第 3 卷◆第 3 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

物联网技术下的计算机网络安全问题研究

夏芙蓉
湖南涉外经济学院
DOI:10.12238/acair.v3i3.15586

[摘　要] 在社会的不断进步与发展下,计算机网络技术已在各行各业得到广泛应用,推动众多行业的快速发展。然而,尽管计算机网络技术为人们带来极大的便利,但其所伴随的安全隐患却不容忽视,深入探讨计算机网络安全问题,并结合物联网技术来制定相应的防范措施,是完善计算机网络体系,确保其安全性与稳定性的手段。基于此,本文对物联网技术下的计算机网络安全问题进行探讨。
[关键词] 物联网技术；计算机；网络安全
中图分类号：G633.67　文献标识码：A

Research on Computer Network Security Issues under Internet – of – Things Technology

Furong Xia
Hunan International Economics University

[Abstract] With the continuous progress and development of society, computer network technology has been widely applied in various industries, promoting the rapid development of many industries. However, although computer network technology has brought great convenience to people, the security risks associated with it cannot be ignored. In − depth exploration of computer network security issues and the formulation of corresponding preventive measures combined with Internet − of − Things technology are means to improve the computer network system and ensure its security and stability. Based on this, this paper discusses the computer network security issues under Internet−of−Things technology.
[Key words] Internet−of−Things technology; Computer; Network security

引言

随着物联网技术的不断成熟,推动了社会进步,促进各领域发展。在此背景下,计算机网络技术得到快速发展,并逐渐成为人们日常生活和工作中重要的一部分。在网络应用的普及下,计算机网络安全问题引起越来越多的关注,成为当今社会亟须解决的关键问题。网络安全关乎个人隐私保护,影响国家在全球竞争中的战略地位,应提升计算机网络的安全防御能力,在物联网环境下加强安全防范,确保网络健康发展。

1 案例分析

以2016年“Mirai僵尸网络”事件为例,黑客感染大量不安全的物联网设备,形成庞大的僵尸网络。该网络利用这些被感染的设备发动大规模的分布式拒绝服务攻击,导致多个知名网站瘫痪,影响数百万用户的正常使用。该事件反映了物联网设备普遍存在安全漏洞,且缺乏足够的防护措施,成为黑客攻击的理想目标。同时,物联网设备数量庞大,种类繁多,导致传统网络防护机制难以有效应对。

2 物联网技术概念

物联网技术将物理世界中的各类设备嵌入式传感器、无线通信等技术,转化为具有自我调节功能的网络节点,其具备基本的数据采集与传输能力,能够实时分析优化决策过程,从而形成协同工作的智能网络。物联网技术架构主要包括感知层、网络层、应用层,感知层负责信息采集,网络层提供设备间的数据传输与交互功能,应用层则依据用户需求实现多种智能服务。由于物联网设备种类繁多且部署在高度异构的环境中,导致其存在安全隐患,物联网的广泛接入性使得其易成为网络攻击的目标,对物联网的数据安全造成严重影响[1]。

3 物联网技术下的计算机网络安全问题

3.1感知层存在的安全问题

由于感知层涉及大量分布式传感器,存储能力较低,导致其在面临复杂的安全防护需求时较为脆弱,感知设备的物理防护能力较弱,易受到物理破坏,导致敏感数据泄露。感知层的设备采用无线通信技术进行数据传输,而无线信号的易受干扰性使其受到窃听、信号劫持等攻击,无线通信中缺乏有效的加密机制,使攻击者通过中间人攻击伪造传输数据,进而影响数据的可靠性。感知层设备在物联网系统中常呈现高度异构性,设备类型的差异导致其采用的安全机制不统一,增加安全防护的复杂性。部

分感知设备缺乏适当的访问控制措施，易成为未经授权的设备接入的入口，形成潜在安全漏洞，攻击者可冒充合法设备实施入侵。感知层设备的维护周期较短且更新不及时，部分设备在出厂时未考虑未来的安全性需求，存在未修复的安全漏洞，长期处于未补丁状态，导致这些设备在遭遇已知攻击时无力抵抗。

3.2数据保护中的问题

物联网系统利用大量感知设备采集并传输海量的敏感数据，这些数据涉及用户隐私和企业机密，因而其保护需求极为严峻。由于物联网的设备种类繁多且分布广泛，数据在整个系统中的传输与存储过程常面临多种安全风险。物联网中的数据传输依赖无线通信，使得数据在传输过程中易受到窃听、篡改等攻击，且由于无线信道的开放性特点，未加密的数据流极易被攻击者通过中间人攻击篡改，导致数据完整性遭到破坏。物联网系统的设备计算能力有限，存储资源匮乏，导致对数据加密的支持能力较弱，部分设备未能实现端到端的加密保护，数据在不同节点间的传输缺乏有效加密措施，从而增加数据泄露的风险。物联网中的数据保护还面临设备的身份验证与访问控制问题，由于缺乏严格的认证机制，攻击者可以伪造合法设备，篡改设备身份以获得数据的访问权限，对于未经授权的设备，攻击者可以通过远程操控窃取存储在设备中的敏感数据[2]。

3.3通信安全问题

物联网通信依赖多种无线技术如Wi-Fi、蓝牙等，此类通信方式易受干扰，遭受信号篡改。无线信号传播不受物理隔离的限制，攻击者可以通过各种手段接入通信信道，实施中间人攻击，进而获取干扰通信内容。物联网中大量设备连接至网络，其数量庞大且分布广泛，通信链路多样且复杂，使得网络拓扑难以有效控制，此种环境下设备间的数据加密机制不完善，未加密的通信数据易被恶意篡改，影响通信的完整性。物联网通信采用轻量级协议，其在设计时优先考虑低功耗、高效率，未能充分考虑通信的安全性，导致其在遭遇特定攻击时易成为突破口。部分协议未对数据进行严格的加密保护，存在明文传输问题，导致通信过程中的数据易被篡改，同时物联网设备在通信过程中多依赖公网连接，而公网本身的安全性较低，易受到大规模网络攻击的影响，导致物联网通信链路的可用性遭到破坏。

3.4物联网系统被攻击的范围变大

物联网系统将大量设备、传感器等连接到网络，导致网络攻击面大幅度扩展，传统计算机网络主要面临终端设备、服务器的攻击，而物联网设备种类繁多，分布广泛且互联互通，其物理空间和虚拟空间的结合使得攻击者能够在更广阔的范围内进行攻击。物联网设备本身具有较低的存储能力，部分设备并未充分部署安全防护措施，攻击者可以以各种手段轻松入侵设备，从而扩大攻击范围。物联网设备的多样性使得安全漏洞难以统一修复，攻击者可利用不同设备之间的漏洞差异突破系统防线，实现大规模入侵。随着物联网系统的规模不断扩大，攻击者能够以单一设备进行攻击，并以横向传播的方式，借助网络中的其他设备形成链式反应扩大攻击的影响范围。物联网系统的云平台使物联网依赖传统数据中心，攻击者破坏边缘节点的安全间接影响整个物联网系统的运作[3]。

4 物联网技术下的计算机网络安全应对措施

4.1强化防火墙与入侵检测技术的应用

防火墙是物联网网络安全的第一道防线，需根据物联网的特点进行定制化设计。传统防火墙基于端口进行流量控制，但物联网中部分设备以非标准端口进行通信，防火墙需具备深度包检测能力，能够识别并过滤异常流量。物联网防火墙应支持动态访问控制，基于设备身份、设备行为模式进行实时调整，以应对不断变化的攻击模式。针对物联网中的低功耗设备，防火墙设计应考虑资源限制，采取轻量级且高效的安全策略，减少对设备性能的影响。与防火墙相辅相成的是入侵检测技术，物联网系统中的入侵检测系统应具备多层检测能力，能够在不同层级识别潜在攻击。基于网络流量的入侵检测可以分析流量模式，发现恶意攻击的迹象，而基于主机的入侵检测则可以深入到每个设备的操作系统，检测恶意软件、数据篡改等行为。为提高检测的准确性，入侵检测系统应支持行为分析技术，对设备的正常行为模式进行建模，及时发现偏离常规的异常活动。入侵防御系统可以与IDS紧密集成，在发现入侵迹象后主动阻断攻击流量，确保系统的可用性。针对物联网设备的异构性，入侵检测技术应实现跨平台的协同工作，以多维度的数据源进行联动分析，增强整体防御能力，图为入侵检测技术。

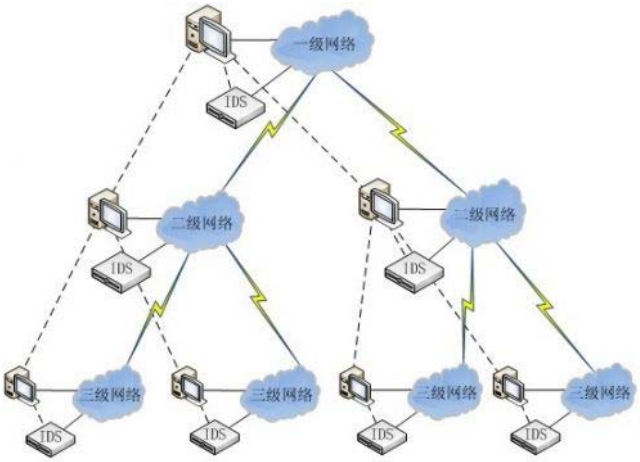

图 入侵检测技术

4.2加强网络安全防御机制的管理

物联网系统的安全防御机制应建立健全的管理框架，以定义明确的安全角色与权限，确保各类设备和节点在接入、通信及数据交换过程中遵循严格的安全要求。在此框架下，应结合基于风险管理的安全评估模型，对网络中每个环节的安全状况进行定期检测与评估，及时识别系统中的潜在漏洞，并制定相应的补救措施。物联网网络的安全防御机制应实施全面的访问控制，基于设备身份对所有接入点进行动态监控，避免未经授权的设备对系统控制，对于不同类别的物联网设备，访问控制应采用轻量化、低延迟的方式，同时保证防护措施的有效性。加强网络流

量的监控与分析，部署智能化的流量分析工具实时识别潜在攻击模式，确保在攻击发生初期能够迅速响应并采取防御措施。流量分析工具应具备自学习功能，根据网络的正常通信模式进行动态调整，以适应不断变化的网络威胁。为提高防御机制的管理水平，应强化多层次的防护体系，在网络边界、终端设备层面设置多个防御层次，形成闭环防护，确保在一个环节被突破时其他环节能够继续发挥作用。针对大规模物联网系统的管理要求，采用集中式与分布式相结合的安全管理方式，结合边缘计算平台优势实现对物联网设备的集中监控与分布式防护，从而有效提升系统对大规模攻击的防御能力[4]。

4.3对系统进行实时监测控制

物联网系统应部署全面的实时监控机制，确保在第一时间检测到异常行为，实时监控应结合网络流量分析，对网络流量进行深度包检测与行为分析及时发现异常流量、数据篡改等攻击迹象，防止攻击在系统内蔓延。系统应配备智能化的入侵检测系统与入侵防御系统，对网络行为进行持续监测与实时分析，在发现攻击企图时立即触发警报并采取自动化防御，隔离受攻击的设备，从而有效阻断攻击传播。为实时控制物联网系统，安全运维平台应整合集中式与分布式的监控机制，借助边缘计算技术在网络边缘实时处理数据，减少数据传输延迟并提高响应速度，确保云平台可以集中汇总分析所有安全事件，并根据全局视角优化防御策略。设备性能监测也应嵌入实时控制机制中，定期获取设备的固件版本、漏洞扫描结果，并利用自动化更新与修复机制确保设备处于最新的安全状态。

4.4建立安全路由器

安全路由器应集成深度包检查功能，实时分析传输中的数据包，检测并阻止潜在攻击。对网络流量实时监控，安全路由器能够识别异常行为，及时防御来自内外部的威胁。对于物联网环境中常见的无线通信技术，路由器需支持高级的加密算法，确保数据在传输过程中的机密性，防止数据被篡改。为防止路由器自身成为攻击目标，路由器应具备固件保护功能，定期进行漏洞修补，防止通过路由器漏洞进行远程攻击。安全路由器应具备自动检测并隔离潜在威胁的能力，在发现攻击行为时自动切断恶意连接，减轻攻击的影响并防止攻击蔓延，同时支持跨协议的安全保护，在不同通信标准之间提供安全保障[5]。

5 结束语

综上所述，计算机网络安全是物联网系统中至关重要的一环，是确保信息安全的核心要素。在目前物联网环境下，计算机网络安全仍面临诸多挑战，导致数据泄漏风险。在构建物联网系统时，需应用防火墙技术，实施入侵检测机制，并建立完善的网络安全防护体系，以动态监控来实时跟踪系统运行状况，从而有效提升物联网系统的安全性，推动其稳步发展。

[参考文献]

[1]娄元柱,杨冲,孙鑫.物联网技术在煤矿提升机运行状态实时监控中的应用[J].内蒙古煤炭经济,2023,(24):136-138.

[2]高巍,仲园园,苏静.基于物联网技术的智慧农业应用研究[J].世界热带农业信息,2023,(12):6-7.

[3]王洁,戚军娜,王飞,等.物联网技术在特需病房空气消毒机管理中的应用[J].医疗装备,2023,36(24):54-56.

[4]胡志军,张婷,贾子昊,等.基于物联网技术配电线路智能终端的分析[J].中国信息界,2023,(06):170-173.

[5]严彪.物联网技术在消防监督管理中的应用分析[J].消防界(电子版),2023,9(24):66-68.

作者简介：

夏芙蓉(1982--),女,汉族,河北省邢台人,硕士研究生,高级工程师,研究方向：计算机网络。