Content Accessibility in Optical Cloud Networks Under Targeted Link Cuts

(Invited Paper)

Carlos Natalino*, Aysegul Yayimli†, Lena Wosinska*, and Marija Furdek*
*Royal Institute of Technology (KTH), Stockholm, Sweden. E-mail: {carlosns, wosinska, marifur}@kth.se
†Istanbul Technical University (ITU), Istanbul, Turkey. E-mail: gencata@itu.edu.tr

***Abstract*—One of the key enablers of the digital society is a highly reliable information infrastructure that can ensure resiliency to a wide range of failures and attacks. In cloud networks, replicas of various content are located at geographically distributed data centers, thus inherently enhancing cloud network reliability through diversification and redundancy of user accessibility to the content. However, cloud networks rely on optical network infrastructure which can be a target of deliberate link cuts that may cause service disruption on a massive scale. This paper investigates the dependency between the extent of damage caused by link cuts and a particular replica placement solution, as a fundamental prerequisite of resilient cloud network design that lacks systematic theoretical quantification and understanding.**

To quantify the vulnerability of optical cloud networks based on anycast communication to targeted link cuts, we propose a new metric called Average Content Accessibility (ACA). Using this metric, we analyze the impact of the number and the placement of content replicas on cloud network resiliency and identify the best and the worst case scenarios for networks of different sizes and connectivity. We evaluate the efficiency of simultaneous and sequential targeted link cuts, the latter reassessing link criticality between subsequent cuts to maximize disruption. Comparison with Average Two-Terminal Reliability (A2TR), an existing robustness measure for unicast networks, shows great discrepancy in the vulnerability results, indicating the need for new measures tailored to anycast-based networks.

I. INTRODUCTION

The cloud networking paradigm relies on replicating data resources, i.e., content, and placing the replicas at geographically distributed data centers. End users may connect to any of the data centers that host the desired replica following the anycast communication paradigm where the destination node of each user request is not predetermined, but is selected from a set of possible destinations [1]. Cloud computing principles allow for lowering the latency in accessing the content and balancing the load across the data center nodes. To support cloud services the underlying optical network infrastructure must, aside from providing tremendous capacity and low latency, also assure high reliability. Optical networks that support Content Delivery Networks (CDNs) are vulnerable to a wide range of physical-layer attacks aimed at service degradation [2]. Link cuts are a straightforward way of causing outright service interruption at a relatively low level of attack sophistication. To boost the efficiency of link cuts, attackers are typically interested in targeting the most critical links and causing maximum damage to the network.

Content replication in CDNs inherently increases network resiliency by providing users with access to content replicas at several locations that can be reached via diverse paths. However, the exact extent of the damage caused by link cuts greatly depends on the number of replicas and their particular placement, as well as the number and locations of the cut links. In order to design the network in a resilient way and to aid Service Level Agreement (SLA) definition, cloud service providers must be able to evaluate and quantify the resiliency of their network.

Different vulnerability metrics were defined in the literature to model robustness of a physical network topology in terms of network connectivity in the presence of component failures [3], [4]. Some of the metrics, such as connectivity and Average Two-Terminal Reliability (A2TR), use structural properties of the network topology graph to express the level of difficulty to disconnect parts of the network. Other metrics quantify the centrality of individual components in terms of, for example, the nodal degree or betweeness, i.e., the number of shortest paths that traverse it. However, none of the existing metrics are applicable to the CDN environment with geographically distributed content replicas and anycast communication.

This paper proposes a new performance metric, called Average Content Accessibility (ACA), to measure the robustness of a CDN. ACA is defined as the ability to guarantee accessibility to content even if the network is partitioned by failures. The new metric is applied to gauge the vulnerability of the cloud network to targeted link cuts as a function of the number and the placement of content replicas. It allows us to calculate the upper and the lower bound on network robustness for a given number of replicas and a set of cut links partitioning the network, denoted as Best Case Scenario (BCS) and Worst Case Scenario (WCS), respectively. We also assess the ACA for a more realistic scenario with predetermined replica locations, denoted as Real Case Scenario (RCS). Our study considers targeted attacks that are generally more disruptive than random failures [4], [5]. We evaluate ACA for two types of targeted attacks that *(i)* calculate the link betweeness centrality once and cut a portion of links with the highest betweeness simultaneously, and *(ii)* cut the links with the highest betweeness sequentially, reassessing their betweeness in the changed topology to maximize damage.

The remainder of the paper is organized as follows. Section II provides an outline of the related works. Section III describes the content accessibility model used in the study along with an illustrative example. Section IV presents details of the problem considered in this work, formally defines the proposed ACA metric and specifies the calculation of its BCS, WCS and RCS variants. Numerical results are presented in Section V, while Section VI provides concluding remarks.

II. RELATED WORK

The tolerance of large-scale communication network topologies to targeted attacks is investigated in [5], [6]. The robustness analyses therein indicate that the removal of a few vital nodes or links can severely damage network connectivity. Several metrics have been proposed to evaluate the network reliability under attack or failure scenarios. The authors in [3] define Average Two-Terminal Reliability (A2TR) as a measure of how the disruption of network elements (nodes or links) affects connectivity between node pairs. For each node pair, two-terminal reliability is equal to 1 if there is a path between them, and 0 otherwise. The A2TR then is the average value over all node pairs in the network. A thorough robustness analysis of 15 network topologies is presented in [4], evaluating the topologies for a variety of structural, centrality and functional measures. Network planning approaches to increase robustness are proposed in [7], [8]. The work in [7] compares reliability and cost of real-world network topologies and topologies designed to maximize reliability, indicating that reliability maximization may result in network topologies with lower cost. All of these works consider unicast traffic and are not applicable to anycast-based CDNs.

An optimization model for routing of unicast and anycast traffic to protect the traffic against attacks is proposed in [8]. The authors state that the current irregular network topologies require new routing strategies to reduce the damage caused by attacks. Namely, attacks usually target high-degree nodes which are traversed by a great number of shortest paths in the network. Results show that by avoiding high-degree nodes as replica hosts and by routing traffic away from such nodes, the connection disruption caused by attacks can decrease up to 7 times. However, the work does not provide any theoretical assessment of a CDN vulnerability to attacks applicable to different replica placement strategies and routing approaches.

The study in [9] focuses on the identification of critical network nodes. The authors propose optimization models which identify the set of nodes that, if removed, minimize the network connectivity. The resulting set of critical nodes can indicate, for example, which nodes to reinforce, and the analysis is agnostic to traffic.

This paper focuses on evaluating the robustness of CDNs to targeted link cuts by proposing a measure for content accessibility and assessing the impact of replica placement on this measure. To the best of our knowledge, this is the first work to model and quantify content accessibility in CDNs.

III. CONTENT ACCESSIBILITY IN CDNS

In the context of this work, content accessibility in a multi-replica cloud network is defined as the ability of a given segment of the network topology (e.g., a network node) to access the content that is replicated over a number of nodes. The network topology is represented by a set of nodes interconnected by network links. Our study focuses on the core network segment, where the network nodes represent aggregation nodes that serve a number of users, and are interconnected by high capacity links. We consider the case where all network nodes are equipped with storage capabilities and can therefore host the content replicas.

TABLE I
PARAMETERS AND NOTATION.

Symbol	Description
$G(V, E)$	The graph representing network topology with $\|V\|$ nodes and $\|E\|$ links after a link cut attack.
r	The number of content replicas in the network.
C	The set of connected components of graph $G(V, E)$ separated by the link cuts. Each component C_i comprises $\|C_i\|$ nodes.
x_i	A binary variable that is equal to 1 if there is a content replica hosted in any of the nodes within the connected component C_i.

The link cut attacks to the network infrastructure cause outright connectivity loss of the affected links. As a result of the link cuts, the network is partitioned into several connected components, i.e., segments or subgraphs. Nodes within a connected component can communicate with each other, but are completely isolated from the remainder of the network. In the presence of an attack, a content is considered accessible if the requesting (source) node can connect to any of the nodes hosting a replica of that content, i.e., there exists a path in the partitioned network between the requesting node and any of the replicas. The parameters and notation used to model the described scenario are presented in Table I.

The content placement, i.e., the distribution of replicas over CDN nodes is a vital factor in determining the ability of the network to maintain content accessibility under targeted attacks. In an effort to make the network more robust to attacks, content placement can be carried out in accordance to different robustness measures, selecting the nodes with the highest values of these measures as replica hosts. In this paper, we consider the following four robustness measures as criteria for content placement.

- *Degree centrality* is the simplest node centrality metric that is determined by the physical degree of a node [4];
- *Betweeness centrality* is defined as the number of shortest paths (between all pairs of nodes in the network) that traverse a network element (link or node) [4];
- *Closeness centrality* measures the importance of a node based on its average distance from all other nodes [4];
- *Clustering classification* measures the distance of nodes, groups the nodes into a number of pre-defined clusters, and defines a centroid for each cluster. Different clustering algorithms can be applied.

The impact of content placement according to the above criteria on content accessibility is illustrated on a simple CDN example with 5 nodes denoted as A-D, 6 links and 2 replicas

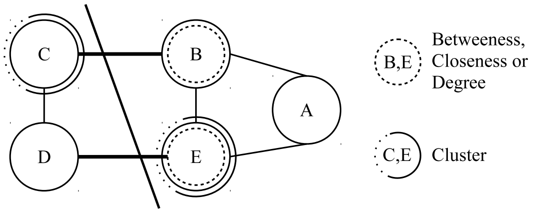


Fig. 1. An illustrative CDN example with 2 content replicas placed according to 4 different criteria: node betweeness, closeness and degree centrality, and clustering. Links with the highest betweeness (B-C and D-E) are cut by the attacker.

shown in Fig. 1. Two links with the highest betweeness, i.e., links B-C and D-E are cut by the attacker in an effort to maximize the damage. Applying node degree, closeness or betweeness centrality measures as criteria for replica placement all yield the same solution where nodes B and E are selected as replica hosts. In the considered attack scenario targeting the two most vulnerable links B-C and D-E, both content replicas would be placed in the same connected component of the network comprising nodes {A,B,E}, thus leaving the content inaccessible to nodes {C,D} in the other connected component. This indicates that traditional robustness metrics are not suitable for replica placement, as they tend to concentrate the replicas in a central region of the network, or at nodes close to each other.

To increase content accessibility, spreading the replicas over different regions of the network topology may be a better strategy to prevent an attacker from isolating the replicas in more central nodes and to aggravate the effort required to disconnect the replicas. The clustering approach in the illustrative example would place replicas at nodes C and E, making the content accessible to all network nodes even after the two most vulnerable links are cut.

IV. AVERAGE CONTENT ACCESSIBILITY (ACA)

To quantify the ability of a CDN to maintain content accessibility in the presence of link cuts, we propose a new robustness metric called Average Content Accessibility (ACA). For a given network topology partitioned by link cuts and a given number of content replicas, the ACA is defined as the percentage of network nodes that are still able to connect to a content replica. If the network is unpartitioned or if all nodes can reach a content replica within their connected component, content accessibility is equal to 1. If some nodes in the partitioned network cannot access any of the content replicas, the ACA value is between 0 and 1. To investigate the impact of replica placement on the resulting ACA values, we evaluate the best case, the worst case, and realistic scenarios.

A. The ACA in the Best Case Scenario (ACA-BCS)

The Average Content Accessibility in the Best Case Scenario (ACA-BCS) is a theoretical metric that calculates the upper bound on the ACA value for a given network topology and a number of content replicas. The value of ACA is the highest when content is spread across the largest connected components, such that each of the components hosts one replica. If there is only 1 replica in the example network from Fig. 1, ACA-BCS is achieved when that replica is placed in the largest connected component {A,B,E}.

Algorithm 1: Algorithm for the ACA_{wcs}

```
Data: $G(V,E)$, $r$, $C$
Result: $ACA_{wcs}(r)$
for combination in binary $0..2^{|C|}-1$ do
    $sum \leftarrow \sum_{i=1}^{|C|} |C_i| \times combination_i$;
    if $sum = r$ then
        return $\frac{sum}{|V|}$;
$\bar{r} \leftarrow r$; $CP \leftarrow C$; $sum \leftarrow 0$;
while $\bar{r} > 0$ do
    if $\exists_i$ such that $|CP_i| > \bar{r}$ then
        $C_{BF} \leftarrow min_i(|CP_i| - \bar{r})$;
        $\bar{r} \leftarrow \bar{r} - |C_{BF}|$;
        $sum \leftarrow sum + |C_{BF}|$;
        $CP \leftarrow CP \backslash C_{BF}$;
    else
        $C_{BF} \leftarrow min_i(\bar{r} - |CP_i|)$;
        $\bar{r} \leftarrow \bar{r} - |C_{BF}|$;
        $sum \leftarrow sum + |C_{BF}|$;
        $CP \leftarrow CP \backslash C_{BF}$;
return $\frac{sum}{|V|}$;
```

ACA-BCS is calculated by first sorting the set of connected components in the descending order of their size. For the example in Fig. 1, the resulting sorted set C^{desc} is equal to $\{\{A, B, E\}, \{C, D\}\}$, with $|C_1^{desc}| = 3$ and $|C_2^{desc}| = 2$. The value of ACA-BCS is determined by Eq. (1), dividing the total size of r largest components by the number of nodes in the network.

$$ACA_{bcs}(r) = \frac{\sum_{i=1}^{r} |C_i^{desc}|}{|V|} \tag{1}$$

ACA-BCS for our simple example in Fig. 1 and $r = 1$ equals:

$$ACA_{bcs}(1) = 3/5 = 0.6, \tag{2}$$

meaning that 60% of nodes have access to the content. For $r = 2$, ACA-BCS is equal to 1, obtained by placing a replica at each of the two connected components.

B. The ACA in the Worst Case Scenario (ACA-WCS)

The Average Content Accessibility in the Worst Case Scenario (ACA-WCS) is a theoretical metric that calculates the lower bound on the ACA value for a given network topology and a number of content replicas. The lowest value of ACA occurs in two situations, depending on the relation between the number of replicas and the size of network partitions: the exact fit or the best fit. The exact fit occurs when the number of replicas is equal to the number of nodes in one or more connected components. Placing all replicas in those components leaves the content inaccessible to nodes in all other components. In the example from Fig. 1, the exact fit happens when considering 2 or 3 content replicas. For 2 replicas, they would be placed at nodes C and D, yielding ACA-WCS equal to 0.4. For 3 replicas, they would be placed at nodes A, B and E, yielding the ACA-WCS value of 0.6. If the replicas do not fit exactly to any subset of network partitions, ACA-WCS is calculated by searching for the best fit of replicas to the smallest connected components. For the Fig. 1 example with a single replica, ACA-WCS is obtained by placing it into the smallest connected component, i.e., {C,D}, resulting with ACA-WCS equal to 0.4.

Algorithm 1 presents the heuristic used to calculate ACA-WCS for a given number of replicas. The algorithm first attempts to find an exact fit for placing all replicas into one or more connected components (lines 1-4). The exact fit part starts by enumerating all possible combinations of the connected components (line 1) hosting content replicas by using a binary vector with $|C_i|$ elements. Element i is equal to 1 if every node in the corresponding connected component C_i hosts one replica, and to 0 if there are no replicas in C_i. The total number of nodes that host a replica for a given binary representation, denoted as sum, is obtained by adding up the sizes of components whose corresponding element in the binary vector equals 1 (line 2). If this number matches the number of replicas (line 3), the algorithm has found the worst case according to the exact fit scenario and returns the calculated ACA-WCS value (line 4).

If an exact fit does not exist, the algorithm searches for ACA-WCS according to the best fit (lines 5-19). The number of replicas to install, denoted as $\bar{r}$, is initialized to r (line 5), a working copy CP of the set of connected components is made (line 6), and the value of sum is initialized to zero (line 7). While there are still replicas to install (line 8), and if there exist connected components with size greater than $\bar{r}$ (line 9), the algorithm finds the best fit component C_{BF} whose size is the closest to $\bar{r}$ (line 10), places replicas at all nodes of C_{BF}, decreases the value of $\bar{r}$ by $|C_{BF}|$ (line 11), and counts all nodes from C_{BF} as connected to a replica (line 12). The case when the remaining components are smaller than $\bar{r}$ is analogous, using the same absolute difference between the size of connected components and the number of unassigned replicas to find the best fit component C_{BF} (lines 14-18).

The difference in the worst and the best case ACA is drastic even in our simple example. For the content to be accessible to all nodes using the worst case placement, i.e., for ACA-WCS to be equal to 1, four replicas need to be placed in the network, while two replicas suffice to achieve ACA-BCS equal to 1.

C. The ACA in a Real Case Scenario (ACA-RCS)

While ACA-BCS and ACA-WCS calculate the hypothetical best and worst case replica placement for a given network partitioned by link cuts, Average Content Accessibility in a Real Case Scenario (ACA-RCS) needs to consider the actual replica placement modeled by the variables x introduced in Table I. For each connected component C_i, the associated x_i variable is equal to 1 if C_i hosts at least one replica, and 0 otherwise. The value of ACA-RCS for a given placement of r replicas is calculated by multiplying the number of nodes in each connected component by the associated x_i using Eq. (3).

$$ACA_{rcs}(r) = \frac{\sum_{i=1}^{|C|} |C_i| \times x_i}{|V|}. \tag{3}$$

V. NUMERICAL RESULTS

The ACA analyses under targeted simultaneous and sequential link cut attacks were carried out using a custom-built Java-based tool on 3 network topologies represented with GraphStream library [10], with characteristics summarized in Table II. For each topology, the four criteria described in Section III are used to define the placement of different numbers of replicas. The K-Means clustering algorithm from Weka library [11] is used to perform clustering of the topologies, relying on the shortest path length between nodes as the distance function.

In each experiment, the links are sorted in the descending order of their betweeness centrality and a portion of the most central links is removed from the graph to simulate the attack. In simultaneous cut attack, the link betweeness centrality is evaluated on the initial topology and the links are cut at once, while in sequential cut attack the betweeness centrality of links is re-evaluated upon the removal of each link.

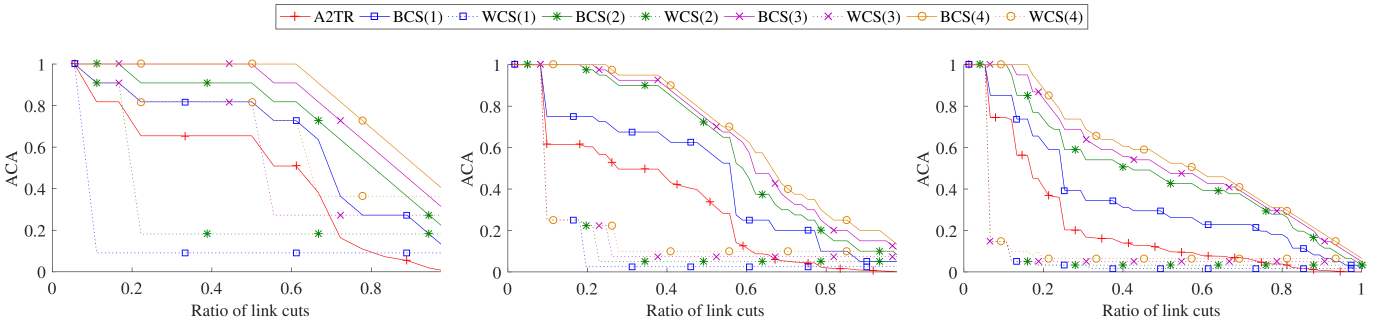
A. The Impact of the Number of Replicas on ACA

Fig. 2 shows the ACA values for BCS and WCS with 1-4 replicas under simultaneous link cuts. The values of ACA-BCS and ACA-WCS are separated by a large gap, showing that the replica placement strategy plays a huge role in the overall content accessibility. For the same percentage of link cuts, the ACA values exhibit drastically different trends for the different topologies. For instance, in the Sprint topology with 4 replicas, ACA-BCS stays at 100% up to 60% of cut links (Fig. 2a). For the Garr topology (Fig. 2c), the 100%-content accessibility is maintained only up to 20% of cut links. This can be explained by the fact that the Garr network has the lowest average nodal degree among the considered topologies. Therein, 20% of cut links correspond to the removal of 15 links, a number that is able to isolate several nodes in the network.

The number of replicas, as expected, significantly changes the ACA values. The increase from 1 to 2 replicas already considerably improves ACA in all topologies. However, further increase of the number of replicas does not achieve the equivalent additional gain. The gain in content availability that stems from having more than 2 replicas is meaningful only at a medium to large number of link cuts, e.g., after around 20% of link cuts in the case of Géant and Garr.

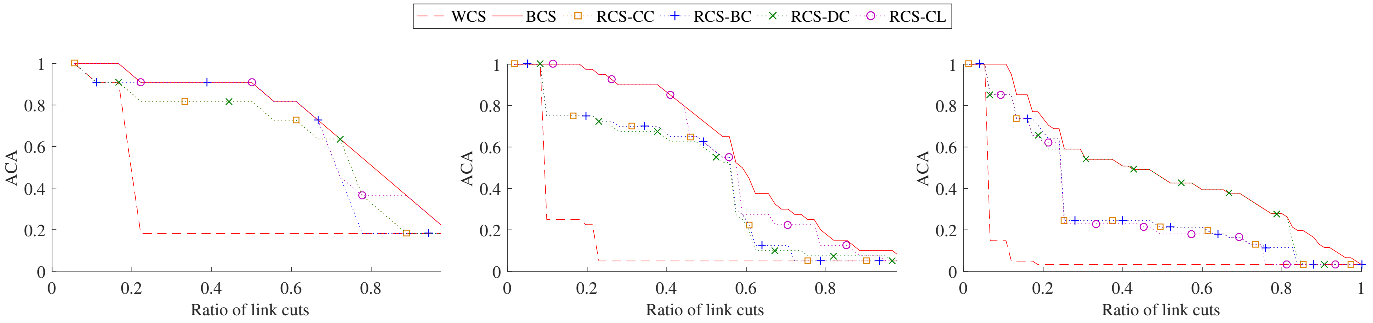
TABLE II
SET OF TOPOLOGIES CONSIDERED FOR THE EXPERIMENTS [12].

Topology	n	m	$k \pm StDev$	D
Sprint	11	18	3.27 ± 1.42	4
Géant	40	61	3.05 ± 1.92	8
Garr	61	75	2.45 ± 2.58	8

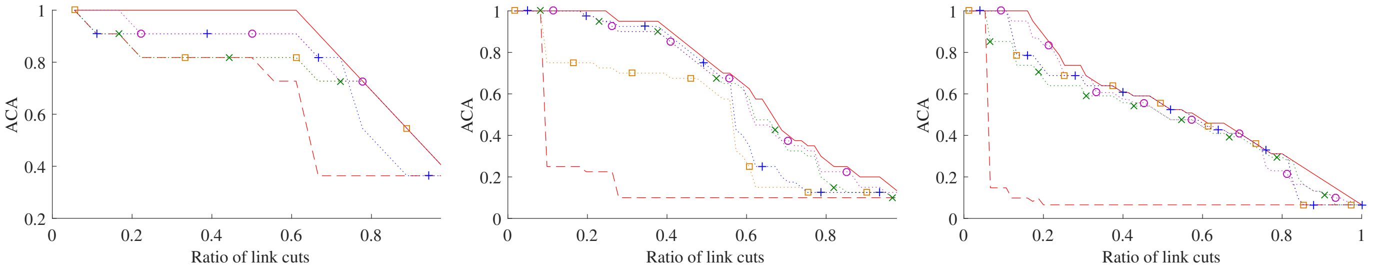


(a) Sprint (b) Géant (c) Garr

Fig. 2. A2TR and ACA metric for BCS and WCS for 1-4 replicas under simultaneous link cuts with highest betweeness centrality.



(a) Sprint with 2 replicas (b) Géant with 2 replicas (c) Garr with 2 replicas



(d) Sprint with 4 replicas (e) Géant with 4 replicas (f) Garr with 4 replicas

Fig. 3. ACA metric for networks under simultaneous link cuts based on link betweeness centrality with RCS for different content placement strategies: closeness centrality (CC), betweeness centrality (BC), degree centrality (DC) and clustering (CL).

Fig. 2 also shows the A2TR metric, applicable for unicast-based networks, for comparison purposes. A2TR follows similar trends as ACA-BCS, but at drastically different values, and is completely different from ACA-WCS. The large discrepancy between A2TR and ACA indicates the inability of A2TR to accurately capture content accessibility in CDNs.

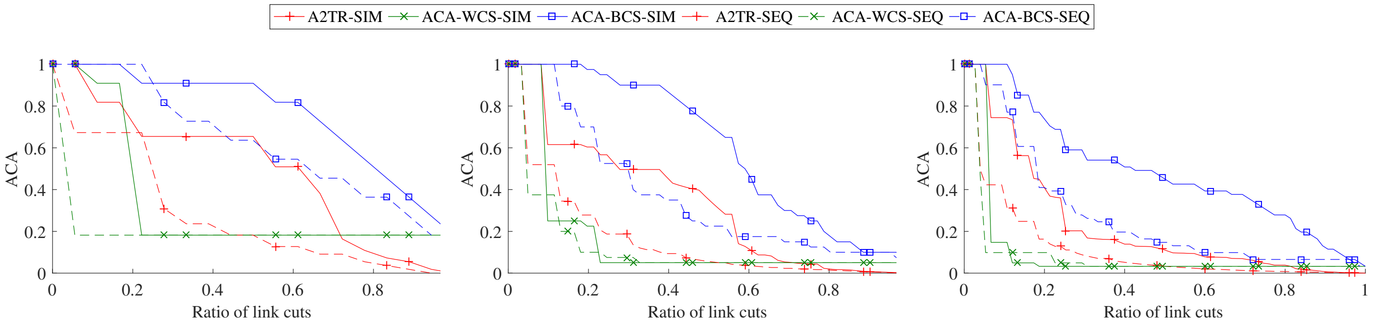
B. The Impact of the Replica Placement on ACA

Fig. 3 shows the effect of four different replica placement strategies to ACA-RCS, for 2 (Fig. 3a-c) and 4 replicas (Fig. 3d-f). WCS and BCS show the lower and upper bounds for each scenario, respectively. The closer the ACA-RCS value gets to the BCS, the better the placement strategy is.

In general, the clustering approach achieves better performance than the three replica placement strategies based on centrality measures, especially for attacks that cut up to 20% of network links. For instance, in the Géant topology with 2 replicas (Fig. 3b), the clustering placement is able to achieve the BCS performance for up to 40% of links cut. The centrality-based strategies perform the worst in most cases for lower ratio of link cuts. However, in Garr topology with 2 replicas (Fig. 3c), the degree centrality-based replica placement reaches BCS for 30% or more link cuts. This behavior can be explained by the high variability of the nodal degree in this network (Tab. II), which makes the highly connected nodes more difficult to disconnect. When the number of replicas increases to 4 (Fig. 3f), the performance of other placement strategies improves and their ACA increases. Interestingly, the WCS rises only for the Sprint network, in which 4 replicas make a more significant portion of the total number of network nodes than in the larger two networks.

C. The Impact of Simultaneous and Sequential Targeted Attacks on ACA

Fig. 4 shows how ACA-BCS and ACA-WCS change for simultaneous (SIM) and sequential (SEQ) targeted link cuts.



(a) Sprint (b) Géant (c) Garr

Fig. 4. ACA and A2TR for BCS and WCS metrics for networks with 2 replicas under simultaneous (continuous lines) and sequential (dashed lines) link cuts based on link betweeness.

A2TR is also shown for comparison. In general, sequential attacks are more effective in decreasing the content accessibility by cutting the same number of links as the simultaneous strategy.

The greater damage caused by sequential targeted attacks can be explained by the fact that when links are cut, the connectivity of the network changes. As the simultaneous targeted attack evaluates the importance of each link at the beginning of the attack, it does not foresee the changes in link importance in the modified topology. The results also show that sequential attacks can be less disruptive than the simultaneous ones in specific cases. Such cases occur when the network is divided into several connected components and, as the connectivity changes, links with the highest link betweeness emerge in the center of a subgraph. The removal of such link will not divide the connected component, and will thus not decrease ACA in the same way as simultaneous attacks.

VI. CONCLUSION

This paper introduces the concept of content accessibility in multi-replica content delivery networks in the presence of targeted link cuts by proposing a new performance metric called Average Content Accessibility (ACA). We evaluate the dependence of ACA on the number and the placement of replicas in the network partitioned by link cuts, as well as the influence of two different attack strategies. By calculating the values of ACA in the best and the worst case scenarios, denoted as BCS and WCS, respectively, we assess the lower and the upper bound on network vulnerability to attacks.

The experiments performed on real-world topologies show that the proposed metric is more suitable to represent content accessibility than the existing metrics in the literature. The increase of the number of replicas proves effective in enhancing the ACA values when considering the increment from 1 to 2 replicas, but further increase does not exhibit equally proportional improvement of content accessibility. The results also indicate a strong influence of replica placement strategies on ACA, where the strategies based on clustering and nodal degree centrality are capable of reaching the BCSs values under certain circumstances.

For future work, we plan to extend the analysis to consider the relation between additional parameters and the ACA. The obtained insights will then be applied to develop approaches for increase content accessibility by sparsely adding network components at key locations and perform replica placement so as to increase network robustness to targeted attacks.

ACKNOWLEDGMENT

This article is based upon work from COST Action CA15127 (“Resilient communication services protecting end-user applications from disaster-based failures – RECODIS”) supported by COST (European Cooperation in Science and Technology).

REFERENCES

[1] J. Simmons, *Optical network design and planning*, 2nd ed. Springer, 2014.
[2] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, “Physical-layer security in evolving optical networks,” *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, 2016.
[3] S. Rai and D. Agrawal, *Distributed computing network reliability*. Los Alamitos, CA (USA); IEEE Computer Society, Jan 1990.
[4] D. F. Rueda, E. Calle, and J. L. Marzo, “Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements,” *Journal of Network and Systems Management*, vol. 25, no. 2, pp. 269–289, 2017.
[5] R. Albert, H. Jeong, and A.-L. Barabasi, “Error and attack tolerance of complex networks,” *Nature*, vol. 406, pp. 378–382, July 2000.
[6] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang, “Attack robustness and centrality of complex networks,” *PLoS ONE*, vol. 8, no. 4, Apr 2013.
[7] C. Pavan, L. S. de Lima, M. H. M. Paiva, and M. E. V. Segatto, “How reliable are the real-world optical transport networks?” *IEEE/OSA J. Opt. Commun. Netw.*, vol. 7, no. 6, pp. 578–585, June 2015.
[8] J. Rak and K. Walkowiak, “Reliable anycast and unicast routing: protection against attacks,” *Telecommunication Systems*, vol. 52, no. 2, pp. 889–906, 2013.
[9] D. Santos, A. F. Sousa, and P. Monteiro, “Compact models for critical node detection in telecommunication networks,” in *International Network Optimization Conference (INOC)*, Feb 2017, pp. 1–10.
[10] Y. Pign, A. Dutot, F. Guinand, and D. Olivier, “Graphstream: A tool for bridging the gap between complex systems and dynamic graphs,” in *Emergent Properties in Natural and Artificial Complex Systems at ECCS’2007*, Dresden, Germany, 2007.
[11] I. Witten and E. Frank, *Data Mining: Practical Machine Learning Tools and Techniques, Second Edition*, ser. The Morgan Kaufmann Series in Data Management Systems. Elsevier Science, 2005.
[12] S. Knight, H. X. Nguyen, N. Falkner, R. Bowden, and M. Roughan, “The internet topology zoo,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 9, pp. 1765–1775, Oct 2011.