 DOI: https://doi.org/10.12349/iser.v3i4.834

Research on the Security Guarantee Mechanism of Wireless Communication Network

Xiaopeng Han Hui Yu

Shenzhen Shiji Xinyang Technology Co., Ltd., Shenzhen, Guangdong, 518000, China

Abstract

With the development of science and technology, wireless communication technology is playing an increasingly important role in daily life. As a new way of network communication, network security has also been widely concerned. People also have new requirements for wireless network construction, but there are still many problems in the practical application process. This paper mainly analyzes and studies the current security mechanism in China, and puts forward these suggestions, and hopes to provide reference value for the construction of perfect theory system, promote the development level of wireless communication network and social and economic development, so as to promote the whole industry to a faster and better direction.

Keywords

wireless communication network; security guarantee mechanism; research

无线通信网络安全保障机制研究

韩晓鹏 余辉

深圳市世纪欣阳科技有限公司，中国·广东 深圳 518000

摘　要

随着科学技术的发展，无线通信技术在日常生活中发挥着越来越重要的作用。而作为一种新型网络通信方式—网络安全也受到广泛关注。人们对于无线网络建设也已经有了新要求，但是在实际应用过程中仍然存在着很多问题。论文主要通过对中国当前的安全机制现状进行分析和研究，并结合提出相应措施和建议来解决这些现实难题；同时希望能够为以后其他领域通讯网构建完善性理论体系提供参考价值与借鉴作用力，促进无线通信网络发展水平进一步提高以及社会经济建设进步发展，从而推动整个行业向着更快更好方向发展。

关键词

无线通信网络；安全保障机制；研究

1 引言

随着无线通信技术的发展，其应用领域也越来越广泛，但是随之而来的是信息安全问题日益严重。论文主要研究在网络运行中保障机制。从理论上分析了无线通信中各节点之间数据传输时可能会发生的一些危险情况并提出应对方案；同时通过对目前中国有线网络存在着诸如硬件设施落后、路由协议不完善以及病毒木马等缺陷进行具体阐述并且给出相应解决方案，希望能够为今后无线通信技术提供参考价值。

2 无线网络安全

2.1 无线通信网络安全基本概念

无线网络安全是指通过各种手段对有线通信网、移动通讯设备及相关系统进行有效的保护，防止其遭受到黑客或病毒袭击而造成信息丢失，影响用户使用体验。无线通信网络安全是指以有线或电磁理论为基础，通过对各种信息资源进行有效的保护，确保其能够在实际使用中不被损坏、丢失和毁坏。在互联网高速发展下人们生活更加趋向于数字化和信息化。随着计算机技术水平不断提升以及手机功能逐渐强大等一系列因素导致了网络规模越来越大且复杂多样；与此同时由于无线通信中存在着大量的应用终端、传输线路多并且覆盖范围广等等特点使得移动通信设备中的安全问题也越来越严重，其中通信网络安全问题也逐渐成为无线通信中的重点研究对象。

无线网络云管端保护机制流程如图 1 所示。

2.2 无线网络的特点

①无线网络的开放性，使得其可以实现无限延伸。在使用有线通信技术时，需要对所有接入设备进行设置和管理。

②由于无线网具有很强的隐蔽保护功能以及安全性能

【作者简介】韩晓鹏（1972–），男，中国陕西西安人，本科，从事无线网络研究。

高、安全性强等特点；同时随着计算机系统及应用软件技术不断发展成熟后也出现了很多新型网络，如虚拟机系、数字电视等等一系列新的通讯方式，使得人们可以通过各种途径来获取到自己想要得到信息资源与服务内容，从而使其能够在互联网上进行传播。

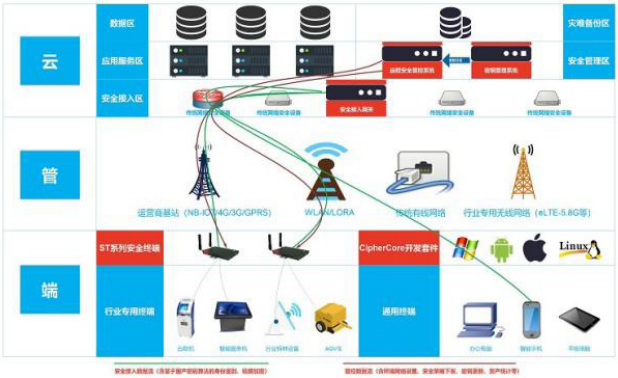

图 1 无线网络云管端保护机制流程

③无线网速快，可穿透性强。在高速运行时，信号的传输速度很高。而在低速时则要短。所以可以说其是一种非常理想的通信方式；同时也由于它有较好的保密性能和安全性、可靠性等特性被广泛应用到各种领域中去了；因此无线网络具有良好安全系数、可靠度以及灵活性这几方面特点：首先，无线网速比较快且可穿透性强，而且它可以穿透任何电子元件，这也是为什么无线网络能够广泛应用于军事领域的原因。其次，由于无线通信技术具有高可靠性、高安全性等优点而被广泛应用到各种军事通信系统当中。最后，因为其可靠性能和安全系数较低且容易受到攻击或破坏后造成难以挽回损失并导致无法修复、难以恢复以及成本高等问题使得在实际应用中很少采用这种方式来进行信息传输。因此，人们越来越重视对无线网络的研究与发展。

3 无线通信网络安全现状

3.1 当前无线通信网络中的存在的风险

无线通信网络的安全是指以有线或电磁系统为基础，通过对其数据信息、传输线路等重要硬件设施和环境进行有效管理，确保在应用中不被黑客或者病毒入侵而影响到正常使用的情况下可以可靠地运行。目前中国关于无线通信中存在着较多安全隐患：

①防火墙技术不足。随着计算机通信网络发展进程加快以及移动互联网用户量增大及网络接入点增多，各种安全威胁因素会逐渐增加。

②网络漏洞。在无线通信中，由于系统的管理和维护不足，会造成信息泄露、丢失等问题。

③数据加密技术不到位。无线通信协议中存在着大量的信息安全隐患需要及时更新与完善；重要保障措施有待提高：加强硬件设备防护性能以及提升软件功能应用水平以应对可能出现攻击行为和威胁因素并制定相应防范机制来进行有效规避风险发生。

④恶意软件入侵。由于无线网络的开放性特点，在进行数据传输过程中，容易遭受到黑客攻击，导致信息丢失或泄露；如图 2 所示恶意软件入侵。

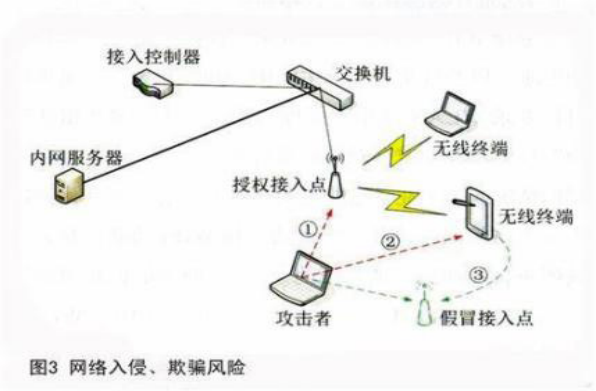

图3 网络入侵、欺骗风险

图 2 恶意软件入侵

⑤网络病毒入侵。随着互联网技术的发展，各种黑客通过非法手段侵入无线通信系统，对人们生活带来了极大影响。

⑥窃听。由于无线通信中存在着大量病毒以及恶意程序等会造成信息安全问题隐患；在中国一些重要领域中也普遍出现过短信诈骗、电话诈骗和邮件盗窃现象等等危害用户财产及人身权益的事件发生。

3.2 线通信网络安全保障的主要方法

①数据加密技术。在无线通信中，数据的传输是非常重要的步骤，因为它不仅仅关系到通信网络中所有信息之间是否安全。因此必须采用一定方法来保护其机密。例如将一些敏感文件放到密保库里面进行处理和控制；或是通过对信道、收发器等设备采取不同手段来确保保密性；还可以采取防火墙或加密软件等措施防止被黑客攻击或者窃取数据资料等等。

②安全协议、加密。在有线通信网络中，数据传输过程中需要通过不同的传输方式进行信息传递。因此，对无线通信网安全性和保密性提出更高要求。为了保证系统运行时的可靠性以及数据完整性等问题不被破坏而采取了加密技术来保障其安全可靠性能是目前最主要解决办法之一。

③加强网络安全的技术研究。在无线通信网中，我们可以通过采用一些先进、科学合理和可靠的方法来提高对计算机系统安全性问题。首先要进行防火墙设计，防止黑客入侵；其次是建立一个有效的内部控制机制来保证信息数据不被非法访问或窃取；最后就是需要制定一套完整而又行之有效的管理制度用来规范企业员工行为准则以及维护网络安全等措施 [1]。

④加强无线通信网中硬件设备和软件的建设与升级、完善相关技术标准体系。

⑤通过制定合理的管理标准来规范企业内部人员、系

统及设备等。在无线通信中实现信息资源共享是一个重要环节；也是最主要的是保证其安全性和可靠性以及确保其能够顺利完成工作所必须采取的措施手段，如对数据进行加密处理、采用防火墙技术等都是非常必要且必须要解决问题。

4 无线通信网络安全保障机制研究与建议

4.1 完善无线通信网络安全保障系统结构

在无线通信中，由于通信网络的复杂性，会产生很多问题。因此要对有线数据进行保护和管理是非常有必要，需要加强系统结构设计、优化配置等工作。在无线通信中，需要构建完善的网络安全保障体系，才能有效保证通信系统和数据传输过程中信息的安全性。首先要加强对用户身份认证工作。通过用户登录密码、口令证书等方式，来确保使用者输入授权文件时不存在非法操作；其次是增强防火墙技术应用：对于一些重要或者敏感设备采取防火墙设置措施防止黑客入侵或病毒侵入导致不必要损失浪费钱财；另外就是完善网络安全管理机制，在日常运行当中不断更新系统的漏洞和缺陷并加以改进以提高安全性。

4.2 加强无线通信网络的信息安全传输

在无线通信网络中，信息传输是非常重要的，因为它可以确保用户能够安全可靠地接收和发送数据。因此必须加强无线信道的安全性。首先要提高系统自身性能。其次要对硬件进行升级、增加软件加密技术以及采用防火墙等措施来防止黑客或者病毒入侵到内部网络，从而保障信号传输过程当中不受到干扰；最后还需要保证无线通信设备在应用中具有良好运行环境，以避免受到攻击，确保信息传递不会受损害或影响正常工作和使用功能，进而降低数据的丢失率 [2]。

4.3 加强无线通信网络安全保障风险监控

加强无线通信网络安全的风险监控。在实际工作中，为了更好地应对各种可能存在威胁到系统的隐患，需要对无线网内所有设备和设施进行全面监测。例如：主机、路由器等重要信息数据都会被检测出来；传输通道上安装了数字证书以及防火墙等等防护措施来保证其安全性；对于终端产品来说需要定期检查是否出现病毒或者是黑客入侵行为导致数据包丢失的情况发生 [3]。

在网络通信运行期间，要加强无线信道的监控，防止信息泄露。首先可以通过设置防火墙系统来提高其安全性。由于无线通信中信号传输具有一定时间段内不可恢复性和易受干扰因素影响而导致数据丢失、误码率上升等问题；其次还应该注意到：一是对重要用户进行加密处理并及时更新密码以保证重要客户不受到攻击或破坏通信环境。二是在网络中使用防火墙技术，防止非法入侵者通过网络进入系统造成信息泄露。三是加强无线信道监控，防止非法入侵者通过网络破坏通信信道，造成信息泄露。四是还需要加强数据加密，保证无线通信中的重要用户不受到攻击。

4.4 提升硬件和软件设施

首先，要加强防火墙技术的应利用，用网络安全协议对计算机系统、数据信息进行控制。同时在日常工作中也应该定期检查和维护内部文件。其次，硬件设备方面采用先进可靠稳定的光纤宽带传输方式与移动通信终端建立无线局域网连接；使用数字证书认证等手段提高无线信道性能水平；对有线接入方式采取保护措施，防止因人为因素导致信号被破坏或丢失造成不必要损失，从而保证数据信息安全、完整无误地传递至接收端并进行有效处理。

5 结语

无线网络的发展是伴随着通信技术不断进步而得到快速提升，同时也促进着人们生活质量的提高。但是，由于中国在无线通信中还存在许多安全问题、管理漏洞等。因此为了使我们国家能更好地建设好国际信息沟通平台和国际社会交流合作机制以及为人民服务的目的出发提出了很多新要求来满足未来发展需求；另一方面来说网络环境是一个开放性系统并且具有不确定因素，这就对通信技术带来一定挑战也会阻碍其进一步进步。

参考文献

[1] 卿立银,万里冰,罗俊海.5G环境下信息系统网络安全保障模型研究[J].数字技术与应用,2021(4).

[2] 王小虎,王超,李群,等.基于黑盒遗传算法的电力系统网络安全漏洞挖掘方法[J].沈阳工业大学学报,2021(5).

[3] 李凤华,张林杰,陆月明,等.天地网络安全保障技术研究[J].天地一体化信息网络,2020(1).