通信者通信范围内的节点，在不被感知的情况下可以窃取合法通信者间传输的信息，也有一些节点发送恶意的干扰信号来对合法通信过程实施干扰，从而显著减少合法通信节点的可用信道资源，无线网络节点的这些带有主观恶意性的认知行为给无线通信带来了新的安全问题。

综上所述，随着协作通信、认知无线电等新技术的研究和实用化，无线网络节点的行为研究是一个不可回避的问题。研究无线网络中节点的行为，寻找对付节点自私行为和恶意行为的方法，对提高网络性能、增强网络安全具有重要意义。

1.2研究现状

无线网络节点的自私性使得网络节点并不会“无私”协作，而节点的恶意认知行为也使得网络中的不可信节点可以不受约束地窃听信息、干扰合法通信。近年来人们已开始用博弈论等经济学理论对于无线网络节点间的竞争、协作、认知等行为模式进行研究，进而提出了一系列激励自私节点进行合作、限制节点恶意行为以保证安全通信的理论和方法。

1.2.1 节点自私行为研究

节点自私行为是指网络节点为节省自身资源，不愿意无条件为其他节点转发数据的行为。无线网络中节点的自私行为制约着网络各种传输和路由机制的实施，影响着网络流量、网络资源分配等。在最易受节点自私行为影响的 Ad hoc 网络中，Dewan[1]等人指出，由于存在自私节点而使一些常见的如 DSR 或者 AODV 等协议失效，并通过仿真实验显示，如果网络中 40%的节点有自私行为，整个网络的吞吐量将降低一半。

为了减少网络节点自私行为对网络性能的影响，激励网络自私节点进行协作，目前研究者们提出了基于信誉、市场概念和博弈论的节点间协作的激励机制[2]。前两种机制通过引入信誉值和市场概念等外部机制来迫使节点协作，基于博弈论的方法则是通过分析和利用利益驱动的本质对节点决策行为的影响来引导合作。由

于考虑了节点动机，而且当网络规模不断扩大时，博弈论的分析结果能够很好地推广和应用，因此，用博弈论的方法来分析无线网络中节点的自私行为已成为一种非常有效的研究方法。人们首先使用博弈论研究了 Ad hoc 网络的节点自私行为建模和激励机制，如针对 Ad hoc 网络中的路由机制研究出了一系列基于博弈论的路由协议拍卖机制 Ad Hoc-VCG[3]、Corsac[4]、Team[5]、Rpp[6]等；随后 Felegyhazi 等人[7]针对节点拓扑依赖关系建立了无线 Ad Hoc 网络的博弈模型；同时 Srinivasan 等人[8]也提出了 GTFT 模型，王堃[9]针对 Ad Hoc 网络的节点转发过程，提出了一个基于全局惩罚机制的重复博弈转发模型，这些博弈模型的建立对 Ad hoc 网络理论和技术的研究具有重要的指导意义。

然而，目前基于博弈论的自私行为和激励机制的研究多出现在 Ad hoc 网络中，研究的目标也多局限为网络层中的路由优化问题，对其他协作通信技术的关注度不高。近年来，依赖于节点间密切协作的网络编码技术逐渐被人们所重视，网络编码技术利用节点的存储计算及转发能力，由于具有提高网络吞吐量、网络带宽资源利用率，平衡链路负载等优点，而成为进入 21 世纪后通信领域的一项重大突破性技术。在网络编码技术中，网络节点扮演着路由器和编码器双重角色，强调节点之间相互合作，节点的自私行为将对网络编码性能产生直接的影响。因此，分析网络编码技术中的节点行为模式及其激励机制对提高网络编码性能具有重要作用。目前用博弈论等方法对网络编码技术中节点自私行为的研究才刚刚起步，Marden 等人[10]提出了一种基于网络编码的路由博弈方法，从提高网络编码机会和缩短路由路径出发，考虑了链路自私性与网络编码性能的关系，并给出了纳什均衡策略。但是，文献[10]中的研究模型略显简单，仅考虑了包含通信双方的博弈模型，没有从整个网络的设计角度进行分析，没有考虑通信链路乃至整个网络中涉及的其他节点的自私性行为，极易导致网络出现流量不均衡的问题。为此，本文第一个工作将以此为切入点研究网络编码技术下的链路节点的自私行为问题。

1.2.2 节点恶意行为研究

与有线网络不同，无线网络的开放性为网络节点实施恶意行为带来了便利。除正常的认知行为外，节点的窃听、干扰等行为都可以称为节点的恶意行为，这种恶意行为直接导致了无线网络的通信安全问题。目前，针对无线网络中的通信安全问题，人们仍采用传统有线网络中使用的加密解密安全机制，如 DES[11]、AES[12]等加以解决。但是，这种加解密安全机制基本上是在网络协议的高层（链路层以上）实现的，对无线网络中物理层出现的窃听和加扰行为针对性不强，因此，近年来，基于信息理论安全原理的物理层安全技术越来越引起了学术界的重视。物

理层安全技术利用无线网络物理层的信道特点，通过波束赋形、人工加扰等方法恶化窃听者接收信号的信噪比，从而使窃听者不能无差错地获取明文信息，放宽了密码机制中“窃听者能够无差错地获取明文信息”这一限制条件，能够在不需要密钥的情况下实现安全传输，被认为是解决无线网络安全问题的一种有效理论。

根据信息理论安全原理，三节点窃听模型是物理层安全技术中的基本模型，如图 1-1 所示，两个合法的通信者 Alice 和 Bob 通过一条主信道进行通信，而第三方 Eve 试图通过窃听信道窃取 Alice 和 Bob 之间的通信信息。研究者们在三节点窃听模型基础上发展出了多种类型的窃听信道模型。Barros 和 Rodrigues[13]研究了慢衰落信道的秘密容量。Liang[14]等人得到了各态历经的衰落信道的秘密容量(ergodic secrecy capacity)。随着 MIMO 技术的日趋成熟，研究者们在窃听模型的节点 Alice、Bob 和 Eve 处加入了多天线技术，以提高信道的容量和可靠性，从而出现了 MIMO 窃听信道模型。文献[15]中给出了 MIMO 高斯窃听信道的秘密容量的闭合表达式。

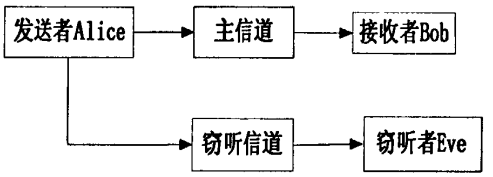


图 1-1 三节点窃听模型

然而，目前的研究中并没有考虑到窃听模型各个节点的行为特性。Eve 节点仅实施窃听行为的假设不尽合理，在实际无线网络中，如果窃听信道质量很差，Eve 在不能得到满意的窃听效果情况下，会选择恶意地干扰 Bob 来破坏正常通信。另外，加入了多天线技术以后，窃听模型中的发送者 Alice 除了执行发送任务外，也可以选择利用部分天线对窃听者进行人工加扰，来保证通信安全。因此，在考虑 Eve 和 Alice 有多种行为选择，而且双方行为决策相互影响的情况下，用博弈论的方法来研究窃听模型中节点的决策问题，以及节点行为选择对安全通信的影响，成为了窃听模型研究的一种新思路。

用博弈论的方法分析窃听模型节点行为的研究才刚刚起步，目前仅有一篇研究文献，就是 A. Mukherjee 等人[16]在 2010 年提出了一种针对 MIMO 窃听信道的博弈模型，本文将在这方面做进一步的研究工作。

1.3主要研究内容

本文主要研究无线网络中节点行为对网络性能及安全性的影响，针对无线网络节点中普遍存在的自私行为、恶意行为这一线索展开。一方面结合网络编码技术研究了网络节点的自私行为，主要着眼于分析自私行为带来的影响，并结合分

析提出限制节点自私性的激励机制，改善网络性能；另一方面是结合 MIMO 窃听信道模型研究网络节点的恶意行为，主要着眼于选择提高系统保密率，防止节点恶意行为的策略，以增强网络安全。

论文主要研究内容如下：

(1) 将博弈论作为分析工具引入到无线网络节点行为研究中，介绍了博弈论基础知识，描述了网络节点的自私行为、恶意行为，分析了博弈论适合研究无线网络节点行为的原因，并总结了无线网络节点之间存在的几类博弈问题。

(2) 从提高网络性能的角度，结合网络编码技术研究了网络节点的自私行为。分析了现有基于网络编码的链路博弈，指出其由于没考虑链路中间节点自私行为，将导致出现网络资源分配不均衡的问题。然后通过建立链路中间节点的重复博弈模型，分析了链路中间节点自私行为造成的后果以及影响因素。最后设计了链路博弈和报价机制相结合的方案，来解决网络流量分配不均衡的问题 。

(3) 从提高网络物理层安全的角度，结合 MIMO 窃听信道模型研究了网络中节点的恶意行为。研究了现有 MIMO 窃听信道博弈模型，分析了恶意攻击者位置、天线数量以及发射功率等因素对博弈结果及保密率的影响，并讨论了存在中继节点时中继窃听信道的保密率问题。

1.4论文结构和安排

论文一共分为五章，文章结构和各章内容如下：

第一章绪论。介绍了论文的研究背景和研究现状，概括了论文的主要工作，并列出了论文的组织结构。

第二章博弈论及其在无线网络节点行为研究中的应用。介绍了博弈论的基础知识，描述了无线网络节点的自私、恶意行为，重点分析了博弈论适合研究无线网络节点行为的原因，并总结了无线网络节点之间存在的几类博弈问题。

第三章基于网络编码的节点自私行为分析。在前人提出的基于网络编码的链路博弈模型基础上，指出了其由于没有考虑链路上中间节点的自私行为而导致的流量分配不均衡的问题；通过建立链路中间节点的重复博弈模型，分析得出影响节点自私的因素；提出了链路博弈和报价机制相结合的解决方案，解决流量分配不均衡的问题，并给出了仿真实验。

第四章基于窃听信道的节点恶意行为分析。在前人提出的 MIMO 窃听信道博弈模型基础上，分析了恶意攻击者位置、天线数量及发射功率三个因素对博弈结果和系统保密率的影响，讨论了存在中继节点时中继窃听信道的保密率问题。

第五章总结与展望。对本文所做的工作进行总结，并展望今后研究的方向。

2 博弈论及其在无线网络节点行为研究中的应用

博弈论作为一种处于各学科之间的研究人类行为的方法，也是研究协作问题的有效工具。虽然博弈论起源于研究经济学和行为学，并非无线通信领域的主要研究范畴，但由于网络节点的行为是操作网络设备的人出于一定动机的决策结果，与人的行为有相似之处，因此博弈论同样适合研究无线网络节点行为。本章首先对博弈论的基本知识进行了介绍；然后分析了博弈论适合研究网络节点行为的原因；并结合网络节点的行为对节点之间的几类博弈问题进行了简要介绍。

2.1 博弈论基础

2.1.1 概述

“博弈论”译自英文 Game Theory，是研究决策主体的行为发生直接相互作用时的决策及这种决策的均衡问题，从本质上来说，博弈研究的是决策问题[17]。

博弈论的思想及对具有博弈论性质问题的研究可以追溯到 19 世纪以前，但是系统的博弈论问题的建立和发展则是在 20 世纪中期。总体来看，博弈的发展主要经历了三个阶段[9]。

第一阶段的研究重点是合作博弈(cooperative game)。继冯·诺依曼提出合作博弈之后，合作博弈论在 20 世纪 50 年代发展到鼎盛期，Nash 和 Shapley 等人相继提出了合作博弈的一些核心概念，这些概念一直沿用到今天。

第二阶段的研究重点是非合作博弈(Non-cooperative game)。1950 年数学家 Nash 在发表的论文中提出了著名的“纳什均衡(Nash equilibrium)”的概念，同年 Tucker 定义了“囚徒困境”，从此奠定了非合作博弈研究的基石。在此之后，人们对博弈论的研究基本上都是沿着纳什均衡这条主线展开的。1965 年，Selten 将纳什均衡的概念扩展到动态甚至是多阶段博弈，证明了非合作博弈中并不是所有纳什均衡是同样合理的。1967 年， Harsanyi 针对非合作博弈中的不完全信息提出了海萨尼转换，将不完全信息的非合作博弈转化成不完全的信息博弈，从而将博弈论的发展推向了另一个全新的阶段。

第三阶段是博弈论的应用研究。博弈论以往常被研究者视作经济学的一个分支，而实际上它是一种广义的行为学方法论，应用领域也从经济学扩展到了政治学、国际关系、生物学、计算机科学、通信理论等领域。

2.1.2 博弈论理论框架

1. 博弈论的三要素

一个最基本的博弈结构至少包括三个基本要素，即参与者(player)、策略集合(strategy set)和效用函数(payoffs function)。

1) 参与者

参与博弈的当事人、博弈的决策主体或博弈策略的制定者称为博弈的参与者，也称为参与人或局中人，通常用 N 表示其集合。一个博弈中至少要有两个参与者，参与者除了可以是自然人以外，还可以是代表共同利益的一个集团，如球队、企业、国家等。参与者参加博弈的目的是通过合理选择自己的行动，来取得自己效用 (收益)水平的最大化，因此在博弈过程中，参与者必须有不同的行动可作应对选择，并在博弈的结局中能计算出各种不同的行动组合分别产生的效用 (收益)。

2) 策略集合

策略也称为战略，是指博弈中参与者选择的一个实际可行的、完整的行动方案，是博弈方进行博弈的工具和手段。在任何一个博弈中，每个策略集合至少应该包括两个不同的策略，如果某个参与者只有一个策略，那么博弈的结果将完全取决于其他参与者，该参与者便失去了作为参与者的资格。在博弈论中，通常用 S_i 来表示参与者 i 所有可选择的策略集合。

3) 效用函数

效用函数是指在特定策略组合下参与者得到的确定的效用或者期望效用，通常用 U_i 表示参与者 i 的效用函数。所谓效用即博弈结果中每个参与者的得与失，可以用数值刻画其大小。不同的策略选择决定了博弈参与者的效用，博弈论的一个基本特征是一个参与者的效用不仅取决于自己的策略选择，还取决于所有参与者的策略选择。

一般地，参与者、策略集和以及效用函数这三个基本要素确定之后，一个博弈模型也就确定了。任意一个博弈 G 可以用数学表达式表示为：$G=\{N,\{S_i\},\{U_i\}\}$。

2. 博弈论的分类

根据不同的划分标准，博弈可分为不同的类型。

1) 合作博弈和非合作博弈

合作博弈和非合作博弈的主要区别在于相互发生作用的当事人之间有没有一个具有约束力的协议，如果有，就是合作博弈，如果没有，就是非合作博弈。合作博弈亦称为正和博弈，是指博弈双方的利益都有所增加，或者至少是一方的利益增加，而另一方的利益不受损害，因而整体利益有所增加。合作博弈主要研究参与者达成合作时如何分配合作得到的收益，即收益分配问题。而非合作博弈并

不是说每个参与者总是拒绝和其他参与者合作，而是在博弈中参与者只根据他们的"可察觉的自我利益"来决策，即使在博弈之前参与者可以相互沟通，他们之间的协议、威胁或许诺也是无法实施的。非合作博弈主要研究人们在利益相互影响的局势中如何决策使自己的收益最大，即策略选择问题。

2) 静态博弈和动态博弈

根据博弈问题本身包含的参与者决策时序的差异，可以将博弈问题分为静态博弈、动态博弈两类。静态博弈是指在博弈中，参与者同时选择或虽非同时选择，但后行动者并不知道先行动者采取了什么具体行动；动态博弈是指在博弈中，参与者的行动有先后顺序，且后行动者能够观察到先行动者所选择的行动。例如，"囚徒困境"就是同时决策的，属于静态博弈；而棋牌类游戏等决策或行动有先后次序的，属于动态博弈。

3) 完全信息博弈和非完全信息博弈

根据博弈问题中参与者对其他参与者了解程度，可以将博弈问题分为完全信息博弈和不完全信息博弈。完全信息博弈是指在博弈过程中，每一位参与者对其他参与者的特征、策略集合及效用函数有准确的信息，也就是在博弈开始前所有参与者对博弈问题本身没有任何不确定性；而不完全信息博弈则意味着在博弈开始之前，至少有一个参与者对博弈问题信息结构的某一方面没有完全了解，存在事前不确定性。

此外，博弈论还有很多分类，比如以博弈进行的次数或者持续长短可以分为有限博弈和无限博弈；以表现形式也可以分为策略型博弈或者展开型博弈等。

3. 博弈论的分析基础

在求解博弈问题时，不同问题可用不同的博弈模型进行描述或建模，但是无论用哪种方式描述博弈问题，分析框架中都隐含着以下假设。

(1) 参与者完全理性。完全理性是指参与者在追逐效用最大化时能前后一致地作决策。它包含两方面的含义，一是每个参与者能对自己的行为有个正确的预期；二是每个参与者对其他参与者的行为也有一个正确的预期。博弈论的精髓就在于，博弈中每个参与者能从其他参与者的角度来观察事件的发展，能够预测出其他参与者可能会选择的行为和策略，从而根据这个策略来决定自己的最佳行动。

(2) 对博弈问题的描述和完全理性是共同知识。共同知识是指这样一种信息，这种信息每个参与者都知道它，并且每个参与者都知道每个参与者都知道它，每个参与者都知每个参与者都知道每个参与者都知道它，……，如此等等。这个假设是博弈分析中参与者进行分析、预测和逻辑推理的基础，它确保了每个参与者的决策环境、理性层次及逻辑思维层次是完全相同的。

4. 博弈问题的解

博弈问题的解定义为：所有参与者都预测到的结果，即参与者的一致性预测。需要注意的是，这种一致性的预测不仅仅是所有参与者都预测到某个结果会出现，而且是所有参与者都预测到所有参与者都预测到某个结果会出现，等等，也就是说这种一致性预测是共同知识。那么对于一个博弈问题什么样的结果可以成为一致性的预测呢？这个问题目前人们已有了比较一致的认识，即将纳什均衡作为博弈问题的一致性预测，也就是博弈问题的解。

2.1.3 纳什均衡

博弈问题的解，也就是该博弈最可能出现的结果，称为"均衡"。博弈问题中最重要、最基本的均衡是纳什均衡。假设博弈中有 n 个参与者，在给定其他参与者策略的条件下，每个参与者选择自己的最优策略（个人最优策略可能依赖于也可能不依赖于他人的策略），使自己利益最大化，所有参与者的策略构成一个策略组合。纳什均衡指的是这样一种策略组合，这种策略组合由所有参与者的最优策略组成。即在其他参与者不改变当前策略的前提下，任何一个参与者都无法通过单方改变自己的策略来获取更高的收益。

定义 2-1[17] 对于博弈 $G=\{N,\{S_i\},\{U_i\}\}$，如果由各个参与者的任意策略组成的某个策略组合 $(s_1^*,\cdots,s_n^*)$ 中，任意参与者 i 的策略 s_i^*，都是对其他参与者策略组合 $s_{-i}^*=(s_1^*,\cdots,s_{i-1}^*,s_{i+1}^*,\cdots,s_n^*)$ 的最佳对策，即 $U_i(s_i^*,s_{-i}^*)\geq U_i(s_i,s_{-i}^*)$ 对任意 $s_i\in S_i$ 都成立，则称 $(s_1^*,\cdots,s_n^*)$ 为 G 的一个纳什均衡。

定理 2-1[17] 每一个有限 n 人非合作博弈至少存在一个纳什均衡。

纳什均衡刻画了理性选择的结果，即利益冲突达到一种稳态以至无人会单方面加以改变。假使其他参与者不变换其策略，则任何参与者都不能通过单方面变换自己的策略来增加其效用。纳什均衡的概念提供了一种非常重要的分析手段，使博弈论研究可以在一个博弈结构中找到比较有意义的结果。

2.1.4 博弈模型

1. 囚徒困境博弈

囚徒困境博弈是由 A. W. Tucker 于 1950 年定义的一个两个参与者的战略式博弈，是博弈论的一个经典案例，也是本文研究的博弈模型的基础。经典的囚徒困境假设这样一个情境，警方逮捕两名嫌疑犯（Tom，Jerry），但没有足够证据指控二人入罪。于是警方分开囚禁嫌疑犯，分别和二人见面，并向双方提供以下相

同的选择：如果两人均坦白，将被各判刑 4 年；如果两人均抵赖，将会因为证据不足而各判 1 年；如果其中一人坦白另一人抵赖，坦白的人将会得到宽大处理而被无罪释放，而抵赖的将被重判，判刑 6 年。

在“囚徒困境”博弈问题中，参与者是两个嫌疑犯 Tom 和 Jerry，每个参与者有两个策略：坦白和抵赖，参与者的效用（支付）是判刑的年数。图 2-1 给出了“囚徒困境”博弈问题的支付矩阵。

		Jerry	
		坦白	抵赖
Tom	坦白	-4，-4	0，6
	抵赖	-6，0	-1，-1

图 2- 1“囚徒困境”博弈支付矩阵

支付矩阵中每个表格里的数字代表对应策略组合下两个囚徒的收益，前一个是 Tom 的收益，后一个是 Jerry 的收益。如图 2-1 所示，对于每个囚徒，当对方坦白时，自己坦白得-4，抵赖得-6，所以应该选择“坦白”；而当对方抵赖时，自己坦白得 0，抵赖得-1，所以还是应该选择“坦白”。也就是说，无论对方如何选择，每个囚徒都会选择“坦白”，因此策略组合（坦白，坦白）是每个参与者最佳的策略组合，是囚徒困境博弈唯一的纳什均衡解。

这样的结果似乎与我们的直觉相矛盾，因为从两个囚徒的观点来看，纳什均衡解（坦白，坦白）的收益明显劣于策略组合（抵赖，抵赖）所得到的收益。这就说明了存在利益冲突的情况下，利己主义个人理性选择的结果在总体上并不是最有效的，这也反映出现实生活中经常出现的“个人理性与集体理性之间的矛盾”，因此纳什均衡揭示了利己理性的弱点。

2. 重复博弈

重复博弈是一种特殊的博弈，在博弈中，相同结构的博弈重复多次，甚至无限次，其中每次博弈称为“阶段博弈”。在重复博弈中，每次博弈的条件、规则和内容都是相同的， 但由于有一个长期利益的存在，因此各参与者在当前阶段的博弈中要考虑到不能引起其他参与者在后面阶段的对抗、报复或恶性竞争，即不能像在一次性静态博弈中那样毫不顾及其他参与者的利益。有时，一个参与者做出一种合作的姿态，可能使其他参与者在今后阶段采取合作的态度， 从而实现共同的长期利益。

以“囚徒困境”博弈问题为例，博弈只进行一次时存在唯一的纳什均衡解(坦白，坦白)，这种情况下博弈参与者认为以后继续合作的可能性不大，因此倾向于选择背叛策略来使自己收益更大。如果囚徒困境博弈重复进行两次，甚至 N 次，则参

与者未来合作带来的收益很大，超过了采取相互背叛策略所获得的短期收益，那么出于长远考虑，参与者之间会逐渐形成一种默契，使得双方都从默契的合作中得到更多的收益。因此，在囚徒困境的重复博弈中，如果采用适当的激励策略，就能使参与者之间相互合作。

3. 零和博弈

零和博弈又称零和游戏，与非零和博弈相对，属于非合作博弈，指参与博弈的各方，在严格竞争下，一方的收益必然意味着另一方的损失，博弈各方的收益和损失相加总和永远为"零"，双方不存在合作的可能。零和博弈的结果是一方吃掉另一方，一方的所得正是另一方的所失，整体利益并不会增加。

现实生活中随处可见与零和博弈类似的局面，胜利者的光荣后面往往隐藏着失败者的辛酸和苦涩。在20世纪人类经历了两次世界大战，经济的高速增长、科技进步、全球化以及日益严重的环境污染之后，"零和游戏"观念正逐渐被"双赢"观念所取代。人们开始认识到"利己"不一定要建立在"损人"的基础上。通过有效合作，皆大欢喜的结局是可能出现的。但从"零和游戏"走向"双赢"，要求各方要有真诚合作的精神和勇气，在合作中不要耍小聪明，不要总想占别人的小便宜，要遵守游戏规则，否则"双赢"的局面就不可能出现，最终吃亏的还是自己。

2.2博弈论与无线网络节点行为

2.2.1 无线网络节点行为概述

无线网络节点可以分成三种类型[18]：①正常节点，它们行为良好，能无私地为其他节点提供服务；②自私节点，它们谨守本分，只对与自己有关的数据感兴趣，但是为了自己的利益，不愿无条件为其他节点转发数据包；③恶意节点，它们恶意攻击破坏网络，甚至不惜以牺牲自身的能量、带宽为代价。自私节点和恶意节点统称为不良节点，它们的行为通常不按照网络配置者的要求，严重危害着网络的性能及安全。下面将详细介绍节点的自私行为和恶意行为。

1. 节点自私行为

在一些多跳无线网络（如Ad-hoc网络）中，节点通常扮演着终端和路由器双重角色，因此节点在保证自身正常通信的同时，也要为网络的其他节点提供转发数据和选路的服务。然而网络中的节点并非都像人们假设的那样，具有良好的合作性，考虑到自身利益，一些节点存在着自私行为，它们不愿无条件为其他节点发送数据包。

节点自私行为的动机是为了节省自身的资源，因为网络节点本身受到电池能量、无线带宽、计算能力、内存空间等各种资源的限制，如果节点拒绝提供替其他节点转发数据包的服务，它将节省大量能量，从而大大延长其生存时间。节点自私行为通常有两种表现形式[19]。

(1) 参与路由服务，但不愿提供数据包的转发服务。自私节点通过采用各种策略来躲避替其他节点转发数据包的任务，从而节省大量能量，其中最直接的策略是丢弃其他节点请求转发的数据包。如图 2-2 所示，这种节点的自私行为将直接导致链路信息的丢失。

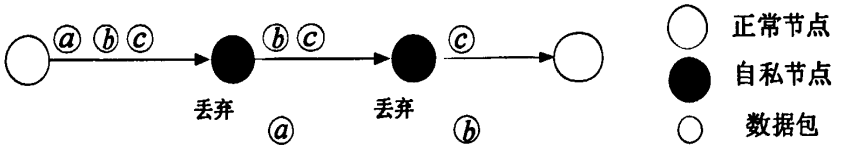


图 2-2 节点自私性行为类型一

(2) 不愿参与路由服务。自私节点通过操纵路由协议，使之不选择以自己作为中间节点的路径，达到不参与任何数据包的转发工作的目的。如图 2-3 所示，这种节点的自私行为将导致最后数据传输路径不是预期的最短高效路径，从而增加了网络能耗，造成了网络资源的浪费。

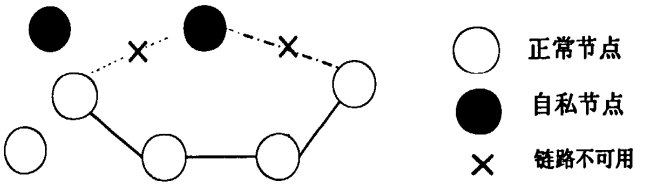


图 2-3 节点自私性行为类型二

2. 节点恶意行为

节点恶意行为是指节点的窃听、干扰等行为。无线网络由于信道的广播特性，比起有线网络，更容易受到节点恶意行为的攻击，从而给网络安全带来严重的隐患。这里将重点讨论节点恶意行为中窃听行为和干扰行为。

1) 窃听行为

无线网络中节点的窃听行为是指驻留在正常节点传输范围内的网络节点利用无线信道的广播特性监听有价值的通信信息的行为。如图 2-4 所示，无线网络中不仅恶意节点存在窃听行为，网络中的合法节点、甚至是能够转发数据的中继节点，当其收到并解码不属于自己的信息时，也能成为窃听节点。

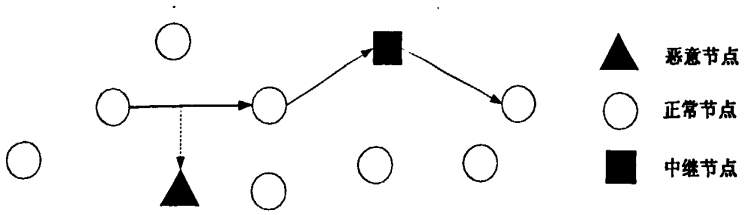


图 2-4 节点窃听行为示意图

2) 干扰行为

无线网络中节点的干扰行为是指网络中的节点通过发射无线干扰信号来妨碍其他节点通信的行为。如图 2-5 所示，在实际的无线网络中，不仅网络中的恶意节点可以实施干扰行为来阻止正常节点交换数据，网络中的正常节点也可以通过人工加扰来阻止其他节点窃听自己的通信信息。

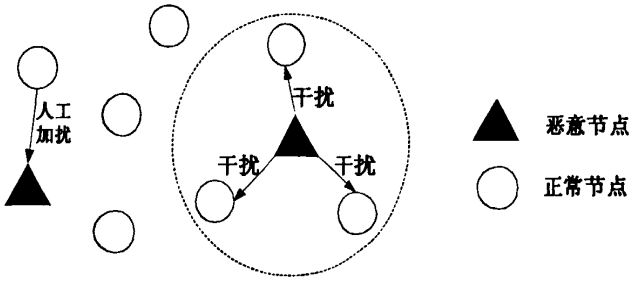


图 2-5 节点干扰行为示意图

无线网络中的节点一般是一些无线设备（如笔记本电脑等），不管是节点的自私行为还是节点的恶意行为，都是操作设备的人出于一定动机的决策结果，因此，作为研究人与人交互行为有效工具的博弈论，也同样适合研究网络节点之间的行为交互。具体来说，用博弈理论来分析无线网络节点行为主要有以下原因。

(1) 博弈论的分析基础是假设博弈参与者是“理性”的，在研究人与人之间的行为交互时，人是不完全符合理性假设的，人经常犯错，但是无线网络中的节点，有精确的计算能力也不会出错，完全符合“理性”的假设。

(2) 博弈参与者具有模仿能力，个体参与者的行为会潜在地影响到所有其他的参与者，因此博弈模型里，每个参与者的收益不仅取决于他自身的行为，而且也取决于其他人的行为，而无线网络中节点之间的行为也是相互影响的。

(3) 博弈参与者的目标是追求个人利益最大化，在无线网络中，无论是服务的提供者——服务器、路由器、网络链路等，还是服务的要求者——用户都不在意全局网络的成本和效率，而是“自私”地追求各自利益最大化，两者动机一致。

因此，博弈论可以帮助我们建立无线网络节点之间的冲突与合作的模型，使网络布局者很好地理解网络节点的期望行为，从而通过设计方法或机制来诱导网

络节点选择一个全局满意的纳什均衡策略。

2.2.2 网络节点的博弈问题

如果把一个无线网络抽象成一个博弈模型，按照博弈的三要素，博弈的参与者对应于网络中的节点、链路等；博弈中参与者的策略集合对应于被研究的网络功能的相关动作集合；博弈的效用函数则对应于一些网络性能参数。表 2-1 给出了无线网络与博弈模型之间的对应关系。

表 2-1 无线网络与博弈模型对应表

博弈三要素	无线网络成分
参与者	网络节点、链路等
策略集合	被研究功能的相关动作集合，如路由路径选择、节点是否转发数据包（包转发概率等）、节点发送方案、节点窃听或干扰方案等
效用函数	网络性能参数，如能量消耗、吞吐量、保密率等

因此，无线网络中节点追求不同类型的效用（利益）时，会出现不同类型的博弈问题。下面将介绍几种常见的网络节点之间的博弈问题，本文第三、四章中对节点行为的研究就是针对其中的几种博弈问题。

1. 用户转发困境博弈

无线网络中可能存在如图 2-6 所示网络拓扑。图中两用户 S_1 和 S_2 分别要发送一个数据包到其接收者 D_1 和 D_2，在同一时隙里每个用户必须要对方用户进行转发才能完成通信。每个用户为对方转发包都要消耗一个成本，而如果通信成功，都能得到一个收益。每个用户为节省自身能耗都不愿替对方用户转发包，但又希望对方为自己转发包以完成通信任务，因此 S_1 和 S_2 之间就形成了一个转发困境博弈。

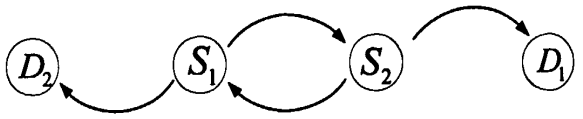


图 2-6 节点转发困境网络拓扑

网络中的这类博弈问题类似于博弈理论中的囚徒困境问题，是由于网络节点的自私行为导致的，如 P2P 网络中的“搭便车”（free-riding）问题（P2P 网络中节点只享用系统中的资源，而不对系统贡献自己的资源，从而破坏网络中节点的公平共享）就属于这类博弈问题。

2. 节点包转发博弈

在如图 2-7 所示网络拓扑中，源节点 S 想在每个时隙里发送数据包到其目的节

点D，必须依靠中间节点P_1和P_2来为其转发包。同样，中间节点转发包需要消耗一个成本，而如果通信成功（P_1和P_2都转发），则中间节点也会接收到一个收益。P_1和P_2可以选择转发包和不转发包两种策略，因此P_1和P_2之间就形成了一个节点转发博弈。

图 2-7 节点转发博弈网络拓扑

节点包转发博弈问题也是由于网络节点的自私行为导致的，在研究无线网络路由协议时常会出现，我们希望通过激励自私的中间节点进行协作来实现预期的路由。本文第三章中研究的基于网络编码的节点重复博弈模型，就是针对这类博弈问题建立的。

3. 节点干扰博弈

在如图 2-8 所示的网络拓扑中，发送者S想在每个时隙里发送数据包到其接收者D，而节点E可以干扰S和D之间的通信。S和E的收益互为相反数，通信越成功，S的收益越大，E的收益越小。因此S会选择一些策略行为来使通信成功，E也会选择一些策略行为来破坏通信，S和E之间就形成了一个节点干扰博弈。

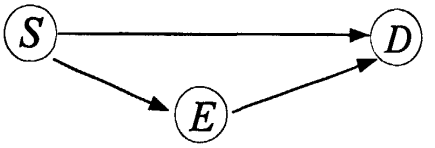


图 2-8 节点干扰博弈网络拓扑

节点干扰博弈问题是由于节点的恶意行为导致的，大多出现在窃听信道、节点攻击等网络场景中，我们希望设计机制使节点的决策结果最有利于网络的安全通信。本文第四章中研究的 MIMO 窃听信道博弈就是这类节点博弈问题。

4. 网络链路博弈

在如图 2-9 所示的网络拓扑中，节点S_1到其接收者 D_1之间的链路通信需要依靠中间节点P_1或者P转发包，节点S_2到其接收者D_2之间的链路通信需要依靠中间节点P_2或者P转发包。每条通信链路都有不同的路径策略选择，如图（a）或者图（b）中的情况，不同路径组合对网络性能（能耗、吞吐量等）的影响也不同，因此两条链路之间就形成了一个网络的链路博弈。

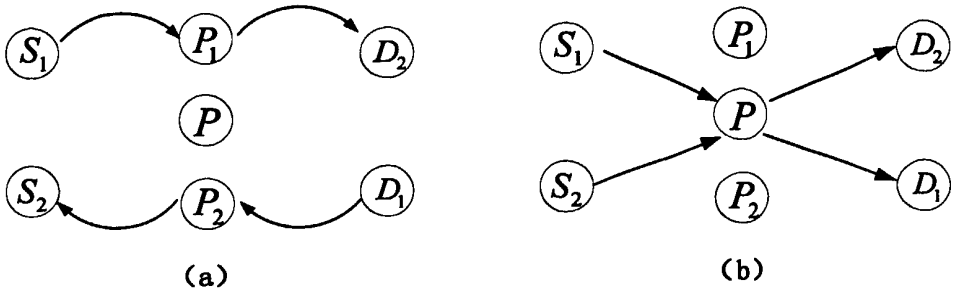


图 2-9 网络链路博弈拓扑

这类博弈问题是由于节点自私行为导致的，在很多网络场景中都会出现，而且应用于不同的场景时节点的决策结果也不同。比如在研究网络资源（如流量）分配问题时，我们希望节点的决策结果如（a）图，以达到资源分配均衡的目的；在研究网络编码问题时，我们则希望节点的决策结果如（b）图，以来提高网络编码机会，达到合作双赢的目的。本文第三章中介绍的基于网络编码的链路博弈就是这一类的节点博弈问题。

2.3本章小结

本章主要研究的是博弈论和无线网络节点行为研究的关系。首先介绍了博弈论的相关理论，然后对无线网络中节点的行为进行了概述，详细介绍了节点自私行为和节点恶意行为，最后分析了博弈论方法适合无线网络节点行为研究的原因，并介绍了网络节点之间存在的几种博弈问题，为后几章的分析奠定了基础

3 基于网络编码的节点自私行为分析

无线网络中自私节点为了节省自身资源，不愿意无条件为其他节点转发数据包，这种节点的自私行为将制约网络各种传输和路由机制的实施，造成资源浪费，严重影响网络性能。近年来出现的网络编码技术作为一种协同技术与编码技术的有机结合，强调节点之间相互合作，运用节点合作编码的概念来提高网络的整体性能。因此网络中节点的自私行为将直接导致网络编码不能顺利进行。为了研究存在网络编码的网络中节点的自私行为，Marden 等人[10] 从提高网络编码机会和缩短路由路径的角度，提出了基于网络编码的链路博弈模型。本章将此基础上，提出链路博弈由于没考虑链路中间节点自私性，而出现的网络资源分配不均衡的问题。然后通过建立链路中间节点的重复博弈模型，分析链路中间节点自私行为造成的后果以及影响因素。最后将设计链路博弈和报价机制相结合的方案，来解决网络流量分配不均衡的问题，并给出相关仿真实验。

3.1预备知识

3.1.1 网络编码基本原理

香农曾指出："通信网络端对端的最大信息流，是由网络有向图的最小割决定"，采用传统路由的方法无法确保信息传输速率达到最大流最小割定理所确定的信源和信宿间的最大流量。传统的路由方法中信息传输都是由源节点经过中间节点，以存储转发的方式传送到目标节点。一般来说，在网络的中间节点除了数据复制以外，并不需要做任何数据处理，普遍认为中间节点所进行的数据处理不会给数据传输过程本身并带来任何好处。然而，网络编码的提出彻底推翻了这一结论。2000 年，Ahlswede 等人[20]在一篇题为"网络信息流"的文章中提出了网络编码的概念，并证明了在单点对多点的组播通信网络中，通过在节点进行编码的方式可使信息传输速率达到网络的最大流量。

在传统的数据包传送方式中，中间节点仅仅扮演着转发器的角色，而在网络编码技术中，网络中的节点不仅可以参与数据的发送与接收，还可以对接收到的信息进行一定形式的编码处理，然后再传输出去。下面通过一个基本的网络编码单元来说明网络编码的基本思想及其带来的好处。如图 3-1 所示，节点 1 要发送数据包 X 到节点 3，节点 3 要发送同样大小的数据包 Y 到节点 1。节点 1 和 3 不在相互的通信范围内，必须借助于中间节点 2 来转发。如果用传统的发送方式，总共

需要4次发送来完成数据包X和Y的传送，数据包X经过$1\rightarrow 2$，$2\rightarrow 3$两次，数据包Y经过$3\rightarrow 2$，$2\rightarrow 1$两次。如果采用网络编码技术，可以先让节点1发送数据包X到节点2，然后节点3发送数据包Y到节点2，在节点2处对数据包X和Y进行"异或"处理，再把处理后的结果$X\oplus Y$进行广播发送，节点1接收到$X\oplus Y$后，通过把$X\oplus Y$和X异或得到Y，同理，节点3也得到X。因此总共只需要3次发送就完成数据包X和Y的传送，从而大大减少了发送次数，提高了网络的吞吐量。

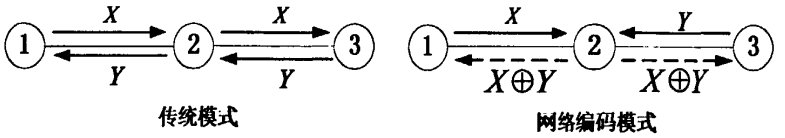


图3-1 网络编码基本原理示意图

3.1.2 网络编码网络模型

在存在网络编码的网络中，由于网络节点的功能发生了变化，因此对网络的描述也需要作相应改变。对一个无线网络进行数学抽象，定义网络中的节点集合为$V=\{v_1,\cdots,v_m\}$，对于任意$v_i\in V$，它的邻居节点为$N(v_i)\subseteq V$。$a_i=\{v_1,v_2,\cdots,v_{|a_i|}\}$表示从源节点$s_i$到目的节点$t_i$的一次通信中路由路径上的节点，其中$|a_i|$表示节点的数目，$v_1=s_i$，$v_{|a_i|}=t_i$。

定义3-1 存在网络编码的无线网络中，为了描述节点之间的网络编码机会，用网络编码基本单元（图3-1所示的对传结构）来定义路径$I(a_i)$，表达式为[10]：

$$I(a_i):=\left\{v_1[\phi,v_2],v_2[v_1,v_3],\cdots,v_{|a_i|-1}\left[v_{|a_i|-2},t_i\right]\right\} \tag{3-1}$$

其中，$v_k[v_{k-1},v_{k+1}]$表示v_k节点从v_{k-1}节点获得数据包，并把数据包传送给v_{k+1}节点（或者v_{k-1}节点要向v_{k+1}节点发送数据包，必须借助v_k节点进行转发），$v_1[\phi,v_2]$表示v_1节点作为源节点向v_2节点传送数据包。

定义3-2 为描述网络的能量消耗，假定每个网络节点$v\in V$能耗为$C_v(a)$，在网络编码的情况下，节点的能耗只与该节点传输次数有关，$C_v(a)$表示为[10]：

$$C_v(a):=\sum_{(v_x,v_y)\in N(v)^2:x>y}\max\left\{\delta\left(a,v\left[v_x,v_y\right]\right),\delta\left(a,v\left[v_y,v_x\right]\right)\right\} \tag{3-2}$$

其中，$\delta\left(a,v\left[v_x,v_y\right]\right)$表示需要把数据从节点$v_x$经由节点$v$传到节点$v_y$的通信的次数，为方便描述，规定从节点$v_x\rightarrow$节点$v\rightarrow$节点$v_y$传输数据的方向为正方向，从节点$v_y\rightarrow$节点$v\rightarrow$节点$v_x$传输数据的方向为反方向，因此，式（3-2）表示路由路径a上的节点v的能耗就是利用该节点进行通信的正方向通信数量和反方向通

信数量中的较大值。

定义 3-3 整个网络的系统能耗就是网络中所有节点能耗的和，表示为[10]：

$$C(a):=\sum_{v\in V}C_v(a) \tag{3-3}$$

3.2基于网络编码的链路博弈

无线网络中链路通信可选择多种路由路径，所有链路的路径选择就构成了不同的路径组合，每种路径组合对应的网络收益（能耗等）不同。在不存在合作的情况下，每条链路都会自私地选择对自己最有益的路径，而网络编码技术的引入为网络链路之间带了“合作双赢”的机会，因此怎样选择路径才能使网络编码机会最大，成为了一个网络链路的决策问题。Marden 等人[10]把此问题看作是一场非合作博弈，建立了链路博弈模型对其进行分析，模型只针对网路编码最简单的对传结构（如图 3-1 所示），认为只要网络中存在这种对传结构，在中间节点处就可以进行网络编码。文献[10]中通过设计合适的目标函数来使链路选择最合适的路由路径，达到在满足路由要求的前提下使系统的能耗最小的目的。

3.2.1 链路博弈模型介绍

链路博弈模型中参与者集合用 $N=\{1,\cdots,n\}$ 表示，参与者 i 代表的是从源节点 s_i 到目的节点 t_i 的一次通信过程。选取每次通信选择的路由路径作为博弈的策略空间 A，$A=\prod A_i$，其中 A_i 表示参与者 i 的所有策略集合（即从源节点 s_i 到目的节点 t_i 的可行路径集合）。

定义 3-4 博弈中参与者的目标是选择合适的路由路径，使得自己完成通信任务的链路能耗最小，因此博弈的效用函数是每个参与者的通信成本（能耗），参与者 i 的效用函数 $J_i(a)$ 可以表示为[10]：

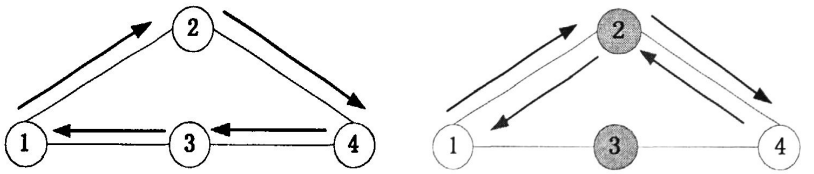
$$J_i(a_i,a_{-i}):=C(a_i,a_{-i})-C(a_i^0,a_{-i}) \tag{3-4}$$

其中，$C(a_i,a_{-i})$ 表示当参与者 i 选择路径 $a_i=\{v_1,v_2,\cdots,v_{|a_i|}\}$，而其他参与者选的路径集合是 a_{-i} 时，路径 a_i 上的链路总能耗；a_i^0 表示参与者 i 自己不发送数据包的情况，也就是说，$C(a_i^0,a_{-i})$ 表示参与者 i 自己不发送数据包时路径 a_i 上的链路能耗（即该路径替其他参与者转发数据的链路能耗）。因此，两者之差表示参与者 i 选择路径 a_i 来完成自己的通信任务时需要付出的链路能耗，即参与者 i 的效用函数。文献[10]中也给出了 $J_i(a)$ 的具体计算方法，即：

$$J_i(a)=N_i^{(>)}(a):=\sum_{v[v_x,v_y]\in I(a_i)}1\left\{\delta\left(a,v\left[v_x,v_y\right]\right)>\delta\left(a,v\left[v_y,v_x\right]\right)\right\} \qquad (3\text{-}5)$$

其中，$1\left\{\delta\left(a,v\left[v_x,v_y\right]\right)>\delta\left(a,v\left[v_y,v_x\right]\right)\right\}$表示对于路径$a$上的任意节点$v$，如果使用$v_x\to v\to v_y$方向（参与者$i$传送数据的方向）传送数据的参与者的数量大于使用$v_y\to v\to v_x$方向传送数据的参与者的数量，则节点$v$的能耗为1，否则为0。

考虑如图3-2所示的网络场景，节点1要向节点4传送数据包，节点4也要向节点1传送数据包，此场景可以看作是一个有两个参与者的非合作博弈。参与者1为节点1到节点4的通信，参与者2为节点4到节点1的通信。每个参与者均有两种策略，均可以选择底部的通信路径（经过节点1、3、4的路径，用B表示该策略），也可以选择顶部的通信路径（经过节点1、2、4的路径，用T表示该策略），因此有4种可能的策略组合。



(a) 策略集合 (T,B)　　(b) 策略集合 (T,T)

图3-2 链路博弈网络场景一

根据式（3-4）设计的效用函数和系统能耗函数式（3-3）能得到如图3-3所示的博弈支付矩阵。由（a）知，(B,B)和(T,T)为博弈的两个纳什均衡解，在（b）中这两种策略组合分别对应的系统消耗也是最小的。可以发现，(B,B)和(T,T)路径组合中均有可以进行网络编码的节点（分别为节点3、2），也就是说根据式(3-4)设计的效用函数，参与者选择合适的通信路径使自己的通信成本最小，同时这样的路径组合也能使网络中网络编码的机会最大，从而降低网络的系统能耗。

参与者2

参与者1	B	T
B	1,1	2,2
T	2,2	1,1

(a)参与者的能耗矩阵

参与者2

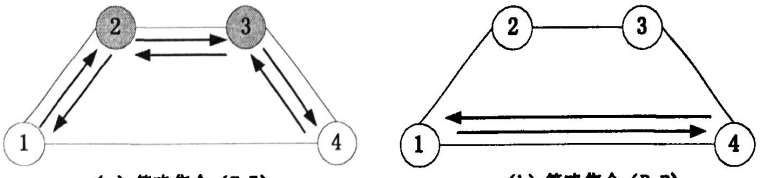
参与者1	B	T
B	2	4
T	4	2

(b)系统的能耗矩阵

图3-3 场景一的博弈支付矩阵

文献[10]中证明了根据式（3-4）设计的效用函数该博弈最终能达到纳什均衡，而且纳什均衡解并不唯一。显然，纳什均衡解集的策略一定是使每个参与者自身链路能耗最小的路径组合，但是这样的策略对应的系统总能耗并不一定都是最优的，也就是说在存在利益冲突的情况下，利己主义个人理性选择的结果在总体上并不一定是最好的。如图3-4所示的网络场景，与场景一类似，节点1要向节点4

传送数据包，节点 4 也要向节点 1 传送数据包，每个参与者也可以选择底部（B）或者顶部（T）两种通信策略。



（a）策略集合（T,T）　　（b）策略集合（B,B）

图 3-4 链路博弈网络场景二

博弈支付矩阵如图 3-5 所示。由（a）知，(B,B)和(T,T)为博弈的两个纳什均衡解，但在（b）中(B,B)对应的系统能耗较之(T,T)对应的系统能耗大，这也说明纳什均衡解对应的系统能耗并不全是最优的。文献[10]中分析了造成这种结果的原因是效用函数式（3-4）的设计仅仅考虑了怎样提高网络编码机会，并没考虑路径长短的因素。

参与者2

参与者1	B	T
B	1,1	1,3
T	3,1	1,1

(a)参与者的能耗矩阵

参与者2

参与者1	B	T
B	3	4
T	4	2

(b)系统的能耗矩阵

图 3-5 场景二的博弈支付矩阵

定义 3-5　对目标函数式（3-4）进行改进，加入路径因素，改进后参与者的效用函数为[10]：

$$J_i(a_i,a_{-i}) := \phi(a_i,a_{-i}) - \phi(a_i^0,a_{-i}) \tag{3-6}$$

其中，$\phi(a)=(\partial-1)C(a)+\sum_{i\in V}|I(a_i)|$，显然，改进后的效用函数除了考虑链路上节点的能耗以外，还考虑了该链路的路径长短，两种因素的影响程度通过参数∂来调整，因此式（3-6）可以表示为[10]：

$$J_i(a_i,a_{-i}) := |I(a_i)| + (\partial-1)\left(C(a_i,a_{-i}) - C(a_i^0,a_{-i})\right) \tag{3-7}$$

文献[10]中也给出了改进后参与者效用函数的具体计算方法，即：

$$J_i(a) = \partial N_i^{(>)}(a) + N_i^{(<)}(a) + N_i^{(=)}(a) \tag{3-8}$$

其中，

$$N_i^{(=)}(a) := \sum_{v[v_x,v_y]\in I(a_i)} 1\left\{\delta\left(a,v[v_x,v_y]\right) = \delta\left(a,v[v_y,v_x]\right)\right\} \tag{3-9}$$

$$N_i^{(<)}(a) \coloneqq \sum_{v[v_x,v_y] \in I(a_i)} 1\left\{\delta\left(a, v\left[v_x, v_y\right]\right) < \delta\left(a, v\left[v_y, v_x\right]\right)\right\} \tag{3-10}$$

文献[10]中也证明了改进效用函数以后博弈最终能达到纳什均衡，而且纳斯均衡解对应的系统总能耗较之前更优。

3.2.2 链路博弈存在的问题

链路博弈中，任意参与者i通过决策最后选择了路径$I(a_i)$，是基于该参与者认为路径$I(a_i)$对他本身来说通信成本最小，而且路径$I(a_i)$上的所有节点都会无条件地协作来完成此次通信任务。这就会存在很多参与者最后选择同一条路由路径的情况，导致网络的资源分配不均衡，所有流量都集中在某些节点或者路径上，一方面使这些链路出现过载、拥塞现象，另一方面加重了某些节点的负担， 使其因为过度耗损自身能量而过早消亡。

事实上，链路上节点的转发能耗通常远远大于路由能耗，为了节省自身资源，链路中的节点不会像参与者预料的那样，无条件协作，中间节点可能会拒绝为它人提供转发服务的请求，中间节点的这种自私行为将导致链路博弈选择的最优路径并不能完成通信任务。

考虑如图3-6所示的网络场景，网络拓扑包括8个网络节点，博弈有4个参与者，参与者1是源节点1到目的节点4的通信，可以选择的策略$A_1=\{a_1,a_1'\}$；参与者2是源节点4到目的节点1的通信，可以选择的策略$A_2=\{a_2,a_2'\}$；参与者3是源节点7到目的节点8的通信，可以选择的策略$A_3=\{a_3\}$；参与者4是源节点8到目的节点7的通信，可以选择的策略$A_4=\{a_4\}$。

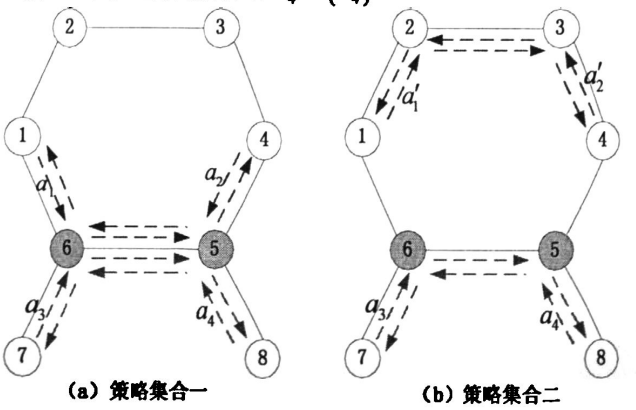
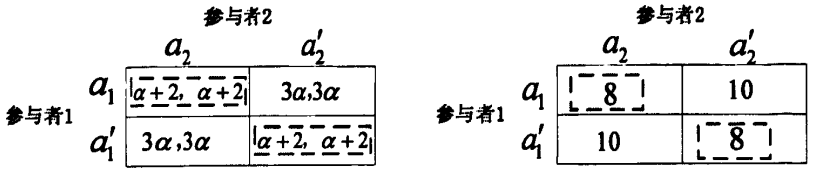


图3-6路由博弈网络场景三

参与者3和参与者4均只有一种策略，因此博弈的结果由参与者1和参与者2的策略来决定，按照效用函数式（3-7）和系统能耗函数式（3-3）可以得到如图3-7所示的支付矩阵。



(a)参与者的消耗矩阵　　(b)系统的消耗矩阵

图 3-7 网络场景三的博弈支付矩阵

其中，$\alpha \le 1$，由（a）知，(a_1,a_2)和(a_1',a_2')为博弈的两个纳什均衡解，这两种策略组合在（b）中对应的系统消耗也是最小的。因此，博弈的结果只能是这两种策略组合中的一种。表 3-1 为这两种策略组合下节点和系统的能耗。

表 3-1 纳什均衡策略集合下节点和系统的能耗对照

策略集合	节点 2	节点 3	节点 5	节点 6	系统
(a_1,a_2)	2	2	0	0	8
(a_1',a_2')	1	1	1	1	6

由表 3-1 可知，如果参与者最后选择的策略是(a_1,a_2)，那么完成 4 个参与者的通信任务对于节点 2 和节点 3 来说需要的能耗是 2，而节点 5 和节点 6 却是 0 损耗。考虑节点的自私性，节点 2 和节点 3 为了节省自身的能量，并不愿意转发所有的数据包，可能会丢弃部分数据包，从而影响整个网络的通信。如果参与者最后选择的策略是(a_1',a_2')，那么每个节点需要的能耗是 1，这样每个节点的负担均衡，节点不合作的概率变小。

由上述分析可知，链路博弈虽然可以找到合适的路径使系统的能耗变小，但是考虑到链路中间节点的自私行为，通过链路博弈选出来的路径并不一定能完成通信任务，也就是说路径上的中间节点不一定愿意合作来转发数据包。因此在链路博弈的基础上，分析链路上中间节点的协作性显得尤为重要。下面将对链路中间节点进行重复博弈建模来分析中间节点的自私行为，希望能在链路博弈得到的纳什均衡解集中再挑选出最优的解（最可能完成通信任务的路径）。

3.3基于网络编码的链路节点自私行为分析

对整个无线网络来说，节点与节点之间的通信并不是一次性的，由于网络系统的动态性，因此节点当前的决策结果可能会影响后续的行为选择，因此可以把通信过程中链路上中间节点之间是否合作的问题看作一个重复的博弈过程。假设网络中的节点都是理性的，即只要其符合节点的要求(指定的优化目标)，节点就会合作，而且链路中数据包丢失的主要原因是节点拒绝转发。这里只考虑最简单的

网络编码对传模型（如图 3-1 所示），假设整个系统时间由一系列离散的协作时隙t构成，在任意时隙中，每一中间节点只要符合对传结构，均有进行网络编码的机会，且同一时隙中路由状态不会发生改变，单一时隙长度足以保证每一数据包均能抵达目的节点。

3.3.1 博弈建模

无线网络中链路表示为$I(a)=\{s,v_1,v_2,\cdots,v_L,t\}$，$s$为源节点，$t$为目的节点，$L$为中间节点的个数。选取$I(a)$上所有的中间节点为博弈参与者，参与者的集合用$N=\{1,\cdots,n\}$表示。为了描述节点之间的协作性，选取节点的包转发概率p作为博弈的策略集合。

定义 3-6 节点i在时隙t内以$p_{i(t)}$的概率转发数据包，$p_i(t)\in[0,1]$，$p_{i(t)}=0$表示节点拒绝转发，$p_{i(t)}=1$表示节点完全协作。路径$I(a)=\{s,v_1,v_2,\cdots,v_L,t\}$上，所有中间节点$i$在时隙$t$内的策略集合为$S_{i(t)}$，即$S_{i(t)}=\left(p_{1(t)},p_{2(t)},\cdots,p_{i(t)}\right)$。则数据包在时隙$t$内到达中间节点$i$的概率是：

$$p_{i(t)}\left(S_{i(t)}\right)=\prod_{k=1}^{L_k}p_{k(t)} \tag{3-11}$$

其中，$k\in I(a)=\{s,v_1,v_2,\cdots,v_{i-1}\}$，$L_k$为到达节点$i$的跳数。

定义 3-7 $R(i)$为包含中间节点i的路由集合，则网络中所有$I(a)$上的数据包在时隙t内到达中间节点i的代价是：

$$\eta_{i(t)}\left(S_{i(t)}\right)=\sum_{I(a)\in R(i)}C_a p_{i(t)}\left(S_{i(t)}\right) \tag{3-12}$$

其中，C_a为节点i转发数据包的代价，存在网络编码的情况下，节点的转发代价只与节点的传输次数有关，或者说只与利用此节点转发数据的“流”（这里的“流”指的是源节点到目的节点的通信过程）的数量有关。

定义 3-8 网络中的节点可以发送、接收或转发数据包，我们用(S,D,F)的三元二值布尔变量表示节点的行为[21]，变量取值为 0 或 1。这里，用S代表节点i发送数据包的情况；D代表节点i接收数据包的情况；F代表节点i转发数据包的情况。因为节点i在同一时隙不能同时发送或接收数据包，所以S与D的取值总是不同。因此，节点i在时隙t内的效用函数可以表示为 [9]：

$$U_{i(t)}\left(S_{i(t)}\right)=S\cdot\sum_{(i,j)\in N}B_{ij}s_{i(t)}\left(p\left(S_{i(t)}\right)\right)+D\cdot\sum_{(s,i)\in N}B_{si}d_{i(t)}\left(p\left(S_{i(t)}\right)\right)-F\cdot\eta_{i(t)}\left(S_{i(t)}\right) \tag{3-13}$$

其中，B_{it}是源节点i为自己发送数据的效用，B_{si}是目的节点i接收数据的效用，等式右边前两项为节点i发送或接收数据的收益。$s_{i(t)}\left(p\left(S_{i(t)}\right)\right)$和$d_{i(t)}\left(p\left(S_{i(t)}\right)\right)$分别表示节点$i$在时隙$t$内发送和接收数据包的效用函数[21]（正的、非递减凹函数，定义为某种物理上有意义的实值函数。凹型效用函数代表了经济学中的边际效用）。$p\left(S_{i(t)}\right)$为$S_{i(t)}=\left(p_{1(t)},p_{2(t)},\cdots,p_{i(t)}\right)$的多项式。

3.3.2 纳什均衡解

结论 3-1 对于路由路径$I(a)$上的任意节点i，当其在时隙t选择拒绝转发数据包（$p_{i(t)}=0$）时，会导致该路由路径上的所有节点均会采取拒绝转发的策略。

时隙t内，在路径$I(a)=\{s,v_1,v_2,\cdots,v_L,t\}$上，所有中间节点$i$不能同时发送或接收数据包，我们取$(S,D,F)=(0,1,1)$，由式（3-13）可得节点$i$的效用函数：

$$\begin{aligned}U_{i(t)}\left(S_{i(t)}\right)&=D\cdot\sum_{(s,i)\in N}B_{si}d_{i(t)}\left(p\left(S_{i(t)}\right)\right)-F\cdot\eta_{i(t)}\left(S_{i(t)}\right)\\&=\sum_{(s,i)\in N}B_{si}d_{i(t)}\left(p\left(S_{i(t)}\right)\right)-\sum_{I(a)\in R(i)}C_a\prod_{k=1}^{L_a}p_{k(t)}\end{aligned}\tag{3-14}$$

路径$I(a)$上的所有中间节点都是理性的，它们会调整自己的包转发概率来实现自身效用的最大化，即中间节点i在时隙t内的目标是选择策略$S_{i(t)}$来最大化效用函数$U_{i(t)}\left(S_{i(t)}\right)$。假设在时隙$t$内$S_{i(t)}=\left(p_{i(t)},p_{-i(t)}\right)$，即节点$i$选择的策略是以$p_{i(t)}$转发数据包，除节点$i$以外的其他中间节点的包转发概率表示为$p_{-i(t)}=\left(p_{1(t)},\cdots,p_{(i-1)(t)}\right)$，根据纳什均衡的定义，当网络达到纳什均衡时一定满足：

$$U_{i(t)}\left(p^*_{i(t)},p^*_{-i(t)}\right)=\max U_{i(t)}\left(p_{i(t)},p_{-i(t)}\right)\tag{3-15}$$

因为效用函数式（3-14）右边的第一项大于 0，对于任意节点i，当其选择拒绝转发（$p_{i(t)}=0$）时，$U_{i(t)}\left(S_{i(t)}\right)$能达到最大值，因此$I(a)$上的其他所有中间节点均会采取拒绝转发的策略，以达到自身效用的最大化，此时（$p_{1(t)}=p_{2(t)}=\cdots=p_{i(t)}=0$）。我们可以发现，所有节点都“永不合作”总是一种纳什均衡，而当网络中所有节点处于这种纳什均衡状态，互不协作时，网络即将瘫痪。文献[9，21]中考虑了不存在网络编码时重复博弈模型其他情况的纳什均衡，并证明其他情况下，$p^*=0$仍然可以使$U_{i(t)}\left(S_{i(t)}\right)$达到局部最优，也就是说其他纳什均衡下，节点也会拒绝协作，拒绝转发数据包，从而导致不理想的稳定状态，这个结论同样适合存在网络编码的网络。

3.3.3 影响节点自私的因素

由前面分析可知，链路上的节点可能完全协作，也可能拒绝转发，那么节点何时会协作何时不协作呢？下面来分析一下影响节点包转发概率的因素。

结论 3-2 当路由路径的跳数 L 固定时，节点的包转发概率 p 随转发代价 C 的增加而降低，也就是说当需要付出的转发代价越大时，节点选择转发的可能性越小，以此来保存自身的能量，当转发代价高到一定程度时，节点就会拒绝转发，处于完全不合作的状态。影射到现实生活中，当人们见义勇为、做好人好事的代价很高时，就会使人畏首畏尾、明哲保身，没有人为了公众利益，挺身而出。

为简化模型，考虑任意路径 $I(a)$，假设该路径含有 n 个中间节点，所有中间节点在时隙 t 内有相同的转发策略，即 $S_{i(t)}=\left(p_{i(t)},p_{i(t)},\cdots,p_{i(t)}\right)$。如果节点 i 是路由 $I(a)$ 上源节点的第 $n+1$ 跳节点，则数据包在时隙 t 内到达中间节点 i 的概率为：

$$p_{i(t)}\left(S_{i(t)}\right)=p_{i(t)}^{n} \tag{3-16}$$

假设 $c(n)$ 为节点 i 转发数据包的代价（c 只和通过此节点进行转发的“流”的数量有关，假设对所有节点均相同），$b(n)$ 为节点 i 接收源节点 s 发送的数据包的收益，在时隙 t 内节点 i 的效用函数可简化为：

$$U_{i(t)}\left(S_{i(t)}\right)=\sum_{n=0}^{\infty}b(n)d_{i(t)}\left(p\left(S_{i(t)}\right)\right)-\sum_{n=0}^{\infty}c(n)p_{i(t)}^{n} \tag{3-17}$$

L 为源节点到目的节点的跳数，则 $n+1=1,2,\cdots,L-1$，为了简化分析，我们假设对于任一节点 i，$b(n)=1,c(n)=c$，在时隙 t 内节点 i 的效用函数简化为：

$$U(p)=d\left(p(p)\right)-\sum_{n=1}^{L-2}cp^{n} \tag{3-18}$$

其中，$p(p)=p^{L-1}$，上式对 p 求偏导可得：

$$U'(p)=d'\left(p(p)\right)(L-1)p^{L-2}-\sum_{n=1}^{L-2}cnp^{n-1} \tag{3-19}$$

当选用的效用函数为 $d(x)=\ln(100x+1)$[21]时，可得：

$$U'(p)=\frac{100(L-1)p^{L-2}}{100p^{L-1}+1}-\sum_{n=1}^{L-2}cnp^{n-1} \tag{3-20}$$

跳数 L 为固定值，因为节点的目标是选取 p 来最大化 $U(p)$，则令 $U'(p)=0$，可以看出 $p=0$ 是一个局部最大值，当 $p\neq 0$ 时，p 随 c 的增加而减小。

在存在网络编码的情况下，节点的转发代价只和通过此节点进行转发的“流”

的数量有关，经过节点的“流”越多，节点不协作的概率越大。因此，仅仅考虑链路消耗来进行链路博弈，用得到的纳什均衡解来决定路由路径，可能会导致经过某些节点的“流”很多，而另外一些节点处于空闲状态，从而使负荷大的节点拒绝协作，出现数据包丢失的情况，影响网络的整体性能。为了能在链路博弈的纳什均衡解集中挑选使网络流量均衡的解（路由路径），需要再加入激励机制。

3.3.4 解决方法

这里考虑网络编码技术和现有报价机制的结合，来解决链路博弈中链路节点自私的问题。由于无线网络数据传输的特性，价格信息的传递和其真实性的保证等是需要解决的关键问题，而网络编码由于数据是编码后传输的，本身就具有安全性的特质，可以自然地保证数据和报价信息的保密性。

首先需要确定的是从源节点到目的节点的路由集合，这里我们采用文献[10]中提出的链路博弈，链路博弈的结果是一组综合考虑了编码机会和路径长短因素的纳什均衡解集（路径集合），为了在这些路径集合中选出最优（使网络流量均衡或者资源分配均衡的）路径，引入拍卖机制，让每条路径的中间节点报价，从而得到每条路径的传输价格，需要传输数据的节点通过比较各条路径的出价后，选择价格合理的路径进行传输。

这里需要解决的关键问题是每条路径上的中间节点的报价问题。基于我们的初衷是希望网络的流量或者是资源分配均衡，避免造成某些节点负担过重或者某些链路出现过载、拥塞现象，因此这里利用市场模型来解决报价问题，让供求关系来决定价格。

由结论 3-2 可知，节点的包转发概率随转发代价的增加而降低，在网络编码的情况下，节点的转发代价只和通过此节点进行转发的“流”的数量有关，也就是说经过节点的“流”越多，节点不协作的概率越大。因此，中间节点的价格由经过该节点的“流”的数量决定，这也就是经典的多买家和多卖家的模型。具体来说，就是经过节点的“流”的数量越多，该节点越忙碌，处于“供不应求”的状态，该节点的报价就越高；经过节点的“流”的数量较少时，该节点处于空闲状态，该节点的报价就越低。

3.4仿真实验

本文运用 Matlab 仿真工作进行仿真实验。实验采用了如图 3-8 所示的正八边形网络拓扑。网络拓扑由 9 个网络节点组成，存在八条“数据流”，分别为源节点

1 到目的节点 5 的通信、源节点 5 到目的节点 1 的通信、源节点 2 到目的节点 6 的通信、源节点 6 到目的节点 2 的通信、源节点 3 到目的节点 7 的通信、源节点 7 到目的节点 3 的通信、源节点 4 到目的节点 8 的通信、源节点 8 到目的节点 4 的通信。

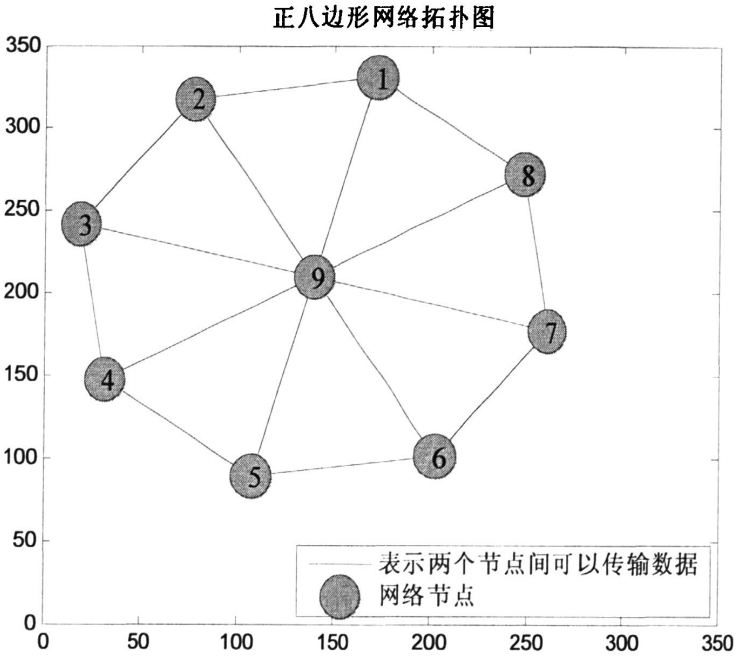


图 3-8 正八边形网络拓扑

按照文献[10]中的链路博弈模型，把八条“数据流”分别作为博弈的八个参与者，按照式（3-7）设计的目标函数让参与者选择路径，最后得到的博弈纳什均衡解集中包括四种策略组合，分别如图 3-9、3-10、3-11、3-12 所示。引入报价机制后，得到的最终结果是图 3-10 所示的策略二的路径集合。

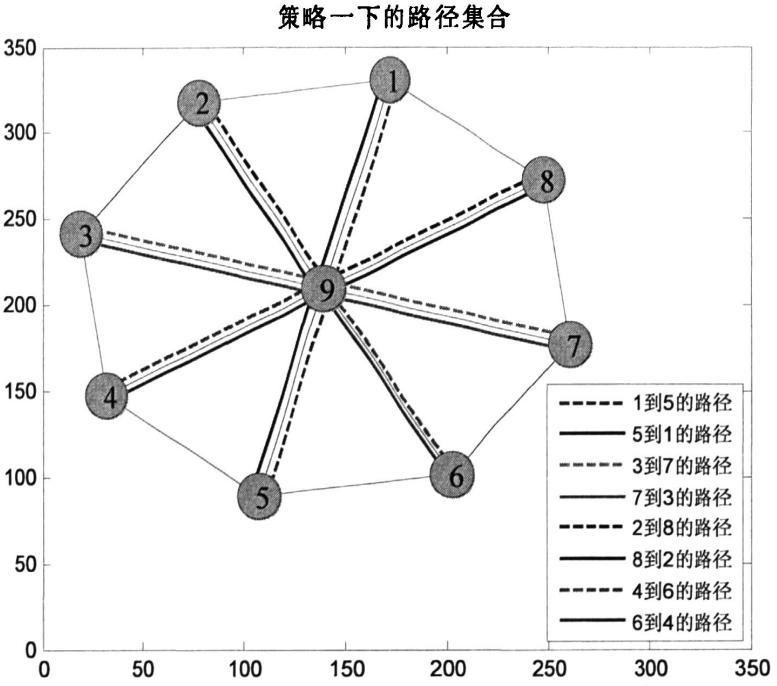


图 3-9 纳什均衡解一对应的路径组合

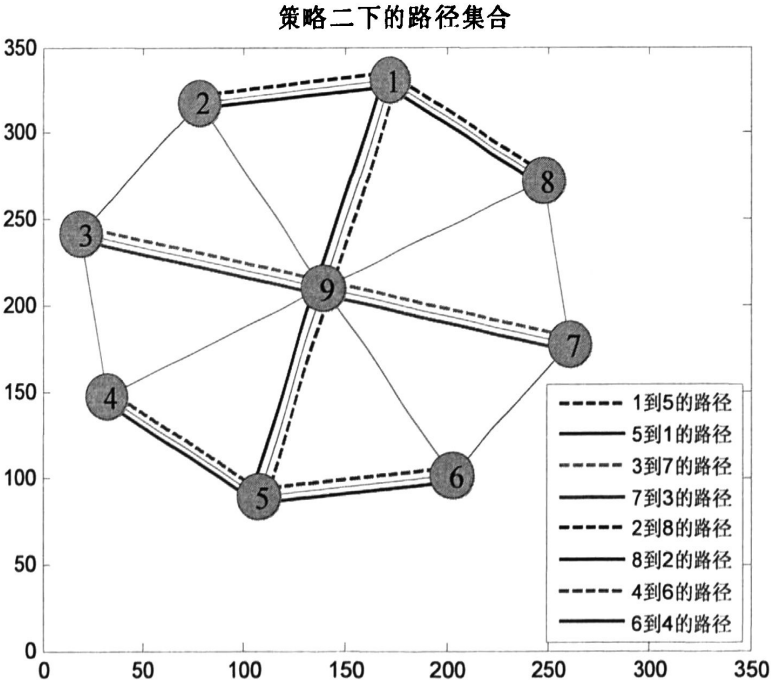


图 3-10 纳什均衡解二对应的路径组合

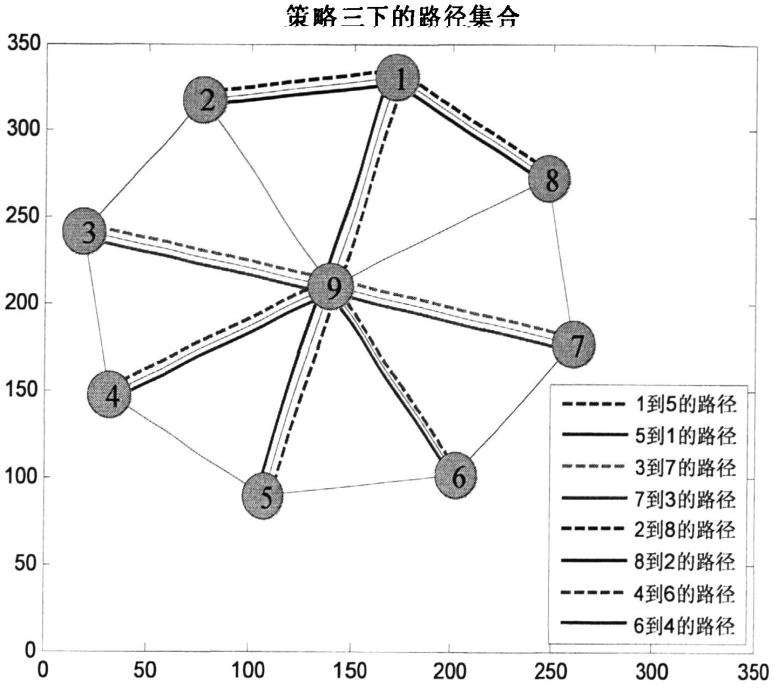


图 3- 11 纳什均衡解三对应的路径组合

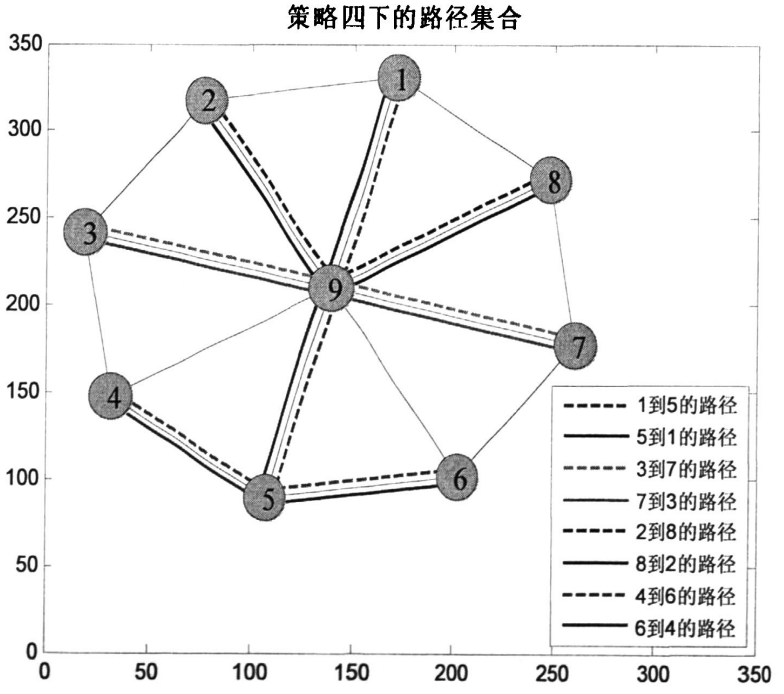


图 3- 12 纳什均衡解四对应的路径组合

这四种路径策略集合下的系统能耗一致，各节点的能耗分布如图 3-13 所示。

由图可知对于策略一的路径集合，节点 2 和节点 6 处于闲置状态，节点 9 的能耗非常大；策略三和策略四的路径集合中，节点 6 和节点 2 分别处于闲置状态，节点 9 的能耗比较大；策略二的路径集合中，各节点的能耗基本均衡，没有闲置节点，也没有负担过大的节点，从而实现了网络资源的均衡分配。

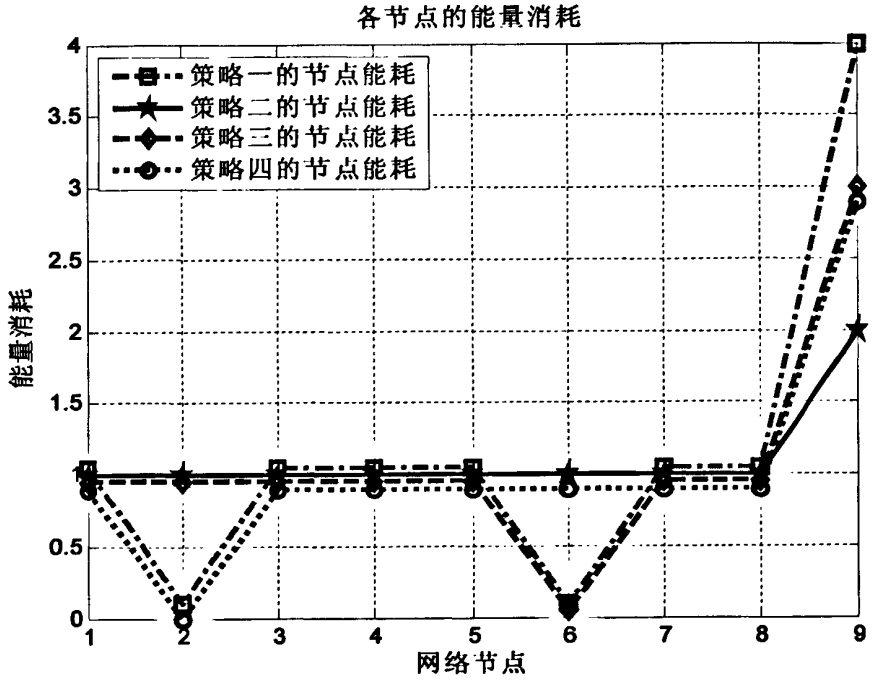


图 3- 13 四种路径策略集合下的节点能耗分布

3.5本章小结

本章首先介绍了网络编码技术的基本原理，描述了存在网络编码下的网络模型，并介绍了 Marden 等人提出的链路博弈；然后分析了链路博弈由于没有考虑链路上中间节点的自私行为而导致的流量分配不均衡问题；再次，通过建立链路中间节点的重复博弈模型，分析得出影响节点自私的因素；最后提出了链路博弈和报价机制相结合的解决方案，解决流量分配不均衡的问题，并给出了仿真实验。

4 基于窃听信道的节点恶意行为分析

无线信道的开放性使得无线网络中的节点更容易实施窃听和干扰等恶意行为。为了防止节点的恶意行为，实现无条件保密通信，根据信息理论安全原理，Wyner 等人[22]提出了最基本的第一类窃听信道模型。后来随着 MIMO 技术的日趋成熟，研究者们在第一类窃听信道模型的节点处加入了多天线技术，以提高信道的容量和可靠性，从而出现了 MIMO 窃听信道模型。

尽管研究者们针对窃听信道做了大量研究，但是这些研究都是针对恶意节点的窃听行为，在实际的无线网络中，恶意节点除了窃听行为还可以选择干扰接收者等其他恶意行为。另外，加入了多天线技术以后，窃听模型中的发送者既可以只执行发送任务，也可以选择利用部分天线对窃听者进行人工加扰，来保证通信安全。因为窃听模型中节点的行为决策是相互影响的，比如发送者对恶意节点人工加扰时，恶意节点选择窃听行为就是徒劳，此时选择干扰行为更好；而发送者对恶意节点人工加扰虽然可以防止窃听行为，但是对恶意节点的干扰行为作用却适得其反。因此，在节点相互都不知道对方行为选择决策的情况下，节点将怎样选择自己的策略达到自身目的可以看作一场博弈游戏。

文献[16]针对上述问题建立了 MIMO 窃听信道博弈模型，提供了一种分析窃听信道的新思路。但文献[16]中仅仅研究了在 Eve 和 Alice 行为相互影响时，两者该如何决策的问题，事实上，Eve 的自身因素如位置等也将影响其决策。且文献[16]中并没有考虑模型中存在中继节点的情况。本章将在此基础上研究节点位置、天线数量以及发射功率等因素对博弈结果以及系统保密率影响，并将在此基础上扩展模型，研究存在中继节点时中继窃听信道的保密率问题。

4.1 预备知识

4.1.1 第一类窃听信道

根据信息理论安全原理，无条件安全通信系统最基本的模型是 Wyner 等人[22]提出的第一类窃听信道模型。如图 4-1 所示，第一类窃听信道模型中包括三个网络节点，即发送者 Alice、接收者 Bob 和窃听者 Eve。两个合法的通信者 Alice 和 Bob 通过一条主信道进行通信，而窃听者 Eve 试图通过窃听信道窃取 Alice 和 Bob 之间的通信信息。窃听信道理论证明了存在合适的编码/解码方案使得信息在信道上传

输时具有良好的健壮性(差错概率小)，同时也能保证一定的信息安全性。

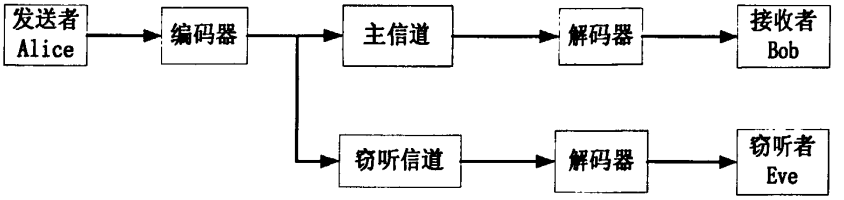


图 4- 1 第一类窃听信道示意图

为了描述窃听信道的特性，我们引入几个定义。假设 Alice 发送信息w^k，编码后得到x^n，合法接收者 Bob 与窃听者 Eve 分别收到的信息为y^n和z^n。

定义 4-1 模糊率R_e反映的是 Eve 受到的信息w^k与正确信息z^n相比，信息损失的程度，表示为[23]：

$$R_e = \frac{1}{n} h\left(w^k \mid z^n\right) \tag{4-1}$$

其中，$h(*)$为熵函数，$0 \le R_e \le h\left(w^k\right)/n$。如果$R_e = h\left(w^k\right)/n$，则$I\left(z^n, w^k\right) = 0$，即$z^n$与$w^k$的互信息为 0，即实现了完美通信。

定义 4-2 这里我们给出保密率的概念。对于任意$\varepsilon, \varepsilon' > 0$，存在一种编码方式$(n,k)$，$n$为码组长度，$k$为信息位长度，对于任意$n \ge n\left(\varepsilon, \varepsilon'\right)$，有[23]：

$$P_e \le \varepsilon' \tag{4-2}$$

$$R_s - \varepsilon \le R_e \tag{4-3}$$

其中，P_e为解码的错误概率，代表信息传输的可靠性，R_s为保密率，用来表示发送者能够安全传送数据到合法接听者的速率，

定义 4-3[23] 系统的秘密容量C_s是保密率的最大值，它是窃听信道中的一个重要概念，学者们希望通过研究窃听信道找到提高系统秘密容量的方法。

第一类窃听信道建立以后，研究者们在此基础上发展出了多种类型的窃听信道模型。近年来， MIMO 技术被证明不仅可以提高信道的容量，还可以提高信道的可靠性，降低误码率，因此，研究者们逐渐把 MIMO 技术应用到窃听信道中，形成了 MIMO 窃听信道。

4.1.2 MIMO 窃听信道

当图 4-1 中的 Alice，Bob 和 Eve 分别拥有N_a、N_b、N_e根天线时，窃听信道模型就可用 MIMO 窃听信道描述，如图 4-2 所示。

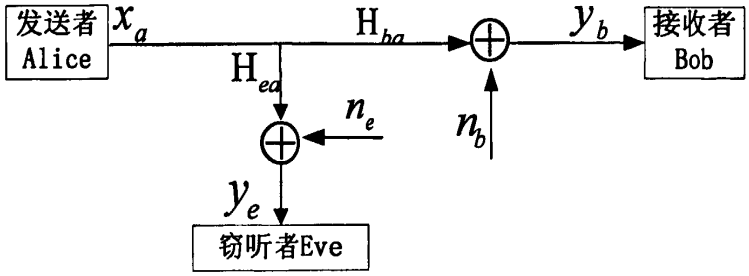


图 4-2MIMO 窃听信道示意图

图 4-2 中，Bob 和 Eve 收到的信息可以表示为：

$$y_b = \mathrm{H}_{ba} x_a + n_b \tag{4-4}$$

$$y_e = \mathrm{H}_{ea} x_a + n_e \tag{4-5}$$

其中，x_a 为 $N_a \times 1$ 维向量，其协方差矩阵 $\mathbf{Q}_a$ 满足 $\varepsilon\{x_a x_a^H\} = \mathbf{Q}_a, \mathrm{Tr}(\mathbf{Q}_a) \le P_a$，$\mathrm{Tr}(\mathbf{Q}_a)$ 为 $\mathbf{Q}_a$ 的迹，P_a 是 Alice 的发送功率。n_b, n_e 分别为 Bob 和 Eve 接收到的信道中的噪声，$\mathrm{H}_{ba}, \mathrm{H}_{be}$ 分别为 $N_b \times N_a$，$N_b \times N_e$ 的信道矩阵。

定义 4-4[23] 在 MIMO 信道中，由于信道矩阵是随机的，故容量也是随机的，因此对其求解时必须用数学统计量，于是引入了遍历信道容量的概念。MIMO 遍历信道容量定义为：$C = E_H\{\max I(X;Y)\}$，$E_H\{*\}$ 是对信道矩阵 H 取数学期望。

图 4-2 中 MIMO 窃听信道的遍历秘密容量 C_s 为[23]：

$$\begin{aligned} C_s &= E_H\left\{\max_{\mathbf{Q}_a \ge 0} I(\mathbf{X}_a;\mathbf{Y}_b) - I(\mathbf{X}_a;\mathbf{Y}_e)\right\} \\ &= E_H\left\{\max_{\mathbf{Q}_a \ge 0}\left[\log\det\left(\mathbf{I} + \mathrm{H}_{ba}\mathbf{Q}_a\mathrm{H}_{ba}^H\right) - \log\det\left(\mathbf{I} + \mathrm{H}_{ea}\mathbf{Q}_a\mathrm{H}_{ea}^H\right)\right]\right\} \end{aligned} \tag{4-6}$$

其中，$\mathbf{X}_a, \mathbf{Y}_b, \mathbf{Y}_e$ 为 x_a, y_b, y_e 的随机值。$\det[A]$ 为矩阵 A 的行列式，H^H 为矩阵 H 的共轭转置矩阵。

图 4-2 中 MIMO 窃听信道的边遍历保密率 R_s 为[23]：

$$R_s = E_H\left\{\max_{\mathbf{Q}_a \ge 0}\left[\log\det\left(\mathbf{I} + \mathrm{H}_{ba}\mathbf{Q}_a\mathrm{H}_{ba}^H\right) - \log\det\left(\mathbf{I} + \mathrm{H}_{ea}\mathbf{Q}_a\mathrm{H}_{ea}^H\right)\right]\right\} \tag{4-7}$$

下面将给出 MIMO 遍历保密率的另一种计算方法及相关结论。

定义 4-5 在 MIMO 窃听信道中，发送方发送信号给合法接收者时，假设信道矩阵用 $N \times L$ 的 $\mathbf{X}$ 表示，其元素均独立服从循环对称复高斯分布 $CN(0,1)$，信噪比 SNR 为 ∂。当接收者接收的信号中不存在干扰信号，而且在发射端天线采用功率平均分配方式时，遍历的 MIMO 保密率可以表示为[24]：

$$R=E\left\{\log\left|\mathbf{I}+\frac{\partial}{L}\mathbf{X}\mathbf{X}^{H}\right|\right\} \tag{4-8}$$

用λ表示沃什矩阵$\frac{1}{L}\mathbf{X}\mathbf{X}^{H}$的特征值，则遍历的MIMO保密率可以表示为[24]：

$$R=\min(N,L)\varepsilon_{\lambda}\left\{\log(1+\partial\lambda)\right\} \tag{4-9}$$

如果式（4-8）中沃什矩阵$\frac{1}{L}\mathbf{X}\mathbf{X}^{H}$的特征值服从以下分布[24]：

$$p(\lambda_a)=\begin{cases}\dfrac{1}{\pi}\sqrt{\dfrac{\beta}{\lambda_a}-\dfrac{1}{4}\left(1+\dfrac{\beta-1}{\lambda_a}\right)^2} & \left(\sqrt{\beta}-1\right)^2\le\lambda_a\le\left(\sqrt{\beta}+1\right)^2\\ 0 & other\end{cases} \tag{4-10}$$

其中，$\beta=N/L$。则当发送端天线采用功率平均分配方式时，遍历MIMO保密率满足[25,26]：

$$R=\min(N,L)\varepsilon_{\lambda_a}\left\{\log(1+\partial\lambda_a)\right\}=N\cdot F(\beta,\partial) \tag{4-11}$$

其中，

$$\begin{aligned}F(\beta,\partial)=&\log\left(1+\partial\left(\sqrt{\beta}+1\right)^2\right)+(\beta+1)\log\left(\frac{1+\sqrt{1-a}}{2}\right)\\&-\log(\mathrm{e})\sqrt{\beta}\frac{1-\sqrt{1-a}}{1+\sqrt{1-a}}+(\beta-1)\log\left(\frac{1+\gamma}{\gamma+\sqrt{1-a}}\right)\end{aligned} \tag{4-12}$$

$$a=\frac{4\partial\sqrt{\beta}}{1+\partial\left(\sqrt{\beta}+1\right)^2}\qquad\gamma=\frac{\sqrt{\beta}-1}{\sqrt{\beta}+1} \tag{4-13}$$

4.2基于MIMO窃听信道的博弈模型

在对图4-2所示MIMO窃听信道模型的大部分研究中，Eve仅被当成窃听者对待，而实际无线网络中，如果Eve和Alice之间的信道质量很差，Eve并不能很好地实施窃听行为，此时Eve会选择干扰Bob来破坏Alice和Bob之间的通信。不仅节点Eve可以选择多种行为，发送端的多天线特性让节点Alice也可以选择多种行为。在不知道窃听信道状态信息的情况下，Alice可以选择全功率传送数据给Bob，也可以选择利用部分功率传送数据给Bob而另外部分功率对Eve进行人工加

扰，因为人工加扰可以降低窃听信道信噪比，加强合法通信的安全。因此，在考虑 Eve 和 Alice 有多种行为选择的情况下，A．Mukherjee 等人[16]提出了一种基于 MIMO 窃听信道的博弈模型来分析 Eve 和 Alice 的行为决策问题。

4.2.1 博弈系统模型

在考虑 Eve 和 Alice 有多种行为选择的情况下，MIMO 窃听信道模型如图 4-3 所示。Alice，Bob 和 Eve 分别拥有 N_a、N_b、N_e根天线。Alice 可以选择全功率传送数据给 Bob，也可以选择利用部分功率对 Eve 进行人工加扰。攻击者 Eve 既可以窃听 Alice 和 Bob 之间的通信信息，也可以发送干扰信号干扰 Bob。

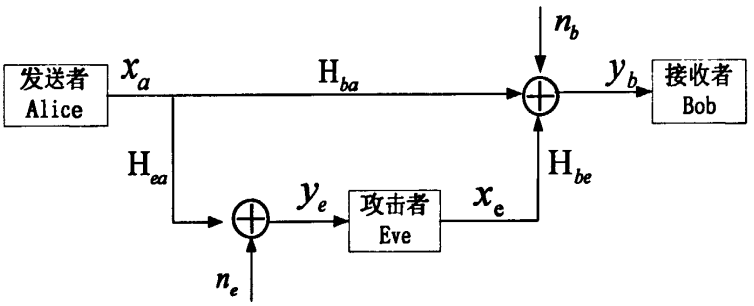


图 4-3 博弈系统模型

在 Eve 干扰 Bob 的情况下，Bob 收到的信息 y_b 可以表示为：

$$y_b = \mathrm{H}_{ba}x_a + \sqrt{g_2}\mathrm{H}_{be}x_e + n_b \tag{4-14}$$

在 Eve 窃听 Alice 的情况下，Eve 收到的信息 y_e 可以表示为：

$$y_e = \sqrt{g_1}\mathrm{H}_{ea}x_a + n_e \tag{4-15}$$

其中，x_a为发送方 Alice 的发送信号，x_e为窃听者 Eve 发送的干扰信号，n_b,n_e分别为 Bob 和 Eve 接收到的合法信道和窃听信道中的噪声，H_{ba},H_{be},H_{ea}分别为 $N_b \times N_a$，$N_b \times N_e$，$N_e \times N_a$的信道矩阵，假设信道矩阵各元素均独立服从循环对称复高斯分布 $CN(0,1)$，g_1和g_2分别表示窃听信道（Alice 和 Eve 之间的信道）和干扰信道（Bob 和 Eve 之间的信道）的因子，用来标识信道的质量。

假设图 4-3 中的噪声为零均值加性高斯白噪声，满足$\varepsilon\{n_k n_k^H\} = \delta_k \mathrm{I}$，$k = b,e$分别代表 Bob 和 Eve。Alice 的发射功率限制为 P_a，Eve 发送功率限制为 P_e。因为 Alice 发送信号时有两种策略选择，因此将发送的信号 x_a表示为：

$$x_a = \mathrm{T}z + \mathrm{T}'z' \tag{4-16}$$

其中，z表示发送给 Bob 的$d \times 1$的信号，z′表示用来干扰 Eve 的$(N_a - d) \times 1$的

干扰信号，$\mathbf{T},\mathbf{T}'$分别为$N_a\times d, N_a\times(N_a-d)$的矩阵，也就是说 Alice 用了$d$根天线来传送数据给 Bob，剩下的$(N_a-d)$根天线用来干扰 Eve。为了确保干扰信号不会影响正常信号，文献[16]中给出了一种方法使得两种信号正交，如果 Alice 知道$\mathbf{H}_{ba}$，我们可以通过选择$\mathbf{T},\mathbf{T}'$来达到要求。

发送信号x_a的协方差矩阵$\mathbf{Q}_a$满足$\varepsilon\{x_a x_a^H\}=\mathbf{Q}_a, \mathrm{Tr}(\mathbf{Q}_a)\le P_a$，表示为：

$$\mathbf{Q}_a=\mathbf{T}\mathbf{Q}_z\mathbf{T}^H+\mathbf{T}'\mathbf{Q}_z'\mathbf{T}'^H \tag{4-17}$$

其中，$\mathbf{Q}_z,\mathbf{Q}_z'$分别为z,z'的协方差矩阵。如果用$\rho$表示 Alice 用于发送信息给 Bob 的功率占其总功率的比重，则有$\mathrm{Tr}(\mathbf{T}\mathbf{Q}_z\mathbf{T}^H)=\rho P_a, \mathrm{Tr}(\mathbf{T}'\mathbf{Q}_z'\mathbf{T}'^H)=(1-\rho)P_a$。在 Bob 和 Eve 处接收到的噪声加上干扰信号的协方差矩阵为：

$$\mathbf{Q}_b=g_2\mathbf{H}_{be}\mathbf{Q}_{be}\mathbf{H}_{be}^H+\delta_b^2\mathbf{I} \tag{4-18}$$

$$\mathbf{Q}_e=g_1\mathbf{H}_{ea}\mathbf{T}'\mathbf{Q}_z'\mathbf{T}'^H\mathbf{H}_{ea}^H+\delta_e^2\mathbf{I} \tag{4-19}$$

其中，$\mathbf{Q}_{be}$为 Eve 发送的用来干扰 Bob 的干扰信号的协方差。

图 4-3 所示的 MIMO 窃听信道模型中，遍历保密率R_s为[16]：

$$R_s=E_{\mathrm{H}}\left\{\log_2\left|\mathbf{I}+\frac{\rho P_a}{d}\mathbf{H}_{ba}\mathbf{T}\mathbf{T}^H\mathbf{H}_{ba}^H\mathbf{Q}_b^{-1}\right|-\log_2\left|\mathbf{I}+\frac{\rho P_a}{d}\mathbf{H}_{ea}\mathbf{T}\mathbf{T}^H\mathbf{H}_{ea}^H\mathbf{Q}_e^{-1}\right|\right\} \tag{4-20}$$

在如图 4-3 所示的模型中，Alice 和 Eve 都不知道对方的选择，但是她们的行为相互影响。例如 Alice 对 Eve 进行人工加扰虽然可以防止 Eve 的窃听行为，但是对 Eve 干扰行为的作用却适得其反。对于 Eve 而言，当 Alice 选择人工加扰时，Eve 选择窃听行为就是徒劳，此时选择干扰行为更好。Alice 和 Eve 之间可以看作一场博弈游戏，在这场游戏中，节点 Eve 的动机是破坏 Alice 和 Bob 之间的通信（减少保密率），节点 Alice 的动机则是保证她和 Bob 之间的通信安全（提高保密率）。由于 Alice 的收益必然意味着 Eve 的损失，博弈双方的收益和损失之和永远为“零”，因此这实质上是一种零和博弈。

4.2.2 博弈假设条件

对于如图 4-3 所示的模型，Alice 和 Eve 之间博弈关系的成立基于如下假设。

(1) 对于发送方 Alice，为了使 Alice 发射给 Eve 的干扰信号不会影响发射给 Bob 的正常信号，假定 Alice 知道她和 Bob 之间的信道信息$\mathbf{H}_{ba}$。

(2) 对于接收方，假设 Eve 知道她和 Alice 之间的信道信息$\mathbf{H}_{ea}$和$\mathbf{Q}_e$，Bob 知

道他和 Eve 之间的信道信息 H_{be} 和 $\mathbf{Q}_b$。

(3) 模型中所有信道的元素相互独立且服从循环对称复高斯分布 $CN(0,1)$。

(4) 当 Eve 仅发射干扰信号干扰 Bob 时，她并不知道信道信息 H_{be}，因此选择把总的发射功率 P_e 平均分配到 N_e 根天线上对 Eve 来说是一种最优方案，此时

$$\mathbf{Q}_{be}=\frac{P_e}{N_e}\mathbf{I} \tag{4-21}$$

(5) 当 Alice 发射干扰信号干扰 Eve 时，她并不知道信道信息 H_{ea}，因此选择把用于发射干扰信号的功率 $(1-\rho)P_a$ 平均分配到用于发射干扰信号的 (N_a-d) N_e 根天线上对 Alice 来说也是一种最优方案，此时

$$\mathbf{Q}'_z=\frac{(1-\rho)P_a}{(N_a-d)}\mathbf{I} \tag{4-22}$$

(6) 当 Alice 发射信号给 Bob 时，因为知道信道信息 H_{ba}，其最优的选择是通过注水算法来分配发送功率，但是为了简单化模型，我们假设 Alice 用于发射信号给 Bob 的发射天线也满足等功率分配，即

$$\mathbf{Q}_z=\frac{\rho P_a}{d}\mathbf{I} \tag{4-23}$$

(7) 假设 Alice 发射的信号 z,z′ 均服从循环对称复高斯分布。

基于假设(4)(5)(6)前面的公式（4-17）、（4-18）、（4-19）可以写为：

$$\mathbf{Q}_a=\frac{\rho P_a}{d}\mathbf{T}\mathbf{T}^H+\eta_a\mathbf{T}'\mathbf{T}'^H \tag{4-24}$$

$$\mathbf{Q}_b=\frac{g_2P_e}{N_e}\mathrm{H}_{be}\mathrm{H}_{be}{}^H+\delta_b^2\mathbf{I} \tag{4-25}$$

$$\mathbf{Q}_e=g_1\eta_a\mathrm{H}_{ea}\mathbf{T}'\mathbf{T}'^H\mathrm{H}_{ea}^H+\delta_e^2\mathbf{I} \tag{4-26}$$

其中，

$$\eta_a=\frac{(1-\rho)P_a}{(N_a-d)} \tag{4-27}$$

4.2.3 博弈建模分析

这场零和博弈中有两个参与者，即 Alice 和 Eve，每个参与者都有两种策略，

Alice 的策略集合记为S_A，Alice 用全部功率发射数据的策略记为 F(Full-power)，用部分功率发射干扰信号的策略记为 A(Artificial noise)，因此$S_A=\{\mathbf{F},\mathbf{A}\}$。Eve 的策略集合记为$S_E$，Eve 窃听的策略记为 E(Eavesdropping)，干扰 Bob 的策略记为 J(Jamming)，因此$S_E=\{\mathbf{E},\mathbf{J}\}$。选定 Alice 和 Bob 之间的通信的 MIMO 保密率R_s作为 Alice 的效用函数（Alice 和 Eve 的效用为相反数），显而易见，Alice 的目标是使R_s变大，而 Eve 的目标是使R_s减小。

当 Eve 选择策略 E，即窃听 Alice 和 Bob 之间的通信信息时，$\mathrm{H}_{be}=0$，因此由公式（4-25）知$\mathbf{Q}_b=\delta_b^2\mathbf{I}$，代入公式（4-20）可得，此时 Alice 和 Bob 之间的 MIMO 保密率为：

$$R_{iE}=E_{\mathrm{H}}\left\{\log_2\left|\mathbf{I}+\frac{\rho P_a}{d\delta_b^2}\mathrm{H}_{ba}\mathbf{T}\mathbf{T}^H\mathrm{H}_{ba}^H\right|-\log_2\left|\mathbf{I}+\frac{g_1\rho P_a}{d}\mathrm{H}_{ea}\mathbf{T}\mathbf{T}^H\mathrm{H}_{ea}^H\mathbf{Q}_e^{-1}\right|\right\} \tag{4-28}$$

当 Eve 选择策略 J，即发射干扰信号干扰 Bob 时，$\mathrm{H}_{ea}=0$，由公式（4-20）可得此时 Alice 和 Bob 之间的 MIMO 保密率为：

$$R_{iJ}=E_{\mathrm{H}}\left\{\log_2\left|\mathbf{I}+\frac{\rho P_a}{d}\mathrm{H}_{ba}\mathbf{T}\mathbf{T}^H\mathrm{H}_{ba}^H\mathbf{Q}_b^{-1}\right|\right\} \tag{4-29}$$

其中，$i=\mathbf{F},\mathbf{A}$代表的是 Alice 选择的发送策略。当 Alice 选择策略 F，即用全部功率发射数据给 Bob 时，相当于$d=\min(N_a,N_b)$。

文献[27]中证明在合法发送者、接收者、攻击者的天线数分别为L,N,M的 MIMO 信道中，当信噪比 SNR 为∂，干扰和噪声比 INR 为η，MIMO 保密率满足：

$$R_I\le(L+M)F\left(\frac{N}{L+M},(\partial+\eta)\right)-MF\left(\frac{N}{M},\eta\right) \tag{4-30}$$

根据式（4-11）、(4-30)，我们可以得出每种策略组合下 Alice 和 Bob 之间的 MIMO 保密率为[16]：

$$R_{AE}\le dF\left(\frac{N_b}{d},\frac{\rho P_a N_a}{d\delta_b^2}\right)-\left[N_aF\left(\frac{N_e}{N_a},\frac{g_1P_a}{\delta_e^2}\right)-(N_a-d)F\left(\frac{N_e}{(N_a-d)},\frac{g_1(1-\rho)P_a}{\delta_e^2}\right)\right] \tag{4-31}$$

$$R_{AJ}\le(N_e+d)F\left(\frac{N_b}{N_e+d},\frac{\rho P_a N_a}{d\delta_b^2}+\frac{g_2P_e}{\delta_b^2}\right)-N_eF\left(\frac{N_b}{N_e},\frac{g_2P_e}{\delta_b^2}\right) \tag{4-32}$$

$$R_{FE}\le N_aF\left(\frac{N_b}{N_a},\frac{P_a}{\delta_b^2}\right)-N_aF\left(\frac{N_e}{N_a},\frac{g_1P_a}{\delta_e^2}\right) \tag{4-33}$$

$$R_{FJ}\le(N_e+N_a)F\left(\frac{N_b}{N_e+N_a},\frac{P_a+g_2P_e}{\delta_b^2}\right)-N_eF\left(\frac{N_b}{N_e},\frac{g_2P_e}{\delta_b^2}\right) \tag{4-34}$$

在下面的分析中，假设在MIMO窃听信道模型中以下的两个条件始终成立：

(1) $R_{FE} \le R_{AE}$，即当Eve窃听Alice时对其人工加扰总能增大保密率。

(2) $R_{AJ} \le R_{FJ}$，即当Eve干扰Bob时对其人工加扰会减小保密率。

做一些近似处理，如 $N_b / N_a \to \infty, N_e / N_a \to \infty, N_b / N_e = 1$，当 $\beta \to \infty$ 时，$F(\beta,\partial) \approx \log(\partial\beta)$；当 $\beta \to 1$ 时，$F(1,\partial) \approx \log(1+4\partial) - 2 - \log(e)$。简化处理后，Alice和Bob之间的MIMO保密率可以简化为[16]：

$$R_{AE} \le d\log\left(\frac{\rho N_b N_a P_a}{d^2\delta_b^2}\right) - N_a\log\left(\frac{g_1 N_e P_a}{\delta_e^2 N_a}\right) + (N_a - d)\log\left(\frac{g_1(1-\rho)N_e P_a}{\delta_e^2(N_a - d)}\right) \quad (4\text{-}35)$$

$$R_{AJ} \le (N_e + d)\log\left(\frac{N_b}{\delta_b^2(N_e + d)}\left(\frac{\rho P_a N_a}{d} + g_2 P_e\right)\right) - N_e\log\left(\frac{g_2 N_b P_e}{\delta_b^2 N_e}\right) \quad (4\text{-}36)$$

$$R_{FE} \le N_a\log\left(\frac{N_b P_a}{\delta_b^2 N_a}\right) - N_a\log\left(\frac{N_e g_1 P_a}{\delta_e^2 N_a}\right) \quad (4\text{-}37)$$

$$R_{FJ} \le (N_e + N_a)\log\left(\frac{N_b}{\delta_b^2(N_e + N_a)}(P_a + g_2 P_e)\right) - N_e\log\left(\frac{g_2 N_b P_e}{\delta_b^2 N_e}\right) \quad (4\text{-}38)$$

4.2.4 纯策略纳什均衡

在以上的零和博弈中，我们假设参与者Alice和Eve同时选择策略，而且相互不知道对方选择的策略，博弈的支付矩阵如图4-4所示：

		Eve	
		窃听（E）	干扰 Bob（J）
Alice	全部功率用来发射（F）	R_{FE}	R_{FJ}
	部分功率用来干扰（A）	R_{AE}	R_{AJ}

图4-4 MIMO窃听信道模型支付矩阵

结论4-1[16] 在MIMO窃听信道模型中，当 $R_{FJ} \le R_{FE}$ 时，博弈存在纯战略纳什均衡点 R_{FJ}；当 $R_{AE} \le R_{AJ}$ 时，博弈存在纯战略纳什均衡点 R_{AE}。

首先考虑Eve选择策略J的情况，即Eve选择干扰Bob时，由式（4-29）可知，此时Alice可以通过提高她用来发射正常信号的这部分功率来增大保密率，也就是 $R_{AJ} \le R_{FJ}$，因此对于Alice来说，她有动机选择$(\mathbf{F},\mathbf{J})$的策略组合，如果 $R_{FJ} \le R_{FE}$，那么对于想要减少保密率的Eve来说，她没有动机偏离$(\mathbf{F},\mathbf{J})$而去选择$(\mathbf{F},\mathbf{E})$，这种情况下，R_{FJ} 是一个纳什均衡点，因为Alice和Eve都不能通过单方面改变策略来获得更好的效用。

另一方面，考虑 Eve 选择策略 E 的情况，即当 Eve 选择窃听 Alice 时，因为 $R_{FE} \le R_{AE}$ 始终成立，因此对于 Alice 来说，她有动机选择 (A,E) 的策略组合，如果 $R_{AE} \le R_{AJ}$，那么对于想要减少保密率的 Eve 来说，她没有动机偏离 (A,E) 而去选择 (A,J)，这种情况下，R_{AE} 是一个纳什均衡点。

A. Mukherjee 等人[16]提出的基于 MIMO 窃听信道的博弈模型为窃听信道的研究提供了一种新思路。但是文献[16]中仅仅研究了在 Eve 和 Alice 行为相互影响时，两者该如何决策的问题，事实上，Eve 选择何种恶意行为不仅和 Alice 的决策有关，Eve 的自身因素如位置等也将影响 Eve 的决策。下面我们将研究节点 Eve 位置、天线数量以及发射功率等因素对博弈结果以及系统保密率影响。

4.1 节点 Eve 的行为分析

4.1.1 Eve 的位置

在实际无线网络，窃听者 Eve 不会总是处于 Alice 和 Bob 的中间，她的位置可能比较接近发送者 Alice，也可能比较接近接受者 Bob。处于不同的位置时，为了使自身的效用最大，Eve 会偏向于采取不同的策略，从而将对整个博弈产生一定影响。为了分析 Eve 相对 Alice 和 Bob 的位置对博弈的影响，我们假设 MIMO 窃听信道模型中的节点都拥有相同数量的天线，即 $N_a = N_b = N_e$，且 $P_a \approx P_e$。

结论 4-2 如果 Eve 位置相对 Alice 近，博弈存在纯战略纳什均衡点 R_{AE}；如果 Eve 相对 Bob 近，博弈存在纯战略纳什均衡点 R_{FJ}。

当 Eve 相对 Alice 近时，Alice 和 Eve 之间的信道质量较好，Eve 和 Bob 之间的信道质量较差，即 g_1 比 g_2 大，尤其 Eve 十分接近 Alice 时，可认为 $g_1 \gg 1, g_2 \to 0$，做近似处理 $F(\beta,0) \approx 0$，$F(\beta,\infty) \approx \log(\partial)$，由式（4-31）到式（4-34）可知，此时，四种策略组合下的 MIMO 保密率大小顺序为 $R_{FE} \le R_{AE} \le R_{AJ} \le R_{FJ}$，博弈的纯战略纳什均衡点为 R_{AE}，因此，Eve 会更偏向于选择窃听 Alice 的信息。

同理，如果 Eve 相对 Bob 近，即 g_2 比 g_1 大，当 Eve 非常靠近 Bob 时，$g_2 \gg 1, g_1 \to 0$，由式（4-31）到式（4-34）可知，此时，四种策略组合下的 MIMO 保密率大小顺序为 $R_{AJ} \le R_{FJ} \le R_{FE} \le R_{AE}$，博弈的纯战略纳什均衡点为 R_{FJ}。因此，Eve 会更偏向于选择干扰 Bob。

下面考虑一个具体的例子，假设MIMO窃听信道模型中 $N_a = N_b = N_e = 6$，$d = 4$，$P_a \approx P_e \approx 20\mathrm{dB}$，$\delta_e^2 = \delta_b^2 = 1$，四种策略组合下的MIMO保密率与Eve相对Alice的位置的关系如图4-5所示。其中，Eve相对Alice的位置用 g_2 / g_1 来描述，g_2 / g_1 越

大说明Eve离Alice越远（离Bob越近），g_2/g_1越小说明Eve离Alice越近（离Bob越远）。由图4-5可知，当Eve相对Alice越近时，对于想要增大MIMO保密率的Alice来说，策略A总比策略F好，而对于想要减小MIMO保密率的Eve来说，策略E总比策略J好，所以两者选择的策略组合肯定是$(\mathbf{A},\mathbf{E})$而不会偏离，博弈的纯战略纳什均衡点为R_{AE}。同样，当Eve相对Bob近时，由图4-5可知，博弈的纯战略纳什均衡点为R_{FJ}，与以上分析的结果一致。

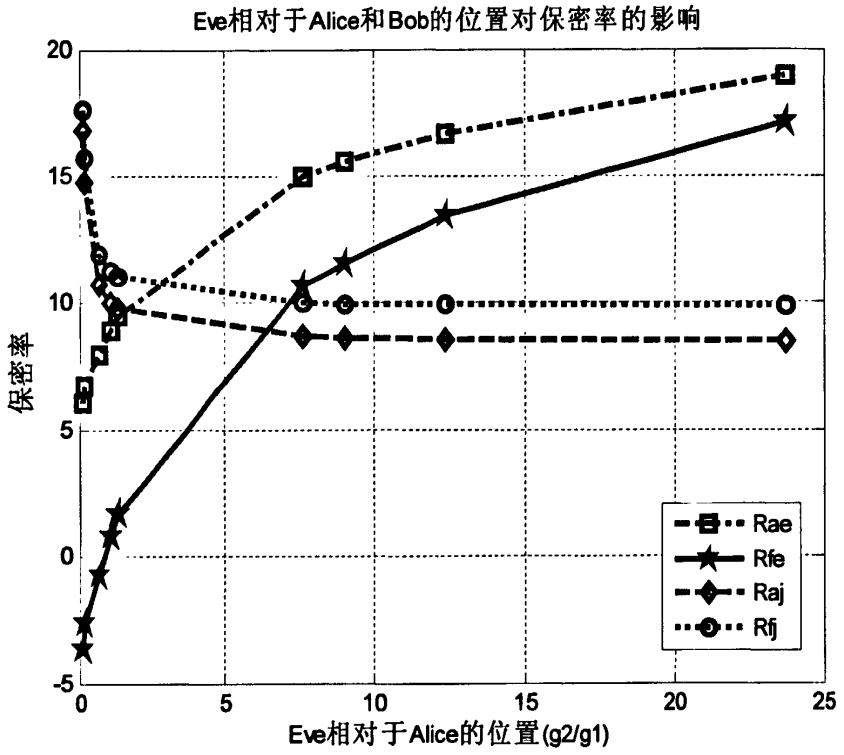


图 4- 5 MIMO 保密率与 Eve 位置的关系图

4.1.2 Eve 的天线数量

攻击者 Eve 天线数量同样也将影响博弈的结果，我们将从四个方面来分析。

结论 4-3 Eve 最坏的情况就是她的天线数量非常少而不能自由选择策略，假设$N_e=1, N_a=N_b>>1$，此时 Eve 无法用单天线来窃听 Alice 发射的多天线信号，因此 Eve 只能选择干扰 Bob，即策略 J，则博弈的纯战略纳什均衡点为R_{FJ}。

结论 4-4 Eve 最好的情况就是她的天线数量非常多，假设$N_e>>N_a=N_b$且$P_a\approx P_e$，也就是说 Eve 相对于 Alice 和 Bob 来说有很大优势，那么不管 Alice 和 Eve 选择什么策略，Alice 和 Bob 之间的 MIMO 保密率都会趋近于 0，此时每个参与者都没有动机选择任何策略，该博弈就没有意义。

结论 4-5 当 Eve 的天线比 Alice 和 Bob 多时，假设 $N_e > N_a = N_b$，且 $P_a \approx P_e$。如果 $N_e > 3(N_a + N_b)$，MIMO 保密率的顺序为 $R_{FE} \le R_{AE} \le R_{AJ} \le R_{FJ}$，此时博弈的纯战略纳什均衡点为 R_{AE}。如果 $N_a < N_e < 3(N_a + N_b)$，因为 N_e 接近 N_a，因此 R_{AE} 和 R_{FE} 均大于 0，博弈存在混合纳什均衡。

结论 4-6 当 Eve 的天线比 Alice 和 Bob 少时，假设 $N_e < N_a, N_e < N_b, N_a \ge N_b$，且 $P_a \approx P_e$。此时如果 $N_e \le (N_a - d)$，也就是说 Alice 用于人工干扰 Eve 的天线数量比 Eve 接受 Alice 信号的天线数量多，显然 Eve 无法阻止 Alice 的人工干扰信号，因此 Eve 只能选择干扰 Bob，此时博弈的纯战略纳什均衡点为 R_{FJ}。如果 $N_e \le (N_b - d)$，也就是说 Eve 用于干扰 Bob 的天线数量比 Bob 接收 Eve 干扰信号的天线数量少，Bob 可以阻止 Eve 发射的干扰信号，恢复 Alice 发送的秘密信息，因此 Eve 只能选择窃听 Alice 的信息，此时博弈的纯战略纳什均衡点为 R_{AE}。

比如当 MIMO 窃听信道模型中 $N_a = 6, N_b = 3$，$d = 2$，$\delta_e^2 = \delta_b^2 = 1$，$g_1 = 0.9, g_2 = 1.1$，$P_a = 55dB, P_e = 75dB$ 时，四种策略组合下的 MIMO 保密率与 Eve 相对 Alice 的天线的关系如图 4-6 所示。由图可知，当 $N_e / N_a \ge 1$，即 Eve 的天线比 Alice 和 Bob 多时，MIMO 保密率的大小顺序为 $R_{FE} \le R_{AE} \le R_{AJ} \le R_{FJ}$，此时 Alice 和 Bob 的最佳策略组合为 $(\mathbf{A}, \mathbf{E})$，与分析的结果一致。

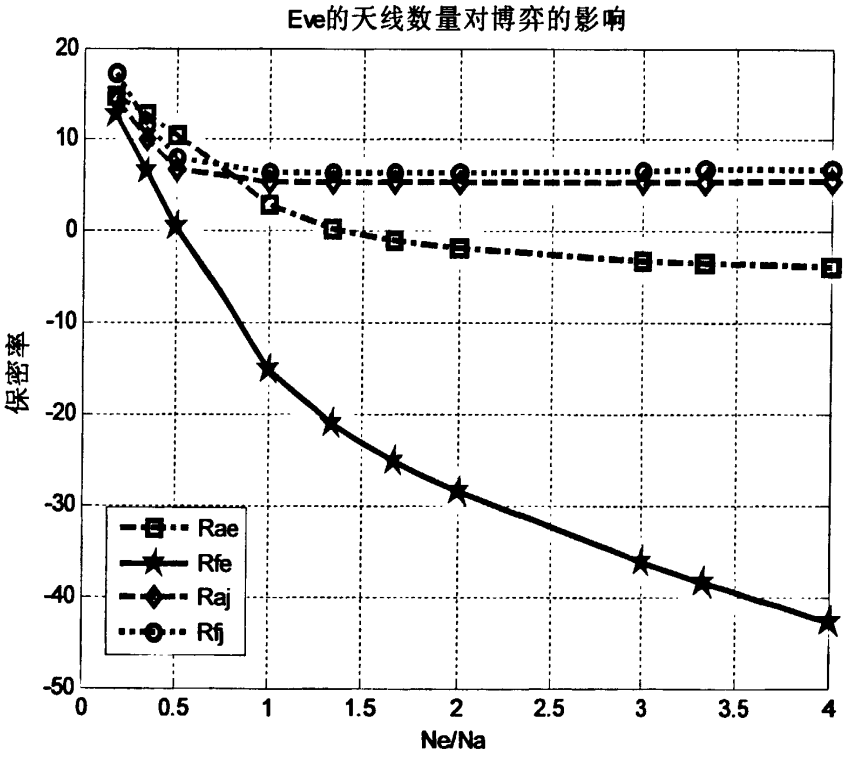


图 4-6 Eve 天线数量对 MIMO 保密率的影响

4.1.3 Eve 的发射功率

在讨论 Eve 的相对位置和天线数量时，我们都假设 $P_a \approx P_e$，事实上，Eve 的发射功率对其策略选择也有一定的影响，下面我们将考虑两种极限情况。

结 4-7 当 Eve 的发射功率 P_e 非常小，假设 $P_e << P_a$，此时，Eve 只能选择窃听 Alice 的信息，即此时 Eve 只能选择策略 E，所以两者最后选择的策略组合肯定是 $(\mathrm{A,E})$。

我们来考虑一个具体的例子，假设 MIMO 窃听信道模型中 $N_a = N_b = N_e = 6$，$d = 4$，$\delta_e^2 = \delta_b^2 = 1$，$g_1 = 0.9, g_2 = 1.1$，$P_e = 1dB$，四种策略组合下的 MIMO 保密率与 Eve 相对 Alice 的发射功率的关系如图 4-7 所示。图 4-7 中横坐标为 Eve 的发射功率 P_e 与 Alice 的发射功率 P_a 的比值，可以看出 P_e 远小于 P_a，此时，四种策略组合下的 MIMO 保密率的大小顺序为 $R_{FE} \le R_{AE} \le R_{AJ} \le R_{FJ}$，博弈的纯战略纳什均衡点为 R_{AE}，与分析的结果一致。

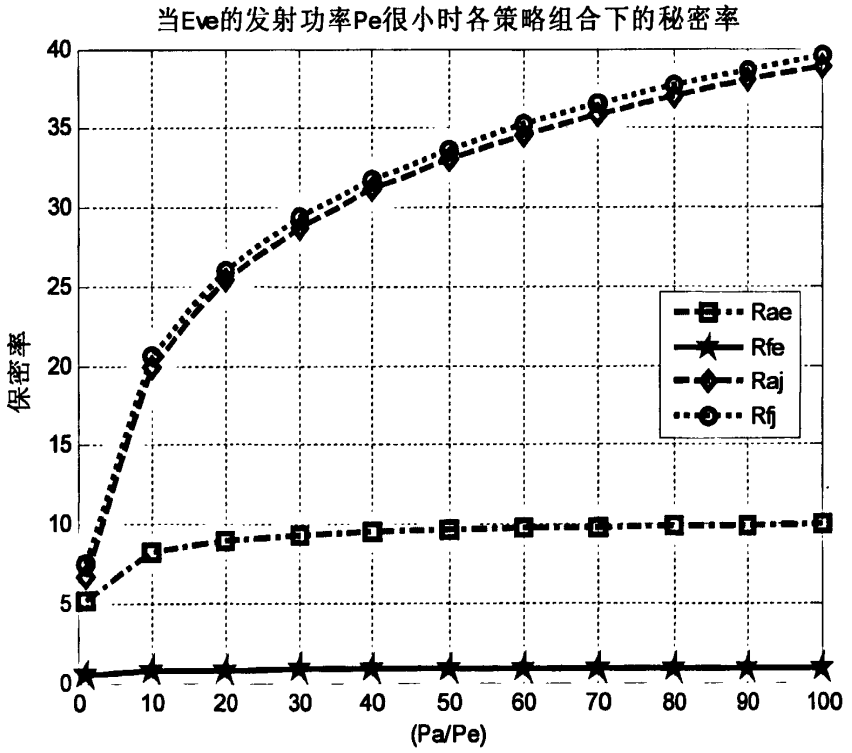


图 4-7 Eve 的发射功率远小于 Alice 的发射功率时的 MIMO 保密率

结论 4-8 当 Eve 的发射功率非常大，假设 $P_e >> P_a$，甚至满足 $P_e \to \infty$，由式（4-35）到式（4-38）知，$R_{AJ} \le R_{FJ} \le R_{FE} \le R_{AE}$ 始终成立，此时，博弈的纯战略纳什均衡点只能为 R_{FJ}。

我们来考虑一个具体的例子，假设 MIMO 窃听信道模型中 $N_a = N_b = N_e = 6$，

$d=4$，$\delta_e^2=\delta_b^2=1$，$g_1=0.9, g_2=1.1$，$P_e=10000dB$，四种策略组合下的MIMO保密率与Eve相对Alice的发射功率的关系如图4-8所示。图4-8横坐标为Eve的发射功率P_e与Alice的发射功率P_a的比值，可以看出P_e远大于P_a，由图4-8可知，此时Alice和Eve的最佳策略组合为$(\mathbf{A},\mathbf{E})$，与分析的结果一致。

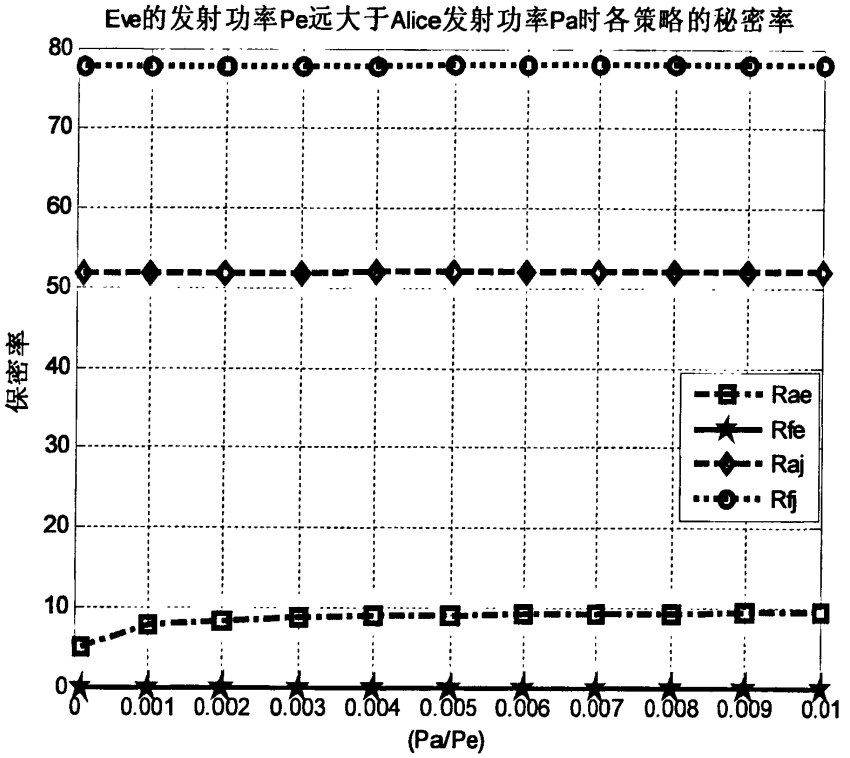


图4-8 Eve的发射功率远大于Alice的发射功率时的MIMO保密率

4.2基于中继窃听信道的节点行为分析

A. Mukherjee等人[16]提出的基于MIMO窃听信道的博弈针对的是最基本的三节点模型，在实际的无线网络中，由于节点的通信覆盖范围有限，两个节点之间常常要借助中继节点来辅助通信。本小节将研究存在中继节点的中继窃听信道模型的保密率问题。

4.2.1 中继窃听信道系统模型

本节讨论的中继窃听信道模型如图4-9所示，该模型包括四个多天线的节点，除合法发送方Alice、合法接收者Bob、攻击者Eve外，还包括中继节点Relay。无线网络中的中继节点分很多种类型，每种类型的中继节点分别扮演着不同的角

色，如友好的中继节点可以帮助发送方传送信息，恶意的中继节点可以帮助窃听者窃听信息等。在如图 4-9 所示的中继窃听信道模型中，假设中继节点 Relay 是友好的，一方面，它可以选择帮助发送者 Alice 转发信息给接收者 Bob，另一方面它也可以人工干扰窃听者 Eve，但是此时认为中继节点是聋的，也就说它听不到 Alice 发送给 Bob 的信息，只作为干扰者来协作 Alice 和 Bob 通信。

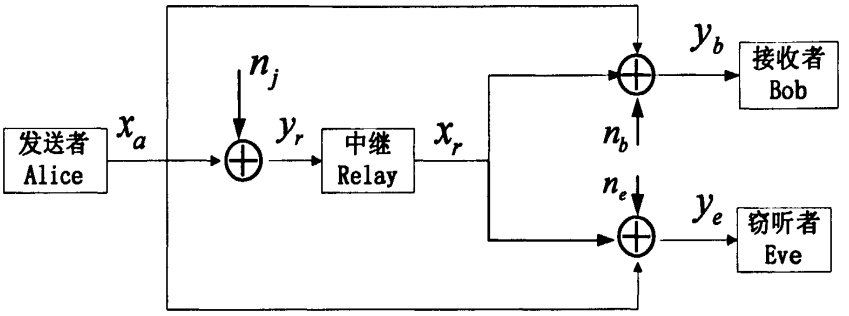


图 4-9 中继窃听信道示意图

图 4-9 中，接收者 Bob、中继节点 Relay 和窃听者 Eve 收到的信息分别表示为：

$$y_b = \mathrm{H}_{ba}x_a + \mathrm{H}_{rj}x_r + n_b \tag{4-39}$$

$$y_r = \mathrm{H}_{ra}x_a + n_r \tag{4-40}$$

$$y_e = \mathrm{H}_{ea}x_a + \mathrm{H}_{re}x_r + n_e \tag{4-41}$$

其中，Alice 发送的信号 x_a 为 $N\times 1$ 维向量，x_r 为中继 Relay 发送的信号，当 Relay 选择替 Alice 转发数据时，x_r 为经过处理将要发送给 Bob 的信息；当 Relay 选择干扰 Eve 时，x_r 为与 x_a 独立的干扰信息。n_b, n_r, n_e 分别为 Bob、Relay 和 Eve 接收到的信道中噪声，假设均为零均值的加性高斯白噪声。$\mathrm{H}_{ba}, \mathrm{H}_{rb}, \mathrm{H}_{ra}, \mathrm{H}_{ea}, \mathrm{H}_{re}$ 分别为 $N\times N$ 的信道矩阵，信道矩阵各元素都相互独立且服从循环对称复高斯分布 $CN(0,1)$。

4.2.2 中继节点行为分析

在中继窃听信道模型中，中继节点 Relay 有两种策略可以选择，一方面，Relay 可以作为普通的中继节点，将收到的 Alice 的信息进行处理后发送给 Bob，此时在 Relay 处可以有多种信息处理方式，这里选择译码前传策略（Decode and Forward，DF），即 Relay 对接收到的 Alice 的信息进行译码后重新编码发送给 Bob，实现和发送者 Alice 的协作。另一方面，Relay 也可以作为一个聋的中继节点，也就是说

它不能听到 Alice 发送过来的信息，但是可以人工干扰窃听者 Eve，需要指出的是此时 Relay 发送的干扰信号与 Alice 发送给 Bob 的信号相互独立，这种策略我们称之为噪声前传策略（Noise and Forward，NF）。下面将对这两种策略下系统的保密率进行分析。

这里将引用文献[28]中的一些结论，文献[28]证明在中继窃听信道中，如果中继节点选择译码前传策略，则此时系统的保密率为：

$$R_s^{(DF)}=\sup\left[\min\left\{I(x_a,x_r;y_b),I(x_a;y_r\mid x_r)-I(x_a,x_r;y_e)\right\}\right]^+ \tag{4-42}$$

在图 4-9 所示的模型中，当中继节点选择译码前传策略时，令 x_r 为 $n\times1$ 维向量，服从高斯分布，均值为 0，协方差矩阵为 K_r，x_n 为 $n\times1$ 维向量，服从高斯分布，均值为 0，协方差矩阵为 K_n，假设

$$x_a=cx_r+x_n \tag{4-43}$$

其中，c 为指定的常数，x_n 为经 Relay 处理后的新信息，x_r 代表的是信号中发送者 Alice 和中继节点 Relay 用于波束赋形的那部分信息。则此时：

$$I(x_a;y_r\mid x_r)=\log\det\left(I+H_{ra}K_nH_{ra}^H\right) \tag{4-44}$$

$$I(x_a,x_r;y_b)=\log\det\left\{I+(cH_{ba}+H_{br})K_r(cH_{ba}+H_{br})^H+H_{ba}K_nH_{ba}^H\right\} \tag{4-45}$$

$$I(x_a,x_r;y_e)=\log\det\left\{I+(cH_{ea}+H_{er})K_r(cH_{ea}+H_{er})^H+H_{ea}K_nH_{ea}^H\right\} \tag{4-46}$$

由式（4-42）可知，此时的系统保密率为：

$$\begin{aligned}R_s^{(DF)}=\max\Bigg[\min\Bigg\{&\log\frac{\left|\det\left(I+H_{ra}K_nH_{ra}^H\right)\right|}{\left|\det\left\{I+(cH_{ea}+H_{er})K_r(cH_{ea}+H_{er})^H+H_{ea}K_nH_{ea}^H\right\}\right|},\\&\log\frac{\left|\det\left\{I+(cH_{ba}+H_{br})K_r(cH_{ba}+H_{br})^H+H_{ba}K_nH_{ba}^H\right\}\right|}{\left|\det\left\{I+(cH_{ea}+H_{er})K_r(cH_{ea}+H_{er})^H+H_{ea}K_nH_{ea}^H\right\}\right|}\Bigg\}\Bigg]^+\end{aligned} \tag{4-47}$$

文献[28]证明在中继窃听信道中，如果中继节点选择噪声前传策略，则此时系统绝对保密率为：

$$\begin{aligned}R_s^{(NF)}=\sup\Big[&I(x_a;y_b\mid x_r)+\min\left\{I(x_r;y_b),I(x_r;y_e\mid x_a)\right\}\\&-\min\left\{I(x_r;y_b),I(x_r;y_e)\right\}-I(x_a;y_e\mid x_r)\Big]^+\end{aligned} \tag{4-48}$$

在图 4-9 所示的模型中，当中继节点选择噪声前传策略时，假设发送者 Alice 的发送功率为 P_a，发送信号 x_a 为 $n\times1$ 维向量，服从高斯分布，均值为 0，协方差矩阵为 K_a，满足 $\mathrm{Tr}(K_a)\le P_a$，中继 Relay 向窃听者 Eve 发送干扰信号时发射功率为 P_r，干扰信号 x_r 为 $n\times1$ 维向量，服从高斯分布，均值为 0，协方差矩阵为 K_r，满足 $\mathrm{Tr}(K_r)\le P_r$，则此时：

$$I(x_a;y_b\mid x_r)=\log\det\left(I+H_{ba}K_aH_{ba}^H\right) \tag{4-49}$$

$$I(x_a,x_r;y_b)-I(x_a,x_r;y_e)=\log\frac{\left|\det\left(I+H_{ba}K_aH_{ba}^H+H_{br}K_rH_{br}^H\right)\right|}{\left|\det\left(I+H_{ea}K_aH_{ea}^H+H_{er}K_rH_{er}^H\right)\right|} \tag{4-50}$$

$$I(x_r;y_e\mid x_a)+I(x_a;y_b\mid x_r)-I(x_a,x_r;y_e)=\log\frac{\left|\det\left(I+H_{er}K_rH_{er}^H\right)\det\left(I+H_{ba}K_aH_{ba}^H\right)\right|}{\left|\det\left(I+H_{ea}K_aH_{ea}^H+H_{er}K_rH_{er}^H\right)\right|} \tag{4-51}$$

由式（4-48）可知，此时的系统保密率为：

$$R_s^{(NF)}=\left[\min\left\{\log\det\left(I+H_{ba}K_aH_{ba}^H\right),\log\frac{\left|\det\left(I+H_{ba}K_aH_{ba}^H+H_{br}K_rH_{br}^H\right)\right|}{\left|\det\left(I+H_{ea}K_aH_{ea}^H+H_{er}K_rH_{er}^H\right)\right|},\log\frac{\left|\det\left(I+H_{er}K_rH_{er}^H\right)\det\left(I+H_{ba}K_aH_{ba}^H\right)\right|}{\left|\det\left(I+H_{ea}K_aH_{ea}^H+H_{er}K_rH_{er}^H\right)\right|}\right\}\right]^+ \tag{4-52}$$

对于中继节点存在多种行为选择的 MIMO 中继窃听信道的研究目前处于起步阶段，这里我们假设模型中中继节点是友好的，推到了两种策略下系统的保密率。事实上，中继节点也可以是恶意的，它既可以帮助窃听者窃听发送者的信息，也可以干扰接收者，因此未来这方面还有很多工作可以研究。

4.3 本章小结

本章首先介绍了 MIMO 窃听信道博弈模型，分析了恶意攻击者位置、天线数量以及发射功率三个因素分别对博弈结果和系统保密率的影响，然后加入了友好的中继节点将模型变为中继窃听信道，并假设中继节点可以有解码传输和干扰传输两种策略，分析了中继节点不同策略选择下中继窃听信道的绝对保密率。

5 总结与展望

5.1 工作总结

本文主要研究无线网络中节点行为对网络性能及安全性的影响，针对无线网络节点中普遍存在的自私行为、恶意行为这一线索展开。一方面结合网络编码技术研究了网络节点的自私行为，主要着眼于分析自私行为带来的影响，并结合分析提出限制节点自私性的激励机制，改善网络性能；另一方面是结合 MIMO 窃听信道模型研究网络节点的恶意行为，主要着眼于选择提高系统保密率，防止节点恶意行为的策略，以增强网络安全。

论文的主要工作总结如下：

1. 把博弈论作为分析工具引入网络中的节点行为研究中。

本文介绍了博弈论的基础知识，给出了博弈三要素、纳什均衡解、博弈分析基础等基本概念，以及重复博弈、零和博弈等博弈模型。分析了无线网络中存在的节点自私行为、窃听行为和干扰行为。把应用于经济学领域的博弈理论引入到网络研究中，分析了博弈论适合用于研究网络节点行为的主要原因，并描述了网络节点之间存在的几种博弈问题：①用户转发困境博弈；②节点包转发博弈；③节点干扰博弈；④网络链路博弈。

2. 对已有的基于网络编码的链路博弈进行了分析，指出了其存在问题，并运用博弈方法重新建模分析了问题存在的原因，提出了激励机制。

分析了文献[10]中基于网络编码的链路博弈模型，指出链路博弈仅仅考虑了链路能耗，并没有考虑链路中间节点自私性，将导致出现网络资源分配不均衡的问题。然后通过建立链路中间节点的重复博弈模型，分析得出链路中间节点的包转发概率随节点转发代价增加而减小的结论，从而指出促使网络流量分配均衡的必要性。最后提出了链路博弈和报价机制相结合的解决方案，来解决网络流量分配不均衡的问题，并通过仿真实验给出了八边形网络拓扑的策略选择。

3. 分析了 MIMO 窃听信道模型中攻击者的行为对系统保密率的影响，并在模型中加入了中继节点，分析了中继节点两种行为选择下的中继窃听信道保密率。

针对文献[16]中提出的 MIMO 窃听信道博弈模型，分析了攻击者窃听者位置、天线数量以及发射功率三个因素分别对博弈结果和系统保密率的影响，然后加入了友好的中继节点将模型变为中继窃听信道，并假设中继节点可以有解码传输和干扰传输两种策略，分析了中继节点不同策略选择下中继窃听信道的保密率。

5.2工作展望

由于研究时间限制，本文的许多工作还没有进一步深入和展开，未来还可以从以下几个方面进行研究。

1. 基于网络编码的节点自私行为研究部分。

本文基于网络编码的节点重复博弈模型中考虑了流量是否分配均衡的问题，后续还可以研究怎样分配流量使得网络编码效率更高。为了更进一步提高编码效率，还可以继续在流量分割方面做一些工作， 另外，文献[10]中的链路博弈模型只考虑了网络编码机会和路由路径长短，本文的模型针对流量均衡因素对链路博弈模型进行了改进，未来还可以研究其他通信因素，如网络延时、网络容量等，继续对模型进行改进。

2. 基于窃听信道的节点恶意行为研究部分。

本文中研究的 MIMO 窃听信道模型是三节点的，事实上在无线网络中，还可以研究很多类似的其他场景。另外，本文研究的中继窃听信道中假设中继节点是友好的，它协作通信，事实上，中继节点也可以是恶意的，他可以帮助窃听者窃听发送者的信息，也可以干扰接收者，以降低系统的保密率，未来可以研究恶意的中继节点的行为对保密率的影响。

参考文献

[1] Dewan P，Dasgupta P and Bhattacharya A. On using reputations in ad hoc networks to counter malicious nodes[C]. Proceedings of the tenth International Conference on parallel and Distributed Systems，California，USA，2004.

[2] 汪洋，林闯，李泉林. 基于非合作博弈的无线网络路由机制研究. 计算机学报，2009. 1（32）：54-68.

[3] Anderegg，L&Eidenbenz S. Ad Hoc-VCG：a Truthful and Cost-Efficient Routing Protocol for Mobile Ad Hoc Networks with Selfish Agents[A]. Proc. of the ACM Mobicom2003[C]. ACM Press，New York. 2003：245-259.

[4] Anderegg，L&Eidenbenz S. On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks[J]. In：Proc. of the ACM MobiCom 2005. NewYork：ACM Press，2005：117-131.

[5] Cai，J&Pooch U. Play alone or together-Truthful and efficient routing in wireless Ad-Hoc networks with selfish nodes[A]. Proc. of the IEEE Int'l Conf. on Mobile Ad-hoc and Sensor Systems(MASS 2004)[C]. Washington，2004：457-465.

[6] Wu，MY&Shu W. RPP：A distributed routing mechanism for strategic wireless Ad Hoc networks[A]. Proc. of the IEEE Global Telecommunications Conf. (GlobeCom 2004)[C].

[7] Felegyhazi，M&Hubaux J. -P. et al. Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks[J]. IEEE Trans. on Mobile Computing. 5(4)，2006：463-476.

[8] Srinivasan，V&P. Nuggehalli et al. Cooperation in Wireless Ad Hoc Networks[A]. Proc. of IEEE INFOCOM[C]. Washington，IEEE Computer Society Press. March 2003：808-817.

[9] 王堃. 无线多跳网络中基于可信的安全协作通信关键技术研究[D]. 南京邮电大学，2009.

[10] J. R. Marden，M. Effros. A Game Theoretic Approach to Network Coding. Information Theory Workshop on Networking and Information Theory，June，2009.

[11] Data Encryption Standard(DES). Federal Information Processing Standard Publication 46. 1977

[12] Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES -The Advanced Encryption Standard." Springer, 2002.

[13] M. Bloch, J. Barros, M. R. D. Rodrigues, S. W. McLaughlin. Wireless Information-Theoretic Security. IEEE Transactions on Information Theory, Special Issue on Information-Theoretic Security, Vol. 54, No. 6, pp. 2515-2534, June 2008.

[14] Y.Liang, H. V. Poor and S. Shamai." Secure communication over fading channels,"IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security, 54(6),

2470-2492, June 2008.

[15] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. In Proc. 2007 Allerton Conference on Communication, Control and Computing, 2007.

[16] A. Mukherjee, A. L. Swindlehurst. Jamming Games in the MIMO Wiretap Channel With an Active Eavesdropper. IEEE Transactions on Wireless Communications, 2011.

[17] 罗云峰. 博弈论教程. 北京：清华大学出版社，2007.

[18] 李莉，董树松，温向明. 无线传感器网络中的分簇算法[J]. 无线通信技术，2006，15(3)：47-51，62.

[19] 叶阿勇，许力. 移动 Ad Hoc 网络中节点协作性研究[J]. 小型微型计算机系统，26(11)，2005：1886-1889.

[20] R. Ahlswede, N. Cai, S. R Li, and R. W. Yeung. Network information flow[J]. IEEE Transactions on Information Theory, July2000, 46：1204-1216.

[21] E. Altman, A. Kherani. Non-Cooperative forwarding in ad-hoc networks. Proceedings of IFIP Networking Conference(IFIP 2005)[C], Waterloo Ontario Canada, Page(s): 486-498, May, 2005.

[22] A. D. Wyner. The wire-tap channel. The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[23] 黄崇炯. 基于 MIMO 的窃听信道建模[D]. 电子科技大学，2010

[24] E. Telatar. Capacity of multi-antenna Gaussian channels. EuropeanTrans. Telecommun, vol. 10, pp. 585-596, 1999.

[25] B. Hochwald, T. Marzetta, B. Hassib. Space-time autocoding. IEEE Trans. Inf. Theory, vol. 47, no. 7, pp. 2761-2781, Nov. 2001.

[26] B. Hochwald, T. Marzetta, V. Tarokh. Multiple-antenna channel hardening and its implications for rate feedback and scheduling. IEEE Trans. Inf. Theory, vol. 50, no. 9, pp. 1893-1909, Sep. 2004.

[27] A. L. Moustakas, S. Simon, and A. M. Sengupta. MIMO capacity through correlated channels in the presence of correlated interferers and noise: A (not so) large N analysis. IEEE Trans. Inf. Theory, vol. 49, pp. 2545-2561, Oct. 2003.

[28] Lifeng Lai, Hesham El Gamal. The Relay-Eavesdropper Channel: Cooperation for Secrecy. IEEE Transactions on Information Theory 54(9): 4005-4019 (2008).

[29] Frank H. P. Fitzek, Marcos D. Katz 著. 程卫军译. 无线网络中的合作原理与应用. 北京：机械工业出版社，2009.

[30] J. Mitola, G. Q. Maguire. Cognitive radio: making software radios more personal, IEEE Personal Communications, vol. 6, nr. 4, pp. 13-18, Aug. 1999.

作者简历

黄莉，女，1988 年 1 月出生，籍贯：湖南省益阳市。2009 年 7 月毕业于北京交通大学计算机与信息技术学院生物医学工程专业，并获得工学学士学位；2009 年 9 月至今，就读于北京交通大学信息科学研究所信号与信息处理专业，研究方向是通信信号处理。

论文发表情况：

黄莉，王升辉. 基于流量预测的 TCP-Friendly 拥塞控制机制研究. 海峡两岸信息科学与信息技术交流会，2010.

学位论文数据集

表 1.1： 数据集页

<table>
<tr><td>关键词*</td><td>密级*</td><td>中图分类号*</td><td>UDC</td><td>论文资助</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">学位授予单位名称*</td><td>学位授予单位代码*</td><td>学位类别*</td><td>学位级别*</td></tr>
<tr><td colspan="2">北京交通大学</td><td>10004</td><td></td><td></td></tr>
<tr><td colspan="2">论文题名*</td><td colspan="2">并列题名</td><td>论文语种*</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td>作者姓名*</td><td colspan="2"></td><td>学号*</td><td></td></tr>
<tr><td colspan="2">培养单位名称*</td><td>培养单位代码*</td><td>培养单位地址</td><td>邮编</td></tr>
<tr><td colspan="2">北京交通大学</td><td>10004</td><td>北京市海淀区西直门外上园村 3 号</td><td>100044</td></tr>
<tr><td colspan="2">学科专业*</td><td>研究方向*</td><td>学制*</td><td>学位授予年*</td></tr>
<tr><td colspan="2"></td><td></td><td></td><td></td></tr>
<tr><td>论文提交日期*</td><td colspan="4"></td></tr>
<tr><td>导师姓名*</td><td colspan="2"></td><td>职称*</td><td></td></tr>
<tr><td>评阅人</td><td colspan="2">答辩委员会主席*</td><td colspan="2">答辩委员会成员</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="5">电子版论文提交格式 文本（ ） 图像（ ） 视频（ ） 音频（ ） 多媒体（ ） 其他（ ）
推荐格式：application/msword；application/pdf</td></tr>
<tr><td colspan="2">电子版论文出版（发布）者</td><td>电子版论文出版（发布）地</td><td colspan="2">权限声明</td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td>论文总页数*</td><td colspan="4"></td></tr>
<tr><td colspan="5">共 33 项，其中带*为必填数据，为 22 项。</td></tr>
</table>