

# Analysis of Failures Characteristics in the UNINETT IP Backbone Network

Andrés J. González and Bjarne E. Helvik

Centre for Quantifiable Quality of Service in Communication Systems\*

Norwegian University of Science and Technology, O.S. Bragstads plass 2E, N-7491. Trondheim, Norway

Email: {andresgm,bjarne}@q2s.ntnu.no

Phone: (+47) 735 92783 , 735 92667 Fax: (+47) 73 59 27 90

**Abstract**—Core backbone networks must be designed to guarantee high levels of availability. Any interruption in the services that they provide may have massive consequences. For this reason there is a huge interest in developing methods able to keep the network robustness in the desired level. For the design of these methods are used models that need input information such as the operational state of network components which are stochastic variables. The aim of this paper is to provide an insight into the core networks behavior based on real operational data in order to help future related works to take more realistic assumptions. Based on failure logs provided by UNINETT we analyze availability levels and failure intensities in routers and links. We show that links may be classified in three groups with different properties. Additionally we observe that some links have similar dependability features than routers, making the perfect node assumption used on many related studies not correct. Finally, there were used parametrization techniques in order to fit the empirical processes with well-known distributions. We observe that the Weibull assumption that is traditionally used to model link failures processes fits properly the behavior of routers and short distance links but for the case of long distance fibers the gamma distribution seems to fit better.

## I. INTRODUCTION

Offer very high levels of availability in core networks is a matter of huge interest. The parameters to be guaranteed by the network operator are usually defined clearly in a Service Level Agreement (SLA) where the violation of the agreed values may have large economical and reputational consequences. There are many works interested in developing techniques that help to fulfill specific availability values. For instance in [4] is analyzed the relevance that interval availability analysis has on SLAs under unprotected and shared protected connections, assuming exponential and Weibull failure and repair distributions. In [5] is proposed an algorithm that allocates connections in network's links with assumed steady state availability values, fulfilling bandwidth and availability requirements. Nevertheless most of those works assume theoretical failure and reparation stochastic processes due to the lack of empirical based information.

Analysis of real failure processes in networks are mandatory in order to get the appropriate information for availability

dimensioning and to deal with the risks associated with SLA agreements. In spite of this, for a number of reasons, among them that failures of their network are not what operators like to have exposed in a competitive commercial marketplace, the access to such failure log information is very limited. In [2] a study of spatial and temporal failures and outages in an access network was performed to assess availability. A study of the failure behavior in an operational backbone network is reported by Iannaccone et al. [6]. They examine the frequency and duration of failure events and discuss various statistics, for instance the distribution of inter-failure times and distribution of link failure durations, nevertheless some information is missed given that for proprietary reasons they normalized the values shown. This work was continued by Markopoulou et al in [7], where failures and repairs in the Sprint IP backbone Network are classified and analyzed.

Our work is based on operational data and is focused on evaluate availability parameters on links and routers, and characterize the observed failure process using fitting and estimation techniques. The investigation is based on logged failures made available by the Norwegian academic network operator UNINETT [10]. The results shown here are based on observations made since January 2008 until December 2009 given that during this period the core network did not suffer relevant changes neither in topology nor infrastructure.

We classify the network devices according to the failure processes that affect them, obtaining four different groups. Then we evaluate availability values and failure intensities in order to know the differences and similarities between those groups and also to have an initial impression of the dependability features of the UNINETT core network. Based on the obtained results we study the consequences of assuming perfect routers, giving the popularity of this assumption in some related studies.

An important objective in this paper is to fit the observed failure processes with well known distributions in order to offer information that may be used as operational based input in future studies. There are many procedures in order to have trustable distribution fitting of dependability sampled data like quantile-quantile plots (Q-Q plots) and the method of maximum likelihood estimation. Additionally, specific tests that evaluate whether a data set is well-modeled by the estimated distributions or not may be implemented. In [3] and [8] is

\*“Centre for Quantifiable Quality of Service in Communication Systems, Centre of Excellence” appointed by The Research Council of Norway, funded by the Research Council, NTNU, UNINETT and Telenor. <http://www.q2s.ntnu.no>

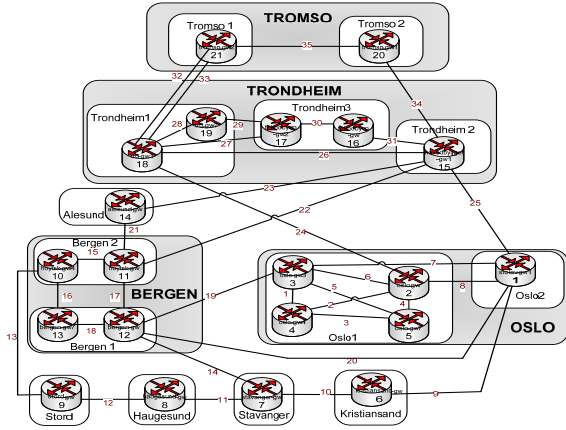


Fig. 1. UNINETT Core Network Topology.

presented a statistical toolkit to perform these procedures.

We found a clear difference between the failure processes that affect fibers that interconnect short and long distances. In this way we show that the Weibull assumption that is traditionally assumed for modeling link failures processes is not precise for the case of long distance fibers where the gamma distribution is a more accurate decision.

This paper is organized as follows. First, the UNINETT’s IP backbone network and the information collection method are presented. In Section III are analyzed features as failure intensity and unavailability values. Section IV explains the different techniques used for the characterization of failure processes, analyze the obtained results through the use of cumulative density and hazard functions and show the estimated values. Finally Section V concludes the paper summarizing the most relevant findings of this study.

## II. UNINETT NETWORK DESCRIPTION

UNINETT is the network that connects universities, colleges and research institutions in Norway. The core of the network interconnects the main norwegian cities through optical fiber connections of 10 and 2.5 gigabit per second (Gbps) forming rings to ensure that the loss of a single link does not cause any loss of connectivity.

In this paper we are interested in analyze the features of core networks, therefore we select the subset of connections considered by UNINETT as the backbone. They are at the same time the connections that interconnect the main cities in Norway as is shown in figure 1. The failure and reparation processes of the routers and links shown in this figure will be analyzed in the next chapters.

The failure logs were obtained through a centralized network management controlled form the UNINETT NOC (Network Operations Center) in Trondheim that register irregularities in the network at the IP level. The analysis performed in this paper belongs to the period form January 2008 to December 2009 given that during this time the network did not suffer any relevant change neither in the topology nor in the devices used for transmission. Router’s and link’s failures are

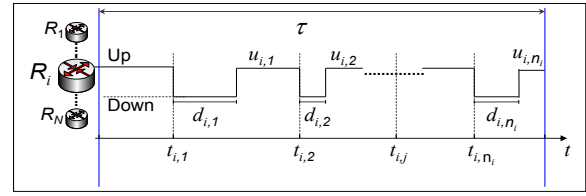


Fig. 2. On-Off behavior of a Network component.

TABLE I  
NETWORK DEVICE CLASSIFICATION

Group ID	Group Name	Characteristic
$G_1$	Routers	High Capacity Routers
$G_2$	Short Links	Same Room (Few meters fiber)
$G_3$	Medium Links	Same City (Few kilometers fiber)
$G_4$	Long Links	Inter City (Hundreds of kilometers fiber)

registered with a precision of seconds and the data collection method follows SNMP standards that enable the detection of changes in the network operation.

In our study, when a router goes down, the analyzed logs do not consider individual down reports for the links connected to it. Therefore we may assume that links and routers failures are analyzed independently.

A very important phase in our study was the “*filter phase*” when through the implementation of PERL scripts were obtained clean ON/OFF state information in time for each network component. Additionally we verified the obtained failure information using alternative mechanism as analysis of traffic logs.

The studied backbone is operated using WDM technology and routers form several brands that use IS-IS as routing protocol. Full details about the UNINETT topology can be found in [9].

## III. AVAILABILITY OF NETWORK COMPONENTS

A first objective in this paper is to have a general understanding of the main variables that may have an important role in the dependability of the UNINETT network. The network to be analyzed is shown in figure 1 and the observation period  $\tau$  is from January 2008 to December 2009 ( $\tau = 01/2008 - 12/2009$ ).

The following notation and considerations are used. The failure events on the described core network will be considered during  $\tau$ , where  $N$  network components are regarded. Each device  $i$  ( $i = 1, 2, \dots, N$ ) has an operational state that may be described by an ON/OFF signal as illustrates figure 2. A failure  $j$  occurs at time  $t_{i,j}$ . The downtime duration will be denoted by  $d_{i,j}$  and  $n_i$  is the total number of failures of device  $i$  during  $\tau$  and  $j = 1, 2, \dots, n_i$ . After the reparation, the time when the device is working properly before a new failure occurs will be defined as up-time and will be denoted as  $u_{i,j}$ .

In this study we classify the network devices according to common features that may be relevant for the dependability equipment in order to have a more organized information and to make easier the identification of similar stochastic behavior.

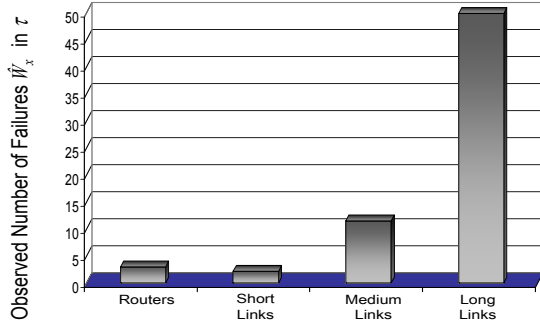


Fig. 3. Observed Number of failures  $\hat{W}_x$  during  $\tau$ .

Basically this classification is made in four different groups  $G_x$  ( $x = 1, 2, 3, 4$ ) as is shown in the table I, taking into account the trivial case where routers and links are studied separately. Additionally based on UNINETT experience we may say for instance that short distance links are affected most of the time by synchronization problems, electrical fluctuations and additionally for circumstances that may happen inside a controlled access room. On the other hand medium distance links have the probability of being affected by any related activity that occurs in the non controlled access areas between the connected routers where weather may have a small incidence, in addition to the short distance links threats. Finally, long distance links are fibers that connect far located cities, using usually the electrical and train system infrastructure. Therefore those connections have a much higher number of threats where giving the climatological norwegian conditions, weather may have a strong incidence.

The first variable to be studied is the average number of failures defined as follows:

$$\hat{W}_x = \sum_{i=1}^{M_x} \frac{n_i}{M_x}. \quad (1)$$

Where  $M_x$  is the total number of elements on  $G_x$ .

Taking into account that links and routers failures are analyzed separately, figure 3 illustrates how are distributed the different values of  $\hat{W}_x$  on each of the groups shown in table I, during the observation period  $\tau$ .

Many differences may be appreciated in this figure, e.g. the number of failures in long distance links is approximately fifteen times more than in routers and short distance links and 5 times more than medium distance links. This difference was expected, giving the bigger amount of threats that long distance fibers are exposed to. At the same time medium distance links present approximately four times more failures than routers and *same-room* links. Finally, we notice that devices from group  $G_1$  and  $G_2$  have similar average number of failures, representing a relevant warning for researches where the routers are assumed to be perfect, considering only links failures on the developed models.

On the other hand, we will also analyze availability levels on routers and links during the observation period  $\tau$ . The

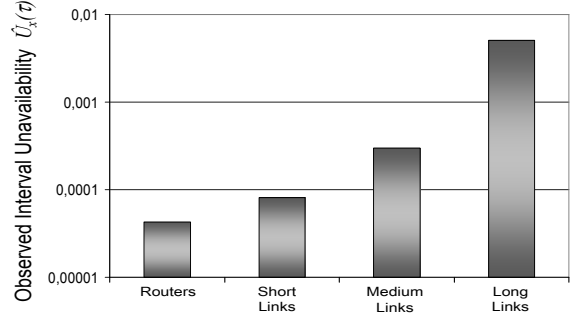


Fig. 4. Observed Average Interval Unavailability  $\hat{U}_x(\tau)$ .

observed unavailability  $\hat{U}_i(\tau)$  of a single component  $i$  will be calculated as follows:

$$\hat{U}_i(\tau) = \frac{\sum_{j=1}^{n_i} d_{i,j}}{\tau}. \quad (2)$$

Based on the classification made on table I, it is important to obtain the average unavailability per group  $G_x$  which will be calculated as indicate the next equation:

$$\hat{U}_x(\tau) = \sum_{i=1}^{M_x} \frac{\hat{U}_i(\tau)}{M_x}. \quad (3)$$

Where  $M_x$  is the total number of elements that belong to  $G_x$ .

Figure 4 shows the obtained values of  $\hat{U}_x(\tau)$  described in (3) where we may say for instance that the average time-out for short distance links and routers during  $\tau$  is in the order of minutes, for medium distance links is around 3 hours and for long distance links is almost two days.

#### IV. UP TIME DISTRIBUTIONS

In this section we analyze the stochastic behavior of the network components through the estimation of up time distributions.

First the methodology used for distribution fitting and for the estimation of parameters will be explained. Then we will show the result of applying the described methodology on the UNINETT failure logs, and finally the obtained results will be analyzed .

##### A. Distribution Fitting and Goodness of Fit

In this section we explain the methodology used to determine when the empirical data obtained from the UNINETT log failure may come from a known stochastic distribution.

A recommended initial procedure is the use of Q-Q plots that allow the comparison of the sampled data with well known distribution. However the use of more accurate techniques is needed in order to have stronger conclusions. We use the method of maximum likelihood estimation in order to estimate parameters that may fit a hypothesized theoretical distributions where respective confidence bonds are founded. We evaluate

if the empirical CDF does not lie beyond the limits of the confidence bounds to verify if the tentative CDF may fit the empirical data.

The resulting MLE information used to determine the parameters of the hypothesized CDF may be tested through the use of well known goodness-of-fit test i.e. Kolmogorov-Smirnov, Camer-von Mises and Anderson Darling.

Given that this kind of procedures are nowadays widely needed for the scientific community, the NIST has developed in cooperation with other institutions a well defined handbook [1] when all this issues are explained in detail as well as software that may be used to evaluate sampled data. In this paper we use some of the theoretical and software tools that they provide as well as other well know software tools such as Matlab and Wolfram Mathematica in order to verify the obtained results through different methods.

### B. Up-Time Fitting

Based on previous studies we are interested in verify if the components that make part of the UNINETT core network may be modeled by a Weibull distribution. In order to clarify the notation, the probability density function (pdf) of this distribution will be defined as follows:

$$f(t) = \frac{\beta(t)^{\beta-1}}{\theta\beta} e^{-\left(\frac{t}{\theta}\right)^\beta}, \forall t \geq 0, \theta > 0, \beta > 0. \quad (4)$$

Where  $\theta$  is the scale parameter and  $\beta$  the shape parameter.

We use the filtered data obtained from the UNINETT failure log and apply all the procedures explained in IV-A in order to verify if the Weibull distribution may be used to model up times behavior from the operational devices evaluated. In figure 5 we provide an example that describes the typical behavior observed when a Cumulative Distribution Function (CDF) fit is performed on up-times of routers and links with short and medium distance. This figure shows the maximum likelihood estimates (MLEs) for the parameters of a gamma and a Weibull distribution with respective confidence bounds of 95%.

When the upper confidence bound of the Gamma fit is observed, we can notice how the empirical CDF lies out of that limit for up-time values around  $0.1 \times 10^7$  seconds. This observation gives some hints about the convenience of the Weibull fit and on the other hand the low accuracy of the gamma fit. Nevertheless the estimated parameters were verified using the goodness-of-fit tests described in IV-A in order to prove that the up times of devices that belong to  $G_1$ ,  $G_2$  and  $G_3$  are well described by a Weibull distribution. This finding does not seem to be valid for the case of long distance links that interconnect far located cities.

The verified estimated parameters are shown explicitly in table II for the case of links. The values shown are based on equation (4), where the shape parameter ( $\beta$ ) is less than 1 for all the cases and where the scale parameter ( $\theta$ ) is given in seconds. Due to UNINETT is a network open for research proposes the parameters shown on this table are not

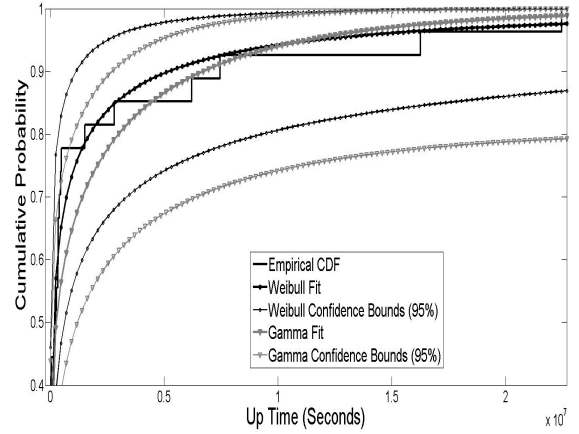


Fig. 5. Cumulative Distribution fitting for Up-Times in routers and links with short and medium distance.

TABLE II  
LINKS UP-TIMES THAT FIT A WEIBULL DISTRIBUTION

Link ID	Distance	Scale Parameter ( $\theta$ )	Shape Parameter ( $\beta$ )
15	Short	4450480	0,3645
16	Medium	1452318	0,3561
17	Medium	2684259	0,3573
18	Medium	400670	0,3254
26	Medium	1414095	0,331
27	Medium	4378835	0,4251

normalized, offering a big advantage and allowing their direct use.

Table III also shows the verified estimated parameters for the case of routers with enough number of samples in order to obtain trustable results and satisfy the goodness-of-fit test.

As we mention before, the Weibull fit is not valid for long distance links. Therefore we have to evaluate other options that may model better those up times. After developing the respective tests we found that the gamma distribution is a more accurate option.

In order to clarify the notation, the probability density function (pdf) of the gamma distribution will be defined as:

$$f(t) = \frac{(t)^{\alpha-1}}{\lambda^\alpha \Gamma(\alpha)} e^{-\left(\frac{t}{\lambda}\right)}, \forall t \geq 0, \lambda > 0, \alpha > 0. \quad (5)$$

Where  $\lambda$  is the scale parameter and  $\alpha$  the shape parameter.

In order to show more explicitly the difference with the Weibull fit performed before, in figure 6 is shown the typical result obtained when a CDF fit is performed for up-times on links that interconnect far located cities ( $G_4$ ). This figure also uses maximum likelihood estimates (MLEs) with confidence

TABLE III  
ROUTERS UP-TIMES THAT FIT A WEIBULL DISTRIBUTION

Link ID	Distribution	Scale Parameter ( $\theta$ )	Shape Parameter ( $\beta$ )
9	Weibull	1603156	0.549
13	Weibull	1819710	0.460
16	Weibull	5910717	0.358

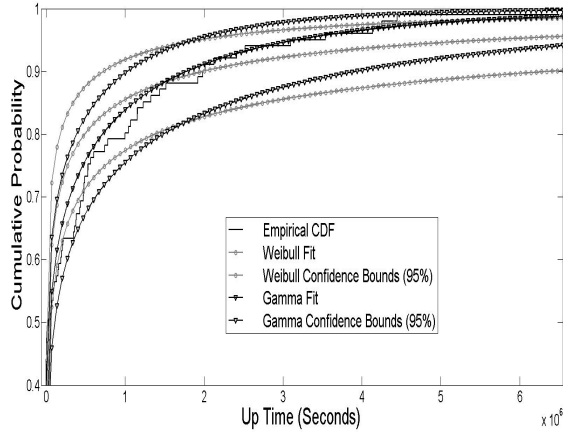


Fig. 6. Cumulative Distribution fitting for Up-Times in links that connect different cities.

TABLE IV  
LINKS UP-TIMES THAT FIT A GAMMA DISTRIBUTION

Link ID	Distance	Scale Parameter ( $\lambda$ )	Shape Parameter ( $\alpha$ )
9	Long	3419930	0,172
10	Long	6648830	0,175
11	Long	3104930	0,128
13	Long	2061830	0,138
14	Long	9526930	0,165
19	Long	11323500	0,154
20	Long	4162060	0,182
22	Long	3727250	0,348
23	Long	6125220	0,203
24	Long	8708750	0,244
25	Long	6200540	0,189

intervals of 95%. In this case we observe how the empirical CDF lies out of the lower confidence bound of the Weibull fit for up time values around  $0.5 \times 10^6$  seconds. As was made before, we performed the respective goodness-of-fit tests that confirm that the behavior of long distance links may be characterized by a gamma distribution.

The estimated parameters are shown explicitly in table IV (devices with enough number of samples that offer trustable results). The shown values are based on equation (5) where the shape parameter ( $\alpha$ ) is even shorter than for the case of Weibull fitting indicating a higher burstiness in the failure process. The scale parameter ( $\lambda$ ) is also given in seconds.

Table III also shows the verified estimated parameters for the case of routers and satisfy the goodness-of-fit test.

### C. Differences Between the Weibull and Gamma processes

We will study the differences between the gamma and the Weibull distributions in order to have a better understanding of the phenomenon described in the previous section.

From the theoretical point of view the Weibull and gamma distributions may be used to model monotonically increasing or decreasing failure rates. Those rates may be described by the failure rate function  $h(t)$ , which is the probability per time unit that a system fails during a short interval after having been operational without failure up to time  $t$ , defined as follows:

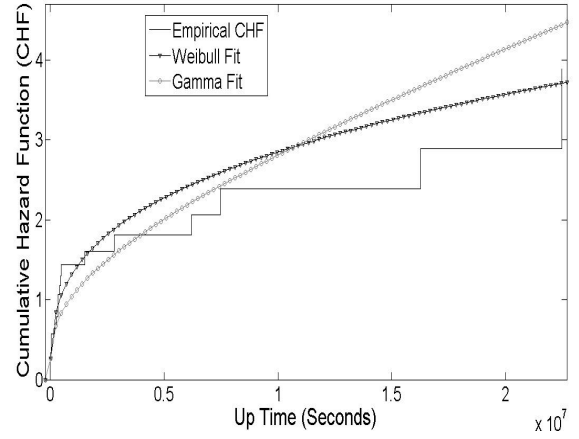


Fig. 7. Cumulative Hazard Function (CHF) fitting for Up-Times in routers and links with distance 2 and 1.

$$h(t) = \lim_{\Delta t \rightarrow 0} \frac{P(t < UP \leq t + \Delta t \mid UP > t)}{\Delta t} \quad (6)$$

The main difference between the gamma and the Weibull distribution lies on the fact that the failure rate function of the gamma distribution gets stable and tends to a constant real value for high  $UP$  values, contrary to the Weibull distribution where for shape parameters bigger than one the failure rate always increase up to infinity and for values of  $\beta$  shorter than 1 decrease monotonically, reaching values very close to 0.

Using the previous theoretical information and in order to verify the results observed on figures 6 and 5, now we will present the results obtained after fitting the Cumulative Hazard Function  $H(t) = \int_{-\infty}^t h(x)dx$ .

In figure 7 we show the typical behavior observed when a CHF fit is performed for up-times on devices that belongs to  $G_1$ ,  $G_2$  and  $G_3$ . The Weibull fit shows a CHF with a big increase at the beginning of the curve, for short up-time values that gradually reduce the increase rate up to 0 ( $dH_w(t)/dt \rightarrow 0$ ) for big up-times, describing more precisely the empirical CHF observed. According to the hazard definition this fact indicates that when a devices has survive a long period the probability of failing per unit of time decrease considerably to values close to 0. The devices that present this behavior ( $G_1$ ,  $G_2$  and  $G_3$ ) are affected by failures which in some way may be controlled by the network operator, i.e. the probability that one of those devices survive for a very long up time is small (according to the CDF) but if this happens, that means that the threats have been controlled successfully. We may say that the longer the survival time, the bigger the probability of having optimal operational conditions.

On the other hand, figure 8 shows the typical behavior observed when a CHF fit is performed for up-times on links that interconnect far located cities ( $G_4$ ). In this case the gamma fit shows a CHF with a more moderate increase rate than the Weibull fit for short up-time values and that gradually converge to a constant increase rate ( $dH_g(t)/dt \rightarrow C$ ), describing more

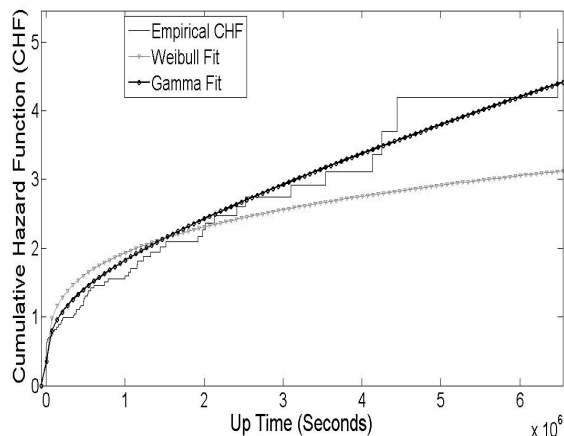


Fig. 8. Cumulative Hazard Function (CHF) fitting for Up-Times in link that connect different cities.

precisely the observed empirical behavior of this kind of links, indicating that when those devices have survive for a long period the probability of failing per unit of time is not reduced to values close to zero but get fixed in a constant value instead. For the case of  $G_4$  devices were identified in section III a bigger number of threats, where some of them are hard to be controlled e.g. weather conditions. Therefore we may say that for long distance links a long survival time imply just partial optimal operational conditions while there are some remaining threats that are out of the control of the operators.

The presented CHF figures confirm not only the results observed in figures 6 and 5 but also offer a clearer explanation of the observed difference, given that the theoretical differences of the Weibull and the gamma distribution are directly highlighted.

## V. CONCLUDING REMARKS

This paper yields an improved insight into the failure characteristics at a real operational core network. First is made a pre-classification based on the types of threats that may affect the devices. The differences and similarities among the defined groups were analyzed through the evaluation of the expected number of failures and the expected unavailability. It was found that the most unreliable kind of devices are the links that interconnect far located places, both in unavailability and number of failures. Three different orders of magnitudes were observed for unavailability values. First the routers and short distance links which present down times in the order of minutes, then the medium distance links with values in the order of hours and finally the long distance links where the total down time in the observation period may be specified in days.

A very interesting observation is the fact that routers and short distance links have similar behavior, making very unprecise the assumption made in some related works when the routers are assumed to be perfect, considering only failures on links.

For some UNINETT devices we confirm the findings of some previous works where the Weibull distribution seems to be a good option in order to model failure processes of network components. Nevertheless this assumption seems to be not valid for the case of links that cover long distances where the gamma distribution is a more accurate option, showing that when long distance links have survive a long period, the probability of failing per unit of time does not decrease monotonically up to zero but after some survival time this probability get fixed at some constant value. This phenomenon suggests that for routers and not very long links the longer the survival time, the bigger the probability to have optimal operational conditions, while for the case of long fibers there are some threats out of the control of the operators.

This work shows specific values that clearly describe the distributions that may fit up times of operational devices from a real network where the obtained shape parameters for long distance links suggest a high burstiness on the failure processes. Additionally the provided values do not have any kind of normalization, and for this reason this information may be useful for related works where this information is need as input.

## REFERENCES

- [1] NIST/SEMATECH. e-handbook of statistical methods, <http://www.itl.nist.gov/div898/handbook/>, 2010.
- [2] Baek Young Choi, Sejun Song, George Koffler, and Deep Medhi. Outage analysis of a university campus network. *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*, pages 675 – 680, 13-16 Aug. 2007.
- [3] G.A.P. Cirrone, S. Donadio, S. Guatelli, A. Mantero, B. Mascialino, S. Parlati, M.G. Pia, A. Pfeiffer, A. Ribon, and P. Viarengo. A goodness-of-fit statistical toolkit. *Nuclear Science, IEEE Transactions on*, 51(5):2056 – 2063, oct. 2004.
- [4] A.J. Gonzalez and B.E. Helvik. Guaranteeing service availability in SLAs; a study of the risk associated with contract period and failure process. *Communications, 2009. LATINCOM '09. IEEE Latin-American Conference on*, pages 1 –6, sep. 2009.
- [5] A.J. Gonzalez and B.E. Helvik. Dynamic sharing mechanism for guaranteed availability in mpls based networks. *International Communications Quality and Reliability Workshop Communications, CQR 2010*, Jun. 2010.
- [6] Gianluca Iannaccone, Chen nee Chuah, Richard Mortier, Supratik Bhattacharyya, and Christophe Diot. Analysis of link failures in an IP backbone. *In Proc. of the Internet Measurement Workshop*, pages 237–242, 2002.
- [7] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C. N. Chuah, Y. Ganjali, and C. Diot. Characterization of failures in an operational ip backbone network. *IEEE/ACM Transactions on Networking*, 16(4):749–762, Aug. 2008.
- [8] B. Mascialino, A. Pfeiffer, M. G. Pia, A. Ribon, and P. Viarengo. New developments of the goodness-of-fit statistical toolkit. *Nuclear Science, IEEE Transactions on*, 53(6):3834 –3841, dec. 2006.
- [9] The Norwegian Research Network UNINETT. Network Topology. [online]. Available at: <http://drift.uninett.no/stat-q/load-map/uninett,,traffic,peak>.
- [10] The Norwegian Research Network UNINETT. Status of Networks and Services. [online]. Available at: <http://drift.uninett.no/>.