Critical Region Identification and Geodiverse Routing Protocol under Massive Challenges

Yufei Cheng*, and James P.G. Sterbenz*†‡
*Information and Telecommunication Technology Center
Department of Electrical Engineering and Computer Science
The University of Kansas, Lawrence, KS, 66045, USA
† School of Computing and Communications (SCC) and InfoLab21
Lancaster LA1 4WA, UK
‡Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong
{yfcheng|jpgs}@ittc.ku.edu, jpgs@comp.{lancs.ac.uk,polyu.edu.hk}
www.ittc.ku.edu/resilinets

***Abstract*—Regionally-correlated failures or attacks pose a great challenge to the normal network communication for physical backbone networks. When the same intensity of challenges occur at different physical locations, the damage to the network connectivity varies greatly. In this paper, we propose a critical region identification model and demonstrate its effectiveness in finding critical regions for fiber-level networks under regionally-correlated failures or attacks. We apply the model on several real-world backbone networks to demonstrate its efficiency using both unweighted and weighted topologies. Furthermore, the identified critical region result is used to improve the routing performance using GeoDivRP, a resilient routing protocol with geodiversity considered.**

***Index Terms*—network resilience and survivability; regionally-correlated challenges; critical region identification; geodiverse routing protocol; network simulation;**

I. Introduction and motivation

The requirement for Internet resilience has been increasing tremendously. Telecommunication networks are widely used for carrying user traffic and they rely heavily on the physical infrastructure such as optical fibers, routers, and switches to maintain normal operations. The resilience of these topologies to various faults and challenges is important to be analyzed [1].

Network monitoring and protection are important for maintaining normal network operations. Detection of the vulnerable areas or critical regions has several practical applications, fibers in these regions can be either protected by shielding, strengthening, or closely monitoring for resilient network communication. The fiber-level network is usually deployed in a large geographical region which complicates either the protection or monitoring. However, if the critical region could be identified, these regions can have better concentration of resources and the benefit of protection can be maximized.

Networks are generally studied as pure graphs without considering the geographical properties of nodes and links [2]. Network components in physical adjacency may fail together during an electrical blackout or an earthquake; these are the geographically-correlated failures. The impact on the Internet from regionally-correlated failures is still an open issue. Several works have studied the geometric property of the network under regional challenges [3]. The smallest-enclosing circle problem [4] is used for critical region identification. We design our critical-region identification mechanism using a well-known property of the smallest-enclosing circle problem [5] and employ multiple fiber-level network topologies in different continents to verify the effectiveness of our model. We further employ this model in network simulation and demonstrate its efficiency in terms of bypassing the failure region.

Local graph metrics such as centrality metrics have been used in network vulnerability analysis [6], [7]. We employ centrality metrics to guide the selection among the failed nodes for prioritized protection in the face of regional challenges. We present the performance improvement from the prioritized protection through graph analysis and further verify our graph analysis using network simulations. As far as we know, this is the first work to use centrality metrics in prioritizing the restoration of network services during regional challenges.

In the following sections, we present the background and related work in Section II. We introduce our identification model and disaster mitigation mechanism in Section III. We present our numerical results of the model in Section IV. Section V concludes the paper and suggests future work.

II. Background and related work

Considerable research effort has been devoted to the vulnerability analysis for the fiber-level networks [8], [9], which has led to several vulnerability metrics to evaluate the resilience of network topologies [10]. Survivable fiber-level networks under random link and non-correlated failures has been a popular research domain [11], [12], and a number of link protection mechanisms have been proposed [13], [14]. Identifying critical nodes and links is crucial for analyzing the network resilience to random failures and has shown to be NP-complete [15]. Heuristics have been proposed to solve this problem polynormially [15], [16].

Recently the research community has become more concerned about the potential damage caused by large-scale challenges and intentional attacks; efficient mechanisms have

been proposed to mitigate their impacts [17]–[20]. A vertical line cut segment has been identified [17] and geometric probabilistic techniques have been used [18], [19]. The impact of the regional correlated challenges for overlay networks has been assessed, and a proximity-aware overlay network construction mechanism has been proposed to select overlay neighbors with limited shared underlay [21].

A related notion to the critical node identification in the regionally correlated failure domain is the identification of critical regions. Network vulnerability analysis has been done for multiple probabilistic physical attacks, and an approximation algorithm has been proposed to find the most vulnerable location [8], [22]. Critical region identification models have been proposed for several failure shapes including circular, polygon, and ellipse [23]. However, none of these works considers the impact on the routing protocol performance for regional failures or attacks with a large impact zone, e.g., an earthquake or hurricane that has a challenged radius of up to 500 miles, which can cause failed nodes and links with substantial damage to the normal network communications [24].

III. Critical region identification

We define the network as $G = (V, E)$ with V representing the vertices or nodes, and E representing the edges or links. The network nodes are embedded in an Euclidean space and we assume the network links as straight lines. We refer to the layout of the network as the network geometry. A geometry-based circular region f is defined as the circular area with failure center c and radius r:

$$f = (c, r) \tag{1}$$

We further define d_{c,v_i} as the distance from node v_i to the failure center c. The challenge node set for a given failure is the node set V that qualifies the following condition:

$$V | d_{c,v_i} \leq r \tag{2}$$

In other words, the challenge node set for a given failure region is the set of nodes that can be covered by the failure circle f. Any node within the circle will be disrupted and removed from the connectivity calculation, along with its connected links, of course.

We define the failure impact ratio (FIR) as the ratio of the graph resilience after challenge $\mathbf{R}(G_c)$ according to a specified graph metric divided by the original resilience $\mathbf{R}(G)$.

$$\text{FIR} = \mathbf{R}(G_c)/\mathbf{R}(G) \tag{3}$$

The objective of the identification model is to find the smallest circle that covers the challenged node set; with whose removal can the flow robustness drop below the targeted FIR using that challenge. The evaluating graph metric can be any global measure such as the network efficiency or the giant component size. We use flow robustness (FR) [25], [26] in this work for two reasons; first it matches the packet delivery ratio (PDR) result in network simulations for all node pairs communicating with constant bit rate (CBR) traffic, and second it is effective in terms of evaluating the network connectivity.

A. Flow Robustness

Flow robustness [26] is defined as the ratio between the number of reliable flows and the total number of flows. A flow is considered *reliable* if at least one path remains connected during the failure. The algorithmic complexity depends on the time to find the number of components in a given graph, which makes the complexity as $\mathrm{O}(|V|+|E|)$. The limitation of flow robustness is that it is based on the network connectivity and does not consider traffic. In the network simulation section IV-E, we provide the PDR result using CBR traffic, which is related to the FR metric in the simulation context.

A related metric, all-terminal reliability [27], calculates the probability that a given node pair can communicate with each other for a given period of time. However, FR considers the connectivity of a given node pair at any given instance of time; it is efficient in the scenario of this work since we are concerned with instantaneous connectivity. Furthermore, all-terminal reliability requires a connected graph.

B. Physical topologies dataset

We use datasets from KU-TopView [28], [29] and Internet Topology Zoo [30]. The KU-TopView network topology viewer provides open network graph data representation and visualization. The Internet Topology Zoo is a project to collect network topologies data from around the world and we use its physical-level topologies of Europe and South America.

Analyzing physical-level graphs with link weights provide a more accurate prediction of critical regions. Therefore, we extend our critical region identification model to weighted graph analysis. There is no link traffic information for the commercial carrier networks and we employ a weight assignment method [31], [32] to apply node weights to the topology based on city populations. The population estimate is for the year 2011 taken from the US Census Bureau [33]. If we define the population for each node as POP_{v_i} and POP_{v_j} for link $ij \in E$, with natural logarithm $\ln$ applied on the population, the link weight $w(ij)$ is defined as:

$$w(ij) = \ln_{(\mathrm{POP}_{v_i})} \times \ln_{(\mathrm{POP}_{v_j})} \tag{4}$$

The weighted flow robustness (WFR) is defined as the product of the unweighted flow robustness (FR) times the total weight for all the remaining nodes after a challenge:

$$\text{WFR} = \text{FR} \times \sum w(ij), ij \in E \tag{5}$$

This method considers the total population for each node (city) and it stems from the understanding that city population affects the traffic demand among cities at a certain level. We argue that by assigning weights to the commercial topology, we can analyze the topology in a more realistic way than using the unweighted graph.

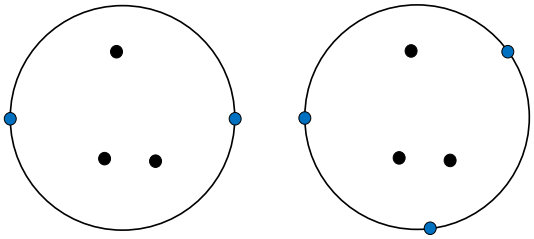


Fig. 1. Smallest-enclosing circle problem

C. Identification model

The smallest-circle problem results in the well-known fact that the minimum-covering circle of a node set can be determined by at most three points and they have to lie on the rim of the circle [5]. The points considered in the smallest-circle problem can be considered as the network nodes and the covering circle the challenge area. As shown in Figure 1, the minimum circle to cover a given node set is either determined by two nodes that form the diameter of the circle, or three nodes on the rim of the circle.

By considering all the circles enclosed by two nodes and three nodes, the model obtains a list of candidate failure regions with their corresponding challenged node set covered (challenged) by the circle (failure region). By calculating the flow robustness of the topology after removing each challenged node set sequentially, we can find the minimum enclosing circle which can drop the flow robustness below a given failure impact ratio (FIR). This is one complement work to our previous work to reduce the computation complexity [20], [34].

The algorithm's complexity can be divided into two parts. The first one is the identification of every possible failed region, which is $O(|V|^3)$. It is the complexity of finding candidate failure circles using three nodes. The second part that calculates the flow robustness after each circular challenge is $O(|V| + |E|)$, as mentioned in the previous section. Since $|E|$ is generally in the same magnitude of $|V|$ for fiber-level networks, the complexity is further reduced to $O(|V|)$. Therefore, the overall complexity of the identification model is $O(|V|^4)$. Since the identification is deterministic for the fiber-level networks, given the slow deployment of new fiber, it can be easily calculated for most of the considered topologies with the number of nodes $|V|$ in the scale of hundreds.

D. Disaster mitigation and network simulation

After the critical region has been challenged, we restore the service of a number of failed nodes for the disaster mitigation analysis[1] to analyze the level of restoration. Flow robustness (FR) is calculated after each added node along with its adjacent links. We further verify the disaster mitigation result in the context of the network simulation using the Level 3 network topology [35]. The critical region identification model guides the disaster mitigation by identifying the critical regions on which to concentrate the mitigation resources. We have selected the critical region for FIR equals 0.6; the detailed example is shown in Section IV-C. By adding three nodes out of a total of failed six back into the network topology, we verify the improved results using our GeoDivRP routing protocol and compare it with OSPF.

The resilient routing protocol GeoDivRP with intermediate WayPoint Shortest Path (iWPSP) heuristic is used in the simulation; the detailed implementation is shown in previous work [20], [34], [36]–[38]. We use single path for routing to match the flow robustness result from the graph analysis.

[1]The protection mechanism can either by shielding or hot-standby nodes

IV. Numerical results

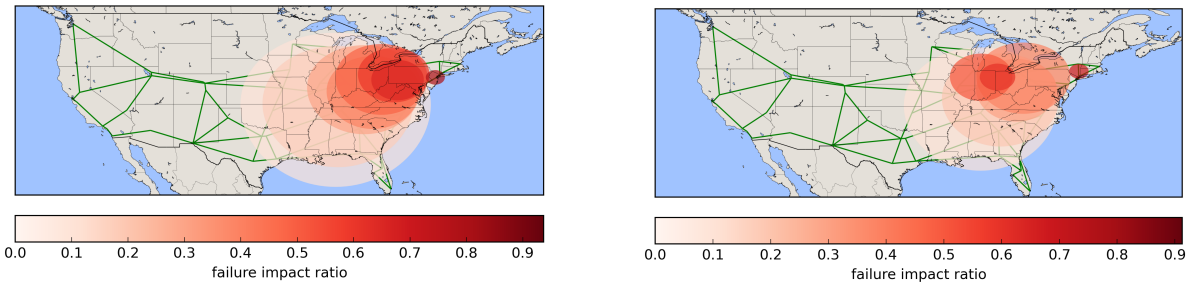
We analyze the fiber-level topologies from different continents. The physical topologies in US include Level 3 [35] and Sprint [39] networks for the US, and the Bestel network [40] for Mexico. For European topologies, we include Oteglobe [41], LambdaNet [42], and NORDUnet [43]. Oteglobe is based in Europe and serves as one intracontinental network.

For the critical distance comparison, we further include US topologies such as AT&T [44], CORONET [45], Internet2 [46], and TeliaSonera [47] networks. SUNET (Swedish University Computer Network) [48] is included as an European research topology.

A. North American topologies

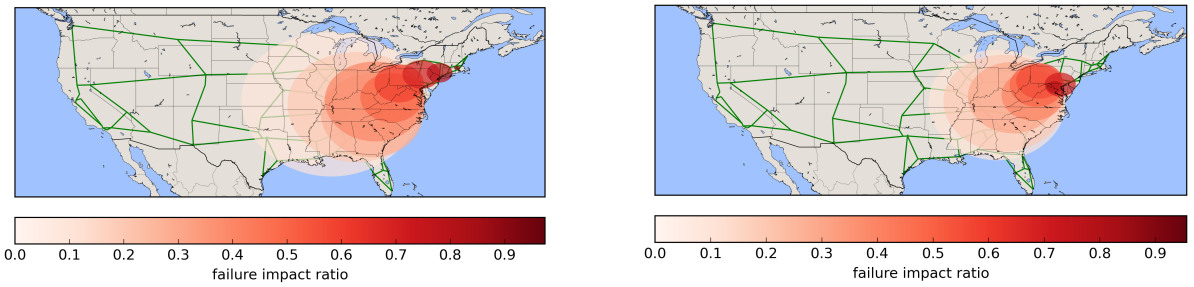
We start by presenting the critical region result for the Level 3 network in Figure 2a. The failure impact ratio (FIR) is shown in different color shades to represent the varying challenge levels. The circles shown are the minimum failure regions to reduce the flow robustness of a given topology below the given FIR. The darker color shade represents a larger FIR, and the better the network performs. All the critical regions are in the northeast corner of the topology. The critical regions for the larger FIR concentrate around New York City and gradually shift in the southwest direction as the FIR becomes smaller. For example, when FIR is 0.9, the critical region centers at New York, NY, and shifts to Butler, PA as FIR becomes 0.6. This is because for the larger FIR (smaller failure region), the most effective location is around New York City as it has a more dense network component concentration; and for the smaller FIR (larger failure region), the failure regions center around Pennsylvania and can efficiently disrupt the connection between the east and the west coast as it is a narrow corridor for the US topology.

However, when we introduce population-based weighted topology, the critical region shifts to more populated regions. As shown in Figure 2b, with a larger FIR, the critical region shifts from the northeast corner of the topology for the unweighted graph to Chicago. For example, the failure region for the unweighted graph centers at Butler, PA when FIR is 0.6, yet it moves toward Van Wert, OH for the weighted. This is because the Chicago node contributes more weight to its adjacent links due to its large population.



(a) Level 3 unweighted network (b) Level 3 weighted network

Fig. 2. Level 3 network critical region analysis



(a) Sprint unweighted network (b) Sprint weighted network

Fig. 3. Sprint network critical region analysis

We further present results for the unweighted Sprint network in Figure 3a. It presents a similar result to Level 3. To achieve the same FIR, the Sprint network has a comparatively smaller circular region due to its more concentrated network components than Level 3.

For the weighted graph as shown in Figure 3b, the degree of shifting towards Chicago for Sprint is smaller than the Level 3 network. This is because the Sprint network has some highly-populated nodes around West Virginia, Virginia, and Kentucky which Level 3 lacks.

We carry out similar analysis for the the Bestel [40] network, one of the largest telecommunication networks in Mexico. As shown in Figure 4, the critical regions for different FIR values are spread out. For the larger FIR, the failure radius is pretty small and it affects only a single node on the edge of the topology. As the FIR decreases, the failure region grows larger and most of the critical regions focus around Mexico City.

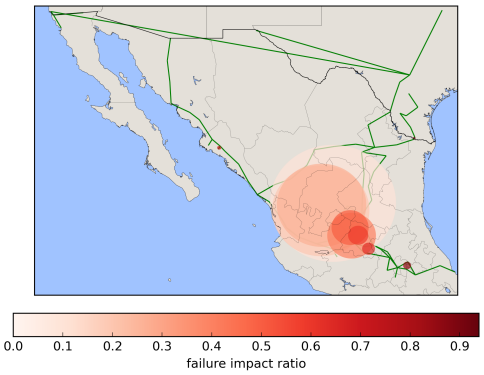


Fig. 4. Bestel network critical region analysis

B. European topologies

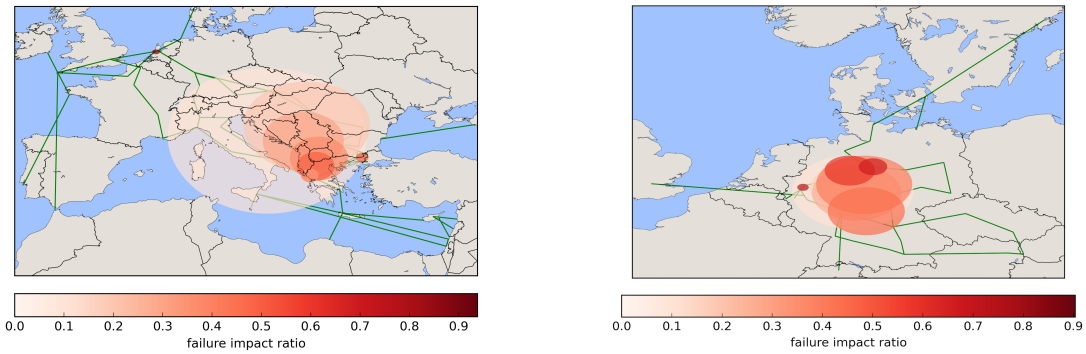
Similar analysis is carried out on European topologies. We begin with Oteglobe [41], an international carrier which is strong in southeast Europe. As shown in Figure 5a, the critical regions focus around Greece as it is the network headquarter with higher degree. The network is more resilient to regional failures due to the fact that the network spans across a wider geographical region and the topology is relatively sparse compared to the US carriers.

LambdaNet is a network topology owned by euNetworks [42] and it lies mostly in Germany. Contrary to other large-scale networks, it is a regional and relatively small-scale network. As shown in Figure 5b, the failure regions focus around the geographical center of Germany.

C. Critical distance comparison

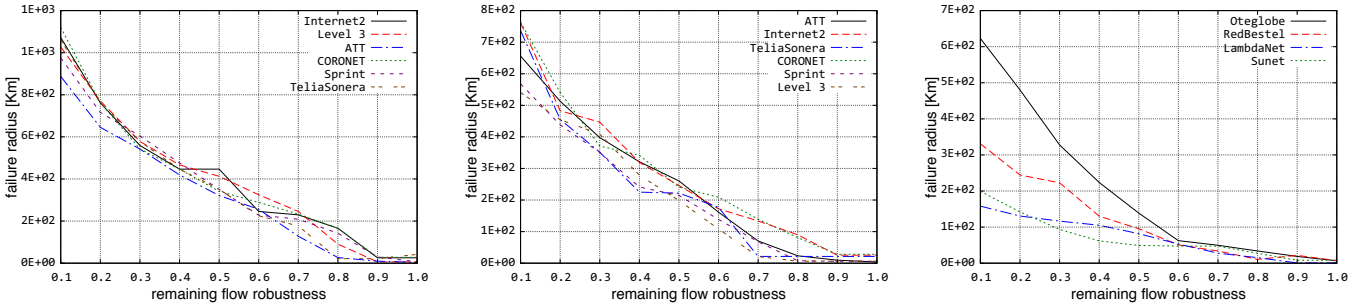
We present the critical failure distance results for the US networks in Figure 6a. We can observe that all the topologies have similar critical distances; this means that to achieve similar damage to the considered US networks, a similar scope of challenge is required. As the FIR increases, the failure radius decreases almost linearly.

The results for the weighted graphs are shown in Figure 6b. Contrary to the unweighted graphs, the weighted ones require smaller failure radii to reduce the network connectivity to a similar level. This is because the most populated nodes are



(a) Oteglobe network critical region analysis (b) LambdaNet network critical region analysis

Fig. 5. European networks critical regions



(a) Challenge distances for unweighted US graph (b) Challenge distances for weighted US graph (c) Challenge distances for different continents

Fig. 6. Flow robustness for different challenge distances

located in the east coast and the critical regions are mostly there already for the unweighted topologies. The same failure region will cause more damage since the nodes and links have greater weights.

Overall, we list the critical failure distances for different continents in Figure 6c. To reduce the FIR to 0.1, the failure radius is 600 km for Oteglobe while 170 km for LambdaNet. This is because the Oteglobe network spans across multiple countries and covers a wider geographical area.

We further include the detailed vulnerable locations for the FIR of 0.6 in Table I. The locations are centered around Virginia and Pennsylvania; this is because if the challenges occurred in these locations, most of the northeast US will be disconnected from the rest of the network. Note that the center of the failure is not necessarily at a particular node in the topology.

D. Disaster mitigation

Based on the critical regions identified, various protection mechanisms can be applied. We carry out disaster mitigation analysis for the FIR equals 0.6 with the result shown in Table I. By restoring failed nodes in the challenged topologies one by one beginning with the highest betweenness centrality, the flow robustness improvement is significant. The reason for adding nodes with higher betweenness centrality is that betweenness defines the number of shortest path passing through a node and can offer better restoration results with traffic considered. As shown in Figure 7, with only two protected nodes, the flow robustness for all the topologies increases from below 50% to around 80%.

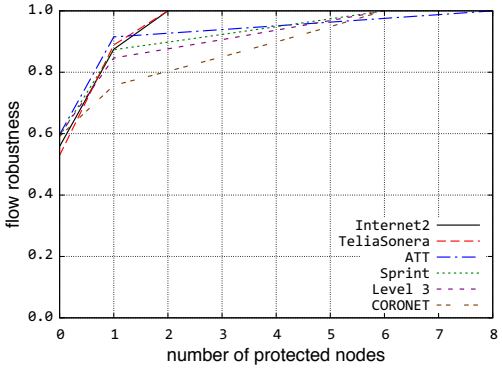


Fig. 7. Flow robustness improvement for unweighted graph

E. Network challenge simulation

We further carry out network simulation to evaluate the mitigation results and demonstrate the performance of GeoDivRP. The ns-3 [49] simulation is carried out with the link bandwidth as 10 Mb/s and the delay as 2 ms. The total simulation time is 100 s. Using the challenged node set identified for the failure impact ratio (FIR) equals 0.6, the first challenge starts from 20 s and lasts for 20 s. The second challenge occurs from 60

TABLE I
PHYSICAL TOPOLOGY VULNERABLE LOCATIONS (FIR=0.6)

Network	Number of Nodes	Number of Links	Flow Robustness	Challenge Centers	Challenge Coordinates	Challenge Radius (Km)	Number of Failed Nodes
AT&T	162	244	0.59	Morgantown, WV	39.67, -79.81	256	8
CORONET	39	63	0.59	West Decatur, PA	40.95, -78.32	289	6
Internet2	16	24	0.56	Stahlstown, PA	40.19, -79.35	246	2
Level 3	63	94	0.59	Butler, PA	40.84, -79.86	325	6
Sprint	77	114	0.59	Rockwood, PA	39.99, -79.27	228	6
TeliaSonera	18	21	0.53	Greensburg, PA	40.26, -79.58	225	2

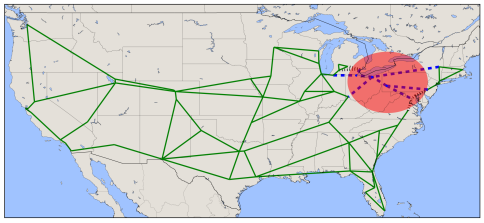


Fig. 8. Challenge location with protected nodes for Level 3 network

to 80 s with the protected nodes. The total protected nodes are three out of the six failed ones, which means three of the highest betweenness nodes are added to the failed topology for the second challenge.

We present the result for the Level 3 network. As shown in Figure 8, the challenge location is for the FIR equals 0.6. Nodes in the range of the circle are disrupted, along with the links connecting to them as shown in black dotted lines. The three protected nodes and its adjacent links are shown in blue dashed lines.

As shown in Figure 9a, for the first unprotected challenge, the PDR drops to around 60%, which closely matches the flow robustness (FR) result. OSPF needs 10 s to converge after the challenge, which is shown as the PDR decreases from 20 to 30 s. On the other hand, it takes only 1 s for GeoDivRP to reconverge and provide paths bypassing the challenge. The second challenge with the protected nodes has a PDR above 90%. For the same reason, it takes OSPF 10 s to converge and the PDR decrease is larger compared to the previous challenge; with the protected nodes, some previously disconnected nodes are connected in the network and OSPF cannot provide shortest path for the newly connected node pairs until reconvergence.

As shown in Figure 9b, the end-to-end delay for OSPF drops during the challenge before reconvergence because OSPF has around 5% to 10% (first and second challenge respectively) more packet drops compared to GeoDivRP and the dropped packets are not counted in the delay result. After the convergence, from 30 to 40 s and 70 to 80 s, there is 1 ms extra delay for GeoDivRP compared to OSPF. This is because GeoDivRP calculates paths with greater path stretch [50] provided by the routing heuristic. However, 1 ms extra delay is justified by the 5% to 10% PDR improvement.

V. CONCLUSION AND FUTURE WORK

We have presented a critical region identification model and applied it to analyze different weighted and unweighted physical network topologies. Furthermore, the network simulation result has confirmed the graph analysis and offered design guidelines for resilient routing protocols in the face of regionally-correlated challenges. For future work, we plan to extend the weighted graph analysis to more topologies and analyze how different recovery mechanisms can improve the network resilience. Furthermore, we plan to study synthetically generated graphs such as Gabriel graphs and analyze how they compare to the real-world topologies.

ACKNOWLEDGMENTS

The authors would like to thank Mohammed Alenazi for the weighted flow robustness discussion and the members of the ResiliNets group for discussions which led to this work. This research was supported in part by NSF grant CNS-1219028 (Resilient Network Design for Massive Failures and Attacks).

REFERENCES

[1] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[2] F. A. Kuipers, "An overview of algorithms for network survivability," *CN*, vol. 2012, pp. 24:24–24:24, Jan. 2012.

[3] H. Saito, "Analysis of geometric disaster evaluation model for physical networks," *Networking, IEEE/ACM Transactions on*, vol. PP, no. 99, pp. 1–1, 2014.

[4] J. J. Sylvester, "A question in the geometry of situation," *Quarterly Journal of Pure and Applied Mathematics*, vol. 1, 1857.

[5] D. J. Elzinga and D. W. Hearn, "The minimum covering sphere problem," *Management science*, vol. 19, no. 1, pp. 96–104, 1972.

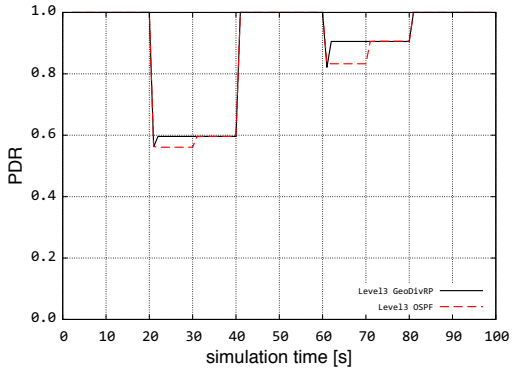
[6] T. Feyessa and M. Bikdash, "Geographically-sensitive network centrality and survivability assessment," in *System Theory (SSST), 2011 IEEE 43rd Southeastern Symposium on*, pp. 18–23, March 2011.

[7] E. K. Çetinkaya, M. J. F. Alenazi, J. P. Rohrer, and J. P. G. Sterbenz, "Topology Connectivity Analysis of Internet Infrastructure Using Graph Spectra," in the 4th IEEE/IFIP RNDM, (St. Petersburg), pp. 752–758, October 2012.

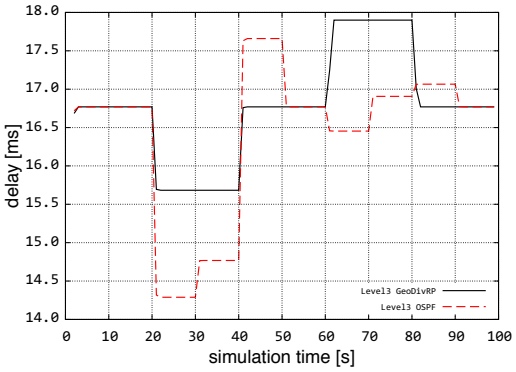
[8] P. K. Agarwal, A. Efrat, S. Ganjugunte, D. Hay, S. Sankararaman, and G. Zussman, "Network Vulnerability to Single, Multiple, and Probabilistic Physical Attacks," in *Military Communications Conference, 2010 - MILCOM 2010*, pp. 1824–1829, 2010.

[9] X. Wang, X. Jiang, A. Pattavina, and S. Lu, "Assessing physical network vulnerability under random line-segment failure model," in *High Performance Switching and Routing (HPSR), 2012 IEEE 13th International Conference on*, pp. 121–126, June 2012.

[10] M. J. F. Alenazi and J. P. G. Sterbenz, "Evaluation and Comparison of Several Graph Robustness Metrics to Improve Network Resilience," in the 7th IEEE/IFIP RNDM, (Munich), October 2015.



(a) Packet delivery ratio for Level 3 network



(b) End-to-end delay for Level 3 network

Fig. 9. Level 3 simulation results with network protection

[11] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, "Resilience of the Internet to Random Breakdowns," *Phys. Rev. Lett.*, vol. 85, pp. 4626–4628, November 2000.

[12] D. Magoni, "Tearing down the Internet," *IEEE J.Sel. A. Commun.*, vol. 21, pp. 949–960, September 2006.

[13] S. S. Lumetta, M. Medard, and Y.-C. Tseng, "Capacity versus robustness: a tradeoff for link restoration in mesh networks," *Lightwave Technology, Journal of*, vol. 18, pp. 1765–1775, Dec 2000.

[14] M. Johnston, H.-W. Lee, and E. Modiano, "A robust optimization approach to backup network design with random failures," in *INFOCOM, 2011 Proceedings IEEE*, pp. 1512–1520, April 2011.

[15] A. Arulselvan, C. W. Commander, L. Elefteriadou, and P. M. Pardalos, "Detecting critical nodes in sparse graphs," *Comput. Oper. Res.*, vol. 36, pp. 2193–2200, July 2009.

[16] T. Dinh, Y. Xuan, M. Thai, P. Pardalos, and T. Znati, "On new approaches of assessing network vulnerability: Hardness and approximation," *Networking, IEEE/ACM Transactions on*, vol. 20, pp. 609–619, April 2012.

[17] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano, "Assessing the Impact of Geographically Correlated Network Failures," in *IEEE MILCOM 2008*, pp. 1–6, 2008.

[18] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano, "Assessing the Vulnerability of the Fiber Infrastructure to Disasters," *IEEE/ACM Transactions on Networking*, vol. 19, no. 6, pp. 1610–1623, 2011.

[19] S. Neumayer and E. Modiano, "Network Reliability With Geographically Correlated Failures," in *Proc. of IEEE INFOCOM*, pp. 1–9, March 2010.

[20] Y. Cheng, J. Li, and J. P. G. Sterbenz, "Path Geo-diversification: Design and Analysis," in the 5th IEEE/IFIP RNDM, (Almaty), September 2013.

[21] K. Kim and N. Venkatasubramanian, "Assessing the impact of geographically correlated failures on overlay-based data dissemination," in *IEEE GLOBECOM 2010*, pp. 1–5, IEEE, 2010.

[22] P. K. Agarwal, A. Efrat, S. K. Ganjugunte, D. Hay, S. Sankararaman, and G. Zussman, "The Resilience of WDM Networks to Probabilistic Geographical Failures," *IEEE/ACM Transactions on Networking*, vol. PP, no. 99, p. 1, 2013.

[23] S. Trajanovski, F. A. Kuipers, A. Ilic, J. Crowcroft, and P. V. Mieghem, "Finding critical regions and region-disjoint paths in a network," *Networking, IEEE/ACM Transactions on*, vol. PP, no. 99, pp. 1–1, 2014.

[24] M. J. F. Denise M. B. Masi, Eric E. Smith, "Understanding and Mitigating Catastrophic Disruption and Attack," *Sigma Journal*, pp. 16–22, September 2010.

[25] J. P. Rohrer and J. P. G. Sterbenz, "Predicting topology survivability using path diversity," in the IEEE/IFIP RNDM, (Budapest), pp. 95–101, October 2011.

[26] J. P. Rohrer, A. Jabbar, and J. P. Sterbenz, "Path Diversification for Future Internet End-to-End Resilience and Survivability," *Springer Telecommunication Systems*, vol. 56, pp. 49–67, May 2014.

[27] C. J. Colbourn and D. D. Harms, "Bounding All-terminal Reliability in Computer Networks," *Networks*, vol. 18, no. 1, pp. 1–12, 1988.

[28] J. P. Rohrer, M. J. F. Alenazi, and J. P. G. Sterbenz, "ResiliNets Topology Map Viewer." http://www.ittc.ku.edu/resilinets/maps/v1, January 2011.

[29] A. Cosner, J. P. Rohrer, M. J. F. Alenazi, and J. P. G. Sterbenz, "ResiliNets Topology Map Viewer Version 2." http://www.ittc.ku.edu/resilinets/maps/v2, January 2015.

[30] S. Knight, H. X. Nguyen, N. Falkner, R. Bowden, and M. Roughan, "The Internet Topology Zoo," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 9, pp. 1765–1775, 2011.

[31] E. K. Cetinkaya, M. J. Alenazi, Y. Cheng, A. M. Peck, and J. P. Sterbenz, "A comparative analysis of geometric graph models for modelling backbone networks," *Optical Switching and Networking*, vol. 14, Part 2, pp. 95 – 106, 2014.

[32] E. K. Çetinkaya, M. J. F. Alenazi, Y. Cheng, A. M. Peck, and J. P. G. Sterbenz, "On the Fitness of Geographic Graph Generators for Modelling Physical Level Topologies," in the 5th IEEE/IFIP RNDM, (Almaty), pp. 38–45, September 2013.

[33] "US Census Bureau Population Estimates." http://www.census.gov/popest/data/cities/totals/2011/files/SUB-EST2011_ALL.csv, 2013.

[34] Y. Cheng, M. T. Gardner, J. Li, R. May, D. Medhi, and J. P. Sterbenz, "Analysing GeoPath Diversity and Improving Routing Performance in Optical Networks," *Computer Networks*, vol. 82, pp. 50–67, May 2015.

[35] "Level 3 Network Map." http://maps.level3.com.

[36] Y. Cheng and J. P. Sterbenz, "Geodiverse routing with path jitter requirement under regional challenges," in the 6th IEEE/IFIP RNDM, pp. 179–186, Nov 2014.

[37] Y. Cheng, M. T. Gardner, J. Li, R. May, D. Medhi, and J. P. Sterbenz, "Optimised Heuristics for a Geodiverse Routing Protocol," in the IEEE 10th DRCN, (Ghent, Belgium), pp. 1–9, April 2014.

[38] Y. Cheng, D. Medhi, and J. P. Sterbenz, "Geodiverse Routing with Path Delay and Skew Requirement under Area-based Challenges," *Networks (Wiley)*, June 2015.

[39] "Sprint." http://www.sprint.com.

[40] "Bestel." http://www.bestel.com.mx/.

[41] "OTEGLOBE Network Map." http://www.oteglobe.gr/.

[42] "euNetworks." http://www.eunetworks.com/.

[43] "NORDUnet: Nordic infrastructure for research & education." http://www.nordu.net/, December 2009.

[44] "AT&T." http://www.att.com.

[45] "The Next Generation Core Optical Networks (CORONET)." http://www.darpa.mil/Our_Work/STO/Programs/Dynamic_Multi-Terabit_Core_Optical_Networks_(CORONET).aspx.

[46] "Internet2." http://www.internet2.edu.

[47] "TeliaSonera." http://www.teliasoneraic.com.

[48] "Swedish University Computer Network Map." http://basun.sunet.se/engelska.html.

[49] "The ns-3 Network Simulator." http://www.nsnam.org, July 2009.

[50] M. Motiwala, M. Elmore, N. Feamster, and S. Vempala, "Path Splicing," in *Proceedings of the ACM SIGCOMM*, (Seattle, WA), pp. 27–38, August 2008.