DOI:10.19652/j.cnki.femt.2305760

基于深度学习的无人机自组网分层入侵检测方法

杜玉航 王 伟
(西安工程大学 西安 710048)

摘 要:针对无人机自组网携带重要信息却容易受到各种攻击的问题,提出了一种分层检测响应的方案。首先采用端节点误用检测方法,监测无人机行为并报告规则验证的结果。接着,地面站利用深度神经网络分类算法进一步优化验证结果。为抵御如干扰、黑洞、灰洞等不同类型网络攻击提供了新的解决方案。最后,与BRUIDS方案和分布式检测方案进行模拟分析和实验对比。结果表明,相较于另外两种方案,方法在检测率方面的下降率均保持在10%以内,检测率高达93%以上。误报率提升了1.2%,在检测攻击延迟方面与分布式方案相差无几,通信开销减少了约53.5 KBps,且对未知攻击检测问题有显著改善。

关键词:深度学习;分层检测;入侵检测;无人机自组网
中图分类号:TP393 **文献标识码**:A **国家标准学科分类代码**:520.3040

Layered intrusion detection method for unmanned aerial vehicle Ad Hoc networks based on deep learning

Du Yuhang Wang Wei
(Xi'an Polytechnic University, Xi'an 710048, China)

Abstract: This paper proposes a layered detection response scheme to address the problem of unmanned aerial vehicle (UAV) self-organizing networks carrying important information but being susceptible to various attacks. Firstly, the end node misuse detection method is adopted to monitor the behavior of drones and report the results of rule validation. Subsequently, the ground station utilized deep neural network classification algorithms to further optimize the validation results. Provided new solutions to resist different types of network attacks such as interference, black holes, and gray holes. Finally, this article conducts simulation analysis and experimental comparison with the BRUIDS scheme and distributed detection scheme. The results show that compared to the other two schemes, the decrease rate of detection rate in our method remains within 10%, with a detection rate of over 93%. The false alarm rate has increased by 1.2%, which is almost the same as the distributed scheme in detecting attack latency. The communication overhead has been reduced by about 53.5 KBps, and there is a significant improvement in the detection of unknown attacks.

Keywords: deep learning; layered detection; intrusion detection; unmanned aerial vehicle

0 引 言

随着无人机的普及和相关技术领域的进步,网络移动通信、防范恶意节点行为、未授权访问以及信息安全变得至关重要。移动自组织网络(MANETs)由于节点的高速移动性和快速拓扑变化而更适合基础设施较少的移动网络。然而,这种灵活性也带来了新的安全风险,密码学和入侵检测系统(intrusion detection system,IDS)是两种主要的安全机制。

一方面,密码学用于确保消息的保密性和节点的认证[1-3],以防止外部入侵者渗透网络。另一方面,IDS使用特殊代理来分析被监视节点的异常行为[4],有效地保护网络免受内部和外部入侵者的攻击。虽然关于有线网络的研究已提出了许多入侵检测方法,但由于其特定特征不能直接应用于无人机自组网中,因此需要为MANETs设计特定的IDS。目前已提出了各种方法来解决大型数据集中的异常检测[5]。此外,IDS主要依赖于两种检测技术。

1)异常检测,它构建正常配置文件的模型,并尝试跟

收稿日期:2023-11-15

踪可能受到异常或可能的入侵的正常行为的偏差[6-7]。尽管该技术可以检测到系统先前未观察到的新攻击，但其资源开销较大。异常检测通常使用学习算法，如神经网络和支持向量机（support vector machines，SVM）来检测被监控节点的异常行为。

2）基于规则的入侵检测，将被监控节点的行为与一组与特定已知攻击行为相关的规则进行比较[8]。这些规则由一组攻击签名定义。在这种情况下，需要不断更新攻击特征。在时延容忍网络（delay tolerant networks，DTN）中部署 IDS 具有较大难度，因为一组 IDS 节点难以监测分布在范围较大而较少无人机节点的情况。

因此，更为合适的是结合两种技术并进行优化的解决方案，其中整个网络中所有节点通过混杂监听方式激活其 IDS 代理，以监测其邻居的行为[9]。在稀疏网络中，仅基于很少节点（一个或两个）来确定其他节点的恶意行为较为困难，并该决策应由集中式可信节点[10]基于节点的历史行为来做出。因此，分层入侵检测和响应[11]是较为合适的解决方案，其中不同的检测和响应技术运行在无人机层与地面站层。应用于无人机（unmanned aerial vehicle，UAV）网络的现有安全机制[12]基于密码学确保消息隐私和节点认证。

针对入侵检测方向存在的问题，许多学者开始尝试深度学习方法。Feng 等[13]采用了卷积神经网络[14]和长短期记忆网络，用于检测 MANETs 中的拒绝服务和隐私攻击。Meddeb 等[15-16]提出了一种基于异常的技术，以监控 MANETs 的流量模式，并概述了一种数据收集方法，用于构建包括正常行为和拒绝服务等攻击场景的行为数据库，然而，此类方法可能仅限于它们所训练的特定攻击类型，无法良好地适应检测新的或未知的攻击。泛化能力受到训练数据的质量和数量、特征的选择以及训练模型的影响。文献[17]设计的框架是唯一一个公开可用的依赖检测技术进行入侵检测防护，其中，一个无人机的正常行为被建模为一组规则，IDS 代理包含所有规则并与邻居节点交互以检测恶意异常节点。然而，这种方案引起了较高的通信开销，并且根据模拟结果，该系统存在高误报的问题。

相较之下，本文提出的入侵检测技术直接应用于 MANETs，而不考虑无人机网络的要求，如节点的移动性和资源的有限性。

因此，本文提出了一种新的入侵检测和响应方案，旨在检测针对无人机网络的最致命的网络攻击，包括干扰[18]、灰洞和黑洞攻击以及拒绝服务等。该方案在攻击检测方面表现迅速，通信开销轻量级且可扩展，同时实现了高准确性的检测率。

如图 1 所示，根据在无人机中检测到的网络攻击结果输出到地面站，地面站利用深度神经网络（deep neural networks，DNN）提取流量并将其分类为正常、异常或恶意。为了实现高精度，分层方案结合了误用检测技术和异常检测技术。基于这些检测技术，设计了一个新的响应方案。DNN 分类器根据被检测的无人机的行为结果标记为正常，异常和恶意。使得在原检测的基础上又添加了一层未知网络攻击特征分类检测。

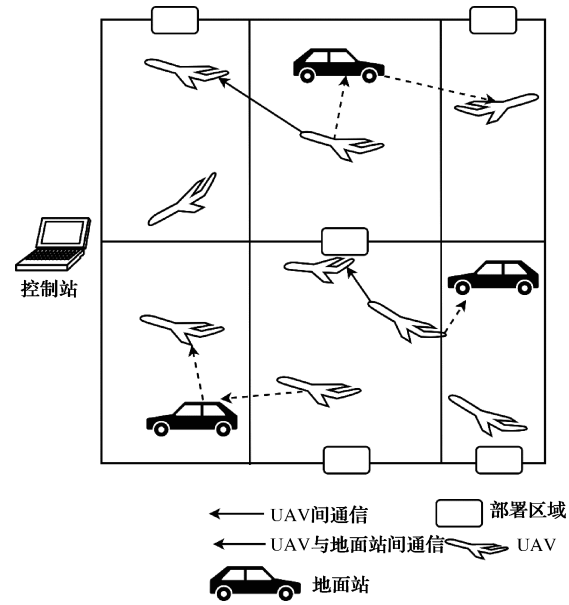


图 1　无人机与地面站的部署

Fig. 1　Deployment of drones and ground stations

实验结果表明，检测准确率明显提升，同时改善了入侵检测误报率及漏报率高的问题，提高了 IDS 的鲁棒性和可靠性。

1　本文方法

1.1　入侵检测机制

针对移动自组网的入侵检测系统[19]在提高检测精度和降低误报率方面仍然面临挑战。在该方法中，每个无人机节点通过使用混杂监听模式激活 IDS 代理，即 UDA 可以监听其通信范围内的所有数据包，并观察其邻居 UAV 的行为。每个 UAV 可以作为 UDA 监视其邻居节点进行相互监测，此外，一旦 UDA 被地面站检测并分类为异常或恶意节点，则将无法继续监测邻居节点，形成 UDA 信任团体。最终，对被监测的 UAV 节点是否为可疑或恶意节点由 UDA 节点决定，地面站减少误报并进行深度分析分类来评估检测结果。

本文 UDA 节点使用基于规则的入侵检测方法，以便快速检测 UAV 攻击行为，针对 UDA 节点和 UDA 输出的检测结果时，DNN 分类器作为将其作为输入特征进行评估分类。该入侵检测方案通过 UDA 节点监测 UAV 节点，同时地面站监测 UDA 节点，以防范攻击、识别异常或恶意行为，从而实现对无人机网络攻击的高检测率和低误报率。

1）干扰攻击检测规则

干扰攻击旨在通过欺骗性和随机干扰通信，随后进行 GPS 欺骗以改变 GPS 坐标。根据这些攻击的特征，定义如下。

(1)大量包的发送(NPS)不同于它的邻居节点,当节点进行干扰攻击时,它会发送大量的数据包,并且发送包的数量显著不同于其邻居节点。

(2)干扰器激活时抖动非常大,当干扰器被激活时,网络中的抖动非常显著。基于这些特征,定义了基于规则的检测方法,用于检测此类攻击。具体而言,UDA 在其收集范围内接收来自节点包(例如无人机和攻击者)的数据包,然后利用正态分布的概念对 NPS 和 JITTER 的分布进行评估,如果 NPS 和 JITTER 位于平均值加减 3 倍标准差($\pm 3\sigma$)内,则被认为是正确分布的。这种方法有助于识别异常的包发送数量和抖动程度,从而检测干扰攻击。

$$\begin{cases} Mean(NPS) = \sum_{j=1}^{k} \dfrac{NPS_j}{k} \\ \sigma(NPS_j) = \sqrt{\dfrac{1}{k}\sum_{j=1}^{k}(NPS_j - Mean(NPS))^2} \end{cases} \tag{1}$$

$$\begin{cases} Mean(JITTER) = \sum_{j=1}^{s} \dfrac{JITTER_j}{s} \\ \sigma(JITTER_j) = \\ \quad \sqrt{\dfrac{1}{s}\sum_{j=1}^{s}(JITTER_j - Mean(JITTER))^2} \end{cases} \tag{2}$$

式中:k 是由 UDA 监测到的可疑节点的邻居的数量;s 是由可疑节点发送的消息数量。

在这种情况下,代理检查 NPS 和抖动是否遵循正态分布,即平均值±抖动范围内。如果被监视节点的 NPS 和抖动不在该范围内,则判断该节点正在执行干扰攻击。为了提高检测准确性,设置了一个固定阈值 TH_{NPS}。当被监测节点的 NPS$>TH_{NPS}$ 时,该节点被判断正在进行干扰攻击。

该阈值通过支持向量机(support vector machine,SVM)算法随时间更新。当 UDA 检测到干扰攻击时,它存储包并将入侵数据转发到地面站。入侵数据包括可疑节点的身份、检测到的干扰的类型(欺骗性或随机干扰)以及攻击者的 NPS 和 JITTER。用于检测干扰攻击的规则如算法 1 所示。这种方法允许动态调整阈值,并通过传递入侵数据来及时更新,以提高系统的适应性和效率。

算法 1　干扰攻击检测算法

规则:UDA 检测来自邻居无人机节点的 NPS 和 JITTER 的分布

输出:入侵报告(恶意 UAV 节点的身份、NPS、JITTER 和干扰信息)

```
if (NPS_i ∈ [(mean_nps − 3σ_nps), (mean_nps + 3σ_nps)] && JITTER_i ∈ [(mean_jitter − 3σ_nps), (mean_jitter + 3σ_nps)])
//判断发射节点进行干扰攻击
    if (NPS_i > TH_NPS)
        //发射节点是干扰机
        //transmit_intrusion_report(identity_malicious_UAV,NPS_attacker,JITTER_attacker,info)
        //转发入侵报告
        update TH_NPS_based_on_SVM()
        //基于 SVM 更新 TH_NPS
    end if
end if
```

2)灰洞和黑洞攻击的检测规则

在攻击发生时,节点可能会丢弃所有或一定数量的接收到的数据包。由于无人机的移动性和频繁断开连接,UDA 节点在网络中监测此类攻击变得困难。假设地面站是可信的静态节点,从而允许它们检测网络内的数据包。

在地面站附近的每个 UAV 向地面站发送相邻分组。此分组包含节点类型(源节点或中继节点)、下一跳节点(即 UAV 向其转发分组的相邻节点)以及上一跳节点(即 UAV 节点从其接收分组的相邻节点)。为了最小化误报,地面站收集来自正常相邻节点的数据包,并忽略从异常和恶意 UAV 节点接收的数据包。接着,地面站检查中继节点是否转发分组,并计算丢弃的分组数(NPD)。NPD 也可能由碰撞和由于障碍物引起的信号衰减引起。但这类数据包丢弃事件相较于黑洞和灰洞攻击引起的事件更加少。为了区分它们,分别设置了新的阈值 TH_{BH} 和 TH_{GH}。这些阈值将通过使用 SVM 算法进行更新,灰洞和黑洞攻击的检测规则如算法 2 所示。

算法 2　灰洞和黑洞攻击检测算法

规则:UDA 监测无人机节点的 NPD

输出:入侵报告(恶意 UAV 节点的身份、NPD 等信息)

```
listen_to_UAV_NPD()
//监听节点的 NPD
if NPD_i > TH_GH
    //节点进灰洞攻击
else if NPD_i > TH_BH
    //节点进行黑洞攻击
update_thresholds_using_SVM()
//基于 SVM 更新 TH_GH、TH_BH
end if
```

这种策略允许地面站通过收集和分析数据包来检测网络中的攻击,尤其是涉及数据包丢弃的情况。动态调整的阈值以及使用 SVM 算法进行更新提高了系统对这类攻击的适应性和检测准确性。

1.2 入侵响应机制

响应机制应用于地面站，利用深度神经网络在恶意节点分类和检测方面达到更高的准确率，该方法由如下4个模块组成。

数据收集和训练模块，入侵检测节点被设置为混杂模式，用于收集网络流量数据[20]和路由数据包。这些特征用于检测任何可疑行为并发现对网络中的潜在攻击。

攻击签名生成模块，通过对收集的数据进行分析，定义了一组代表正常和异常行为的攻击签名。数据集定期更新以保持签名数据库的最新状态，指定模糊相关特征模块来降低数据收集的维数，减少特征之间的相关性，提高检测网络攻击的准确性和有效性。

相关特征降维模块，使用降维技术获得相关特征，选择半监督学习方法处理标记和未标记的数据，以更好地表示数据的底层结构。通过自训练过程，使用分类器将标签分配给未标记的数据，并重新训练分类器，重复迭代过程，直到满足停止条件。首先使用标记数据（30%标记数据）训练分类器。然后，应用未标记的数据进行逐步学习。此阶段给每个未标记的数据分配一个标签，随后参与学习。

深度学习入侵检测模块，使用深度学习方法对数据集进行评估。利用DNN学习数据包中的特定特征，生成一个向量对应于进入攻击特征库的每个数据包。利用注意层对与每个攻击签名相关的数据包向量组成的序列数据进行表示学习。注意层可以对特征进行筛选，得到网络流量向量，有助于实现更准确的网络流量分类。DNN模型由输入层、多个隐藏层和输出层3部分组成。在输入层，DNN模型将表示数据流量行的每个实例转换为单热数据格式。每一行数据流量被编码为一个20维向量。在将数据流量转换成数值形式后，进行归一化操作，同时将数值数据转换成流量图像。随后提取每个数据包的流量上的特征，用于分析数据包向量的重要程度，获得对恶意流量检测更为突出的细粒度特征。在输出层，再将注意机制生成的特征导入到全连接层进行特征融合，得到准确表征网络流量行为的关键特征。最后，将融合的特征发送到分类器，得到最终的识别结果。

对于DNN模型的超参数进行了多次迭代训练，选择准确率最高的超参数作为模型参数。实验表明，使用5个隐藏层的DNN模型能有效构建入侵检测的预测模型。

这一套方法结合了数据收集、特征生成、降维技术和深度学习入侵检测，旨在提高对恶意节点的准确分类和检测能力。

1.3 深度神经网络

使用深度学习方法[21]进行入侵检测响应。相较于传统机器学习方法[22]，深度学习具有几个优势，因为可以自动从数据中学习特征，从而消除了手动特征工程的需要，并能够处理具有高维数的大型复杂数据集，使其更具灵活性和适应性。将最优特征作为输入输入给深度神经网络。提出的入侵检测模型包括隐藏层和输出层。所有的信息在每一层之间以正向的方式传递。对于给定的输入$\{X_1, X_2, \cdots, X_{m_n}\}$在隐藏层中执行的计算给出为：

$$h_i(x) = f(w_i^t x + b_i) \tag{3}$$

隐藏元素$h_i(x)$取决于输入向量的大小，f是激活函数。所提出的网络模型的最后一层使用$SoftMax$作为激活函数，表示为：

$$SoftMax(x_i) = \frac{e^{v^i}}{\sum_{j=1}^{j} e^{x_j}} \tag{4}$$

对于初始层，采用ReLU作为激活函数，消除了消失状态和误差。与其他激活函数相比，ReLU速度更快，能够训练大量隐藏层，数学上表示为$f(x)=\max(0,x)$损失函数用于定义实际结果与预测结果之间的差异，得到：

$$l(a,p) = \| a - p \|^2 \tag{5}$$

其中，a为实际值；p为预测值。对于多类分类，利用实际值的概率，得到：

$$l(a, P(ap)) = -\log P(ap) \tag{6}$$

网络获得最优特征列表作为输入并产生输出，减少平均损失也是必要的，通过式(7)实现。

$$l(x_n, y_n) = \frac{1}{n}\sum_{i=1}^{n} l(y_n, f_\vartheta(x_n)) \tag{7}$$

式中：X_n是输入集和输出集，基于隐函数最小化损失函数。

$$l_{x_y}(\vartheta) = \frac{1}{n}\sum_{i=1}^{n} l(y_n, f_\vartheta(x_n)) \tag{8}$$

而$\vartheta = (w_1, b_1, w_2, b_2, \cdots, w_n, b_n)$。为了不断更新参数，在提出的方法中使用了梯度下降优化器。连续更新的条件为：

$$\vartheta^{new} = \vartheta_{old} - \varphi \nabla_\vartheta l(\vartheta) \tag{9}$$

其中，φ表示学习率。对每一层都执行了归一化过程，并且所有的连接都是完全连接的前馈神经网络。这个过程从初始化节点和网络参数开始。数据从网络中的所有节点获取，并在处理前进行归一化处理。为了选择最优特征，需要考虑每个数据点之间的相关性选择最优特征。选择的特征作为输入提供给深度神经网络层。使用ReLU激活函数消除初始层中的消失状态和误差。在输出层使用SoftMax激活函数对输入特征进行分类。对超参数设置如表1所示。

表1 DNN中的超参数

Table 1 Hyperparameters in DNN

超参数	取值
学习率(LR)	0.01～0.5
epoch数	150
隐藏节点(HN)	15～100
批量大小	1 000
分类函数	ReLU
激活函数	SoftMax

2 模拟和结果

实验的硬件环境采用一台高性能计算机，配备了多核心处理器用于并行计算和模型训练。实验的软件环境用于搭建、训练和评估深度神经网络模型，选择主流学习框架如 TensorFlow、PyTorch 或 Keras，用于搭建和训练 DNN 模型；使用 Python 编程语言进行实验，并根据选择的深度学习框架使用相应的库和工具来监视模型训练过程；实验使用 NS3 模拟器评估分层检测和响应方案的性能，并将其与 BRUIDS 方案、分布式方案[23]进行比较，其中基于规则的检测、UAV 节点评估分类在无人机层完成。此外，将 3 种方案进行了性能比较。本文综合对比了检测率、误报率、效率和通信开销，定义如下。

1）检测率是正确识别的攻击者与攻击者总数的比率。

2）误报率是指被错误分类为攻击者的正常无人机节点数量与正常无人机节点总数之比。

3）效率是 UDA 检测异常或恶意无人机节点所需的时间，计算如下：

$$Effciency = \sum_{i=1}^{N} \frac{DT_i - MT_i}{Sampling\ frequency \cdot N} \tag{10}$$

式中：MT_i 是攻击开始的时刻；DT_i 是网络攻击的检测时间；N 是网络攻击的数量。

4）通信开销是由入侵检测所产生的字节量，以实现高检测率和低误报率。

2.1 移动模型和仿真设置

为了模拟真实的 UAV 网络，使用了确定性移动模型。本文使用 PPRZM（paparazzi mobility）模型[24]，其中无人机遵循明确定义的轨迹。无人机探索的地图被映射到具有均匀正方形的网格上，每个 UAV 探索被监控区域并收集关键信息，然后将其传输到合适的下一跳节点，即 UAV 或地面站，传输过程采用贪婪转发机制，选择最远的下一跳来中继数据。与每个攻击的检测相关的阈值通过 SVM[25]进行学习，并随时间更新。

由于如下原因则进行强制更新：攻击者可能知道阈值并设置相应适当的阈值，使得基于规则的检测无效。在模拟开始时（即 $t=0$），每个阈值已经被设置为有初始值。主要模拟参数如表 2 所示。

表 2 模拟参数

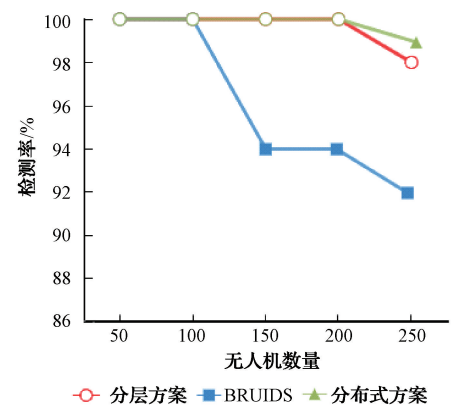
Table 2 Simulation parameters

模拟区域	5 000 m×5 000 m
模拟时间	1 800 s
移动模型	PPRZM 模型
UAV 数量	50～250
UAV 速度	60～150 km/h，步距 15
链路层	802.11 b～11 Mbps
传输层	UDP
UAV 传输范围	27 m
路由算法	DTN 路由
TH_{NPS}	（$t=0$ 时）与正常 UAV 节点相比，发送了超过 15%的数据包
TH_{RTT}	（$t=0$ 时）180 ms
TH_{GH}	（$t=0$ 时）34%的数据包被丢弃
TH_{BH}	（$t=0$ 时）84%的数据包被丢弃

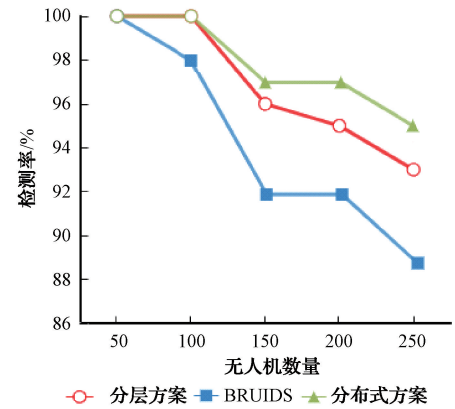
2.2 结果分析

对于检测率方面，因 BRUIDS 方案存在检测 GPS 欺骗、灰洞和黑洞能力限制，因此实验中注入特定类型的攻击，确保能够识别这些攻击。为了模拟不同类型的网络环境，实验控制了不同比例的攻击节点数量，分别为 10%、20%和 30%，来评估在不同攻击强度下的性能表现。结果显示，随着无人机数量的增加，各检测方案的检测率均下降。然而，本方案与分布式方案下降率均保持在 10%以内，并且检测率保持在 93%以上。

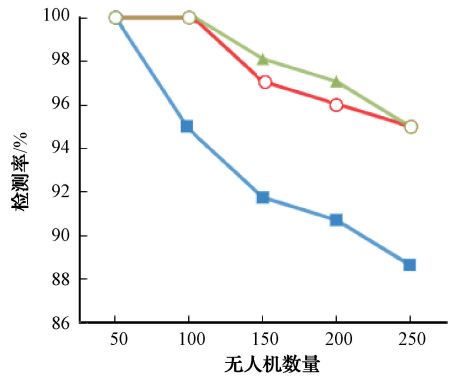
当攻击节点占总节点数比例增加时，本文依然保持在较高水平，结果如图 2 所示。针对于检测率方面的综合考虑，由于本文方案采用深度学习算法，在发现未知攻击方面仍有较大优势。相比较分布式方案，在检测率相同的情况下，其检测方式相对单一难以应对未知网络环境。在实



(a) 攻击节点数量占总无人机节点的10%
(a) The number of attack nodes accounts for 10% of the total drone nodes



(b) 攻击节点数量占总无人机节点的20%
(b) The number of attack nodes accounts for 20% of the total drone nodes



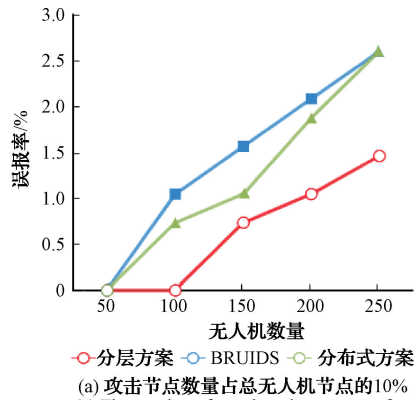
(c) 攻击节点数量占总无人机节点的30%
(c) The number of attack nodes accounts for 30% of the total drone nodes

图 2 不同攻击节点数占比下的检测率对比

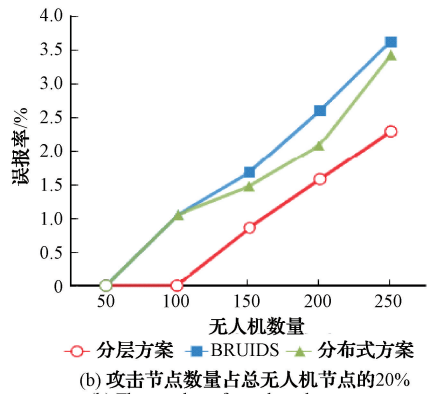
Fig. 2 Comparison of detection rates under different proportions of attack nodes

际环境中，本文方案的检测率将高于分布式方案。

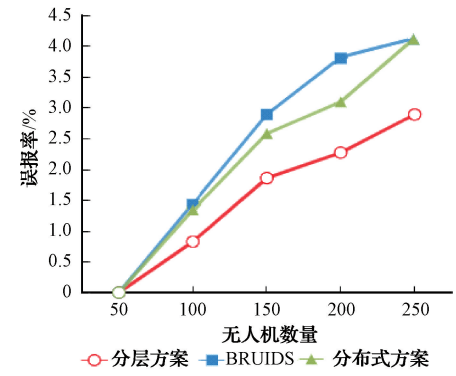
对于误报率方面，当攻击节点数量占总节点的 10%、20%和 30%时，本文在无人机层和地面站层运行的入侵检测代理相互协同，共同检测恶意节点并作出决策。并且，利用误用检测技术和异常检测技术的结合，从而能够更准确地检测恶意节点，结果如图 3 所示，产生的误报率小于 3%。



(a) 攻击节点数量占总无人机节点的10%
(a) The number of attack nodes accounts for 10% of the total drone nodes



(b) 攻击节点数量占总无人机节点的20%
(b) The number of attack nodes accounts for 20% of the total drone nodes

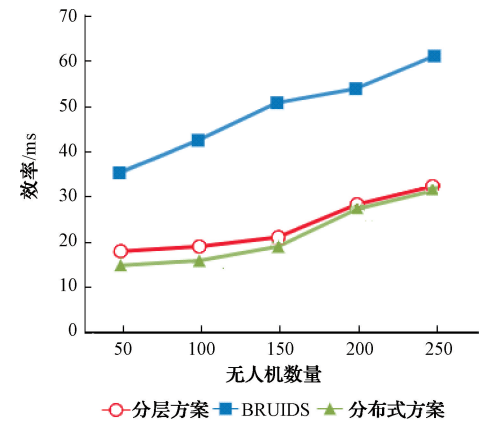


(c) 攻击节点数量占总无人机节点的30%
(c) The number of attack nodes accounts for 30% of the total drone nodes

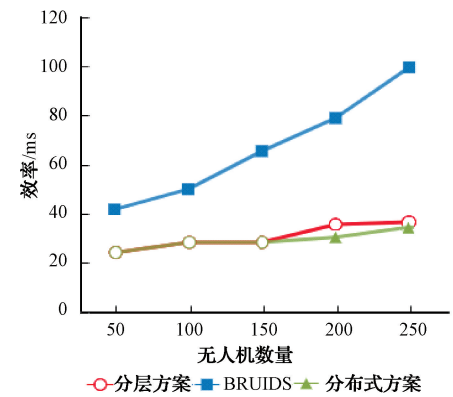
图 3 不同攻击节点数占比下的误报率对比

Fig. 3 Comparison of false alarm rates under different proportions of attack nodes

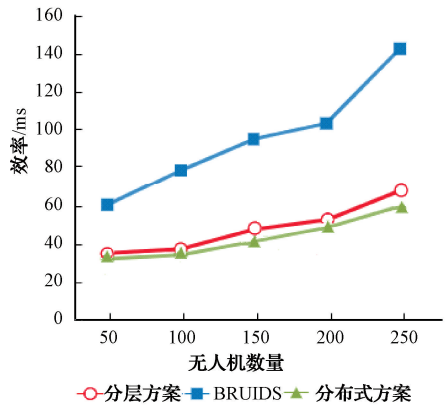
对于效率方面，尤其当无人机的数量非常多时，分层方案和分布式方案的效率几乎相同。由于 BRUIDS 方案中的 IDS 代理需要遍历所有规则来检测恶意或异常行为，因此会导致较高的检测延迟。根据实验结果如图 4 所示，即便在 UAV 节点和攻击者节点分别占总节点的 10%、



(a) 攻击节点数量占总无人机节点的10%
(a) The number of attack nodes accounts for 10% of the total drone nodes



(b) 攻击节点数量占总无人机节点的20%
(b) The number of attack nodes accounts for 20% of the total drone nodes



(c) 攻击节点数量占总无人机节点的30%
(c) The number of attack nodes accounts for 30% of the total drone nodes

图4 不同攻击节点数占比下的效率对比

Fig. 4 Efficiency comparison under different proportions of attack nodes

20%和30%的情况下，本文检测到攻击也在毫秒级。在本文方案中所有UAV节点都具有监测邻居节点能力，但当被检测为异常或恶意节点时失去UDA检测能力。因此只有可信的UDA能够执行检测，从而减少检测恶意UAV节点所需的时间。

通信开销，实验将节点数量固定在总节点的30%，比较了分层方案、BRUIDS方案和分布式方案产生的通信开销，如图5所示。在无人机节点数量增加的情况下，分层方案相比其他方案局域较低的通信开销去检测网络攻击。

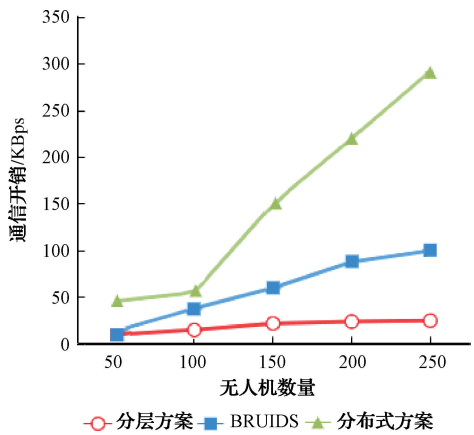


图5 攻击节点数占比30%时通信开销对比

Fig. 5 Comparison of communication overhead when attacking 30% of nodes

通过预训练和微调，逐步调整神经网络参数。训练和验证过程保持稳定，并且模型在数据上迅速收敛。观察到模型在训练数据集的损失曲线几乎始终低于验证数据集，这表面存在一些差距需要考虑。这种差距可能意味着验证数据集相对于训练集更容易让模型进行预测。

为了应对过拟合，引入了一种正则化技术为Dropout，其工作原理是在训练过程中，以一定的丢弃率(在此设置为30%)随机关闭隐藏层中的神经元。具体而言，每个训练阶段都有1/3的神经元被随机忽略。通过这种方式，神经网络更广泛地学习不依赖于任何单个神经元的特征。Dropout本质上创建了一个神经网络集合，其中每个训练示例用于训练不同的随机采样架构。这种神经网络的集成提高了最终模型的泛化能力，使其在未知数据上表现更好，不依赖于现存稳定的特征。

3 结 论

本文主要讨论了在无人机自组网网络中进行异常检测的问题，为了分析数据集并提升模型性能，进行了相关特征的重构和模型简化。使得数据集能够以另一种形式呈现特征，并在训练深度神经网络时有助于防止过拟合。实验表明，采用分层检测机制下，基于深度学习的IDS具有更高的准确性，并可用于检测恶意节点。此方法的优势在于能够实时识别节点行为的异常，以及提高模型准确性。与基于规则或基于签名的检测系统相比，该方法在检测未知攻击方面更有效，并且能够适应不断变化的网络条件。提供了一种新的方法来检测异常的移动自组织网络。在后续实验中需考虑不平衡数据集的影响，并需要更多实验来验证该方法对于更复杂攻击类型的检测的有效性。

参 考 文 献

[1] XIAO Y, ZHANG X. Micro-UAV detection and identification based on radio frequency signature[C]. 2019 6th international conference on systems and informatics (ICSAI). IEEE, 2019: 1056-1062.

[2] FAYYAZ F, GHAZAL T M, AFIFI M A M, et al. Drones network security enhancement using smart based block-chain technology[C]. 2022 International Conference on Cyber Resilience (ICCR). IEEE, 2022: 1-6.

[3] SUN J, WANG W, KOU L, et al. A data authentication scheme for UAV Ad Hoc network communication[J]. The Journal of Supercomputing, 2020, 76: 4041-4056.

[4] MIAO Y, TANG Y, ALZAHRANI B A, et al. Airborne LiDAR assisted obstacle recognition and intrusion detection towards unmanned aerial vehicle: Architecture, modeling and evaluation [J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22(7): 4531-4540.

[5] SAYEED M A, KUMAR R, SHARMA V. Safeguarding unmanned aerial systems: An approach for identifying malicious aerial nodes [J]. IET Communications, 2020, 14(17): 3000-3012.

[6] JITHISH J, SANKARAN S. A game-theoretic approach

for ensuring trustworthiness in cyber-physical systems with applications to multiloop UAV control [J]. Transactions on Emerging Telecommunications Technologies, 2021, 32(5): e4042.

[7] LI Z, XU J, GUO Q. Cooperative location method of muti-UAV system under environment of communication jamming based on tri-layer trust model[C]. 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC). IEEE, 2018: 108-112.

[8] BARKA E, KERRACHE C A, LAGRAA N, et al. UNION: A trust model distinguishing intentional and unintentional misbehavior in inter-UAV communication[J]. Journal of Advanced Transportation, 2018, 2018.

[9] SINGH K, VERMA A K. A fuzzy-based trust model for flying Ad Hoc networks (FANETs) [J]. International Journal of Communication Systems, 2018, 31(6): e3517.

[10] KHANNA N, SACHDEVA M. Study of trust-based mechanism and its component model in MANET: Current research state, issues, and future recommendation[J]. International Journal of Communication Systems, 2019, 32(12): e4012.

[11] 游文静, 董超, 吴启晖. 大规模无人机自组网分层体系架构研究综述[J]. 计算机科学, 2020, 47(9): 226-231.
YOU W J, DONG CH, WU Q H. Research review on layered architecture of large scale unmanned aerial vehicle Ad Hoc networks [J] Computer Science, 2020,47(9):226-231.

[12] JIANG C, FANG Y, ZHAO P, et al. Intelligent UAV identity authentication and safety supervision based on behavior modeling and prediction[J]. IEEE Transactions on Industrial Informatics, 2020, 16(10): 6652-6662.

[13] FENG F, LIU X, YONG B, et al. Anomaly detection in Ad-Hoc networks based on deep learning model: A plug and play device [J]. Ad Hoc Networks, 2019, 84: 82-89.

[14] 梁欣怡,行鸿彦,侯天浩. 基于自监督特征增强的CNN-BiLSTM网络入侵检测方法[J]. 电子测量与仪器学报,2022,36(10):65-73.
LIANG X Y, XING H Y, HOU T H. A CNN BiLSTM network intrusion detection method based on self supervised feature enhancement [J]. Journal of Electronic Measurement and Instrumentation, 2022, 36(10): 65-73.

[15] MEDDEB R, JEMILI F, TRIKI B, et al. Anomaly-based behavioral detection in mobile Ad-Hoc networks[J]. Procedia Computer Science, 2019, 159: 77-86.

[16] MEDDEB R, TRIKI B, JEMILI F, et al. Dataset for intrusion detection in mobile Ad-Hoc networks[C]. 19th International Conference on Intelligent Systems Design and Applications (ISDA 2019). Berlin: Springer International Publishing, 2021: 24-34.

[17] OHIRA S, DESTA A K, ARAI I, et al. Normal and malicious sliding windows similarity analysis method for fast and accurate IDS against DoS attacks on in-vehicle networks[J]. IEEE Access, 2020, 8: 42422-42435.

[18] 姚昌华,高泽郜,韩贵真,等. 基于数据辅助的无人机集群协同空域抗干扰[J]. 电子测量技术, 2022, 45(16):164-170.
YAO CH H, GAO Z H, HAN G ZH, et al. Data assisted collaborative airspace anti-interference of unmanned aerial vehicle clusters [J]. Electronic Measurement Technology, 2022, 45(16): 164-170.

[19] 杜雪茹,王迪,曹越,等. 无人机网络入侵检测与信任体系研究综述[J]. 武汉大学学报(理学版), 2023, 69(5):665-676.
DU X R, WANG D, CAO Y, et al. Review of research on drone network intrusion detection and trust system [J]. Journal of Wuhan University (Science Edition), 2023,69(5): 665-676.

[20] 周显春. ARMA融合CNN-LSTM的传感器流数据异常检测方案[J]. 国外电子测量技术,2022,41(4):55-61.
ZHOU X CH. ARMA fusion CNN-LSTM sensor flow data anomaly detection scheme [J]. Foreign Electronic Measurement Technology, 2022, 41(4): 55-61.

[21] 陈帅,尹洋,杨全顺. 基于深度学习的无人机入侵检测方法[J]. 计算机系统应用,2021,30(4):32-38.
CHEN SH, YIN Y, YANG Q SH. Drone intrusion detection method based on deep learning [J]. Computer System Applications, 2021,30(4): 32-38.

[22] ZHANG D, YU F R, YANG R. A machine learning approach for software-defined vehicular Ad Hoc networks with trust management [C]. 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, 2018: 1-6.

[23] 陈赵懿,高秀峰,王帅,等. 基于信誉评估的Ad Hoc分布式入侵检测[J]. 火力与指挥控制,2020,45(9):6-11.
CHEN ZH Y, GAO X F, WANG SH, et al. Ad Hoc distributed intrusion detection based on reputation

evaluation [J]. Fire and Command Control, 2020, 45(9): 6-11.

[24] RONDINONE M, GOZALVEZ J. Contention-based forwarding with multi-hop connectivity awareness in vehicular Ad-Hoc networks[J]. Computer Networks, 2013, 57(8): 1821-1837.

[25] 付乐天,李鹏,高莲.考虑样本异常值的改进最小二乘支持向量机算法[J].仪器仪表学报,2021,42(6):179-190.
FU L T, LI P, GAO L. Improved least squares support vector machine algorithm considering sample outliers [J]. Chinese Journal of Scientific Instrument, 2021,42(6): 179-190.

作 者 简 介

杜玉航,硕士研究生,主要研究方向为无人机自组网安全。
E-mail:uniqueme911@163.com

王伟,博士,副教授,主要研究方向为网络信息安全、网络智能化应用。
E-mail:17445643@qq.com