基于内存增强自编码器的轻量级无人机网络异常检测模型

胡天柱[1,2]，沈玉龙[3]，任保全[2]，何吉[2,3]，刘成梁[2,3]，李洪钧[2]
（1.西安电子科技大学网络与信息安全学院，陕西 西安 710126；2.军事科学院系统工程研究院，北京 100070；
3.西安电子科技大学计算机科学与技术学院，陕西 西安 710126）

摘　要：为了解决传统智能攻击检测方法在无人机网络中存在的高能耗以及高度依赖人工标注数据的问题，提出一种基于双层内存增强自编码器集成架构的轻量级无人机网络在线异常检测模型。采用基于操作系统的消息队列进行数据包缓存，实现对高速数据流的持久化处理，有效提升了模型的稳定性和可靠性。基于衰减窗口模型计算数据流复合统计特征，以增量更新方式降低了计算过程中的内存复杂度。利用层次聚类算法对复合统计特征进行划分，将分离的特征输入集成架构中的多个小型内存增强自编码器进行独立训练，降低了计算复杂度，同时解决了传统自编码器因重构效果过拟合而导致的漏报问题。在公开数据集和NS-3仿真数据集上的实验表明，所提模型在保证轻量级的同时，与基线方法相比，假阴性率分别平均降低了35.9%和48%。

关键词：无人机网络；异常检测；轻量级在线检测；内存增强自编码器
中图分类号：TP309.1
文献标志码：A
DOI：10.11959/j.issn.1000−436x.2024011

Lightweight anomaly detection model for UAV networks based on memory-enhanced autoencoders

HU Tianzhu[1,2], SHEN Yulong[3], REN Baoquan[2], HE Ji[2,3], LIU Chengliang[2,3], LI Hongjun[2]
1. School of Cyber Engineering, Xidian University, Xi'an 710126, China
2. Academy of Systems Engineering, Academy of Military Sciences, Beijing 100070, China
3. School of Computer Science and Technology, Xidian University, Xi'an 710126, China

Abstract: In order to solve the problems of high energy consumption and high reliance on manual annotation data of traditional intelligent attack detection methods in UAV networks, a lightweight UAV network online anomaly detection model based on a double-layer memory-enhanced autoencoder integrated architecture was proposed. The message queue based on the operating system was used for data packet caching to achieve persistent processing of high-speed data streams, which effectively improved the stability and reliability of the model. The composite statistical characteristics of the data flow were calculated based on the damped window model, and the memory complexity in the calculation process was reduced in an incremental update manner. The hierarchical clustering algorithm was used to divide the composite statistical features, and the separated features were input to multiple small memory-enhanced autoencoders in the integrated architecture for independent training, which reduced the computational complexity and solved the problem of false negatives caused by the overfitting of the reconstruction effect of the traditional autoencoder. Experiments on public data sets and NS-3 simulation data sets show that while ensuring lightweight, the proposed model reduces the false negative rate by an average of 35.9% and 48% compared with the baseline method.

Keywords: UAV network, anomaly detection, lightweight online detection, memory-augmented autoencoder

收稿日期：2023–07–05；**修回日期**：2023–09–23
通信作者：沈玉龙，ylshen@mail.xidian.edu.cn
基金项目：国家自然科学基金资助项目（No.62220106004, No.61972308）；国家自然科学基金重大研究计划基金资助项目（No.92267204）；陕西省重点研发计划基金资助项目（No.2022KXJ-093, No.2021ZDLGY07-05）；陕西省创新能力支撑计划基金资助项目（No.2023-CX-TD-02）
Foundation Items：The National Natural Science Foundation of China (No.62220106004, No.61972308), Major Research Plan of the National Natural Science Foundation of China (No.92267204), The Key Research and Development Program of Shaanxi Province (No.2022KXJ-093, No.2021ZDLGY07-05), Innovation Capability Support Program of Shaanxi (No.2023-CX-TD-02)

0 引言

随着计算机技术的不断发展，智能无人系统已在众多领域得到了广泛应用。然而，受限于系统网络的开放性、决策的部分自主性以及资源的有限性，这些智能无人系统在面对如未知攻击、复杂攻击等新型安全挑战时，其安全性备受威胁。尤其在无人机网络这类典型的智能无人系统中，安全问题更为明显。当前，针对智能无人系统网络安全问题的主流解决方案是在系统中部署网络入侵检测系统（NIDS, network intrusion detection system），旨在对恶意或异常的网络流量进行有效的识别与筛选[1]。

NIDS是一种部署于计算机网络关键节点的设备或软件，其主要职责是在检测到异常网络流量或活动时向网络管理员发出警告。近年来，得益于机器学习技术的快速发展，基于机器学习的NIDS已取得了显著的进步[2-4]。与基于攻击特征匹配的传统NIDS相比，基于机器学习的NIDS更擅长学习数据的复杂非线性特征[5-8]，并能利用网络的自相似性，采用异常检测的方式来识别未知或新型的攻击[9]。其典型的实施方式包括收集网络中一段时间内的流量数据，在特定的学习节点上利用这些数据对神经网络进行训练，然后将训练完成的神经网络模型部署于网络节点，并基于此模型对网络流量进行检测。当网络流量数据被判断为异常或恶意流量时，系统会向管理员发出警报[10]。然而，为了提升NIDS的准确性，神经网络常常趋于复杂，包括增加神经网络的层数和神经元数量，从而使特定学习节点对计算能力的需求大幅提升。将这类NIDS应用于无人机网络时，会面临以下几个主要挑战。

1) 无法在资源受限的无人机上部署。当前采用的模型算法在设计初期并未考虑资源有限的情况，导致模型对计算能力和内存的需求超出了无人机节点的承受范围。大部分无人机无法提供模型训练或运行所必需的计算资源。尽管可以在大型无人机或远程云服务器上进行模型训练或推理，但高频的数据回传在消耗大量网络带宽的同时，也会面临更高的安全风险（如隐私泄露和网络窃听）。

2) 难以实现在线检测。集中训练和检测模型在运行过程中通常需要汇总各无人机节点的数据包，这增加了传输时间，降低了攻击检测的时效性。复杂检测模型即使在算力充足的节点完成训练后部署至资源受限的节点，其高计算复杂度也导致数据包检测效率低下，难以满足动态复杂的无人机网络的在线检测需求。

3) 数据需要大量的人工标注。当前基于监督学习的NIDS需要使用带有标签的数据，而对数据标注需要消耗大量的人力资源。此外，基于人工标注数据的检测方法，无法有效应对样本缺失的新型和未知攻击。

为了解决上述问题，本文采用无监督学习的思想，提出了一种基于内存增强自编码器的轻量级在线检测模型，在不需要对数据进行人工标注的同时，能够有效应对新型攻击和未知攻击检测。具体地，针对单个自编码器性能有限且模型复杂度较高的问题，本文预先将多维网络特征按其相关性分类，然后分别放入多个较小规模的自编码器中，通过自编码器集成架构，实现性能提升的同时降低了总体模型复杂度。在此基础上，本文采用了内存增强自编码器进行集成，能够有效解决传统自编码器在异常数据上重构能力过强的问题，进而降低无人机网络异常检测的漏报率。此外，本文在检测模型数据包处理模块中加入了基于操作系统的消息队列，在保证低环境依赖性的同时可有效应对流量突发场景，提高了模型的稳定性。为了验证所提方法的有效性，本文在公开数据集之外，基于NS-3网络模拟器构造了面向无人机网络的攻击检测数据集。在2个数据集上的实验结果表明本文方法具有低计算复杂度的同时，对无人机网络攻击具有更好的检测效果。

1 相关工作

近年来，虽然机器学习技术的不断进步推动了异常检测技术的日益成熟，然而，面向无人机网络的网络攻击异常检测解决方案却相对较少。其主要原因如下：相较于传统的ad hoc网络攻击检测场景，无人机网络攻击检测更敏感地考虑能量消耗，并且其NIDS节点的资源受到严重限制[11]。目前，大部分网络攻击异常检测解决方案假设对模型训练和部署节点的能量与算力资源没有任何限制[12-14]。尽管这些模型和算法提升了异常检测性能，但设计的神经网络结构复杂、计算复杂度过高，无人机节点无法支撑高的能量消耗和算力需求。同时，现实中大规模标注完整的真实无人机网络攻击数据集的匮乏，也使部分基于监督学习的异常检测解决方案

无法适用于无人机网络异常检测场景。因此，本文在考察相关工作时，特别关注了适用于传统网络的轻量级和无监督学习的异常检测解决方案。

在轻量级异常检测解决方案领域，文献[15]提出了一种全自动、无监督的网络流量有效负载建模方式。这种基于有效负载的异常检测器在训练阶段计算配置文件的字节频率分布，并向单个主机和端口传送应用程序有效负载的标准偏差；在检测阶段，使用马氏距离来计算新数据与预先计算的配置文件的相似性，该检测器将此计算值与预设阈值进行比较，一旦超出阈值则发出警报。尽管此方法在1999 DARPA IDS等数据集上表现良好，但由于整体流程过于简单，其性能仍有限。文献[16]提出了一种基于超网格结构的K近邻（KNN）在线检测方案，目的是克服惰性学习问题。该方案通过将异常检测区域从超球体重新定义为超网格结构，显著降低了计算复杂度。同时，采用附加系数将超网格结构转换为正坐标空间，保留了在线更新的冗余度和位操作剪裁能力。因此，该方案可以在任何环境中成功运行，不需要人工干预。然而，由于需要积累大量数据进行训练和检测，该方法并不适用于本文所研究的无人机网络场景。

在无监督学习领域，自编码器是最常用的深度学习模型之一。文献[17]基于堆叠去噪自动编码器（SDAE, stacked denoising auto encoder）来处理在线环境中的对象追踪问题。SDAE的每一层都视为原始图像数据的不同特征空间。该研究将SDAE的每一层转化为深度神经网络，从而应用于二元分类器的网络攻击鉴别。尽管该研究在在线环境中使用了自编码器，但并未进行异常检测或实现在线检测。此外，深度神经网络的训练过程复杂，难以在简单的无人机上实际部署。文献[18-19]尝试通过自动编码器从数据集中提取特征，以提高网络威胁的检测能力，然而其并未直接利用自动编码器进行异常检测，而是采用传统分类器进行网络威胁的检测，这导致该类方法需要专家对样本进行标注。进一步，文献[20]提出了一种基于自编码器集成结构的攻击检测模型，首次将自编码器作为核心应用于网络流量的异常检测，通过降低单个自编码器隐含层数并集成多个小型自编码器，实现了轻量级的在线检测。在此基础上，各种改进型自编码器，如降噪自编码器[21]、堆叠自编码器[22]、变分自编码器[23]、内存增强自编码器[24]被应用于网络攻击异常检测中，其通过对传统自编码器添加约束或修改网络结构实现了检测性能的提升。

上述方法为无人机网络异常检测提供了一些建设性思路，基于普通自编码器的集成结构虽可实现轻量级异常检测，但普通自编码器以最小化重构误差为优化目标而导致可能无法学习数据本质特征，检测性能较差。为了提升检测性能，改进型自编码器检测方案往往需要增加神经网络层数或神经元个数，模型结构趋于复杂，模型整体计算复杂度较高。因此，本文提出一种基于内存增强自编码器集成结构的异常检测模型，通过将多个神经网络层数较少的小型内存增强自编码器进行集成，在保证检测性能的情况下，实现了轻量级的在线异常检测。

2　无人机网络异常检测问题描述

本节介绍了无人机网络异常检测场景并描述了在该场景下的网络异常检测问题。

如图1所示，本文研究的无人机网络主要包含地面基站、中继无人机及终端无人机等三类节点。地面基站负责统一管理所有无人机节点，包括接收无人机安全警报并依据警报内容制定相关防御策略。中继无人机主要作为通信中继节点对本机和其他无人机向地面基站发送的安全警报及其他数据进行多跳传输，最终转发至地面基站。终端无人机主要接收中继无人机转发的数据，并在受到网络攻击时发出警告。

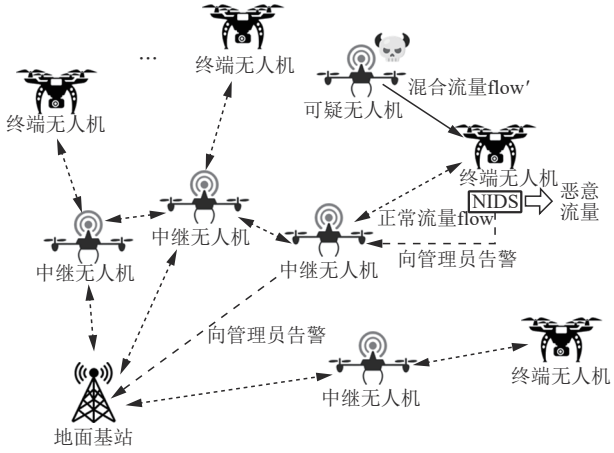


图1　无人机网络攻击检测场景

在本文所研究场景中，NIDS部署于无人机节点。在无网络攻击情况下，部署于无人机的NIDS

采集本节点与其他无人机节点产生的正常流量，并学习其数据特征。当遭受网络攻击时，NIDS从包含攻击流量的混合流量中，分辨出恶意攻击流量，并通过其他中继无人机将警报转发至地面基站。针对上述场景，可给出如下攻击检测问题描述：给定正常流量flow = { $p_1,p_2,\cdots,p_m$ }，其中p_m包含了此流量中第m个数据包的全部信息。在此条件下，对混合流量flow′ = { $p'_1,p'_2,\cdots,p'_n$ }中数据包进行标记，正常标记为0，异常标记为1，其中p'_n包含了此流量中第n个数据包的全部信息。

3　异常检测模型设计

针对上述问题，本文提出一种基于双层内存增强自编码器集成结构的异常检测模型，以满足无人机节点网络攻击检测需求。所提模型主要包含数据包处理模块、特征处理模块以及异常检测模块。其中，数据包处理模块主要基于网络嗅探器和消息队列技术，实现数据包采集、报文解析及数据缓存功能；特征处理模块主要提取数据流，并基于衰减窗口模型对数据流进行序列划分，选择并计算复合统计特征，采用层次聚类方法构建网络流量特征矩阵及网络流量特征组；异常检测模块主要基于双层内存增强自编码器的集成结构进行网络流量异常检测。

异常检测模型工作流程如图2所示。数据包处理模块首先采集网络流量，包括训练过程中的正常流量flow及测试过程中的混合流量flow′，对其进行解析形成正常数据信息集合P及混合数据信息集合P'，并依据本地配置和性能决定是否基于消息队列技术以缓存形式将解析信息传送至特征处理模块。特征处理模块对P及P'进行处理，抽取数据流并基于衰减窗口模型对数据流进行序列划分，在此基础上选择并计算各数据序列的复合统计特征，以构建正常数据流特征矩阵$\boldsymbol{f}$及混合数据流特征矩阵$\boldsymbol{f}'$。而后采用层次聚类算法，根据特征的关联性将此矩阵中特征向量分为若干个包含强关联特征的特征类集合H及H'，这些特征类将作为后续异常检测模块中自编码器的输入。异常检测模块首先接收待训练的网络流量特征类集合H，并将其输入双层自编码器集成结构中进行学习和训练，同时计算正常流量的重构误差阈值。待检测流量特征类集合H'输入模块时，则依次计算每个数据包的重构误差，若此误差超出了正常流量重构误差阈值，则将其标记为异常。所有数据包完成标记后，返回其中标记为异常的数据包序列号集合S，完成网络异常检测。

3.1　数据包处理模块

为了解决流量突发导致的数据包采集、解析以及模块间处理速度的不匹配问题，本文设计了一种以消息队列技术为基础的数据包处理模块。该模块的主要职能包括数据包的采集、解析以及信息传输。通过将基于操作系统的消息队列与网络嗅探器相结合，有效地解决了数据包处理模块与特征处理模块之间的处理速度差异问题。这种设计策略实现了模块间的解耦，进而提升了模型的整体可靠性。

如图3所示，数据包处理模块基于传统网络嗅探器及其应用程序接口（API），对正常流量flow及混合流量flow′进行采集并解析其包含的数据包，从中提取出正常数据信息集合P = { $p_1,p_2,\cdots,p_m$ }和混合数据信息集合P' = { $p_1,p_2,\cdots,p_n$ }，其中，p_m包含正常集合中第m个数据包的全部信息。

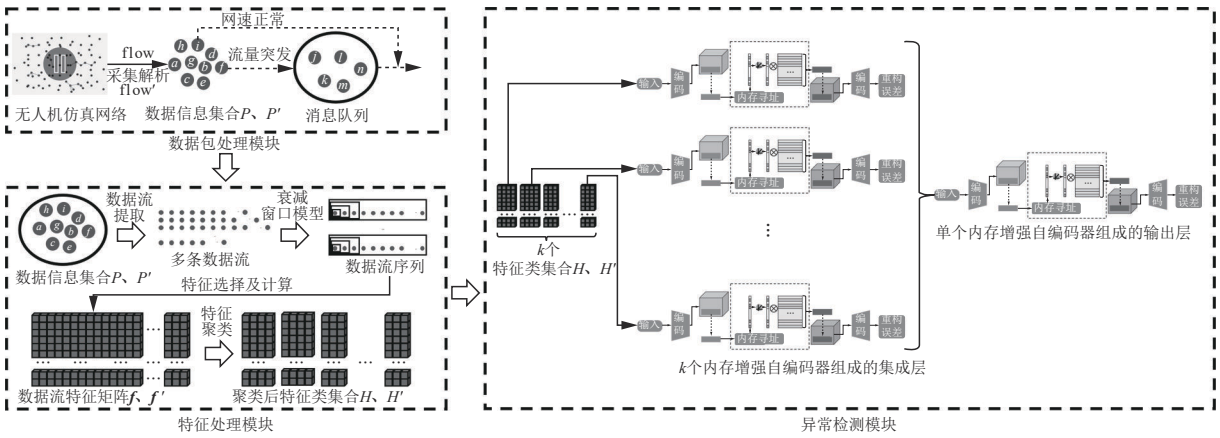


图2　异常检测模型工作流程

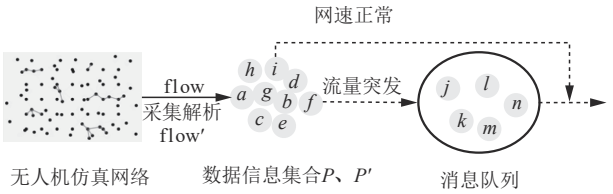


图3　数据包处理模块工作流程

在网速正常情况下，数据包处理模块直接将此集合传输至后续特征处理模块。而在流量突发场景下，NIDS 节点固定的硬件配置使特征处理模块处理网络数据包的速率具有上限，这将导致特征处理模块的处理速度难以与数据包采集速率保持同步。因此，本文使用基于操作系统的消息队列在流量突发场景下进行辅助传输。基于操作系统的消息队列本质是利用操作系统提供的消息队列 API，在操作系统内核空间维护一个消息链表，通过将暂时无法处理的数据信息缓存至内存空间，由特征处理模块依据自身处理速度以“先进先出”原则依次取出数据特征信息进行处理，保障了流量突发情况下系统的稳定持续运行。

基于操作系统的消息队列相对于目前主流的基于数据库的消息队列技术，去除主流消息队列中用于实现分布式通信和高并发请求的功能模块，仅用于本地流量“削峰填谷”和模块间解耦，有效提高流量突发场景下整体模型的稳定性且更加轻量级；基于操作系统原装 API，软件依赖更少，启动更快，适用于流量突发时临时调用辅助传输。由于上述优点，本文基于此消息队列技术所设计的数据包处理模块更加适用于轻量级在线检测场景，满足无人机网络对 NIDS 鲁棒性和可靠性的需求。

3.2　特征处理模块

为降低数据流数据挖掘中的内存复杂度，提高异常检测模型检测性能，本文设计了特征提取模块。该模块主要负责数据流提取、数据流序列划分、特征选择、特征计算和特征聚类。首先，在正常数据信息集合 $P=\{p_1,p_2,\cdots,p_m\}$ 和混合数据信息集合 $P'=\{p_1,p_2,\cdots,p_n\}$ 中提取网络数据流，并采用衰减窗口模型对数据流进行序列划分，在此基础上选择并计算数据流复合统计特征，构建正常数据流特征矩阵 $\boldsymbol{f}$ 及混合数据流特征矩阵 $\boldsymbol{f}'$。最后，基于层次聚类方法依据特征间相关性将数据流特征矩阵中的多维特征分为若干个特征类，构建正常流量特征类集合 H 及混合流量特征类集合 H'，以备后续异常检测模块中多个自编码器调用，其中，H 作为异常检测模块训练过程的输入，H' 作为异常检测模块检测过程的输入。特征处理模块工作流程如图 4 所示。

3.2.1　特征选择及计算

数据特征是数据对事实本身的客观描述。在异常检测中，因网络流量的自相似性，网络攻击发生时，数据包及数据流的特征均将发生变化，因此可通过对关键数据特征的选择、提取和分析来对网络攻击进行识别。特征的选择直接影响到异常检测的效果。目前，绝大多数网络攻击往往无法通过对单个数据包基本特征进行分析来完成识别，必须依赖网络通信数据包上下文信息即网络数据流特征进行分析判断。例如，单个请求服务可能是正常的，但是短时间内大量请求服务却可能是分布式拒绝服务（DDoS）攻击；单个基于传输控制协议（TCP）或

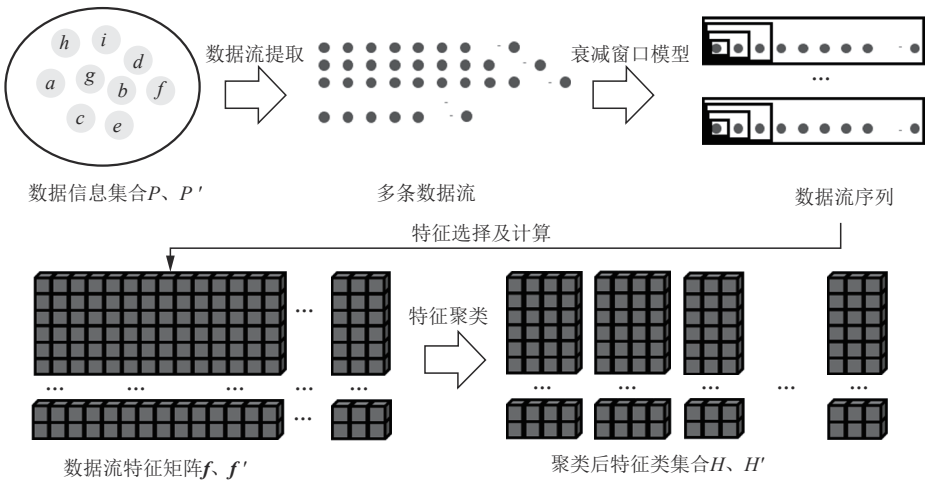


图4　特征处理模块工作流程

用户数据报协议（UDP）的端口连接请求可能是正常的，但是对于某台主机多个端口的频繁连接请求却可能是高级长期威胁（APT）攻击入侵阶段的端口扫描。因此，本文选用数据流复合统计特征作为异常检测的分析基础。在选择并计算复合统计特征前，首先从自数据包处理模块接收到的大量数据信息集合P及P'中提取数据流，然后基于衰减窗口模型将数据流划分为多个数据流序列，最后选择并计算复合统计特征，分别形成数据流特征矩阵$\boldsymbol{f}$及$\boldsymbol{f}'$。

在数据流提取方面，由于当前网络中存在大量IP地址伪造情况，仅依据特定IP地址提取数据流很容易将伪造IP地址的恶意流量混入正常流量中，针对此问题，本文提取基于源MAC地址和IP地址的出站流量、源IP地址的出站流量；针对网络攻击的单向性，本文选用源IP与目的IP间产生的出入站流量；考虑到特定应用或进程产生数据流量的差异性，本文进一步选用源TCP/UDP套接字与目的TCP/UDP套接字之间产生的出入站流量。上述选用数据流量共计4种。

为了更好地学习数据流特征，本文采用衰减窗口模型对数据流进行处理，以得到多个数据流序列。在主流窗口模型中，传统界标窗口模型未考虑数据包与时间的关系，而滑动窗口模型通过固定时间大小或数据包个数进行序列划分，因而必须存储窗口中所有数据包信息，内存复杂度为$O(n)$。考虑到数据包时序性和处理过程中的内存复杂度，本文基于衰减窗口模型[25]对数据流进行处理。

如图5所示，衰减窗口模型计算特定数据包到达时动态数据流统计特征的对象是从初始时刻到数据包到达时刻间隔内所有数据包。当有新数据包到达时，在窗口内的所有数据包依据其自身时间戳与到达时刻差值，基于时间衰减窗口模型所定义的衰减函数计算其对应衰减权重，并基于此权重对其自身数据包各数据进行衰减，以体现数据流量的时序性。衰减函数计算式为

$$\gamma_{\lambda,i}=d_\lambda(t_i)=2^{-\lambda(t_{\text{new}}-t_i)} \tag{1}$$

其中，$\lambda(\lambda>0)$表示衰减因子，t_i表示第i个数据到达时间，t_{new}表示最新数据到达时间。当有新数据到达窗口时，历史序列数据及新数据将依据式(1)计算衰减权重进行衰减，以构成新的数据序列。从式(1)可以看出，最新到达数据权重恒为1。通过调整λ取值，可动态调整模型对历史数据的关注度。例如，当$\lambda\to+\infty$时，$d_\lambda(t)\to 0$，窗口模型不关注历史数据，待衰减序列在衰减过程中完全从窗口中删除；当$\lambda=0$时，$d_\lambda(t)=1$，历史数据与最新数据权重相同，对历史数据和最新数据同样关注。

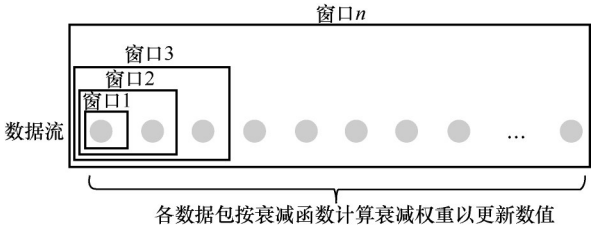


图5　衰减窗口模型

基于上述衰减窗口模型，本文以增量更新方式计算窗口模型中数据流序列的复合统计特征。以正常数据信息集合P为例，第i个数据包到达时的衰减窗口中数据流序列可表示为

$$\text{IS}_{i,\lambda}=\{w_i,\text{LS}_i,\text{SS}_i,\text{SR}_{i,j},t_i\} \tag{2}$$

其中，w_i表示当前序列权重，LS_i表示序列中所有数据包统计对象数值的和，SS_i表示序列中所有数据包统计对象数值的平方和，$\text{SR}_{i,j}$表示流量序列S_i、S_j残差积的和。

当第$i+1$个数据包到达时，首先根据式(1)计算$\text{IS}_{i,\lambda}$衰减权重$\gamma_{\lambda,i+1}$，并代入式(3)～式(6)中，分别更新每一项值。

$$w_{i+1}=\gamma_{\lambda,i+1}w_i+1 \tag{3}$$

$$\text{LS}_{i+1}=\gamma_{\lambda,i+1}\text{LS}_i+x_{i+1} \tag{4}$$

$$\text{SS}_{i+1}=\gamma_{\lambda,i+1}\text{SS}_i+x_{i+1}^2 \tag{5}$$

$$\text{SR}_{i+1,j}=\gamma_{\lambda,i+1}\text{SR}_{i,j}+r_{i+1}r_{j+1} \tag{6}$$

其中，x_{i+1}为第$i+1$个数据包的统计值，$r_{i+1}=\left(x_{i+1}-\dfrac{\text{LS}_{i+1}}{w_{i+1}}\right)$为序列$S_i$中第$i+1$项数值的残差。则衰减得到的新序列可表示为

$$\text{IS}_{i+1,\lambda}=\{w_{i+1},\text{LS}_{i+1},\text{SS}_{i+1},\text{SR}_{i+1,j},t_{i+1}\} \tag{7}$$

完成数据流序列划分后，可基于式(7)选择并计算复合统计特征。为充分描述每种数据流量的传输特征，针对4种流量得到的数据流序列，以数据包大小、个数及时延抖动作为统计对象，分别计算不同数据序列的复合统计特征，包括权重w_i、平均值σ_i、均方差μ_i。对于源IP与目的IP、源套接字与目的套接字2种流量，考虑到其包含出入站流量，因此选用二维均值$\|s_i,s_j\|$、二维方差$R_{s_is_p}$、协方差$\text{Cov}_{s_is_j}$及相关系数$P_{s_is_j}$等双序列相关型特征，其中

S_i、S_j分别代表出入站流量序列，i、j代表序列中统计时刻到达的数据包项数。综上，本文所选复合统计特征共23个，如表1所示。

表1　　复合统计特征

数据流量	统计对象	复合统计特征
源MAC与IP	数据包大小	μ_i,σ_i
	数据包个数	w_i
源IP	数据包大小	μ_i,σ_i
	数据包个数	w_i
源IP与目的IP	数据包大小	μ_i,σ_i
	数据包个数	w_i
	数据包时延抖动	w_i,μ_i,σ_i
	出入站流量数据包大小相关性	$\|s_i,s_j\|,R_{s_is_j},\mathrm{Cov}_{s_is_j},P_{s_is_j}$
源套接字与目的套接字	数据包大小	μ_i,σ_i
	数据包个数	w_i
	出入站流量数据包大小相关性	$\|s_i,s_j\|,R_{s_is_j},\mathrm{Cov}_{s_is_j},P_{s_is_j}$

基于更新后序列式(7)中的每一项，可以计算出每个数据包到达时对应的一组复合统计特征的值，如表2所示。

表2　　复合统计特征计算方法

统计特征	符号	计算方法
权重	w_i	w_i
平均值	σ_i	$\dfrac{\mathrm{LS}_i}{w_i}$
均方差	μ_i	$\sqrt{\left\|\dfrac{\mathrm{SS}_i}{w_i-\left(\dfrac{\mathrm{LS}_i}{w_i}\right)^2}\right\|}$
二维均值	$\|s_i,s_j\|$	$\sqrt{\mu_i^2+\mu_j^2}$
二维方差	$R_{s_is_j}$	$\sqrt{(\sigma_i^2)^2+(\sigma_j^2)^2}$
协方差	$\mathrm{Cov}_{s_is_j}$	$\dfrac{\mathrm{SR}_{ij}}{w_i+w_j}$
相关系数	$P_{s_is_j}$	$\dfrac{\mathrm{Cov}_{s_is_j}}{\sigma_{S_i}\sigma_{S_j}}$

为全面刻画流量随时间变化的关系，一般选用多个衰减因子，基于每个衰减因子，每个数据包可计算得到23个特征值，设选择多个衰减因子可共产生n个特征，数据流特征矩阵可构建为

$$\boldsymbol{f}=\begin{pmatrix}\boldsymbol{v}_1 & \boldsymbol{v}_2 & \cdots & \boldsymbol{v}_j & \cdots & \boldsymbol{v}_n\end{pmatrix}=\begin{pmatrix}x_{1,1} & x_{1,2} & \cdots & x_{1,n}\\ x_{2,1} & x_{2,2} & \cdots & x_{2,n}\\ \vdots & \vdots & x_{i,j} & \vdots\\ x_{m,1} & x_{m,2} & \cdots & x_{m,n}\end{pmatrix} \tag{8}$$

其中，$\boldsymbol{f}$为$m\times n$的矩阵，m为数据包个数，n为矩阵中特征向量数量；$\boldsymbol{v}_j$为列向量，表示矩阵中第j个数据流特征向量，分别对应不同衰减因子下表1所列出的不同统计特征；$x_{i,j}$表示第j个特征向量中关于第i（$0<i\leqslant n,i\in N^*$）个数据包的特征值。依据上述特征处理方法，同样可得到混合数据信息集合P'混合数据流特征矩阵$\boldsymbol{f}'$。

本节基于衰减窗口模型对数据流进行处理进而构建数据流特征矩阵，相对于界标窗口模型，此方法可以刻画出时间与数据流量的关联关系，以提升异常检测性能；相对于滑动窗口模型，可采用增量更新方式对窗口数据序列进行更新，其内存复杂度为$O(1)$，更适合于轻量级无人机网络异常检测场景。

3.2.2　特征聚类

特征聚类主要指将上述构建的数据流特征矩阵$\boldsymbol{f}$及$\boldsymbol{f}'$中n个数据流特征向量划分为k个特征类，每个特征类中特征向量数量不超过l。其目的是降低单个自编码器的输入特征向量的数量，从而降低模型计算复杂度。以正常数据流特征矩阵$\boldsymbol{f}$为例，设其聚类后的特征类集合为H，初始情况下将$\boldsymbol{f}$中每个数据流特征向量均视为一个特征类，则初始的n个特征类$H=\{H_1,H_2,\cdots,H_n\}$通过聚类降维度，最终结果可表示为

$$H=\{H_1,H_2,\cdots,H_k\} \tag{9}$$

本文基于层次聚类方法实现特征聚类，依据特征类特征向量间的相关性距离合并特征类，通过维护所有特征类特征向量相关性距离矩阵更新各相关性距离。设向量$\boldsymbol{c}_i$与$\boldsymbol{c}_j$分别为特征类H_i和H_j的特征向量，则其特征向量间相关性距离$d_{i,j}$表示为

$$d_{i,j}=1-\frac{(\boldsymbol{c}_i-\bar{c}_i)(\boldsymbol{c}_j-\bar{c}_j)}{\|(\boldsymbol{c}_i-\bar{c}_i)\|_2\|(\boldsymbol{c}_j-\bar{c}_j)\|_2} \tag{10}$$

其中，$\bar{c}_i$及$\bar{c}_j$分别为是向量$\boldsymbol{c}_i$及$\boldsymbol{c}_j$中特征值的平均值。由式(10)可计算出初始状态下特征类集合H中n个特征类特征向量相关距离矩阵$\boldsymbol{D}$为

$$\boldsymbol{D}=\begin{pmatrix}d_{1,1} & d_{1,2} & \cdots & d_{1,n}\\ d_{2,1} & d_{2,2} & \cdots & d_{2,n}\\ \vdots & \vdots & d_{i,j} & \vdots\\ d_{n,1} & d_{n,2} & \cdots & d_{n,n}\end{pmatrix} \tag{11}$$

其中，$\boldsymbol{D}$为$n\times n$的矩阵，$0<i,j\leqslant n$，$i,j\in N^*$。

循环选择$\boldsymbol{D}$中相关性距离最小且特征类中特征数量和不超过l的2个特征类进行聚类，并更新$\boldsymbol{D}$，直到特征类数量等于k完成特征聚类。本文提出的复合特征的层次聚类算法如算法1所示。

算法1　复合特征的层次聚类算法

输入　数据流特征矩阵$\boldsymbol{f}$，数据流特征向量数量n，最终特征类数量k，单个特征类特征向量限制数量l

输出　特征类聚类结果集合H

$H \leftarrow \text{zeros}(n)$ //初始化特征类集合
for $\boldsymbol{v}_t$ in $\boldsymbol{f}$:
　H_t.append($\boldsymbol{v}_t$) //每个数据流特征向量视为一个特征类
　$\boldsymbol{c}_t = \boldsymbol{v}_t$ //特征类特征向量等于其中的数据流特征向量
　H.append(H_t.)
end for
for i = 1 to n:
　for j = 1 to n:
　根据式(10)、式(11)计算以及$\boldsymbol{D} \leftarrow \text{update}(d_{i,j})$ //更新矩阵$\boldsymbol{D}$
　end for
end for
while num(H) > k//特征类数量大于k时循环
　$\min(d_{i,j} \text{ in } \boldsymbol{D})\&\&(\text{size}(H_i)+\text{size}(H_j) \leqslant l)$//选择最小相关距离，且对应特征类中特征向量数量和小于或等于l
　H_i.append(H_j) //合并特征类
　$\boldsymbol{c}_i = \dfrac{\boldsymbol{c}_i + \boldsymbol{c}_j}{2}$//更新特征类特征向量
　for t = 1 to num(H): //依据当前特征类数量更新相关距离矩阵
　　$\boldsymbol{D} \leftarrow \text{update}(d_{i,t},d_{t,i})$//更新合并后新特征类的对应矩阵信息
　　$\boldsymbol{D} \leftarrow \text{delete}(d_{j,t},d_{t,j})$//删除已合并旧特征类的对应矩阵信息
　end for
　delete(H_j) //删除已合并特征类
end while
return H //返回所有聚类，共k个

基于上述层次聚类算法，最终将正常数据流特征矩阵$\boldsymbol{f}$降维为单个特征向量均不超过l的k个特征类，且每个特征类内的特征间都具有强相关性，特征类集合记为H。同理，亦可将混合数据流特征矩阵$\boldsymbol{f}'$划分为k个特征类，每个特征类中特征向量数量不超过l，其聚类结果记为H'。本节所提算法仅通过维护$n \times n$的相关距离矩阵实现降维，其计算及内存复杂度为$O(n^2)$。

3.3　基于内存增强自编码器集成结构的异常检测模块

异常检测模块是本文所提异常检测模型的核心，其主体是一个基于双层内存增强自编码器集成结构的无监督神经网络，主要对完成特征处理的正常特征类集合H进行学习，对混合特征类集合H'进行异常检测。

3.3.1　内存增强自编码器

与正常数据相比，自动编码器对异常输入产生更高重构误差，以此作为识别异常的标准。然而因为数据模式问题，传统自动编码器往往能较好地重建异常，导致异常的漏检测。针对传统自编码器对异常重构过拟合导致漏报率高的问题，本文采用内存增强自编码器[24]作为异常检测模型的组成核心，其结构如图6所示。

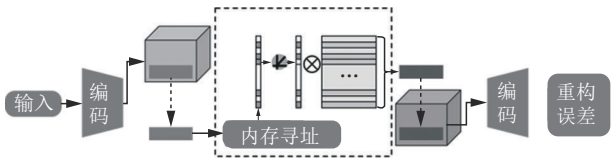


图6　内存增强自编码器结构

内存增强自编码器主要由编码器、解码器和内存模块组成。编码器主要用于对一个训练集或测试集的输入进行编码，该编码后续将作为查询内容来检索内存中的相关项，因此编码器在内存增强编码器中可以看作一个查询生成器。解码器主要负责将检索到的记忆项作为输入来重构样本。内存模块由用于记录原型编码模式的内存和用于访问内存的基于注意力的寻址操作符组成。

基本工作流程如下。给定一个输入，首先通过编码器获得该输入的编码，以此编码为查询依据，内存模块通过基于注意力的寻址操作符检索内存中最相关的项；然后，将其传递到解码器进行重构。在训练过程中，以最小化重构误差为目标对编码器和解码器进行优化，并通过更新内存内容，记录已编码的正常数据模式。在检测过程中，此自编码器不改变模型参数，在对待检测数据完成编码的基础

上，仅使用内存中记录的有限数量的正常模式来重构待检测数据，因此待检测数据中正常样本的重构误差小，异常样本的重构误差大，可有效提升异常检测性能（内存增强自编码器详细原理可见文献[24]）。

内存增强自编码器在设计之初主要用于视频流的异常检测，本文将其作为本文所提异常检测模型核心组成单位，相对于传统自编码器，可有效提升检测性能，并实现无监督学习，解决高度依赖人工标注数据的问题。

3.3.2　双层内存增强自编码器集成结构

如图7所示，双层内存增强自编码器包含集成层$L^{(1)}$与输出层$L^{(2)}$，集成层由k个内存增强自编码器组成，输出层由一个内存增强自编码器组成，每个内存增强自编码器包含一个隐含层。添加输出层自编码器的原因是基于各相关特征训练的集成层自编码器所输出的重构误差仍能反映训练数据在不同特征组间的数据模式信息，因此通过添加输出层自编码器学习集成层中多个自编码器的重构误差可将对模式信息的学习最大化，有效提高检测性能。

设H_i为正常特征类集合H中第i个特征类，H_i'为混合特征类集合H'中第i个特征类。首先在所提的双层内存增强自编码器集成结构中进行模型训练，而后基于训练好的模型进行检测。在进行模型训练时，将H_i输入集成层的第i个内存增强自编码器θ_i并计算其重构误差。将所有集成层重构误差组成误差向量，提交到输出层的内存增强自编码器进行学习，并在输出的最终重构误差向量中选择最大的误差值作为重构误差阈值。

在基于训练后的模型进行异常检测时，将H_i'输入第i个内存增强自编码器θ_i，集成层自编码器向输出层提交每个特征组的数据重构误差，而后将集成层所有重构误差组合，由输出层统一计算给出最终重构误差向量。当此重构误差向量中某误差值大于重构误差阈值时，则其对应的数据包判定为异常。所有数据包完成标记后，返回其中标记为异常的数据包序列号集合S，即完成网络异常检测。本文采用的集成结构异常检测算法伪代码可归纳为算法2。

算法2　集成结构异常检测算法

输入　数据聚类结果H，待检测数据聚类结果H'

输出　异常数据包序号集S

init $\vec{z}[\,],\vec{e}[\,],e_{\max},S$//初始化集成层和输出层重构误差向量$\vec{z}[\,],\vec{e}[\,]$,以及重构误差阈值$e_{\max}$

for (θ_i in $L^{(1)}$):

　$\theta_i \leftarrow H_i$ //训练集成层自编码器，返回重构误差向量

end for

$\vec{z}[i] \leftarrow \text{train}(\theta_i)$

$L^{(2)} \leftarrow \vec{z}$

$\vec{e}[i] \leftarrow \text{train}(L^{(2)})$ //训练输出层自编码器，返回最终重构误差向量

for ($\vec{e}[i][j]$ in $\vec{e}[i]$):

　if $\vec{e}[i][j] > e_{\max}$:

　　$e_{\max} = \vec{e}[i][j]$ //选择最终重构误差向量中最大的值作为重构误差阈值

　end if

end for

init $\vec{z}[\,],\vec{e}[\,]$//初始化输出层输入、输出层输出并开始检测

for (θ_i in $L^{(1)}$):

　$\theta_i \leftarrow H_i'$

　$\vec{z}[i] \leftarrow \text{run}(\theta_i)$ //利用集成层自编码器开始计算重构误差

end for

$L^{(2)} \leftarrow \vec{z}$

$\vec{e}[i] \leftarrow \text{run}(L^{(2)})$ //利用输出层自编码器得出最终重构误差向量

for ($\vec{e}[i][j]$ in $\vec{e}[i]$):

　if $\vec{e}[i][j] > e_{\max}$:

　　S.append(j) //重构误差高于阈值则判断为异常并更新序列

　end if

end for

return S

双层内存增强自编码器集成结构中每个集成层自编码器输入的特征类所包含的最大特征数量不超过l，则最差情况下，集成层单个自编码器（包含一个隐含层）计算复杂度为$O(l^3)$。集成层包含k个内存增强自编码器，输出层包含1个内存增强自编码器，输出层自编码器的输入为集成层的k个自编码器输出的k维向量，则算法2计算复杂度为$O(kl^3 + k^3) = O(k^3)$。

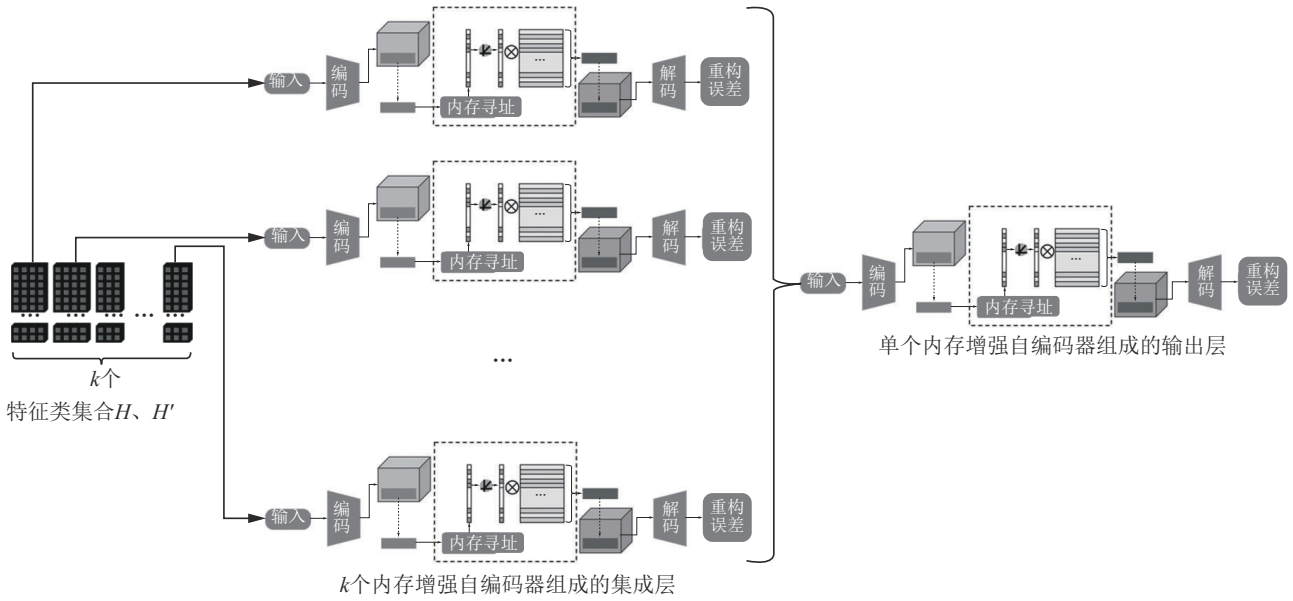


图7　双层内存增强自编码器集成结构

基于上述检测算法可得到包含所有异常数据包序号的序列集合S。双层内存增强自编码器集成结构通过集成若干个小型内存增强自编码器，降低了整体模型计算复杂度，并且缓解了普通自编码器漏报高的问题，提升了检测性能，适用于无人机网络攻击检测。

4　实验对比及性能分析

针对本文所提出的面向无人机网络攻击检测的轻量级在线检测模型，本节主要通过在UNSW-NB15以及NS-3数据集上进行实验对比，以验证所提模型的有效性。

4.1　实验验证数据集

4.1.1　UNSW-NB15公开数据集

本文采用的UNSW-NB15数据集是澳大利亚网络安全中心（ACCS）的实验室基于IXIA完美风暴工具创建的典型数据集[26-27]，其包含了现代网络攻防场景下的攻击，数据结构如表3所示。UNSW-NB15虽非产生自无人机网络，但其作为广受认可的公开数据集包含了当前无人机网络所存在的典型网络攻击。其与无人机网络在网络协议和网络拓扑上的差异使数据包级别特征如协议类型等存在差异，但在本文所关注的网络数据流级别的复合统计特征上却是一致的，因此可用于评估无人机网络入侵检测方法性能。

在本文实验中，将所有的攻击统一标记为异常，选取正常数据中的60%作为训练数据并取最大重构误差作为阈值。剩余正常数据及异常数据统一输入异常检测框架中，计算其重构误差，若误差大于阈值，则将其标记为异常，反之标记为正常。

表3　UNSW-NB15数据集数据结构

标注	数量/个	备注
Normal	2 218 761	正常传输数据
Fuzzers	24 246	模糊攻击
Analysis	2 677	端口扫描、垃圾邮件和html文件渗透等攻击
Backdoors	2 329	后门攻击
DoS	16 353	拒绝服务攻击
Exploits	44 525	漏洞攻击
Generic	215 481	分组密码攻击
Reconnaissance	13 987	模拟收集信息的攻击
Shellcode	1 511	利用软件漏洞有效载荷的代码攻击
Worm	174	蠕虫攻击

4.1.2　NS-3数据集

考虑到UNSW-NB15数据集并非产生自无人机网络且当前没有公开的受广泛认可的无人机网络数据集，因此本文在前述工作基础上，基于NS-3网络模拟器模拟无人机网络，通过采用802.11、自组织按需距离向量路由协议（AODV)、TCP、UDP等无人机网络典型协议，加入无人机网络所存在的多种典型网络攻击，生成了NS-3无人机网络模拟数据集，以验证本文所提模型在无人机仿真网络中的性能。NS-3仿真实验采用无线自组织网络作为

网络拓扑，对每个无人机设置了随机方向的移动，相关仿真实验参数如表 4 所示。

表 4　　仿真实验参数

参数	取值	意义
Topo	ad hoc	无线自组织网络
Normal_num	12	正常节点数量
Attack_num	1	攻击节点数量
interval	100	网络正常 TCP 通信数据包每秒发送数量
Time/min	10	正常通信持续的时间
Scan_ interval	100	端口扫描每秒扫描所产生的总数据包
Flood_ interval	200	SYN 泛洪攻击每秒所产生的总数据包
Dos_ interval	200	拒绝服务供给每秒所产生的总数据包

仿真共持续 10 min，前 7 min 未发生攻击，采用 NS-3 中 ad hoc 默认协议栈进行通信，在最后 3 min 依次执行端口扫描、SYN 泛洪、TCP 重置、会话劫持和 DoS 攻击，每次攻击约持续 0.5 min。而后通过消息队列将网络中所有数据包进行采集、解析及存储，生成可用于异常检测的 NS-3 数据集，其结构如表 5 所示。

表 5　　数据集数据结构

标注	数量/个	备注
Normal	467 921	正常传输数据
Scan	13 982	针对主机特定端口的频繁扫描
Flood	15 639	基于 TCP SYN 的典型泛洪攻击
Reset	1 123	针对特定会话的 TCP 重置攻击
hijack	1 374	针对特定会话的 TCP 会话劫持攻击
DoS	27 913	针对单个端口的拒绝服务攻击

4.2　离线检测性能评估

4.2.1　评价方法

作为典型的异常检测任务，本文选取了真阳性率（TPR, true positive rate）和假阴性率（FNR, false negative rate）作为评价指标，其计算式分别如下

$$\mathrm{TPR}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{12}$$

$$\mathrm{FNR}=\frac{\mathrm{FN}}{\mathrm{FN}+\mathrm{TP}} \tag{13}$$

其中，TP 为真阳性样本的数量，FN 为假阴性样本的数量。

4.2.2　数据集检测效果评估

本文参考文献[20,25]，为平衡包处理速度和检测性能，对特征选择、计算及聚类过程中关键参数进行取值。衰减因子个数为 5，其取值依次为 λ=10,5,1,0.1,0.01，数据流特征子矩阵数量 k=33，单个子矩阵特征数量限制 m=10。在此基础上，本文以文献[20]所提出的 Kitsune 作为基线方法，同时与分别加装了去噪自编码器（DAE, denoising autoencoder）、堆叠自编码器（StackAE, stacked autoencoders）、稀疏自编码器（SAE, sparse autoencoder）的 Kitsune 和本文方法进行对比。

UNSW-NB15 数据集实验结果如表 6 所示。由表 6 可看出，本文方法在真阳性率上高于 Kitsune+SAE 和 Kitsune+StackAE，低于其余方法，而本文方法选择了可有效降低漏报率的内存增强自编码器，因此假阴性率显著优于其他方法，相对于对比方法，假阴性率平均降低了 35.9%。综上，在公开数据集上的实验结果证明了本文方法的对于攻击检测的有效性。

表 6　　UNSW-NB15 数据集实验结果

标注	真阳性率	假阴性率
Kitsune	0.853	0.025
Kitsune +DAE	0.852	0.017
Kitsune+StackAE	0.867	0.014
Kitsune +SAE	0.868	0.023
本文方法	0.858	0.012

NS-3 数据集实验结果如表 7 所示。由表 7 可以看出，本文方法在 NS-3 数据集上的表现与在 UNSW-NB15 数据集上的表现大致类似，在真阳性率上高于除去 Kitsune+SAE 以外的其余方法，而在假阴性率上，显著优于其他方法，相对于对比方法，假阴性率平均降低了 48%。同时，通过对比表 6 和表 7 可知，所有方法在 NS-3 数据集上的结果要显著优于在 UNSW-NB15 数据集上的结果。主要由于 NS-3 数据集中各种攻击与正常数据的模式信息更为固定，且差异更大。因此，此实验结果也证明了本文方法在模拟无人机网络的仿真数据集上进行攻击检测更加有效。

4.3　在线检测性能评估

为了评估本文所提方法的在线检测效果，在前述分析各方法在公开数据集上性能时，通过内嵌计时和数据包计数模块，计算出了各方法在树莓派 4B 和 i5-10200H CPU 配置下的平均包处理速度。在 NS-3 仿真实验中，通过实时将 NS-3 网络中的数据包推送至消息队列，再从消息队列中实时取出数据包进行检测，模拟了真实环境下无人机

网络的在线异常检测。考虑到NS-3网络模拟器采用多种网络协议导致NS-3网速并不能完全掌控的因素，本文在控制通信节点TCP通信数据包发送速度的基础上，确定了实验时间段内的平均网速，通过判断在消息队列内部滞存的网络数据包数量，评估在线检测的效果，在线检测性能对比如图8所示。

表7　　NS-3数据集实验结果

标注	真阳性率	假阴性率
Kitsune	0.942	0.013
Kitsune+DAE	0.936	0.007
Kitsune+StackAE	0.949	0.005
Kitsune+SAE	0.962	0.010
本文方法	0.956	0.004

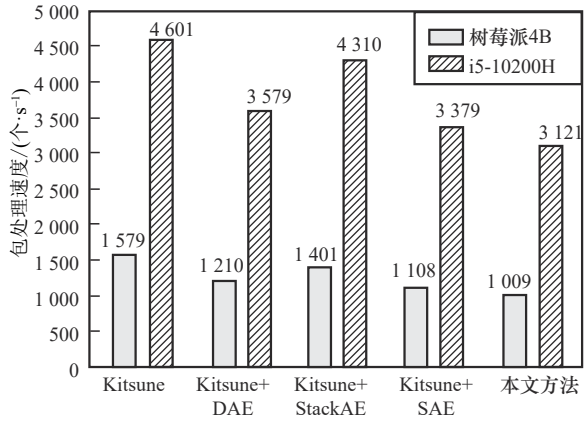


图8　在线检测性能对比

从图8可知，本文方法相对于其他方法包处理速度有所降低，但结合对应包处理速度的NS-3平均网速，本文方法已初步实现了在树莓派4B配置下平均230 KB/s的在线检测。当网速高于此速度时，可通过提升硬件性能如增加CPU数量来提升包处理速度，但当硬件固定时，若不采用消息队列等传输中间件技术而直接将数据包输入后续模块，随着网速的增大，系统将出现卡顿甚至发生崩溃。为验证消息队列对模型稳定性的影响，分别测试不使用消息队列与使用基于操作系统的消息队列的检测模型基于前述树莓派4B在不同网速下的数据包处理情况，检测模型稳定性对比如图9所示。

由图9可知，在仿真网速达到在线检测网速临界值（图9中约为260 KB/s，随不同NS-3仿真实验而有所波动）前，2种检测模型均能较好地完成检测任务。但当网络超过此值后，不使用消息队列的检测模型后续模块开始出现卡顿现象，反映到图中为随着网速增大，单位时间内处理数据包的数量不断下降，而使用消息队列的检测模型因将无法处理的数据包暂存于消息队列中，待空闲时进行处理，其后续模块处理速度基本不受影响，更具稳定性。

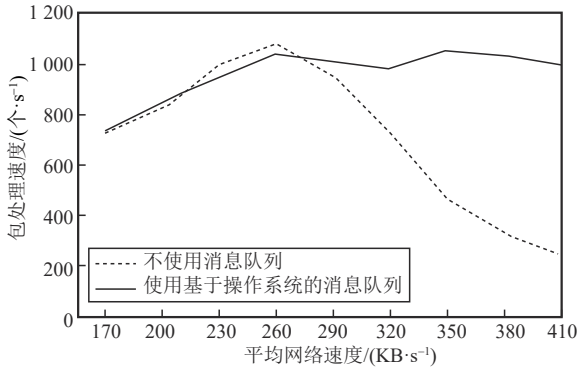


图9　检测模型稳定性对比

4.4　轻量级分析

相比传统基于机器学习的无人机网络攻击检测架构，本节从模型设计、软件依赖程度及硬件依赖程度三方面对本文所提模型的轻量级进行分析。

在模型设计方面，本文基于衰减窗口模型，以增量更新方式计算数据流序列对应的复合统计特征，内存复杂度仅为$O(1)$，相较于滑动窗口模型的$O(n)$，有效降低了处理过程中的内存复杂度。本文基于层次聚类算法将复合统计特征划分为多个特征类，并输入包含多个小型内存增强自编码器的集成结构中，其模型总体计算复杂度仅为$O(k^3)$，远小于传统检测方案计算复杂度。

在软件依赖程度方面，本文所提模型在单点无人机数据采集方面与传统方案相似，仅依靠传统网络嗅探器及其API。但在主体数据传输及学习模型方面对复杂软件依赖更小。一方面，本文所提模型部署于单点，数据传输中所使用的基于操作系统的消息队列仅用于模块间解耦，可直接调用操作系统底层接口实现，不需要额外部署数据库等中间件；另一方面，本文采用的智能算法仅依赖numpy、sys、scipy、pandas等Python库，不需要安装额外的复杂机器学习框架，部署简单。

在硬件依赖程度方面，传统基于机器学习的检测方案往往需要高性能CPU甚至GPU的支撑。主流无人机厂商如大疆的工业级无人机往往配置酷睿i5、i7等系列CPU，极少数配置AI芯片或GPU，

Syma 公司的 X30 无人机配置的骁龙 765 处理器中最低单核主频仅为 1.8 GHz。本文在 CPU 主频为 1.5 GHz、内存为 2 GB 的树莓派 4B 上进行了大量实验，实现了网速不超过 230 KB/s 的在线检测，且内存占用不超过 20 MB，对硬件要求远小于传统的智能检测方案。

5　结束语

本文提出了一种面向无人机网络的基于内存增强自编码器集成架构的异常检测模型，旨在实现可部署于无人机的轻量级在线异常检测。采用基于操作系统的消息队列，实现了流量突发场景下低软件依赖的高稳定性异常检测。基于衰减窗口模型以增量更新方式计算复合统计特征，降低了内存复杂度。利用层次聚类算法分离复合统计特征，并将其输入自编码器集成结构中的多个小型自编码器，降低了模型总体的计算复杂度。采用内存增强自编码器作为集成架构的核心，克服了传统自编码器重构效果过拟合导致的漏报率高的问题，显著提升了检测性能。最后，公开数据集与 NS-3 数据集上进行的实验表明，相对于基线方法，在略微提高真阳性率的基础上，本文方法假阴性率分别平均降低了 35.9% 和 48%；在线仿真实验也同样证明了本文方法可实现轻量级的在线异常检测。前述工作由于研究时间和实验环境限制，仅通过公开数据集及 NS-3 仿真验证，仿真结果应略优于实际结果，未来将搭建无人机网络硬件实验平台，在实际场景下验证所提模型检测性能并评估仿真误差和能耗情况。

参考文献：

[1] ALSHAMRANI A, MYNENI S, CHOWDHARY A, et al. A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1851-1877.

[2] TUAN T A, LONG H V, SON L H, et al. Performance evaluation of botnet DDoS attack detection using machine learning[J]. Evolutionary Intelligence, 2020, 13(2): 283-294.

[3] LIMA F F S D, SILVEIRA F A F, MEDEIROS B A D, et al. Smart detection: an online approach for DoS/DDoS attack detection using machine learning[J]. Security and Communication Networks, 2019, 2019: 1574749.

[4] SOE Y N, FENG Y K, SANTOSA P I, et al. Machine learning-based IoT-botnet attack detection with sequential architecture[J]. Sensors, 2020, 20(16): 4372.

[5] ZHAI S F, CHENG Y, LU W N, et al. Deep structured energy based models for anomaly detection[C]//Proceedings of International Conference on Machine Learning. New York: ACM Press, 2016: 1100-1109,.

[6] BIN Z, LI F F, XING E P. Online detection of unusual events in videos via dynamic sparse coding[C]//Proceedings of the CVPR. Piscataway: IEEE Press, 2011: 3313-3320.

[7] ZHAO Y R, DENG B, SHEN C, et al. Spatio-temporal autoencoder for video anomaly detection[C]//Proceedings of ACM on Multimedia Conference. New York: ACM Press, 2017: 1933-1941.,.

[8] ZHOU C, PAFFENROTH R. Anomaly detection with robust deep autoencoders[C]//Proceedings of ACM SIGKDD. New York: ACM Press, 2017: 665-674.

[9] AHMAD Z, SHAHID K A, WAI S C, et al. Network intrusion detection system: a systematic study of machine learning and deep learning approaches[J]. Transactions on Emerging Telecommunications Technologies, 2021, 32(1): e4150.

[10] THAKKAR A, LOHIYA R. A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions[J]. Artificial Intelligence Review, 2022, 55(1): 453-563.

[11] 冯智伟. 面向多旋翼无人机GPS劫持攻击检测和拒绝服务攻击抵御技术的研究[D]. 沈阳: 东北大学, 2020.
FENG Z W. Research on GPS hijacking attack detection and denial of service attack defense technology for multi-rotor UAV [D]. Shenyang: Northeastern University, 2020.

[12] 段雪源, 付钰, 王坤, 等. 基于多尺度特征的网络流量异常检测方法[J]. 通信学报, 2022, 43(10): 65-76.
DUAN X Y, FU Y, WANG K, et al. Network traffic anomaly detection method based on multi-scale characteristic[J]. Journal on Communications, 2022, 43(10): 65-76.

[13] 张凤登, 谢力, 应启戛. 噪声环境中采用探询机制的局域网性能分析[J]. 通信学报, 2002, 23(6): 6-13.
ZHANG F D, XIE L, YING Q J. Performance analysis of LANs using polling mechanism in a noisy environment[J]. Journal on Communications, 2002, 23(6): 6-13.

[14] 侯重远, 江汉红, 芮万智, 等. 工业网络流量异常检测的概率主成分分析法[J]. 西安交通大学学报, 2012, 46(2): 70-75.
HOU C Y, JIANG H H, RUI W Z, et al. A probabilistic principal component analysis approach for detecting traffic anomaly in industrial networks[J]. Journal of Xi'an Jiaotong University, 2012, 46(2): 70-75.

[15] WANG K, STOLFO S. Anomalous payload-based network intrusion detection[C]//Proceedings of International Symposium on Recent Advances in Intrusion Detection. Berlin: Springer, 2004: 203-222.

[16] XIE M, HU J, HAN S, et al. Scalable hypergrid k-NN-based online anomaly detection in wireless sensor networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 24(8): 1661-1670.

[17] ZHOU X Z, XIE L, ZHANG P, et al. An ensemble of deep neural networks for object tracking[C]//Proceedings of the 2014 IEEE Interna-

tional Conference on Image Processing. Piscataway: IEEE Press, 2014: 843-847.

[18] YOUSEFI-AZAR M, VARADHARAJAN V, HAMEY L, et al. Autoencoder-based feature learning for cyber security applications[C]// Proceedings of the 2017 International Joint Conference on Neural Networks. Piscataway: IEEE Press, 2017: 3854-3861.

[19] JAVAID A, NIYAZ Q, SUN W Q, et al. A deep learning approach for network intrusion detection system[C]//Proceedings of the Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies. New York: ACM Press, 2016: 21-26.

[20] MIRSKY Y, DOITSHMAN T, ELOVICI Y, et al. Kitsune: an ensemble of autoencoders for online network intrusion detection[J]. arXiv Preprint, arXiv: 1802.09089, 2018.

[21] 平国楼, 曾婷玉, 叶晓俊. 基于评分迭代的无监督网络流量异常检测[J]. 清华大学学报(自然科学版), 2022, 62(5): 819-824.
PING G L, ZENG T Y, YE X J. Unsupervised network traffic anomaly detection based on score iterations[J]. Journal of Tsinghua University (Science and Technology), 2022, 62(5): 819-824.

[22] 董书琴, 张斌. 基于深度特征学习的网络流量异常检测方法[J]. 电子与信息学报, 2020, 42(3): 695-703.
DONG S, ZHANG B. Network traffic anomaly detection method based on deep features learning[J]. Journal of Electronics & Information Technology, 2020, 42(3): 695-703.

[23] 杨岳毅, 王立德, 陈煌, 等. 基于变分自编码器的MVB网络异常检测方法[J]. 铁道学报, 2022, 44(1): 71-78.
YANG Y, WANG L, CHENG H, et al. Anomaly detection method for MVB network based on variational autoencoder[J]. Journal of the China Railway Society, 2022, 44(1): 71-78.

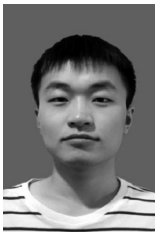
[24] GONG D, LIU L Q, LE V, et al. Memorizing normality to detect anomaly: memory-augmented deep autoencoder for unsupervised anomaly detection[C]//Proceedings of the 2019 IEEE/CVF International Conference on Computer Vision. Piscataway: IEEE Press, 2019: 1705-1714.

[25] AGGARWAL C C, PHILIP S Y. A framework for clustering uncertain data streams[C]//Proceedings of IEEE 24th International Conference on Data Engineering. Piscataway: IEEE Press, 2008: 150-159.

[26] WELLER-FAHY D J, BORGHETTI B J, SODEMANN A A. A survey of distance and similarity measures used within network intrusion anomaly detection[J]. IEEE Communications Surveys & Tutorials, 2015, 17(1): 70-91.

[27] LEE C H, SU Y Y, LIN Y C, et al. Machine learning based network intrusion detection[C]//Proceedings of the 2017 2nd IEEE International Conference on Computational Intelligence and Applications. Piscataway: IEEE Press, 2017: 79-83.

[作者简介]

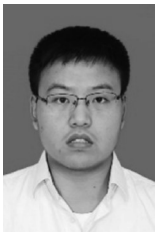


胡天柱（1996– ），男，河南濮阳人，西安电子科技大学与军事科学院联合培养博士生，主要研究方向为智能信息网络内生安全、APT攻击检测等。

沈玉龙（1978– ），男，江苏泗洪人，博士，西安电子科技大学教授、博士生导师，主要研究方向为云计算与数据安全、智能网络内生安全等。

任保全（1974– ），男，陕西周至人，博士，军事科学院研究员、博士生导师，主要研究方向为智能信息网络架构与内生安全等。

何吉（1989– ），男，重庆人，博士，西安电子科技大学讲师、硕士生导师，主要研究方向为物理层安全、智能信息网络内生安全等。



刘成梁（1996– ），男，江苏镇江人，西安电子科技大学与军事科学院联合培养博士生，主要研究方向为智能信息网络安全、APT攻击检测等。

李洪钧（1985– ），男，博士，军事科学院高级工程师，主要研究方向为通信网络技术、物联网技术等。