物联网背景下计算机网络安全技术分析

李雍冰
新疆天山职业技术大学　新疆　乌鲁木齐　830017

摘　要：本文深入探讨了物联网技术背景下的计算机网络安全技术。物联网作为21世纪信息技术的重大创新，正逐步改变着我们的生活和生产方式。首先概述了物联网技术的三个核心层面及其广泛应用。详细分析了计算机网络安全技术的四大关键领域：身份认证与访问控制、数据加密与安全传输、安全漏洞监测与修复以及网络安全防御技术。还指出了物联网背景下计算机网络面临的三大挑战，包括大规模连接带来的安全挑战、设备多样性与安全漏洞以及数据隐私与保护问题。最后文章提出针对性的应对策略，旨在构建更加安全的物联网生态系统。

关键词：物联网；下计算机网络；安全技术

1 物联网技术概述

物联网技术，作为21世纪信息技术的重大创新之一，正逐步渗透并改变着我们的生活和生产方式。其核心在于将各类物理设备、传感器、智能系统等通过互联网连接起来，实现设备间的信息交换与协同工作，从而构建一个智能化、互联互通的物理世界。物联网技术的基础在于感知层、网络层和应用层三个层面的紧密协作。感知层通过各类传感器、RFID标签、摄像头等设备，实时采集和识别物体的状态信息；网络层则利用无线传感器网络、移动通信网络等通信技术，将感知层获取的信息进行传输和汇聚；应用层则是对汇聚的信息进行智能化处理，为用户提供丰富多样的服务，如智能家居控制、环境监测、工业自动化等。物联网技术的应用领域极为广泛，几乎涵盖了社会的方方面面。在智能家居领域，物联网技术让家中的各类电器设备实现互联互通，用户可以通过手机等智能终端远程控制家电的开关、调节温度等，极大地提升生活的便捷性。在工业领域，物联网技术则推动了智能制造的快速发展，实现生产设备的远程监控、故障预警和智能调度，提高了生产效率和质量。另外，物联网技术还在农业、交通、医疗等领域发挥着重要作用[1]。在农业领域，物联网技术可以实时监测土壤湿度、温度等环境参数，为精准灌溉和病虫害预警提供依据。在交通领域，物联网技术可以实现车辆的智能调度和交通流量的实时监控，提高道路通行效率。在医疗领域，物联网技术则可以实现远程医疗、健康监测等功能，为患者提供更加及时和便捷的医疗服务。

2 计算机网络安全技术分析

2.1 身份认证与访问控制技术

身份认证与访问控制技术是确保计算机网络安全的基石。身份认证技术通过验证用户的身份信息，确保只有合法的用户才能访问网络资源。这通常涉及用户名和密码的验证，以及更高级的生物特征识别（如指纹、面部识别）或硬件令牌的使用。访问控制技术则基于用户的身份和权限，决定其可以访问哪些资源和执行哪些操作。例如，基于角色的访问控制（RBAC）系统会根据用户的角色（如管理员、普通用户）来授予相应的权限。这些技术共同构成了网络安全的第一道防线，有效防止未经授权的访问和滥用。

2.2 数据加密与安全传输技术

数据加密与安全传输技术是保护数据在传输和存储过程中不被窃取或篡改的关键。数据加密技术通过将敏感数据转换为无法直接读取的乱码形式，确保即使数据被截获，也无法被未授权的第三方理解和利用。安全传输技术，如SSL/TLS协议，则在数据传输过程中提供加密保护，确保数据在客户端和服务器之间传输时保持机密性和完整性。数据备份和恢复策略也是确保数据安全的重要措施，以防数据丢失或损坏。

2.3 安全漏洞监测与修复技术

安全漏洞监测与修复技术是维护网络安全的不可或缺的一部分，它扮演着及时发现并应对网络威胁的重要角色。在数字化时代，系统和应用程序的复杂性日益增加，安全漏洞成为黑客和恶意用户入侵的潜在途径。安全漏洞扫描工具是这一过程中的关键工具。这些工具能够定期或根据特定需求对系统和应用程序进行全面的扫描，旨在揭示潜在的安全漏洞和弱点。这些扫描可能包括代码审查、配置检查以及网络通信分析等，以确保每一个可能被利用的漏洞都能被发现。当漏洞被扫描工具识别后，接下来的步骤是进行风险评估。风险评估旨在量化漏洞的潜在影响，包括漏洞被利用的可能性以及可能导致的后果。基于这些信息，组织可以决定漏洞的优

先级，即哪些漏洞需要立即修复，哪些可以稍后处理；修复过程通常涉及更新和补丁管理。更新是指替换存在漏洞的组件或代码，而补丁则是对现有系统或应用程序的局部修改，旨在消除已知的漏洞。组织和企业必须确保其系统和应用程序保持最新状态，并应用所有必要的补丁，以防止已知的漏洞被利用。

2.4 网络安全防御技术

网络安全防御技术旨在构建多层次的防御体系，以应对不断演化的网络威胁。这包括防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）等。防火墙作为第一道防御，根据预定义的规则过滤进出网络的数据包。IDS则能够实时监测网络活动，并检测可疑行为，如未经授权的访问或恶意软件的传播。IPS则更进一步，能够自动对检测到的威胁采取行动，如阻止攻击流量。网络安全防御技术还包括安全信息和事件管理（SIEM）、威胁情报共享以及定期的安全培训和意识提升等活动，以增强整个网络的安全态势感知和防御能力。

3 物联网背景下计算机网络安全面临的挑战

3.1 大规模连接带来的安全挑战

在物联网背景下，设备的大规模连接给计算机网络安全带来了前所未有的挑战。物联网网络通常包含大量的智能设备、传感器和控制系统，这些设备通过网络进行互联互通，形成一个庞大的生态系统。随着连接设备的数量激增，网络攻击面也随之扩大，使得恶意攻击者更容易找到并利用安全漏洞进行攻击。大规模连接还可能导致网络拥堵和性能下降，为黑客提供了利用网络拥堵进行DDoS攻击等恶意行为的机会。因此，如何确保物联网网络在大规模连接下的安全性和稳定性，是当前计算机网络安全领域面临的一大难题。

3.2 设备多样性与安全漏洞

物联网生态系统中的设备种类繁多，从智能家居设备到工业控制系统，从可穿戴设备到车载系统，各种设备的硬件、软件和通信协议各不相同。这种多样性使得统一的安全策略和标准难以实施，给黑客提供更多的攻击机会[2]。由于物联网设备通常具有较高的集成度和复杂性，其固件和软件可能存在安全漏洞，这些漏洞一旦被黑客利用，就可能对整个物联网网络造成严重的威胁。因此，如何针对物联网设备的多样性制定有效的安全措施，是保障物联网安全的关键所在。

3.3 数据隐私与保护问题

在物联网环境下，数据隐私和保护问题也日益凸显，物联网设备通过传感器和数据采集系统不断收集大量的个人和企业数据，这些数据通常包含敏感信息，如个人身份信息、位置信息、健康状况等。一旦这些数据被泄露或被恶意利用，将对个人隐私和企业安全构成严重威胁。由于物联网设备通常处于无人值守或远程管理的状态，数据的安全存储和传输也面临巨大挑战。因此，如何确保物联网数据在采集、传输、存储和处理过程中的安全性和隐私性，是当前计算机网络安全领域亟待解决的问题。

4 物联网背景下计算机网络安全技术的应对策略

随着物联网技术的迅速发展，其在计算机网络安全领域所带来的挑战也日益凸显。为了有效应对这些挑战，确保物联网环境下的网络和数据安全，必须采取一系列针对性的安全技术应对策略。

4.1 加强身份认证与访问控制

身份认证与访问控制是物联网环境下计算机网络安全的第一道防线。在物联网网络中，设备和用户数量众多，且通常具有不同的访问权限和功能需求。因此，加强身份认证与访问控制显得尤为重要。（1）建立完善的身份认证机制。传统的用户名和密码认证方式已无法满足物联网环境下的安全需求。为此，可以采用多因素认证技术，如结合生物特征识别（指纹、面部识别等）、硬件令牌等多种方式进行身份验证。这种多因素认证方式能够显著提高身份认证的安全性，有效防止未经授权的访问和恶意攻击[3]。（2）实施严格的访问控制策略。基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC）是两种常用的访问控制方法。在物联网环境下，可以根据设备和用户的角色、属性等信息，为其分配相应的访问权限。通过细粒度的权限控制，可以确保只有合法的设备和用户才能访问到特定的资源和数据。（3）加强对物联网设备的身份管理和密钥管理。物联网设备通常具有有限的计算能力和存储空间，因此需要采用轻量级的身份认证和密钥协商协议。同时，应定期对密钥进行更新和更换，以防止密钥泄露和过期使用所带来的安全风险。

4.2 优化数据加密与安全传输

数据加密与安全传输是保护物联网环境中数据机密性和完整性的关键措施。在物联网网络中，数据通常通过无线方式传输，这增加了数据被窃取或篡改的风险。因此，必须采用有效的数据加密和安全传输技术来确保数据的安全性。第一，采用先进的加密算法对数据进行加密。加密算法的选择应根据数据的敏感程度和计算资源的可用性进行综合考虑。对于高度敏感的数据，可以采用高强度的对称加密算法或非对称加密算法进行加密。同时，应定期对加密算法进行更新和升级，以应对

不断出现的新的安全威胁。第二，建立安全的数据传输通道。在物联网环境中，数据传输通常涉及多个设备和网络节点。为了确保数据在传输过程中的安全性，可以采用安全套接层（SSL/TLS）等安全协议来建立加密的数据传输通道。这些协议能够对传输的数据进行加密和完整性校验，从而确保数据在传输过程中不被窃取或篡改。第三，加强对物联网设备的数据存储管理。物联网设备通常具有有限的存储空间和计算能力，因此需要采用高效的数据存储和压缩技术来减少数据存储的开销。同时，应定期对存储的数据进行备份和恢复测试，以确保数据的可靠性和可用性。

4.3 提升安全漏洞监测与修复能力

安全漏洞监测与修复能力是确保物联网环境下计算机网络安全的重要保障。在物联网网络中，设备和系统的数量众多且分布广泛，这使得安全漏洞的监测和修复变得尤为困难。因此，必须采取有效的措施来提升安全漏洞监测与修复能力。通过定期扫描和分析物联网设备和系统的安全漏洞，及时发现并报告潜在的安全风险。建立漏洞信息共享机制，及时获取并分享漏洞信息，以便其他组织和机构能够及时采取措施进行防范和应对；物联网设备和系统通常具有较长的生命周期，因此需要定期对其进行更新和维护以确保其安全性。这包括更新操作系统、固件和应用程序等组件的最新版本，以及安装和更新安全补丁来修复已知的安全漏洞。通过及时更新和维护物联网设备和系统，可以有效降低安全风险并提高其防御能力；定期对物联网设备和系统进行安全审计和评估可以了解其安全性能和合规性情况，从而及时发现并解决潜在的安全问题[4]。同时，还可以根据审计和评估结果制定针对性的安全措施和策略来提高物联网设备和系统的安全性。

4.4 强化网络安全防御体系

在物联网网络中，由于设备和用户的多样性以及数据的敏感性等特点，使得网络安全防御变得更加复杂和困难。因此，必须采取有效的措施来强化网络安全防御体系。网络安全架构应基于分层防御和纵深防御的原则进行设计和实施。通过在网络的不同层次和区域部署相应的安全设备和系统（如防火墙、入侵检测系统、安全网关等），形成多层次、多层次的防御体系来抵御外部攻击和内部威胁；物联网设备和系统通常具有不同的安全性能和配置要求。根据其特点和需求采取相应的安全防护措施来确保其安全性。例如，对于智能家居设备可以采用基于网络的安全隔离技术来防止外部攻击者入侵；对于工业控制系统可以采用基于主机的入侵检测和防护技术来及时发现并应对安全威胁；通过实时监控和分析物联网网络和数据的行为和状态可以发现潜在的安全风险和异常情况。同时，还可以根据监控结果制定相应的安全措施和策略来提高物联网网络和数据的安全性。例如，可以建立基于大数据分析的安全威胁感知和预警系统来及时发现并应对潜在的安全威胁；可以建立基于云计算的弹性安全服务来提供灵活可扩展的安全防护措施等。

结束语

综上所述，物联网技术正以前所未有的速度改变着我们的生活和工作方式，但同时也给计算机网络安全带来了新的挑战。为了应对这些挑战，我们必须不断创新和完善计算机网络安全技术，加强身份认证与访问控制，优化数据加密与安全传输，提升安全漏洞监测与修复能力，以及强化网络安全防御体系。只有这样，才能确保物联网环境下的网络和数据安全，为社会的可持续发展提供坚实的技术保障。未来，随着物联网技术的进一步发展，计算机网络安全技术也将迎来更多的创新和突破。

参考文献

[1]金超.物联网计算机网络安全及其远程控制技术分析[J].电子技术与软件工程,2023(06):25-28.

[2]罗振营.基于物联网的计算机网络安全分析[J].信息记录材料,2022,23(08):17-19.

[3]郭娇娇.物联网背景下计算机网络安全技术研究[J].电子技术与软件工程,2022(11):30-33.

[4]张蒙恩,郭萌萌.基于物联网的计算机网络安全分析[J].电脑知识与技术,2021,17(07):34-35.