基于人工智能的5G网络安全管理技术分析

黄敏　李伟渊　何伟贤

（中国移动通信集团广西有限公司，广西　南宁　530028）

摘　要：传统常规的网络安全管理技术尚不具备5G网络数据的处理能力，即便是将其运用到5G网络环境，最终取得的处理效果也并不理想，而利用人工智能算法优化5G网络安全管理技术就能有效解决以上问题。基于此，本文简要概述了5G网络与人工智能的概念，分析了5G网络的安全需求背景，以及人工智能对5G异常网络的定位与检测方法，还提出了人工智能应用于5G网络安全管理技术的实施策略，旨在充分发挥人工智能算法在5G网络安全管理技术应用中的优势。

关键词：人工智能；5G网络；安全管理技术

传统5G网络安全管理技术仍然存在管理效率低的问题，但将人工智能应用于5G网络安全管理技术就能精准识别网络运行环境的安全风险，切实提高5G网络运行环境的管理效率。人工智能指人工制造而成的机器具有良好的智能化特点。以人工智能为基础优化5G网络安全管理技术设计，可以有效突破传统网络安全管理技术的弊端，并为5G网络运行的稳定性提供基本保障[1]。

1　5G网络与人工智能

1.1　5G网络

自移动通信技术推广与发展以来，其不仅经历了模拟到数字、语音到数字、窄带到宽带的推陈出新阶段，还在每一次技术变革期间极大地推动了人类社会的发展进程，并为通信行业带来了一定的机遇与挑战。5G网络作为面向未来发展阶段的新型通信技术，不仅有效提高了信息传播与共享的速度，还将人与人之间的通信上升到万物互联的层面。目前5G网络的应用场景主要包括以下三个方面：第一，移动宽带，主要适用于高效化、大容量的数据传输场景，如超高清3D视频、虚拟现实等。第二，超可靠低时延类通信，适用于对网络可靠性与延时性要求相对较高的智能驾驶、远程医疗等领域。第三，海量机器类通信，主要用于接入和管理大规模、低功耗的传感器，如工业物联网、智慧城市、环境监测等对数据传感与采集要求较高的应用场景。

1.2　人工智能

随着计算机与信息技术的快速发展，传统以知识为驱动的智能系统正朝着以数据为驱动的计算智能、机器算法等方向升级转型。在海量数据信息不断增长的背景下，我国现有的硬件设施建设、先进学习算法以及神经网络架构愈发趋于完善，极大地突破了传统人工智能研发中存在的弊端，而具有性能优良、效率高、适用性强等优点的多层神经网络，更是凭借深度学习、强化学习等优势在各行业领域中得到了广泛应用。在新时代背景下，人工智能逐渐在图像识别、数据分析、无人驾驶、机器人等多个新型领域中有着广泛的应用前景，真正为传统行业的现代化发展带来了全新的机遇[2]。

在通信工程领域，人工智能主要用于流量监测、智能运维、安全保护、业务分析等多个方面，而5G时代的到来，又为人工智能在通信网络中的应用创造了良好的先决条件。如我国新型网络架构体系不仅克服了底层硬件的差异，还为人工智能的未来规划布局奠定了良好基础。而5G网络在新时代背景下正面临着复杂的环境变化需求，这也使得传统以人工模式为主的网络逐渐趋向于由AI主导的智能模式发展。

1.3　人工智能在5G网络中的应用优势

5G网络适用的三种应用场景与垂直行业的创新性发展之间存在密切的关联，有助于推动人类社会实现智能化、信息化发展目标。最主要的是，5G网络的衍生可以有效加快数字社会的发展进程，使得通信市场的未来发展阶段迎来全新的机遇，真正意义上达到了以市场需求为驱动促进技术成熟发展的目的。与此同时，5G时代的到来使得业务需求多元化、网络环境复杂化、用户体验个性化，这也在一定程度上加大了网络运营维护的难度[3]。

海量数据信息、云端化基础架构为人工智能的培育和应用奠定了良好的基础，使得人工智能还具有的超强计算能力、算法精准以及海量数据支撑等基本特征。而5G网络的内在资源需求与外在应用需求，又使得人工智能可以与5G网络共创优势互补、互利共赢的发展局面。

2　5G网络的安全需求背景

5G网络的开放性功能可以位于网络控制功能之上，以此有效促进网络服务与管理功能朝着第三方开放。而5G网络的开放性功能不仅局限于整个网络能力的开发，其更多的是体现在内部网元之间的能力开放。相比于这个网络的点对点开放流程，5G网络的各个网元都可以实现开放服务，并利用应用程序接口在不同网元之间调用开放能力。基于此，5G网络的安全需求应以核心网内部网元与外部第三方网元为基础，保证其具有灵活的安全能力，以此为不同业务的签约和发布奠定良好基础，使得每位用户都能享有安全服务。

基于5G网络的多元化接入方式与设备形态，在未来发展阶段必须建立一个统一的认证框架，以此将各种接入认证方式进行有效整合，同时对现有安全认证协议进行优化与革新，切实提高终端在移动网络间切换时的安全认证效率，使其在更换终端或接入方式时也能获得持续的业务安全保障。最后，对于5G网络的发展，还需要构建一个统一的身份管理系统，以此满足不同认证方式、不同身份标识以及认证凭证的实际需求，真正为不同形态、不同能力的差异化终端奠定良好的平台基础。

3　人工智能对5G异常网络定位与检测

当前，5G网络正面临着严峻的安全问题，特别是在复杂的网络环境下很难对入侵病毒进行检测与防御。传统网络防御工具只能对已知的恶意代码进行检测，黑客或病毒只需要对恶意代码中的某个部分进行整改，就可以突破这种网络防御，而人工智能下的网络防御则能精准识别网络中的异常行为模式，及

时检测网络运行中存在的异常情况，并针对未知攻击制定出科学可行的应对方法[4]。

将人工智能应用于5G异常网络的定位与检测时，由于5G网络在未来发展阶段，会将宏基站与微基站进行有机结合，形成一个集4G、5G、WiFi等多种接入方式于一体的异构网络。但在新时代发展形势下，随着通信业务的不断增加，用户的需求将会愈发趋于多元化，仅依赖于WiFi优先的接入准则难以满足用户日益增长的业务需求，也不利于资源利用率的提高。而AI技术却能通过分析功能，检测用户的业务需求与网络环境，实现接入网络的自动化选择，同时根据用户的移动轨迹与访问记录自动进行预设置，以此完成不同网络、不同区域之间的顺利过渡，切实提高用户服务体验的实效性。

5G网络最鲜明的一个特征在于将人与人之间的互通互联延展为万物互联，极大地扩展了网络规模及复杂程度，这也使得网络运行与维护成本急剧增长，传统以人工、预先策略为主的运行维护机制早已无法满足新时代发展需要。但将人工智能应用于5G网络运维，就能深入挖掘其中蕴含的历史数据，同时构建一个健康的网络安全模型，实时评估与检测网络的运行态势，基于人工智能的时序推理能力，科学预测网络的流量趋势，并对网络资源进行合理化配置与调用，提供高效化服务的同时减少能源损耗。最后，针对监视与警告信息的关联性进行分析，还能第一时间定位故障的具体位置，并排查引发故障的主要原因，以此在短时间内快速排除5G网络运行故障[5]。

4 人工智能应用于5G网络安全管理技术

4.1 5G网络节点安全分级

基于人工智能算法计算5G网络节点的重要性值时，可以将网络节点科学划分成四个安全等级，而不同安全等级的网络节点，需要采用不同的安全管理方式及管理手段，以此实现5G网络节点的安全分级。假如G由具有m个5G网络节点V与n条网络传输链路E的无向图构成，在m×n关联矩阵的支持下显示网络结构中各节点相应链路之间的关联，并将这一关系矩阵定义为R。其中矩阵的每一行都可以表示为5G网络的一个节点，而矩阵的每一列则代表网络节点及对应边的关系属性值，并将矩阵R中的各个元素取值为0或1。若矩阵元素表示为0，说明对应链路与指定网络节点并无关联；若矩阵元素取值为1，那么对应链路与网络节点正相关。

4.2 5G网络数据库安全管理

5G网络服务器中的数据库主要以网络数据信息的存储终端为基础，但这也同样导致不法分子会恶意攻击、窃取网络数据库中的信息。基于此，对5G网络数据库进行安全管理时，具体可从以下三个方面着手：第一，对数据库中存储的数据信息进行加密处理，将数据库中以明文形式存储的数据处理为密文的形式，并由数据库管理员做好加密密钥管理工作，从根本上保障5G网络数据库管理的安全性。第二，一旦发现硬盘数据丢失或者数据库发生运行故障，就会导致数据库出现数据丢失的情况，使得5G网络运行异常，因此必须将数据库中的信息进行备份处理。最后，针对数据库角色、服务器角色、视图角色以及存储过程角色进行优化设置，切实提高数据库存储的安全性。由于网络系统可以为不同用户角色赋予不同的数据调用与访问权限，因此5G网络数据库的运行安全也能得到基本保障。

4.3 5G网络安全接入与传输控制

在5G网络安全接入与传输控制过程中，必须在原有网络传输协议的基础上，按照不同的网络风险等级选择不同的网络传输协议。通常情况下，网络传输协议以TCP/IP协议为主，一旦发生网络安全风险，就使用IPSec协议，以此为IP网络通信提供公开透明的安全服务，从源头上避免TCP/IP通信受到网络窃取和攻击，极大地提高了网络传输协议的安全性。若网络安全风险等级较高，那么则需要使用SCPS-SP协议，从而在协议约束下保护数据隐私，以最小的通信成本提高空间通信数据的安全性与保密性，同时保证空间数据安全传输认证的多元化。

5 结语

随着互联网技术的快速发展，黑客攻击、病毒、远程控制、数据盗窃等新型入侵技术也随之应运而生，以人工智能为基础的5G网络安全管理技术则可以有效应对这种恶意攻击，同时降低网络安全事件对用户及网络环境造成的消极影响，进一步推动5G网络的拓展与安全运行。基于此，在未来发展阶段，必须加大基于人工智能的5G网络安全管理技术的研究力度，充分利用先进的技术手段保障5G网络运行的安全性与稳定性。

参考文献

[1] 熊祖雄 . 简析大数据背景下信息通信网络安全管理策略 [J]. 网络安全技术与应用 ,2021(3):125–127.

[2] 乔宏明 , 梁奂 , 姚文胜 , 等 . 面向 5G 网络的 DevOps 安全管理探讨 [J]. 移动通信 ,2019,43(10):53–57.

[3] 赵悦 , 马俊达 , 李翀 .5G 通信网络中的安全布局分析 [J]. 电信工程技术与标准化 ,2019,32(5):70–73.

[4] 高严军 .5G 无线通信系统网络安全问题的分析与探究 [J]. 百科论坛电子杂志 ,2021(7):73.

[5] 郭海丽 . 基于人工智能的 5G 网络安全管理技术研究 [J]. 长江信息通信 ,2020(12):260–262.