文章编号:1003－6199(2024)02－0156－06 DOI:10.16339/j.cnki.jsjsyzdh.202402026

基于快速时域关联规则发现算法的政务系统独立通信层信号安全检测模型

韩建良†

(绍兴市大数据保障中心,浙江 绍兴 312000)

摘 要:以保障政务系统通信传输安全为目的,设计基于快速时域关联规则发现算法的政务系统独立通信层信号安全检测模型。该模型通过计算政务系统独立通信信道频率响应,使用Anritsu信号分析仪采集独立通信层信号信息并进行归一化处理和平衡化预处理;利用快速时域关联规则得到独立通信层信号数据之间的关联规则,描述异常信号与正常信号之间的关系;经过网络迭代,依据独立通信层信号数据之间的关联规则输出其正常信号和异常信号类别,完成政务系统独立通信层信号安全检测。实验表明:该模型具备较强的信号采集能力、信号数据预处理能力以及信号安全检测能力,应用效果较佳。

关键词:快速时域;关联规则;政务系统;独立通信层;信号安全检测;深度学习

中图分类号:TP391 **文献标识码**:A

Signal Security Detection Model of Independent Communication Layer in Government Affairs System Based on Fast Time-domain Association Rule Discovery Algorithm

HAN Jianliang

(Shaoxing Big Data Security Center, Shaoxing, Zhejiang 312000, China)

Abstract: In order to ensure the security of communication and transmission in government system, a signal security detection model of independent communication layer in government system based on fast time domain association rule discovery algorithm is designed. The model calculates the frequency response of the independent communication channel of the government system, uses Anritsu signal analyzer to collect the signal information of the independent communication layer, and carries out normalization and balance preprocessing. The association rules between independent communication layer signal data are obtained by using fast time domain association rules to describe the relationship between abnormal signals and normal signals. After network iteration, the normal signal and abnormal signal categories are output according to the association rules between the signal data of the independent communication layer, and the signal security detection of the independent communication layer of the government system is completed. The experiment shows that the model has strong signal acquisition ability, signal data preprocessing ability and signal safety detection ability, and the application effect is better.

Key words: fast time domain; association rules; government affairs system; independent communication layer; signal safety detection; deep learning

政务系统是伴随着信息技术发展以及政府部门数字化办公需求应运而生的公务信息处理系统,其是连接政府和人民群众的纽带[1,2],也是政府部门由传统办公方式转向数字化办公的重要工具。

收稿日期:2023－02－03

作者简介:韩建良(1977—),男,浙江绍兴人,本科,高级工程师,研究方向:电子政务网络,政务云,设计建设与管理等。

† **通信联系人**,E-mail: luwu78724@163.com

政府系统内存在较多部门，每个部门互相独立且又存在业务关联，因此每个部门之间在政务系统内的通信方式为独立单层通信，该种类型通信方式传输信息不会存在拥堵现象[3,4]，信息安全性相对较高。但政务系统在应用中，会存在不法分子攻击入侵情况，所以检测政务系统独立通信层信号安全意义重大。目前也有很多学者针对信号安全检测展开研究，如许耀华等人[5]提出的 MIMO 系统信号检测算法，该算法通过采集独立通信层实时信号后，利用加速松弛迭代算法实现信号安全检测。李恒武等人[6]提出网络独立通信层信号安全检测方法，该方法使用多尺度小波包分析方法分析网络通信层内存在的干扰信号后，对该干扰信号进行 DEM 分解后，得到干扰信号阈值，再利用傅里叶变换与敏感数据检测方实现网络独立层信号安全检测。上述两种方法虽均可实现独立层信号安全检测，但均存在检测精度不足和检测及时性差的缺陷。

关联规则发现算法是大数据挖掘技术中的一种，其是从大量数据内遍历，依据关联规则信任度和支持度挖掘满足条件数据的算法[7]。该算法在识别、检索、特征提取等领域应用较为广泛[8]。在此本文从独立通信层信号时域角度入手，以关联规则发现算法为基础，提出基于快速时域关联规则发现算法的政务系统独立通信层信号安全检测模型，以提升政务系统通信安全性。

1　政务系统独立通信层信号安全检测模型

1.1　独立通信层信道状态信息采集

政务系统独立通信层在传输信号时，独立通信层信道会出现冲击响应，其表达公式如下：

$$h(t)=\sum_{i=1}^{N}\alpha_i(t)e^{-j\varphi_i(t)}(\tau-\tau_i(t)) \tag{1}$$

上述公式中，$h(t)$ 表示政务系统独立通信层信道冲击响应函数；N 表示子载波总数；$\alpha_i(t)$、$\varphi_i(t)$、$\tau_i(t)$ 分别表示第 i 条子载波在时刻为 t 时的振幅、相位、时延；j 表示虚数；e 表示正态分布函数；τ 表示载波通信时间。

对公式(1)结果进行快速傅里叶变换，可得到政务系统独立通信层信道频率响应，其表达公式如下：

$$Y=HX+N \tag{2}$$

上述公式中，Y 表示政务系统独立通信层信道频率响应数值，其为接收信号向量；X 表示独立通信信道发射信号向量；H 表示独立通信信道状态矩阵；N 表示独立通信信道内高斯白噪声。

利用 Anritsu 信号分析仪采集政务系统独立通信层信道频率响应的采样值，其表达公式如下：

$$H^n=[H_1^n,H_2^n,\cdots,H_{i-1}^n,H_i^n] \tag{3}$$

其中，

$$H_i^n=|H_i^n|e^{j\sin\angle H_i^n} \tag{4}$$

上述公式中，H^n 表示第 n 条信号分析仪天线对应的政务系统独立通信层信道频率响应的采样值矩阵；H_i^n 表示第 n 条天线的第 i 条子载波对应的信道频率响应采样值；$|H_i^n|$、$\angle H_i^n$ 分别表示第 n 条天线的第 i 条子载波对应的信道频率响应幅度和相位。

利用公式(3)即可得到政务系统独立通信层信道状态信息。

1.2　政务系统独立通信层信号安全检测模型构建

构建政务系统独立通信层信号安全检测模型，模型总体框架如图 1 所示。

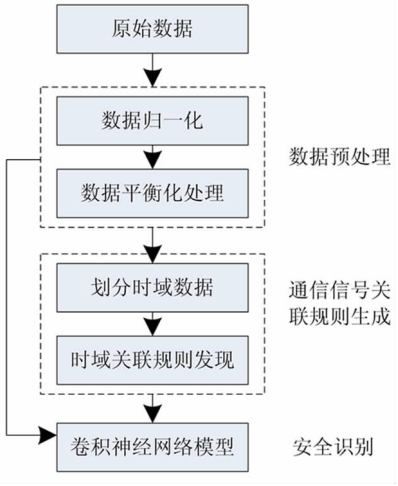

图 1　政务系统独立通信层信号安全检测模型

政务系统独立通信层信号安全检测模型将采集到的独立通信层信道状态信息作为原始数据，对该原始数据进行归一化处理后，再对其进行平衡化处理，完成数据预处理过程。然后对不平衡的独立通信层信号进行平衡化后，使用基于快速时域关联规则发现算法挖掘政务系统独立通信层信号之间的关联规则，再将预处理后的独立通信层信号和信号之间的关联规则输入到卷积神经网络模型内，卷积神经网络模型依据信号之间的关联规则，迭代识别出安全和存在不同类型网络攻击的系统独立通信层信号，实现政务系统独立通信层信号安全检测。

1.2.1 数据预处理

由于政务系统独立通信层信号内存在噪声，会出现奇异样本[9]，需对其输入的数据样本进行归一化处理，去除数据样本内的奇异样本，提升卷积神经网络训练速度和收敛能力[10]。在此先对采集到的政务系统独立通信层信号数据进行归一化处理，归一化表达公式如下：

$$y=(x-\min(z))\frac{1}{\max(z)-\min(z)} \tag{5}$$

上述公式中，y 表示政务系统独立通信层信号数据归一化输出数值；x 表示政务系统独立通信层信数据属性转换后的数值；$\max(z)$、$\min(z)$ 分别表示独立通信层数据属性转换后的最大数值和最小数值。

由于政务系统独立通信层信道经常受到攻击，导致正常信号和存在攻击的信号之间出现不平衡现象[11]，需对不平衡的政务系统独立通信层信号数据进行平衡化处理。在此使用综合采样人工合成数据算法（Synthetic Minority Oversampling Technique，SMOTE）对不平衡的政务系统独立通信层信号数据进行平衡化处理，其详细步骤如下：

第一步：当政务系统独立通信层信号数据为少数类中的随机样本时[12,13]，通过欧式距离方式计算该样本到其他样本的距离，依据该距离得到其 K 近邻，在近邻内选出前 N 个样本。

第二步：将选取的 N 个政务系统独立通信层信号数据样本与原始样本集结合，建立新的 N 个样本，其表达公式如下：

$$X_{\text{new}}=X+rand(y[i])-rand(X) \tag{6}$$

上述公式中，X_{new} 表示选取的政务系统独立通信层信号数据样本与原始样本结合后形成的新样本；X 表示选取的政务系统独立通信层信号样本的少数类样本集合；$rand$ 表示 0－1 区间任意选取常数的函数；$y[i]$ 表示 X 的第 i 个邻近样本，其中 $i=1,2,\cdots,N$。

第三步：经过上述步骤不断循环，即可生成较为平衡的政务系统独立通信层信号数据样本。

1.2.2 基于快速时域关联规则发现算法的信号关联规则挖掘

对政务系统独立通信层信号数据进行预处理后，使用基于快速时域关联规则发现算法挖掘政务系统独立通信层信号之间的关联关系，其关联关系可呈现异常信号和正常信号之间的差别[14,15]。

首先划分政务系统独立通信层信号数据的时域数据，时域数据是带有时间属性的政务系统独立通信层信号事务集，其表达公式如下：

$$T=\bigcup_{1\leqslant i\leqslant n}|T_i| \tag{7}$$

上述公式中，T 表示政务系统独立通信层信号时域数据集；$|T_i|$ 表示第 i 个政务系统独立通信层信号时域数据的时间长度，该时间长度为人工设置的；n 表示信号时域数据总数，且 $i=1,2\cdots,n$。我们的目的就是挖掘 $|T_i|$ 内政务系统独立通信层信号之间存在的关联关系。

其次使用挖掘关联关系频繁项集的 Apriori 算法挖掘 $|T_i|$ 内政务系统独立通信层信号之间存在的关联关系，其步骤如下：

第一步：设置政务系统独立通信层信号数据样本参数，其项目集、数据数据库、时域周期分别由 I、D、C 表示，事务最小支持度、最小信任度和最小时域分别由 $s_{\min}$、$c_{\min}$、$T_{\min}$ 表示，最小事务数量由 $COUNT_{\min}$ 表示。

第二步：依据政务系统独立通信层信号数据样本的时域周期，对其数据样本的分布进行动态距离处理，在每个事务涵盖的时域扩展项目集 I。

第三步：精简处理。令 L_k 表示涵盖 k 个项目的一般频繁项集，当 k 数值等于 2，且 L_{k-1} 为非空集时，由 L_{k-1} 生成涵盖 k 个项目的候选项目集，其由 C_k 表示。对 C_k 进行精简操作，扫描事务数据数据库 D，定义满足一般频繁项目集条件如下：

$$L_k=\{X\} \tag{8}$$

扫描数据库完成后，得到精简后的政务系统独立通信层信号数据样本的一般频繁项目集，其表达公式如下：

$$Result=\bigcup L_k\{1\leqslant k\leqslant n\} \tag{9}$$

第四步：强时域周期频繁集生成。扫描事务数据数据库 D，确定 $Result$ 内一般频繁项集是否为强时域周期频繁项集，若是，保留该频繁项集，反之，则删除。

第五步：强时域周期关联规则生成。

令 $AB[t_1,t_2]$ 和 $A[t_1',t_2']$ 均表示强时域周期频繁项集，且 $A[t_1',t_2']\in AB[t_1,t_2]$，其中 t_1、t_1' 均表示强时域周期起点；t_2、t_2' 均表示强时域周期终点，当 $AB[t_1,t_2]$ 和 $A[t_1',t_2']$ 满足下式时：

$$conf=\min\left\{\frac{support_{Ti}(AB[t_1,t_2])}{support_{Ti}(A[t_1',t_2'])}\right\}\leqslant c_{\min} \tag{10}$$

上述公式中，$support_{Ti}(AB[t_1,t_2])$ 和 $support_{Ti}(A[t_1^{'},t_2^{'}]$ 分别表示 $AB[t_1,t_2]$ 和 $A[t_1^{'},t_2^{'}]$ 的一般项集；$conf$ 表示约束条件。

则生成 $AB[t_1,t_2]$ 和 $A[t_1^{'},t_2^{'}]$ 快速时域关联规则如下：

$$Q = A \rightarrow B[T,t_1,t_2,conf,D] \tag{11}$$

经过上述步骤，得到政务系统独立通信层信号数据样本之间的关联规则，利用该关联规则描述正常信号和异常信号之间的关系。

1.2.3　构建卷积神经网络安全检测模型

将预处理后的政务系统独立通信层信号数据样本和数据样本之间的关联规则作为输入，使用卷积神经网络模型识别政务系统独立通信层信号中的安全信号和存在攻击的异常信号类别，卷积神经网络模型安全检测过程如下：

卷积神经网络由输入层、卷积层、输出层等组成，将政务系统独立通信层信号数据样本和数据样本之间的关联规则输入到网络模型的输入层内，该层将所有信号数据映射处理后输入到卷积层，卷积层执行卷积操作得到政务系统独立通信层信号和关联规则的特征，其表达公式如下：

$$\Phi_i = f(Q \times W_i + b_i) \tag{12}$$

上述公式中，Φ_i 表示卷积层第 i 个卷积核输出结果；f 表示激活函数；W_i 、b_i 分别表示第 i 个卷积核权值和偏移向量。

然后将公式(12)结果输入到池化层内，该层对其进行下采样处理，表达公式如下：

$$\Phi'_i = subsanpling(Q) \tag{13}$$

上述公式中，Φ'_i 表示下采样后的输出结果；$subsanpling(\cdot)$ 为池化规则。

然后将公式(13)结果输入到隐含层内，该层利用 ReLU 函数作为激活函数，减少运算量和梯度误差，其表达公式如下：

$$R(x) = \max(0,x) \tag{14}$$

上述公式中，$x = \{X_{new},Q\}$ 表示待激活目标。

将激活后的政务系统独立通信层信号和关联规则特征输入到网络模型的全连接层内，该层将政务系统独立通信层信号和关联规则特征综合到一起，其表达公式如下：

$$F(x) = f(x \times W + b) \tag{15}$$

上述公式中，$F(x)$ 表示全连接层目标函数；W 、b 分别表示全连接层的权值和偏置。

利用 Softmax 层计算政务系统独立通信层信号数据检测时的分类概率，对于信号数据 x，其属于类别 j 的概率输出计算公式如下：

$$H(y^i = j \mid x^i,\theta) = e^{\theta_j^T x^i} \frac{1}{\sum_{i=1}^{k} e^{\theta_j^T x^i}} \tag{16}$$

上述公式中，$H(y^i = j \mid x^i,\theta)$ 表示信号数据 x 属于类别 j 的概率；θ 表示待拟合参数；e 表示正态分布函数。

卷积神经网络输出层依据公式(16)结果，输出政务系统独立通信层信号在其时域内的安全类别和异常攻击类别，实现政务系统独立通信层信号安全检测。

2　实验分析

以某市政务系统作为实验对象，该政务系统主要负责公文管理，向市民发送通知、公告，向内部工作人员发布工作日程，做工作计划总结，以及各个部门办公资源共享等，该政务系统具备 21 个独立通信层，分属 21 个不同职能部门。使用本文模型检测该政务系统独立通信层信息安全，分析本文模型实际应用效果。

2.1　独立通信层信道状态信息采集

以某时间段为时间对象，使用本文模型采集该政务系统某个独立通信层信道状态信息，并以瀑布图的方式呈现出来，采集结果如图 2 所示。

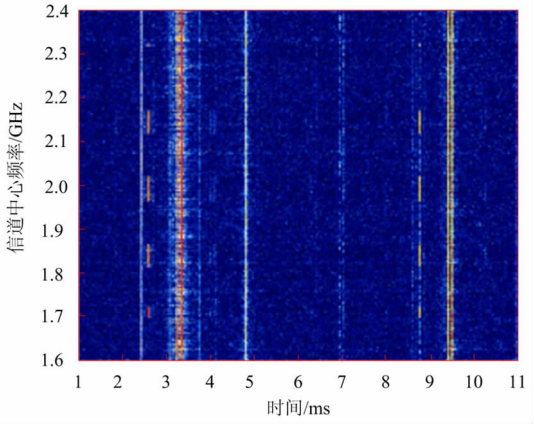

图 2　独立通信层信道状态信息采集测试结果

分析图 2 可知，从政务系统独立通信层信道状态信息瀑布图内可清晰看到竖向中心频率变化线，说明此时该独立通信层信道正在传输信息，被本文模型采集到。该结果说明：本文模型可有效采集政

务系统独立通信信道在通信状态下的信息，为后续检测该独立通信层信道安全打下良好的基础。

2.2 数据预处理检验

以采集到的政务系统独立通信层信号作为实验对象，使用本文模型对其进行归一化和均衡化处理。以数据标准化差距作为衡量本文模型对政务系统独立通信层信号预处理效果衡量指标，测试在政务系统独立通信层信号数量不同情况下，本文模型对其预处理效果，并设置信息预处理标准化差距阈值为 7%。测试结果如图 3 所示。

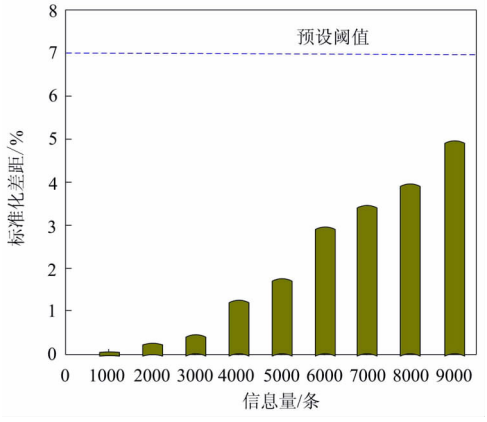

图 3 数据预处理检验结果

分析图 3 可知，当政务系统独立通信信道信息量较少时，对其进行预处理后的标准化差距数值越小，随着信息量不断增加，数据预处理后，其标准化差距数值不断增加，但最大标准化差距数值仅为 5%，低于预设阈值。上述结果说明：本文模型具备较好的政务系统独立通信信道信息预处理能力。

2.3 快速时域关联规则挖掘测试

以 10 个政务系统独立通信层信号数据作为实验的对象，以政务系统独立通信层信号关联规则的置信度和支持度作为衡量指标，测试本文模型挖掘该 10 个政务系统独立通信层信号关联规则能力，测试结果如表 1 所示。

分析表 1 可知，使用本文模型挖掘 10 个政务系统独立通信信道信号之间关联规则时，其关联规则的置信度波动区间为 0.917－0.959，支持度在 0.903－0.931 之间。挖掘到的关联规则置信度和支持度数值均较高，该结果说明：本文模型挖掘政务系统独立通信层信号关联规则较为准确，也从侧面说明本文模型检测政务系统独立通信层信号安全能力较强。

2.4 独立通信信道安全检测验证

验证本文模型检测政务系统独立通信信道安全能力。以该政务系统某个独立通信信道作为实验对象，分别在通信信道通信的第 33 min、42 min、101 min 设置一次蠕虫病毒攻击、SQL 注入攻击、SQL 注入攻击，在第 77 min 设置 2 次 DDoS 攻击，使用本文模型对该信道安全展开检测，检测结果如图 4 所示。

表 1 信号关联规则置信度与支持度数值

独立信道编码	置信度	支持度
1	0.924	0.917
2	0.917	0.903
3	0.933	0.906
4	0.956	0.921
5	0.955	0.926
6	0.927	0.931
7	0.936	0.909
8	0.959	0.918
9	0.925	0.927
10	0.933	0.925

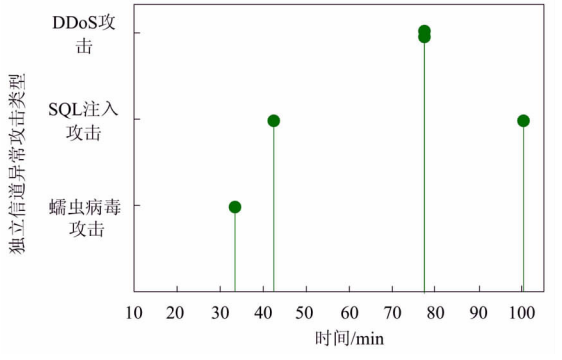

图 4 独立通信信道安全检测验证

分析图 4 可知，本文模型可有效检测该政务系统独立通信信道受到的不同攻击类型，检测结果与实验设置完全吻合，说明其检测精度达到 100%，本文模型具备较为显著的应用效果。

以检测政务系统独立通信信道安全时的错误接受比例（FAR）作为衡量指标，测试本文模型在不同信噪比和信道遭受攻击强度不同时，其检测结果的错误接受比例，结果如图 5 所示。

分析图 5 可知，本文模型在检测政务系统独立通信信道安全时，在信道遭受攻击强度越高的情况下，其检测结果错误接受比例数值越低，而信道信噪比数值越高，在相同攻击强度时的检测结果错误接受比例越大，但最大错误接受比例数值仅为

0.042%左右，数值较小。上述结果说明：本文模型可在信道受攻击强度较小时，有效检测其攻击情况，检测信道安全能力较强。

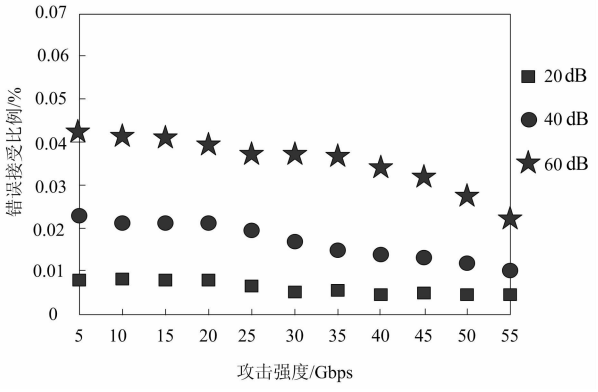

图 5　信道安全检测错误接受比例

3　结　论

提出了基于快速时域关联规则发现算法的政务系统独立通信层信号安全检测模型，并将其应用到某政务系统独立信道安全检测过程中，经过多角度验证，本文模型可有效采集独立信道通信信息，并可较好地对信息进行预处理，同时可检测独立通信信息内存在的异常信息，其检测政务系统独立通信信道安全能力较强。

参考文献

[1]　王永贵，谢南，曲海成. 基于存储改进的分区并行关联规则挖掘算法[J]. 计算机应用研究，2020，37(1)：167－171.

[2]　毛伊敏，邓千虎，陈志刚. 基于信息熵与遗传算法的并行关联规则增量挖掘算法[J]. 通信学报，2021，42(5)：122－136.

[3]　刘美玉，祁建军，刘伟. 三支概念格中的关联规则提取算法[J]. 西安交通大学学报，2021，55(9)：189－196.

[4]　孙江，行鸿彦，吴佳佳. 基于 IA－SVM 模型的混沌小信号检测方法[J]. 探测与控制学报，2020，42(3)：119－125.

[5]　许耀华，尤扬扬，胡梦钰，等. 基于 SAOR 的 Massive MIMO 系统信号检测算法[J]. 数据采集与处理，2020，35(1)：139－146.

[6]　李恒武，高勇，李汉宁，等. 5G 环境下网络独立通信层信号安全检测[J]. 计算机仿真，2022，39(3)：434－438.

[7]　王安义，李立. 基于高阶累积量和 DNN 模型的井下信号识别方法[J]. 工矿自动化，2020，46(2)：82－87.

[8]　李亚利，刘佳. 基于非平稳信号时频分析的 DDoS 攻击检测仿真[J]. 计算机仿真，2021，38(5)：353－356＋370.

[9]　左婷，王法松，张建康，等. 室内可见光通信系统中基于压缩感知的空移键控信号检测方法[J]. 电子学报，2022，50(1)：36－44.

[10]　康颖，赵治华，吴灏，等. 基于 Deep SVDD 的通信信号异常检测方法[J]. 系统工程与电子技术，2022，44(7)：2319－2328.

[11]　许耀华，朱成龙，王翊，等. 基于神经网络的高并行大规模 MIMO 信号检测算法[J]. 系统工程与电子技术，2022，44(12)：3843－3849.

[12]　苏宁远，陈小龙，关键，等. 基于深度学习的海上目标一维序列信号目标检测方法[J]. 信号处理，2020，36(12)：1987－1997.

[13]　张盛魁，姚志成，范志良，等. 基于局部自适应阈值的跳频信号提取和检测[J]. 电光与控制，2020，27(1)：68－72.

[14]　王明月，李方伟，景小荣，等. 大规模 MIMO－TRDMA 系统中的改进 SOR 信号检测算法[J]. 通信学报，2021，42(10)：153－161.

[15]　吴睿，廖聿宸，宗周红，等. 基于 GNSS 信号的随机子空间模态参数识别方法[J]. 东南大学学报(自然科学版)，2020，50(6)：1045－1051.