

Design of Mobile Communication Network Slicing Security Deployment System Based on Machine Learning

Ziqian Yin

Taishan College of Science and Technology, Tai'an, Shandong, 271000, China

Abstract

In order to improve the prediction accuracy and capability of big data flow and meet the requirements of security and utilization of mobile communication network traffic packets, a mobile communication network slicing security deployment system based on machine learning is designed. Network is organized through network slicing to improve the adaptability of network and service, so as to realize the prediction of big data flow. In this paper, system topology, slicing and hierarchy were created, and machine learning structures were used to create security deployment and resource allocation programs for communication network slicing. Experimental results showed that the prediction accuracy of the system exceeded 95%, and initial parameters could be well selected to improve the reliability of system security deployment.

Keywords

machine learning; mobile communication; network slicing; network security

基于机器学习的移动通信网络切片安全部署系统设计

尹子骞

泰山科技学院, 中国 · 山东 泰安 271000

摘 要

为了使大数据流的预测精度和能力得到提高, 移动通信网络流量包的安全性和利用率满足需求, 实现移动通信网络切片安全部署系统设计。根据网络切片组织网络, 使网络与业务适配度得到提高, 从而实现大数据流的预测。论文创建系统拓扑、切片和层次结构, 使用机器学习结构创建通信网络切片安全部署和资源分配程序。通过实验结果表明, 系统预测精度超过95%, 能够良好选择初始参数, 提高系统安全部署可靠性。

关键词

机器学习; 移动通信; 网络切片; 网络安全

1 引言

在移动通信技术不断发展的背景下, 移动通信网络也在持续发展, 人们也越来越依赖移动通信网络。移动通信主要优势为机动便捷、随遇入网、快速高效等, 在此背景下的网络安全问题也越来越突出。移动通信网络平台在设计过程中要充分考虑其安全性, 比如网络接入安全、网络域安全、后台应用域安全等。针对移动通信网络传输信息的敏感性来说, 缺乏独立应用域空间, 无法隔离普通公网用户, 存在非法访问、信息窃取和病毒摆渡等威胁。因此, 论文提出了移动通信网络切片安全部署系统, 从而使系统安全保密问题得到解决。

2 系统的架构设计

针对移动通信中的网络威胁所导致出现的安全隐患, 设计了移动通信网络安全架构, 详见图 1。创建移动密码基础设施, 根据安全模块能够实现应用层、传输层等应用需求。移动密码管理基础设施能够将管理密码资源, 移动通信网络的每个端设备身份认证标识为入网号码, 使应用系统根据地域划分成为多个小型 IB 域, 通过 PKI 管理 IBE 域, 并且发放域证书, 创建信任关系, 对系统参数进行共享。在域的内部能够利用密码服务, 创建高效信任体系。安全构件能够通过标准接口连接安全模块, 实现安全协议的设计, 从而保护信息。利用安全芯片实现移动平台的设计, 从而开展一体化平台的设计, 对安全芯片密码服务进行调用, 从而实现信息存储和传输保护, 使高敏感信息安全防护需求得到满足; 配套设施能够构成相应标准体系, 系统运维管理人员能够实现系统安全构件的运行、审计、监控等, 从而保证系统运行正常。

【作者简介】尹子骞 (2002-), 男, 中国山东泰安人, 本科, 从事通信工程研究。

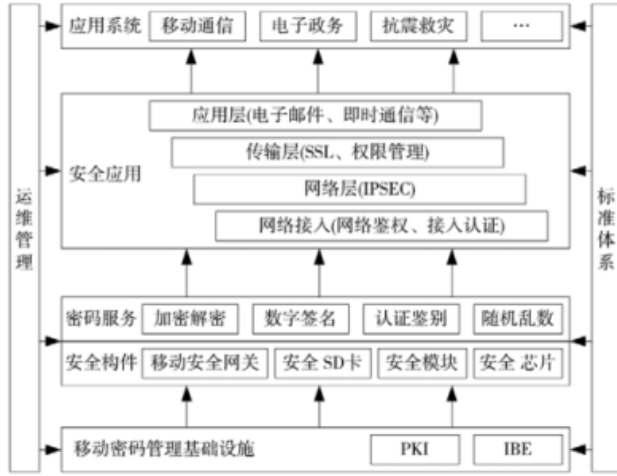


图1 系统安全框架

3 移动通信网络切片安全部署系统的设计

3.1 安全部署的问题描述

在部署网络切片时的业务场景和资源需求都各有不同，所以要设置不同的网络切片结构。在底层物理网络中设置端到端网络切片，比如核心网、接入网或者传输网，实现切片之间的协作和连接。论文通过节点的安全信任值展现网络资源的安全性，一般取值为0~1。在增加安全信任值时，能够使网络安全性得到提高。

在网络切片部署过程中，节点部署为主要环节。在部署请求时 VNF 部署 CPU 资源值为重点，还包括资源的安全信任需求值和自身安全信任值。在切片部署的过程中，要求满足节点 VNF 部署请求的值都能够超过网络资源中的相应值，不仅能够保证网络资源充足，还不会影响到底层物理网络的部署。

3.2 资源分配程序设计

将机器学习为基础设计移动通信网络切片安全部署系统，对信息资源进行分配。要求创建系统切片结构模型，系统结构关键节点和虚拟模型节点对应，其中的网络切片控制方式为模型程序，为用户提供系统网络服务，并且创建数字系统模型，将网络资源分配给系统。基于通信运营商管控，移动通信有一个网络基础，无向图 P 指的是通信网络数字模型，计算公式为：

$$P = (A, B, C) \quad \text{公式 1}$$

其中，A、B、C 分别为网络关系链路、网络节点的集合和网络切片资源数量。

针对资源数量和分布的约束情况，从而分配资源的优化，r 表示节点的变化，资源流动变量详见公式 2：

$$J_m \in \{0, 1\} \quad \text{公式 2}$$

其中， J_m 为单位时间内节点 r 网络资源中网络切片 Q_n 的分配数量，约束公式详见公式 3：

$$\sum_{n=1}^q J_m T \leq C_r \quad \text{公式 3}$$

其中，T 为单位时间长度；n 为网络资源的分配数量； C_r 为资源数量；q 为最大的网络资源分配数量，要求能够结合资源分配的价格计算资源分配价格约束公式：

$$S_n = \sum_{n=1}^q J_m T S \quad \text{公式 4}$$

其中，S 为网络资源分配价格，和网络切片资源的分配结合，从而对资源进行控制，得到不同部分网络资源最优化配置资源。

3.3 网络切片的安全隔离技术

本地用户无法使用移动通信网络业务资源，并且不会存储在云中，无法控制其中的数据。多租户数据存在模糊的数据边界，而且还出现各种风险，比如私有、共有的数据非法流动、迁移等。那么，要重视共有数据和私有数据的控制和隔离。为了在独立虚拟安全切片中实现数据资源的分布，要求研究逻辑边界层和数据层。在逻辑边界层识别租户资源的安全边界，有效控制虚拟转发表租户的数据。在数据中对租户数据进行绑定，对多租户私有、共有的数据进行区分，根据标识为基础的访问控制机制限定虚拟机信息流动，避免私有数据出现泄露等问题，还要能够保证租户数据的安全性。

①基于逻辑边界。此方法主要包括对多租户逻辑边界进行检测、识别和划分，在此过程中能够绑定租户标识和虚拟域的逻辑，通过量化不同租户的服务器请求，从而有效识别非法租户的越界访问行为。针对边界租户数据的流动性要设置安全防护策略，从而转发虚拟网络切片限定的数据，避免出现非法流动等问题。

②基于数据层次。为了能够保证租户私有数据应用过程中的安全性，要对租户数据进行识别，并且设置不同的权限，避免不同租户的虚拟机数据流非法流动和数据泄露。设计服务器监控机制，并且提取租户数据流的标识，以此判断是否会出现在虚拟机租户中。如果不是，就要对虚拟机是否迁移进行判断。如果没有迁移，就要禁止租户数据流入。要不然，要以租户标识，在虚拟机中迁移合法的数据。利用数据和逻辑边界的安全隔离，实现 UE 接入访问虚拟域的创建，从而满足数据之间的隔离需求，避免租户数据流动和用户信息泄露，从而创建虚拟网络安全切片。

3.4 切片内部的安全通信

切片内部安全通信能够使接入网和核心网的子切片安全通信问题得到解决，UE 利用无线和网络相互连接，与 5G 核心网络 CN 相互连接，要求 RAN 和 CN 能够传递信令，从而接入 UE，对信令安全性进行保证，避免被篡改，保证安全接入。实现 CN 切片和 RAN 的安全通信，并且协商两者的安全通信参数。论文基于用户身份标识创建动态安全通道机制，实现公私对和身份标识的分配，实现临时会话密钥 k 的生成。通过 SG 公钥加密，发送到 SG 中。SG 使用自身

的密钥对临时会话密钥 k 进行解密, 然后使用 k 解密对信令进行发送, 并且全面验证 ENode 合法性, 还要保证信令安全性, 避免伪基站攻击。在切换 UE 移动基站切换时, 将原本安全通道撤销, 实现新安全通道的创建, 部分安全通信主要代码如下:

```
public class TestSocketManager : System.IDisposable
{
    public TestSocketTcpRoutine m_MainSocket;
    public void Init()
    {
        m_MainSocket = CreateSocketTcpRoutine();
    }
    public void Connect(string ip, int point, System.
Action<bool> connectComplete)
    {
        m_MainSocket.Connect(ip, point, connectComplete);
    }
    public TestSocketTcpRoutine CreateSocketTcpRoutine()
    {
        return TestGameEntry.PoolMgr.Class_Dequeue<TestSocketTcpRoutine>();
    }
    public void Update()
    {
        if (m_MainSocket != null)
        {
            m_MainSocket.OnUpdate();
        }
    }
    public void Dispose()
    {
    }
}
```

4 实验研究

为了对论文研究效果进行验证, 要求对其进行设计和实验。

4.1 实验设置

选择不同的三个数据集进行实验, 对部署系统的实际的应用效果进行验证, 表 1 为数据流的特点。

表 1 数据流的特点

数据流大小 /bit	数据关系模式
1200	联机表达模式
2400	数据到达模式
3600	数据无限模式

4.2 实验结果

通过实验结果表示, 在数据流大小为 1200bit 的时候, 预测方法的预测能力良好, 预测精度超过 95%; 在数据流为 2400bit 的时候, 三种预测方法存在差异, 论文基于机器学习的预测精度在 95% 以上, 并且没有下降; 在数据流为 3600bit 的时候, 论文的预测效果比其他两种方法理想, 能够为后期的安全工作打下基础。

另外, 论文方法的平均部署成本优于其他的算法。是因为论文的算法根据不同的业务类型和不同域资源差别分配资源, 制定部署方案, 使平均部署成本得到降低。其他的方法寻找虚拟链路的时间比较长, 从而使节点和链路出现重合等问题, 从而提高了部署成本。在部署中设计请求拓扑, 剩下了底层部分资源, 使部署成本增加。

5 结语

论文实现移动通信网络切片安全部署系统的设计, 利用设计系统切片结构能够通过最大熵算法预测系统网络流量数据, 在复杂的网络下精准预测不同时间段的流量数据, 及时处理预测问题并且进行修复, 有效满足安全部署系统的需求。开展实验对比标识, 论文方法具有较高的预测精度, 能够使工作过程中的效率得到提高, 还能够有效保证网络运行过程中的平稳性。

参考文献

- [1] 赵志俊. 基于机器学习的通信网络安全漏洞监测系统[J]. 长江信息通信, 2022, 35(12): 175-177.
- [2] 蒋志顺, 范雷. 基于机器学习的无线通信网络安全漏洞智能监测系统[J]. 电子设计工程, 2021, 29(15): 115-119.
- [3] 王可阳. 基于机器学习的网络安全态势感知系统研究[J]. 无线互联科技, 2023, 20(6): 161-164.
- [4] 杨婉琳. 基于机器学习的网络安全态势感知系统研究[J]. 无线互联科技, 2022, 19(18): 163-165.
- [5] 夏海亮, 钱锡颖, 叶明达, 等. 基于机器学习的电力信息通信风险感知研究[J]. 电子设计工程, 2023, 31(13): 141-145.
- [6] 石乐义, 刘佳, 刘祎豪, 等. 网络安全态势感知研究综述[J]. 计算机工程与应用, 2019, 55(24): 1-9.
- [7] 隆峻, 陈佐璇. 基于机器学习的通信网络安全防护过程数据加密方法[J]. 自动化技术与应用, 2022, 41(12): 81-85.
- [8] 蒋建峰, 张凤岩, 孙金霞, 等. 基于隔离粒子群算法的智慧矿山 5GSA 网络切片部署策略[J]. 国外电子测量技术, 2022, 41(4): 42-48.
- [9] 于运涛, 张大松, 姜洪朝, 等. 基于区块链的网络安全系统关键数据存储处理系统设计[J]. 电子技术应用, 2023, 49(4): 78-82.
- [10] 顾仁龙, 曾鸿孟, 徐超, 等. 基于机器学习的云原生结构数据攻击检测系统设计[J]. 电子设计工程, 2023, 31(14): 62-65+70.