



TITLE

Diego Ximenes Mendes

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Engenharia de Sistemas e Computação, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Engenharia de Sistemas e Computação.

Orientador: Edmundo Albuquerque de Souza
e Silva

Rio de Janeiro
Janeiro de 2017

TITLE

Diego Ximenes Mendes

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA (COPPE) DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

Examinada por:

RIO DE JANEIRO, RJ – BRASIL
JANEIRO DE 2017

Ximenes Mendes, Diego

TITLE/Diego Ximenes Mendes. – Rio de Janeiro:
UFRJ/COPPE, 2017.

VIII, 15 p.: il.; 29, 7cm.

Orientador: Edmundo Albuquerque de Souza e Silva

Dissertação (mestrado) – UFRJ/COPPE/Programa de
Engenharia de Sistemas e Computação, 2017.

Bibliography: p. 13 – 15.

1. Network Measurements. I. Albuquerque de Souza
e Silva, Edmundo. II. Universidade Federal do Rio de
Janeiro, COPPE, Programa de Engenharia de Sistemas e
Computação. III. Título.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

TITLE

Diego Ximenes Mendes

Janeiro/2017

Orientador: Edmundo Albuquerque de Souza e Silva

Programa: Engenharia de Sistemas e Computação

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

TITLE

Diego Ximenes Mendes

January/2017

Advisor: Edmundo Albuquerque de Souza e Silva

Department: Systems Engineering and Computer Science

Contents

List of Figures	vii
List of Tables	viii
1 Introduction	1
1.1 Contributions	1
1.2 Dissertation Outline	1
2 Literature Review - Networking Problem Localization Using End-to-End Measurements	2
3 Change Point Detection	4
3.1 Problem Definition	4
3.2 Notation	5
3.3 Sliding Windows	6
3.4 Optimization Model	7
3.5 HMM (Hidden Markov Model)	8
3.6 Bayesian Inference	9
4 Methodology	10
5 Results	11
6 Conclusions	12
Bibliography	13

List of Figures

3.1	Toy example of a sliding windows method.	7
-----	--	---

List of Tables

Chapter 1

Introduction

1.1 Contributions

1.2 Dissertation Outline

Chapter 2

Literature Review - Networking Problem Localization Using End-to-End Measurements

Argus: Detect and localize end-to-end service quality issues ISP's networks using traffic data passively monitored at the ISP side, the ISP network topology, routing tables, and geographic information. "Argus" has been successfully deployed in a tier-1 ISP to monitor millions of users of its CDN service and assist operators to detect and localize end-to-end service quality issues.

Active probing: periodically probe the service from agents at different network locations to detect end-to-end performance issues.

Disadvantages of active probing: - without active probes from a vast number of network locations throughout the Internet, the monitoring coverage is limited and some end-to-end service quality issues may not be detected. - probe packets also place additional overhead on the network and may be treated differently than normal packets.

Passive monitoring: each end-user detects the end-to-end service quality issues individually based on performance metrics extracted from passively monitored traffic and service quality issues detected by individual end-users are correlated spatially and temporally to determine the scope of the problem.

Disadvantages of passive monitoring: - effectiveness of these systems is limited by the sparsity of passive end-to-end performance measurements for individual end-users, which further depends how frequently they access the services. For example, if an end-user only accesses the service a few times in a day, systems based on passive monitoring at end-user side may not have sufficient samples to detect service events.

Argus architecture: Spatial aggregation -> temporal aggregation -> event detection -> event localization -> event prioritization

Spatial aggregation: - Spatially aggregates end-users into user-groups, in order to avoid keeping track of the end-to-end service quality associated with millions of individual end-users. Each user-group is a set of end-users that share some common attributes, such as BGP prefix or users in the same AS. These attributes can be collected from different data sources such as network topology and routing information. The type of spatial aggregation will influence the type of location that is expected to localize problems.

Temporal aggregation: - How to detect service anomaly events for each user-group? end-to-end performance metrics from each user group can be quite noisy since they are collected from different end-users. The Argus solution focus on the summary statistics (e.g., 50th percentile, 95th percentile, min, max, etc) of the distribution instead of based on individual end-to-end performance measurements. In this procedure some details about individual end-users are lost but the goal is to detect service events that impact the user-groups. For each user-group the measurements of all end-users of this group is aggregated in time-bins, and then, for each time-bin, a summary statistics is selected, forming then a summary time series. Different statistics may provide an advantage for tracking certain type of issues. For example, the min may capture the baseline RTT due to propagation delay while average can capture network congestion. Argus uses median since they find median effective in tracking service or network side issues while being robust to variability in performance of individual end-users due to their local processing or local queuing delays.

Event detection: Apply time series analysis techniques to extract service anomaly detection algorithms. Due to scale of the system, it is desirable to have online anomaly detection with minimal runtime complexity and memory requirements. Argus applies additive Holt-Winters to do this detection. Argus also applies some other techniques to improve robustness, for example, when there is a level shift in the time series.

Event localization: The localization algorithm is not presented in the paper.

Event prioritization: The event prioritization occurs based on the significance of the anomaly detected, measured through a score resulted from the holt winters, and also considers the number of end-users impacted by the anomaly.

Results: Argus was applied to RTT measurements in a CDN hosted in a tier-1 ISP. During a one month period using time-bins of 1 hour. In this period Argus detected 2909 anomaly events, and in general, lower level user-groups were more responsible for these anomalies than the higher level groups. For each type of user-group, only a small fraction are responsible for the anomaly events. Majority of the anomalies are very short in duration.

Chapter 3

Change Point Detection

A change point detection algorithm seeks to identify points in time where the statistical properties of a time series changes. This problem has a broad application in different knowledge areas, and in general, an algorithm's performance is closely related with the time series characteristics. Further, if the latent information of the procedures that generated the time series is missing, the target statistical properties can be considered subjective, bringing difficulties not only in the detection phase but also in the problem formalization.

In this context, this chapter studies the problem and briefly discusses several change point detection algorithms. The literature of this area is extensive, and it is common to find methods that presents a poor performance due to a variety of reasons, such as being too specific to the application area, or because the mechanisms were only analyzed through theoretical aspects. Therefore, it were selected a set of techniques with a good level of theoretical formalism, and flexibility to adapt, in order to handle specifities of the problem domain. Furthermore, this chapter exposes several challenges when dealing with real data, and some adopted solutions which are not described in the literature.

3.1 Problem Definition

The problem can be offline or online. In the offline version, to decide if a specific point at time t is a change point, the solver has available the whole time series, including past and future information w.r.t. t . On the other hand, in the online version, the information is available up to time t . The choice between these options is defined by the application domain. In some cases data are processed in real time, and change points should be detected as soon as possible. But in other applications changes are identified by historical purposes, and offline algorithms can be used.

It is intuitive that the offline case is more robust, since there is more information to analyze. In practice, to increase the statistical confidence of a decision, the online

definition is relaxed, and to decide if a point in time is a change point it is possible to use data up to a small window in the future, which in real time processing means that the application should wait until additional data is available. Hence, there is a trade-off between minimizing the time to detect a change and correctly classify a point. Therefore, in some cases, the online version can be transformed in offline by minor modifications.

In this work it is considered the following input and change points attributes, which were defined considering the final application scenario:

- Univariate time series. However, it is possible to extend several methods presented here to deal with multivariate data.
- Unevenly spaced time series, that is, data is not regularly sampled in time.
- Time series with different lengths.
- Unknown number of change points.
- Different number of points between change points.
- Focus on changes in the underlying mean and distribution, disregarding other kinds of changes, such as in periodicity.
- Outliers are not considered statistical changes.
- There is no latent information of the time series.
- It is considered the online and offline options.

3.2 Notation

An univariate time series composed of n points is defined by two vectors, $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$. The value y_i indicates the i -th sampled value, and x_i indicates the associated sample time. It is assumed that the points are sorted by time, that is, $x_{i-1} < x_i$ for $i = 2, \dots, n$. Since unevenly spaced time series is considered, $x_i - x_{i-1}$ can be different for different i values. For $s \leq t$ the following notation is adopted: $\mathbf{y}_{s:t} = (y_s, \dots, y_t)$.

The presence of k change points implies that data is split into $k + 1$ segments, also called windows. Let τ_i indicates the i -th change point for $i = 1, \dots, k$. Also let $\tau_0 = 0$, $\tau_{k+1} = n$ and $\boldsymbol{\tau} = (\tau_0, \dots, \tau_{k+1})$. Then, the i -th segment is defined by $\mathbf{y}_{\tau_{i-1}+1:\tau_i}$, assuming that $\tau_{i-1} < \tau_i$ for $i = 1, \dots, k + 1$.

Through the previous definitions, change point detection algorithms mainly aim to find both k and $\boldsymbol{\tau}$.

3.3 Sliding Windows

Sliding windows techniques use two sliding windows over the time series, and reduce the problem of detecting change points to the problem of testing whether data from the segments were generated by different distributions. One approach is to consider a distance metric between two empirical distributions as the base to infer the change points. Letting $d(\mathbf{a}, \mathbf{b})$ be the distance between two empirical distributions defined by the windows \mathbf{a} and \mathbf{b} , and considering windows of length m , the Algorithm 1 presents a simple sliding windows method.

Algorithm 1 Sliding Windows

```

1:  $i \leftarrow 1$ 
2: while  $i + 2m - 1 \leq n$  do
3:   if  $d(\mathbf{y}_{i:i+m-1}, \mathbf{y}_{i+m:i+2m-1}) > \alpha$  then
4:     Report  $i + m - 1$  as a change point
5:      $i \leftarrow i + m$ 
6:   else
7:      $i \leftarrow i + 1$ 
8:   end if
9: end while

```

In this mechanism, when the distance between the distributions is above some threshold α a change point is reported. This is a common approach for an online application, however, it is possible to increase the classification accuracy in offline cases. As an example, the top plot of Figure 3.1 presents a simulated time series. The segment $\mathbf{y}_{1:1000}$ was generated sampling a $N(1, 0.2)$ distribution, and $\mathbf{y}_{1001:2000}$ was sampled through $N(5, 0.2)$. The distribution of a window was constructed binning the data with bins of size 0.02. The bottom plot of the same figure presents the associated Hellinger distance [1] between two sliding windows, where the point (i, H_i) represents the distance between the windows $\mathbf{y}_{i-100:i-1}$ and $\mathbf{y}_{i:i+99}$.

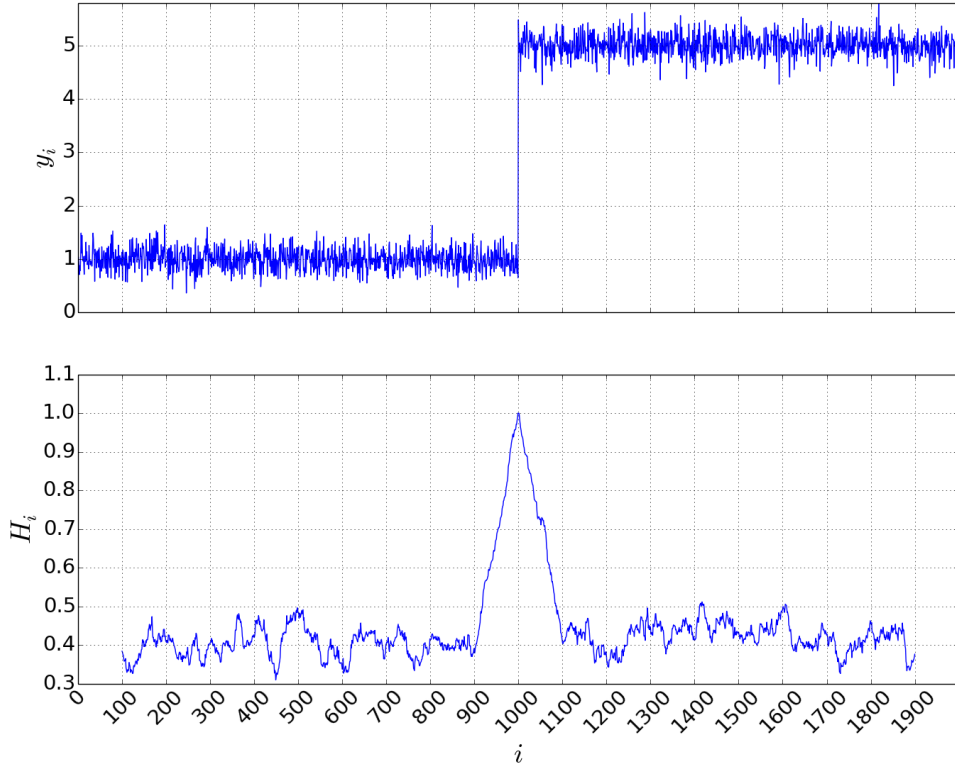


Figure 3.1: Toy example of a sliding windows method.

It can be observed that there is a peak on the distance in the exact location where the distribution changed. However, using only the threshold method it is possible to prematurely infer the position of the change point. Therefore, an alternative is to also use a peak detection algorithm. Besides, the distance function choice has a direct impact on the classification accuracy.

As stated in [2], a performance improvement can be achieved concurrently executing the same sliding windows algorithm with different windows lengths. This change facilitates the detection of segments with distinct number of points.

3.4 Optimization Model

Given a fixed value of k , one approach is to define a cost function that measures the homogeneity of a window, and therefore, choose the change points that globally optimize this homogeneity. Let the cost of the i -th segment be defined as $C(\mathbf{y}_{\tau_{i-1}+1:\tau_i})$, then the cost of a segmentation is the sum of all segments costs.

A common choice for the function C is the MSE (Mean Squared Error), which can capture changes in the mean. Another usual approach is to consider distribution changes through negative maximum log-likelihood functions, considering that data within a window is iid.

Therefore, given a fixed k , the optimal segmentation is obtained through the following optimization problem, which is called the constrained case [3]:

$$\min_{\tau_{1:k}} \sum_{i=1}^{k+1} C(\mathbf{y}_{\tau_{i-1}+1:\tau_i}) \quad (3.1)$$

This problem can be solved using dynamic programming with $O(kn^2f(n))$ time complexity, where $f(n)$ is related with the cost function evaluation. Several segment cost functions can be evaluated in $O(1)$ after a $O(n)$ preprocessing phase, implying in an overall $O(kn^2)$ complexity. It is possible to prove that MSE, negative maximum log-likelihood functions of normal, exponential, poisson and binomial distributions have this characteristic. Also, the formulation can consider a minimum value of a window length.

Modeling segments with distributions can lead to practical difficulties. One of them is the fact that segments can form degenerate distributions, that is, the data of a window can have zero variance, which is always the case of unitary length windows. In these scenarios the negative maximum log-likelihood can be undefined. Two approaches can be used to overcome this situation. The first one tries to avoid degenerate segments adding a white noise with small variance to the data stream. The second one considers that the cost of any degenerate distribution is equal to a constant.

When the number of change points is unknown, an usual way is to introduce a non decreasing penalty function $g(k)$. Then, the new optimization problem, called penalized case [3], is:

$$\min_{k, \tau_{1:k}} \sum_{i=1}^{k+1} C(\mathbf{y}_{\tau_{i-1}+1:\tau_i}) + g(k) \quad (3.2)$$

This problem can be solved in $O(Kn^2f(n))$. However, if the penalty function is linear in k , the problem can be formulated more efficiently and solved in $O(n^2f(n))$.

Also, there are several pruning algorithms to speedup the computation [3–5], in general trying to reduce the τ search space but maintaining optimality.

3.5 HMM (Hidden Markov Model)

The idea that each segment is associated with a specific latent configuration has a direct interpretation to a HMM model [6–8]. In this context, each window is related to a hidden state of a HMM, and the observation distribution of this state represents the distribution of that segment. Therefore, the mechanism models the time series using a HMM, and through the hidden state path, assesses the times

when a transition between different hidden states occur.

There are several approaches in the detection and training phases. For example, given a trained HMM, the most probable hidden state path can be checked through the Viterbi algorithm. Also, it is possible to evaluate the probability of a transition between different hidden states at time t , and then apply a threshold and peak detection methods, as well as in sliding windows techniques. For the training step, it is possible to use several time series to train a single HMM, and then use this model to detect change points in all time series. Another way is to, for each data stream, train a single model using only the target time series.

It is important to note that the structure of the hidden state graph has a large impact on the performance. Using a fully connected graph, the number of states defines the maximum number of distribution configurations. Employing a left to right structure, the number of hidden states will impact the maximum number of segments.

In [8] is stated that when using a fully connected structure, the time interval that a time series stays in the same hidden state is low, which can not reflect real data. To overcome this problem, [8] suggests to increase the time that a time series stands in the same hidden state using a dirichlet prior regularization.

3.6 Bayesian Inference

There are several Bayesian methods which aims to assess the probability that a point is a change point. Following an offline fashion, the work of [9] recursively calculates, for each i , the probability of $\mathbf{y}_{i:n}$ given a change point at i . With these probabilities is possible to simulate the time of the first change point, and then, compute the conditional distribution of the time of the second change given the first, and so on. To achieve this, the mechanism assumes that observations are independents, and that each segment is modeled by conjugate priors. Also, the procedure considers priors to model the number of changes and the time between two consecutive change points. The overall complexity of this method is $O(n^2)$, considering that the likelihood of a segment can be evaluated in $O(1)$.

In [10] it is also considered that parameters of different segments are independents, and that data within a window is iid. However, through an online mode, the procedure is concerned with the estimation of the distribution of the length of the current time since the last change point, called run length, given the data so far observed. To achieve this, the method assumes the probability of current run length given the last run length as a prior. Assuming exponential-family likelihoods to model a segment, the time complexity to process a point is linear in the number of points already observed.

Chapter 4

Methodology

Chapter 5

Results

Chapter 6

Conclusions

Future work: - collect detailed topology from the ISP which will enable more precise localizations - previous problems database and end-users reclamations to the ISP call center. This can enable the problem be interpreted as a supervised problem. - model the system as a reinforcement learning procedure, in which operators can feedback the system with correct/mistakes in the detection and localization of problems, then the system can be able to adapt automatically choosing the best algorithms and hyperparameters. - active increase measurement frequency in locations with potential problems, avoiding incorrect classifications and decreasing the detection time. - choose best network metrics that can increase the system performance - if a more data is available try space aggregation techniques, as in Argus - correlate path change in traceroute with changes in end-to-end metrics

Bibliography

- [1] WIKIPEDIA. “Hellinger distance”. 2016. https://en.wikipedia.org/wiki/Hellinger_distance/.
- [2] KIFER, D., BEN-DAVID, S., GEHRKE, J. “Detecting Change in Data Streams”. In: *Proceedings of the Thirtieth International Conference on Very Large Data Bases - Volume 30*, VLDB '04, pp. 180–191. VLDB Endowment, 2004. ISBN: 0-12-088469-0. Disponível em: <<http://dl.acm.org/citation.cfm?id=1316689.1316707>>.
- [3] MAIDSTONE, R., HOCKING, T., RIGAILL, G., et al. “On optimal multiple changepoint algorithms for large data”, *Statistics and Computing*, pp. 1–15, 2016.
- [4] KILLICK, R., FEARNHEAD, P., ECKLEY, I. “Optimal detection of change-points with a linear computational cost”, *Journal of the American Statistical Association*, v. 107, n. 500, pp. 1590–1598, 2012.
- [5] HAYNES, K., ECKLEY, I. A., FEARNHEAD, P. “Computationally Efficient Changepoint Detection for a Range of Penalties”, *Journal of Computational and Graphical Statistics*, v. 0, n. ja, pp. 1–28, 0. doi: 10.1080/10618600.2015.1116445. Disponível em: <<http://dx.doi.org/10.1080/10618600.2015.1116445>>.
- [6] KEHAGIAS, A. “A hidden Markov model segmentation procedure for hydrological and environmental time series”, *Stochastic Environmental Research and Risk Assessment*, v. 18, n. 2, pp. 117–130, 2004. ISSN: 1436-3259. doi: 10.1007/s00477-003-0145-5. Disponível em: <<http://dx.doi.org/10.1007/s00477-003-0145-5>>.
- [7] LUONG, T. M., ROZENHOLC, Y., NUEL, G. “Fast estimation of posterior probabilities in change-point analysis through a constrained hidden Markov model”, *Computational Statistics and Data Analysis*, v. 68, pp. 129 – 140, 2013. ISSN: 0167-9473. doi: <http://dx.doi.org/10.1016/>

j.csda.2013.06.020. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S0167947313002326>>.

- [8] MONTAÑEZ, G. D., AMIZADEH, S., LAPTEV, N. “Inertial Hidden Markov Models: Modeling Change in Multivariate Time Series”. In: *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence*, AAAI’15, pp. 1819–1825. AAAI Press, 2015. ISBN: 0-262-51129-0. Disponível em: <<http://dl.acm.org/citation.cfm?id=2886521.2886573>>.
- [9] FEARNHEAD, P. “Exact and efficient Bayesian inference for multiple change-point problems”, *Statistics and Computing*, v. 16, n. 2, pp. 203–213, 2006. doi: 10.1007/s11222-006-8450-8. Disponível em: <<http://dx.doi.org/10.1007/s11222-006-8450-8>>.
- [10] ADAMS, R. P., MACKAY, D. J. “Bayesian online changepoint detection”, *arXiv preprint arXiv:0710.3742*, 2007.
- [11] MENDES, D. X., SENEGES, G. D. S., SANTOS, G. H. A. D., et al. “A Preliminary Performance Measurement Study of Residential Broadband Services in Brazil”. In: *Proceedings of the 2016 Workshop on Fostering Latin-American Research in Data Communication Networks*, LANCOMM ’16, pp. 16–18, New York, NY, USA, 2016. ACM. ISBN: 978-1-4503-4426-5. doi: 2940116.2940135. Disponível em: <<http://doi.acm.org/2940116.2940135>>.
- [12] YAN, H., FLAVEL, A., GE, Z., et al. “Argus: End-to-end service anomaly detection and localization from an ISP’s point of view”. In: *2012 Proceedings IEEE INFOCOM*, pp. 2756–2760, March 2012. doi: 10.1109/INFOCOM.2012.6195694.
- [13] AUGER, I. E., LAWRENCE, C. E. “Algorithms for the optimal identification of segment neighborhoods”, *Bulletin of Mathematical Biology*, v. 51, n. 1, pp. 39–54, 1989. ISSN: 1522-9602. doi: 10.1007/BF02458835. Disponível em: <<http://dx.doi.org/10.1007/BF02458835>>.
- [14] JAMES, N. A., KEJARIWAL, A., MATTESON, D. S. “Leveraging Cloud Data to Mitigate User Experience from” Breaking Bad”, *arXiv preprint arXiv:1411.7955*, 2014.
- [15] LIU, S., YAMADA, M., COLLIER, N., et al. “Change-point detection in time-series data by relative density-ratio estimation”, *Neural Networks*, v. 43, pp. 72 – 83, 2013. ISSN: 0893-6080. doi: <http://dx.doi.org/10.1016/j>.

neunet.2013.01.012. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S0893608013000270>>.

- [16] HOCKING, T., RIGAILL, G., PHILIPPE VERT, J., et al. “Learning Sparse Penalties for Change-point Detection using Max Margin Interval Regression”. In: Dasgupta, S., Mcallester, D. (Eds.), *Proceedings of the 30th International Conference on Machine Learning (ICML-13)*, v. 28, pp. 172–180. JMLR Workshop and Conference Proceedings, maio 2013. Disponível em: <<http://jmlr.org/proceedings/papers/v28/hocking13.pdf>>.