Computer Science and Application 计算机科学与应用, 2025, 15(11), 68-74
Published Online November 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.1511284

Hans汉斯

物联网面临的安全挑战及一种IDPS应对方案

徐小龙

曲阜师范大学实验教学与设备管理中心，山东 日照

收稿日期：2025年10月1日；录用日期：2025年10月28日；发布日期：2025年11月5日

摘　要

物联网作为新一代信息网络，在多个领域发挥着重要作用，网络安全已成为影响其健康发展的重要因素。入侵检测系统通过监控网络流量在保护网络安全方面发挥着重要作用。由于物联网自身的特性如设备异构性、资源限制、动态性，大大增加了网络安全与物联网环境集成的难度。本研究探讨了物联网网络安全面临的挑战，并研究了使用入侵检测与防御系统应对这些挑战的方法。

关键词

物联网，入侵检测，入侵防御，网络安全

Security Challenges Faced by the Internet of Things and an IDPS Response Method

Xiaolong Xu

Experiment Teaching Center, Qufu Normal University, Rizhao Shandong

Received: October 1, 2025; accepted: October 28, 2025; published: November 5, 2025

Abstract

As a new generation of information network, the Internet of Things plays an important role in multiple fields, and network security has become an important factor affecting its healthy development. Intrusion detection systems play an important role in protecting network security by monitoring network traffic. Due to the inherent characteristics of the IoT, such as device heterogeneity, resource limitations, and dynamism, it greatly increases the difficulty of integrating network security with the IoT environment. This study explores the challenges faced by IoT network security and investigates methods for using intrusion detection and prevention system to address these challenges.

文章引用: 徐小龙. 物联网面临的安全挑战及一种 IDPS 应对方案[J]. 计算机科学与应用, 2025, 15(11): 68-74.
DOI: 10.12677/csa.2025.1511284

Keywords

Internet of Things, Intrusion Detection, Intrusion Prevention, Network Security

1. 引言

物联网设备的激增彻底改变了各个领域，从智能家居和医疗保健到工业自动化和交通运输。然而，物联网的快速增长也带来了重大的安全挑战。保证物联网的安全可以防止未经授权的访问、数据泄露和对关键服务的潜在干扰[1]。在部署物联网时集成网络安全措施集对保障物联网的安全十分重要。

物联网系统由大量相互连接的设备、传感器和网关组成，它们相互通信并与云端通信。这些设备收集和传输敏感数据，容易成为网络攻击的目标[2]。传统的网络安全措施如防火墙和入侵检测系统需要进行调整以适应物联网的特性。网络安全集成对于提供端到端的安全性和保护整个物联网基础设施至关重要。

网络安全与物联网环境的集成面临许多挑战。设备的异构性、资源限制、网络拓扑的动态性以及对可扩展性的需求，这些问题都是物联网安全的重大障碍[3]。确保安全通信、在物联网中实施强大的认证机制和隐私保护机制也是需要认真考虑的问题。应对这些挑战对于建立强大的物联网安全框架是必需的。

物联网的入侵检测与防御在生产生活的各个领域都有应用，文献[4]提出了一种基于改进支持向量机的电力物联网入侵检测方法，使用粒子群优化方法改进支持向量机，构建检测模型，以进行电力物联网系统的入侵检测。文献[5]提出了一种基于物联网技术的医院网络自动防入侵模型，基于物联网技术对医院的网络数据进行标准化处理，再利用主分量分析法对标准化的网络数据进行线性的特征提取，构建入侵检测模型。文献[6]提出了一种多模型组合的船舶物联网非法入侵行为检测方法，以改善非法入侵行为检测效果，确保船舶物联网的安全运行。本研究主要针对智能家居物联网环境，设计了一种分层结构的入侵检测与防御系统，以保证居家物联网环境的安全，并尽量减少对用户的干扰，保障用户的居家体验。主要目标是：

- 识别、分析将网络安全集成到物联网中所面临的一系列挑战。
- 研究将分层结构的入侵检测与防御系统应用到智能家居物联网中，以保证居家信息安全。

通过实现这些目标，以加强对物联网环境中网络安全集成的理解和推动，最终促进物联网系统安全可靠的发展。

2. 物联网网络安全集成面临的挑战

A) 设备异构性和资源限制

在物联网中集成网络安全的主要挑战之一是联网设备的广泛异构性。物联网由具有不同操作系统、协议和安全功能的各种设备组成[7]。保护这种异构环境需要标注每个设备的安全漏洞。此外，物联网设备通常只具有有限的处理能力、内存和能量资源，对其实施资源密集型安全机制具有一定的难度。

B) 网络拓扑的动态性

物联网呈现出动态和自组织的网络拓扑，设备经常加入或离开网络[8]。这种动态特性给网络安全集成带来了挑战。为静态网络设计的传统安全解决方案可能难以适应不断变化的物联网网络拓扑。在物联

网的动态特性中，确保无缝的安全措施并保持一致的安全处理方式是一项重要课题。

C) 有限的处理能力和存储空间

物联网设备通常具有有限的处理能力和内存，因为它们的设计就是以最少的资源来实现高效运转。这种资源限制阻碍了在设备上实施强大的安全机制。加密技术、认证技术和入侵检测算法可能会给资源受限的设备带来巨大的计算负担。平衡对强大安全措施的需求与物联网设备的有限资源之间的矛盾是一项关键挑战。

D) 隐私与数据保护问题

物联网设备产生大量数据，经常包含个人隐私信息。保护用户数据免受未经授权的访问或滥用是一项关键挑战。在保证物联网应用程序的可用性和功能的同时，实施强大的数据加密、访问控制和匿名化技术需要仔细研究。

E) 通信安全

保护物联网的通信渠道对于保护敏感数据和防止未经授权的访问至关重要。物联网设备可以使用具有不同安全功能的各种通信协议。一些协议可能缺乏内置的加密或身份验证机制，使其容易受到窃听、篡改或欺骗攻击。以无缝和标准化的方式保护不同设备和协议之间的通信是一项重大挑战。

3. 一种物联网入侵检测和防御系统的实现方案

入侵检测和防御系统(Intrusion Detection and Prevention System, IDPS)在增强物联网安全方面发挥着重要作用。该系统监控网络流量、设备行为和通信模式以识别和应对潜在的入侵行为。可以采用多种方法将 IDPS 有效地集成到物联网中。

3.1. 网络分段和隔离

为了进行集中监控和检测，可以根据设备类型、功能或安全要求将物联网划分为逻辑子网。通过将关键设备或敏感数据隔离在单独的网段中，可以控制潜在的入侵并将其影响降至最低。IDPS 可以部署在每个网段的边界以监控流量并检测任何未经授权的活动。

网络分段和隔离是在物联网环境中集成网络安全的一种重要方法。它根据设备类型、功能或安全要求将物联网划分为逻辑子网或网段[9]，如图 1 所示。这样就能够对每个网段进行集中监控、控制和保护。

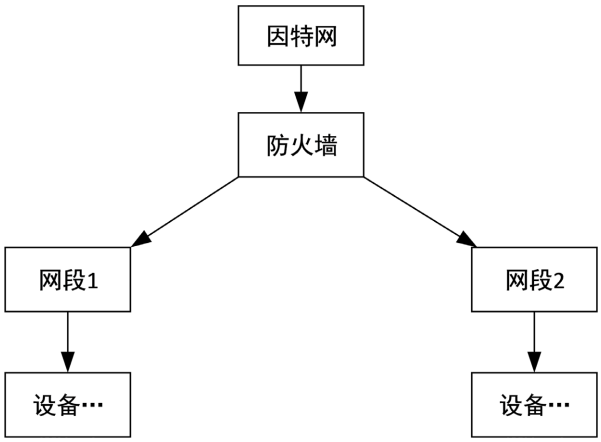

Figure 1. Network segmentation and isolation
图 1. 网络分段和隔离

在表 1 中，根据设备类型、功能和安全要求将物联网分成两个逻辑网段。网段 1 包括智能恒温器和

智能照明系统等设备，主要用于暖通空调控制和照明控制。网段 2 由用于监控的网络摄像头和用于访问管理的访问控制系统组成。基于设备所处理的数据，每个部分都有不同层次的安全要求。

Table 1. IoT segmented devices
表 1. 物联网细分设备

网段	标准	设备
网段 1	设备类型	智能恒温器，智能照明系统
	功能	暖通空调控制，照明控制
	安全要求	中等
网段 2	设备类型	网络摄像机，网络门禁系统
	功能	监控，访问管理
	安全要求	高

通过网络分段并在分段边界实施适当的安全措施如防火墙和 IDPS，可以保护网络免受未经授权的访问和潜在的入侵。对每个网段内的网络流量和设备行为进行持续监控和分析，有助于发现可能的安全事件并及时采取相应措施。

IDPS 部署在网段边界以监控网络流量，检测异常行为或潜在入侵并采取预防措施以保护网络。通过在每个网段的边界设置 IDPS，系统可以分析传入和传出的流量，检测已知的攻击模式或可疑行为并做出相应的响应。

图 2 描述了部署在每个分段边界处的 IDPS 系统。它们监控并分析进入和离开相应网段的流量，实时检测潜在的入侵或恶意活动。

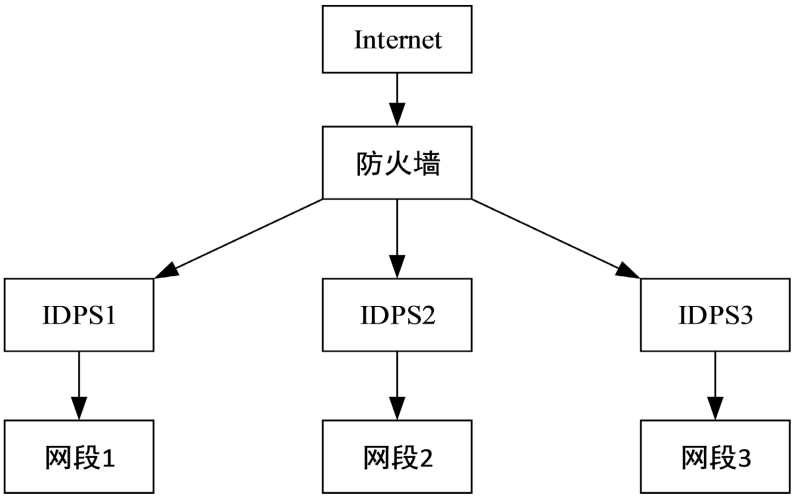

Figure 2. IDPS segmentation system
图 2. IDPS 分段系统

图中的三个 IDPS 负责监控和分析通过各自网段边界的流量。通过在网段边界部署 IDPS，物联网能够在增强的安全措施、快速的安全事件检测以及对潜在威胁的及时响应等方面得到加强。这有助于保护各个独立部分和整个网络免受非法访问、数据泄露或其他恶意活动的侵害。

3.2. 网段边界的 IDPS 部署算法

步骤 1：对于物联网中的每个网段边界，

a) 确定边界中涉及的网络设备和通信渠道。

b) 确定特定分段边界的安全要求和目标。

步骤 2：根据已确定的分段边界，在适当位置部署 IDPS。

a) 选择一个符合物联网网络安全需求的 IDPS。

b) 在网段边界安装并配置入 IDPS。

步骤 3：在每个分段边界配置 IDPS。

a) 根据进出流量确定监控范围和流量捕获点。

b) 根据网络的安全策略设置检测机制，如基于签名的检测、异常检测或基于行为的检测。

c) 对检测到的入侵或恶意活动配置响应机制，如警报、阻断流量或隔离受感染的设备。

d) 建立安全事件的记录和报告机制。

步骤 4：确保 IDPS 系统与相应网段的连接和集成。

a) 在 IDPS 和网段边界的网络设备之间建立必要的通信信道。

b) 配置网络设备与 IDPS 进行适当交互，确保流量的流畅性。

步骤 5：测试和验证 IDPS 部署。

a) 进行彻底的测试，确保 IDPS 正常运行并能捕获预期的网络流量。

b) 验证入侵检测和响应机制的准确性和有效性。

c) 根据测试结果和反馈调整 IDPS 配置。

步骤 6：持续监控和管理 IDPS 系统。

a) 定期用最新的安全补丁、签名或检测规则更新 IDPS。

b) 监控 IDPS 日志和报告以发现潜在的安全事件或异常。

c) 分析和调查检测到的安全事件，采取适当的行动并在必要时调整 IDPS 配置。

步骤 7：定期评估 IDPS 的有效性。

a) 评估 IDPS 在检测和预防入侵或恶意活动方面的性能和效率。

b) 收集安全管理员和网络使用者的反馈，以确定需要改进之处。

c) 进行必要的调整以增强整个网络的安全性。

4. 实验设计与性能评估

4.1. 实验设计

为了验证文中所提出的部署算法的有效性，设计了一个日常智能家居的场景进行实验。选取 25 台物联网设备组成了一个星型结构的网络，设备包括智能恒温器、智能灯泡、网络摄像头等。实验目的是检验系统对入侵行为的检测能力，并对资源利用率、响应时间、出错率等多项指标进行评估。控制变量包括异常数据注入方式、物联网设备类型以及数据的采集频率等。汇聚节点采用 ARM9 架构的 S3C2440 微处理器芯片(主频 400 MHz，内部静态 RAM 4 KB)，边缘网关采用 Intel i5-8400 处理器(2.80 GHz, 8 GB RAM)。

实验过程为：

(1) 在传感层部署设备并对相应参数进行初始化，如特征上报周期为 20 s，最大周期为 200 s。

(2) 模拟入侵行为，通过脚本模拟流量异常、网络行为异常、资源使用情况异常等行为，观察并记录

系统的响应情况。

(3) 收集、整理、分析系统的日志数据。

对系统的评估选择以下几个指标：检出率、漏报率、误报率、响应时间和 CPU 占用率。实验数据包含正常数据和异常数据各半，总量为 100,000 条行为记录。

4.2. 性能评估

在衡量物联网入侵检测与防御系统的性能时，根据不同的应用场景和威胁模型，对性能的要求也不相同。根据本实验所设定的智能家居的应用场景，检出率较高即可，允许漏掉一些低风险攻击。这种场景首要的是用户体验，为了不影响用户体验，必须有极低的误报率。因此根据应用场景和行业经验，本实验中系统性能指标的合理预设目标为：检出率 ≥93%，漏报率 ≤7%，误报率 ≤1%，平均响应时间 ≤1 s，平均 CPU 占用率 ≤50%。

通过实验得到了如表 2 所示的各性能指标的统计数据。可以看出，系统在观测的五个指标上都达到了预期。95.1%的检出率表示系统能够发现大多数的入侵行为；0.5%的误报率达到了系统要求，减少了对用户的干扰；0.6s 的响应时间表示系统有较强的实时性；39%的 CPU 利用率减少了资源占用；4.9%的漏报率达到了预设目标，满足系统要求。

Table 2. Experimental results
表 2. 实验数据

	检出率(%)	漏报率(%)	误报率(%)	响应时间(s)	CPU 占用率(%)
目标	≥93	≤7	≤1	≤1	≤50
结果	95.1	4.9	0.5	0.6	39

根据以上实验结果可以看出，该 IDPS 系统具有高效、准确的特点，有较高的实用价值。但该方案也存在一定的局限性，如没有涉及端到端加密流量的检测问题，处理这个问题需要一套多层次的、创新的解决方案，在后续的研究中将持续关注这一问题。

5. 结论

物联网中的网络安全集成对于确保物联网系统的安全性、可靠性和保密性至关重要。本研究针对物联网面临的安全问题展开，实行网络分段和隔离，在网段边界部署入侵检测和预防系统，通过检测和防御潜在入侵来增强物联网的整体安全性。实验表明，该系统能高效、准确地检测出异常行为，对提高物联网的安全性、稳定性、效率成效显著。

参考文献

[1] 魏政花. 物联网在智能家居中的安全防护技术研究[J]. 信息与电脑, 2025, 37(3): 81-83.

[2] 孙英梅. 物联网技术下的计算机网络安全问题探讨[J]. 网络安全技术与应用, 2024(6): 144-146.

[3] 尤耀华. 物联网环境下计算机网络安全技术影响因素及防范措施[J]. 网络安全和信息化, 2024(8): 26-28.

[4] 张恩, 黄永腾, 江泽, 等. 基于改进支持向量机的电力物联网入侵检测方法[J]. 电工技术, 2023(21): 101-103.

[5] 乔艳丽, 胡静. 基于物联网技术的医院网络自动防入侵模型构建[J]. 自动化技术与应用, 2023, 42(8): 103-106.

[6] 张晓伟. 多模型组合的船舶物联网非法人侵行为检测研究[J]. 舰船科学技术, 2023, 45(19): 189-192.

[7] 郭志林. 面向物联网环境的入侵检测与防御系统设计[J]. 信息记录材料, 2025, 26(8): 205-207.

[8] Jawad Khadim Alsayyad, M. (2024) Researching Issues in Information Security in Internet of Things (IoT) Systems: Challenge & Solution. *Journal of Al-Qadisiyah for Computer Science and Mathematics*, **16**, 251-263. https://doi.org/10.29304/jqcsm.2024.16.41786

[9] Sisodia, R., Banerjee, C. and Kaushik, M. (2023) Problems and Prospects in Internet of Things (IoT) Security Threats. *AIP Conference Proceedings*, **2760**, Article 020008. https://doi.org/10.1063/5.0148939