同济大学
TONGJI UNIVERSITY

September 24, 2019
Edition: 2.1

软件工程课程设计

第一次报告

姜华

软件工程课程设计
Tongji University
School of Software Engineering

Contents

Part 1 GAN+RL For Anomaly Detection

1

1.1 Abstract

摘要中提出了两个问题

- abnormal samples occur rarely.
- anomalies contain local patterns having the same distribution as normal data is harder to detect.

解决方案

- 本文设计了一个用于异常检测的深度学习模型（C-LSTM），对数据进行了合理的预处理，避免了数据的不平衡。然后结合 C-LSTM、GAN 和强化学习的新模型来检测数据集中的异常。

1.2 Model

1.2.1 C-LSTM

LSTM 和 RNN 善于处理周期性的数据。序列数据可以映射成多维图像，通过 CNN 提取其空间特征。但是处理时间序列数据时，时间信息在卷积和池化中丢失，所以需要建立一个既能提取数据序列的时间特征，又能提取空间特征的模型。

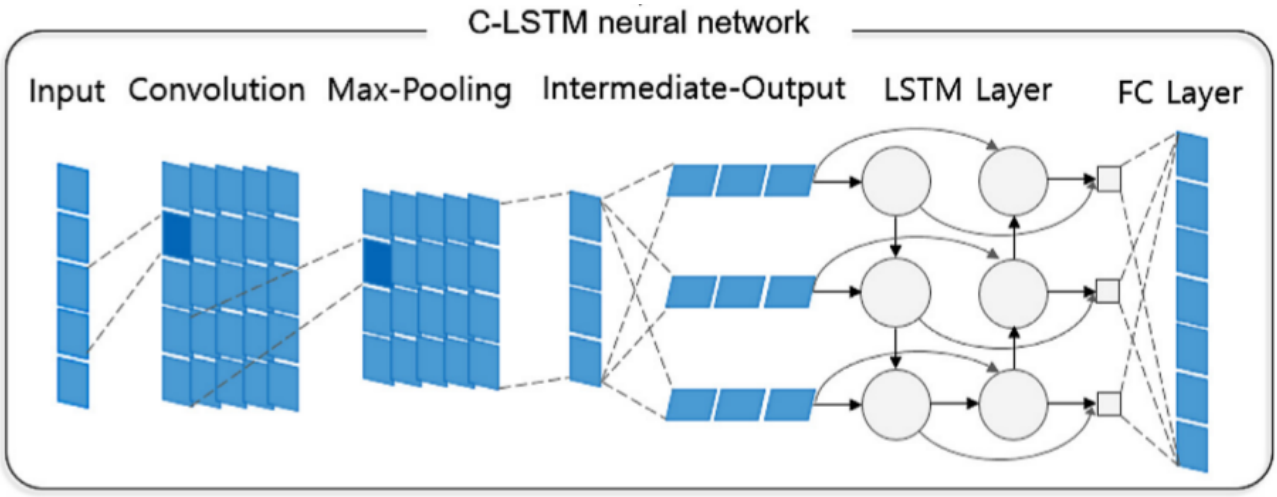

Fig 1.1: C-LSTM

C-LSTM 使用预处理的数据作为输入。输入是由时间序列正常和异常网络流量数据组成的数据序列，一旦序列有异常数据，则该序列为异常。空间特征由 CNN 层提取。然后由 LSTM 层提取时间特征。然后，训练模型使用 Softmax 分类器对测试数据执行异常检测。

1.2.2 GAN for AD

C-LSTM 可以对正常和异常数据进行分类，但是由于训练的异常样本的数据很少，存在数据不平衡问题，不能保证模型学习到如何对正常和异常数据进行分类。将 gan 应用于异常检测任务的最初目的是了解正常状态的分布，然后通过实际样本与所学分布的差异来判断测试样本是否处于异常状态。并且他的相关工作只是将传统的神经网络应用于发生器和鉴别器中 (第一篇引文)，并没有利用时空信息。所以本文提出了 sequence GAN network，同时为了避免离散数据的问题，将 GAN 和强化学习进行了结合 (第三篇引文)

强化学习

当噪声通过 DNN 时，我们就获得了 generator 产生的数据，这可以看成是一个 action, 然后把产生的数据送入 C-LSTM 分类器，可以获得一个分数 (通过某种 policy 计算)，这个分数可以认为是被分类器认为是真实数据的概率。使用分类器作为回报函数的优点是可以动态改进 generator model。当 generator 产生了一个数据序列，就可以看成是执行了一个 action，然后 discriminator 会输出一个 reward value, 根据 reward 更新 generator model。

1.2.3 Training

Pre-train the C-LSTM classifier

- 一般数据中 normal 的数据会比很多，所以只能分别出 normal data, 不能很好地分辨出 abnormal data，并且能够分辨出 noise-generated data。
- 相比于生成的数据，异常序列获得的分数会更高。在训练呢的过程中，只需要更新 noise-to-generated data neural network parameters，确保产生贴近真实的数据。

1.2.4 Anomaly Assessment

对于 C-LSTM 分类，它只能判断一个数据序列是否包含异常数据，因此在进行评估时，我们只关注测试数据集中的序列。对于 gan 网络，鉴别器不具备区分正常和异常数据的能力，发生器中的 c-lstm 分类器也不具备鉴别能力。我们需要设计一种计算分数的方法，该分数表示学习分布和测试数据之间的差异有多大。给定一个测试数据，

就可以计算出一个分数，然后判断这个数据是否正常。分数实际上是由中间层从鉴别器计算出来的。进行评估时，有两个标准：

- 设定一个特定的基准分数，分数大于该基准的数据应被视为异常，而其他数据则是正常的。(只能靠经验实现)
- 我们可以猜测异常数据在整个数据集中所占的百分比，也可以通过训练数据集来达到这个百分比，并将最高分作为异常分。

1.2.5 Experiments

Yahoo S5 Webscope Dataset and Pre-processing

- 67 个文件，94866 个值中只有 1669 个异常值，所以希望使异常数据量的百分比更大
- 使用滑窗的方式，含有异常数据的称为 abnormal sequence，使得异常数据量提高

Deep Learning Experiments

构造了 CNN+LSTM+DNN 来测试数据集，并将其作为我们的基准之一。

Gan experiments

在 gan 模型上构建了实验。先使用另一个 gan 网络它简单地使用 dnn 网络作为基准。该模型是为了在 kdd 数据集中进行异常检测而设计的，该数据集不是时间序列，即相邻数据之间是相互独立的。因此，基准模型不使用时空信息，当通过梯度更新参数时，该模型相当传统，而本文的模型使用的是策略梯度。结果表明策略梯度得到的序列 gan 性能优于传统 gan。

Part 2 References

2

2.1 EFFICIENT GAN-BASED ANOMALY DETECTION

2.1.1 Abstract

- 生成性对抗网络（gans）能够模拟真实世界数据的复杂高维分布，这表明它们可以有效地进行异常检测。
- 正文提到的将 GAN 用于 AD 的最初目的: 了解正常状态的分布，然后通过实际样本与所学分布的差异来判断测试样本是否处于异常状态。

2.2 Web trac anomaly detection using C-LSTM neural networks

2.2.1 Abstract

本文提出了一种 c-lstm 神经网络，用于有效地对一维时间序列信号中包含的时空信息进行建模。提出了一种从原始数据中自动提取时空信息鲁棒特征的方法。实验表明，该方法结合卷积神经网络（cnn）、长短期记忆（lstm）和深神经网络（dnn），能够提取出更复杂的特征。cnn 层用于减少空间信息的频率变化；lstm 层用于建模时间信息；dnn 层用于将数据映射到更可分离的空间。我们的 C-LSTM 方法还可以对网络传输数据实现近乎完美的异常检测性能，即使对于以前认为很难分类的非常相似的信号也是如此。最后，c-lstm 方法在雅虎著名的 webscope s5 数据集上优于其他最先进的机器学习技术，在测试数据集上获得了 98.6% 的总体准确率和 89.7% 的召回率。

2.2.2 借鉴

借鉴了它的 C-LSTM 思想，同时提取空间特征和时间特征，也借鉴了其直接用于进行异常检测，而不是正文作者的设计。

2.3 SeqGAN

2.3.1 Abstract

生成性对抗网络作为一种新的生成性模型训练方法，利用判别模型来指导生成性模型的训练,在生成真实数据方面取得了相当大的成功。但是,当目标是生成离散 token 序列时，它有限制。一个主要原因在于生成模型的离散输出使得将梯度更新从判别模型传递到生成模型变得困难。此外，判别模型只能评估一个完整的序列，而对于一个部分生成的序列，在整个序列生成后，平衡其当前得分和未来得分是非常重要的。本文提出了一个序列生成框架 seqgan 来解决这些问题。在强化学习（rl）中将数据生成器建模为随机策略时，seqgan 通过直接执行梯度策略更新来绕过生成器微分问题。rl 奖赏信号来自基于完整序列的 gan 鉴别器，并通过 monte carlo 搜索传回中间状态动作步骤。对合成数据和实际任务的大量实验表明，与强大的基线相比，有着显著的改进。

2.3.2 借鉴

由于 SeqGAN 的数据是离散的，但是异常检测的一些特征是连续的，但是为了避免遗传算法的离散数据问题所以主要借鉴了 GAN+RL 强化学习的思想。

Appendix A

3

Image Index