# **个人技术报告**

## **一、个人基本情况与技术工作概览**

本人毕业于天津城建大学网络工程专业，后以劳务派遣身份加入中国科学院信息工程研究所网络攻防研究室宋振宇教授团队。工作期间，深度参与网络测试床构建、移动终端加密、城市网络测试床重构三大核心工程，在复杂网络系统研发与安全技术领域积累关键实践能力。

在网络测试床课题中，全流程参与技术攻坚：从基础网络设备运维切入，依托软件定义网络（SDN）技术搭建多协议自发现网络，参与开发SDN环境流量异常检测模块（参与撰写专利《面向软件定义网络的异常检测方法、装置及设备》）；在K8s环境下，攻克Windows、Linux、Android多系统在容器嵌套虚拟机场景下的自定义初始化适配，实现异构系统镜像的标准化构建；主导分布式任务调度中台二次开发（合作申请专利《面向用户的网络测试床场景业务调度方法及装置》），同时主导既有业务基于K8s的全流程容器化微服务改造；全程支撑项目在甲方单位的离线交付及使用报告编制。

在移动终端安全课题中，参与可信应用市场管理中心的开发与部署，合作申请《一种终端设备、数据加密方法、解密方法及电子设备》《一种数据加密方法、终端设备及电子设备》两项发明专利，聚焦终端数据加密技术突破，构建安全可信的移动应用分发体系。

在城市网络测试床课题中，基于K8s架构重构分布式任务调度中台，通过架构升级，实现多用户、多容器场景下的资源隔离与高效调度，支撑复杂网络仿真任务并行运行。

技术特长聚焦SDN应用开发、K8s微服务搭建、分布式调度中台构建，擅长从技术方案设计到工程化落地的全链路推进，累计参与4项发明专利撰写，在复杂网络场景中沉淀系统级架构设计与运维、开发能力。

## **二、代表性项目**

### **（一）项目一：网络测试床场景业务调度与协同体系构建**

#### **1. 项目背景**

互联网规模指数级增长，传统网络测试环境存在异构设备虚拟化难、大规模拓扑调度低效、安全检测滞后等问题。需构建集资源调度、网络发现、安全检测、多环境部署于一体的测试床系统，支撑复杂网络场景测试需求 。

#### **2. 技术难点**

多资源协同调度需解决多类型资源统一管理、资源冲突与隔离问题。网络自动化发现与协议模拟需兼容异构设备，保障拓扑信息实时准确。容器与虚拟化融合需在K8s环境下实现多用户资源管理，解决虚拟机自动化部署的兼容性与性能损耗。安全检测实时性需在SDN环境下精准识别异常流量，平衡检测精度与网络负载。

#### **3. 拟解决的技术问题**

构建一体化测试床体系，实现资源高效调度、网络自动发现、容器-虚拟机协同和安全实时检测，满足复杂网络攻防演练需求。

#### **4. 解决问题的思路**

采用分层架构+分布式队列+微服务架构实现资源调度；基于Ceph与K8s实现资源池化；通过分层架构与分布式队列拆分任务逻辑；利用SDN控制器北向API与LLDP/BGP协议实现拓扑发现；构建LSTM模型与SDN流表联动机制，实现异常流量实时拦截。

#### **5. 具体解决技术问题的技术方案**

* 多资源协同调度

基于 Ceph 构建计算、存储、网络资源池，通过标签化与动态算法实现资源精准匹配及自动回收，避免冲突。采用三层架构（Ceph 存储池化、K8s 管理容器 / 虚拟机、Celery 队列拆分调度），引入图论算法优先调度核心设备。以 K8s 命名空间隔离多用户资源，结合流量控制器与 HPA 实现弹性扩缩容，资源请求经消息队列解耦。

* 网络构建与异构自动发现

基于 SNMP/LLDP 开发拓扑发现模块，SDN 控制器模拟 BGP Speaker 学习路由，北向 API 生成可视化拓扑。基于 OpenFlow 下发三类流表：基础转发（MAC 学习）、路由、异常响应（攻击封堵），匹配域含五元组及流持续时间。

* 容器嵌套虚拟机与多环境部署

基于 kubevirt 在 K8s 容器部署 QEMU 虚拟机，支持多系统镜像自动化安装，通过 virtio-fs 共享文件、VNC 传输界面。开发 Operator 以 CRD 定义规格，结合控制器管理生命周期，YAML 模板库支持一键部署。以 Namespace 隔离多用户容器，HPA 基于消息队列阈值扩展 Worker Pod。

* SDN 异常检测与响应

基于 SDN 控制器采集流量数据，按五元组与应用类型分类。三层 LSTM 网络结合交叉熵分类器识别攻击，经 Min-Max 归一化与 Adam 优化器训练，推理延迟≤15ms，异常检测后 30 秒内下发流表封禁。模型基于 InSDN 数据集训练，滑动窗口 6 时 F1 分数达 97.08%。

#### 6. **技术设计**

##### 多资源协同调度技术设计

* 资源池整合实体机、虚拟机及网络设备，通过标签化分类；动态算法按任务需求匹配标签，采用贪心策略分配空闲资源，通过分布式锁防冲突，任务完成后自动回收。三层架构：底层 Ceph RADOS 集群实现存储池化；中层 K8s Namespace 隔离多用户，配置 ResourceQuota 控制资源上限；顶层用分布式队列拆分子任务异步处理。引入紧密度中心性算法，优先调度核心网络节点保障稳定性。

##### 网络构建与异构自动发现技术设计

* 通过 Open vSwitch 创建虚拟网络，配置桥接接口与 VLAN，控制器下发 MAC 学习流表实现二层转发。拓扑发现流程：控制器周期性下发 LLDP 报文，收集链路信息构建初始拓扑；结合 SNMP 设备信息生成可视化图谱；模拟 BGP Speaker 学习路由，下发含 IP、协议类型的路由流表。流表采用 idle\_timeout 机制（300 秒）自动清理。

##### 容器嵌套虚拟机与多环境部署技术设计

* 基于 kubevirt 实现 K8s 容器嵌套 QEMU 虚拟机，通过 virtio-fs 共享文件（延迟≤10ms）、VNC 传输图形界面，资源占用减少 30%，启动时间缩至 10 秒内。Operator 通过 CRD 定义虚拟机规格，结合 K8s 控制器管理全生命周期；YAML 模板库支持一键部署多系统。K8s 编排：NetworkPolicy 隔离网络，HPA 基于消息队列阈值扩缩 Worker Pod，StatefulSet 保障有状态服务稳定。

##### SDN 异常检测与响应技术设计

* 控制器采集 OpenFlow 流量数据，按五元组与应用类型分类，经滑动窗口聚合与归一化处理，每秒提取 18 维特征。三层 LSTM 模型（128 神经元 / 层）用 Adam 优化器（0.001）训练，推理延迟 15ms，F1 分数 97.08%。异常响应：控制器下发流表至交换机执行丢弃，经消息总线同步全局流表，启动定时任务记录日志，总延迟≤30 秒。

#### **7. 实现效果**

* 资源调度：千级异构节点拓扑部署时间从2小时缩短至20分钟，K8s多用户场景下资源冲突率降至0.3%，支撑复杂网络测试 。
* 网络构建：城市网络环境秒级构建，分钟级协议收敛，拓扑发现延迟小于10秒，适配华为、思科等多厂商设备，构建真实网络测试环境 。
* 容器-虚拟机协同：百级异构虚拟机部署时间缩短至1小时以内，满足多环境并行测试需求 。
* 安全检测：SDN异常检测误报率降至3%，攻击隔离时间小于25秒。

### **（二）项目二：可信系统及应用市场**

#### **1. 项目背景**

移动终端智能化水平提升，应用日益丰富，可信执行环境依托终端软硬件构建，广泛应用于安全智能设备、安全支付等领域，旨在解决各类安全问题。但当前其与通用操作系统的物理资源未彻底隔离，导致移动端数据传输的完整性和合法性难以保障。

#### **2. 技术难点**

需构建通用操作系统与可信执行环境间高效安全的数据交互机制；在 Modem 中合理设置验签模块，确保发送数据为预定格式加密数据，且具备高准确性与实时性；精确设计双加密算法及封包规则，保障两次加密的有效性与兼容性。

#### **3. 拟解决的技术问题**

构建具备终端静态度量、动态度量、可信验证、可信策略管理、可信审计等功能的可信系统及应用市场，显著提升移动终端数据的安全性和保密性。

#### **4. 解决问题的思路**

在通用操作系统与可信执行环境间建立共用内存，实现数据安全交互；在 Modem 中设置验签模块，严格验签密文文件；采用双加密流程，数据生成阶段首次加密，IP 封包后二次加密，提升传输安全性。

#### **5. 具体解决技术问题的技术方案**

##### 可信终端

* 针对 REE 环境数据泄露风险，将加密核心程序部署于 TEE，与 REE 物理隔离，通过共用内存由 REE 中 CA 中转数据。数据传输加密采用双加密，TEE 加密芯片先对应用数据 AES 处理，再对 IP 包 RSA 加密。Modem 部署验签模块，解析 IP 头部加密标记和哈希值，验证双加密，拒绝不合规数据。

##### 应用市场构建

* 管理中心有四大方案：①APP 生命周期以 FSM 状态机驱动，集成 MobSF 安全校验；②审核发布调用 HSM 生成 ECDSA 签名，经 Jenkins+K8s 灰度部署；③风险策略基于 InfluxDB 时序建模，MQTT 保障指令投递；④权限管控用 JWT+RBACv3，实现双因子认证与细粒度控制。

#### **6. 技术设计**

##### 6.1 可信终端技术设计

* 三层安全架构：
  + REE 层：含 IP 协议栈与第一 CA，获取待加密数据存共用内存，转发密文至 Modem，扩展 IP 协议栈添加加密标记和哈希字段。
  + TEE 层：集成加密芯片与第一 TA，经共用内存交互。首次用 AES-256 加密，二次用 RSA 加密，更新加密标记并计算哈希。
  + Modem 层：含第二 CA、验签模块及 TEE 中第二 TA、加密芯片。第二 CA 存封包数据，第二 TA 触发二次加密；验签模块验证后放行。
* 双加密流程：
  + 首次加密：REE 中 CA 存数据，TEE 中 TA 调用芯片 AES 加密，CA 转发至 IP 协议栈封包并设加密标记。
  + 二次加密：CA 存 IP 包数据，TA 用 RSA 加密，更新标记并生成哈希，CA 转发至 Modem。
* Modem 验签机制：解析加密标记和哈希，仅放行验证通过的密文。

##### 6.2 应用市场技术设计

* 接口层：定义 RESTful 端点，日志下载异步处理，实时反馈断点续传进度。
* 数据层：设计核心表，Elasticsearch 支撑检索，InfluxDB 优化时序分析。
* 流程层：HSM 生成签名，Jenkins+K8s 实现灰度部署，全链路追踪故障。

#### 7. **实现效果**

* 可信终端：REE与TEE内存隔离粒度达256B，侧信道攻击成功率降为0；Modem验签模块实现100%合规性验证。
* 应用市场：恶意APK拦截率100%；审核周期从24小时缩至45分钟，灰度发布切换时间≤30秒；在10万级设备并发场景下达达率99.99%。

## **三、今后工作展望**

基于过往在复杂网络系统研发与安全技术领域的实践积累，未来将以 “技术落地服务实际需求” 为导向，在夯实专业能力的同时注重工程化思维与创新意识的双重提升：持续依托 SDN 与 K8s 技术底座探索网络调度与容器化部署的深度融合，强化微服务架构的数据安全防护机制及弹性扩展方案设计，以支撑高并发低延迟的网络仿真与攻防测试场景；突破单一技术栈局限，在网络攻防、系统安全、云计算等交叉领域深化研究，探索 “网络 - 终端 - 应用” 全链条安全加固方案，通过参与重大项目积累大规模分布式系统架构设计经验，逐步成长为兼具技术深度与系统思维的复合型研发骨干。