Accuracy of Third-Party Cloud Availability Estimation through ICMP

Maurizio Naldi
Department of Computer Science and Civil Engineering
University of Rome Tor Vergata
00133, Rome, Italy
Email: naldi@disp.uniroma2.it

***Abstract*—Third-party measurements of cloud availability are needed as a checkpoint of cloud providers' quality statements, and ICMP has been proposed to carry on such measurements. Simple ICMP-based measurement schemes, however, provide a poor discrimination between false outages and true cloud outages, unless the cloud outage probability is quite higher than the packet loss rate incurred by probing packets due to network failures. The use of a closely spaced sequence of probing instances, proposed to get rid of false outages, is ineffective for the purpose, unless the cloud itself is free of unavailability glitches.**

***Keywords*—Cloud, Availability, Cloud monitoring, ICMP.**

I. Introduction

Cloud availability is a major performance parameter for cloud platforms. When an individual or a company switch to the cloud, they wish the platform to be at least as available as their in-house infrastructure. For that reason, availability is always present among the parameters to be monitored in cloud monitoring systems [1] and to be considered in cloud platform assessment systems [2][3]. All major commercial cloud platforms typically include it in SLAs [4][5], and boast of their values: in the survey reported in [6], 15 providers out of 17 declared at least 99.9% availability, with 12 providers declaring 100% availability.

In order to check such performance claims, third-party availability measurements are strongly desired. While a model to predict cloud reliability has been proposed in [7], and the availability of single servers has been analysed in [8], not many efforts are present in the literature to investigate the overall availability actually offered on commercial platforms. For example, availability is not considered in the comparison carried out in [9]. In the description of a major commercial platform, Microsoft Azure, provided in [10], though a high availability is claimed right in the title, no figures are provided for the expected availability. Notable exceptions are represented by [11] and [12], where a probing method based on ICMP (Internet Control Message Protocol), suitable for third-party measurements, is adopted, though exhibiting several criticalities [13]. A different approach relies on reported data rather than actual measurements: data from cloud provider status dashboards and press releases have been collected and analysed in [14] and [15].

In this paper we investigate the critical issues arising from the use of ICMP to measure the availability of a cloud. We show that ICMP provides very weak discrimination between false outages, due to network failures, and true cloud outages, unless the cloud outage probability is much larger than the packet loss rate.

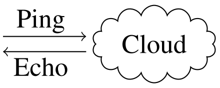

Fig. 1. Testing arrangement

The paper is organized as follows. In Section II we describe the testing arrangement based on ICMP, while its performances are analysed in Sections III through V.

II. Testing Arrangement

ICMP can be used to test cloud availability through a very simple testing arrangement. In this section, we describe that arrangement and its leverages.

The use of ICMP to test cloud availability is based on the *ping* command, as shown in Fig. 1, which operates by sending echo request packets to the target cloud (the front-end server, e.g., the hostname in the URL of the stored object for cloud storage) and counting the echoes as a measure of success as in [16] [11] [12]. After waiting for ICMP echo replies, the protocol reports packet loss and round-trip time statistics.

Positive replies are considered as successful, while lack of a reply or any error code are considered as a cloud outage. The actual arrangement needs some calibration and post-processing. For example, in [12] measurements are calibrated by probing two control sites, discarding cloud measurements when either of these control sites is unavailable.

ICMP allows for continuously sending echo requests. We consider here, as in [12], that the test is conducted by a sequence of closely spaced k echo requests and repeated at periodic intervals, so as to filter out unavailability glitches.

III. False Outages

The actual output of the testing process is impacted by both network and cloud failures. In this section, we examine the testing process when the cloud is actually available, but network failures are present.

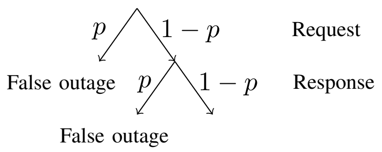

Fig. 2. Probability tree (no cloud failure)

If the cloud is available, we expect to receive a positive echo response for each request, but probing packets routinely get lost due to network failures. If p is the packet loss probability on the testing station-cloud path (we assume that it is the same in either way, and the failures on the two trips are uncorrelated due to time spacing), the resulting sequence for a single probing instance is shown in Fig. 2. Two leaves of the binary tree give rise to a negative outcome, and just one (both trips occurring with no packet loss) is reported as successful.

Since the cloud is available, what is reported as a failure is actually a false outage, whose probability in a single probing instance is therefore

$$P_{\text{fo}} = p + (1-p)p = p(2-p) \simeq 2p. \tag{1}$$

When accounting for the closely spaced repetition of k probing instances, we have several options to declare an outage (a false outage), among which the most relevant are

- majority voting;
- all failures.

According to the first criterion, we declare a cloud outage after a sequence of k echo requests when we have at least $k_{\text{min}} = \lceil \frac{k+1}{2} \rceil$ negative responses (no echoes). Under the second criterion, we must instead receive no echoes in a sequence of k requests to declare the cloud down.

If successive probing instances are uncorrelated, the false outage probability with k probing instances is

$$P_{\text{fo}}^{(k)} = \begin{cases} \sum_{i=k_{\text{min}}}^{k} \binom{i}{k} P_{\text{fo}}^{i}(1-P_{\text{fo}})^{k-i} & \text{majority voting} \\ P_{\text{fo}}^{k} & \text{all failures} \end{cases} \tag{2}$$

The aim of the close repetition of probing instances is to knock down the probability of false outages. In Fig. 3, we see that, for the choice $k=9$ adopted in [12], the repetition mechanism is highly effective: even when the packet loss probability is quite high ($p = 0.05$), the probability of false outage is as low as $8 \cdot 10^{-10}$ when the all failures rule is chosen and $8 \cdot 10^{-4}$ with majority voting. As expected, the all failures rule is much more effective than majority voting.

The number of retries has of course a significant impact. In Fig. 4, plotted for $p = 0.01$, we see the exponential fall of the probability of false outages under the all failures rule; majority voting exhibits a softer descent, whose staircase-like appearance is an artifact due to the majority rule (e.g., when passing from 4 to 5 retries the usefuls cases are respectively 3 or 4 out of 4 and 3, 4, or 5 out of 5).

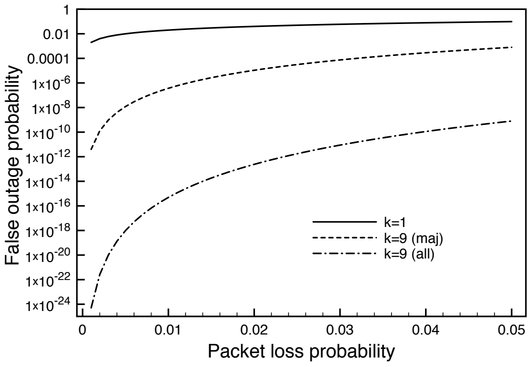

Fig. 3. Probability of false outage (k=9)

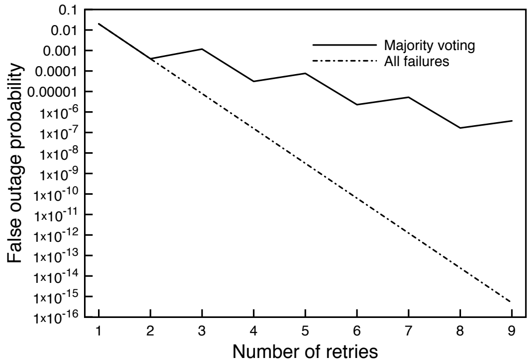

Fig. 4. Impact of the number of retries on false outage probability (p=0.01)

IV. Detection Performance

In Section III, we have examined how outages are declared even when the cloud is perfectly working. However, we must also examine if true outages are correctly detected. In this section, we compute the detection probability.

When the cloud is unavailable, the testing station receives no echo responses. In Fig. 5 we see how the various path sections contribute to the outage detection probability.

The probability of declaring a cloud failure is equal to the probability of receiving no response. If the cloud outage probability is r, the detection probability (on a single probing instance) is equal to the sum of the probabilities of the three

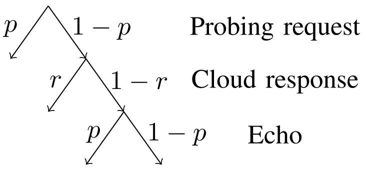

Fig. 5. Probability tree (cloud failure)

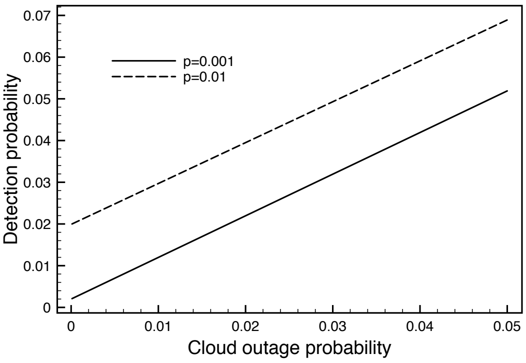

Fig. 6. Probability of detection

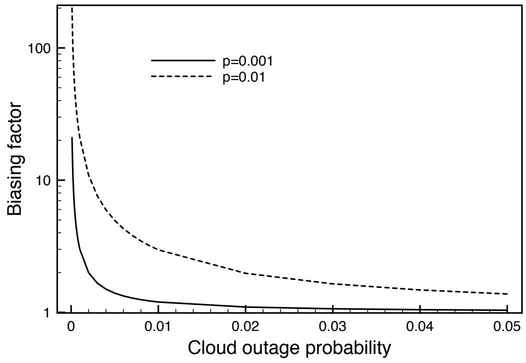

Fig. 7. Biasing factor

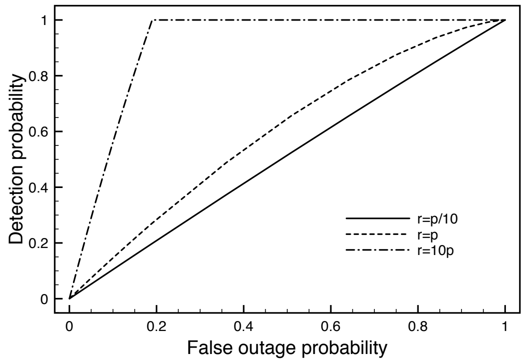

Fig. 8. ROC curve for single probing instances (k=1)

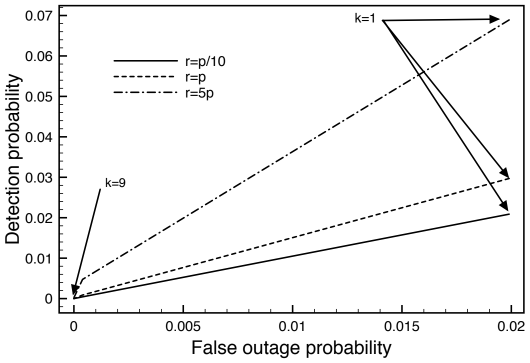

Fig. 9. Classifier performances for $p = 0.01$

left branches in the tree:

$$\begin{aligned} P_{\text{det}} &= p + (1-p)r + (1-p)(1-r)p \\ &= p(2-p) + r(1-p)^2 \simeq 2p + r, \end{aligned} \tag{3}$$

where we see clearly the contribution due to network failures (first term of the sum) and that due to the cloud (second term). In Fig. 6 we see that the probability of declaring an outage is a linear function of r and biased approximately by a $2p$ term. The biasing factor P_{det}/r may indeed be very large, as shown in Fig. 7, especially when $p > r$.

From Equations (1) and (3), we see that both the probability of false outage and the probability of detection are increasing functions of the packet loss rate p, so that we expect a trade-off to be established between the two performance indicators. We use the Receiver Operating Characteristic (ROC) to gain an overall view of the measurement scheme performance. In Fig. 8 we consider three cases, where the cloud outage probability is respectively much lower, equal, or much larger than the packet loss rate; in the last case, for $p > 0.1$ we consider a never responding cloud, i.e. $r = 1$. The three curves are plotted for a single probing instance ($k = 1$). As we can see, the ICMP-based approach performance is practically equal to a random classifier when $r \leq p$, and gets quite good just when $r \gg p$. The resulting value of the Area Under Curve is in fact 0.51 (barely higher than the 0.5 figure of a random classifier) when $r = p/10$, but jumps to to 0.91 when $r = 10p$.

With a series of probing instances, both the false outage probability and (unfortunately) the detection probability go down. In Fig. 9, we observe them both when $p = 0.01$ and k ranges from 1 to 9 (under the *all failures* criterion as defined in Section III). We see that adding more repetitions does not achieve a better trade-off, since we move along a straight line. In addition, as already noticed, there is very little discriminating power when $r \leq p$.

V. Detection of Long Outages

So far, the analysis has been focused on a single sequence of k probing instances, fired off at very close intervals. However, the measurement scheme proposed in [12] envisages the repetition of these sequences on longer intervals (10-11 minutes), to get a continuous monitoring of cloud failures, supposed to last longer than network failures. In this section, we assess the accuracy of such a monitoring scheme, and show that outages of duration lower than the interval between successive probing sequences may not be detected at all.

If we mark the occurrence of the measurement timepoint preceding the failure as time 0, so that the next measurement takes place at the time T (e.g., 10 or 11 minutes), the failure

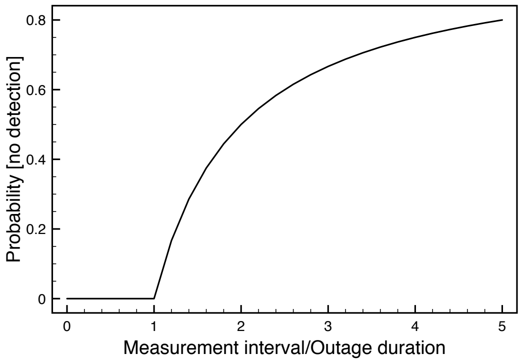

Fig. 10. Probability of an outage going undetected

will take place at a random time X such that $0 \leq X \leq T$. If we consider X to be uniformly distributed, the failure will not be detected if the recovery is achieved before the next measurement interval. If the outage duration is L, that condition can be expressed as $X + L < T$. The probability that the outage goes undetected is then

$$\begin{aligned} P_{\text{nodet}} &= \mathbb{P}[X + L < T] \\ &= \mathbb{P}\left[\frac{X}{T} < 1 - \frac{L}{T}\right] = \begin{cases} 0 & \text{if } T \leq L \\ 1 - \frac{L}{T} & \text{if } T > L \end{cases} \end{aligned} \quad (4)$$

The resulting no-detection probability is shown in Fig. 10.

Finally, the use of such a long measurement interval makes it difficult to obtain an accurate statistical distribution of outage durations. In turn, it becomes difficult to compute the extent of SLA violations and the amount of possible compensations or insurance claims [17][18][19]. In fact, of the three measures (Number of failures; Number of long outages; Cumulative outage duration.) envisaged to be used in an insurance policy for network failures in [20] (but applicable straightforwardly to the case of clouds), just one is considered in [12]. The cumulative outage duration is equal to the overall unavailability, but the number of failures is heavily distorted, since short-lived outages may go undetected, and the number of long outages may be underestimated as well, unless the threshold is longer than the measurement interval.

VI. Conclusion

The accuracy of ICMP-based third-party measurements of cloud availability is heavily affected by the presence of network failures, unless the cloud outage probability is quite higher than the packet loss rate. The use of a sequence of closely spaced probing instances to get rid of false outages lowers the detection probability by roughly the same factor, unless the cloud itself is immune from unavailability glitches. In addition, the use of a long measurement interval may make short unavailability periods undetected.

References

[1] J. Montes, A. Sánchez, B. Memishi, M. S. Pérez, and G. Antoniu, “Gmone: A complete approach to cloud monitoring,” *Future Generation Computer Systems*, vol. 29, no. 8, pp. 2026–2040, 2013.

[2] Z. Li, L. O’Brien, H. Zhang, and R. Cai, “On a catalogue of metrics for evaluating commercial cloud services,” in *Grid Computing (GRID), 2012 ACM/IEEE 13th International Conference on*, Sept 2012, pp. 164–173.

[3] R.N. Calheiros, R. Ranjan, A. Beloglazov, C.A.F. De Rose, and R. Buyya, “Cloudsim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms,” *Software: Practice and Experience*, vol. 41, no. 1, pp. 23–50, 2011.

[4] A. Cuomo, G. Di Modica, S. Distefano, A. Puliafito, M. Rak, O. Tomarchio, S. Venticinque, and U. Villano, “An SLA-based broker for cloud infrastructures,” *Journal of Grid Computing*, vol. 11, no. 1, pp. 1–25, 2013.

[5] V. C. Emeakaroha, M. A. Netto, R. N. Calheiros, I. Brandic, R. Buyya, and C. A. D. Rose, “Towards autonomic detection of {SLA} violations in cloud infrastructures,” *Future Generation Computer Systems*, vol. 28, no. 7, pp. 1017 – 1029, 2012.

[6] E. Casalicchio and L. Silvestri, “Mechanisms for SLA provisioning in cloud-based service providers,” *Computer Networks*, vol. 57, no. 3, pp. 795–810, 2013.

[7] Y.-S. Dai, B. Yang, J. Dongarra, and G. Zhang, “Cloud service reliability: Modeling and analysis,” in *15th IEEE Pacific Rim International Symposium on Dependable Computing*, 2009.

[8] K. V. Vishwanath and N. Nagappan, “Characterizing cloud computing hardware reliability,” in *Proceedings of the 1st ACM symposium on Cloud computing SoCC*. ACM, 2010, pp. 193–204.

[9] A. Li, X. Yang, S. Kandula, and M. Zhang, “Cloudcmp: comparing public cloud providers,” in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, 2010, pp. 1–14.

[10] B. Calder, J. Wang, A. Ogus, N. Nilakantan, A. Skjolsvold, S. McKelvie, Y. Xu, S. Srivastav, J. Wu, H. Simitci *et al.*, “Windows azure storage: a highly available cloud storage service with strong consistency,” in *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*. ACM, 2011, pp. 143–157.

[11] D. Ford, F. Labelle, F. I. Popovici, M. Stokely, V.-A. Truong, L. Barroso, C. Grimes, and S. Quinlan, “Availability in globally distributed storage systems,” in *9th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2010*, Vancouver, BC, Canada, October 4-6, 2010, pp. 61–74.

[12] Z. Hu, L. Zhu, C. Ardi, E. Katz-Bassett, H. Madhyastha, J. Heidemann, and M. Yu, “The need for end-to-end evaluation of cloud availability,” in *Passive and Active Measurement*, ser. Lecture Notes in Computer Science, M. Faloutsos and A. Kuzmanovic, Eds. Springer International Publishing, 2014, vol. 8362, pp. 119–130.

[13] M. Naldi, “A note on ”the need for end-to-end evaluation of cloud availability”,” *arXiv CoRR Preprint Series*, vol. abs/1408.0510, 2014.

[14] C. Cérin, C. Coti, P. Delort, F. Diaz, M. Gagnaire, Q. Gaumer, N. Guillaume, J. L. Lous, S. Lubiarz, J.-L. Raffaelli, K. Shiozaki, H. Schauer, J.-P. Smets, L. Séguin, and A. Ville, “Downtime statistics of current cloud solutions,” International Working Group on Cloud Computing Resiliency, Tech. Rep, June 2013.

[15] M. Naldi, “The availability of cloud-based services: Is it living up to its promise?” in *9th International Conference on the Design of Reliable Communication Networks, DRCN 2013, Budapest, Hungary*, March 4-7, 2013, pp. 282–289.

[16] D. D. Long, J. L. Carroll, and C. Park, “A study of the reliability of internet sites,” in *Reliable Distributed Systems, 1991. Proceedings., Tenth Symposium on*. IEEE, 1991, pp. 177–186.

[17] M. Naldi and L. Mastroeni, “Violation of service availability targets in service level agreements,” in *Federated Conference on Computer Science and Information Systems - FedCSIS 2011, Szczecin, Poland*, 18-21 September 2011, pp. 537–540.

[18] L. Mastroeni and M. Naldi, “Compensation policies and risk in service level agreements: A value-at-risk approach under the on-off service model,” in *7th International Workshop on Internet Charging and QoS Technologies, ICQT 2011, Paris, France*, ser. Lecture Notes in Computer Science, vol. 6995. Springer, October 24, 2011, pp. 2–13.

[19] P. Cholda, E. L. Følstad, B. E. Helvik, P. Kuusela, M. Naldi, and I. Norros, “Towards risk-aware communications networking,” *Rel. Eng. & Sys. Safety*, vol. 109, pp. 160–174, 2013.

[20] L. Mastroeni and M. Naldi, “Network protection through insurance: Premium computation for the on-off service model,” in *8th International Workshop on the Design of Reliable Communication Networks DRCN, Krakow, Poland*, 10-12 October 2011, pp. 46–53.