5G通信时代计算机网络信息安全问题探究

赵永杰
石家庄市轨道交通集团有限责任公司运营分公司　河北　石家庄　050000

摘　要：5G通信时代计算机网络信息安全问题备受关注。本文针对5G网络所带来的新挑战，探讨了其相关信息安全问题。5G的高速率和大容量带来更大的数据传输量，同时也增加数据泄露害的风险。5G网络的边缘计算和物联网的大规模连接，为黑客入侵提供了更多入口。5G网络无处不在，复杂的网络结构和多样的终端设备使得网络管理和监管更加困难。必须重视并积极应对5G通信时代计算机网络信息安全问题，加强网络安全防护，保障网络安全。

关键词：5G通信；计算机网络；问题探究

1 5G 通信技术概述

5G（第五代移动通信技术）是指第五代移动通信技术，是继4G之后的下一代无线网络技术。相较于前几代移动通信技术，5G具有更高的数据传输速度、更低的延迟、更大的容量和更广泛的连接性。5G技术的最显著特点是极高的传输速度，通过使用更高频段、更大带宽和更先进的多天线技术，5G网络可以实现更快的数据传输速度，让用户在手机上进行高清视频播放、云存储、实时游戏等多种应用时，体验到更加流畅和更加快速的网络连接。5G技术带来了更低的网络延迟，5G网络的响应时间极短，使得物联网、自动驾驶、远程医疗等对时延敏感的应用能够得到更好的支持。这种低延迟的特性也为虚拟现实、增强现实等新兴应用提供了更好的用户体验。5G技术还具有更大的容量和更广泛的连接性，通过使用更多的小基站、网络虚拟化技术和大规模MIMO技术，5G网络可以承载更多的设备连接，并在高密度设备的环境下实现更可靠的通信服务，为城市智能化、工业生产等大规模连接场景提供支持[1]。5G技术还涉及到网络切片、人工智能、边缘计算等领域的深度融合，为用户提供更为个性化和智能化的网络服务。同时，5G技术的发展也需要跨国合作、标准制定和政策支持，以实现全球范围内的5G网络覆盖与应用。

2 5G 通信网络的优势

5G通信网络作为第五代移动通信技术，在与之前的4G网络相比较时，具有许多显著的优势，这些优势将为用户和产业带来更先进、更高效的通信体验：首先，最突出的优势是更高的传输速度，5G网络的更高频段和更大带宽使其具备比4G更快的数据传输速率。这意味着用户可以更快地下载和上传数据，观看高清视频、进行实时视频通话和进行大型文件传输等内容时，能够更加流畅、无卡顿地进行操作。其次，5G网络具有更低的延迟，网络延迟是指数据在发送和接收之间的时间间隔，5G网络大大降低了这一延迟，让通信更加即时和快速。这对于一些对网络延迟要求严格的应用场景，比如自动驾驶汽车、工业自动化和远程医疗等领域，具有非常重要的意义。另外，5G网络还拥有更大的容量，通过使用更多的小基站、网络虚拟化和技术创新，5G网络能够承载更多的设备连接，同时保持稳定的网络质量。这意味着更多的设备可以同时连接到网络，支持大规模的物联网和智能设备的应用，进一步推动数字化转型和智能化发展。5G网络的广泛连接性也是其优势之一，5G支持更大规模、更高密度的设备连接，为人们提供更加便捷、更智能的生活方式。通过5G网络的广泛连接，城市智能化、智能交通、智能制造等领域的发展也将迎来更好的支持和推动。

3 5G 时代计算机网络信息安全问题

3.1 网络通信安全问题

随着5G时代的到来，计算机网络信息安全问题将变得更为严峻。网络通信安全是一个重要的议题，尤其在数字化时代，对于个人隐私和商业数据的保护至关重要。5G网络的更广泛连接性和更高速的传输会带来更多的网络攻击风险。犯罪分子可能利用5G网络的高速通信特性进行数据窃取、网络入侵和勒索活动，对用户造成隐私泄露和财产损失[2]。5G网络的低延迟和高容量也可能会增加网络的脆弱性，使网络更容易受到分布式拒绝服务（DDoS）攻击、勒索软件攻击等恶意行为的影响。这些攻击不仅会造成网络瘫痪和服务中断，还可能导致企业和用户遭受重大经济损失。5G网络中大规模部署的物联网设备也可能成为网络安全的隐患。由于许多物联网设备存在安全漏洞或默认密码，黑客可能利用这些弱点入侵设备、控制网络，甚至对整个网络进行攻击。5G网络中的网络切片技术，虽然能够根据不同的应用需求

提供定制化的网络服务，但也增加了网络和数据安全管理的复杂性。如果网络切片管理不当，可能导致数据泄露、信息混淆等问题，危害用户数据安全。

3.2 安全管理尚不到位

5G时代的计算机网络信息安全问题备受关注，因为虽然5G网络为我们提供了更高效、更便捷的通信服务，但与此同时也存在着许多潜在的安全风险。当前情况显示，尽管对于5G网络的信息安全已经有了初步的规划和安全标准制定，但安全管理在实际应用中尚未到位。许多用户和企业对于5G网络的安全意识不足，他们往往忽视安全更新、漏洞补丁等关键安全实践，容易成为网络攻击的目标。对于5G网络中新兴的安全威胁和攻击方式了解不足也是一个问题。5G网络中的物联网设备安全问题引人担忧，由于这些设备往往存在着设计缺陷、默认密码等安全隐患，黑客可能利用这些漏洞对设备进行攻击，从而威胁到整个网络的安全。由于5G网络的复杂性和高度自动化，安全管理面临着更多挑战，网络切片技术的复杂性意味着需要对网络进行更加精细的安全管理，而一旦管理不当，可能导致数据泄露、网络入侵等问题。5G网络的高速传输与低延迟特性让网络安全问题变得更为危急，网络攻击往往能够快速广泛地传播，造成更大的损失。同时，随着量子计算、人工智能等新技术的发展，网络安全防护也需加速创新。

3.3 数据安全问题

5G时代的计算机网络信息安全问题中，数据安全问题日益凸显。5G网络的快速传输和低延迟性质使得海量数据更加流畅地传输，但同时也给数据安全带来了新的挑战。数据在传输过程中容易受到窃取和篡改的威胁，由于5G网络传输速度快，黑客有更多的机会在数据传输过程中截取敏感信息，例如个人隐私、商业机密等，进而滥用或者泄露这些数据，对用户和组织造成不可挽回的损失。5G网络中广泛部署的物联网设备增加了数据泄露的风险，这些设备通常携带大量敏感信息，例如家庭生活习惯、健康数据等，如果设备的安全性得不到保障，可能会被黑客利用，严重威胁用户隐私和数据安全[3]。由于5G网络的高容量和低延迟，用户数据存储容易分散在不同地理位置和云端服务器上，这也为数据管理与保护带来了挑战。数据的分散存储可能使得数据管理和权限控制变得更加复杂，导致数据泄露隐患。5G网络中的网络切片技术也对数据安全提出了挑战，虽然网络切片能够为不同应用提供个性化的服务，但一旦网络切片管理不当，可能导致不同切片的数据混淆，甚至是数据泄露。

4 5G 通信时代计算机网络信息安全的防护措施

4.1 加强对加密技术的应用

在5G通信时代，计算机网络信息安全的重要性日益凸显，为了有效保护数据安全，加强对加密技术的应用是至关重要的防护措施之一。加密技术可以有效地加固数据传输的安全性，防止数据在传输和存储过程中被窃取或篡改。对于5G通信时代的网络通信安全，应加强对端到端的数据加密保护，通过使用强大的加密算法，确保数据在传输过程中得到有效加密，即使黑客截取到数据包，也无法窃取其中的敏感信息。这种端到端的数据加密可以防止中间人攻击和数据泄霎的风险。对于物联网设备的数据安全保护，引入端点加密技术是一项关键措施，通过在物联网设备上部署加密模块，对设备产生的数据进行加密处理，加强对设备数据的保护。这可以有效防止黑客通过物联网设备入侵网络和窃取数据。加强对数据库和云端数据的加密保护也是关键举措，对于存储在云端或数据中心的敏感信息，采用加密技术进行数据加密，防止黑客通过恶意手段获取数据。定期进行数据库加密密钥的更换和管理，确保数据长期安全存储。加密技术的应用还需要与访问控制、身份验证等安全机制相结合，建立多层次的安全防护体系。通过合理配置访问权限、强化用户身份验证手段，加强对数据的访问管控，确保只有授权用户能够访问和使用数据，从而提高数据安全性[4]。

4.2 全方位强化网络监督管理

在5G通信时代，为强化计算机网络信息安全保护，全方位加强网络监督管理显得尤为关键。建立完善的网络监测系统是保障网络安全的前提。通过实时监测网络流量、行为模式和异常事件，及时发现网络攻击行为，并采取相应的防护措施，防止网络安全事件扩大。加强对网络设备和系统的安全管理，定期对网络设备进行漏洞扫描和安全漏洞修补，强化设备访问控制和权限配置，避免设备被黑客攻陷。加强系统安全性配置，设置强密码、定期更新安全补丁，防止系统入侵和数据泄霜。强化对网络数据的安全管理和监控，建立数据分类和加密管理机制，对不同重要性的数据进行不同级别的保护，并合理使用加密技术保护数据的传输和存储过程。建立数据访问审计和监测机制，对数据访问行为进行记录和分析，发现异常使用行为。加强员工网络安全意识培训，定期开展网络安全培训，强调网络安全政策和规范，提醒员工注意网络安全风险，教育员工如何防范网络攻击、如何识别网络钓鱼邮件等常见网络安全问题。员工的网络安全意识提升，对整体网络安全具有积

极影响。建立健全的网络安全法律法规和政策体系，完善相关法规，规范网络安全管理和处罚机制，保障网络安全法治化。加强对网络安全事件的溯源追踪和应急响应处理，及时处理网络安全威胁，降低网络安全事件对网络的影响。

4.3 加快5G安全数据防护系统的升级

在5G通信时代，加快升级5G安全数据防护系统是至关重要的一项信息安全防护措施。需要及时更新安全数据防护系统，确保系统能够随着网络威胁的不断演变而保持有效性。通过不断升级系统软件和安全模块，及时修复已知漏洞和弱点，提升系统的抗攻击能力和安全性。加快部署并优化安全数据分析技术，引入先进的数据分析技术，实现对大规模数据的实时监测和分析，检测网络异常流量和行为，以便及时发现潜在的安全威胁。通过快速准确地识别安全事件和攻击，及时采取应对措施，降低网络风险[5]。加强网络安全协同防护机制的建设，建立网络安全协同联动机制，促进不同系统和设备之间的信息共享和协同作战，加强网络攻击事件的跨系统协同防御，提高整个网络的安全性。加强行业间的信息共享和合作，形成安全生态圈，共同应对网络安全挑战。加快推进5G网络中端到端加密技术的部署，通过实现端到端的数据加密传输，保障数据在传输过程中的机密性和完整性，有效防范中间人攻击和数据泄露风险。加强对加密技术的研发和应用，完善加密标准和协议，保障5G通信数据的安全性。

4.4 加强5G时代计算机网络信息安全培训

在5G通信时代，为加强计算机网络信息安全的防护措施，加强对5G时代计算机网络信息安全培训显得至关重要。组织网络安全培训，定期启动网络安全意识教育活动，提高员工和用户的网络安全意识。通过教育解释网络安全政策和规定，使员工能够辨识网络威胁和攻击手段，并使他们了解如何规避此类风险。加强网络技术人员的专业培训和认证，提高其对网络安全技术的熟悉程度和实践经验。培训网络管理员和技术人员熟练掌握最新的网络安全技术和方法，保证他们对网络系统、设备和数据的安全性有清晰的了解和有效的保护。定期进行模拟网络安全演练和实战训练，增强员工在面对实际网络安全威胁时的应急反应能力。通过模拟网络攻击事件，检测员工应对网络安全威胁的表现，并针对性地提供针对性的培训和指导，提高网络安全应急响应速度和准确性。加强网络用户的网络安全教育和培训，让用户掌握网络安全知识、措施和技术。

结束语

在5G通信时代，计算机网络信息安全问题将面临更为严峻的挑战。随着5G技术的广泛应用，网络攻击手段也将日益翻新，数据泄露和网络威胁的风险愈发增加。为确保网络通信的安全和稳定，必须加强对5G时代网络安全问题的探究和应对。这需要全社会的共同努力，包括政府、企业、学术界和个人，共同推动网络安全技术的发展和应用，加强网络安全意识教育，强化安全管理机制和监管体系。只有通过合作与努力，才能有效应对5G通信时代的网络安全挑战，实现网络信息安全和数字化社会的可持续发展。

参考文献

[1]刘棟.孟宪民.李阳.5G安全及网络监管问题探析[J].国防科技.2020(03):76-79+85.

[2]覃德泽.李立信.李立礼.5G背景下高校信息安全风险分析及防范策略[J].网络安全技术与应用.2020(08):93-94.

[3]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(08):33-35.

[4]陈云杰.游伟.5G移动通信中基于安全信任的网络切片部署策略研究[J].通信技术.2020.53(9):2206-2209.

[5]朱君.胡淼.网络时代视角下网络通信安全问题的内外部原因及防范手段[J].现代工业经济和信息化.2022.12(01):121-122.