Research Report One

Xinpeng Hong

Number 2019-0001
September 24 2019

同济大学
软件学院
杜庆峰教授实验室
邱娟博士课题组

Research Report One

Xinpeng Hong

Tongji University, School of Software Engineering, 2019-0001

September 24 2019

1 背景知识学习

DNN(深度神经网络), CNN(卷积神经网络), RNN(循环神经网络), LSTM(长短期记忆网络), GAN(生成式对抗网络), RL(强化学习)

2 主体报告阅读

2.1 标题

GAN+RL For Anomaly Detection

2.2 摘要

Web 服务器流量异常检测是一个时间序列分类问题。
由于异常样本只占总样本的很小一部分，传统分类方法不能很好解决这类问题。
异常类型分三种：上下文异常 (contextual anomaly)、点异常 (point anomaly) 和集合异常 (collective anomaly)。
异常可能同时包含全局模式和局部模式，前者更容易识别，后者更难检测。
本文设计了一个用于异常检测的深度学习模型 (CLSTM)，对数据进行预处理以避免数据不平衡。
在此基础上提出了一种结合 CLSTM、GAN 和 RL 的数据集异常检测新模型。

2.3 背景

K-means、随机森林、支持向量机等不能正确分类和正常数据相同分布的异常数据。
LSTM 等 RNN 能较好处理具有周期性的数据，但如果数据没有周期性则性能会大大降低。
CNN 能提取序列数据映射成多维图像的空间特征，但对于时间序列数据，时间信息会在卷积和池化操作中丢失。

CLSTM 对于数据不平衡问题做得不好，比如训练集中只含有少量正样本 (不正常的样本)。
GAN 能生成正常数据的值分布，我们能通过真实样本和学习到的分布的差异进行异常评估。Houssam 等通过将测试数据和生成数据转换为潜在空间对异常进行评估，但是对时间序列的数据表现不佳。最著名的处理时间序列的 GAN 模型为 SeqGAN，但其针对的数据是离散的，能构造一个字典来存储所有单词，而有些特征是连续的，因此 SeqGAN 不能用于异常检测。
结论：CLSTM 在提取时空特征方面做得很好，GAN 在学习数据价值效率分布方面做得很好，二者结合可以做得更好。

2.4 模型

Generator: C-LSTM 见论文
Overall Model: GAN+RL 见论文
Discriminator: DNN 见论文
Defination: 见论文

2.5 训练

在对判别器进行更新的时候，存在多个损失函数来衡量两个分布之间的差异，如 cross entropy、JS divergence、Wasserstein distance 等。这里我们使用 Wassertein distance 更新 discriminator。
Algorithm: GAN+RL for AD network 见论文。
对 CLSTM 分类器进行预训练，让它学习如何对正常数据序列进行分类，但是由于只有很少正样本，某些异常序列在训练前的 CLSTM 网络工作中能取得较高分数，在 GAN 中需要对 CLSTM 中不变的参数进行修正，更新噪声到生成数据的神经网络参数，这样能保证生成器生成真实的网络流量序列。

2.6 异常评估

CLSTM 分类器只能判断某数据序列是否包含异常数据，评估的时候只关注测试数据集中的序列。
GAN 网络，discriminator 不能区分正常数据和异常数据，generator 中 CLSTM 分类器也不能，GAN 评估不关注测试数据序列，而是比较差异。
评估的两个标准：设置特定的基准得分和将猜测的异常数据在整个数据集中所占的最高百分比作为异常值。后者更为适用。

2.7 实验

数据集：Yahoo S5 Webscope
预处理：滑动窗口算法
LSTM+DNN

CNN+DNN
CNN+LSTM+DNN 见论文
GAN+RL 见论文

2.8 结论

优点：在具有时间和空间特征的数据集上使用 GAN+RL 方法取得了很好的结果。
缺点：很难拟合和训练；参数更新是通过梯度下降来完成的，因此较大奖励可能不会导致较大的梯度变化；即使导致了较大梯度变化，它也有可能与 generator 返回的动作相矛盾，模型可能永远不会收敛。
改进：提高鲁棒性，使适用于更多数据集。

3 参考文献阅读

Houssam Zenati, Chuan-Sheng Foo, ”Efficient GAN-Based Anomaly Detection”, Workshop Track, ICLR, 2018: 生成式对抗网络 (GANs) 能够对真实数据的复杂高维分布进行建模，这表明它可以有效地进行异常检测。然而，很少有研究探讨 GANs 在异常检测任务中的应用。这篇文章利用最近开发的 GAN 模型进行异常检测，并在图像和网络入侵数据集上实现了最先进的性能，同时在测试时比唯一发布的基于 GAN 的方法快数百倍。
Tae-Young Kim, Sung-Bae Cho, ”Web traffic anomaly detection using C- LSTM neural networks” , Expert Systems With Applications 106 (2018) 6676, 2018: 这篇文章提出了一种 C-LSTM 神经网络，用于对一维时间序列信号中的交通数据进行有效的时空信息建模。实验表明，C-LSTM 方法结合了传统的神经网络 (CNN)、长短时记忆 (LSTM) 和深度神经网络 (DNN)，可以提取出更复杂的特征。利用 CNN 层降低空间信息的频率变化；LSTM 层适用于时间信息的建模；DNN 层用于将数据映射到更可分离的空间。C-LSTM 方法对于 web 流量数据也实现了近乎完美的异常检测性能，即使对于非常相似的信号，以前认为是非常难以分类的。
Lantao Yu, Weinan Zhang, ”SeqGAN: Sequence Generative Adversarial Nets with Policy Gradient” , AAAI, 2017: 当目标是生成离散标记序列时，GAN 有一定的限制，一个主要原因是生成模型的离散输出使得梯度难以从判别模型更新到生成模型。此外，判别模型只能对一个完整的序列进行评价，而对于一个部分生成的序列，一旦生成了整个序列，平衡它当前的分数和未来的分数是非常重要的。在这篇文章中提出了一个序列生成框架 SeqGAN 来解决这些问题。将数据生成器建模为 RL 中的一个随机策略，SeqGAN 通过直接执行梯度策略更新，绕过了生成器的微分问题。RL 奖励信号来自于一个完整序列判断的 GAN 识别器，并通过蒙特卡罗搜索返回到中间状态-动作步骤。

Bachman, P., and Precup, D., "Data generation as sequential decision making", NIPS, 32493257, 2015i: 通过广泛类别的生成模型对顺序决策的共同依赖来连接它们，对现有模型进行扩展，然后在数据输入的背景下进一步探索这一想法——这可能是研究传统生成模型和条件生成模型之间关系的最简单的设置。将数据输入定义为一个 MDP，并开发能够表示其有效策略的模型。利用神经网络建立模型，并利用引导策略搜索对模型进行训练，模型通过反馈和细化的迭代过程生成预测。结果表明，该方法能有效地解决不同难度、不同数据集之间的归算问题。

Bengio, S.; Vinyals, O.; Jaitly, N.; and Shazeer,N., "Scheduled sampling for sequence prediction with recurrent neural networks", NIPS, 11711179, 2015: 可以训练 RNN 生成给定输入的标记序列。当前训练它们的方法包括在给定当前 (递归) 状态和前一个令牌的序列中最大化每个标记的可能性。在推断时，未知的先前标记将被模型本身生成的标记替换。训练和推断之间的这种差异会产生错误，这些错误会沿着生成的序列迅速累积。这篇文章提出了一种课程学习策略，以温和地改变训练过程，从使用真正的前一个标记的完全引导方案，到使用生成的标记的较少的引导方案。

Chunting Zhou, Chonglin Sun, "A C-LSTM Neural Network for Text Classification", November 2015: 结合卷积神经网络 (CNN) 和递归神经网络 (RNN) 这两种体系结构的优点，提出了一种新的统一的句子表示和文本分类模型 C-LSTM。C-LSTM 利用 CNN 提取一系列高级短语重述语句，并将其输入长短时记忆递归神经网络 (LSTM) 中，得到句子的表示形式。C-LSTM 既能捕捉短语的局部特征，又能捕捉句子的全局和时态特征。实验结果表明，C-LSTM 算法的性能优于 CNN 和 LSTM 算法。

4 个人想法计划

依次实现 LSTM+DNN、CNN+DNN、CNN+LSTM+DNN，证明 CNN+LSTM+DNN 的分类性能最好。

实现 CNN+LSTM+GAN+RL，证明其能避免数据不均衡问题，性能相对于不会利用时空信息的 benchmark 模型会更好。

Policy Gradient 算法可能使模型永不收敛或只能收敛到局部最优而非全局最优，可以试试 Deterministic Policy Gradient 算法和 Deep Deterministic Policy Gradient 算法。

更换其他数据集进行测试。