基于轻量级密集神经网络的车载自组网入侵检测方法*

黄学臻[1],翟　翟[2],周　琳[2],祝雅茹[2]
(1.公安部第一研究所,北京 100044;2.北京交通大学 智能交通数据安全与隐私保护技术北京市重点实验室,北京 100044)

摘　要：在车载自组网中,攻击者可以通过伪造、篡改消息等方式发布虚假交通信息,导致交通拥堵甚至是严重的交通事故,而传统的入侵检测方法不能满足车载自组网的应用需求。为了解决现阶段车载网中入侵检测方法性能低且存储与时间成本高的问题,提出了一种基于密集神经网络的入侵检测方法 L-DenseNet(Light Dense Neural Network),通过降低模型复杂性,提升算法训练速度和部署适应性,使其更适用于车载自组网中的入侵检测。在 VeReMi 数据集上进行对比实验,结果表明,该方法在识别各类攻击的精确率和召回率的综合表现最好,且具有较少的时间成本和存储开销。

关键词：车载自组网;密集神经网络;入侵检测;深度学习
中图分类号：TN915.08　　**文献标识码**：A　　DOI:10.16157/j.issn.0258-7998.222843

中文引用格式：黄学臻,翟翟,周琳,等. 基于轻量级密集神经网络的车载自组网入侵检测方法[J].电子技术应用,2022,48(7):67-73.
英文引用格式：Huang Xuezhen,Zhai Di,Zhou Lin,et al. Intrusion detection method for VANET based on light dense neural network[J]. Application of Electronic Technique,2022,48(7):67-73.

Intrusion detection method for VANET based on light dense neural network

Huang Xuezhen[1],Zhai Di[2],Zhou Lin[2],Zhu Yaru[2]
(1.The First Research Institution of Ministry of Public Security of PRC,Beijing 100044,China;
2.Security and Privacy in Intelligent Transportation,Beijing Jiaotong University,Beijing 100044,China)

Abstract: In the vehicular ad-hoc network, attackers can publish false traffic information by forging or tampering with messages, etc., resulting in traffic congestion or even serious traffic accidents. However, traditional intrusion detection methods cannot meet the application requirements of vehicular ad-hoc network. In order to solve the problems such as low performance, instability and high storage and time cost of intrusion detection methods in the current vehicular ad-hoc network, this paper proposes an intrusion detection method L-DenseNet(Light Dense Neural Network) based on dense neural network. The L-DenseNet is proposed to reduce the complexity of the model and improve the training speed and deployment adaptability of the detection algorithm. The proposed method is more suitable for intrusion detection in vehicle ad hoc networks. This paper conducts comparative experiments on the VeReMi dataset. The results show that the method proposed has the best overall performance in identifying various types of attacks in terms of precision and recall. As the same time, this method has less time cost and storage overhead.
Key words: vehicular ad-hoc network;dense neural network;intrusion detection;deep learning

0 引言

随着当前车辆激增,交通拥堵及交通事故等严重影响了社会生活,为了满足人们对于提升出行质量的需求,车载自组网(Vehicular Ad-Hoc Network,VANET),简称车载网,逐渐成为实现智能交通系统的基础之一。虽然 VANET 能够为人们的出行质量提供有力保障,但是大量的车辆数据通过无线通信共享,任何交换恶意信息的节点都会损害网络安全性,因此,VANET 的安全性成为了车联网领域的重点研究目标。

为了提高 VANET 安全性,避免入侵行为产生的危害,首先需要明确其面临的安全问题。VANET 中入侵行为主要源自于自私的驾驶者和恶意的攻击者,自私的驾驶者主要是为了私利而独享道路、节约自身资源等;恶意的攻击者使车辆无意或有意地在网络中传输不正确的信息(例如错误的位置或速度坐标),影响车载网的正常工作,威胁驾乘者的生命财产安全[1]。然而,面对日益复杂的车载网络环境,传统的入侵检测方法呈现出相当多的问题。其中最主要的问题是:大数据背景下传统入侵检测方法性能低下,存储与时间成本高,准确性不高。

为了有效解决上述问题,本文提出了一种在 VANET

* 基金项目:国家重点研发计划(2020YFB2103800)

场景下的高效入侵检测方法，将基于轻量级密集卷积神经网络的入侵检测方法部署在 RSU 上，以对车辆发来的消息及时进行检测。实验结果表明，本文所提出的模型在 VeReMi 数据集上具有较高的准确率，在各攻击类别和正常类别的识别上均具有稳定的性能。同时，在训练过程中消耗时间短，模型参数总量相对较少，进一步节省计算开销与存储开销。

1 相关工作

随着机器学习与深度学习的广泛应用，研究人员提出了各种基于机器学习或深度学习方法的入侵检测方法。在基于机器学习方法的研究中，Zhang 等[2]提出了一种分布式检测方案，该方案可以在网络中的单个车辆上运行，并且可以协作进行异常信息交换；Garg 等[3]提出了一种基于机器学习的入侵检测方案，该方案结合了椭圆曲线密码学和模糊 C-means 聚类；Schmidt 等[4]提出了一种结流分类模型，该模型采用 k 均值聚类算法进行动态聚类；Bangui 等[5]提出一种混合机器学习模型，该方法主要利用随机森林的优点来检测已知的网络入侵。然而，这些传统的机器学习方法虽然透明简单且训练直观，但是需要手动处理特征且对入侵行为分类精度不够高，已经不能满足车载网络的安全需求。

经过研究人员的广泛探究与实践，基于深度学习的入侵检测方案已成为目前车载网安全领域内相对成熟和主流的方式。Van 等利用 CNN 来检测由车辆传输的异常传感器数据[6]，然而，他们只考虑了少数异常类型；Nie 等探索了使用 CNN 的无监督方法，该方法使用 VANET 流量的时空和稀疏特征以及基于马哈拉诺比斯距离的损失函数的 CNN 架构[7]，并在其最新工作中使用监督技术进一步扩展[8]；Ning 等[9]对边缘服务器进行了深度强化学习，进一步解决了入侵检测问题中的计算问题；Alladi 等人[10]提出了基于深度神经网络的车辆异常检测方案，使用序列重建方法来区分正常车辆数据和异常数据。但是这些工作往往只关注某一类或者某几类异常攻击类型，且需要较大的计算与存储开销。

2 应用场景

VANET 旨在最大限度地减少交通堵塞、交通事故等问题，虽然 VANET 可以实现车辆间通信以及交通数据共享，但是也容易遭受到各种攻击。因此，采取措施加强车载网络安全至关重要。在本节中，首先讨论本文考虑的车载网络场景，再具体介绍在此场景下本文方案主要针对的攻击类型。

2.1 车载自组网网络模型

如图 1 所示，本文所假设的 VANET 系统模型包括以下 3 类实体[11]：

(1)车载单元(On Board Unit，OBU)：安装在车辆中，用于在 VANET 中发布和接收交通路况消息，从而及时调整行车路线，避免交通拥堵等事故发生。

(2)路边单元(Road Side Unit，RSU)：部署在十字路口以及停车场等场所，负责管辖其所在位置一定范围内的车辆，本文提出的入侵检测模型就部署在 RSU 上。

(3)可信中心(Trusted Authority，TA)：TA 是可信的，负责维护 RSU 的身份与位置映射列表，根据 RSU 的实际情况动态地更新映射列表，对列表中长时间无响应的 RSU 进行删除，因此 RSU 也是可信的。

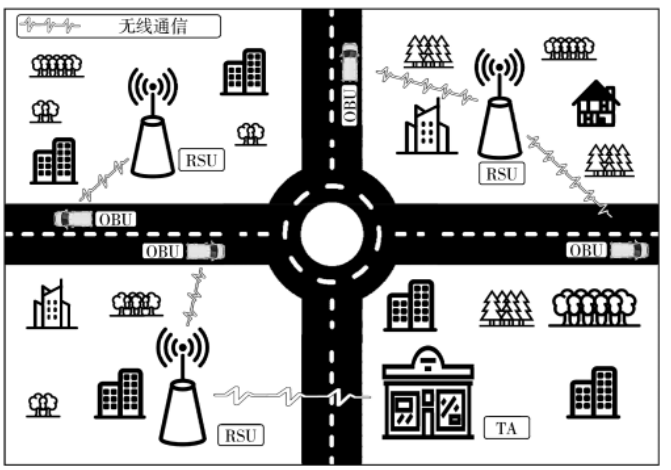

图 1 车载网网络模型

2.2 攻击类型

在不同车流量场景和不同的攻击者密度下，内部攻击者修改基础安全消息(Basic Safety Message，BSM)[12]以生成虚假或错误的位置与速度信息，并在 DSRC 上进行广播。在车载网络中，恶意车辆可能会发送虚假信息，造成车辆混乱，严重影响其他节点的安全应用。表 1 列出了本文所采用的 VeReMi 数据集中建模的攻击类型及使用的参数[13]。

3 基于轻量级密集神经网络的入侵检测方法

本节给出了入侵检测方法的设计目标，并提出了轻量级密集神经网络模型，以及基于此模型的入侵检测方法。

表 1 攻击类型及参数

标签	攻击类型	描述	参数
1	Constant	传输具有固定位置的伪造消息(预先配置)	x=5 560，y=5 820
2	Constant Offset	通过添加预先配置的偏移量来传输具有固定位置的伪造消息	Δx=250，Δy=-150
4	Random	从模拟区域传输具有随机位置值的伪造消息	在模拟区域内均匀随机
8	Random Offset	在节点周围的预先配置的矩形中传输具有随机位置的伪造消息	Δx，Δy 在[-300，300]内均匀随机
16	Eventual Stop	车辆在指定的时间间隔内表现正常，然后重复传输当前位置	每个位置更新停止概率+=0.25(10 Hz)

3.1 设计目标

针对车载网中恶意攻击者传输错误数据的行为，并结合现有入侵检测方案存在的不足，本文提出的入侵检测方法设计目标为：

(1)RSU 及时检测入侵行为。当网络中有恶意攻击者传输不正确数据时，RSU 需要及时检测出入侵行为。

(2)设计轻量级且精度高的模型。VANET 场景下，网络结构快速变化，信息交互迅速，实时性高，要求具有较低的模型检测时间与存储成本。

(3)检测多类攻击行为。为使 RSU 更好地响应和处理接收到的车辆数据，需要实现对多种不同攻击行为的准确识别。

3.2 轻量级密集神经网络模型

密集神经网络(Dense Neural Network，DenseNet)[14]是一种高效的神经网络模型，解决了网络过深引起的梯度消失、参数爆炸而导致网络难以训练的问题。为了将 DenseNet 应用于车载自组网的入侵检测，本文对 DenseNet 进行改进，设计了轻量级密集神经网络(Light Dense Neural Network，L-DenseNet)。

原始 DenseNet 主要由稠密块(Dense Block)、过渡层(Transition Layer)和增长率(Growth Rate)构成。其中，Dense Block 定义了输入和输出的连结方式；Transition Layer 用来控制通道数，防止通道数过多；Growth Rate 表示每个 Dense Block 中每层输出的 feature map 个数。一个完整 DenseNet 由 4 个 Dense Block 和 3 个 Transition Layer 组成，Transition Layer 存在于两个相邻的 Dense Block 中间。以 DenseNet-121 为例，完整的 DenseNet 结构如图 2 所示。

由于车载网络中传输的车辆数据大小比原始的 DenseNet 的图像数据简单得多，因此不需要使用如此复杂的结构。本文通过减少其组件以及调整参数，使模型变得更加轻便高效。L-DenseNet 模型调整了 Dense Block 和相应 Transition Layer 的数量，减少了 2 个 Dense Block 和 2 个 Transition Layer。

Dense Block 内部采用多层结构，每层数据都通过一个非线性变换函数 H 传递给下一层，且每层的输入来自前面所有层的输出。如图 3 所示，L 层的 Dense Block 有 $L(L+1)/2$ 个连接。这一结构更有效地利用了数据特征，同时减少了参数数量。其中，非线性变化函数 H 包括了 BN(Batch-Normalization)、激活函数(ReLU)以及卷积(Conv)3 种操作(BN+ReLU+3×3 Conv)。由于后面层的输入会非常大，因此，Dense Block 内部采用了 Bottleneck 层来减少计算量，在原有的结构中增加 1×1 Conv，降低特征数量。

本文提出的 L-DenseNet 在减少 Dense Block 数量的基础上，还对其内部结构和参数进行了修改。针对车载

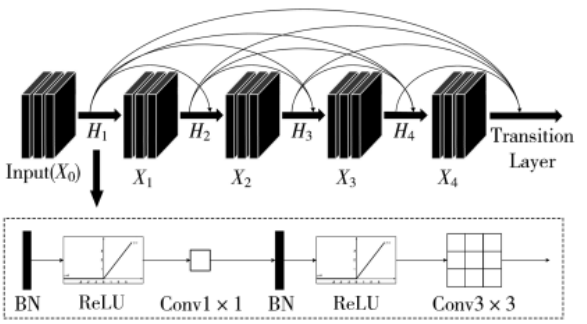

图 3 Dense Block 内部结构图

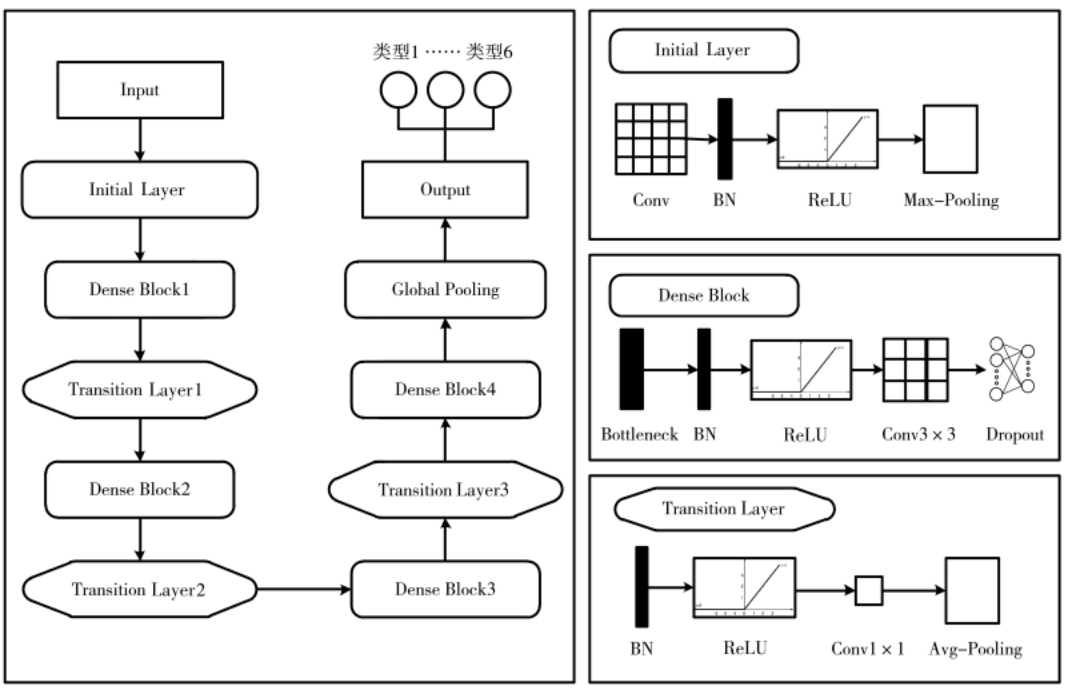

图 2 完整的 DenseNet-121 结构图

网络中的一维数据集，本文的 L-DenseNet 将原二维卷积均改成一维卷积，并对卷积核的尺寸做了相应改变。L-DenseNet 的 Dense Block 使用了 BN+ReLU+1 Conv+BN+ReLU+3 Conv+Dropout 结构。Dropout 的使用进一步简化了网络结构复杂度，衰退率设置为 0.001。

Transition Layer 保证了每个 Dense Block 后面的特征维度统一，一般结构为 BN+ReLU+1×1 Conv+2×2 Avg-Pooling。通过 1×1 卷积层来减小通道数，使用步幅(stride)为 2 的平均池化层(average pool)来进一步降低模型复杂度。本模型使用 stride 为 1 的 average pool。

表 2 为原始 DenseNet 和 L-DenseNet 的结构以及输出维度对比。通过创建一个更轻量级的模型，减少了内存需求和参数的数量，使模型更适用于拓扑结构快速变化的车载网。

模型的输出为攻击样本的类型，若是正常数据，则 RSU 可正常响应并与其他车辆进行数据共享；若为异常数据，RSU 则不在其管理域内共享该数据。

3.3 基于轻量级密集神经网络的入侵检测方法

本小节基于 3.2 节提出的 L-DenseNet，给出了一种轻量级的入侵检测方法，如图 4 所示。

VANET 中入侵检测方案的应用流程如下：

(1)车辆将其位置、车速等相关数据封装成消息，发送给 RSU；

(2)RSU 提取多维度的时间、位置、车速等相关数据，进行数据标准化；

(3)将步骤(2)得到的数据作为神经网络模型的输

表 2 DenseNet-121 与 L-DenseNet 的参数配置及输出对比

网络结构	DenseNet121(k=32)	输出尺寸	L-DenseNet(k=32)	输出尺寸
Convolution	7×7 conv, stride 2	112×112	3 conv, stride 1	8×16
Pooling	3×3 max pool, stride 2	56×56	3 max pool	8×16
Dense Block1	$\begin{bmatrix}1\times1\ \text{conv}\\3\times3\ \text{conv}\end{bmatrix}\times6$	56×56	$\begin{bmatrix}1\ \text{conv}\\3\ \text{conv}\end{bmatrix}\times4$ dropout(0.001)	8×144
Transition layer1	1×1 conv 2×2 average pool, stride 2	28×28	1 conv 2 average pool, stride 1	8×72
Dense Block2	$\begin{bmatrix}1\times1\ \text{conv}\\3\times3\ \text{conv}\end{bmatrix}\times12$	28×28	$\begin{bmatrix}1\ \text{conv}\\3\ \text{conv}\end{bmatrix}\times8$ dropout(0.001)	8×328
Transition Layer 2	1×1 conv 2×2 average pool, stride 2	14×14	–	–
Dense Block3	$\begin{bmatrix}1\times1\ \text{conv}\\3\times3\ \text{conv}\end{bmatrix}\times24$	14×14	–	–
Transition Layer 3	1×1 conv 2×2 average pool, stride 2	7×7	–	–
Dense Block 4	$\begin{bmatrix}1\times1\ \text{conv}\\3\times3\ \text{conv}\end{bmatrix}\times16$	7×7	–	–
输出层	7×7 全局 average pool	1×1		328
	1 000 维全连接 softmax	–	6 维全连接 softmax	–

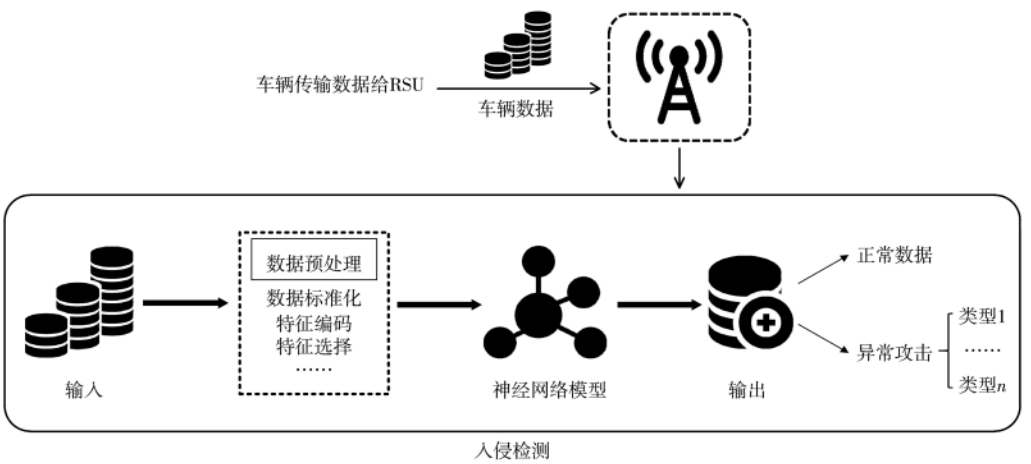

图 4 基于轻量级密集神经网络的入侵检测方法

入，其输出是相应的攻击类型编号，类型 0 代表无攻击。

4 实验及分析

本文使用车载自组网中的经典数据集 VeReMi 数据集进行实验验证，并与其他入侵检测方法进行对比分析。

4.1 实验设置

(1)数据集

VeReMi 数据集[15]总共包括 225 个模拟的车辆运行过程，在这些车辆中，一部分是恶意的，通过采样均匀分布([0，1])并将其与攻击者分数参数进行比较，使每个车辆基本具有该概率作为攻击者。同时，所有归类为攻击者的车辆都执行相同的攻击算法，数据集中的异常数据也相应分为 5 类攻击，如表 1 所示。

(2)数据预处理

VeReMi 数据集一共分为 5 类攻击文件，每个文件有 17 列特征值和一个标签值，如表 3 所示。由于每条数据的标签都为正常/异常，因此首先对 5 类攻击文件进行合并，贴上相应标签，并将样本标签的数值转化为 6 维 one-hot 编码。最后对数据集进行归一化处理。

表 3 VeReMi 数据集各特征含义

特征	含义	特征	含义
Sendtime1	接收时间	Sendtime2	传输时间
sender_1	收货人	sender_2	发射者
messageID	消息 ID	pos-x2	发射器 x 位置
pos-x1	接收器 x 位置	pos-y2	发射器 y 位置
pos-y1	接收器 y 位置	pos-z2	发射器 z 位置
pos-z1	接收器 z 位置	spd-x2	发射器 x 速度
spd-x1	接收器 x 速度	spd-y2	发射器 y 速度
spd-y1	接收器 y 速度	spd-z2	发射器 z 速度
spd-z1	接收器 z 速度	AttackerType	攻击类型(0/1)

(3)评价指标

深度学习模型通常使用的评价指标有准确率(accuracy)、召回率(recall)、精确率(precision)、F1 值。这 4 种指标可以利用一个混淆矩阵来计算得出。混淆矩阵各类数据统计量及其之间的关系如表 4 所示。

表 4 混淆矩阵

	预测正常	预测攻击	总计
真实正常	TP	FN	TP+FN
真实攻击	FP	TN	FP+TN
总计	TP+FP	FN+TN	N

准确率指正确检测的样本数量占样本总数的比例，计算公式如下：

$$accuracy=(TP+TN)/N \tag{1}$$

精确率指被检测为正常且检测正确的样本数量占所有被预测为正常样本数量的比例，计算公式如下：

$$precision=TP/(TP+FP) \tag{2}$$

召回率指被检测为正常且检测正确的样本数量占所有正常样本数量的比例，计算公式如下：

$$recall=TP/(TP+FN) \tag{3}$$

F1 值指精确率和召回率的加权调和平均值，计算公式如下：

$$F1=2\times precision\times recall/(precision+recall) \tag{4}$$

4.2 实验结果及分析

首先在不同的学习率、增长率参数设置下进行实验，以找到较为适合 L-DenseNet 模型结构的参数设置，接下来将使用 L-DenseNet 在 VeReMi 数据集上进行实验所得到的各攻击类别精确率、召回率等评价指标与几种现有模型进行对比分析，以说明 L-DenseNet 应用于车载自组网场景时所具有的优势。

4.2.1 参数设置对实验结果的影响

学习率是深度神经网络模型最重要的超参数之一，它通过调节模型权重更新的速度从而控制模型学习的进度。为了确定最佳学习率大小，本文在当学习率分别设置为 0.001、0.005、0.01、0.05、0.1、0.5 时进行实验，并将测试集上的准确率作为评价指标，实验结果如图 5 所示。

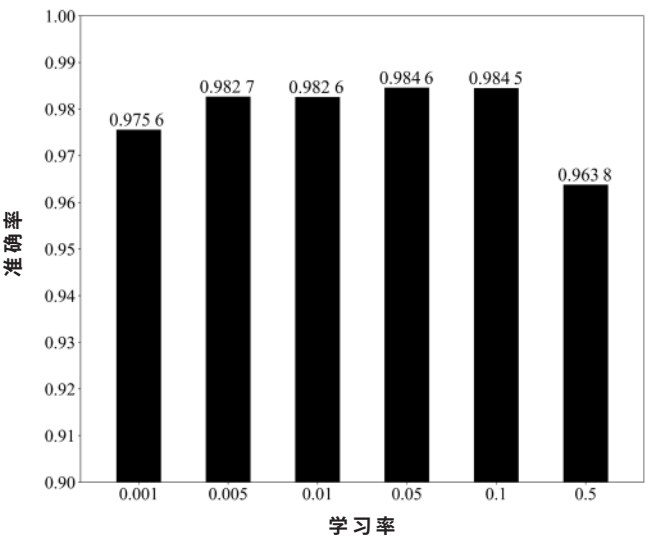

图 5 不同学习率设置下的测试集准确率

根据实验数据，当学习率取值为 0.05 或 0.1 时较为适合本模型结构。

此外，由于 DenseNet 网络的增长率参数控制着每个 Dense Block 输出的特征映射数量，因此增长率参数的取值大小也会对模型的准确率造成一定的影响。本文对增长率参数选取为 8、16、24、32 的情况依次进行实验，并将测试集上的准确率作为评价指标，实验结果如图 6 所示。

根据图 6 可知，在网络深度一定的情况下，适当增加增长率可以在一定程度上使模型的准确率得到提升。但是增长率的增加也会引起模型参数量的急剧增加，当

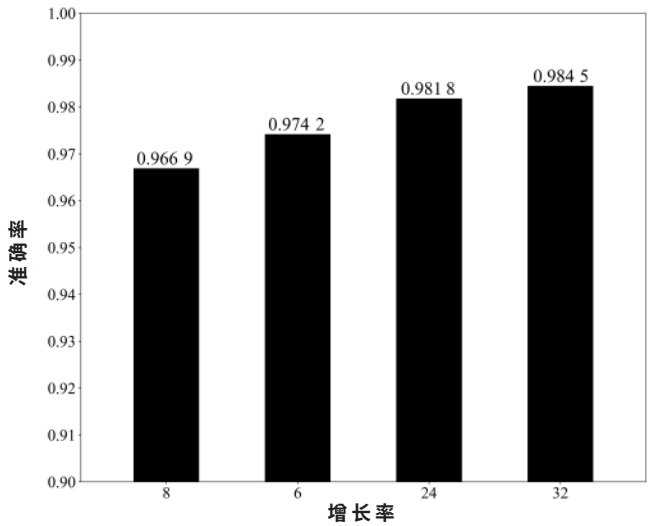

图 6 不同增长率设置下的测试集准确率

增长率取值为 8、16、24、32 时，L-DenseNet 的参数总量分别为 18 622、59 342、123 102、209 902，需要结合实际应用中 RSU 的存储和计算能力在模型准确率和规模之间做出一定的权衡。

4.2.2 本文模型与其他模型性能对比分析

文献[15]最初提出了 VeReMi 数据集并且展示了它如何应用在入侵检测场景中，文献[16]使用传统机器学习方法来对 VeReMi 数据集中的攻击类型进行分类检测，文献[17]提出了另外一种基于 DenseNet 的多分类模型。本文将 L-DenseNet 在 VeReMi 数据集上进行实验所得到的各攻击类型精确率、召回率与文献[15]、文献[16]、文献[17]相关的实验结果进行对比，如表 5 所示。

表 5 中与文献[15]、文献[16]的对比结果说明，本文所提出的 L-DenseNet 模型在 VeReMi 数据集上各攻击类型的检测中均具有较高准确率；并且在各攻击类型的精确率、召回率上可以看出，虽然文献[15]对于 Attack1、Attack4 的检测精确率、召回率较高，但是其 Attack2、Attack8 的精确率明显低于平均水平。同理，文献[16]中的模型在 Attack2 和 Attack16 的检测上均表现欠佳，这反映出上述模型存在检测准确率分布不均匀的问题，而本文所提出的 L-DenseNet 模型对于上述 5 种攻击类型的检测能力相对稳定，避免了不同攻击类型精确率、召回率等指标高低差别大的情况。特别是对于 Attack2 和 Attack16 的检测，L-DenseNet 表现出了显著优越性。

表 5 与文献[17]的对比结果说明，本文在进一步缩减模型规模的基础上仍然实现了令人满意的准确率。文献[17]同样使用密集连接结构的神经网络，在各种攻击类型的检测上也取得了较为理想的效果，但是文献[17]中的模型参数总量为448 746，增长率取值相同的情况下，本文所提出的 L-DenseNet 参数总量仅为 209 902，参数总量少于文献[17]中模型的 1/2，然而各攻击类型的精确率、召回率均大于文献[17]中的模型。另外，当增长率取值为 8 时，本文模型的参数总量仅为 18 622，训练一个轮次耗时仅300 s，总体准确率却可达到 96.69%，这更加体现了 L-DenseNet 模型轻便高效的特点。

5 结论

本文针对 VANET 中的常见入侵行为进行研究，提出了 L-DenseNet 模型以及相应的入侵检测方法。L-DenseNet 模型不仅保留了 DenseNet 可以缓解梯度消失或者爆炸问题的优点，同时降低了 DenseNet 模型的架构复杂性，使其更适用于 VANET 中简单、高效的入侵行为检测。此外，在 VeReMi 数据集上对各类指标进行评估，与现有方案的对比分析表明，所提出的方案在准确率、计算开销及存储开销等方面均优于现有方案，在车载网络场景下具有更高的可行性。

参考文献

[1] 李春彦，刘怡良，王良民.车载自组网中基于交通场景的入侵行为检测机制[J].山东大学学报(工学版)，2014，44(1)：29-34.

[2] ZHANG T，ZHU Q.Distributed privacy-preserving collaborative intrusion detection systems for VANETs[J].IEEE Transactions on Signal and Information Processing over Networks，2018，4(1)：148-161.

[3] GARG S，KAUR K，KADDOUM G，et al.SDN-based secure and privacy-preserving scheme for vehicular networks：a 5G perspective[J].IEEE Transactions on Vehicular Technology，2019，68(9)：8421-8434.

[4] SCHMIDT D A，KHAN M S，BENNETT B T.Spline-based intrusion detection for VANET utilizing knot flow classification[J].Internet Technology Letters，2020，3(3)：e155.

[5] BANGUI H，GE M，BUHNOVA B.A hybrid data-driven model for intrusion detection in VANET[J].Procedia Computer Science，2021，184：516-523.

[6] VAN W F，WANG Y，KHOJANDI A，et al.Real-time sensor anomaly detection and identification in automated vehicles[J].

表 5 本文模型与其他现有模型对比

模型	攻击类型 1		攻击类型 2		攻击类型 4		攻击类型 8		攻击类型 16	
	精确率/%	召回率/%	精确率/%	召回率/%	精确率/%	召回率/%	精确率/%	召回率/%	精确率/%	召回率/%
文献[15]	100	100	40	100	100	99	70	95	80	90
文献[16]	95.2	83.2	56.1	19.3	95	83.6	96.2	82.5	71.4	42.5
文献[17]	99.1	99.6	93.2	99	100	99.7	97.7	71.6	97.2	88.1
本文	99.6	99.8	95.5	99.8	100	99.7	99	85.8	97.8	91

IEEE Transactions on Intelligent Transportation Systems, 2019, 21(3): 1264-1276.
[7] NIE L, WANG H, GONG S, et al. Anomaly detection based on spatio-temporal and sparse features of network traffic in VANETs[C]//2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2019: 1-6.
[8] NIE L, NING Z, WANG X, et al. Data-driven intrusion detection for intelligent Internet of vehicles: a deep convolutional neural network-based method[J]. IEEE Transactions on Network Science and Engineering, 2020, 7(4): 2219-2230.
[9] NING Z, DONG P, WANG X, et al. Deep reinforcement learning for intelligent internet of vehicles: an energy-efficient computational offloading scheme[J]. IEEE Transactions on Cognitive Communications and Networking, 2019, 5(4): 1060-1072.
[10] ALLADI T, AGRAWAL A, GERA B, et al. Deep neural networks for securing IoT enabled vehicular ad-hoc networks[C]//ICC 2021-IEEE International Conference on Communications. IEEE, 2021: 1-6.
[11] 吴静雯, 殷新春, 宁建廷. 车载自组网中可撤销的聚合签名认证方案[J]. 计算机应用, 2022, 42(3): 10.
[12] SAXENA R, JAIN M, SHARMA D P, et al. A review on VANET routing protocols and proposing a parallelized genetic algorithm based heuristic modification to mobicast routing for real time message passing[J]. Journal of Intelligent & Fuzzy Systems, 2019, 36(3): 2387-2398.
[13] SINGH P K, GUPTA S, VASHISTHA R, et al. Machine learning based approach to detect position falsification attack in vanets[C]//International Conference on Security & Privacy. Springer, Singapore, 2019: 166-178.
[14] HUANG G, LIU Z, VAN DER MAATEN L, et al. Densely connected convolutional networks[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017: 4700-4708.
[15] HEIJDEN R W, LUKASEDER T, KARGL F. Veremi: a dataset for comparable evaluation of misbehavior detection in vanets[C]//International Conference on Security and Privacy in Communication Systems. Springer, Cham, 2018: 318-337.
[16] SO S, SHARMA P, PETIT J. Integrating plausibility checks and machine learning for misbehavior detection in VANET[C]//2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, 2018: 564-571.
[17] 缪祥华, 单小撒. 基于密集连接卷积神经网络的入侵检测技术研究[J]. 电子与信息学报, 2020, 42(11): 2706-2712.

(收稿日期: 2022-04-11)

作者简介:
黄学臻(1984-), 女, 博士, 工程师, 主要研究方向: 数据安全和隐私保护。
翟翟(1998-), 女, 硕士研究生, 主要研究方向: 数据安全。
周琳(1998-), 通信作者, 女, 硕士研究生, 主要研究方向: 网络安全, E-mail: zhoulin01@bjtu.edu.cn。

扫码下载电子文档

(上接第 66 页)

空输电线路故障测距研究[J]. 电工电气, 2018(10): 49-53.
[14] 李娟, 高厚磊, 弓新月, 等. 一种用于配电网故障数据自同步的故障时刻检测方法[J]. 电力系统保护与控制, 2018, 46(4): 92-98.
[15] 刘斯琪, 喻锟, 曾祥君, 等. 基于零序电流幅值连调的小电流接地系统故障区段定位方法[J]. 电力系统保护与控制, 2021, 49(9): 48-56.

(收稿日期: 2021-11-18)

作者简介:
王毅(1981-), 男, 博士, 副教授, 主要研究方向: 宽带电力线载波通信、智能电网、电力物联网。
李曙(1996-), 通信作者, 男, 硕士研究生, 主要研究方向: 配电网故障检测与诊断, E-mail: 455938969@qq.com。

扫码下载电子文档

版权声明