南京郵電大學
Nanjing University of Posts and Telecommunications

个人学习情况汇报
2024.4.21

汇报人：徐方泽

目 录

01

文献阅读

Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection

《紧张的军备竞赛:当前恶意软件威胁的概述及其检测趋势》

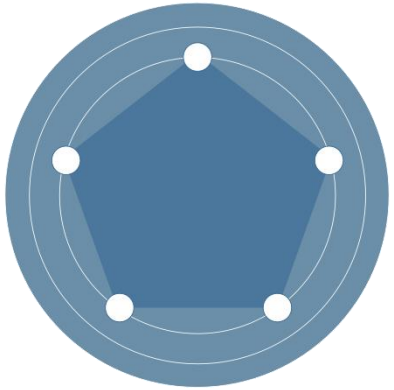
Caviglione L, Choraś M, Corona I, et al. Tight arms race: Overview of current malware threats and trends in their detection[J]. IEEE Access, vol. 9, pp. 5371-5396, 2021.

恶意软件检测的方法

（3）基于启发式的方法

（2）基于行为的方法

（4）基于能量的方法

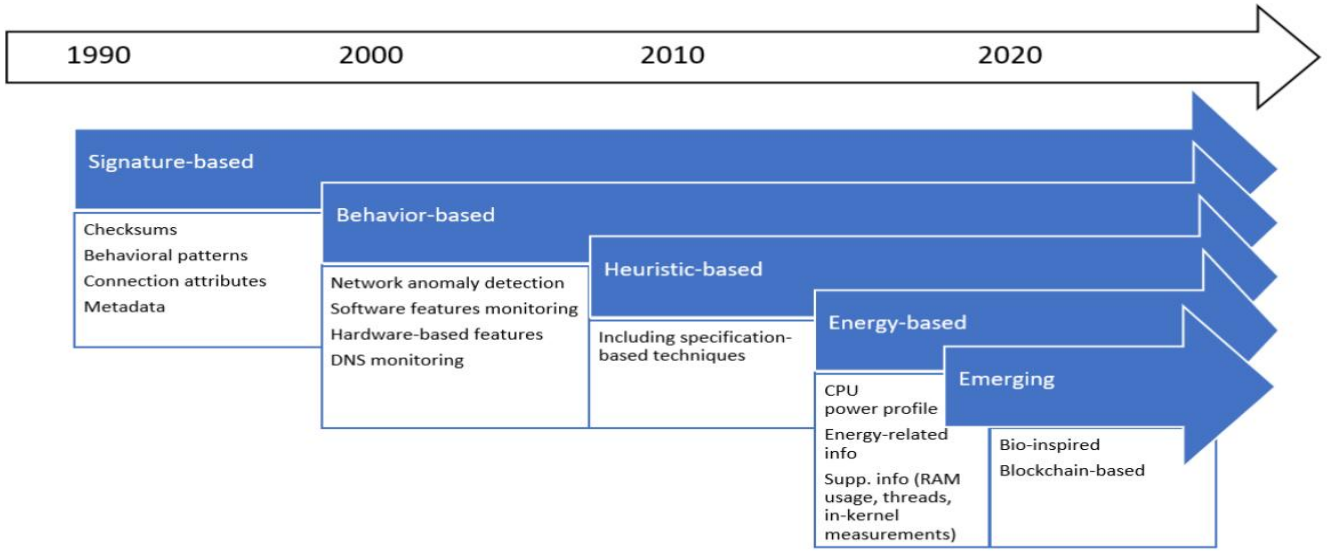


（1）基于签名的方法

（5）新型方法(生物启发、基于区块链)

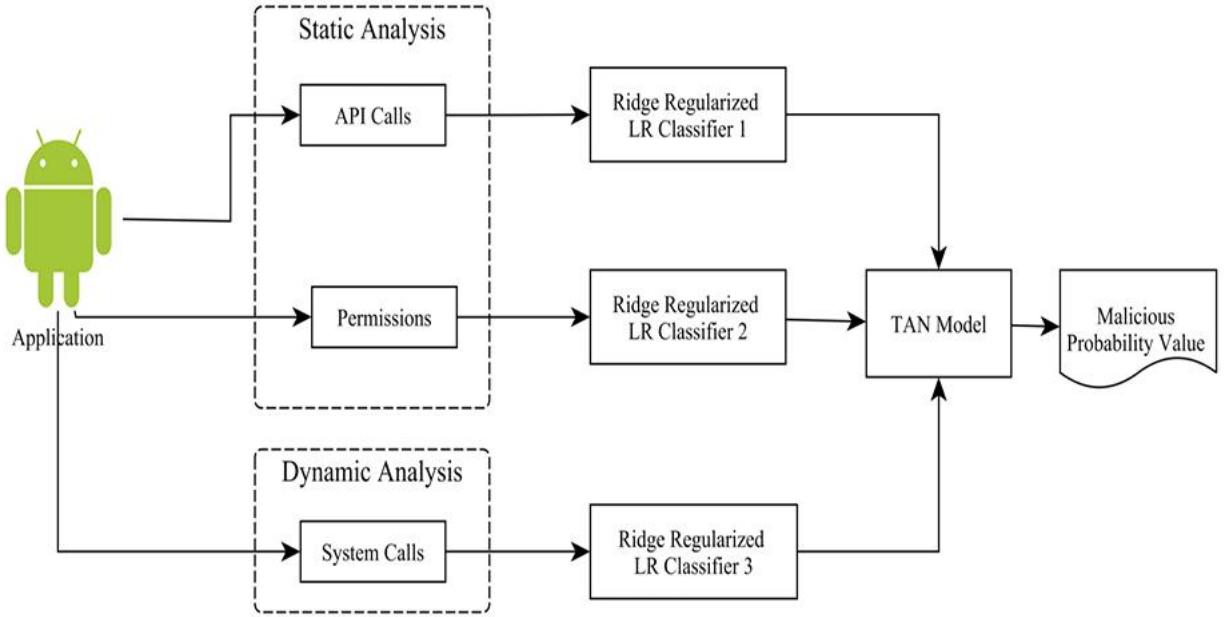
恶意软件检测的发展趋势

针对已知的威胁，几十年前开发的检测技术（例如，基于签名的技术）仍在使用。然而，为了应对隐藏的、模糊的和复杂的攻击，出现了更新的、更复杂的方法（例如，生物启发的或基于能量的）。



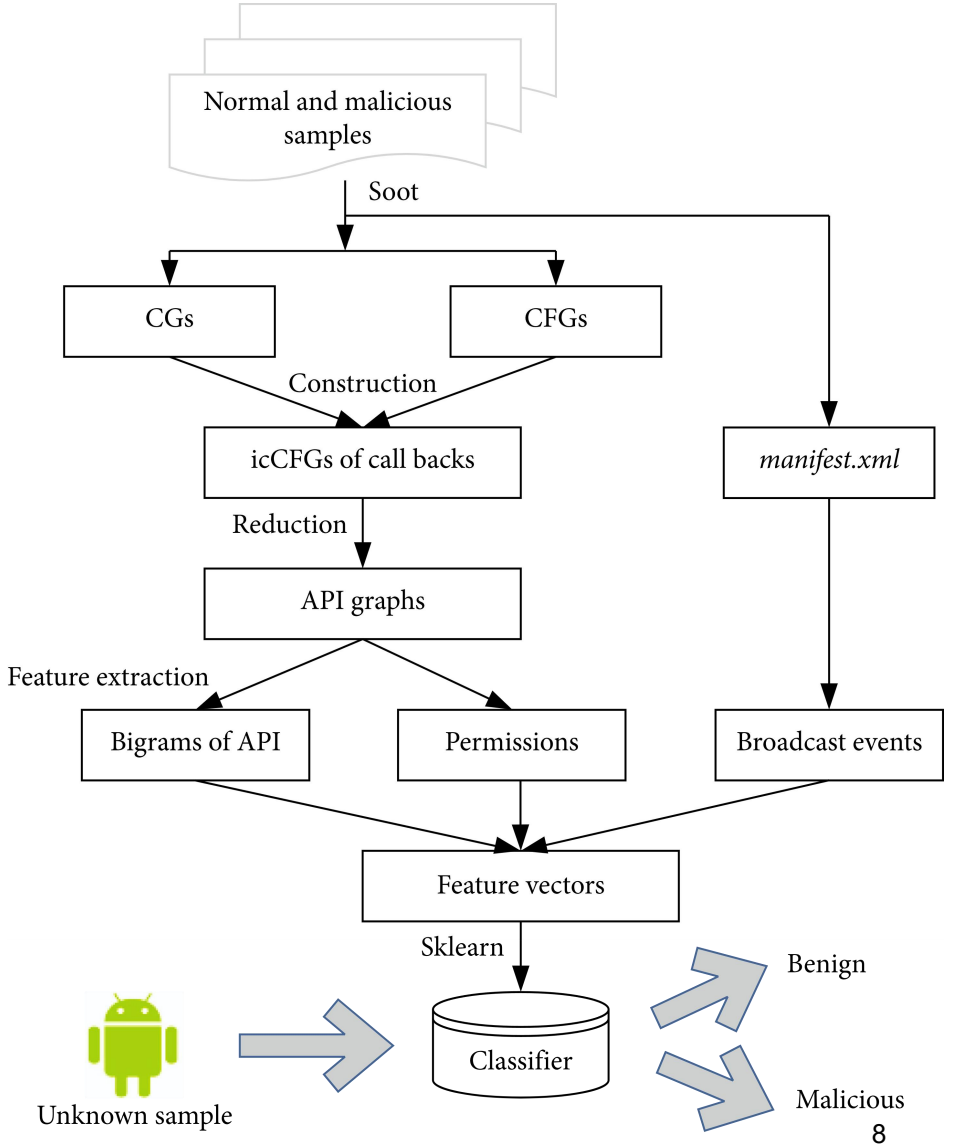
浅层机器学习算法

由于恶意软件检测通常是一项分类任务，因此使用了各种经典的基于机器学习的分类器，如逻辑回归，支持向量机，k-近邻(k- nn)，决策树，rf ， Naïve贝叶斯分类器。它们在各种特征空间中运行，包含静态特征，如字符串(例如，文件名，代码片段)，N-grams, API调用，熵，恶意软件表示为灰度图像，函数调用图(fcg)， cfg或动态特征。



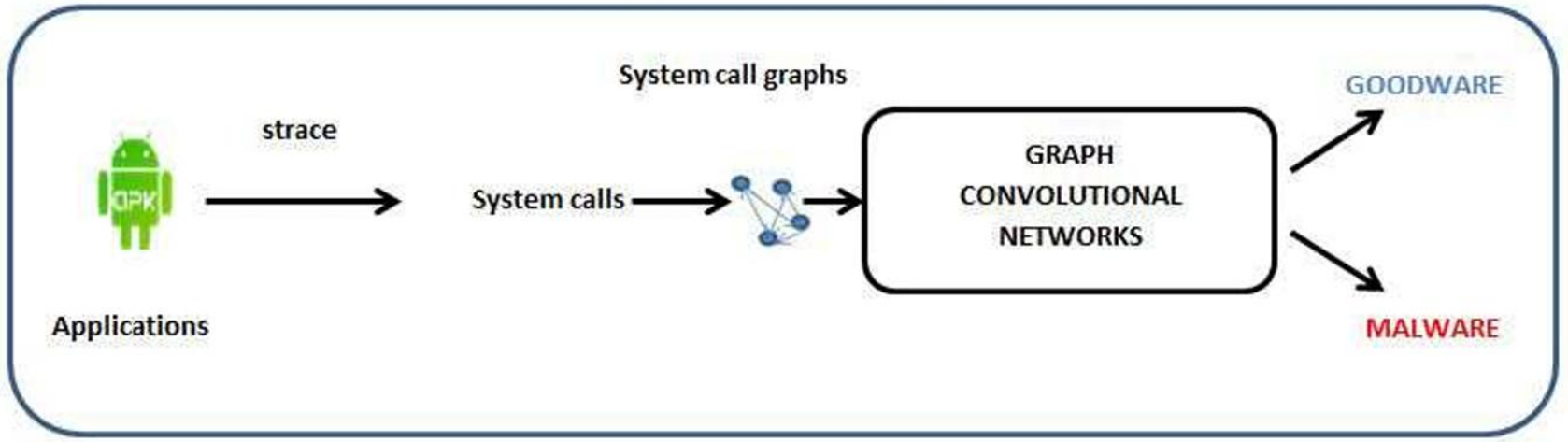
研究浅层机器学习的新特征

在机器学习中，特征的选取对于最后的训练结果起着关键的作用，原先提出的各种特征已经不能完全满足各种新场景下的需求，许多新的特征被提出。如使用应用程序接口调用转换矩阵(API-CTM)来生成网络拓扑并分析各种网络指标以提取特征。将数据字节转换为音频信号，并使用声学特征空间:mel-frequency倒谱系数(MFCCs)在音频信号中搜索相似的模式。或者基于图的Android应用程序特征生成方法。将原始特征及其上下文结合在一起，生成比原始特征拥有更丰富语义信息的新特征等。



利用深度学习研究新特征

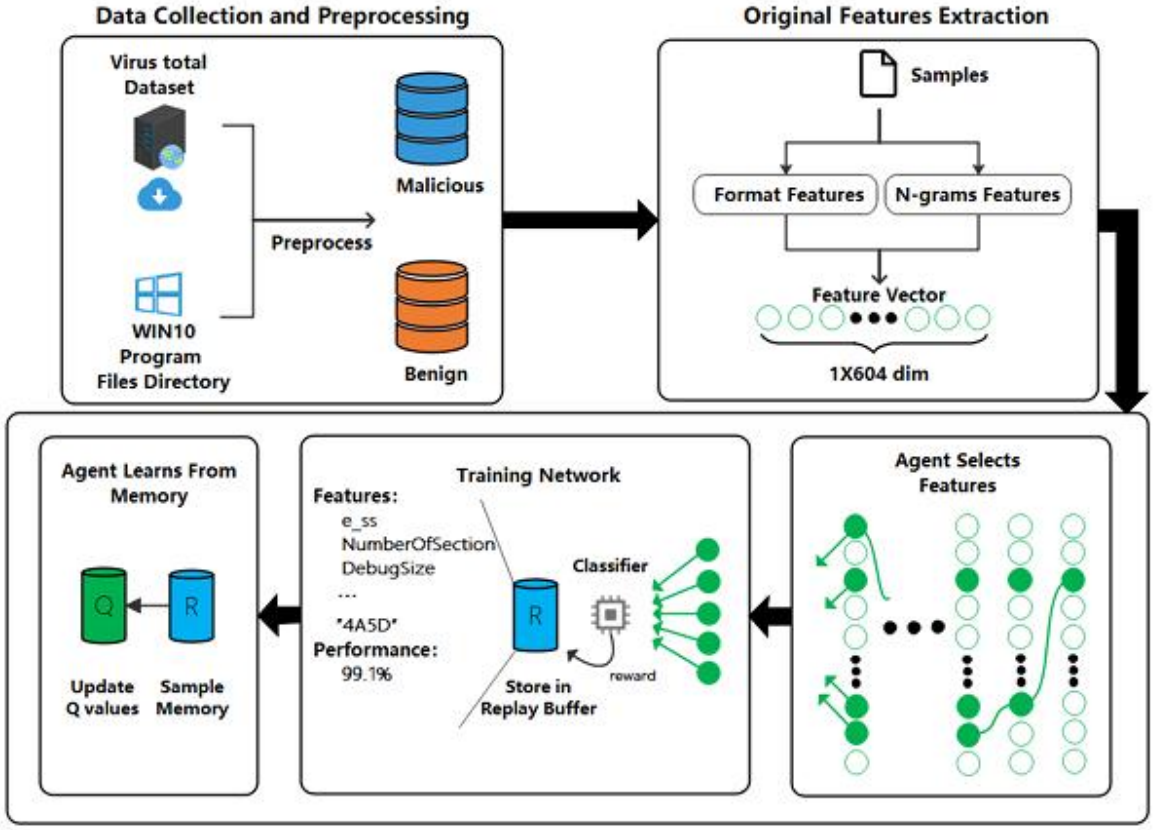
自2010年代初以来，恶意软件检测采用了多种深度神经网络(dnn)架构:多层感知器(mlp)、递归神经网络(rnn)或卷积神经网络(cnn)、卷积递归神经网络(crnn)、自动编码器和长短期记忆(LSTM)模型。举例来说，有将系统调用建模为图来帮助捕获系统调用之间的结构依赖关系。使用扩展的深度学习模型图卷积网络(GCN)，设计一种基于GCN的新型Android恶意软件动态检测机制，该机制使用图的中心性度量作为输入特征。



恶意软件检测

利用深度学习研究新特征

最近，带有强化学习(DRL)的深度学习已经被证明可以有效地用于恶意软件检测。在[1]中，作者提出了一种在云环境中高效检测恶意软件的基于drl的方法。该方法能够在降低成本的同时实现接近最优的检测率。一种基于drl的方法也被用于了解最新恶意软件变体的实时特征分布和特征选择过程[2]。



[1]Birman Y, Hindi S, Katz G, et al. Cost-effective malware detection as a service over serverless cloud using deep reinforcement learning[C]//2020 20th IEEE/ACM international symposium on cluster, cloud and internet computing (CCGRID). IEEE, 2020: 420-429.
[2] Fang Z, Wang J, Geng J, et al. Feature selection for malware detection based on reinforcement learning[J]. IEEE Access, 2019, 7: 176177-176187.

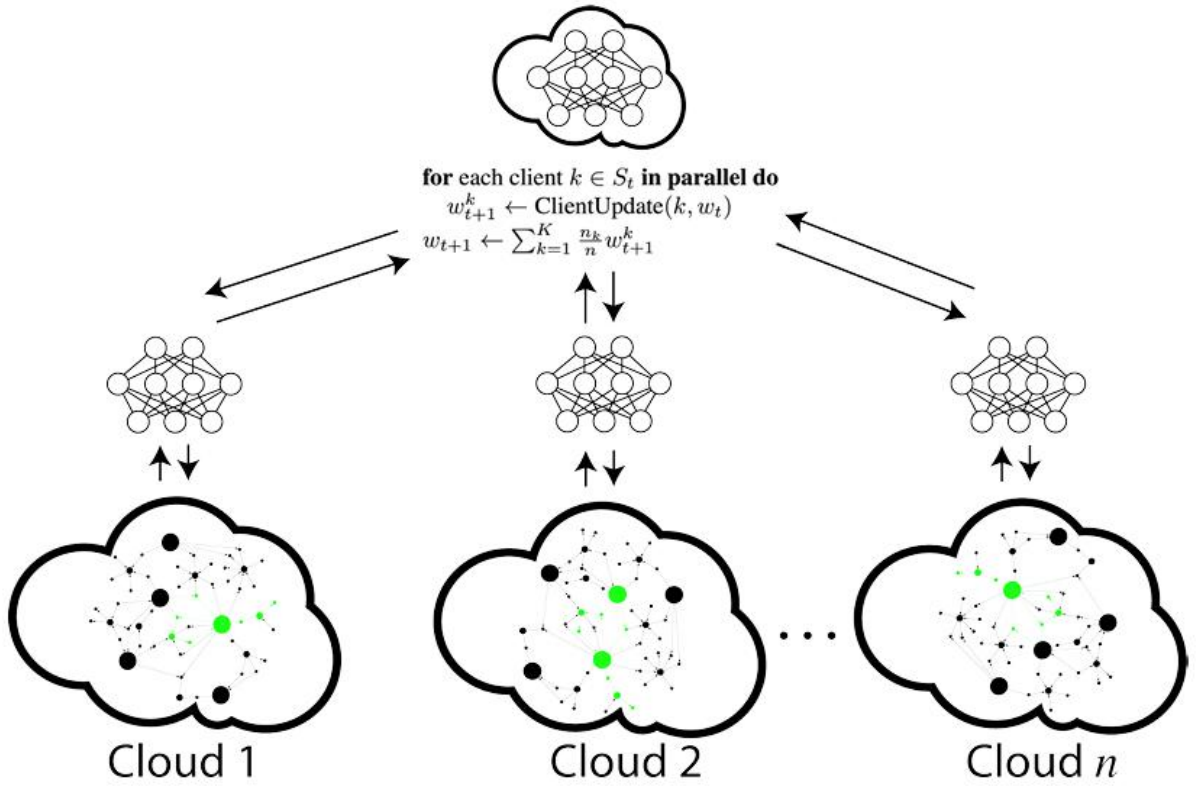
集成分类器

集成分类器在恶意软件检测中的成功应用呈现增长趋势。集成方法的目标是将几个基本模型组合成一个强大的模型，以提高输出模型的准确性。一般来说，集成模型属于三种类型之一:顺序、并行和堆叠。

- **顺序方法**(如boosting):模型是按顺序生成的，试图在学习过程中通过重新加权错误分类的例子来改善结果。
- **并行方法**(如bagging):在数据集的不同样本上训练几个模型后，使用投票或对结果进行平均，
- **堆叠方法:**在对基本模型的输出进行训练的同时，将不同基本分类器的决策组合在一起。

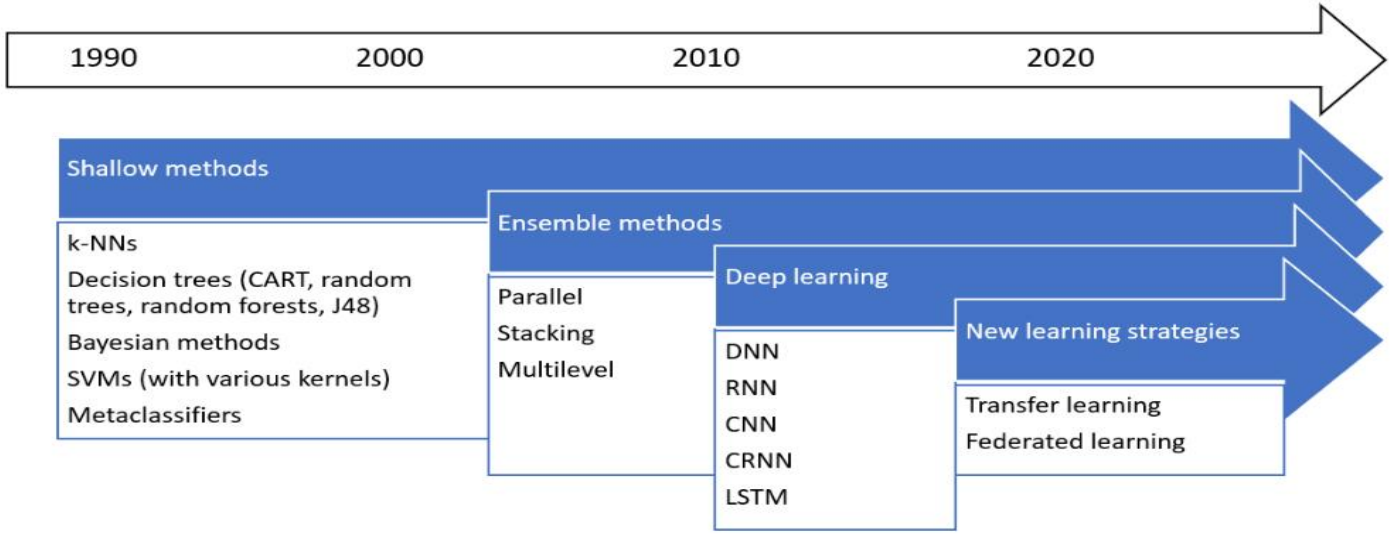
应对安全挑战的机器学习

为了保证机器学习训练数据的隐私性，提出了一种联邦学习机制。这种分布式ML的概念被用于多云环境中，在多云环境中，多个云协同工作以防止恶意软件的传播，而不会暴露敏感信息。



机器学习应用于恶意软件检测的演变

尽管浅层方法仍在使用并且通常会产生良好的结果，但深度神经网络正快速发展。复杂的神经架构往往会取代特征工程过程，因为深度神经网络是由原始输入驱动的。目前集成分类器和新训练方法（如迁移或联邦学习）也得到了较多关注。

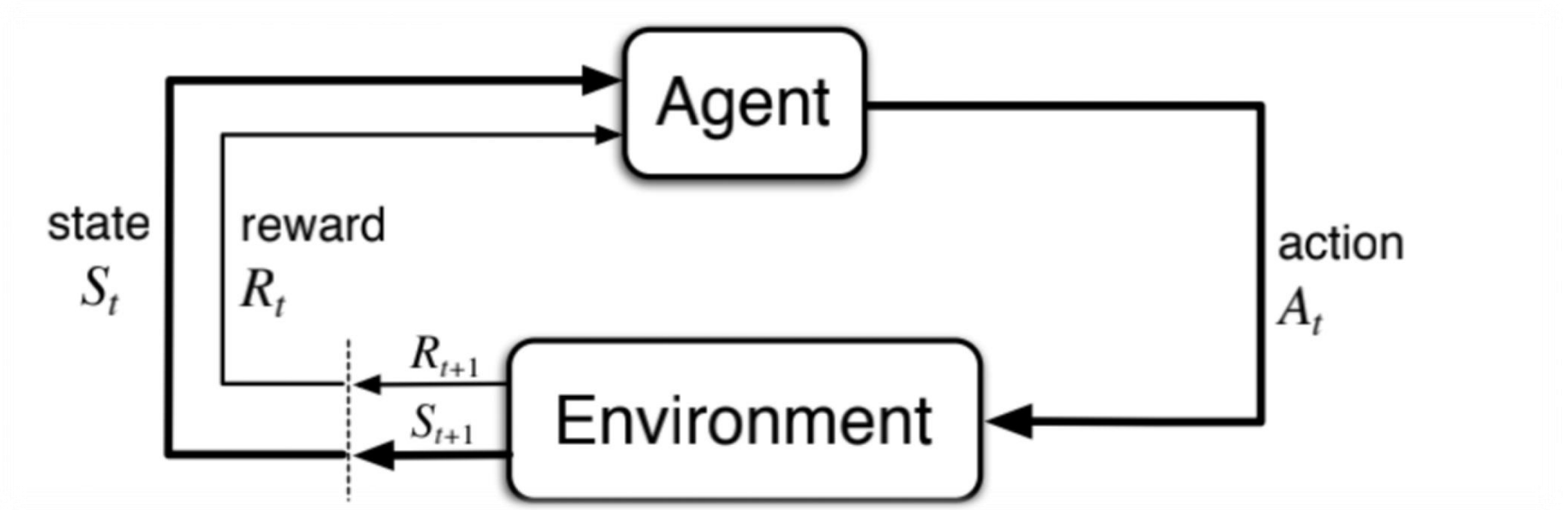


02

当前重心

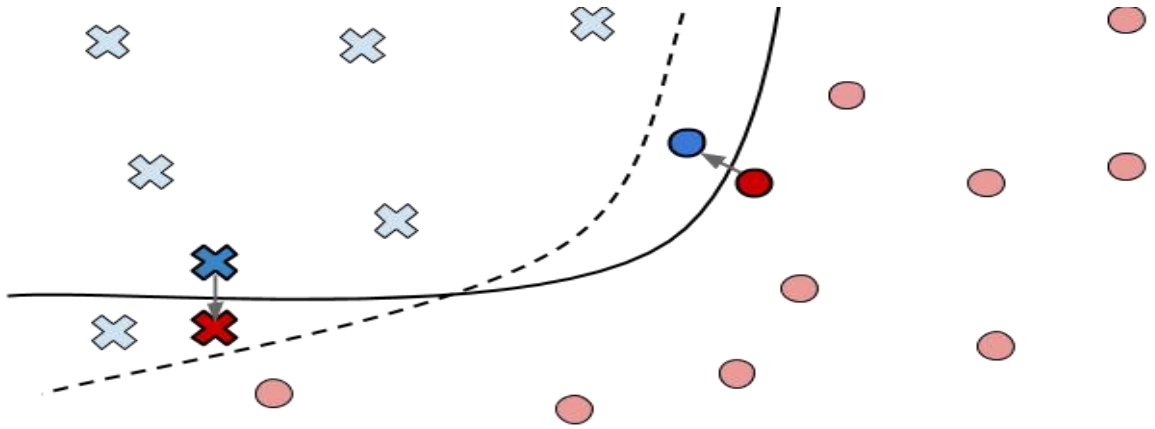
马尔科夫过程与强化学习

- 马尔科夫性：下一个状态仅与当前状态有关，与之前状态无关
- 马尔科夫决策过程：描述了Agent与环境之间的交互过程，其中状态转移满足马尔科夫性
- 马尔科夫决策过程是强化学习的基本框架



任务：恶意软件**对抗样本**

- **状态*S***：恶意特征“位置”等
- **动作*A***：加入空指令等
- **奖励*R***：让杀软误判等
- **状态转移概率*P***：根据S和A，转变到到下一状态的概率



03

个人专利

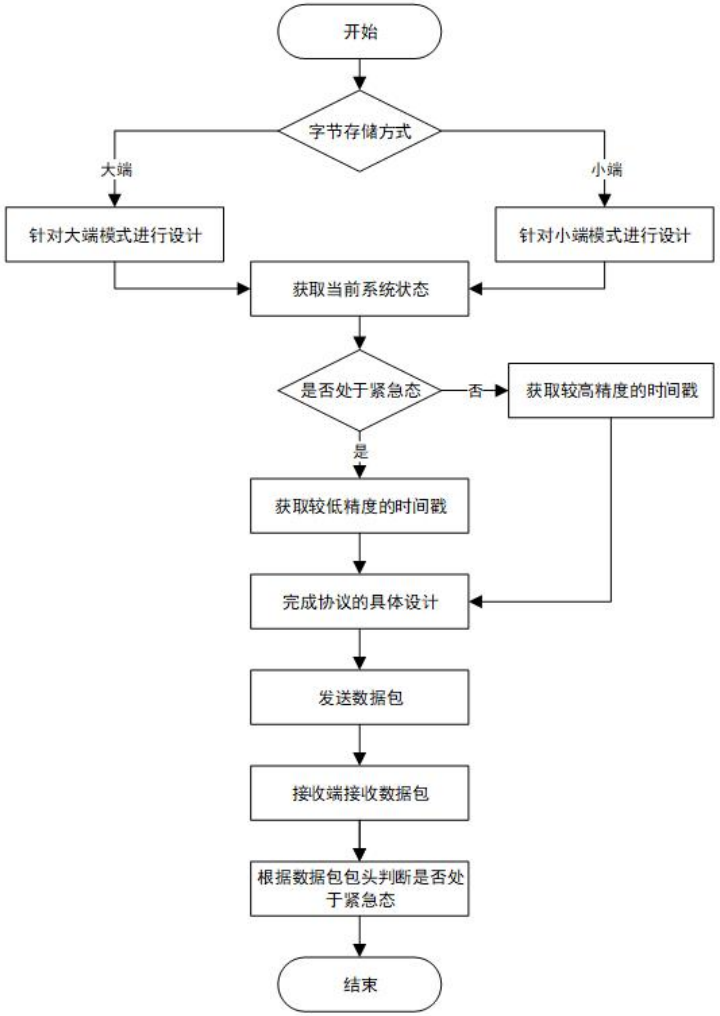
《一种基于时态弹性协议的智能电网通信方法》

■ 方案简介

本时态弹性协议考虑到现有协议在智能电网场景下存在时间精度不足和状态位冗余的问题，将原有32位时间戳拓展至61位、6个状态位缩减至3个，解决了无法精准控制和信息浓度过低的问题。实现高精度时间控制和低通信代价。

■ 基本流程

考虑不同接收端的字节序排序方式，设计相应的时态弹性协议；控制中心判断当前智能电网，决定获取时间戳的精度；完成整个数据包包头部分的时态弹性协议字段设计；接收端接收到相应数据包包头后，分析时态弹性协议字段，第一时间得知紧急状态下的命令转发。



专利介绍

南京邮电大学 Nanjing University of Posts and Telecommunications

■ 具体协议

数据帧格式具体为1比特的紧急指针，2比特的状态位和61比特的时间戳；考虑接收端的大小端，设计了不同模式下的时态弹性协议，保证了接收端存储的一致性。

■ 创新点

结合智能电网的实际通信情况，提高数据包中的信息浓度、降低了通信代价；基于64位寄存器的时间戳、状态和紧急指针的存储和处理方案，实现微秒级的时间敏感，达到精准控制的目标。

Byte1	bit1	紧急指针	1代表是紧急状态，0代表非紧急状态
	bit2-bit3	状态位	01代表校正态，10代表预防态
	bit4-bit8	时间戳	存放获取到的61位时间戳的1-5位
Byte2	时间戳		存放获取到的61位时间戳的6-13位
Byte3	时间戳		存放获取到的61位时间戳的14-21位
Byte4	时间戳		存放获取到的61位时间戳的22-29位
Byte5	时间戳		存放获取到的61位时间戳的30-37位
Byte6	时间戳		存放获取到的61位时间戳的38-45位
Byte7	时间戳		存放获取到的61位时间戳的46-53位
Byte8	时间戳		存放获取到的61位时间戳的54-61位

URG	表示紧急状态的命令
ACK	表示确认收到请求
PSH	表示推送操作
RST	表示连接复位请求
SYN	用于建立连接
FIN	表示发送端已达到数据末尾

2144895	L1_127_P221_ZT	100	5/3/2024 08:28:39
2144896	L1_127_P221_CDZ	0	5/3/2024 08:28:39
2144897	L1_127_P221_FDZ	0	5/3/2024 08:28:39
2144898	L1_127_P221_SOH	100	5/3/2024 08:28:39
2144899	L1_127_P221_SOC	100	5/3/2024 08:28:39
2145111	L1_127_P221_ZT	513	5/3/2024 08:28:41
2145112	L1_127_P221_PL	4997	5/3/2024 08:28:41
2145113	L1_127_P221_ZLDL	-2	5/3/2024 08:28:41
2145114	L1_127_P221_ZLDY	23	5/3/2024 08:28:41
2145115	L1_127_P221_YG	0	5/3/2024 08:28:41

感谢观看