DOI:10.13878/j.cnki.jnuist.2020.01.006

戴跃伟[1]　刘光杰[1]　曹鹏程[2]　刘伟伟[2]　翟江涛[1]

# 无线隐蔽通信研究综述

**作者简介**:戴跃伟(1962—),男,南京信息工程大学教授、博士生导师,南京理工大学兼职教授、博士生导师,兼任中国指挥控制学会海上指挥控制专委会副主任委员、中国电子学会通信学分会理事、中国高教学会理事.主要研究方向为网络与多媒体信息安全、复杂系统建模与控制等,长期从事信息隐藏、数字水印、隐蔽信道等方面的理论和技术研究,部分成果得到了实际应用.近年来主持完成了包括国家科技重大专项、武器装备探索研究课题、国家自然科学基金面上项目、国防预研课题在内的50余项研究课题,获批相关发明专利10余项,获得省部级科技和教学奖励6项,发表研究论文150多篇,其中被SCI收录50余篇.
E-mail:dyw@ nuist.edu.cn

**收稿日期** 2020-02-02
**基金项目** 国家自然科学基金(U1636117,U1836104,61702235);中央高校基本科研业务费专项资金(30918012204).

1 南京信息工程大学 电子与信息工程学院,南京,210044
2 南京理工大学 自动化学院,南京,210094

**摘要**

无线隐蔽通信是将消息隐藏在无线通信数据帧和信号中进行隐蔽传输的技术,属于无线通信和信息隐藏技术的交叉领域,其理论与技术的研究方兴未艾.本文分析了无线隐蔽通信的系统模型和主要能力要素,总结归纳了噪声式隐蔽信道容量的理论以及链路层、编码层、调制层和信号层中无线隐蔽通信技术的研究进展,并指出了需要进一步研究的问题.

**关键词**

无线隐蔽通信;信息隐藏;隐蔽信道

**中图分类号** TP391
**文献标志码** A

## 0　引言

随着以5G为代表的移动通信技术的飞速发展以及人类活动向太空和深海的延伸,利用电磁波、声波、光等作为信息传输媒介的现代无线通信技术已成为各场景中主要的通信方式.依据介质类型,无线通信可分为无线电通信、声波通信、自由空间光通信、磁通信等.其中,无线电通信是当前最广泛使用的通信方式.无线电介质的开放性,使得通信信号很容易被第三方拦截和窃听[1],进而导致通信内容的泄露或通信意图的暴露.传统上,通常采用信息加密来保障信息的机密性,用扩频等降低信号功率的手段提高信号的抗截获能力.现代信息隐藏技术的发展给通信内容和行为保护带来了更多的选择.

现代网络通信一般采用包含物理层、链路层、网络层、传输层和应用层的五层结构来作为体系架构,其中物理层又可进一步分解为编码层、调制层和信号层,具体如图1所示.传统信息隐藏主要以图像、音频、视频和文本作为载体,主要是多媒体领域的信息隐藏.网络通信领域的信息隐藏以网络数据报文和通信信号作为载体.通常网络层以上的技术被认为是网络范畴,该范畴中的信息隐藏称为网络隐蔽信道(Network Covert Channel)[2-5],包含基于冗余字段替换、协议混淆伪装、协议隧道封装等存储式方法和基于数据包时标信息的时标式方法.与网络范畴对应,链路层解决通信介质利用问题,物理层解决信息与信号之间的转化问题,构成通信范畴.该范畴中的信息隐藏称为隐蔽通信.具体到无线通信(包含组网情形下的无线网络通信,以及非组网情形下的点对点和点对多点通信)场景中的信息隐藏技术即

为无线隐蔽通信[6],本文重点探讨无线电通信领域的隐蔽通信问题.为了避免过细的界定导致陈述上的繁复,本文后续所述无线隐蔽通信将专指无线电隐蔽通信.

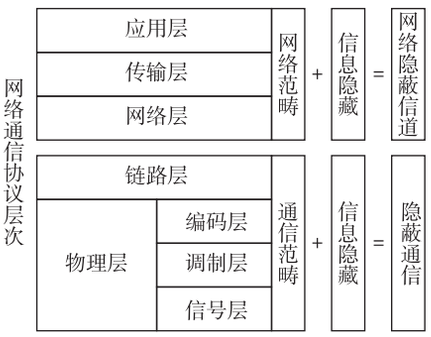


图 1　网络通信领域的信息隐藏研究范畴

Fig. 1　Information hiding research scope in field of network communication

无线隐蔽通信是在无线通信数据帧和通信信号中进行信息隐藏的技术,其采用的隐藏手段主要是替换数据帧域冗余字段、引入额外编码域错误、插入额外信号频带、引入额外信号噪声等方式,主要涉及传输速率、可靠性和隐蔽性等能力要素.无线隐蔽通信作为一种以隐蔽性为主要追求的特殊通信方式,涉及多种场景下的隐蔽信道容量分析等信息论新问题,和一系列以无线通信为背景的信息隐藏方法,在复杂对抗环境中的军事通信、物理隔离环境下的情报通信等领域有着重要的应用前景.

基于链路层的隐蔽通信主要利用链路帧字段的替换和插入实现信息隐藏,如基于无线局域网 802.11 协议族和 4G 移动通信的 LTE 等主流无线通信协议中的数据帧报文头冗余字段[7-8]、填充部分[9-11]和序列号[12-13]的方法.亦有学者提出了将网络隐蔽信道与无线隐蔽通信相结合的混合网络通信隐蔽信道方法[14-15].这类方法的通信速率与可靠性主要取决于所采用的隐蔽通信载体,由于难以抵抗模式匹配[16-17]和统计分析[18-19]等检测方法,隐蔽性较弱.

物理层中编码和调制层的隐蔽通信可以利用信道编码冗余[20-27]、多载波调制 OFDM 的循环前缀[28-29]和空闲频谱资源[30-31]来实施.在信号层,通常利用无线信道中天然存在的噪声作为掩护,将信息调制为低功率噪声直接发送,抑或叠加在载体通信信号上发送.信号层无线隐蔽通信理论上属于一类低检测概率(Low Probability Detection,LPD)通信问题.该领域最早的研究假设理想的高斯信道下检测方已知信道噪声的功率值,并基于假设检验来判断是否存在隐蔽通信,发送方在满足隐蔽性的前提下能够可靠传输的信息量满足平方根定律(Square Root Law,SRL)[32],且隐蔽通信速率随着利用信道时频资源数量的增加而趋向于 0.研究者进一步分析了在发送方[33-34]、接收方[35-37]以及额外节点[38-41]引入人工噪声干扰等对检测方不利的因素的场景下的隐蔽通信容量.该领域研究成果也被进一步扩展至中继通信[42-45]、多天线[46-47]、广播通信[48-49]等其他通信场景.

信号层无线隐蔽通信方法一般假设检测方仅拥有信道噪声的部分知识,较常见的是假设检测方知道信道噪声分布类型而不清楚其功率大小.发送方将信息调制成与正常信道噪声相似的信号实施隐蔽通信.早期方法中,发送方信息嵌入到一段服从 $\alpha$ 稳定分布[50-51]或高斯分布[52]的噪声序列特征参数中,接收方通过估计特征参数来提取信息,这类方法传输速率较低,且存在序列同步问题[53].后续方法将信息调制为特定噪声后叠加在正常通信信号上进行传输,或将随机噪声与调制的特定噪声叠加[54]或混合[55]来提高隐蔽性,这类方法需要消耗一定的通信带宽,隐蔽性也不够理想[17].文献[56]提出一种基于星座图拟形调制的无线隐蔽信道,发送方利用星座图拟形调制技术实现了更好的隐蔽性与可靠性.

无线隐蔽通信的研究经过多年的发展,已经逐步形成了噪声式隐蔽信道容量理论以及链路层、编码层、调制层和信号层的各种方法,近些年也发展了一些针对隐蔽通信的检测技术.本文重点对无线隐蔽通信的系统模型、基本理论以及各方向上的技术进展情况进行总结和归纳,并在此基础上给出该领域有待进一步研究的问题.

本文结构安排如下:第一节介绍无线隐蔽信道的系统模型和能力要素,第二节介绍典型无线协议中的链路层无线隐蔽通信方法并对其隐蔽性进行分析,第三节总结物理层无线隐蔽通信理论与技术的进展,第四节对有待研究的问题进行展望,第五节给出全文的总结.

## 1　无线隐蔽通信系统模型

### 1.1　系统模型

与著名的“囚徒通信”问题[57]类似,标准无线隐蔽通信系统模型中包含发送方(Alice)、接收方

(Bob)和检测方(Willie)这三个角色(如图2所示),Alice将信息$\boldsymbol{m}$嵌入正常的无线通信载体对象$\boldsymbol{x}$中生成载密无线信号$\boldsymbol{y}$并在通信区域$R$内传播;Bob从经过信道传输后衰落的信号$\hat{\boldsymbol{y}}$中提取出信息$\hat{\boldsymbol{m}}$;由于无线信号的广播特性,Willie可截获信号$\tilde{\boldsymbol{y}}$(由于Willie和Bob空间位置和关于通信先验知识方面的差异,$\hat{\boldsymbol{y}}$和$\tilde{\boldsymbol{y}}$可能不一致),并判断该信号中是否存在隐蔽信息.上述三个过程可以表述为:

$$\begin{aligned}&\text{信息隐藏}:H(\boldsymbol{x},\boldsymbol{m})\rightarrow\boldsymbol{y},\\&\text{信息提取}:E(\hat{\boldsymbol{y}})\rightarrow\hat{\boldsymbol{m}},\\&\text{检测攻击}:D(\tilde{\boldsymbol{y}})\rightarrow B\in\{0,1\}.\end{aligned}\tag{1}$$

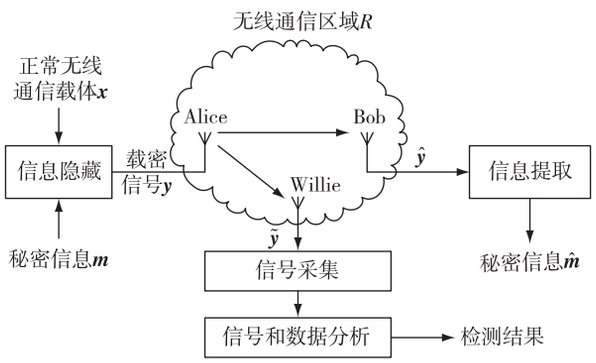


图2 标准无线隐蔽通信模型

Fig. 2 Standard wireless covert communication model

上述模型体现了Alice/Bob与Willie之间的通信对抗关系.在这一对抗关系中,Alice/Bob希望尽可能多地透过无线通信区域$R$不被Willie发现来传输信息;Willie希望尽可能多地利用关于信道和Alice/Bob通信机制的先验知识,并以尽可能高的准确率判断信号是否存在隐蔽通信.

信息隐藏函数$H$一般有三种典型算子,分别为替换算子Sub、叠加算子Add和转换算子Con.其中,Sub算子将$\boldsymbol{m}$通过某种转换编码得到的值$\boldsymbol{v}$替换$\boldsymbol{x}$或其某种变换的分量;Add算子将$\boldsymbol{m}$通过某种转换编码得到的值$\boldsymbol{v}$叠加到$\boldsymbol{x}$或其某种变换量上,Sub和Add操作不应该引起$\boldsymbol{x}$在形式、语法、语义、统计等特征上的明显差异(这些差异通常是函数Det的检测依据);Con算子直接将$\boldsymbol{m}$通过某种转换形式,转换为与$\boldsymbol{x}$在形式、语法、语义、统计等特征上一致或相近的信号.

信息提取函数$E$代表与$H$配合使用的信息提取过程.函数$E$通常需要利用一些用于提取信息的先验信息,包括$H$函数中使用的密钥、载体$\boldsymbol{x}$的全部信息或部分信息,以及关于信道的假设或估计等.

检测攻击函数$D$直接作用于截获信号产生检测结果.函数$D$的检测能力依赖于Willie对$\hat{\boldsymbol{y}}$所服从统计分布的掌握情况,理论上是关于截获信号是否服从于$P(\hat{\boldsymbol{y}})$的假设检验问题.实际的检测攻击要复杂得多,首先检测可能与空间、电磁传播环境、具体网络协议应用等有关系,可能存在多种模态上的分布函数或分布函数本身也缺乏准确建模;Willie还可以利用连续、多次、多个采样点的截获信号相关性进行检测,此时检测涉及的信息既包括相关性信息也包括具体信号的特性;再次Willie可利用对Alice/Bob隐蔽通信机制的先验信息进行针对性的检测分析;最后Willie还可对通信场景、通信参与者、通信时机、载体选择等要素发起通信行为方面的检测攻击.

需要指出的是:图2给出的是一个标准模型,仅涉及Alice、Bob和Willie三个角色.在这一标准模型中增加新的角色可以得到其他的扩展模型.如在通信场景中增加干扰器Jammer的辅助通信场景,在Alice和Bob之间增加一个或者多个Relay的中继通信场景,包含一个Alice和多个Bob的多播或广播通信场景,同时有多个Alice和Bob传输的多输入多输出通信场景,或具有多个空间上不同位置的Willie的场景等.此外,这些通信场景还可以进一步组合得到更为复杂的通信场景,如具有加扰器的中继通信场景和广播通信场景等.

### 1.2 能力要素

无线隐蔽通信主要涉及隐蔽性、可靠性和通信速率三个主要能力要素,下面简单对其内涵进行解释.

1)隐蔽性

隐蔽性广义上包括信号隐蔽性和行为隐蔽性.行为隐蔽性涉及通信场景、通信参与者、通信时机、载体选择等要素,属于无线隐蔽通信运用层面的问题;信号隐蔽性是在使用层面具体描述隐蔽通信信号和正常载体信号之间区分度的评估要素,技术上可以用某种检测方法的检测错误率来衡量其隐蔽性.

2)可靠性

可靠性指无线隐蔽通信抵抗信道干扰的能力.信道干扰可能来自于信道自然衰落,也可能来自于通信对抗干扰设备.技术上可以用给定信噪比下接收方信息的误比特率来衡量通信的可靠性.在越强的信道干扰下,信息误比特率越低,则可靠性越强.

3)通信速率

隐蔽通信速率指单位时间无线隐蔽通信可靠传

输的信息比特数,与可靠性之间存在制约关系.为了达到更好的可靠性,有时需要降低隐蔽通信速率.通信速率可以通过计算平均每单元数据帧/符号/信号携带的秘密消息比特数来衡量.

除了上述三个要素之外,无线隐蔽通信系统还涉及载体广泛性、方案可实施性、通信计算复杂性等能力要素.

## 2 链路层无线隐蔽通信

### 2.1 WLAN 无线隐蔽通信方法

当前广泛使用的 WLAN 协议(即 IEEE 802.11 标准)可为无线隐蔽通信提供良好的载体.文献[7]提出了一种基于 WLAN 的无线隐蔽信道,其在 802.11 协议 MAC 层帧的序列控制域,或在 WEB 加密安全协议帧的初始矢量域中嵌入信息.文献[9-10]提出了一种在 WLAN 帧填充部分嵌入信息的 WiPad 方法,并给出了数据帧与应答帧的隐蔽传输速率.针对 802.11 各协议,也有许多具体的研究成果.如基于 802.11e 协议,文献[58]设计了两种无线隐蔽通信方法,信息分别嵌入在关联请求与重新关联请求帧的 QoS 容量字段和每个数据帧 QoS 控制域中的 TXOP 和 TID 字段中.

### 2.2 LTE 无线隐蔽通信方法

4G 移动通信的普及使得 LTE 成为主流的无线通信协议之一,利用 LTE 协议的 MAC、RLC 和 PDCP 层的冗余可实施隐蔽通信.文献[8]给出了一种在 LTE-A 协议冗余字段嵌入信息的方法,信息可以嵌入在 MAC 层协议数据单元(Protocol Data Unit,PDU)子帧报头前两保留位、RLC 层的应答模式和未确认模式 PDU 的序列号保留位,以及 PDCP 层的 PDU 序列号保留位中进行传输.文献[11]提出的 LaTEsteg 是利用 LTE-A 协议中 MAC 层数据包的填充字段嵌入信息.文献[12]提出了一种基于 LTE-A 协议的方法,通过修改每个 PDU 的序号保留位来标示是否载密,并填充字段用来传输信息.文献[13]提出的 SNsteg 通过修改 LTE-A 中 RLC 和 PDCP 数据包包头中的序列号来传输信息,该方法利用了 PDU 序号的唯一性,如果某一 PDU 与新接收到 PDU 的序列号相同,则系统将丢弃新的 PDU.SNsteg 信息以序号的最低位来表示.当连续发送两个 PDU 时,假设一个 PDU 序号的最后一位是“0”(标记为“0”PDU),另外一个 PDU 序号的最后一位是“1”(标记为“1”PDU).若要发送隐蔽信息“0”,可以在上述的“0”PDU 和“1”PDU 之间插入一个“0”PDU.反之,若要发送隐蔽信息“1”,则插入一个“1”PDU.由于系统将丢弃具有相同序号的新的 PDU,所以非授权接收方不能得到隐藏位,且不影响正常通信,具有很好的抗检测性能.

文献[14]提出了一种利用 LTE 上 MAC 层协议字段与数据包时延一起构建的混合隐蔽通信方案.相较于单纯的时间式网络隐蔽通信,该方案的隐蔽性与可靠性都得到了有效提高.另一种混合隐蔽通信方案 HyLTEsteg 是将 SNsteg 与时间式网络隐蔽通信结合,其中时间式网络隐蔽通信方案起着隐蔽传输的触发功能,而 SNsteg 负责传输信息[15].

### 2.3 链路层方法隐蔽性分析

链路层协议及其具体实现具有明显的规律性,这使得绝大多数链路层无线隐蔽通信方法都难以抵抗针对性的模式匹配或统计检测.文献[16-17]针对多种 802.11 协议无线隐蔽通信利用的协议字段特征,设计了模式匹配检测方法,可实现有效检测.针对隐蔽性较好的 SNsteg[13],文献[18]和文献[19]分别提出了一种基于邻近序列号差值的修正条件熵检测方法和一种基于 KNN 分类器的检测方法.针对链路层无线隐蔽通信,可进一步借鉴针对协议层面的网络隐蔽信道的检测机制,设计基于规则集的链路层隐蔽通信检测体系.

## 3 物理层无线隐蔽通信

### 3.1 编码层无线隐蔽通信方法

编码层采用纠错编码技术引入比特冗余来提高传输可靠性,纠错编码产生的比特冗余可以用来实施信息隐藏.文献[20]研究了利用常见的分组码、卷积码等纠错编码冗余的隐蔽通信容量问题.理论分析与实验结果表明,信息可嵌入容量随信道噪声增大而减小,最大嵌入容量随信源数据和信道编码纠错能力的增加而增加.同等条件下基于卷积码的隐蔽通信最大嵌入容量大于基于分组码的隐蔽通信最大嵌入容量.这类利用编码纠错能力冗余构建的隐蔽信道具有广泛的适用性.

在无线个域网(Wireless Personal Area Network,WPAN)的 802.15.4 物理层协议中,4 bit 信息符号被映射成 32 bit 直接序列扩频码字序列,具有可供利用的编码冗余.文献[21]通过翻转 802.15.4 物理层协议中的直接序列扩频码字位数来嵌入信息.文献[22]通过替换该协议物理层中的直接序列扩频码

字位数来嵌入信息.值得指出的是:随着嵌入信息量的增大,以上两种方法对直接序列扩频码字的固定位进行修改均会导致采用部分扩频序列的载体信息的误码率显著增加.文献[23]通过随机置乱直接序列扩频码字修改位,来避免由于嵌入信息量较大而导致的误比特率显著增加问题.文献[24]提出了一种修改无线传感网络中直接序列扩频码字来传输信息的方法.

文献[25]研究了两种基于RS码冗余的自适应码率无线隐蔽通信理论问题,分别讨论了正常通信选取不同编码方案下信息的平均理论容量以及每种编码方案下信息最大理论容量.二进制对称信道下的仿真结果表明:这两种基于RS码冗余的无线隐蔽通信方案容量均好于基于分组码与卷积码的方案.针对WiMAX协议,文献[26]也提出了一种通过修改RS码码字比特嵌入秘密信息的方法.针对具有自适应可变码率的协议,文献[27]提出的无线隐蔽通信方案利用低速率编码的校验位来传输信息.

目前尚无专门针对编码层无线隐蔽通信的检测方案,部分针对基于802.15.4物理层协议的无线隐蔽通信方案的文献中以载密直接序列扩频码字与正常直接序列扩频码字之间的汉明距离来衡量这类方法的隐蔽性.文献[23]证实了降低码字汉明距离可以降低对正常通信误码率的影响,提高隐蔽通信的抗检测能力,但会带来隐蔽通信可靠性的降低.在信道状态确知的场景中,误码率和误码图样可能会成为揭示是否存在隐蔽通信的指标,有待进一步深入研究.

### 3.2 调制层无线隐蔽通信方法

多载波调制的正交频分复用(Orthogonal Frequency Division Multiplexing, OFDM)技术已在WLAN、LTE等主流通信协议中得到广泛应用.OFDM信号调制过程中通过给每个符号添加循环前缀来抵抗多径延时,从而保证符号周期完整.文献[28]提出了一种基于循环前缀的无线隐蔽通信方法,利用802.11协议中符号循环前缀实现了高速率的无线隐蔽通信.这种方法随后被推广到所有采用OFDM通信系统中[29].显而易见的是OFDM符号循环前缀来嵌入信息的隐蔽通信方法会降低通信抗多径延时可靠性.

OFDM系统的部分子载波频段一般被预留作为信道间隔或进行收发双方同步,有时由于信道响应较差而放弃使用.这些未被使用的子载波频段资源也可用来构建独立的隐蔽信道[30].发送方利用空置子载波频段可向接收方传输信息的方法依赖无线通信环境中存在未被使用的子载波频段,对空置子载波的利用会导致OFDM信号的正交性受影响.针对该问题,文献[31]中提出了一种基于认知无线电进行频谱感知来得到未用频段信息的方法,并采用跳频技术在空置频谱上传输信息.

文献[59]设计了针对802.11a/g的四种隐蔽通信方法,其构造原理分别为:修改短训练序列的相位、修改载波频率偏移量、通信协议伪装以获取额外的子载波频段以及替换部分循环前缀.在修改短训练序列相位的方法中,发送方通过修改短训练序列的相位值嵌入信息,接收方通过长训练序列得到信道参数,通过提取短训练序列的相位偏移得到信息;在修改载波频率的偏移的方法中,发送方通过修改载波频率偏移嵌入信息,接收方通过导频信息估计频率偏移得到信息;在通信协议伪装的方法中,发送方将802.11a/g信号伪装成802.11n信号,使得可用子载波数由52增加到56,利用额外的四个子载波进行隐蔽信息传输,回避了文献[30]方法存在的信号正交性受影响问题;替换部分循环前缀的方法是在文献[28-29]方法的基础上提出的,发送方通过替换一半乃至1/4的循环前缀嵌入信息,降低了信息嵌入对正常通信抵抗多径延时能力的影响.

目前较少见专门针对该层级隐蔽通信的检测工作.文献[17]借鉴了网络隐蔽信道中常用的检测方法,给出了在不同场景下的检测结果,检测结果表明,当检测点的位置接近发送方,基于短训练序列的相位修改、载波频率偏移修改和循环前缀修改的调制层隐蔽信道易被数值统计方法检测出来.在隐蔽性分析方面,文献[59]中以载体信息的误比特率来衡量物理层之上的隐蔽性,以相位误差、频率偏移量、频谱等信号分析指标来衡量物理层的隐蔽性.

### 3.3 信号层无线隐蔽通信

信号层方法将信息调制为与信道噪声相似的信号来实现隐蔽通信,其本质上是一类LPD通信问题[32],其将通信信号淹埋在背景噪声中的做法也可以归结为噪声式无线隐蔽通信,相关的研究内容主要包含噪声式隐蔽信道理论容量分析和实际通信方法设计等.

#### 3.3.1 噪声式隐蔽信道容量分析

噪声式无线隐蔽信道作为一种附带了隐蔽性要求的新型信道,当前取得的理论成果丰富了信息论

的研究范畴,已逐步发展成为一个相对独立的信息论分支领域.信道容量的研究主要包括标准通信场景(标准模型仅包括 Alice、Bob 和 Willie 三个参与方)、辅助通信场景(在标准模型中增加了 Jammer 干扰器角色)、中继通信场景(在标准模型中增加了 Relay 中继器角色),以及其他通信场景(MIMO、广播通信、非高斯信道衰落等形式)等.下面分别介绍相关研究结果.

1)标准通信场景

文献[32]针对如图 3 所示通信模型,首次对加性白高斯噪声(Additive White Gaussian Noise,AWGN)信道中低概率检测(Low Probability Detection,LPD)通信的信道容量进行了分析.论文假设 Willie 掌握信道噪声的全部先验知识,以 AWGN 信道中截获信号与信道噪声信号的假设检验作为出发点,通过推导得到通信双方 $n$ 个信道基本时频单位可安全可靠地传输 $\mathcal{O}(\sqrt{n})$ 比特信息,该定律也称为平方根定律 SRL.隐蔽传输速率随时频单位的增大而趋向于 0,即 SRL 和数字隐写中的平方根定律[60-61]密切相关,文献[32]中详细分析了这两者的关系.值得指出的是文献[32]给出的是 LPD 通信的安全可靠通信容量的分析,其得到的结果是一个一般性的深刻结果,也适合扩频通信等其他形式的隐蔽通信,是隐蔽通信领域的奠基性理论结果.

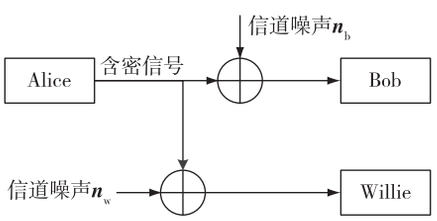


图 3 AWGN 信道隐蔽通信模型

Fig. 3 Covert communication model with AWGN channel

文献[62]从功率角度分析了文献[32]所述的隐蔽信道的通信速率问题,Willie 根据信号功率大小判断其是否存在信息.假设 Alice 至 Bob 与 Willie 的信道分别是方差为 $\sigma_{\mathrm{b}}^2>0$ 和 $\sigma_{\mathrm{w}}^2>0$ 的 AWGN 信道,当 Alice 不传输信息时,检测方 Willie 观察到 $n$ 个信道时频单位总功率为 $\sigma_{\mathrm{w}}^2 n$,所观察功率统计上大概率在 $c\sigma_{\mathrm{w}}^2\sqrt{n}$ 之内.为了保证信道的隐蔽性,发送方 Alice 的发射功率需要限制为 $\mathcal{O}(\sigma_{\mathrm{w}}^2\sqrt{n})$,这使得 Alice 最多可以传输 $\mathcal{O}(\sigma_{\mathrm{w}}^2\sqrt{n}/\sigma_{\mathrm{b}}^2)$ 比特信息,该结论与文献[32]中的结论一致.

文献[63]假设 Alice 到 Willie 的离散无记忆信道比到 Bob 的信道噪声更大,分析表明 $n$ 个信道时频单位仍仅能隐蔽可靠传输 $\mathcal{O}(\sqrt{n})$ 比特信息.文献[64-65]进一步给出了比例系数的表达形式.文献[66]讨论了两种情形:若不顾通信质量,仅需通信双方共享 $\mathcal{O}(\sqrt{n})$ 比特的秘钥而不是文献[32]中需要的 $\mathcal{O}(\sqrt{n}\log n)$ 比特,$n$ 个信道时频单位仍能可靠传输 $\mathcal{O}(\sqrt{n})$ 比特信息;若 Alice 到 Willie 的信道比到 Bob 的信道噪声更大,$n$ 个信道时频单位仍仅能隐蔽可靠传输 $\mathcal{O}(\sqrt{n})$ 比特信息,且无需共享秘钥.当离散无记忆多址信道中存在两个发送方对一个接收方时,若 Willie 的离散无记忆多址信道差于隐蔽通信信道,$n$ 个信道基本时频单位仅能隐蔽可靠地传输大约 $\mathcal{O}(\sqrt{n})$ 比特信息,且不需要通信秘钥[67].文献[68]进一步将其拓展到了拥有 $K$ 个发送方的场景,此时每个发送方 $n$ 个信道时频单位仍仅能隐蔽可靠传输 $\mathcal{O}(\sqrt{n})$ 比特信息.

相关研究也讨论了增加 Willie 对信道和噪声不确定性的结果.文献[69]讨论了当通信双方在 $T(n)$ 个时隙(每个时隙由 $n$ 个符号周期构成)中秘密地选择一个时隙,若 Willie 无法得知具体的通信时间,此时 Alice 仅需传输 $\log T(n)$ 比特的秘钥即可传输 $\mathcal{O}(\min\{n,\sqrt{n\log T(n)}\})$ 比特信息.文献[70]分析了 Willie 已知 $T(n)$ 和 $n$ 这两个参数时,可以通过一定手段将隐蔽信道速率限制到依然遵循平方根定律.文献[71]分析了当 Willie 对应的信道背景噪声功率不确定时,隐蔽通信速率为正值.文献[72]在文献[71]的基础上,假设隐蔽信道噪声功率也不确定性时,隐蔽通信速率趋近于 0.

2)辅助通信场景

通过在标准模型中增加了对检测方 Willie 不利的因素,增加 Willie 作出判断的不确定性,可将标准模型推到辅助通信场景.考虑信道中存在信号干扰器 Jammer 的情形,文献[38]假设 Willie 无法获取信道噪声功率,$n$ 个信道时频单位能隐蔽可靠地传输 $\mathcal{O}(n)$ 比特的信息.文献[39]探讨了存在多个 Jammer 发出人工辅助噪声对检测进行干扰的节点的情形,并推导了此时隐蔽可靠传输的比特数可增大为 $\mathcal{O}(m^{\gamma/2}\sqrt{n})$($m$ 为协作节点分布的密度,$\gamma$ 为路径损耗指数).若存在密度为 $m$ 且满足二维泊松点过程分布的协作节点,且这些协作节点距离检测方更近并发射人工辅助噪声对 Willie 进行干扰,Alice 可

以隐蔽可靠地传输 $\mathcal{O}(\min\{n,m^{Y/2}\sqrt{n}\})$ 比特信息[34,41].文献[40]讨论了存在泊松分布 Jammer 的情形,若信道噪声可以忽略不计,Jammer 的密度和功率不会影响隐蔽传输速率;若人工辅助噪声与信道噪声功率相近,隐蔽传输速率随干扰器的密度和功率的增大而增加.文献[73]进一步讨论了 Jammer 策略问题,若 Bob 和 Willie 同时受干扰器影响,干扰器策略与双方信道参数有关;若 Bob 不受影响,则干扰器策略仅与 Willie 信道参数相关.文献[33]讨论了当 Alice 一侧存在 Jammer 时可使得信道传输速率最大的功率分配方案.若全双工接收方在接收消息的同时发送人工辅助噪声,此时接收方的人工辅助噪声既导致隐蔽传输受到干扰也使得隐蔽通信速率为正[35].文献[36]进一步优化了全双工接收方人工辅助噪声功率的分配策略,在时延约束的通信场景下,全双工接收方发出人工辅助噪声功率为恒定值时为最佳情况[37].

3)中继通信场景

由于无线隐蔽通信采用很低的信号功率进行通信,其通信距离难以满足长距离通信的场景需要,因此引入一个或者多个中继 Relay 节点是可有效扩展通信距离的实际场景.文献[42]讨论了具有隐蔽传输功能的中继节点为实现最大隐蔽传输速率,对应的通信速率受限模式与功率受限模式的切换条件.文献[43]分析了当隐蔽中继节点采取时分模式与功率分割模式传输信息时,隐蔽通信速率相同.文献[44]分析了在分组衰落信道中,当中继节点作为合作干扰器发射随机功率的人工辅助噪声时,可增加隐蔽传输的安全性.文献[45]讨论了衰落中继信道中存在两个非合谋检测方的情形,给出了信息与密钥的最优比例系数.文献[74]讨论了当发送方距离接收方过远且存在多个协作检测方时,多跳中继传输较单跳传输在隐蔽性上有明显提高.在中继网络中,Willie 信道噪声的不确定性能使得 $n$ 个信道时频单位仍仅能可靠传输 $\mathcal{O}(n)$ 比特信息[75].

4)其他通信场景

通信速率分析的研究还被进一步拓展到无线中继网络、MIMO 和广播通信等其他通信场景中.文献[46]假设 Willie 不清楚各路径噪声功率,MIMO 场景对应的理论隐蔽通信速率为正值.MIMO 场景下的高斯信道中,当天线数与时频资源数量有限时,平方根定律依旧成立[47].文献[48-49]分析了离散无记忆广播场景下的无线隐蔽信道速率.文献[76]讨论了存在多个接收者的场景中,发送方采取时分复用通信方式能取得更好地隐蔽通信速率的比例系数.进一步地,当信道时频资源有限时,隐蔽传输速率随信道时频资源数量的增加而变大[77-78].

分组衰落信道[79]、无人机网络[80]、IOT 网络[81]、慢衰落信道[82]、连续时间无限带宽的泊松信道[83]、连续时间无限带宽的高斯信道[84]、存在主动检测方[85]、多天线系统[86]以及后向散射通信系统[87]等情形下的理论隐蔽通信速率也得到了相应的研究.

### 3.3.2 信号层无线隐蔽通信方法

基于实际的无线电对抗情景,噪声式无线隐蔽通信方法通常假定 Willie 仅知道信道噪声的分布类型而不知道具体功率.为避免对正常通信的调制解调造成明显的影响,载密噪声的功率一般设置得较小.早期的噪声式无线隐蔽信道将信息嵌入在一段噪声序列的特征参数中.对于部分通信场景,信道噪声具有显著的尖峰脉冲特性,此时可以使用 $\alpha$ 稳定分布的载密噪声信号来携带信息.文献[50]提出了一种将信息嵌入到脉冲特征参数 $\alpha$ 中的无线隐蔽通信方法,Alice 将信息编码为具备不同脉冲特征参数 $\alpha$ 的噪声序列,Bob 通过估计脉冲特征参数 $\alpha$ 来提取信息.偏斜 $\alpha$ 稳定分布的信号也被用来设计无线隐蔽通信方法[51],Alice 将信息比特生成具有相反偏斜参数 $\beta$ 的噪声序列,使最终产生的噪声序列是无偏的,Bob 通过估计偏斜参数 $\beta$ 来提取信息.文献[53]分析了同步误差时对隐蔽通信可靠性的削弱作用,文献[88]针对该问题设计了导频辅助的同步算法,通过计算分数低阶协方差相关来实现同步,提高了隐蔽信道的可靠性.文献[89]优化了接收端的分数低阶协方差相关器,进一步提高了通信的可靠性.文献[90]提出了一种基于修正极值法的隐蔽通信方法,相较于传统参数估计器,该方法能够快速提取信息.高斯噪声序列也被用于设计无线隐蔽通信方法.文献[52]提出了一种通过修改连续高斯序列的相关系数来嵌入信息的方法.

叠加噪声与正常噪声差异使得基于噪声叠加的方法存在隐蔽性缺陷,引入随机噪声可一定程度地增强隐蔽性.典型的“污染星座图”方法即通过对扩展星座图进行旋转、混合随机噪声等操作来增加隐蔽性[55].文献[54]提出了一种基于信号复用的无线隐蔽通信方法,该方法通过在信号中叠加随机噪声来增强隐蔽性,并利用直接序列扩频来提高传输可

靠性.这种方法被进一步拓展到 MIMO 场景,并可根据路径特征值选择在信道衰落较小的路径上传输[91].文献[92]提出了一种在 MIMO 场景下通过同时修改控制信道与数据信道信号的无线隐蔽通信方法.引入随机噪声的机制需要额外的共享映射序列带宽和随机噪声额外功率的局限性[17].文献[56]提出了一种将信息直接调制成噪声信号并叠加到正常信号的方法,该方法根据参考信道噪声,通过星座图拟形调制直接将信息调制成与参考噪声统计分布相同的载密噪声信号,并直接叠加到载体信号上生成载密信号.

#### 3.3.3 信号层方法隐蔽性分析

目前尚无专门针对噪声式无线隐蔽通信的检测工作,部分隐蔽通信方法设计的文献中提及了一些衡量隐蔽性的指标.如文献[55]中,采用频域信号的误差矢量幅度、同向和正交方向分量、幅值以及相位、时域信号的功率时变特性和峰均比等信号分析特征来衡量隐蔽性,通过各特征是否在正常波动范围内取值,判断“星座图污染”方法的隐蔽性.文献[54]将去除了载体信号成分的残差信号作为检测分析对象,利用残差信号的峰度值、带内功率比以及分布不重叠值来衡量所提方案的隐蔽性.文献[56]以残差信号与正常信道噪声的 KS 距离以及残差信号的规则度来衡量所提方案的隐蔽性.

## 4 研究展望

无线隐蔽通信是无线通信与信息隐藏的交叉研究领域,这两个技术领域的发展必然会进一步推动无线隐蔽通信的发展.该领域经过近些年的研究产生了诸如噪声式无线隐蔽信道理论与方法、编码和调制冗余分析和利用等具有相对独立内涵的方向,针对无线隐蔽通信检测技术的研究也刚刚起步.总体来说,无线隐蔽通信仍有许多需要进一步深入解决和值得探索的新问题.

1)在链路层隐蔽通信方法设计方面,已经出现了一些链路层无线隐蔽通信混合时间式网络隐蔽信道的方法,进一步探讨链路层无线隐蔽通信混合网络隐蔽信道和物理层隐蔽通信的方法,并发展混合信道的协作方式会是一个潜在的研究方向.此外,随着无线通信技术的发展和推广使用,诸如 802.11ax 和 5G 以及物联网无线通信领域即将发展成为事实标准的 NB-IoT 和 LoRa 等将会很快成为实用的通信标准.这些新通信标准涉及的链路层、编码和调制层的冗余和信号形式将会启发研究人员提出新的无线隐蔽通信方法.

2)噪声式无线隐蔽信道容量在多种典型通信场景中已有许多理论成果.隐蔽通信速率的 SRL 定律已经在多种通信场景和信道模型中得到证明.关于噪声不确定性、信道不确定性和人工辅助噪声不确定性带来的突破 SRL 界的新结论还在逐渐完善中并仍然有许多新场景、组合场景和不同信道条件的工作需要进一步开展,尤其是拓展到有限块长域的一些理论结果还刚刚起步.此外,从理论分析的角度,带干扰的主动式 Willie 和 Alice 之间的博弈建模和优化策略等问题也有待深入研究.

3)噪声式无线隐蔽通信采用将信息转化为噪声后与载体进行叠加的形式,在实际通信方案设计过程面临的主要问题依然是低功率条件下的通信可靠性提高的问题,这涉及到波形、码字、编码、信道估计和补偿等方面的设计和优化,当前这方面的研究还非常有限.此外,实际通信方案还涉及隐蔽密钥交换、远距离中继节点传续方案等一系列技术问题也有待开展.

4)基于噪声信号的统计分布差异的假设检验是当前理论分析过程中常采用的隐蔽通信检测机制,然而针对具体噪声式隐蔽通信系统(如星座调制类、噪声模拟类等)检测的研究才刚刚起步.初步的研究表明基于隐蔽通信信号残差的统计特征能够实现较好的检测效果,然而这种方法依赖参考信号的选取,因此需要对参考信号模型进行精准建模,这在信道环境复杂的实际通信环境中是困难的.尚需研究不依赖具体参考信号的通用检测方法,以及可进一步实现隐蔽通信参数(如通信波形、通信速率等)估计的方法.此外,当在空间中可设置不同位置的多个检测器时,且针对有否干扰器的场景,如何利用多个检测器信号进行协同检测也是非常值得研究的问题.

## 5 结束语

无线隐蔽通信的研究方兴未艾,本文从网络通信和信息隐藏领域交叉的角度界定了无线隐蔽通信的研究范畴,对无线隐蔽通信的系统模型和主要能力要素进行了分析,总结并归纳了链路层和物理层无线隐蔽通信的理论与技术进展,具体涵盖了噪声式隐蔽信道容量的理论分析以及链路层、编码层、调制层和信号层中的无线隐蔽通信方法.论文最后分析并指出了需要进一步研究的问题.

## 参考文献
References

[1] Csiszar I, Korner J. Broadcast channels with confidential messages[J]. IEEE Transactions on Information Theory, 1978,24(3):339-348
[2] Gianvecchio S, Wang H N, Wijesekera D, et al. Model-based covert timing channels: automated modeling and evasion[M]// Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008: 211-230
[3] Kothari K, Wright M. Mimic: an active covert channel that evades regularity-based detection [J]. Computer Networks,2013,57(3):647-657
[4] Walls R J, Kothari K, Wright M. Liquid: a detection-resistant covert timing channel based on IPD shaping[J]. Computer Networks,2011,55(6):1217-1228
[5] Liu W W, Liu G J, Zhai J T, et al. Designing analog fountain timing channels: undetectability, robustness, and model-adaptation[J]. IEEE Transactions on Information Forensics and Security,2016,11(4):677-690
[6] Girling C G. Covert channels in LAN's[J]. IEEE Transactions on Software Engineering,1987,SE-13(2):292-296
[7] Frikha L, Trabelsi Z, El-Hajj W. Implementation of a covert channel in the 802.11 header[C]//2008 International Wireless Communications and Mobile Computing Conference, August 6-8, 2008. Crete Island, Greece. IEEE,2008:594-599
[8] Rezaei F, Hempel M, Peng D M, et al. Analysis and evaluation of covert channels over LTE advanced[C]//2013 IEEE Wireless Communications and Networking Conference (WCNC), April 7-10,2013. Shanghai, China. IEEE, 2013:1903-1908
[9] Szczypiorski K, Mazurczyk W. Hiding data in OFDM symbols of IEEE 802.11 networks[C]//2010 International Conference on Multimedia Information Networking and Security, November 4-6, 2010. Nanjing, China. IEEE, 2010:835-840
[10] Szczypiorski K, Mazurczyk W. Steganography in IEEE 802.11 OFDM symbols[J]. Security and Communication Networks,2016,9(2):118-129
[11] Grabska I, Szczypiorski K. Steganography in long term evolution systems[C]//2014 IEEE Security and Privacy Workshops, May 17-18,2014. San Jose, CA. IEEE, 2014: 92-99
[12] Liu J H, Chen W J, Wen Y X. A robust and flexible covert channel in LTE-A system[J]. Journal of Physics: Conference Series,2018,1087:062027
[13] He Z Q, Huang L S, Yang W, et al. A novel covert channel in LTE-A system[C]//2016 5th International Conference on Computer Science and Network Technology (ICCSNT), December 10-11, 2016. Changchun, China. IEEE,2016:662-666
[14] Xu G L, Yang W, Huang L S. Hybrid covert channel in LTE-A: modeling and analysis[J]. Journal of Network and Computer Applications,2018,111:117-126
[15] Wang Z K, Huang L S, Yang W, et al. A hybrid covert channel over LTE-A system[C]//Proceedings of the 3rd International Conference on Wireless Communication and Sensor Networks (WCSN 2016), December 10-11, 2016. Wuhan, China. Paris, France: Atlantis Press, 2017
[16] Grabski S, Szczypiorski K. Network steganalysis: detection of steganography in IEEE 802.11 wireless networks[C]//2013 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), September 10-13, 2013. Almaty, Kazakhstan. IEEE,2013:13-19
[17] Szczypiorski K, Janicki A, Wendzel S." The Good, The Bad And The Ugly": evaluation of Wi-Fi steganography [J]. Computer Science,2015
[18] Wang Z K, Huang L S, Yang W, et al. An entropy-based method for detection of covert channels over LTE[C]// 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD), May 9-11,2018. Nanjing. IEEE,2018:872-877
[19] Wang Z K, Huang L S, Yang W, et al. A classifier method for detection of covert channels over LTE[C]//2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), October 12-14,2017. Nanjing, China. IEEE,2017:454-460
[20] 闫雪虎.基于纠错码的信息隐藏容量模型[J].计算机工程,2010,36(3):172-173,176
YAN Xuehu. Information hiding capacity model based on error-correcting codes[J]. Computer Engineering, 2010, 36(3):172-173,176
[21] Kho T. Steganography in the 802.15.4 physical layer[J]. UC Berkeley,2007
[22] Mehta A M, Lanzisera S, Pister K S J. Steganography in 802.15.4 wireless communication[C]//2008 2nd International Symposium on Advanced Networks and Telecommunication Systems, December 15-17, 2008. Mumbai, India. IEEE,2008:1-3
[23] Zielinska E, Szczypiorski K. Direct sequence spread spectrum steganographic scheme for IEEE 802.15.4[C]// 2011 Third International Conference on Multimedia Information Networking and Security, November 4-6, 2011. Shanghai, China. IEEE,2011:586-590
[24] Nain A K, Rajalakshmi P. A reliable covert channel over IEEE 802.15.4 using steganography[C]//2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), December 12-14, 2016. Reston, VA, USA. IEEE, 2016: 711-716
[25] Ma H T, Yi X W, Wu X H, et al. A capacity self-adaption information hiding algorithm based on RS code[C]// 2014 International Conference on Multisensor Fusion and Information Integration for Intelligent Systems (MFI), September 28-29,2014. Beijing, China. IEEE,2014:1-8
[26] Grabska I, Szczypiorski K. Steganography in WiMAX networks[C]//2013 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), September 10-13, 2013. Almaty, Kazakhstan. IEEE,2013:20-27
[27] Harley P M B, Tummala M, McEachen J C. High-throughput covert channels in adaptive rate wireless communication systems[C]//2019 International Conference on

Electronics, Information, and Communication (ICEIC), January 22-25, 2019. Auckland, New Zealand. IEEE, 2019:1-7
[28] Grabski S, Szczypiorski K. Steganography in OFDM symbols of fast IEEE 802.11n networks[C]//2013 IEEE Security and Privacy Workshops, May 23-24, 2013. San Francisco, CA. IEEE, 2013:158-164
[29] Praveenkumar P, Thenmozhi K K, Vivekhanandan S, et al. Intersect embedding on OFDM channel: a stego perspective[C]//2013 IEEE Conference on Information & Communication Technologies, April 11-12, 2013. Thuckalay, Tamil Nadu, India. IEEE, 2013:1211-1214
[30] Hijaz Z, Frost V S. Exploiting OFDM systems for covert communication[C]//2010-Milcom 2010 Military Communictions Conference, October 31-November 3, 2010. San Jose, CA, USA. IEEE, 2010:2149-2155
[31] Shabsigh G, Frost V S. Covert communications in wideband OFDMA primary networks[C]//2015 IEEE Globecom Workshops (GC Wkshps), December 6-10, 2015. San Diego, CA, USA. IEEE, 2015
[32] Bash B A, Goeckel D, Towsley D. Limits of reliable communication with low probability of detection on AWGN channels[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9):1921-1930
[33] Yan S H, Zhou X Y, Yang N, et al. Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation[J]. IEEE Transactions on Wireless Communications, 2016, 15(12):8286-8297
[34] Liu Z H, Liu J J, Zeng Y, et al. On covert communication with interference uncertainty[C]//2018 IEEE International Conference on Communications (ICC), May 20-24, 2018. Kansas City, MO. IEEE, 2018:1-6
[35] Hu J S, Shahzad K, Yan S H, et al. Covert communications with a full-duplex receiver over wireless fading channels [C]// 2018 IEEE International Conference on Communications (ICC), May 20-24, 2018. Kansas City, MO. IEEE, 2018:1-6
[36] Shahzad K, Zhou X Y, Yan S H, et al. Achieving covert wireless communications using a full-duplex receiver[J]. IEEE Transactions on Wireless Communications, 2018, 17(12):8517-8530
[37] Shu F, Xu T Z, Hu J S, et al. Delay-constrained covert communications with a full-duplex receiver [J]. IEEE Wireless Communications Letters, 2019, 8(3):813-816
[38] Sobers T V, Bash B A, Goeckel D, et al. Covert communication with the help of an uninformed jammer achieves positive rate[C]//2015 49th Asilomar Conference on Signals, Systems and Computers, November 8-11, 2015. Pacific Grove, CA, USA. IEEE, 2015:625-629
[39] Soltani R, Bash B, Goeckel D, et al. Covert single-hop communication in a wireless network with distributed artificial noise generation[C]//2014 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton), September 30-October 3, 2014. Monticello, IL, USA. IEEE, 2014:1078-1085
[40] He B, Yan S H, Zhou X Y, et al. Covert wireless communication with a Poisson field of interferers [J]. IEEE Transactions on Wireless Communications, 2018, 17(9):6005-6017
[41] Soltani R, Goeckel D, Towsley D, et al. Covert wireless communication with artificial noise generation[J]. IEEE Transactions on Wireless Communications, 2018, 17(11):7252-7267
[42] Hu J S, Yan S H, Zhou X Y, et al. Covert communication achieved by a greedy relay in wireless networks[J]. IEEE Transactions on Wireless Communications, 2018, 17(7):4766-4779
[43] Hu J S, Yan S H, Shu F, et al. Covert transmission with a self-sustained relay[J]. IEEE Transactions on Wireless Communications, 2019, 18(8):4089-4102
[44] Shahzad K. Relaying via cooperative jamming in covert wireless communications[C]//2018 12th International Conference on Signal Processing and Communication Systems (ICSPCS), December 17-19, 2018. Cairns, Australia. IEEE, 2018:1-6
[45] Kumar Arumugam K S, Bloch M R, Wang L G. Covert communication over a physically degraded relay channel with non-colluding wardens [C] // 2018 IEEE International Symposium on Information Theory (ISIT), June 17-22, 2018. Vail, CO, USA. IEEE, 2018:766-770
[46] Lee S, Baxley R J, McMahon J B, et al. Achieving positive rate with undetectable communication over MIMO rayleigh channels[C]//2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM), June 22-25, 2014. A Coruna, Spain. IEEE, 2014:257-260
[47] Abdelaziz A, Koksal C E. Fundamental limits of covert communication over MIMO AWGN channel[C]//2017 IEEE Conference on Communications and Network Security (CNS), October 9-11, 2017. Las Vegas, NV. IEEE, 2017:1-9
[48] Arumugam K S K, Bloch M R. Covert communication over broadcast channels[C]//2017 IEEE Information Theory Workshop (ITW), November 6-10, 2017. Kaohsiung. IEEE, 2017:299-303
[49] Kumar Arumugam K S, Bloch M R. Embedding covert information in broadcast communications[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(10):2787-2801
[50] Cek M E, Savaci F A. Stable non-Gaussian noise parameter modulation in digital communication[J]. Electronics Letters, 2009, 45(24):1256
[51] Cek M E. Covert communication using skewed α-stable distributions[J]. Electronics Letters, 2015, 51(1):116-118
[52] Xu Z J, Gong Y, Wang K, et al. Covert digital communication systems based on joint normal distribution[J]. IET Communications, 2017, 11(8):1282-1290
[53] Ahmed A, Savaci F A. Measure of covertness based on the imperfect synchronization of an eavesdropper in random communication systems [C] // 2017 10th International Conference on Electrical and Electronics Engineering (ELECO). IEEE, 2017:638-641
[54] Kitano T, Iwai H, Sasaoka H. A wireless steganography technique by embedding DS-SS signal in digital mobile communication systems [J]. Science & Engineering Review of Doshisha University, 2011, 52:127-134

[55] Dutta A,Saha D,Grunwald D,et al.Secret agent radio:covert communication through dirty constellations[M]// Information Hiding. Berlin, Heidelberg: Springer Berlin Heidelberg,2013:160-175
[56] Cao P C,Liu W W,Liu G J,et al.A wireless covert channel based on constellation shaping modulation [J]. Security and Communication Networks,2018,2018:1-15
[57] Simmons G J.The prisoners' problem and the subliminal channel[M] // Advances in Cryptology. Boston, MA: Springer US,1984:51-67
[58] Zhao H. Covert channels in 802. 11e wireless networks [C] // 2014 Wireless Telecommunications Symposium, April 9-11,2014.Washington,DC,USA.IEEE,2014:1-5
[59] Classen J,Schulz M,Hollick M.Practical covert channels for WiFi systems[C]//2015 IEEE Conference on Communications and Network Security (CNS),September 28-30,2015.Florence,Italy.IEEE,2015:209-217
[60] Ker A D,Pevný T,Kodovský J,et al.The square root law of steganographic capacity[C]//Proceedings of the 10th ACM workshop on Multimedia and Security, September 22-23, 2008. Oxford, United Kingdom. New York, USA: ACM Press,2008:107-116
[61] Ker A D.The square root law of steganography:bringing theory closer to practice[C]//Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security,2017:33-44
[62] Bash B A, Goeckel D, Towsley D, et al. Hiding information in noise:fundamental limits of covert wireless communication [J]. IEEE Communications Magazine, 2015,53(12):26-31
[63] Che P H,Bakshi M,Jaggi S.Reliable deniable communication:hiding messages in noise[C]//2013 IEEE International Symposium on Information Theory, July 7-12, 2013.Istanbul,Turkey.IEEE,2013:2945-2949
[64] Wang L G,Wornell G W,Zheng L Z.Limits of low-probability-of-detection communication over a discrete memoryless channel[C]//2015 IEEE International Symposium on Information Theory (ISIT), June 14-19, 2015. Hong Kong,China.IEEE,2015:2525-2529
[65] Wang L G,Wornell G W,Zheng L Z.Fundamental limits of communication with low probability of detection[J]. IEEE Transactions on Information Theory,2016,62(6):3493-3503
[66] Bloch M R.Covert communication over noisy channels:a resolvability perspective[J].IEEE Transactions on Information Theory,2016,62(5):2334-2354
[67] Arumugam K S K,Bloch M R.Keyless covert communication over multiple-access channels[C]//2016 IEEE International Symposium on Information Theory (ISIT), July 10-15, 2016. Barcelona, Spain. IEEE, 2016: 2229-2233
[68] Arumugam K S K,Bloch M R.Covert communication over a K-user multiple-access channel[J].IEEE Transactions on Information Theory,2019,65(11):7020-7044
[69] Bash B A, Goeckel D, Towsley D. LPD communication when the warden does not know when[C]//2014 IEEE International Symposium on Information Theory,June 29-July 4,2014.Honolulu,HI,USA.IEEE,2014:606-610
[70] Goeckel D,Bash B,Guha S,et al.Covert communications when the warden does not know the background noise power[J].IEEE Communications Letters,2016,20(2):236-239
[71] Lee S,Baxley R J,Weitnauer M A,et al.Achieving undetectable communication[J].IEEE Journal of Selected Topics in Signal Processing,2015,9(7):1195-1205
[72] He B, Yan S H, Zhou X Y, et al. On covert communication with noise uncertainty[J].IEEE Communications Letters,2017,21(4):941-944
[73] Shmuel O,Cohen A,Gurewitz O.Jamming strategies in covert communication[M]// Lecture Notes in Computer Science.Cham:Springer International Publishing,2019:1-15
[74] Sheikholeslami A,Ghaderi M,Towsley D,et al.Multi-hop routing in covert wireless networks[J].IEEE Transactions on Wireless Communications,2018,17(6):3656-3669
[75] Wang J Q,Tang W B,Zhu Q Q,et al.Covert communication with the help of relay and channel uncertainty[J]. IEEE Wireless Communications Letters, 2019, 8(1): 317-320
[76] Tan V Y F,Lee S H.Time-division is optimal for covert communication over some broadcast channels[J].IEEE Transactions on Information Forensics and Security, 2018,14(5):1377-1389
[77] Yan S H,He B,Cong Y R,et al.Covert communication with finite blocklength in AWGN channels[C]//2017 IEEE International Conference on Communications (ICC),May 21-25,2017.Paris,France.IEEE,2017:1-6
[78] Yan S H,He B,Zhou X Y,et al.Delay-intolerant covert communications with either fixed or random transmit power[J].IEEE Transactions on Information Forensics and Security,2019,14(1):129-140
[79] Shahzad K,Zhou X Y,Yan S H.Covert communication in fading channels under channel uncertainty[C]//2017 IEEE 85th Vehicular Technology Conference (VTC Spring),June 4-7,2017.Sydney,NSW.IEEE,2017:1-5
[80] Zhou X B,Yan S H,Hu J S,et al.Joint optimization of a UAV's trajectory and transmit power for covert communications[J].IEEE Transactions on Signal Processing, 2019,67(16):4276-4290
[81] Liu Z H,Liu J J,Zeng Y,et al.Covert wireless communications in IoT systems:hiding information in interference [J].IEEE Wireless Communications, 2018, 25(6): 46-52
[82] Tang H Y,Wang J T,Zheng Y R.Covert communications with extremely low power under finite block length over slow fading[C]//IEEE Infocom 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), April 15-19, 2018. Honolulu, HI. IEEE, 2018:657-661
[83] Wang L G.The continuous-time Poisson channel has infinite covert communication capacity[C]//2018 IEEE International Symposium on Information Theory (ISIT), June 17-22,2018.Vail,CO,USA.IEEE,2018:756-760
[84] Wang L G.On covert communication over infinite-bandwidth Gaussian channels[C]//2018 IEEE 19th International Workshop on Signal Processing Advances in Wire-

less Communications (SPAWC), June 25-28, 2018. Kalamata.IEEE,2018:1-5
[85] Zhang Q E,Bakshi M,Jaggi S.Covert communication over adversarially jammed channels[C]//2018 IEEE Information Theory Workshop (ITW),November 25-29,2018. Guangzhou.IEEE,2018:1-5
[86] Zheng T X, Liu H W, Zhao B Q, et al. Multi-antenna covert communications in random wireless networks [J]. IEEE Transactions on Wireless Communications, 2019, 18(3):1974-1987
[87] Shahzad K,Zhou X Y,Yan S H.Covert communication in fading channels under channel uncertainty[J].arXiv Preprint,2017,arXiv:1703. 02169[cs.IT]
[88] Ahmed A, Savaci F A. Synchronisation of alpha-stable levy noise-based Random Communication System[J].IET Communications,2018,12(3):276-282
[89] Ahmed A, Savaci F A. On optimizing fractional lower order covariance based synchronization method for random communication systems[C]//2018 26th Signal Processing and Communications Applications Conference (SIU),May 2-5,2018.Izmir,Turkey.IEEE,2018:1-4
[90] Ahmed A, Savaci F A. Random communication system based on skewed alpha-stable levy noise shift keying[J]. Fluctuation and Noise Letters,2017,16(3):1750024
[91] Hokai K, Sasaoka H, Iwai H. Wireless steganography using MIMO system[C]//2014 IEEE Fifth International Conference on Communications and Electronics (ICCE), July 30-August 1,2014.Danang,Vietnam.IEEE,2014
[92] Wang X S, Liu Y, Lu X, et al. CovertMIMO: a covert uplink transmission scheme for MIMO systems[C]// 2017 IEEE International Conference on Communications (ICC),May 21-25,2017.Paris,France.IEEE,2017:1-6

# A survey of wireless covert communications

DAI Yuewei[1] LIU Guangjie[1] CAO Pengcheng[2] LIU Weiwei[2] ZHAI Jiangtao[1]
1 School of Electronic and Information Engineering,Nanjing University of Information Science and Technology,Nanjing 210044
2 School of Automation,Nanjing University of Science and Technology,Nanjing 210094

**Abstract** Wireless covert communication is the technology of hiding messages in wireless communication data frames and signals for covert transmission, which belongs to the cross-field of wireless communication and information hiding technology.This paper analyzes the system model and main ability factors of wireless covert communication,summarizes the theory of noise-type covert channel capacity and the research progress of wireless covert communication technology in link layer,coding layer,modulation layer and signal layer,and gives the problems that need further study.

**Key words** wireless covert communication;information hiding;covert channel