面向物联网多设备通信的边缘计算网络安全监测管理系统研究

武少鹏[1]
WU Shaopeng

摘 要 随着第五代移动通信技术（5G）的快速落地，为物联网及工业互联网场景下的大规模设备接入、云数据通信传输创造条件。但与此同时，移动边缘计算（mobile edge computing, MEC）网络的上下行链路数据传输，却频繁面临分布式拒绝服务（distributed denial of service, DDoS）、远程非授权访问（remote-to-login, R2L）、用户提权（user to root, U2R）、探测（Probe）等越权攻击威胁。为此，基于（client-server, C/S）网络架构、SDN（software defined network）控制器、网络路由、核心交换机、SQL Server 数据库、边缘云服务器等软硬件技术，构建起内生边缘计算网络安全管理系统，利用 IDS（intrusion detection system）入侵探测器组件监测多网络节点的入侵数据流量，使用 LSTM（long short-term memory）网络算法作出入侵访问数据流量的时序提取及分类，采用区块链 DID（decentralized identifier）认证机制验证接入用户身份，最大程度保障网络入侵数据监测、系统防护管理的安全性。

关键词 物联网；多设备通信；边缘计算；网络安全管理系统

doi：10.3969/j.issn.1672-9528.2025.10.022

0 引言

传统基于复合型防火墙、静态 / 动态路由协议的网络安全访问验证管理模式，通常难以抵御入侵主机伪造 IP 地址、伪造 ARP/Hello 请求报文等越权访问攻击。且随着 5G 移动通信网络中海量化的设备联网、数据流量接入传输，传统依托网络防火墙、代理网关的入侵访问检测过滤模式，面临着任务处理的拥塞或溢出问题。在这一背景下，引入融合 SDN 软件定义网络、NFV（network functions virtualization）功能虚拟化模型等组件的边缘计算技术，在云服务器内设置虚拟化网络的分布式边缘网元节点，启用区块链 DID 认证机制，为跨域入侵用户访问、设备终端数据通信提供分布式身份认证、安全运维管理服务，解决物联网安全监测控制执行效率

1. 武警内蒙古总队乌兰察布支队 内蒙古乌兰察布 012000

[6] SHI J, ZHOU Y F ,LI Z, et al. Delay minimization for NOMA-mmW scheme-based MEC offloading[J]. IEEE internet of things journal, 2022, 10(3): 2285-2296.

[7] SHI L Q, CHU X L,SUN H J,et al.Wireless-powered OFDMA-MEC networks with hybrid active-passive communications[J]. IEEE internet of things journal, 2023, 10(12): 10484-10496.

[8] HU Y L, YUAN X P, YANG T Y, et al. On the convex properties of wireless power transfer with nonlinear energy harvesting[J]. IEEE transactions on vehicular technology, 2020, 69(5): 5672-5676.

[9] HUA M, WU Q Q. Throughput maximization for IRS-aided MIMO FD-WPCN with non-linear EH model[J]. IEEE journal of selected topics in signal processing, 2022, 16(5): 918-932.

[10] MUSTAFA E, SHUJA J, ZAMAN S-K U, et al. Joint wireless power transfer and task offloading in mobile edge computing: a survey[J]. Cluster computing, 2022, 25: 2429-2448.

[11] DING Z G, XU D F, SCHOBER R, et al. Hybrid NOMA offloading in multi-user MEC networks[J]. IEEE transactions on wireless communications, 2022, 21(7): 5377-5391.

【作者简介】

段云阁（1998—），女，陕西渭南人，硕士研究生，研究方向：无线供电与移动边缘计算方向。

富爽（1982—），女，黑龙江大庆人，博士，副院长、教授，研究方向：认知无线电、信号传输与处理、无线携能传输和移动边缘计算。

（收稿日期：2025-03-07 修回日期：2025-10-16）

和精度不高的问题。

1 基于 5G 移动边缘组网模式的物联网多设备通信安全威胁问题

1.1 边缘计算节点的越权攻击安全威胁

DoS 或 DDoS 的分布式拒绝服务攻击，主要通过伪造的 IP 地址、MAC 地址、ARP/Hello 请求报文等向网络系统发送访问请求，占用计算机、后台服务器等设备的数据处理资源，使得正常的网络信道链路节点通信、请求响应及任务处理受到严重影响。在网络主机或服务器出现响应中断、瘫痪的情况下，边缘计算节点的物联网多设备接入将出现问题 [1]。恶意代码注入、XSS 跨站脚本、DNS 缓存投毒为非授权的分布式攻击类型。SQL 注入攻击是将结构化的 SQL 语言写入系统主机或应用程序，通过主机互相感染造成错误指令、虚假数据的散布传播；XSS 或 DNS 攻击则是通过操纵 DNS 记录，引导用户进入恶意 IP 网站，篡改或窃取其访问账号、密码信息，导致其他设备接入的数据泄露问题。

1.2 恶意网关接入系统攻击的安全威胁

恶意网关接入攻击包括 MITM 中间人攻击、恶意节点攻击等类型。MITM 中间人攻击是在主机与主机、用户与主机发生合法通信时，拦截网络信道的正常数据，嗅探、窃听和篡改系统数据信息，使得用户身份被冒充、数据泄露或完整性被破坏。在广场、商场、车站等公共物联网场景中可能发生中间人攻击问题。恶意节点攻击是在非授权主机用户访问后，主机用户控制边缘云服务器的网络节点，对传入 / 传出的节点通信信息作出控制，包括向核心网络发送虚假数据信息、向接入设备发送错误指令信息，恶意节点攻击相比 MITM 中间人攻击有着更大的威胁性、破坏性。

2 基于 C/S 架构的物联网通信边缘计算安全监测管理系统架构建设

在物联网主机用户接入的智能网络流量控制、安全监测管理中，基于 MVC 软件框架、C/S 服务器 - 客户机网络架构、SQL Server 数据库、边缘云服务器、认证服务器、SDN 控制器、网络路由、核心交换机等软硬件技术，建构涵盖基础层、核心网通信层、安全监测与调度层、身份验证层的内生边缘计算网络管理系统，经由 POSIX 等 API 标准接口形成用户接入访问、应用进程创建 / 终止、数据信号收发的通信连接 [2]，具体结构如图 1 所示。由边缘云服务器设置面向海量化数据任务处理的 VMWare 虚拟机、虚拟存储器、TaskDecomp 任务调度器等虚拟组件，负责响应外网、内网用户数据请求的任务调度操作。由 SDN 控制器将网络路由、交换机等设备的通信控制与转发功能相分离，配置出 SMF 会话管理功能模块、NFV 网络功能虚拟化模块等通信管理模块，SMF 模块负责网络用户对应用程序或服务访问的通信控制、端到端服务链的创建和修改，NFV 模块用于虚拟化硬件资源的分配和调度。

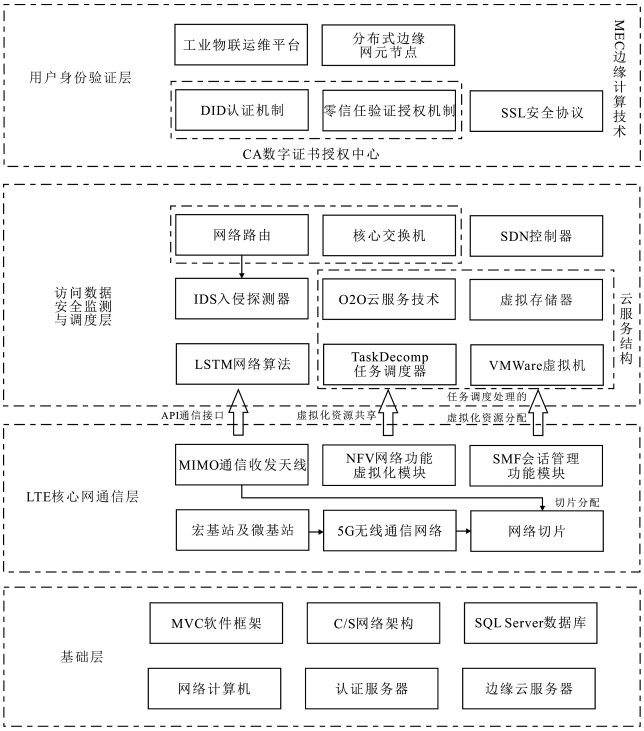

图 1 物联网通信边缘计算安全监测管理系统架构

由图 1 的物联网边缘计算网络安全管理系统结构可得，基于 5G 端到端组网技术可按需做出无线网络切片、逻辑隔离，为物联网通信的多样化应用场景、用户需求提供适配，边缘计算（MEC）节点靠近于接入网络用户端一侧，可对核心交换机处理后的网络数据提供请求响应、身份验证服务。先由部署于网络路由或核心交换机中的 Suricata/Snort 入侵探测器组件，实时监测采集 5G 无线网络接入的主机用户数据包流量、UDP 报文信息，经由网络路由防火墙的深度包过滤规则“Sip=192.168.1.10&dip=10.0.0.1”“src-mac=00:1A:2B:3C:4D:5E”“action=permit”、ACL 访问控制列表规则，作出一般入侵攻击用户的身份验证与过滤 [3]。引入 LSTM 网络算法负责入侵访问数据流量的时序提取及分类，配置于云服务中心的 DID 身份验证与授权机制，负责边缘计算节点越权用户访问的动态身份验证、授权管理。

3 基于 LSTM 算法的网络入侵用户数据流量时序提取及分类

3.1 基于 Haar 小波变换的图像冗余噪声过滤处理

为降低采集的入侵用户数据流量的噪声干扰问题，工业物联运维平台监控人员应根据正常数据的空间属性特征，合理设置数据信号频率阈值、信噪比阈值，而后对输入数据信号频率按照每 1 MHz 的带宽分为 N 个频点，作出包含底噪数

据信号样本的中值滤波、线性拟合等傅里叶变换（FFT），得到在信号中心频率附近均值加减后、不同频率点信号的自适应阈值[4]，具体计算公式为：

$$A_{\text{th}} = E\text{-}\sqrt{2}\sigma \cdot \text{erf}\frac{1}{1\text{-}2P} \tag{1}$$

式中：A_{th} 表示网络异常信号的频率阈值；E 和 σ 分别表示含有加性噪声的数据信号频率均值、频率方差；erf() 表示底噪误差函数；P 表示将噪声信号误判的恒虚警率。

随后使用 Haar 小波变换算法将采集到的不同频率信号进行噪声滤除处理，设定 Haar 小波变换函数的平移和伸缩尺度因子为 α、β，对采集到的高或低频率数据信号作出多阶小波变换处理，计算公式为：

$$\hat{\psi}_{\alpha,\beta}(t) = \frac{1}{\sqrt{|\alpha|}}\psi\left(\frac{t-\beta}{\alpha}\right) \tag{2}$$

$$\omega\left\{I_{\alpha,\beta}(t)\right\} = \frac{1}{\sqrt{|\alpha|}}\int_{+\infty}^{-\infty} I_0(t)\psi\left(\frac{t-\beta}{\alpha}\right)\text{d}t \tag{3}$$

式中：$\psi(t)$ 为入侵用户数据流信号的基本小波；$\hat{\psi}_{\alpha,\beta}(t)$为入侵用户数据流信号频率的快速傅里叶变换；$\omega\left\{I_{\alpha,\beta}(t)\right\}$为 Haar 小波变换后的信号频率谱，经过小波变换函数的尺度平移、尺度伸缩计算后，可得到噪声滤除后的高质量被测输入访问用户数据信号。

3.2 基于 LSTM 网络算法的入侵用户数据流量时序提取与分类

（1）数据流归一化处理。将噪声滤除后的入侵用户数据流量输入 LSTM 长短期记忆网络算法中，设置 LSTM 算法的输入 / 输出门、遗忘门的门控单元，作出不同边缘节点的数据流量监测。利用 LSTM 网络算法的 Sigmoid 激活函数、设置 [0,1] 范围内的门控输入 / 输出压缩值，进行入侵访问用户数据流量的时序属性特征提取，包括数据流量归一化处理、属性数据样本的概率预测，计算公式为[5]：

$$\text{Sigmoid}(\boldsymbol{x}) = \frac{1}{\exp \boldsymbol{y} + 1} \tag{4}$$

$$\text{ReLU}(\boldsymbol{x}) = \max\left(\frac{\exp \boldsymbol{y}\text{-}(\exp \boldsymbol{y})^{-1}}{\exp \boldsymbol{y} + (\exp \boldsymbol{y})^{-1}}, 0\right) \tag{5}$$

式中：Singmoid($\boldsymbol{x}$) 表示利用 sigmoid 激活函数作出入侵用户数据流属性向量的偏导，输出的用户数据流属性偏导矩阵值控制在 [0,1] 的范围内；$\boldsymbol{x}$ 和 $\boldsymbol{y}$ 分别表示入侵用户数据流量值、数据流量的属性特征值；ReLU(s) 表示对入侵用户数据流属性向量进行整流运算的非线性变换处理后的结果，比较 $\frac{\exp \boldsymbol{y}\text{-}(\exp \boldsymbol{y})^{-1}}{\exp \boldsymbol{y} + (\exp \boldsymbol{y})^{-1}}$和数值 0 后保留更大值。

（2）时序提取。由 LSTM 算法设置的遗忘门门控单元接收 t 时刻的数据属性，至当下时点，根据 t 时刻的输出数据属性状态 y_t、t+1 时刻输入至下一节点的数据属性状态 y_{t+1}，由遗忘门单元计算并保留有用的数据属性状态信息，计算公式：

$$f_{t+1} = \text{Sigmoid}\left(\boldsymbol{W}_f\left(y_t, y_{t+1}\right) + \boldsymbol{b}_f\right) \tag{6}$$

式中：f_{t+1} 为遗忘门保留 t+1 时刻有用数据属性状态信息的程度，f_{t+1} 趋近于 1 则表示保留有用数据属性状态信息、遗忘无用信息的程度越高；$\boldsymbol{W}_f(y_t, y_{t+1})$ 表示相连时刻节点输入、输出的数据属性状态参数矩阵；$\boldsymbol{b}$ 为算法偏置参数、控制数据属性特征提取的输入门偏置。

（3）分类输出。若入侵用户数据流属性包含 c 个类别，则对于属性类别为 j 的数据流，将 $\boldsymbol{W}_f(y_t, y_{t+1})$ 的数据属性状态参数矩阵设为 $\boldsymbol{h}_j = \boldsymbol{W}_f(y_t, y_{t+1})$，并基于 Softmax 分类器工具将完成时序属性提取后的入侵用户数据流进行空间归类，基于 Loss function 损失函数对归类后的入侵用户数据流与后台数据库的特征规则预测值进行非线性匹配对照，计算公式分别为：

$$\text{Softmax}(x_{t+1})_{\text{c}} = \frac{e^{h_c(x_{t+1})}}{\sum_{j=1}^{c} e^{h_j(x_{t+1})}} \tag{7}$$

$$\text{Loss}\left(y_t^c\right) = \frac{1}{n}\sum_{j=1}^{c}\left[y\log\left(O_t\right) + (1-y)\log\left(1-O_t\right)\right] \tag{8}$$

式中：x_{t+1} 表示在 t+1 时刻提取时序属性的入侵用户数据；$e^{h_c(x_{t+1})}$和$\sum_{j=1}^{c} e^{h_j(x_{t+1})}$分别表示单一类别、所有类别数据属性状态得分指数，则 Softmax$(x_{t+1})_{\text{c}}$ 表示输入入侵用户数据 x_{t+1} 属于第 c 个类别的概率；O_t 表示后台数据库特征规则的预测值；n 表示训练样本总数，当 y 和 O_t 值趋近于 1 时，交叉熵损失值趋近于 0，$\text{Loss}\left(y_t^c\right)$损失函数值趋近于无穷。根据损失函数输出误差与学习率成正比的设定，只有在$\text{Loss}\left(y_t^c\right)$损失函数值尽可能小的情况下，属性特征匹配误差才越小，因此需控制 $\text{Loss}\left(y_t^c\right)$损失函数值以提升数据分类精度。

4 基于 DID 认证机制实现入侵用户身份验证与授权

传统基于 CA 数字授权中心的 PKI（public key infrastructure）公钥基础设施认证模式，可能存在签发用户私钥泄露、单点认证失效等问题，因而本文使用区块链 DID 的去中心化标识符数字认证机制，设置边缘计算节点的系统公钥、非对称私钥，为每个入侵访问主机用户颁发可验证的数字签名、数字证书，作出主机用户数据流的身份双向认证，具体执行流程[6] 如下：

（1）主机用户向认证服务器的边缘计算节点发出跨中心身份认证请求 $x_i \rightarrow C_k$，认证服务器的数据中心收到请求后向其返回x_i:$\{\text{PK}_i \mid \text{Nonce}, \text{att}_k\}$，其中 Nonce 和 att_k 分别表示在模 p 下请求响应生成的随机数、随机数 Nonce 的原根，PK_i 为系统公钥。

（2）定义属性模 p 下的公开生成元为 G，整合属性机构的生成元 G、请求响应随机数原根 att_k，计算入侵主机用户明文数据加密后的密文，计算公式为：

$$R_i = G^{\mathrm{att}_k} \cdot \left(x_i \,|\, \mathrm{MSK}_i\right) \tag{9}$$

式中：MSK_i 为入侵用户私钥。

（3）由认证服务器基于 $e_u = (\mathrm{uid}_u, \mathrm{PK}_i, \mathrm{APK}_i)$ 的计算公式，验证入侵主机用户哈希标识符、应用公钥信息、传输至下一节点公钥信息是否正确，若正确则调用智能合约为用户颁发跨域通信的身份认证证书，将数字认证证书 $\mathrm{digital}_u$ 的区块链消息 (R_u, $\mathrm{digital}_u$, APK_i) 返回主机用户，由数字授权中心作出用户数字签名、数字证书的认证。

5 仿真实验及结果分析

5.1 实验环境设置

基于 Intel Pentium G6405 @3.8 GHz CPU 16 GB 1 TB 网络计算机、Linux 网络操作系统搭建 MATLAB R2022a 仿真软件的运行环境，选用 UNSW-NB15 数据集的 10 000 条数据作为实验数据集，合理设置数据信号频率阈值 ρ=0.9、信噪比阈值 S=20 dB，监测 DDoS 拒绝服务、R2L 远程非授权访问、U2R 提权、Probe 探测等越权攻击的出现情况。

5.2 实验结果分析

根据不同入侵数据包流量的属性特征，基于 LSTM 网络算法作出属性向量的偏导与整流运算，依照时序提取与保留有用的数据属性状态信息，基于 Softmax 分类器工具将呈散点分布的入侵用户数据流作出空间归类，利用 Loss function 损失函数对时序提取后的数据集进行特征规则匹配，算法迭代次数控制在 100 次以内，实验结果如表 1、图 2 所示。由表 1、图 2 的仿真实验结果可得，基于 LSTM 神经网络算法的入侵用户数据监测、时序特征提取与分类，数据信号监测分类准确率为 96.23%、召回率为 95.85%，显著优于改进 K-means 聚类算法，且随着仿真参与的入侵攻击数据量增加，基于改进 K-means 聚类算法的入侵用户数据集预测分类精度出现下降趋势，而 LSTM 神经网络算法的预测分类精度呈稳步增长，且迭代收敛的效率、F-score 更优，表现出良好的算法分类性能和鲁棒性，可辅助管理人员完成外网访问用户的安全监测工作。

表 1 基于 LSTM 神经网络算法的入侵用户数据流监测结果

监测算法	准确率 /%	召回率 /%	F-score	攻击监测结果数据量 / 个
LSTM 神经网络算法	96.23	95.85	0.93	Normal:7453; DOS:498; R2L:1542; U2R:121; PRO:386
改进 K-means 聚类算法	78.42	79.19	0.72	Normal:8405; DOS:329; R2L:601; U2R:243; PRO:422

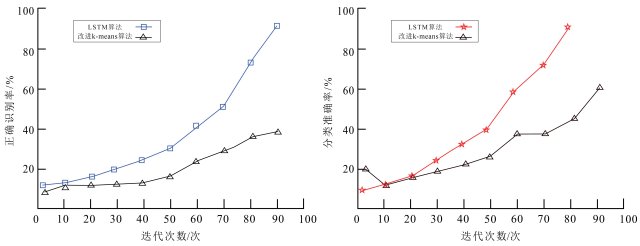

图 2 基于 LSTM 神经网络算法的入侵用户数据监测仿真结果

6 结语

边缘云服务器中网络功能服务的高度虚拟化，使得边缘网元节点极易受到 5G 网络接入用户的入侵攻击、通信数据截取，虽然核心云控制中心添加业务网关防火墙，但仍难以避免越权访问的网络攻击。因而在物联网多设备通信接入复杂环境下，利用软件定义网络的 SDN 控制器、NFV 功能虚拟化组件，将网络信道通信的用户主机接入控制、数据包转发功能相分离，面向边缘计算网络节点的用户入侵访问检测建立 n 元数据集属性模型，基于 Haar 小波变换、LSTM 长短期记忆网络算法对异常入侵用户数据流作出行为集度量分析，由 Haar 小波变换将采集的数据集分解为不同频率的子带、通过阈值过滤去除冗余噪声，再根据异常入侵用户数据流量的空间属性作出时序数据提取、数据分类存储管理，完成用户身份的 DID 认证验证与授权，提升网络安全监测防御管理水平。

参考文献：

[1] 杨柯 . 基于边缘计算的智能物联网网关关键技术及应用 [J]. 自动化应用 , 2024,65(6):158-160.

[2] 李飞翔 , 李宁 , 刘明哲 , 等 . 基于边缘计算技术的智能无人系统 [J]. 太赫兹科学与电子信息学报 , 2024,22(1):80-86.

[3] 孙宇彤 . 基于人工智能的边缘计算系统设计与实现 [J]. 科技创新与应用 , 2023,13(33):132-135.

[4] 李雪 , 包渝林 , 杨宇朗 , 等 . 基于负载均衡的边缘网络方案设计及应用 [J]. 中国交通信息化 , 2024(S1):443-445.

[5] 李云飞 . 信息安全在边缘计算中的重要性研究 [J]. 中国新通信 , 2024,26(5):41-43.

[6] 吴冬升 , 郑廷钊 , 郑泽彬 , 等 . 边缘计算在智慧交通和智能网联行业的应用分析 [J]. 自动化博览 , 2023,40(2):32-35.

【作者简介】

武少鹏（1986—），男，内蒙古呼和浩特人，本科，助理工程师，研究方向：密码通信。

（收稿日期：2025-04-21 修回日期：2025-10-11）