# 基于多尺度低秩模型的电力无线接入网异常流量检测方法

周伯阳[1],郭志民[1],王延松[2],阮 伟[3],吴春明[4],周 宁[1],张 伟[1],程国振[5]
(1. 国网河南省电力公司电力科学研究院,河南郑州 450000;2. 中兴通讯股份有限公司,江苏南京 210012;
3. 浙江大学控制科学与工程学院,浙江杭州 310027;4. 浙江大学计算机科学与技术学院,浙江杭州 310027;
5. 国家数字程控交换工程技术研究中心,河南郑州 450002)

**摘 要:** 电力无线接入网的安全性对于电网生产至关重要,然而由于其 IEC 60870-5-104 规约控制数据存在着高维度的特点,且无线信道质量动态变化,难以快速、有效地检测控制数据的异常. 鉴于此,本文提出了一种基于多尺度低秩的电力无线网异常流量检测器,首先构建一种规约深度分析的多尺度低秩模型,对其安全特征进行归一化和维度缩减,然后采用改进的递归特征选取和聚焦分类算法实现异常数据的检测. 实验结果表明异常流量分类的准确性和维度缩减的性能.

**关键词:** 电力无线接入网; IEC 60870-5-104; 多尺度低秩模型; 特征选择; 多维尺度分析; 异常流量检测
**中图分类号:** TP393 **文献标识码:** A **文章编号:** 0372-2112(2020)08-1552-06
**电子学报 URL:** http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.08.013

# An Anomaly Traffic Detection Method Using Multi-resolution Low Rank Model for Wireless Access Network of Electric Power Grids

ZHOU Bo-yang[1], GUO Zhi-min[1], WANG Yan-song[2], RUAN Wei[3], WU Chun-ming[4], ZHOU Ning[1], ZHANG Wei[1], CHENG Guo-zhen[5]
(1. *State Grid Henan Electric Power Research Institute, State Grid Henan Electric Power Company, Zhengzhou, Henan* 450000, *China*;
2. *ZTE Corporation, Nanjing, Jiangsu* 210012, *China*;
3. *College of Control Science and Engineering, Zhejiang University, Hangzhou, Zhejiang* 310027, *China*;
4. *College of Computer Science and Technology, Zhejiang University, Hangzhou, Zhejiang* 310027, *China*;
5. *National Digital Switching System Engineering & Technological R&D Center, Zhengzhou* 450002, *China*)

**Abstract:** The security of the wireless access network of electric power grids is critical for power grid productions. However, the control data anomalies are difficult to be detected in a fast and effective manner, due to the high dimension of the control protocol data in IEC 60870-5-104 protocol, as well as the dynamics on the quality of wireless channels. To this end, this paper proposes an anomaly traffic detector (ATD) for the wireless network of power girds based on multi-resolution low rank (MRLR) model. Firstly, the ATD is designed with the MRLR for the protocol, to regularize and reduce the security feature dimensions. Secondly, it utilizes the improved recursive feature selection and focused classification algorithms for accurate data anomaly detection. The results demonstrate the accuracy for the classification on data anomalies, and the performance for the dimensionality reduction.

**Key words:** wireless access networks for power grids; IEC 60870-5-104; multi-resolution low rank model; feature selection; multi-resolution analytics; anomaly traffic detection

## 1 引言

随着电网的智能化演进,大量的配电自动化终端,如配电终端单元、环网柜等,采用了基于 2G ~ 5G 无线通信的接入方式实现与配电网主站之间的遥控、遥测和遥信的信息交互. 然而,该无线通信网络中可能存在

收稿日期:2018-04-19;修回日期:2018-06-05;责任编辑:诸叶梅

诸多异常,如无线信号干扰、木马恶意攻击等[1],可导致电力通信网络性能下降甚至脱网、非法终端控制,引发设备误动等问题,影响电网业务的安全稳定运行和安全生产. 由于配电网无线接入的差异性,难以有效对网络数据监测策略进行定制,造成电力无线网中的配电自动化工控规约的异常通信数据难以被有效检测.

目前,配电终端常采用基于 IEC 60870-5-104 规约[2](简称 IEC 104)进行控制,IEC 104 规约应用服务控制单元(Application Service Data Unit,ASDU)可用于承载状态采集、命令传输、时钟同步、文件传输等业务数据,单个数据包可承载多个 ASDU,同时,由于多业务无线接入的信道质量动态性,其业务数据流量的吞吐量、延迟、数据包达到时间存在着动态变化特性. 因此,其流量具有特征维度高、规律性强、非线性的特点,导致异常流量检测处理时间长、实时性差等,然而选择较少的特征可能会导致畸形数据包、木马、缓冲区溢出等攻击类型难以被发现. 因而,选择合适的数据降维方法和构建高效率的安全检测算法模型,对于实现实时的配电网安全检测,具有重要的意义.

为提升无线核心网的灵活性,软件定义网络(Software-Defined Networking,SDN)成为了新型无线核心网的架构范例[3],可与 2G ~ 5G 的无线核心网设备进行无缝对接,用于承载 IP 数据业务,它采用了区分服务类型的业务承载分片、细颗粒度的数据流转发控制等技术,显著提高数据传输的实时性和可靠性. SDN 通过把路由控制逻辑集中到控制器中,将传统的分布式路由控制改变为集中式的网络控制,允许控制器对底层的交换机数据流进行动态实时的测量与采样,并运行复杂的数据分析算法对网络的安全威胁或异常进行动态检测.

为此,本文提出一种采用 SDN 电力无线异常流量检测器(Anomaly Traffic Detector for wireless network of power girds,ATD),ATD 对底层的交换机设备进行实时采样与异常检测,实现快速准确的异常流量检测. ATD 采用了一种面向 IEC 60870-5-104 规约数据无线接入的多尺度低秩模型(Multi-Resolution Low Rank model for IEC 104,MRLR-104)对配电网数据进行归一化和维度缩减,该模型充分考虑基于 IEC 104 规约的配电网中遥测数据的监测过程及网络安全特性;然后,ATD 采用改进的递归分类算法、聚焦分类算法实现针对 IEC 104 规约异常数据的准确检测,实现对非线性特征数值的快速准确分类.

## 2　相关工作

关于配电网工控协议的异常流量检测是一个热点问题. 尚文利等人提出基于 Modbus TCP 流量模式序列频率统计的粒子群异常检测方法[4];姜红红等人提出基于局部异常因子和支持度向量域的电力异常流量的分类方法[5];Yang 等人提出采用有限状态机分析 IEC 104 规约控制过程的中间人攻击检测方法[6];Udd 等人提出基于 IEC 104 数据包到达间隔时间异常检测的方法[7]. 然而,上述研究未涉及到对 IEC 104 规约承载数据的深度数据包解析与异常检测,难以防御传感器数据篡改攻击.

关于 IEC 104 异常流量分类实时性与准确性的主要工作如下:Soule 等人提出基于 Kalman 滤波器的 DoS/DDoS 攻击检测方法[8];刘永庆等人提出基于 Markov 链主机异常方法[9];Silveria 等人提出一种基于经验模型和小尺度数据流相关性分析方法[10];大量研究工作提出了基于主成分分析的流量矩阵异常状态的检测方法[11~13];闫伟等人提出基于小波阈值和回声状态网络的时间序列异常流量检测方法[14]. 然而,上述研究工作未考虑应用层数据异常的深度分析. 程国振等人提出基于多尺度低秩模型的异常流量检测方法,动态学习“适合”的流特征并进行快速分类[15],可应用于大量的流特征异常状态特征筛选,本文改进了该方法,将其应用于配网 IEC 104 数据异常检测中.

## 3　多维尺度分析的电力无线异常流量检测

### 3.1　架构与设计

如图 1 所示,所提出的面向多维尺度低秩模型的电力无线网异常流量检测器作为一个 SDN 的控制服务运行于 OpenFlow 控制器[3]之上,ATD 与无线核心网设备相连接. 在运行中,ATD 首先要对底层 IEC 104 规约进行适配训练,然后对底层的数据流异常状态进行识别、预警和阻断. 在分类模型的训练方面,考虑到 IEC 104 规约数据通常流量较小,ATD 首先通过将底层被监测的规约数据流量发送到 OpenFlow 控制器,以实现对控制面对于数据流的监测;然后在控制器上提取 IEC 104 规约数据及其通信信道特征,通过 104-MRLR 模型对特征进行降维、训练分类模型,实现快速训练和数据流的动态适配. 在异常流量识别方面,ATD 对底层数据流进行采样导入到控制器中,对数据流的异常状态进行动态识别、预警和阻断.

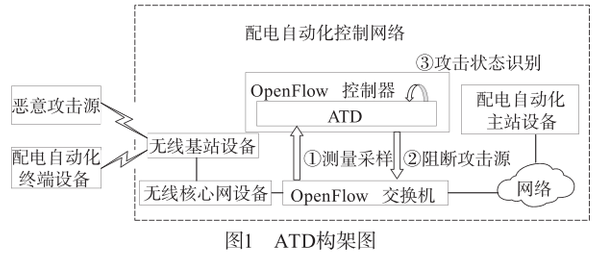


图1　ATD构架图

### 3.2 IEC 104 规约与通信信道的安全特征提取

IEC 104 帧分为 I 帧、U 帧和 S 帧,其中 I 帧用于传输业务数据(用于承载配电网设备遥测消息的传输,以及配电主站向配电终端发送的时间同步消息、遥控命令消息等),单个 I 帧的安全特征可定义为向量 $\boldsymbol{\Phi}=[t,a,w,l,\boldsymbol{A}']$,其中,$t$ 为该帧的到达时间;$a$ 是配电自动化终端的 IP 地址;$w$ 是 TCP 的拥塞窗口大小(反映出终端发送的);$l$ 是帧的长度(字节);$\boldsymbol{A}'$为集合 $A$ 中所有数值的向量化展开,$A$ 是一个应用服务数据单元(Application Service Data Unit,ASDU)中域值的集合化表示,$A=\{a_i\mid a_i=(\sigma_i,H_i)\}$,其中 $H=\{h_i\mid h_i=(\xi_i,v_i)\}$,包括如下字段数值:$\sigma$ 是 ASDU 单元对应的地址(对应具体设备的标识),$H$ 为采样数值的集合,$\xi$ 和 $v$ 分别是传感器的 IO 地址(IOA)以及传感器的数值,在 $\boldsymbol{\Phi}$ 的整体结构方面,单个 $\boldsymbol{A}'$可包括多个 $A$ 的数值,$A$ 中的每个元素可包括多个传感器 I/O 地址(IOA)及其传感器的数值信息(记作 $H$). U 帧分别用于 IEC 104 帧的传输控制,S 帧由接收方向发送方反馈最后一帧的帧编号. 由于端到端加密和身份认证的不足,$\boldsymbol{\Phi}$ 存在规约数据伪造、数据监听等安全隐患,因而监测 $\boldsymbol{\Phi}$ 具有重要意义.

然而,IEC 104 规约中 $A$ 及其 $H$ 的元素数量存在着不确定性,与配电终端设备数量和传感器规模有着直接关系. 同时在配电网运维中,配电终端设备存在着传感器和设备的动态开闭情况,导致监测到数据维度可发生动态的变化. 在基于 TCP/IP 的以太网中,因此单个 IP 帧中能传输传感器数值对的理论最大数量为$\lfloor \mathrm{MTU}/8-8.25 \rfloor$,其中 MTU(Maximum Transport Unit)为最大传输单元数值.

### 3.3 面向 IEC 104 规约的多尺度低秩降维

假设 IEC 104 规约中可标识异常的流特征对象为矩阵 $\boldsymbol{X}=[\hat{\boldsymbol{\Phi}}_1,\hat{\boldsymbol{\Phi}}_2,\cdots,\hat{\boldsymbol{\Phi}}_n]$,其中$\hat{\boldsymbol{\Phi}}_i$是对$\boldsymbol{\Phi}_i$平面化(flatten),使得 $|\hat{\boldsymbol{\Phi}}_i|=\max_i(|H_i|)$,$\hat{\boldsymbol{\Phi}}(t)$表示多维特征的时间序列构成的向量,每个特征是在一定的时间段内统计得到的,经过多个连续的时间段的统计形成特征时间序列. 由于 $X$ 存在着高维度的特性,需采用多尺度低秩模型对其进行维度简约,以增加实时处理能力. 104-MRLR 模型采用启发式和特征数值计算相结合方式对 IEC 104 数据进行降维. 对于每个 IEC 104 规约数据包的特征向量 $\hat{\boldsymbol{\Phi}}$,单个 ASDU 的数值范围大,同时由于 ASDU 所采集传感器的数量存在不确定性,使得 $\hat{\boldsymbol{\Phi}}$ 维度不确定,需要对 $\hat{\boldsymbol{\Phi}}$ 进行数据降维. 算法 1 给出了 104-MRLR 数据降维的算法描述,执行步骤如下:

(1)对 ASDU 数据进行归一化,由于 IOA(I/O Address)位宽达 24 位,其传感器浮点数值位宽为 32 位,然而由于配电台区终端设备数量有限,因而 IOA 数值集合大小存在着上限,故将 IOA 数值通过哈希表的方式映射到一个有限集合中.

(2)对传感器数值降低精度以提高后续的异常状态分类效率,假定传感器数值符合正态分布,对传感器数值进行数据标准化,形成不同的数值状态估计,这是由于处于异常状态的传感器数值由于数据篡改等攻击原因会造成数值大幅度的偏离,而正常数值同行变化范围较小. 将映射后的 IOA 及其变换后的数值追加到相应的 $\hat{\boldsymbol{\Phi}}$ 向量中.

(3)将 TCP 拥塞窗口、数据包长度等 IEC 104 底层的信道通信特性增加到相应的 $\hat{\boldsymbol{\Phi}}$ 向量中.

(4)将高维度的数据 $\boldsymbol{X}$ 映射到低维度中,假设距离邻近度矩阵 $\Delta=[\sigma_{ij}]$,其中 $\delta_{ij}$为向量$\hat{\boldsymbol{\Phi}}_i$ 和$\hat{\boldsymbol{\Phi}}_j$ 之间的欧几里得距离. 目标是寻找一个新数据映射点矩阵 $\boldsymbol{Y}=[y_1,y_2,\cdots,y_m]$,使得式(1)最小化,其中 $\delta_{ij}^X=\|\hat{\boldsymbol{\Phi}}_i-\hat{\boldsymbol{\Phi}}_j\|^2$,$\delta_{ij}^Y=\|y_i-y_j\|^2$,则 $\boldsymbol{X}$ 到 $\boldsymbol{Y}$ 的具体映射方法为:通过已知的 eigen 函数计算 $\Delta$ 矩阵的特征值 $\boldsymbol{\Lambda}$ 及其特征矩阵 $\boldsymbol{V}$,其中 $\boldsymbol{H}=\boldsymbol{I}-n^{-1}\cdot\boldsymbol{1}_n\times\boldsymbol{1}_n$;然后从 $\boldsymbol{\Lambda}$ 中选取前 $p$ 个特征值及其特征向量,组成新的特征向量$\boldsymbol{\Lambda}'$及其新的矩阵 $\boldsymbol{V}'$;最后计算出 $\boldsymbol{Y}=\boldsymbol{V}'\times\boldsymbol{\Lambda}'^{1/2}$.

$$\min_Y\sum_i\sum_j(\delta_{ij}^X-\delta_{ij}^Y)^2 \tag{1}$$

算法 1 的执行时间复杂度分析如下:步骤 1 和 2 所需的执行时间均为 $O(|\boldsymbol{A}'|)$,步骤 3 所需执行时间为 $O(|\boldsymbol{X}|^3+|\boldsymbol{X}|^{2+}|\boldsymbol{X}|^2\cdot q+p\cdot q)$,其中 $q=|A|/|\boldsymbol{X}|$,即每个终端的平均传感器数量,因此总的时间复杂度为 $O(|\boldsymbol{X}|^3+(|\boldsymbol{X}|^2+p)\cdot q])$. 算法 1 执行的空间复杂度为 $O(|\boldsymbol{X}|\cdot q^2+|\boldsymbol{X}|^2+|\boldsymbol{X}|\cdot p)$.

**算法 1 104-MRLR 算法:104-MRLR($X$,$p$,$r$)**

**输入:**

$\boldsymbol{X}$: A matrix of the detected features of flows in IEC 104.

$p$: The number of columns of $\boldsymbol{Y}$ after the reduction on $\boldsymbol{X}$.

$r$: The size of a set ($M$) for recording sensor values.

**输出:**

$\boldsymbol{Y}$: The output matrix reduced from $\boldsymbol{X}$ by the algorithm.

$G=\varnothing$; $M=\varnothing$; // $G$ and $M$ are two hash map sets.

$\hat{\boldsymbol{\Phi}}_{1\le i\le e}=[\,]$, $e$ is the number of columns of $\boldsymbol{X}$

Foreach column vector $\hat{\boldsymbol{\Phi}}_i$ in $\boldsymbol{X}$ do

  For each value $a_j$ in $\boldsymbol{A}'$ of $\hat{\boldsymbol{\Phi}}_i$ do

    For each pair $(\xi_k,v_k)\in a_j$ do

      If $G[\xi_k]=\varnothing$ then

        $G[\xi_k]=[\,|G|_{\text{keys}}+1\,]^{\mathrm{T}}$ // $G[\xi_k]$ refers to a col. vector

      End if

      //The $\boldsymbol{U}$ below is a column vector referred from $M[\xi_k]$

      $\boldsymbol{U}=M[\xi_k]$, $\boldsymbol{U}=[\boldsymbol{U};v_k]$

      Remove the rest elements of $\boldsymbol{U}$ except the top $r$ elements recently added.

      If $|\boldsymbol{U}|=r$ then

        $\boldsymbol{U}'=(\boldsymbol{U}-\mathrm{mean}(\boldsymbol{U}))/\mathrm{var}(\boldsymbol{U})+\min(\boldsymbol{U})$

$\boldsymbol{\Phi}_i = [\boldsymbol{\Phi}_i; G[\xi_k]; \boldsymbol{U}']$
End if
End for
$\boldsymbol{\Phi}_i = [\boldsymbol{\Phi}_i; w; l]$　　//Add TCP CWnd & packet length
End for
End for
$\delta_{ij} = \| \boldsymbol{\Phi}_i - \boldsymbol{\Phi}_j \|^2, \boldsymbol{H} = \mathbf{I} - n^{-1} \cdot \mathbf{1}_n \times \mathbf{1}_n$
$(\boldsymbol{\Lambda}, \boldsymbol{V}) = \text{eigen}(\boldsymbol{H} \times [-0.5 \cdot \delta_{ij}^2] \times \boldsymbol{H})$
$\boldsymbol{Y} = \boldsymbol{V}' \times \boldsymbol{\Lambda}'^{1/2}$//$\boldsymbol{\Lambda}'$ and V′ are vectors and their eigen values from $\boldsymbol{\Lambda}$ with the top-p eigen values.

在 104-MRLR 模型中,由于 ASDU 存在大量的终端和传感器,通常对于单个设备的攻击仅会造成少量的传感器数值发生变化,或者造成设备通信链路的拥塞和传感器数据延迟到达等情况. 该类异常呈现出局部集聚特性,单个异常仅反映在少数的流特征上,常见流量异常的发生仅导致低维流特征表现为异常. 从矩阵的角度分析,低秩与稀疏性相似,因为低秩矩阵的奇异谱是稀疏的. 值得说明的是,传统地检测异常的方法均假设异常改变了正常流量的结构特性.

### 3.4　IEC 104 规约与通信信道的安全特征提取

考虑配电网对于异常分类实时性和准确性的要求,在文献[15]基础上,一方面,增加了由该文献所提出的递归缩减特性算法(Recursive Reducing Features, RRF)针对 104 规约数据与底层信道通信特性的深度分析,具体 RRF 算法改进如下:

(1)对偏离函数 $V(\cdot)$ 进行适配,增加触感器数值变化的敏感,使之更快速地检测出 $\boldsymbol{Y}$ 的异常状态值,$V(\boldsymbol{y}_i) = |\boldsymbol{y}'_i - \text{mean}(\boldsymbol{y}'_i)|/\text{var}(\boldsymbol{y}'_i)$,其中 $\boldsymbol{y}'_i = \partial/\partial(\boldsymbol{y}_i)$ 即 $\boldsymbol{y}_i$ 对时间 $t$ 的一阶导数;

(2)对 reduce 和 augment 函数进行了适配,令 reduce($\Psi$) = $\Psi/2$, argument($\Psi$) = $\Psi + K$,其中 $K$ 是常量,采用成倍减少、逐渐增加的方式,实现对于门限数值 $\Psi$ 的快速调整,这考虑到了 IEC 104 规约传感器的正常数值变化范围存在相对稳定的特性,而异常数据通常处于偏离数值.

另一方面,改进了文献[15]所提出的聚焦分类算法(Focused Classification Algorithm, FCA)对于 IEC 104 规约分类的适配,这是考虑到 IEC 104 规约数据异常表现出的不同规律性之间差异较大,在由 104-MRLR 模型生成的稀疏矩阵上表现尤为明显,文献[15]所提出的 FCA 算法直接使用效果并不理想,例如流量频繁波动的攻击行为,会导致流特征信号在高频区域出现较大值;相反,DDoS 这类攻击通常以填满带宽为目的,那么稀疏矩阵的非零值聚集在低频区域. 具体改进方法如下:

针对异常类型的分布规律,为不同的异常类型生成矩阵掩码,每次判定具体的异常类型时,过滤掉由其它异常带来的噪声干扰,以便能够精确地判定异常类型. 形式化地,假设异常类型集合 $C = \{c_1, c_2, \cdots, c_n\}$,类型 $c_i$ 对应于矩阵 $\boldsymbol{B}$ 的掩码矩阵为 $\boldsymbol{M}_i$,每次判定是否存在 $c_i$ 的异常前,首先进行掩码操作,即 $\boldsymbol{B}' = \boldsymbol{B} \cdot \boldsymbol{M}_i$,屏蔽可能存在的"噪声". 然后,再对 $\boldsymbol{B}'$矩阵应用 FCA($\boldsymbol{B}'$).

## 4　配电网异常流量检测性能评估

### 4.1　实验场景仿真场景设置

如图 1 所示,基于 FloodLight SDN 控制器实现了 ATD,底层数据面采用 NS-3 模拟器进行仿真,为真实模拟电力无线网数据,在交换机上重放采用了某地的 4G 电力无线专网数据(其中涵盖了 IEC 104 控制规约数据). 图 2 给出了该数据集上来自 142 个传感器的 IOA 及其所测量到的传感器数值均值以及 25 和 75 百分位的数值统计情况,很明显传感器数值在正常情况下处于稳定状态.

为模拟数据篡改、效果,在重放数据时对其中的一个或多个 ASDU 传感器数据、对数据包长度进行修改,来模拟攻击效果,造成传感器数值出现较大的误差,造成配电网主站产生底层配电终端设备的状态估计偏差,产生攻击效果;为模拟拒绝服务(Denial-of-Service, DoS)攻击效果,在重放数据时加大 TCP 拥塞窗口大小,从而模拟典型 104-MRLR 攻击类型,以验证 ATD 在配电网无线异常流量检测的有效性.

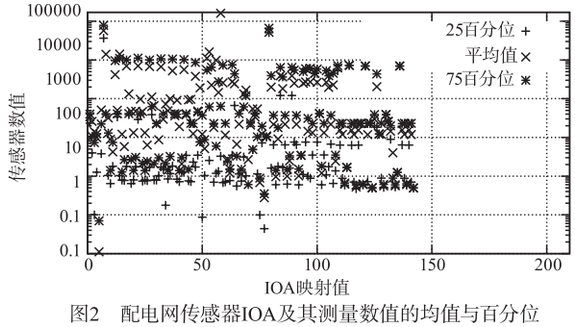

图2　配电网传感器IOA及其测量数值的均值与百分位

### 4.2　配电网 104-MRLR 模型性能测试

图 3 给出了配电网 104-MRLR 算法在不同的 IOA 输入规模 $|H|$ 下的运行时间执行效率,分别给出了 $q$ = 20、40、60 和 80 的 IOA 平均维度下的运行时间变化,以及相应的曲线拟合结果,分别如式(2)~(5)所示,其中假定 104-MRLR 算法的输入参数 $q = 100, p = 20$. 实验结果说明了该模型具备 $\boldsymbol{O}(|\boldsymbol{X}|^3 + |\boldsymbol{X}|^2)$ 多项式的时间复杂度.

$$f_{20} = 1.88 \cdot 10^{-9} |\boldsymbol{X}|^3 + 4.9636 \cdot 10^{-7} |\boldsymbol{X}|^2 + 0.0525 \tag{2}$$

$$f_{40} = 2.489 \cdot 10^{-10} |\boldsymbol{X}|^3 + 1.7854 \cdot 10^{-6} |\boldsymbol{X}|^2 - 0.0467 \tag{3}$$

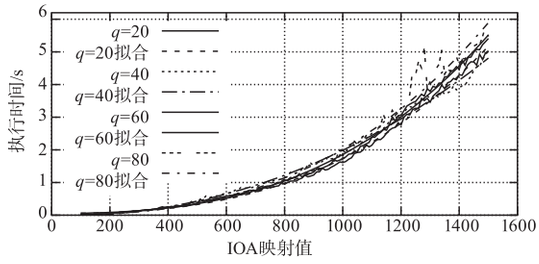


图3 配电网104-MRLR算法执行时间的测试结果

$$f_{60}=1.245\cdot10^{-9}|\boldsymbol{X}|^3+5.6124\cdot10^{-7}|\boldsymbol{X}|^2+0.0538 \tag{4}$$

$$f_{80}=1.192\cdot10^{-9}|\boldsymbol{X}|^3+8.3216\cdot10^{-7}|\boldsymbol{X}|^2+1.37\cdot10^{-6} \tag{5}$$

### 4.3 异常流量检测准确率与性能测试

关于异常检测有效性的采用 ROC(Receiver Operating Characteristics)曲线进行测试,该指标将真阳率(True Positive Rate,TPR)表示为假阳率(False Positive Rate,FPR)的函数,能有效测试出二进制分类算法的准确性. 对于某类正常的状态数值,定义某类网络状态攻击对系统的扰动系数 $u$ 为发送均值和方差 $u$ 倍的高斯随机数,因此设置不同的 $u$ 可产生对原有配网系统不同程度的扰动效果,进而影响 ATD 检测效果. 结合不同的 $u$ 数值,以产生不同类型攻击,图 4 给出了在不同攻击扰动程度下的 ROC 曲线,其中 RRF 门限值 $\Psi$ 定义了分类算法的敏感程度,实验结果中设置 $\Psi$ 在[0.5,1.5]范围内不同数值,异常密度 $r=0.3$[15],可以看出:当 $u$ 大于 2 时,ATD 检测算法具备较高的 TPR 而保持较低的 FPR,说明了该检测算法对于配电网异常流量检测的有效性.

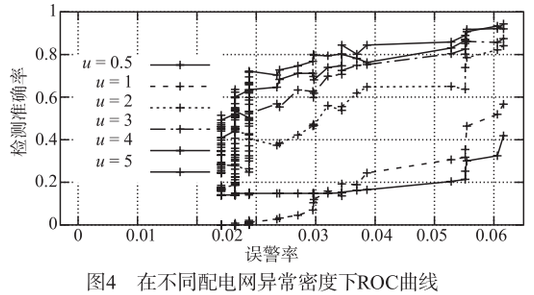


图4 在不同配电网异常密度下ROC曲线

## 5 结论

本文提出一种针对配电自动化无线网 IEC 104 规约的多尺度低秩模型,并改进了递归缩减特性算法. 该模型充分考虑了 IEC 104 规约的深度分析,对其进行了有效的数据降维,构建了高效的异常流量分类方法,满足配电自动化控制的实时性要求. 实验部分在真实业务数据集上进行测试与验证,结果验证了 104-MRLR 算法适用于配电 IEC 104 规约的高维度数据分析,能够有效检测出异常流量攻击,具备良好的分类正确性与性能.

### 参考文献

[1] 蔡昊,周欣,王宏延,等. LTE 电力无线专网业务安全风险分析及应对策略[J]. 电力信息与通信技术,2016,14(5):137 – 141.
H Cai,X Zhou,H Wang,et al. Service security threats analysis and strategies for LTE based wireless networks for electric power grids[J]. Electric Power Information and Communication Technology,2016,14(5):137 – 141. (in Chinese)

[2] IEC 60870-5-104-2006, Telecontrol Equipment and Systems. Part 5-104:Transmission Protocols[S].

[3] D Kreutz,F M V Ramos,P E Verissimo,et al. Software-defined networking:a comprehensive survey[J]. Proceedings of the IEEE,2014,103(1):10 – 13.

[4] 尚文利,张盛山,万明,等. 基于 PSO-SVM 的 Modbus TCP 通讯的异常检测方法[J]. 电子学报,2014,42(11):2314 – 2320.
W Shang,S Zhang,M Wan,et al. Modbus/TCP communication anomaly detection algorithm based on PSO-SVM [J]. Acta Electronica Sinica,2014,42(11):2314 – 2320. (in Chinese)

[5] 姜红红,张涛,赵新建,等. 基于大数据的电力信息网络流量异常检测机制[J]. 电信科学,2017,33(3):134 – 141.
H Jiang,T Zhang,J Zhao,et al. Traffic anomaly detection mechniam based on big data for information network in power grids[J]. Telecommunication Science,2017,33(3):134 – 141. (in Chinese)

[6] Y Yang,K Mclaughlin,S Sezer,et al. Stateful intrusion detection for IEC 60870-5-104 SCADA security[A]. PES General Meeting [C]. National Harbor,MD,USA:IEEE,2014. 1 – 5.

[7] R Udd,M Asplund,S Nadjm-Tehrani,et al. Exploiting bro for intrusion detection in a SCADA system[A]. The 2nd Workshop on Cyber-Physical System Security[C]. Xi'an,China:ACM,2016. 44 – 51.

[8] A Soule,K Salamatian,N Taft. Combining filtering and statistical methods for anomaly detection[A]. Conference on Internet Measurement[C]. Berkeley,CA,USA:USENIX,2005. 31 – 31.

[9] 刘永庆,刘东生. 基于马尔科夫链的主机异常检测方法研究[J]. 计算机与数字工程,2010,38(7):20 – 23.
Y Liu,D Liu. Research on host anomaly detection method based on Makov model[J]. Computer & Digital Engineering,2010,38(7):20 – 23. (in Chinese)

[10] F Silveira,C Diot,N Taft,et al. ASTUTE:detecting a dif-

ferent class of traffic anomalies[J]. ACM SIGCOMM Computer Communication Review, 2010, 40(4): 267-278.

[11] M Ding, H Tian. PCA-based network traffic anomaly detection[J]. Tsinghua Science & Technology, 2016, 21(5): 500-509.

[12] 钱叶魁,陈鸣. 面向 PCA 异常检测器的毒害攻击和防御机制[J]. 电子学报,2011,39(3):543-548.
Y Qian, M Chen. Poison attack and defense strategies on PCA-based anomaly detector [J]. Acta Electronica Sinica, 2011, 39(3): 543-548. (in Chinese)

[13] 郭小芳,李锋,宋晓宁. 一种基于 PCA 的时间序列异常检测方法[J]. 江西师范大学学报(自然版),2012(3):280-283.
X Guo, F Li, X Song. A time series anomaly detection method based on PCA[J]. Journal of Jiangxi Normal University(Natural Sciences Edition), 2012(3): 280-283. (in Chinese)

[14] 张军,闫伟. 基于时间序列分析的网络流量异常检测[J]. 吉林大学学报(理学版),2017,55(5):1249-1254.
J Zhang, W Yan. Network traffic anomaly detection based on time series analysis [J]. Journal of Jilin University(Science Edition), 2017, 55(5): 1249-1254. (in Chinese)

[15] 程国振,程东年,俞定玖. 基于多尺度低秩模型的网络异常流量检测方法[J]. 通信学报,2012,33(1):182-190.
GCheng, D Cheng, D Yu. Network traffic detection based on multi-resolution low rank model [J]. Journal on Commuincations, 2012, 33(1): 182-190. (in Chinese)

## 作者简介

**周伯阳**　男,1986 年出生,河南驻马店人,博士,高级工程师. 研究方向为电力无线通信安全、智能电网通信技术.
E-mail:boyang319@qq.com

**郭志民**　男,1977 年出生,河南南阳人,本科,教授级高级工程师,国网河南省电力公司电力科学研究院设备状态评价中心副主任,研究方向为电力系统自动化、电力信息安全.
E-mail:zhimin.guo@163.com

**阮　伟(通信作者)**　男,1969 年出生,新疆伊宁人,工学博士,教授级高级工程师. 2000 年浙江大学能源系硕士、博士毕业,现工作于浙江大学控制学院. 长期从事自动控制系统软硬件、优化控制策略的研究、现场工程应用等,承担多项科技部、工信部工业控制系统信息安全领域重大研究项目.
E-mail:ruanwei@zju.edu.cn