UPPSALA
UNIVERSITET

University of Uppsala

Department of Information Technology
Division of Computing Science

Master Thesis Specification

Network Anomaly Detection and Root Cause Analysis With Deep Generative Models

---

Student
Alexandros Patsanis
Supervisor
Kim Seonghyun
Reviewer
Niklas Wahlström

A specification submitted to the University of Uppsala in accordance with the requirements of starting a Master thesis.

JANUARY 2019

Contents

1 Master Thesis Project at Ericsson AB

This master thesis project will be done at Ericsson AB based in Kista, Stockholm. Ericsson is a Swedish multinational networking and telecommunication company and is one of the leading providers of ICT to service providers, where around 40% of the world's mobile traffic passes through the Ericcson' networks. The company offers many services such as software telecommunications operators, equipment, mobile and fixed broadband operations.

2 Background

2.1 Purpose of the Project

The companies' telecommunication networks generate massive amounts of data, which means that the complexity of the networks is high. As a result, it is crucial for the network to be stable. Indeed, real-time anomaly detection plays an important role ensuring that the network operation is working efficiently. Ensuring that the network is stable can be done by taking actions in detecting anomalies and preventing many anomalous activities by identifying the cause of the problem.

Ericsson deploys an extensive number of new features in its customer network. The operations that these features are accomplished in the nodes of the radio base stations generate a large amount of data. Moreover, during the day the amount of traffic load increases as people are working at the same time. On the other hand, during the night the traffic load decreases dramatically. This variation between night and day creates a pattern of behavior that can be used to identify possible divergences in the network.

As a result, when a divergence occurs in the behaviour pattern of the network this will means that a network anomaly exists. Next, it will be analyzed the root cause of that anomaly, which will be identified.

2.2 The Aim of the Project

The purpose of this project is divided into two tasks. The first task is to detect network anomalies which are unknown behaviour patterns in the network. The second task is that after the successful detection of the anomaly, it is crucial to identify the cause of that anomaly, which might be due to hardware malfunction or software fault.

Moreover, both network anomaly detection and root cause analysis should be done automatically. Because of that both manual network anomaly detection and root cause analysis can be very difficult, and even more time-consuming.

Usually, the rules to identifying an anomaly are based on domain expert knowledge. Ericsson's radio base stations are provided in two types of Performance Management which are Performance Measurement Counter and Events. [7] The aim of the project is the implementation of a model that uses PM Counters, which refers to the number of traffic events that have occurred in a certain period. The recorded output period for generating these files is 15 minutes.

There are three general categories of anomaly detection techniques. The first is called Supervised Anomaly detection and it needs a labelled and balanced training data set.

The second is called Semi-Supervised Learning, where a small amount of labelled data exist and the rest is unlabeled. The last technique, which will be used in this project is called Unsupervised Learning and all the training data set is unlabeled.

Overall, anomaly detection is a challenging area, where studies in statistical approaches have been done as early of the 19th century [6]. Deep learning has been quite successful the last years, new algorithms have been invented. These algorithms gave a higher accuracy and speed. Therefore, this project aims to research deep generative models in the area of network anomaly detection and root causes analysis in order to find state-of-the-art approaches for identifying a network anomaly and root cause of that anomaly.

3 Description of the Task

Deep Generative models [8] seem to be one of the most promising methods for network anomaly detection and root cause analysis. Deep learning which is mentioned before has been successful for the last years and generative models ,which are explained in methods section, have been also popular the last year.

3.1 Data - Training Input

The number of times traffic events have occurred within a certain period are referred to as Performance Measurement Counters (PMs). PMs are used to generate Key Performance Indicators (KPIs). [7]. Performance Management data are generated by eNodeB and then stored as an XML file. Moreover, these data are being transferred to external databases, where we can fetch these data.

3.2 Deep Generative Models

An Unsupervised Learning [11]is an effective way to learn any kind of data distribution by using Deep Generative models [8] [1]. The intuition behind the generative models follows the quote of Richard Phillips Feynman [2], who received the Nobel Prize in Physics in 1965.

> *"What I Cannot Create, I Do Not Understand"* -Richard Phillips Feynman

The main idea behind this model is that through the learning to generating something, which is a way to learn the properties of the data that are generated. In other words, generative models can achieve learning without any ground truth. Thus, the model is able to learn a variety of the normal network pattern and develop itself based on the reconstruction error of the behaviour pattern. In this way, the model is able to learn an additional accompanying anomaly scoring scheme.

In addition, we can make use of that reconstruction error in order to identify an anomaly. The model can learn a manifold of the natural network patterns. In this way, the model will recognize the standard behaviour of the network as it will be trained with some reference data of the network.

3.3 Training Generative Models

In order to train a generative model we will need a large collection of data performance measurements counters and then simply train a model to generate data similar to the input.Generative model's purpose is first to learn the real data distribution that contains the training set and secondly to generate data points. It is not always possible to learn the distribution of the real data, but is possible to leverage the ability of neural networks in learning to approximate a model distribution to the real distribution.

This is done by using deep generative models which have an significantly smaller number of parameters compared with the quantity of the data which used for training. Thus, the models are forced to find the important features of the data to efficiently generate a similar data distribution.

3.3.1 Popular approaches for deep generative models

This subsection introduces two of the most commonly used and efficient approaches for anomaly detection that last years.

3.3.1.1 Generative Adversarial Networks (GANs)

One of the most commonly and recently used approaches for network anomaly detection are Generative Adversarial Networks GANs [9], which introduced by Ian Goodfellow. The intuition behind this algorithm is that pose the process of the training as a game between the two networks which are the generator and the discriminator network. Generator fake samples which pass to the discriminator. Then, discriminator job is to distinguish whether the sample is real or is from the generator. The generator learns to fool the discriminator, and simultaneously the discriminator learns to not be fooled by the generator, we can think it as a mini-max game. The next figure illustrates an example of the training process.

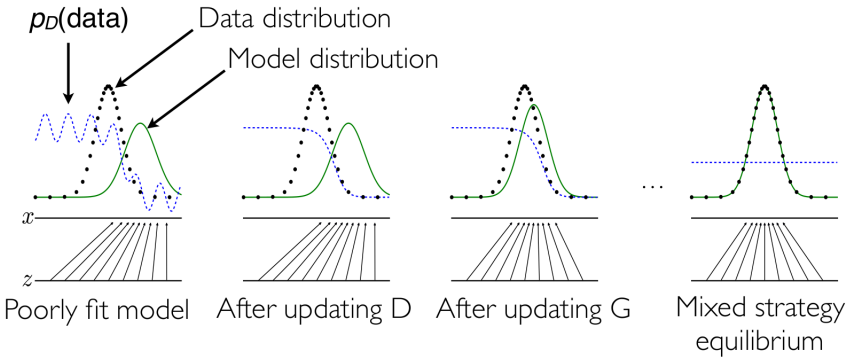


Figure 1: Learning process: 2014 NIPS Workshop on Perturbations, Optimization, and Statistics — Ian Goodfellow

3.3.1.2 Variational Autoencoders (VAEs)

Variational Autoencoders VAEs [12]are based on the idea of classical auto-encoder. VAEs

are Neural Networks which include an encoder, a decoder and a loss. VAEs are directed probabilistic graphical models, which try to form an autoencoder-like architecture. [4]

3.4 Anomaly Detection & Root Cause Analysis

The real data distribution that is generated from the Ericsson's networks can be used in order the model to learn a manifold of the usual network patterns. As a result, the model will learn the standard behaviour of the network as it will be trained with some reference data of the network which have captured before a change of the natural behaviour of the network.

Learning models on the normal behaviour of some reference data is crucial for dynamic network traffic environments. Due to the fact that, in order to perform a successful detection of anomalies and causal cause analysis, the training model must be based on observed data collected before an event occurs.

4 Methods

4.1 Grid Image as a Training Input

In this project, our intention is to use an existing tool or implement a new solution to generate a layout image. The output that we want to achieve is a grid image. The grid image will represent the density of a node in different locations. Similar to this, there is a tool called DeepST [17], which can be modified for our purposes.

In order to generate this grid image we will need the following inputs:

- A data frame that has a traffic intensity for nodes.
- An extra data frame that has node locations, like latitude and longitude.
- The resolution of grid layout.
- Colour setting.

4.2 Anomaly Detection with Deep Learning & GANs

The parallel training of a generator (G) and a discriminator (D) in this adversarial way is highly suggestive for using the Generative Adversarial Network framework for anomaly detection as is mentioned in the preview section. Recurrent Neural Networks (RNNs) are frequently used to model sequences of data. Furthermore, an efficient way of dealing with time series data is explained in "Continuous recurrent neural networks with adversarial training". [15]

Moreover, Long Short Term Memory (LSTM) Networks [14] are a particularly useful way for learning times series. Stacking RNNs hidden layers in such networks can due to their ability to maintain long term memory. LSTM with stacking recurrent hidden layers in such networks is capable of learning some series by taking backwards information. Overall, some theoretical properties based on the GANs [5] will be examined in more detailed. Therefore, a combination of an effective GAN-based approach for detecting network anomalies with both LSTM and RNN appears to be an effective start in addressing network anomaly detection and root cause analysis.

4.2.1 Anomaly Detection with GANs & LSTM-RNNs

A similar novel approach, which is worth to considering, has been proposed for anomaly detection in Multivariate Time Series of a network, in order to deal with Cyber-Physical Systems(CPS). [13]

4.2.2 Wasserstein Generative Adversarial Models

Training Generative Adversarial Networks sometimes is very hard. There are cases where the generator produces limited varieties of samples and this is called mode collapse. Wasserstein GANs [10] aims to eliminate this problem by introducing a state-of-the-art anomaly detection on MNIST DB and is worth to examine.

4.3 Tools

- Model : Generative Models, LSTM-RNNs , Generative Adversarial Models.
- Development: Python, TensorFlow [3], Keras, SciPy
- Documentation : Overleaf - LaTeX editor, Github

5 Relevant Courses

5.1 The courses which have taken at Uppsala University.

- Project CS (30c):
  The course was in collaboration with Ericsson AB involving robotics, deep neural network for reinforcement learning to teach a robot to share the same environment by solving tasks and avoid dynamic obstacles, like humans. Furthermore, augmented reality is used for visualization of safety zones.
- Artificial intelligence (5c)
- Data Mining I, (5c)
- Advanced Software Design, (5c)
- Database Design II, (5c)
- Intelligent Interactive Systems, (5c)

5.2 Course during Bachelor studies

- Pattern Recognition - Neural Networks
- Software Engineering
- Probability Theory and Statistics

6 Delimitations

Furthermore, in a relevant master thesis study [18], where generative models like GANs [16]were discarded due to the limitation of the training data.

Therefore, it can be hard to detect network anomalies with typical KPIs as the problems may be subtle with little degradation in performance. The intention of this project is to use grid layout images to avoid the problem presented with a preview work. This can be time-consuming due to the limited time of this thesis work..

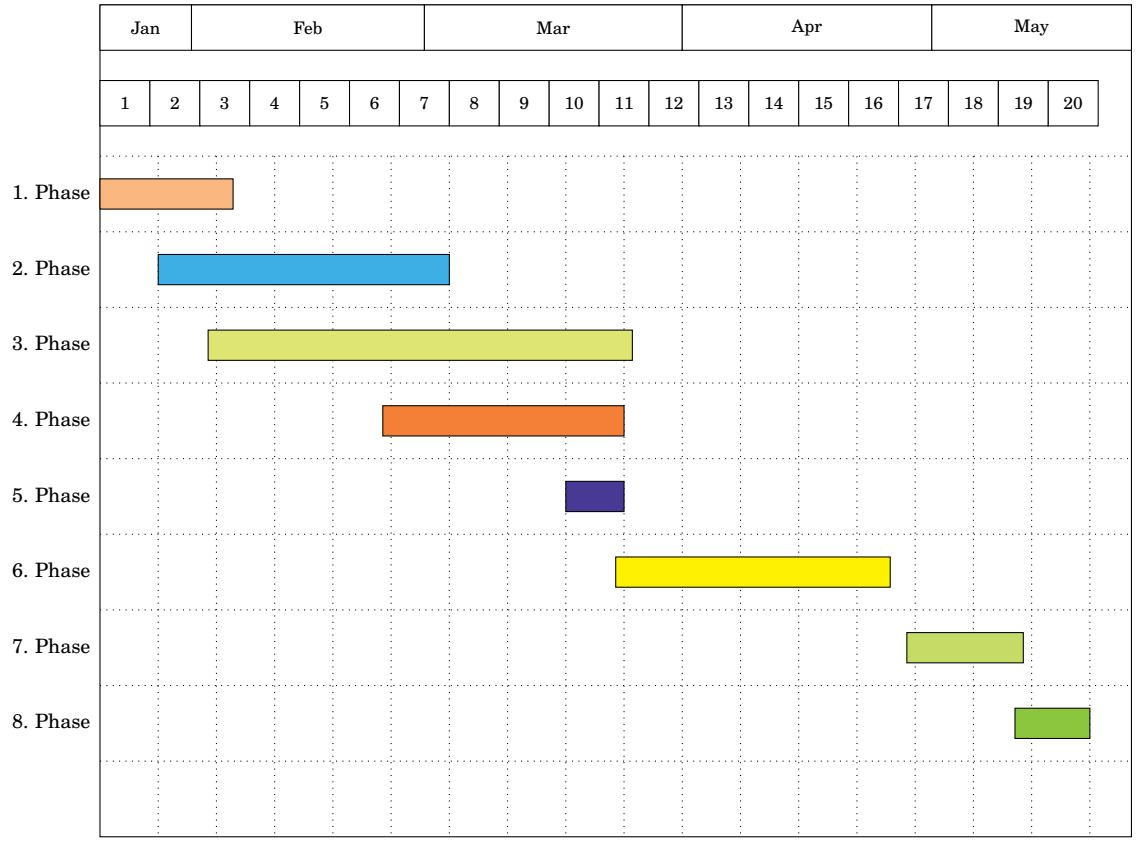
In addition, LSTM-RNN can be an effective way of detecting network anomalies and root cause analysis, but it may be difficult to optimize the model. Therefore, if problems arise, different approaches will be considered.

Overall, this project aims to detect network anomalies and root cause analysis by using Deep Generative models. Therefore, in the case that recently state-of-the-art approaches are not efficient for our purposes, other approaches will be examined.

7 Time plan

The Master thesis will begin on 21 January, 2019 and it will continue for approximately 20 weeks.

Weeks	Description
1 - 3 (Phase 1)	Literary study, studying related state-of-the-art research based on deep generative models, data processing.
2 - 7 (Phase 2)	Investigating problem solutions.
3 - 11 (Phase 3)	Implement those models and training.
6 - 12 (Phase 4)	Analyze and evaluate the results, compare with already existing methods.
10 - 11 (Phase 5)	Midterm meeting with reviewer and supervisor.
11 - 16 (Phase 6)	Integration of all components for the final compilation of the report complete final draft for feedback.
17 - 19 (Phase 7)	Prepare presentation, documentation for prototype
19 - 20 (Phase 8)	Submission of the report.



Bibliography

[1] *Deep generative models*.
`https://towardsdatascience.com/deep-generative-models-25ab2821afd3`.
Accessed: 2019-01-9.

[2] *Richard feynman*.
`https://en.wikipedia.org/wiki/Richard_Feynman`.
Accessed: 2019-01-9.

[3] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard, et al., *Tensorflow: a system for large-scale machine learning.*, in OSDI, vol. 16, 2016, pp. 265–283.

[4] J. An and S. Cho, *Variational autoencoder based anomaly detection using reconstruction probability*, Special Lecture on IE, 2 (2015), pp. 1–18.

[5] G. Biau, B. Cadre, M. Sangnier, and U. Tanielian, *Some theoretical properties of gans*, arXiv preprint arXiv:1803.07819, (2018).

[6] V. Chandola, A. Banerjee, and V. Kumar, *Anomaly detection for discrete sequences: A survey*, IEEE Trans. on Knowl. and Data Eng., 24 (2012), pp. 823–839.

[7] ERICCSON, *"LTE/SAE System Overview". In: Ericsson AB,*, 2009.

[8] I. GOODFELLOW, Y. BENGIO, AND A. COURVILLE, *Deep Learning*, MIT Press, 2016. http://www.deeplearningbook.org.

[9] I. GOODFELLOW, J. POUGET-ABADIE, M. MIRZA, B. XU, D. WARDE-FARLEY, S. OZAIR, A. COURVILLE, AND Y. BENGIO, *Generative adversarial nets*, in Advances in neural information processing systems, 2014, pp. 2672–2680.

[10] I. HALOUI, J. S. GUPTA, AND V. FEUILLARD, *Anomaly detection with wasserstein gan*, arXiv preprint arXiv:1812.02463, (2018).

[11] T. HASTIE, R. TIBSHIRANI, AND J. FRIEDMAN, *Unsupervised learning*, in The elements of statistical learning, Springer, 2009, pp. 485–585.

[12] D. P. KINGMA AND M. WELLING, *Auto-encoding variational bayes*, arXiv preprint arXiv:1312.6114, (2013).

[13] D. LI, D. CHEN, J. GOH, AND S. NG, *Anomaly detection with generative adversarial networks for multivariate time series*, CoRR, abs/1809.04758 (2018).

[14] P. MALHOTRA, L. VIG, G. SHROFF, AND P. AGARWAL, *Long short term memory networks for anomaly detection in time series*, in Proceedings, Presses universitaires de Louvain, 2015, p. 89.

[15] O. MOGREN, *C-RNN-GAN: continuous recurrent neural networks with adversarial training*, CoRR, abs/1611.09904 (2016).

[16] T. SCHLEGL, P. SEEBÖCK, S. M. WALDSTEIN, U. SCHMIDT-ERFURTH, AND G. LANGS, *Unsupervised anomaly detection with generative adversarial networks to guide marker discovery*, CoRR, abs/1703.05921 (2017).

[17] J. ZHANG, Y. ZHENG, AND D. QI, *Deep spatio-temporal residual networks for citywide crowd flows prediction*, in Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence (AAAI-17), 2017, pp. 1655–1661.

[18] S. L. ÁLVAREZ, *Anomaly detection in evolved node b's resource consumption*, 2018.