

蓝牙无线通信技术简介

蓝牙技术是一种无线数据和语音通信开放的全球规范，它是基于低成本的近距离无线连接，为固定和移动设备建立通信环境的一种特殊的近距离无线技术连接。^[1]

蓝牙使当前的一些便携移动设备和计算机设备能够不需要电缆就能连接到互联网，并且可以无线接入[互联网](#)。^[1]

应用

一 在汽车领域的应用

1 蓝牙免提通讯。

将蓝牙技术应用到车载免提系统中，是最典型的汽车蓝牙应用技术。利用手机作为网关，打开手机蓝牙功能与车载免提系统，只要手机在距离车载免提系统的 10 米之内，都可以自动连接，控制车内的麦克风与音响系统，从而实现全双工[免提通话](#)。利用车载免提应用框架作为蓝牙免提通讯技术的基础，很好的规范蓝牙设备，并且汇集蓝牙功能集，这样就可以控制蓝牙技术。^[4]

2 车载蓝牙娱乐系统。

车载蓝牙娱乐系统，主要包括 USB 技术、音频解码技术、蓝牙技术等，将上述技术相融合，利用汽车内部麦克风、音响等，播放储存在 u 盘中的各种音频以及电话簿等，还增添了流行音乐等播放功能。以 CAN 为基础连接车载系统中的网络，这样就可以实现[车载信息娱乐系统](#)的运行。同时也为系统保留了可扩展性。^[4]

3 蓝牙车辆远程状况诊断。

车载诊断系统主要依靠蓝牙远程技术，及时进行车辆检修，尤其对[汽车发动机](#)进行实时监测，帮助车辆时刻掌握不同功能模块的具体运行情况，一旦发现系统运行不正常，利用设定好的计算方法准确判断出现故障的原因与故障类型，将故障诊断代码上传到车载运行系统存储器中。取更加方便快捷。^[4]

4 汽车蓝牙防盗技术。

随着技术得逐渐成熟，蓝牙在应用广泛性、使用安全性、传输准确性、传输高效性等方面会有更进一步的改善。尤其是蓝牙防盗器的应用，如果汽车处于设防状态，蓝牙感应功能将会自动连接汽车车主手机，一旦车辆状态出现变化或者遭受盗窃，将会自动报警，蓝牙防盗技术的应用，为汽车提供更安全环境。^[4]

二 蓝牙技术应用于工业生产中

1 技术人员对[数控机床](#)的无线监控。

蓝牙技术在数控机床中的应用，主要体现于无线监控方面，利用蓝牙技术安装相应的监控设施，为数控机床用户生产提供方便，同时也维护了数控机床生产的安全。技术人员根据携带的蓝牙监控设备，随时监控与管理机床运行，发现数控机床生产问题及时治理。尤其是无线数据链路下实现的自动监控能力，可以适当干预机床运行，比如停止主轴或者系统停机等。^[4]

2 零部件磨损程度的检测。

蓝牙检测功能还体现于工业零部件磨损方面，利用蓝牙检测软件结合磨损检测材料进行实验研究，可以具体到耐磨性优劣，及时利用蓝牙无线传输将磨损检测程度数据传输到相关设备中，相关设备进行智能分析，并将结果告知技术人员。^[4]

3 功率输出标准化。

蓝牙技术在工业生产的功率输出方面也十分重要。调节设备利用蓝牙技术传输生产功率变化，将其与标准运行功率对比，如果存在功率变化异常，便会及时调整，并将调整数据上传。^[4]

4 蓝牙监控系统对数控系统运行状态的实时和完整的记录。

蓝牙传输设备作为监控系统主要组成，随时记录数控系统运行状态，并且将数控系统运行期间的任何波动全部传输到储存设备中，利用通信端口上传信息，为数控生产管理人员提供更多参考资料。^[4]

三 蓝牙技术应用于医药领域

随着现代医疗事业的蓬勃发展，医院监护系统和医疗会诊系统的出现为现代医疗事业的发展做出突出贡献，但在在实际应用过程中也存在一些问题，例如当前对重症病人的监护设备都采用有线连接，当病人有活动需求时难免会影响监控仪器的正常运行，但是蓝牙技术的出现可以有效改善上述情况，不仅如此，蓝牙技术还在诊断结果传输与病房监护方面起到了重要作用。^[4]

1 诊断结果输送。

以蓝牙传输设备为依托，将医院诊断结果及时输送到存储器中。蓝牙听诊器的应用以及蓝牙传输本身耗电量较低，传输速度更加快速，所以利用电子装置及时传输诊断结果，提高医院诊断效率，确保诊断结果数据准确。^[4]

2 病房监护。

蓝牙技术在医院病房监护中的应用主要体现于病床终端设备与病房控制器，利用主控计算机，上传病床终端设备编号以及病人基本住院信息，为住院病人在配备病床终端设备，一旦病人有突发状况，利用病床终端设备发出信号，蓝牙技术以无线传送的方式将其传输到病房控制器中。如果传输信息较多，会自动根据信号模式划分传输登记，为医院病房管理提供了极大的便利。^[4]

产品介绍

蓝牙是一种支持设备短距离通信（一般 10m 内）的无线电技术，能在包括移动电话、PDA、无线耳机、笔记本电脑、相关外设等众多设备之间进行无线信息交换。利用蓝牙技术，能够有效地简化移动通信终端设备之间的通信，也能够成功地简化设备与因特网 Internet 之间的通信，从而数据传输变得更加迅速高效，为无线通信拓宽道路。^[2]

蓝牙作为一种小范围无线连接技术，能在设备间实现方便快捷、灵活安全、低成本、低功耗的数据通信和语音通信，因此它是实现无线个域网通信的主流技术之一。与其他网络相连接可以带来更广泛的应用。是一种尖端的开放式无线通信，能够让各种数码设备无线沟通，是无线网络传输技术的一种，原本用来取代红外线通信。^[3]

蓝牙技术是一种无线数据与语音通信的开放性全球规范，它以低成本的近距离无线连接为基础，为固定与移动设备通信环境建立一个特别连接。其实质内容是为固定设备或移动设备之间的通信环境建立通用的无线电空中接口（Radio Air Interface），将通信技术与计算机技术进一步结合起来，使各种 3C 设备在没有电线或电缆相互连接的情况下，能在近距离范围内实现相互通信或操作。简单的说，蓝牙技术是一种利用低功率无线电在各种 3C 设备间彼此传输数据的技术。蓝牙工作在全球通用的 2.4GHz ISM（即工业、科学、医学）频段，使用 IEEE802.15 协议。作为一种新兴的短距离无线通信技术，正有力地推动着低速率无线个人区域网络的发展。 [2]

原理

蓝牙是一种无线技术标准，可实现固定设备、移动设备和楼宇个人域网之间的短距离数据交换(使用 2.4~2.485GHz 的 ISM 波段的 UHF 无线电波)。蓝牙可连接多个设备，克服了数据同步的难题。 [4]

蓝牙技术是世界著名的 5 家大公司一爱立信(Ericsson)、诺基亚(Nokia)、东芝(Toshiba)、国际商用机器公司(IBM)和英特尔(Intel)，于 1998 年 5 月联合宣布的一种无线通信新技术。蓝牙设备是蓝牙技术应用的主要载体，常见蓝牙设备比如电脑、手机等。蓝牙产品容纳蓝牙模块，支持蓝牙无线电连接与软件应用。蓝牙设备连接必须在一定范围内进行配对。这种配对搜索被称之为短程临时网络模式，也被称之为微微，可以容纳设备最多不超过 8 台。蓝牙设备连接成功，主设备只有一台，从设备可以多台。蓝牙技术具备射频特性。采用了 TDMA 结构与网络多层次结构，在技术上应用了跳频技术、无线技术等，具有传输效率高、安全性高等优势，所以被各行各业所应用。 [4]

特点

蓝牙技术及蓝牙产品的特点主要有：

- 1 蓝牙技术的适用设备多，无需电缆，通过无线使电脑和电信连网进行通信。 [5]
- 2 蓝牙技术的工作频段全球通用，适用于全球范围内用户无界限的使用，解决了蜂窝式移动电话的国界障碍。蓝牙技术产品使用方便，利用蓝牙设备可以搜索到另外一个蓝牙技术产品，迅速建立起两个设备之间的联系，在控制软件的作用下，可以自动传输数据。 [5]
- 3 蓝牙技术的安全性和抗干扰能力强，由于蓝牙技术具有跳频的功能，有效避免了 ISM 频带遇到干扰源。蓝牙技术的兼容性较好，蓝牙技术已经能够发展成为独立于操作系统的一项技术，实现了各种操作系统中良好的兼容性能。 [5]
- 4 传输距离较短：现阶段，蓝牙技术的主要工作范围在 10 米左右，经过增加射频功率后的蓝牙技术可以在 100 米的范围进行工作，只有这样才能保证蓝牙在传播时的工作质量与效率，提高蓝牙的传播速度。另外，在蓝牙技术连接过程中还可以有效的降低该技术与其他电子产品之间的干扰，从而保证蓝牙技术可以正常运行。蓝牙技术不仅有较高的传播质量与效率，同时还具有较高的传播安全性特点。 [6]
- 5 通过跳频扩频技术进行传播：蓝牙技术在实际应用期间，可以原有的频点进行划分、转化，如果采用一些跳频速度较快的蓝牙技术，那么整个蓝牙系统中的主单元都会通过自动跳频的形式进行转换，从而将其以随机的进行跳频。由于蓝牙技术的本身具有较高的安全性与抗干扰能力，在实际应用期间可以蓝牙运行的质量。 [6]

系统组成

1 底层硬件模块。

蓝牙技术系统中的底层硬件模块由基带、跳频和链路管理。其中，基带是完成蓝牙数据和跳频的传输。无线调频层是不需要授权的通过 2.4GHz ISM 频段的微波，数据流传输和过滤就是在无线调频层实现的，主要定义了蓝牙收发器在此频带正常工作所需要满足的条件。链路管理实现了链路建立、连接和拆除的安全控制。^[5]

2 中间协议层。

蓝牙技术系统构成中的中间协议层主要包括了服务发现协议、逻辑链路控制和适应协议、电话通信协议和串口仿真协议四个部分。服务发现协议层的作用是提供上层应用程序一种机制以便于使用网络中的服务。[逻辑链路控制](#)和适应协议是负责数据拆装、复用协议和控制服务质量，是其他协议层作用实现的基础。^[5]

3 高层应用。

在蓝牙技术构成系统中，高层应用是位于协议层最上部的框架部分。蓝牙技术的高层应用主要有文件传输、网络、局域网访问。不同种类的高层应用是通过相应的应用程序通过一定的应用模式实现的一种无线通信。^[5]

存在问题

蓝牙存在的问题主要有以下几个：

（1）蓝牙的[功耗](#)问题。蓝牙传输数据的频率不高，在传输数据的过程中耗能较少，但是，为了及时响应连接请求，在等待过程中的轮询访问却是十分耗能的。^[7]

（2）蓝牙的连接过程烦琐。蓝牙的连接过程中涉及多次的信息传递与验证过程，表面上来看似乎并不能让使用者感受到复杂的连接程序，但是，反复的数据加解密过程和每次连接都需进行的身份验证过程却是对于设备计算资源的一种极大的浪费。^[7]

（3）蓝牙的安全性问题。蓝牙的首次配对需要用户通过 PIN 码验证，PIN 码一般仅由数字构成，且位数很少，一般为 4~6 位。[PIN 码](#)在生成之后，设备会自动使用蓝牙自带的 E2 或者 E3 加密算法来对 PIN 码进行加密，然后传输进行身份认证。在这个过程中，黑客很有可能通过拦截数据包，伪装成目标蓝牙设备进行连接，或者采用暴力攻击的方式来破解 PIN 码。^[7]

此外，在蓝牙传输数据的过程中使用的加密算法的安全性也有待提高。出现以上情况的原因在于蓝牙技术的本身，由于蓝牙的设计目标为设备间组成一个无基站式局域网（类似于 [WLAN](#) 的 [AdHoc](#) 模式），进行多设备间的近距离通信，为了保证私密性和安全性，蓝牙协议要求每次连接前必须进行身份认证。^[7]

发展前景

1 普及蓝牙技术的认知与利用

虽然在现阶段，蓝牙技术已经在实际的生活与工作中有了较多的应用，但是人们对于蓝牙技术并没有过多的认识，除了在手机蓝牙的传输功能与语音功能的应用外，对于[无线打印机](#)、无线会议等蓝牙应用没有足够的认

识。因此，在未来的蓝牙技术发展中，应对蓝牙技术进行宣传，将成本低和技术先进的蓝牙技术推广在更广泛的应用平台中。^[5]

2 拓展蓝牙技术的应用领域

蓝牙技术的应用领域要向广度发展。蓝牙技术的第一阶段是支持手机、PDA 和笔记本电脑，接下来的发展方向要向着各行各业扩展，包括汽车、信息家电、航空、消费类电子、军用等。^[5]

3 与更多的操作系统之间兼容

在计算机系统中，若要进一步提高蓝牙技术的应用，就要将蓝牙兼容技术与计算机操作系统同步发展，除了与 [Windows](#)、xp 和 pc 平台兼容外，还要跟进技术水平，例如在 win8 系统的计算机应用中建立支持性，提高蓝牙技术在计算机和相关工程中的应用。另外，在兼容性的技术发展中，要不断的对电子产品的发展方向进行研究，在预见性的规划安排中，提高蓝牙技术的应用能力。^[5]

4 低成本发展，芯片小巧且价格下降

蓝牙技术中应用的芯片的成本较低，并且在向着单芯片的方向发展，已经开发除了嵌入电池中的单芯片，蓝牙芯片将越来越小巧，价格越来越低。^[5]

5 加强合作开发趋势

蓝牙技术的发展主要得益于通讯技术的支持，在未来的经济建设中，各行各业都需要在信息自动化的应用中提高生产水平，因此，要将蓝牙应用技术与多种行业建立合作形式。比如在汽车制造中，可以将蓝牙技术设计到汽车的智能化应用系统中，增加汽车的使用功能，通过无线数据的连接，将汽车、计算机、手机和人进行紧密的联系，通过手机等设备的简单操作就可以控制汽车运行系统等，如在手机中下载汽车的开关系统，一是保证了汽车的个人使用安全，二是在忘记开关车门时可以避免回到停车地点复查。^[5]

2021 年 6 月 1 日，福州市区首批 32 个共享单车驿站正式启用“蓝牙道钉”装置。这种装置可发射信号，与安装在共享单车上的北斗卫星高精度分体锁通信，实现单车无桩式定点停放，提高共享单车智能化、科学化监管水平。^[9]

蓝牙版本

[蓝牙 2.0](#)、蓝牙 2.1、[蓝牙 3.0](#)、[蓝牙 4.0](#)、蓝牙 4.2、[蓝牙 5.0](#)、蓝牙 5.1、[蓝牙 5.2](#)、蓝牙 5.3、^[10]蓝牙 5.4^[11]。

蓝牙漏洞

2021 年 12 月，达姆施塔特大学、布雷西亚、CNIT 和安全移动网络实验室的研究人员发表了一篇论文，揭示了攻击者可以通过针对具有多种无线技术的移动设备的蓝牙组件来提取密码并操纵 Wi-Fi 芯片上的网络流量。

智能手机、平板电脑和其他现代移动设备的芯片系统（SoC）包含独立的蓝牙、Wi-Fi 和 LTE 组件，每个组件都有自己专门的安全措施。然而，这些组件往往共享许多相同的资源，如设备的天线或无线频谱。

根据上述论文，攻击者有可能利用这些共享资源作为桥梁，跨越无线芯片边界发起横向权限升级攻击。如果攻击者能够利用这些漏洞，他们可以实现代码执行、内存读出和拒绝服务。

为了利用这些漏洞，研究人员首先需要在蓝牙或 Wi-Fi 芯片上进行代码执行。完成后，他们就能通过使用共享内存资源对设备的其他芯片进行横向攻击。

研究人员总共发现了九个不同的漏洞，虽然有些漏洞可以通过固件更新来修复，但一些漏洞只能通过新的硬件修改来修复，这使得数十亿的现有设备处于潜在的被攻击风险之中。

在他们的测试中，研究人员调查了博通、Silicon Labs 和 Cypress 的芯片，这些芯片存在于数十亿的设备中。在他们向这些芯片供应商报告了这些缺陷后，一些供应商已经发布了安全更新来解决这些问题。然而，一些厂商还没有解决这些问题，因为它们影响到不再支持的产品，如 Nexus 5 和 iPhone 6。^[8]