基于深度生成模型的半监督入侵检测算法

曹卫东 许志香 王 静
(中国民航大学计算机科学与技术学院 天津 300300)

摘 要 针对基于监督学习的入侵检测算法所需训练样本标签难以收集、无监督学习算法准确度不高,以及网络入侵检测中的高维数据处理的问题,提出一种基于深度生成模型的半监督入侵检测方法。该方法旨在构建合理有效的目标函数,提高模型的分类准确率及泛化能力。首先,用变分自编码(Variational Auto-Encoder,VAE)将高维原始数据双向映射至低维空间,以获得原始数据的低维表示;然后,用数据的生成模型提高单独使用有标签数据时的分类准确率。实验表明,该方法利用少量有标记数据能够取得较高的检测准确率。

关键词 入侵检测,生成模型,半监督,变分自编码
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.03.029

Intrusion Detection Based on Semi-supervised Learning with Deep Generative Models

CAO Wei-dong XU Zhi-xiang WANG Jing
(College of Computer Science and Technology,Civil Aviation University of China,Tianjin 300300,China)

Abstract Aiming at the difficulties that training samples of intrusion detection algorithms based on supervised learning are insufficient,and unsupervised algorithms have low detection rate,a new semi-supervised intrusion detection method based on deep generative models was proposed. This method aims to improve the detection accuracy and the generalization ability of the model by constructing an effective objective function. First,variational auto-encoder in the model is employed to map the vector of raw data from the high-dimensional space to low-dimensional,and the corresponding optimal low-dimension representation of raw can be obtained. Then,the generative model is used to improve the classification accuracy by only using the labeled samples. Experiments show that this method can achieve high accuracy while using a limited number of labeled samples.

Keywords Intrusion detection,Generative model,Semi-supervised,Variational autoencoder

1 引言

随着网络与信息技术日新月异的发展,网络安全问题已经成为一个备受关注的重大问题。入侵检测(Intrusion Detection)是一种积极主动的安全防护技术[1],通过分析网络流量或系统审计记录发现入侵行为,当发现可疑通信时发出告警或采取防御措施以保证系统安全。

Denning[2]于1987年首次提出入侵检测,如何迅速有效地发现各类新的入侵行为一直是各界关注的焦点。利用机器学习的方法进行入侵检测是当下比较流行的趋势[3]。机器学习分为两类:有监督学习算法和无监督学习算法。利用有监督学习算法进行入侵检测时虽然准确率高,但所需训练样本需要带有大量先验信息,而且仅能检测已知的攻击类型[4]。无监督算法根据数据的相似性进行分组[5],不要求训练样本带有任何先验信息[6],能够有效地检测未知攻击。无监督虽然弥补了监督学习中需要先验知识的不足,但检测精度不高。针对监督与无监督学习的缺陷,文献[7-9]采用半监督学习(Semi-Supervised Learning,SSL)方法,利用少量有标签数据获得大规模的训练数据,一定程度上弥补了有监督学习与无监督学习的不足。已有的半监督入侵检测算法虽然避免了人工标记大量样本的工作,但没有使用有效的方法构造多层网络,容易导致欠拟合,并且检测精度和异常数据的区分度仍有待提高[10]。

针对以上问题,本文提出一种基于深度生成模型的半监督入侵检测算法(Semi-Supervised with Deep Generative Models,SS-DGM),将深度神经网络与概率建模相结合,用数据的生成模型来提高单独使用有标签数据时的分类准确率。首先,利用生成模型中的变分自编码[11]技术将有标签和无标签数据在原空间中的高维特征表示转换成新特征空间的低维表示,对低维特征向量加一个约束使之服从高斯正态分布,得到隐变量 z;进而利用生成模型学习到的特征向量 z 对标记数据进行分类,计算分类误差并进行数据重构,无标记数据用 z 预测类标签[12],然后用 z 和预测得到的标签进行数据重构。经实验验证,该方法具有较高的鲁棒性和检测精度,并且大大

到稿日期:2018-01-18 返修日期:2018-05-23 本文受机载网络安全防护适航审定技术研究项目(AADSA0018)资助。
曹卫东(1964—),女,博士,副教授,CCF会员,主要研究方向为数据库与数据挖掘、民航信息系统软件可靠性;许志香(1993—),女,硕士生,主要研究方向为网络安全、深度学习,E-mail:358459893@qq.com(通信作者);王 静(1980—),女,博士,讲师,主要研究方向为网络安全。

减少了对先验知识的需求，增强了实用性。

2 半监督学习

Merz 等[13]于 1992 年提出 SSL，并首次将 SSL 用于分类问题。其借助无标记样本训练有标记样本，获得了比单独使用有标记样本训练得到的分类器性能更优的分类器，弥补了有标记样本的缺陷。

2.1 基于生成模型的半监督分类算法

生成式方法假设所有数据(无论是否有标记)都由一个潜在的模型“生成”[14]。给定样本数据 $X=\{x^{(i)}\}_i^N=1$，将其真实类标记为 $y\in Y$，其中 $Y=\{1,\cdots,L\}$。假设样本由高斯混合模型生成，且每个类别都对应一个高斯混合成分[14]，换言之，数据样本按式(1)的概率密度函数生成：

$$p(x)=\sum_{i=1}^{N}\alpha_i\cdot p(x|\mu_i,\Sigma_i) \tag{1}$$

其中，混合系数 $\alpha_i\geqslant 0$，$\sum_{i=1}^{L}\alpha_i=1$；$p(x|\mu_i,\Sigma_i)$是样本 x 属于第 i 个高斯混合成分的概率；μ_i 和 Σ_i 为该高斯混合成分的参数。

令 $f(x)\in Y$ 表示模型 f 对 x 的预测标记，$\Theta\in(1,2,\cdots,L)$表示样本 x 隶属的高斯混合成分，由最大化后验概率可知：

$$\begin{aligned}f(x)&=\arg\max_{j\in Y}p(y=j|x)\\&=\arg\max_{j\in Y}\sum_{i=1}^{L}p(y=j,\Theta=i|x)\\&=\arg\max_{j\in Y}\sum_{i=1}^{L}p(y=j|\Theta=i,x)\cdot p(\Theta=i|x)\end{aligned} \tag{2}$$

其中，$p(y=j|\Theta=i,x)$为 x 由第 i 个高斯混合成分生成且类别为 j 的概率，因此需要使用有标签样本才能获得。

式(3)为 x 由第 i 个高斯混合成分生成的后验概率，不涉及标签，因此有标签样本和无标签样本均可，通过引入大量的无标签数据，能够获得更准确的样本概率估计值。这一项的估计可望由于数据量的增长而更为精确，由此可以看出无标签数据可以辅助提高分类器的性能。

$$p(\Theta=i|x)=\frac{\alpha_i\cdot p(x|\mu_i,\Sigma_i)}{\sum_{i=1}^{L}\alpha_i\cdot p(x|\mu_i,\Sigma_i)} \tag{3}$$

2.2 变分推断

2.1 节中提到所有的样本都由一个潜在模型“生成”，这个潜在模型即某个随机采样过程。在入侵检测环境中，一条连接记录代表一个样本 $x^{(i)}$，$z^{(i)}$ 代表由 $x^{(i)}$ 生成的隐变量。随机采样过程分为两个步骤[11]：1)从先验分布函数 $p_\theta(z)$采样样本 $z^{(i)}$；2)根据条件概率分布函数 $p_\theta(x|z)$采样得到样本 $x^{(i)}$。采样过程如图 1 所示。入侵检测的目标是用 z 判断网络中的连接是否恶意，下面主要阐述如何通过样本 x 生成隐变量 z。

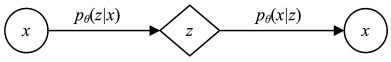

图 1 变分随机采样原理图

Fig. 1 Variational random sampling

通过观察到的变量 x 来估计隐变量 z，即求解式(4)：

$$p_\theta(z|x)=p_\theta(x|z)p_\theta(z)/p_\theta(x) \tag{4}$$

由于真实数据分布难以获得，通常采用近似推断法来逼近其真实值，典型方法为变分推断(Variational Inference)。变分推断法通常使用已知的简单分布来近似逼近需要推断的复杂分布，并通过限制近似分布的类型来达到一种局部最优；同时，它又是一种具有确定解的近似后验分布[15]。用 $q_\phi(z|x)$逼近真实后验概率 $p_\theta(z|x)$。生成模型的目标是生成一些具有多样性的样本，利用极大似然法来估计可学习的参数，常取式(5)的对数似然函数：

$$\log p_\theta(x^{(1)},\cdots,x^{(N)})=\sum_{i=1}^{N}\log p_\theta(x^{(i)}) \tag{5}$$

针对某单个样本点，其目标是最大化式(6)中的边缘对数似然函数：

$$\begin{aligned}\log p_\theta(x^{(i)})=&D_{\mathrm{KL}}(q_\phi(z|x^{(i)})\parallel p_\theta(z|x^{(i)}))+\\&\mathcal{L}(\theta,\phi;x^{(i)})\end{aligned} \tag{6}$$

其中，$D_{\mathrm{KL}}(q_\phi(z|x^{(i)})\parallel p_\theta(z|x^{(i)}))$为 KL 散度公式，用于衡量两个分布的相似度，其值非负，值越小说明两个分布越接近。用变分推断法优化式(7)使其接近于 0，从而使两个分布函数相似，因此须最大化式(6)中的 $\mathcal{L}(\theta,\phi;x^{(i)})$，称其为变分下界(Lower Bound)。

$$D_{\mathrm{KL}}(q_\phi(z|x^{(i)})\parallel p_\theta(z|x^{(i)})) \tag{7}$$

对于单个样本点，目标函数为：

$$\begin{aligned}\mathcal{L}(\theta,\phi;x^{(i)})&=\mathbb{E}_{q_\phi(z|x)}[-\log q_\phi(z|x)+\log p_\theta(x,z)]\\&=-D_{\mathrm{KL}}(q_\phi(z^{(i)}|x)\parallel p_\theta(z))+\\&\quad\mathbb{E}_{q_\phi(z|x^{(i)})}(\log p_\theta(x^{(i)}|z))\end{aligned} \tag{8}$$

由于采样过程取决于模型的参数，因此这个过程不可微，从而不能对模型参数寻优。VAE 利用重构参数这一技巧巧妙地解决了这一问题。

2.3 变分自编码

自编码网路是由 Hinton 提出的一种用于学习高效编码的人工神经网络，通过学习获得数据集的压缩编码，它采用自适应、多层编码网络将高维原始数据转换成低维表示[16]。VAE 经过自编码学得数据的低维表示之后，给其加入一个约束 ψ 项使其服从高斯正态分布，得到隐变量 z，这样在网络训练完成后就可以从高斯正态分布中采样一个样本 z。图 2 给出了 VAE 的工作原理，一方面通过 z 结合少量标记数据训练分类器，另一方面用 z 结合所有训练样本生成新样本，并用生成的新样本来提高模型的泛化能力。

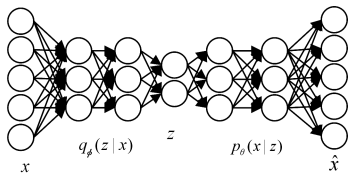

图 2 基于生成模型的 VAE 结构图

Fig. 2 Structure of VAE based on generative model

本文用多层感知机(Multilayer Perceptron，MLP)作为 VAE 的编码方式。假设 $q_\phi(z|x)$为具有对角线协方差结构的多元高斯分布，对其取对数之后得：

$$\log q_\phi(z|x^{(i)})=\log\mathcal{N}(z;\mu^{(i)},\sigma^{2(i)}I) \tag{9}$$

其中，$\mu^{(i)}$ 和 $\sigma^{(i)}$ 分别代表样本 $x^{(i)}$ 经过 MLP 编码之后的均值和方差。令 $z^{(i)}=\mu^{(i)}+\sigma^{(i)}\cdot\varepsilon$，其中 $\varepsilon\sim\mathcal{N}(0,I)$，经贝叶斯变分推导，式(6)中的变分下界转化为：

$$\begin{aligned}&\frac{1}{2}\sum_{j=1}^{J}(1+\log((\sigma_j^{(i)})^2-(\mu_j^{(i)})^2)-(\sigma_j^{(i)})^2)+\\&\log p_\theta(x^{(i)}|z^{(i)})\end{aligned} \tag{10}$$

其中，J 是隐变量 z 的维度。

图 3 形象化地描述了 VAE 重构参数的技巧。

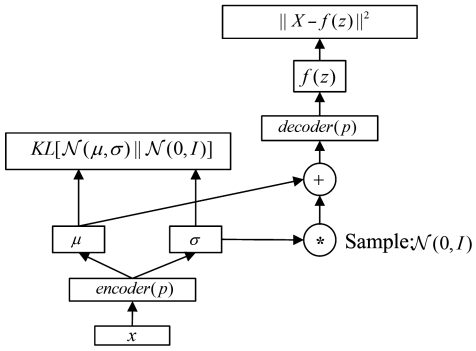

图 3　VAE 重构模型

Fig. 3　VAE reconstruction model

3　半监督入侵检测算法

本文提出的基于 SS-DGM 的入侵检测算法将深度神经网络与概率建模相结合，借此构建合理有效的目标函数来提高模型的分类准确率与泛化能力。给定有标签样本 $(X,Y)=\{(x_1,y_1),\cdots,(x_N,y_N)\}$，其中 $x^{(i)}\in\mathbb{R}^D$，$y_i\in\{1,\cdots,L\}$，假定有标签样本服从 $p_l(x,y)$ 分布，无标签样本服从 $p_u(x)$ 分布。

3.1　模型设计

基于 SS-DGM 的入侵检测的总体架构如图 4 所示。

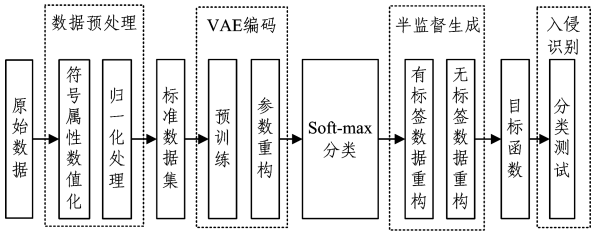

图 4　SS-DGM 流程图

Fig. 4　Flowchart of SS-DGM

SS-DGM 算法的步骤如下：

Step1　数据预处理，即对数据集中的符号性属性特征进行数值化，之后对数据进行归一化处理；

Step2　将预处理之后的数据作为 VAE 的输入，并建立高维空间到低维空间的双向映射，VAE 的结构设计见 3.2 节；

Step3　VAE 编码训练所有样本，得到的隐变量 z 结合少量有标签数据进行监督学习，然后用 z 和标签 y 共同生成 x_l；

Step4　对于无标签数据，利用 z 预测其标签属于每一个类别的概率 $\pi_\phi(x)$；

Step5　将无标签样本的标签作为除 z 之外的另一个隐变量，设其类别 y 服从多项式分布，即 $p(y)=Cat(y|\pi_\phi(x))$，然后用 z 和 y 共同生成样本 x_u；

Step6　利用 x_l 和 x_u 计算模型重构误差及 Step3 中的分类误差，调整参数，并训练模型直至收敛。

3.2　VAE 网络结构的设计

VAE 的编码和解码方式有很多种，根据入侵检测的数据类型，选择相对简单的 MLP 编码方式，用具有对角线协方差结构的多元高斯作为 MLP 的编码器和解码器。MLP 编码结构如式(11)所示：

$$\begin{cases}\log q_\phi(z|x)=\log\mathcal{N}(z;\mu_\phi(x),\mathrm{diag}(\sigma_\phi^2(x)))\\ \log q_\phi(z|y,x)=\log\mathcal{N}(z;\mu_\phi(y,x),\mathrm{diag}(\sigma_\phi^2(x)))\\ q_\phi(y|x)=Cat(y|\pi_\phi(x))\\ \text{where}\\ h=\tanh(W_1x+b_1)\\ \mu=W_2h+b_2\\ \log\sigma^2=W_3h+b_3\\ z=\mu+\sigma\cdot\varepsilon,\varepsilon\sim\mathcal{N}(0,I)\end{cases}\tag{11}$$

其中，$\phi=\{W_1,b_1,W_2,b_2,W_3,b_3\}$ 是编码器的各层参数值。

对有标签数据和无标签数据分别计算代价损失函数，优化的目标函数是变分下界，有标签数据和无标签数据的变分下界分别如式(12)和式(13)所示：

$$\mathcal{L}(x,y)=\mathbb{E}_{q_\phi(z|x,y)}[\log p_\theta(x|y,z)+\log p_\theta(y)+\log p_\theta(z)-\log q_\phi(y,z|x)]\tag{12}$$

$$\mathcal{U}(x)=\mathbb{E}_{q_\phi(y,z|x)}[\log p_\theta(x|y,z)+\log p_\theta(y)+\log p_\theta(z)-\log q_\phi(y,z|x)]\tag{13}$$

MLP 的解码结构如式(14)所示：

$$\begin{cases}\log p_\theta(x|z)=\log\mathcal{N}(x;\hat{\mu},\hat{\sigma}^2I)\\ \text{where}\\ \hat{h}=\tanh(W_4z+b_4)\\ \hat{\mu}=W_5\hat{h}+b_5\\ \log\hat{\sigma}^2=\tanh(W_6\hat{h}+b_6)\end{cases}\tag{14}$$

其中，$\theta=\{W_4,b_4,W_5,b_5,W_6,b_6\}$ 是解码器各层的参数值。

经过 VAE 编码，有标签样本得到隐变量 z，利用式(15)进行分类预测。

$$y_{\text{pred}}=\arg\max(soft\ \max(W_7z+b_7))\tag{15}$$

利用式(16)计算交叉熵，得到分类误差损失。

$$\log q_\phi(y|z)=y\log y_{\text{pred}}+(1-y)\log(1-y_{\text{pred}})\tag{16}$$

模型整体的代价损失函数如式(17)所示：

$$cost=\sum_{((x,y)\sim p_l)}\mathcal{L}(x,y)+\sum_{(x\sim p_u)}\mathcal{U}(x)+\alpha\cdot\mathbb{E}_{p_l(x,y)}[\log q_\phi(y|x)]\tag{17}$$

其中，系数 α 用于控制分类模型与生成模型的权重。

4　实验与分析

实验数据集采用 NSL-KDD[17]，该数据集主要有 4 种攻击类型：DOS(Denial of Service)拒绝服务、Probe 端口扫描、R2L(Remote-to-Local)远程到本地的攻击，以及 U2R(User-to-Root)未经授权且试图获取超级用户和 root 权限访问。每种攻击类型又可划分为相应的子类型，详细信息如表 1 所列。

表 1　NSL-KDD 属性描述

Table 1　Attribute description of NSL-KDD

DOS	Probe	U2R	R2L
Back	IP sweep	Perl	FTP write
Land	Nmap	Buffer overflow	Guess password
Neptune	Port sweep	Load module	Imap
Ping of death	Satan	Rootkit	Multi HOP
Smurf	Saint	Sqlattack	Phf
Teardrop		Xterm	SPY
			Wareclient
			Warezmaster

4.1 数据预处理

NSL-KDD 数据集中的每条连接记录由 41 个属性组成，其中包含 38 个数字型属性和 3 个符号型属性。因此，数据预处理首先将类标签和符号型属性数值化，然后对所有数值属性进行归一化处理。

1)符号型属性数值化

属性 protocal_type 有 3 种不同的取值，即“tcp”“udp”“icmp”。用 OneHot 编码将其扩展到 3 维，如“tcp”用[1,0,0]表示，“udp”用[0,1,0]表示，“icmp”用[0,0,1]表示。同理，service 属性的 70 种符号型取值和 flag 的 11 种符号型取值可以建立类似符号型取值和数值型取值间的映射。41 维特征经过 OneHot 编码后，变为 122 维特征。

2)归一化

对原始数据用最小-最大化方法进行归一化处理，使各属性取值处于同一数量级，有利于综合对比评价。根据 $x'=\frac{x-min}{max-min}$ 将数据型数据线性映射到[0,1]区间，其中 x 是属性值，min 是该属性的最小取值，max 是该属性的最大取值。

4.2 模型参数设置和评估标准

本实验在 Intel CPU 1.70GHz、4GB 内存、64b 硬件环境和 Windows7 操作系统上，使用 python3.5 和深度学习开源框架 TensorFlow 编码实现。将 20% 的 NSL-KDD 作为训练集，记为 Train-20，随机从原 NSL-KDD 中选择 20% 的数据作为测试集。实验中每种攻击类型的分布如图 5 所示。

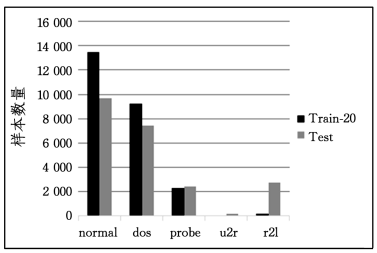

图 5 训练集和测试集的样本分布图

Fig. 5 Sample distribution in training and testing datasets

本文利用 VAE 对原数据中的高维特征向量进行压缩处理，使其映射到一个低维的空间，VAE 采用 MLP 编码。预处理之后，NSL-KDD 的属性特征为 122 维。因此，MLP 的输入层节点数为 122，输出层节点数为隐变量维度。

在入侵检测性能评估对比实验中，采用准确率、检测率和召回率作为评价指标来衡量本文所提方法的性能。准确率(Accuracy)、检测率(Detection Rate)和召回率(Recall Rate)的定义如下：

$$AC=(TP+TN)/(TP+TN+FP+FN)$$

$$DR=TP/(TP+FP)$$

$$RR=TP/(TP+FN)$$

其中，TP(True Positive)是正确识别的正常记录数，TN(True Negative)是正确识别的攻击记录数，FP(False Positive)是错误识别的正常记录数，FN(False Negative)是错误识别的攻击记录数。

4.3 对比实验分析

为检测 SS-DGM 算法对入侵检测的有效性，本文设计了两组实验。

实验 1 分析 SS-DGM 模型各参数对入侵检测效果的影响。

实验 2 与其他入侵检测算法的分类准确率与训练时间进行对比。

首先，验证本文方法在有标签数据样本比例不同时的入侵检测性能，借此来评价半监督算法是否有利于提高入侵检测的检测精度。分别对 5%，20%，50%，80% 的测试样本进行标记，实验结果如图 6 所示。由图 6 可知，随着标记数据样本的增加，模型的分类准确率不断提升，当标记数据占总训练样本的 20% 时，模型的分类准确率达到 90%。由此可知，本文提出的半监督入侵检测算法不仅能有效缓解难以获得标记数据的问题，还能够准确检测网络中的恶意连接。

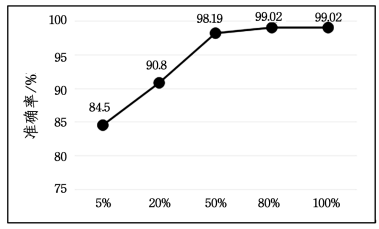

图 6 不同比例标记数据的准确率比较

Fig. 6 Comparison of experimental results with different proportion of labeled dataset

随着模型深度的增加，高层特征的表示能力更抽象，分类准确率也由此提升，但训练时间大幅增加，过多的层数容易导致过拟合现象。本实验设置了 3 种不同深度的 MLP 模型，其中有标记样本占训练样本的 50%，隐变量维度设置为 30，各隐藏层节点个数为 200 时，其性能的对比结果如图 7 所示。

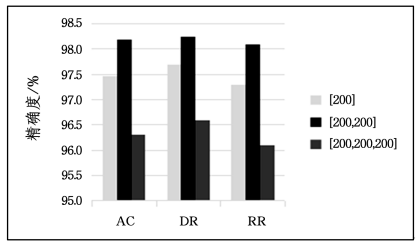

图 7 模型深度不同时检测精度的比较

Fig. 7 Comparison of experimental results with different depths

由图 7 可知，当模型深度为 2 时，检测精度最高，而当模型深度为 3 时，检测精度却大大降低，这是因为当隐藏层个数设置为 200 时，模型的特征学习能力已达到较强水平，继续增加模型深度不但使训练时间大大增加，而且会导致过拟合，因此对拥有较多“陌生”甚至未知属性值的测试集来说，模型检测的精度会降低。

本文的另一个研究重点是选择最小的特征向量来提高入侵检测识别率。为了测试隐变量维度对检测效果的影响，采用两层的 MLP[200,200]作为 VAE 的编码结构，将隐变量维度从 10 变化到 50，其他参数不变，实验结果如图 8 所示。由图 8 可知，当隐变量维度设置为 30 时，模型的准确率和检测率最高。这是因为当隐变量维度过低时，模型学习的特征不完全，无法表征原始数据；当隐变量维度过高时，模型趋向于过拟合，使得模型的泛化能力降低，从而导致测试准确率不高。

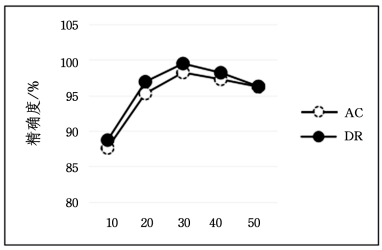

图 8　隐变量维度不同时检测精度的比较

Fig. 8　Comparison of experimental results with different dimension of hidden variables

表 2 比较了有标记数据占 50%时，各个半监督算法分类的准确率与训练时间。由表 2 可以看出，本文所提算法在分类准确率上均优于其他半监督算法，虽然精确率 *DR* 低于 SS-DNN[9]，但召回率高出 SS-DNN 将近 2%。入侵检测系统要对进入系统的流量做全面检测，因此算法的查全率更为重要。从模型的训练时间来看，两个深度模型所用时间均多于前两个模型，这是由于深度模型需要训练迭代并调整大量参数，导致模型学习时间过长。综合 *AC*，*DR*，*RR* 三者来看，本文所提算法的可行性更高。

表 2　各算法检测精度与训练时间的比较

Table 2　Comparison of experimental results with different detection accuacy and training time

	AC/%	*DR*/%	*RR*/%	训练时间/s
LapSVM[7]	96.79	97.56	96.23	567.03
文献[8]	83.46	84.12	82.32	238.78
SS-DNN[9]	96.34	98.79	96.34	1311.86
SS-DGM	98.19	98.37	98.13	658.05

结束语　本文针对网络入侵检测的问题，借鉴生成模型和无监督学习的思想，提出了一种基于深度生成模型的半监督算法。首先，利用变分自编码学习提取原始数据的低维特征向量；然后，借助低维向量，结合少量标签训练分类器，利用无标签数据和低维向量预测类标签，同时利用低维向量和类标签重构数据，训练整个模型。该方法一方面能借助少量有标签数据进行检测；另一方面，基于生成模型的检测算法生成的样本具有多样性，能够提高模型的泛化能力。另外，该模型虽然分类准确率高，但无法检测特定的攻击类型(如 R2L)，因此，针对特定攻击类型的检测，该模型有待改进，这也是下一步的研究方向。

参 考 文 献

[1] CHANDOLA V, BANERJEE A, KUMAR V. Anomaly detection: A survey[J]. ACM Computing Surveys (CSUR), 2009, 41(3): 1-58.

[2] DENNING D E. An Intrusion-Detection Model[J]. IEEE Transactions on Software Engineering, 2006, SE-13(2): 222-232.

[3] SOMMER R, PAXSON V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection[C]// IEEE Symposium on Security and Privacy. IEEE Computer Society, 2010: 305-316.

[4] LASKOV P, DÜSSEL P, SCHÄFER C, et al. Learning Intrusion Detection: Supervised or Unsupervised? [C]// International Conference on Image Analysis and Processing. Springer-Verlag, 2005: 50-57.

[5] LIANG C, LI C H. Novel Intrusion Detection Method Based on Semi-supervised Clustering[J]. Computer Science, 2016, 43(5): 87-90. (in Chinese)
梁辰，李成海. 一种新的半监督入侵检测方法[J]. 计算机科学，2016，43(5)：87-90.

[6] YANG S L, YANG Y H, SHEN Q N, et al. A method of Intrusion Detection Based on Semi-Supervised GHSOM[J]. Journal of Computer Research and Development, 2013, 50(11): 2375-2382. (in Chinese)
阳时来，杨雅辉，沈晴霓，等. 一种基于半监督 GHSOM 的入侵检测方法[J]. 计算机研究与发展，2013，50(11)：2375-2382.

[7] ZHANG X, ZHU P, TIAN J, et al. An effective semi-supervised model for intrusion detection using feature selection based Lap-SVM[C]// 2017 International Conference on Computer, Information and Telecommunication Systems (CITS). Dalian, 2017: 283-286.

[8] ASHFAQ R A R, WANG X Z, HUANG J Z, et al. Fuzziness based semi-supervised learning approach for intrusion detection system[J]. Information Sciences An International Journal, 2017, 378(C): 484-497.

[9] NOSADA G, OMOTE K, NISHIDE T. Network Intrusion Detection Based on Semi-supervised Variational Auto-Encoder[C]// European Symposium on Research in Computer Security—ESORICS 2017. Cham: Springer, 2017.

[10] FITRIANI S, MANDALA S, MURTI M A. Review of semi-supervised method for Intrusion Detection System[C]// Multimedia and Broadcasting. IEEE, 2017: 36-41.

[11] KINGMA D P, WELLING M. Auto-Encoding Variational Bayes [C]// Conference proceedings: papers accepted to the International Conference on Learning Representations (ICLR). 2014.

[12] KINGMA D P, REZENDE D J, MOHAMED S, et al. Semi-Supervised Learning with Deep Generative Models[J]. Advances in Neural Information Processing Systems, 2014, 4: 3581-3589.

[13] MERZ C J, CLAIR D C, BOND W E. SeMi-supervised adaptive resonance theory (SMART2)[C]// International Joint Conference on Neural Networks. IEEE, 1992.

[14] 周志华. 机器学习[M]. 北京：清华大学出版社，2016：298-297.

[15] LIU J W, LIU Y, LUO X L. Semi-Supervised Learning Methods [J]. Chinese Journal of Couputers, 2015, 38(8): 1592-1617. (in Chinese)
刘建伟，刘媛，罗雄麟. 半监督学习方法[J]. 计算机学报，2015，38(8)：1592-1617.

[16] GAO N, GAO L, HE Y Y, et al. A Lightweight Intrusion Detection Model Based on Autoencoder Network with Feature Reduction[J]. 2017, 45(3): 730-739. (in Chinese)
高妮，高岭，贺毅岳，等. 基于自编码网络特征降维的轻量级入侵检测模型[J]. 电子学报，2017，45(3)：730-739.

[17] TAVALLAEE M, BAGHERI E, LU W, et al. A detailed analysis of the KDD CUP 99 data set[C]// IEEE International Conference on Computational Intelligence for Security & Defense Applications. IEEE, 2009: 1-6.