基于计算机技术的无线通信网络安全风险预测研究

张　一
汉中职业技术学院　陕西汉中　723000

摘　要：社会科技与经济水平的快速发展促使人们对互联网环境的安全提出了更高的要求。通信网络作为城市虚拟化建设的重要组成部分，与人们的生活和工作息息相关，如何构建科学高效的无线通信网络安全评价模型已成为重点研究内容。随着信息化的发展，我国已步入通信时代，网络系统结构等方面发生较大变化，通信网络安全问题不仅会对用户体验产生影响，还会对地区网络安全造成威胁，从而影响地区经济。本文主要分析基于计算机技术的无线通信网络安全风险预测研究。

关键词：风险预测；网络安全；无线通信；计算机技术

Research on Security Risk prediction of Wireless Communication Network based on computer technology

Yi Zhang
Hanzhong Vocational and Technical College, Shaanxi Hanzhong 723000

Abstract: The rapid development of social science and technology and the economic level prompts people to put forward higher requirements for the security of the Internet environment. As an important part of city virtualization construction, the communication network is closely related to people's life and work. How to build a scientific and efficient wireless communication network security evaluation model has become the focus of research. With the development of information technology, great changes have taken place in the structure of network systems and so on. Communication network security issues will not only affect the user experience but also pose a threat to regional network security, thus affecting the regional economy. This paper mainly analyzes the research of wireless communication network security risk prediction based on computer technology.

Key words: risk prediction; network security; wireless communication; computer technology

引言

无线通信网络已融入人们的日常生活与工作中，极大地改变了人们的生活方式。然而，无线通信网络也为部分非法分子提供了可乘之机，其利用各种非法手段对无线通信网络进行攻击，从而窃取用户的重要数据信息。因此，现阶段的无线通信网络在创新发展过程中必须重视安全问题。本研究针对现有的无线通信网络安全风险问题预测评估模型中存在的精确度不高等问题进行分析，提出了基于计算机技术的无线通信网络安全风险问题预测评估模型，并通过试验测试证明了该模型的实际应用效果，以此希望能为行业人士研究提供一定帮助。

一、无线通信网络结构与安全风险概述

现阶段，无线通信网络可分为固定网络与移动网络两种。其中，固定网络是指固定有线的电话网络，包括宽带网络和电话网络；移动网络是指互联网与移动通信结合的通信网络技术。随着我国进入通信时代，移动网络在社会发展中占据的地位也越来越重要。从本质上讲，移动网络是通过保障无线通信网络畅通来提供更高质量的网络服务，从而实现超远距离的通信传输，其存在着一定的有线传输，包括光缆传输与电缆传输。从结构上来看，无线通信网络包括核心网和接入网。核心网将用户的请求数据传递到不同网络系统中，承担着管理员的责任。核心网包含移动网、传输网、数据网、承载网、交换网等。交换网由电路域、EPC 及分组域等结构组成，各结构之间相互协调配合，从而实现对不同用户数据连接、综合管理及业务承载等功能[1]。接入网是相对核心网而言，通过网络用户与交换机之间进行有效的通信沟通，从而实现数据资源的交互。接入网是确保用户能够将自身请求信息发送到核心网的重要保障，其作用相当于服务大厅，用户请求的信息只有进入服务大厅后才能进入下一步程序。从理论角度来讲，通过核心网与接入网即可实现无线通信网络的应用，但是从实际角度来说，要想实现信息数据的有效传输，还要有承载网、传输网等网络系统的辅助。承载网介于交换机与接入网之间，主要负责对语音等数据业务进行传输。传输网主要对不同地区的信息进行有效传输和连接，是实现远距离信号

数据传输的重要保障。对无线通信网络风险进行分析预测，能够使人们深入理解和认知风险，同时能帮助人们判断风险问题是否得到有效的解决，依据分析预测结果制定更为科学合理的保障措施[2]。

对无线通信网络进行分析可以从以下两方面进行。①通信网络系统风险分析。复杂的无线网络系统及多元化的网络服务需求导致无线通信网络产生“潮汐效应”。人流量过于密集的区域，由于该区域的无线网络容量有限，在高峰阶段网络质量与传输效率等受到干扰，导致用户体验感较差。现阶段，无线通信网络由光传输系统、电源系统及基站系统等构成。其中，电源系统是确保整个无线通信网络能够正常运行的基础，所以要确保通信电源的稳定性、安全性及可靠性。②无线通信网络安全风险分析。与有线网络相比，无线通信网络具有更加包容与开放的网络信号，能为用户提供更加方便的通信服务，但也增加了潜在风险，如信息监听、数据泄露等。无线信号窃听是无线通信网络中常见的安全风险问题，即用户基础身份信息、数据信息、无线信息等被第三方窃取得到；假冒攻击是盗用者将用户的身份信息进行拦截后，冒用其身份进行其他操作；信息数据篡改是攻击者通过一系列的手段进入到用户无线通信网络中，并对其相关信息数据进行随意修改[3]。

二、无线通信网络安全关键技术

2.1 无线无线通信网络安全体系设计

对于目前无线无线通信网络所面临的安全威胁而言，绝大多数都是在各协议层对网络实施窃听、干扰、入侵与分析等，以此达到降低或者破坏通信网络本身效能的目的。为此在实际进行安全设计时，还需从以下几方面着手：第一，将重点放在协议层，把纵深防御作为基本目标，使防御重心下移，提升物理介质层以及访问控制层的安全防御效果，由此在信号和链路层面达到高强度的身份认证以及访问控制。一般有效防御协议层次越低，网络攻击给整个系统带来的影响也就越小。第二，对网络层安全机制进行简化，针对传输层及其以上的应用层安全机制实施有效处理，尽可能减少将端到端等方面作为基础的安全措施使用。这是由于这类安全措施往往需要极大的网络开销，网络连通方面也有很高的要求，无法真正适用于吞吐量较低、间歇性中断以及延迟较高的无线无线通信网络。第三，把重点放在无线网络系统上，在通信介质层以及链路层当中应用异构体制的设计方法，以系统层面为核心，提升无线网络的应用性能[4]。

2.2 网络信誉安全管理机制

在目前的管理机制当中，最常见的是基于信任的管理机制，其中以信誉安全管理最为典型，十分适合应用在广域部署、异构、开放的海洋无线无线通信网络环境当中。它主要依照网络各节点的各项行为特征对可信任程度实施量化评估，其中节点信誉的产生、更新、融合、发布等相关操作都由信誉体系架构决定，主要分为中心式及分布式两类。（1）中心式。即将网络当中的所有节点的信誉数据都存放在一个及以上的中心节点或者信誉管理节点上，然后管理节点再应用融合算法综合评估所有网络节点的信誉情况，最后将获得的数值分享到网络当中。在这之中，节点信誉数据的获取十分便捷，但只要管理节点崩溃或关键链路被阻塞，就会导致整个信誉体系难以正常运转。（2）分布式。直接应用完全对层或者分层对等的架构，最常见于分布式、异构等网络环境当中。在这之中，所有节点都基于一致或独立性的算法机制分析与评估网络层、介质层所能感知的各节点网络行为，然后再分散保存到网络当中，利用广播查询或者信任链的形式得到目标节点的实际信誉数值，由此展开本地计算。这一模式能有效解决中心式架构单点失效的问题，并且还能有效获得节点本身一定范围网络当中的节点可信任度。但由于其实现机制复杂，在多跳场景当中需要一定的网络开销。受到无线无线通信网络实际应用和结构特征的影响，该荣誉体系更具优势。以节点可信任性将其划分成不同等级的子集合，最终在重叠网络机制与物理网络下建立各级逻辑子网。

三、无线通信技术网络安全性提升的措施

3.1 构建安全架构

当前无线通信技术的发展速度飞快，在未来的通信事业中必然占据重要地位，且能够具有较大的影响力，所以必须从不同的角度出发对其应用进行探究。提升网络的安全性，应首先完善无线通信技术相关的综合维护工作，并以此为基础对安全架构进行构建。对于网络环境来说，因为其自身具有较高的开放程度，所以遭遇网络攻击的可能性较大，在此情况之下，应该首先坚决拒绝受传统思想的束缚，积极构建起无线通信技术专属的安全架构，并寻找一条与实际情况相符的新思路，尽可能避免网络安全受到攻击，也就更有利于保护用户的隐私。需要注意的是，对安全架构进行构建具有一定的难度，其中需要应用的技术较多，所以可以选择将 4G 作为基础进行升级，逐步开展技术的革新和设备的优化[5]。

3.2 建立高效的加密算法

促使网络安全性得到提升的过程中，必须注意对无线通信技术中所具有的特殊性进行充分考虑，且需保障算法中具有良好的加密型和高效性。在对无线通信技术进行应用时，其中能够体现出延时性低的优势，而在进行传输时，则能够体现出高密度的优势，以此为基础，网络安全漏洞较为显著。从实际上来看，在对流密码体制进行应用之后，无线通信技术之中的加密效果更加良好，同时轻量级加密算法的开发工作也能够得到进一步优化。对网络安全进行维护，加密算法属于其中的重要手段之一，对其进行应用，也需要从多个角度出发进行考虑，才能够对无线通信技术在未来的发展方向进行全面掌握。另外，针对加密算法进行测试，其中力度的调整应该通过逆向思维进行确认，例如，不法分子在进行

违法行为时，可能如何进行破译和攻击等，以促使加密算法具有更加良好的性能和应用效果。

3.3 全面探究与清除网络中可能包含的漏洞及问题

在开展局域网评估工作时，当查找到安全性能不高或者存在软件应用风险等问题时，都必须要充分重视网络安全问题的分析。在实际进行问题分析过程中，网络维护人员应当要对各个网络数据信息进行探讨，以此来判定网络受影响程度，假使表明有侵入影响，则需要尽快强化网络安全性能。例如可以采用 IP 访问限制的手段强化数据通信网络的安全性。

四、结束语

综上所述，无线通信技术可以在一定程度上根据用户需求进行发展，不仅能够呈现出更高的可行性，也具有更加多元化的操作方法，并能够在生产、生活等多个方面发挥出重要作用。并且，对于网络安全来说，相应的管理和防护体系不断趋于完善，网络安全中的综合保障也就得到了持续的强化，所以未来有必要针对网络安全相关技术进行更加深入的探究，以促使网络安全防护技术更加完善，并能够体现出更加显著的应用价值。

参考文献：

[1] 杨屹 . 大数据背景下计算机信息技术在网络安全中的运用探析 [J]. 信息记录材料，2021(9)：47-48.

[2] 张勇，沈磊 . 烟草企业计算机网络安全的风险识别及应对策略 [J]. 网络安全技术与应用，2021(7)：133-135.

[3] 程艳艳 . 基于计算机技术的无线通信网络安全风险预测研究 [J]. 信息通信，2020(8)：67-68.

[4] 梅映天 . 基于信息挖掘技术的网络信息安全风险预测分析 [J]. 信息记录材料，2020(8)：41-43.

[5] 张春萌 . 网络安全风险可视化系统的研究与实现 [D]. 青岛：山东科技大学，2020.