南京郵電大學
Nanjing University of Posts and Telecommunications

个人学习进展汇报
2024.6.10

2024.1-2024.6

汇报人：唐俊

CONTENT

南京郵電大學
Nanjing University of Posts and Telecommunications

01

专利

专利介绍

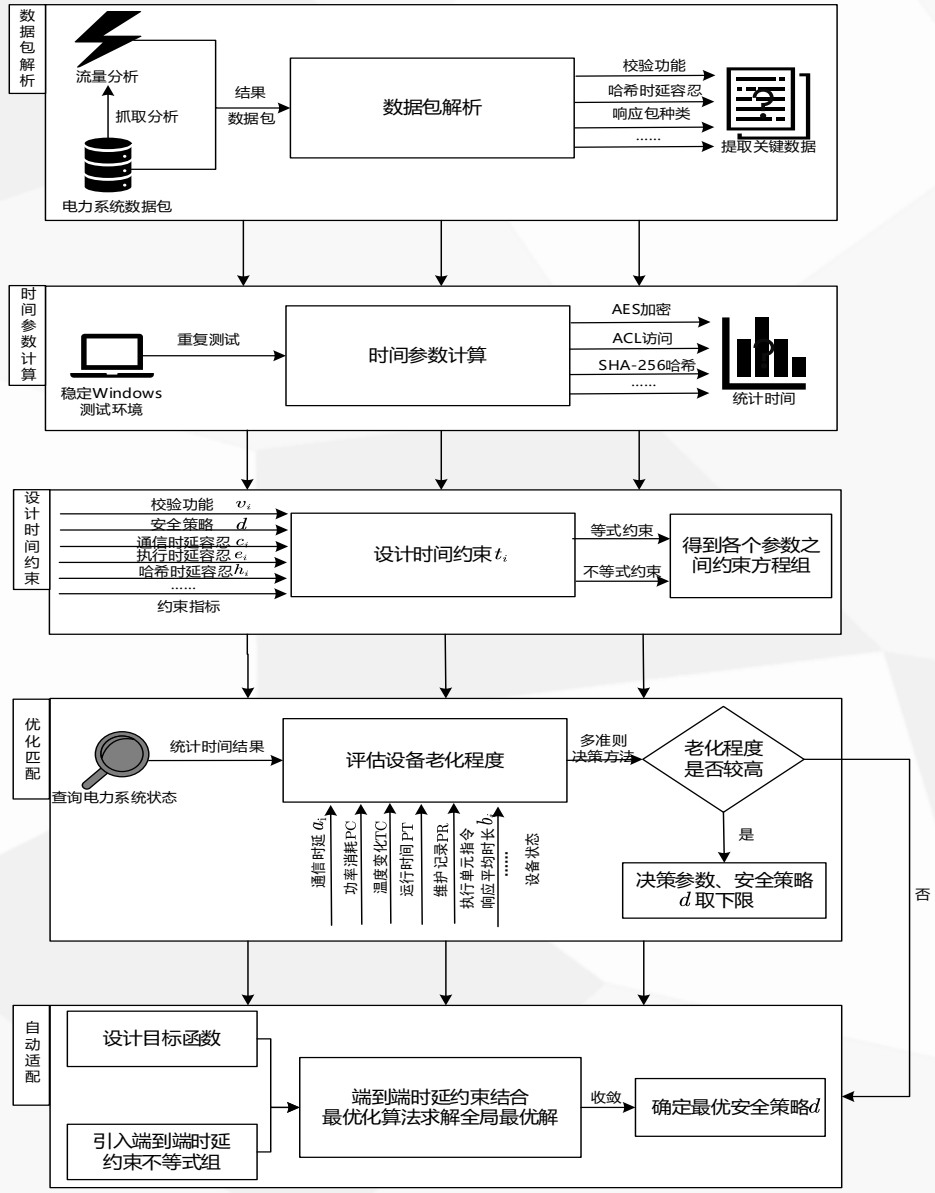
《一种基于端到端时延约束的电力系统安全策略适配方法》

方案简介

本发明提供了一种基于**端到端时延约束**的电力系统安全策略适配方法，通过统计电力系统内数据包，将目标信息转为时间参数，使用梯度下降算法确定最优安全策略。在正常状态下，根据设备老化状况从**安全策略下限**调整以节约能源；在异常状态下，根据各设备的最优策略确定系统的最优安全策略，实现自动适配。

基本流程

数据包解析，分析系统运行决策数据包；时间参数计算，决策数据转换为具体时间参数；设计时延约束，确定设备时延约束条件；优化匹配，统计设备的实时状态，评估老化状况；自动适配，依据目标时延选择**最优安全策略**。



专利整体流程图

专利介绍

具体算法

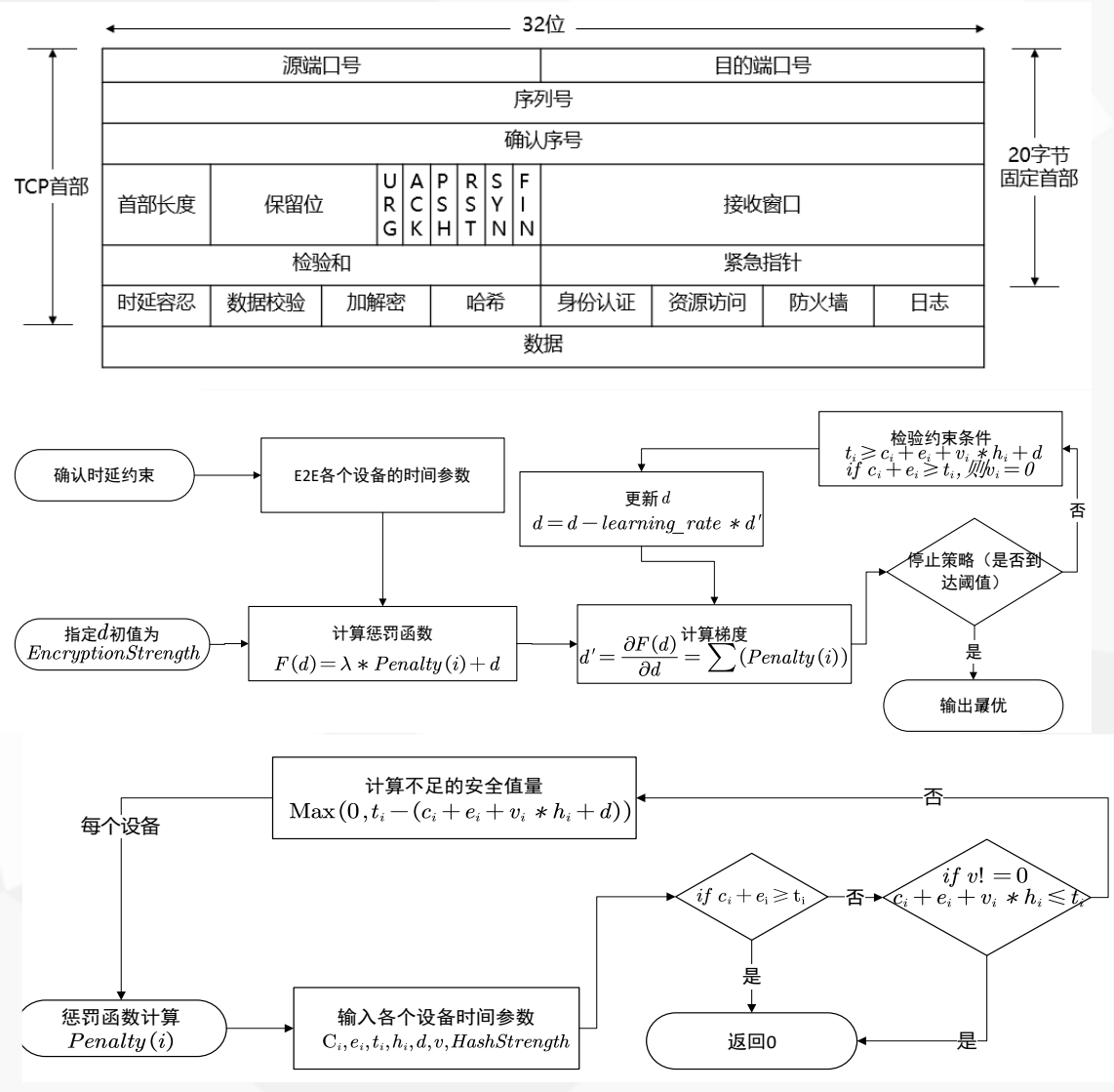
$F(d)=\lambda * \Sigma Penalty(i)+d$ 是目标函数， 其中 λ为惩罚系数，$Penalty(i)$ 是针对各个电力设备不满足安全策略时的惩罚项。参数 $t_1, c_1, e_1, v_1, h_1, d$ 分别表示设备的时延容忍、通信时延容忍、执行时延容忍、校验功能标志、哈希时延容忍以及安全策略。

创新点

动态适配：利用数据包时间参数和梯度下降算法动态优化安全策略，增强系统可控性和实时适应能力。

设备老化评估：综合多项指标优化设备运行策略，减少资源损耗，提高经济可靠性。

综合安全策略：基于时延约束，建立线性不等式组和线性组合目标函数，确保设备稳定性，提升安全策略适配能力。



数据包设计图、算法流程图

南京郵電大學
Nanjing University of Posts and Telecommunications

02

毕业设计

系统设计

《面向微电网智能设备的攻击防御技术研究》

✓智能微电网系统脆弱点分析

依据CPS常见网络安全攻击模式分析和查阅思科路由器路由器安全公告，利用动态和静态文件分析，找出智能设备漏洞点，并对局域网内部进行端口扫描，评估**智能微电网系统脆弱点。**

✓模拟微电网系统搭建

根据现代微电网的基本结构图，搭建**以路由器为中心**的简易微电网系统并完成系统模拟。

✓构建APT攻击链

依据ATT&CK矩阵，分析攻击者战术和技术，对APT攻击进行逆向分析，构造**APT攻击链。**

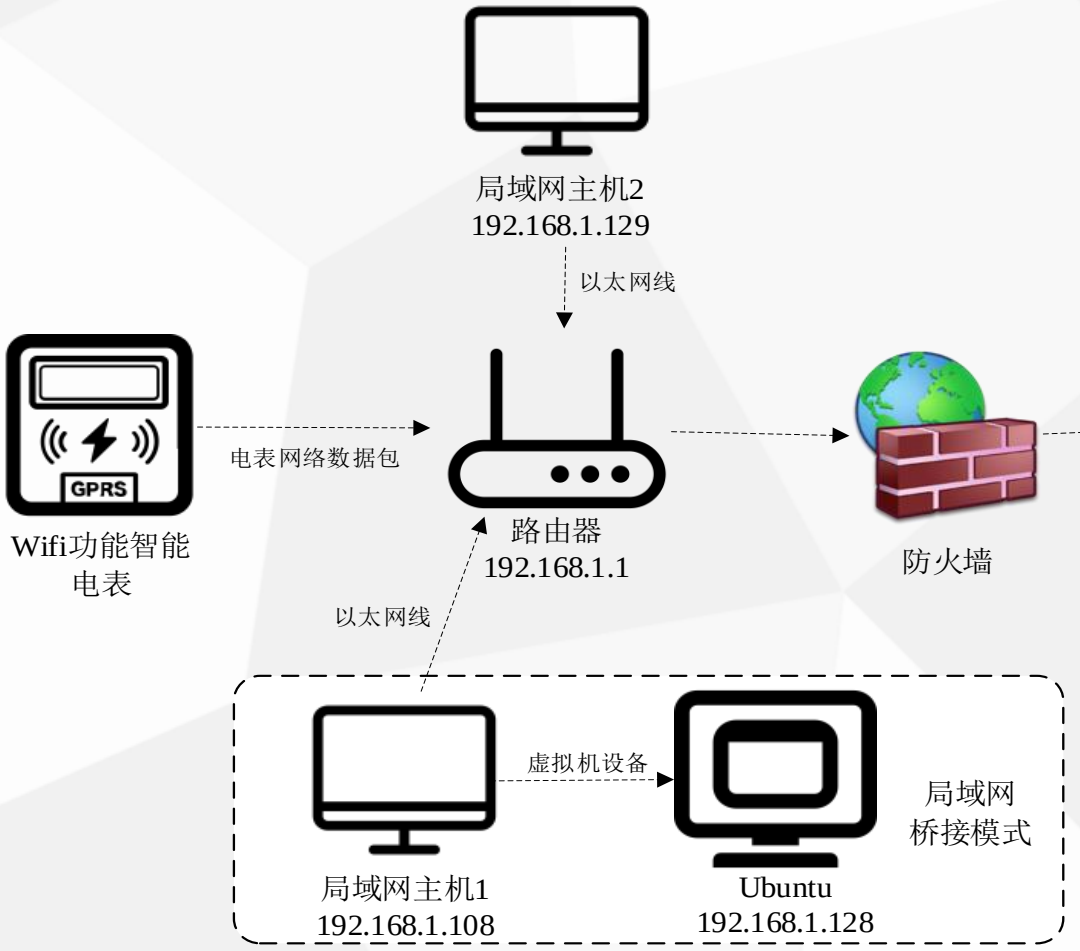
✓ATT&CK框架模拟APT攻击

在微电网系统模拟**APT攻击**者的行为和技术，包括固件逆向、API调用链分析和攻击实现。

✓APT主动防御策略实现

根据ATT&CK框架分析，采取基于主机和网络的主动防御策略。

模拟系统

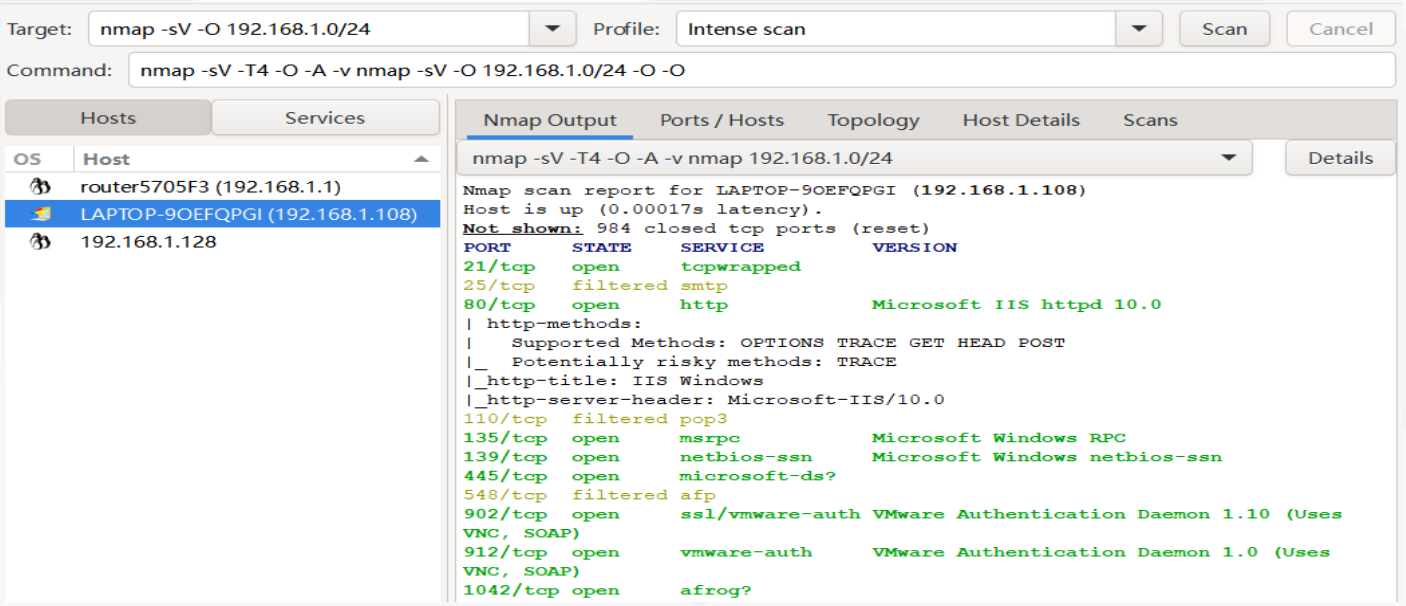


简易智能微电网系统架构

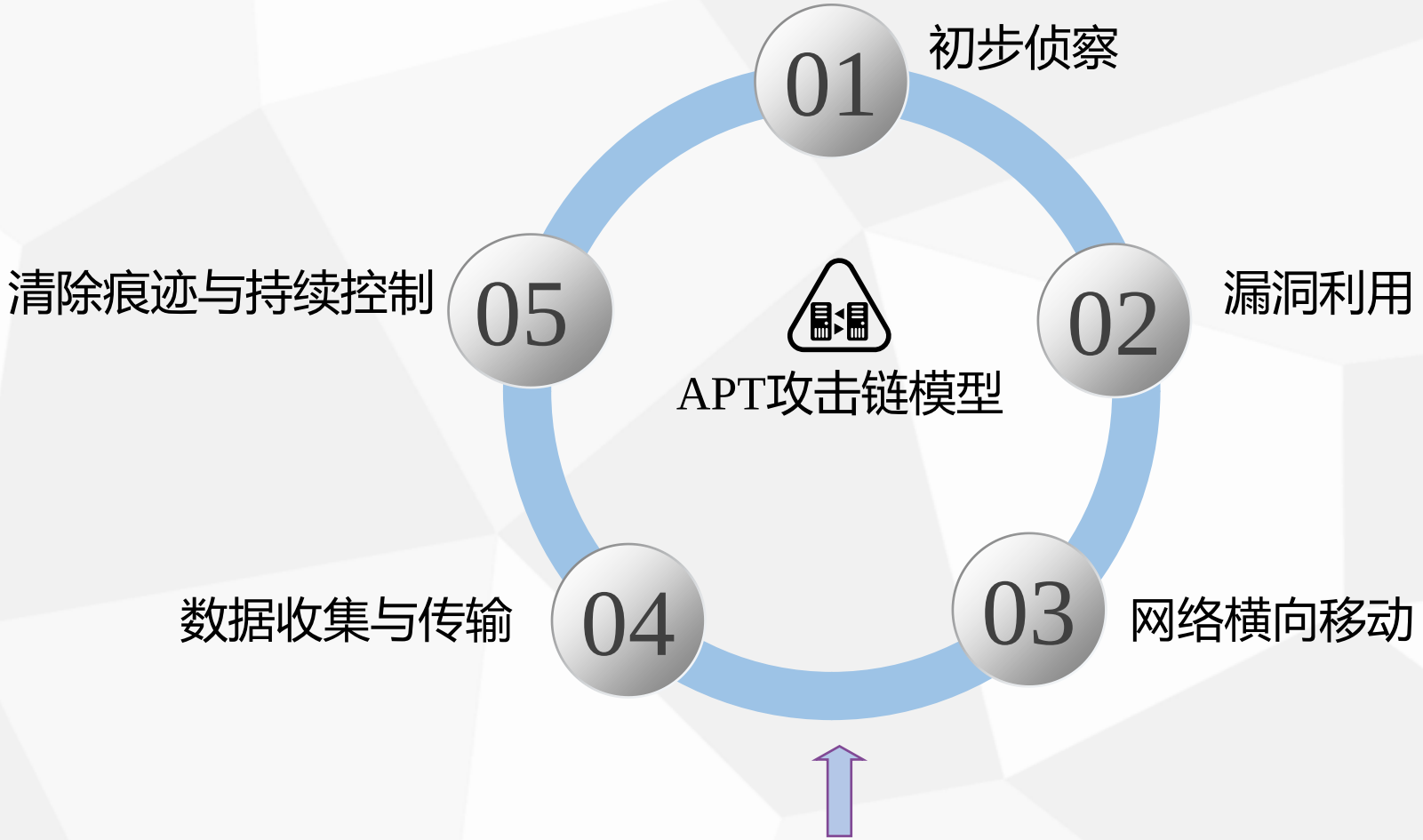
局域网网关IP：192.168.1.2

子网掩码：255.255.255.0

局域网网段：192.168.1.1-192.168.1.255



攻击链模型



优点：

划分攻击阶段，增强攻击模拟的系统性。

针对每个阶段设计具体的攻击方法和工具。

ATT&CK将APT攻击技术划分为了14个战术，导致对APT攻击过程划分过于繁琐，使得攻击的流程不易于分析，可以将攻击流程根据攻击阶段划分为5个阶段。

南京郵電大學
Nanjing University of Posts and Telecommunications

03

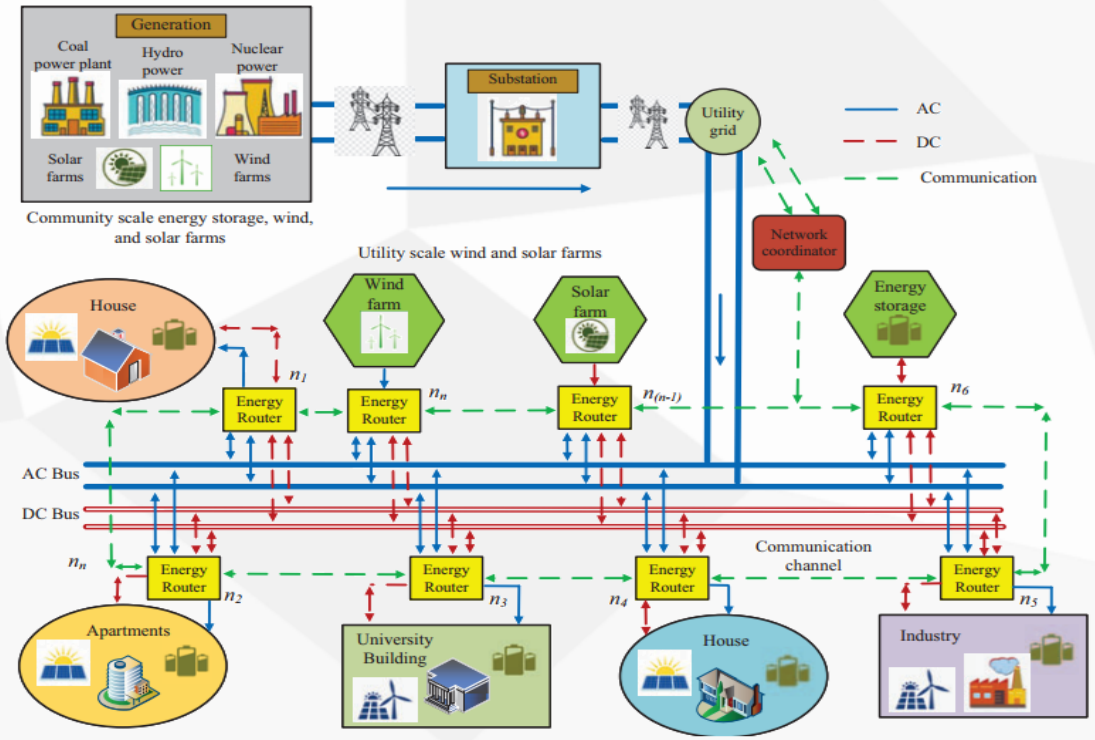
文献阅读

微电网组件的HPC定制

为了保护微电网关键基础设施，我们需要有效的检测机制。传统防病毒软件因计算开销高和缺乏稳健性而不足。硬件辅助恶意软件检测 (HMD) 利用硬件性能计数器 (HPC) 分析硬件指标检测恶意活动，但传统控制器缺乏HPC支持。我们建议设计定制HPC，监控固件指令序列，利用机器学习分类器识别异常行为。

ER路由器架构

微电网通过能源路由器 (ER) 与电网连接，形成交互节点 (n1、n2、...nn)。这些 ER 节点通过通信通道与电网中的 DC/AC 总线和其他 ER 节点交互。ER 是一种紧凑型设备，由电力电子转换器、智能控制和传感设备、通信模块组成，用于将分布式能源资源 (RES)、储能装置 (ES) 和 DC/AC 负载与电网连接。



南京郵電大學
Nanjing University of Posts and Telecommunications

《Hardware-based Detection of Malicious Firmware Modification in Microgrids》
《基于硬件的微电网恶意固件修改检测》

关键词：硬件性能计数器、微电网、时间序列分类、数字信号处理

Srivastava, Amisha, et al. "Hardware-based Detection of Malicious Firmware Modification in Microgrids." 2024 37th International Conference on VLSI Design and 2024 23rd International Conference on Embedded Systems (VLSID). IEEE, 2024.

DSP固件攻击

固件攻击：固件攻击旨在破坏固件调节设备的功能或操纵它以产生错误的系统输出。在DSP板中利用的两种攻击类型：拒绝服务(DoS)攻击和破坏DSP板信号感应功能的攻击。

中断操作攻击：DoS攻击使系统无法运行。一种方式是反复开关DSP板，通过触发特定操作引发中断。中断持续时间取决于系统参数，导致DSP板运行不稳定。利用系统计时器，攻击破坏电路组件的可用性，导致间歇性中断和系统不可用。

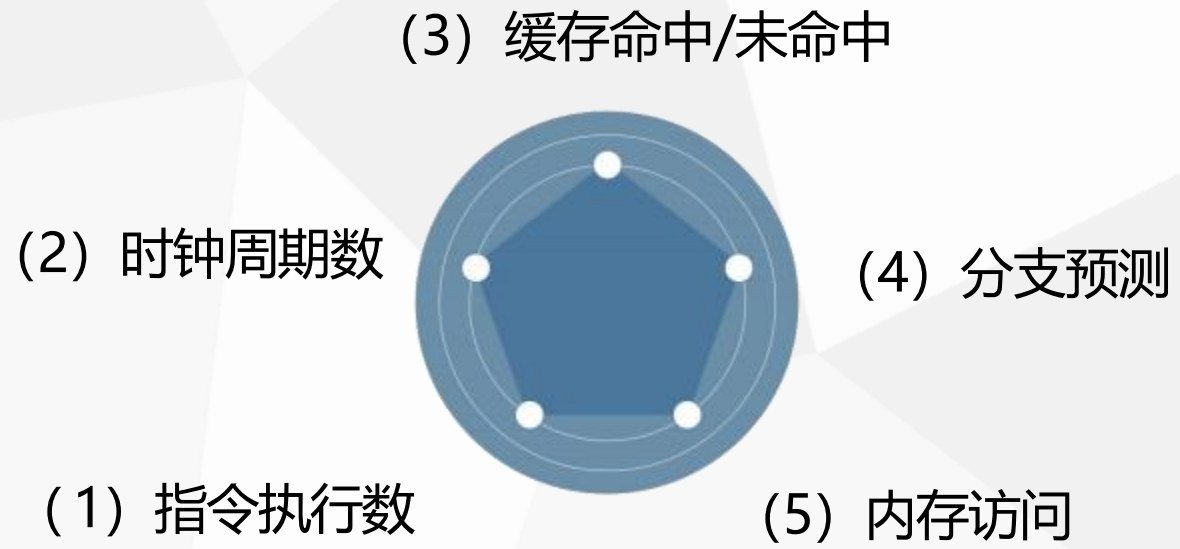
信号感知攻击：由于DSP板利用模拟数字转换器(ADC)来解释输入信号并做出适当响应。

- **循环攻击:**改变逻辑循环条件使DSP板陷入无限循环，阻止其执行预期任务并导致系统冻结
- **读数更改:**替换ADC参数为不正确的值，导致错误读数和系统错误。
- **窗口更改:**通过修改ADC分辨率窗口，破坏数据转换的精度，导致系统故障

基于硬件性能计数器的恶意软件检测

- **威胁模型：**创建欺诈性固件版本，利用静态固件更改来启动异常功能。
- **定制HPC设计：**监视二进制可执行文件中嵌入的特定汇编指令序列。

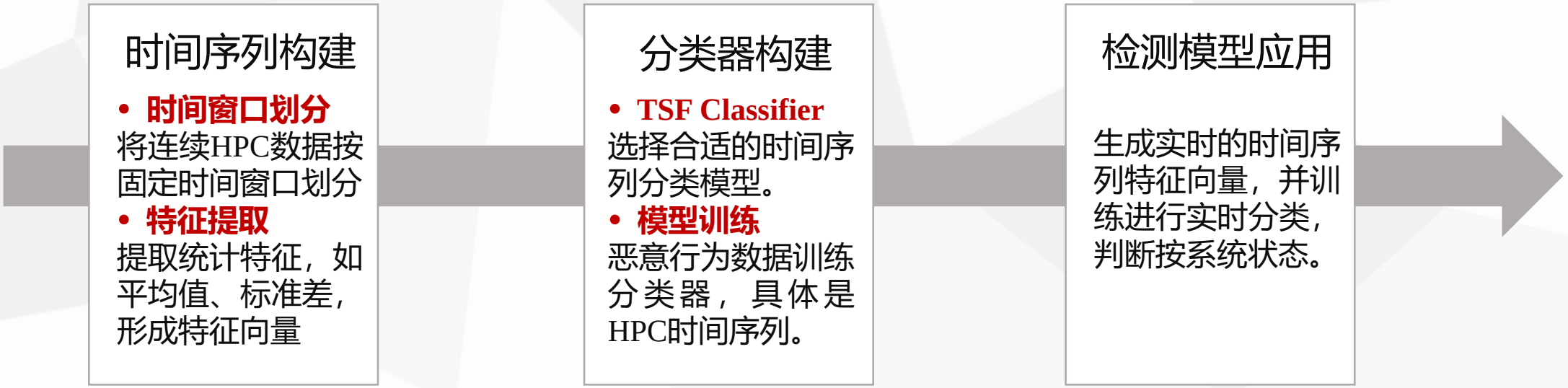
常见的HPC指标



基于硬件性能计数器的恶意软件检测

基于硬件性能计数器的恶意软件检测技术包括数据采集，模型生成，恶意软件检测模块。

- **数据采集：**数据采集模块通过一定的手段记录并读取硬件性能计数器的值。
- **模型生成：**模型生成模块以格式化的HPC数据作为输入，通过选定与程序特点相关的HPC事件，并结合一定的算法来生成模型。
- **恶意软件检测：**恶意软件检测模块通过利用生成模块输出的模型，以数据采集模块采集到的各程序的HPC值作为输入，判断HPC值所代表的程序是良性的还是恶意的。



相关工作

使用 HPC 进行 ROP 检测

通过模拟真实漏洞环境并使用性能监视中断（PMI）方法评估了检测ROP攻击的有效性，结果显示PMI方法在准确性上与结合上下文切换的CS-PMI方法相差不大。

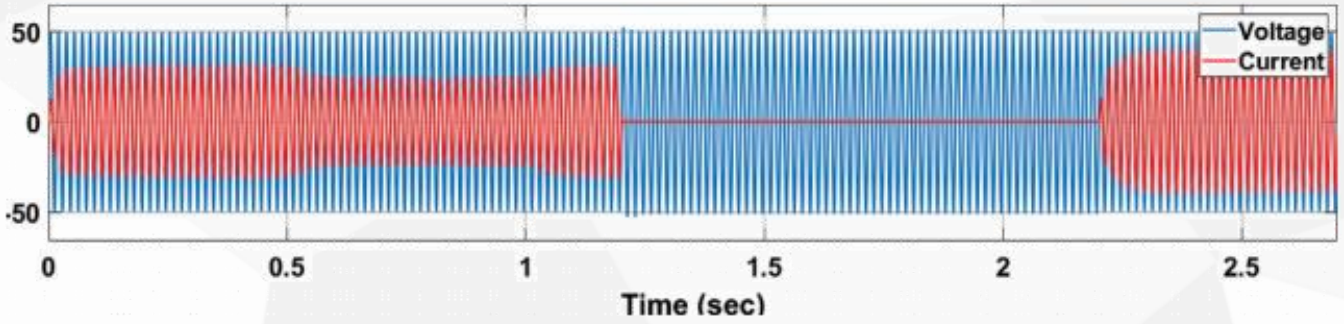
使用 HPC 进行恶意软件检测

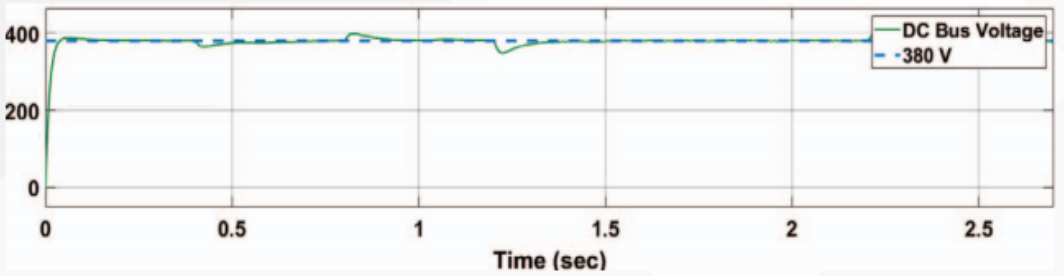
使用机器学习 (ML) 方法对恶意软件和良性程序进行分类，使用不同的分类方法发现记录数据的方式和所采用的方法的差异不仅会影响最终技术的准确性。

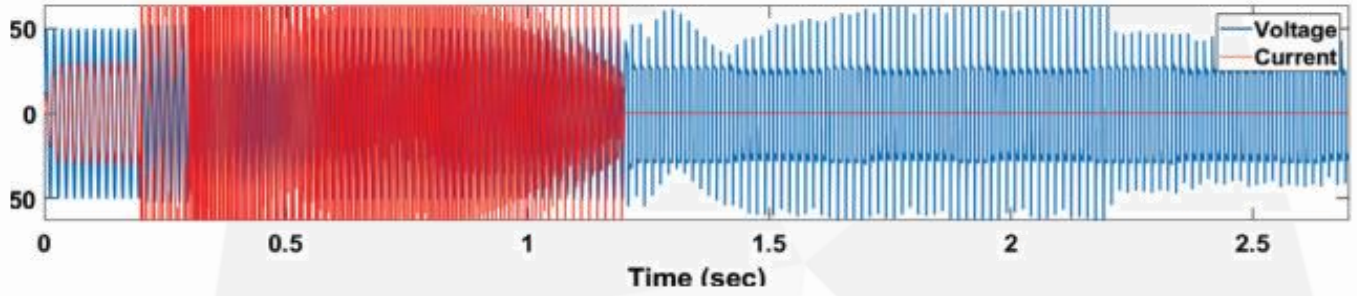
基于HPC的安全防御本质上取决于特定时间的阈值，攻击者可以诱发页面错误，显著影响测量事件的准确性。

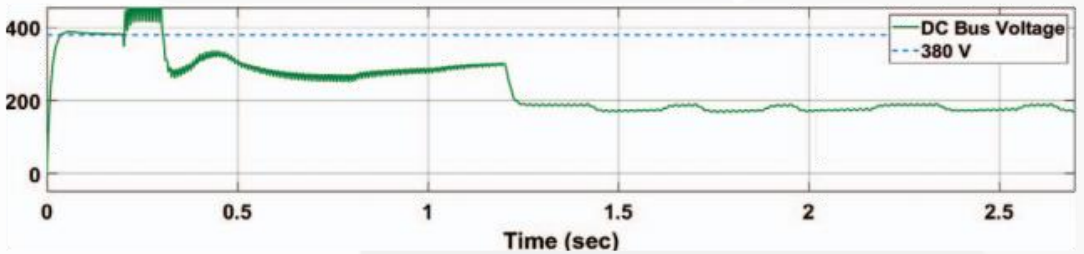
[1]Liu, Tong-Yu, Jianmei Guo, and Bo Huang. "Efficient Cross-platform Multiplexing of Hardware Performance Counters via Adaptive Grouping." ACM Transactions on Architecture and Code Optimization 21.1 (2024): 1-26.
[2]Das, Sanjeev, et al. "Sok: The challenges, pitfalls, and perils of using hardware performance counters for security." 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019.
[3]户彦飞, and 文雨. "基于硬件性能计数器的恶意软件检测技术综述." Computer Science and Application 12 (2022): 2896.

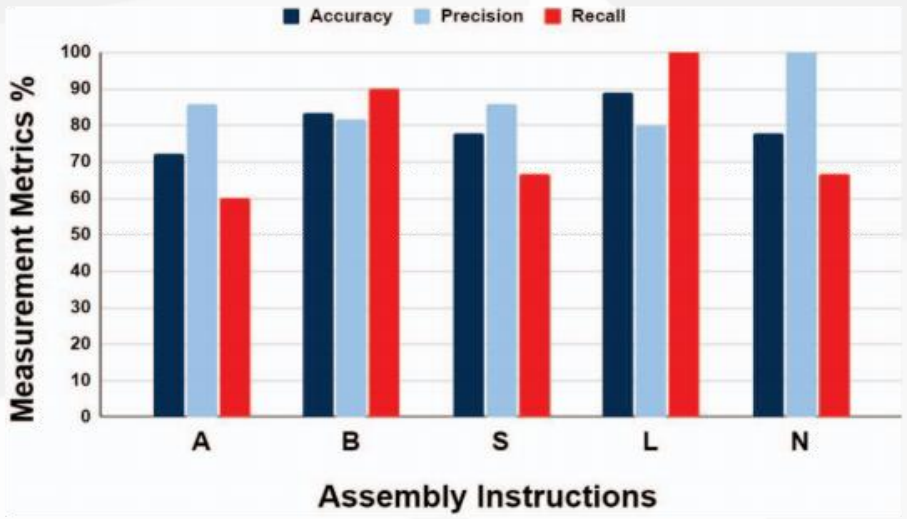
检测效果

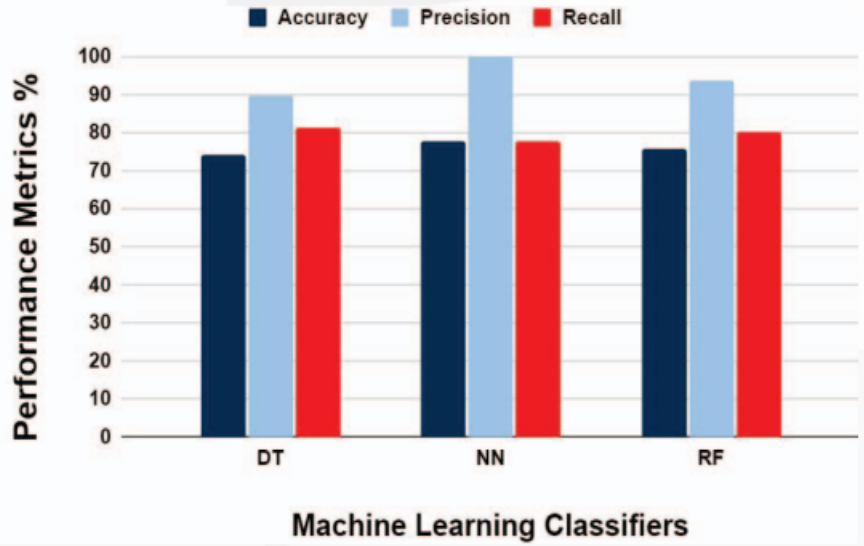

Voltage
Current
Time (sec)


DC Bus Voltage
380 V
Time (sec)


Voltage
Current
Time (sec)


DC Bus Voltage
380 V
Time (sec)


Accuracy
Precision
Recall
Measurement Metrics %
A
B
S
L
N
Assembly Instructions


Accuracy
Precision
Recall
Performance Metrics %
DT
NN
RF
Machine Learning Classifiers

南京郵電大學
Nanjing University of Posts and Telecommunications

《Threat Modeling of Cyber-Physical Systems - A Case Study of a Microgrid System》
《威胁建模的网络物理系统-微电网系统的案例研究》

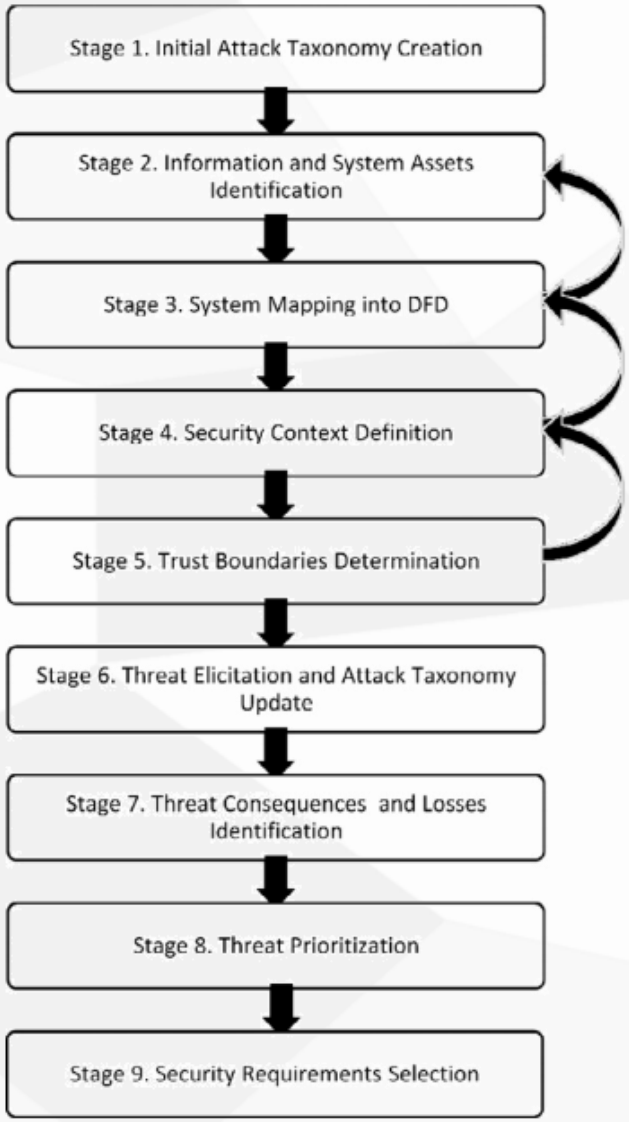
关键词：威胁建模、网络物理系统 (CPS)、 工业控制系统 (ICS) 、STRIDE、微电网

Khalil, Shaymaa Mamdouh, et al. "Threat modeling of cyber-physical systems-a case study of a microgrid system." Computers & Security 124 (2023): 102950.

背景介绍

CPS系统威胁建模方法：计算和通信领域的快速发展使得信息物理系统（CPS）在关键基础设施中的作用日益重要。然而，在CPS系统的开发过程中，人们往往忽视了网络威胁和恶意行为对系统的潜在影响。实际案例和研究表明，网络攻击对CPS系统构成了真正的威胁，可能导致严重的物理后果。

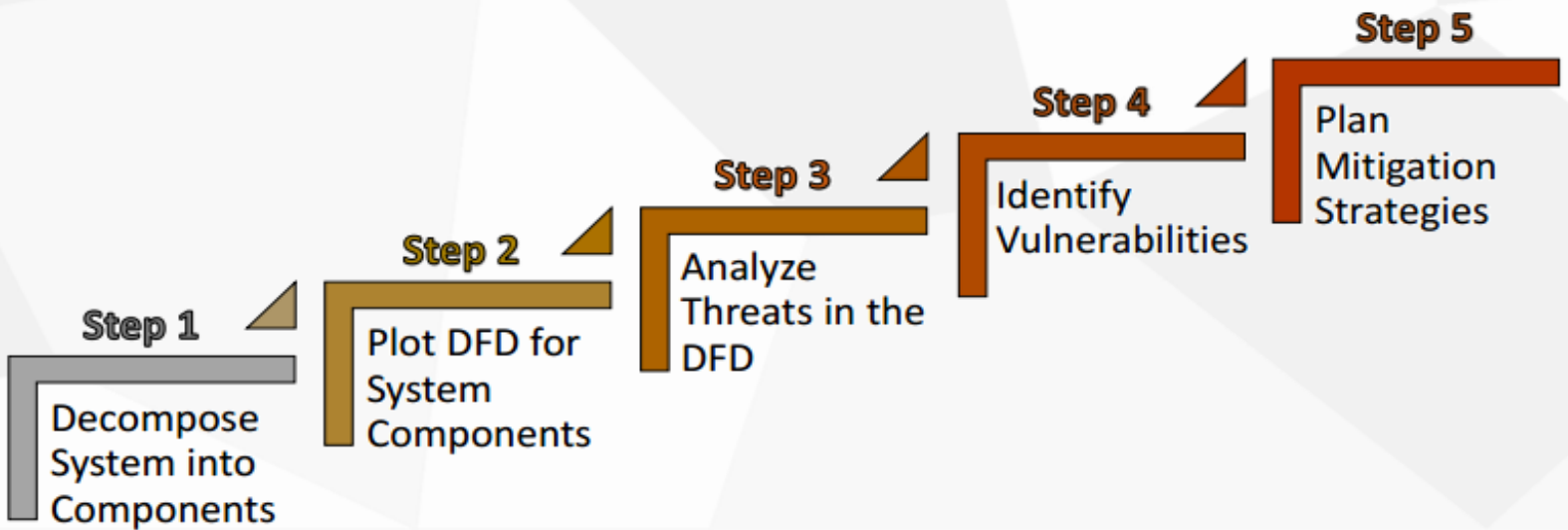
具体方案：本文提出了一种系统的威胁建模方法，将 STRIDE 应用于网络物理系统 (CPS)，通过微电网案例验证。主要贡献包括：描述网络与物理空间交互的DFD，提出资产识别和信任边界程序，系统识别威胁，制定威胁优先级排序，并展示其在 IEC 62443 安全需求识别中的应用。



SITRE方法

STRIDE 方法由 Microsoft 提出，代表六种不同类型安全威胁。

（1）欺骗：伪装合法用户、流程或系统元素；
（2）篡改：修改 / 编辑合法信息；
（3）否认：否认或放弃在系统中执行的某个操作；
（4）信息泄露：数据泄露或未经授权访问机密信息；
（5）拒绝服务 (DoS)：中断合法用户的服务；
（6）特权提升：权限受限的用户获得对系统元素的更高特权访问权限



04

当前重心

微电网智能设备脆弱性分析

当前重心

目标

评估微电网智能终端设备的安全脆弱性，通过系统性分析和攻击模拟，识别和修复潜在的安全漏洞。

研究内容

安全评估框架：构建针对微电网智能终端的安全评估框架。

脆弱点分析：识别系统的潜在漏洞，通过静态和动态分析结合的方式。

攻击模拟：生成对抗样本模拟真实攻击，评估系统的脆弱性。

南京郵電大學
Nanjing University of Posts and Telecommunications

感谢观看

汇报人：唐俊