Computer Science and Application 计算机科学与应用, 2017, 7(11), 1146-1155
Published Online November 2017 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2017.711129

Hans汉斯

A Method of APT Attack Detection Based on DBN-SVDD

Feifan Liu[1], Yuan Li[1], Fei Xia[2], Jing Zhou[3]

[1]Computer School of Wuhan University, Wuhan Hubei
[2]National Network Jiangsu Power Company Information Communication Branch, Nanjing Jiangsu
[3]Beijing Huitong Golden Finance Information Technology Ltd., Beijing
Email: zhanglq@whu.edu.cn

Received: Nov. 12th, 2017; accepted: Nov. 23rd, 2017; published: Nov. 30th, 2017

Abstract

Advanced Persistent Threat (APT) causes high attention for it is frequently used to steal enterprise core data and bring about extremely harsh effects. The APT attack adopts the attack mode of persistent network attack for a long time, and it has the characteristics of high concealment and latency; therefore, the traditional detection technology cannot be effectively identified. At present, the detection scheme for APT attack has three schemes: sandbox scheme, network anomaly detection scheme and full flow scheme. However, the existing APT attack detection method has low accuracy in the detection, a need for large numbers of marked samples and other shortcomings. In this paper, a network intrusion detection model (DBN-SVDD) based on depth learning is proposed by using the network intrusion detection scheme. This method uses DBN to reduce the structure dimension and improve the detection efficiency. Then, the SVDD is used to detect the data set. The experimental results of NSL-KDD dataset show that the detection rate of this method is high; the method has unmanned supervision; and it can effectively deal with high-dimensional data and so on. It can be effectively applied to APT attack detection.

Keywords

Advanced Persistent Threat, Deep Learning, Data Mining, Semi-Supervised Learning

一种基于DBN-SVDD的APT攻击检测方法

刘飞帆[1]，李　媛[1]，夏　飞[2]，周　静[3]

[1]武汉大学计算机学院，湖北　武汉
[2]国网江苏省电力公司信息通信分公司，江苏　南京
[3]北京汇通金财信息科技有限公司，北京
Email: zhanglq@whu.edu.cn

文章引用: 刘飞帆, 李媛, 夏飞, 周静. 一种基于 DBN-SVDD 的 APT 攻击检测方法[J]. 计算机科学与应用, 2017, 7(11): 1146-1155. DOI: 10.12677/csa.2017.711129

收稿日期：2017年11月12日；录用日期：2017年11月23日；发布日期：2017年11月30日

摘　要

由于高级持续性威胁(Advanced Persistent Threat, APT)常用于窃取企业核心资料且带来极其恶劣的影响而引起高度关注。因为APT攻击的攻击方法是对特定的攻击目标长期进行持续性网络攻击，具有极高的隐蔽性、潜伏性等特点；所以传统检测技术无法进行有效识别。目前针对APT攻击的检测方案有沙箱方案、网络异常检测方案、全流量方案这三种检测方案，然而现有的APT攻击检测方法中存在检测准确性较低、需要大量经过标记的样本等缺点。本文提出一种基于深度学习的网络入侵检测模型(DBN-SVDD)，该方法利用DBN进行结构降维、提高检测效率，再利用SVDD对数据集进行识别检测。在NSL-KDD数据集的实验结果表明，该方法的检测率可以达到93.71%。该方法具有无人监督、无需大量标记样本、可以有效处理高维数据等特点，能够有效地应用于APT攻击检测中。

关键词

高级持续性威胁，深度学习，数据挖掘，半监督学习方法

1. 引言

随着全球信息化以及网络技术的迅速发展，针对特定攻击对象的有组织的高级持续性威胁(Advanced Persistent threat, APT)日益增多，带来的后果愈发严重，许多企业甚至国家的信息安全都受到严重威胁[1] [2] [3]。2008 年，来自美国国防部的黑客攻击渗透中国长城网；2010 年，“震网”病毒成功攻击了伊朗的工业控制系统，导致了伊朗核计划的推迟；2011 年，“夜龙行动”窃取了多个能源巨头公司的核心敏感文件；2012 年，“火焰”成功获取中东各国的大量机密信息。由此可知，APT 攻击对于国家网络空间主权、工业控制系统以及企业数据的信息安全具有十分恶劣的不良影响与巨大的威胁，因此，亟需针对 APT 攻击进行有效的检测与防护。

APT 攻击是长期的、持续性的网络攻击，攻击行为藏匿在正常行为中难以被发觉。因此，攻击检测成为 APT 攻击防御工作中最关键而且最困难的部分。然而，传统的攻击检测技术无法有效处理数据量极大的数据记录集。此外，传统的攻击检测技术往往只能识别检测出较为明显的异常或攻击行为，用来检测隐匿在正常行为中的 APT 攻击并不能得到理想的检测结果。所以，传统的攻击检测技术大多无法有效检测 APT 攻击[4]。现有的 APT 攻击检测方案分沙箱方法、异常检测方法和全流量审计方法[5]三种。沙箱方法主要解决特征匹配对新型攻击的滞后性问题。该方法将实时流量引入沙箱中，通过对沙箱中的文件系统、网络行为、进程、注册表实施监控，检测是否存在恶意代码。异常检测方法可以解决特征匹配和实时监测的不足，通过对网络中的正常行为模式建模从而识别异常行为。全流量审计方案也是为了解决传统特征匹配不足而提出的，该方法对链路中的流量进行深层次的协议解析和应用还原，识别其中是否包含攻击行为。在这三种方法中，异常检测与全流量审计都需要处理海量数据，因此 APT 攻击检测的模型应适用于数据量极大的情况。

深度学习模型是一种多处理层的计算模型，通过组合多层非线性的简单模块来实现多层表征学习，每层都会从上一层的简单表征里学习更抽象复杂的表征，从海量高维的原始数据中识别出复杂的模型。所以，研究人员已经开始探索深度学习在网络异常检测中的应用。

目前，利用深度学习模型[6]对网络中的 APT 攻击检测技术研究主要包括以下三个方面：无监督学习、监督学习和半监督学习。无监督学习直接学习数据的内在结构，无需样本的标签数据，不需要对样本进行大量标记，但检测率较低。Kingsly 等人[7]提出以基于聚类算法的网络异常检测方法，将网络数据通过聚类分为若干组，根据这些分组识别每条数据是否为正常数据。有监督学习需要提前对训练样本进行标记，该方法首先使用有标签的训练集学习分类器，然后使用学习后的分类器对网络行为做识别检测。文献[8]提出将支持向量机(Support Vector Machines, SVM)方法应用到 APT 攻击检测中。除此之外，朴素贝叶斯(Naïve Bayes, NB) [9]、遗传算法(Genetic Algorithm, GA) [10]也都应用到入侵检测领域。有监督学习的方法往往表现出优异的检测效果，然而需要对样本进行标记后再训练，对于数据量大的数据集不具有较高的实用性。半监督学习是监督学习与无监督学习相结合的一种方法，该方法主要考虑利用少量的标注数据和大量的未标注数据进行分类[11] [12]。Yasami 等[13]利用 k-means 聚类和 ID3 决策树学习算法进行网络异常的检测，首先利用 k-means 对训练集进行训练，再使用 ID3 决策树检测判断是否发生异常。文献[14]提出基于深度信念网络(Deep Belief Networks, DBN)和支持向量机(Support Vector Machines, SVM)的混合模型进行网络入侵检测。

针对数据属性数量较多、维度较高的问题，Rubinstein 等人[15]提出使用主成分分析法提取出主分量，选择重要的主成分对数据进行结构降维。针对结构降维问题，还有文献[16] [17] [18]提出可以使用 DBN(Deep Belief Networks, DBN)进行结构降维。通过结构降维的方法，深度学习模型利用学习低维特征能够很好地解决传统机器学习面临的“维数灾难”，并且有效地提高了深度学习模型的训练时间和测试时间，具有较高的检测效率，在高维复杂的网络数据中取得了较好的检测效果。

根据上述分析，本文提出一种基于半监督学习的 APT 攻击检测方法。首先采用无监督学习的 DBN [16]进行初步的降维与分类，然后在 DBN 算法的基础上，使用 SVDD 算法进行进一步的训练与检测。实验结果表明，本文提出的方法在攻击检测中具有较高的准确率，能够有效地检测网络异常行为，利用该方法检测 APT 攻击具有一定的可行性。同时，该算法相较于基于监督学习的异常检测而言，不需要大量经过标记的样本；相较于无监督学习的异常检测而言，具有较高的检测准确性。

本文组织如下：第二部分介绍基于半监督学习的网络异常检测模型，第三部分介绍相关实验步骤及实验结果分析，第四部分对本文进行总结。

2. 基于半监督学习的 APT 检测模型

2.1. 深度信念网络 DBN

2006 年 Hinton 等人[17]提出深度信念网(Deep Belief Net, DBN)，它是由多层无监督的限制玻尔兹曼机网络和一层有监督的反向传播网络组成，结构如图 1 所示。

DBN 是一种无监督学习的方法，目前已被建议作为一个多层次分类器和降维工具。DBN 多层生成模型，学习一个层的特性与未标记的数据，后提取的特征作为输入的训练下一层。这种高效的学习可以通过微调后的权重提高整个网络的性能。该方法适用于数据量大且高维的数据集，对于 APT 攻击的检测具有很高的实用价值。

DBN 使用未标记的数据、一次学习一层特征的多层生成模型。DBN 具有对于数据量庞大的数据集执行非线性维数降低的能力和对高维流形数据的学习能力，可以使用受限玻尔兹曼机(Restricted Boltzmann Machines, RBM)以多层方式高度训练。

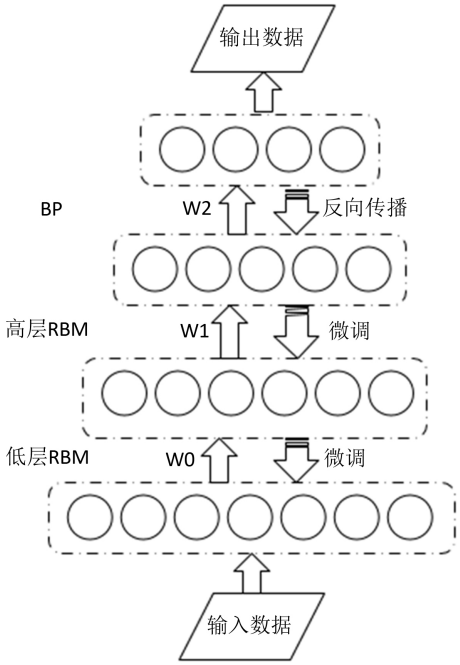

Figure 1. DBN structure
图 1. DBN 结构图

在 RBM 中可见单元 v 为表示特征，隐藏单元 h 学习表示特征，即它将来自维度为 n 的输入空间的输入向量 v 映射到维度为 $d=|h|$ 的特征空间里，其中 $p(v,h)$。给定数据集 $D_{m\times n}$ 作为输入，RBM 将其映射到 $X_{m\times d}$ 中。在 RBM 中，相同级别的单元之间没有连接，即可见－可见或隐藏－隐藏连接，并且图的两层用隐藏和可见单元对之间的对称权重 W 连接。

在原始的玻尔兹曼机器架构中，隐藏和可见向量的联合分布 $p(v,h)$ 是根据能量函数 $E(v,h)$ 定义的，假设输入向量是具有方差 σ 的高斯随机变量，则该高斯伯努利 RBM 的能量函数 $E(v,h)$ 可以被获得为：

$$E(v,h)=\frac{1}{2}\sum_i (v_i-c_i)^2-\sum_j b_j h_j-\sum_{i,j} w_{i,j}v_i h_j \tag{1}$$

其中 v_i 和 h_j 分别是具有 $W_{i,j}$ 的对称权重的可见 v 层和隐藏 h 层的第 i 和第 j 个单元，以及相应的偏差 c_i 和 b_j，因此 $p(v,h)$ 的公式如下所示：

$$P(v,h)=\frac{e^{-E(v,h)}}{Z} \tag{2}$$

其中 Z 是称为分区函数的归一化因子，并且计算为：

$$Z=\sum_{v,h} e^{-E(v,h)} \tag{3}$$

联接配置的值由相对于网络参数的值 $\theta=(W,b,c)$ 来确定，其中 b 和 c 分别是对隐藏层和可见层的偏差。隐含层 h 是二进制的，并且隐藏单元是伯努利随机变量，而输入单元可以是二进制或实值。给定二元隐藏单元 h_j，由于隐藏单元之间没有连接，所以可以直接计算条件分布 $P(h|v)$：

$$P(h|v)=\prod_j P(h_j|v)=\prod_j sigm\left(b_j+\sum_i w_{i,j}v_i\right) \tag{4}$$

并且类似地，由于在可见单元之间没有连接，因此：

$$P(v|h)=\prod_i P(v_i|h)=\prod_i N\left(c_i+\sum_j w_{i,j}h_{j,\sigma}\right) \tag{5}$$

其中：

$$Sigm(x)=\frac{1}{1+e^{-x}} \tag{6}$$

是逻辑 S 型函数和 $N(\mu,\sigma)$ 表示具有均值 μ 和方差 σ 的高斯分布。训练 RBM 意味着找到参数 θ 的值，使得能量最小化。一种可能的方法旨在最大化由其相对于模型参数的梯度估计的 v 的对数似然：

$$\frac{\partial \log p(v)}{\partial \theta}=E_P(h|v)\left[\frac{\partial E(v,h)}{\partial \theta}\right]-E_P(v|h)\left[\frac{\partial E(h,v)}{\partial \theta}\right] \tag{7}$$

由于对数似然的第二项的精确计算是难以处理的，所以可以使用称为对比度发散(CD) [19]的方法来估计梯度。CD 近似通过 k 次迭代的吉布斯采样(通常 k = 1)的期望以更新网络权重：

$$\frac{\partial \log P(v)}{\partial W_{i,j}}\approx\langle v_i h_j\rangle^0-\langle v_i h_j\rangle^k \tag{8}$$

其中 $\langle\circ\rangle^I$ 表示对比发散迭代 I 的平均值。在训练 RBM 之后，另一个 RBM 可以堆叠在第一个 RBM 的顶部，即隐藏单元的推断状态 $X_{m\times d}$ 用作用于培训新的 RBM 的可见单位。上层可以是伯努利伯努利 RBM，其中与第一层的主要区别在于二元可见单位和能量函数[20]。堆叠 RBM 使得人们能够建模早期 RBM 的隐藏单元之间的显着依赖性。更具体地，可以堆叠多层 RBM 以产生不同层的非线性特征检测器，其表示数据中逐渐更复杂的统计结构。在 RBM 的堆栈中，所得 DBN 的自底向上识别权重被用于初始化多层前馈神经网络的权重。该网络可以用作用于降维的工具，或者用逻辑回归层来顶端并且通过用于分类的反向传播来进行区别地微调。

2.2. 支持向量数据描述方法 SVDD

支持向量数据描述方法(Support Vector Data Description, SVDD)是由 Tax 等人结合 SVM 方法与最小包围球而提出的一种数据描述方法。其主要思想为在高维特征空间中找寻一个尽可能将所有训练样本都包围起来的最小超球体，并以这个最小超球体的决策边界对数据进行分类和描述。由于 SVDD 对异常点十分敏感，所以常常用于处理异常检测等问题，且 SVDD 相较于 SVM 而言具有训练速度快等特点。

SVDD 需要在高维特征空间中找寻一个尽可能将所有训练样本都包围起来的最小超球体，实际情况下数据并不是集中分布，因此往往会引入一个松弛变量[21]。所以很清楚地可以知道求解最小超球体的问题可以描述为：

$$\min R^2+C\left(\sum_i \xi_i\right)^K \tag{9}$$

其中 C 为一个常数，是对错误分类样本的惩罚程度，K 也是用户指定的一个常数，一般情况下 K = 1，并且上述问题描述应该满足约束条件：

$$0\le R^2+\xi_i,\xi_j\le(x_i-a)(x_i-a)^{\mathrm{T}} \tag{10}$$

a 为要构造的超球体的球心向量，利用其中半径的计算公式为：

$$R^2=(x_u,x_u)-2\sum_{j=1}^n \alpha_j(x_u,x_j)+\sum_{i=1}^n\sum_{j=1}^n \alpha_i\alpha_j(x_i,x_j) \tag{11}$$

2.3. 基于半监督学习的攻击检测方法

图 2 为 DBN-SVDD 模型图，该模型图分为三部分：数据预处理、DBN 训练阶段、SVDD 识别检测阶段。其中数据预处理分为字符型属性映射和数据属性归一化。NSL-KDD 数据集的每一条数据记录有 38 个数字型特征和 3 个字符型特征，因此需要先将字符型属性映射成数字型属性。由于数据本身的定性特征没有明显的顺序，故采用哑编码进行映射。又因为特征向量中每一个特征量纲不同，取值范围不一，所以需要对数据属性归一化。

在这里我们选择开源框架 keras 建立 DBN 网络，keras 是一个高层神经网络 API，keras 由纯 Python 编写而成并基于 Tensorflow、Theano 以及 CNTK 后端。keras 为支持快速实验而生，能够把你的 idea 迅速转换为结果。

在 DBN 训练阶段，得到标准数据集以后，我们使用 DBN 模型对其降维。低层 RBM 进行初步降维以后再使用高层 RBM 从低层 RBM 传来的简单表征里学习更抽象复杂的表征，并反向调整权值，提取出特征优秀的数据。再将 DBN 处理过的数据分为训练集和测试集，提供数据记录给 SVDD 进行训练和识别检测，最终得到检测结果。该攻击检测方法的具体步骤如下：

步骤 1：使用哑编码做字符型属性映射

步骤 2：对步骤 1 处理过的数据属性进行归一化

步骤 3：使用 keras 开源框架建立 DBN 网络

步骤 4：使用 DBN 网络进行降维和提取优秀的特征向量

步骤 5：构建 SVDD 网络

步骤 6：对训练集进行训练

步骤 7：对测试集进行仿真和测试

该实验流程如图 3 所示。

3. 仿真与实验

3.1. 实验环境与评价指标设计

本文对提出的基于半监督学习的攻击检测模型进行仿真实验。采用的数据集为 NSL-KDD 数据集，该数据是 KDDCU99 的改进版，包含了 KDDTrain+、KDDTrain_20percent、KDDTest+和 KDDTest-21 四个子数据集，其中它们分别有 125,973、25,192、22,544、11,850 条数据记录。

该仿真实验在 Ubuntu 6.04LTS 环境下进行，使用 Keras 神经网络库、Sklearn 机器学习包构建 DBN-SVDD 网络，并且使用 Tensorflow 0.8 作为后端计算框架，DBN 层数设置为 2 层，低层 RBM 将 41 个特征降维成 13 个特征，高层 RBM 将 13 个特征价格为成 5 个特征。测试机的配置如表 1 所示。

为了评价与比较相关的攻击检测模型，本文采用的是检测率和测试时间这两个性能指标。其中检测

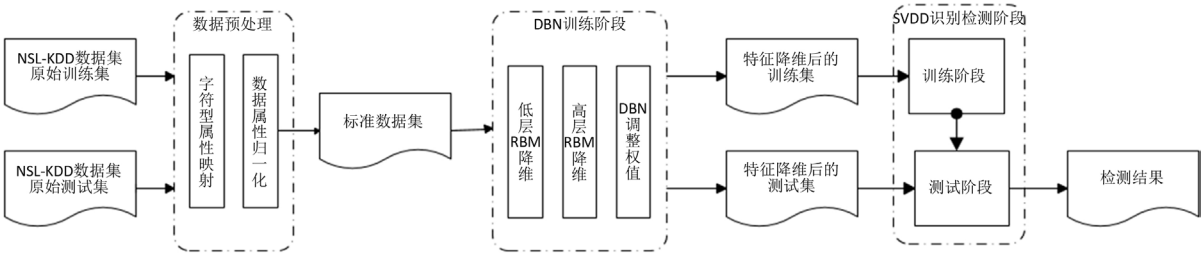

Figure 2. DBN-SVDD model diagram
图 2. DBN-SVDD 模型图

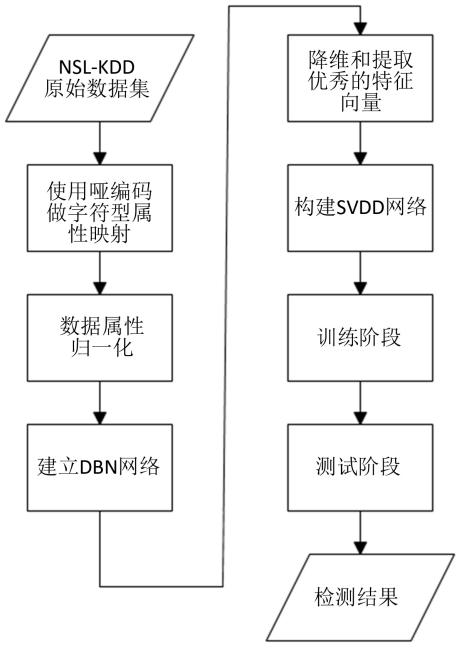

Figure 3. Experimental flow chart of DBN-SVDD
图 3. DBN-SVDD 实验流程图

Table 1. The detailed configuration information of testing machine
表 1. 测试机详细配置

类别	参数
内存容量	8 GB
内存类型	DDR4 2400
核心	四核
CPU 类型	Intel 第七代酷睿
固态硬盘	128GB SSD

率是指检测到的异常数据样本和实际的异常数据样本的数据比率，测试时间是指测试数据所花费的时间，该指标可以反映在实际应用中模型的运行时间。

3.2. 数据预处理

NSL-KDD 数据集的每条记录都包括了三方面的特征信息，1~9 为基本信息特征，10~22 为内容特征，23~31 为基于时间的流量特征，32~41 为基于主机的流量特征[22]。训练集中包含了 22 种攻击，为了模拟实际情况中有一些新的攻击出现，测试集中包含了 17 种训练集中没有出现过的攻击类型。而所有攻击数据主要可划分为以下四类攻击：拒绝服务攻击(DoS)、远程网络用户攻击(R2L)、提升权限攻击(U2R)和探测攻击(Probe)。其中 DoS 攻击为 APT 攻击的主要攻击方式之一。

由于 NSL-KDD 每条实验记录不仅有 38 个数字型属性特征，还有 protocol_type、service、flag 这 3 个字符型属性特征，其中 protocol_type 有 3 种特征值，service 有 70 种特征值，flag 有 11 种特征值，因此我们需要将原始记录中字符型特征进行映射转换成数字型属性。本文使用哑变量(Dummy Variables) [23]编码的方式对这 3 种字符特征进行编码，将每一条原始的数据记录变成一个 122 维的特征向量。

由于特征向量中每一个特征量纲不同，取值范围不一，所以我们需要对每个特征向量进行标准化(Standardization or Mean Removal and Variance Scaling)，变换后各维特征有 0 均值，单位方差。也叫 z-score 规范化(零均值规范化)。计算方式是将特征值减去均值，除以标准差。本文在 train 集上做标准化后，用同样的标准化器去标准化 test 集。

最后，由于该数据集的攻击主要分为四类，因此我们将数据集的类标分为 5 类。

3.3. 实验结果与分析

3.3.1. 不同数据降维的比较

在前言中已经提到解决传统机器学习面临的“维数灾难”研究人员提出了使用结构降维的方法先对数据进行降维，其中常用的三种降维方法有 PCA、GAB RATB、DBN。其中文献[24]提出对这 3 种不同的降维方法做出了不同数据降维方法间的比较。分别给 PCA、GAB RATB、DBN 设置了训练数据 20%、40%、60%、80%的数据量。性能对比分析结果如图 4 所示，从以上数据可以看出 DBN 的降维效果相对较好，四个数据量都达到了 90%以上，更加适合处理高维数据。

3.3.2. 与其他深度学习模型的比较

前言中我们已经简要阐述了用于网络异常检测的深度学习模型有聚类模型、DBN-SVM、DBN、SVM 等，由于篇幅有限，不再对这些方法进行详细的阐述。接下来本小节将要阐述实验过程，然后给出实验结果最后分析出实验结论。

本文提出的方法与其他几种深度学习的方法的对比实验结果如表 2 所示，使用 NSL-KDD 数据进行模型训练时，K-means 由于是无人监督的机器学习模型，因此所需时间短，但其检测率较低。本文提出来的方法其运行时间比 DBN-SVM 长 0.48 s，但其准确率略胜 DBN-SVM，达到 93.71%的准确率。

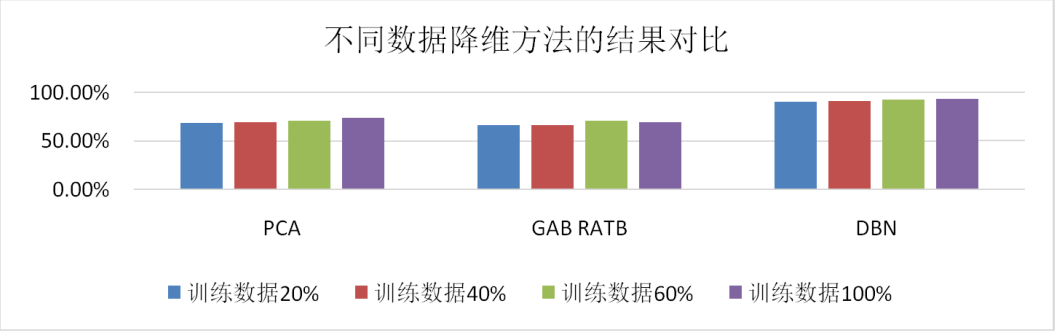

Figure 4. Comparison of results of different data reduction methods
图 4. 不同数据降维方法的结果对比

Table 2. Comparison with the results of other deep learning methods
表 2. 与其他深度学习方法的结果数据比较

Methods	Acc	Test time
DBN	86.90%	0.76s
SVM	89.25%	32.30s
DBN-SVM	93.14%	7.75s
K-means	71.70%	0.51s
DBN-SVDD	**93.71%**	8.23s

综上可以看出，本文提出的 DBN-SVDD 异常检测模型，相较于其他模型具有一定的优势，具有较强的潜力。该模型有以下几种优势：1) 该模型是一种无人监督的机器学习模型，不需要大量数据标记样本适用于检测海量的数据记录；2) 该模型具有较高的检测率，且其运行时间比有监督学习短但比无监督学习强，综合检测率和运行时间具有较为优秀的应用性能；3) 该模型适用于高维数据，具有突出的降维效果。

4. 结束语

本文提出了一个基于 DBN-SVDD 的攻击检测模型，其中 DBN 用于特征降维和提取优秀的特征向量，SVDD 是用于数据分类与检测。通过 NSL-KDD 数据集的实验结果表明，DBN-SVDD 拥有很好的分类效果，并且对数据的降维极大地提高了测试时间。同时，DBN 比 PCA 具有更好的性能；此外，SVDD 与 SVM 相比也具有很好的分类效果。该攻击检测模型适用于无人监督的数据量大且具有高维特征的攻击数据检测中，且具有优异的检测效果，十分贴合对 APT 攻击检测模型的需求。在接下来的工作中，我们将考虑如何降低该模型的性能开销，并进一步讨论如何提高该模型的检测率。总之，该模型极大地提高了入侵检测速度且具有优秀的检测效果，是一种可行的、高效的 APT 攻击检测模型。

参考文献 (References)

[1] Chen, P., Desmet, L. and Huygens, C. (2014) A Study on Advanced Persistent Threats. *Lecture Notes in Computer Science*, **8735**, 63-72. https://doi.org/10.1007/978-3-662-44885-4_5

[2] Virvilis, N. and Gritzalis, D. (2013) The Big Four—What We Did Wrong in Advanced Persistent Threat Detection? *IEEE Eighth International Conference on Availability, Reliability and Security*, Regensburg, 2-6 September 2013, 248-254. https://doi.org/10.1109/ARES.2013.32

[3] Yang, G., Tian, Z. and Duan, W. (2015) The Prevent of Advanced Persistent Threat. *Journal of Chemical & Pharmaceutical Research*, **6**, 572-576.

[4] Giura, P. and Wang, W. (2013) Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats. *Science*, **1**, 93-105.

[5] 马琳. 基于大数据的 APT 攻击方法和检测方法[J]. 计算机光盘软件与应用, 2014(10): 91.

[6] 付钰, 李洪成, 吴晓平, 等. 基于大数据分析的 APT 攻击检测研究综述[J]. 通信学报, 2015, 36(11): 1-14.

[7] Leung, K. and Leckie, C. (2007) Unsupervised Anomaly Detection in Network Intrusion Detection Using Clusters. *Twenty-Eighth Australasian Computer Science Conference on Computer Science*, Newcastle, January 2005, 333-342.

[8] 郑黎明, 邹鹏, 韩伟红, 等. 基于多维熵值分类的骨干网流量异常检测研究[J]. 计算机研究与发展, 2012, 49(9): 1972-1981.

[9] 李柏生, 林亚平, 鄢喜爱. 基于朴素贝叶斯网络的入侵检测分析[J]. 网络安全技术与应用, 2007(9): 23-25.

[10] 史长琼, 王大卫, 黄辉, 等. 基于粗糙集与小生境 GA 的网络入侵规则提取[J]. 计算机工程与应用, 2009, 45(5): 110-112.

[11] Erman, J., Mahanti, A., Arlitt, M., *et al.* (2007) Semi-Supervised Network Traffic Classification. *ACM SIGMETRICS Performance Evaluation Review*, **35**, 369-370.

[12] Ashfaq, R.A.R., Wang, X.Z., Huang, J.Z., *et al.* (2016) Fuzziness Based Semi-Supervised Learning Approach for Intrusion Detection System. *Information Sciences*, **378**, 484-497.

[13] Yasami, Y. and Mozaffari, S.P. (2010) A Novel Unsupervised Classification Approach for Network Anomaly Detection by k-Means Clustering and ID3 Decision Tree Learning Methods. *The Journal of Supercomputing*, **53**, 231-245. https://doi.org/10.1007/s11227-009-0338-x

[14] Salama, M.A., Eid, H.F., Ramadan, R.A., *et al.* (2011) Hybrid Intelligent Intrusion Detection Scheme. In: Gaspar-Cunha, A., Takahashi, R., Schaefer, G. and Costa, L., Eds., *Soft Computing in Industrial Applications. Advances in Intelligent and Soft Computing*, Vol. 96, Springer, Berlin, Heidelberg, 293-303.

[15] Rubinstein, B.I.P., Nelson, B., Huang, L., *et al.* (2009) Stealthy Poisoning Attacks on PCA-Based Anomaly Detectors. *ACM SIGMETRICS Performance Evaluation Review*, **37**, 73-74. https://doi.org/10.1145/1639562.1639592

[16] Hinton, G.E. and Salakhutdinov, R.R. (2006) Reducing the Dimensionality of Data with Neural Networks. *Science*,

313, 504-507. https://doi.org/10.1126/science.1127647

[17] Hinton, G.E., Osindero, S. and Teh, Y.-W. (2006) A Fast Learning Algorithm for Deep Belief Nets. *Neural Computation*, **18**, 1527-1554. https://doi.org/10.1162/neco.2006.18.7.1527

[18] Liu, Y., Zhou, S. and Chen, Q. (2011) Discriminative Deep Belief Networks for Visual Data Classification. *Pattern Recognition*, **44**, 2287-2296. https://doi.org/10.1016/j.patcog.2010.12.012

[19] Hinton, G.E. (2002) Training Products of Experts by Minimizing Contrastive Divergence. *Neural Computation*, **14**, 1771-1800. https://doi.org/10.1162/089976602760128018

[20] 阜艳, 李霆, 黄日辉, 等. 一种改进的支持向量数据描述算法[J]. 五邑大学学报(自然科学版), 2008, 22(2): 52-56.

[21] Larochelle, H., Bengio, Y., Louradour, J. and Lamblin, P. (2009) Exploring Strategies for Training Deep Neural Networks. *Journal of Machine Learning Research*, **10**, 1-40.

[22] 张新有, 曾华燊, 贾磊. 入侵检测数据集 KDD CUP99 研究[J]. 计算机工程与设计, 2010, 31(22): 4809-4812.

[23] Neter, J., Kutner, M.H., Nachtsheim, C.J., *et al.* (1996) Applied Linear Statistical Models. Irwin, Chicago.

[24] 杨昆朋. 基于深度信念网络的入侵检测模型[J]. 现代计算机: 普及版, 2015(1):10-14.