

## 蓝牙技术数据传输综述

钱志鸿<sup>1</sup>, 刘丹<sup>2</sup>

(1. 吉林大学 通信工程学院, 吉林 长春 130025; 2. 大连海洋大学 信息工程学院, 辽宁 大连 116023)

**摘要:** 比较了蓝牙协议各个版本对其数据传输性能的影响, 分类讨论了分组选择算法、重传机制、数据传输的干扰及安全等。针对目前存在的问题, 提出了引入扩展戈莱编码和最小频移键控(MSK)调制的数据分组改进方案, 提高了系统的抗干扰性和吞吐量, 并提出了基于信道转换与 MSK 调制的同频干扰抑制方法, 使皮可网的载干比和吞吐量有明显改善, 最后总结并对未来工作提出设想和展望。

**关键词:** 无线通信; 蓝牙; 数据传输; 干扰; 安全

中图分类号: TN92

文献标识码: A

文章编号: 1000-436X(2012)04-0143-09

## Survey on data transmission in Bluetooth technology

QIAN Zhi-hong<sup>1</sup>, LIU Dan<sup>2</sup>

(1. College of Communication Engineering, Jilin University, Changchun 130025, China;

2. College of Information Engineering, Dalian Ocean University, Dalian 116023, China)

**Abstract:** The different impact assessments on performance of data transmission of multiple Bluetooth protocol versions were analyzed. Packet selection algorithms, retransmission mechanisms, interference and security were discussed respectively. Strategies, employing extended-golay code and minimum frequency shift keying (MSK) modulation were proposed, which enhanced the probability of anti-interference and throughput of data packet. Moreover, a co-channel interference suppression approach based on channel switching and MSK modulation was proposed, which improved the carrier to interference ratio and throughput in piconets. Finally, the work was summarized and expectations as well as premeditation of the future were presented.

**Key words:** wireless communications; Bluetooth; data transmission; interference; security

### 1 引言

蓝牙技术是一种无线数据与语音通信的开放性全球规范, 它以低成本的短距离无线通信为基础, 为固定与移动设备的通信环境提供特别连接的通信技术。由于蓝牙技术具有可以方便快速地建立无线连接、移植性较强、安全性较高且蓝牙地址唯一、支持皮可网与分散网等组网工作模式、设计开发简单等优点<sup>[1]</sup>, 蓝牙技术近几年来在众多短距离

无线通信技术中备受关注。

众所周知, 数据传输是实现数据通信的基础。以往的数据传输采用的是有线连接方式, 其优点是传输速度快、安全性高以及实现简单, 但随着生产以及生活需求越来越大, 要求越来越高, 有线连接已经逐渐显现出自身的不足, 例如传输距离有限、成本高和布线困难等, 这些因素严重制约了其发展。为了解决有线传输带来的不便, 很多研究人员开始考虑尝试以无线的方式实现数据交换。由于无

收稿日期: 2011-11-08; 修回日期: 2012-02-20

基金项目: 国家自然科学基金资助项目(61071073); 教育部高等学校博士学科点专项科研基金资助项目(20090061110043)

**Foundation Items:** The National Natural Science Foundation of China (61071073); The Specialized Research Fund for the Doctoral Program of higher Education of China (20090061110043)

线传输技术自身的特点,可以有效解决有线传输带来的不便,使现有的数据传输不再需要繁重的布线,而且数据传输方便快捷,所以对于无线数据传输技术的研究有着重大的意义。

近些年,无线传输技术得到了迅猛发展,相继出现了红外技术、HomeRF、蓝牙<sup>[2]</sup>、无线局域网(WLAN, wireless local area network)、ZigBee、RFID等,这些技术都有各自的优势和应用领域,大大改善了现有的数据传输方式。

现有的无线通信技术各有特点,并且在很大程度上与蓝牙技术相互补充。蓝牙技术由于成本低、功耗低和组网容易等特点,在无线数据传输领域得到了广泛的应用。目前,对于蓝牙技术的研究,大部分集中在数据传输性能的改善方面。杨帆等集中研究了蓝牙技术数据传输的网络拓扑问题,给出了改进的拓构成算法,增强了网络的可拓展性<sup>[3,4]</sup>。HAGER 和 BANDYOPADHYAY 等对蓝牙技术安全方面存在的问题进行了大量的分析,指出蓝牙技术在安全方面仍存在不足,包括蓝牙技术的认证、PIN 码的安全以及匹配问题等<sup>[5-7]</sup>。GOLMIE 等对蓝牙设备与 802.11 设备共存时的相互干扰情况进行了详细的分析并提出了解决方案<sup>[8]</sup>。CHEN 等研究了平均接收信噪比与分组错误概率间的关系<sup>[9]</sup>。

本文首先从协议方面分析了数据传输性能的改善,然后讨论了现有关于蓝牙技术数据传输的研究,指出了各个方案的优缺点,并提出了相应的改进构想和今后的研究展望。

## 2 蓝牙协议标准中数据传输的演进过程

自从完成了第 1 版蓝牙标准的制定以来,蓝牙特别兴趣小组(SIG, special interesting group)仍然持续不断地对蓝牙技术进行修正与改版的工作,目的是期望蓝牙技术能够充分满足系统产品更易于使用的需求,尤其是蓝牙技术数据传输方面的需求,如数据传输速率、能耗以及安全问题等。因此不断演进的蓝牙标准版本,对于整体蓝牙技术的发展带来了至关重要的影响。

蓝牙规范 1.0 版本主要是针对点对点的无线数据传输,给出了标准的数据传输分组格式以及分组类型。随后的 1.1 版本将 1.0 版本的点对点扩展为点对多点的数据传输,并修正了前一版本中错误和模糊的概念。蓝牙技术 1.1 版本规定的传输速率峰值为 1Mbit/s,而实际应用中的是 723kbit/s。蓝牙技术 1.2 版

本的传输速率与 1.1 版本相同,但实现了设备识别的高速化,增强了数据传输的抗干扰能力,与现有的 1.1 版本完全兼容,确保其向后兼容 1.1 版本的产品<sup>[10]</sup>。蓝牙协议规范 1.2 版本中有以下的改进和增强:更加快速地连接、自适应跳频(AFH, adaptive frequency hopping)、扩展的同步面向连接链路、增强的错误检测与信息流、增强的同步能力、增强的流规范等<sup>[11]</sup>。这些改进可以增加数据传输的抗干扰性和可靠性,为其实时传输提供了有力支撑。

从蓝牙 2.0 版本开始,增加了增强型数据速率(EDR, enhanced data rate)协议,大大提高了蓝牙技术数据传输的性能。它的主要特点是数据传输速率可达 1.2 版本传输速率的 3 倍(在某些情况下可高达 10 倍),各版本的数据传输速率比较如图 1 所示。

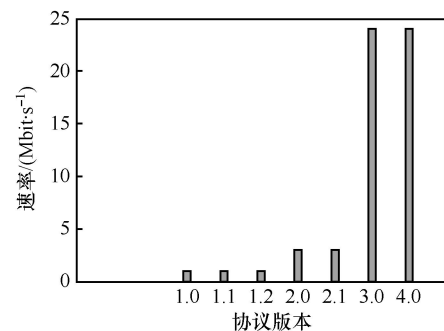


图 1 各协议版本数据传输速率的比较

2.0 版本通过减少工作负载循环降低了能源消耗,增加带宽简化了多连接模式,可与以往的蓝牙规范兼容,降低了比特误差率<sup>[12]</sup>。蓝牙 2.1+EDR 标准在 2.0 版本的基础上对数据传输的性能加以改善,具有 3 个主要特征:改善装置配流程、节约能源和增强安全性等<sup>[13]</sup>。

目前,较新的版本是蓝牙技术联盟在 2009 年 4 月颁布的蓝牙 3.0+HS 高速核心规范和在 2009 年 12 月颁布的蓝牙 4.0 低功耗核心规范。前者采用交替射频技术,并且集成了 IEEE 802.11 协议适应层,使蓝牙数据传输速率提高至 24Mbit/s。此外,蓝牙 3.0+HS 还增加了单播无连接数据传输模式和增强功率控制等新功能<sup>[14]</sup>。蓝牙规范 4.0 可以说是蓝牙 3.0+HS 规范的补充,降低了蓝牙技术数据传输的能耗<sup>[15]</sup>,这个版本主要应用在医疗保健、运动与健身、安全及家庭娱乐等全新的市场。

## 3 蓝牙技术数据传输的研究

现有关于蓝牙技术数据传输的研究主要集中在

在以下几个方面: 数据分组的选择对于传输性能的影响、数据传输过程中的干扰和数据传输过程中的安全等问题。

### 3.1 蓝牙技术数据传输性能分析

基于蓝牙技术的无线数据传输过程主要由传输层协议来管理, 该层负责蓝牙设备间对方位置的确认, 以及建立和管理蓝牙设备之间的物理与逻辑链路。除此之外传输协议又可细分为底层传输协议和高层传输协议 2 个重要部分。底层传输协议侧重语音与数据无线传输的实现, 主要包括射频、基带和链路管理协议 3 个部分; 高层传输协议主要包括逻辑链路控制与适配层协议和主机控制器接口, 其主要功能包括: 为高层应用程序屏蔽诸如跳频序列选择等底层传输操作; 为高层应用程序的实现提供更加有效和易于实现的数据分组格式。

#### 3.1.1 蓝牙技术底层数据传输分组选择

通信设备间物理层的数据传输连接通道就是物理链路<sup>[1]</sup>, 为此蓝牙协议定义了 2 种类型的链路: 同步面向连接链路和异步无连接链路 (ACL, asynchronous connectionless link)。蓝牙皮可网采用分组形式进行数据传输, 基带层给出了 2 种分组格式: 一种是蓝牙协议 1.0 中规定的标准分组格式, 主要由接入码、分组头和有效载荷 3 部分组成; 另一种是蓝牙协议 2.0+EDR 版本提出的增强型数据分组格式, 将其原有分组格式的有效载荷部分分成同步码、净荷和尾码 3 个部分, 保留了原有的接入码和分组头 2 个部分, 数据部分采用相移键控 (PSK, phase shift keying) 调制方式, 并在数据分组中引入了保护周期。

蓝牙皮可网中使用的分组类型与使用的物理链路有关。对于蓝牙数据传输链路, 协议给出了如下分组类型: DM1 分组、DH1 分组、DM3 分组、DH3 分组、DM5 分组、DH5 分组、AUX1 分组、HV1 分组、HV2 分组、HV3 分组和 DV 分组。2.0 规范新增了 2-DH1 分组、2-DH3 分组、2-DH5 分组、3-DH1 分组、3-DH3 分组和 3-DH5 分组等。

现有的关于蓝牙技术底层数据传输的研究主要集中在数据分组选择问题上, 由于协议给出的分组类型性能各不相同, 如数据载荷的大小和采用的纠错机制等, 对数据传输性能会产生很大的影响。针对此问题, 国内外的研究人员均已取得了一定的进展。SARKAR 等在假设信道状态已知的情况下,

利用所建立的数学模型求出吞吐量最大时数据分组大小的最优值, 进一步提高了系统的整体性能<sup>[16]</sup>。杨帆等分析了蓝牙 2.0+EDR 新规范定义的 3 种调制方式在加性高斯白噪声 (AWGN, additive white Gaussian noise) 信道下的位错误率与平均接收信噪比的关系, 根据不同分组的特性, 提出了在 AWGN 信道下的自适应分组选择策略<sup>[17]</sup>。徐飞等在原有的蓝牙 2.0+EDR 协议中加入采用 BCH 编码的数据分组, 有效提高了蓝牙数据传输效率、抗干扰能力以及在 AWGN 信道下的数据传输吞吐量<sup>[18]</sup>。

杨帆等提出了一种基于信噪比的蓝牙自适应分组类型选择方法。其原理就是根据接收信噪比的不同情况选择最佳的分组类型进行传输, 给出了进行分组类型切换时信噪比的门限值, 改善了在信道状态不佳时的系统性能<sup>[19]</sup>。

JU 等提出了一种基于信道估计的蓝牙系统分组选择策略, 针对不同信道误比特率的差异, 结合现有蓝牙数据分组的特点, 提高了原有系统的吞吐量。这种自适应分组选择策略不仅可以有效地提高系统吞吐量, 还能够降低数据传输的延迟, 在一定程度上可以解决无线个域网的信息拥塞问题<sup>[20]</sup>。

因此, 不同误码率和数据分组对于系统吞吐量的影响是有差异的。当系统不存在干扰或者干扰很小的时候, 小时隙的分组会增加数据分组的冗余开销, 降低吞吐量。但是如果存在干扰, 小时隙的分组可降低基带分组传输期间受到干扰的可能性, 减少出错重传的概率。以上的参考文献虽然给出了自适应分组选择策略, 但在不改变蓝牙硬件的基础上, 得到或者准确估计和跟踪信道质量是比较困难的, 所以分组选择的难点在于如何估计或者判断信道质量。

基于以上问题, 王雪等提出把不同误码率下的最佳分组按照其吞吐量进行分级, 并计算出分组吞吐量临界点的重传次数, 同时与每个分组的平均重传次数比较, 调整分组区间上下限的级别以得到该区间的最佳分组类型。该方法通过实时跟踪信道质量, 做出相应的分组选择策略, 尤其对于不稳定的信道, 大大提高了系统的性能<sup>[21]</sup>。

数据分组选择虽然可以有效改善蓝牙技术数据传输的性能, 但是分组本身还存在一定的不足, 例如 DH 分组载荷部分没有任何差错控制机制, 当信道环境较差时, 会严重影响蓝牙数据分组的传输性能。针对这个问题, 可以尝试对 DH 分组的载荷

部分采取合理的编码方式,纠正随机发生的比特错误,进而降低数据分组的重传次数,提高蓝牙技术数据传输的性能。现有的纠错编码方式有很多,例如 BCH 码<sup>[22]</sup>、RS 码、汉明码和 Turbo 码<sup>[23]</sup>等,由于每种编码方式的复杂度和纠错能力都存在差异,所以可根据不同的应用需求选择适合蓝牙技术数据分组的编码方式以保证数据分组在环境质量较差情况下的传输性能。

针对 EDR 格式分组本身存在抗干扰能力差的问题,本文为 EDR 格式分组引入了扩展戈莱编码方法。EDR 格式数据分组有效载荷部分采用扩展戈莱编码(24,12),该编码可以纠正随机的 3bit 错误,在低信噪比或环境质量较差的情况下有效降低蓝牙 EDR 分组出错的概率,提高蓝牙数据分组的吞吐量。与此同时,由于分组误比特率与所采用的调制方式存在一定的函数关系,因此调制方式性能的好坏影响了蓝牙数据分组的传输性能。从蓝牙 2.0+EDR 版本开始,数据载荷部分分别采用 8DPSK (differential phase shift keying) 和  $\pi/4$ -DQPSK (differential quadrature reference phase shift keying)2 种调制方式。

如果引入最小频移键控(MSK, minimum shift keying)调制方式,随着比特信噪比的增加,MSK 调制方式的误比特率要优于以上 2 种调制方式,如图 2 所示。因此,将扩展戈莱编码与 MSK 调制方式相结合的方法可以有效改善蓝牙数据分组的抗干扰能力。改进后的新增 DH 分组在信噪比为 3dB 时,吞吐量就呈明显上升趋势,较协议原有的新增 DH 数据分组提高近 5dB,如图 3 所示。

可见,本文提出的将扩展戈莱编码与 MSK 调制方式相结合的数据分组改进方案可以提高信噪比较低情况下的数据分组可靠性,并且可以进一步提高数据分组的抗干扰性能和吞吐量。

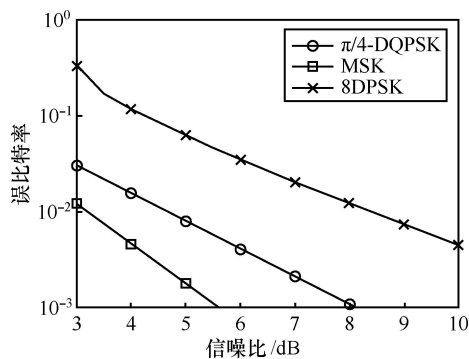


图 2 3 种调制方式误比特率比较

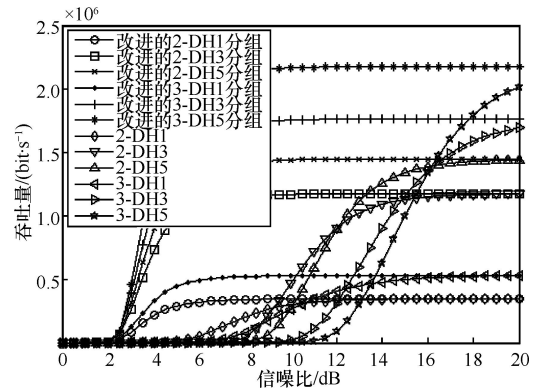


图 3 采用 MSK 调制方法与扩展戈莱编码后 DH 分组性能的改善

### 3.1.2 蓝牙技术高层数据传输重传机制

为了实现高层应用,高层传输协议提供了更加有效和易于实现的数据分组格式。其中较重要的逻辑链路及适配协议负责将基带层的数据分组转换为便于高层应用的数据分组格式,并提供协议复用和服务质量交换等功能。

蓝牙协议体系结构中的逻辑链路及适配协议(L2CAP, logical link control and adaptation protocol)处于基带协议的上层并与蓝牙服务搜索协议、串口仿真协议和电话控制等其他通信协议具有通信接口。L2CAP 是基于分组的,但是其通信模型是基于信道的。一个信道表示的是 2 个 L2CAP 实体之间的数据流。信道既可以是面向连接的,也可以是无连接的。L2CAP 层协议定义了 4 种数据帧结构,以满足不同数据传输的需要。例如基本 L2CAP 模式下的面向连接信道采用 B-帧,数据帧包括长度字段、信道 ID 以及信息载荷 3 个部分;对于无连接信道则采用 G-帧,与前者不同在于该帧引入了协议/服务复用字段,并且信道 ID 为 0x0002,用于数据成员的加入与剔除;为了保证数据传输的可靠性,该协议层采用了数据重传机制,引入的 S-帧和 I-帧负责 L2CAP 实体间信息的监控和传输。

现有的关于蓝牙 L2CAP 层的研究主要集中在该层的自动请求重传(ARQ, automatic repeat request)机制上。传统的重传机制有 3 种:停等式 ARQ 机制、回退 N 帧 ARQ 机制和选择重传 ARQ<sup>[24]</sup>机制,其性能比较如表 1 所示。

重传机制	效率	复杂度	存储空间	信道利用率
停等式	低	低	低	低
回退 N 帧	较高	较高	低	高
选择重传	高	高	高	高

停等式 ARQ 机制, 实现简单, 但其信道利用率较低; 回退 N 帧 ARQ 机制, 信道利用率要优于前者, 但是在信道条件较差的情况下, N 帧将会很大, 这将严重影响数据传输的吞吐量; 选择重传 ARQ 机制, 可以有效地解决前两者存在的问题, 而且信道利用率高, 吞吐量等性能也优于前两者。由以上分析可知, 合理地选择重传机制有利于提高数据传输的效率和可靠性。近几年, 对于数据重传机制的研究也取得了一定的成果。VALENTI 等人研究了加性高斯白噪声与瑞利衰落信道下分组重传的概率与蓝牙链路吞吐量的关系<sup>[25]</sup>。RAZAVI 等提出一种基于模糊控制的自适应 ARQ 机制, 通过对发送缓存器剩余空间的监测, 运用模糊控制的方法决定数据分组的重传次数, 这种机制有效地降低了数据传输过程中的分组丢失率<sup>[26]</sup>。CYRIL 等针对现有的 ARQ 协议进行了比较分析, 给出了引入 BCH 错误检测码对于停止等待 ARQ 协议性能的改善方法, 并分析了前向纠错码对于系统时延的影响<sup>[27]</sup>。

L2CAP 层所采用的是回退 N 帧的 ARQ<sup>[28]</sup>机制, 该机制一方面因连续发送数据帧可以提高效率, 但另一方面, 在重传时又必须把原来已正确传送过的数据帧重复传送, 因此又降低了传送效率。为了进一步提高信道的利用率, 可以设法只重传出现差错的数据帧或者定时器超时的数据帧。所以结合 L2CAP 层的特点, 在不改变协议的基础上, 采用选择重传 ARQ 机制, 进而改善数据传输的性能。蓝牙 L2CAP 层可以支持多个逻辑信道, 这与基带层只支持一条 ACL 链路不同, 通过信道标识可以区分不同的逻辑信道, 这为采用选择重传 ARQ<sup>[29]</sup>机制提供了可能。但需要考虑的是如何连接逻辑信道, 为一个数据流建立 2 个逻辑信道: 数据 L2CAP 信道和重传 L2CAP 信道。选择重传 ARQ<sup>[30]</sup>机制只传送错误的数据帧, 这样就降低了采用回退 N 帧 ARQ<sup>[31]</sup>机制引入的传输延迟, 提高了数据传输的性能, 该方法可以应用在现有的蓝牙系统中。

根据现有 ARQ 重传机制各自的特点以及存在的不足, 仅使用一种重传机制虽然可以在一定程度上解决吞吐量的问题, 但是又会引入新的问题。例如采用选择重传 ARQ 可以有效提高数据的吞吐量, 但该机制本身实现复杂, 且对于硬件要求较高, 须有足够大的存储容量以防止数据溢出, 在实际应用中存在一定的局限性。单一的重传机制很难满足不同的需求, 因此如果将多种重传机制相结合, 互补优势, 可以有效

地克服各种重传机制本身存在的缺陷, 例如采用回退 N 帧的 ARQ 机制和选择重传 ARQ 机制两者技术相结合的方式, 一方面可以解决回退 N 帧 ARQ 机制吞吐量低的问题, 另一方面还可以同时解决选择重传 ARQ 机制数据溢出的问题, 从整体上提高了蓝牙技术 L2CAP 层数据传输的性能。

### 3.2 蓝牙技术数据传输干扰问题

蓝牙技术工作在 2.4GHz 的免费 ISM 频段, 该频段也同时被其他无线通信技术所使用, 如 ZigBee、RFID、HomeRF 和 WLAN 等, 所以不可避免地会存在彼此间的数据干扰。不仅如此, 蓝牙皮可网之间也同样存在数据的同频和邻频干扰<sup>[32]</sup>。

#### 3.2.1 非蓝牙设备间的干扰

目前, 针对非蓝牙设备对蓝牙设备数据传输干扰的研究工作主要集中在蓝牙与 WLAN 之间。WLAN 网络的主要技术包括 IEEE 802.1x 系列标准, 其中在与蓝牙数据传输干扰方面最受研究人员关注的标准是 IEEE 802.11b。IEEE 802.15 委员会成立了专门的组织(IEEE 802.15.2 共存工作组)对蓝牙技术和 IEEE 802.11b 标准进行了修改, 以降低相互之间的干扰。现有的修改方案有协作方案和非协作方案 2 种: MEHTA (MAC enhanced temporal algorithm) 和 AWMA (alternating wireless medium access) 是 2 个典型的协作算法, 可以减少甚至完全避免蓝牙与 WLAN 相互通信时产生的干扰; 而自适应跳频属于非协作算法, 它是建立在自动信道质量分析基础上的一种频率自适应和功率自适应控制相结合的技术, 可以避免 2 种网络各自通信时产生的数据干扰。

#### 3.2.2 蓝牙皮可网间的干扰

蓝牙系统采用跳频技术, 发射频率在 79 个跳频频点之间伪随机地选择, 并且各个皮可网的跳频序列是相互独立的<sup>[33]</sup>。所以在皮可网密集的地方, 某个皮可网很有可能和相邻的皮可网跳到相同(相邻)的频点, 从而产生同频(邻频)干扰, 影响蓝牙设备之间正常的数据传送。当今蓝牙产品使用非常广泛, 几乎每一部手机中都含有蓝牙功能, 因此蓝牙同频干扰问题亟待解决。

从蓝牙技术诞生至今, 研究人员不断地对蓝牙皮可网间的同频干扰问题进行研究。研究工作主要集中在: 1) 对干扰情况下的蓝牙系统进行性能分析, 包括数据分组类型、同步异步、跳频保护间隔、网间距离以及无线传输环境等因素对存在干扰的同类<sup>[34,35]</sup>或异类<sup>[36,37]</sup>皮可网的吞吐量和分组

错误率的影响；2) 对抗同频干扰方法的研究，主要包括速率自适应控制算法<sup>[38]</sup>、正交跳频序列方法<sup>[39]</sup>、时间同步方法<sup>[40]</sup>、冲突解决增强型接收机<sup>[41]</sup>、双信道传输方法<sup>[42,43]</sup>等。

以上文献从不同角度、针对不同因素对蓝牙皮可网间的同频干扰问题进行了研究，但是在同频干扰情况下，对蓝牙网络性能的分析还存在以下需要解决的问题：目前的研究大都假设皮可网之间同频就会产生干扰，并没有分析皮可网在同频情况下的载干比；文献中分析的分组错误率实际上是蓝牙皮可网间同频的概率，并没有考虑返回分组是否发送成功；现有的干扰抑制方法也是基于同频就会产生干扰的假设而分析的。

为了更好地抑制蓝牙皮可网之间的同频干扰，本文提出了一种基于信道转换与 MSK 调制的同频干扰抑制方法，该方法在蓝牙皮可网重传时进行信道转换，并采用 MSK 调制方式代替高频移键控调制方式。为了使网络性能的分析更加完善，该方法根据载干比值判断皮可网是否受到同频干扰，并且分析了多个蓝牙皮可网之间的同频概率，在同频概率分析过程中考虑了返回分组、跳频保护间隔、满载与非满载、3 种时隙数据分组共存等多种情况。

网络数量  $N$  取不同值时，干扰抑制前、后参考网不受同频干扰时主从设备之间的最大距离  $D_{max}$  如表 2 所示。可见，采用信道转换与 MSK 调制相结合的干扰抑制方法后， $D_{max}$  值明显增大，尤其在网络数量小于 10 时更加明显。

表 2 载干比(C/I)大于 11dB 时参考网主从设备间最大距离

网络数量 $N$	干扰抑制前 C/I>11dB 时的 $D_{max}$ 值/m	干扰抑制后 C/I>11dB 时的 $D_{max}$ 值/m
2	6.0	10.0
3	5.6	10.0
4	5.3	9.5
5	5.1	8.7
6	4.8	8.1
7	4.6	7.2
8	4.4	6.4
9	4.2	5.7
10	4.0	5.2
20	2.7	2.9
50	1.4	1.7
$N \geq 90$	1.0	1.2

干扰抑制前，当网络数量大于 20 时，参考网在各种比例混合的传输方式下吞吐量都在 100kbit/s 以下，可知参考网吞吐量受同频干扰的影响很严重。干扰抑制后，参考网吞吐量得到了很大程度的改善，尤其在  $14 \leq N \leq 57$  区间内，皮可网吞吐量最大可增加 260kbit/s，如图 4 所示。

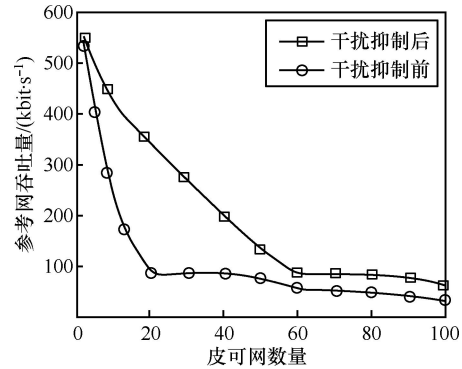


图 4 干扰抑制前后参考网吞吐量最大值的比较

因此，本文提出的基于信道转换与 MSK 调制的同频干扰抑制方法能够有效地提高参考网的载干比和吞吐量，使主从设备间不受同频干扰的最大传输距离有所增加，很大程度上减少了同频干扰的范围。

### 3.3 蓝牙技术数据传输安全问题

蓝牙标准定义了一系列安全机制，为短距离无线数据传输提供了基本的保护<sup>[44]</sup>。现有蓝牙数据传输的安全机制主要存在 2 个问题：一个是单元密钥的使用容易受到外界的针对性攻击<sup>[45]</sup>问题；另一个是蓝牙单元提供的个人识别码的不安全问题。解决这些问题的关键在于如何采用更为强健的加密算法以及较为完善的访问控制机制。

蓝牙作为一种短距离无线通信技术，与其他网络技术一样存在着数据传输的各种安全隐患，近些年来很多研究人员致力于这方面的研究，提出了一些行之有效的安全算法和控制访问方法。郁滨等针对于蓝牙协议的基带层加密方案中密钥容易受攻击的问题，根据蓝牙的特点提出了一种基于主机控制器接口的加密方案<sup>[44]</sup>；谭永亮等在分析了蓝牙加密算法的基础上，提出了一种以 IDEA(international data encryption algorithm)为基础的蓝牙加密算法<sup>[46]</sup>；徐向东等通过分析蓝牙技术数据安全加密算法的不足，提出了将 DES(data encryption standard)加密算法用于蓝牙技术中，从而替代原有 E0 加密算法<sup>[47]</sup>。针对数据访问控制问题，郁滨等基于不同协议层的

控制特点,提出一种蓝牙访问控制方案,实现了三层协议联合访问控制的目的,有效地提高了数据传输的安全性<sup>[48]</sup>;卢小亮等针对蓝牙访问控制存在的设备授权不灵活、无用户授权、资源完整性保护不足等问题,提出一种基于角色的访问控制方案,实现了用户的安全访问以及提高了数据交换的安全性<sup>[49]</sup>。

虽然针对蓝牙数据传输安全方面的研究已经取得了一定的进展,但仍有一些问题有待进一步解决,例如如何保证初始字的复杂度,蓝牙技术单元字方案的可行性和蓝牙设备地址的安全性等。研究人员可以考虑将现有的多种安全加密算法相结合或者采用可靠性更高的访问控制机制,对其加以改进。

## 4 结束语

由于无线数据传输自身的特点,在采用无线方式进行数据传输的过程中,难免会遇到安全、干扰以及传输性能等方面的问题。本文针对蓝牙技术数据传输本身存在的问题,从数据分组选择、重传机制、数据间的干扰和数据传输的安全等几个方面进行了深入研究。首先讨论了蓝牙协议的各个演进版本对数据传输的影响,给出了各协议传输速率的变化;然后对蓝牙数据传输性能进行了研究,针对分组选择和重传机制的研究现状,分析了已有算法的优缺点,并提出了引入扩展戈莱编码方法和采用恒定包络连续相位调制方式等相应改善数据传输性能的方案;最后分别从数据干扰和安全2个方面,对蓝牙技术数据传输存在的问题以及现有的解决方案进行了分析,同时首次深入地研究了多个皮可网的同频干扰概率和干扰信号的功率等问题,并提出了基于信道转换与MSK调制的同频干扰抑制方法,减小了皮可网间的同频概率和分组错误率。

近几年,蓝牙技术数据传输的研究是一个迅速发展的领域,总体来说,还有以下几个方面需要深入研究。

1) 进一步提高数据传输的性能,降低传输的能耗。蓝牙技术组网节点本身电池能量有限,而且还要参与网络中的设备配对和数据交换。因此,数据传输过程不应占用过多的能量资源,否则将影响整个系统的正常运行。设计和采用一些节能算法,同时简化蓝牙设备间的配对过程,降低其能量的消耗。

2) 增强网络的可扩展性。有些蓝牙拓扑算法在节点数目较少时,性能优越,但是当节点数目增加

时,系统的性能就会明显下降。如蓝牙网络中节点数目增多时,配对和维护过程的花费将会明显增加,而且有些算法还会出现节点负载过重的现象,成为系统的瓶颈。所以对于整个系统来说,具有可扩展性的算法是今后研究的一个方向。

3) 降低蓝牙设备的连接时间。蓝牙技术采用的是快速跳频方式进行通信,这意味着蓝牙必须通过跳频同步才能通信。在没有通信的情况下,设备的连接将消耗很多时间,影响数据传输的实时性,所以应采用一些开销小的方法来解决这些问题,例如减少配对过程中的回退时间,改变蓝牙查询的跳频序列或者采用改进的蓝牙协议等。

在蓝牙技术数据传输的研究领域中,除了本文论述的几个主要研究方面,还有一些领域有待于进一步拓展。

1) 蓝牙皮可网的调度算法<sup>[50]</sup>。由蓝牙设备组成的网络中,采用何种轮询方式与多个从设备进行通信,以降低数据传输的延迟,提高传输效率。

2) 蓝牙散射网的吞吐量研究。当设备节点数量很大时,单个皮可网是不能满足数据传输需要的,可以同时几个皮可网组成更为复杂的散射网,进行数据交换。因此散射网的吞吐量是值得考虑的重要问题,进而使整体性能达到最优。

## 参考文献:

- [1] 钱志鸿,杨帆,周求湛. 蓝牙技术原理开发与应用[M]. 北京:北京航空航天大学出版社,2006.  
QIAN Z H, YANG F, ZHOU Q Z. Bluetooth Technology Principle Development and Application[M]. Beijing: Beihang University Press, 2006.
- [2] 马建仓. 蓝牙核心技术及应用[M]. 北京:科学出版社,2003.  
MA J C. Bluetooth Core Technology and Application[M]. Beijing: Science Press, 2003.
- [3] 杨帆,钱志鸿,王雪. 一种改进的蓝牙分散网构成算法[J]. 哈尔滨工业大学学报,2008,40(11):1825-1829.  
YANG F, QIAN Z H, WANG X. An improved Bluetooth scatternet formation algorithm[J]. Journal of Harbin Institute of Technology, 2008,40(11):1825-1829.
- [4] 杨帆,王珂,钱志鸿. 链式结构的蓝牙分散网拓扑构成算法与性能仿真[J]. 通信学报,2006,27(1):29-30.  
YANG F, WANG K, QIAN Z H. Chain structure Bluetooth scatternet topology formation algorithm and performance simulations[J]. Journal on Communications, 2006,27(1):29-30.
- [5] HAGER C T, MIDKIFF S F. An analysis of Bluetooth security vulnerabilities[A]. Wireless Communications and Networking, WCNC 2003[C]. New Orleans, 2003.1825-1831.

- [6] HAGER C T, MIDKIFF S F. Demonstrating vulnerabilities in Bluetooth security[A]. IEEE Global Telecommunications Conference GLOBECOM'03[C]. San Francisco, 2003.1420-1424.
- [7] BANDYOPADHYAY S, MAJUMDAR A. A proposal for improvement in service-level security architecture of Bluetooth[A]. IEEE TENCON 2003: Conference on Convergent Technologies for the Asia-Pacific Region[C]. Bangalore, India, 2003. 1057-1061.
- [8] GOLMIE N, DYCK R E, SOLTANIAN A. Interference of Bluetooth and IEEE 802.11: simulation modeling and performance evaluation[A]. ACM MSWiM 2001 Proceedings of the 4th ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems[C]. Rome, Italy, 2001. 11-18.
- [9] CHEN L J, KAPOOR R, SANADIDI M Y, *et al.* Enhancing Bluetooth tcp throughput via link layer packet adaptation[A]. 2004 IEEE International Conference on Communications[C]. Paris, France, 2004. 4012- 4016.
- [10] Bluetooth SIG, Specification of the Bluetooth system version 1.1[EB/OL]. <http://www.bluetooth.org>, 1999.
- [11] Bluetooth SIG, Specification of the Bluetooth system version 1.2[EB/OL]. <http://www.bluetooth.org>, 2003.
- [12] Bluetooth SIG, Specification of the Bluetooth system version 2.0 EDR[EB/OL]. <http://www.bluetooth.org>, 2004.
- [13] Bluetooth SIG, Specification of the Bluetooth system version 2.1 EDR[EB/OL]. <http://www.bluetooth.org>, 2007.
- [14] Bluetooth SIG, Specification of the Bluetooth system version 3.0+HS[EB/OL]. <http://www.bluetooth.com>, 2009.
- [15] Bluetooth SIG, Specification of the Bluetooth system version 4.0[EB/OL]. <http://www.bluetooth.com>, 2009.
- [16] SARKAR S, ANJUM F, GUHA R. Optimal communication in Bluetooth piconets[J]. IEEE Transactions of Vehicular Technology, 2005, 54(2): 709-721.
- [17] 杨帆, 王珂, 钱志鸿. 蓝牙分组传输性能分析与自适应分组选择策略[J].通信学报, 2005, 26(9): 97-102.  
YANG F, WANG K, QIAN Z H. Performance analysis of Bluetooth packet transmission and adaptive packet selection strategy[J]. Journal on Communications, 2005, 26(9): 97-102.
- [18] 徐飞, 庄亦琪, 郭锋. BCH 编码对蓝牙数据传输性能改善的分析与仿真[J]. 系统仿真学报, 2007, 19(23):5549-5552.  
XU F, ZHUANG Y Q, GUO F. Analysis and simulation of BCH encoding on the improvement of Bluetooth's transmission performance[J]. Journal of System Simulation, 2007, 19(23):5549-5552.
- [19] 杨帆, 王珂, 钱志鸿. 基于信噪比的蓝牙自适应分组选择算法[J]. 吉林大学学报(工学版), 2006, 36(1): 103-107.  
YANG F, WANG K, QIAN Z H. Bluetooth adaptive packet selection algorithm based on signal-to-noise ratio[J]. Journal of Jilin University Engineering and Technology Edition, 2006, 36(1):103-107.
- [20] JU M C, PARK H, HONG D K, *et al.* Packet selection scheme based on a channel quality estimation for Bluetooth systems[A]. 2004 IEEE Wireless Communications and Networking Conference[C]. Atlanta, GA, United States, 2002. 228-231.
- [21] 王雪, 钱志鸿, 李冰等. 蓝牙自适应分组选择策略与选择重传算法研究[J]. 通信学报, 2011, 32(1):151-158.  
WANG X, QIAN Z H, LI B, *et al.* Adaptive packet selection scheme and selective retransmission algorithm for Bluetooth[J].Journal on Communications, 2011,32(1):151-158.
- [22] 唐建军, 纪越峰.超高速 BCH 码解码改进算法研究[J].通信学报, 2004, 25(9): 21-27.  
TANG J J, JI Y F. Modified decode algorithm of BCH code for ultrahigh-speed system[J]. Journal on Communications, 2004, 25(9):21-27.
- [23] 王亚峰, 杨鸿文, 杨大成. 采用 Turbo 码的 type III HARQ 性能分析[J].通信学报, 2004, 25 (6): 139-146.  
WANG Y F, YANG H W, YANG D C. Performance analysis of type III HARQ with Turbo codes[J]. Journal of China Institute of Communications, 2004, 25(6): 139-146.
- [24] LADAS C, AMIEE R M, MAHDAVI M, *et al.* Class based selective-ARQ scheme for high performance TCP and UDP over wireless links[A].Mobile and Wireless Communications Network, 4th International Workshop on [C]. 2002. 311-315.
- [25] VALENTI M C, ROBERT M, REED J H. On the throughput of Bluetooth data transmission[A]. 2002 IEEE Wireless Communications and Networking Conference[C].Orlando, Florida, USA, 2002. 119-123.
- [26] RAZAVI R, FLEURY M, GHANBARI M. Fuzzy logic control of adaptive ARQ for video distribution over a Bluetooth wireless link[J].Advances in Multi-media, 2007(1), 2007: 1-12.
- [27] CYRIL S K, LEUNG, ALBERT L. Forward error correction for an ARQ scheme[J]. IEEE Transactions on Communications,1981,29(10): 1514-1519.
- [28] YU D Y. An effective go-back-N ARQ scheme for variable-error-rate channels[J]. IEEE Transactions on Communications, 1995, 43(1): 20-23.
- [29] CHANG J F, YANG T H. End-to-end delay of an adaptive selective repeat ARQ protocol[J]. IEEE Transactions on Communications, 1994, 42(11): 2926-2928.
- [30] 肖峻峰, 邱晶, 程时端.相关衰落信道下的一种层间联合自适应 SR-ARQ 传输机制[J].通信学报, 2006, 27(4):1-15.  
XIAO J F, QIU J, CHENG S D. Cross-layer adaptive transmission scheme combined with SR-ARQ over correlated fading channels[J].Journal on Communications, 2006, 27(4):1-15.
- [31] ANNAMALAI, BHARGAVA A, LU V K. An adaptive go-back-ARQ protocol for variable-error rate channels[J].IEEE Transactions on Communications, 1998, 46(11): 1405-1408.
- [32] 严德政, 黄爱苹, 仇佩亮等.多个蓝牙匹克网共存的系统建模与性能仿真[J].通信学报, 2002, 23(3):35-43.  
YAN D Z, HUANG A P, QIU P L, *et al.* Modeling and performance simulation on multi-piconet Bluetooth system[J]. Journal on Communications, 2002, 23(3):35-43.
- [33] 沈连丰, 宋铁成, 范佳曦等. Lawrence Nui Bluetooth 系统基带关键算法的研究及其仿真[J].电子学报, 2000, 28(11A):165-168.  
SHEN L F, SONG T C, FAN J X, *et al.* Lawrence Nui study and

- simulation of the key algorithms of the baseband in Bluetooth[J]. Chinese Journal of Electronics, 2000, 28(11A): 165-168.
- [34] KIM S Y, KIM S J, LEE H W, *et al.* Packet interference and aggregated throughput of Bluetooth piconets using an adaptive frequency hopping in rician fading channels[A]. 2008 International Conference on Information Networking[C]. Busan, Korea, 2008. 1-5.
- [35] LIN T Y, LIU Y K, TSENG Y C. An improved packet collision analysis for multi-Bluetooth piconets considering frequency-hopping guard time effect[J]. IEEE Journal on Selected Areas in Communications, 2004, 22(10): 2087- 2094.
- [36] NAIK K, WEI D S L, SU Y T, *et al.* Analysis of packet interference and aggregated throughput in a cluster of Bluetooth piconets under different traffic conditions[J]. IEEE Journal on Selected Areas in Communications, 2005, 23(6): 1205-1218.
- [37] NAIK K, WEI D S L, SU Y T, *et al.* Packet interference in a heterogeneous cluster of Bluetooth piconets[A]. 2003 IEEE 58th Vehicular Technology Conference[C]. Orlando, FL, United States, 2003. 582- 586.
- [38] 叶芝慧, 沈连丰, 沈克勤等. 无线个域网应用环境下速率自适应算法的研究[J]. 通信学报, 2004, 25(4):160-167.  
YE Z H, SHEN L F, SHEN K Q, *et al.* Study on adaptive rate control scheme in WPAN system[J]. Journal on Communications, 2004, 25(4):160-167.
- [39] 昌庆江, 邹静娴, 纪志成. 多个蓝牙匹克网共存时的同频干扰性能分析[J]. 计算机工程与设计, 2006, 27(1): 103- 105.  
CHANG Q J, ZOU J X, JI Z C. Performance analysis of co-channel interference on multi-piconets Bluetooth system[J]. Computer Engineering and Design, 2006, 27(1): 103-105.
- [40] ASHRAF I, GKELIAS A, DOHLER M, *et al.* Time-synchronised multi-piconet Bluetooth environments[J]. IEEE Proceedings: Communications, 2006, 153 (3): 445-452.
- [41] LI J L, LIU X Q. A collision resolution technique for robust co-existence of multiple Bluetooth piconets[A].2006 IEEE 64th Vehicular Technology Conference[C]. Montreal, QC, Canada, 2006. 1-5.
- [42] LI J, LIU X. Evaluation of cochannel and adjacent channel interference for multiple Bluetooth piconets with dual channel transmission[A]. IEEE Wireless Communications and Networking Conference[C]. Kowloon, China,2007. 2355-2360.
- [43] LI J L, LIU X Q, SWAMI A. Collision analysis for coexistence of multiple Bluetooth piconets and WLAN with dual channel transmission[J]. IEEE Transactions on Communications, 2009,57(4):1129- 1138.
- [44] 郁滨, 李颖川. 一种蓝牙传输加密方案的设计与实现[J]. 计算机工程, 2009, 35(6): 183-185.  
YU B, LI Y C. Design and implementation of encryption scheme of Bluetooth communication[J]. Computer Engineering, 2009, 35(6): 183-185.
- [45] 张卫明, 李世取. 组合生成器的多线性相关攻击[J]. 电子学报, 2005, 33(3): 427-432.  
ZHANG W M, LI S Q. Multi-linear correlation attack on combiners[J]. Chinese Journal of Electronics, 2005,33(3): 427-432.
- [46] 谭永亮, 于海勋, 王亮. 蓝牙加密算法的改进及 FPGA 实现[J]. 信息安全与通信保密, 2008,(8):122-123,126.  
TAN Y L, YU H X, WANG L. The improvement of Bluetooth encryption algorithm and implementation on FPGA[J]. Information Security and Communications Privacy, 2008,(8):122-123,126.
- [47] 徐向文. 蓝牙技术中的一种基于DES加密的安全策略[J]. 通信技术, 2008, 41(11):150-152.  
XU X W. An security strategy based on DES encryption in Bluetooth technology[J]. Communications Technology, 2008, 41(11):150-152.
- [48] 郁滨, 王利涛. 一种蓝牙访问控制方案的设计与实现[A]. 2007年首届仪表、自动化与先进集成技术大会[C]. 北京, 中国, 2007. 524- 527.  
YU B, WANG L T. Design and implementation of an access control scheme in Bluetooth[A].2007 First Appearance, Automation and Integration of Advanced Technology Conference[C]. Beijing, China, 2007. 524-527.
- [49] 卢小亮, 刘连东, 郁滨. 一种基于角色的蓝牙强制访问控制方案的设计[A]. 全国第19届计算机技术与应用(CACIS)学术会议[C]. 合肥, 中国, 2008. 1328-1333.  
LU X L, LIU L D, YU B. Design of a role-based mandatory access control scheme in Bluetooth[A]. The 19th Computer Application Federation of China Instrument and Control Society[C]. Hefei, China, 2008. 1328-1333.
- [50] 杨帆, 王珂, 钱志鸿. 按需轮循的蓝牙微微网调度算法与性能评估[J]. 电子学报, 2007, 35(4): 647-652.  
YANG F, WANG K, QIAN Z H. Polling-on-demand scheduling algorithm for Bluetooth piconets and performance evaluation[J]. Chinese Journal of Electronics, 2007, 35(4): 647-652.

#### 作者简介:



钱志鸿(1957-), 男, 吉林长春人, 博士, 吉林大学教授、博士生导师, 主要研究方向为基于蓝牙、RFID等短距离无线通信技术的无线个域网与无线传感器网络。



刘丹(1978-), 女, 吉林省吉林市人, 博士, 大连海洋大学讲师, 主要研究方向为无线个域网与无线传感器网络。