中国民航大学
Civil Aviation University of China

基于机器学习的僵尸网络检测技术研究

吴优

学科专业名称：航空工程
指　导 教 师：顾兆军 教授

2018-09-29

报告内容

1. 课题研究背景
2. 国内外研究现状
3. 研究内容
4. 研究方案
5. 拟解决的关键问题
6. 前期研究成果
7. 工作计划

1. 课题研究背景

1.1 当前网络环境

早期的互联网环境相对简单，仅依赖端口信息就可以对流量进行有效的分类监管。而当前网络环境主要有以下特点：

- 数据量庞大、结构复杂
- 存储大量有价值信息
- 安全威胁普遍存在
- 技术发展变化十分迅速

网络安全问题日益突出，网络环境的治理和监管措施亟待加强。

1. 课题研究背景

1.2 僵尸网络的影响

僵尸网络是指由攻击者集中操控的主机集群，可以用来实施大规模的网络攻击，其主要特点有：

- 规模可不断扩展，需要一段时间进行部署
- 对受控主机影响较小，不易发觉
- 攻击行为影响巨大

近年来发生了多起利用僵尸网络实施的大规模攻击事件，造成了巨大损失，有必要加强相应防护工作。

1. 课题研究背景

1.2 流量分析技术的发展现状

目前广泛使用的分析技术是深度包分析（DPI），该方法从数据包中提取序列规则，利用该序列对流量进行匹配分类。

该方法的主要有以下局限性：

- 需要存储大量特征库
- 匹配速度受限
- 依赖人工分析，无法及时更新
- 涉及用户数据隐私

基于机器学习的流量分析方法能有效解决上述问题。

2. 国内外研究现状

基于机器学习的分类方法最早在2004提出。

2005年，剑桥大学的Moore等人进行了流量采集工作，并提出了248种可用于机器学习的流量特征，最后使用朴素贝叶斯算法对流量进行了分类

之后基于机器学习的流量分类方法受到了广泛关注，并不断发展，之后被用于威胁检测中，并2006年Livadas等人首次将机器学习应用在僵尸网络的检测上。

国内的互联网发展较晚，因此在该领域相对落后，机器学习在网络安全领域的应用研究较少。2013年才开始将神经网络用于检测僵尸网络。

3. 研究内容

目前对僵尸网络已经有较多研究成果，但目前仍存在以下问题：

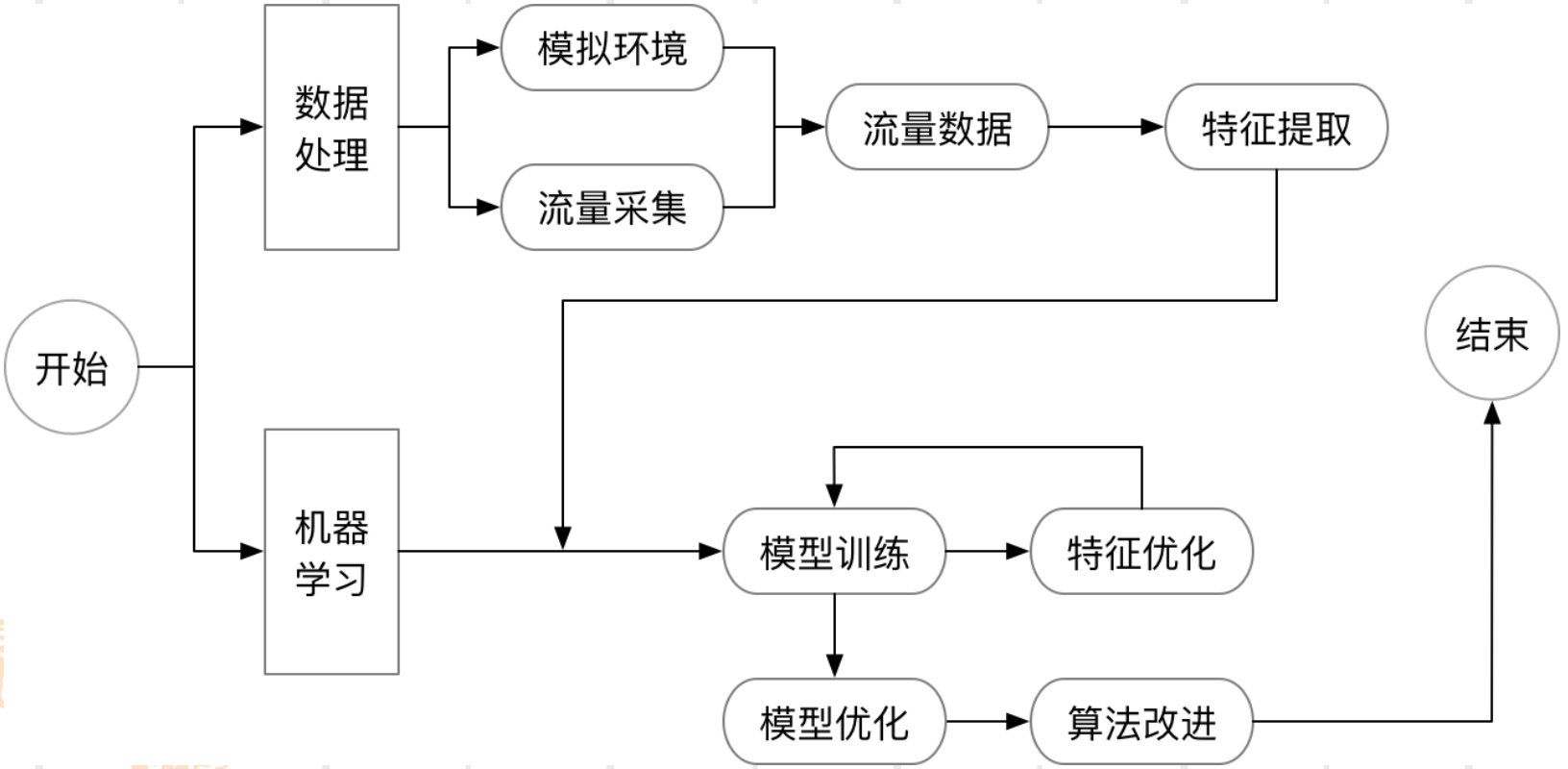
- 目前大多研究成果主要针对传统的僵尸网络，传统僵尸网络通常由一台主机直接控制，从而更加容易防治。而新型僵尸网络的行为更加复杂，因此需要提出更加灵活的检测方法。
- 由于网络环境的多变性，对机器学习算法提出了更多要求，其使用方式也不同于其他领域，因此寻找更加合适的算法以及数据特征是一个关键问题。

本文研究的主要内容是通过搭建模拟的僵尸网络环境进行流量的采集，并利用机器学习算法将其与正常流量进行区分。

4. 研究方案

4.1 研究流程

课题的主要研究流程如下图所示



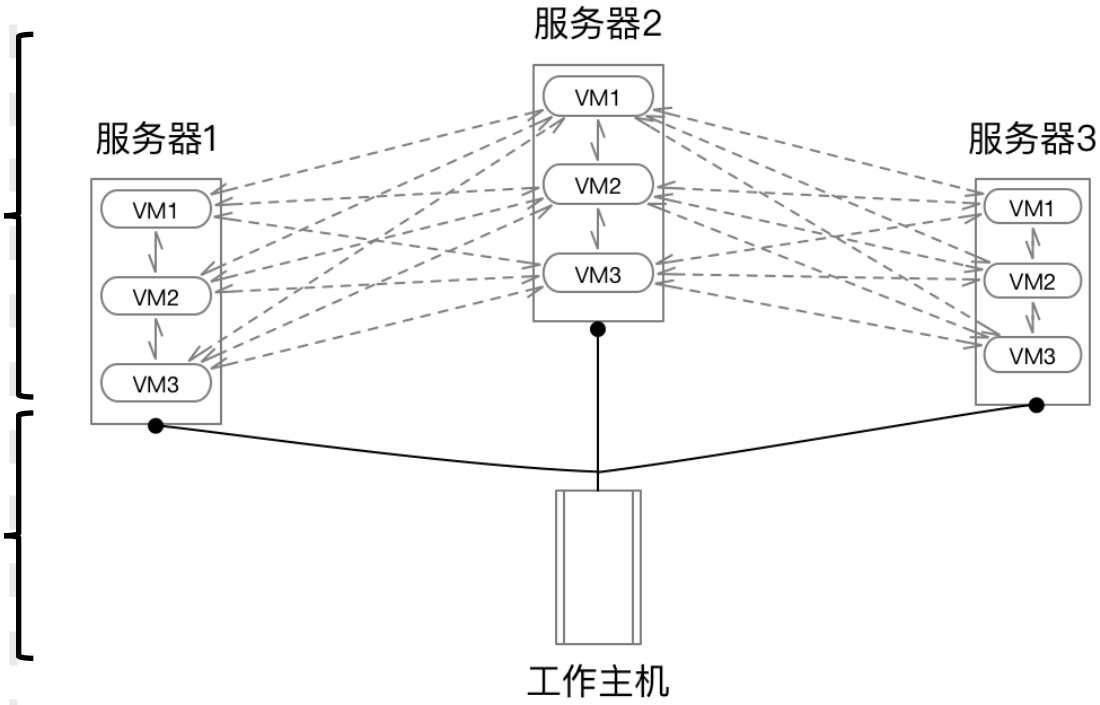
4. 研究方案

4.2 数据收集和处理

通过对现实网络环境的模拟，可以收集到符合研究目的的的流量数据，模拟网络结构如图

搭建多虚拟机模拟环境，产生流量数据

收集汇总并在工作主机对数据进行处理

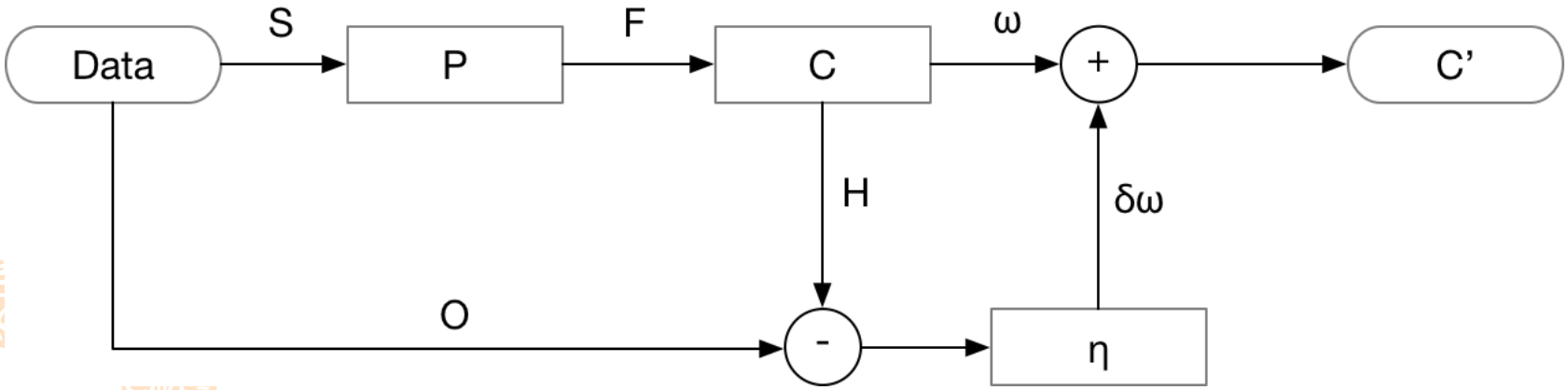


4. 研究方案

4.3 算法优化和改进

该部分主要有以下工作内容，过程如下图所示:

1) 将各类机器学习算法进行对比，并选择效果最佳的算法
2) 对所使用的数据特征进行优化，并对算法的参数进行调整
3) 结合相关专业知识和算法理论，对分类方法进行改进，并验证其有效性



5. 拟解决的关键问题

1) 僵尸网络活动环境、行为方式的模拟仿真，生成可用数据

2) 进行数据的收集和处理，从流量数据中提取可用特征，并进行优化

3) 选择机器学习算法进行优化和改进，实现对僵尸网络流量的有效识别

6. 前期研究成果

6.1 算法对比

为了评价算法的效果，首先需要选定明确的评价指标，本文决定使用一下指标，各指标均可根据如下所示的混淆矩阵计算得到

- 准确率（Accuracy）

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

- 精确率（Precision）

$$\text{Precision} = \frac{TP}{TP+FP}$$

- 召回率（Recall）

$$\text{Recall} = \frac{TP}{TP+FN}$$

		True class: p	True class: n
Hypothesis output	Y	TP (True Positives)	FP (False Positives)
	N	FN (False Negatives)	TN (True Negatives)
Column counts:		P_C	N_C

6. 前期研究成果

首先我们利用了现有的流量数据，对一些根据所确定的上述指标，利用现有数据，对常用机器学习算法的效果进行了初步对比，并对数据特征进行了一定分析：

- 确定了248种特征中的前30个最优特征用于后续研究
- 相对于传统的机器学习算法以及深度学习算法，集成机器学习的方法更适用于网络安全问题
- 试验了传统的DPI分析方法，后续可能将其与机器学习结合从而形成新的算法

7. 工作计划

时 间	内 容
2018年9月~11月	查找并阅读与课题相关的文献，学会如何使用Python的各类API实现相关功能
2018年12月~2019年2月	研究僵尸网络的主要运作方式，并在实验室中搭建模拟环境，用于模仿僵尸网络的行为，并收集网络流量，获取可用数据。
2019年3月~4月	完成数据的预处理工作，并对比不同算法的效果。编程实现数据分析工具，进行特征优化工作并确定最终使用的特征集合，之后利用该特征集合进行算法模型的调优工作。
2019年5月~7月	算法优化，综合考虑数据和算法的特点，进行有效的理论分析，并进行现有分类方法的改进，并通过实验对比改进方法和原方法的分类效果，以验证方法的有效性
2019年8月~12月	工作总结，撰写学位论文，以及发表小论文

致谢

谢谢，敬请批评指正！