无线通信研究
2020 年 8 月第 2 卷第 3 期

Research on Security Problems and Prevention Strategies of Wireless Communication Network

Lai Qingde

ZTE Technology Communication Co., Ltd., Shenzhen

Abstract: This paper studies the security problems and preventive strategies of wireless communication network, briefly describes the problems of information theft and information tampering, network damage, false message, signal control and other problems in the use of wireless communication network, and proposes strengthening the security evaluation of communication network, improving the technical standard of identity authentication, encrypting wireless communication network and setting network resource rights The strategy of limiting the level of prevention.

Key words: Wireless communication network; Security issues; Information theft

Received:2020-08-13; Accepted:2020-08-25; Published:2020-08-27

文章引用：赖清德. 无线通信网络的安全问题及防范策略研究 [J]. 无线通信研究, 2020 (3): 96-101.
https://doi.org/10.35534/rwc.0203015c

无线通信网络的安全问题及防范策略研究

赖清德

中兴科技通讯有限公司，深圳

邮箱：1020209697@qq.com

摘　要：文章对无线通信网络的安全问题及防范策略进行了研究，简要说明了无线通信网络使用过程中存在的信息盗取和信息篡改、网络破坏、虚假消息、信号控制等问题，提出了加强通信网络安全评估、提高身份认证技术标准、无线通信网络加密以及设置网络资源权限等防范策略。

关键词：无线通信网络；安全问题；信息盗取

投稿日期：2020–08–13；录用日期：2020–08–25；发表日期：2020–08–27

近年来，科学技术得到了前所未有的发展，为人们生活带来便利的同时，

https://doi.org/10.35534/rwc.0203015c

也带来了困扰，主要是给无线通信网络自身开放性的特点埋下了安全隐患。在用户使用中，由于操作不当或者网络自身问题导致网络安全问题出现，给用户带来不利影响。因此，对其防范策略进行探究具有重要的现实意义。

1 无线通信网络的安全问题

1.1 信息盗取和信息篡改

在无线通信网络运行的过程中，不法分子能够通过非法手段进入到使用者的计算机中，对使用者计算机中的信息进行盗取、篡改，或是在信息传播的过程中将其截取，并对其进行修改。一般来说，不法分子盗取和篡改信息的原因有以下几种：一是通过盗取用户的信息来牟取利益；二是通过篡改信息来获得信息接受者的信任，从而达到一定的目的；三是通过篡改信息来破坏信息发送者和接收者之间的关系。

1.2 网络破坏

通常情况下，网络安全问题往往伴随着病毒对计算机的攻击，病毒通过某种途径进入计算机中，破坏计算机的系统。病毒的种类成千上万，带来的影响也不同，但是都会对计算机的使用造成影响，使计算机无法正常运行。如果在工作的过程中发生了这种现象，很可能会给使用者带来经济上的损失，尤其对于金融行业。

1.3 虚假消息

虚假消息是指部分用户通过无线通信网络在网络中发布一些不实消息，从而影响网络安全。具体表现在以卜几个方面：利用网络中的虚假信息骗取用户的信任，然后对其进行诈骗，牟取经济利益；在网络中传递大量的垃圾信息，造成网络拥堵的现象，给无线通信网络的正常运行带来影响，降低用户的网络速度。

2 无线通信网络安全问题的防范对策

2.1 加强通信网络安全评估

加强通信网络的安全评估工作，能够为无线通信网络的安全运行提供保障。因此，在对无线通信网络进行管理的过程中，管理人员需要根据具体情况对网络的安全进行评估。评估的主要对象是无线通信网络的用户和潜在用户，评估的内容包括信息来源等与网络安全有关的因素，并尽量确保评估结果的准确性和具体性。目前，专家评价法、模糊综合评判法、事故树分析法是最常见的几种通信网络安全评估法。例如，针对网络漏洞问题，可以采用专家评价法对其进行全面的分析和评估。在此过程中，需要选择具有权威性的专家，分析漏洞本身的相关参数，评估每个漏洞对系统造成的伤害程度等，进而有针对性地解决相应的安全问题。

加强对无线通信网络的安全分析。在无线通信网络的管理中，需要对网络本身进行分析，从而找出网络中可能存在的问题，并及时进行处理。同时，相关技术人员应该对网络安全分析的方法和解决问题的策略进行进一步优化，提高对网络安全问题的预防能力，减少安全问题出现的可能性。需

要注意的是，对无线通信网络的安全分析，应该根据通信网络的具体情况进行。例如，目前市面上存在的计算机病毒种类繁多，技术人员需要对计算机病毒的种类和传播方法有充分的了解，并对病毒可能产生的影响作出评估，一旦出现病毒感染的情况应迅速预警，使技术人员能够及时对病毒进行处理，减少其对网络安全造成的危害。

加强无线通信网络安全保障。我国无线通信网络的发展十分迅速，信息网络技术被应用于各行各业中，网络安全技术也得到了极大的提高，减少了网络安全问题发生的可能性。目前人们常用的网络安全技术有信息加密技术、网络防火墙以及漏洞扫描技术等，能够极大地提高使用者计算机的安全性能，提高网络防护技术的水平以及无线通信网络的安全性和稳定性。

https://doi.org/10.35534/rwc.0203015c

2.2 提高身份认证技术标准

身份认证技术是一种在计算机网络中对使用者身份进行确认的技术，能够有效地对用户的网络资产进行保护，避免不法分子非法占用或修改无线通信中的信息，保护用户数据信息的安全，减少网络安全问题发生的可能性。在环境相对开放的无线通信网络中，身份认证技术能够阻止不法分子进入通信网络中，提高网络的质量和安全性。其主要标准有以下几方面：一是身份认证技术需要能够对传播和接收的信息进行辨认，确定其真实性。二是能够判断用户接受的信息是否完整，防止不法分子在信息传递的过程中对其进行截取和篡改。因此，身份认证技术在无线通信网络的安全防护中有很大的作用，能够降低不法分子进入通信网络的可能性，从而提高网络的安全性和稳定性。

2.3 设置网络资源权限

目前，用户在无线通信网络中并非是完全不受限制的，在资源应用以及访问网络的过程中，会需要一定的权限，从而对用户的使用造成限制。在对网络资源设置权限时，需要结合实际情况来进行，科学设定用户获得资源的条件，使用最为广泛的方法将用户传出的信号进行加密，只有在用户输入了正确的密码后才能够正常读取信息。这种方式可以减少不法分子进入系统的可能性，提升无线通信网络的安全性和稳定性。

3 结语

随着科技的进步，信息网络技术已经深入人们的日常生活和工作中，无线通信网络也得到了很大的发展。目前，我国无线通信网络中存在许多安全问题，为了提升网络的安全性和稳定性，相关人员需要对这些安全问题予以足够的重视，及时发现无线通信网络中存在的不足，并对其进行调整，促进我国通信事业健康、稳定的发展。

参考文献

［1］庄勇．无线通信传输安全问题分析［J］．中国新通信，2020，22（13）：

169.

［2］杨纪岩. 无线电子通信技术应用的安全问题分析［J］. 中国新通信，2020，22（9）：30.

［3］段翠华，孙忠阁，孙远芳. 浅析无线通信网络安全保障机制［J］. 网络安全技术与应用，2020（3）：70–71.

https://doi.org/10.35534/rwc.0203015c