
给物联网装上哨兵，实时入侵检测与防御系统解析

MDPI ASI

作者：writer 来源：科学网

本文原地址：<https://www.iikx.com/news/progress/42465.html>

本文仅供学习交流之用，版权归原作者所有，请勿用于商业用途！

给物联网装上哨兵，实时入侵检测与防御系统解析 MDPI ASI。论文标题：Real-Time Large-Scale Intrusion Detection and Prevention System (IDPS) CICIoT Dataset Traffic Assessment Based on Deep Learnin

论文链接：<https://www.mdpi.com/2571-5577/8/2/52>

期刊名：Applied System Innovation

期刊主页：<https://www.mdpi.com/journal/asi>

一、引言

从智能医疗、智能交通，到智慧农业、智慧城市，物联网（IoT）正在连接越来越多的设备与应用场景。设备变得更智能的同时，网络也面临着更多潜在的安全威胁。在庞大复杂的物联网系统中，大量设备持续产生并交换数据，而 DDoS、DoS、中间人攻击（MITM）、Mirai 僵尸网络攻击以及侦察扫描（Recon）等威胁，也在不断寻找可以突破的入口。如何及时识别这些威胁，并在发现异常后迅速采取防御措施，仍然是一个值得关注的问题。

针对这一挑战，来自美国佛罗里达农工大学的研究团队构建了一套融合深度学习多层感知机（D LMLP）与入侵防御机制的系统模型——DLMIDPSM。基于CICIoT2023数据集，此模型将入侵检测（IDS）与入侵防御（IPS）结合起来，不仅能够识别包括五类入侵攻击和一类良性流量在内的六大类网络流量，还能根据检测结果自动触发相应的防御措施。这为进一步探索面向大规模物联网环境的自动化安全防护方案奠定了基础。

二、材料与方法

要让入侵检测模型具备实际应用价值，除了模型本身的识别能力，也需要有贴近真实场景的数据作为支撑，更重要的是能够在检测之后进行响应。围绕这一思路，研究团队从实验环境搭建、网络流量采集，到模型训练与防御机制设计进行了完整的实验验证，并通过与传统机器学习方法对比，进一步评估模型的表现。

研究团队没有依赖仿真环境，而是在 CIC（加拿大网络安全研究院）实验室中，使用真实的传感

器、摄像头、微控制器和树莓派等设备，搭建了一套包含超过 106 台物联网设备的实验拓扑（IDPST）。其中，直接参与攻击实验的设备超过 68 台，另有 39 台 Zigbee 设备通过 6 个网关连接组网。

整套网络由交换机、无线接入点和千兆网络分流器（network tap）等设备组成，可以在不影响正常通信的情况下，对网络中的良性流量和恶意攻击流量进行捕获，为后续的数据分析和模型训练提供真实的网络流量样本。

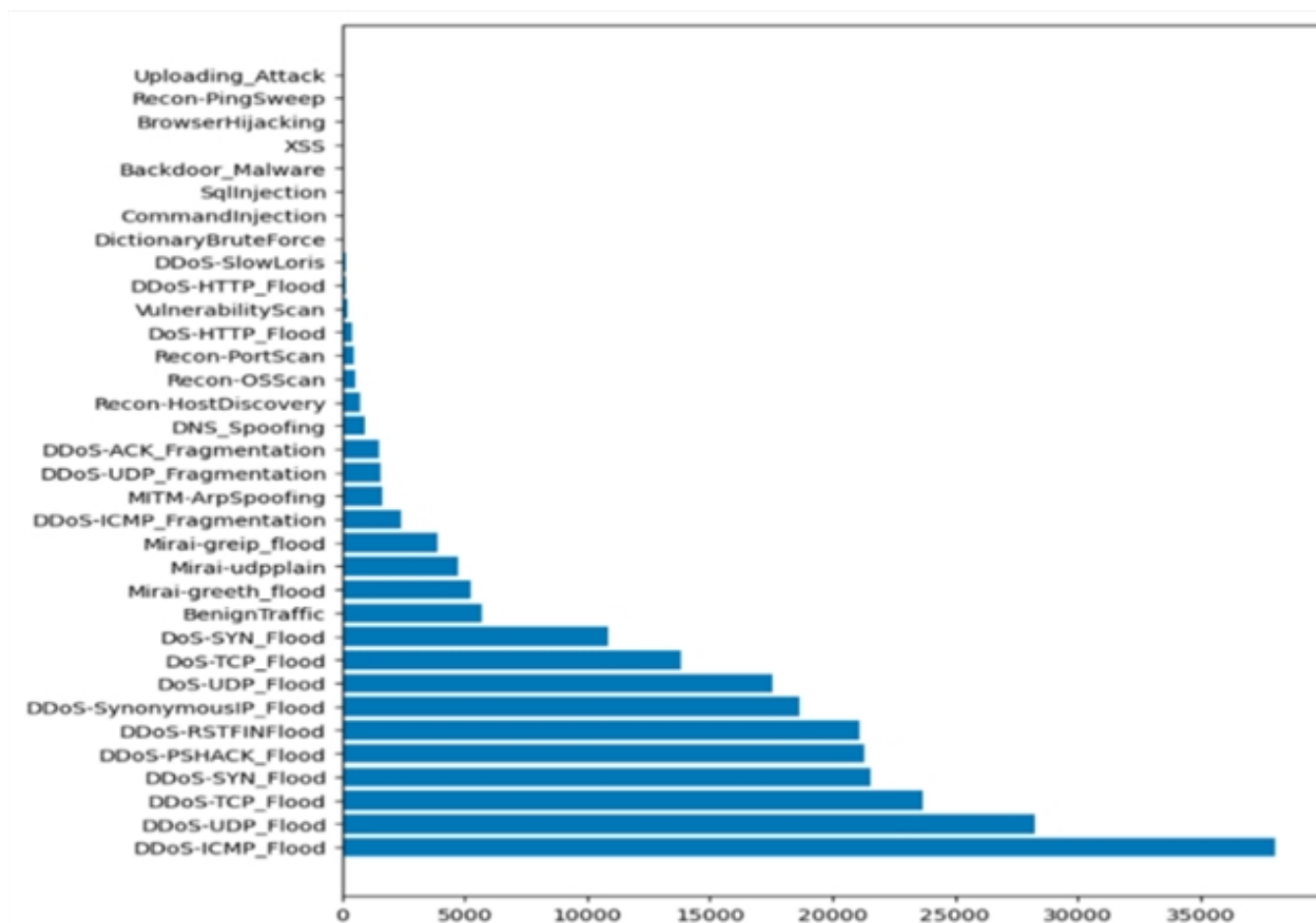


图1. CIC实验室物联网设备拓扑.

三、分析与结果

在搭建好的实验环境中，研究团队针对 IoT 设备实际执行了 33 种入侵攻击，并将相关流量归为 DDoS、DoS、中间人攻击（MITM）、Mirai 僵尸网络、侦察扫描（Recon）以及良性流量六大类。

整个攻防实验持续超过 20 小时，累计产生超过 520 GB 的原始网络流量。研究团队将这些数据按照不同大小的数据包批次进行并行处理，并提取上百个网络流量特征，最终整理形成可用于模型训练的结构化数据集。这样得到的数据，不仅包含不同类型的攻击流量，也保留了真实 IoT 网络环境中的良性通信。



(a) (b)

图2. 各攻击场景在数据集中的样本分布.

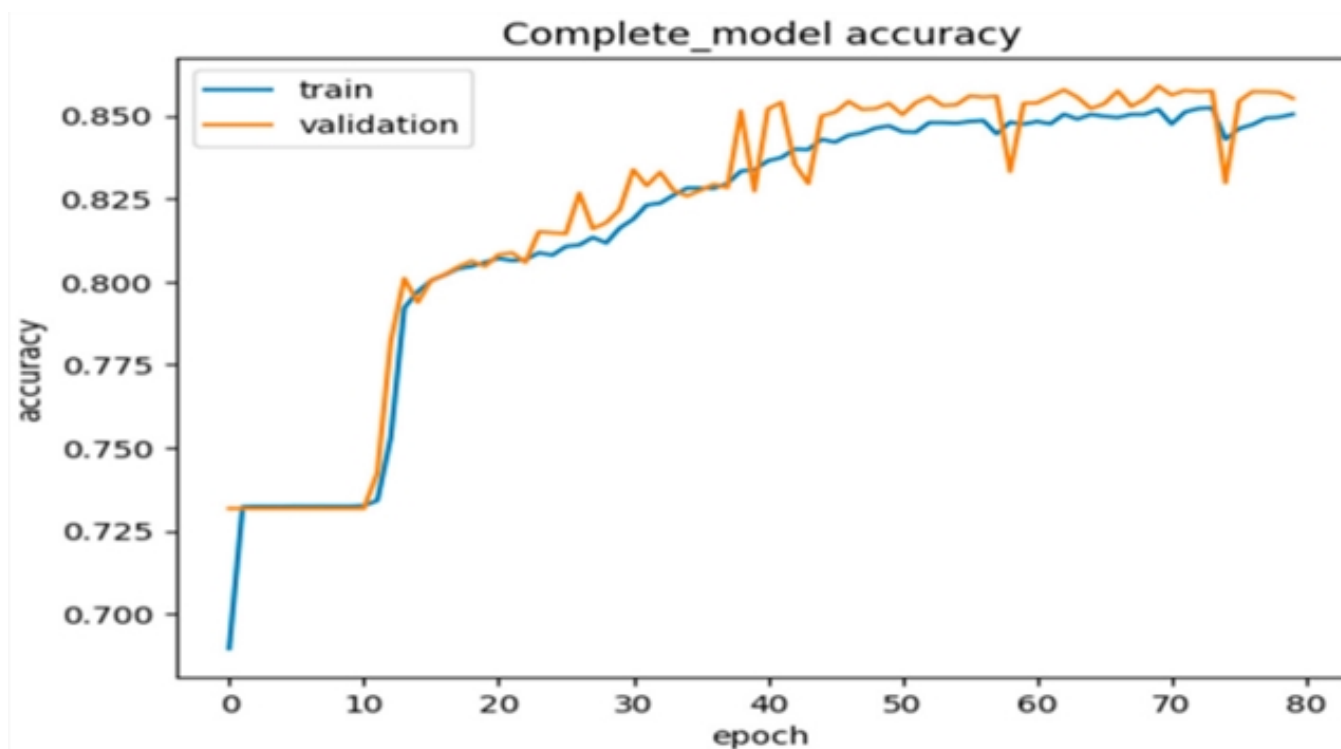
训练深度学习模型，识别六类网络流量

完成数据整理后，研究团队对数据进行独热编码、特征缩放等预处理，并将其输入基于多层感知机（MLP）构建的深度学习模型 DLMIDPSM。模型综合使用人工神经网络、卷积神经网络和循环神经网络相关方法，对不同类型的网络流量进行识别。

经过 80 个训练轮次后，模型的训练与验证准确率均达到约 85%，验证损失约为 1%。在分类评估中，模型精确率达到 99%，说明其对不同类型网络流量具有较好的识别能力。

数据经过独热编码、特征缩放等预处理后，被输入到基于多层感知机（MLP）构建的深度学习模型 DLMIDPSM

中训练，模型综合运用了人工神经网络、卷积神经网络与循环神经网络的能力。经过 80 个训练轮次，模型的训练与验证准确率均达到约 85%，验证损失仅为 1%；在与检测结果配套的分类评估中，精确率更是达到 99%，展现出优异的收敛效果与识别精度。



(a) (b)

图3. 完整模型在80个训练轮次下的准确率与损失变化.

将检测结果与防御动作衔接

为了进一步了解 DLMIDPSM 的表现，研究团队将其与决策树、支持向量机等传统机器学习方法进行了对比。

结果显示，传统方法的入侵检测与防御准确率约为 81%，精确率约为 72%；DLMIDPSM 的准确率则超过 85%，精确率达到 99%。从这组实验结果来看，在该大规模真实物联网数据集上，DLMIDPSM 在准确率和精确率两项指标上均取得了更好的表现。

图4. 各方法在二元分类任务下的混淆矩阵对比

四、展望与结论

本研究在真实的大规模物联网网络环境中，构建并验证了融合入侵检测与防御功能的深度学习系统 DLMIDPSM。研究从真实设备组网和攻击流量采集出发，进一步完成网络流量分类、攻击识别以及防御响应，并通过与传统机器学习方法对比，对模型性能进行了验证。

从实验结果来看，DLMIDPSM 在该数据集上取得了较高的识别准确率和精确率，同时能够根据检测结果执行相应的网络阻断操作。将真实物联网实验环境、网络流量数据以及检测与防御机制结合起来，为智慧医疗、智能交通、智慧农业和智慧城市等物联网应用场景中的网络安全研究提供了一个较为完整的实验框架。

Erskine, S.K. Real-Time Large-Scale Intrusion Detection and Prevention System (IDPS) CICIoT Dataset Traffic Assessment Based on Deep Learning. Appl. Syst. Innov. 2025, 8, 52.

期刊介绍

主编：Prof. Dr. Christos Douligieris, University of Piraeus, Greece

期刊聚焦跨学科系统创新与集成工程技术领域，涵盖智能制造、电气与机械系统、信息系统、人工智能、机器人技术、物联网、医疗信息学等应用系统创新研究。

投稿优势：

更高曝光度

Applied System Innovation期刊目前已被Ei Compendex、Scopus、ESCI (Web of Science), Inspec等多个数据库收录。

更快发表速度

Time to First Decision 21.3 Days

Acceptance to Publication 4.5 Days

开放获取

读者可以免费阅读/期刊文章。

来源：Applied System Innovation

更多 科学进展 请访问 <https://www.iikx.com/news/progress/>

本文版权归作者所有，请勿用于商业用途，[爱科学iikx.com](http://iikx.com)转发