Availability Analysis of Redundant Computer Networks: a Strategy Based on Reliability Importance

Almir Pereira Guimarães[1,2], Hélder May Nunes Oliveira[1] and Rodolfo Barros[1]
[1]Campus Arapiraca
Federal University of Alagoas
Arapiraca, AL, Brazil
e-mail: {almir, heldermay, rodolfobmoraes @arapiraca.ufal.br

Paulo R.M. Maciel[2]
[2]Center of Informatics
Federal University of Pernambuco
Recife, PE, Brazil
e-mail:{ prmm,apg2}@cin.ufpe.br

***Abstract*— In this paper, we investigate the dependability modeling of computer networks with redundancy mechanism. We use Stochastic Petri Net as an enabling modeling approach for analytical evaluation of complex scenarios. We apply our proposed modeling approach in a case study to evaluate the availability of computer networks in four different architectures. Reliability Importance is used to analyze the system availability according to the most important components.**

Keywords-availability; Reliability Importance; Stochastic Petri Nets; Computer Networks;

I. INTRODUCTION *(HEADING 1)*

In an ideal world, a communication network would be working perfectly at any time. In the real world, this is not the case. Random failures affect the network and may be due to physical failures, like fiber cuts, power outages, fires and earthquakes, software failures or failures resulting from unintentional human errors. The possibility of avoiding failures, which may put the business at risk, is an interesting track to be followed by organizations. The design, deployment and management of computer networks infrastructure ought to meet such requirements.

In the last few years, much has been done to deal with issues relating to the dependability of computer networks. Researchers have used different approaches to deal with these problems.

[2] presents a systematic approach for quantifying the reliability of enterprise VoIP networks. [2] provides an enhanced method and procedure of reliability calculation, using a network matrix representation and RBD (Reliability Block Diagram). [8] discusses algorithmic methods to obtain network availability values in a given topology and presents two tools for computation of network availability in large and complex networks. [5] presents a new classification of dependability and security models for systems and networks. And then it presents several individual model types such as availability, confidentiality, integrity, performance, reliability, survivability, safety and maintainability. The dependability/security models can be represented as combinatorial models, state-space models, and hierarchical models.

In this paper we focus on the availability of computer networks, including redundancy mechanisms. Four architectures are evaluated using dependability Stochastic Petri Net (SPN) [3] models. Reliability Importance is used to analyze the system availability according to the most important components. The model parameters used were obtained from manufacturers of network elements, as also from experimental measurements.

The rest of the paper is organized as follows: Section II presents basics of dependability requirements for computer networks, Reliability Importance and RBD. Section III describes the proposed dependability models. Section IV presents the combination of dependability models analysis and *Reliability Importance* values for a range of different architectures. Finally, Section V discusses the results of this study and introduces further ideas for future research.

II. FUNDAMENTAL CONCEPTS

A. Dependability Requirements for Computer Networks

Nowadays computing systems have been adopted for controlling a huge variety of applications, from domestic appliances to satellite systems, in which dependability requirements range in several magnitude orders. In military systems, banking, assurances, telecommunication, public health service, airtraffic control, among others, wrong delivered outputs may cause large economic losses or even human lives. Therefore, dependability is a key issue in such systems.

Dependability of a computer system must be understood as the ability to avoid service failures that are more frequent and more severe than is acceptable [1]. Dependability requirements encompass the concepts of availability, reliability, safety, integrity and maintainability [1].

Dependability evaluation may be carried out through either system measurement or analytical modeling. In many circumstances, modeling is the chosen method either because the system might not yet exist or due to the inherent complexity of creating and controlling specific scenarios. Inputs to dependability include component Mean Times to Failure (MTTF) models and Mean Times To Repair (MTTR). The hardware component MTTFs are supplied by the manufacturer and represent the mean time for a component failure. The MTTRs are tightly related to the maintenance policy adopted.

B. Reliability Importance

The main purpose of system reliability analysis is to identify the weakness in system components and to quantify the impact of failures. The so called *Reliability Importance* or *Birnbaum importance (B-importance)* approach [7] is used for this purpose.

The *Reliability Importance*, I_i^B, of a component is independent of the reliability of the component itself. We can say that the *Reliability Importance* of a component *i* is equal to the amount of increase (at time t) in system reliability when the reliability of component *i* is improved by one unit [7]. This measure provide a numerical rank to determine which components are more important to system reliability improvement or more critical to system failure.

According [7], the *Reliability Importance* of a component *i* is defined as:

$$I_i^B = (\partial Rs(p) / \partial p_i) \quad (1)$$

where p_i is the reliability of component *i*, p is the vector of component reliabilities, and the R_s is the reliability of the system.

This importance measure provide a numerical rank to determine which components are more important to system reliability improvement or more critical to system failure. In this paper, we will use I_i^B to analyze the behavior of the system availability according to the most important components in *Reliability Importance* view.

C. Reliability Block Diagram

A series-parallel reliability block diagram represents the logical structure of a system with regard to how the reliability of its components affect the system reliability [6]. In a block diagram model, components are combined into block in series, in parallel or in *k-out-of-n* configurations.

A series structure impose on a set of components means that, for the whole subsystem to work, every component has to be functioning. A parallel structure means that the whole subsystem can function if any one (or more) of the components is working. A *k-out-of-n* structure means that the whole subsystem can function if *k* or more of the components is working. In turn, series and parallel structures are special cases of *k-out-of-n* structures, a series structure being an *n-out-of-n* and a parallel structure being a *1-out-of-n* structure.

III. Proposed Dependability Models

In this section we present four SPN dependability models (Figures 4, 5, 6 and 7). These models can be evaluated using tools as SPNP (http://people.ee.duke.edu/) and TimeNet (http://www.tu-ilmenau.de/fakia/8086.html).

A. Platform Description

The following four architectures were used as a basis for the dependability models presented in this paper. They also served as experimental testbeds, from which some failure and recovery parameters were obtained. In each described architecture, we used the MyPhone tool as VoIP (myphone.sourceforge.net) workload generator. For data traffic, TFGEN (www.st.rim.or.jp/~yumo) traffic generator was used.

1) First and Second Architectures:

In the first architecture, the testbed is composed of two machines, a switch and two routers (they are named input router, R0, and output router, R2) that are connected by a single link (L0 - see Figure 1). If a component fails, the system goes down. In the second architecture, the testbed is composed of two machines, a switch and two routers that are connected by redundant links (L0 and L1 - see Figure 1). They are named input router (R0) and output router (R2). When the main link (L0) fails, the spare link (L1) assumes the role of the main one. After main link restoration, the system returns to initial condition.

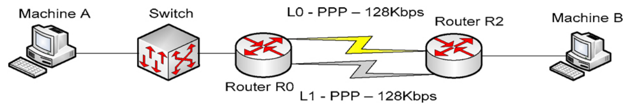


Figure 1: First and Second Architectures

2) Third Architecture

In this architecture, the testbed is composed of two machines, a switch and three routers (see Figure 2). They are named input routers (R0 and R1) and output router (R2). When one of the primary components (R0 or L0) fails, the spare components (R1 and L1) assume the role of the primary components. This switchover process takes a time period that represents the spare components starting operation. After restoration, the system returns to the initial condition.

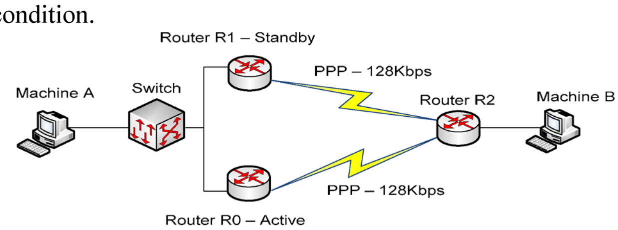


Figure 2: Third Architecture

3) Fourth Architecture

In this architecture, the testbed is composed of two machines, two switches and four routers (see Figure 3). They are named input routers (R0 and R1) and output routers (R2 and R3). When one of the primary components (R0, L0 and R2) fail, the spare components (R1, L1 and R3) assume the role of the primary components. This switchover process takes a time period that represents the spare components starting operation. After restoration, the system returns to the initial condition.

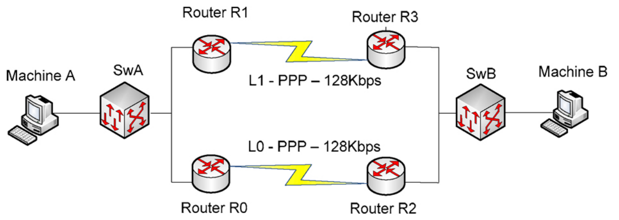


Figure 3: Fourth Architecture

B. *Dependability Model – First Architecture*

The model considers a system that has no redundancy (see Figure 4). The model includes six places, which are R0_ON, R0_OFF, with corresponding places of L0 and R2 components. Places R0_ON and R0_OFF, along with their corresponding pairs, model component's activity and inactivity states, respectively. These components have two parameters, namely MTTF and MTTR, which represent delays associated to corresponding exponential transitions X_MTTF and X_MTTR. In this section, label "X" must be instantiated according to the component name (see Figure 4). This model can compute the availability of the system through *SAFA* variable (*SystemAvailabilityFirstArchitecture*, *SAFA* = P{(#R0_ON=1) AND (#L0_ON=1) AND (#R2_ON=1)}). This expression represents the probability that the system is up.

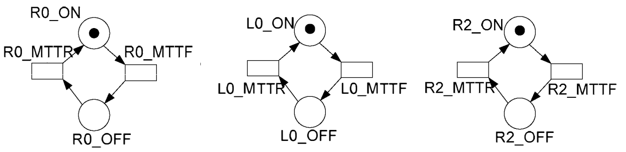


Figure 4: Dependability Model – First Architecture

C. *Dependability Model – Second Architecture*

The model considers a system that has redundancy at the link level (see Figure 5). The model includes ten places, which are R0_ON, R0_OFF, with corresponding places of L0, ASL0 (ActiveSpareL0), SL0 (SpareL0) and R2 components. SL0 and ASL0 represent the spare component of L0 in following situations: SL0 represents the spare component of L0 in active and not operational state. ASL0 represents the spare component of L0 in active and operational state. Places R0_ON and R0_OFF, along with their corresponding pairs, model component's activity and inactivity states, respectively. These components have two parameters, namely MTTF and MTTR, which represent delays associated to exponential transitions X_MTTF and X_MTTR. The spare component, in active and not operational state, has a value of delay (SL0_MTTF) 50% higher than exponential timed transition ASL0_MTTF.

Exponential transition ACT_SP represents the spare component starting operation. This time period (delay), in hours, is named Mean Time to Activate (MTA). As the primary component fails, the transition ACT_SP is fired. This transition firing represents the spare component taking over the failed one. In turn, immediate transition DCT_SP represents the return to normal operation.

This model can compute the availability of the system through *SASA variable* (*SystemAvailabilitySecondArchitecture*, *SASA* = P{(#R0_ON=1) AND (#L0_ON=1 OR #ASL0_ON=1) AND (#R2_ON=1)}). This expression represents the probability that the system is up.

D. *Dependability Model – Third Architecture*

The dependability model represents aspects of faulttolerance based on the so-called *cold-standby* redundancy approach (see Figure 6). The model includes ten relevant places, which are R0_ON, R0_OFF, with corresponding places of R1, R2, L0 and L1 components. Places R0_ON and R0_OFF, along with their corresponding pairs, model component's activity and inactivity states, respectively. These components have two parameters, namely MTTF and MTTR, which represent delays associated to corresponding exponential transitions X_MTTF and X_MTTR (see Figure 6). Exponential transitions ACT_SP_RT and ACT_SP_LK represent the spare components starting operation. This time period, in hours, is named MTA. As the primary components fail, the transitions ACT_SP_RT or ACT_SP_LK are fired. A firing in one of these transitions represent the spare component taking over the failed one. In turn, immediate transition DCT_SP represents the return to normal operation.

This model can compute the availability of the system through *SATA* variable (*SystemAvailabilityThirdArchitecture*, *SATA* = P{((#R0_ON=1 AND #L0_ON=1) OR (#R1_ON=1 AND #L1_ON=1)) AND #R2_ON=1*}*). This expression represents the probability that the system is up.

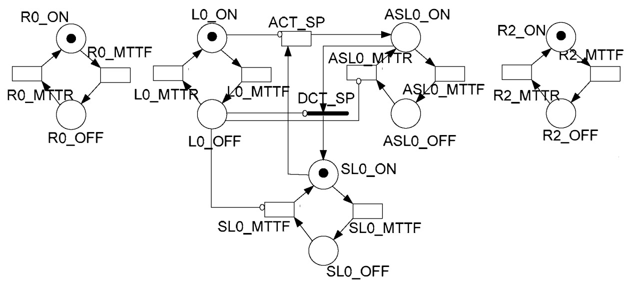


Figure 5: Dependability Model – Second Architecture

E. *Dependability Model – Fourth Architecture*

The dependability model (see Figure 7) represents aspects of fault-tolerance based on the so-called *cold-standby* redundancy approach. The model includes twelve relevant places, which are R0 ON, R0 OFF, with corresponding places of L0, R2, R1, L1 and R3 components. Places R0_ON and R0_OFF, along with their corresponding pairs, model component's activity and inactivity states, respectively. These components have two parameters, namely MTTF and MTTR, which represent delays associated to corresponding exponential transitions X_MTTF and X_MTTR (see Figure 7). Exponential transitions ACT_SP_R0, ACT_SP_L0 and ACT_SP_R2 represent the spare components starting operation. This time period, in hours, is named MTA. As the primary components fail, the transitions ACT_SP_R0, ACT_SP_L0 or ACT_SP_R2 are fired. These transitions firing represents the spare component taking over the failed one. In turn, immediate transition DCT_SP represents the return to normal operation.

This model can compute the availability of the system through *SAFA* variable (*SystemAvailabilityFourthArchitecture*, *SAFA* = P{((#R0_ON=1 AND #L0_ON=1 AND #R2_ON=1) OR (#R1_ON=1 AND #L1_ON=1 AND #R3_ON=1))}). This expression represents the probability that the system is up.

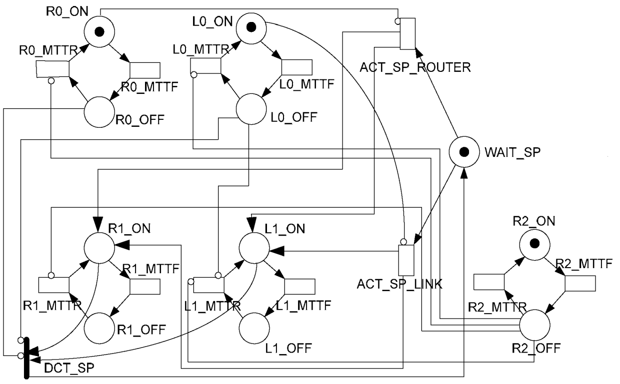


Figure 6: Dependability Model – Third Architecture

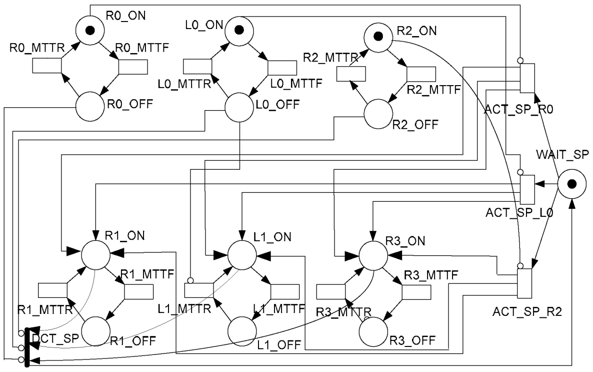
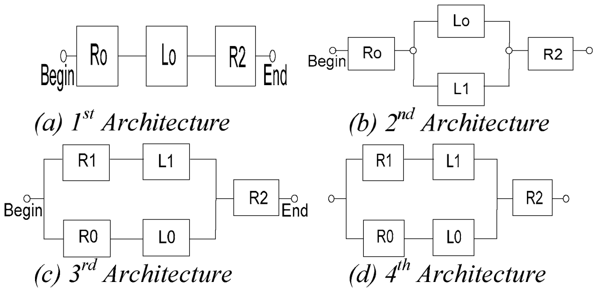


Figure 7: RBD Dependability Model - Fourth Architecture



(a) 1st Architecture *(b) 2nd Architecture*

(c) 3rd Architecture *(d) 4th Architecture*

Figure 8: RBD models of each architecture.

IV. CASE STUDY

Reliability importance values are valuable in establishing direction and prioritization of actions related to an upgrading effort in system design, or suggesting the most efficient way to operate and maintain system status. These values are calculated through analytical approaches. Initially, we consider the architectures shown in Section III-A. Our goal is to compute the network availability using the proposed dependability SPN models (see Section III) combined with *Reliability Importance* values.

The network equipments MTTF and Total Cost of Acquisition (TCA) used in this work are respectively: Component 1, 131,000 hours and US$ 8,390; Component 2, 105,000 hours and US$ 895; Component 3, 68,000 hours and US$ 1,095. The value of MTTR of twelve hours and a WAN link MTTF of 1,188 hours are used. For MTA, a value of 0.0027 hours for the second architecture and a value of 0.0416 for the third and fourth architectures are used. These values shall be considered as the base case throughout this section, unless another value is specified in each scenario.

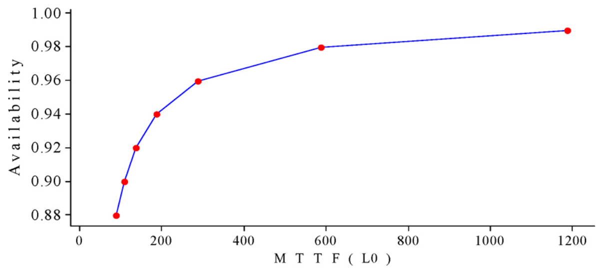


Figure. 9: System availability in accordance with MTTF (L0) – First architecture

System reliability is directly related to MTTF parameter, and the system availability is directly related to MTTF and MTTR parameters. Since MTTF >> MTTR, then we can also evaluate the system availability in terms of the components that have the highest *Reliability Importance* [7] values (see Section II-B).

Figure 8 shows the RBD models [6] used to calculate the *Reliability Importance* values. Figures 8(a), 8(b), 8(c) and 8(d)) show the models of the first, second, third and fourth architectures, respectively.

Reliability Importance is calculated using Astro software package (www.cin.ufpe.br/~bs/DesdacToolDownload) considering the system stationary state[1] in each architecture.

Table I shows the *Reliability Importance* values in each architecture. In the considered time, all the architectures were in stationary state. Link L0, in the first architecture, and links L0/L1 in second, third and fourth architectures, assume the greatest *Reliability Importance* values in system stationary state.

Any change in these components will have a major impact on system availability. Using the dependability SPN models (see Section III), we show the system availability variation in accordance with the most important components parameters.

The importance of the links L0 and L1 is confirmed in Figures 9, 10, 11 and 12. In turn, Figure 13 (Scenario 1,router R1 and first architecture; Scenario 2, router R0 and second architecture; Scenario 3, router R2 and third architecture; Scenario 4, router R3 and fourth architecture) shows that routers R0, R1, R2 and R3 have a smaller impact

[1] State in which the order of the *Reliability Importance* values will not change

on system availability. So, actions to increase the MTTF of links (L0 and L1) should be considered more important than additional efforts to enhance the MTTF of routers (R0, R1, R2 and R3). This kind of decision could not be easily made without an accurate analysis, based in Reliability Importance values, as we have performed in this case study

TABLE I. RELIABILITY IMPORTANCE VALUES

ARCH.	$I_1^B(L0)$	$I_1^B(L1)$	$I_1^B(R0)$	$I_1^B(R1)$	$I_1^B(R2)$	$I_1^B(R3)$
1	1.0	--	0.00126		0.00126	--
2	1.0	1.0	0.00253		0.00253	--
3	1.0	1.0	0.00126	0.00126	0.00253	--
	1.0	1.0	0.00126	0.00126	0.00126	0.00126

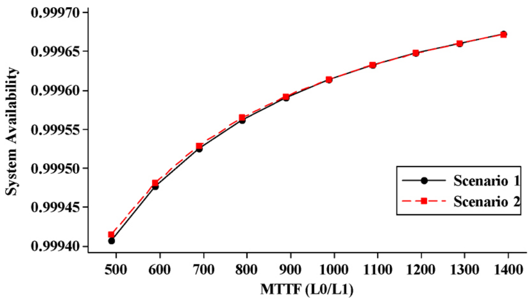


Figure. 10: System availability in accordance with MTTF (L0/L1) – Second architecture.

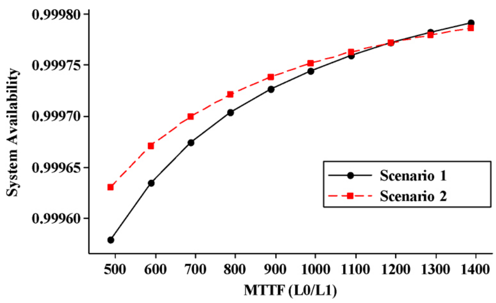


Figure. 11: System availability in accordance with MTTF (L0/L1) – Third architecture.

V. CONCLUSIONS

In this paper, we propose SPN models to evaluate several dependability aspects of computer networks in different architectures. The models support the analysis of system availability along with its services, based on different topologies, redundancy mechanisms and network elements. Reliability Importance was used to analyze the system availability according to the most important components.

For future work, we plan to extend these models to include network availability with redundant topologies, different recov- ery strategies as well as taking into account different failure modes.

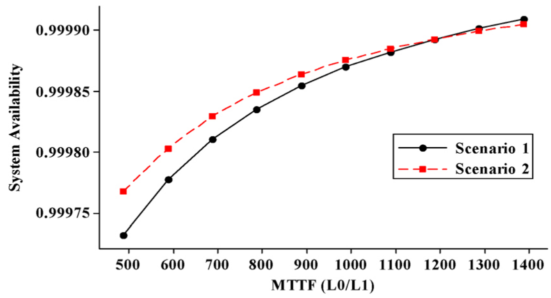


Figure. 12: System availability in accordance with MTTF (L0/L1) – Fourth architecture.

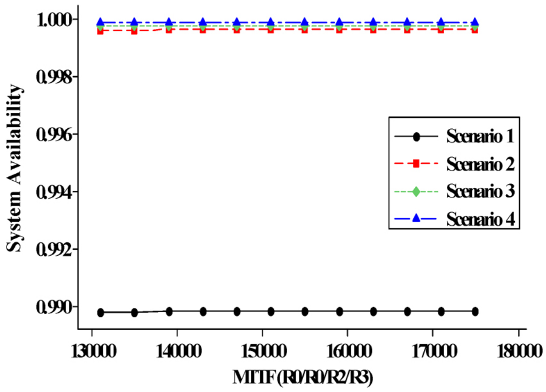


Figure. 13: System availability in accordance with MTTF – Different architectures.

REFERENCES

[1] A. Avizienis and J.C. Laprie and B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing", IEEE Transactions on Dependable and Secure Computing, vol. 1, number 1, pages 11 – 33, 2004.

[2] C.C.H. Kelvin, H. Pant, S.H. Richman and P. Wu, "Enterprise VoIP Reliability", Telecommunications Network Strategy and Planning Symposium, NETWORKS 2006, 12th International, pages 1 – 6, 2007.

[3] G. Bolch and S. Greiner and H. de Meer and K. S. Trivedi, "Queuing Networks and Markov Chain: Modeling and Performance Evaluation with computer Science Applications", ISBN 0-471-19366-6, 2nd edition, John Wiley & Sons, Wiley-Interscience, New York, NY, USA, 1998.

[4] K. S. Trivedi, "*Probability and Statistics with Reliability, Queuing and Computer Science Applications", ISBN 0-471-33341-7, John Wiley and Sons, New York, 2001.*

[5] K.S. Trivedi and D.S. Kim and A. Roy and D. Medhi, "Dependability and Security Models", 7th International Workshop on Design of Reliable Communication Networks, DRCN, pages 11 – 20, 2009.

[6] R. Sahner; K. S. Trivedi; A. Puliafito. "Performance and Reliability Analysis of Computer Systems", Kluwer Academic Publishers Group, ISBN: 0-7923-9650-2, 2002.

[7] W. Kuo and M.J. Zuo, "*Optimal Reliability Modeling:Principles and Applications". John Wiley & Sons. ISBN: 0-471-39761-X, Hoboken, New Jersey, 2003.*

[8] W. Zou and M. Janic and R. Kooij and F. Kuipers, "On the availability of networks", in BroadBand Europe 2007, Antwerp, Belgium, 3-6 December.