# 基于网络流量的僵尸网络检测技术的研究与实现

# 摘要

# Abstract

# 绪论

## 1,1 课题研究背景与意义

主要讲述物联网的发展情况及安全现状，进而引出物联网安全的重要性，其中僵尸网络是物联网安全威胁的重要来源，最后陈述僵尸网络检测的意义。

## 1.2 国内外研究现状

主要讲述僵尸网络国内外论文针对僵尸网络检测的研究工作，主要从论文针对的应用场景、僵尸网络检测的思路、方法及效果来分析。

## 1.3 论文主要工作及组织结构

主要陈述论文的主要研究工作和论文组织架构。

## 1.4 本章小结

# 基础理论和相关技术

本章主要介绍僵尸网络检测的相关概念、基础理论以及工程中涉及相关技术的原理。

## 2.1 僵尸网络分类

主要介绍目前主要的僵尸网络分类及其网络结构、特点等。

## 2.2 常见僵尸网络检测方法

本节着重介绍常见僵尸网络检测的主要方法及算法工作原理。

## 2.3 常用流量采集方法

主要介绍网络流量采集相关技术原理及区别，以及本文方案。

## 2.4 深度学习框架

主要介绍深度学习相关技术架构原理、区别及本文采取深度学习方案及本文应用。

## 2.5 可视化技术

主要介绍可视化展示的相关技术，着重介绍框架概念及前后端架构设计。

## 2.6 本章小结

# 第三章 基于深度学习的僵尸网络检测方法

传统机器学习检测僵尸网络方法如支持向量机、随机森林、DBScan、K-means等都需要人为设计特征的问题，检测效果取决于特征设计的合理性，且在进行特征设计的时候往往会忽略一些信息，而基于深度学习的僵尸网络检测方法不需要进行人为选取特征，只要根据深度学习网络所需参数输入原始的网络数据包数据，网络会自动化学习流量中的特征。不仅不会造成因人为设计特征而丢失信息，而且还能对未知攻击进行检测。

表征学习方法、空间特征（CNN）、时间特征（LSTM）、ｋ折交叉验证技术

双向RNN、双向LSTM，同时利用历史和未来的信息。

## 3.1 卷积神经网络与循环神经网络

主要介绍两种神经网络的网络结构、应用场景、功能特点等。再提出本文所要运用的具体的网络类型。

对卷积的意义的理解：

1. 从“积”的过程可以看到，我们得到的叠加值，是个全局的概念。以信号分析为例，卷积的结果是不仅跟当前时刻输入信号的响应值有关，也跟过去所有时刻输入信号的响应都有关系，考虑了对过去的所有输入的效果的累积。在图像处理的中，卷积处理的结果，其实就是把每个像素周边的，甚至是整个图像的像素都考虑进来，对当前像素进行某种加权处理。所以说，“积”是全局概念，或者说是一种“混合”，把两个函数在时间或者空间上进行混合。

## 3.2 基于两阶段神经网络的僵尸网络检测模型

提出基于网络流量时空特征的僵尸网络检测模型（网络结构图/算法流程图），一阶段模型提取空间特征、二阶段时间特征，两阶段特征融合形成最终的网络流特征进行分类判决。

## 3.3 实验结果与分析

实验仿真，运用深度学习中的精度、检测率和误警率评价算法的可用性与正确性。另外还可以和传统机器学习算法或其他深度学习算法加以对比分析。

## 3.4 本章小结

# 第四章 基于网络流量的僵尸网络检测系统的设计与实现

## 4.1 系统需求分析

主要介绍检测系统要实现的功能需求和可用性需求。

功能需求：

1. 系统登录
2. 僵尸网络节点大屏展示，异常个数统计
3. 流量协议展示
4. 流量大小展示
5. 端口统计
6. 流量采集、流量预处理
7. 支持pcap文件分析，pcap文件上传。
8. 僵尸网络分类（如需扩展）

## 4.2 系统总体结构设计

主要介绍系统的框架设计和总体模块设计。

## 4.3 数据包采集模块设计与实现

主要介绍数据包采集模块的采集方案与具体代码实现。（包含输入、输出）

## 4.4 数据包预处理模块设计与实现

主要介绍数据预处理模块所实现的功能，具体处理方案与代码实现。

## 4.5 僵尸网络检测模块设计与实现

主要介绍检测模块如何将第三章算法应用到系统中来实现僵尸网络的检测。

## 4.6 检测结果可视化模块设计与实现

主要呈现在功能设计阶段所要展示的结果，如僵尸网络节点地理分布、感染节点个数统计、僵尸网络类别统计、僵尸网络异常详情等。

## 4.6 本章小结

# 第五章 僵尸网络检测系统测试与分析

本章主要介绍检测系统部署、测试验证可用性和鲁棒性。

## 5.1 系统实验环境

介绍系统部署的硬件环境，数据来源等。

## 5.2 系统测试实施步骤

测试案例及测试结果。

## 5.3 本章小结

# 第六章 总结与展望

本章主要总结本文相关工作，指出相关工作要点，列举本文主要贡献，本针对本文不足或以后可能的研究方向进行展望，比如数据集来源于真实环境，研究面扩大（研究网络的其他安全威胁检测），目前只针对网络流量进行了研究，未来可结合设备状态和日志审计等关联分析，实现僵尸网络可控（应急响应快速处置）等。