文章编号:1007-1423(2019)05-0033-06 DOI:10.3969/j.issn.1007-1423.2019.05.007

# 基于R-DFA状态机的工控系统异常流量检测

周宇[1],郑荣锋[1],刘嘉勇[2]

(1.四川大学电子信息学院,成都 610065;2.四川大学网络空间安全学院,成都 610065)

**摘要:**

针对以往工控系统异常流量检测系统无法检测上行信道异常的问题,提出以R-DFA为核心的工控异常流量检测方法,R-DFA是输入参数包含PLC向上位机的上行信道信息的有限自动机机。该方法首先建立工控信道的白名单,然后提取工控的正常流量特征,建立状态转换表,训练出R-DFA模型,又在状态机后添加周期状态序列,完善状态机中状态转化依赖于上一个状态的不足。实验结果表明,该方法的异常检测的准确率较高,也能够有效地检测上行信道流量的异常。

**关键词:**

工控系统;流量特征;有限自动机;上行信道信息;异常流量检测系统

## 0 引言

在工业控制系统ICS发展过程中,采取的是封闭隔离形式,具有固定的业务流程,是自动闭环的处理方式,并采用大量私有协议,但是随着ICS开放性的提升和协议逆向技术的发展,安全的私有协议渐渐变成暴露在网络上极易受到攻击的公有协议。

ICS需要符合其特殊性的入侵检测系统,Goldenberg和Wool分别提出了针对Modbus和S7协议的基于状态机的入侵检测方法[1-2],但只是在HMI到PLC方向的下行信道建立DFA(有限状态自动机),不能检测PLC到HMI方向的数据。Zhang J[3]等人提出了基于工控流量数据周期性的特点进行异常检测,并将请求数据的响应时间也加入参考条件,但并没有检测上行信道的数据。Xu J、Feng D[4]提出了SF-FSM模型(包含响应参数的有限状态机)将下行信道PLC响应HMI的数据作为状态机的参数,但如果通过中间人构造响应数据,则此状态机就会失效。

针对上述的问题,提出了R-DFA模型,R-DFA模型是特殊的有限自动机,其输入参数包含请求数据信息,响应数据信息和响应时间信息三元组。最后为了弥补一般自动机的状态转移只依赖前一个状态的缺点,在R-DFA模型后面添加周期状态序列模型以提高准确率。考虑到S7协议语义公开,便于提取特征,本文实验环境基于S7协议的工控系统,实验结果表明R-DFA模型具有较高的准确率,也能够有效的对上行异常流量进行检测。

## 1 异常流量检测方法

### 1.1 数据预处理

本文将工控系统的一个PLC和一个上位机的通信称为一个信道,R-DFA模型异常流量检测是建立在单一信道中。数据预处理有两个目的,一是获得所有信道信息,建立信道白名单模型,过滤异常的信道,二是提取出单一信道,并从单一信道中提取次信道的工控规则信息数据,为后续训练R-DFA模型。

数据预处理分为二步:

(1)通过三元组(s_port,m_IP,s_IP)分离通信信道。其中s_port为S7协议的端口号,s_IP为PLC的IP,m_IP为上位机的IP,并将正常信道的三元组进行记录,组建会话白名单;

(2)在一个信道会话中提取会话规则,过滤掉对规则无用的包,例如心跳包(PLC定时对HMI发送的工控现场实时的数据,ROSCTR为0x07)等,过滤这些包

根据 S7 PDU 的 Header 中的 ROSCTR 字段来过滤，仅仅保留 ROSCTR 字段为 0x01（JOB packet）和 0x03（ACK packet）的数据包。

### 1.2 数据包特征提取

先对 S7 协议字段和语义进行分析，根据先验知识确定 S7 协议中的关键字段来作为特征，提取出一个能代表这

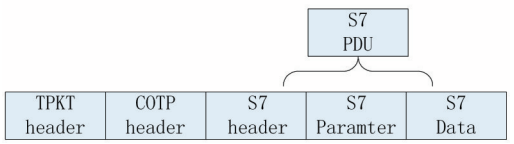


图1 S7协议PDU结构

本文将 S7 协议的数据包特征定义为 S7 PDU 除去 Header 字段包含的 Protol Data Unit Reference 字段的其他所有数据的集合。提取后数据包字段特征进行 md5 产生一个 32 位的数据，本文称为特征指纹，用特征指纹来代替原始的特征数据，这样既能够用特征指纹表现出不同数据包的唯一性，也能够忽略请求数据包和响应数据包的不同所表现出来的特征长度的区别。

### 1.3 R-DFA模型

工业控制系统网络一般具有明显的规律性，可以将工控系统一个信道的工作流程定义为一个有限自动机，R-DFA 和普通的 DFA 一样定义一个五元组（S，$s_0$，∑，δ，F）。

S 是一个有限非空的状态集合，需要用 PLC 的实际状态来定义，第二个参数 $s_0$ 为状态机的初始状态，是 S 的一个元素，所以 S 为：

$$S=\{s_i\},0\leqslant i\leqslant N; \quad (1)$$

∑为输入的信号，是本文状态机的特点，一般的工控系统的状态机的输入信号都是单向的请求（JOB）数据包，这样不能检测出由 PLC 向上位机 HMI 的注入攻击，例如响应注入攻击。∑的元素 $\sum_i$ 是一个三元组为（$P_{req,i}$，$P_{resp,i}$，$\Delta T_i$），因此 S 为：

$$\sum=\{\sum_i\}=\{(P_{req,i},P_{resp,i},\Delta T_i)\},0\leqslant i\leqslant N; \quad (2)$$

$P_{req}$ 是从 JOB（request）数据包中提取的特征指纹，$P_{resp}$ 是从 ACK（response）数据包中提取的特征指纹。ΔT 是 JOB 包和 ACK 包的到达时间差，称为响应时间。使用信道流量上下行的特征作为输入信号，能够建立一个信道上下行的关系，有效的检测出响应注入攻击，响应时间 ΔT 的加入是为了防止攻击者构造响应数据包，从而欺骗上位机 HMI。

δ为状态转移函数，能够通过现在的状态 $s_i$，三维输入参数 $S_i$，转移到下个状态 $s_{i+1}$。F 为状态机的最后一个状态。

定义了状态机的各项参数后，开始建立状态机模型。建立一个二维的状态转换表，第一行为前一个状态，第一列为后一个状态，如果两个状态能够转化则对应表中位置写入输入信号参数，异常检测模型根据状态转换表来确定状态转换是否异常。

例如假设一共有三种状态，建立的状态转换表如表 1 所示。

表 1 状态转换表

| 前一个状态 / 后一个状态 | $s_1$ | $s_2$ | $s_3$ |
|---|---|---|---|
| $s_1$ | —— | —— | （$P_{req,1}$，$P_{resp,1}$，ΔT） |
| $s_2$ | （$P_{req,2}$，$P_{resp,2}$，ΔT） | —— | —— |
| $s_3$ | —— | （$P_{req,3}$，$P_{resp,3}$，ΔT） | —— |

可以看出，$s_1$ 可以通过三维输入信号（$P_{req,2}$，$P_{resp,2}$，ΔT）转换为 $s_2$，且 $s_1$ 只能转换为 $s_2$ 状态，如果 $s_1$ 收到其他输入信号，会触发异常状态转化函数，从而报出异常。$s_1$ 状态转化为稳定的 $s_2$ 状态过程如图 2 所示。

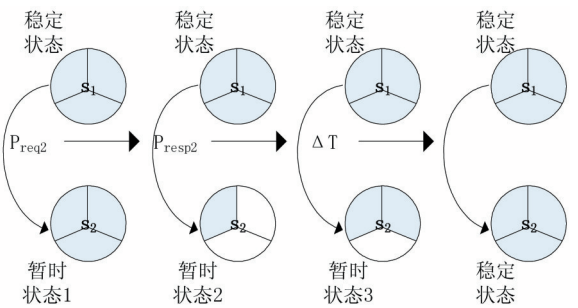


图2 $s_1$ 到 $s_2$ 稳定状态转换过程

异常状态转化函数能够根据不同的错误输入信号触发不同的异常状态，例如 $P_{req}$ 错误则报请求异常，$P_{resp}$ 和 DT 错误，则报响应异常。此状态机模型理论上能够有效检测出以往的工控状态机模型无法检测的响应注入攻击。

### 1.4 周期状态序列模型

状态机模型虽然能够检测出异常攻击，但状态机的状态转换是依赖于上一个状态的，因此状态机模型有一定的局限性，当发生图 3 情况时，状态机模型可能

会出错。

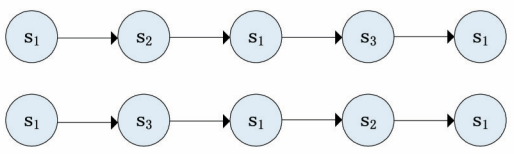


图3 状态机模型无法检测的状态顺序

在图 4 中，$s_2$ 和 $s_3$ 都能转化为 $s_1$ 状态或者从 $s_1$ 转化而来，都保存在了状态转化表中。只使用状态机模型进行异常检测，则上图中错误的顺序也会被状态机认为是正确的，产生漏报。为了解决这种问题，完善异常检测模型，本文又在状态机模型之后添加了周期状态序列模型。

周期状态序列模型由下面步骤建立。

(1)找到单一信道中工控数据流量的最小正周期 n，根据 JOB 数据包的特征指纹顺序建立一个周期内的状态序列模型；

(2)周期状态序列模型会在一开始进行检测时进行计数标记，确保预测的状态和状态机模型将要正确转化的下一个状态一致；

(3)当状态机模型转化为下一个状态时，就会与当前周期状态序列模型所预测的状态进行比对，以确保当前转化状态的正确性。

周期状态序列模型的位于状态机模型后面，当一个周期的状态预测完成后，周期状态序列模型又会从周期初始状态开始预测，循环反复，减低了异常检测系统的负担。

如果只用周期状态序列模型进行异常检测，无法确定工控系统即时的状态，而且少了输入信号量的检测，模型检测不出响应注入等攻击。将状态机模型和周期状态序列模型结合起来，能够避免图 3 的漏报，也能够有效地提高异常检测系统的准确性。

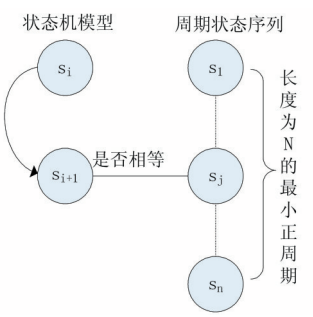


图4 周期状态序列的检测

### 1.5 异常检测系统

以 R-DFA 为核心的异常检测系统由以下步骤建立：

(1)通过正常流量建立会话白名单，提取目标信道的数据包，过滤掉其中的心跳包。

(2)提取目标信道上下行流量的特征，根据目标信道的通信规则建立状态转换表，训练 R-DFA 模型。

(3)根据目标信道通信规则，提取出周期，建立周期序列模型。

(4)将以上的模型按照图 5 顺序组合起来，对实时的流量进行检测，对不正常的行为发出警告。

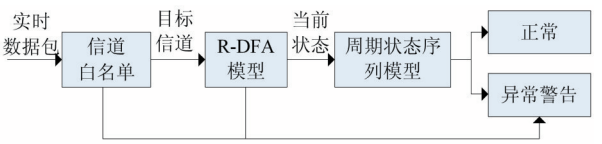


图5 异常流量检测系统

异常警告可以告知检测出的异常行为发生在异常检测系统的哪个阶段，也能将对应的异常的行为记录。这样能够通过异常警告的记录获得流量中异常行为个数，从而验证本文异常检测系统的性能。表 2 为异常警告阶段会记录的异常行为及其阶段。

表 2 异常警告记录的行为和对应阶段

| 异常检测模型的阶段 | 发出的警报 | 具体异常行为 |
|---|---|---|
| 信道白名单 | 未知信道 | 数据包来自一个新的 IP 不在白名单中的连接 |
| R-DFA 阶段 | 响应注入 | 控制PLC对上位机回复错误或者虚假的响应 |
| | 逻辑异常 | 上位机对PLC的请求不符合工业生产流程 |
| 周期状态序列阶段 | 逻辑异常 | 上位机对PLC的请求不符合工业生产流程 |

## 2 实验与结果分析

### 2.1 实验环境和实验数据

为了检测以上方法的可行性，在本地搭建一个小型的工控系统仿真环境进行实验。本文的实验场景如图 5 示的西门子工控实验平台的网络拓扑图。现场设备包含两个 S7-200 和一个 S7-300 的 PLC。S7-300 控制发电机的转速，S7-200 控制蜂鸣器。其中工程师站能够根据设定的流程逻辑编写 PLC 对应的程序。

在控制设备和现场设备之间有换机，能够镜像工控网络中的流量到工控异常检测服务器中，并用抓包

工具捕获 PLC 与 HMI 的实时数据。

实验先通过正常的工控流量数据在服务器中训练出本文提出的异常检测模型，然后将训练完成的异常检测模型监听镜像端口的实时数据，验证异常检测模型的效果。

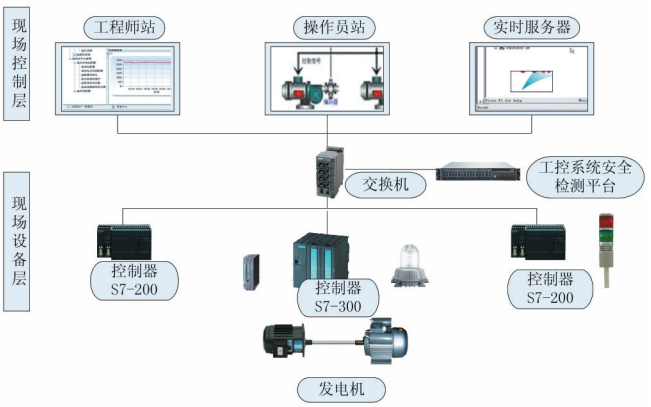


图6 工控网络仿真拓扑图

在本次实验中，选取 S7-300 与上位机的通信信道，此信道能够体现出工控系统的流量数据的特征。

本文实验数据是通过 Python 的 Scapy 库嗅探正常流量和异常的攻击流量，使用正常流量来建立模型，使用恶意的攻击流量验证异常流量检测系统的性能。本文使用以下的攻击方式进行攻击，并捕获异常流量，表 3 为获取实验数据集，数量和实际攻击的单位都是数据包个数。

序列攻击：修改数据包的传送顺序，导致工控逻辑出现异常，从而影响正常的工控系统的运作。

snap7 连接：通过在工控网络中用另外一台设备编写 S7 的程序，利用 PLC 不会对 HMI 设备认证的缺点，控制 PLC 达到攻击的目的。

手动操作：手动的从 HMI 向 PLC 发送一些数据包，使其与正常情况的状态不符合，例如在本实验场景中，HMI 向 PLC 发送的不正常的请求包。

响应构造：通过中间人攻击，构造 PLC 到 HMI 的响应包，让 HMI 误以为 PLC 已经改变状态，达到欺骗 HMI 的目的。

异常响应：直接通过中间人构造异常的响应数据包，从而从上行信道对 HMI 的主机进行攻击。

表 3 实验数据集

| 数据集类型 | 数量 | 实际攻击 |
|---|---|---|
| 正常数据 | 115406 | ---- |
| Snap7 连接 | 16420 | 4050 |
| 序列攻击 | 11815 | 4580 |
| 手动操作 | 12450 | 3260 |
| 响应构造 | 16025 | 3988 |
| 异常响应 | 17439 | 5624 |

## 2.2 实验检测

利用表 3 的正常数据流，建立信道白名单模型，R-DFA 模型和周期序列模型，并将三者根据图 5 串联起来，形成异常检测系统，对表 3 的异常数据流进行检测，本实验使用工具是 Python3。

其中 R-DFA 模型的三元输入参数中的响应时间 DT 需要一个可靠的取值范围，在本文实验环境中，正常的 S7 数据流量的响应时间如图 7 所示。

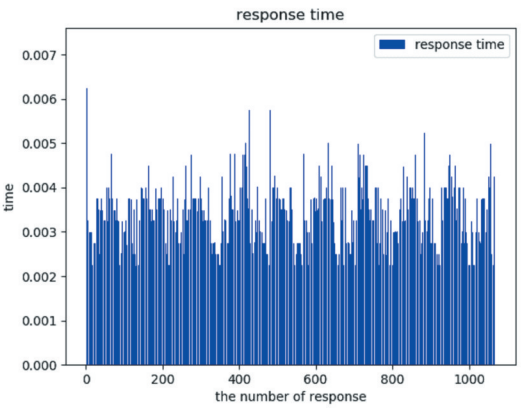


图7 正常流量的响应时间

可以看出在本文的实验环境中工控数据响应时间集中在 0.002s 到 0.005s 之间，但也会有些超过 0.005s，这些响应时间也是正常的，原因可能是网络延迟。

为了规避正常的网络延迟的情况，实验使用核密度估计 ΔT 的概率密度估计，从而定义其取值范围，核密度估计是一种用于估计概率密度函数的非参数方法，正常 n 个样本点 $\Delta T_1, \Delta T_2, \cdots, \Delta T_n$ 为独立同分布的，设其概率密度函数为 f，则其核密度估计为：

$$\hat{f}_h(x) = \frac{1}{n_h} \sum_{i=1}^{n} K\left(\frac{x - x_i}{h}\right), (h > 0) \quad (3)$$

K 为核函数，根据实验，K 选用 Epanechnikov 函数，此核函数的均方误差是最优的。h 为带宽，根据实验得出带宽的最优值为 0.001。实验使用 Python 3 的

scikit-learn 机器学习库对图 6 的正常响应时间数据集进行训练得出 ΔT 的核密度估计，如图 8 所示，选用 ΔT 的范围为(0.0017,0.0095)。

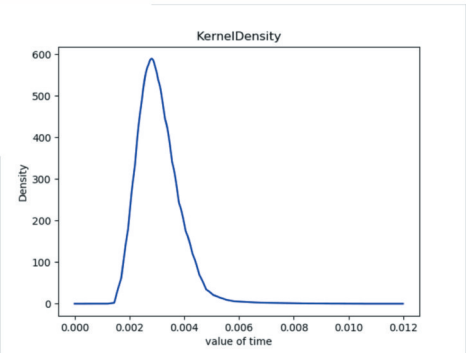


图8 响应时间核密度估计

### 2.3 结果分析

将每个异常数据集的数据包分为两类，正常数据包(normol)和异常数据包(abnormol)，经过实验后得到以下的数据，TP 为真阳性，即 abnormol 被识别为 abnormol；TN 为真阴性，即 normol 被识别为 normol；FP 为假阳性，即 normol 被识别为 abnormal；FN 为假阴性，即 abnormal 被识别为 normal。

本实验采用精确召回率调和平均数(F)、召回率(Rec)、精确率(Pre)来衡量：

$$Pre = \frac{TP}{TP+FP} \times 100\% \quad (4)$$

$$Rec = \frac{TP}{TP+FN} \times 100\% \quad (5)$$

$$F = 2\frac{Pre \times Rec}{Pre + Rec} \times 100\% \quad (6)$$

对异常数据集进行异常检测实验结果如表 4 所示，表 5 还包括此类攻击被检测到的阶段和对应的异常警报。

表 4 异常攻击流量检测结果

| 测试数据集 | 检测阶段 | 异常警报 | TP | TN | FP | FN | Pre | Rec | F |
|---|---|---|---|---|---|---|---|---|---|
| Snap7 连接 | 信道白名单 | 未知信道 | 3969 | 12277 | 93 | 81 | 98.0% | 97.7% | 97.8% |
| 序列攻击 | R-FSM 或 周期状态序列 | 逻辑异常 | 4216 | 6921 | 314 | 364 | 93.1% | 92.0% | 92.5% |
| 手动操作 | R-FSM | 逻辑异常 | 3083 | 8945 | 245 | 177 | 92.6% | 94.6% | 93.6% |
| 响应构造 | R-FSM | 响应注入 | 3768 | 11712 | 325 | 220 | 92.1% | 94.5% | 93.3% |
| 异常响应 | R-FSM | 响应注入 | 5398 | 11663 | 278 | 326 | 95.1% | 94.3% | 94.7% |

根据表 4 的结果，可以看出基于 R-FSM 异常检测系统性能良好，对常见的攻击的异常检测精确率 Pre，召回率 Rec 和精确召回率调和平均数 F 都在 90%以上，也能够检测出 PLC 对上位机方向上行行道的流量异常，也有很高的精确率 Pre，召回率 Rec 和精确召回率调和平均数 F。

## 3 结语

本文在普通的 DFA 模型上添加了 PLC 到 HMI 的数据信息，能够检测出普通工控 DFA 模型无法检测的响应注入的问题，并在 DFA 模型后添加了周期状态序列模型，解决了 DFA 状态转移仅仅依靠前一个状态的不足。在本地基于 S7 协议仿真实验中，异常检测模型运行效果良好，能够准确地识别出工控网络的异常流量。另外此方法也应该能够用在不是 S7 协议的工业控制系统中，这需要后续的研究和确定。

**参考文献：**

[1]Goldenberg N,Wool A. Accurate Modeling of MODBUS/TCP for Intrusion Detection in SCADA Systems[J]. International Journal of Critical Infrastructure Protection,2013,6(2):63-75.

[2]Kleinmann A,Wool A. Accurate Modeling of the Siemens S7 Scada Protocol for Intrusion Detection and Digital Forensics[J]. Journal of Digital Forensics,Security and Law,2014,9(2):4.

[3]Zhang J,Gan S,Liu X,et al. Intrusion Detection in SCADA Systems by Traffic Periodicity and Telemetry Analysis[C]. Computers and Communication (ISCC),2016 IEEE Symposium on. IEEE,2016:318-325.

[4]Xu J,Feng D. Identification of ICS Security Risks toward the Analysis of Packet Interaction Characteristics Using State Sequence Matching Based on SF-FSM[J]. Security and Communication Networks,2017.

[5]Kleinmann A,Wool A. A Statechart-Based Anomaly Detection Model for Multi-Threaded SCADA Systems[C]. International Conference on Critical Information Infrastructures Security. Springer,Cham,2015:132-144.

[6]Maglaras L A,Jiang J. Intrusion Detection in Scada Systems Using Machine Learning Techniques[C]. Science and Information Con-

ference (SAI),2014. IEEE,2014:626-631.
[7]Parvania M,Koutsandria G,Muthukumary V,et al. Hybrid Control Network Intrusion Detection Systems for Automated Power Distribution Systems[C]. Dependable Systems and Networks (DSN),2014 44th Annual IEEE/IFIP International Conference on. IEEE,2014:774-779.
[8]Trifilo A,Burschka S,Biersack E. Traffic to Protocol Reverse Engineering[C]. Computational Intelligence for Security and Defense Applications,2009. CISDA 2009. IEEE Symposium on. IEEE,2009:1-8.
[9]彭勇,向憧,张淼,等. 工业控制系统场景指纹及异常检测[J]. 清华大学学报(自然科学版),2016,56(1):14-21.
[10]赖英旭,刘增辉,蔡晓田,等. 工业控制系统入侵检测研究综述[J]. 通信学报,2017,38(2):143-156.
[11]何钢,周安民. 西门子 SCADA 网络场景指纹自提取及异常检测[J]. 网络安全技术与应用,2017(3):165-167.
[12]程相. 基于信息量的工控网络异常检测技术[J]. 计算机工程与设计,2018.
[13]杨安,孙利民,王小山,等. 工业控制系统入侵检测技术综述[J]. 计算机研究与发展,2016,53(9):2039-2054.
[14]贾涛. 西门子 S7-200 以太网通讯协议研究[J]. 电子技术与软件工程,2014(24):30-32.
[15]彭勇,江常青,谢丰,等. 工业控制系统信息安全研究进展[J]. 清华大学学报:自然科学版,2012,52(10):1396-1408.

**作者简介:**
周宇(1991-),男,四川射洪人,硕士,研究方向为工业控制系统安全
郑荣锋(1990-),男,重庆人,博士,研究方向为工业控制系统安全、网络流量异常检测
刘嘉勇(1962-),男,四川成都人,博士,教授,博士生导师,研究方向为信息安全理论与应用、网络信息处理与信息安全
收稿日期:2018-12-18　　修稿日期:2018-12-27

# Industrial Control System Abnormal Traffic Detection Based on R-DFA State Machine

ZHOU Yu[1], ZHENG Rong-feng[1], LIU Jia-yong[2]

(1. College of Electronics and Information Engineering, Sichuan University, Chengdu 610065;
2. College of Cyberspace Security, Sichuan University, Chengdu 610065)

**Abstract:**
Aiming at the problem that the previous abnormal traffic detection system of the industrial control system could not detect the abnormality of the upstream channel. Proposes an abnormal traffic detection method based on R-DFA, R-DFA is a finite automaton with input parameters containing the upstream channel information of the PLC to the upper computer. This method firstly establishes the whitelist of industrial control channel, then extracts the normal flow characteristics of industrial control, establishes the state transition table, trains the R-DFA model. To improve the state transition in the state machine depends on the deficiency of the previous state, adds periodic state sequence after the state machine adds periodic state sequence after the state machine. The experimental results show that the accuracy of the anomaly detection of this method is high, and it can also effectively detect the abnormality of the upstream channel traffic.
**Keywords:**
Industrial Control System; Flow Characteristics; Finite Automaton; Uplink Channel Information; Abnormal Traffic Detection System