

基于图神经网络与量子密钥分发协议的 局域网安全通信技术

施金诺^{1†},熊贵云¹,童江艳²

(1. 云南省中共怒江州委网信办,云南 怒江 673100;2. 云南省中共怒江州委宣传部,云南 怒江 673100)

摘要:当前局域网安全通信过程中,主要通过密钥分发中心(KDC)对密钥进行集中管理与分发,其分发模式是固定不变的,导致遇到攻击后局域网通信丢包率较高。因此,提出了基于图神经网络与量子密钥分发协议的局域网安全通信技术。运用椭圆曲线密码算法处理网络通信数据,得到一系列加密会话。针对加密流量进行过滤处理后,考虑 TLS 握手原始字节和 TLS 记录长度序列,生成单条加密会话的特征表示向量。构建基于图神经网络的智能分类模型,将加密流量特征表示输入其中,即可检测出恶意流量,将其从加密会话中剔除。最后,引入量子密钥分发协议帮助通信双方生成共享密钥,安全解析加密会话,实现局域网安全通信。实验结果表明:该技术实施后,局域网安全通信过程中产生的丢包率不超过 0.2%,满足了网络信息传输要求。

关键词:局域网;加密;图神经网络;恶意流量;量子密钥分发协议;安全通信

中图分类号:TP391

文献标识码:A

Lan Secure Communication Technology Based on Graph Neural Network and Quantum Key Distribution Protocol

SHI Jinnuo^{1†},XIONG Guiyun¹,TONG Jiangyan²

(1. Office of Nujiang's Cyberspace Affairs Commission,Nujiang, Yunnan 673100, China;

2. Nujiang Prefectural Committee Propaganda Department, Yunnan Provincial
Communist Party,Nujiang, Yunnan 673100, China)

Abstract: In the current process of secure communication in local area networks, keys are mainly centrally managed and distributed through the key distribution center(KDC), and its distribution mode is fixed and unchanged, resulting in a high packet loss rate in local area network communication after encountering attacks. Therefore, a secure communication technology for local area networks based on graph neural networks and quantum key distribution protocols is proposed. Using elliptic curve cryptography algorithm to process network communication data and obtain a series of encrypted sessions. After filtering encrypted traffic, consider the TLS handshake raw bytes and TLS record length sequence to generate a feature representation vector for a single encrypted session. Constructing an intelligent classification model based on graph neural networks, inputting encrypted traffic feature representations into it, can detect malicious traffic and remove it from encrypted sessions. Finally, the introduction of quantum key distribution protocol helps communication parties generate shared keys, securely parse encrypted sessions, and achieve secure communication in local area networks. The experimental results show that after the implementation of this technology, the packet loss rate generated during secure communication in the local area network does not exceed 0.2%, meeting the requirements of network information transmission.

Key words: local area network; encryption; graph neural network; malicious traffic; quantum key distribution protocol; secure communication

规划一个有限的地理区域,利用特定的技术手段,将区域内所有服务器、计算机等设备连接起来,即可形成辅助信息交流与资源共享的局域网。目前,在金融、医疗、军事等高度敏感领域^[1],局域网已经成为促进数据高效流通的关键基础设施。但随着信息技术的快速发展,局域网安全面临着越来越多的挑战,研究和应用先进的局域网安全通信技术显得尤为重要。

Liu 等提出基于混沌同步的安全通信技术^[2],以典型混沌算法为基础,设计网络安全加密通信架构。同时,利用时间同步稳定性理论和范数归一化符号函数,构造同步滑模控制器,应用到安全通信过程中,用以调整混沌加密过程中所有非零状态元素的时间同步,形成稳定性较高的安全通信手段。但是,混沌加密算法的稳定性容易受到初始条件的影响,这导致该方法应用局限性较大。章意等提出基于 SecOC(板端加密通讯)的安全通信技术^[3],将 SM4 密码算法、Blake2s 改进密钥管理算法结合起来,搭建包含信息加密、身份认证两个关键模块的安全防护模型,应用其接口实现网络安全通信。但是,SecOC 机制需要对每个 PDU(协议数据单元)进行加密、MAC 计算和验证等处理,这导致网络安全通信时间延迟较大。李荟杰等提出基于量子安全多方异或协议的安全通信技术^[4],考虑网络通信过程中面临的隐私保护要求,提出量子安全多方逻辑异或思想,并以此为基础生成一个网络安全通信协议。通过加密、传输、解密等环节,确保网络用户通信安全。但是,量子噪声、量子退相干等因素,都可能导致量子信号的衰减和失真,这导致该通信技术的可靠性较差。朱睿等提出基于多 IRS(智能反射面)辅助的安全通信技术^[5],深入分析网络通信过程,并以最大化保密率为目标,建立基于多 IRS 辅助的安全通信目标函数。通过改进交替优化算法求解这一目标函数,即可获得科学的网络安全通信策略。但是,多 IRS 辅助的 MIMO 系统本身也可能存在安全漏洞,IRS 控制信号容易被窃取或篡改,这导致该通信技术安全性无法满足要求。

在研究新型局域网安全通信技术时,将图神经网络与量子密钥分发协议结合起来,利用前者识别恶意流量,优化网络通信信息,提升整体防御能力。同时,结合 QKD 协议,实现局域网内密钥的安全分发与更新,确保数据传输的保密性,为局域网安全通信构建起一道坚不可摧的防线。

1 结合图神经网络与量子密钥分发协议设计局域网安全通信技术

1.1 设计局域网通信加密算法

针对局域网通信数据进行加密处理,是实现网络安全通信的基础。因此,引入椭圆曲线密码算法^[6],设计无证书公钥密码体制下的加密算法。局域网通信过程中,针对代表域推导出一个代数闭域,基于此可以定义仿射平面为:

$$L^2(\hat{A}) = \hat{A} \times \hat{A} = \{(x, y) : x, y \in \hat{A}\} \quad (1)$$

式中, L 表示仿射平面, $\hat{A}$ 表示代表域的代数闭域, (x, y) 表示仿射平面曲线上的一个点。

利用既约多项式在平面上搜索出多个零点,组成一个仿射平面曲线。

$$C = \{(x, y) \in L^2(\hat{A}) : C(x, y) = 0\} \quad (2)$$

式中, C 表示仿射平面曲线。

以仿射平面曲线上任意一个点为例,判断其是否满足公式(3)所示的条件,若满足该条件,则证明该曲线属于椭圆曲线,可以用式(3)、式(4)进行描述。

$$y^2 + a_1 + xy + a_3 y = x^3 + a_2 x + a_4 x + a_5 \quad (3)$$

$$E = \{(x, y) \in L^2(\hat{A}) : E(x, y) = 0\} \cup \{O\} \quad (4)$$

式中, a_1, a_2, a_3, a_4, a_5 表示辅助计算参数, E 表示椭圆曲线, O 表示域中心点。

由于椭圆曲线在同构计算时,其自身性质不会发生改变,根据这一特点将网络通信标准型加密描述为公式(5)所示的简单计算过程。

$$\begin{cases} b(\hat{A}) \neq 2, 3 & y^2 = x^3 + a_4 x + a_5 \\ b(\hat{A}) = 2 \text{ 且 } j \neq 0 & y^2 + xy = x^3 + a_2 x + a_5 \\ b(\hat{A}) = 2 \text{ 且 } j = 0 & y^2 + a_3 y = x^3 + a_4 x + a_5 \\ b(\hat{A}) = 3 \text{ 且 } j \neq 0 & y^2 = x^3 + x^2 + a_5 \\ b(\hat{A}) = 3 \text{ 且 } j = 0 & y^2 = x^3 + x^2 - a_5 \end{cases} \quad (5)$$

式中, j 表示有理点数量, b 表示字符函数。

根据实际网络通信场景,选择适当的加密公式处理通信信息,使得网络中传输内容呈现为密文。

1.2 建立加密流量处理与表示方案

为了更好地区别局域网通信过程中出现的恶意加密流量,在粒度层级上对加密会话进行预处理,并从多条 TLS(改进协议传输层安全协议)记录入手,进一步表征网络加密会话。

网络加密会话的预处理过程涉及三个核心步骤,分别是拆分、重组与过滤^[7]。从会话粒度层级入手,原始加密流量被精细拆分为独立的分析单

元,每个单元由共享相同五元组(源 IP、源端口、目的 IP、目的端口、协议)的会话构成。进入重组阶段后,充分考虑局域网安全通信过程中网络流量 MTU (最大传输)限制,以及 TLS 记录多样性,从多个 TCP 段中智能还原通信会话。最后,从重组会话中检索出所有非加密会话,并将其直接丢弃,完成原始加密流量的过滤处理,为后续的加密恶意流量检测提供了更为高效、纯净的数据基础。

为了更好地表示局域网加密流量,获取握手阶段的 TLS 记录数据,并将这一阶段单条加密会话的原始字节表示为:

$$R(i) = (v_1^i, v_3^i, v_3^i, \cdots, v_m^i)$$

(6)

式中, R 表示握手阶段加密会话对应的原始字节, i 表示加密会话编号, v 表示字节, m 表示单条加密会话中字节总数。应用一维卷积网络,设计如图 1 所示的加密流量表示架构。

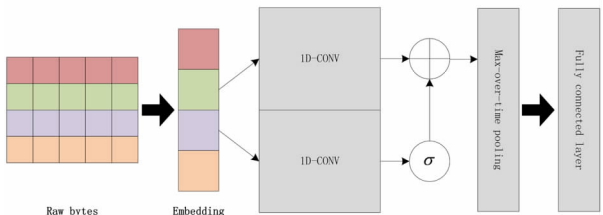


图 1 网络加密流量表示

如图 1 所示,将原始字节输入其中,完成特征向量的分析和映射,即可得到原始字节流量表示结果为:

$$H(i) = D(e(R(i)))$$

(7)

式中, H 表示流量表示结果, D 表示一维卷积网络计算函数, e 表示映射函数。

1.3 构建图神经网络恶意流量检测模型

以图神经网络为基础,构建如图 2 所示的恶意加密流量检测模型。将基于流量表示结果构造的流量交互图上传到图神经网络中^[8],通过网络层的学习和分类,划分正常流量与恶意流量^[9]。

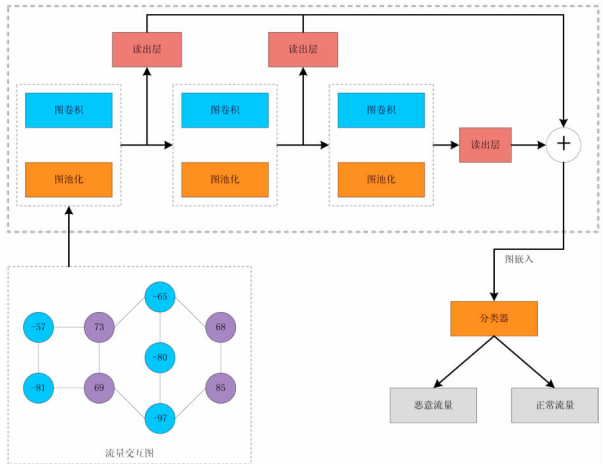


图 2 图神经网络分类模型

图 2 所示的智能分类模型投入应用时,在特征提取环节融入共享线性变换权重矩阵,最终得到加密流量数据特征提取结果为:

$$h'_k = Wh_k$$

(8)

$$\eta'_k = \sigma(\sum_{q=1}^Q \alpha_{q,k} Wh'_k)$$

(9)

式中, k 表示加密会话节点, h 表示最初提取特征, h' 表示优化后特征表示向量, W 表示共享线性变换权重矩阵, l 表示 TLS 记录长度, σ 表示激活函数, Q 表示邻居节点数量, q 表示邻居节点编号, η 表示聚合后形成的特征矩阵。

将公式(9)给出的特征信息代入到分类过程中,即可实现恶意和正常流量的自动划分。

$$Y = \lambda[W(\eta \parallel \tilde{\omega}) + g]$$

(10)

式中, Y 表示加密流量检测标签, λ 表示分类器计算函数, $\tilde{\omega}$ 表示特征差异度矩阵, g 表示偏置量。

依托于图神经网络模型,检测出局域网通信过程中产生的所有恶意流量,将其从加密会话中剔除,保证通信流量的安全。

1.4 基于量子密钥分发协议实现安全通信

由于局域网通信传输的均是密文信息,对其进行安全解密是实现网络安全通信的核心环节^[10]。对此,将量子密钥分发协议引入到通信解密阶段,以量子为信息载体,帮助通信用户生成不可复制的安全密钥,实现对加密会话的有效解析^[11]。其中,量子密钥分发工作原理如图 3 所示。

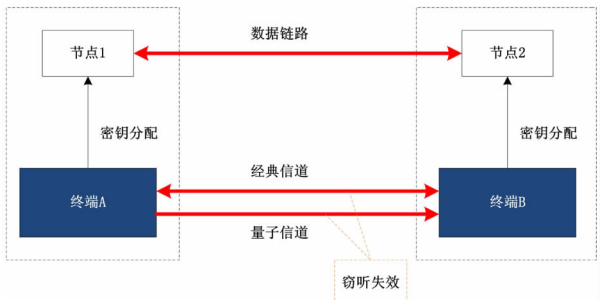


图 3 量子密钥分发点对点工作原理

依靠量子密钥分发协议生成密钥之前,需要在局域网环境中,由通信双方各自准备多个贝尔态,作为量子密钥分发的基础资源,信息发送方和接收方选择数量相同的粒子组成粒子序列,确保二者各自持有一半的纠缠粒子对。接下来,信息发送方将粒子序列发送给接收方,并告知对方已完成传输。接收方在确认收到后,同样将粒子序列发送给发送方,这种双向传输机制增加了通信的复杂性和安全

性,避免传输过程中出现拦截或篡改。

网络通信接收方得到传输过来的粒子序列后,任选几个组成检测样本集,并统计每个粒子样本的所处位置、测量基,将这些信息全部告知信息发送方,发送方对目标粒子获取同样信息,对比接收方给出的信息,若二者之间的相似度低于预设阈值,代表本次局域网通信可能受到了攻击,直接放弃通信。

在确认信道安全后,双方去除用于检测的粒子,剩下的粒子将用于生成密钥。该阶段信息双方需要对不同序列中相同位置的粒子进行贝尔测量,参考贝尔测量结果,制定密钥规则为:

$|\varphi^+\rangle \rightarrow 00, |\varphi^-\rangle \rightarrow 01, |\psi^+\rangle \rightarrow 10,$
 $|\psi^-\rangle \rightarrow 11$

(11)

式中, $\varphi^+、\varphi^-、\psi^+、\psi^-$ 表示四种贝尔态。

根据调整后的密钥生成结果,解析加密通信会话,即可实现局域网安全通信。

2 实验

参考某电力公司无线局域网架构,搭建如图 4 所示的实验网络。

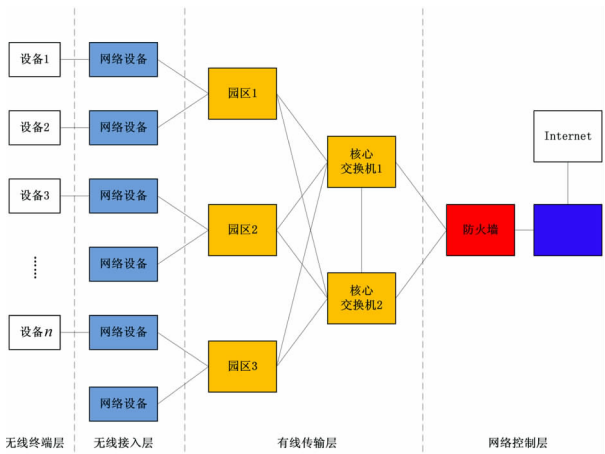


图 4 无线局域网架构图

如图 4 所示的无线局域网环境中,添加另外三台计算机,模拟字典攻击、中间人攻击和重放攻击,干扰局域网通信过程。

将新提出的安全通信技术,和另外两种常用的方法(基于 SecOC 的安全通信模型、基于多 IRS 辅助的安全通信方法)分别应用到上述实验环境中,观察各方法实施效果,从而判断新技术是否值得推广应用。

依靠图神经网络检测网络加密通信过程中存在的恶意流量时,设置各项超参数如表 1 所示。

表 1 图神经网络超参数设置

参数项	数值或名称
训练轮数	100
隐藏层节点数量	128
学习率	0.01
权重衰减系数	0.001
激活函数	ReLU
优化器	Adam

通过图神经网络的学习和分类,加密流量数据可以被明显区分为正常流量和异常流量两类,二维可视化显示结果如图 5 所示。

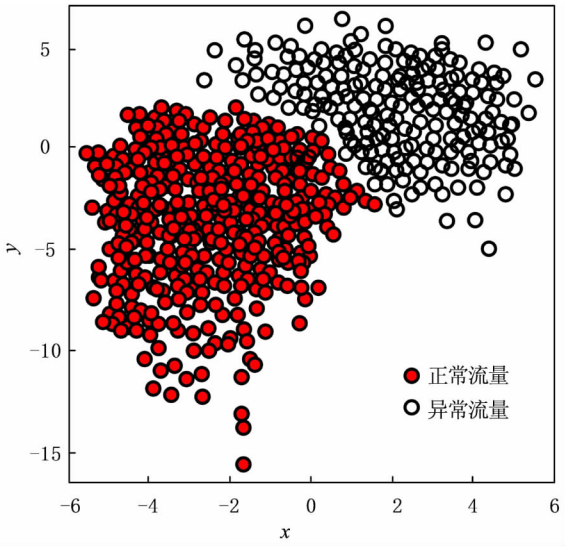


图 5 恶意流量检测结果可视化

从图 5 可以看出,图神经网络的应用实现了两类流量的明显区分,将恶意流量从加密会话中剔除,剩余正常流量数据参与后续局域网安全通信环节。

通信信息的加密结果和恶意检测结果如图 6 所示。

从图 6 可以看出,原始通信数据通过加密处理,转化为一系列密文数据,避免了不符合要求的局域网访问用户获取通信内容。而红色标注区域就是受到攻击影响出现的恶意流量,其与正常密文代码存在明显差异。

恶意流量数据剔除后,利用量子密钥分发协议,可以实现攻击场景下局域网安全通信。满足安全通信要求的用户,最终可以得到如图 7 所示的解密效果。

从图 7 可以看出,基于图神经网络与量子密钥分发协议的通信技术为无线局域网通信安全提供了有效保障,达到了预期设计要求。

