This peer-reviewed full text paper was presented at RNDM 2012-4th International Workshop on Reliable Networks Design and Modeling, co-located with ICUMT 2012 Conference

REASoN - REliability and/or Availability Evaluation for Sustainable Networking

Marcelo C. Amaral, Carlos H. A. Costa, Tereza C. M. B. Carvalho
Escola Politécnica, University of São Paulo
São Paulo, SP, Brazil
{mamaral,chancosta,carvalho}@larc.usp.br

Catalin Meirosu
Ericsson Research, Packet Technologies,
Sockholm, Sweden
catalin.meirosu@ericsson.com

***Abstract*—Sustainable computer networking approaches adapt network node power states dynamically in response to traffic demand. This scenario imposes new challenges to the way the network resilience is evaluated based on reliability and availability metrics. The traditional assessments of reliability and availability based on Markov models or the Cut-Set and Tie-Set techniques are based on static values and do not take into account the dynamic changes observed in an energy efficient network. We present REASoN, a method that extends and merges the Markov model and the Cut and Tie set technique in a way that allows an accurate evaluation of the network reliability and availability with dynamically adjustable power levels. A numerical evaluation of our method shows that even for a reduced network topology the impacts of energy efficient operations on reliability metrics are significant to a 1st decimal digit change in reliability.**

***Index Terms*—Availability; Reliability; Sustainability; Network;**

I. Introduction

In recent years, network service providers (NSPs) have been racing to deploy more sustainable wired networks. It takes place due to the exacerbated global network traffic increases. Also, the reduction of carbon footprint starts to be taken into consideration [1]. The NSPs competitiveness can be effectively improved with the deployment of sustainability-oriented resources and management techniques. The gains of such competitiveness are mainly related to reducing costs through a more efficient use of electric power, which attempts to keep the devices in a reduced power mode. Furthermore, the related reduction in the carbon footprint is a potential additional source of revenues through the trading of carbon credits. Projections show that, until 2015, the global network traffic will scale exponentially, due to both increases in the number of subscribers and access bandwidth [2].

Routers/switches are the primary source of energy consumption in standard fixed network infrastructures [3]. However, for the sake of performance, it is certainly appropriate to maintain the routers/switches always in hot standby, a situation in which the system is fully capable of handling the traffic (fully operational). This situation is desirable because it makes possible traffic engineering, and thus also a better utilization of network resources. Keeping the devices in hot standby helps to avoid network overload. On the other hand, in order to save energy, sustainable networking attempts to set the devices in reduced power consumption modes, which are not fully operational. In a performance point of view, these other modes are similar to leaving the corresponding devices in cold standby. Inspired by this fact, current research efforts on sustainable networking have focused on novel approaches for improving energy efficiency in these devices. Examples are *(a)* demand-aware CPU frequency scaling, *(b)* switch/router power mode adaptation, and *(c)* energy-efficient traffic engineering [4], [5].

Assessing the impact of putting a node into or off sleep mode, and assessing the time it takes to switch between power modes (the so-called "wakeup delay") are paramount for making informed decisions on whether and which nodes may have their state changed, what would impact the network performance. Unfortunately, the existing measuring approaches [6], [7], [8], [9], [10], [11], and [12] are not suitable for this context, as they do not take the volatility of the network state into account. Rather, they usually consider a static network whose elements become unavailable only in failure case, essentially basing the probability of such events on the time elapsed since the system has started and on the expected lifetime of the devices.

To the best of this work acknowledgement, there is no method that dynamically evaluates the side effects of sustainable networking on the overall network reliability or availability by considering as unavailable the interval during which devices switch power state. Aiming to tackle this issue, the method proposed by this work is called *REliability and/or Availability evaluation for Sustainable Networking* (REASoN), which calculates the network reliability and/or availability considering the network dynamism and the underlying wakeup delays of the devices. This method is an extension and combination of two known techniques: the **Markov model** and the **Cut-Set and Tie-Set**. This way, REASoN allows the evaluation of the trade-offs between service level agreement (SLA) and energy efficiency to be defined and accurately assessed. The result here is to answer how the reliability and availability evaluated by standard methods differ from those achieved by REASoN.

The remaining of the paper is organized as follows. Section II presents the usual definition of the network or individual switch/router reliability and availability. Section III describes the proposed method. Section IV presents the evaluation of the proposed solution. Section V outlines the conclusions and

978-1-4673-2017-7/12/$31.00

future works.

II. Network Reliability and Availability

The common definitions in the literature are provided in this paper as a common ground for further discussion. In addition, this section includes a discussion on optimization approaches and numerical calculation techniques.

A. Definitions

The **reliability** $R(t)$ of a system *"is a function of time, defined as the conditional probability that the system will operate correctly throughout the interval* $[t_0, t]$*, given that the system was performing correctly at the time* t_0*"* [13]. In other words, the reliability is the probability that the system will operate correctly throughout a complete interval of time. A reliable system is not necessarily fault tolerant, what means that being reliable does not imply that the system must tolerate any single hardware or software error that may occur. In addition, fault tolerance does not represent high reliability, for the problems could be so frequent that the reliability would be extremely low.

The **availability** $A(t)$ *"is a function of time defined as the probability that a system is operating correctly and is available to perform its functions at the instant of time* t*"* [13]. A system can be considered highly available and yet experience frequent periods of inoperability, as long as the duration of each inaccessibility period is extremely small. The availability depends on how fast the network can be repaired, which implies that a system with high availability should have undetectable periods of inaccessibility (also known as "down time") [6].

Availability differs from reliability in that reliability depends on an *interval* of time whereas availability is taken at an *instant* of time. Moreover, reliability is most often used to characterize systems in which even momentary periods of incorrect performance are unacceptable, or in which it is impossible to repair the system. On the other hand, availability is most used as a design goal when the primary purpose of the system is to provide services as uninterrupted as possible [13].

Reliability and availability, from a networking perspective, can be regarded in two ways: **two-terminal** that implies the presence of one or more operating paths between two network nodes, namely, s (source) and e (target), or as **all-terminal** that is related to all network nodes being able to communicate with each other [6]. The decision of evaluating the network reliability, or availability, or both may depend on the service level agreement (SLA) between the NSPs and the clients.

B. Optimization

The reliability and the availability of a system are typically optimized through including redundancy. In networking, this optimization is achieved by means of multiple redundant paths between a host and an end-router, as depicted in Figure 1, (b) and (c). Therefore, a single failed path does not necessarily interrupt the connection between two points, a fact that increases the chances of keeping the network operating, and leads to higher network availability.

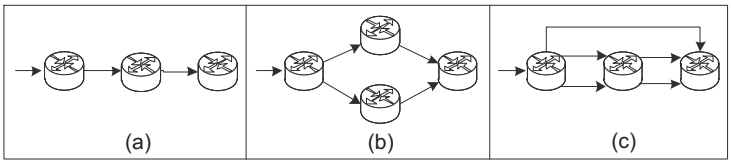

Figure 1: (a) no redundancy, (b) redundant router, (c) redundant link (connection) [6]

The redundancy can be either for the network devices and/or for the links, and both may increase the $R(t)$ or $A(t)$ as in Figure 1. The redundancy may be classified in two types: (i) parallel (also called hot standby) with all components operating, and (ii) cold standby with only the necessary components on that maintain the network operating. In the case of the (ii), cold standby, the components are inactivated, so that they are not susceptible for failure until be activated [6].

As time goes, the failure probability of all components tend to increase, due to the continuous utilization. In this way, a system whose every component is active and susceptible to failure has itself higher probability to failure than a system of which some components are inactive for a while has (if comparing systems whose components have same failure rate). Hence, if the probability of an inactive component (cold standby) switching to active state is 100%, a system in cold standby will have a higher $R(t)$ or $A(t)$ than another in hot standby. This probability is called coverage factor "c", and it is related to the activation of a redundant component either for hot or cold standby. However, whether the "c" of a system composed by components in cold standby is lower than another system with hot standby, its may have lower $R(t)$ or $A(t)$ than the other.

The decision of choosing between the use of parallel redundancy or cold standby always involves a probability analysis, which, in turn, depends on the properties of the switching mechanism. The decision may also involve analysis of parameters related to performance, because the use of hot standby can help the NSPs to better manage the network, through traffic engineering. In a sustainable networking context, the decision of keeping a device in cold standby can be performed strategically in order to save energy.

C. Calculation

In this section, this work presents the most relevant methods to evaluate the reliability and availability: (1) Markov model and (2) Cut-Set and Tie-Set. This discussion will then serve as a basis for the work proposal, detailed in Section III, in which both methods are extended and used in a complementary way.

1) Markov model: is used to describe the state of the system and the transitions between the states [13]. The states are divided as operational or failed, depending on the system

availability functionality. The basic assumption in the Markov model is that the system is memoryless, that is, that the transition probabilities are determined only on the basis of the present state, not on the basis of the whole or recent history.

In reliability or availability analysis based on Markov models, the probability of a transition is specified by the assumption of exponential distributions for failure and repair times. The system states and its transitions can be represented by *state transition diagrams*, for instance, the directed graphs in Figure 2. These diagrams contain sufficient information for developing the state equations [14].

The Markov models for $R(t)$ or $A(t)$ are illustrated in Figure 2, which presents a router composed by two redundant connections (in parallel or cold standby). Δt is the aggregated time elapsed since the system started in t_0; "c" is the coverage factor that represents the probability of a failure being detected, and the backup component being activated; λ is the failure rate; μ_1 is the preventive maintenance rate; and μ_2 is the repair rate. The main difference between μ_1 and μ_2 is that the former happens only when the system is operating, and the other the system has failed. The states are written as $(s_i s_j)$, where s_i and s_j determine the state of the i^{th} and j^{th} devices, respectively. States can assume the values 1 (fully operational), 0 (not operational), or S (cold standby).

2) Cut-Set and Tie-Set method: performs, in a combinatorial fashion [6], the calculation of the network reliability and/or availability for: two-terminal, that represents a pair of s (source) and e (target) nodes; or all-terminal that represents all nodes. For calculating the two-terminal,all Tn are enumerated, resulting in the Tie-Sets. Each Tn is a minimal combination of network links that connects s to e. Also, all C_n are enumerated, resulting in the Cut-Sets. Each C_n is a minimal combination of links that, if all of them are down, s gets disconnected from e. For calculating the all-terminal it is performed the union of all two-terminal $R(t)$ or $A(t)$. If there are n elements in Tie-Set, the $R(t)$ and/or $A(t)$ is given by the *principle of inclusion and exclusion* as in equation 1, which $R(t)_{\text{se}}$ or $A(t)_{\text{se}}$ is the union probability of all elements in Tie-Set, or conversely, the complement of the union probability of all elements in Cut-Set, i.e. $1 - (P(C_1 \cup C_2 \cup ... \cup C_{\text{n}}))$.

$$\begin{aligned} T_{\text{n}} &= Router_1 \cap Router_2 \cap ... \cap Router_{\text{m}} \\ R(t)_{\text{se}} or A(t)_{\text{se}} &= P(T_1 \cup T_2 \cup ... \cup T_{\text{n}}) \\ &\equiv \sum_{i=1}^{n} P(T_{\text{i}}) - \sum_{i<j} P(T_{\text{i}} \cap T_{\text{j}}) \\ &\quad + \sum_{i<j<k} P(T_{\text{i}} \cap T_{\text{j}} \cap T_{\text{k}}) - ... \\ &\quad + (-1)^{\text{n-1}} P(T_1 \cap T_2 \cap ... \cap T_{\text{n}}) \end{aligned} \quad (1)$$

The computation of this method is less complex than the Markov model. The Markov model analyzes all combinations of success and fails, instead the Cut-Set and Tie-Set analyzes only the combinations of success or fails.

III. The proposed method - REASoN

This section presents a method for measuring the side effects that the use of power adaptation features of devices

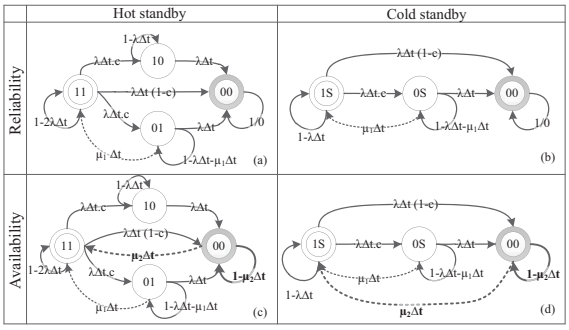

Figure 2: State transition diagram for Markov model of reliability and availability for parallel and cold standby redundancy

causes on the network reliability or availability. This method is called *REliability and/or Availability evaluation for Sustainable Networking* (REASoN). More specifically, this work allows the evaluation of the network $R(t)$ or $A(t)$ by taking into account the network traffic information and the wakeup delay of switches and routers as the network is being dynamically adapted. Hence, every time the network state changes, the $R(t)$ or $A(t)$ are reevaluated.

In order to do so, REASoN evaluates reliability and availability in two steps. First, it uses an extended **Markov model** to calculate, for each switch/router, the $R(t)$ or $A(t)$, considering as redundant all the connections that make available a path to the End-Router, if more than one connection exists. For instance, in the Figure 1 (b) the Host-Router is connected with two other routers that connect it to the End-Router, what results in redundant connections. Then, after gathering each router $R(t)$ or $A(t)$, REASoN calculates the two-terminal network availability or reliability of each pair source to target, using the extended **Cut-Set and Tie-Set** method. This method considers as unavailable any path composed by links whose traffic demand is higher than a pre-defined threshold or composed by any router in cold standby (or inactive).

The extended **Markov model**, depicted in Figure 3, represents the probability of a router keep forwarding data, considering all operational connections. The core of the extension is related to the cold standby, for which a state for the wakeup delay was included. In this model, α represents 1/(time that a device takes to *wakeup*), this time is related to the time that the network takes to stabilize, and the time that a device takes to be activated; "c" is the coverage factor, which means the probability that an error is identified and the probability of the successfully switching, which could be related with the update rate of the network information; μ_1 represents the time spent in the preventive *maintenance* of errors, and the network did not have failed; and μ_2 represents the time spent in the *repair* of a failure, and the network has failed.

REASoN method differs from the standard Markov model in the modeling of a cold standby because it includes an additional "penalty state" related to the wakeup time to switch the state. It is different from the coverage factor "c", described in section II, due to the "penalty state" represents only a delay to activate the backup component.

REASoN considers the time the network spends to become

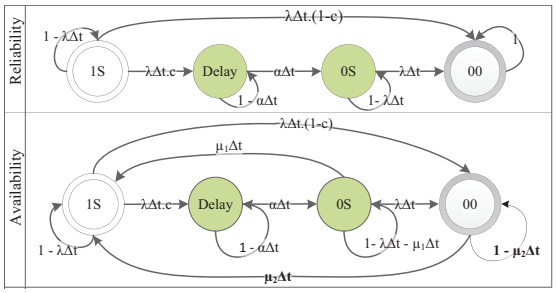

Figure 3: Extended Markov model of a router with two connections in cold standby that considers the time to activate the standby (α).

fully operant and the time taken by a device in cold standby to wakeup, which depends on the specific implementation of such power mode in the device (OS activity, memory allocation, operations related to state switching, subsystems power activity, etc.). The net result of such penalty state is that the probability of staying at this state interferes in the overall probability of the system be operating, thus degrading reliability and availability. In this way, the probability of has a device at wakeup delay state is added to the overall probability of the not operational states.

For the configuration with a router supporting two redundant connections in cold standby (one activated and other not), the state diagram is defined in Figure 3. From it, the $R(t)$ or $A(t)$ are respectively expressed by:

$$\begin{array}{lcl} P(t+\Delta t)_{1S} & = & P(t)_{1S} * (1-\lambda\Delta t) \\ P(t+\Delta t)_{Delay} & = & P(t)_{1S} * \lambda\Delta tc + P(t)_{Delay} * (1-\alpha\Delta t) \\ P(t+\Delta t)_{0S} & = & P(t)_{Delay} * \alpha\Delta t + P(t)_{0S} * (1-\lambda\Delta t) \\ P(t+\Delta t)_{00} & = & P(t)_{0S} * \lambda\Delta t + P(t)_{00} \\ \mathbf{R}(t+\Delta t) & = & P(t+\Delta t)_{1S} + P(t+\Delta t)_{0S} \\ \mathbf{R}(t+\Delta t) & \equiv & 1 - (P(t+\Delta t)_{00} + P(t+\Delta t)_{Delay}) \end{array} \quad (2)$$

$$\begin{array}{lcl} P(t+\Delta t)_{1S} & = & P(t)_{0S} * \mu_1\Delta t + P(t)_{00} * \mu_2\Delta t \\ & & +P(t)_{1S} * (1-\lambda\Delta t) \\ P(t+\Delta t)_{Delay} & = & P(t)_{1S} * \lambda\Delta tc + P(t)_{Delay} * (1-\alpha\Delta t) \\ P(t+\Delta t)_{0S} & = & P(t)_{Delay} * \alpha\Delta t + P(t)_{0S} * (1-\lambda\Delta t + \mu_2\Delta t)) \\ P(t+\Delta t)_{00} & = & P(t)_{0S} * \lambda\Delta t + P(t)_{00} * (1-\mu_1\Delta t) \\ \mathbf{A}(t+\Delta t) & = & P(t+\Delta t)_{1S} + P(t+\Delta t)_{0S} \\ \mathbf{A}(t+\Delta t) & \equiv & 1 - (P(t+\Delta t)_{00} + P(t+\Delta t)_{Delay}) \end{array} \quad (3)$$

These expressions are solved analytically in an iterative fashion as described in Algorithm 1. This algorithm considers that all components are properly working at the starting time, i.e., it is assumed that, at instant $t = 0$, the first state has probability 1 while all other states have probability 0. Time is then incremented iterating the expressions given by the Markov states, for instance the equations 2 and 3. The second step in REASoN is performed by the extended Cut-Set and Tie-Sets, previously described. The procedure to calculate it is presented in the algorithm 2.

IV. Numerical results

In order to evaluate the proposed method, this work implements an iterative numerical calculation following the specification given in the previous section. The results obtained by REASoN are compared to the standard approaches, showing the reliability degradation when a wakeup delay is considered in the calculation. All experiments were based on the network

Algorithm 1: Iterative procedure to analytically evaluate a Markov model

input : Constants Δt, λ, α, C and μ
output: The individual $R(t) or A(t)$ of a network device

t is the current time;
n is the last instant of time to be analyzed;
i is the current Markov states;
w is the amount of Markov states;
$P(t)$ is the probability of each Markov state;
The calculation of R(t) or A(t) depends on the used Markov model that define the equations;

for $t \leftarrow 0$ **to** $n-1$ **do**
  if *t = 0* **then**
    $P(0)_0 \leftarrow 1$ $P(0)_{1...w} \leftarrow 0$
    $R(0) or A(0) = P(0)_i * ... * P(0)_w$
  else
    for $i \leftarrow 0$ **to** $w-1$ **do**
      $R(t) or A(t) += P(t-1)_i * P(t)_i$
      $i += 1$
  $t += \Delta t$

Algorithm 2: Iterative procedure to analytically evaluate the network reliability or availability using the Cut-Set and Tie-Set

output: Two-terminal $R(t)$ or $A(t)$

The calculation of R(t) or A(t) depends on the used Markov model in Algorithm1;
t is the current time;
T_n is a element in the Tie-Set;
r is a router in the T_n;

for *n in Tie-Set* **do**
  for *r in T_n* **do**
    T_n[r] = Algorithm1(r, t, λ, α, C, μ);
Network $R(t)$ or $A(t)$ = Equation1(*Tie-Set*);

topology depicted in Figure 4. The numerical results are focused on metro networks, because it is related to the context of NSPs. The metro network topology was defined as a ring, which has a good resilience [15]. Notwithstanding, REASoN does not depend on the topology. The decision of switching the power mode of the devices between the cold standby mode (darker switches in Figure 4) or fully operational mode (lighter switches) is outside the scope of this work.

The experiment consists of pre-configured scenarios, of which one has every device in full operational mode. The other scenarios are composed also by some devices already in sleeping mode. The experiment calculates the two-terminal reliability between the switch 21 and the End-Router (core network) in Figure 4. For instance, if the number of rings between them is two ($m = 2$): the Tie-Set is $(21- > 20- > 2- > 1- > 0)$, $(21- > 20- > 2- > 3- > 0)$, $(21- > 2- > 1- > 0)$, $(21- > 2- > 3- > 0)$, and the Cut-Sets are (21), (2), $(1,3)$, and (0). This same pattern occurs for more rings ($m > 2$). The connections classified as Cut-Set are those either in overloaded or in cold standby, and those classified as Tie-Set are composed solely by available

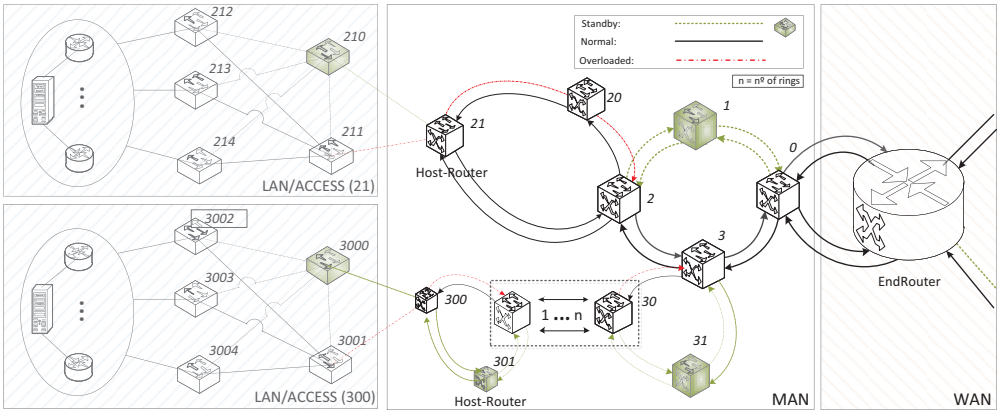

Figure 4: Access and Edge network topology

links.

This experiment evaluates and compares three scenarios. The first and the second were evaluated by the standard methods, and the third, by REASoN. **The first scenario (i)** is composed only by routers in hot standby and does not include cold standby. This scenario evaluates the individual reliability for each router using the standard Markov model for parallel redundancy (Figure 2). **The second scenario (ii)** is composed by some routers in cold standby and others in hot standby. In this scenario, this experiment evaluates the individual reliability for each router using the standard Markov model for cold and hot standby (Figure 2) (i.e., the wakeup delay is not considered). **The third scenario (iii)** is similar to the second, but it is evaluated by REASoN (equation 3), which does considers delay in the calculation. The values defined for the wakeup delay are pessimistic. They are based on the time required to boot a router and on the time commonly spent in getting the network protocols fully operational after booting. Thus, wakeup delay was varied among 15 and 30 minutes.

For all scenarios, after each router reliability evaluation, REASoN evaluates the two-terminal reliability between the router 21 and the End-Router, what is performed using the Cut-Set and Tie-Set method (equation 1). In this experiment, time interval Δt as 1 second, and the MTTF was varied among 60 000, 80 000, and 100 000 hours (values commonly found in data sheets of commercial, high performance routers). The comparison between the results from these scenarios clearly exposes the side effects in the reliability due to the use of cold standby in sustainable networking. First, this work compares the results obtained by calculating the reliability for the router 21 composed by 2 connections ($21- > 2$ and $21- > 20$). Then after, it compares the results of the two-terminal reliability between router 21 and the end-router.

A. Router reliability

The curves in Figure 5 represent the reliability of the scenarios (i) hot standby and (ii) cold standby, calculated by the standard Markov model, and (iii) cold standby, calculated by REASoN. Figure 5 shows that the reliability in scenario (ii) is higher than it is in the other scenarios. This is mainly

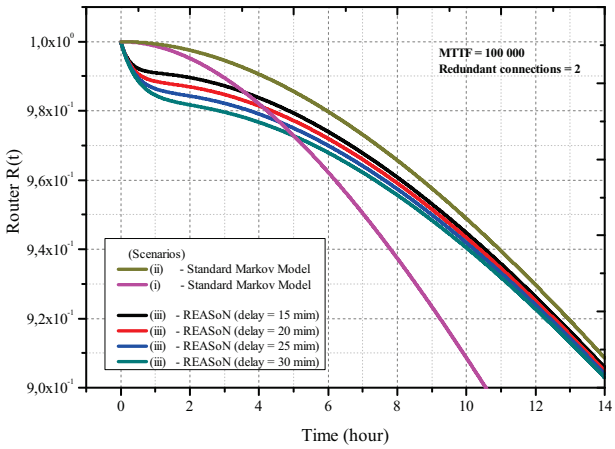

Figure 5: Router reliability varying the delay: (i) parallel (no cold standby), (ii) standard cold standby and (iii) cold standby evaluating wakeup time by REASoN.

because, in cold standby, some devices are kept inactivated until an error occurrence, and those are not susceptible of failure. In this condition, the chance of a component in cold standby failure should be lower than in hot standby (see section II). On the other hand, if the delay is considered in the calculation, as in scenario (iii), there is a penalty in the reliability. The reliability of the system with cold standby may be lower than the reliability of other scenarios. This penalty occurs only during a first period, and the event that leads to such penalty is the occurrence of a failure together with the necessity of waking up a standby component. However, the cold standby eventually makes the device more reliable as time goes, and asymptotically the values obtained by REASoN and those obtained by the standard cold standby become even. The penalty duration depends on the wakeup delay: higher delay implies an increase in duration and in amplitude of penalty. For instance, for 15 minutes of wakeup delay, the penalty lasts less than 4 hours; for 40 minutes of delay, it lasts 5 hours, and the reliability gets low.

The curves in Figures 6 and 7 represent the difference between the reliability of scenarios (iii) and (ii). As it was previously showed in the comparison between scenarios (ii) and (iii), both MTTF and wakeup delay impact the amplitude

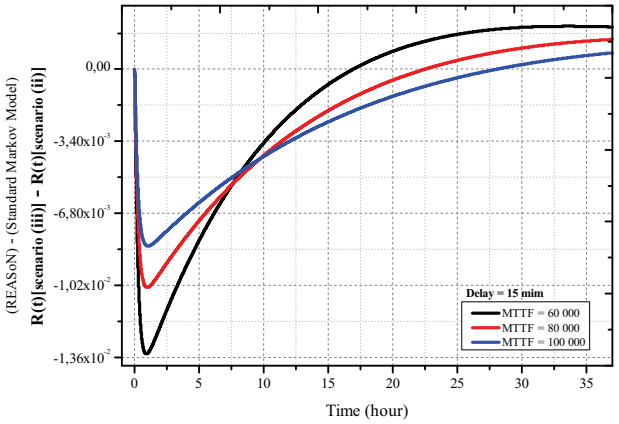

Figure 6: Difference between router reliability of the scenario (iii), evaluated by REASoN, *minus* the scenario (ii), evaluated by the standard method for cold standby. Varying the MTTF.

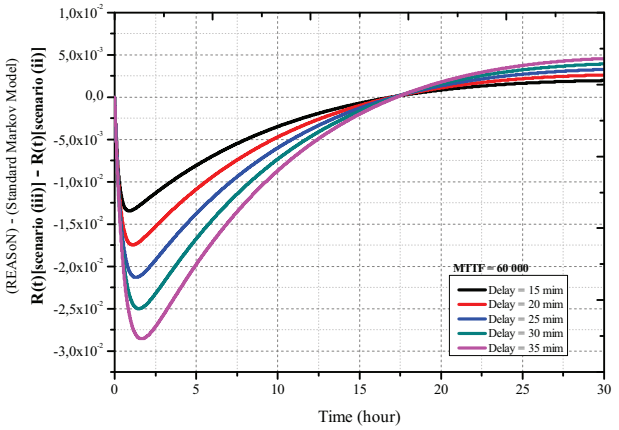

Figure 7: Difference between router reliability of the scenario (iii), evaluated by REASoN, *minus* the scenario (ii), evaluated by the standard method for cold standby. Varying the delay.

and duration of reliability. In Figure 7, however, the reliability calculation using the standard method becomes higher around the 17th hour. Figure 7 shows that the penalty amplitude can be as high as $\approx -2 \times 10^{-2}$, a significant 2nd decimal digit change in the reliability in the first hours of operation.

The comparison here shows that an evaluation that considers the wakeup delay is more accurate than one that does not. In addition, this side-effect of setting routers in sleep mode is captured only by the REASoN method. It also exposes the necessity of dynamically evaluating the reliability, because, every time a device state changes, the reliability of cold standby scenarios may be lower than the expectation set by standard methods. Reliability would, however, asymptotically approach standard method results in time.

B. Two-terminal reliability

The previous section shows how a delayed state switching makes the reliability of switch/router decrease through time. This section shows the behavior of nodes when they are combined to compose a network. It exposes how the wakeup penalty may impact in the overall network reliability. This work wants to answer the question of how the reliability evaluated with the standard method differs from the REASoN results. In order to perform such comparison, this experiment evaluates the reliability of a network with a varying topology size, through increasing the number of rings and keeping the constant redundancy degree. The reliability is numerically evaluated varying the number of nodes (5 to 50) in the topology of Figure 4. We modeled the topology using a constant redundancy ratio of 50% of the paths between the host-router and the end-router. In the case of scenario (ii) and (iii), some redundant paths are set in cold standby using a ratio of 30%, which is an optimistic decision.

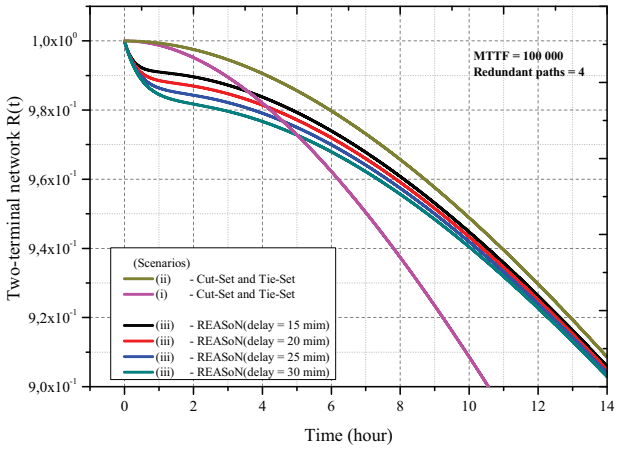

Figure 8: Two-terminal reliability: (i) parallel (no cold standby), (ii) standard cold standby and (iii) cold standby that considers wakeup time using REASoN

Figure 8 presents the two-terminal reliability of router 21 (Figure 4) for the three scenarios, namely, (i) hot standby and (ii) cold standby, calculated by the standard Markov model, and (iii) cold standby, calculated by REASoN. For each scenario, paths with 2 rings (m =2) were evaluated, a situation in which 4 redundant paths are available. That figure shows the reliability in scenario (ii) is higher than in the others scenarios. The scenario (iii) has lower reliability than the other scenarios until almost 5 hours. Moreover, an increase in wakeup delay results in a decrease in reliability. This behavior is similar to the behavior of the reliability of a single router. However, in a larger topology, it is possible to see a change in this behavior, as shown in Figure 9.

The curves in Figure 9 represent the difference between the two-terminal reliability of scenarios (iii) and (ii). That figure exposes that the reliability in scenario (ii) is higher than in scenario (iii) until almost 12 hours (as we also saw in Figure 5). This behavior differs from the evaluation of only one router, in which the duration of the delay lasts almost 5 hours. It means that the impacts of the wakeup delay of a router are more intense on the network than they are on the router itself. This figure also highlights that both the amplitude and the duration of the reliability penalty are affected by the number of devices. It also shows that, the higher the number of devices, the higher the amplitude and the shorter the duration of the penalty. It gets maximum amplitude of $\approx 5.5 \times 10^{-1}$ in the case of 50 devices and maximum duration of ≈ 24 hours for 20 devices. The reliability calculated by both methods eventually converges asymptotically. The results show that, for a network

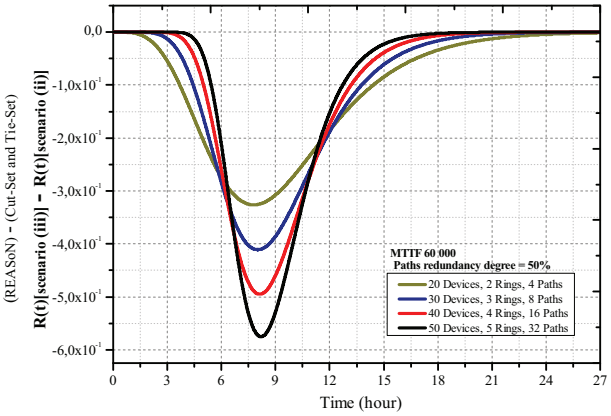

Figure 9: Difference between router reliability of the scenario (iii), evaluated by REASoN, *minus* the scenario (ii), evaluated by the standard method for cold standby

of few dozens of devices, in which cold standby modes are dynamically switched on and off, taking the state transition delay into account represents a considerable reliability penalty (1st decimal digit change). This penalty happens during the first few hours of operation. Such fact may be of importance on determining whether or not it is worth setting devices in cold standby.

V. Conclusions and Future Work

This paper describes and evaluates the REASoN method, which dynamically calculates the reliability and/or availability every time the network state changes (such as a router switch between power states). Such scenarios often occur in sustainable networking. This method produces more accurate results by including in the calculation the delay involved in waking up the devices from standby mode. The experimental results of REASoN show that, when considering such delay, an expressive degradation of reliability can be observed on the network. It shows that the difference between the reliability evaluated through standard methods and that evaluated through REASoN method can be as high as a change in the 1st decimal digit. This difference represents a standby penalty. This maximum of penalty takes place within the first few hours of operation.

The two-terminal network reliability calculation using REASoN shows how the penalty on the reliability of each node impacts the overall network reliability. The amplitude of the penalty translates as a 1st decimal digit change, in the first 25 hours of operation, in reliability. In addition, the results show that the standard methods cannot capture this difference. The dependency of the penalty amplitude and duration on the network size was investigated through evaluation of different topologies. By comparing the standard method to REASoN, one sees that, the higher the number of nodes, then the higher the amplitude of the penalty, and the shorter its duration. This fact directly impacts the decision of whether or not to put a device in a standby mode in order to save energy when traffic demand is low.

REASoN allows a continuous and dynamic evaluation of the network availability as the state of the devices changes, thus providing real-time indication of the impact associated to the activation of power saving modes. This method is helpful for defining and coordinating, at the network management level, trade-off between SLA and energy efficiency, providing a powerful tool for building more sustainable networks. As future work it was envisioned, the integration of REASoN into a power-aware network management system, which would thus provide means of defining, through real-time evaluation, trade-offs between power saving features and reliability or availability.

Acknowledgment

This work was supported by the Innovation Center, Ericsson Telecomunicações S.A., Brazil. Additionally, we thank Marcos A. Simplicio Jr. and Guilherme C. Januario for their insightful comments during the development of this work.

References

[1] GeSI, "Smart 2020: Enabling the low carbon economy in the information age," The Climate Group on behalf of the Global eSustainability Initiative (GeSI), Tech. Rep., Jun. 2008.

[2] C. Lange, D. Kosiankowski, R. Weidmann, and A. Gladisch, "Energy consumption of telecommunication networks and related improvement options," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 17, no. 2, pp. 285–295, Apr. 2011.

[3] R. Bolla, R. Bruschi, F. Davoli, and F. Cucchietti, "Energy efficiency in the future internet: A survey of existing approaches and trends in Energy-Aware fixed network infrastructures," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 223–244, 2011.

[4] U. Lee, I. Rimac, D. Kilper, and V. Hilt, "Toward energy-efficient content dissemination," *IEEE Network*, vol. 25, no. 2, pp. 14–19, Apr. 2011.

[5] R. Bolla, F. Davoli, R. Bruschi, K. Christensen, F. Cucchietti, and S. Singh, "The potential impact of green technologies in next-generation wireline networks: Is there room for energy saving optimization?" *Communications Magazine, IEEE*, vol. 49, no. 8, pp. 80 –86, august 2011.

[6] M. L. Shooman, *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*, 1st ed. Wiley-Interscience, Dec. 2001.

[7] F. Altiparmak, B. Dengiz, and A. Smith, "Reliability estimation of computer communication networks: Ann models," in *Computers and Communication, 2003. (ISCC 2003). Proceedings. Eighth IEEE International Symposium on*, june-3 july 2003, pp. 1353 – 1358 vol.2.

[8] H. Green, J. Hant, and D. Lanzinger, "Calculating network availability," in *2009 IEEE Aerospace conference*. IEEE, Mar. 2009, pp. 1–11.

[9] F. He and H. Qi, "A method of estimating network reliability using an artificial neural network," in *Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008. PACIIA '08*, vol. 2. IEEE, Dec. 2008, pp. 57–60.

[10] Y. F. Lam and V. O. K. Li, "A survey of network reliability modeling and calculations," in *IEEE Military Communications Conference - Communications-Computers: Teamed for the 90's, 1986. MILCOM 1986*, vol. 1. IEEE, Oct. 1986, pp. 1.2.1–1.2.5.

[11] C. Lin, H. Teng, C. Yang, H. Weng, M. Chung, and C. Chung, "A mesh network reliability analysis using reliability block diagram," in *2010 8th IEEE International Conference on Industrial Informatics (INDIN)*. IEEE, Jul. 2010, pp. 975–979.

[12] W. Yeh, Y. Lin, Y. Y. Chung, and M. Chih, "A particle swarm optimization approach based on monte carlo simulation for solving the complex network reliability problem," *IEEE Transactions on Reliability*, vol. 59, no. 1, pp. 212–221, Mar. 2010.

[13] B. W. Johnson, *The Design and Analysis of Fault Tolerant Digital Systems*. Addison-Wesley, Jan. 1989.

[14] K. S. Trivedi and D. Selvamuthu, "Markov modeling in reliability," in *Encyclopedia of Quantitative Risk Analysis and Assessment*. John Wiley & Sons, Ltd, 2008.

[15] CISCO, "Cisco resilient ethernet protocol," Cisco, USA, Tech. Rep., 2007.