文章编号:1671-4598(2024)08-0034-06 DOI:10.16526/j.cnki.11-4762/tp.2024.08.006 中图分类号:TP393 文献标识码:A

云网融合中分布式网络入侵路径跟踪检测方法

杨 波,蒋金陵,徐胜超,王宏杰,毛明扬,蒋大锐
(广州华商学院 人工智能学院,广州 511300)

摘要:随着云计算和网络虚拟化的快速发展,云网融合环境下的分布式网络较普通网络更加复杂和庞大,导致网络入侵路径跟踪的查全率难以得到保障,为此提出云网融合环境下分布式网络入侵路径跟踪检测方法;结合云网融合环境下分布式网络的特性,构建了分布式网络模型,将网络数据流信息转化为统一的格式后,考虑到干扰因素对于网络数据流信息带来的影响,对处理后的信息进行滤波处理,利用网络数据流信息计算云网融合环境下分布式网络的入侵信息特征因子,利用入侵信息特征因子实现对入侵路径的跟踪检测;在测试结果中,网络入侵路径跟踪检测准确性可达99.9%,F_1值始终大于0.85,明显优于对照组,具有较高的查全性能。

关键词:网络入侵路径;云网融合;分布式网络模型;数据流信息;特征因子

Network Intrusion Path Tracking and Detection Method for Cloud Network Fusion Environment

YANG Bo, JIANG Jinling, XU Shengchao, WANG Hongjie, MAO Mingyang, JIANG Darui
(School of Artificial Intelligence, Guangzhou Huashang College, Guangzhou 511300, China)

Abstract: With the rapid development of cloud computing and network virtualization, distributed networks in cloud network fusion environments are more complex and massive than ordinary networks, making it difficult to ensure the recall rate of network intrusion path tracking. Therefore, a distributed network intrusion path tracking and detection method in cloud network fusion environments is proposed. Combined with the characteristics of distributed networks in the cloud network fusion environments, a distributed network model is constructed. After the network data flow information is converted into a unified format, the processed information is filtered and processed by considering the impact of interference factors on the network data flow information. The intrusion information feature factor of the distributed network in the cloud network fusion environment is calculated by using the network data flow information, and the intrusion path is tracked and detected by using the intrusion information feature factor. The test results show that the accuracy of the network intrusion path tracking and detection can reach 99.9%, and the F_1 value is always greater than 0.85, it is significantly better than that of the control group and has high completeness performance.

Keywords: network intrusion path; cloud-network convergence; distributed network model; data flow information; characterization factor

0 引言

云网融合环境在构成方面的特征主要包括云网一体、要素聚合和能力开放。通过技术创新的突破,使得云网融合的新型基础设施能够提供无处不在的连接,并且实现了深度融合了网络与算力的目的[1-2],打破了云网边端在智能互联方面存在的局限性。不仅如此,借助云网融合的新型基础设施,也为大数据、人工智能提供了技术保障和支持,为物联网、区块链和量子安全提供了新的要素拓展空间,从高速通路和算力保障方面实现了集成创新发展。不仅如此,通过协同创新和开放创新全新的数据中心[3-4],也为数字化平台的建设和发展带来了新的可执行方向。通过建立融合发展的新生态,云网融合的新型基础设施具备了更强的能力开放特性,实现不同技术的融合创新和协同发展。

在云网融合背景下,网络入侵可能导致个人隐私的侵

收稿日期:2024-03-29; **修回日期**:2024-05-15。
基金项目:国家自然科学基金面上项目(61772221);广州华商学院校内科研导师制项目(2023HSDS34)
作者简介:杨 波(1977-),男,硕士,副教授。
徐胜超(1980-),男,硕士,副教授。
蒋大锐(1986-),男,博士研究生,副教授。
引用格式:杨 波,蒋金陵,徐胜超,等.云网融合中分布式网络入侵路径跟踪检测方法[J].计算机测量与控制,2024,32(8):34-39.

犯[5-6]，包括窃取个人隐私数据、监控个人行为等。为了应对这些安全威胁，需要采取一系列安全措施，其中网络入侵路径跟踪检测就是极为重要的内容之一[7-8]。针对此，以人工蜂群算法为基础的网络入侵源快速跟踪方法受到了较为广泛的关注，该方法通过对网络入侵源数据进行编码处理，在对群体进行初始化后，构建了目标函数提取网络入侵源数据特征[9-10]，借助人工蜂群算法确定网络入侵路径，其主要解决了跟踪网络入侵源时存在入侵源定位能力差，跟踪路径长，误报个数较多以及数据收敛性差等问题[11-12]。其次，以决策树为基础的网络入侵路径识别跟踪也是较为常见的应用方法之一，其针对缺乏对网络传输节点状态分析的问题，在分析节点状态的过程中引入了决策树机制，利用目标节点与周围节点的状态差异[13-14]，确定节点作为网络入侵路径的概率，并将网络入侵的起始节点状态参数为基础，实现对完整路径的识别跟踪，表现出了较高的准确性与识别效率[15-16]。

在上述基础上，本文提出云网融合环境下分布式网络入侵路径跟踪检测方法，分析云网融合环境下分布式网络特性，构建了分布式网络模型，对网络数据流信息进行格式转化，采用入侵信息特征因子对入侵路径进行跟踪检测，并通过对比测试的方式，分析验证了设计方法的性能。

1　分布式网络入侵路径跟踪检测方法设计

1.1　云网融合环境下分布式网络模型构建

云计算平台提供的多层次安全防护措施和数据备份机制，可以有效保护数据安全，并提高网络的稳定性。在分布式网络模型中，云网融合可以实现数据备份、容灾恢复等功能，能够确保数据的安全性和可靠性[17]。为此，本文以分布式网络模型为基础，以此最大限度保障后续网络入侵路径跟踪检测结果的可靠性[18-19]。其中，对云网融合环境下分布式网络特性如下：

1）拓扑结构。通常使用混合或分层拓扑结构。这种结构通常包括核心网络和边缘网络[20]。核心网络主要负责大规模数据传输和跨节点通信，而边缘网络则更注重实时和本地交互。

2）节点分布。节点可以分布在不同的地理位置和设备上。这包括服务器、存储设备、终端设备等[21]。

3）传输容量。具有大规模的传输能力。这主要是由于引入了虚拟化的云资源，可以提供几乎无限的计算和存储能力[22]。

4）通信协议。通常使用多种通信协议来确保效率和安全性。例如，为了优化数据传输，可以使用改进的应用层协议[23]。

5）网络带宽。其特征在于高带宽。这主要是由于云计算的弹性扩展和虚拟化技术，可以动态增加或减少网络带宽[24]。

6）网络延迟。通常具有较低的网络延迟。这主要是因为云计算中心的位置通常离用户更近，从而减少了数据传输的距离和时间。

7）任务分配。通常基于云计算的弹性可扩展性和虚拟化技术。这允许基于需求将任务动态地分配给可用的计算和存储资源。

8）数据共享。数据存储和管理技术通常基于云计算。这允许多个用户和应用程序共享数据，同时确保数据的安全性和一致性。

综上所述云网融合环境下的分布式网络具有拓扑结构复杂、节点分布广泛、传输容量大、通信协议多样、网络带宽高、网络延迟低、任务分配灵活和数据共享高效等特点。以此为基础，本文构建的分布式网络模型如图 1 所示。

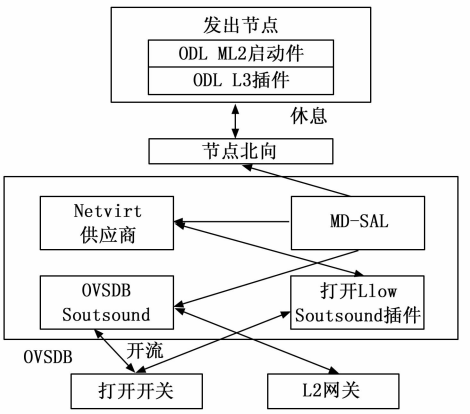

图 1　云网融合环境下分布式网络模型

通过发出节点，启动 ODL ML2 插件与 ODL L3 插件，控制节点进行交互，当节点北向时，经由 MD-SAL 向 Netvirt 供应商、OVSDB Soutsound 发送指令，并在供应商处理后，打开 Llow Soutsound 插件，实现开关控制，通过 OVSDB Soutsound 对 L2 网关进行数据交互，实现对云网融合环境下分布式网络模型的构建，为后续的入侵跟踪检测提供可靠的基础和保障。

1.2　网络入侵路径跟踪检测模型

结合 1.1 节构建的云网融合环境下分布式网络模型，本文在开展网络入侵路径跟踪检测阶段，主要是根据网络数据流状态实现的。

首先，将网络数据流信息转化为统一的格式，以便于后续的分析计算，具体的处理方式可以表示为公式（1）：

$$A_i = \int_{t_0}^{t} \beta * \frac{x_i}{B} \tag{1}$$

其中：A_i 为统一化之后的云网融合环境下分布式网络数据流信息，β 为分布式网络数据流信息的阻尼系数，x_i 为原始云网融合环境下分布式网络数据流信息，B 为分布式网络数据流信息转换器的转换系数，t_0 和 t 分别为原始云网融合环境下分布式网络数据流信息 x_i 在网络内传输对应的起始时间和结束时间。

考虑到干扰因素对于网络数据流信息带来的影响，本

文对处理后的信息进行滤波处理，具体的实现方式可以表示为公式（2）：

$$f(u,v)=\frac{1}{\frac{(u^2+v^2)^{1/2}}{A_i}*(k-1)} \tag{2}$$

其中：f（u，v）为滤波器，u 和 v 分别为滤波的长度参数和宽度参数，k 为截止频率常数。

在此基础上，利用网络数据流信息获取云网融合环境下分布式网络的入侵信息特征因子，以此作为后续入侵跟踪的基准，具体表示为公式（3）：

$$S_{ij}=\frac{\gamma_{ij}\sum(a_i-a_j)}{\sqrt{a_i}\sqrt{a_j}} \tag{3}$$

其中：S_{ij} 表示 a_i 和 a_j 网络数据流信息之间的特征因子，γ_{ij} 表示 a_i 和 a_j 网络数据流信息之间的关联度参数。

结合对入侵信息特征因子的计算结果，本文将取值结果大于 1.0 的参数作为最终的入侵判定标准。其中，峰值是一个时不稳参数，不同的时刻变动很大。则此时的入侵信息峰值因子可以表示为公式（4）：

$$G_h=\frac{\sum maxS_{ij}-\overline{S_{ij}}}{p}/\sqrt{\sum {S_{ij}}^2} \tag{4}$$

其中：G_h 为入侵信息峰值因子，$maxS_{ij}$ 为网络数据流信息之间的特征因子最大值，$\overline{S_{ij}}$ 为网络数据流信息之间的特征因子平均值，p 为极值数量。

峭度因子表示波形平缓程度的指标，用于描述网络数据流信息变量的分布。对应的云网融合环境下分布式网络入侵信息峭度因子可以表示为公式（5）：

$$G_q=\frac{\sum {S_{ij}}^4}{q^4} \tag{5}$$

其中：G_q 为入侵信息峭度因子，q 为云网融合环境下分布式网络流量波动极值的均方根。

而对于波形因子而言，其主要是以云网融合环境下分布式网络交流讯号中无因次量的形式存在，本文对入侵信息波形因子的计算方式可以表示为公式（6）：

$$G_b=\sqrt{\frac{q^2}{{G_h}^2-{G_q}^2}} \tag{6}$$

其中：G_b 为入侵信息波形因子。结合式（6）可以看出，其为云网融合环境下分布式网络流量波动极值的均方根与入侵信息峰值因子和入侵信息峭度因子之差的比值。

按照上述所示的方式，对应的入侵路径容易按照峰值因子、峭度因子以及波形因子由强到弱的方式传递的，以此实现对入侵路径的跟踪检测。具体入侵路径的跟踪检测流程如图 2 所示。

入侵路径的跟踪检测步骤如下：

1）云网融合网络数据流信息格式转化。将云网融合网络数据流信息转化为统一的格式，以便于后续的分析计算。

2）信息滤波处理。通过滤波器对云网融合网络数据流信息进行滤波处理，剔除干扰因素对网络数据流信息带来的影响。

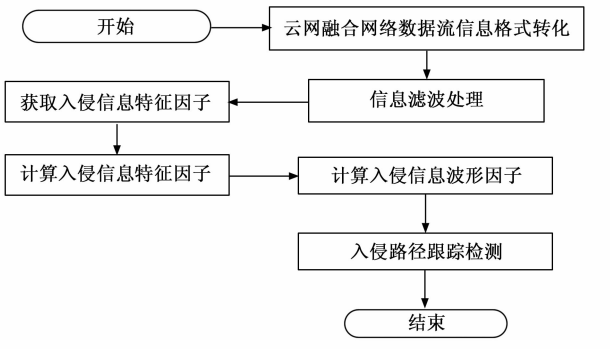

图 2 网路入侵路径的跟踪检测流程

3）获取入侵信息特征因子。利用网络数据流信息获取云网融合环境下分布式网络的入侵信息特征因子，以此作为后续入侵跟踪的基准。

4）计算入侵信息特征因子。通过关联度参数对入侵信息特征因子进行计算，将取值结果大于 1.0 的参数作为最终的入侵判定标准，确定入侵信息峰值因子。

5）计算入侵信息波形因子。获取云网融合环境下分布式网络流量波动极值的均方根与入侵信息峰值因子和入侵信息峭度因子之差的比值，计算得到入侵信息波形因子。

6）入侵路径跟踪检测。对应的入侵路径容易按照峰值因子、峭度因子以及波形因子由强到弱的方式传递的，以此实现对入侵路径的跟踪检测。

但是需要注意的是，可能存在部分峰值因子相同、峭度因子相同，或波形因子相同的情况，此时按照就近原则将当前跟踪结果距离较近的位置作为下一个跟踪目标即可。

2 模型测试与性能分析

2.1 测试准备与性能指标

在分析本文设计云网融合环境下分布式网络入侵路径跟踪检测方法性能的过程中，开展了对比测试。其中，参与测试的对照组分别为以人工蜂群算法为基础的网络入侵源快速跟踪方法，以及以决策树为基础的网络入侵路径识别跟踪方法。

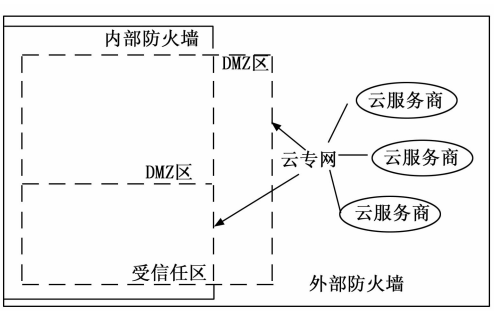

图 3 云网融合环境入侵路径跟踪的拓扑图

在进行云网融合测试时需要建立一个基于软件定义网路（SDN）和网络功能虚拟化（NFV）技术的统一网络架

构。在这个架构中，需要使用以下硬件设备：云计算服务器、虚拟交换机、存储设备、SDN 交换机。为了能够实现对 Internet 和实验网络的有效划分，本文引入了外部防火墙（Firewall-1）结构，将其作为具体的分隔结果。考虑到实际的网络环境也是由多个部分组成的，因此，进一步对实验网络进行分割，本文借助内部防火墙（Firewall-2）将其划分为 DMZ 区和受信任区两个主要区域。在测试的 6 个主机中，设置 H0 为受攻击者控制的主机，设置 H1 为 Web 服务器，设置 H2 为 FTP 服务器，设置 H3 为 E-mail 服务器，设置 H4 为安全管理服务器，设置 H5 为数据库服务器。具体的配置信息和漏洞信息如表 1 所示。

表 1　云网融合测试环境配置信息统计表

主发动机	应用	服务	漏洞
H1	IBM Security Key Lifecycle Manager 3.0	Apache ATS6.2.2	勒索软件攻击
H2	TFTP Server	Windows Server 2008 R2	钓鱼攻击
H3	Oracle E-Business Suite 12.1.1	Apache ATS6.2.2	恶意脚本攻击
H4	openSSh	Windows Server 2008 R2	DDoS 攻击
H5	MySQL Server 8.0.12	Windows Server 2008 R2	零时漏洞攻击

文中，信息波形因子通常取值 0.5，表示信号的功率与基本频率的比例，本文中取值 0.668，入侵信息特征因子表示入侵行为的特征程度或者异常度，本文选择 0.528。

在此基础上，分别采用上述的 3 种方法对测试网络环境的入侵路径进行跟踪测试，分析不同方法测试结果的可靠性。F_1 测试指标计算公式如下：

$$F_1 = 2 * (Precision * Recall)/(Precision + Recall) \quad (7)$$

其中：F_1 是一种综合评价指标，它结合了精确率（*Precision*）和召回率（*Recall*）两个指标，适用于不平衡数据集中跟踪检测方法性能的评估，它的取值范围在 0～1 之间，数值越接近 1 代表跟踪检测性能越好

精确率 *Precision* 计算公式为：

$$Precision = TP/(TP + FP) \quad (8)$$

Precision 为预测为正类中真正为正类的比例。精确率用于评估分类模型对于预测为正类的样本的准确性。

TP 表示真阳性（True Positive），表示模型正确预测出的正类样本数；

FP 表示假阳性（False Positive），表示模型错误地将负类样本预测为正类的样本数。

召回率 *Recall* 计算公式为：

$$Recall = TP/(TP + FN) \quad (9)$$

Recall 是衡量跟踪检测方法能够正确预测正类样本的能力，也称为“查全率”或“灵敏度”。*Recall* 用于评估分类模型找出正类样本的能力。*FN* 表示假阴性（False Negative），表示模型错误地将正类样本预测为负类的样本数。通过计算出 *Precision* 和 *Recall*，可以得到 F_1 值来综合评估模型的性能。

2.2　准确性测试

采用基于人工蜂群的入侵路径跟踪检测方法、基于决策树的入侵路径跟踪检测方法以及本文方法进行入侵路径跟踪检测准确性实验验证与比较，得到结果见表 2。

表 2　分布式网络入侵路径跟踪检测准确性　　%

数据量/GB	人工蜂群算法	决策树算法	本文方法
100	62.5	61.8	99.8
200	65.4	62.3	99.9
300	66.9	66.5	99.6
400	69.2	62.2	99.2

分析表 2 可知，当数据量为 100 GB 时，人工蜂群算法的分布式网络入侵路径跟踪检测准确性为 62.5%，决策树算法的分布式网络入侵路径跟踪检测准确性为 61.8%，本文方法的分布式网络入侵路径跟踪检测准确性为 99.8%；当数据量为 400 GB 时，人工蜂群算法的分布式网络入侵路径跟踪检测准确性为 69.2%，决策树算法的分布式网络入侵路径跟踪检测准确性为 62.2%，本文方法的分布式网络入侵路径跟踪检测准确性为 99.2%；本文方法始终具有较高的分布式网络入侵路径跟踪检测准确性，验证了本文方法的入侵路径跟踪检测效果。得到这样的良好性能是因为本文方法构建分布式网络模型，通过将任务和数据分散在多个节点上处理和存储，及时发现异常行为并追踪其源头，能够快速响应和阻止入侵活动，提高跟踪检测的准确性。

2.3　召回率测试

召回率实验验证比较结果见表 3。分析表 3 可知，当数据量为 100 GB 时，人工蜂群算法的分布式网络入侵路径跟踪检测召回率为 66.5%，决策树算法的分布式网络入侵路径跟踪检测召回率为 68.8%，本文方法的分布式网络入侵路径跟踪检测召回率为 99.6%；当数据量为 400 GB 时，人工蜂群算法的分布式网络入侵路径跟踪检测召回率为 63.2%，决策树算法的分布式网络入侵路径跟踪检测召回率为 62.6%，本文方法的分布式网络入侵路径跟踪检测召回率为 99.0%；本文方法始终具有较高的入侵路径跟踪检测召回率，入侵检测效果好。这是因为本文方法充分利用多种数据源来收集网络流量、日志和事件等信息。通过综合

表 3　分布式网络入侵路径跟踪检测召回率　　%

数据量/GB	人工蜂群算法	决策树算法	本文方法
100	66.5	68.8	99.6
200	62.4	69.7	99.2
300	65.6	62.6	99.0
400	63.2	65.8	98.8

分析不同来源的数据，可以更全面地了解网络活动，并发现潜在的入侵路径。并通过构建分布式网络模型，对数据进行冗余处理和备份，可以提高数据的安全性和灾备能力，有效提升跟踪检测召回率。

2.4 F_1 值测试

在对具体的跟踪结果进行分析时，本文将 F_1 值作为具体的评价指标，对应的入侵类型共设置了 5 种较为常见的入侵攻击，具体分别为勒索软件攻击、钓鱼攻击、恶意脚本攻击、DDoS 攻击以及零时漏洞攻击，以此更加全面地对设计方法的跟踪检测效果进行分析评价。以此为基础，不同方法的测试结果如表 4 所示。

表 4 3 种不同方法的 F_1 值

入侵类型	人工蜂群方法	决策树方法	本文方法
勒索软件攻击	0.775	0.786	0.860
钓鱼攻击	0.784	0.782	0.862
恶意脚本攻击	0.788	0.785	0.883
DDoS 攻击	0.778	0.781	0.868
零时漏洞攻击	0.785	0.782	0.882

结合表 4 的测试结果对 3 种跟踪检测方法的性能进行分析可以看出，在以人工蜂群算法为基础的网络入侵源快速跟踪方法下，F_1 值出现了较为明显的波动，其中，最小值仅为 0.775，最大值达到了 0.794；在决策树为基础的网络入侵路径识别跟踪方法下，F_1 值较为稳定，但是整体水平相对偏低，基本处于 0.78～0.79 区间范围内。相比之下，在本文设计入侵路径跟踪检测方法下，F_1 值始终大于 0.85，明显优于对照组。这是因为本文构建了分布式网络模型，将网络数据流信息转化为统一的格式后，利用入侵信息特征因子实现对入侵路径的跟踪检测，有效提升跟踪检测方法的性能。由此可以得出结论，本文设计的云网融合环境下分布式网络入侵路径跟踪检测方法可以实现对入侵路径的完整检测，具有较高的查全性能。

3 结束语

本文提出云网融合环境下分布式网络入侵路径跟踪检测方法研究，结合云网融合环境下分布式网络特性，构建了分布式网络模型，利用入侵信息特征因子实现对入侵路径的跟踪检测，切实实现了对网络入侵路径的有效跟踪。借助本文的设计与研究，可以为实际的云网融合环境下分布式网络安全管理提供有价值的参考。在之后的研究中，可以进一步深化对不同类型入侵在特征因子方面的差异化表现，以此提高入侵路径跟踪检测准确性方面的性能，保障其在更大范围内的应用价值和应用效果。

参考文献

[1] ZHANG Z, ZHANG Y, GUO D, et al. SecFedNIDS: Robust defense for poisoning attack against federated learning-based network intrusion detection system [J]. Future Generations Computer Systems, 2022, 134 (16): 154 - 169.

[2] A U A, A C W L, C G S B. A resource allocation deep active learning based on load balancer for network intrusion detection in SDN sensors [J]. Computer Communications, 2022, 184 (15): 56 - 63.

[3] MATEUSZ S, PAWLICKI M, KOZIK R, et al. The application of deep learning imputation and other advanced methods for handling missing values in network intrusion detection [J]. Vietnam Journal of Computer Science, 2023, 10 (1): 1 - 23.

[4] SATHIYADHAS S S, ANTONY M C V S. A network intrusion detection system in cloud computing environment using dragonfly improved invasive weed optimization integrated Shepard convolutional neural network [J]. International Journal of Adaptive Control and Signal Processing, 2022, 35 (5): 1060 - 1076.

[5] WANG W, LI J, ZHAO N, et al. MEM-TET: improved triplet network for intrusion detection system [J]. J Computers, Materials & Continua, 2023 (7): 471 - 487.

[6] OJUGO A A, YORO R E. Forging a deep learning neural network intrusion detection framework to curb the distributed denial of service attack [J]. International Journal of Electrical and Computer Engineering, 2021, 11 (2): 1498 - 1509.

[7] ALMOMANI O. A hybrid model using bio-inspired metaheuristic algorithms for network intrusion detection system [J]. J Computers, Materials & Continua, 2021 (7): 409-429.

[8] MASEER K Z, YUSOF R, MOSTAFA A S, et al. DeepIoT. IDS: hybrid deep learning for enhancing IoT network intrusion detection [J]. Computers, Materials Continua, 2021, 69 (3): 3945 - 3966.

[9] FARAH K, CHABIR K, ABDELKRIM M N. High level Petri nets-based proposal of an integrated intrusion detection and prevention mechanism in network controlled systems [J]. IET Communications, 2023, 17 (4): 467 - 477.

[10] HAGHIGHAT M H, LI J. Intrusion detection system using voting-based neural network [J]. Tsinghua Science & Technology, 2021, 26 (4): 484 - 495.

[11] POOJA T S, SHRINIVASACHARYA P. Evaluating neural networks using bi-directional LSTM for network IDS (intrusion detection systems) in cyber security [J]. Global Transformation Collection, 2021, 2 (2): 448 - 454.

[12] MOHAMMADIAN H, GHORBANI A A, LASHKARI A H. A gradient-based approach for adversarial attack on deep learning-based network intrusion detection systems [J]. Applied Soft Computing, 2023, 137: 110173 - 110185.

[13] CAO Z, LI J, FU Y, et al. An adaptive biogeography-based optimization with cumulative covariance matrix for rule-based network intrusion detection [J]. Swarm and Evolutionary Computation, 2022 (75): 1 - 16.

[14] GANGULA R, MURALI M V, KUMARM R. Network in-

trusion detection system for internet of things based on enhanced flower pollination algorithm and ensemble classifier [J]. Concurrency and Computation: Practice and Experience, 2022, 34 (21): 7103 - 7118.

[15] WANG Z, LI Z, HE D, et al. A lightweight approach for network intrusion detection in industrial cyber-physical systems based on knowledge distillation and deep metric learning [J]. Expert Systems with Application, 2022, 206: 1 - 17.

[16] GUPTA K, SHARMA D K, GUPTA K D, et al. A tree classifier based network intrusion detection model for internet of medical things [J]. Computers and Electrical Engineering, 2022, 102: 108158-1-108158-20.

[17] HOSSEINI S, SARDO S R. Network intrusion detection based on deep learning method in internet of thing [J]. Journal of Reliable Intelligent Environments, 2023, 9 (2): 147 - 159.

[18] JINGHONG L, XUDONG L, BO L, et al. A novel hierarchical attention-based triplet network with unsupervised domain adaptation for network intrusion detection [J]. Applied Intelligence: The International Journal of Artificial Intelligence, Neural Networks, and Complex Problem-Solving Technologies, 2023, 53 (10): 11705 - 11726.

[19] KIM T, PAK W. Real-time network intrusion detection using deferred decision and hybrid classifier [J]. Future Generation Computer Systems, 2022, 132: 51 - 66.

[20] YANG Z, LIU Z, ZONG X, et al. An optimized adaptive ensemble model with feature selection for network intrusion detection [J]. Concurrency and Computation: Practice and Experience, 2022, 35 (4): 7529 - 7551.

[21] CAVILLE E, LO W W, LAYEGHY S, et al. Anomal-E: A self-supervised network intrusion detection system based on graph neural networks [J]. Knowledge-based Systems, 2022, 258: 1 - 11.

[22] SAMRIYA J K, TIWARI R, CHENG X, et al. Network intrusion detection using ACO-DNN model with DVFS based energy optimization in cloud framework [J]. Sustain. Comput. Informatics Syst., 2022, 35: 1 - 9.

[23] BASATI A, FAGHIH M M. PDAE: efficient network intrusion detection in IoT using parallel deep auto-encoders [J]. Information Sciences: an International Journal, 2022 (598): 57 - 74.

[24] ALSHAYEJI M H, ALSULAIMI M, ABED S, et al. Network intrusion detection with auto-encoder and one-class support vector machine [J]. International Journal of Information Security and Privacy, 2022, 16: 67 - 84.

(上接第 33 页)

[3] 逯中香，樊彦国，李国胜. 利用时序 InSAR 技术监测青藏铁路沿线地表形变 [J]. 测绘通报，2022 (3)：138 - 142.

[4] 陈文婷，罗文婷，李　林，等. 基于 2D 与 3D 激光图像的轨道扣件状态智能检测 [J]. 仪表技术与传感器，2022 (11)：88 - 95.

[5] 林　军，康高强，涂振威，等. 轨道零部件级联缺陷检测算法 [J]. 控制与信息技术，2022 (3)：59 - 66.

[6] 时佳斌，柴雪松，王智超，等. 轨道变形监测系统设计与应用 [J]. 铁道建筑，2022，62 (4)：14 - 17.

[7] 刘俊博，刘俊尧，孙淑杰，等. 基于激光点云的铁路边坡表面形变检测方法 [J]. 铁道建筑，2021，61 (11)：82 - 85.

[8] 陈宝山，张立峰，何　毅，等. 兰新高速铁路军马场一民乐段地表形变监测及成因 [J]. 兰州大学学报 (自然科学版)，2022，58 (2)：222 - 228.

[9] 王　海，刘明亮，蔡英凤，等. 基于激光雷达与毫米波雷达融合的车辆目标检测算法 [J]. 江苏大学学报 (自然科学版)，2021，42 (4)：389 - 394.

[10] 彭孝东，何　静，时　磊，等. 基于激光雷达和 Kinect 相机点云融合的单木三维重建 [J]. 华中农业大学学报，2023，42 (2)：224 - 232.

[11] 陈勇强，贺　岩，罗　远，等. 基于盖革 APD 阵列脉冲式三维成像激光雷达系统 [J]. 中国激光，2023，50 (2)：97 - 106.

[12] 蒋筱朵，赵晓琛，冒添逸，等. 采用传感器融合网络的单光子激光雷达成像方法 [J]. 红外与激光工程，2022，51 (2)：49 - 55.

[13] 马泽亮，杨风暴. 基于尖 τ 型 DS 证据理论的机载 LiDAR 地物分类方法 [J]. 激光与红外，2021，51 (7)：853 - 858.

[14] 李维刚，梅　洋，樊　响，等. 基于车载激光点云的铁路轨道检测 [J]. 中国激光，2022，49 (4)：168 - 179.

[15] 张海凤. 鲁南高速铁路接入京沪高速铁路路基变形监测 [J]. 铁道建筑，2022，62 (5)：138 - 142.

[16] 刘艳芬，柴雪松，冯毅杰，等. 基于光纤弦测的无砟轨道变形监测关键技术研究 [J]. 铁道建筑，2022，62 (4)：8 - 13.

[17] 潘兴良，刘建国. 基于经验模态分解法的下穿铁路工程对既有轨道变形监测数据降噪方法 [J]. 城市轨道交通研究，2022，25 (6)：96 - 101.

[18] 张　政，董昆灵，刘　明，等. 新型明桥面轨枕板式无砟轨道结构参数研究 [J]. 铁道标准设计，2022，66 (1)：32 - 36.

[19] 闫　斌，程瑞琦，谢浩然，等. 极端温度作用下桥上 CRTS Ⅱ型无砟轨道受力特性 [J]. 铁道科学与工程学报，2021，18 (4)：830 - 836.

[20] 刘伟斌. 高速铁路变形可调板式无砟轨道结构研究 [J]. 铁道建筑，2022，62 (1)：18 - 21.

[21] 栾佳宁，张　伟，孙　伟，等. 基于二维码视觉与激光雷达融合的高精度定位算法 [J]. 计算机应用，2021，41 (5)：1484 - 1491.

[22] 孙淑光，李如伟，李文建. BDS/GPS 双星座卫星轨道 RAIM 检测算法优化 [J]. 计算机仿真，2020，37 (7)：61 - 65.