doi:10.19562/j.chinasae.qcgc.2024.08.006

基于BEGAN的汽车CAN网络入侵检测数据增强方法研究*

汪 想[1],刘蓬勃[1],赵 剑[1],范科峰[2],李琳辉[1]
(1. 大连理工大学汽车工程学院,大连 116024; 2. 中国电子技术标准化研究院,北京 100007)

[摘要] 针对目前汽车CAN网络入侵检测算法因攻击样本缺少而导致数据不平衡问题,提出一种基于BEGAN的CAN入侵检测数据增强方法,引入one-hot编码将CAN报文特征图像化,结合构建的生成对抗网络,生成与真实攻击格式一致且内容差异的有效样本。通过采集实车数据作为真实样本进行训练,从特征图、t-SNE可视化、统计学分析和分类器验证角度验证了所生成的增强数据集的实用性,可提高入侵检测分类器准确率;与传统过采样算法含随机过采样(ROS)、合成少数过采样(SMOTE)、SMOTE-ENN、自适应合成过采样(ADASYN)相比,具有更高的准确率。

关键词:汽车控制器局域网络;入侵检测;生成对抗网络;数据增强

Research on Data Enhancement Methods of BEGAN-Based Intrusion Detection in Automotive CAN Networks

Wang Xiang[1], Liu Pengbo[1], Zhao Jian[1], Fan Kefeng[2] & Li Linhui[1]
1. *School of Automotive Engineering, Dalian University of Technology, Dalian* 116024;
2. *China Electronics Standardization Institute, Beijing* 100007

[**Abstract**] For the data imbalance problem of the current automotive CAN network intrusion detection algorithm due to the lack of attack samples, a CAN intrusion detection data enhancement method based on BEGAN is proposed, which introduces in one-hot coding to image the CAN message features and combines with the constructed Generative Adversarial Network to generate valid samples with the same format as the real attack and with different content. The practicality of the generated enhanced dataset is verified from the perspectives of feature maps, t-SNE visualization, statistical analysis and classifier validation by collecting real vehicle data as real samples for training, which can improve the intrusion detection classifier accuracy. With higher accuracy compared with the traditional oversampling algorithms including Random Oversampling (ROS), Synthetic Minority Oversampling Technique (SMOTE), SMOTE combined with Edited Nearest Neighbors (SMOTE-ENN) and Adaptive Synthetic Oversampling (ADASYN).

Keywords: local area network for automotive controller; intrusion detection; generative adversarial networks; data enhancement

*国家自然科学基金联合基金项目(U1930206)资助。
原稿收到日期为 2023 年 08 月 01 日,修改稿收到日期为 2023 年 10 月 13 日。
通信作者:赵剑,教授,博士,E-mail:jzhao@dlut.edu.cn。

前言

随着网络技术与汽车技术的蓬勃发展,现代汽车智能化功能越来越丰富,汽车与外部信息交互越来越频繁,车载网络受到入侵的风险越来越高[1-2]。而入侵检测算法被应用于汽车控制器局域网络(controller area network,CAN)安全防御中,其检测恶意攻击的能力将对汽车CAN网络的安全性产生影响[3]。入侵检测算法能够识别外部注入CAN网络的恶意报文,也可以区分内部假冒用户的非法操作。目前CAN网络入侵检测技术方案主要分为3类:基于统计学习、基于物理特性以及基于机器学习[4]。其中基于机器学习的入侵检测算法通过学习大量历史数据,发掘内在规律,从而判断网络行为是否异常,具有良好的拓展性,对未知模式下的攻击也具备一定的检测能力,是目前热门的入侵检测算法研究领域[5-6]。

近年来,各国学者对汽车CAN网络的入侵检测算法进行了丰富的探讨和研究。文献[7]~文献[10]中分别以支持向量机(support vector machines,SVM)、随机森林(random forest,RF)、最近邻算法(k-nearest neighbor,KNN)、梯度提升决策树(gradient boosting decision tree,GBDT)为分类器,将CAN数据域作为分类特征,对篡改攻击进行检测。但机器学习的检测性能依赖训练数据的数量及质量,而车载CAN网络中的数据流量较大且各类别比例较为悬殊,训练数据集攻击样本缺乏、类别不平衡,导致入侵检测模型存在过/欠拟合以及训练复杂等问题[11-13]。因此,如何解决数据不平衡问题,确保入侵检测算法的性能安全可靠成为一个新的亟待解决的问题。目前学术界的数据增强方法主要分为两大类,传统的过采样方法和基于生成对抗网络(generative adversarial network,GAN)的生成方法[14-15]。文献[16]中采用随机过采样技术(random over sampling,ROS),通过随机复制重复少数类样本,文献[17]中基于合成少数过采样技术(synthetic minority over-sampling technique,SMOTE)使样本平衡,采用最近邻算法(KNN)生成少数样本,在此基础上,文献[18]中提出一种基于SMOTE-SDSAE-SVM的CAN总线入侵检测方法,利用SMOTE技术对不平衡类别的攻击数据进行近邻采样,从而生成更多攻击类别近似样本,文献[19]中提出一种基于K-means聚类和SMOTE技术混合采样的车载CAN入侵检测方法,对流量较小的数据,使用SMOTE方法平衡数据,文献[20]中在SMOTE基础上引入最近邻规则算法(edited nearest neighbor,ENN)进行改进,有效滤除了冗杂样本,文献[21]中通过自适应合成过采样算法(adaptive synthetic,ADASYN),基于权重分布,为少数较难学习的类别合成更多样本。上述方法虽然解决了数据不平衡问题,但其本质上属于样本的重组复制,不能生成实质性数据,容易造成模型过拟合问题。生成对抗网络(GAN)的问世,为数据增强研究提供了新的思路[22-24]。作为深度学习领域的生成模型之一,GAN在计算机视觉、自然语言处理等领域得到广泛应用,但在网络安全领域的应用却很少[25]。

本文以CAN网络入侵检测技术为研究对象,结合CAN和GAN的特点,提出了一种基于边界平衡生成对抗网络(boundary equilibrium generative adversarial networks, BEGAN)的入侵检测数据增强方法,通过生成对抗网络实现入侵检测数据的自动生成,缓解传统方法难以获取攻击样本而导致的数据不平衡问题,为入侵检测算法提供充足优质数据。

1　边界平衡生成对抗网络

生成对抗网络(GAN)是一种深度学习模型,由Goodfellow等于2014年提出[26]。受博弈论启发,该模型由生成器G和鉴别器D组成,生成器G学习真实样本分布,并基于随机噪声生成数据,鉴别器D接收并区分真实数据和生成数据,通过不断博弈,生成数据在分布上不断逼近真实数据,鉴别准确度越来越高,直至模型达到纳什均衡。

边界平衡生成对抗网络(BEGAN)是为了解决GAN梯度不稳定、训练崩溃、生成模式单一等问题而提出的一种改进方法[27]。BEGAN与GAN的优化目标不同,GAN要求生成器G生成的数据分布尽可能拟合真实数据分布,而BEGAN则希望生成数据和真实数据在通过鉴别器D(自编码器)后的重构数据误差分布不断逼近,输入数据θ经过鉴别器D后的重构数据误差$L(\theta)$如式(1)所示。

$$L(\theta)=\left|\theta-D(\theta)\right|^{\eta} \tag{1}$$

式中$\eta\in\{1,2\}$是范数选择参数,$\eta=1$表示l_1范数,$\eta=2$表示l_2范数。

为了最小化两个重构误差分布之间的

Wasserstein距离,最终BEGAN的优化目标转化为最小化鉴别器D损失函数L_D和生成器G损失函数L_G,如式(2)所示。

$$\begin{cases} L_D = L(x) - k_t L\big(G(z)\big) \\ L_G = L\big(G(z)\big) \\ k_{t+1} = k_t + \lambda_k\big(\gamma L(x) - L\big(G(z)\big)\big) \end{cases} \tag{2}$$

式中:z为服从高斯分布的随机噪声;$L(x)$为真实数据的重构误差;$L\big(G(z)\big)$为生成数据的重构误差;$\gamma \in [0,1]$为超参数,用于保持生成器G和鉴别器D的训练平衡;k和λ_k为超参数,用于维持γ的稳定。对于生成器G来说,其优化目标在于使生成报文的重构误差$L\big(G(z)\big)$尽可能小;而鉴别器D则不同,在保证真实报文的重构误差$L(x)$尽可能小的同时,最大化生成报文的重构误差$L\big(G(z)\big)$。

2 基于BEGAN的CAN入侵检测数据生成方法

本文提出的方法主要使用BEGAN生成车载CAN总线攻击报文,通过生成器与鉴别器之间的不断博弈,生成与真实车辆相匹配的车载CAN总线攻击报文。首先基于one-hot编码对原始CAN报文进行图像转换预处理,得到真实CAN图像;其次将真实CAN图像和随机噪声输入基于BEGAN的数据生成模型中进行训练,生成指定类型的攻击CAN图像;最后利用one-hot解码生成的攻击CAN图像得到攻击CAN报文。

2.1 CAN报文图像转换

CAN报文为一维时序数据,考虑到BEGAN在图像生成领域具有独特优势,因此通过one-hot编码进行升维,将CAN数据域从一维数据转换为二维CAN图像。图1展示了CAN数据域one-hot编码过程。首先,由于CAN数据域为十六进制,因此CAN数据域的每个元素都以16位的二进制数表示,使其中一位为1,其余位为0。例如:“D5 64 27 01 64 19 34 08”的第一个元素“D”,对应十六位二进制数中的第14位为1,其余位为0。最终,每条CAN数据域报文都将转换成[1,256]矩阵,按时间序列拼接CAN数据域矩阵,得到[n,256]矩阵,接着按图像尺寸为256进行裁剪,得到[m,256,256]矩阵,即m张真实CAN图像,完成CAN数据域的图像转换。

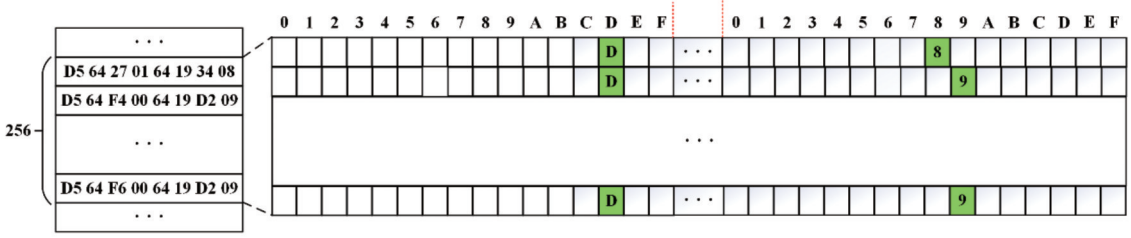


图1 CAN报文图像转换过程

2.2 模型构建与训练

通过one-hot编码对真实CAN报文进行图像转换后,将得到的真实CAN图像样本输入构建的CAN数据生成模型,生成入侵检测数据,如图2所示。首先将随机噪声输入生成器G,输出攻击CAN图像样本;此外将真实CAN图像样本和攻击CAN图像样本输入鉴别器D,鉴别器D对样本进行重构,输出重构误差;经过不断训练博弈,生成攻击CAN图像样本在分布上不断逼近真实CAN图像样本,直至模型达到纳什均衡;最后通过one-hot解码将生成的攻击CAN图像转换为攻击CAN报文,结合正常CAN报文,得到CAN增强数据集。

基于BEGAN构建的CAN数据生成模型,包括生成器G和鉴别器D。生成器G由3层反卷积神经网络组成,如图3(a)所示。生成器G对输入数据进行升维。图3(a)展示了生成器G将输入数据维度扩展到与真实CAN图像一致的升维过程。最后一层的激活函数为Tanh,其余各层的激活函数为Leaky_relu。生成器G以随机噪声为输入,将随机噪声转换至与真实CAN图像大小相同且极为相似的攻击CAN图像并输出。生成器G的优化目标为生成的攻击CAN图像的重构误差尽可能小。

鉴别器D是一个自编码器,由编码器和解码器组成,如图3(b)所示。编码器由3层卷积神经网络组成,编码器对输入数据进行降维。解码器由3层反卷积神经网络组成,解码器对输入数据进行升维。

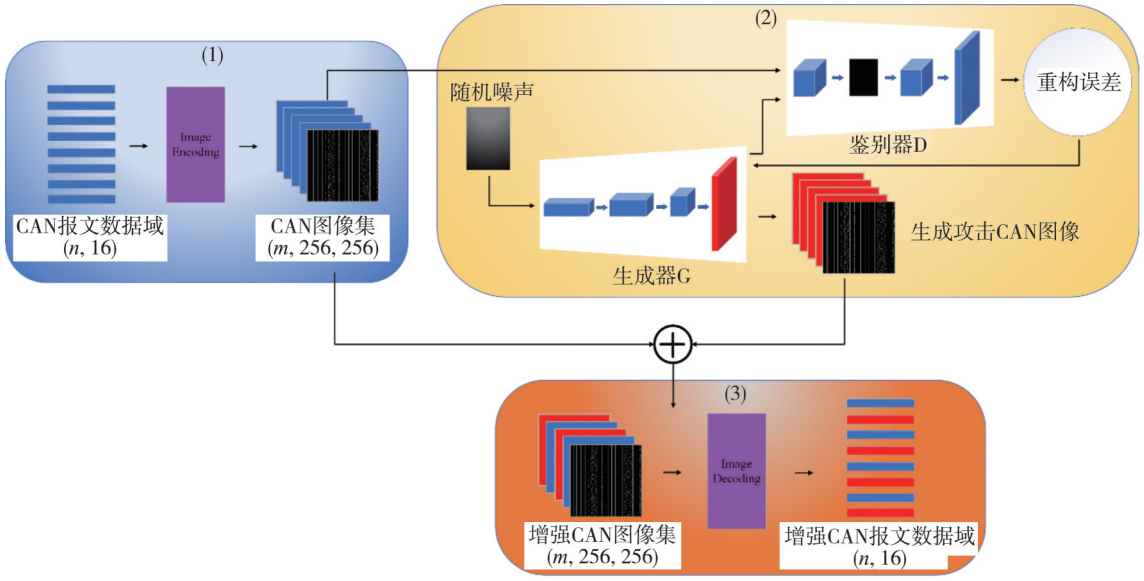
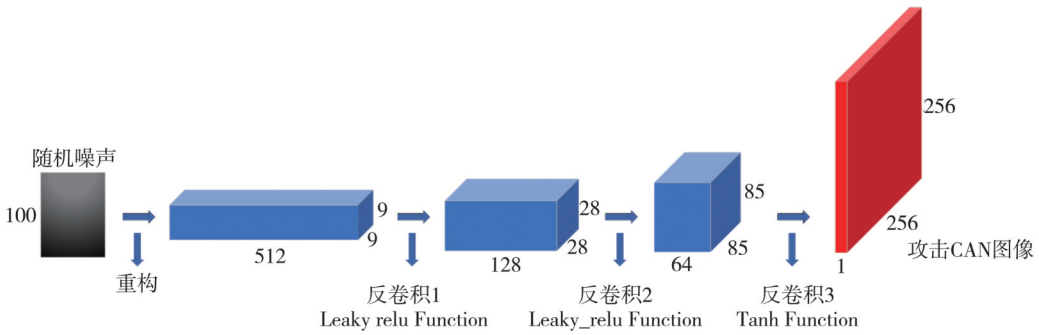
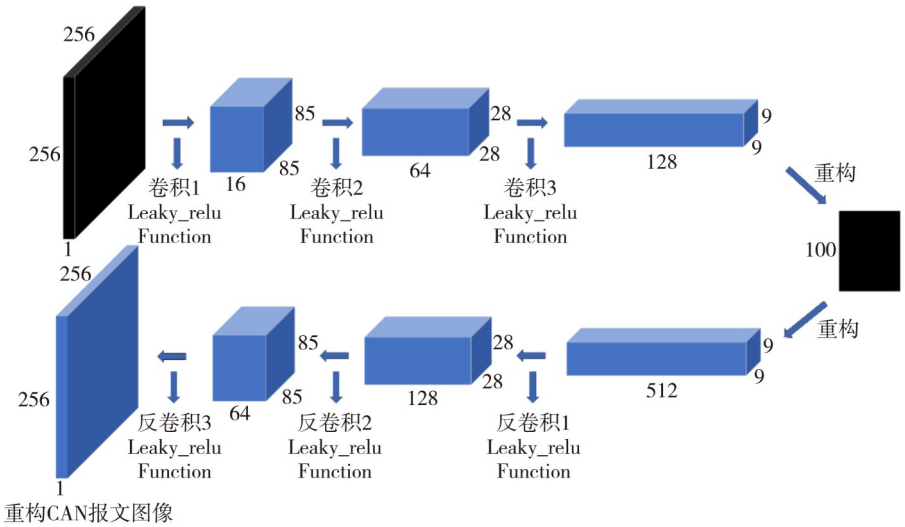


图2　基于BEGAN的入侵检测数据生成方法



(a) 生成器结构



(b) 鉴别器结构

图3　生成器与鉴别器结构

图3(b)展示了鉴别器D将输入数据维度变换至与真实CAN图像一致的重构过程。最后一层的激活函数为Tanh,其余各层的激活函数为Leaky_relu。鉴别器D以CAN图像为输入,基于编码器和解码器对输入CAN图像进行重构,得到重构CAN图像,通过对比重构前后CAN图像,输出重构误差。鉴别器D的优化目标为保证真实CAN图像样本重构误差尽可能小的同时,最大化攻击CAN图像样本的重构误差。

3 实车验证

基于BEGAN的入侵检测数据生成方法可用于CAN总线协议格式未知场景,本方法直接通过采集到的CAN总线报文进行模型训练,适用性更强。具体实验步骤如下。

(1)采集实车训练数据集。为保证生成CAN报文质量可靠,在CAN数据生成模型的训练过程中需要大量真实CAN报文数据。本文使用CAN分析仪,通过汽车的CAN端口获取实车CAN报文数据集,并对报文数据集进行one-hot编码图像化预处理。

(2)模型训练。将处理后的真实CAN图像数据集和随机噪声输入基于BEGAN的数据生成模型,通过训练过程中生成器G和鉴别器D的不断博弈,生成攻击CAN图像,并通过one-hot解码得到生成攻击CAN报文。

(3)生成数据质量评价。为验证生成CAN报文与真实CAN报文具有相似概率分布,可作为攻击CAN报文样本以解决数据不平衡问题,本文从特征图、t-Distributed Stochastic Neighbor Embedding(t-SNE)可视化、统计学分析和分类器验证角度评价生成CAN报文的数据质量。

3.1 数据集

实车数据采集整车连接如图4所示,通过CAN延长线将数据记录装置和汽车CAN网络相连,基于CAN分析仪,数据记录装置可以自动识别CAN速率,检测到待测车辆的CAN电平发送速率为500 kb/s,速率匹配成功之后,连续读取并记录CAN数据流。

由于本次实车实验采用的是静车实验,整车发动机点火但未启动,因此实验数据主要由雨刷信号、车门开闭信号、车窗信号、空调开闭信号以及安全带信号等电控单元数据构成。共采集得到210万条实车CAN报文,通过统计ID数据域格式,筛选提取ID为0x064的CAN报文共220 769条,ID为0x064的报文格式为[D5 64 X_1X_2 0X_3 64 19 X_4X_5 X_6X_7]。对报文数据集进行one-hot编码图像化预处理,得到共862张真实CAN图像,如图5所示。

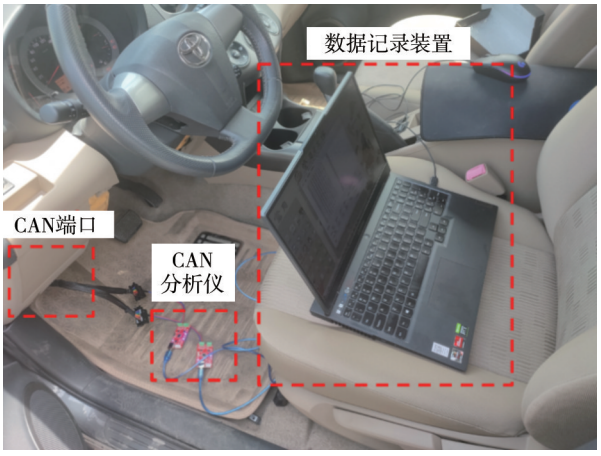


图4 整车连接图

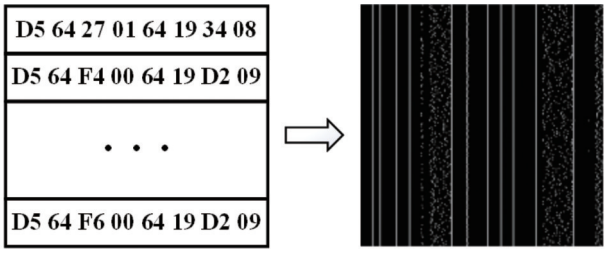


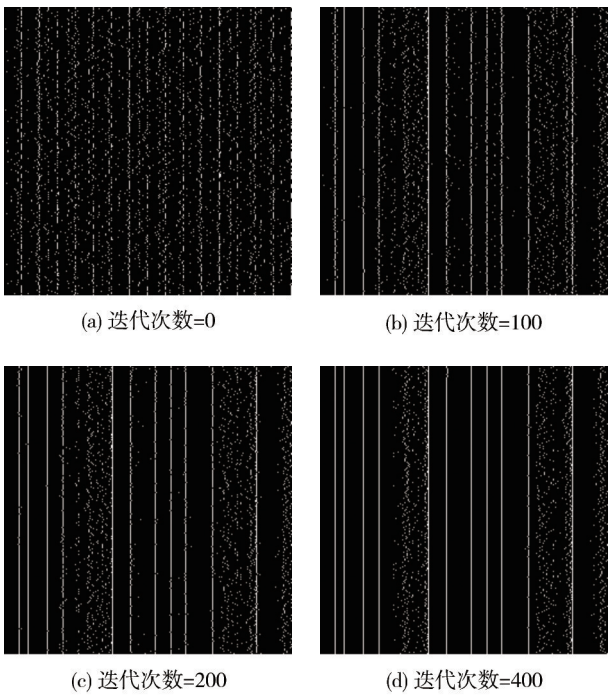
图5 CAN报文图像转换

3.2 模型训练

实验环境如下:主机硬件采用主频为3.30 GHz的AMD Ryzen 5 5600H,所使用的操作系统为Windows 10 64位系统。使用深度学习框架TensorFlow 2.7.0搭建了基于BEGAN的数据生成模型。在一辆真实汽车上进行模型训练和数据生成实验,分析了生成数据结果。将随机噪声输入生成器G,将真实样本和生成的攻击样本输入鉴别器D,用于基于BEGAN的数据生成模型的训练。采用Adam优化器,学习率为0.000 1,迭代次数为400,训练过程如图6所示。

从图6中可以看出,随着迭代次数的不断增加,生成CAN图像逐渐相似真实CAN图像。此外,利用one-hot解码将生成CAN图像转换为CAN报文。ID 0x064对应数据域有8个字节,统计训练过程中生成报文各字节的范围分布,并与真实报文各字节的范围分布进行对比,如图7所示。

从图7中可以看出:训练开始时,生成报文各字节均匀分布于0-255,如图7(a)所示;当训练次数达



(a) 迭代次数=0　(b) 迭代次数=100

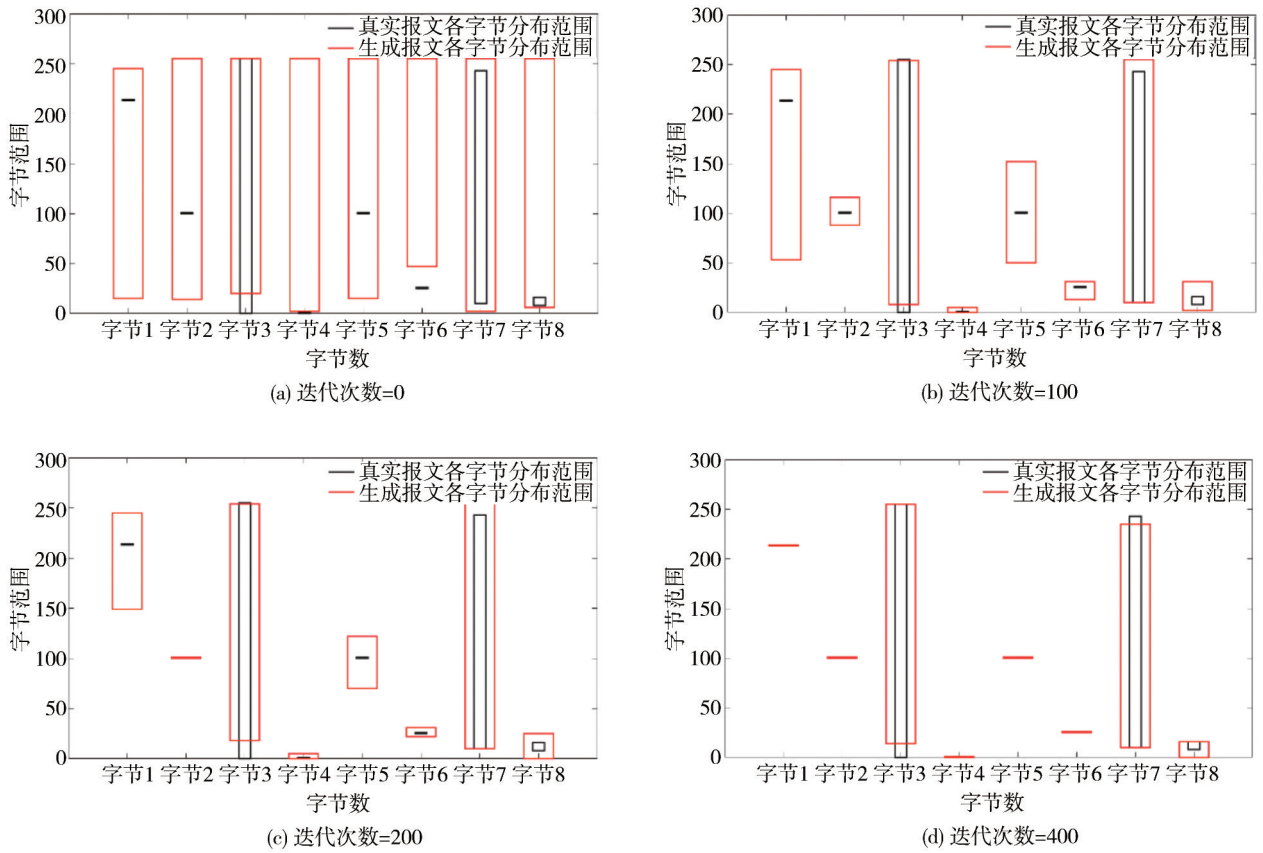
(c) 迭代次数=200　(d) 迭代次数=400

图6　数据生成模型训练过程

到100时,生成报文的字节2、字节3、字节4、字节6、字节7和字节8分布范围已逐渐逼近对应真实报文,如图7(b)所示;当训练次数达到200时,生成报文的字节2分布范围与真实报文完全重合,如图7(c)所示;当训练次数达到400时,生成报文的字节1、字节2、字节4、字节5和字节6分布范围与真实报文完全重合,其余的字节3、字节7和字节8分布范围与真实报文也基本重合,如图7(d)所示。最终训练得到的生成CAN报文各字节的分布范围与真实CAN报文重合度极高。

3.3　生成数据质量评价

基于训练后的数据生成模型生成ID 0x064的862张攻击CAN图像,通过one-hot解码得到共220 672条攻击CAN报文,部分报文数据如表1所示。为使生成报文可作为攻击样本以解决数据不平衡问题,需要保证生成CAN报文与真实CAN报文在格式上保持一致,在内容上有一定差异。因此,本文从特征图、t-SNE可视化、统计学分析和分类器验证角度对生成CAN报文的数据质量进行评价。



(a) 迭代次数=0　(b) 迭代次数=100

(c) 迭代次数=200　(d) 迭代次数=400

图7　生成CAN图像各字节训练过程

表1 基于BEGAN方法生成的部分ID 0x064报文

字节1	字节2	字节3	字节4	字节5	字节6	字节7	字节8
D5	64	FB	00	64	19	FE	0C
D5	64	EC	00	64	19	DA	0A
D5	64	17	01	64	19	3D	09
D5	64	3B	01	64	19	FD	09
D5	64	0E	01	64	19	72	03
D5	64	BF	01	64	19	39	0B

3.3.1 特征图

为便于统计CAN报文数据特征分布,对CAN报文各字节进行归一化处理,其次分别统计真实CAN报文和生成CAN报文的数据特征及频率,如图8所示。从图8中可以看出,生成CAN报文在连续特征分布上与真实CAN报文极为相近,这表明生成的CAN报文与真实CAN报文具有相似的特征分布。

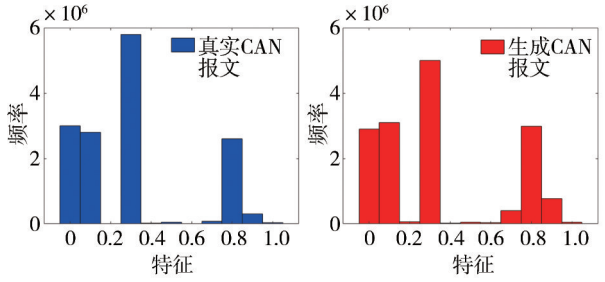


图8 数据特征分布图

3.3.2 t-SNE可视化

为了更加直观展示生成CAN报文与真实CAN报文分布相似,本文采用t-分布随机近邻嵌入(t-SNE)算法进行可视化分析。通过将高维数据降维至2D平面来可视化生成CAN报文与真实CAN报文的分布特征。t-SNE算法首先计算高维空间中数据点之间的相似度,然后在低维空间中为每个数据点找到一个新的位置,并计算低维空间中数据点之间的相似度,最后以梯度下降法最小化高维空间和低维空间中概率分布之间的KL散度[28]。

图9显示了经t-SNE算法降维后的生成CAN报文和真实CAN报文的数据特征分布。从图9中可以看出,本文所提出的方法可以生成与真实CAN报文分布相似的数据。

3.3.3 统计学分析

为验证生成CAN报文与真实CAN报文相似但不相同,本文比较了特征的最大值、最小值、均值和均方差,如表2所示。从表2中可以看出,生成CAN报文与真实CAN报文的均值差值接近于0,这表明两者极为相似,同时两者均方差差值较大,这表明两者仍存在差异。

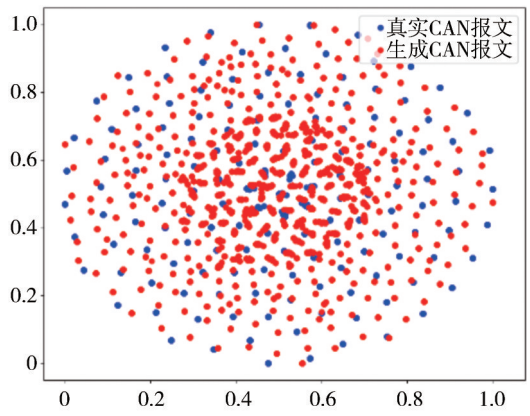


图9 t-SNE可视化CAN增强数据集

表2 统计学分析比较

特征	真实CAN报文				生成CAN报文			
	最大值	最小值	平均值	均方差	最大值	最小值	平均值	均方差
字节1	213	213	213	0	213	213	213	0
字节2	100	100	100	0	100	100	100	0
字节3	255	0	149.38	7 496.85	255	14	143.48	3 543.93
字节4	1	0	0.29	0.21	1	0	0.23	0.45
字节5	100	100	100	0	100	100	100	0
字节6	25	25	25	0	25	25	25	0
字节7	250	0	123.34	5 317.49	245	1	125.62	5 781.88
字节8	16	8	10.75	5.17	15	0	9.80	9.36

3.3.4 分类器验证

为验证本方法生成的CAN报文可作为攻击样本以解决数据不平衡问题,本节将展示增强数据集用于改进基于机器学习的入侵检测分类器的检测性能。为保证测试结果可靠,采用支持向量机(SVM)、随机森林(RF)、最邻近分类器(KNN)和梯度提升决策树(GBDT)4种分类器。对于训练数据集,使用实车采集的CAN总线报文作为正常样本,分别使用人工随机变异和本方法生成攻击样本;对于测试数据,结合人工随机变异和本方法生成的攻击样本进行测试。人工随机变异通过统计各ID数据域各字节数据变化规律,对存在变化的字节数据进行随机变异,其余字节数据保持不变,产生攻击样本。将采集到的210万条实车数据作为正常样本进行测试,并根据ID进行分类保存。分别通过人工随机变异和本方法生成攻击样本,训练不同入侵检测算法的分

类器。

实验中,每个ID的10 000条样本作为训练数据集,包括6 000条正常样本和4 000条攻击样本。攻击样本分别由人工随机变异和本方法生成。测试数据由5 000条人工随机变异和5 000条本方法生成的攻击样本组成。利用python 3.9和相关工具箱实现了基于SVM、RF、KNN、GBDT算法的分类器。

本文采用准确率(Accuracy,Acc)作为分类器的评估指标,计算公式如式(3)所示。

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \tag{3}$$

式中:*TP*为正确分类的正常样本数;*FN*为错误分类的异常样本数;*TN*为正确分类的异常样本数;*FP*为错误分类的正常样本数。

从中选择10条不同ID的CAN报文训练分类器,对应10条ID的CAN报文格式如表3所示。通过人工随机变异和本方法生成的攻击样本进行测试,分别计算准确率,分类器验证结果如表4所示。从表4中可以看出,与原始数据集相比,基于增强数据集训练的分类器准确率有所提高,说明使用增强数据集可以提高分类器性能。不同分类器的准确率均有提高同时也表明本方法生成的增强数据集泛化性较强,可适用于不同场景。

最后,为了验证本文方法的优越性,将本文方法(BEGAN)与传统的随机过采样技术(ROS)[16]、合成少数过采样技术(SMOTE)[17]、SMOTE-ENN[20]、自适应合成过采样算法(ADASYN)[21]进行了比较,仍然使用4种分类器进行验证,利用不同数据增强算法生成的CAN报文构建训练集,不同过采样算法对比结果如表5所示。

从表5中可以看出,本文方法(BEGAN)可以提高入侵检测分类器准确率,具有最高准确率。从原理分析,ROS算法本质上属于简单复制,不能生成实质性数据,容易造成模型过拟合问题[29];SMOTE算法采用最近邻法生成少数样本,容易造成数据重复冗余[30];SMOTE-ENN算法针对高维数据效果不佳[31];ADASYN算法使用T分布自动合成少数样本,容易受到离群点影响[32]。而本文方法通过生成对抗网络拟合原始CAN报文数据分布,生成的CAN报文数据质量较高,适合作为攻击样本以解决入侵检测数据不平衡问题。与上述过采样算法相比,本文方法训练的入侵检测分类器准确率更高,具有明显优势。

表3　选取ID对应CAN报文格式

ID	报文格式	ID	报文格式
064	D5 64 X_1X_2 $0X_3$ 64 19 X_4X_5 X_6X_7	2D5	33 DB X_1X_2 $0X_3$ 00 $0X_5$ X_6X_7 00
0BA	05 F7 X_1X_2 X_3X_4 00 00 00 00 00	3B3	03 X_1X_2 X_3X_4 00 00 00 00 00
2C1	08 FF X_1X_2 X_3X_4 X_5X_6 X_7X_8 00 X_9X_{10}	4C3	04 $0X_1$ 12 05 X_2X_3 X_4X_5 00 X_6X_7
2C4	03 X_1X_2 00 X_3X_4 00 80 13 X_5X_6	620	10 64 X_1X_2 $0X_3$ 30 60 X_4X_5 50
2D0	06 X_1X_2 09 00 10 00 F3 X_3X_4	624	1A 00 43 X_1X_2 X_3X_4 49 40 X_5X_6

表4　不同分类器验证结果

项目	*Acc*			
	SVM	RF	KNN	GBDT
原始数据集	71%	70%	68%	74%
增强数据集	88%	94%	99%	95%

表5　不同过采样算法准确率对比

算法	*Acc*			
	SVM	RF	KNN	GBDT
ROS	72%	72%	69%	74%
SMOTE	73%	73%	70%	76%
SMOTE-ENN	73%	73%	70%	76%
ADASYN	72%	73%	69%	75%
BEGAN	88%	94%	99%	95%

4　结论

本文提出了一种基于BEGAN的CAN入侵检测数据生成方法。本方法基于one-hot编码将CAN报文特征图像化,增加了生成样本与真实样本的相似性,提高了模型的泛化性与样本生成速率,避免因车载CAN报文特征稀疏导致的模型训练难以收敛问题。通过将真实CAN报文和随机噪声输入鉴别器和生成器,得到大量符合车载CAN网络特性的攻击报文,解决了传统CAN入侵检测方法难以获取攻击样本而导致的数据不平衡问题。通过采集实车数据作为样本训练基于BEGAN的数据生成模型,从特征

图、t-SNE可视化、统计学分析和分类器验证角度对生成CAN报文的数据质量进行评价。实验结果表明生成CAN报文与真实CAN报文在格式上一致,在内容上存在差异,满足攻击样本的基本特征。使用本方法生成的增强数据集可以提高入侵检测分类器准确率,适用性更强。与传统过采样算法含随机过采样(ROS)、合成少数过采样(SMOTE)、SMOTE-ENN、自适应合成过采样(ADASYN)相比,准确率更高,具有明显优势。本方法还可以应用于基于机器学习的入侵检测算法评估。

参考文献

[1] JO H J, CHOI W. A survey of attacks on controller area networks and corresponding countermeasures[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(7): 6123-6141.

[2] RATHORE R S, HEWAGE C, KAIWARTYA O, et al. In-vehicle communication cyber security: challenges and solutions[J]. Sensors, 2022, 22(17): 6679.

[3] KAROPOULOS G, KAMBOURAKIS G, CHATZOGLOU E, et al. Demystifying in-vehicle intrusion detection systems: a survey of surveys and a meta-taxonomy[J]. Electronics, 2022, 11(7): 1072.

[4] REN K, WANG Q, WANG C. et al, The security of autonomous driving: threats, defenses, and future directions[J]. Proceedings of the IEEE, 2020, 108(2): 357-372.

[5] ALDHYANI T H H, ALKAHTANI H. Attacks to automatous vehicles: a deep learning algorithm for cybersecurity[J]. Sensors, 2022, 22(1): 360.

[6] ALALWANY E, MAHGOUB I. Classification of normal and malicious traffic based on an ensemble of machine learning for a vehicle CAN-network[J]. Sensors, 2022, 22(23): 9195.

[7] 刘蓬勃,彭海德,赵剑,等. 汽车CAN网络的入侵检测模型及装置研究[J]. 实验技术与管理, 2022, 39(3): 126-131.
LIU P B, PENG H D, ZHAO J, et al. Research on intrusion detection model and device of automobile controller area network (CAN) [J]. Experimental Technology and Management, 2022, 39(3): 126-131.

[8] YUAN L H, LI X X. WSG-InV: weighted state graph model for intrusion detection on in-vehicle network[C]. 2021 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2021.

[9] MARTINELLI F, MERCALDO F, NARDONE V, et al. Car hacking identification through fuzzy logic algorithms[C]. 2017 IEEE International Conference on Fuzzy Systems (FUZZ). IEEE, 2017, 7.

[10] TIAN D X, LI Y Z, WANG Y P, et al. An intrusion detection system based on machine learning for CAN-bus[C]. 2017 Industrial Networks and Intelligent Systems (INISCOM). Social-Informatics and Telecommunications Engineering, 2017, 221: 285-294.

[11] ALSAADE F W, AL-ADHAILEH M H. Cyber attack detection for self-driving vehicle networks using deep autoencoder algorithms[J]. Sensors, 2023, 23(8): 4086.

[12] PARK S, CHOI J Y. Hierarchical anomaly detection model for in-vehicle networks using machine learning algorithms[J]. Sensors, 2020, 20(14): 3934.

[13] ALIWA E, RANA O, PERERA C, et al. Cyberattacks and countermeasures for in-vehicle networks[J]. ACM Computing Surveys, 2021, 54(1): 21.

[14] YUAN L X, YU S Y, YU S Y, et al. A data balancing approach based on generative adversarial network[J]. Future Generation Computer Systems-the International Journal of Escience, 2023, 141: 768-776.

[15] ANDRESINI G, APPICE A, DE ROSE L, et al. GAN augmentation to deal with imbalance in imaging-based intrusion detection[J]. Future Generation Computer Systems-the International Journal of Escience, 2021, 123: 108-127.

[16] EBRAHIMY H, MIRBAGHERI B, MATKAN A A, et al. Effectiveness of the integration of data balancing techniques and tree-based ensemble machine learning algorithms for spatially-explicit land cover accuracy prediction[J]. Remote Sensing Applications: Society and Environment, 2022: 100785.

[17] ZHANG H P, HUANG L L, WU C Q, et al. An effective convolutional neural network based on smote and gaussian mixture model for intrusion detection in imbalanced dataset[J]. Computer Networks, 2020, 177: 107315.

[18] 周志豪,陈磊,伍翔,等. 基于SMOTE-SDSAE-SVM的车载CAN总线入侵检测算法[J]. 计算机科学,2022,49(S1):562-570,801.
ZHOU Z H, CHEN L, WU X, et al. SMOTE-SDSAE-SVM based vehicle CAN bus intrusion detection algorithm[J]. Computer Science,2022,49(S1):562-570,801.

[19] 孙扬威,戚湧. 基于聚类混合采样与PSO-Stacking的车载CAN入侵检测方法[J]. 计算机工程,2023,49(1):138-145.
SUN Y W, QI Y. Intrusion detection method for in-vehicle CAN based on cluster mixed sampling and PSO-Stacking[J]. Computer Engineering, 2023, 49(1):138-145.

[20] MANJU B R, NAIR A R. Classification of cardiac arrhythmia of 12 lead ECG using combination of SMOTEENN, XGBoost and machine learning algorithms[C]. 2019 IEEE International Symposium on Embedded Computing and System Design (ISED). IEEE, 2019: 48-54.

[21] BAE S Y, LEE J, JEONG J, et al. Effective data-balancing methods for class-imbalanced genotoxicity datasets using machine learning algorithms and molecular fingerprints[J]. Computational Toxicology, 2021, 20: 100178.

[22] DENG C Y, DENG Z H, LU S, et al. Fault diagnosis method for imbalanced data based on multi-signal fusion and improved deep convolution generative adversarial network[J]. Sensors, 2023, 23(5): 2542.

(下转第1456页)