无线电子通信技术安全问题与安全技术探析

马德旺
中国联合网络通信集团有限公司北京市分公司　北京　100038

摘　要：随着无线电子通信技术的不断发展，越来越多的人们开始享受到其带来的便利。然而，随之而来的是日益加剧的网络安全问题。未经授权的访问、信息泄露、网络攻击等问题频繁出现，给用户和企业带来严重的损失。本文对无线电子通信技术安全问题进行了分析，并探讨了一些安全技术的应对策略。

关键词：无线电子；通信技术；安全问题；安全技术

1 无线电子通信技术的组成技术分析

1.1 WLAN技术

WLAN技术是无线局域网络技术的简称，它是一项用于实现计算机网络连接的技术，无需使用传统的物理连接，而是通过使用无线电波利用无线电信道实现。WLAN技术具备灵活性高、组网方便、覆盖范围广、便携性强等优点，因此在当今的现代通信系统中得到了广泛的应用。下面是关于WLAN技术的详细介绍：（1）WLAN技术的基础：WLAN技术是一种基于无线电波传输数据的技术。它使用一些特殊的设备，如无线网卡、无线路由器、无线接入点（AP）等来实现，这些设备都是经过特别设计的，具有广泛的接收和发送能力。（2）WLAN技术的工作原理：无线局域网通过无线技术建立起计算机网络，无需进行传统的物理连接。WLAN设备可以接收和发射无线信号，当信号覆盖范围内存在一个或多个无线设备时，就可以实现无线设备之间的通信。（3）WLAN技术的应用：WLAN技术可广泛应用于商业、工业和家庭网络。它被广泛用于公共场所，如机场、咖啡店、购物中心、医院和学校等。此外，在家庭中，WLAN通常应用于家庭办公室、客厅、卧室和厨房等区域，以方便移动设备的连接和使用[1]。

1.2 蓝牙技术

蓝牙技术是一种短距离无线通信技术，用于在设备之间进行通信和数据传输。蓝牙技术的主要优点是无需使用传统的物理连接，而是使用无线电波进行连接，具有节省能源、用户友好以及成本较低等优势。蓝牙技术的应用：蓝牙技术被广泛应用于个人手持设备，如手机、平板电脑、智能手表等。人们通过蓝牙技术在这些设备之间实现通信和数据交换。现代汽车的信息系统使用了蓝牙技术，以便驾驶者可以免提通话、播放音乐、访问导航和发送短信等。家庭音视频设备，如音响、扬声器和电视等也可以通过蓝牙技术进行连接和通信，使得人们可以在不同的房间内无线连接、播放音乐和视频。蓝牙技术还被用于医疗设备，如心脏监控仪、血糖仪、血压计等的数据采集和传输[2]。

1.3 ZigsBee技术

ZigBee技术是一种基于IEEE 802.15.4标准的低功耗、低速率、短距离无线通信技术，用于在各种应用中进行设备之间的通信和数据传输。ZigBee技术主要应用于消费电子、智能家居、工业自动化、建筑自动化和医疗保健等领域。（1）网络设备之间建立通信：ZigBee网络中的设备可以分为终端设备、路由器和协调器三类。协调器是ZigBee网络的控制中心，它负责对整个网络进行管理和监视。路由器是中间节点，用于转发信息。终端设备是网络的末端节点，用于读取传感器数据或执行控制任务。当网络设备之间建立通信时，它们会以广播方式发送帧，以便其他设备能够接收信息[3]。（2）数据传输：ZigBee网络能够传输各种类型的数据，如文本、图像、音频或视频等。传输过程中，数据通常通过广播或多类型转发进行传输，不同节点之间需要协调其传输节奏，以确保数据传递的可靠性和完整性。ZigBee技术是一种短距离无线通信技术，用于实现设备之间的通信和数据传输。它具有低功耗、低成本、通信距离远及网络连接简单等优势，应用于智能家居、工业自动化和物联网等领域。

2 无线电子通信技术中存在的安全问题

2.1 未经授权进行监听

在无线电子通信技术中，经常存在着各种安全问题，其中最重要的之一是未经授权进行监听。这是指未经允许或授权，公然地或秘密地监听另一方的通信内容。虽然监听本身不一定是非法的，但如果进行监听的一方没有获得通信另一方的允许，那么这种监听就是违法的。未经授权的监听对个人隐私和商业机密都会带来严重的影响，并且这种活动也会损害公共安全。除此之

外，恶意的监听者还可能通过监听网络数据包来窃取账户信息、密码、财务信息等敏感数据[4]。

2.2 信息的非法窃取

在无线电子信息技术发展过程当中，信息的非法窃取是非常重要的一项安全问题。在无线电子信息技术发展的过程当中，较为典型的案例是美国的斯诺登窃听丑闻。信息的非法窃取是指黑客利用不正当的手段，对于一些较为重要的数据内容进行窃取，在我们的日常生活当中，黑客只要利用一定的手段就能够顺利地进入到我们的路由器网络当中，从而对整个路由器网络当中的信息数据进行窃取。实际上造成该现象发生的原因，还是由于无线网络接触本身具有较高的开放性导致的。

2.3 非法基站

在无线电子通信技术中，非法基站是另一个常见的安全问题。非法基站一般指一些未经授权的设备或网络，可以用来捕获和劫持无线通信流量，从而获取用户敏感信息，执行拦截、中继等各种攻击。非法基站的存在，不仅扰乱电信市场秩序，损害其他用户的合法权益，而且危害公共安全。非法基站的设立者，为了牟取非法利益，可能会对周围的电磁环境造成严重破坏，影响公众对通信系统的正常使用。此外，非法基站还可能存在被不法分子利用的可能，成为诈骗等违法犯罪活动的工具[5]。

3 保障无线电子通信技术的安全应用

3.1 设置安全防护措施

保障无线电子通信技术的安全应用需要采取一系列的安全措施，以下是一些重要的安全防护措施：（1）加密通信：采用加密技术对通信内容进行加密，对于攻击者无法解密。对于无线电子通信系统，采用加密算法如AES、RSA等进行通信内容加密可以有效保障无线电子通信技术的安全应用。（2）控制接入：采用身份验证等技术控制设备和用户接入，仅允许授权用户和设备接入系统，防止未授权访问和攻击。（3）严格权限控制：为不同的用户或设备分配不同的权限，防止非法用户或设备访问核心信息[6]。（4）防火墙和入侵检测系统：采用防火墙和入侵检测系统对系统进行保护，能有效的发现和防范潜在的攻击行为。（5）定期漏洞扫描和修补：采用定期漏洞扫描和修补，保障无线电子通信系统的安全性能和功能。（6）安全管理和培训：建立全面的安全管理体系，对员工进行安全培训和教育，以增强系统的安全意识和敏感性。总之，通过采取多种有效的安全防护措施，可以保障无线电子通信技术的安全应用，确保通信数据的安全性，避免与数据相关的各种问题和不必要的损失。

3.2 基于蓝牙技术的信号传感器

对于基于蓝牙技术的信号传感器，为保障其安全应用可以采取以下措施：采用蓝牙加密技术，对传感器的蓝牙信号进行加密。蓝牙加密的原理是在蓝牙连接的过程中对传输数据进行加密，防止黑客采用分析和破解等方式获取通信内容。采用蓝牙认证技术，对连接到蓝牙信号传感器的设备进行认证，加强认证机制和安全性。采用跳频技术增强蓝牙信号传输的安全性。跳频技术是指在蓝牙信号的传输过程中按照预先设定的规则随机变化信道，从而增强了信号的保密性和抗干扰性。对连接到蓝牙信号传感器的设备进行限制，仅允许授权设备进行接入。建立黑白名单管理机制，只允许在白名单上的设备进行接入。黑名单是指在安全方面存在风险的设备，白名单是指在安全方面信誉良好或者是已经经过验证认证的设备。在蓝牙信号传感器设备上安装远程管理和监控软件，能够实时监控设备的使用情况和提供紧急处理等安全保障[1]。通过采取以上安全措施，可以有效保障基于蓝牙技术的信号传感器的安全应用，提高设备的应用价值和可信度，保证敏感数据的安全性。

3.3 保证整体网络构架的安全

保障无线电子通信技术的安全应用，需要保证整体网络架构的安全。要保证整体网络架构的安全可以采取以下措施：（1）安全设计：在网络架构的设计中，遵循安全设计的原则和方法，考虑安全性能和安全保障细节，从而降低安全风险。（2）安全设备：在网络架构中部署安全设备，如防火墙、入侵检测系统、安全路由等，对网络的通信和数据进行实时的监控和分析，及时发现和清除安全问题。（3）数据加密：在整个无线电子通信网络中，采用数据加密技术，确保数据传输过程的安全性，避免数据信息在传输过程中被窃取或篡改。（4）访问控制：建立强大的访问控制机制，对不同的用户和设备进行访问控制和分级权限管理，确保核心资源的安全性。（5）异地备份：对网络架构中的重要数据进行异地备份，避免数据丢失或受损，建立健全的数据安全体系[2]。（6）周期漏洞扫描：定期对网络架构及其中的安全设备进行漏洞扫描，及时修补安全漏洞，保证网络的安全性。通过以上的措施，可以提升整体网络架构的安全性能，保障无线电子通信技术的安全应用。同时，组织相关的人员对网络架构和设备进行监控和维护，并定期进行评估，发现并解决安全问题。

3.4 创新网络接入方式

保障无线电子通信技术的安全应用，需要采用创新

的网络接入方式，以下是几种创新的网络接入方式：VPN（Virtual Private Network）虚拟专用网络：采用VPN技术可以建立一条安全的通信隧道，将网络上的数据进行加密，防止数据在传输过程中被窃取，从而安全连接到公共网络。SD-WAN（Software-Defined Wide Area Network）软件定义广域网：SD-WAN可以构建更安全、可靠和性能高的广域网，使用SD-WAN技术可以通过多条公共网络提供私有网络服务，实现灵活且统一的网络连接。IoT（Internet of Things）物联网：IoT是大规模无线设备连接和管理的网络，近年来快速发展。通信网络在IoT中通过智能设备进行连接，为用户提供不同的服务。因此，采用物联网网关和认证技术可以提高网络的安全性。5G网络：5G网络采用的是更为安全性强和可靠性高的通信技术，如NSA（Non-standalone）和SA（Standalone）架构，通过网络工具和协议对用户进行身份验证和流量控制，提高了网络的安全性。通过以上创新的网络接入方式，可以保障无线电子通信技术的安全应用。这些创新的网络接入方式具有高效、可靠、安全的特点，能够提高网络的安全性，为用户和企业提供便捷、可靠、安全的服务[3]。

3.5 建立网络安全机制，提高安全防范意识

保障无线电子通信技术的安全应用需要建立网络安全机制，并提高安全防范意识。建立网络安全管理机制：针对不同网络设备安全问题制定适当的网络安全管理策略，规范网络设备使用标准，建立完善的安全检查机制，对违规行为进行严厉处罚和追究责任。加强网络安全监测：部署网络安全监测系统，对网络加强实时监控，及时发现网络攻击等异常情况，加强风险评估和漏洞排查工作。提高人员安全防范意识：建立系统安全培训机制，为网络管理人员和用户提供安全意识和技术方面的培训，及时更新安全防范知识，防范社会工程学攻击行为，提高人员安全意识。加强网络访问控制：采用网络访问控制技术，对网络中的设备和用户进行访问控制，严格限制外部与内部网络的通信，保证网络的运行安全。建立应急响应机制：建立网络安全应急响应机制，为网络发生安全问题时及时作出决策和行动，保证网络安全可控。通过以上的网络安全机制和提高安全防范意识的措施，可以保障无线电子通信技术的安全应用。这些措施可以加强网络的安全性，为用户和企业提供安全、可靠、高效的服务。

结束语

无线电子通信技术的安全问题日益严重，要想解决这些安全问题，需要采取全面的安全措施。科技公司、政府和个人都需要承担自己的责任，在保护自己的同时，也需要尽力保护整个网络的安全。未来，随着技术的不断进步和安全风险的不断升级，我们需要不断探索更加高效和可靠的安全技术，以实现更加安全和可靠的无线电子通信技术应用。

参考文献

[1]杨柳，李雅洁，马梅芳，刘权，马天福.无线电子通讯技术应用安全探究[J].数字通信世界，2019（10）：65.

[2]廖铮.无线电子通信技术应用安全研究[J].计算机与网络，2021，47(17):53.

[3]程萍.无线通信技术面临的安全问题及防范措施探讨[J].无线互联科技,2021，18(17):5-6+49.

[4]马少华. 无线电子通信技术安全问题与安全技术探析[J]. 信息记录材料，2022（005）：023.

[5]陈志标. 浅析无线电子通信技术应用的安全问题[J]. 电子元器件与信息技术，2020，4（6）：2.

[6]刘佩奇，寇正. 探析无线电子通讯技术应用安全[J]. 电力系统装备，2022（4）：167-169.