试析无线电子通讯技术的应用与安全分析

张晓齐　杜　彪　刘嘉瑛　李林利
北方自动控制技术研究所　山西　晋中　030600

摘　要：伴随时间的不断进步，被普遍应用于通信方面的无线电子通信技术，由于具有对通信环境条件相对低廉的优点，尤其是在互联网科技不断发达的今天，通过网络和无线电子通信技术之间的相互连接，更大大的方便了人类的上网活动。但是无线电子通讯系统还存在着某些缺陷，其对外部环境的反干扰能力也相当薄弱，而且由于它所采用的是广域范围的通信方式，在通讯的过程当中，也就更容易遭到了他人的监听，这样也就对通信的安全度提出了非常大的考验。这篇文章主要针对无线电式子通讯技术的应用与安全展开了分析，并希望对一个国家的电子通信安全的建设产生一定的促进意义。

关键词：无线电子通信技术；通讯模式；通讯技术

1 无线通讯技术概述

所谓无线通信技术，是指利用在自由空间内无线电数据能够进行传递的特性进行数据交流的通信手段。近年来，由于科技的进展，通信技术方面也进行了大开发，包括使用最广泛、进展最大的当属无线通讯技术。无线通讯技术的应用方法大致有二种，其一为数字程控交换，其二为微波通信。所谓数字程控交换是利用人造的地球卫星作为进行无线电波传输的转播台，用于地球站或移动体之间的通讯联系所谓微波通信就是利用微波转播台进行数据传递的方法，由于一个无线电波通信系统，其频段通常非常长，所以在通话时往往能够携带比较大容量的数据，不过由于微波传输间隔通常比较短，一般大约只有几百千米，所以利用微波转播台使用的空间也要保持在几百千米以内。

直至20世纪90年代末，对无线网路提出了自己的体系结构规范，如IEEE802.11，规范了通过无线网络的媒质访问管理层和物理层，其关键内容就是对媒质访问管理层的规范。所有企业在制造电子产品的同时，都可以通过一个资料传输系统进行相互操作，并提供统一的逻辑链路管理层，也就是说通过媒质访问管理层以下一个完全透明的网络应用如此一来，在无线通讯网络的不同攻击行为互联，以及相同攻击行为内的多点连接都质优价廉[1]。在应用领域，解决了互联网的兼容问题就解决了最大的问题，它也代表着互联网的重提速大发展。至此，无线通信科技的发展基石得到了确立，无线通信科技也得到了蓬勃发展，并成为当前人们工作、生活、学习的基本需要。

2 常用的各种无线电通信技术

2.1 无线蓝牙技术

无线蓝牙芯片组技术，是无线电式子通讯科技中发展时期比较长的一种科技，它在一定程度上也属于智能技术领域，它能够利用技术完成电子设备之间的无线通信， 最短可以在三秒内进行接口设计和进行传输数据，并且最大范围可以达到一百m并且还能够使用一定的加密算法完成数据包加密和验证工作[2]。而通常，由于每个数据包的每次连接设备都使用了三十二个定址，因此理论上也可以使用数百亿设备;一对一的优化，并使用星形拓扑的一对或多连接;通过快速接通或者切断，信息就能够直接在网状拓扑中传递而无须维持复杂的网状网络。这种产品在不使用下，可以长期休眠，只有在必须进行工作的时刻才能唤醒。简单的讲就是省电、距离远。目前，无线蓝牙技术在智能家居和个人随身装置上的运用已经更加普遍。例如:将蓝牙技术运用到了智能手机中，当其远离主人的一定范围后，即可进行主动报警。

2.2 Zibee技术

它是近几年比较新型的无线通信发展形式，其基本的原则与蓝牙比较接近，要求在固定的平台上进行相应的短距离和低能耗传输，实现信息的传输。产品本身最大的优点就在于使用的便利性，有效降低费用。在技术运作流程中，技术可进行自主组装，技术同时应用于自动控制和远程管理中也十分适用，为整个设备使用过程提供了保证。需要注意的是，在技术运行体系里最根本的依托就是节点结构，整合无线通信网络建立较小的网络体系和运行模式，确保相关节点能发挥不同的作用，以提升整个项目管控效能，使组网通讯管理更为高效。值得一提的是，对于高效进行组网通信，还可以通过子结点和节点仪器进行分析与汇总，进而改善系统的质量。

2.3 无线局域网技术

这个情况是较为普遍的，有线互联网上存在的问题也能够在这种技术支持下得到较好的改善，这样提高了局域网拓展与应用的合规性。在无线设备应用的过程中，与有线网络之间通过无线网卡也可以形成相应的通信关系，从而保证了设备传输能力与有效应用上的完整性。此外，由于无线局域网技术具有很大的灵活性，这也使其很少能够直接收到线缆的影响，从而确保了其在设置上的随意性，同时还可以保证通信的品质不会受影响，便捷化程度可谓是极高的。此外，由于无线局域网技术的成本不高，避免了在施工现场的大量布线，极大节约了人力和物资，对安装的快捷化也是很大的进步，它不受空间约束的特点也促使了网络的覆盖范围进一步扩大，在现实中的使用也是非常普遍的。

3 无线通信技术在应用中面临的安全隐患

无线通信网络的重大突破个为通信网络的发展提供了基础以及巨大空间及跨越，使其可以通过国际标准中的通信协议的审核，从而使得外界的通信可以进入网络当中，与此同时还邮箱的避免了在常规的有限通信中的时间上的局限。但无线通信的安全隐患却在其不断进步中继续扩大着[3]。这些个存在的安全隐患，不但危害到了人们的通讯效率，而且也对通信设备使用环境中的安全性造成了相当大的冲击。再者，基于无线电子通讯网络的高度开放性的特点，在其实际的通信当中也同样存在着比较多的安全隐患。

3.1 非法窃取

当前，无线通讯技术的发展是十分迅速的，其发展趋势也越来越具有广泛性，最终的发展目标是能够不受其他各种因素的影响， 顺利无阻地实现信息媒体的高速传输。虽然当前无线通讯技术所能引起的影响微乎其微，为人类的日常生活方式创造了极为便利的通信传输条件但其难免出现缺陷。较为明显的就是安全性问题的突出，比如，非法窃听行为，这非常不利消费者信息安全的保障，而且还容易给一些机密文件带来安全风险，消费者因此遭遇了经济损失的现象也很多见。

3.2 用户系统被入侵

一旦无线电子通信网络遭到了入侵，那么系统内的用户安全就将得不到保证。近几年来由于网络架构的复杂程度日益增加，许多操作系统上开始存在着一些病毒文件，这些文件不易被发现，长期保存在系统内，找寻机会窃取信息。比如，很多病毒以广告的方式出现，一旦入侵到系统中或者被用户打开，就会迅速入侵进用户设备中，窃取用户信息，严重的还会导致系统瘫痪，对系统造成无法估计的损失。

3.3 非法基站

如今不法基站可谓是四处横向，以前的不法基站其主要功能就是对个人用户的很多关键个人信息进行盗取，但如今很多的非法基站不但会主动进入互联网对个人信息进行盗取而且还会冒充为电信运营商、银行、国家机关等不同的政府部门人员对个人用户实施欺骗，所以应该说在所有的安全问题中非法基站问题是较为严峻的一个， 其行为也是较为恶劣的[4]。另外，因为不少非法基站都是移动型的，所以要对其实施有效的管理也是存在着一定困难的。

3.4 非法篡改数据

一般来说，黑客会先在网上产生虚假的信息内容，继而对这种虚假信息内容加以包装，使之更加趋向于现实信息，如果有使用者遭到欺诈，便就实现了它们攻击互联网的目的。这种安全隐患已经在网络中遍布，亟需及时进行处理。

3.5 未经授权访问数据

尽管当前无线电子通信技术的发展已经十分迅速，但它依然有着不完善的地方，特别是在对用户信息系统的防护方面，在应用系统的安全体系中还是有着很多漏洞如果这种漏洞被不法分子使用后，它还会在没有系统许可下进入到用户信息系统中，访问用户系统的信息，条件恶劣的还会对系统的信息进行更改，实现盗取客户信息秘密的目的。面对以上这些巨大的安全事件，一旦没有进行及时有效的控制，那么将会使得个人的安全遭受巨大的危险，从而对整个社区的安全产生巨大的影响。

3.6 拒绝访问攻击

在无线电式子通讯技术的实际应用过程中，往往都会用到通信协议。而在通信协议中，由于协议存在着安全漏洞，因此一旦非法分子对这些安全漏洞实施入侵向通信系统发出了大量的非法访问申请，这就会降低了通信用户的访问效果。此外，一旦通讯系统误击无法访问网络连接，使用者的信息面临泄露的风险[1]。不管针对一般的行动电话系统而言，还是针对其子通讯系统而言，非法互联网的入侵都有很大的安全危险。

4 无线电子通信的安全性分析

4.1 对安全认证进行优化

要实现对无线电子通信网络的总体稳定性做出大幅的改善，不但必须系统化的控制其的使用流程，还必须对其使用过程的安全性认证加以完善，而且还必须集中阻止了一些充足安全隐患的网络，以便实现对其的使用流程加以优化。而在访问特权管理和身份验证系统的工作中，则需要通过对加密的方法加以应用，从而不断地

对验证有效性做出大幅的提升，以确保通过对管理水平和安全性的价值进行整合，进而对无线网络部署的有效性进行大幅的提高。同时需要结合实际的应用要求和技术体系，选择加密技术的应用，不但可以对设备提供合理的安全性保障，还可以对应用的安全要求加以全面的解决，也可以对产品的应用年限加以大幅的提升，进而使得各个环节都可以安全的进行操作。

4.2 升级安全内核

升级安全核心对于技术管控效能的提高也十分关键，因为技術人员可以借助系统化核心升级体系的实现，让无线电子通信技术本身拥有更强有力的针对非法侵入者的监测与告警体系， 从而对系统的后续工作进行保护。为了提高操作系统的安全稳定性，首先就必须对操作系统进行内部检查操作，对设备上存在的安全问题加以修改，以此提高安全管理的有效性使应用机制做到最优化。首先，必须扫描网络中的安全漏洞，并及时修补，如果发现了网络上出现的严重漏洞，就必须通过强有力的监测与控制措施，并不定期开展大规模的网络运行维修项目保证了系统运营时稳定的安全性[2]。必须构建起完整的机制，它是提高修复管理性能的关键手段，并为后期的安全提升提供坚实基础。其次，要对系统的安全程度做出判断，然后再按照最终判断结果划分设备应用的级别，而设备的实际工作状况又会对设备的工作参数产生更直接的影响，所以，技术人员要从具体问题分析合理地实施质量控制机制。另外，面对着系统漏洞与病毒攻击，还需要构建完整的管理机制，对定时系统进行安全扫描，以提升系统的安全级别。

4.3 绑定MAC地址

最常见的提高互联网安全的方法就是绑定MAC地址，在任何一种无线网卡上都有独立的一个MAC地址与之相对应把MAC地址注入到AP中，对它做出了相应的识别，以此使AP只有可以通过自己的无线网卡使用网络，而另外的无线网络用户则没有对这个网的使用权利不过由于这个操作方法的困难系数相当大，而且也极易引起骇客的入侵和对合法的MAC地址进行盗用，从而使得其使用范围也相当小，而且只有在特殊的环境中应用。

4.4 采用UMTS AKA可信认证协议

除了上述二种无线电子通讯方式的安全处理方法来说，通信系统也可能使用UMTS AKA的可信验证方案。无线电子通信系统是开放性的，一旦无线电系统不对信息进行安全防护，这些信息都是开放存取的。当访问这些普通消息时，无线电子通讯后台虽然也会提示用户进行安全验证，但通常这种验证方法都是比较为简单的[3]。只只有通过UMTS AKA可信认证协议，才能更好的保障无线电子通讯应用的信息传输安全性，从而避免了信息传输泄露问题。而通过UMTS AKA可信认证协议，相当于在无线电子通讯技术中引入了安全管理实体，电子通信使用者必须通过最高级别的安全密钥方可对这些网络数据进行存取。

结语

随着无线电子通讯科学技术的日益提高，在不同工作领域中的运用也已非常普遍了，对于人类工业生产水平的发展和人民生活水平的不断改善，一直在发挥着其相当大的作用，不过随着愈来愈多的而且越来越严峻的关于无线电式子通讯的完全隐患问题，也继续地向人们敲响了警钟。为了便于提高无线通讯技术的安全性，其范围内的所有相关人员也需要对影响着安全电子通信技术方面的问题加以分析，并采取了相对应的处理方法。以便于对网络通讯进行最大的保障。同时，以便于有效的提高客户终端设备的可靠性，就需要及时对系统进行及时的升级，并且同时要对可能存在的安全漏洞进行扫描。

参考文献

[1]李在林.无线电子通讯技术应用安全浅析[J].信息通信，2020（11）：211-212.

[2]游峥，等.无线网络安全通信探索[J].数字技术与应用，2020（3）：77-78.

[3]田兆东，等.无线网络安全探讨[J].信息与电脑，2019（3）：19-20.

[4]王用方，等.无线通信技术热点及发展趋势[J].科技信息，2019（8）：52-53.