5G通信时代计算机网络信息安全问题探究

丘先文
中国电信股份有限公司南宁分公司　广西　南宁　530022

摘　要：5G通信时代的到来，为计算机网络信息传输带来前所未有的速度与效率，但同时也伴随着复杂多变的信息安全挑战。本文深入探究5G通信技术在应用过程中面临的网络安全问题，包括技术不成熟性、安全防护技术滞后、人为因素等，并分析这些问题对网络安全防护的影响。通过综合考量，本文旨在为构建更加安全、可靠的5G通信网络提供理论支持与实践指导，促进5G技术的健康有序发展。

关键词：5G；通信时代；计算机；网络信息；安全问题

引言：随着5G通信技术的迅猛发展，人类社会正步入一个全新的数字时代。5G技术以其高速率、低时延、大连接等特性，为计算机网络信息传输带来了革命性的变革，技术的飞跃也伴随着新的安全风险与挑战。5G通信网络信息安全问题日益凸显，成为制约5G技术广泛应用与可持续发展的关键因素。因此深入探究5G通信时代计算机网络信息安全问题，提出有效的防护策略，对于保障网络安全、促进数字经济发展具有重要意义。

1 5G 通信技术概述

5G，即第五代移动通信技术，是移动通信技术发展的最新里程碑。相较于前代技术，5G以其高速率、低时延、大连接和低功耗等显著特点，引领着通信技术的革新。在数据传输速率上，5G技术实现了质的飞跃，最高可达10Gbps，是4G技术的几十倍，为用户带来前所未有的流畅体验。5G的时延降低至毫秒级别，仅为4G的几十分之一，极大地提升了实时通信的效率和可靠性，为智能制造、智能交通等领域提供了强有力的支持。5G技术还具备强大的连接能力，能够支持数百万个设备同时在线，为物联网的广泛应用奠定了坚实基础。智能家居、无人机、自动驾驶汽车等设备在5G的赋能下，将实现更高效、更智能的互联互通[1]。从应用领域来看，5G技术已经渗透到工业、医疗、交通、智慧城市等多个领域，推动了各行各业的数字化转型。在智能制造领域，5G技术助力实现生产线的智能化和自动化；在医疗领域，5G支持远程手术和实时健康监测，为患者提供更加便捷和高效的医疗服务；在智慧城市领域，5G技术则支持各种物联网设备和传感器的连接，实现城市内部各个领域的数字化和智能化。

2 5G 通信时代计算机网络信息存在的安全风险

2.1 通信安全风险

在5G通信时代，通信安全面临着前所未有的挑战，5G网络架构的复杂性是其通信安全风险的重要来源。5G引入了网络切片、边缘计算、软件定义网络（SDN）和云计算等新技术，这些技术虽然增强网络的灵活性和可扩展性，但也使得网络结构更加复杂，增加被攻击的风险。5G网络采用开放的架构，支持多种接入技术和应用，这使得网络更容易受到来自不同渠道的攻击。攻击者可能利用无线接口暴露、无线信号干扰或物理层攻击等手段，对5G网络进行破坏。特别是毫米波和大规模MIMO（Multiple Input Multiple Output）技术，虽然提高了数据传输速率和容量，但也带来了新的安全挑战。毫米波信号容易被拦截，而MIMO技术则容易受到射频攻击，这些都增加了通信过程中的不确定性和风险。5G网络的高速率和低时延特性也为攻击者提供了更多便利。攻击者可以更快地发动攻击、传播恶意代码，并收集和分析数据，从而进行更精准、更有效的攻击。例如，中间人攻击、拒绝服务攻击（DDoS）和重放攻击等，在5G环境下都可能造成更大的破坏。

2.2 数据安全风险

在5G通信时代，数据安全风险同样不容忽视。随着5G技术的广泛应用，大量数据在网络中传输，这些数据可能包含个人隐私、商业机密乃至国家安全等敏感信息，5G网络中的数据安全漏洞却为攻击者提供了可乘之机。一方面，5G网络中的网络设备种类繁多，连接紧密，攻击面扩大。攻击者可能通过利用设备中的漏洞，或通过网络协议中的缺陷，窃取或篡改传输中的数据。另一方面，5G网络支持跨网漫游和物联网应用，这也增加了数据泄露的风险。用户在不同网络之间无缝切换时，可能面临中间人攻击的风险；而物联网设备通常安全防护措施薄弱，容易成为攻击者的目标。一旦这些设备被控制，攻击者就可以通过它们窃取或篡改数据，造成严重后果。云计算和大数据等新技术在5G网络中的

广泛应用也带来了新的数据安全挑战，云计算环境中的数据安全问题、大数据环境中的隐私泄露问题等都可能成为数据安全的隐患。特别是在数据共享和交换的过程中，如果安全措施不到位，就可能导致数据被非法获取或滥用。

2.3 隐私安全风险

在5G通信时代，隐私安全风险日益凸显。5G网络中的认证和密钥协议（如AKA）虽然用于保证通信双方的身份验证和密钥协商，但仍存在潜在的隐私泄露问题。例如，用户的位置信息等敏感数据可能在认证过程中被暴露给第三方，攻击者还可能通过伪造或篡改认证消息来窃取用户的身份信息和会话密钥，从而进一步侵犯用户的隐私。物联网设备的广泛应用也增加了隐私泄露的风险，物联网设备通常与用户的日常生活紧密相连，如智能家居、可穿戴设备等。这些设备在收集用户数据的同时，也可能成为隐私泄露的源头。如果设备的安全防护措施不到位或存在漏洞，攻击者就可能通过控制这些设备来窃取用户的隐私信息[2]。随着5G技术的不断发展，网络攻击手段也在不断升级，攻击者可能利用5G网络中的漏洞和弱点，进行各种非法活动，如钓鱼攻击、恶意软件攻击和网络钓鱼攻击等。这些攻击手段不仅可能窃取用户的隐私信息，还可能对用户造成财产损失和心理伤害。

3 5G 通信时代计算机网络信息安全问题的原因分析

3.1 5G通信技术的不成熟性

5G通信技术作为一项新兴技术，尽管在多个方面展现出了巨大的潜力与优势，但其本身仍处于不断发展和完善的过程中，存在一定程度的不成熟性。5G网络架构的复杂性和新技术的引入增加系统的脆弱性，网络切片、边缘计算、软件定义网络等新技术虽然提升网络的灵活性和可扩展性，但同时也带来更多的潜在安全风险。这些新技术的安全性和稳定性尚未经过充分验证，容易成为攻击者利用的目标。5G网络的高速率和低时延特性对安全防护提出了更高的要求，传统的安全防护手段可能难以适应5G网络的高速传输和实时性要求，导致安全防护效果大打折扣，5G网络中的新协议和新标准也可能存在未知的安全漏洞，为攻击者提供了可乘之机。5G技术的快速发展和迭代也加剧了安全问题的复杂性，随着技术的不断演进，新的安全威胁和漏洞层出不穷，而安全防护技术往往难以跟上技术发展的步伐，导致安全漏洞得不到及时修复和弥补。

3.2 安全防护技术的滞后

在5G通信时代，安全防护技术的滞后是导致计算机网络信息安全问题的另一个重要原因。现有的安全防护技术可能无法完全适应5G网络的特点和需求，例如，传统的防火墙、入侵检测系统等安全设备在处理高速、低时延的5G网络流量时可能存在性能瓶颈和漏报误报等问题，这些安全设备可能无法有效识别和防范针对5G网络的新型攻击手段。安全防护技术的更新和升级速度可能无法跟上5G技术的发展步伐，随着5G技术的不断演进和新威胁的不断出现，安全防护技术需要不断更新和完善以应对新的挑战，由于技术更新周期较长、研发投入不足等原因，安全防护技术的更新速度往往滞后于5G技术的发展速度。安全防护技术的普及和应用程度也存在差异，一些企业和组织可能由于技术实力、资金投入等原因无法及时采用先进的安全防护技术，导致网络安全防护水平参差不齐、整体防护能力较弱。

3.3 人为因素的影响

在5G通信时代，人为因素也是导致计算机网络信息安全问题不可忽视的原因之一，安全意识不足是许多企业和组织面临的普遍问题，一些用户和管理员可能缺乏对网络安全重要性的认识和理解，忽视了网络安全防护的重要性。他们可能随意泄露敏感信息、使用弱密码、不及时更新系统和软件等不安全行为，为攻击者提供了可乘之机。操作失误也是导致安全问题的常见原因，在复杂的网络环境中进行操作时，用户和管理员可能会因为疏忽大意、操作不当等原因导致安全漏洞被暴露或利用。恶意攻击是人为因素中最为严重的威胁之一，一些不法分子可能出于经济利益、政治目的或其他原因对5G网络进行攻击和破坏。他们可能利用5G网络中的漏洞和弱点进行渗透、窃密、篡改等恶意行为，对网络系统的稳定性和安全性造成严重威胁，还有一些黑客可能出于竞争或破坏心理对网络进行攻击和破坏活动[3]。

4 5G 通信时代计算机网络信息安全的解决策略

4.1 加强技术研发与创新

面对5G通信时代复杂多变的网络环境，加强技术研发与创新是提升计算机网络信息安全的核心策略。应加大对5G网络核心技术的研发投入，包括网络架构、协议标准、加密算法等方面的研究，确保5G网络在设计之初就具备较高的安全性。针对5G网络中可能出现的新型攻击手段和安全漏洞，应提前进行技术预研和风险评估，制定相应的应对措施。针对5G网络高速、低时延的特性，研发适应性强、性能优越的安全防护设备和软件，如高性能防火墙、智能入侵检测系统、数据加密传输技术等。加强对人工智能、大数据等先进技术的应用研究，提升安全防护的智能化和自动化水平，实现对潜在

威胁的及时预警和快速响应。

还应加强国际合作与交流，共同应对跨国网络攻击和犯罪活动。通过参与国际标准制定、技术共享和联合演练等方式，提升全球范围内的5G网络信息安全防护能力。

4.2 强化用户安全意识教育

用户是网络安全的第一道防线，因此强化用户安全意识教育是提升5G通信网络信息安全的重要途径，应通过多种渠道和形式普及网络安全知识，提高用户对网络安全重要性的认识和理解。加强对用户的安全技能培训，针对不同类型的用户群体（如企业员工、学生、普通网民等），制定针对性的安全技能培训计划，教授用户如何识别网络钓鱼、恶意软件等常见网络威胁，以及如何保护个人信息和隐私安全，鼓励用户定期更新密码、安装安全软件、不随意点击不明链接等，提高自我保护能力。还应建立健全用户举报和奖励机制，鼓励用户积极举报发现的网络安全问题和漏洞，对提供有价值线索的用户给予一定的奖励和表彰，形成全社会共同参与网络安全防护的良好氛围。

4.3 完善法律法规与监管机制

完善的法律法规和有效的监管机制是保障5G通信网络信息安全的重要保障。应加快制定和完善与5G网络信息安全相关的法律法规体系，明确网络运营者、用户、服务提供商等各方的权利和义务，规范网络行为和信息处理流程，加大对违法行为的惩处力度，提高违法成本，形成对潜在犯罪分子的有效震慑。加强对5G网络运营者、服务提供商等关键环节的监管力度，定期开展网络安全检查和评估工作，及时发现和整改安全隐患，建立跨部门、跨行业的协同监管机制，实现信息共享和联合执法，提高监管效率和效果。还应加强对网络犯罪行为的打击力度，加强与公安、司法等部门的合作与联动，建立快速反应机制，对发现的网络犯罪案件进行及时查处和打击。

4.4 建立协同安全防护体系

在5G通信时代，建立协同安全防护体系是提升计算机网络信息安全的重要措施。首先，加强政企合作与协同。政府应加强与网络运营者、服务提供商等企业的沟通与协作，共同制定安全防护策略和标准规范，推动安全防护技术的研发与应用。鼓励企业之间加强合作与交流，共享安全威胁情报和防护经验，提升行业整体安全防护水平[4]。其次，加强技术协同与融合，推动不同领域、不同行业之间的技术协同与融合，形成优势互补、资源共享的安全防护格局。例如，在工业互联网领域加强5G技术与工业控制系统的融合应用，提升工业生产过程的安全性和稳定性；在智慧城市领域加强5G技术与物联网技术的融合应用，提升城市管理和服务的智能化水平等。最后，加强社会协同与参与，鼓励社会各界共同参与网络安全防护工作，形成全社会共同关注、共同参与的良好氛围。例如，通过举办网络安全宣传周、网络安全技能大赛等活动提高公众的网络安全意识和技能水平；通过设立网络安全奖励基金等方式激励社会各界积极投身网络安全事业等。

结束语

5G通信时代计算机网络信息安全问题的探究，不仅关乎技术发展的稳定与安全，更直接影响到社会经济的正常运行与民众生活的安宁。面对挑战，应持续加强技术研发与创新，强化用户安全意识教育，完善法律法规与监管机制，并构建协同安全防护体系。只有这样，才能充分利用5G技术带来的便利与优势，共同守护一个更加安全、可信的数字世界。

参考文献

[1]赵永杰. 5G通信时代计算机网络信息安全问题探究[J]. 电子通信与计算机科学,2024,6(6). DOI:10.37155/2717-5170-0606-49.

[2]旷晖. 5G通信时代计算机网络信息安全问题探究[J]. 电脑与电信,2020(8):33-35.

[3]刘楝,孟宪民,李阳.5G安全及网络监管问题探析[J].国防科技.2020,(3).DOI:10.13943/j.issn1671-4547.2020.03.15 .

[4]郭邵钧.探析5G信息安全风险管理与应对措施[J].电脑编程技巧与维护.2021,(5).DOI:10.3969/j.issn.1006-4052.2021.05.066 .