A practical approach to forecast Quality of Service parameters considering outliers

Ilka Miloucheva Eberhard Müller
Salzburg Research, Jakob Haringer Str. 5/III
5020 Salzburg, Austria
ilka.miloucheva@salzburgresearch.at

Alessandro Anzaloni
Instituto Technologico de Aeronautica
Sao Jose dos Campos – SP-Brazil
anzaloni@ele.ita.br

Abstract

Autoregressive integrated moving average (ARIMA) models are used in different researches for modelling and forecasting of traffic and Quality of Service (QoS) parameter values in telecommunication networks to make reasonable short, medium- and long-term predictions.

We propose methodology to use ARIMA models for QoS prediction in network scenarios based on a preliminary detection and elimination of outliers in the time series data. Outliers are patterns describing QoS behaviour caused by fault events (route failure, operation anomalies, DoS attacks, misconfiguration, etc).

Practically, we show the feasibility of combination of ARIMA prediction with outlier detection for short and medium term forecasting (daily and monthly) using real world end-to-end delay QoS measurement data.

Keywords: ARIMA forecasting,, QoS, outlier, time series data, pattern recognition, network anomaly.

1. Introduction

Prediction of QoS based on real-world measurements is important for end user in order to select providers for optimal QoS provision of their application. Also Internet Service Providers are interested in the forecasting of the QoS in order to plan resource assignment to applications and users, to provide capacity planning and network dimensioning considering short-, medium- and long QoS forecasts based on real network measurements.

QoS forecast should consider that the most real-world time series data of QoS parameter values contain outliers, that are, extreme fluctuations due to rare and anomaly events [BID 02],[YSJ 00]. Outliers are identified by specific QoS pattern reflecting QoS behaviour which is due to abnormal events and exceptions, such as network anomalies and crash, Denial of Service Attacks, inter-domain behaviour due to misconfigurations, topology changes, etc. The detection of outliers is important in order to discard the impact of the unusual behaviour (due to anomaly) on the forecasting. Outliers of time series data of QoS parameter values are described by patterns; which do not appear to follow the characteristic distribution of the rest of the time series data data. Outliers indicate significant fault events and provide useful knowledge for the operation and management of the network.

In the inter-domain networking environment, significant kinds of outliers due to route failures [BID 02], BGP-4 misconfigrations [MWA 02], convergence [NM 02], route flap damping [MGVK 02], DoS attacks [CKT 02], could be identified.

Typically, outliers represent random errors that we would like to be able to control. This control could be more efficient if the cause of the outliers is detected. Theoretical approaches to relate outliers with their origins, i.e. their dependability of specific event patterns, are studied in different researches especially focussed on anomaly and fault studies in communication networks [BP 01], [JKR 02], [Ye 00], [SS 01].

As outliers represent QoS time series data patterns (behaviour), they have an influence on the slope of the regression line and consequently on the value of the correlation coefficient. A single outlier is capable of considerably changing the slope of the regression line and, consequently, the value of the correlation. Just one outlier can be entirely responsible for a high value of the correlation that otherwise (without the outlier) would be close to zero. Outliers may not only artificially increase the value of a correlation coefficient, but they can also decrease the value of a "legitimate" correlation.

A practical forecasting approach based on the preliminary outlier detection and elimination combined with short and medium term QoS prediction is proposed in this paper. The approach is based on the traditional highly successful methodology for forecasting , the so-called Box-Jenkins methodology, or Auto-Regressive Integrated Moving Average (ARIMA) modelling technique [BJR 94], [BD 02], [Pow 99]. ARIMA falls under the class of linear time series forecasting, because it postulates a linear dependency of the future value on the past values. In the area of telecommunication networks and services, the ARIMA modelling was studied for traffic modelling and prediction. A long-term Traffic Prediction based on ARIMA for the NSFNET Backbone is reported in [GP 94]. Fractional ARIMA are used for prediction of long-range dependent traffic [Il 00]. Using ARIMA for univariate and multivariate time series prediction of performance data describing large wide area data transfers is discussed in [VSF 02].

The contribution of this paper is the development of a simple method to detect and remove QoS outliers based on ARIMA forecasting which could be efficiently used for QoS prediction in networking scenarios considering the specific sources of the outliers. Similar approach in the area of econometrics for financial time series data is proposed by [GM 96] and realised in the public domain econometrics software [MC 02] which we use in the area of QoS data prediction. Using this system as experimental environment, the method for QoS forecasting based on outlier detection and elimination based on real world practical QoS measurement scenario is shown. Further work is proposed to enhance this methodology with identification of outliers based on interworking with technologies for anomaly event monitoring and detection. This paper is organised as follows. Section 2 is aimed at outlier identification in time series data of QoS parameters considering anomaly sources. A practical method combining ARIMA forecasting with preliminary outlier detection and elimination is discussed in section 3. Practical realisation of the approach in real networking scenario is shown in section 4. Section 5 concludes this paper with further outlook..

2. Outlier identification in time series data of QoS parameters considering anomaly sources

Outliers are specific QoS pattern (extreme values) which are due to anomaly events and exceptions. Outlier can have significant impact on the estimates of the model parameters of the time series data. Outlier patterns should be identified in order to augment the forecasting methods with techniques detection and discarding of outliers.

Detection of patterns (QoS behaviour) due to fault events, detection and reaction to network crowd, abuse and operation anomalies is addressed in recent works. Current research is aimed at detection of “outliers” and characterisation of abnormal QoS patterns in case of network failure, discussed, for instance in [BID 02], [PMFT 02]. Study of dependencies of anomaly events and QoS “outliers” (patterns) by using of different data mining approaches, as for instance pattern dependency algorithms is proposed in [OSGC 95], [OC 96].

Anomaly detection is aimed at identification of anomaly groups, which exhibit some invariant characteristics, using variety of techniques including simple statistics, time series analysis and wavelet analysis to characterise anomaly features.

Fault and general anomaly detection techniques in networks are important for classification of outliers found in time series data of QoS parameters. Most of this work focuses on how to detect accurately deviations from normal behaviour as well as analysing and characterising statistically specific types of anomalous behaviour.

Grouping anomalies into different categories is useful for identification of different “outlier” sources in order to study “outlier” behaviour (i.e. pattern). Following typical fault events could be found in today networks :

- “Network Operation Anomalies” include network device outages, significant differences in network behaviour caused by configuration changes (e.g. adding new equipment or imposing rate limits) and by traffic reaching environmental limits. Anomalies in this category are distinguished by instantaneous changes in the QoS parameter values.

- "Flash Crowd Anomalies" typically due to either a software release (e.g. UW is a RedHat Linux mirror site) or external interest in a Web. Flash crowd behaviour is distinguished by a rapid rise in traffic flows of a particular type (e.g. FTP flows) or to a well known destination with a gradual drop off over time.
- "Network Abuse" such as DoS flood attacks and port scans. These types of abuse could be observed multiple times per week. Network abuse anomalies are distinct from network operation and flash crowd anomalies in that they are not always readily apparent in bit or packet rate measurements.

The general methodology for QoS outlier identification based on anomaly events and integration in forecasting system is given in the following figure:

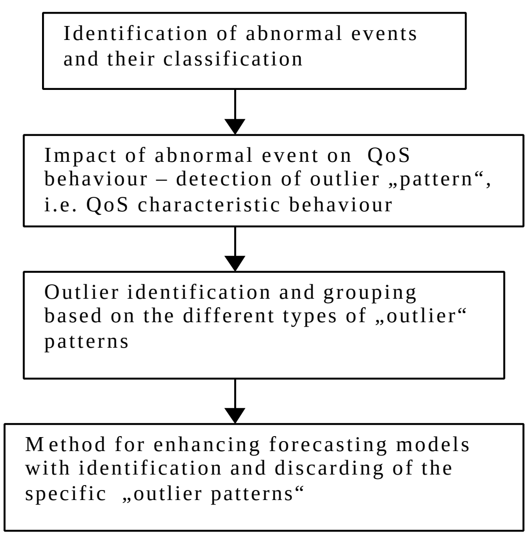

Figure 1: Identification of outlier classes and their patterns dependent on abnormal events

Building an archive of anomalies is the starting point for systematic QoS "outlier" research.
For this purpose different QoS monitoring technologies could be used, IP traffic flow measurements at the router, routing protocol monitoring, measurements at different intervals, etc.
One important direction for characterisation and classification of outliers of QoS data in WAN are traffic measurement techniques for monitoring routers and switches for anomalous traffic behaviour such as outages, configuration changes, flash crowds and abuse. A variety of commercial and open source tools have been developed to assist in this process, however these require policies and/or or thresholds to be defined by the user in order to trigger alerts.
For the identification of QoS outliers, the research on pattern detection in time series data could be considered, for instance in the area of econometrics [JDH 98], [FP 00], [Mon 02], [MC 02] [CMS 01]. Wavelet is a technique which could be efficiently applied for outlier pattern analysis [HFW 01]. Wavelets have advantages over standard Fourier analysis for data sets having sharp spikes. Wavelet analysis shed significant light on the structures of each anomaly and provide additional models for identifying and grouping of outliers. The better the description of the anomalous behaviour, the more effective could be detected the outlier pattern.
Extreme QoS parameter values during small interval exceeding some accepted QoS threshold are usually associated with a network change, e.g. a new route, or a link upgrade. They may also be associated with a remote host change, e.g. a new CPU, the Network Interface Card (NIC), etc. This kind of outliers we define as "additive" with a pattern looking like "spike" compared with the rest of the time series data.
Outlier could have the behaviour of "coffee breaks" as discussed by [SDG 00] in the framework of Voice-over-IP delay patterns. We observed that after some time the coffee breaks could lead to a "peak breaks" (figure 2):

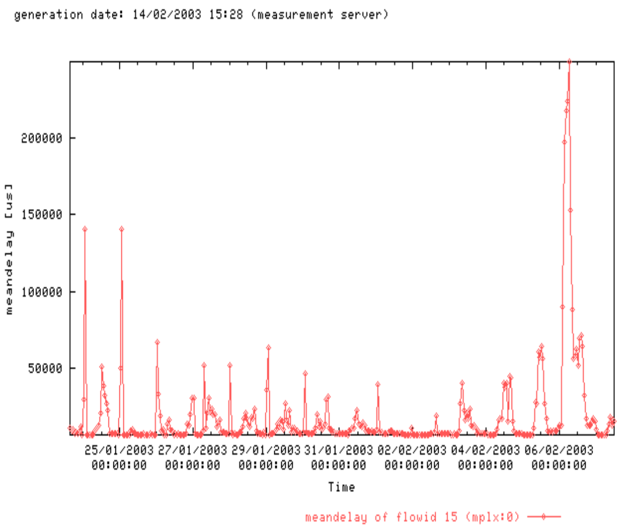

Figure 2: „Coffee“ and „peak“ break outlier in practical end-to-end QoS monitoring scenario

Many aspects of network QoS depend on spikes (peaks) that are caused by rare events:

- cell packet loss and queue overflow,
- worst cases in statistical multiplexing.

In context of the study of the different behaviour of minimum, mean and maximum delay time series data streams, [PMFT 02] observes that very large delay is caused by the implementation of the routers. For instance routers can stop the forwarding of the packets if they are busy with some resource intensive tasks.

In the inter-domain environment, link failures, policy and topological changes [MWA 02] can cause route recomputation and BGP-4 convergence. BGP-4 behaviour studied in different research could be source for specific QoS outliers. Characteristics of BGP-4 routing convergence have a high impact on the network's ability to perform quick route repairs and provide good performance in the presence of network faults [NM 02]. Currently inter-domain route repair convergence in the Internet may have a latency on the order of several minutes. During the latency period end-user QoS parameter are highly degraded i.e. outliers due to "BGP-4 convergence" are raised. Convergence time of BGP is dominated by an implicit MRAI timer setting, the length of the longest alternative AS path between the source and destination, and the set of all possible paths between source and destination. Path selection depends not only on individual timer settings but also on the interaction of timers on multiple alternative paths in a topology. Some BGP-4 routing policies have unpredictable effect on the flow of traffic and the end-to-end QoS in inter-domain environment [FBR 02]. Frequent route flapping causes route recomputation and increases the computation load on the route processor , rapid changes in network reachability and significantly exacerbation of the convergence times of relatively stable routes [MGVK 02]. A route is considered stable if it lasts at least tens of minutes. P*ersistent route oscillations are observed* that are probably caused by inconsistent setting of routing policies in autonomous systems which could last for several hours or more [NM 02].

Anomalies due to inter-domain route failures and BGP-4 (misconfiguration, etc) could be source for outliers of multivariate QoS parameter values. In this case, pattern dependencies of outliers in multivariate time series data (loss and delay behaviour patterns) could be studied.

Practical experience with "multivariate" QoS outlier in end-to-end QoS monitoring scenario (see section 4) is shown in the following figure:

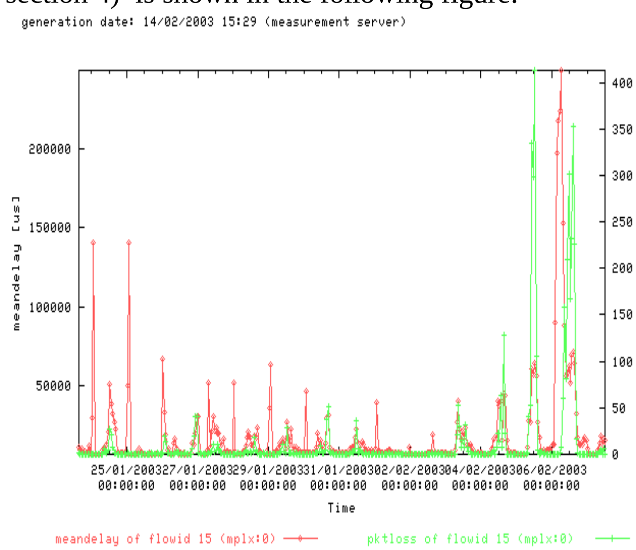

Figure 3: Multivariate QoS outliers - loss and delay

Multivariate QoS outlier are also experienced in the study of VoIP over wide area networks [BID 02] discovered that link failures may be followed by long periods of routing instability, during which packets can be dropped, because forwarded along invalid paths. Such instabilities can last for tens of minutes resulting in the loss of reachability of a large set of end-hosts.

“Congestion“ outliers could be due to fault events, but also based on underestimation of the network resources. When congestion occurs, there could be a significant packet loss and delay decrease for relatively longer periods compared with the shorter periods of “spike” outliers, i.e. severe congestion packets may be dropped or delayed for relatively long periods. Multivariate time series QoS patterns (delay, loss) could explain the congestion outliers in more detailed shape. For more detailed discussion of congestion “outlier” refer to [NLANRSurveyor]. In an uncongested path, the minimum, mean, and maximum time series data should be close to each other. It is expected that the variance of the minimum delay time series data is smaller compared with the mean delay and maximum stream data. In the “congestion” outlier pattern, the minimum delay would likely stay the same if there are not additional problems like routing failures. But the mean and maximum delay streams could "drift" from the blue points considerably. Such drift is a measure of congestion. Changes of the minimum delay values could indicate a change in the path or an extreme case of congestion.

Another outliers could be caused by Denial of Service attacks. [CKT 02] use spectral analysis techniques to identify patterns due to Denial of service attacks.

3. A practical approach for ARIMA forecasting with preliminary outlier identification

Considering that extreme outliers may bias the estimates of the seasonal and trend components of ARIMA model, we propose a practical method combining ARIMA forecasting with preliminary outlier detection and elimination. We consider outliers as extreme values which could be modified and dropped by the use of "statistical control principles", that is, values that are above or below a certain range (expressed in terms of multiples of sigma, the standard deviation), i.e. they could be modified or dropped before final estimates for the ARIMA model (seasonality, etc) are computed. Such outliers are called “additive” or “spike” outliers in the previous section.

Some similarity of our approach could be drown to the forecasting in the context of modelling co-evolving time sequence data addressed in [YSJ 00].

An ARIMA (p,d,q) model is an extension of a set of time series models called

- autoregressive of order p denoted by AR(p)
- moving average of order q denoted by MA(q), and
- autoregressive moving average denoted by ARMA(p,q).

ARMA model of order (p,q) is combination of AR(p) and MA(q). It predicts the current value of the time series based on p previous values and q previous shocks (i.e. random Gaussian noise).

Where the AR(p), MA(q) and ARMA(p,q) models require that the data be stationary, the ARIMA(p,d,q) model transforms the nonstationary data into stationary series by differencing parameter.

ARIMA model of order (p,d,q) is simply an ARMA (p,q) model that is differenced d times, i.e. d is parameter giving the degree of differentiation.

The concept related with the ARIMA model is that ARIMA forecasts the time series value based on the weighted sum of the p previous values of the process plus q which parameter is a random Gaussian noise (white noise).

The Gaussian noise process is characterised by zero mean and a finite variance.

The series data $\{X_t\}$ modelled with ARIMA (p,d, q) satisfies a difference equation of the form

$$\phi^*(B)\ X_t \equiv \phi\ (B)\ (1-B)\ ^d X_t = \theta(B)\ Z_t,\ \{Z_t\} \sim WN\ (0, \sigma^2)$$

where $\phi^*(z)$ and $\theta(z)$ are polynomials of degree p and q, respectively and $\phi\ (z) \neq 0$ for IzI <=0. The polynomial $\phi^*(z)$ has a zero of order d at z= 1. The process $\{X_t\}$ is stationary if and only if d = 0, in which case it reduces to ARMA(p,q) process.

According to this definition, if the ARIMA model parameters are correct, the estimation error will follow the Gaussian distribution $\{Z_t\}$ with 0 mean and standard deviation equal to σ.

Now we are using ARIMA to define a method for "outlier" detection which could be applied to time series data of QoS parameter values.

Informally an outlier is a value that is very different from what we expected. Considering that the estimation error in ARIMA follows a Gaussian distribution with a standard deviation σ, than we label as "outlier" every sample of $\{X_t\}$ that is >= 2 σ away from the estimated value and replace it with estimated value considering ARIMA. The reason is that in a Gaussian distribution, 95% of the probability mass is within + /- 2σ from the mean.

This outlier detection method could be applied to identify different QoS outlier types in the networking scenarios based on sudden unexpected big values (spikes), for instance that which are originated by implementation biases in the routers [PMFT 02].

4. ARIMA forecasting technology considering outliers in real networking scenario

4.1. Experimental software environment for ARIMA forecasting considering outliers

The experimental environment is based on the TSW public domain software (www.bde.es) including TRAMO/TERROR programs used for financial purposes obtained from the bank of Spain [MC 02] [CMS 01].

The background of this software is a methodology (and an associated program) for automatic (or manual) identification of ARIMA models, when observations may be missing and the series may be contaminated by outliers and by special effects (in particular, calendar effects). The automatic performance of program TRAMO ("Time Series Regression with ARIMA noise, Missing values, and Outliers") has been intensively tested and it has proved fast and reliable [FP 00]. TRAMO's automatic model identification procedure is in fact being adapted and incorporated to the official X12 ARIMA US-Bureau of the Census program [Mon 02].

The additive outlier detection combined with ARIMA in TRAMO was found usable to realise the concept of ARIMA forecasting based on the QoS outlier detection.

For each series, the program automatically identifies an ARIMA model, detects and corrects for several types of outliers, and, if appropriate, estimates calendar effects. It also interpolates missing observations if there are any. Next, the one-period-ahead out-of-sample forecast of the series is computed and compared with the new observation. In brief, when the forecast error is, in absolute value, larger than some a priori specified limit, the new observation is identified as a possible error. Summary results for all series and for the aggregate set are also provided.

Program TERROR is simply an application of TRAMO, executed in an automatic manner to the problem of quality control in time series (with several possible options). The program identifies a REG-ARIMA model for each series (perhaps with missing values, outliers, and some deterministic effects) and obtains the standardised forecast error for the period associated with the new data (which is not considered in the process of model identification and forecasting). TERROR is designed to handle large sets of time series with a monthly or lower frequency of observation.

4.2. Experimental testbed

The QoS are monitored between Salzburg Research network and ISP provider network with CM Toolset [AQUILA], [MH 01], [SDH 01}, [HMSP 02]. CM Toolset is an agent based monitoring tool of QoS parameters of application flows. The following picture describes the networking scenario – monitoring of end-to-end delay between access network (Salzburg Research) and ISP (Austria Telekom). Such networking scenario is typical for today customers and providers of networking services and applications.

We have two routers between the end systems, the one of them is the access router of the customer network.

The customer is interested to obtain better QoS provision from ISP network and uses this scenario to study and forecast the end-to-end delay QoS.

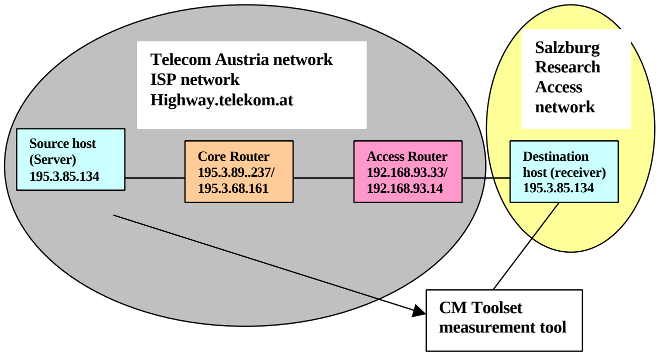

Figure 4: End-to-end QoS measurement scenario

The end-to-end delay monitoring information was aggregated on hourly base, i.e. mean values for QoS parameters are obtained each hour for a period of more weeks. Minimum and maximum delay streams were also obtained but not discussed in the forecasting method. The end-to-end delay measurement approach is based on GPS clock synchronisation.

4.3. Discussion of forecasting experiment and results

In our experiment we used end-to-end delay measurements from one week, exactly 180 delay samples obtained hourly during the week are considered. From the 180 data samples only the first 36 were used for ARIMA forecasting. The forecasted period was 24 (1 day). In order to study the impact of the outlier, an artificial additive outlier was used in the 18^{th} period.

In order to evaluate the impact of the artificial outliers, the following forecasting scenario was used:

- Forecasting using original data (without outlier)
- Forecasting without correction of outliers
- Forecasting with correction of outliers.

The three forecasting scenarios were compared with original data from the 36^{th} to 60^{th} sample (see figure 5).

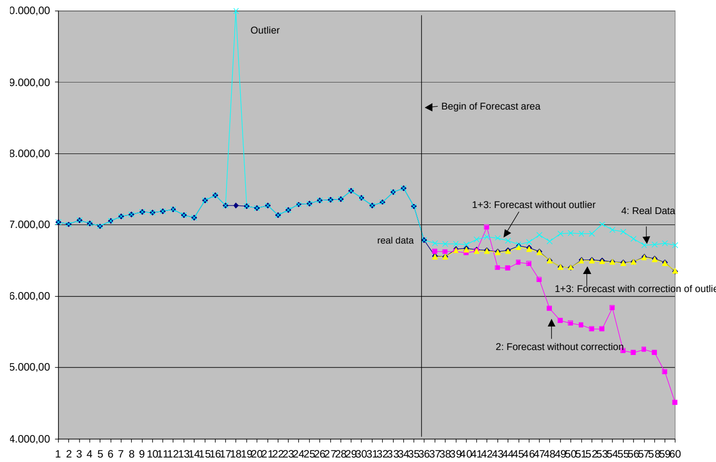

Figure 5: Comparison of different approaches for forecasting - forecast without outlier, with correction of outliers and without correction of outliers with the real data

The experiments have shown that the ARIMA forecast with detection and elimination of the additive outlier have similar behaviour to the real network data and to the forecast using time series data without outlier. The forecast without discarding of the outlier has shown that the outlier has significant impact on the estimates of the model parameters – the predicted values differentiate too much from the real measured QoS data.

5. Conclusions and further work

A methodology to use ARIMA models for QoS prediction of wide area network connections based on a preliminary detection and elimination of outliers in the time series data was proposed. The feasibility of the ARIMA QoS forecasting augmented with outlier removing was shown in a real world experiment for short and medium term forecasting (daily and monthly) using real QoS measurement data obtained during more weeks between customer and ISP network.

The results have shown that:

- Outliers could corrupt the forecasting values for the QoS parameters (delay).

- ARIMA can work in the short and mean range of QoS forecasting periods.

This research is done in the framework of European INTERMON IST project [INTERMON] project and in international research cooperations between ITA Brasil- and Salzburg Research Austria.

Further work will include:

- Analysis of outlier templates (patterns) that can appear in specific networking scenarios
- Understanding of sources of outliers (anomaly grouping and detection [BP 01], [SS 01])
- Study of dependencies between outliers and their sources using data mining techniques such as pattern dependency analysis [OSGC 95], [OC 96]
- New algorithms for outlier detection and elimination considering practical experiments in networking scenarios
- Study of the feasibility of new forecasting techniques for QoS prediction in networking scenarios. In this work we used ARIMA, but other techniques like non-linear forecasting methods constitute an open research area [BD 02], [CE 92] and could be tried.

The integration of the proposed measurement based forecasting method of QoS with technologies and tools for event detection and monitoring of fault events (route failure, operation anomalies, DoS attacks, misconfiguration, etc) is highly desirable to detect the source of the anomalies.

Especially, in the area of inter-domain networking, emerging systems for BGP monitoring, for instance [LZ 02], could be combined with the proposed forecasting technology based on outliers to predict more powerful the inter-domain QoS behaviour. Furthermore, techniques of pattern detection and pattern dependencies in multivariate time series data in combination with technology for event detection and monitoring could be experimented in integrated QoS and event analysis systems.

6. References

[GP 94] N.K. Groschwitz and G.C. Polyzos, "A Time-Series Model of Long-term Traffic on the NSFNET Backbone," Proc. IEEE International Conference on Communications (ICC'94), New Orleans, LA, pp. 1400-1404, May 1994.

[YSJ 00] B.-K. Yi, N.D. Sidiropoulos, T. Johnson, H.V. Jagadish. C. Faloutsos. A. Biliris, Online Data Mining for Co-volving Time Series, ICDE 2000

[NM 02] Johan Nykvist and Lenka Carr-Motyckov a Simulating Convergence Properties of BGP, ICCCN 2002

[MWA 02] R. Mahajan, D. Wetherall, T.Anderson, Understanding BGP Misconfiguration, *ACM SIGCOMM*, Aug 2002

[BID 02] C.Boutremans, G.Iannaccone and C.Diot, *"Impact of Link Failures on VoIP performance"*, NOSSDAV 2002.

[MGVK 02] Zhuoqing Morley Mao, Ramesh Govindan, George Varghese, Randy Katz, Route Flap Damping Exacerbates Internet Routing Convergence, SIGCOMM 2002.

[CKT 02] Chen-Mou Cheng, H.T.Kung, Koan-Sin Tan, Use of Spectral Analysis in Defense Against DoS Attacks, GLOBECOM 2002

[BP 01] P. Barford and D. Plonka, “Characteristics of network traffic flow anomalies,” in *Proceedings of ACM SIGCOMM Internet Measurement Work-sho*p,
San Francisco, CA, November 2001.

[Ye 00] N. Ye, “A markov chain model of temporal behaviour for anomaly detection,” in Workshop on Information Assurance and Security, West Point, NY, June 2000.

[Pow 99]R. S. Povinelli. The time series data mining: identifying temporal patterns for characterisation and prediction of time series events, Dissertation, Wisconsin 1999

[OSGC 95] T. Oates, M.D. Schmill. D.E. Gregory, P.R. Cohen. Detecting complex dependencies in categorical data. In Finding Structure in Data: Artificial intelligence and Statistics, p.185-195, 1995

[OC 96] T. Oates, P.R. Cohen, Searching for structure in multiple streams of data. In Proceedings of the Thirteenth International Conference on Machine Learning, 346-354, 1996

[SS 01] M. Steinder and A. S. Sethi. The present and future of event correlation: A need for end-to-end service fault localisation. *In Proc. World Multi-Conf. Systemics, Cybernetics, and Informatics (SCI)*, Orlando, FL, 2001, vol. XII, pp. 124-129.

[BJR 94]G. Box and G. Jenkins, G. Reinsel, Time series Analysis: Forecasting and control, revised ed., Prentice Hall , 3rd Edition

[BD 02] P.J. Brockwell, R.A. Davis, Introduction to Time Series and Forecasting, Springer Verlag, 2002

[VSF 02] S. Vazhkudai, J.Schorf, I.Foster, Predicting the performance of wide area data transfers. In 16th International Parallel and distributed Processing symposium (IPDPS). 2002, Fort Lauderdale, Florida: IEEE Press

[JKR 02] J. Jung, B. Krishnamurthy, and M. Rabinovich, “Flash crowds and denial of service attacks: Characterisation and implications for CDNs and web sites,” in *WWW-0*2, Hawaii, May 2002.

[CE 92] M. Castagli, S. Eubank, Nonlinear Modelling and Forecasting, Addison Wesley, 1992

[Il 00] J. Ilow, ``Forecasting Network Traffic Using FARIMA Models with Heavy Tailed Innovations'', *ICASSP 2000*, Istanbul, Turkey, June 2000.

[LZ 02] Yihua Liao and Ke Zhang, "BGP Behavior Monitoring and Analysis", ECS 289M (Advanced Topics in Computer Security) project, Spring 2002, http://wwwcsif.cs.ucdavis.edu/~liaoy/research.html

[MC 02] A. Maravall and G. Caporello, A tool for Quality control of time series data, Program TERROR, Bank of Spain, Presented at the conference “Challenges to Central Bank Statistical Activities”, Irving Fisher Committee (ISI) and Bank for International Settlements, Basel, August 2002.

[CMS 01] G. Caporello, A. Maravall and F. J. Sanchez, Program TSW Reference Manual, Banco de Espana, 2001

[HMSP 02] U. Hofmann, I. Miloucheva, F. Strohmeier, T. Pfeiffenberger, Evaluation of architectures for QoS analysis of applications in Internet environment, The 10th International Conference on Telecommunication Systems, Modeling and Analysis Monterey, CA, USA, October 3-6, 2002

[SDH 01] F. Strohmeier, H. Dörken, B. Hechenleitner. AQUILA Distributed QoS Measurement. In Proc. of COMOCON8 Conference, Crete, Greece, pages 177-185, June 2001.

[AQUILA] AQUILA consortium, “Adaptive Resource Control for QoS Using an IP-based Layered Architecture”, AQUILA homepage: http://www.ist-aquila.org

[MH 01] I. Miloucheva, U. Hofmann, Distributed Measurement and Monitoring in IP Networks (CMToolset for AQUILA DiffServ), SCI 2001 /ISAS 2001 Orlando 7/2001

[INTERMON] Advanced architecture for INTER-domain quality of service MONitoring, modelling and visualisation,INTERMON-IST-2001-3412 http://www.ist-intermon.org

[PMFT 02] K. Papagiannali, S. Moon, C. Fraleigh, P. Thiran, F. Tobagi, C. Diod, Analysis of Measured Single-Hop Delay from an Operational Backbone Network, *in Proceedings of INFOCOM 2002*, June 2002, New York

[FP 00] B. Fischer, C. Planas (2000), "Large Scale Fitting of Regression Models with ARIMA Errors," *Journal of Official Statistics, 16, 173-18*4.

[Mon 02] B. C. Monsell “An Update of the Development of the X-12-ARIMA Seasonal Adjustment Program”, *Modeling Seasonality and Periodicit*y, Proceedings of the 3 rd International Symposium on Frontiers of Time Series Modeling, The Institute of Statistical Mathematics, Tokyo: Japan, January 2002.

[GM 96] GÓMEZ, V. and MARAVALL, A. (1996), "Programs TRAMO (Time series Regression with Arima noise, Missing observations, and Outliers) and SEATS (Signal Extraction in Arima Time Series). Instructions for the User", Working Paper 9628, Servicio de Estudios, Banco de España.

[HFW 01] Polly Huang, Anja Feldmann, and Walter Willinger. A non-intrusive, wavelet-based approach to detecting network performance problems. In *Proceeding of ACM SIGCOMM Internet Measurement Workshop 200*1, San Francisco Bay Area, November 2001

[NLANRSurveyor] http://dast.nlanr.net/Articles/measurements/surveyor.html

[JDH 98] Hamilton, J.D., «A new approach to the economic analysis of nonstationary time series and the business cycle», Econometrics, 2, 357-384, 1989

[SDG 00] S. Salza, M. Draoli, C. Gaibisso, A. Laureti Palma, R. Puccinelli, Methods and Tools for the Objective Evaluation of Voice-over-IP Communications , INETProceedings, 2000, http://www.isoc.org/isoc/conferences/inet/00/cdproceedgs/1i/1i_2.htm

[FBR 02] N. Feamster, J. Borkenhagen, J. Rexford, Controlling the Impact of BGP Policy changes on IP traffic, ACM SIGCOMM Internet Measurement Workshop, 2002