硕士专业学位论文

基于空间功率合成的协作干扰技术研究

Research on Cooperative Jamming Technology Based on Space Power Synthesis

作者：范新

导师：黄亮 副教授

北京交通大学

2018 年 5 月

学位论文版权使用授权书

本学位论文作者完全了解北京交通大学有关保留、使用学位论文的规定。特授权北京交通大学可以将学位论文的全部或部分内容编入有关数据库进行检索，提供阅览服务,并采用影印、缩印或扫描等复制手段保存、汇编以供查阅和借阅。同意学校向国家有关部门或机构送交论文的复印件和磁盘。

（保密的学位论文在解密后适用本授权说明）

学位论文作者签名：范新行　　导师签名：黄亮

签字日期：2018 年 5 月 31 日　　签字日期：2018 年 5 月 31 日

中图分类号：TN929.5　　学校代码：10004
UDC：621.39　　密级：公开

北京交通大学

硕士专业学位论文

基于空间功率合成的协作干扰技术研究

Research on Cooperative Jamming Technology Based on Space Power Synthesis

作者姓名：范新　　学　　号：16125009

导师姓名：黄亮　　职　　称：副教授

工程硕士专业领域：电子与通信工程　　学位级别：硕士

北京交通大学

2018 年 5 月

致谢

惊风飘白日，光景西驰流。不知不觉，我已在北京交通大学学习了六年之久，六年过去，感触良多。有过快乐，有过苦涩。六年的经历将永远镌刻我心，值得我用很长的时间去回味。六月，总是鸟语花香；六月，总要学满毕业。毕业带来离别，而我们各奔前程。在此论文即将完稿之际，我谨向硕士期间，给予我帮助的人们，表示深深的感谢！

首先，我要向我的硕士生导师黄亮副教授表达我最崇高的敬意和最诚挚的感谢。是他为我的人生指明了道路，给予了我多种可选之路，并对我的选择无条件支持。最终，我选择了读博，也意味着不能为他做太多的事，他毫无怨言。黄老师为人和善，从不强迫别人。他乐观的性格，豁达的胸怀，深深地影响了我。这样一位尊重学生，肯为学生着想的老师，值得我一生敬重。

我要向我将来的博士生导师霍炎副教授表达我最衷心的感谢。霍老师是我科研之路的启明灯，是我学术研究的领路人。在他的指导和帮助下，我才能快速入门学术研究。在实验室朝夕相处中，霍老师严谨的治学态度以及不知疲倦的工作热情时刻激励着我。今后我还有很长的岁月要和霍老师一起度过，我将更加努力地向霍老师学习，他是我今后的工作动力和不懈追求的目标。

我要衷心地感谢我的室友范铎同学、殷佳佳同学，感谢他们这两年的陪伴和关怀。

我要衷心地感谢实验室和我一起奋斗的各位同学，感谢他们对我的帮助和鼓励。

我要衷心地感谢我的父母和家人，感谢他们对我的理解与支持。

我要衷心地感谢所有关心、支持和帮助过我而又不能一一列举的人们。

最后，我要感谢国家自然科学基金“面上”项目（No. 61572070，61471028，61575053）和中央高校基本科研业务费重点项目（No. 2017JBM004，2017JBM003）对我的研究工作的支持和资助。我还想感谢我的母校北京交通大学，“知行”校训将永远铭记我心，身为交大人是我一生的荣耀！

中文摘要

近年来，无线通信技术的迅猛发展推动了社会的进步，丰富了人们的生活，但是无线网络的安全问题也不容忽视。虽然基于密码学理论的高层加密方法在一定程度上可以保证信息的安全，但是这些方法往往具有较大的计算复杂度而不适用于“低端的设备”。而且在面对具有超级计算能力的窃听者时，通过密钥加密的方法也未必无懈可击。故而，可以和高层加密相辅相成的物理层安全方法逐渐为人们所重视。与高层加密手段不同，物理层安全充分利用了物理信道的各种特性，旨在物理层实现安全传输，为信息网络安全保护问题提供了一个新的解决思路。

目前，物理层安全已获得大量的研究成果，但是大多数的研究都是在假设窃听者信道状态信息已知的情况下完成的。很显然由于信道的不确定性，窃听者的准确的信道状态信息很难获得。尤其是当窃听者仅处在被动窃听的情况时，将不能获得窃听者任何信息。因此，设计窃听者的信道状态信息完全未知情况下的物理层安全传输方案很有必要。本文研究基于空间功率合成的协作干扰策略来抵抗未知信道状态信息的窃听者，以期实现安全传输的目的。具体来讲，本文主要的研究内容以及创新点如下：

1. 首先本文提供了一个多干扰器防窃听模型，并通过多干扰信号叠加理论对该模型进行了公式化。本文开创性地提出利用空间功率合成技术来引入差异性干扰，旨在最小化在合法接收者处合成的干扰信号功率，但是要满足在其他位置仍有一定的干扰。

2. 基于多干扰器防窃听模型，本文分析了干扰信号叠加之后，一定系统区域内各处的功率密度情况。根据多个干扰器的不同位置关系，提出了相应的协作干扰策略。通过公式推导及理论证明，这些协作干扰策略可以实现多个干扰信号的合成功率在合法接收者处为零，而在系统范围内的其它位置不为零。因此，在未知窃听者信道状态信息的情况下，本文所提协作干扰策略同样可以保证信息的安全传输。

3. 基于所提协作干扰策略，本文进一步提出了发送端与干扰器之间的功率分配方案来实现最差情况下的合法用户的安全速率最大化。由于功率分配优化方程的非凸非线性，为了找到其最优解，本文将其分成了两个子优化问题，并提出利用模拟退火算法进行求解。为了降低算法的复杂度，本文提出了两种搜索算法。最终，通过这两个子优化问题的顺序优化可以找到原始问题的可行解。

全文共 5 章，图 16 幅，表格 3 个，参考文献 85 篇

关键词：物理层安全；协作干扰；电磁场与电磁波；空间功率合成；信道状态信息；安全速率；模拟退火算法

分类号：TN929.5

ABSTRACT

In recent years, the rapid development of wireless communication technology has promoted the progress of society and enriched people's lives, but the security of wireless network can not be ignored. Although encryption methods based on cryptography theory can guarantee information security to a certain extent, they often have large computational complexity, which causes them not suitable for "low end devices". And in the face of eavesdroppers with supercomputing power, these key encryption methods have also been challenged. Therefore, physical layer security methods that can be complemented with high-level encryption are gradually paid attention to. Different from high-level encryption, physical layer security makes full use of various characteristics of physical channels. It aims to achieve secure transmission at physical layer, providing a new solution for information network security protection.

At present, physical layer security has obtained a lot of research results, but most of the research is done under the assumption that channel state information of eavesdroppers is known. It is obvious that the accurate channel state information of the eavesdropper is difficult to obtain due to the uncertainty of the channel. Especially when eavesdroppers are only in the case of passive eavesdropping, any information of eavesdroppers will not be obtained. Therefore, it is necessary to design security strategies of the physical layer without pre-known channel state information of eavesdroppers. In this thesis, a novel cooperative jamming strategy based on space power synthesis is investigated to resist eavesdroppers without channel state information, so as to achieve secure transmission. Specifically, the main research contents and innovations of this thesis are as follows:

Firstly, this thesis provides a multi-jammer anti-eavesdropping model, and formulates the model through the multi-interference signal superposition theory. This thesis pioneers the use of the space power synthesis technology to introduce differential jamming, aiming at minimizing the synthetic power of jamming signals at a legitimate receiver, but still existing certain interference in other locations.

Secondly, based on the multi - jammer anti - eavesdropping model, this thesis analyzes the power density at various places within a certain system area after the jamming signals are superimposed. According to the different positional relationship of multiple jammers, corresponding cooperative jamming strategies are proposed. Through the formula deduction and theoretical proof, these cooperative jamming strategies can

achieve the synthetic power of multiple jamming signals is zero at a legitimate receiver, and not zero at other locations within the system. Therefore, in the case of unknown eavesdroppers' channel state information, these proposed cooperative jamming strategies can also guarantee the secure transmission of information.

Thirdly, based on these cooperative jamming strategies, this thesis further proposes a power allocation scheme to maximize the worst-case secrecy rate of legitimate users. Due to the non-convex and nonlinearity of the power allocation optimization equation, this thesis divides it into two sub-optimization problems to find its optimal solution, and proposes a simulated annealing algorithm to solve them. In order to reduce the complexity of the algorithm, two kinds of search algorithms are proposed in this thesis. Finally, through the sequential optimization of the two sub-optimization problems, a feasible solution of the original problem can be found.

This thesis consists of 5 chapters, including 16 figures, 3 tables and 85 references.

KEYWORDS： Physical layer security; cooperative jamming; electromagnetic and electromagnetic wave; space power synthesis; channel state information; secrecy rate; simulated annealing algorithm

CLASSNO： TN929.5

目录

1 绪论

近年来，物理层安全在无线通信和无线网络研究中获得了广泛的关注，本论文以物理层安全中的协作干扰技术为研究对象，利用空间功率合成技术，并结合信息论安全理论、优化问题求解等相关基础理论知识，实现无线网络安全性能的提升。

本章具体内容安排如下：1.1 节介绍了本文的研究背景。1.2 节对物理层安全相关的技术进行了简单的描述，并分析了物理层安全的国内外研究现状。1.3 节阐明了本文的研究动机和意义所在。1.4 节介绍了本论文主要的研究内容和创新之处。1.5 节给出了本论文的章节安排。

1.1 论文研究背景

随着当前社会的发展，科技的进步，无线通信网络已经深入地走进了人们的生活，深层次地影响着人们的衣食住行。随着无线网络用户数量的急剧增多以及网络的应用范围的不断扩大，人们在享受无线网络服务带来的各种便利的同时，也为无线网络通信的安全性感到担忧。黑客搭建无线网络窃取用户信息的事件时有发生，例如，山东聊城的大学生在公共场所使用 wifi 几个小时后，就发现网银被盗的事件。无独有偶，美国史上最大的 wifi 盗窃案的主犯，开车搜寻存在安全隐患的无线网络，盗取了 4100 万个信用卡和提款卡号。诸如此类安全事件一旦出现，往往会造成用户隐私的泄露以及巨大的财产损失，尤其是在涉及银行，军事，医疗等重要场景时。通信信息系统的安全技术已经成为了减少经济损失、保护国家安全、保障社会稳定的重要武器。

安全性是评价一个通信系统好坏的标准，表征了一个通信系统在对抗外来威胁时的能力。不同于具有封闭式物理传输介质的有线传输系统网络，无线通信网络更易受到安全威胁，主要表现在如下几个方面[1][2]：

- 无线通信系统的广播特性使之更易受到安全威胁。
- 无线终端设备的移动性使得安全性管理更困难。
- 无线通信系统的网络拓扑结构的多样性和多变性，使安全性措施的实施更加困难。
- 无线传输信道的不稳定性除了影响有效性和可靠性之外，也给系统的安全性带来了极大的挑战。

目前，无线通信系统的安全性机制主要还是由有线通信系统移植而来。从开放

式系统互联模型的七层结构来看，当前的无线网络安全性的保障主要依靠于网络层以上，并且在研究上层安全技术的时候往往假设低层已经提供了可靠交付。为保障通信系统的安全性，传统的方案通常是利用密钥手段对通信信息进行加密处理。如果没有密钥，则用户不能对该信息解密。例如，网上银行所使用密钥技术，必须输入随机产生的密码才能完成商品交易。还有对于商业的机密信息也要使用密钥进行加密处理，以防止工业间谍的窃取。这些高层的加密手段往往要牺牲复杂度来换取安全性[3][4]。然而，随着量子计算机等具有超级计算能力的设备的出现，一些非法用户的计算能力也得到了大幅度地提升，传统通信网络以及相应信息传输技术的安全性也将面临严峻的挑战。一旦窃听者的计算能力过于强大，则高层加密手段不再那么有效。而且上层加密技术往往复杂度相当高，使得其在满足 5G 广接入、低时延，加解密实时性要求方面面临严峻挑战（高层的加密在一些低端设备上实现很困难）。另外，近些年来，一些新型网络以其较高的灵活性而得到了广泛的应用，例如，无线自组织网络（Mobile Ad hoc network, MANET）、无线传感器网络（Wireless sensor network, WSN）等。这些网络中的节点大多使用电池供电，以至于其根本无法承担传统加解密算法的功耗和成本开销。因此，作为高层加密手段的一种补充，物理层安全（Physical layer security, PLS）逐渐被人们重视。

简单来讲，物理层安全是指通过物理信道的本质特征来实现安全传输的手段，如互异性、唯一性以及随机性等等，而并非使用复杂的数学方法来确保数据的保密性[5]。传统加密手段是利用密码学原理在高层从网络协议的角度实现数据加密，而物理层安全则是通过控制信号传输来实现信息论层面的安全。和高层密钥加密手段相比，物理层安全有着很多自己的优点，例如，有可以进行量化分析的安全评估标准、复杂度相对较低等等。从应用的角度来看，物理层安全更是具有易实现，易维护等优点。从无线网络的发展来看，信道编码的技术革新，多载波技术的广泛应用，多天线技术的飞速发展以及协同中继技术的产生等等，都使物理层资源变得更加丰富，可研究的范围也大大变广。从与传统加密手段结合的角度考虑，物理层加密手段与高层加密技术并不冲突，它是高层加密安全的一种有益补充。两种技术相互作用可以进一步提升整个系统的安全性能。

综上所述，随着无线网络的蓬勃发展和移动终端业务的爆炸式增长，物理层安全使无线通信系统更加有效地利用了物理层资源，为提高信息安全提供了新的方法。另一方面来说，物理层安全技术的研究与高层加密技术相辅相成，可以构建立体化的网络安全体系，具有十分重大的研究价值和现实意义。

1.2 物理层安全国内外研究现状

1.2.1 物理层安全技术的提出

广义上来讲，物理层安全指利用无线信道的固有物理特征，在物理层实现无线通信系统的安全。它是在 Shannon 的“绝对安全”（也称“无条件安全”）基础理论之上建立起来的。1949 年，Shannon 在他的经典论文《保密系统的通信理论》[6]中指出，如果在密钥的熵不小于信息熵的情况下使用“一次一密”方式进行加密，信息的传输过程可以实现理论上的绝对安全。但是令人悲观的是，此绝对安全理论需要解决大量密钥的分配问题，这一条件在现实应用中要求过于苛刻，因而无法实现绝对安全。为解决这一问题，1975 年，Wyner 提出了无线网络的基本窃听信道模型[7]。他在文献[7]中表明，如果窃听者的信道比合法接收者的信道质量差，那么总可以找到一种信道编码方式，使得窃听者无法从其获得的信号中解码出任何有用的信息，而合法用户却可以成功解码。在 Wyner 的窃听信道模型的启发下，很多文献提出了一系列无密钥安全方案[8][9]。这些方案的出发点是，在信道状态信息（Channel state information, CSI）已知的情况下，使得合法用户的信道质量比窃听者的信道要好。然而 Maurer 却认为 Wyner 的窃听信道模型中，假设窃听者的信道比合法接收者的差未必合理[10]。1993 年，Maurer 在他的论文中[10]，提出了一种无需满足窃听者的信道比合法接收者的差的条件，依然可以实现信息安全传输的方法。他的设计思路是利用信道的互异性来产生一组安全密钥。此后，关于物理层安全的研究主要分为了两个方向[9]：1）由 Shannon 和 Maurer 引领的物理层密钥安全机制；2）由 Wyner 引领的物理层无密钥安全机制。

1.2.2 物理层密钥安全机制

物理层密钥安全机制利用合法信道特征的随机性和互异性来生成密钥，这种加密方法与传统的高层加密的实现方式大不相同。该密钥安全机制的典型流程主要包括四个步骤[11]：信道测量、特征提取和量化、信息调和、隐私放大。而这种密钥生成的方法也有其评价标准，通常包括以下三个：

（1） 密钥熵：密钥熵说明了密钥的随机性。密钥熵越大说明密钥随机性越大，而窃听者也越难以破解，通信也就越安全。因此，密钥熵是一个国际认可的评价标准，而 NIST 测试也成为了国际认可的测试熵的方法。

（2） 比特错误率：密钥安全机制下的比特错误率并不是传统意义的误比特率或误码率，而是指的是合法发送端与接收端的生成的密钥的不同比

特概率。

（3） 密钥生成速率：这个标准顾名思义，指的就是密钥生成的速度，它与密钥生成的四个步骤所用的方法都有关系。

在 Maurer 提出利用信源信宿共同的信道随机性生成密钥实现信息加密之后，研究人员陆续提出了大量针对密钥的生成和分配的方案。部分文献研究了信源密钥分配方案[12]，这些方案要求信源和信宿分别生成各自的随机序列，然后利用公共信道接收对方发来的序列，从而完成密钥分配与协商。还有的研究了信道密钥生成方案[13], 在此密钥生成方案中，信源将随机序列通过噪声信道发送给信宿。除了在理论层面的研究外，也有一些面对实际应用的密钥生成方案。有的文献[14]在实际的移动场景和静止场景下，研究了基于信号接收强度（Receive signal strength, RSS）的密钥生成方案，并且分别用实验验证了其有效性。多输入多输出（Multiple input Multiple output, MIMO）技术在提升系统性能方面有着很大的优势，而且在提升密钥随机性和生成速率方面都有所提高。故而有的学者[15]尝试去验证真实场景中，MIMO 系统密钥生成方案的有效性。令人遗憾的是，出于设备、空间等条件，目前的文献仅在虚拟场景下对 MIMO 系统进行了验证。

1.2.3 物理层无密钥安全机制

笼统地讲，物理层无密钥安全机制包括基于信道编码的物理层安全策略[16]和基于信号处理的物理层安全策略[7]。

基于信道编码的物理层安全策略不仅要考虑通信系统的安全性，还要考虑系统的可靠性，大致可以被分为两类：纯安全信道编码[17]和安全可靠信道编码[18]。前者是在系统保证了传输可靠性之后再进行的编码策略，故而仅考虑了系统的安全性。后者则在实行编码策略时同时兼顾考虑系统的可靠性传输以及信息的保密。

基于信道编码的物理层安全方案往往要求窃听者的信道是合法用户的退化信道，这个假设在通信系统实际应用中很难保证。与之相比，基于信号处理的物理层安全策略则从信号处理的角度杜绝被窃听的可能，显得更加实际。

基于信号处理的物理层安全策略的核心思想是，通过预编码（Precoding，PC）技术[19]、波束赋形（Beamforming，BF）技术[20]、人工噪声（Artificial noise, AN）技术[21]等物理层技术，降低窃听者的信号接收质量，或者提高合法接收者的信号接收质量，从信号处理的根本上确保信息不会被非法用户解调。其中，预编码技术是设计发送端信号空间矩阵，充分利用多天线的空分优势，使其在增强合法接收者

信道质量的同时恶化窃听者的信道。波束赋形技术则是将有用信号尽可能地对准合法接收者，相当于消除窃听者的信源，从而达到保密效果。而人工噪声技术的基本思想是，在发送端、接收端或者第三方节点发送人工噪声来降低窃听信道的质量同时尽量不对合法用户造成干扰。

相比于物理层密钥安全机制和基于信道编码的物理层安全策略，基于信号处理的物理层安全策略，复杂度更低，实施起来也较为容易。除此之外，基于信号处理的物理层安全策略还有明确的安全评估标准，如安全容量（Secrecy capacity, SC）[7]、安全中断概率（Secrecy outage probability, SOP）[22]、遍历安全容量（Ergodic secrecy capacity, ESC）[23]等。因此，随着多天线、多载波以及中继协作等物理层技术的飞速发展，基于信号处理的物理层安全策略逐渐成为了主流，获得了重大的研究进展。本文也是研究的基于信号处理的物理层安全策略中的人工噪声技术，其研究意义将在下节介绍。

1.3 本文的研究意义

随着信息价值的不断体现，信息安全越来越受到人们的重视。在无线网络服务中，由于无线网络信道自身的广播特性，使之易于受到非法者的截获或者篡改。尤其是涉及商业机密、军事领域、以及国家安全的无线通信系统，信息与安全处于并重地位。传统的保护信息安全的方式是通过高层运用密钥对信息数据进行加密。随着计算机技术的发展，恶意用户的计算能力也不断的提高，此传统的加密手段也慢慢不能够完全地满足人们的安全需要。因此，物理层安全，作为高层加密的一种补充措施应运而生。通过物理层安全与高层加密手段的相辅相成，可以进一步保证无线通信系统的安全性，使得物理层安全成为了当前无线网络安全的一个研究热点。

本文研究的主要内容是物理层安全技术中的协作干扰技术，该技术可以保证在合法用户的信道质量比窃听者的信道质量差的情况下也能实现信息的安全传输。由上节可知，协作干扰技术是非密钥加密机制物理层安全技术中的基于信号处理的人工噪声策略。人工噪声技术旨在引入差异性干扰，即在合法用户双方通信过程中，由通信的双方或者第三方节点发送人工噪声信号或者干扰（Jamming）信号。此干扰信号可以降低窃听者的信干燥比（Signal-to-Interference-Plus-Noise Ratio，SINR），而又尽量不影响合法用户的接收质量。由第三方节点发送人工噪声的方式被称作协作干扰（Coorperative Jamming, CJ）。

基于协作干扰的物理层安全传输策略最早在2005年由S.Goel和R.Negi提出。在他们发表的文献[24]中，他们开创性地将 BF 与 AN 相结合，提出利用多天线的

BF 技术在主信道的零空间发射 AN，以此来降低窃听信道的接受信噪比。此方法相当于以迫零波束成形（Zero-Forcing Beamforming, ZFBF）的方式发送人工噪声。此后，S.Goel 和 R.Negi 将他们的 AN 方法针对不同窃听信道模型做了进一步的研究工作[25-29]。同时，针对该策略也有别的学者进行了大量的研究[30]。有的研究者从协作干扰过程、人工噪声信号的生成以及性能分析的角度进行了深入研究[30,31]。文献[32]分析了 BF 向量与 AN 矩阵的设计对合法接收者的 SINR 和窃听者的 SINR 的比值的约束作用。考虑单天线和多天线的场景，Jorswieck 在文献[33]中探讨了天线的数量对系统安全性能的影响。而文献[34]和[35]则关注，在有限个合作节点中如何去选择干扰源的问题，期望以最小的能量达到最好的干扰效果。在全局功率限制下，文献[36]和[37]设计了一系列功率分配方案，从而实现最大的系统安全容量。此外，还有一些针对特殊场景的协作干扰安全策略，例如，在 WANETs 中的协作干扰策略[38]、在协作认知无线电网络（Cooperative Cognitive Radio Networks，CCRNs）中的协作干扰策略[37,39]等等。

上述文献在协作干扰安全策略方面取得了重大研究进展，具有重要理论指导意义。但是不仅仅上述文献，现存的大多数文献所提的协作干扰策略都是基于窃听者的 CSI 已知的情况下进行的。很显然，由于信道估计误差等因素，想要获得完美 CSI 是不太现实的。因此，文献[40]和[41]将完美 CSI 已知这个条件退化为部分已知，以一种确定性误差的形式来定义 CSI，从而去优化最差条件安全容量（Worst-case Secrecy Capacity，WCSC）。但是，对于处于完全被动窃听状态的窃听者来说，他们的 CSI 可能是完全未知的，因而很难去计算系统的安全容量。为了解决这一问题，文献[42]-[44]应用了新的物理层安全性指标安全中断容量（SOC）和安全中断概率（SOP），即将 CSI 看作是服从统计分布的变量，从统计概率的角度来分析系统的安全性能。在此基础上，文献[45]和[46]则分别讨论安全区域（Wireless Secrecy Region, WSR）和安全区域最小化（Compromised Secrecy Region Minimization, CSRM）的问题。这些基于概率统计分布的安全策略比较实用，推进了物理层安全的发展。

尽管如此，针对窃听者 CSI 未知的协作干扰策略的研究工作并没有取得实质性的进展，这是因为无论什么策略至少应知道粗糙的窃听者 CSI（不确定性估计，统计概率等）。因此，如何设计窃听者 CSI 未知情况下的协作干扰策略仍然是物理层安全领域研究的关键性问题。

不同于以前的文献，本文研究，在窃听者 CSI 未知情况下，基于空间功率合成的协作干扰策略。利用电磁场与电磁波理论，设计功率合成策略，从而使得多个干扰器发出的噪声在全系统范围内合法接收者处最小，即不管窃听者在系统范围内的何处，其受到的干扰总比合法接收者大。而 ZFBF 技术却只能保证在某一方向干

扰信号最小，故而本文所提策略具有很大的创新性。据调研所知，本文所做工作为协作干扰技术开创了一个新的研究领域。

综上所述，物理层安全技术在当前的无线网络安全研究中深受重视，由于其具有重大应用价值和现实意义。目前，关于物理层安全技术方面的研究还处于不成熟阶段，有待于进一步探索。物理层安全技术中的协作干扰技术研究广泛，但现有的研究成果大多数都基于窃听者 CSI 已知这一假设进行。在现实场景下，这一假设很难实现。因此，设计窃听者的 CSI 未知情况下的协作干扰策略具有重大实际意义，也是本文的研究目的与价值所在。本文的研究成果将对物理层安全在未来的实际应用起到促进作用。

1.4 本文的主要研究内容和创新点

1.4.1 本文主要研究内容

由于基于信号处理的物理层安全策略具有复杂度低、无需密钥生成分发等过程、有明确的性能评价指标等优势，使得其在面对真实场景时更加有效。因此，本文研究了基于信号处理的物理层安全策略中的人工干扰技术。人工干扰技术是物理层安全中的一大类，众多参考文献针对不同系统进行了大量研究，但大多是基于窃听者的 CSI 已知的情况下进行的。然而由于通信环境的复杂性以及窃听者的被动窃听，一般情况下，不能获得窃听者的 CSI。因此，需要设计一种，在不知道窃听者的 CSI 的情况下的人工噪声方案。本篇论文提出了一种新奇的协作干扰方案，该方案不需要知道窃听者的 CSI 同样能达到安全传输目的。本文研究的主要问题如下：

（1） 如何在未知窃听者 CSI 的情况下实现差异性干扰。在协作干扰模型中，要求窃听者的信道容量小于合法用户，这样才能保证一定的安全容量，进而实现信息的安全传输。因此，协作节点干扰信号要有差异性，使得窃听者受到的干扰远远大于合法用户。这就需要选择适当的干扰源来完成干扰任务，设计干扰策略，尽量使它们对合法用户发出的干扰远小于窃听者，这是本文重点解决的问题之一。

（2） 在确定干扰源以及设计协作干扰策略之后，如何进而设计基于协作干扰技术的全局功率优化方案，以期获得较高的安全容量。由于无线网络是功率受限网络，在满足安全通信要求前提下，如何为干扰器和发信方进行合理的功率分配，达到最高的系统安全容量，这亦是本文需要解决的关键问题之一。

（3） 设计干扰策略和全局功率优化方案，都会引入一些优化问题，要从数学上解决上述优化问题也是一个难点。这些优化问题往往不是凸规划问题，虽然遗传算法、模拟退火算法等可以得到上述问题的次优解，但由于算法收敛性低，很难应用于实时的环境中去。如何解决该问题，设计相应的最优或者次优化算法，是本文的重点和难点。

1.4.2 本文主要创新点

本篇论文针对上述问题，利用空间功率合成技术、通信信息论安全理论、优化问题求解等相关理论知识，设计了更加实际有效的新奇物理层安全策略，为物理层安全的研究开拓了一个新的方向。本文的主要创新点总结如下：

（1） 针对研究问题一，本文提出利用空间功率合成技术来引入差异性干扰。通过调节每个干扰器天线的初始发射相位、电流等参数，使各个干扰器发射的电磁波信号在无线空间中进行相互叠加，这必然会出现信号功率在区域内的加强点和削弱点。基于这一思路，本文的目标是使得多个干扰器在合法接收者处的合成干扰功率远小于该区域内的其它所有位置。这样不管窃听者在何位置，其受到的干扰都会大于合法接收者。本文根据多个干扰器的不同位置关系，提出了相应的协作干扰策略，分析了每个干扰器的参数对系统安全性能的影响。

（2） 针对研究问题二，本文将功率分配问题建模成了一个数学优化问题。由于该优化问题的非凸非线性，导致其很难求解，故而本文将其分成了两个易于处理的子优化问题。通过顺序求解这两个子优化问题，可以找到原始问题的解。首先，在固定功率分配情况下，寻找最差的窃听者位置，即系统范围内安全速率最低的位置。接着，本文证明了最差窃听者位置不随功率分配的改变而改变。最后，针对找到的最差窃听者位置进行功率分配，提出了一种功率分配算法来优化最低可达安全速率。

（3） 针对研究问题三，在设计协作干扰策略时，本文根据多个干扰器的不同位置关系，分情况通过数学推导证明了，通过调节各干扰器参数可以实现合成的干扰信号仅在合法接收者处为零的目的。在进行功率分配优化方案时，为了寻找最差窃听者位置，本文提出了一种波浪形之字搜索方法。该方法可以大大降低搜索范围，从而降低算法的计算复杂度。在找到最差窃听者位置后，本文提出利用模拟退火算法进行功率分配优化问题的求解。为了降低计算复杂度，本文进一步提出了一种一维搜索方法，从而有效地解决了功率分配方案设计问题。

本文的研究内容与创新点之间的关系如下列框图所示：

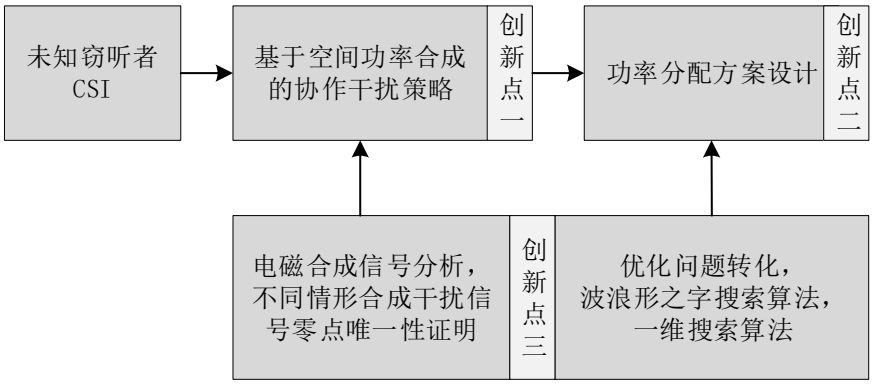


图 1-1 本文研究内容与创新点示意图
Figure 1-1 The sketch of the content and innovation in this paper

1.5 本文的章节结构安排

本文对物理层安全中的协作干扰技术进行了研究和探讨，各章节主要内容和安排如下：

第一章：首先介绍了物理层安全的研究背景；其次介绍了物理层安全中的一些技术的国内外研究现状；接着阐述了本文的研究意义；然后归纳了本文的主要研究内容和创新点；最后介绍了本论文各章节的安排。

第二章：概述了本文的研究内容相关的理论基础知识。首先介绍了物理层安全的相关的基础理论；然后对电磁场电磁波理论中与本文相关部分进行了概述，为后文做了铺垫。

第三章：针对窃听者 CSI 未知的情况下，本文设计了基于空间功率合成的协作干扰策略。首先，本文提出了一个多干扰器协作防窃听模型，并对该模型进行了公式化；接着，根据多个干扰器之间的不同位置关系，分析了各干扰器参数对合成的干扰信号的影响；然后，通过数学推导证明，设计了不同情况下的协作干扰策略；最后，仿真结果表明了本文所提协作干扰策略的有效性。

第四章：在确定协作干扰节点后，本文进一步提出了功率分配方案，以期提升系统的最差可达安全速率。首先，本文提出了一个功率分配问题，并建立了优化方程；接着为了求解该优化问题，本文将其分解为两个子优化问题；然后通过顺序求解这两个子优化问题可得到原始优化问题的可行解；最后，数值仿真结果证明了本文提出的功率优化算法可以进一步提升系统的安全速率，具有良好的性能。

第五章：对本论文的主要工作进行了总结，同时指出了本文的研究内容不足之处，并对未来的研究方向进行了展望。

2 物理层安全和空间功率合成的相关理论基础

本论文的主要研究内容是基于空间功率合成的物理层安全技术，目的是借助空间功率合成技术设计未知窃听者 CSI 的情况下的物理层安全策略。因此，需要将物理层安全和空间功率合成技术的基本理论知识进行介绍，为后文的论述奠定理论基础。

本章节具体内容安排如下：2.1 节介绍了香农信息论基础，包括信息熵、互信息、信道容量以及香农公式等重要概念的定义与基本原理的推导。2.2 节介绍了基于信息论的物理层安全理论基础，对保密通信系统的原理与性质进行了描述。2.3 节介绍了天线与电磁场电磁波理论基础。2.4 节对本章节进行了总结。

2.1 香农信息论基础

物理层安全建立于香农信息论基础之上，故而本节介绍香农信息论相关的基础理论知识，为后文做铺垫。

2.1.1 香农信息论概述

信息无处不在，几乎随着社会文明的发展应运而生。然而，“信息论”作为一门研究信息的学科的建立，却是在 20 世纪中期。1948 年，Shannon 发表的一篇非常著名的论文《通信的数学原理》[47]，成了信息论发展的开山之作，产生了深远的影响力。现如今，信息以爆炸式的增长速度，已经成为了我们生活中的一部分。我们不断的产生信息，同时也利用着信息。香农的信息论在理论基础和思想指导上对信息技术的发展起到了至关重要的作用。现代通信系统、互联网技术以及多媒体技术等都受益于信息论。与此同时，这些信息技术的发展也带动了信息论的发展，丰富了信息论的内容。

香农信息论是 Shannon 综合早起学者们以及同时代的许多著作和实践产物创立的基础理论。香农信息论也被叫做狭义信息论，是在无线通信系统模型中，利用概率统计等数学方法来研究信息以及信息交换的一门学科。香农信息论主要研究通信过程中的信息度量以及信道容量等问题，主要从量的方面描述信息的获取与传输，故而香农信息论又被称作统计信息论。

香农信息论的伟大之处在于其用数学公式来反映信息在统计方面的性质。接下来，本文介绍香农信息论中关于信息表达的一些定义。

2.1.2 熵

信息是一个非常宽泛的概念，人们到底从自己获得的消息、新闻等信息中获得了多少信息量很难去定义描述。Shannon 在信息论中首次提出用信息熵来描述随机变量存在的不确定性，即一个事件发生的概率越大，则其不确定性就越小，反之亦然。而消息的不确定性则代表了信息的价值，不确定性越高的信息包含的信息量越低，价值也就越低，反之亦然。消息的接受者消除了不确定性，这才完成了一次成功的通信。

对于离散信源来讲，如果独立地发送一个有限序列，各个符号被发送的概率$p_1, p_2, \ldots, p_n$已知，则其平均信息熵可由下式（2.1）给出：

$$H = -\sum_{i=1}^{n} p_i \log_c p_i \qquad (2.1)$$

上式（2.1）中 c 表示对数的底，信息熵的单位由它决定。在信息论中，对数的底 c 一般取 2，对应的信息熵的单位是“比特”（*bit*）。**除非另作说明，本文关于信息熵的计算全部以 2 为底。**当然 c 还可以取 3，10，e，它们对应的信息熵的单位分别是“铁特”、“迪特”、“奈特”（相应的英文单位为：*tet*、*det*、*nat*）。当信源以相同的概率发送符号序列时，平均信息熵变为$H = \log n$，此为上式（2.1）的最大值。

由上述可知，对于单个随机变量的信息熵可以用（2.1）式计算。类似地，我们同样可以将信息熵推广到两个或者多个随机变量。以二元随机变量*(X,Y)*为例，如果其联合概率分布为：

$$p(x,y) = P_r\{(X,Y) = (x,y)\} = P_r\{X = x, Y = y\} \qquad (2.2)$$

则由信息熵的定义，我们可以得出此二元随机变量*(X,Y)*的联合熵为：

$$H(X,Y) = -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log \mathrm{p}(x,y) = -E_{X,Y}[\log p(X,Y)] \qquad (2.3)$$

式中$E[\cdot]$算式的作用是求概率统计的数学期望值。信息熵其实是说明了 X、Y 两个事件同时发生的不确定度。当 X、Y 是两个独立的事件时，它们的联合熵等于 X、Y两事件的信息熵之和。

除此之外，若知道两事件的联合概率分布$p(x,y)$，X 关于 Y 的条件概率分布$p(x|y)$，以及 Y关于 X的条件概率分布$p(y|x)$，我们同样可以求出这两事件的条件熵。X关于 Y的条件熵$\mathrm{H}(X|Y)$定义如下：

$$\begin{aligned} H(X|Y) &= -\sum_{y\in Y} p(y)\, H(X|X=x) \\ &= -\sum_{y\in Y} p(y)\sum_{x\in X} p(x|y)\log p(\mathrm{x}|y) \\ &= -\sum_{y\in Y}\sum_{x\in X} p(x,y)\log p(\mathrm{x}|y) \\ &= -\mathrm{E}_{p(x,y)}[\log p(\mathrm{X}|Y)] \end{aligned} \qquad (2.4)$$

同理，Y关于 X的条件熵$H(Y|X)$可以定义为：

$$H(Y|X) = -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(\mathrm{y}|x) = -\mathrm{E}_{p(x,y)}[\log p(Y|X)] \quad (2.5)$$

通过推导，信息熵具有一些重要的性质，由下列**定理 2-1** 给出。

定理 2-1 对于二元离散随机变量*(X,Y),* 它们的熵具有如下性质：

1) $H(X)\geq 0$。
2) $H(X)\leq \log n$，n为符号总数，当且仅当 X服从均匀分布时等号成立。
3) 条件熵减少：$H(X|Y)\leq H(X)$，当且仅当 X与 Y相互独立时等号成立。
4) $H(X,Y)\leq H(X)+H(Y)$，当且仅当 X与 Y相互独立时等号成立。
5) $H(X,Y)=H(X)+H(Y|X)=H(Y)+H(X|Y)$。

2.1.3 互信息

如果信源发送一系列离散符号$X=\{x_1,x_2,\dots,x_n\}$，信宿端接收到从信源发送来的信道输出信号$Y=\{y_1,y_2,\dots,y_n\}$，则通过上小节可知，信息熵表明信息的不确定性。其中，X的信息熵 *H(X)*表明了x_i是否发生的不确定性。而信宿接收到输出信号y_i，会再一次评定x_i的发生的不确定性，这个不确定性即是 X 关于 Y 的条件熵$H(X|Y)$。由**定理 2-1** 的第 3 条性质可知，信息在传递的过程中是有损失的。信息熵 *H(X)*与条件熵$H(X|Y)$的差值代表了此次通信过程信源获得的信息量。该信息量被定义为 X与 Y的平均互信息，用 $I(X;Y)$来表示如下：

$$\begin{aligned} I(X;Y) &= H(X)-H(X|Y) \\ &= -\sum_{x\in X}p(x)\log p(x)+\sum_{y\in Y}\sum_{x\in X}p(x,y)\log p(\mathrm{x}|y) \\ &= -\sum_{y\in Y}\sum_{x\in X}p(x,y)\log p(x)+\sum_{y\in Y}\sum_{x\in X}p(x,y)\log p(\mathrm{x}|y) \\ &= \sum_{y\in Y}\sum_{x\in X}p(x,y)\log\frac{p(\mathrm{x}|y)}{p(x)} \end{aligned} \quad (2.6)$$

由**定理 2-1** 第 5 条性质可得：

$$H(X)-H(X|Y)=H(Y)-H(Y|X) \quad (2.7)$$

因此，Y中含的 X的信息量与 X中含的 Y的信息量相等，故而平均互信息也可以被写作：

$$\begin{aligned} I(X;Y) &= H(Y)-H(Y|X) \\ &= \sum_{y\in Y}\sum_{x\in X}p(x,y)\log\frac{p(x|y)}{p(y)} \end{aligned} \quad (2.8)$$

平均互信息说明了通信过程中信宿接收到由信源发送来的关于 X 的信息量，即若$I(X;Y)>0$，则说明了通信过程中消除了一定的不确定度，从而收获了一定的有用信息量。

2.1.4 信道容量

人们选择道路总是会选那些宽大、能容纳很多车的。而信道如同道路，选择信道也要使得单位时间内尽可能多地传输信息符号，传输每个符号的信息量尽可能地大。由上小节可知，平均互信息表示接受端接收信息符号后获得的平均信息量，故而平均互信息也就表征了信道的平均传输速率 R，即：

$$R = I(X;Y) = H(X) - H(X|Y) \quad (bit/符号) \tag{2.9}$$

而信道容量表示的是，一个信道在单位时间内可以传输的最大信息量。假设单位时间能传送 n 个符号，则信道容量的表达式为：

$$C = nR = n\big(H(X) - H(X|Y)\big) \quad (bit/s) \tag{2.10}$$

信道容量与平均互信息有关，而平均互信息与两个概率相关，$p(x)$和$p(\mathrm{x}|y)$。因此，在所有的 X的分布$p(x)$中，最大平均互信息 $\max I(X;Y)$就是该信道的信道容量，即：

$$C = \max_{p(x)} I(X;Y) \tag{2.11}$$

信道容量表明了信道的特性，是信道能承载的最大传输信息量。此最大传输信息量的大小反映了一个信道的信道传输质量，其值越大说明信道传输质量越高，信道越好。

2.1.5 香农公式

根据上小节关于信道容量的描述，对于一个加性高斯白噪声（Additive White Gaussian Noise, AWGN）信道而言，其信道容量可以被表达为：

$$C = \max_{p(x),E[X^2]<P} I(X;Y) \tag{2.12}$$

其中，平均互信息为：

$$I(X;Y) = h(y) - h(y|x) = h(y) - h(n_0) \tag{2.13}$$

其中，x 与 y 分别表示发送信号与接受到的 x 的信号，n_0则表示与 x 相互独立的 AWGN 信号。假定 x 的发送功率为 S，AWGN 信号的功率为N_0，则接收端接收到的功率为这两部分信号之和，可以表示如下：

$$E[y^2] = E[(x + n_0)^2] = E[x^2] + 0 + E[n_0^2] = S + N_0 \tag{2.14}$$

由平均功率受限情况下的最大熵原理可得：

$$\begin{cases} h(y) \le \frac{1}{2}\log[2\pi e(S+N_0)] \\ h(n_0) = \frac{1}{2}\log(2\pi e N_0) \\ I(X;Y) = h(y) - h(y|x) \le \frac{1}{2}\log[2\pi e(S+N_0)] - \frac{1}{2}\log(2\pi e N_0) = \frac{1}{2}\log\left(1+\frac{S}{N_0}\right) \end{cases} \quad (2.15)$$

由上式与（2.12）可知，信道容量为上式取等式，即

$$C = \frac{1}{2}\log\left(1+\frac{S}{N_0}\right) \quad (bit/符号) \quad (2.16)$$

根据奈奎斯特（Nyquist）抽样定理，系统的抽样频率要大于信号的两倍的带宽，才能避免频谱混叠，才能无差错传输。假设发送信号 x 有效传输的带宽为 B，则信道的最大无差错传输速率可以表示为：

$$C = 2B \times \frac{1}{2}\log\left(1+\frac{S}{N_0}\right) = B\log\left(1+\frac{S}{N_0}\right) \ (bit/s) \quad (2.17)$$

上式（2.17）就是著名的香农信道容量公式，它体现了信道容量、带宽以及信噪比（Signal-to-Noise Ratio，SNR）三者之间的关系，同时还取决于编码方式。现如今数字通信系统中的技术，如分集、均衡以及各种多址技术等，都是为了追求更高的信道容量，以及更大的频谱利用率。这些通信系统的核心技术都围绕香农公式发展，也体现了它的现实意义。另外，香农信道容量公式也指出，当信息的传输速率$R \le C$，则在理论上存在一种信道编码，能够让信息无差错地在信道中传输。

2.2　物理层安全理论基础

2.2.1　基本窃听信道模型

继 Shannon 在《保密系统的通信理论》[6]中提出了具有开创性意义的加密系统之后，Wyner 在 1975 年提出了非常著名的窃听信道模型[7]。此模型为今后的无线通信物理层安全领域的研究奠定了基础。如图 2-1 所示，该模型中主要包括三个节点：发送者（Alice）、合法接收者（Bob）以及窃听者（Eve）。其中，Alice 与 Bob 之间的通信信道被称作主信道，而 Alice 与 Eve 之间的信道被称作窃听信道。

这三个节点的天线数目决定着不同模型的类型，如单输入单输出单窃听（SISOSE）窃听信道模型、单输入多输出多窃听（SIMOME）窃听信道模型、多输入多输出多窃听（MIMOME）窃听信道模型等等。而且，主信道与窃听信道可以建模成不同类型的信道衰落模型，如高斯信道衰落模型、瑞利信道衰落模型等等。下图 2-1 则是物理层安全中，无线通信网络的最初始最基本的窃听信道模型。

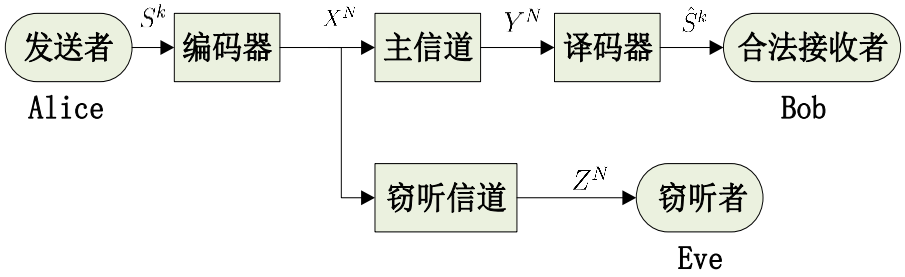


图 2-1 Wyner 所提的无线通信基本窃听信道模型

Figure 2-1 Wyner's basic wiretap channel model in wireless communication

假设发送者要向合法接收者发送 K 个源消息$S^K = (S_1, S_2, \dots, S_K)$，这 K 个源消息为来自于有限集合 S 的独立同分布的变量。此源消息 S^K 首先通过一个二进制编码器进行编码，成为一个 N 位的二进制序列$X^N = (S_1, S_2, \dots, S_N)$。合法接收者接收到由主信道传来的信号$Y^N = (Y_1, Y_2, \dots, Y_N)$，则主信道的信道转移概率可以表示为：

$$Q_M^{(N)}(Y|X) = \prod_{n=1}^{N} Q_M^{(N)}(Y_n|X_n) \tag{2.18}$$

合法接收端的接收器在接收到由主信道传来的信号后，会先用译码器对信号进行解码，译码器输出信号为$\hat{S}^K = (\hat{S}_1, \hat{S}_2, \dots, \hat{S}_K)$。$\hat{S}^K$其实是一个估计信号，是对 S^K 的一个估计值。比对 S^K 与$\hat{S}^K$，可以求出此次信号传输过程中信息出错的概率，即误码率：

$$P_e = \frac{1}{K}\sum_{k=1}^{K} \boldsymbol{Pr}\{S_K \neq \hat{S}_K\} \tag{2.19}$$

误码率代表了通信系统的可靠性，显然，误码率越小越好。

与此同时，非法用户 Eve 同样可以通过窃听信道也接收到码字。该码字表示为$Z^N = (Z_1, Z_2, \dots, Z_N)$，则窃听信道的信道转移概率可以表示为：

$$Q_W^{(N)}(Z|X) = \prod_{n=1}^{N} Q_W^{(N)}(Z_n|X_n) \tag{2.20}$$

同样地，为衡量 Eve 接收到的信息的准确度，定义窃听信道的归一化信道疑义度为：

$$\Delta \triangleq \frac{1}{K} H(S^K|Z^N) \tag{2.21}$$

式中$H(S^K|Z^N)$为条件熵。

信道疑义度 Δ 刻画了窃听者 Eve 在获取了 Z^N之后，仍然对发送者 Alice 传递的信息存在的不确定度。很显然，疑义度越大则信息的不确定度越高，即越安全。当 Δ=1 时，说明窃听者 Eve 对于发送者 Alice 发送的消息一无所知，即此次传输过程最安全；相反，若 Δ=0 时，Eve 对接收到的信息不存在不确定度，即完全知晓了 Alice 发送的消息。

总之，误码率与信道疑义度衡量了一个通信系统的有效性和安全性。

2.2.2 窃听信道的安全容量

安全容量其实表征的是合法用户之间的信息传输速率 R 与窃听信道的信道疑义度 Δ 之间的关系。出于安全通信的考虑，我们要尽可能大地获取传输速率 R，并且要保证尽可能大的疑义度 Δ。然而，这 R 与 Δ 之间却有着复杂的相互制约关系。为了定量地研究它们之间的可达性与相互制约的关系，Wyner 定义了一个参数对 (R, d)，并且讨论了 (R, d) 的可达性。如果对于任意足够小的 $\epsilon > 0$，(R, d) 均满足以下条件：

$$\begin{cases} \frac{S^K}{N} \geq R - \epsilon \\ \Delta \geq d - \epsilon \\ P_e \leq \epsilon \end{cases} \tag{2.22}$$

则称 (R, d) 是可达的。

上式（2.22）给出了信息传输速率与疑义度之间的关系，在满足上式的情况下，尽可能地使 R 和 d 同时最大，这样才能同时保证通信的有效性和安全性。

Wyner 在此基础上，又进一步推导了 (R, d) 可行域：

$$0 \leq R \leq C_M \tag{2.23}$$

$$0 \leq d \leq 1 \tag{2.24}$$

$$Rd \leq \max\{I(X;Y) - I(X;Z)\} \tag{2.25}$$

上面三个式子其实是 (R, d) 可行域的三个约束条件。从这三个约束条件来看，R 越大则 d 越小。当 R 取最大值 C_M 时，d 取最小值 $\max\{I(X;Y) - I(X;Z)\}/C_M$。

为了使窃听者 Eve 接收不到任何有用的信息，则信道疑义度 d 应取最大值 1，这种情况被称作完美安全通信。能够实现完美安全通信的最大信息传输速率被称作安全容量。

根据式（2.25），安全容量为：

$$C_S = \max\{I(X;Y) - I(X;Z)\} \tag{2.26}$$

上述安全容量表达式（2.26）说明了，当 Eve 的信道比 Bob 的信道差时，总能找到一种编码-解码方式使得在满足 Bob 以一定信息传输速率传递信息的同时，而 Eve 却不能获得任何有用的信息。另一方面来说，安全容量的定义 C_S 也表明了，信息安全传输也可以不依赖密钥从而达到绝对安全的效果。此定义式为物理层安全领域的研究定义了公众认可的安全性评价标准，并且对于各种信道模型都适用，至今仍然是众多物理层安全方案的优化目标。

以上是物理层安全研究的最基本的窃听信道模型，为物理层安全领域的研究

引导了方向，奠定了理论基础。随着无线通信技术的发展，新的物理层技术研究也有了重大的突破。物理层安全窃听信道模型也进一步得到了拓展，例如，多用户窃听信道（Multi-user Wiretap Channel, MUWT）模型[48-54]、多天线窃听信道（Multi-antenna Wiretap Channel, MAWT）模型[55-63]、中继窃听信道（Relay Wiretap Channel, RWT）模型[64-72]、协作窃听信道（Cooperative Wiretap Channel, CWT）模型[73-76]等等。这些新的窃听信道模型丰富了物理层安全研究的内容，也为物理层安全提供了理论指导。

2.2.3 基于人工噪声的安全容量提升方法

上小节所述基本窃听信道模型需要窃听者的信道条件比合法用户差，才能保证一定的安全容量，才能实现安全通信。但这个要求在现实生活中很难实现。既然这种情况大多数情况下不能被满足，就需要想办法去降低窃听者的信道质量，或者提升合法用户的信道质量。人工噪声技术就是这样的一种方法，此方法旨在降低窃听信道的信号接收质量，使其低于主信道。

人工噪声的种类多样，大致可以被分为如下几类[5][8][9][30]：

（1） 高斯噪声：此种噪声产生比较简单，也便于分析和实现。但是其对安全容量的提升作用有限。虽然可以有效地降低窃听者的接收信噪比，但同时也降低了合法接收者的接收质量。

（2） 已知的噪声信号：这种噪声在发送之前，合法接收端提前已知。这样合法接收端就可以在接收到的信号中去除该噪声信号，但窃听者却不能消除该信号。因此，可以实现噪声信号在将降低窃听者的接收信号质量的同时对合法用户没有影响。此种方式要求合法接收端具有合理的消除方法，复杂度一般也比较高。另外，噪声信号要以私密的形式传递给合法接收端。传递的信道要求是安全信道，此安全信道能否保证一定安全同样也是一个问题。

（3） 公共密码本中的随机码字：由于公共密码本所有节点均知道，故而不需要安全信道传输。但是要求合法接收端有解码和消除干扰信号的能力，即使它需要一个复杂的自干扰消除接收器来解码码字。当然，此方法还要要求窃听者不具备消除该干扰信号的能力。不然，此干扰信号将毫无作用，徒增复杂度而已。

（4） 所有合法节点的有用信号：利用各个合法接受端传输的信号之间的相互影响，来实现互助的人工噪声。由于多个传输对的多变性，这种方式很难得到应用。

人工噪声除了种类多样外，发送方式也分很多种。可以由发送端以信息内部嵌入噪声发送，可以由目的节点自己发送，还可以通过第三方节点协作发送。

此外，人工噪声技术还可以和其它技术结合使用，以便进一步提升系统安全性能，包括多天线技术、波束赋形技术、博弈论、以及功率分配算法等等。

下面本文以 SISOSE 窃听信道模型为例，具体介绍此方法的基本原理。

2.2.3.1 SISOSE 窃听信道模型

本小节先分析，在没有第三方节点辅助情况下，SISOSE 窃听信道模型所能达到的安全容量。后一小节则以此来对比，分析第三方节点协作发送人工噪声对于安全容量的提升效果。

如图 2-2 所示，SISOSE 窃听信道模型是最简单的三点式系统模型，这三个节点均采用单天线进行收发信号。

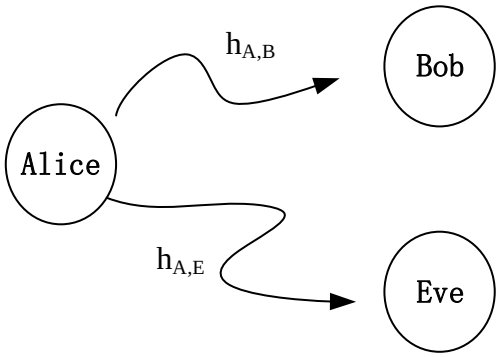


图 2-2 SISOSE 窃听信道模型

Figure 2-2 SISOSE wiretap channel model

假设信源 Alice 以功率 P 向 Bob 发送 0 均值的复高斯信号 x，即$\mathrm{E}(|x|^2)=P$。此时，合法接收端 Bob 和窃听端 Eve 接收到的信号分别为：

$$\mathrm{y}_B = h_{A,B}x + n_B \tag{2.27}$$

$$\mathrm{y}_E = h_{A,E}x + n_E \tag{2.28}$$

其中$h_{A,B}$，$h_{A,E}$分别表示 Alice 与 Bob 之间的信道增益和 Alice 与 Eve 之间的信道增益。而n_B和n_E分别表示 Bob 和 Eve 处接收到的加性高斯白噪声信号，其分别服从均值为0方差为σ_B^2和均值为0方差为σ_E^2的高斯分布。

根据上述 Bob 与 Eve 接收到的信号，可以写出它们的信噪比，分别如下：

$$\gamma_B = \frac{Ph_{A,B}}{\sigma_B^2} \tag{2.29}$$

$$\gamma_E = \frac{Ph_{A,E}}{\sigma_E^2} \tag{2.30}$$

进而根据香农公式和安全容量的定义，安全容量为主信道的信道容量与窃听信道的信道容量之差。又由于安全容量的非负性，故而可以得到 SISOSE 窃听信道模型的安全速率表达式，如下：

$$C_S = \begin{cases} C_B - C_E, & C_B > C_E \\ 0, & C_B \le C_E \end{cases} \tag{2.31}$$

其中，

$$C_B = \log_2(1+\gamma_B) = \log_2\left(1+\frac{Ph_{A,B}}{\sigma_B^2}\right) \tag{2.32}$$

$$C_E = \log_2(1+\gamma_E) = \log_2\left(1+\frac{Ph_{A,E}}{\sigma_E^2}\right) \tag{2.33}$$

分别表示主信道和窃听信道的单位带宽下的信道容量。

由上式（2.31）~（2.33）可以看出，当$h_{A,B} > h_{A,E}$时，$\gamma_B > \gamma_E$，故而安全速率为正值；反之，当$h_{A,B} \le h_{A,E}$时，$\gamma_B \le \gamma_E$，安全速率则为 0。安全速率为 0 表明，主信道不可能以大于零的传输速率进行安全通信。

因此，在上述 SISO 系统中，一旦窃听信道的信道质量比主信道的质量好，则合法用户不可能进行安全通信。

2.2.3.2 人工噪声辅助的 SISO 系统的安全容量

接下来，本文讨论人工噪声辅助下的 SISOSE 窃听信道模型的安全容量。由于在某些情况下，Bob 的信道增益未必比 Eve 强，故而不能实现安全通信。若要实现 Alice 与 Bob 之间的安全通信，可以在 SISOSE 窃听信道模型中，加入一个第三方节点，如图 2-3 所示。此第三方节点作为合法用户的协作节点 Jm，帮助其发送人工干扰噪声信号，用来辅助合法用户，以期实现安全通信的目的。

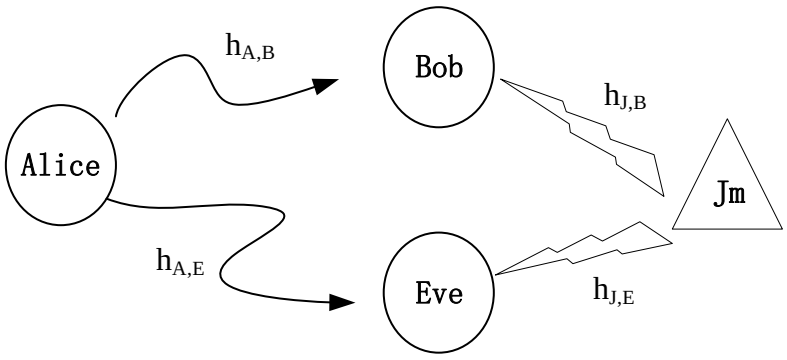


图 2-3 AN 辅助的 SISOSE 窃听信道模型

Figure 2-3 AN aided SISOSE wiretap channel model

根据协作节点的天线数量以及发送的噪声类型，其最终所实现的效果也不一

样。下面，本文主要分以下几种情况进行讨论：

（1）Jm 利用单天线发送全向干扰信号且 Bob 不能消除

此种情况下，Jm 与 Bob、Eve 之间的信道增益$h_{J,B}$，$h_{J,E}$为标量。Bob 和 Eve 接收到的信号如下：

$$y_B = h_{A,B}x + h_{J,B}v + n_B \tag{2.34}$$

$$y_E = h_{A,E}x + h_{J,E}v + n_E \tag{2.35}$$

其中，v为 Jm 发送的干扰信号，$E(|v|^2) = P_J$。

按照上一小节推导过程，此种情况下的安全速率可以被推导出，如下：

$$C_S = [C_B - C_E]^+ = \left[\log_2\left(1 + \frac{Ph_{A,B}}{P_J h_{J,B} + \sigma_B^2}\right) - \log_2\left(1 + \frac{Ph_{A,E}}{P_J h_{J,E} + \sigma_E^2}\right)\right]^+ \tag{2.36}$$

其中，运算式$[x]^+ = max(0, x)$，表示取 0 与x之中的较大者。

由上式（2.36）可知，若主信道的信道质量比窃听信道差，即$h_{A,B} \le h_{A,E}$，同样也可以保证安全速率大于 0，只要满足$h_{J,B} < h_{J,E}$，即 Jm 发出的噪声对 Bob 的干扰强度小于 Eve。

一般这种情况，系统需要找到距离 Eve 近而距离 Bob 远的第三方节点来发送干扰信号，并且需要控制干扰信号的强度，使得其不能对 Bob 产生的干扰过大而影响其正常接收。但是，Eve 的位置信息如何获得是一个很大的问题。

（2）Jm 利用单天线发送全向干扰信号但 Bob 可以消除

此种情况下，由于 Bob 可以消除 Jm 发来的干扰信号，即$h_{J,B}v = 0$，其安全速率表达式只是与式（2.36）略有不同，表示如下：

$$C_S = [C_B - C_E]^+ = \left[\log_2\left(1 + \frac{Ph_{A,B}}{\sigma_B^2}\right) - \log_2\left(1 + \frac{Ph_{A,E}}{P_J h_{J,E} + \sigma_E^2}\right)\right]^+ \tag{2.37}$$

从上式可以看出，此种干扰发送方式性能明显优于上一种情况，由于干扰信号对 Bob 没有影响。此种方式的干扰当然也能实现主信道的信道质量比窃听信道差的情况下的信息安全传输。性能虽好，但要保证 Bob 可以消除干扰信号是个难点，前文已分析。

（3）Jm 利用多天线发送迫零干扰信号

多天线场景下的波束赋形和预编码技术，可以有针对性地调整天线角度，使得发送信号的方向对合法用户更有利。而 Jm 利用迫零波束赋形技术可以将干扰信号对 Bob 迫零，使得干扰信号对其不产生影响。

此种情况下，由于多天线，$\boldsymbol{h}_{J,B}$，$\boldsymbol{h}_{J,E}$均为矢量，维度与天线数相同。而信号v也为矢量信号，$\boldsymbol{v} = \boldsymbol{w}s$，其中$\boldsymbol{w}$为波束赋形矢量，$\|\boldsymbol{w}\| = 1$，$s$为复高斯信号，$E(|s|^2) = P_J$。

系统需要在发送干扰信号之前，设计 Jm 的波束赋形矢量，使得$\boldsymbol{h}_{J,B}^{H}\boldsymbol{w}=0$，即发送的干扰信号在合法用户的零空间内。

经推导，此种情况的全速率表达式如下：

$$C_S=[C_B-C_E]^+=\left[\log_2\left(1+\frac{Ph_{A,B}}{\sigma_B^2}\right)-\log_2\left(1+\frac{Ph_{A,E}}{\boldsymbol{h}_{J,E}^{H}\boldsymbol{w}+\sigma_E^2}\right)\right]^+ \quad (2.38)$$

此情况对 Bob 要求较低，不需要其具有消除干扰信号的能力。其复杂度主要集中在波束赋形设计上。

（4）Jm 利用多天线发射定向干扰

与上种情况类似，但是本干扰方式是将方向直指窃听者，将天线信号集中发向 Eve。在发射干扰信号之前，需要设计波束赋形矢量，使得$\boldsymbol{h}_{J,E}^{H}\boldsymbol{w}$最大化。此种情况下的安全速率表达式如下：

$$C_S=[C_B-C_E]^+=\left[\log_2\left(1+\frac{Ph_{A,B}}{\boldsymbol{h}_{J,B}^{H}\boldsymbol{w}+\sigma_B^2}\right)-\log_2\left(1+\frac{Ph_{A,E}}{\boldsymbol{h}_{J,E}^{H}\boldsymbol{w}+\sigma_E^2}\right)\right]^+ \quad (2.39)$$

这种情况虽然会对 Bob 造成轻微干扰，但是可以给予 Eve 更大干扰强度，获得的安全性能也同样更高。但是，需要知道 Eve 的完美 CSI 才可以进行波束赋形设计。

2.3　天线与电磁波传播理论基础

由于本论文的研究内容是基于空间功率合成的物理层安全技术，故而本小节简单介绍一下关于功率合成部分的基础理论知识。

2.3.1　天线的工作原理

由麦克斯韦的电磁场与电磁波理论可知，导体上通过高频振荡电流，其周围会产生电磁场。电磁波传播过程中，电场与磁场循环地进行着转换，传递着信息和能量，并且电场与磁场的方向始终保持垂直。

电磁辐射体辐射出的交变电磁场可以根据空间特性分为两部分：（1）距离天线比较近的部分，由于此部分区域电磁能量不向外辐射，被称作感应场区，也可以叫做近场区或者菲斯涅耳（Fresnel）区；（2）距离天线比较远的部分，电磁场脱离辐射源的束缚向周围空间辐射出去，这部分区域称为辐射场区，也被叫做远场区或者弗朗霍法（Fraunhofer）区。

关于这两个场区的划分有很多种说法，按 Fraunhofer 区的定义，超过远场区距离d_f的区域为远场区。此远场区距离d_f也称作 Fraunhofer 距离，与天线的长度（L）

以及载波波长（λ）有关。Fraunhofer 将其定义为：

$$d_f = 2L^2/\lambda \quad (m) \tag{2.40}$$

其中，L 为天线的最大的物理线性尺寸。此外，d_f还必须满足：

$$d_f \gg L \tag{2.41}$$

和

$$d_f \gg \lambda \tag{2.42}$$

需要指出的是，当天线长度 L 远小于载波波长λ时，辐射场强很微弱。但是，当天线长度几乎和波长相等时，辐射强度将会显著增大。通常，将能产生较大辐射强度的通电直导线称作“振子”。

2.3.2　电基本振子的辐射场

电基本振子，也被叫做电流元，是一段长度极短的通高频均匀电流的直导线。事实上，任意有限长度的线天线均可看成是一系列电基本振子组成的，所以这里首要讨论电基本振子。

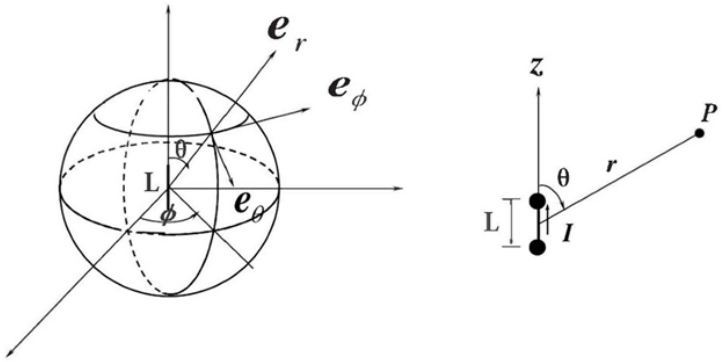


图 2-4 电基本振子电磁场强方向示意图

Figure 2-4 A diagram of electromagnetic field direction of electric basic oscillator

如图 2-4 所示，将一个长度为 L 的线性导体放在球坐标系的中心，如果通上强度为 I 的电流，此线性导体辐射出的电磁场可以表示如下[77-79]：

$$E_r = \frac{ILcos\,\theta}{2\pi\varepsilon_0 c}\{\frac{1}{r^2} + \frac{c}{j\omega_c r^3}\}e^{j\omega_c(t-r/c)} \tag{2.43}$$

$$E_\theta = \frac{ILsin\,\theta}{4\pi\varepsilon_0 c}\{\frac{j\omega_c}{r} + \frac{c}{r^2} + \frac{c^2}{j\omega_c r^3}\}e^{-j\omega_c(t-r/c)} \tag{2.44}$$

$$H_\phi = \frac{ILsin\,\theta}{4\pi c}\left\{\frac{j\omega_c}{r} + \frac{c}{r^2}\right\}e^{j\omega_c\left(t-\frac{r}{c}\right)} \tag{2.45}$$

$$E_\phi = H_r = H_\theta = 0 \tag{2.46}$$

其中，E表示电场强度；H表示磁场强度；下标 r、θ、φ 分别代表球坐标系中的各分量的方向；t为时间；c为光速；ε_0表示自由空间的媒质介电常数，一般取 8.854*10$^{-12}F/m$；ω_c表示载波角频率；r表示目标点与原点之间的距离。

上式（2.43）~（2.46）中，所有的$\frac{1}{r}$，$\frac{1}{r^2}$，$\frac{1}{r^3}$分量分别表示辐射场，感应场以及静电场的成分。在辐射场区，静电场和感应场的成分衰减速度要比辐射场成分快得多。因此，在辐射场区，一般忽略静电场与感应场，只考虑辐射场成分E_θ与H_ϕ。在辐射场区，电场与磁场在空间上相互正交、时间上相位相同，且都垂直于波的传播方向。

另外，由于辐射场区，电场分量$E_r \ll E_\theta$，而磁场分量仅有横向分量H_ϕ，因而辐射场区的波特性与平面波相同，故辐射场区的电磁波近似可以看作横电磁（Transverse Electric and Magnetic Field, TEM）波。

2.4 本章小结

信息论是物理层安全的基础，本章首先介绍了香农信息论基础理论知识，包括信息熵，互信息以及香农容量等基本概念，其中涉及理论知识介绍以及部分相关公式的推导，为后文物理层安全的理论研究做了铺垫。接着，本章从香农信息论引出物理层安全的研究内容。介绍了 Wyner 提出的最基本的窃听信道模型，此模型为物理层安全的研究奠定了的理论基石。本文针对该基础窃听信道模型，结合上文的信息论知识，介绍了安全容量的定义。此定义为物理层安全指明了评价指标，影响至今，本文的最终优化目标也是最大化安全容量。最后，由于本文所研究的内容是基于空间功率合成的物理层安全技术，故而本章介绍了天线以及电磁场等相关基础理论知识，并且推导了远场区电磁波的表达式，为后文做了铺垫。

3 基于空间功率合成的协作干扰方案

3.1 引言

第二章介绍了 Wyner 的基础窃听信道模型，以及由该模型衍生出的其它多种窃听信道模型。Wyner 向世人证明，在不依靠密钥的情况下，也能实现发送端与接收端的安全保密通信。但是有个前提条件：主信道的信道质量比窃听信道的好。本章讨论的主要内容是物理层安全技术中的协作干扰技术，该技术无需上述条件也能保证通信的安全性。

通过第二章的分析可知，安全容量是评价一个通信系统安全性的指标。若想提升安全容量则需：(1)提升合法用户的接收信噪比；(2)降低窃听者的接收信噪比。而协作干扰技术就是利用人工干扰信号来降低窃听者的信噪比，从而实现安全通信的手段。

现有的协作干扰技术往往需要已知窃听者的 CSI 才能进行干扰方案设计。不同于以前的文献，本文研究的内容是基于空间功率合成的协作干扰策略。该策略无需知晓窃听者的 CSI 也能确保信息的安全传输。

本章具体内容如下：首先 3.2 节介绍了系统模型的建立以及问题公式化；3.3 节证明了该问题解存在性；3.4 节则为了使得干扰只在合法接收者处为 0，通过调节干扰器参数，证明了解的唯一性；3.5 节给出了本章所提干扰策略的数值仿真结果；3.6 节对本章进行了总结。

相关的研究内容已经发表于 2017 年的 CCF-C 国际会议 Wireless Algorithms, Systems, and Applications（WASA2017）的论文集中。

3.2 系统网络模型的建立与问题公式化

3.2.1 网络模型

如图 3-1 所示，本文提出了物理层安全方面的一个多干扰器协作防窃听无线网络模型。此无线网络模型包括一个合法发送端（Tx）、一个合法接收端（Rx）、一些窃听者（Eve）以及一些友好的邻居节点（He）。在这个系统区域内，Tx 与 Rx 之间可以相互传递分享私密数据信息。但是在该私密信息传递的过程中，由于无线媒质的广播特性，一些非法的接收者同样也可以接收到。为了防止自己传递的私密信

息被窃听者窃听，Tx 在发送信息之前要从这些候选的邻居节点（He）中选择一个或多个作为友好的干扰者（Jm）。这些被选择的 Jm 在私密信息传输的过程中广播人工噪声信号。该人工噪声信号既要对窃听者造成足够影响，同时又不能影响合法用户的正常接收。

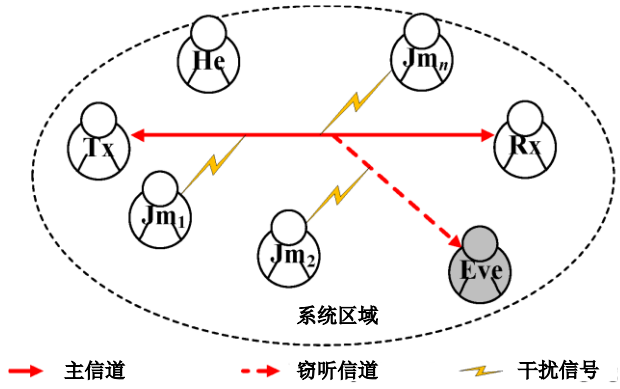


图 3-1 多干扰器协作防窃听模型

Figure 3-1 Illustration of multi-jammer cooperative anti-eavesdropping model

针对此网络模型，本文要达到的目标是，通过空间功率合成理论来引入差异性干扰，从而降低窃听者的 SINR 同时又不影响合法用户的 SINR。换句话说，通过调节不同 Jm_i，$i = 1,2,\ldots,n$发射的干扰信号，使得它们在 Rx 处的合成功率最小，但是在系统范围内的其他位置仍然有一定的干扰效果。如果这样的话，尽管不知道窃听者的 CSI，系统的安全容量也将会得到提升，因为合法用户处收到的干扰比系统范围内其他位置都低的多。

3.2.2 问题公式化

在上述网络模型中，本文仅分析了单用户在自由空间路径损耗模型下进行通信的场景。在以后的工作中，本文作者将会研究多用户以及阴影衰落、多径效应等小尺度衰落等场景。在这些场景下，对于安全性的研究将会涉及幅度和相位补偿等内容。

假设所有节点都是单天线节点，用户之间的通信过程仅考虑大尺度衰落忽略小尺度衰落。根据自由空间路径传播模型以及电磁场与电磁波基础理论[80-82]，经公式推导，n 个 Jm 发射的人工干扰信号在远场区的合成电场强度表达式可以表示如下：

$$E = \sum_{i=1}^{n} \frac{f_i(\theta,\phi) I_i L \eta}{2\lambda r_i} e^{j(\beta r_i + \varphi_i)} e^{j\omega t} \tag{3.1}$$

式中$f_i(\theta,\phi) = \sin\theta$定义为 Jm_i的方向性函数。为了方便阅读，公式（3.1）中其余

符号含义详见表 1。

表 1：公式（3.1）中符号含义

Table1: The meaning of notations in equation (3.1)

符号表示	符号含义
$\boldsymbol{L}$	天线长度
I_i	Jm_i的天线上的电流
φ_i	Jm_i发送的信号初始相位
λ	发送信号波长
r_i	Jm_i与目标点之间的距离
η	无线传播媒介的波阻抗
β	相位常数
ω	传输信号的载波角频率

不失一般性，假设所有节点的天线均具有同样的长度（$L=\frac{\lambda}{4}$），并且所有节点的载波频率都一样。另外，在自由空间中，相位常数$\beta=\frac{2\pi}{\lambda}$，固有波阻抗$\eta \triangleq 120\pi$。仅考虑二维平面模型，即$\theta=\frac{\pi}{2}$，则方向性函数$f_i(\theta,\phi)=\sin\theta=1$。因此，公式（3.1）可以被简化如下：

$$E=\sum_{i=1}^{n} A_i e^{j(\beta r_i+\varphi_i)} e^{j\omega t} \tag{3.2}$$

上式（3.2）中，$A_i \triangleq \frac{15\pi I_i}{r_i}$表示第 i 个干扰信号的幅度。

根据波印亭定理和麦克斯韦方程[83]，合成信号的功率密度可以表示如下：

$$P_r=\frac{1}{2}\mathrm{Re}(\vec{E}\times\vec{H}^{*})=\frac{|E|^2}{2\eta} \tag{3.3}$$

上式（3.3）中，符号Re{·}代表取复数的实部，而[·]*表示共轭变换。另外，$H=\frac{E}{\eta}$表示叠加的磁场强度。

很显然，目标点的合成功率密度和电场强度幅度的平方有如下正比例关系：

$$P_r \propto |E|^2 \tag{3.4}$$

而电场强度的大小与下列因素相关：Jm 的数量 n、每个 Jm 天线上的电流大小I_i、目标点与每个 Jm 的距离r_i、每个 Jm 的初始相位φ_i。因此，为了在未知窃听者的 CSI 情况下提升系统的安全性能，使得合成功率密度P_r在系统范围内的 Rx 处最小，下一步需要分析这些因素对合成功率密度P_r的影响，并证明是否存在一组天线参数解可以使得各个干扰器发射的干扰信号的合成功率密度P_r在 Rx 处最小。

3.3 解的存在性

本小节主要内容在于探究：是否存在一组 Jm 参数可以实现各个 Jm 的合成功率密度在 Rx 处最小（最好为 0，从而使干扰信号对 Rx 没有影响）。很显然，这个目标不能通过一个单天线的 Jm 实现，因此，应先从两个 Jm 的系统进行分析。为了进一步探究公式（3.4）中的正比例关系，本文给出以下定理来分析两个 Jm 的协作干扰系统。

定理 3-1：考虑一个两个协作 Jm 的系统，合成功率密度与两个干扰信号的幅度的平方有如下的正比例关系：

$$P_r \propto A^2 = A_1^2 + A_2^2 + 2A_1A_2\cos(\triangle \phi) \tag{3.5}$$

其中，$\triangle \phi = \varphi_2 - \varphi_1 + \beta(r_2 - r_1)$是相应的相位差。

证明：根据式（3.2），两个协作 Jm 的系统的合成的电场强度可以被表达为：

$$E = \frac{15\pi I_1}{r_1} e^{j(\beta r_1 + \varphi_1)} e^{j\omega t} + \frac{15\pi I_2}{r_2} e^{j(\beta r_2 + \varphi_2)} e^{j\omega t} \tag{3.6}$$

根据欧拉公式，上式（3.6）可以被重新写成实部与虚部的形式，即：

$$E = \mathrm{Re}(E) + j\mathrm{Im}(E) \tag{3.7}$$

其中，$\mathrm{Re}(\cdot)$与$\mathrm{Im}(\cdot)$分别表示取复数的实部和虚部。$\mathrm{Re}(E) = A_1\cos(\omega t + \beta r_1 + \varphi_1) + A_2\cos(\omega t + \beta r_2 + \varphi_2)$，$\mathrm{Im}(E) = A_1\sin(\omega t + \beta r_1 + \varphi_1) + A_2\sin(\omega t + \beta r_2 + \varphi_2)$。

在旋转矢量算法的帮助下，公式（3.7）可以被进一步推导成下面的形式：

$$E = Acos(\omega t + \varphi) + jAsin(\omega t + \varphi) = Ae^{j(wt+\varphi)} \tag{3.8}$$

上式（3.8）中，$A = \sqrt{A_1^2 + A_2^2 + 2A_1A_2\cos(\varphi_2 - \varphi_1 + \beta(r_2 - r_1))}$表示两个干扰信号的叠加幅度。$\varphi = \arctan\frac{A_1\sin(\beta r_1 + \varphi_1) + A_2\sin(\beta r_2 + \varphi_2)}{A_1\cos(\beta r_1 + \varphi_1) + A_2\cos(\beta r_2 + \varphi_2)}$则是相应的叠加相位。

根据公式（3.4）中合成功率密度P_r与合成电场强度幅度的平方$|E|^2$的关系，公式（3.5）得证。**定理 3-1** 证毕。

同样地，通过数学推导，也可以得出这样的结论：多个（两个或两个以上）干扰器场景下，合成功率密度同样也正比于多个干扰信号的叠加幅度的平方。由**定理 3-1** 可知，在 Rx 位置已知的情况下，如何找到合适的 Jm 以及如何给这些选中的 Jm 分配最优的参数（电流和初始相位）是非常关键的问题。

按照前面的描述，多干扰器在 Rx 处的合成功率密度P_r应该是 0。本文给出下列**定理 3-2** 来说明P_r为 0 需满足的条件。

定理 3-2：对于两个 Jm 的协作干扰系统，若两 Jm 的合成功率密度在 Rx 处为 0，则两 Jm 的电流和初始相位应满足以下条件：

$$\text{相位条件：}\quad \triangle\phi = (2k+1)\pi \quad k \in Z \tag{3.9}$$

$$\text{幅度条件：}\quad \frac{I_1}{r_1} = \frac{I_2}{r_2} \tag{3.10}$$

证明：若要P_r=0，则$|E|^2 = 0$，即$A^2 = 0$。

根据公式（3.8），可得：

$$|A_1 - A_2|^2 \leq A^2 = A_1^2 + A_2^2 + 2A_1A_2\cos\left(\varphi_2 - \varphi_1 + \beta(r_2 - r_1)\right) \leq |A_1 + A_2|^2 \tag{3.11}$$

若要上式（3.11）最左侧的等号成立，则：

$$\triangle\phi = (2k+1)\pi \quad k \in Z$$

若要$|A_1 - A_2|^2 = 0$，则：

$$A_1 = A_2 \Leftrightarrow \frac{I_1}{r_1} = \frac{I_2}{r_2}$$

即$A^2 = 0$，则公式（3.9）和公式（3.10）成立。**定理 3-2** 得证。

通过以上的分析，可以得出一组基础解系：

$$\alpha^* = (I_1, I_2, \varphi_1, \varphi_2) = (I_1, \frac{r_2}{r_1}I_1, \varphi_1, \triangle\phi + \varphi_1 + \beta(r_1 - r_2)) \tag{3.12}$$

此基础解系说明，合成的功率密度可以在 Rx 处为 0，只要相应的幅度条件和相位条件满足。至此，解的存在性得证。

3.4 解的唯一性

由上小节 3.3 可知，至少存在一个解，可以使得合成的功率密度在 Rx 处为 0. 但是，在系统范围内是否还存在别的功率密度为零的点（后文简称“零点”）仍然是一个问题。因为为了保证系统的安全性，需要零点只在 Rx 处，防止窃听者在别的零点处窃听。因此，本小节进一步讨论和证明零解的唯一性。

根据**定理 3-2** 中零解的两个存在性条件，联立公式（3.9）和公式（3.10），可以求出合成功率密度为零的目标点与两个 Jm 之间的距离r_1和r_2，需要分别满足下列关系：

$$\begin{cases} r_1 = \frac{(2k+1)\pi + \varphi_1 - \varphi_2}{\beta(I_2 - I_1)} I_1 \\ r_2 = \frac{(2k+1)\pi + \varphi_1 - \varphi_2}{\beta(I_2 - I_1)} I_2 \end{cases} \quad (k \in Z) \tag{3.13}$$

为了更好的理解上式（3.13），本文以两个圆的位置关系来描述，如图 3-2 所

示。假如以两个 Jm 的位置为圆心画两个分别以半径r_1和r_2的圆，则两圆的交点位置即为零点的位置。由图 3-2 可以看到，对于每一个 k 这两个圆都有可能有两个交点，即两个零点（两个相同的交点说明两圆相切，两圆有两个相同的交点）。

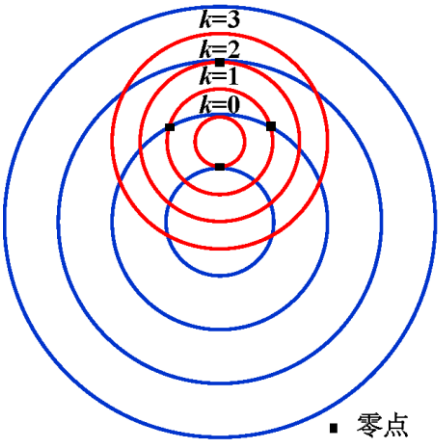


图 3-2 零点位置示意图
Figure 3-2 Diagram of zero points location

从这个角度分析，只需调节参数，使两圆随着 k 的改变有且仅有一个交点即可。接下来，本文将针对 Rx 与 Jm 的不同的位置关系给出相应的分析。

3.4.1 Rx 与两个 Jm 共线情形

在 Rx 与 Jm 共线的情况下，需要进一步分析两种情况：（1）Rx 位于两 Jm 之间；（2）Rx 位于两 Jm 的一侧。其位置关系示意图如下图 3-3 所示。

（a）Rx 位于两 Jm 之间
（a）Rx is located between two Jms

（b）Rx 位于两 Jm 的一侧
（b）Rx is on the outside of two Jms

图 3-3 Rx 与两 Jm 位置关系示意图
Figure 3-3 Schematic diagram of the relationship between Rx and two Jms

假设$d_{i,j}$定义为节点 i 与节点 j 之间的距离，其中，i，$j \in \{Rx, Jm_1, Jm_2\}$。接下来，本文给出如下**定理 3-3** 与**定理 3-4**，来分别阐述这两种不同的共线场景的零解的唯一性。

定理 3-3：假设 Rx 位于两 Jm 之间，对于某一个$k = k^*$，当以两 Jm 所在位置为圆心、r_1和r_2为半径的两圆在 Rx 处外切时，那么两圆随着 k 的改变（增大或减小）不存在其它的交点，当且仅当下列条件成立：

$$\lambda > \lambda_{ext} = d_{Jm_1,Jm_2} + d_{Rx,Jm_1} - d_{Rx,Jm_2} \quad (3.14)$$

其中，$d_{Rx,Jm_2} > d_{Rx,Jm_1}$。

证明：当$k = k^*$两圆外切于 Rx，零解的两个存在性条件（3.9）和（3.10）可以被重新成：

$$I_2^* = \frac{d_{rx,Jm_2}}{d_{rx,Jm_1}} I_1^* \quad 和 \quad \Delta\phi^* = \varphi_2^* - \varphi_1^* + \beta(d_{Rx,Jm_2} - d_{Rx,Jm_1}) = (2k^* + 1)\pi$$

如图 3-2 所示，当两圆外切时，随着 k 的减小两圆将会相离，即没有交点（根据公式（3.13），两圆的半径减小了）。

此外，当 k 增大时，如果两圆的半径之差大于圆心距，两圆将会出现内含关系，即两圆也不会有交点。因此，要使 k 增大时，两圆也不存在交点，只需要当$k = k^* + 1$，$\triangle\phi = (2k^* + 3)\pi$时，两圆半径$r_1$和$r_2$之差满足以下关系：

$$|r_2 - r_1| = r_2 - r_1 = \frac{2\pi}{\beta} + (d_{Rx,Jm_2} - d_{Rx,Jm_1}) > d_{Jm_1,Jm_2} \quad (3.15)$$

上式（3.15）中，$r_2 > r_1$是由于$d_{Rx,Jm_2} > d_{Rx,Jm_1}$。

因此，（3.14）可由（3.15）经推导而来。**定理 3-3** 证毕。

定理 3-4：假设 Rx 位于两 Jm 的一侧，对于某一个$k = k^*$，当以两 Jm 所在位置为圆心、r_1和r_2为半径的两圆在 Rx 处内切时，那么两圆随着 k 的改变（增大或减小）不存在其它的交点，当且仅当下列条件成立：

$$\lambda > \lambda_{int} = d_{Rx,Jm_2} - d_{Rx,Jm_1} - \frac{I_2 - I_1}{I_1 + I_2} d_{Jm_1,Jm_2} \quad (3.16)$$

其中，$d_{Rx,Jm_2} > d_{Rx,Jm_1}$。

证明：与**定理 3-3** 的证明类似，当$k = k^*$两圆内切于 Rx，Rx 与两 Jm 的距离有如下关系：

$$d_{Rx,Jm_2} - d_{Rx,Jm_1} = d_{Jm_1,Jm_2}$$

当 k 增大时，由于两个圆的半径均增大，但是$r_2 > r_1$（由于$d_{Rx,Jm_2} > d_{Rx,Jm_1}$），$r_2$增大的速度比$r_1$更快。随着两圆半径的增大，最终以半径为$r_2$的大圆将会内含半径为$r_1$的小圆。

此外，当 k 减小时，如果两圆的半径之和小于圆心距，两圆将会出现相离现象，即两圆也不会有交点。因此，要使 k 减小时，两圆也不存在交点，只需要当$k = k^* - 1$，$\triangle\phi = (2k^* - 1)\pi$时，两圆半径$r_1$和$r_2$之和满足以下关系：

$$r_1 + r_2 = \frac{(2k-1)\pi + \varphi_1 - \varphi_2}{\beta} \frac{I_1 + I_2}{I_2 - I_1} < d_{Jm_1,Jm_2} \quad (3.17)$$

然后，经进一步推导可得公式（3.16）。**定理 3-4** 证毕。

综上所述，当 Rx 与两 Jm 共线时，零解的唯一性可以得到保证，只要在满足幅度和相位条件的同时，给予波长不同的限制条件。

3.4.2 Rx 与两个 Jm 不共线情形

对于 Rx 与两 Jm 不共线的场景，由于两圆不可能相切在 Rx，故而零解的唯一性不能被保证。但是，可以保证系统范围内，两圆有且仅有两个交点，如下面的定理 3-5 所述。

定理 3-5：在 Rx 与两 Jm 不共线且两 Jm 的参数满足**定理 3-2** 的情况下，当半径分别为r_1和r_2的两圆相交于 Rx 处时，随着 k 的变化（增大或者减小），两圆不存在其它的交点，当且仅当下面的条件成立：

$$\lambda > max(\lambda_{ext}, \lambda_{int}) \tag{3.18}$$

证明：根据**定理 3-3** 和**定理 3-4**，随着 k 的增大，两圆不再有交点当且仅当公式（3.14）成立；而随着 k 的减小，两圆也不会相交当且仅当公式（3.16）成立。因此，波长（λ） 应该同时满足公式（3.14）和（3.16），即λ应大于λ_{ext}，λ_{int}中的最大的一个。**定理 3-5** 得证。

根据**定理 3-5**，如果想要实现在 Rx 处有唯一的零点，则需要另外选择一对 Jm，使它们同样满足**定理 3-5** 的条件。另外，还需要这两组 Jm 只在 Rx 处有唯一一个相同的交点。因此，当 Rx 与两 Jm 不共线，通过两组 Jm（四个 Jm），零点的唯一性同样可以得到保证。

3.4.3 特殊情形

本小节讨论一种上述两种情形的特殊情况，Rx 位于两 Jm 的垂直平分线上，即$d_{Rx,Jm_1} = d_{Rx,Jm_2}$。在这种情况下，只要**定理 3-2** 的两个条件满足，Rx 处的合成功率密度就为 0。

但是，除了 Rx 之外，整条垂直平分线上的点处的合成功率密度均为 0。为了实现在 Rx 处有唯一零点的目的，同样可以采取上一小节的方法，考虑使用两组 Jm，即四个 Jm。如果这样，唯一零点就是两条垂直平分线的交点（即 Rx 位于两条垂直平分线的交点上）。值得注意的是，这两条垂直平分线不能平行，否则也得不到唯一零点。

另外，可以选择一组非垂直平分线的 Jm 使其满足**定理 3-5**，且有一个交点在 Rx 处。也就是说，这两组 Jm 在 Rx 处有且仅有一个相同的零点。这样也可以实现

唯一零解的目的。

3.4.4 其它情形

由上面的分析可知，零解的唯一性可以通过两个 Jm（或者两组 Jm）来保证。但是，还有别的情况可以实现唯一的零解的目的。比如三个 Jm 的协作干扰系统，同样可以根据旋转矢量算法得到唯一零解。这里，本文直接给出这种情况下的相应的结论，如下：

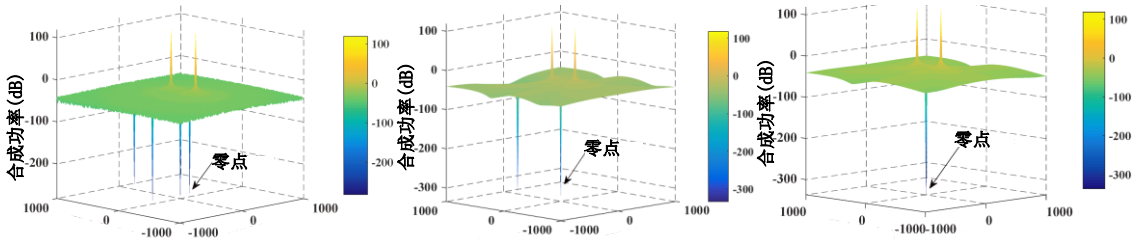
$$\begin{cases} A_3^2 = A_1^2 + A_2^2 + 2A_1A_2\cos\varphi_{2,1} \\ \varphi_3 + \beta d_{Rx,Jm_3} - \varphi = (2k+1)\pi \end{cases} \tag{3.19}$$

其中，$\varphi = \arctan\frac{A_1\sin(\beta d_{Rx,Jm_1}+\varphi_1)+A_2\sin(\beta d_{Rx,Jm_2}+\varphi_2)}{A_1\cos(\beta d_{Rx,Jm_1}+\varphi_1)+A_2\cos(\beta d_{Rx,Jm_2}+\varphi_2)}$，$\varphi_{2,1} = \varphi_2 - \varphi_1 + \beta\left(d_{Rx,Jm_2} - d_{Rx,Jm_1}\right)$。$d_{Rx,Jm_3}$定义为 Rx 与 Jm_3之间的距离。

只要上述关系式可以被满足，就可以实现在 Rx 处有唯一零解。其他情况下，相似的结论也可以被推导出来，这里本文省略了。而且，用不超过四个 Jm 就可以实现唯一零点的目标，没有必要考虑更多协作干扰器的方案。

3.5 数值仿真分析

本小节以数值仿真的形式讨论不同场景下，Jm 的各参数对合成功率的影响。所有节点（包括合法用户和窃听者）坐落于一个限定的区域内（2000*2000 m^2）。其中，窃听者位置未知，其位置可以是除了合法节点外的系统内任何一点。对于前面讨论过的场景，本小节给出了相应的三维功率热图。系统区域内每一点的功率大小可以通过颜色分辨，而且零点位置用箭头标出。



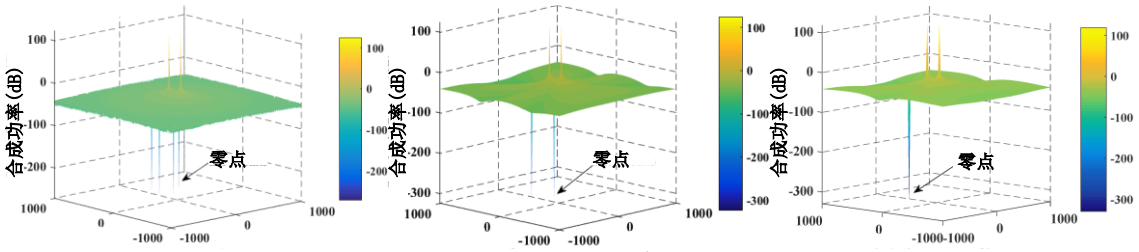
(a) $\lambda = 0.2, \varphi_1 = 999\pi, \varphi_2 = 0$ (b) $\lambda = 300, \varphi_1 = 0, \varphi_2 = \frac{\pi}{3}$ (c) $\lambda = 400, \varphi_1 = 0, \varphi_2 = \frac{\pi}{2}$

图 3-4 Rx 位于两 Jm 之间情况下不同波长对合成功率的影响

Figure 3-4 The effect of different λ on Synthetic jamming power when Rx is between two Jms

首先，Rx 位于两 Jm 之间但不在两 Jm 的垂直平分线上的场景下，不同波长的干扰信号经过合成后，系统范围内各点的合成功率如图 3-4 所示。仿真参数设置如

下：Rx、Jm_1、Jm_2的坐标分别为（0, 0）、（0, 150）、（0, -250）。另外，$I_1 = 3A$，$I_2 = 5A$。由图 3-4（a）可看出，当 Jm 发出的信号波长不满足公式（3.14）时，两 Jm 的合成功率为 0 的点是四个；当波长到达临界条件时，零点变成了两个，如图 3-4（b）；而当波长满足公式（3.14）时，有且仅有一个零点在 Rx 处。此现象证明了**定理 3-3** 的正确性。



(a) $\lambda = 0.2, \varphi_1 = 1999\pi, \varphi_2 = 0$ (b) $\lambda = 150, \varphi_1 = \frac{5}{3}\pi, \varphi_2 = 0$ (c) $\lambda = 200, \varphi_1 = \pi, \varphi_2 = 0$

图 3-5 Rx 位于两 Jm 一侧的情况下不同波长对合成功率的影响

Figure 3-5 The effect of different λ on synthetic jamming power when Rx is on one side of two Jms

相似地，当 Rx 位于两 Jm 的一侧但不位于它们的垂直平分线上时，两 Jm 的波长对合成信号功率的影响如图 3-5 所示。其仿真参数设置如下：Rx、Jm_1、Jm_2的坐标分别为（0, 450）、（0, 150）、（0, -50）。另外，$I_1 = 3A$，$I_2 = 5A$。同样，由图 3-5 可以看出当 Jm 的波长满足公式（3.16）的条件时，也可以实现仅有一个零点在 Rx 处的目的。

尽管两个 Jm 的系统可以实现本文想要的干扰效果，但是却存在着难以解决的问题：在某些场景下，信号的波长要求的条件可能过于苛刻，以至于在设计天线时遇到很大的难度。另一方面来讲，根据第二章所介绍的远场区的概念，即$r_i > d_f$（此处参见第二章公式（2.40）~（2.42））。而$d_f > \lambda$，如果按照如图 3-4（c）中的波长（$\lambda = 400m$）来计算，近场区的范围过大，这么大的范围无法按照前面所推公式进行计算和分析，则无法保证近场区的安全性。因此，三个 Jm 或者四个 Jm 的协作干扰系统应更加受到关注。

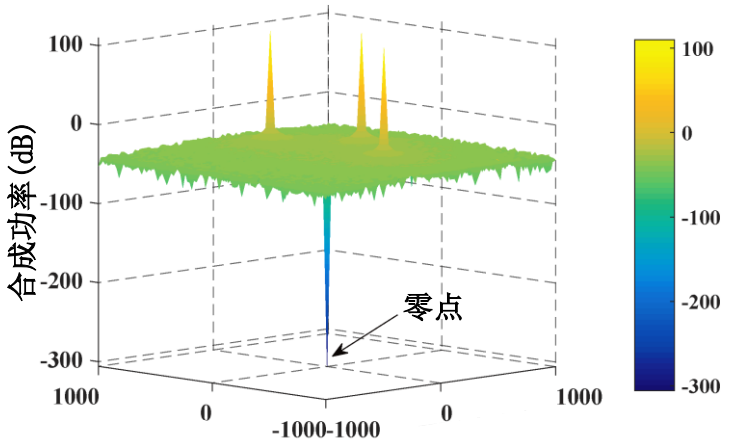


图 3-6 三个 Jm 的系统的合成干扰功率示意图

Figure 3-6 Synthetic jamming power of three jammers distribution diagram

如图3-6所示，为三个Jm的协作干扰系统的合成功率在系统范围内的示意图。仿真参数设置如下：Rx、Jm_1、Jm_2以及Jm_3的坐标分别为（0, 0）、（0, 500）、（0, -500）、（300,0）。另外，$\lambda = 0.3m$，$I_1 = I_2 = 3$A。图 3-6 证明了，只要三个 Jm 的参数满足公式（3.19），就可以实现系统范围内只有一个零点在 Rx 处。

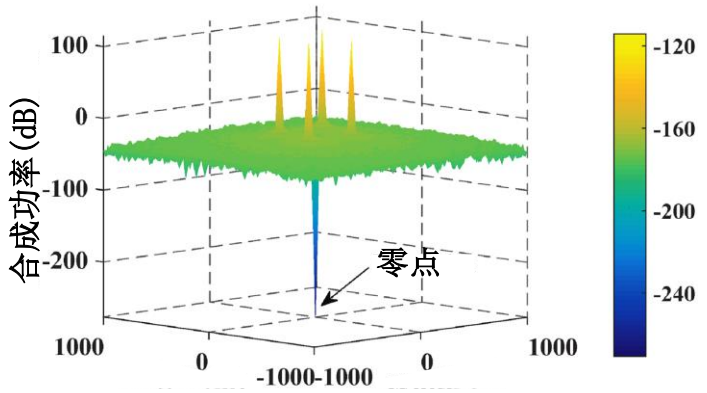


图 3-7 四个 Jm 的系统的合成干扰功率示意图
Figure 3-7 Synthetic jamming power of four jammers distribution diagram

图 3-7 则揭示了四个 Jm 的协作干扰系统的情况，其中 Rx 与四个 Jm 均不共线，且不位于任意两个 Jm 的垂直平分线上。其仿真参数设置如下：Rx、Jm_1、Jm_2、Jm_3以及Jm_4的坐标分别为（0, 0）、（144, -192）、（-256, -192）、（-144, 192）、（256, 192）。另外，$\lambda = 0.4m$，$I_1 = I_3 = 3$A，$I_4 = I_2 = 4$A，$\varphi_1 = \varphi_3 = 0$，$\varphi_2 = \varphi_4 = \pi$。如图 3-7 所示，通过调节两对 Jm（四个 Jm）的参数同样可以得到在 Rx 处的唯一零点。

由以上仿真分析可知，通过调节 Jm 的天线参数，可以实现多个 Jm 发射的干扰信号的合成功率在 Rx 处为 0，而在系统范围内的其它区域不为 0 的目的。此仿真结果也表明，本文所提的基于空间功率合成的协作干扰方案的可行性以及有效性。在窃听者 CSI 未知的情况下，通过本文所提协作干扰方案依然可以实现信息的安全传输。

3.6 本章小结

在这一章，本文提出了一种新奇的协作干扰方案来实现安全通信。首先，本章第一小节先介绍了，协作干扰的研究现状以及存在的问题，同时也揭示了本文的创新点以及研究意义所在。接着第二小节建立了本文的协作干扰网络模型，并对本文研究的问题进行了公式化建模，提出了所要解决的优化问题。第三小节则根据第二小节所提出的问题进行求解，经过理论及数学公式推导证明了所求问题解的存在

性，即至少存在一组解可以使得各个 Jm 的合成功率在 Rx 处为 0。然后，为了使零解有且仅有一个在 Rx 处，而系统内别的位置不存在零解，第四小节对各 Jm 的参数进行了进一步分析。分析了 Rx 与 Jm 的各种不同位置关系的解的情况，证明了通过调节 Jm 的参数，可以实现零解的唯一性。最后，为了验证理论推导的正确性，本章第五小节给出了，第四小节中的各种情况下的数值仿真分析结果。数值分析结果表明，通过调节不同 Jm 的参数，可以实现不同场景下的零解的唯一性。通过本章节的内容可知，本文可以在未知窃听者 CSI 情况下，实现系统的安全传输。第六小节对本章内容进行了概括总结。

4 最差可达安全速率优化方案

上一章本文提出了不同场景下的协作干扰方案，从理论上分析，这些协作干扰方案可以提升系统的安全性能。但是，并未给出性能提升的定量分析，而且如果对干扰器以及 Tx 的功率进行优化的话，系统性能还能进一步提升。因此，本章根据上一章提出的协作干扰方案，提出了最差情况下的功率分配优化方案，以期探讨并进一步提升系统的安全性能。

本章具体内容如下：4.1 小节根据上一章的协作干扰方案提出了功率优化问题，并对该问题进行了公式化，建立了优化方程；4.2 小节针对给定功率分配情况下，提出了一种搜索算法，此搜索算法可以找到系统范围内最差的窃听者位置（安全容量最低的位置）；4.3 小节首先证明了上一小节搜索到的最差位置与功率分配无关，进而基于找到的最差位置，本小节在全局功率受限的情况下，提出了一种功率分配方案；4.4 小节对本章所提算法、方案进行了数值仿真分析；4.5 小节对本章进行了总结。

相关的研究内容已经发表于 SCI 期刊 IEEE Access 中。

4.1 功率分配问题及其公式化

本小节根据上一章所提协作干扰策略，提出了一个优化问题。该优化问题，旨在提升系统安全速率来对抗最差情况的窃听者（系统范围内对合法用户的安全性威胁最大的窃听者）。由于窃听者位置未知，故而系统范围内窃听者能获得的容量最大的位置，即为最差窃听者位置。针对该最差窃听者位置，本小节建立了最差可达安全速率优化方程。

具体来讲，首先分别定义P_{Tx}和P_{Jm_i}，$i \in \{1,2,\ldots,n\}$作为合法发送端 Tx 和第 i 个协作干扰者 Jm_i的传输信号功率。另外，系统内所有发射信号的发射总功率有一个上限P^{max}。如此，每个发射端节点的发射功率的可行域可以被定义如下：

$$\mathbb{P} = \{0 \le P_{Tx} + \sum_{i=1}^{n} P_{Jm_i} \le P^{max}\} \tag{4.1}$$

根据**定理 3-1**，系统对功率的限制其实是对电流的限制，故而（4.1）可以转化如下：

$$\mathbb{I} = \{0 \le I_{Tx}^2 + \sum_{i=1}^{n} I_{Jm_i}^2 \le I_{max}^2\} \tag{4.2}$$

其中，I_{Tx}和I_{Jm_i}，$i \in \{1,2,\ldots,n\}$分别表示 Tx 与Jm_i的天线上的电流，I_{max}表示最大

电流之和的上限。

于是，最差情况可达安全速率优化问题可以被公式化如下：

$$\mathbf{P1:}\ \max_{\mathbb{J}\in\mathbb{JM}}\ \max_{I_{Tx},I_{Jm_i}}\ \min_{e\in\mathbb{E}} C_{\mathbb{J},e}(I_{Tx},I_{Jm_1},\ldots,I_{Jm_n}) \tag{4.3}$$

其中，$\mathbb{JM}$表示所有协作节点的候选集，而$\mathbb{J}$表示被选中的协作干扰节点的集合。$\mathbb{E}$定义为所有窃听者的集合，而 e 表示最差的窃听者的指示标号。

此优化问题是非凸非线性的，以至于难以处理。本文的研究重点不在于协作干扰节点的选择问题，一旦得到下面选定的协作干扰节点的优化问题 **P2** 的解，则 **P1** 的求解则会变得容易得多。假设已通过第三章选定了 Jm，则本文重点关注的优化问题 **P2** 可以被描述如下：

$$\mathbf{P2:}\ \max_{I_{Tx},I_{Jm_i}}\ \min_{e\in\mathbb{E}} C_{\mathbb{J},e}(I_{Tx},I_{Jm_1},\ldots,I_{Jm_n}) \tag{4.4}$$

但是，**P2** 仍然是个非凸的优化问题。为了求解 **P2**，本文将其分解成两个易于处理的子优化问题，然后最终给出它们的联合解。

4.2 特定功率分配下的最低安全速率

本小节研究两个 Jm 的协作干扰系统的可达安全速率，其它情景的分析类似。考虑到窃听者的位置未知，本文首先在功率分配方案确定的情况下，寻找全系统范围内窃听者有可能处在的最差位置，以最差窃听者位置的安全速率为系统的最低可达安全速率，称作最差可达安全速率。

对于两个 Jm 的系统来说，其安全速率可以被表示为：

$$C(x_{Ev},y_{Ev}) \triangleq \log_2(1+SINR_r) - \log_2(1+SINR_e) \tag{4.5}$$

上式中，$SINR_r \triangleq \frac{A_{Tx,Rx}^2}{2\eta\sigma_R^2}$和$SINR_e \triangleq \frac{A_{Tx,Ev}^2}{B_{Jm}+2\eta\sigma_E^2}$分别表示 Rx 与 Eve 处的 SINR。

其中，

$$B_{Jm} \triangleq A_{Jm_1,Ev}^2 + A_{Jm_2,Ev}^2 + 2A_{Jm_1,Ev}A_{Jm_2,Ev}\cos(\varphi_{Jm_2,Jm_1})$$

$$A_{i,j} = \frac{15\pi I_i}{d_{i,j}}, \quad i,\ j \in \{Tx,Rx,Jm_1,Jm_2\}$$

$$\varphi_{Jm_2,Jm_1} = \varphi_{Jm_2} - \varphi_{Jm_1} + \beta(d_{Jm_2,Ev} - d_{Jm_1,Ev})$$

另外，σ_R^2与σ_E^2分别表示在 Rx 与 Eve 处的 AWGN 信号功率。

假设 Tx，Rx 位置已知，且已选好了 Jm，即 Jm 的位置也已知。在给定功率分配下，各发射端的电流也已知且不再变化。则寻找最差窃听者的位置的优化方程，相当于问题 **P2** 的子优化问题，其可以被描述如下：

$$\textbf{P3: } \min_{e\in\mathbb{E}} C(x_{Ev}, y_{Ev}) \tag{4.6}$$

其中，(x_i, y_i)表示节点i，$i \in \{Tx, Rx, Jm_1, \cdots, Jm_n\}$的二维坐标。

考虑一个半径为 R 的圆形系统区域，则 Eve 可能坐落的位置的可行集可以被定义如下：

$$\mathbb{E} = \begin{Bmatrix} x_{Ev}^2 + y_{Ev}^2 \le R^2 \\ d_{Jm_1,Ev} \ge d_{min} \\ d_{Jm_2,Ev} \ge d_{min} \\ d_{Tx,Ev} \ge d_{min} \\ d_{Rx,Ev} \ge d_{min} \end{Bmatrix} \tag{4.7}$$

其中，d_{min}定义为 Eve 与合法用户的应保持的最小距离。一般来讲，窃听者为了避免被发现，都不会离合法用户很近。

因此，问题 **P3** 可以转化为如下形式：

$$\textbf{P4: } \min_{(x_{Ev},y_{Ev})\in\mathbb{E}} C(x_{Ev}, y_{Ev}) \tag{4.8}$$

问题 **P4** 实际上是一个在搜索域（4.7）寻最小值的点的优化问题。显然，该问题，仍然不是一个凸优化问题。尽管一些强搜索算法可以找到最优解或者次优解，但是由于搜索域（4.7）的存在，会造成解空间的非连续性。因此，为了减轻搜索复杂度，接下来本文提出了一种缩小搜索空间的方法。

4.2.1 一种缩小搜索空间的方法

为了更好地解决问题 **P4**，本文提出了一种方法，可以缩小解空间的搜索范围的方法。此种方法，可以减轻搜索时间复杂度，而且没有性能损失，即对最优解不造成影响。本文用**定理 4-1** 来描述该方法，如下：

定理 4-1：问题 **P4** 的最优解（x_{Ev}^*, y_{Ev}^*）在如图 4-1 的红色区域内。在图 4-1 中，L_{Tx,Jm_1}和L_{Tx,Jm_2}分别代表过 Tx 与两 Jm 的两条直线，即：

$$\begin{aligned} L_{Tx,Jm_1}&: y = k_{Tx,Jm_1}(x - x_{Tx}) + y_{Tx} \\ L_{Tx,Jm_2}&: y = k_{Tx,Jm_2}(x - x_{Tx}) + y_{Tx} \end{aligned} \tag{4.9}$$

其中，$k_{Tx,Jm_1} = \frac{y_{Jm_1} - y_{Tx}}{x_{Jm_1} - x_{Tx}}$，$k_{Tx,Jm_2} = \frac{y_{Jm_2} - y_{Tx}}{x_{Jm_2} - x_{Tx}}$。

证明：一旦合法用户的位置，以及 Tx 的发射功率已经确定，则系统的安全速率只与窃听者的 SINR 有关。窃听者的 SINR 越高，则系统的安全性能越差。一般来讲，窃听者为了获得更高的接收 SINR，它会尽可能地离 Tx 近一点，而离两个 Jm 远一些。考虑一个以 Tx 为圆心的系统区域，如图 4-1 所示。如果以 Tx 为圆心

在上述圆形区域内画无数个圆，则对于任意一个圆上的点来讲（例如圆 *A-Tx-B*），圆与直线L_{Tx,Jm_1}的交点 *A* 就是接收到来自 Jm_1的干扰信号强度最小的位置。换句话说，对于整个圆 *A-Tx-B* 上的点，它们收到来自 Tx 发来的信号的强度都一样，但是 *A* 点受到的干扰最小，故而 A 点就是相对于 Jm_1而言的整个圆 *A-Tx-B* 上的最差窃听者的位置。同理，*B* 点则是相对于 Jm_2而言的整个圆 *A-Tx-B* 上的最差窃听者的位置.那么，如果是两个 Jm 同时作用的话，最差窃听者位置一定在圆弧 AB 上。故而，所有的最差窃听者的位置应该是位于所有的以 Tx 为圆心的圆的圆弧上，即如图 4-1 所示的两条直线L_{Tx,Jm_1}和L_{Tx,Jm_2}之间的红色区域。**定理 4-1** 证明完毕。

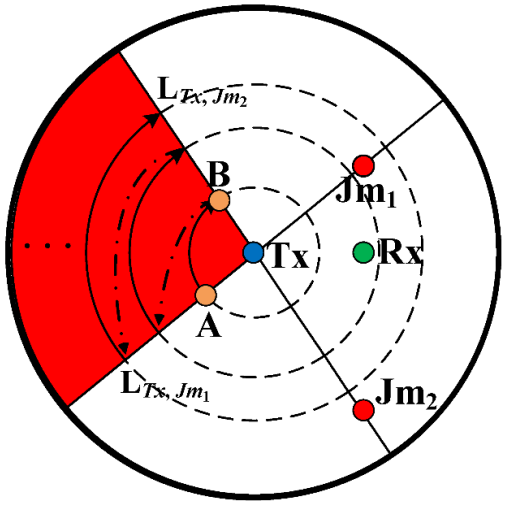


图 4-1 缩小的搜索区域及搜索路径示意图
Figure 4-1 Diagram of the narrowed research area and the research path

根据**定理 4-1**，缩小的区域的边界可以被定义如下：

$$\mathbb{EE}=\begin{Bmatrix} x_{Ev}^2+y_{Ev}^2\le R^2 \\ d_{Tx,Ev}\ge d_{min} \\ k_{Tx,Jm_1}(x-x_{Tx})+y_{Tx}\ge y_{Ev} \\ k_{Tx,Jm_2}(x-x_{Tx})+y_{Tx}\le y_{Ev} \end{Bmatrix} \tag{4.10}$$

很显然，上述区域比公式（4.7）给出的范围小得多，从而计算复杂度也要降低很多。

4.2.2 一种波浪形之字搜索算法

为了快速找到问题 **P4** 的最优解，在缩小的搜索区域的基础上，本小节提出一种波浪形之字搜索算法，算法的搜索路径如图 4-1 所示。图中，箭头方向为算法搜索方向。

根据几何关系，图 4-1 中 *A* 点与 *B* 点的坐标可以被计算出，如下：

$$(x_A, y_A) = (\frac{y_A - y_{Tx}}{k_{Tx,Jm_1}} + x_{Tx}, y_{Tx} - \frac{rk_{Tx,Jm_1}}{\sqrt{k_{Tx,Jm_1}^2 + 1}})$$

$$(x_B, y_B) = (x_{Tx} - \frac{y_B - y_{Tx}}{k_{Tx,Jm_2}}, y_{Tx} - \frac{rk_{Tx,Jm_2}}{\sqrt{k_{Tx,Jm_2}^2 + 1}})$$

其中，$d_{min} \le r \le R$。r 为以 Tx 为圆心的圆的半径。

显然，对于每一个 r，问题 **P4** 仅有一个优化变量y_{Ev}。因此，问题 **P4** 可以被转化为问题 **P5**，如下：

$$\textbf{P5:} \min_{\substack{y_A \le y_{Ev} \le y_B \\ d_{min} \le r \le R}} C(r, y_{Ev}) \qquad (4.11)$$

接下来，本文将利用之字形搜索算法，在减小的可行域内来寻找问题 **P5** 的可行解。该方法旨在对每一个 r 进行遍历搜索，直到找到可行解。设计的具体方法总结成伪代码如下表 2 所示：

表 2：波浪形之字搜索算法

Table 2: A wavy zigzag search algorithm

算法 4-1 波浪形之字搜索算法

输入：

搜索最大半径 R；

窃听者与合法用户应保持的最短距离d_{min}；

初始搜索位置的纵坐标$y_{Ev} = y_A$；

初始的搜索半径 r；

搜索半径间隔Δr。

输出：

最优解(r^*, y_{Ev}^*)。

步骤：

1. 初始化$r^* = r$，和$y_{Ev}^* = y_{Ev}$；

2. 根据公式（4.11），计算$C(r^*, y_{Ev}^*)$；

3. **While** $r \le R$ **do**

4. 根据 r 更新y_A和y_B；

5. 重新设置$y_{Ev} = y_A$；

（表 2 续表）

算法 4-1 波浪形之字搜索算法

6. 在搜索区域$y_A \le y_{Ev} \le y_B$上，通过一维搜索算法解决问题 **P5**，从而得到可行解$(r, y_{Ev}^{(r)})$；

7. 计算差值：$\Delta C = C(r^*, y_{Ev}^*) - C(r, y_{Ev}^{(r)})$；

8. **If** $\Delta C < 0$ **then**

9. 令$(r^*, y_{Ev}^*) = (r, y_{Ev}^{(r)})$；

10. **End if**

11. 设置$r = r + \Delta r$。

12. **End while**

13. **Return** (r^*, y_{Ev}^*)

备注 1：最差的窃听者的位置(x_{Ev}^*, y_{Ev}^*)可以由几何关系以及上述**算法 4-1** 得到的(r^*, y_{Ev}^*)计算而来。

备注 2：算法 4-1 的计算复杂度取决于搜索半径间隔Δr，随着Δr的减小，计算复杂度也会增大，但是计算的精确度却提高了。在实际应用中，可以适当的牺牲准确度来提高计算的效率，从而满足某些硬件设备的限制。

4.3 最差情况下的功率分配方案

在上一小节，本文在固定功率分配的情况下，通过搜索算法找到了系统范围内的最差窃听者的位置。但是，随着功率的改变，该最差窃听者的位置是否会发生变化仍然是一个问题。因此，本小节首先证明了最差窃听者的位置不随功率分配的改变而变化，如下面的**定理 4-2** 所述。然后，针对找到的最差窃听者位置，本文提出了一个功率分配方案，以期进一步提升系统安全速率。

定理 4-2：当仅考虑窃听者的信干比（Signal-to-Interference-Ratio, SIR），即忽略 AWGN 功率σ_E^2的情况下，对于不同的功率分配，系统内最差窃听者的位置始终不变。

证明：一旦 Rx 处的合成干扰功率被消除掉，则**定理 3-2** 中的两个条件被满足。于是，可以得到：

$$I_{Jm_2} = \frac{d_{Rx,Jm_2}}{d_{Rx,Jm_1}} I_{Jm_1} \tag{4.12}$$

将公式（4.12）带入问题 **P3**，则 **P3** 的优化方程的目标函数可以被转换化为如下形式：

$$C\left(X, I_{Tx}, I_{Jm_1}, I_{Jm_2}\right) = \log_2\left(1+\frac{A_{Tx,Rx}^2}{2\eta\sigma_R^2}\right) - \log_2\left(1+\frac{225\pi^2 I_{Tx}^2}{225\pi^2 I_{Jm_1}^2 X(x_{Ev}, y_{Ev}) + 2d_{Tx,Ev}^2\eta\sigma_E^2}\right)$$

其中，

$$X(x_{Ev}, y_{Ev}) = \frac{d_{Tx,Ev}^2}{d_{Jm_1,Ev}^2} + \frac{d_{Tx,Ev}^2 d_{Jm_2,Rx}^2}{d_{Jm_2,Ev}^2 d_{Jm_1,Rx}^2} + \frac{d_{Tx,Ev}^2 d_{2Jm_2,Rx}}{d_{Jm_1,Rx} d_{Jm_1,Ev} d_{Jm_2,Ev}} \cos\varphi_{Jm_2,Jm_1}$$

一般来讲，σ_E^2相当的小几乎可以忽略。当$\sigma_E^2 \approx 0$时，$C(X, I_{Tx}, I_{Jm_1}, I_{Jm_2})$是关于$X(x_{Ev}, y_{Ev})$的单调递增函数。因此，最差窃听者的位置不随功率分配的变化而改变，即$(I_{Tx}, I_{Jm_1}, I_{Jm_2})$的变化不会影响$X(x_{Ev}, y_{Ev})$，两者相互独立。**定理 4-2** 证毕。

根据**定理 4-2**，由**算法 4-1** 计算而来的最差窃听者的位置就可以被看作是系统的安全性最低的位置。此位置的安全速率即是系统的最低可达安全速率，如果此位置的安全速率可以到达系统要求的安全标准的话，则此通信系统就可以被看作是一个“绝对安全”的通信系统。故而优化此位置的安全速率是重中之重。本文将为该位置提出一种功率优化方案，来提升系统的可达安全速率。

在确定了最差窃听者位置之后，此功率优化问题相当于问题 **P2** 的另一个子优化问题，可以被描述如下：

$$\textbf{P6:} \quad \max_{I_{Tx}, I_{Jm_1}, I_{Jm_2}} \quad C\left(I_{Tx}, I_{Jm_1}, I_{Jm_2}\right) \qquad \text{s.t.} \quad I_{Tx}^2 + I_{Jm_1}^2 + I_{Jm_2}^2 \le I_{max}^2 \tag{4.13}$$

优化问题 **P6** 同样也是一个非凸的问题，本文将讨论两种算法来求解该问题：启发式模拟退火算法（Heuristic Simulated Annealing Algorithm，HSA）和一维搜索算法（One-Dimensional Search, 1-D Search）。

4.3.1 基于模拟退火算法的直接求解算法

为了求解非凸的优化问题，在公式（4.2）所描述的搜索域$(I_{Tx}, I_{Jm_1}, I_{Jm_2})$中运用一些强搜索算法可以得到该问题的最优或次优解。这里，我们讨论一种基于模拟退火算法的解法。

模拟退火算法是一种启发式随机搜索算法。此种算法核心思想是利用蒙特卡洛（Monte-Carlo）迭代进行最优化问题的求解，其具体的原理介绍，参见文献[84]。

本文基于模拟退火算法设计的求解方法的流程简要概括如下：

第一步：设置满足公式（4.2）所描述的搜索域的初始解的值（$I_{Tx}^0, I_{Jm_1}^0, I_{Jm_2}^0$），并且计算问题 **P6** 的目标函数的值；

第二步：在（$I_{Tx}^0, I_{Jm_1}^0, I_{Jm_2}^0$）附近产生随机扰动的新的解，然后重新计算问题 **P6** 的目标函数值；

第三步：如果新的目标函数值比初始解的目标函数值大，则用新产生的扰动解代替初始解。否则，则以某种概率接受新的扰动解；

第四步：重复步骤二和步骤三，直到找到最优解或者达到最大迭代次数。

具体的解法的伪代码如下面的**算法 4-2** 所示：

表 3：启发式模拟退火算法

Table 3: Heuristic simulated annealing algorithm

算法 4-2：启发式模拟退火算法

输入：

设定初始解（$I_{Tx}^0, I_{Jm_1}^0, I_{Jm_2}^0$）；

定义初始温度t_0和最终温度t_{min}；

定义冷却系数ρ，$0 < \rho < 1$；

定义当前温度 *t*；

设定每个 *t* 值的迭代次数 *m* 和最大迭代次数m_{max}；

设定总的最大迭代次数l。

输出：

最优解$(I_{Tx}^*, I_{Jm_1}^*, I_{Jm_2}^*)$。

步骤：

1. 初始化$m = 0$，$t = t_0$；

2. **While** $t > t_{min}$ **or** $i \le l$

3. 在（$I_{Tx}^{i-1}, I_{Jm_1}^{i-1}, I_{Jm_2}^{i-1}$）附近随机扰动产生新的解（$I_{Tx}^{i}, I_{Jm_1}^{i}, I_{Jm_2}^{i}$）；

4. 计算两次目标函数的差值：$\Delta C = C(I_{Tx}^{i-1}, I_{Jm_1}^{i-1}, I_{Jm_2}^{i-1}) - C(I_{Tx}^{i}, I_{Jm_1}^{i}, I_{Jm_2}^{i})$；

5. **If** $\Delta C < 0$ **then**

6. 令$(I_{Tx}^{i-1}, I_{Jm_1}^{i-1}, I_{Jm_2}^{i-1}) = (I_{Tx}^{i}, I_{Jm_1}^{i}, I_{Jm_2}^{i})$；

7. $m = 0$；

8. **Else**

（表 3 续表）

算法 4-2：启发式模拟退火算法

9. 以概率$\exp(\frac{\Delta C}{t})$令$(I_{Tx}^{i-1}, I_{Jm_1}^{i-1}, I_{Jm_2}^{i-1}) = (I_{Tx}^{i}, I_{Jm_1}^{i}, I_{Jm_2}^{i})$；

10. $m = m + 1$；

11. **End if**

12. **If** $m > m_{max}$ **then**

13. 令$(I_{Tx}^{*}, I_{Jm_1}^{*}, I_{Jm_2}^{*}) = (I_{Tx}^{i-1}, I_{Jm_1}^{i-1}, I_{Jm_2}^{i-1})$；

14. **Break**

15. **End if**

16. 令$t = \rho t$；

17. **End while**

18. **Return** $(I_{Tx}^{*}, I_{Jm_1}^{*}, I_{Jm_2}^{*})$

备注 3：本文所提出的基于模拟退火算法的解法在经历了一定次数的迭代之后会收敛到一个值$(I_{Tx}^{*}, I_{Jm_1}^{*}, I_{Jm_2}^{*})$。其收敛性的具体证明过程见参考文献[85]，本文不再给出。

备注 4：启发式模拟退火算法是一种概率性算法，具有一定的全局优化性能。本文由该启发式模拟退火算法得到的解，大概率可能是优化问题 **P6** 的最优解或者是一个可以接受的好的次优解。

4.3.2 一维搜索算法

众所周知，模拟退火算法等强搜索算法虽然可以解决一些非凸的优化问题，但是其较高的计算复杂度，使得其无法应对实时性较高的场景。因此，很有必要设计一种低复杂度的算法，尽管可能存在性能损失。

本小节提出了一种一维搜索算法来解决优化问题 **P6**，该算法可以大大地降低计算复杂度。接下来，本文给出**定理 4-3** 来将问题 **P6** 转化为一个求解一维变量的优化问题：

定理 4-3：在问题 **P6** 中，实现安全速率最大化的最优解$(I_{Tx}^{*}, I_{Jm_1}^{*}, I_{Jm_2}^{*})$必定满

足下列条件：

$$I_{Tx}^2+\frac{d_{Rx,Jm_1}^2+d_{Rx,Jm_2}^2}{d_{Rx,Jm_1}^2}I_{Jm_1}^2=I_{max}^2 \tag{4.14}$$

证明：根据**定理 3-2** 中的幅度条件，可以得到：

$$I_{Jm_1}^2+I_{Jm_2}^2=\frac{d_{Rx,Jm_1}^2+d_{Rx,Jm_2}^2}{d_{Rx,Jm_1}^2}I_{Jm_1}^2$$

由**定理 4-2** 的证明过程可以看出，安全速率$C\left(I_{Tx},I_{Jm_1},I_{Jm_2}\right)$是随着$I_{Jm_1}^2$的增大而单调递增的。

再根据公式（4.2）中的电流限定域，若要实现安全速率最大（即问题 **P6** 中目标函数最大），则问题 **P6** 的最优解$(I_{Tx}^*,I_{Jm_1}^*,I_{Jm_2}^*)$必定满足$I_{Tx}^2+\frac{d_{Rx,Jm_1}^2+d_{Rx,Jm_2}^2}{d_{Rx,Jm_1}^2}I_{Jm_1}^2=I_{max}^2$。**定理 4-3** 证毕。

由**定理 4-3**，I_{Jm_1}和I_{Jm_2}可以表示如下：

$$\begin{aligned}I_{Jm_1}&=d_{Rx,Jm_1}\sqrt{\frac{I_{max}^2-I_{Tx}^2}{d_{Rx,Jm_1}^2+d_{Rx,Jm_2}^2}}\\I_{Jm_2}&=d_{Rx,Jm_2}\sqrt{\frac{I_{max}^2-I_{Tx}^2}{d_{Rx,Jm_1}^2+d_{Rx,Jm_2}^2}}\end{aligned} \tag{4.15}$$

由上式（4.15）可知，若将（4.15）代入$C\left(I_{Tx},I_{Jm_1},I_{Jm_2}\right)$，则问题 **P6** 中的$I_{Jm_1}$和$I_{Jm_2}$可以被$I_{Tx}^2$替换掉。

因此，三个变量的优化问题 **P6** 可以被转化成一个单一变量的优化问题 **P7**，即：

$$\begin{aligned}\textbf{P7:}\quad &\max_{I_{Tx}} && C(I_{Tx}^2)\\&\text{s.t.} && 0<I_{Tx}\le I_{max}\end{aligned} \tag{4.16}$$

其中，$C(I_{Tx}^2)$为关于I_{Tx}^2的函数。

由此可见，问题 **P7** 可以在一维空间进行快速求解。较之**算法 4-2**，此方法将搜索维度从三维降低到一维，可以有效地降低计算复杂度，并且没有任何优化性能上的损失。

至此，本文所提出的基于协作干扰策略的功率分配优化方案设计完成。理论上来讲，此功率分配方案在找到最差窃听者位置后，进行功率分配可以提升系统的安全性能。接下来，本文给出此方案的仿真分析结果。

4.4 数值仿真结果及分析

本小节对本章所提的最差可达安全速率优化方案进行仿真分析。本小节所有的算法均在 Matlab 2016a 平台上运行，所有结果均是采用蒙特卡洛仿真进行了 1000 次随机迭代并求取平均的结果。

仿真参数设置如下：设定系统范围为以 Tx 为圆心，半径为 R=1000m 的圆形系统区域内。其中，Tx，Rx，Jm_1，以及 Jm_2分别位于坐标系中的（0, 0）、(100, 0)、(100, 150)、和（100, -250）点。AWGN 功率设定为-80dBm。

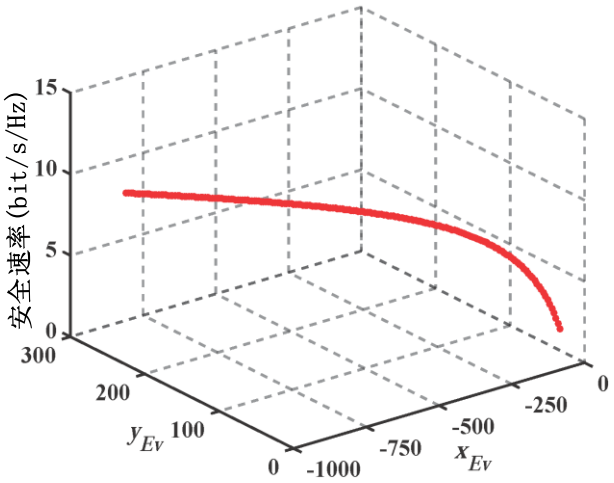


图 4-2 不同 r 下的最差窃听者的位置

Figure 4-2 The worst locations for different r

图 4-2 给出了每一个 r 的最差窃听者的位置的安全速率，称为每一个 r 的最差安全速率。由图 4-2 可以看出，随着 r 的增大最差安全速率也不断增大。因此，最差窃听者的位置应位于以半径$r = d_{min}$的圆弧上。

另外，通过对仿真结果的深入分析，发现每一个 r 的最差窃听者的位置都位于一条双曲线附近。这条双曲线以两 Jm 的位置为焦点，双曲线上的点$H(x_h, y_h)$满足以下关系式：

$$d_{Jm_2,H} - d_{Jm_1,H} = \frac{\pi - \varphi_{Jm_2} + \varphi_{Jm_1}}{\beta}$$

事实上，上述分析说明了，当 Eve 在双曲线上时，两 Jm 到 Eve 的相位差 $\varphi_{Jm_2,Jm_1} = \pi$。因此，可以得到下面的结论：

$$A_{Jm_1,Ev}^2 + A_{Jm_2,Ev}^2 + 2A_{Jm_1,Ev}A_{Jm_2,Ev}\cos(\varphi_{Jm_2,Jm_1}) = (A_{Jm_1,Ev} - A_{Jm_2,Ev})^2$$

很显然，这就是每一个 r 上找到的最差窃听者的位置都位于一条双曲线附近的原因。由**定理 3-2** 的证明过程可以看出，上式使得公式（3.11）左侧等号成立。但是这条双曲线上的点受到的干扰不为 0，因为其与两 Jm 的位置关系无法满足幅

度条件：

$$\frac{I_{Jm_1}}{d_{Jm_1,H}} = \frac{I_{Jm_2}}{d_{Jm_2,H}}$$

故而$\left|A_{Jm_1,H} - A_{Jm_2,H}\right|^2 \neq 0$，其合成功率密度不为 0。所以，尽管这条双曲线处受到的干扰会比较小，但是不为 0。

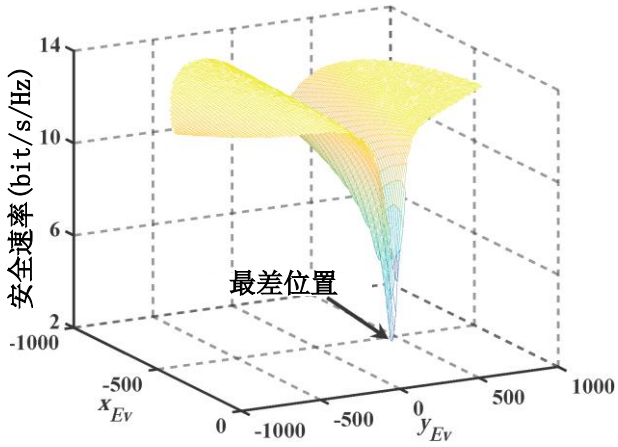


图 4-3 安全速率 ***vs.*** 窃听者的位置

Figure 4-3 Secrecy rate *vs.* Eve's locations

图 4-3 给出了对于搜索域内的每一个窃听者可能出现的位置，经过功率优化算法优化的结果。系统中最差窃听者的位置已用箭头标出，该点的安全速率代表了系统的最差可达安全速率。由图 4-3 可以看出，搜索域内各点的安全速率的三维空间图谱为“蝴蝶形”，而最差窃听者位置位于一条“沟壑”内。此仿真现象也进一步印证了最差窃听者位置在搜索域内呈现出双曲线特征。

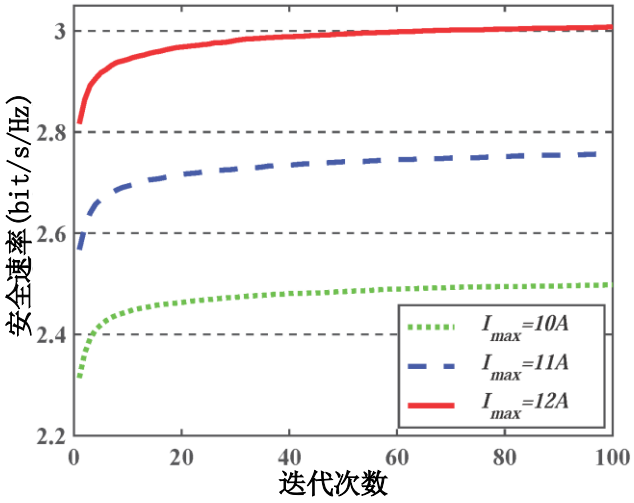


图 4-4 功率分配算法的收敛性

Figure 4-4 The convergence of power allocation algorithm

接下来，本文给出了图 4-4 来分析不同全局功率上限的情况下，功率分配算法

的收敛性。对于不同的电流限制，仿真结果表明了一系列最差可达安全速率的上限。由图 4-4 可见，随着电流上限的增加，最差可达安全速率也随之增大。

4.5 本章小结

本章根据上一章提出的协作干扰方案，提出了相应的功率分配方案，旨在提升系统的最差可达安全速率。首先在 4.1 小节，提出了功率优化问题，并对该问题进行了公式化，列出了相应的优化方程。为了求解该优化方程，将其分解成了两个易于处理的子优化问题，分别于 4.2 和 4.3 小节求解。在 4.2 小节中，在给定功率分配条件下，提出了一种在系统范围内快速搜索最差窃听者位置的方法。通过理论分析，先缩小了搜索范围，进而在缩小的搜索范围内，又提出一种波浪形之字搜索算法寻找最差窃听者位置。该搜索算法大大提高了搜索的有效性，降低了搜索复杂度。在 4.3 小节先证明了 4.2 小节找到的最差窃听者位置，就是系统范围内的最差窃听者的位置，不论功率如何变化。然后，针对该最差窃听者位置，对其进行了功率分配。为了求解该功率分配优化方程，本章提出了一种基于启发式模拟退火算法的解决方法。为了降低计算复杂度，本文进一步提出了一种一维搜索算法。4.5 小节给出了本章的优化算法的数值仿真结果分析，仿真结果说明了本文所提算法的有效性。

5 总结与展望

5.1 论文的工作总结

本论文以无线网络安全中的物理层安全问题为主要研究对象。针对网络中窃听者的信道状态信息未知的情况，本文研究了一种新奇的基于空间功率合成的协作干扰方案。与传统的方案相比，本文所提方案无需知道窃听者的任何信道状态信息也可以提高无线网络的安全速率，实现保密通信。本文的主要工作概括如下：

（1）首先，对本文研究内容的背景知识，国内外研究现状进行了总结，并指出了本文的研究意义和创新之处。

（2）其次，通过公式推导和理论分析，对物理层安全和功率合成相关的基础理论知识进行了归纳，为后文做了铺垫。基于香农理论知识，引出了物理层安全的概念。从 Wyner 的基本窃听信道模型引出安全容量公式，进而引出本文所利用的基于人工噪声的物理层安全技术。此外，又对本文所涉及的电磁场电磁波部分的相关知识进行了总结。

（3）之后，研究了适用于无线网络的基于空间功率合成的协作干扰方案。在窃听者信道状态信息完全未知的情况下，提出利用友好的相邻的合法用户发送人工噪声信号来干扰窃听者，而不干扰合法的接收者的安全传输策略。根据电磁波在空间中的叠加特性，本文研究了各协作节点的天线的参数，使得它们发出的信号在空间中叠加后，不对合法用户造成干扰，而在系统范围内的其它位置仍保留一定的噪声强度。本文根据 Rx 与各 Jm 的不同位置关系，证明了在 Rx 处合成干扰信号为 0 的解的存在性。而为了保证系统内其它位置不存在为 0 的点，本文又进一步证明了通过调节协作节点的天线参数可以实现零解的唯一性。

（4）最后，在确定协作干扰节点以及各节点的天线参数符合零解在 Rx 处唯一的情况下，进一步研究了 Tx 与各 Jm 的功率分配问题。为了分析系统的最低可达安全速率，本文首先提出了一种寻找系统范围内最差窃听者位置的方法。在缩小了搜索范围后，提出利用波浪形之字搜索法来快速寻找最差窃听者位置。在找到最差窃听者位置，并证明了最差窃听者位置不随功率分配的改变而变化之后，本文提出了一个功率分配优化问题。为了解决该优化问题，本文讨论了两种解决优化问题的算法：基于启发式模拟退火算法的方法和一维搜索算法。最后通过数值仿真分析，证明了本文所提算法可以有效地提高系统的最差可达安全速率。

（5）此外，对本文第三章和第四章所提的协作干扰策略以及功率分配方案分别进行了仿真分析。仿真结果证明了本文所提安全传输方案的有效性。

5.2 未来展望

本文对物理层安全中的协作干扰策略进行了深入研究，提出了基于空间功率合成的协作干扰策略，为协作干扰技术开辟了一个新的研究方向。但是，由于本人的理论水平以及思维的限制，本文也存在着一定的不足之处和进一步完善的空间。以下列举本人发现的尚有的不足之处，以及需要在今后的工作中进一步研究的问题：

（1）本文研究的是窃听者信道状态信息未知情况下的协作干扰问题，但是是在假设信号在自由空间中传播的前提下进行的。在只探究大尺度衰落的条件下，研究起来自然很容易。然而在现实场景下，不可能不考虑小尺度衰落。在实际应用过程中，多径效应，阴影衰落等不可避免，也不可能不给予考虑。故而，将来的关于本文工作的研究必须将小尺度衰落考虑进去。

（2）本文考虑的是二维平面内的空间功率合成问题，同样是将问题简单化了。在实际场景应用中，必定是三维空间。二维空间要求的条件过于苛刻，现实中不可能让两个天线完全等高。因此，三维空间的功率合成问题也是将来要研究的工作重点。

（3）本文研究的是一对用户进行通信的场景，对于多用户场景却没有进行分析。而在大多数情况下，多用户场景才是一个完备的无线通信系统。多用户之间存在的干扰问题远非单用户可以比拟。因此，多用户场景下的空间功率合成问题也有待研究。

（4）本文研究内容是静态环境下的通信场景，对于移动场景下，如何保证功率合成效果，是一个很大的难点。

（5）本文各节点均为单天线节点，而现今随着无线技术的发展，多天线的优势不言而喻。多天线场景下的功率合成问题，同样也需要引起重视。

总之，本文的研究还只存在于理论层面，如何将理论与现实联系起来是将来的研究工作的重点内容。

参考文献

[1]. Zou Y, Zhu J, Wang X, et al. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends[J]. Proceedings of the IEEE, 2015, 104(9):1727-1765.

[2]. 胡爱群. 无线通信网络的安全问题及对策. 电信科学, 2003,19 (12): 42~45.

[3]. Ravi K, Khanai R, Praveen K. Survey on pairing based cryptography for wireless sensor networks[C]// International Conference on Inventive Computation Technologies. IEEE, 2017:1-4.

[4]. Kumarasubramanian A. Connecting Theory and Practice in Modern Cryptography[J]. Dissertations & Theses - Gradworks, 2017.

[5]. A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” IEEE Communications Surveys and Tutorials, vol. 16, no. 3, pp. 1550 – 1573, 2014.

[6]. Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4):656-715.

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

[8]. Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, “Physical layer security in wireless networks: a tutorial,” IEEE Wireless Communications, vol. 18, pp. 66 – 74, April 2011.

[9]. A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” IEEE Communications Surveys and Tutorials, vol. 16, no. 3, pp. 1550 – 1573, 2014.

[10]. Maurer U M. Secret key agreement by public discussion from common information[J]. Information Theory IEEE Transactions on, 1993, 39(3):733-742.

[11]. 蔡文炳. 基于无线信道特性生成密钥的理论限及量化方法研究[D]. 解放军信息工程大学, 2013.

[12]. Csiszar I, Narayan P. Secrecy Capacities for Multiple Terminals [J]. Information Theory IEEE Transactions on, 2004, 50(12):3047-3061.

[13]. Csiszar I, Narayan P. Secrecy Capacities for Multiterminal Channel Models [J]. Information Theory IEEE Transactions on, 2008, 54(6):2437-2452.

[14]. Patwari N, Croft J, Jana S, et al. High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements[J]. IEEE Transactions on Mobile Computing, 2009, 9(1):17-30.

[15]. Pawar S, Rouayheb S E, Ramchandran K. Securing Dynamic Distributed Storage Systems Against Eavesdropping and Adversarial Attacks[J]. IEEE Transactions on Information Theory, 2011, 57(10):6734-6753.

[16]. Ozarow L H. The Wire-tap Channel II [J]. At & T Bell Labs Tech J, 1984, 63:2135-2157.

[17]. Thangaraj A, Dihidar S, Calderbank A R, et al. Applications of LDPC Codes to the Wiretap Channel [J]. Nformaon Hory Ranaon on, 2007, 53(8):2933-2945.

[18]. Tan V Y F. Achievable Second-order Coding Rates for the Wiretap Channel [C]// IEEE International Conference on Communication Systems. IEEE, 2012:65-69.
[19]. Tsai S H, Poor H V. Power Allocation for Artificial-Noise Secure MIMO Precoding Systems [J]. IEEE Transactions on Signal Processing, 2014, 62(13):3479-3493.
[20]. Nghia N T, Tuan H D, Duong T Q, et al. MIMO Beamforming for Secure and Energy-Efficient Wireless Communication [J]. 2017.
[21]. Hu J, Cai Y, Yang N, et al. Artificial-Noise-Aided Secure Transmission Scheme With Limited Training and Feedback Overhead [J]. IEEE Transactions on Wireless Communications, 2016, PP(99):1-1.
[22]. Wu H, Tao X, Li N, et al. Secrecy Outage Probability in Multi-RAT Heterogeneous Networks [J]. IEEE Communications Letters, 2015, 20(1):1-1.
[23]. Alotaibi E R, Hamdi K A. Ergodic Secrecy capacity Analysis for Cooperative Communication with Relay Selection under Non-identical Distribution [C]// IEEE International Conference on Communications. IEEE, 2016:1-6.
[24]. R. Negi and S. Goel, "Secret communication using artificial noise," in VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, vol. 3, pp. 1906-1910, Sept 2005.
[25]. Goel S, Negi R. Secret communication in presence of colluding eavesdroppers[C]// Military Communications Conference, 2005. Milcom. IEEE, 2005:1501-1506 Vol. 3.
[26]. Goel S, Negi R. Guaranteeing Secrecy using Artificial Noise[J]. Wireless Communications IEEE Transactions on, 2008, 7(6):2180-2189.
[27]. Goel S, Negi R. Obtaining Secrecy through Intentional Uncertainty[J]. 2009:19-37.
[28]. Goel S, Aggarwal V, Yener A, et al. The Effect of Eavesdroppers on Network Connectivity: A Secrecy Graph Approach[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(3):712-724.
[29]. Bassily R, Ekrem E, He X, et al. Cooperative Security at the Physical Layer: A Summary of Recent Advances[J]. IEEE Signal Processing Magazine, 2013, 30(5):16-28.
[30]. Atallah M, Kaddoum G, Kong L. A Survey on Cooperative Jamming Applied to Physical Layer Security[C]// IEEE International Conference on Ubiquitous Wireless Broadband. IEEE, 2015:1-5.
[31]. T.T.Tran and H.Y.Kong, "CSI-secured orthogonal jamming method for wireless physical layer security," IEEE Communications Letters, vol. 18, no. 5, pp. 841–844, May 2014.
[32]. Ghogho M, Swami A. Physical-Layer Secrecy of MIMO Communications in the Presence of a Poisson Random Field of Eavesdroppers[C]// IEEE International Conference on Communications Workshops. IEEE, 2011:1-5.
[33]. E.A.Jorswieck, "Secrecy capacity of single-and multi-antenna channels with simple helpers," in International Itg Conference on Source and Channel Coding, 2010, pp. 1–6.
[34]. C. Wang, H.-M. Wang, X.-G. Xia, and C. Liu, "Uncoordinated jammer selection for securing simome wiretap channels: A stochastic geometry approach," IEEE Transactions on Wireless Communications, pp. 2596 –2612, May 2015.
[35]. H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," IEEE Signal Processing Letters, vol. 22, no. 8, pp. 1147–1151, 2015.
[36]. Liu M, Liu Y. Power Allocation for Secure SWIPT Systems with Wireless-Powered

Cooperative Jamming[J]. IEEE Communications Letters, 2017, PP(99):1-1.

[37]. Z. Li, T. Jing, X. Cheng, Y. Huo, W. Zhou, and D. Chen, "Cooperative jamming for secure communications in MIMO cooperative cognitive radio networks," in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2015, pp. 7609–7614.

[38]. B. Han, J. Li, J. Su, M. Guo, and B. Zhao, "Secrecy capacity optimization via cooperative relaying and jamming for wanets," IEEE Transactions on Parallel and Distributed Systems, pp. 1117 – 1128, April 2015.

[39]. Liu W, Sarkar M Z I, Ratnarajah T. On the security of cognitive radio networks: Cooperative jamming with relay selection[C]// European Conference on Networks and Communications. IEEE, 2014:1-5.

[40]. Z. Li, T. Jing, Y. Huo, and J. Qian, "Worst-case jamming for secure communications in multi-antenna cooperative cognitive radio networks with energy harvesting," in Proc. Int. Conf. Identification, Inf., Knowl. Internet Things (IIKI), Oct. 2015, pp. 110–115.

[41]. Z. Li, T. Jing, L. Ma, Y. Huo, and J. Qian, "Worst-case cooperative jamming for secure communications in CIOT networks,"Sensors,vol.16, no. 3, p. 339, 2016.

[42]. Rawat D, White T, Parwez M S, et al. Evaluating Secrecy Outage of Physical Layer Security in Large-Scale MIMO Wireless Communications for Cyber-Physical Systems[J]. IEEE Internet of Things Journal, 2017, PP(99):1-1.

[43]. Bao V N Q, Cuu H V. Secure distributed switch-and-stay combining networks: Secure outage probability analysis[C]// Information and Computer Science. IEEE, 2016:101-106.

[44]. Zheng T X, Wang H M, Huang R, et al. Secrecy-throughput-optimal artificial noise design against randomly located eavesdroppers[C]// International Conference on Computing, NETWORKING and Communications. IEEE, 2016:1-5.

[45]. J.P.Vilela, M.Bloch, J.Barros, and S.W.McLaughlin, "Wireless secrecy regions with friendly jamming,"IEEE Trans. Inf. Forensics Security, vol.6, no. 2, pp. 256–266, Jun. 2011.

[46]. H. Li, X. Wang, and W. Hou, "Security enhancement in cooperative jamming using compromised secrecy region minimization," in Proc. 13th Can. Workshop Inf. Theory, Jun. 2013, pp. 214–218.

[47]. Shannon C E. A Mathematical Theory of Communications [J]. The Bell System Technical Journal, 1948，27（-）: 379-423, 623-656.

[48]. Fujita H. On the Secrecy Capacity of Wiretap Channels With Side Information at the Transmitter[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(11):2441-2452.

[49]. 陈莹. 基于信息理论的多用户信道的安全性能研究[D]. 南京邮电大学, 2011.

[50]. 李娜. 多用户系统的物理层安全性能研究[D]. 北京邮电大学, 2015.

[51]. Helal N, Nosratinia A. Multiple access wiretap channel with cribbing[C]// IEEE International Symposium on Information Theory. IEEE, 2017:739-743.

[52]. Nafea M, Yener A. A new multiple access wiretap channel model[C]// Information Theory Workshop. IEEE, 2016:349-353.

[53]. Nafea M, Yener A. The multiple access wiretap channel II with a noisy main channel[C]// IEEE International Symposium on Information Theory. IEEE, 2016:2983-2987.

[54]. 宋欢欢, 唐杰, 文红,等. 一种提高多用户 MIMO 广播信道安全性能的方案[J]. 通信技

术, 2015, 48(2):135-139.

[55]. Tie Liu, Shamai S. A note on the secrecy capacity of the multiple-antenna wiretap channel. IEEE Transactions on Information Theory, 2009, 55(6): 2 547~2 553.

[56]. A. Khisti, G Wornell. The MIMOME channel[C]. in Proceedings of the 45th Annual Allerton Conference on Co1rununication, Control and Computing, Monticello, IL, USA, September 2007.

[57]. Tan F Wong, Matthieu B, John M S. Secret sharing over fast-fading MIMO wiretap channels. EURASIP Journal on Wireless Communications and Networking, 2009.

[58]. Hyadi A, Rezki Z, Alouini M S. On the Secrecy Capacity of the Multiple-Antenna Wiretap Channel with Limited CSI Feedback[J]. 2016:1-6.

[59]. F. Oggier, B. Hassibi. The secrecy capacity of the capacity of the MIMO wire-tap channel[C]. in Proceedings of the 45th Annual Allerton Conference on Communication, Control and Computing, Monticello, IL, USA, September 2007.

[60]. H. Weingarten, T. Liu, S. Shamai (Shitz), Y. Steinberg, P. Viswanath. The capacity region of the degraded MIMO compound broadcast channel[C]. in Proceedings of the IEEE International Symposium on Information Theory (ISIT), Nice, France, 2007.

[61]. S. Shafiee, N. Liu, S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel：The 2-2-1 channel [J]. IEEE Transactions on Information Theory, 2007.

[62]. R. Bustin, R. Liu, H. V. Poor, S. Shamai (Shitz). An MMSE approach to the secrecy capacity of the MIMO Gaussian wire-tap channel[J]. EURASIP Journal on Wireless Communications and Networking, 2007.

[63]. 张海洋. 多天线窃听信道的安全性能研究[D]. 南京邮电大学, 2012.

[64]. T. M. Cover, A. A. El Gamal. Capacity theorems for the relay channel[J]. IEEE Transactions on Information Theory, 1979, 25: 572-584.

[65]. E. C. van der Meulen, Three-terminal communication channels[J]. Advances in Applied Probability, 1971, 3: 120-154.

[66]. Lifeng Lai, Hesham E G. The relay-eavesdropper channel: cooperation for secrecy. IEEE Transactions on Information Theory, 2008, 54(9): 4 005~4 019.

[67]. Lai L, Gamal H E. Cooperation for Secure Communication: The Relay Wiretap Channel[C]// IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2007:III-149 - III-152.

[68]. 瞿桢. 双向中继窃听信道的网络安全研究[D]. 深圳大学, 2015.

[69]. Aggarwal V, Sankar L, Calderbank A R, et al. Secrecy capacity of a class of orthogonal relay eavesdropper channels. EURASIP Journal on Wireless Communications and Networking, 2009.

[70]. Mirzaee M, Akhlaghi S. Secrecy Capacity of Two-Hop Relay Assisted Wiretap Channels[J]. Wireless Personal Communications, 2016:1-23.

[71]. Zheng M, Tao M, Chen W, et al. Secure Polar Coding for the Two-Way Wiretap Channel[J]. IEEE Access, 2017, PP(99):1-1.

[72]. 陈莹, 王保云. 多级中继窃听信道的可达安全速率[J]. 应用科学学报, 2011, 29(3):243-250.

[73]. Zhu Han, Ninoslav Marina, Mérouane Debbah, et al. Physical layer security game:

interaction between source, eavesdropper and friendly jammer. EURASIP Journal on Wireless Communications and Networking, 2009.

[74]. 蒋卫恒. 基于协作的无线窃听信道安全通信与功率分配[D]. 重庆大学, 2015.

[75]. Yan S, Zhou X, Yang N, et al. Artificial-Noise-Aided Secure Transmission in Wiretap Channels With Transmitter-Side Correlation[J]. IEEE Transactions on Wireless Communications, 2016, PP(99):1-1.

[76]. Vilela J P, Bloch M, Barros J, et al. Friendly Jamming for Wireless Secrecy[C]// IEEE International Conference on Communications. IEEE, 2010:1-6.

[77]. Griffiths J. Radio Wave Propagation and Antennas[J]. and 1800 MHz," in Proc. IEEE Veh. Technol. Conf, 1987(1):159.

[78]. 徐立勤, 曹伟. 电磁场与电磁波理论(高等院校教材)[M]. 科学出版社发行处出版社, 2006.

[79]. Griffith, Whitfield B. Radio-electronic transmission fundamentals[J]. Electromagnetic News Report, 2000(6):19.

[80]. T.S. Rappaport, Wireless Communications: Principles and Practice, vol.2. Englewood Cliffs, NJ, USA: Prentice-Hall, 1996.

[81]. R.A.York and R.C. Compton, ‘‘Coupled-oscillator arrays for millimeterwave power-combining and mode-locking,’’ in IEEE MTT-S Int. Microw. Symp. Dig., vol. 1. Jun. 1992, pp. 429–432.

[82]. K. Zhang, Z. Liu, J. Nie, X. Zhu, and G. Sun, ‘‘Spatial power combining based on distributed antennas in earth station,’’ Acta Aeronautica ET Astronautica Sinica, vol. 37, no. 6, pp. 1912–1920, 2016.

[83]. B.S.Guru and H.R.Hiziroglu, Electromagnetic Field Theory Fundamentals. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[84]. D. Bertsimas and J. Tsitsiklis, ‘‘Simulated annealing,’’ Statist. Sci., vol. 8, no. 1, pp. 10–15, 1993.

[85]. V. Granville, M. Krivanek, and J.-P. Rasson, ‘‘Simulated annealing: A proof of convergence,’’ IEEE Trans.Pattern Anal.Mach.Intell.,vol.16, no. 6, pp. 652–656, Jun. 1994.

作者简历及攻读硕士学位期间取得的研究成果

● 教育经历

2016.9-2018.6 电子与通信工程专业 硕士 北京交通大学

2012.9-2016.7 通信工程（理科试验班）专业 本科 北京交通大学

● 发表论文

[1]. **Fan X**, Huang L, Huo Y, et al. Space Power Synthesis-Based Cooperative Jamming for Unknown Channel State Information [C]// International Conference on Wireless Algorithms, Systems, and Applications. Springer, Cham, 2017:483-495.（**EI 会议，CCF：C 类，对应学位论文第三章内容**）

[2]. Huang L, **Fan X**, Huo Y, et al. A Novel Cooperative Jamming Scheme for Wireless Social Networks Without Known CSI [J]. IEEE Access, 2017, PP(99):1-1.（**SCI 期刊，IF：3.244，对应学位论文第四章内容**）

[3]. Luwei Wei, Tao Jing, **Xin Fan**, Yingkun Wen, Yan Huo. The Secrecy Analysis over Physical Layer in NOMA-enabled Cognitive Radio Networks [C]. IEEE International Conference on Communications (IEEE ICC 2018). **ISTP/EI 会议**

[4]. Mi Xu, Tao Jing, **Xin Fan**, Yingkun Wen, Yan Huo. Secure Transmission Solutions in Energy Harvesting Enabled Cooperative Cognitive Radio Networks [C]. IEEE Wireless Communications & Networking Conference (IEEE WCNC 2018). **ISTP/EI 会议**

[5]. Yanyan Zhang, Liang Huang and **Xin Fan**. Failure Feature Extraction of Analogue Active Filter Based on Attenuation Sensitivity [C]. IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IEEE IMCEC 2018). **ISTP/EI 会议**

● 科研经历

[1]. 国家自然科学基金“面上”，移动社交网络中考虑用户自私性的路由协议研究，No.61471028

[2]. 国家自然科学基金“面上”，协作认知无线电网络中物理层安全问题研究，No.61572070

[3]. 中央高校基本科研业务费重点项目，面向 5G 的低功耗巨连接关键技术研究，No.2016JBZ003

[4]. 中央高校基本科研业务费重点项目，面向区域协同干扰的隐蔽通信策略研究，No.2017JBM004

[5]. 国家自然科学基金“面上”，室内基于 WMNs 节点定位关键技术研究，No.311010533

[6]. 基本科研业务费，基于超宽带的精确定位技术研究，No.12006536

独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作和取得的研究成果，除了文中特别加以标注和致谢之处外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得北京交通大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

学位论文作者签名：范新 签字日期：2018年5月31日

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>物理层安全；协作干扰；电磁场与电磁波；空间功率合成；信道状态信息；安全速率；模拟退火算法</td><td>公开</td><td>TN929.5</td><td>621.39</td><td>自然科学基金“面上”项目（61572070，61471028，61575053）和中央高校基本科研业务费重点项目（2017JBM004，2017JBM003）</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>工学</td><td>硕士</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">基于空间功率合成的协作干扰技术研究</td><td colspan="2"></td><td>汉语</td></tr>
<tr><td>作者姓名*</td><td colspan="2">范新</td><td>学号*</td><td>16125009</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">电子与通信工程</td><td>无线通信</td><td>两年</td><td>2018 年</td></tr>
<tr><td>论文提交日期*</td><td colspan="4">2018 年 5 月</td></tr>
<tr><td>导师姓名*</td><td colspan="2">黄亮</td><td>职称*</td><td>副教授</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">侯建军</td><td colspan="2">路勇、郝晓丽、邵小桃、魏杰</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 colspan="2">电子版论文出版（发布）地</td><td>权限声明</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td>论文总页数*</td><td colspan="4">67</td></tr>
<tr><td colspan="5">共 33 项，其中带*为必填数据，为 22 项。</td></tr>
</table>