Tongji University

School of Software Engineering

GAN+RL For Anomaly Detection

X-Lab Report 1

Student:

Name: Liang Wang

E-mail: leonwangchn@163.com

Instructor:

Jasper Qiu

September 24, 2019

Contents

1 Introduction

异常检测的特点：
1. 单变量时序分类问题
2. 异常数据占的比例很小（样本不均衡）=> 传统分类方法不适用
3. 异常的三种类型：contextual anomaly, point anomaly, collective anomaly
4. 异常都有 global 和 local 两种模式，其中 local 和正常数据有相同的分布，所以更难识别 => 普通的深度学习模型不适用

Contributions：
1. 设计了用于异常检测的 CLSTM
2. 数据预处理，消除样本不均衡
3. new model = CLSTM + GAN + RL

2 Background

2.1 传统分类方法

传统分类方法仅在 statistical anomalies 上表现好，但是不能准确区分与正常数据有同样分布的异常数据

2.2 DL 方法

C-LSTM

- 结合 cnn 与 rnn, can both extract temporal and spacial features in data sequences
- cnn 与 lstm 线性连接
- 论文 6
- 原本用于文本分类，本文重新设计后用于异常检测
- 实际上本文中的模型和实验数据来自论文 2

2.3 GAN 方法

论文 1:

- 基于 GAN 进行异常检测

- background 倒数第二段提到其缺点：不能处理时序数据

论文 3:

- 能处理时序数据的 GAN：SeqGAN
- 但是是用于生成 word sentences 的，其数据特征与异常检测不同（离散与连续），所以不能应用于异常检测
- 但可以借鉴其部分思想，即引入强化学习

2.4 综上

综上：有多种方法能够实现对数据序列的异常检测。一是 CSTM，可以提取时空特征。二是 GAN，更能够很好地学到数据的值的分布。所以本文模型结合以上两种网络：
CNN + RNN + GAN + RL

3 Our Model

CNN + LSTM => 分类器
GAN + RL => 解决数据不平衡问题

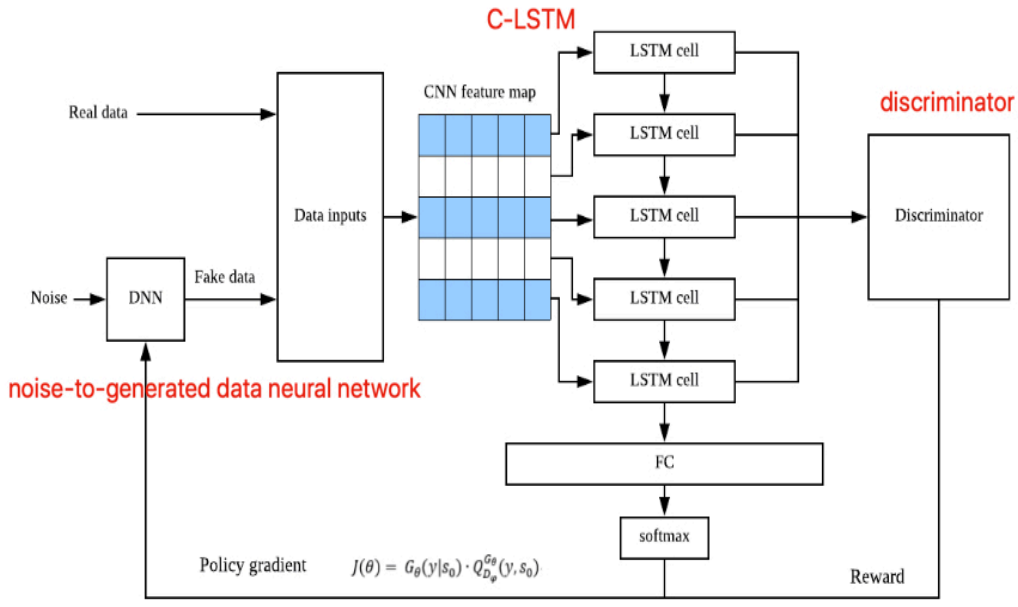

Figure 1: Network

3.1 C-LSTM Classifier for AD

介绍用于异常检测的 C-LSTM 网络，取自论文 2

3.2 GAN for AD

正样本太少，所以传统深度学习模型不好
介绍最早用于异常检测的 GAN，即论文 1 中的模型
借鉴论文 3 中的思想，构建 SeqGAN 模型，引入强化学习

3.3 GAN via Policy Gradient

SeqGAN 中的策略梯度算法，借鉴论文 3
用 GAN 解决数据不平衡问题，在引入 seqGAN 解决提取时空特征的问题，再把 GAN 与 RL 结合，解决只能用于离散数据的问题
不需要使用蒙特卡洛搜索 dual

3.4 Training

具体训练的过程，在论文 3 的基础上进行的修改
训练的过程：
1. 先预训练 CLSTM 分类器。只用不含异常的 sequence 进行训练，所以此时它并不能很好地区分无异常 sequence 和有异常 sequence，但是它能很好地区分真实数据和生成的数据。
2. 训练生成数据的网络
3. 训练判别器网络
4. 重复 2 ~ 3，进行对抗

3.5 Anomaly Assessment

对于 DL 方法：直接评估序列是否异常
对于 GAN+RL 方法：

- 针对 single data，而不是 sequence
- 通过判别器的一些中间层的输出计算一个分数，从而判定是否异常

4 Experiment

4.1 Yahoo S5 数据集和数据预处理

滑窗算法进行预处理，把 single data 处理成 sequence，正样本比例 1669/94866 => 8556/90913

4.2 软硬件

4.3 DL 方法的实验

（这部分完全来自论文 2，可能只是为了和 4.4 的实验做个对比，没有太大的意义）
最终的结论是 CNN + LSTM + DNN 的网络结构比其他 DL 网络表现更好

4.4 GAN 方法的实验

以论文 1 中的 GAN 模型作为 benchmark，实验证明我们提出的 GAN + RL 模型表现更好

5 引文研究

5.1 CLSTM 相关

[6]Chunting Zhou, Chonglin Sun, "A C-LSTM Neural Network for Text Classification", November 2015.
提出了 C-LSTM，结合 CNN 和 LSTM，提取空间和时间特征，用于文本分类。
本文进行重新设计后，用于异常检测。

> C-LSTM(proposed by Chunting Zhou, Chonglin Sun, 2015[?]) is to make use of the two features. It consists of CNN and LSTM layers, structured linearly. The spatial features of the data sequence is extracted by the convolution and pooling layers, and the temporal features are extracted by the LSTM layers. C-LSTM was proposed to do text classification, we redesigned the network structure and use it to do anomaly detection.

[2]Tae-Young Kim, Sung-Bae Cho, "Web traffic anomaly detection using CLSTM neural networks", Expert Systems With Applications 106 (2018) 6676, 2018
SCI 期刊
摘要
Web traffic refers to the amount of data that is sent and received by people visiting online websites. Web traffic anomalies represent abnormal changes in time series traffic, and it is important to perform detection quickly and accurately for the efficient operation of complex computer networks systems. In this paper, we propose a C-LSTM neural network for effectively modeling the spatial and temporal information contained in traffic data, which is a one-dimensional time series signal. We also provide a method for automatically extracting robust features of spatial-temporal information from raw data. Experiments demonstrate that our C-LSTM method can extract more complex features by combining a convolutional neural network (CNN), long short-term memory (LSTM), and deep neural network (DNN). The CNN layer is used to reduce the frequency variation in spatial information; the LSTM layer is suitable for modeling time information; and the DNN layer is used to map data into a more separable space. Our C-LSTM method also achieves nearly perfect anomaly detection performance for web traffic data, even for very similar signals that were previously considered to be very difficult to classify. Finally, the C-LSTM method outperforms other state-of-the-art machine learning techniques on Yahoo's well-known Webscope S5 dataset, achieving an overall accuracy of **98.6%** and recall of **89.7%** on the test dataset.
论文中 deep learning experiments 中的数据来自此文。

CLSTM 应用于异常检测，CNN + LSTM + DNN 的表现最好。

5.2 GAN 相关

[1]Houssam Zenati, Chuan-Sheng Foo, "Efficient GAN-Based Anomaly Detection", Workshop Track, ICLR, 2018

- 提出了把 GAN 应用于异常检测。生成器和判别器都采用 DNN 结构，并通过计算测试样本和生成样本的距离作为异常评估。缺点是指处理没有时间的数据。

  提供了 GAN 的思路，提供了通过计算距离进行异常评估的思路。

  discriminator 不只考虑输入（真实还是生成的），还考虑输入的潜在表示，从而进行分类

- 在 GAN 实验中被用作 benchmark

  > we constructed experiments on our GAN model. We use another GAN network (Houssam Zenati [?]) which simply uses DNN network in generator and discriminator as benchmark. This model is designed to do anomaly detection in KDD dataset, and this data set is not time-serial, that is, neighboring data is independent with each other. So the benchmark model doesn't using the spatial and temporal information, and when updating parameters via gradients, this model is quite traditional, while our model using policy gradient.

[3]Lantao Yu, Weinan Zhang, "SeqGAN: Sequence Generative Adversarial Nets with Policy Gradient", AAAI, 2017

在论文 [1] 的基础上，提出能够处理时间序列的 GAN（通过 LSTM），即 SeqGAN。
缺点是它处理的数据的值是离散的，而异常处理数据的值是连续的，所以不能直接用于异常处理。但可以借鉴其中的思想，如引入 RL。

5.3 其他

[4]Bachman, P., and Precup, D., "Data generation as sequential decision making", NIPS, 32493257, 2015i

SeqGAN 的引文
sequential procedures for generating data 指的是生成模型，强化学习对此提供帮助
MDP：马尔可夫决策过程
生成模型的训练与强化学习中的策略搜索相结合

结合 data imputation（数据填补/缺失值处理）问题进行讨论

[5]Bengio, S.; Vinyals, O.; Jaitly, N.; and Shazeer,N., "Scheduled sampling for sequence prediction with recur-rent neural networks", NIPS, 11711179, 2015

SeqGAN 的引文

提出了训练 RNN 的 trick：计划采样

scheduled sampling 翻译成 "计划采样", 用于解决 exposure bias 问题针对 sequence-to-sequence 框架下的 decoder 阶段，在训练时，生成 y_t 时，输入的 y_{t-1} 是训练集中标注序列中的 true value, 然后在预测是，输入的 y'_{t-1} 是在 t-1 时刻生成的 label, 该标签可能是正确的，也可能是预测错误的标签，如果是错误的标签就会导致一个问题，就是错误爆炸，说白了就是 y'_{t-1} 是错误标签，那么以它为输入生成的 y_t 也是不可信的。针对这种问题，提出了 scheduled sampling 的解决方法。Scheduled Sampling 是指 RNN 训练时时会随机使用模型真实 label 来作为下一个时刻的输入，而不像原先那样只会使用预测输出。训练时网络将不再完全采用真实序列标记做为下一步的输入，而是以一个概率 p 选择真实标记，以 1-p 选择模型自身的输出。"计划采样" 即 p 的大小在训练过程中是变化的，就像学习率一样。作者的思想是：一开始网络训练不充分，那么 p 尽量选大值，即尽量使用真实标记。然后随着训练的进行，模型训练越来越充分，这时 p 也要减小，即尽量选择模型自己的输出。这样就尽量使模型训练和预测保持一致。

6 疑问

1. 为什么说异常数据和正常数据可以有相同的分布?
2. 为什么网络可以对 single data 进行异常评估