物联网背景下计算机网络安全技术分析

陆　阳
苏州城市学院　江苏　苏州　215104

摘　要：物联网背景下，计算机网络安全技术的重要性愈发凸显。面对数据保护难题、设备安全隐患、网络协议缺陷及大数据安全风险，深入剖析防火墙、加密认证、入侵检测与防御、网络监测预警及隐私保护等核心安全技术。这些技术共同构建了多层次的防护体系，旨在全面防御外部侵扰与内部漏洞，确保物联网系统的平稳运行与数据安全。通过综合运用这些技术手段，我们能够更加有效地保护物联网生态环境，推动其健康发展。

关键词：物联网；计算机网络；安全技术

1 物联网背景下计算机网络安全技术的重要性

在物联网时代背景下，计算机网络安全技术的重要性愈发凸显。物联网技术的飞速发展，将各类智能设备、传感器、控制系统等紧密相连，形成一个庞大的网络生态系统。这一变革极大地提升生产效率、优化生活体验，但同时也带来前所未有的网络安全挑战。计算机网络安全技术成为保护这一庞大网络免受外部威胁和内部漏洞侵害的关键屏障。它不仅能够确保数据的机密性、完整性和可用性，防止敏感信息泄露、篡改或丢失，还能有效抵御黑客攻击、病毒入侵等安全威胁，保障物联网系统的稳定运行。随着物联网设备数量的激增和应用场景的日益丰富，网络攻击面也随之扩大。一旦关键设备或系统被攻破，可能会引发连锁反应，影响到整个物联网生态的安全[1]。因此，加强计算机网络安全技术的研发与应用，构建全方位、多层次的防护体系，对于维护物联网安全、促进物联网产业的健康发展具有重要意义。

2 物联网面临的主要安全威胁

2.1 数据保护问题

在物联网（IoT）的广泛应用中，数据保护问题是最为紧迫且复杂的挑战之一。物联网设备通常产生并传输大量敏感数据，包括但不限于个人身份信息、位置信息、生活习惯乃至企业运营数据等。这些数据一旦泄露或被非法利用，将对个人隐私、企业商业机密乃至国家安全构成严重威胁。第一，物联网设备的分散性和多样性增加了数据保护的难度。相较于传统的计算机系统，物联网网络中的设备种类繁多，包括智能手机、智能家居设备、工业传感器等，它们的数据处理和存储能力参差不齐，安全防护水平也各不相同。这种异构性使得统一的数据保护策略难以实施，容易形成安全漏洞。第二，数据传输过程中的安全性难以保证。物联网设备往往需要与云端服务器或其他设备进行远程通信，数据传输过程中可能遭遇中间人攻击、数据截获、篡改等风险。尤其是在使用公共网络时，缺乏有效加密措施的数据包很容易被黑客窃取。第三，数据存储环节也面临诸多挑战。随着物联网数据的爆炸式增长，如何安全、高效地存储这些数据成为一大难题。一些物联网设备由于资源有限，可能无法本地存储大量数据，必须依赖云端或其他远程服务器。然而，云服务商的安全保障能力、数据访问控制机制等都会影响数据存储的安全性。若云端服务器遭受攻击或内部人员违规操作，都将导致数据泄露的风险增加。

2.2 设备安全问题

物联网设备作为物联网系统的基本组成单元，其安全性直接关系到整个系统的稳定运行和数据安全。由于物联网设备种类繁多、应用场景广泛，很多设备在设计和生产过程中并未充分考虑安全因素。例如，一些智能家居设备为了降低成本和简化操作，往往简化了安全验证流程或采用了较弱的加密算法。这些设备一旦接入物联网网络，就可能成为黑客攻击的目标。与传统的计算机系统不同，物联网设备的固件更新通常需要用户手动操作，且更新流程复杂、耗时较长。很多用户由于不了解或忽视更新提示，导致设备长期存在已知的安全漏洞。另外，一些物联网设备的厂商在设备发布后就不再提供固件更新服务，这使得设备的安全性无法得到持续保障。一些物联网设备需要部署在户外或无人值守的环境中，容易受到物理破坏或恶意篡改[2]。例如，工业控制系统中的传感器和控制器若被非法更换或破坏，可能导致整个生产流程中断或失控。

2.3 网络安全协议问题

当前物联网在网络安全协议方面存在诸多问题，严重威胁着物联网系统的安全稳定运行。不同的物联网设

备可能采用不同的通信协议进行数据交换，这些协议在安全性方面往往存在差异。一些老旧的或非主流的协议可能存在安全漏洞或未实现必要的安全机制，容易被黑客利用进行攻击。网络安全协议的实现可能存在缺陷；即使选择安全性较高的通信协议，但在具体实现过程中也可能因为设计不当、编码错误等原因导致安全漏洞的产生。例如，协议中的加密算法可能存在已知的安全隐患、身份认证机制可能不够严密等。在解决协议兼容性的过程中，可能会牺牲部分安全性以确保互操作性，这为黑客提供了可乘之机。例如，某些设备可能为了与老旧系统兼容，不得不使用不再受支持或已知存在漏洞的协议版本。

2.4 大数据安全隐患

物联网的广泛应用产生海量的数据，这些数据对于分析用户行为、优化系统性能、支持决策制定等方面具有重要价值。大数据的集中处理和存储也带来诸多安全隐患。物联网系统往往需要将收集到的数据传输到云端或数据中心进行集中处理和分析。然而，这些数据中心可能成为黑客攻击的重点目标。一旦数据中心被攻破，大量敏感数据将面临泄露的风险。物联网数据往往包含个人隐私信息，如个人位置、生活习惯、健康状况等。在数据处理和分析过程中，如何保护个人隐私成为一大挑战。不当的数据使用和共享可能导致个人隐私泄露，引发严重的社会问题[3]。物联网数据具有异构性、动态性和海量性等特点，这使得传统的安全管理和防护手段难以适应。如何有效地对数据进行分类、标记和监控，以及如何构建高效的数据安全防护体系成为亟待解决的问题。

3 物联网背景下计算机网络安全技术分析

3.1 防火墙技术

在物联网环境中，防火墙技术作为网络安全的第一道防线，其重要性不言而喻。物联网设备的多样性和大量连接特性使得网络边界模糊，传统的防火墙技术需要进行适应性改进以满足新的安全需求。现代防火墙不仅具备数据包过滤功能，还融合了状态检测、应用层过滤、入侵防御等高级功能，形成了更为强大的综合防护体系。在物联网系统中，防火墙被部署在网络入口点，对进出流量进行精细控制，确保只有经过授权和验证的流量才能穿越边界。随着云技术的兴起，云防火墙作为一种新的解决方案，通过虚拟化技术实现灵活部署和扩展，为物联网系统提供更加便捷和高效的安全防护。物联网防火墙的设计还需要考虑设备的资源限制和通信协议的多样性；为了减少对设备性能的影响，防火墙通常采用轻量级架构和优化算法，确保高效运行。支持多种通信协议和接口标准，以确保与不同品牌和型号的物联网设备兼容；智能学习和自适应能力是现代防火墙的重要特征之一，通过分析网络流量模式和用户行为，自动调整安全策略和规则，提高防护的准确性和实时性。

3.2 加密与认证技术

由于物联网设备经常跨越不同的网络域和地理位置，数据在传输过程中极易受到监听和篡改。因此，采用加密技术对敏感数据进行加密处理，确保数据传输的机密性和完整性，是防止数据泄露的重要手段。认证技术用于验证设备身份和授权访问，确保只有合法的设备才能接入网络并交换数据。在加密方面，物联网系统通常采用对称加密和非对称加密相结合的方式。对称加密速度快，适用于大量数据传输场景；非对称加密则安全性高，适用于密钥交换和数字签名等场景。为了满足物联网设备的资源限制，轻量级加密算法如AES-GCM等得到广泛应用。在认证方面，基于公钥基础设施（PKI）的数字证书和密钥管理机制成为主流，通过数字证书验证设备身份，实现设备间的互信。随着物联网设备的智能化和网联化趋势加强，生物特征识别、多因素认证等新技术也逐渐被引入物联网安全领域。这些技术通过结合多种验证方式，提高认证的复杂度和安全性，进一步增强物联网系统的防护能力[4]。

3.3 入侵检测与防御技术

在物联网的广阔天地中，入侵检测与防御技术犹如两道坚固的屏障，守护着每一个连接点的安全。入侵检测系统（IDS）扮演着侦探的角色，通过深度分析网络流量、系统日志和应用程序行为，及时发现并报告任何异常或可疑活动。这些系统利用模式匹配、统计分析、机器学习等先进技术，建立正常行为的基线模型，并对偏离基线的行为进行预警，从而有效抵御潜在的网络攻击。而入侵防御系统（IPS）则更进一步，它不仅检测威胁，还能自动采取措施阻止这些威胁。IPS部署在网络的关键路径上，对数据包进行深度检查和过滤，阻止恶意流量进入网络。与IDS相比，IPS更加主动，能够在攻击者造成实际损害之前将其拦截，保护物联网系统的安全和稳定。为了适应物联网环境的多样性，入侵检测与防御技术也在不断进化。它们需要支持多种设备和通信协议，具备高度的灵活性和可扩展性。同时，为了应对日益复杂的攻击手段，这些技术还需要不断引入新技术和新方法，如人工智能、大数据分析等，以提高检测的准确性和响应的及时性。

3.4 网络安全监测与预警技术

通过持续监测网络状态和安全事件，及时发现潜在

的安全风险，并提前预警，为后续的应对措施提供宝贵的时间和空间。监测技术包括对网络流量、系统日志、安全设备等多种数据源的实时监控和分析。通过大数据分析技术，对海量数据进行挖掘和关联分析，发现隐藏在数据背后的安全威胁。利用人工智能算法进行智能分析，提高监测的准确性和效率。预警系统则是根据监测结果，对潜在的安全风险进行评估和预测，并生成预警报告或触发预警响应机制。预警信息可以通过多种方式传达给相关人员，如电子邮件、短信、系统通知等，以便及时采取措施应对潜在的安全威胁。在物联网环境下，网络安全监测与预警技术还需要考虑设备间的联动和协同工作。通过建立统一的安全管理平台，实现跨设备、跨系统的安全监测和预警，形成全面的安全防护体系。

3.5 隐私保护与数据安全管理

物联网设备在收集、处理和传输数据的过程中，面临着数据泄露、篡改和滥用等风险。因此，加强隐私保护和数据安全管理对于维护用户权益和确保系统稳定运行至关重要。在物联网系统中，应采取加密技术对用户数据进行加密存储和传输，确保数据在传输过程中的机密性和完整性。制定严格的隐私政策和数据访问权限管理制度，限制对隐私数据的访问和使用。从数据的收集、存储、处理到销毁等各个环节，都需要制定详细的安全规范和操作流程。采用先进的数据加密、数据备份和恢复技术，确保数据的安全性和可用性。建立数据安全审计和监控系统，对数据的操作行为进行记录和跟踪，及时发现和处理潜在的安全风险。为了应对物联网环境的复杂性和多样性，还需要加强跨设备、跨系统的数据安全管理。通过建立统一的数据安全标准和协议，实现不同设备和系统之间的安全互操作和数据共享。同时，加强与其他安全领域的协同工作，如网络安全、物理安全等，形成全面的数据安全管理体系。

4 物联网安全技术的未来发展趋势

物联网安全技术的未来发展趋势展现出了前所未有的活力与创新。这一领域将日益趋向智能化与自动化，借助人工智能、机器学习等先进技术，实现自我学习、自适应以及自动化应对安全威胁的能力，显著提升安全响应速度与防护效果。同时，随着物联网生态系统的日益庞大，安全技术也将更加集成化和协同化，打破设备、系统和协议间的壁垒，实现跨平台、跨领域的统一安全管理和防护。考虑到物联网设备的资源限制，未来安全技术将追求轻量级与高效化，通过算法优化和资源管理，确保安全防护的同时不影响设备的正常运行[5]。区块链技术因其去中心化、不可篡改的特性，将在物联网安全领域发挥重要作用，增强数据的安全性和可信度。隐私保护将成为安全技术不可忽视的一环，通过加强隐私政策和数据访问权限管理，结合先进的加密和匿名化技术，保护用户的个人信息安全。此外，标准化与合规性也将成为物联网安全技术发展的重要方向，通过制定统一的安全标准和协议，促进物联网行业的健康、有序发展，确保各参与方在遵循法律法规的前提下，共同推动物联网安全技术的进步与创新。

结束语

物联网技术的迅猛发展为生产生活带来了革命性的变化，但同时也对计算机网络安全技术提出更高的要求。面对不断演进的威胁和挑战，需要持续加强技术创新与研发，推动安全技术向智能化、集成化、轻量级和标准化方向发展。只有这样，才能确保物联网的可持续发展，为构建更加安全、可信、智能的网络世界奠定坚实基础。

参考文献

[1]刘畅.物联网计算机网络安全与控制策略分析[J].无线互联科技,2022,19(03):11-12.

[2]韩军峰.物联网计算机网络安全与远程控制技术分析[J].中国新通信,2019,21(21):160.

[3]石乐义,刘佳,刘祎豪,朱红强,段鹏飞.网络安全态势感知研究综述[J].计算机工程与应用,2019,55(24):1-9.

[4]王志强.物联网计算机网络安全与远程控制技术初探[J].电子测试,2020(13):96-97.

[5]何飞勇,卜新华.基于物联网环境的网络安全技术分析[J].魅力中国,2021(5):337-338.