文章编号:1671-4598(2024)08-0014-06 DOI:10.16526/j.cnki.11-4762/tp.2024.08.003 中图分类号:TP393 文献标识码:A

基于双向 AC 算法的列车通信网络异常入侵检测系统设计

贾寒霜[1]，张 卡[2]，杨碎明[1]
(1. 西安交通工程学院 土木与铁道工程学院，西安 710300；
2. 中国化学工程第十四建设有限公司，南京 210044)

摘要：列车通信网络异常流量的类型和形式多样化，特征提取难度较大，异常入侵检测效果较差，为此，设计基于双向 AC 算法的列车通信网络异常入侵检测系统；采集层利用网络数据采集器，在列车通信网络内，采集列车通信网络信息；存储层以分布式存储、列式存储与结构化存储方式，存储采集的信息；分析层利用协议解析模块，解析信息，得到符合规范的信息；其中，深度包过滤模块利用白名单技术深度包过滤符合规范的信息，提取关键信息；入侵特征模式提取模块能够在关键信息内提取异常入侵特征模式；特征模式匹配模块利用双向 AC 算法，自动匹配提取的特征模式与入侵特征模式库内的特征模式；入侵响应模块通过分析自动匹配结果，完成列车通信网络异常入侵检测；可视化层以可视化的报表形式，呈现异常入侵检测结果；实验结果表明，该系统可有效采集列车通信网络信息，完成异常入侵特征模式提取，该系统可快速自动匹配异常入侵特征模式，异常入侵检测精度较高。

关键词：双向 AC 算法；列车通信网络；异常入侵；检测系统；采集器；协议解析

Design of Abnormal Intrusion Detection System for Train Communication Network Based on Bidirectional AC Algorithm

JIA Hanshuang[1], ZHANG Ka[2], YANG Suiming[1]
(1. School of Civil and Railway Engineering, Xi'an Traffic Engineering Institute, Xi'an 710300, China;
2. China National Chemical Engineering No. 14 Construction Co., Ltd., Nanjing 210044, China)

Abstract: There are the characteristics of diverse types and forms of abnormal traffic, difficult feature extraction, and poor effectiveness of abnormal intrusion detection in train communication networks. Therefore, a train communication network abnormal intrusion detection system based on bidirectional AC algorithm is designed. The collection layer utilizes a network data collector to collect train communication network information within the train communication network; The storage layer stores the collected information through the distributed storage, columnar storage, and structured storage methods; The analysis layer utilizes a protocol parsing module to parse the information and obtain the information that meets the specifications. Among them, the deep packet filtering module applies a whitelist technology to filter the compliant information and extract the key information; The intrusion feature pattern extraction module can extract abnormal intrusion feature patterns from the key information; The feature pattern matching module utilizes the bidirectional AC algorithm to automatically match the extracted feature patterns with the feature patterns in the intrusion feature pattern library; The intrusion response module completes abnormal intrusion detection in the train communication network by analyzing the automatic matching results. The visualization layer presents anomaly intrusion detection results in the form of visual reports. Experimental results show that the system can effectively collect train communication network information and extract abnormal intrusion feature patterns. The system can quickly and automatically match abnormal intrusion feature patterns, with a high accuracy of abnormal intrusion detection.

Keywords: bidirectional AC algorithm; train communication network; abnormal intrusion; detection system; collector; protocol parsing

0 引言

列车通信网络是指用于列车内部和列车与地面之间通信的一系列网络设备和通信协议。随着信息技术的不断发展，列车通信网络已经成为现代铁路运输中不可或缺的一部分。列车通信网络主要包括列车内部通信网络和列车与地面通信网络两个部分。列车内部通信网络主要用于列车内各个部件之间的通信，如列车控制系统、乘客信息显示系统、安全监控系统等。列车与地面通信网络主要用于列

收稿日期:2023-07-14； **修回日期**:2023-08-21。
基金项目:西安交通工程学院 2023 年度中青年基金项目(2023KY-43)。
作者简介:贾寒霜(1988-),女,大学本科,讲师。
杨碎明(1971-),男,硕士,副教授。
引用格式:贾寒霜,张 卡,杨碎明.基于双向 AC 算法的列车通信网络异常入侵检测系统设计[J].计算机测量与控制,2024,32(8):14-19.

车与地面之间的通信，如列车位置和速度信息传输、列车调度和监控等[1-3]。列车通信网络主要是基于闭环系统，具有相对封闭的架构，因此网络入侵的风险相对较低。然而，随着列车通信网络与外界的连接性增强，例如与其他铁路系统、互联网和无线网络的连接，它也面临着各种安全威胁，如未经授权的入侵、恶意软件攻击等。网络攻击者有机会利用这些连接进行恶意入侵，从而对列车运行和乘客安全造成严重安全威胁。这些安全威胁可能会导致列车通信网络中的数据泄露、通信中断，甚至列车系统故障，严重影响铁路运输的安全性、可靠性和稳定性[4]。为了保护列车通信网络的安全，需要设计一种高效、准确、实时的异常入侵检测系统。

何发镁等人[5]提出了基于特征分组聚类的异常入侵检测系统，通过 K-means 算法，降维处理网络连接数据，提取网络流量特征，在决策树算法内输入提取的网络流量特征，完成网络异常入侵检测，该系统可有效检测网络异常入侵情况。于怡然等人[6]提出了基于 Wi-Fi 信道状态信息的免训练入侵检测系统，通过 WiFi 设备捕捉通信网络信息，通过多重信号分类算法，提取并分解网络信息特征，完成网络异常入侵检测。该系统网络异常入侵检测的平均假阳性为 1.07%，平均假阴性为 1.87%。但这两个系统均易受通信网络信息模式串长度与文本特征影响，影响抗攻击效果，在处理海量网络数据包时，异常入侵检测速度较慢。

双向 AC 算法具备较优的抗攻击性能，且不受模式串长度与文本特征影响，同时异常入侵检测效率较快[7-8]。为此，设计基于双向 AC 算法的列车通信网络异常入侵检测系统，以确保列车安全运行。通过网络数据采集器，实时采集列车通信网络信息，可以获得准确且丰富的数据源。由于列车通信网络的复杂性和实时性要求，采集层的网络数据采集器为后续的分析提供了高质量的数据基础。采用分布式存储、列式存储与结构化存储方式，将采集到的信息进行存储。这样的多元化存储方式既能够满足海量数据的高效存储需求，又能保证数据的完整性和易于访问性。设计入侵特征模式提取模块，在关键信息内提取异常入侵特征模式。该模块利用算法和模式识别技术，可以自动提取出与入侵相关的特征模式，从而实现对异常入侵行为的快速检测。通过入侵响应模块对自动匹配结果进行分析，可以实现对列车通信网络异常入侵的检测。该模块结合了前面各层的数据和处理结果，能够快速准确地判断是否存在入侵，并及时采取相应的响应措施。通过可视化层以报表形式展示异常入侵检测结果，用户可以清晰直观地了解检测到的入侵事件和相关信息。这种可视化呈现方式提高了数据分析和决策的效率，使用户对列车通信网络安全状况有更直观的认识。通过以上描述的采集层、存储层、入侵特征模式提取模块、特征模式匹配模块、入侵响应模块和可视化层，该系统实现了列车通信网络异常入侵检测。

1　列车通信网络异常入侵检测系统设计

列车运行过程中，会产生海量网络数据包，双向 AC 算法具备高效处理海量网络数据包的功能，为此，设计基于双向 AC 算法的列车通信网络异常入侵检测系统，该系统的整体结构如图 1 所示。

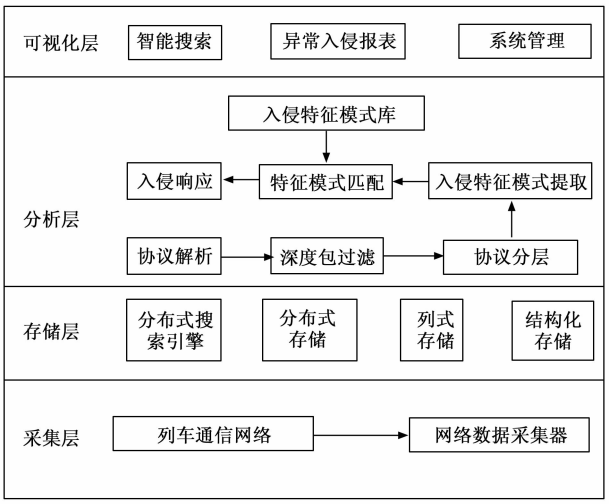


图 1　列车通信网络异常入侵检测系统整体结构

采集层属于列车通信网络异常入侵检测系统的基础层，负责为上层应用提供数据支持。利用网络数据采集器提取列车通信网络相关信息[9]。

存储层以分布式存储、列式存储与结构化存储的 3 种方式，存储网络层传输的列车通信网络信息，并利用分布式搜索引擎，任意调取各个数据库内存储的列车网络信息。

分析层调取存储层内存储的列车通信网络信息后，利用协议解析模块，解析列车通信网络信息，得到符合通信协议规范的列车通信网络信息[10-12]；深度包过滤模块利用白名单技术对符合通信协议规范的通信网络信息，进行深度包过滤，提取关键通信网络信息；协议分层模块负责分类处理关键网络信息；入侵特征模式提取模块，利用主成分分析法，在分类后的关键网络信息内，提取列车通信网络异常入侵特征模式；特征模式匹配模块，利用双向 AC 算法，对提取的异常入侵特征模式与入侵特征模式库内的特征模式进行自动匹配，并传输匹配结果至入侵响应模块；入侵响应模块通过分析匹配结果，完成列车通信网络异常入侵检测，当提取的异常入侵特征模式与入侵特征模式库内的特征模式匹配，则输出对应的异常入侵检测结果；反之，列车通信网络无异常入侵情况。

可视化层负责以可视化的报表形式，呈现异常入侵检测结果，并为用户提供智能搜索功能与系统管理功能。

1.1　列车通信网络数据采集器

采集层利用网络数据采集器，在列车通信网络内，采集列车通信网络相关信息，网络数据采集器的结构如图 2 所示。

网络数据采集器的核心是基于现场可编程门阵列（FPGA）技术。它具有高度灵活性和可定制性，能够与列车通信网络的随机端口进行连接，实现对网络数据的 100%采集与转发，从而极大地提升了列车通信网络信息采集的效果。

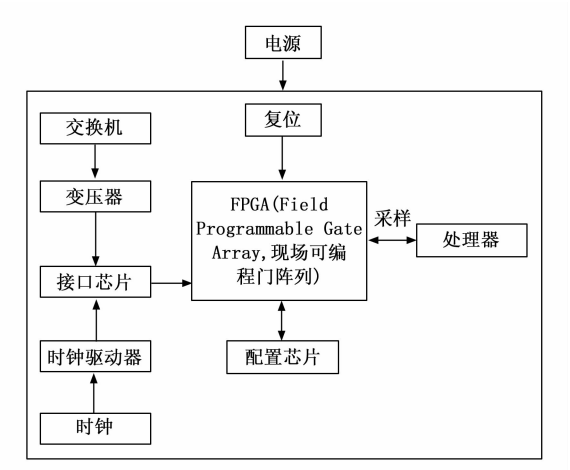


图 2 网络数据采集器结构图

通过将 FPGA 技术应用于网络数据采集器，可以充分发挥其优异的并行处理能力和快速数据传输能力。FPGA 具备可编程的硬件逻辑单元，可以根据特定需求和协议要求，灵活定制和优化采集器的功能和性能。它能够高速采集列车通信网络的数据，并通过专门设计的输入/输出接口与网络设备进行快速数据交换。网络数据采集器的连接性能优势使得它能够可靠地连接到列车通信网络的随机端口，无论是在高负载、高速率的数据传输还是复杂网络拓扑结构下，都能保证稳定的连接和数据传输。这种连接能力确保了对列车通信网络中所有节点的信息进行全面采集，从而提供了更完整和准确的数据基础。使用基于 FPGA 的网络数据采集器，可以实现对列车通信网络内各个子系统和设备的实时监控和数据采集。它能够捕捉和提取网络数据的关键信息，为进一步分析和处理提供有价值的数据资源。同时，FPGA 技术的高度可编程性还能够满足未来对采集器功能的扩展需求，以适应不断演变的列车通信网络环境和技术要求。

网络数据采集器内 FPGA 的结构如图 3 所示。

MAC 控制管理单元包含数据接口、MAC 与 Physical 间的管理接口，数量各一个。该单元负责发送与接收列车通信网络信息，且两个通道间彼此无影响[13]。数据接口通过时钟信号与数据信号组建而成，用于监视、控制 MAC 与 Physical 间的管理接口。

PCI 接口控制单元负责为后端提供读写控制信号，该信号用于翻译用户读写时序，实现读写控制 FPGA 的内部资源，加快列车通信网络信息采集速度。

完整性检查模块包含完整性检查表和标志位寄存器，能够提升列车通信网络信息采集的完整性。通过完整性检查表，可以验证采集到的信息帧的完整性，检测是否出现了数据错误或损坏。而标志位寄存器用于存储第一次采集的列车通信网络信息帧，以提供对后续数据采集的参考[14]。

余度管理单元负责轮询调度接收 MAC 接口的状态，按照" 有效性原则"，剔除多余的列车通信网络信息帧[15]，以加快信息采集速度。通过判断接收到的信息帧是否满足有

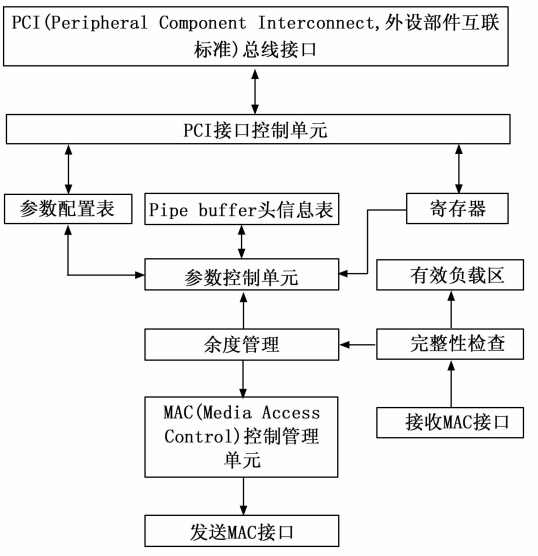


图 3 FPGA 的结构图

效性要求，可以及时过滤掉不符合要求的信息帧，确保只采集到真正需要的数据。

参数控制单元具备列车通信网络信息帧过滤和参数选择的功能。通过配置端口号来过滤采集的信息帧，只有满足特定端口号条件的信息帧才会被采集。同时，在经过过滤后的信息帧中，根据选择参数配置信息，选择指定的列车通信网络信息进行采集。

综上所述，MAC 控制管理单元、PCI 接口控制单元、完整性检查模块、余度管理单元和参数控制单元等模块，共同构成了一个功能完备且高效的列车通信网络信息采集系统。这些模块的功能设计和协同工作，能够提升列车通信网络信息采集的质量和速度，以满足实时监测和分析的需求。

1.2 列车通信网络信息的协议解析流程

分析层利用协议解析模块，对存储层内存储的列车通信网络信息进行协议解析，得到符合通信协议规范的网络信息，协议解析流程如图 4 所示。

列车通信网络信息的协议解析流程为：

按照列车通信网络的 IP 协议规范，检查前 6 位版本号，若版本号是 6，那么代表该列车通信网络信息的 IP 协议符合 IPv6 标准，随后检查列车通信网络信息的协议标识，若标识是 6，那么列车通信网络使用的信息传输协议是 TCP 协议，按照 TCP 协议规范，读取列车通信网络信息的目的端口号，若目的端口号为 20450，那么传输的列车通信网络信息属于 TRDP-MD 报文（MD 代表列车通信网络故障与诊断信息），按照 TRDP-MD 报文规范，直接调取用户信息部分。若目的端口号不是 20450，则对比分析解析的字段信息和期望字段信息，分析解析的字段信息是否符合通信协议规范。若符合规范，那么认定该列车通信网络信息为合法的，反之，认定该列车通信网络信息为非法的，剔除该信息。

若列车通信网络信息的协议标识不是 6，则按照 UDP 协议规范，读取列车通信网络信息的目的端口号，若目的端口号为 20446，那么传输对列车通信网络信息属于 TDRP-

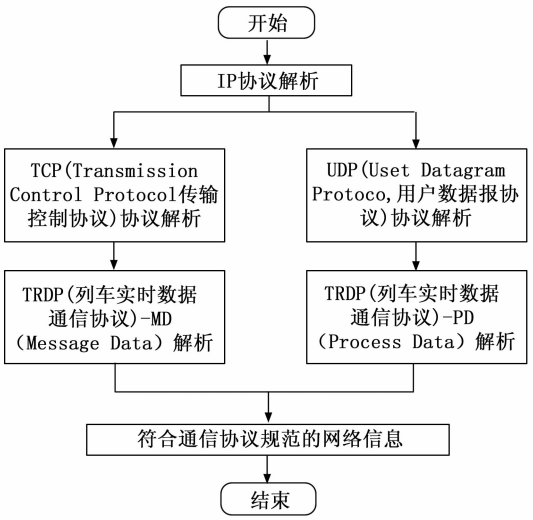


图 4　列车通信网络信息的协议解析流程

PD 报文（PD 代表列车通信网络的列车控制信息），按照 TRDP-MD 报文规范，直接调取用户信息部分。

通过上述流程了解列车通信网络各层协议的类型与包头位置，按照相应的协议规范，高效解析获取列车通信网络信息内的各字段。继续分析下一个列车通信网络信息，以全部网络信息完成分析为止，得到符合通信协议规范的列车通信网络信息。

1.3　关键列车通信网络信息提取

分析层中的深度包过滤模块利用基于白名单技术的方法，对符合通信协议规范的列车通信网络信息进行关键信息提取，从而加快后续网络异常入侵检测的效率。通过采用白名单技术，深度包过滤模块可以事先定义一个合法通信规范的白名单列表，其中包含了正常的、符合规范的列车通信网络信息。当采集到网络数据的时候，深度包过滤模块会将这些数据与白名单列表进行比对。如果网络数据与白名单列表中的通信规范完全匹配，即符合通信协议规范，深度包过滤模块将判断该网络数据为合法的列车通信网络信息，然后进行关键信息提取。白名单技术能够在网络数据流入分析层之前，快速准确地识别出符合通信协议规范的信息，避免了对无关的或冗余的数据进行后续处理和分析。以此大幅提高网络异常入侵检测的效率，减少不必要的计算和存储开销。

设置白名单规则，Action 代表与后续随机一个规则匹配成功后执行的动作，Action 的规则为［Action：Pass］，Pass 代表允许通过；MAC 代表源目的 MAC 地址，MAC 的规则为［MAC：MAC_{start} ＞ MAC_{end}］其中，代表 MAC_{start}、MAC_{end}源、目的 MAC 地址列表。IP 地址的规则为［IP：IP_{start}＞IP_{end}］，IP_{start}、IP_{end}是源、目的 IP 地址列表；端口号 P 的规则为［P：P_{start}＞P_{end}］，其中，源、目的端口号列表是 P_{start}、P_{end}；通信模式 M 的规则为 M 列表；通信端口 C 规则为 C 列表；应答端口 R 规则为 R 列表；应答地址 A 规则为 A 列表。在此基础上，设置警报规则，负责对疑似非法操作展开报警，提升关键列车通信网络信息提取的安全性。设置拦截规则，令对列车通信网络信息发出警报为 Alert；如果 Pass 与 Alert 均未匹配成功，那么拦截该信息，拦截规则为［Action：Deny］；［IP：IP_{start}＞IP_{end}］；［P：P_{start}＞P_{end}］；［M：any］；［C：any］；［R：any］；［A：any］；其中，拦截信息是 Deny。

通过上述规则便可完成关键列车通信网络信息提取。综上所述，通过在分析层中引入深度包过滤模块，利用白名单技术进行关键信息提取，可以有效加快后续网络异常入侵检测的效率。

1.4　基于双向 AC 算法的异常入侵特征模式自动匹配

双向 AC 算法是一种高效的字符串匹配算法，它结合了正向 AC 自动机和反向 AC 自动机的优点。该算法可以快速地在一个文本串中搜索多个模式串，并且在时间复杂度上具有线性级别的优势。算法的基本思想是：构建两个 AC 自动机，一个用于正向匹配，另一个用于反向匹配。对于每个文本串，分别在这两个自动机中进行匹配，并记录匹配到的状态。如果在两个自动机中都匹配到了某个状态，则表示该文本串中存在相应的模式串。双向 AC 可以同时处理正向和反向的匹配，从而提高了匹配的准确性和效率。

分析层中特征模式匹配模块，利用双向 AC 算法，对提取的列车通信网络异常入侵特征模式，与异常入侵特征模式库内的特征模式进行自动匹配，并将自动匹配结果传输至入侵响应模块内，完成列车通信网络异常入侵检测。

令异常入侵特征模式库为 Q，对 Q 展开预处理，得到两个有限状态自动机 S_1、S_2，分别是正向自动机与反向自动机。利用 S_1 与 S_2 各扫描一次提取的列车通信网络异常入侵特征模式串 B，以 B 的中心为起点，分别向左与向右扫描。

S_1 的构造过程为：从左到右扫描 Q，建立模式树 $\hat{Q}_1$。将 $\hat{Q}_1$ 的每个节点当作状态，以根节点为最初状态 $q_0 \in Q$，模式节点标签为最终状态 $F \in Q$，同时在 $\hat{Q}_1$ 内引入转向与失效函数 φ、f。扩展 $\hat{Q}_1$ 获取一个有限自动机，得到 S_1 的表达式如下：

$$S_1 = (\hat{Q}_1, B, \varphi, f, q_0, F) \tag{1}$$

S_2 的构造步骤与 S_1 是反向的，过程如下：

从右到左扫描 Q，建立模式树 $\hat{Q}_2$。将 $\hat{Q}_2$ 的每个节点当作状态，以根节点为最初状态 $q_0 \in Q$，模式节点标签为最终状态 $F \in Q$，同时在 $\hat{Q}_2$ 内引入转向与失效函数 φ、f。扩展 $\hat{Q}_2$ 获取一个有限自动机，得到 S_2 的表达式如下：

$$S_2 = (\hat{Q}_2, B, \varphi, f, q_0, F) \tag{2}$$

利用 S_1 与 S_2 自动匹配 Q 与 B 时，先以 B 的中心为起点，以最长异常入侵特征模式串为匹配时的反复区域，确定 S_1 与 S_2 的自动匹配起点；再利用 S_1 与 S_2 进行自动匹配；最后，得到列车通信网络异常入侵特征模式自动匹配结果。

2　实验分析

为验证所提基于双向 AC 算法的列车通信网络异常入侵检测系统的有效性，以某列车通信网络为实验对象，该列车通信网络的结构如图 5 所示。

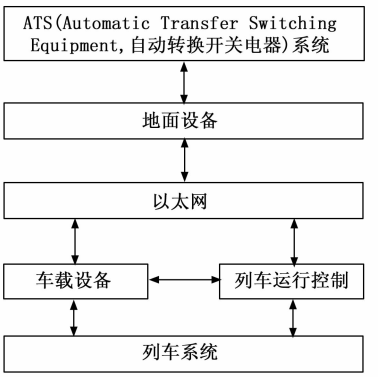


图 5 列车通信网络结构图

实验环境设置如下：

1）Matlab 仿真软件：使用 Matlab 仿真软件模拟真实的列车通信网络环境，生成各种类型的通信数据包。

2）网络数据采集器：使用以太网、WiFi、RS485 网络数据采集器作为实验中的数据采集设备，用于连接到目标设备或网络中进行数据采集，实现对列车通信网络信息的采集和转发。

3）存储设备：采用分布式存储、列式存储和结构化存储方式组成存储层，用于存储采集到的列车通信网络信息。

4）入侵特征模式库：建立一个包含预定义入侵特征模式的数据库，用于与采集的关键信息进行特征模式匹配。

实验参数设置如下：

1）仿真软件：设置仿真软件产生的通信数据包类型为数据传输包、命令包、状态包、数据包的发送频率设置为 20 个/s、存储格式为数据库格式。

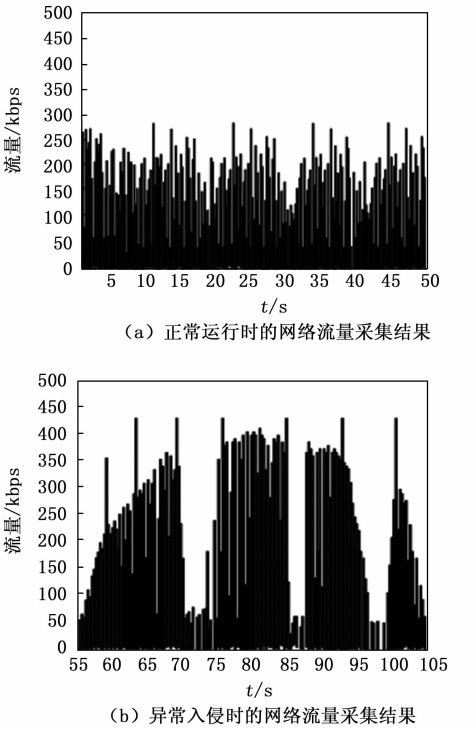
2）数据采集器参数：配置网络数据采集器的工作模式、采集速率、连接端口等参数，确保其能够准确地采集列车通信网络信息。

工作模式包括主动采集和被动采集。主动采集模式下，网络数据采集器定期主动发起请求并接收数据；被动采集模式下，采集器处于监听状态，等待被采集设备主动发送数据；采集速率 1 000 个/s；以太网端口规格为 1 000 Mbps。

在该列车通信网络运行至 55 s 时，注入 DoS 攻击，攻击持续时间为 50 s。利用所提系统采集该列车通信网络在正常运行时与异常入侵时网络信息，以网络流量信息为例，采集结果如图 6 所示。

根据图 6（a）可知，在列车通信网络运行至 50 s 时，该列车通信网络流量整体波动幅度较小，最高网络流量在 290 kpbs 左右；根据图 6（b）可知，在列车通信网络运行至 55 s 时，该列车通信网络流量出现大幅度波动情况，说明此时列车通信网络存在异常情况。实验证明：对于正常情况与异常情况，所提系统均可有效实现列车通信网络信息采集。

利用所提系统提取列车通信网络异常入侵特征模式，所提系统提取的异常入侵特征模式如表 1 所示，当累积贡献率达到 98%时，对应主成分前的全部主成分便可代表全部入侵



（a）正常运行时的网络流量采集结果

（b）异常入侵时的网络流量采集结果

图 6 正常与异常入侵时的网络流量采集结果

特征模式，其余主成分便可剔除，且不会缺失较多信息。

表 1 列车通信网络异常入侵特征模式提取结果

编号	特征模式名称	描述	累积贡献率/%
1	back	网络漏洞	15.8
2	phf	脚本远程执行任意命令漏洞	21.8
3	perl	脚本执行拒绝漏洞	32.9
4	xlock	参数格式化字符串漏洞	40.8
5	pod	黑客攻击	51.5
6	spy	雷达模拟攻击	66.7
7	land	局域网拒绝服务攻击	76.1
8	rootkit	恶意软件攻击	84.3
9	DoS	拒绝服务攻击	90.7
10	Loadmo	安全服务器出错	98.7
11	TCP sessJOn hijacking	TCP 会话劫持	100
12	DDOS	分布式拒绝服务攻击	100
13	SQL Injection	SQL 注入攻击	100
14	Cross Site Script	跨站脚本攻击	100
15	WannaRen	勒索病毒攻击	100

根据表 1 可知，所提系统可有效提取列车通信网络异常入侵特征模式，编号为 10 的特征模式累积贡献率为 98.7%，超过了 98%，即选择前 10 个主成分为列车通信网络异常入侵特征模式。实验证明：所提系统可有效将 15 维特征模式，降低至 10 维特征模式，降维可以减少冗余的特征，从而降低模型的复杂度，避免过拟合问题，提高模型的泛化能力，提高了数据处理效率。降维后的特征集合更容易理解和解释，便于找出与入侵相关性更高的特征和模

式，实现入侵特征模式提取。

在该列车通信网络信息内，随机选择 12 个信息样本，其中异常入侵样本数量为 6 个，正常样本数量为 6 个，利用所提系统对 12 个信息样本进行异常入侵检测，检测结果如图 7 所示。

	编号	内容名称	内容描述	入侵检测结果
□	1	etbTopoCnt	列车静态拓扑序列	正常样本
□	2	back	网络漏洞	入侵样本
□	3	ReplyStatus	响应状态	正常样本
□	4	perl	脚本执行拒绝漏洞	入侵样本
□	5	opTrnTopoCnt	列车运行拓扑序列	正常样本
□	6	Trans_protocol	传输协议	正常样本
□	7	xlock	参数格式化字符串漏洞	入侵样本
□	8	pod	黑客攻击	入侵样本
□	9	Destination_IP	目的IP地址	正常样本
□	10	loadmo	安防服务器出错	入侵样本
□	11	ChannelId	信道标识	正常样本
□	12	rootkit	恶意软件攻击	入侵样本

图 7　列车通信网络异常入侵检测结果

根据图 7 可知，所提系统可有效检测列车通信网络异常入侵情况，由检测结果可知，编号为 1、3、5、6、9、11 的样本为正常样本，其余样本为入侵样本，正常样本与入侵样本数量各 6 个，与实际情况相符。实验证明所提系统具备较高的异常入侵检测精度。所设计特征模式匹配模块采用双向 AC 算法，能够智能匹配提取的特征模式与入侵特征模式库内的特征模式，可以有效提高匹配的准确性和效率，从而更好地判断是否存在入侵行为。

利用所提系统对提取的异常入侵特征模式进行自动匹配，分析所提系统在不同规则数时，异常入侵特征模式的匹配效率，分析结果如图 8 所示，匹配效率阈值为 80 s。

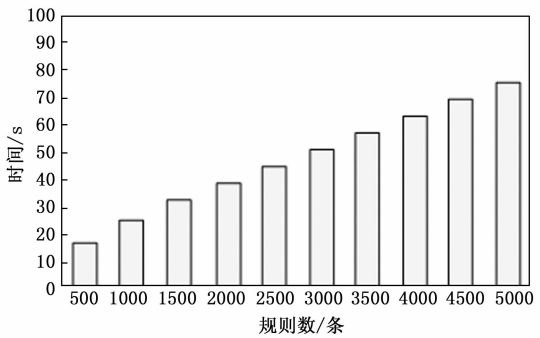


图 8　异常入侵特征模式的匹配效率分析结果

由图 8 可知，随着规则数的增长，所提系统自动匹配异常入侵特征模式的时间随之提升，最长自动匹配时间在 75 s 左右，并未超过设置阈值，说明所提系统自动匹配异常入侵特征模式的时间较短。实验证明所提系统可快速自动匹配异常入侵特征模式。该系统通过利用白名单技术的深度包过滤模块，可以筛选出符合规范的信息，提取关键信息。相比传统的包过滤方法，该模块能够更加准确和高效地提取出需要的信息，避免了冗余和无用的数据，能够有效提升异常入侵特征模式的匹配效率。

3　结束语

列车通信网络虽然具备成本低与效率高等优势，但却会降低列车内部通信的安全性。为此，设计基于双向 AC 算法的列车通信网络异常入侵检测系统，通过使用双向 AC 算法，系统可以实时检测和识别列车通信网络中的异常行为和入侵尝试，及时发出警报并采取相应的安全防护措施。针对列车通信网络中存在的多样化攻击形式和入侵手段，使用强大的可扩展双向 AC 算法来建立高效的检测模型。使得系统能够快速地匹配和识别包括已知和未知的恶意行为。实验结果表明，所设计系统能够提升异常入侵检测精度，避免列车通信网络受异常入侵影响，导致列车无法正常运行，为确保列车安全运行提供保障。

参考文献：

[1] 李　伟，陈　则，秦元庆，等. 一种基于移动目标防御的列车通信网络闭环动态安全防护方法 [J]. 小型微型计算机系统，2022，43 (11)：2394－2398.

[2] 谢雨飞，田启川. 基于隐马尔可夫模型的 CTCS 无线通信系统入侵检测分析 [J]. 铁道学报，2021，43 (8)：73－80.

[3] 王俊彦，衣　然，张　斌，等. 新型入侵检测技术在城市轨道交通信号系统中的应用研究 [J]. 城市轨道交通研究，2022，25 (7)：43－46.

[4] 班玉友，贺德强，陈彦君，等. 基于旗鱼优化器的列车通信网络拓扑优化研究 [J]. 铁道科学与工程学报，2021，18 (12)：3146－3154.

[5] 何发镁，马慧珍，王旭仁，等. 基于特征分组聚类的异常入侵检测系统研究 [J]. 计算机工程，2020，46 (4)：123－128.

[6] 于怡然，常　俊，吴柳繁，等. 基于 Wi-Fi 信道状态信息的免训练入侵检测系统 [J]. 微电子学与计算机，2020，37 (5)：18－22.

[7] 姜海洋，李雪菲，杨　晔. 基于距离比较的 AC 自动机并行匹配算法 [J]. 电子与信息学报，2022，44 (2)：581－590.

[8] 熊仁都，杨嘉佳，朱广宇，等. PARA-AC：一种基于 AC 自动机的高性能匹配算法 [J]. 电子技术应用，2020，46 (11)：87－90.

[9] 王振东，刘尧迪，杨书新，等. 基于天牛群优化与改进正则化极限学习机的网络入侵检测 [J]. 自动化学报，2022，48 (12)：3024－3041.

[10] 夏景明，丁春健，谈　玲. 基于灰狼算法的深度信念网络入侵检测方法 [J]. 计算机工程与设计，2020，41 (6)：1534－1539.

[11] 刘　洋. 基于改进白名单过滤的跨网入侵检测仿真 [J]. 计算机仿真，2020，37 (1)：385－389.

[12] 杨彦荣，宋荣杰，周兆永. 基于 GAN-PSO-ELM 的网络入侵检测方法 [J]. 计算机工程与应用，2020，56 (12)：66－72.

[13] 尹晟霖，张兴兰，左利宇. 双重路由深层胶囊网络的入侵检测系统 [J]. 计算机研究与发展，2022，59 (2)：418－429.

[14] 马　琳，王云霄，赵丽娜，等. 基于多模型判别的网络入侵检测系统 [J]. 计算机科学，2021，48 (s2)：592－596.

[15] 王　璐，文武松. 基于人工智能的分布式入侵检测研究 [J]. 计算机科学，2022，49 (10)：353－357.