Availability Assessment of IP Multimedia Subsystem in an NFV-based Environment

Mario Di Mauro[1], Giovanni Galatro[1], Maurizio Longo[1], Fabio Postiglione[1], Marco Tambasco[1,2]
[1]Dept. of Information and Electrical Engineering and Applied Mathematics (DIEM)
University of Salerno, Fisciano (SA), Italy
[2]Research Consortium on Telecommunications (CoRiTeL)
Via G. Paolo II, 84084, Fisciano (SA), Italy
email: {mdimauro, longo, fpostiglione}@unisa.it,
g.galatro1@studenti.unisa.it, marco.tambasco@coritel.it

***Abstract*—Network Function Virtualization (NFV) is considered one of the most influencing concepts in modern telecommunication frameworks, since it has the merit of transposing (and adapting) the virtualization paradigms from the computer world to the networking context. An instance of NFV is known as a Virtual Network Function (VNF), and represents a virtualized abstraction of a network element such as a router, a firewall, a load balancer, deployed in a virtualized environment. Actually, complex infrastructures, such as IP Multimedia Subsystem (IMS), a framework in charge of providing advanced multimedia services, can benefit of a virtualized deployment by implementing its constitutive elements as VNFs. The resulting architecture is a vIMS that, in this work, is characterized in terms of availability. More specifically, relying on a failure/repair model of a generic vIMS entity (modeled as a three-layer structure composed of hardware, hypervisor and software), we propose an availability assessment of the whole system by means of Stochastic Reward Networks framework.**

***Keywords*–Availability analysis; Stochastic Reward Networks; virtualized IP Multimedia Subsystem.**

I. INTRODUCTION

Nowadays, telecom and network operators compete in deploying new services quickly and cheaply. Network Function Virtualization (NFV) [1] represents a valuable solution to face such issues, by implementing a *pay-per-use* model that allows to exploit a network service only as needed. According to this paradigm, a relocation or a hardware update of a traditional router, for example, can be replaced by manageable operations on a Virtual Network Function (VNF) exhibiting the same functionalities of the router itself. Generally speaking, a VNF can be represented by a three-layer structure composed of: a *hardware* layer representative of physical equipments (e.g., CPU, memory, etc.), a *hypervisor* layer serving as interface between hardware and software, and a *software* part representative of the particular VNF logic (e.g., routing, switching, etc.). In a similar manner, network elements of an IP Multimedia Subsystem (IMS) framework [2] can be recasted in terms of VNFs as pointed out in [3], [4], obtaining a virtualized IMS infrastructure denoted by vIMS. Starting from a vIMS exemplary architecture, in this work we advance a twofold contribution: first, we introduce a failure/repair model of a generic vIMS node compliant to the three-layer structure characterizing a VNF, and then, we perform an availability analysis of the resulting vIMS aimed at characterizing the optimal configuration that respects the “five nines” availability requirement, namely a maximum downtime tolerance of 5 minutes and 26 seconds per year. Such an assessment is obtained by application of Stochastic Reward Networks (SRN) framework when analyzing a single vIMS node, and, then, by considering the pipe of interconnected nodes by means of Reliability Block Diagram (RBD) representation. The paper is organized as follows: Section 2 contains a brief description of related research in the considered area. In Section 3, an overview about a vIMS deployment is offered. Section 4 introduces the availability model of a vIMS node, along with some details about the adopted methodologies (SRN and RBD). A numerical experiment useful to validate the considered model is proposed in Section 5, and, finally, concluding remarks end the work in Section 6.

II. RELATED WORK

In the field of telecommunication networks, availability issues are becoming crucial especially for those operators that have to obey some rigid Service Level Agreements. Besides, unlike the past, such issues have also to account for the massive presence of virtualized infrastructures characterizing modern telecommunication systems in cloud environments. Consequently, no wonder the technical and scientific literature is taking an interest about these aspects. Some valuable examples follow. Kim, Machida, and Trivedi in [5] propose one of the first availability models that consider the failure (and corresponding repair) events associated to the virtualization layer of a system, in addition to classical hardware and software failure actions. In particular, the authors largely exploit the Continuous-Time Markov Chain structures to model the behavior of some subsystems, such as CPU, memory, hypervisor, etc. A method useful to estimate some dependability attributes (availability among them) in virtualized environments has been proposed in [6], where the authors exploit the properties of Stochastic Petri Nets [7], a state-based model useful to account for redundancy strategies aimed at guaranteeing some availability requirements. The work presented in [8] is devoted at presenting a framework to evaluate the reliability of an NFV infrastructure where the focus is on some algorithms able to discover the minimum number of nodes that would cause the malfunctioning of the overall NFV deployment. In this case, the proposed model accounts for failure events but not repair actions. An approach based on the software rejuvenation applied to virtual environments and useful to cope with the occurrence of unplanned failures has been presented in [9] enriched with a detailed availability analysis, although hardware failures are not considered for simplicity. Another interesting approach is presented in [10], aimed at coping with novel container-based infrastructures by means of SRN

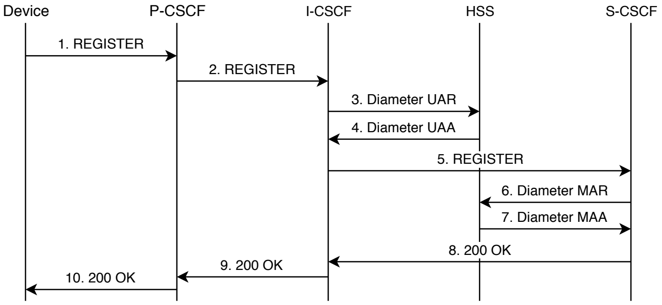

Figure 1. Registration procedure in IMS domain (simplified).

methodology. In line with this literature, in the present work we analyze a network infrastructure already considered in [11], [12], namely, a virtualized IMS framework, composed of hardware, hypervisor and software layers. However, differently from the previous work, here we adopt a double-layer availability model combining the expressive power of RBD, and the concise modeling offered by SRN.

III. IP Multimedia Subsystem overview

IMS enables a huge variety of architectures to provide multimedia services such as audio/video sessions, presence services, enriched communications. Furthermore, it has been elected as the reference architecture to support delivery of new voice services (e.g., Voice over LTE - VoLTE) across an all-IP network [13]. From an architectural perspective, IMS relies on a group of Call Session Control Function (CSCF) servers that communicate among them by means of Session Initiation Protocol (SIP) [14]. More specifically, the *Proxy* CSCF (P-CSCF) is the first contact point between a device and the IMS domain. The *Serving* CSCF (S-CSCF) represents the core of IMS and plays the role of a controller able to supervise critical aspects such as subscriber's service procedures or session status maintenance. The *Interrogating* CSCF (I-CSCF) acts as a gateway among multiple IMS domains determining whether or not the SIP messages forwarding is allowed from an operator to another. Finally, the Home Subscriber Server (HSS) is an evolved database which retains all the user data and is accessed by other CSCFs through Diameter protocol. For instance, when a user requests an access to the IMS domain, the S-CSCF queries to the HSS (via Diameter) to retrieve user profile in order to verify his/her grants. Typically, the message flow within an IMS domain follows a predefined path traversing a series of IMS nodes. It is the case of Registration procedure (depicted in Figure 1) where: a device requests to access the IMS domain by sending a REGISTER message to P-CSCF (1); such a message is passed to I-CSCF (2) that, in turn, queries the HSS the proper S-CSCF address that will manage the whole session. Such a query/response is identified by a couple of messages: User Authentication Request (UAR) (3), and User Authentication Answer (4). Once REGISTER message arrives to the S-CSCF (5), it retrieves user profile by the HSS through another couple of messages: Message Authentication Request (MAR) (6) and Message Authentication Response (7). If all goes well, the S-CSCF transmits a *200 OK* message to the device (8), (9), (10) and the registration procedure terminates.

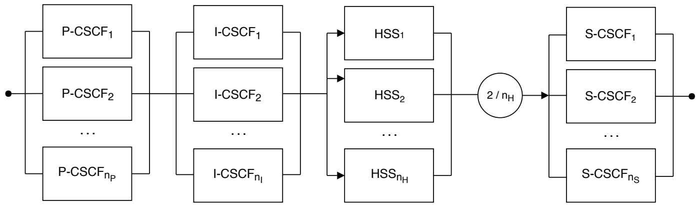

Figure 2. RBD representation of a vIMS domain, with HSS deployed in a 2-out-of-n$_H$ redundancy configuration.

A. IMS within an NFV environment

IP Multimedia Subsystem can surely benefit from an NFV-based environment, by inheriting some advantages in terms of: *i)* flexibility: a vIMS element can be easily moved across geographical locations resulting in a cost-effective operation for a network provider; *ii)* manageability: a vIMS infrastructure can be effortlessly handled from a unified control center; *iii)* scalability: the hardware and software resources can be assigned to the vIMS framework in proportion to the real needs. Accordingly, an IMS node can be modeled as a three-layer structured VNF composed of:

- *Hardware (HW)*: typifies the physical components such as storage, CPU, memory, network etc.;
- *Virtual Machine Monitor (VMM)*: is the hypervisor, namely, the element which acts as an interface between hardware and software layers;
- *Software (SW)*: represents the application layer of each VNF which executes a specific functionality (X-CSCF, HSS, etc.).

In our scenario, two assumptions hold. First, hardware and hypervisor are reasonably supposed the same for all IMS elements recasted as VNFs. Secondly, the software layer admits different characterization for CSCF and HSS nodes.

IV. Availability Analysis

As previously stated, the availability analysis of a vIMS infrastructure performed in this work relies on a model which exploits two combined formalisms: RBD and SRN. The former offers a comfortable way to characterize the vIMS system by a macroscopic perspective, namely, in terms of high-level interconnections among nodes as depicted in Figure 2. In particular, the sketched representation embodies three aspects: *i)* a series model is used to characterize the chain of connections among the vIMS nodes; *ii)* a parallel configuration (per vIMS node) is representative of a redundancy strategy to cope with possible failures by assuming load balancing; *iii)* HSS element is supposed to be deployed in a *2-out-of-n_H* setting, meaning that 2 working HSS replicas are needed to consider HSS perfectly functioning. On the other hand, SRN methodology is exploited to model the interactions among the three layers (HW, SW, VMM) composing a generic vIMS node. The SRN framework [15] is a state-space model (derived from Markov Reward Models [16]) open to characterize a system in terms of its states distribution, by admitting a concise representation useful to mitigate the uncontrolled state space growth that typically occurs when dealing with classical probabilistic models. Basically, an SRN can be represented by a bi-partite directed graph with places (depicted by circles) representative of conditions (e.g., the system is up or down), and transitions (depicted by rectangles) that account for actions (e.g., the system crashes or is restored). A place can contain a *token* (represented by a dot or a number) that indicates a particular holding condition, and that can be transferred to another place if a transition is *fired*, namely, if an action occurs. Transition times are supposed to be exponentially distributed and characterized by rates λ and μ associated to failure and repair actions, respectively. Evaluating an SRN means characterizing its *marking*, namely, its tokens distribution that changes across the time and provides information about system dynamics. From an analytical perspective, we are interested in evaluating the *reward function*, say $Z(t)$, a non-negative random process that can be associated to some relevant dependability metrics such as the availability. More specifically, the instantaneous availability obeys the following expression:

$$A(t) = Pr\{Z(t) = 1\} = E(Z(t)) = \sum_{i \in S} r_i \cdot p_i(t), \qquad (1)$$

where S represents the set of markings, split in a subset of up states (for which reward rate $r_i = 1$), and a subset of down states (for which $r_i = 0$), and where $p_i(t)$ denotes the probability of system being in state i. According to the three-layer model of a vIMS node, the corresponding SRN model of a vIMS node (either CSCF or HSS nodes) is as follows (see Figure 3):

- *Places* (circles): the set of places P_{upSW} $[P_{dnSW}]$, P_{upVMM} $[P_{dnVMM}]$, P_{upHW} $[P_{dnHW}]$ accounts for the working [failure] conditions of software, hypervisor and hardware parts, respectively. The tokens within the “up” places are representative of initial working conditions.
- *Timed Transitions* (thick and unfilled rectangles): the set of transitions T_{fSW} $[T_{rSW}]$, T_{fVMM} $[T_{rVMM}]$, T_{fHW} $[T_{rHW}]$ accounts for failure [repair] activities characterizing software, hypervisor and hardware parts, respectively.
- *Immediate Transitions* (thin and filled rectangles): the couple of transitions t_{SW} and t_{VMM} accounts for instantaneous actions occurring in an almost-zero transition time.

A. SRN model dynamics

Let study the SRN evolution of a generic vIMS node when failure and repair activities occur. Start from an initial working condition with 3 tokens in the three up places, consider the leftmost part of SRN in Figure 3. When a software failure occurs (e.g., the application part on top of CSCF or HSS node breaks) the token in P_{upSW} moves to P_{dnSW} as a consequence of fired transition T_{fSW}. The token will return in its original place (P_{upSW}) once a repair action occurs, namely, once T_{rSW} transition is fired. Instead, if a failure affects the hypervisor, the transition T_{fVMM} is fired, thus, the token leaves P_{upVMM} and arrives to P_{dnVMM}. In this case, an inhibitory arc (the segment between P_{upVMM} and t_{SW} with a little circle closer to the latter) becomes inactive and lets t_{SW} fire (no working software part is allowable when hypervisor fails). On the other hand, the inhibitory arc between P_{dnVMM} and T_{rSW} disables the latter by stopping the repair of the only software part when hypervisor is down (in other words, software and hypervisor repair is simultaneous through T_{rVMM}). Finally, upon a hardware layer failure, transition T_{fHW} is fired and the token, initially dwelling in P_{upHW}, is transferred to P_{dnHW}. In this case, the inhibitory arc between P_{upHW} and t_{VMM} entails the hypervisor failure once hardware fails, whereas, the arc connecting P_{dnHW} with T_{rVMM} avoids that a hypervisor repair activity be enabled until T_{rHW} is fired, namely, until the hardware is fixed. At this point we can define:

- $r_{i,k}$: reward rate pertaining to marking i for the k-th node replica;
- $p_{i,k}(t)$: probability of being in marking i at time t for the k-th node replica, computed by solving SRN in Figure 3 for each node.

Being all possible markings mutually exclusive, we can exploit (1) to derive the instantaneous availability $A^{(k)}(t)$ as

$$A^{(k)}(t) = \sum_{i \in I} r_{i,k} \cdot p_{i,k}(t), \qquad (2)$$

where I is the set of markings characterized by no immediate transitions enabled, and called *tangible markings*. Again, given marking i, the pertinent reward rate $r_{i,k}$ is defined as

$$r_{i,k} = \begin{cases} 1 & \text{if } (\#P_{upSW} = 1) \\ 0 & \text{otherwise,} \end{cases}$$

where # symbol denotes the number of tokens in a specific place. It is useful to notice that, such a condition does not account for “up” state of hardware and hypervisor, being basically contained in the SRN depicted in Figure 3 by means of inhibitory arcs By considering $\lim_{t \to \infty} A^{(k)}(t)$ we obtain the *steady-state availability* given by:

$$A^{(k)} = \lim_{t \to +\infty} A^{(k)}(t) = \sum_{i \in I} r_{i,k} \cdot p_{i,k}, \qquad (3)$$

where $p_{i,k}$ is the steady-state probability, namely $p_{i,k} = \lim_{t \to +\infty} p_{i,k}(t)$. By simple inspection of Figure 2, the vIMS infrastructure can be modeled by series/parallel interconnections among independent subsystems. Using (3), the steady-state availability of the whole vIMS system is given by:

$$A_{vIMS} = \left[1 - \prod_{k=1}^{n_P} \left(1 - A_P^{(k)}\right)\right] \cdot \qquad (4)$$
$$\left[1 - \prod_{k=1}^{n_S} \left(1 - A_S^{(k)}\right)\right] \left[1 - \prod_{k=1}^{n_I} \left(1 - A_I^{(k)}\right)\right] \cdot$$
$$\sum_{k=2}^{n_H} \binom{n_H}{k} A_H^k \left(1 - A_H\right)^{n_H - k},$$

where:

- $A_P^{(k)}$, $A_S^{(k)}$, $A_I^{(k)}$ and $A_H^{(k)} = A_H$: steady-state availabilities of k-th replica of P-CSCF, S-CSCF, I-CSCF and HSS respectively;

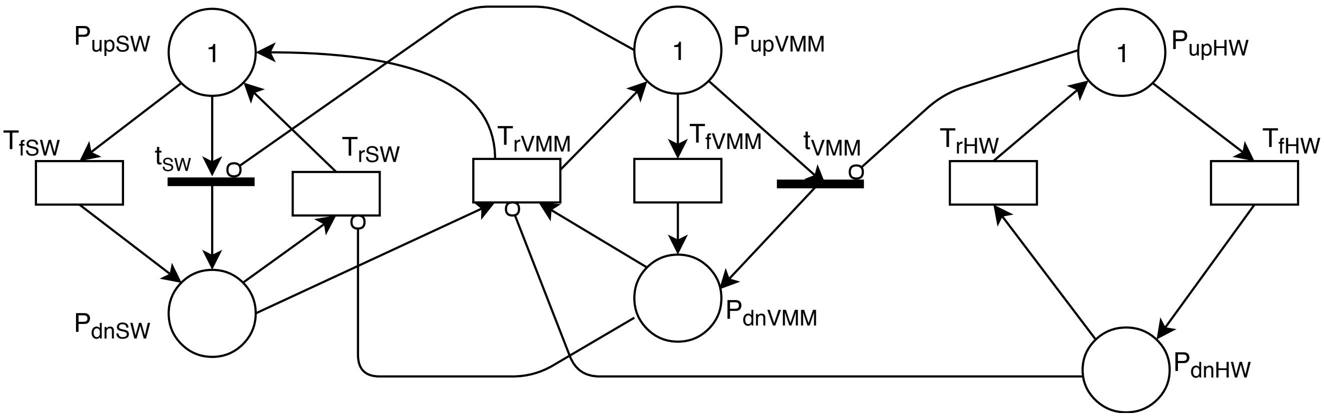

Figure 3. SRN model of a generic (either CSCF or HSS node) vIMS node according to the three-layer structure including: hardware (HW), virtual machine monitor (VMM) and software (SW).

TABLE I. INPUT PARAMETERS

Parameter	Description	Value
$1/\lambda_{HW}$	mean time for hardware failure	60000 hours
$1/\lambda_{VMM}$	mean time for hypervisor failure	5000 hours
$1/\lambda_{CSCF}$	mean time for CSCF node failure	3000 hours
$1/\lambda_{HSS}$	mean time for HSS node failure	2000 hours
$1/\mu_{HW}$	mean time for hardware repair	8 hours
$1/\mu_{VMM}$	mean time for hypervisor repair	2 hours
$1/\mu_{CSCF}$	mean time for CSCF software repair	1 hour
$1/\mu_{HSS}$	mean time for HSS software repair	1 hour

TABLE II. AVAILABILITY RESULTS OF VIMS BY CONSIDERING 5 EXEMPLARY SETTINGS ($S_1, \ldots, S_5$).

Setting	Redundancy Level	A_{vIMS}
S_1	$CSCF = [2, 2, 2]$, $HSS = 2$	0.997867
S_2	$CSCF = [2, 2, 3]$, $HSS = 2$	0.997868
S_3	$CSCF = [2, 2, 2]$, $HSS = 3$	0.999994
S_4	$CSCF = [2, 2, 3]$, $HSS = 3$	0.999995
S_5	$CSCF = [2, 3, 3]$, $HSS = 4$	0.999999

- n_P, n_S, n_I and n_H: number of redundant subsystems of each functionality (P-CSCF, S-CSCF, I-CSCF and HSS respectively).

The steady-state availability in (4) appears as a product of the first three factors associated to the series of nodes P-CSCF, S-CSCF and I-CSCF replicated in a parallel configuration. The last term addresses the *2-out-of-n_H* scheme characterizing HSS node.

V. Numerical Example

By starting from the previously modeled vIMS framework, in this section we propose a numerical experiment with the support of an effective tool named SHARPE [17]. In particular, we perform an availability analysis aimed at identifying the optimal configuration respecting the "five nines" condition, by exploiting values reported in Table I (in line with [11]). We make two assumptions: first, we consider that software instances on top of CSCF nodes are characterized by the same failure and repair rates, with the exception of HSS database which is intrinsically prone to more faults. Second, we assume that hypervisor and hardware layers are the same for all nodes. The steady-state availability analysis is performed by considering different system configurations. We report here five exemplary settings $S_1, \ldots, S_5$ (among the tested ones) to show how the number of parallel nodes influences system availability:

- S_1: 2 replicas for each vIMS node (CSCFs and HSS);
- S_2: 2 replicas for a couple of CSCFs, 3 replicas for the remaining CSCF and 2 replicas for HSS;
- S_3: 2 replicas for each CSCF and 3 replicas for HSS;
- S_4: 2 replicas for a couple of CSCFs, 3 replicas for the remaining CSCF and 3 replicas for HSS;
- S_5: 2 replicas for a single CSCF, 3 replicas for a couple of CSCFs and 4 replicas for HSS.

The results are reported in Table II. Notice that S_1 and S_2 settings are far below the "five nines" availability requirement, due to the lack of any redundant node for HSS. On the other hand, S_3 and S_4 settings satisfy both the desired condition with 9 and 10 node replicas, respectively, thus, S_3 is preferable being more cost-effective. Finally, setting S_5, with 12 node replicas and two redundant nodes for HSS, allows to achieve a "six nines" availability condition which is required in some strongly critical infrastructures.

VI. Conclusions

Nowadays, network infrastructures can derive copious advantages from Network Function Virtualization (NFV) paradigm in terms of flexibility, scalability, cost saving and maintenance. A paramount example is represented by IP Multimedia Subsystem (IMS), the framework acting as core network for modern telecommunication infrastructures such as Voice over LTE (VoLTE) or Voice over Wi-Fi (VoWi-Fi). Such a framework is prone to adhere to the NFV standard by virtualizing its main nodes, namely, the CSCFs and the HSS. Accordingly, in this work we propose an availability analysis of a virtualized IMS infrastructure (that we call vIMS) performed through two formalisms: the Reliability Block Diagram (RBD) useful to characterize the high-level interconnections among vIMS nodes, and the Stochastic Reward Nets (SRN) helpful to model in a probabilistic way the failure/repair events occurring at any of the three layers (software, hypervisor, hardware) of a vIMS node. Such an availability analysis can be easily afforded by exploiting well-assessed software tools (SHARPE) and results advantageous to identify the optimal vIMS configuration matching the "five nines" availability requirements.

Future works will take into account: more sophisticated performance models (with a view to the so-called performability analysis), more complex interconnections among the three-layer structure of a vIMS node, where a co-location of some nodes could be considered as is the case of more realistic scenarios, and fault injection methods aimed at characterizing more realistically the recovery time.

REFERENCES

[1] ETSI, "Network Functions Virtualisation: An introduction, benefits, enablers, challenges and call for action," Tech. Rep., 2012.

[2] G. Camarillo and M. Garcia-Martin, The 3G IP Multimedia Subsystem, 3rd ed. John Wiley and Sons, 2008, ISBN: 9780470516621.

[3] Ericsson Review, "Virtualizing network services - the telecom cloud," 2014 [Online], available: https://www.ericsson.com/en/ericsson-technology-review/archive/2014/virtualizing-network-services---the-telecom-cloud [accessed:2018-07-10].

[4] "Project clearwater," available: http://www.projectclearwater.org/ [accessed:2018-07-10].

[5] D. S. Kim, F. Machida, and K. S. Trivedi, "Availability modeling and analysis of a virtualized system," in Proc. IEEE PRDC 2009, 2009, pp. 365–371.

[6] S. Fernandes, E. Tavares, M. Santos, V. Lira, and P. Maciel, "Dependability assessment of virtualized networks," in Proc. IEEE ICC 2012, 2012, pp. 2711–2716.

[7] M. A. Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis, Modelling with Generalized Stochastic Petri Nets, 1st ed. John Wiley & Sons, Inc., 1994, ISBN:0471930598.

[8] J. Liu, Z. Jiang, N. Kato, O. Akashi, and A. Takahara, "Reliability evaluation for NFV deployment of future mobile broadband networks," IEEE Wireless Communications, vol. 23, no. 3, 2016, pp. 90–96, ISSN: 15361284.

[9] T. Thein and J. Sou Park, "Availability analysis of application servers using software rejuvenation and virtualization," Journal of Computer Science and Technology, vol. 24, no. 2, 2009, pp. 339–346, ISSN: 18604749.

[10] S. Sebastio, R. Ghosh, and T. Mukherjee, "An availability analysis approach for deployment configurations of containers," IEEE Transactions on Services Computing, 2018, pp. 1–1, ISSN: 19391374.

[11] M. Di Mauro, G. Galatro, M. Longo, F. Postiglione, and M. Tambasco, "Availability evaluation of a virtualized IP Multimedia Subsystem for 5G network architectures," in Safety and Reliability - Theory and Applications, M. Cepin and R. Bris, Eds. Taylor & Francis Group, 2017, pp. 2203–2210, ISBN: 9781351809726.

[12] M. Di Mauro, M. Longo, F. Postiglione, and M. Tambasco, "Availability modeling and evaluation of a network service deployed via NFV," in Digital Communication. Towards a Smart and Secure Future Internet, A. Piva, I. Tinnirello, and S. Morosi, Eds. Springer International Publishing, 2017, pp. 31–44, ISBN: 9783319676395.

[13] Nokia Networks, "Evolve to richer voice with Voice over LTE (VoLTE)," 2014 [Online], available: https://onestore.nokia.com/asset/200306/Nokia_VoLTE_White_Paper_EN.pdf [accessed:2018-07-10].

[14] J. D. Rosenberg et al., "Session Initiation Protocol (SIP)," 2002, IETF RFC 3261.

[15] J. K. Muppala, G. Ciardo, and K. S. Trivedi, "Stochastic Reward Nets for reliability prediction," in Communications in Reliability, Maintainability and Serviceability, 1994, pp. 9–20.

[16] A. Reibman, R. Smith, and K. S. Trivedi, "Markov and Markov reward model transient analysis: An overview of numerical approaches," European Journal of Operational Research, vol. 40, no. 2, 1989, pp. 257–267, ISSN: 03772217.

[17] K. S. Trivedi and R. Sahner, "SHARPE at the age of twenty two," SIGMETRICS Perform. Eval. Rev., vol. 36, no. 4, 2009, pp. 52–57, ISSN: 01635999.