# 5G物联网安全：基于神经网络的高效XSS攻击检测方案

作者：writer 来源：科学网

本文原地址：https://www.iikx.com/news/progress/40332.html



**5G物联网安全：基于神经网络的高效XSS攻击检测方案**。论文标题：Advancing XSS Detection in IoT over 5G: A Cutting-EdgeArtificial Neural Network Approach

论文链接：https://www.mdpi.com/2624-831X/5/3/22

期刊名：IoT

期刊主页：https://www.mdpi.com/journal/IoT

文章导读

随着5G技术的普及，物联网（IoT）在电子学习、远程医疗和智能制造等领域的应用深度不断加强。然而，5G的高带宽和低延迟特性在提升连接能力的平衡点上也带来了更复杂的安全挑战。跨站脚本（XSS）攻击作为一种常见的Web漏洞，能够通过恶意脚本渗透物联网设备的Web管理界面，导致敏感数据泄露或设备失控。传统的安全防护手段在面对海量且异构的物联网设备时，往往受限于计算资源或识别精度，难以在5G环境下提供实时有效的防御。本文提出了一种基于人工神经网络（ANN）的创新检测框架，旨在实现对5G物联网系统中XSS攻击的精准识别。研究通过引入过滤式（Filter）和包装式（Wrapper）特征选择方法，显著优化了模型的预测性能，并通过NF-ToN-IoT-v2和Edge-IIoTset两个主流数据集验证了方案的鲁棒性。如何在资源受限且数据量庞大的5G物联网环境中，实现对XSS攻击的高精度检测与低延迟防御，是本文旨在解决的核心问题。

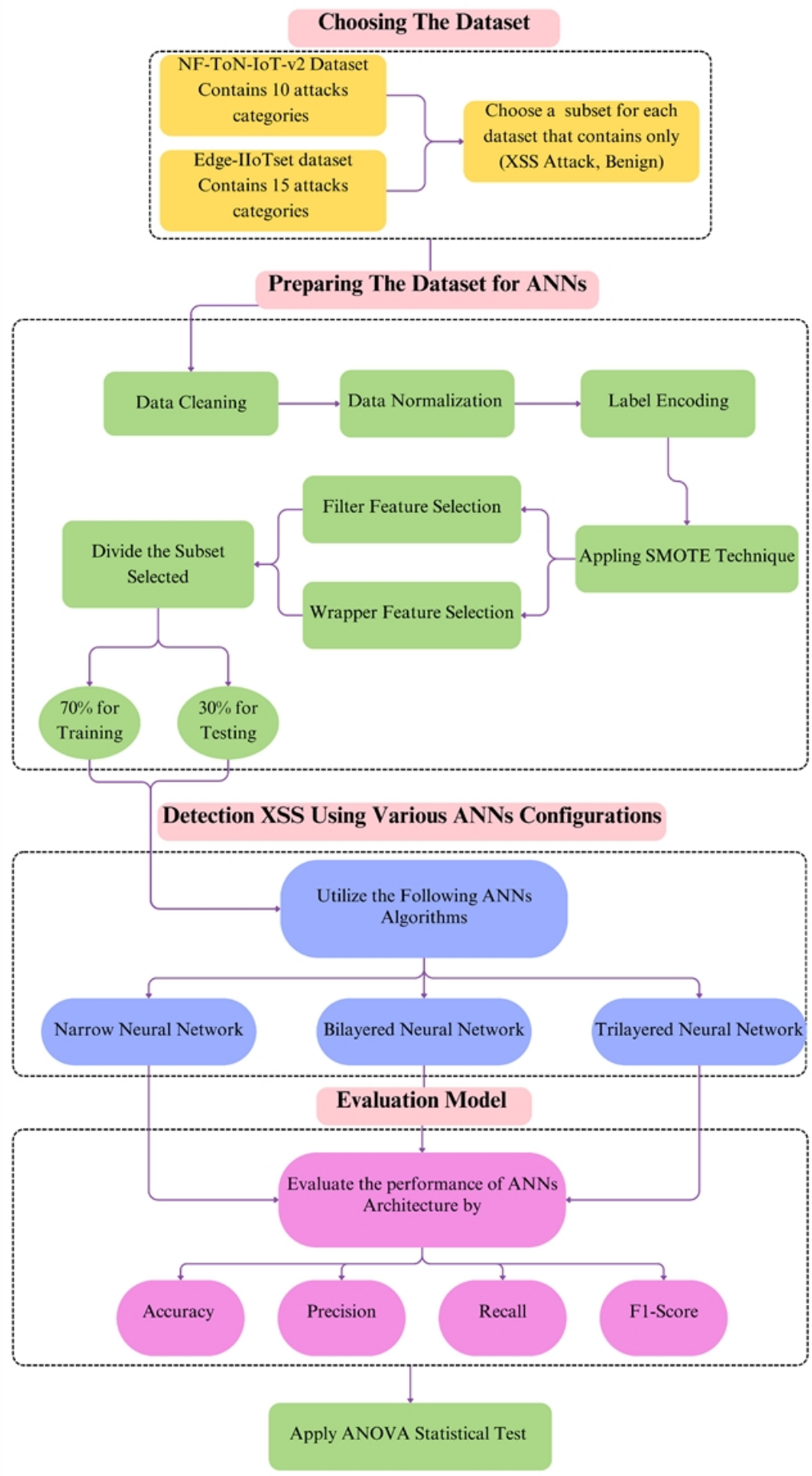
Choosing The Dataset
NF-ToN-IoT-v2 Dataset Contains 10 attacks categories
Edge-IIoTset dataset Contains 15 attacks categories
Choose a subset for each dataset that contains only (XSS Attack, Benign)
Preparing The Dataset for ANNs
Data Cleaning
Data Normalization
Label Encoding
Filter Feature Selection
Divide the Subset Selected
Appling SMOTE Technique
Wrapper Feature Selection
70% for Training
30% for Testing
Detection XSS Using Various ANNs Configurations
Utilize the Following ANNs Algorithms
Narrow Neural Network
Bilayered Neural Network
Trilayered Neural Network
Evaluation Model
Evaluate the performance of ANNs Architecture by
Accuracy
Precision
Recall
F1-Score
Apply ANOVA Statistical Test

图1.
提出的XSS攻击检测框架流程图：包含数据集选择、预处理、特征选择、模型训练及统计验证。

研究内容与结果

本研究设计了一套完整的深度学习流水线，核心在于通过特征工程提升ANN的检测效能。在预处理阶段，研究采用了合成少数类过采样技术（SMOTE）来解决数据集中类别不平衡的问题，确保模型不会偏向多数类样本。特征选择是提升性能的关键：研究首先利用基于互信息（MI）的过滤法识别出与攻击标签相关性最强的核心属性，随后结合基于递归特征消除（RFE）的包装法进一步筛选出最具判别力的特征子集。在分类器设计上，研究人员对比了不同深度的架构，利用MATLAB平台对各模型的超参数进行了精细化调优。这种多层次的筛选与建模机制，使得系统能够在减少计算负荷的同时，捕获5G流量中潜在的异常模式。

实验结果进一步证实了该框架在不同物联网场景下的卓越表现。在NF-ToN-IoT-v2数据集上，采用过滤特征选择的双层神经网络实现了高达99.84%的检测准确率；在更复杂的Edge-IIoTset数据集上，三层神经网络则取得了99.79%的最佳准确率。为了评估模型的稳健性，研究团队引入了方差分析（ANOVA）测试。结果显示，p值均远大于0.05，这表明不同神经网络模型之间的检测准确率不存在统计学上的显著差异，证明了训练过程具有极高的稳定性，且各模型在不同初始条件下均能保持一致的高性能。对比分析表明，本研究所采用的特征选择策略与深层ANN架构的组合，在识别精度上显著优于现有的随机森林（RF）、决策树（DT）、LSTM-AE及CNN等方法，为5G物联网环境下的实时入侵检测确立了新的性能基准。

总结和展望

本文通过整合先进的特征选择方法与深度神经网络架构，为5G物联网系统的安全防护提供了一种高效的XSS攻击检测手段。研究证明，在保持较低计算复杂度的前提下，ANN能够有效应对5G网络中高速且多样化的威胁特征，展现出强大的泛化能力与实际部署潜力。此外，统计验证确保了该方案在不同初始参数下的可靠性，为物联网安全审计提供了坚实的量化依据。展望未来，研究方向可进一步向轻量化边缘部署以及更广泛的未知漏洞检测领域延伸，以适应日益复杂的网络安全态势。随着5G及未来6G网络的演进，这种具备高稳健性的神经网络防御方案，将成为守护物联网数字生态安全的关键基石。

期刊介绍

主编: Amiya Nayak, University of Ottawa, Canada

IoT（ISSN2624-831X）创刊于2020年，发表物联网各个领域的原创论文、综述和快讯等。期刊发文方向包括但不限于：物联网中的人工智能和分析;物联网隐私、安全和信任;物联网网络设计和架构；物联网赋能技术（包括超低功耗物联网技术）；物联网技术在智能环境中的应用；物联网平台:基于云、网关和雾的物联网解决方案；工业物联网：信息物理系统、SCADA平台、5G及超越；物联网交互：物联网中的增强现实和虚拟现实（如社交物联网）等。

2024 Impact Factor：2.8

2025 CiteScore：8.0

Time to First Decision：25.5天

Acceptance to Publication：5.3 天

来源：IoT