This paper was presented at RNDM 2013 - 5th International Workshop on Reliable Networks Design and Modeling, co-located with ICUMT 2013 Congress (Sept. 10-12, 2013, Almaty, KZ)

Path Geo-diversification: Design and Analysis

Yufei Cheng*, Junyan Li*, 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
{yfcheng|balee|jpgs}@ittc.ku.edu
†School of Computing and Communications (SCC) and InfoLab21
Lancaster LA1 4WA, UK
jpgs@comp.lancs.ac.uk
www.ittc.ku.edu/resilinets

***Abstract*—The path geo-diversification mechanism introduced in this paper takes geographical diversity of physical network topology into consideration when making routing decisions. It enables the network to be more resilient against area-based challenges by exploiting nodes' multiple ingress and egress ports. It shows better performance compared to OSPF when the network is subject to area-based challenges since the end nodes have access to multiple geographically diverse paths for their communication. We further incorporate geographical diversity into a new graph resilience metric cTGGD (compensated geographical graph diversity). This way we can effectively compare the resilience level of different topologies under regional-based network failures.**

***Keywords*-path geo-diversitiy; resilience; topology; multi-path routing; geodiverse routing; measurement; network resilience; survivability**

I. Introduction and Motivation

Telecommunication networks rely heavily on physical infrastructure to maintain normal operation, for example, optical fibers, amplifiers, routers, and switches. The geolocation of network infrastructure and their relative distance between each other affect the survivability of the network since a significant percentage of challenges affect a wide range of nodes and links. Most of the previous works consider only random link and non-correlated failures [1], [2]. We have modelled correlated failures and attacks in our earlier work [3]. In contrast, we consider events that cause a large number of failures in a geographical region. When a large-scale disaster occurs, such as a hurricane, tsunami, or earthquake, it can affect a region of physical network elements with catastrophic damage. We study the geo-diversity characteristics of the network graph to understand how geographical challenges affect connectivity of the network. Based on our analysis, we have designed a geographic routing protocol to route the traffic around the challenges by exploiting the diversity in the underlying physical topologies.

In this paper we extend the path diversification metric [4] to take into account the *geographic separation* of nodes and links. This is an extension to our previous mechanism in order to represent graph resilience to geographically correlated failures, as opposed to only individual node and link outages. We present this extension with two input parameters: minimum distance between any nodes on alternate paths, and the polygon area between the two paths. We use an objective function to weight the significance of each of these diversity measures. Additionally we compare these measures to commonly used graph metrics to examine their effectiveness as an indicator for regionally-correlated failures.

We present *path geo-diversitification*, a new mechanism (proposed in [5]) that can be used to select single or multiple geographically diverse paths between a given node pair using a quantified geo-diversity measure to achieve high survivability. This mechanism is designed for intra-realm[1] routing within a single service provider, which has geo-coordinate information of their routers. This work is based on our previous work that uses path diversification to improve flow reliability using multiple paths [4]. We then apply this metric in the context of several real-world service provider graphs to analyse the gain in flow reliability and packet delivery ratio when routing protocol is considered.

There has been previous work on understanding the geographic vulnerabilities for certain topologies [6]; based on the vulnerable areas identified, they have proposed optimisation mechanisms to alleviate these impacts [7]. Another vulnerable network zone identification mechanism [8] divides the whole network area into a number of cells, to identify the geographical distribution and size of the vulnerable network zones. However, a mechanism to efficiently route traffic around the vulnerable areas was not proposed, and we argue that it is not realistic to divide the network into equal size cells artificially since this makes the assumption that each cell is contributing equal weight to the total network geographical diversity. This is not the case since some cells have more dense network components compared to others. We propose one effective mechanism to identify the vulnerable locations in the network topology and describe our methodology and analysis in section II-B.

Another previous work assessed the impact of geographically correlated network failures in order to identify vulnerable network locations under regional challenges [9], and assumed

[1] For purpose of this paper AS and service-provider domain are synonymous with our use of *realm*

978-1-4799-1177-6/13/$31.00 ©2013 IEEE

that the link or node is either working or failed under challenges. However, some of the physical attacks are related to the topological distance to the challenge center and are probabilistic in nature. Multiple simultaneous attack cases are not considered.

In this paper, we have applied one similar probabilistic regional attack model [8], [10] when network components near the attack center fail with high probability, while those far from the center linearly decrease in failure probability. This model provides different failing probability parameter settings to reflect different types of network challenges. We propose an effective routing methodology in Section III and it follows the following design guidelines.

A. Design Guidelines

In order to achieve resilience, a routing protocol should be able to exploit both multipath diversity and geographical diversity to the degree that it is present in the physical topologies. A routing protocol that takes geo-diversity into account should consider the following design guidelines:

- **Alternative diverse paths:** When one path fails, an alternative path with appropriate geographical diversity should be used either in real-time via erasure coding or as a hot standby that can be quickly switched in.
- **High node-pair flow robustness:** Each node pair should maintain at least one flow for reliability.
- **System control:** The end systems should be given some level of control over the path, while the intermediate system need not participate in the choices.
- **Less intrusive:** There should not be a negative impact on the current network design.

The remaining sections of the paper are organized as follows: Section II presents the path geo-diversification mechanism, our evaluation methodology and presents our findings. Section III describes the routing protocol design and path selection algorithm we use for multipath routing. Section IV presents the simulation cases we run to analyse our routing protocol. Section V concludes the paper and suggests future work.

II. Path Geo-diversification Overview

Most networked devices have access to multiple partial or complete physical-layer paths between endpoints, and many of these paths have a certain degree of geographical diversity. However, we are currently unable to benefit from them since design decisions in the current Internet protocol stack assume unipath and shortest path routing. This dramatically decreases the ability of the network to provide resilience to either attacks or area-based challenges. We can achieve improved performance and increased resilience with multiple paths.

This paper presents a formal definition of the *Path Geo-diversity* metric, and its aggregate properties when applied to each node pair as well as to complete network graphs. This metric is an extension from our previous link-disjoint and node-disjoint diversity and takes into account *geographical* diversity between different paths. We then explore how our metric would be able to provide connectivity and ensure flow reliability when the network is undergoing regional challenges. We further explore how different degrees of *challenge boundary prediction* accuracy would affect the overall performance of our routing protocol.

A. Alternative Path Mechanism

The primary concern of geo-diversification is to select alternative paths to get around a challenge area when we have some estimated challenge boundaries. For example, consider an ongoing power failure that is spreading to a range of network components, for which can get estimation of the challenge boundary. Based on this information, our protocol can quickly respond to this challenge in terms of routing and path selection. We use these mechanisms for path selection based on link-disjoint diversity and geo-diversity:

- **Path cache:** indexed by source-destination pairs and includes the unique identifiers for each node and link traversed.
- **Path diversity mode:** using different mode of path diversity and the path geo-diversity metric, which consider both minimum distance and area between different paths.
- **Path selection:** according to the higher layer requirement and current network conditions, choose paths that meet these requirements, either one single path or multiple paths.
- **Packet forwarding:** based on the source routes selected from the path cache.

B. Area Scanning Mechanism

Before we explain our area scanning mechanism, we define the flow robustness as follows.

1) Flow Robustness: A flow is established between each node pair using a set of paths determined using the path geo-diversification algorithm and specified diversity threshold. Link and node failures by removal based on fixed probability of failure have been analysed [5]. We now consider regional challenges, where one challenge takes down nodes that have been covered in the area and links that are connected to the challenged nodes. A flow is considered *reliable* if at least one path remains connected during the failure. We compute the *flow robustness* to be the number of the reliable flows divided by the number of total flows that are exist.

2) Scanning Mechanism: This scanning mechanism starts by embedding the topology in the Euclidean plane based on each node's geolocation and operates greedily by scanning through the entire topology for possible vulnerable areas. This model takes two parameters from the user: the radius of the scanning circle and the degree that it forwards each step along longitude scale. The unit for both of the two parameters is degree of diameter in latitude and longitude. The nodes that fall into the circle at any given degree step are defined as the *challenged node set*. Whenever the circle covers one *challenged node set* that has distinct node members compared to the previous circles, we record the node set as one possible area-challenged set. When the *challenged node* *set* is exhausted in the longitude level of the topology, the model forwards along latitude scale for one step and repeats the above process until all the *challenged node sets* are found. By repeating this mechanism for any set of topology, we will be able to identify all the cases that the network might have whenever there is one geographically correlated challenge. This is a very simple yet effective mechanism for scanning through all the possible distinct node sets that can be used to analyse the different challenge locations and then to identify possible vulnerable areas. We are able to run flow-robustness cases to compare the degree of different areas of the network that contribute to overall network resilience. We define the *remaining flow percentage* as the percentage of flow robustness that remains after the different area challenges. Based on the different flow-robustness value for different areas, we plot on the map in different color shades to demonstrate the relative importance of different areas.

After all the distinct areas have been identified, we run our path geo-diversification algorithm on selected *challenged node sets* as follows.

- **Area selection:** We pick areas that have different scale of *remaining flow percentage*.
- **Flow robustness:** We run flow robustness analysis to analyse how much multipath mechanism improves performance.
- **Probabilistic challenges:** We repeat the flow robustness analysis with an inner circle that has node/link failing with probability one while outer circle has failing component with probability 0.5.

C. Path Geo-diversity

We define the geo-diversity as how much two paths are separated from each other in geographical scale. This metric starts from the geographical diversity calculation as follows.

Path is defined as one vector that contains all the links L and intermediate nodes N from source s to destination d

$$P = L \cup N \tag{1}$$

Geographic path diversity between two paths P_a and P_b given previous definitions of P is

$$D_{\mathrm{g}}(P_b, P_a) = \omega d_{\min}^2 + (1-\omega)A \tag{2}$$

where $d_{\min}$ is the minimum distance between any member of the vector P_a and that of P_b, and A is the area of the polygon whose borders are formed by paths P_a and P_b as shown in Figure 1. ω is weighting factor in the range of $[0,1]$ and we use 0.5 for the experiments in this paper.

Based on this metric, we start our effective geographical diversity metric calculation by taking weighted additional diversity from added paths similar to [5].

$$\mathrm{EGPD} = 1 - e^{-\lambda k_{sd}} \tag{3}$$

where k_{sd} is a measure of the added diversity defined as

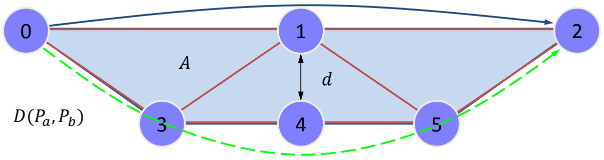

Fig. 1. Geographic diversity: distance d and area A

$$k_{sd} = \sum_{i=1}^{k} D_{\min}(P_i) \tag{4}$$

where $D_{\min}(P_i)$ is the minimum diversity of path i when evaluated agains each member of the previously selected path sets $\{P_1..P_{i-1}\}$, where P_0 is the shortest path. Here $D_{\mathrm{g}}(P_i, P_0)$ is the geographic path diversity between path P_i and P_0 according to Formula 2

$$D_{\min}(P_i) = \min(D_{\mathrm{g}}(P_i, P_0)) \tag{5}$$

λ is an experimentally determined constant that scales the impact of k_{sd} based on the utility of this added diversity. A high value of λ (> 1) indicates lower marginal utility for additional paths, while a low value of λ indicates a higher marginal utility for additional paths. We use $\lambda = 1$ in this paper.

The total graph diversity (TGGD) is simply the average of the EPGD value of all node pairs within that graph. Based on the TGGD value we have, we can calculate the cTGGD value as follows

$$\mathrm{cTGGD} = e^{\mathrm{TGGD}-1} \times \|G\|^{-\rho} \tag{6}$$

Based on the EPGD metric, we get the cTGGD (compensated total geographical graph diversity) value, which is useful as one global graph metric to characterise the graph resilience to area-based challenges. We then verify that our cTGGD metric is accurately demonstrating the effectiveness of one specific topology sustaining area-based failures. $\|G\|$ is the total number of links inside of this topology G, we weight the graph diversity based on the total number of links of one topology to eliminate the penalty to a dense network for a given size of physical region. This is because a dense network will have less geographical diversity for one node pair within a given area as the links are not able to be as separated geographically compared to a sparse network. ρ is experimentally chosen as 0.05.

We calculate TGGD values for different topologies and we compare it with TGD [5] and some other common graph metrics as shown in Table I. We will verify the accuracy of cTGGD by measuring the aggregated flow robustness of the whole graph under area failure in Section II-D.

Our previous path diversity work [5] shows the flow robustness in face of random link failures, but it did not demonstrate the flow robustness in terms of targetted area-based challenges.

TABLE I
NETWORK CHARACTERISTICS

Network	Nodes	Links	Avg. Node Degree	TGD $k = 4$	TGGD $k = 4$	Clustering Coefficient	Diam.	Radius	Hopcount	Closeness	Node Between.	Link Between.
AboveNet	22	80	**7.27**	0.8559	0.9094	**0.6514**	**3**	**2**	**1.72**	**0.5947**	196	**21**
AT&T	108	141	2.61	0.5881	0.8426	0.3274	6	3	3.37	0.3030	4160	943
AT&T Phys.	361	466	2.58	**0.9014**	0.9265	0.0550	37	19	13.57	0.0763	4527	1893
EBONE	28	66	4.71	0.8635	0.9000	0.3124	4	3	2.28	0.4507	132	42
Level 3	53	456	**17.20**	**0.9154**	**0.9379**	**0.7333**	4	**2**	**1.77**	**0.5845**	664	84
Sprint	44	106	4.82	0.8120	0.8855	0.3963	5	3	2.68	0.3853	602	129
Sprint Phys.	263	311	2.37	0.8821	**0.9280**	0.0340	37	19	14.78	0.0700	3609	1637
Telstra	58	60	2.07	0.1295	0.2120	0.2411	6	3	3.30	0.3095	2136	806
Tiscali	51	129	5.06	0.7785	0.8625	0.5068	5	3	2.42	0.4236	656	96
Verio	122	310	5.08	0.8104	0.8858	0.3509	8	4	3.10	0.3335	3736	480
VSNL	7	7	2.00	0.2001	0.4214	0.4167	4	**2**	2.09	0.4982	**18**	**12**

We analyse the flow robustness under these challenges and simulate how the geographic multi-path mechanism improves flow robustness.

D. Evaluation

We evaluate path geo-diversification based on its ability to reflect the connectivity of the underlying graph, and the cost incurred in doing so in terms of path stretch. We are exploiting the path diversity that exists in the physical topology. For this analysis, we have selected the well-connected Level 3 physical and Sprint physical topologies [11], [12].

We combine the area scanning mechanism and flow-robustness calculation to identify geographically vulnerable areas. First we find all the unique *challenged node sets* inside of one topology, then we calculate flow robustness of the remaining network when the nodes in the *challenged node sets* are taken down. This way we can identify the relative contribution of the network components in each area to resilience of the whole network, in another words, we can identify the vulnerability area in the network and offer better optimisation suggestions. We design our evaluation experiments to meet two purposes at the same time. First, we evaluate the area scanning mechanism combined with flow-robustness to identify vulnerable areas. We have used different color scheme in the Sprint and Level 3 physical topology to demonstrate as shown in Figure 2 and 3. The darker shade means that more vulnerable areas. The radius for the area scanning mechanism is five degrees with one degree of step. This is a fairly large range of challenge and we simply use it for easy demonstration. The dark color circles in the Chicago area causes the flow-robustness to drop to 30%, and is the most vulnerable area inside this topology. The slightly lighter color circle along New York area drops the flow-robustness to around 70%, while the even lighter circle along San Diego area only drops it to around 90%. The probabilistic failing case introduced in Section II-B shows similar relative vulnerability levels and is not presented.

Second, we have used this mechanism as verification for path geo-diversification mechanism. Our model first scans the same topology that we would like to verify with a fine-grained radius with one degree increment and records the different *challenged node set*. The mechanism was explained in detail in Section II-B Then we calculate the flow robustness of the network with one unique *challenged node set* taken down each time. After getting the *remaining flow percentage* for taking down each of the *challenged node set*, we calculate the average value for all the them. We define this value as *aggregated remaining flow* for a certain topology and the value is within the range of $[0, 1)$. It is a natural indicator for graph resilience to area-based challenges, yet very computationally complex since the number of different *challenged node sets* is $\mathrm{O}(nm)$, with n as degree at longitude scale and m at latitude scale. However, we have compared *aggregated remaining flow* with the cTGGD value for all the topologies and find an exact match between the two metrics. This way we have verified that cTGGD we proposed effectively indicates the resilience level of different topologies under regional-based challenges while at the same time exponentially decreases the calculation time compared to *aggregated remaining flow*.

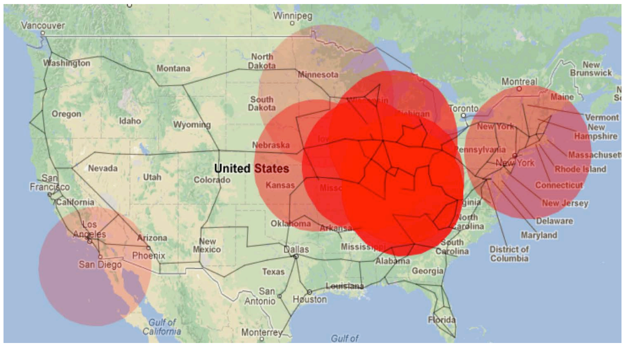

Fig. 2. Sprint network with different vulnerable areas

III. ROUTING AROUND CHALLENGED AREAS

Traditional routing protocols are designed to create one shortest path for each destination in the current Internet architecture. However, this comes with cost of not having the option to choose alternate paths when the current path is unavailable due to challenges or failures. Fast IP reroute [13] is designed to protect the network from the event of a single failure, yet it lacks protection capacity for multiple simultaneous failure events. With a realistic regional-based challenge model, in order to quickly route around the challenged area, we need to

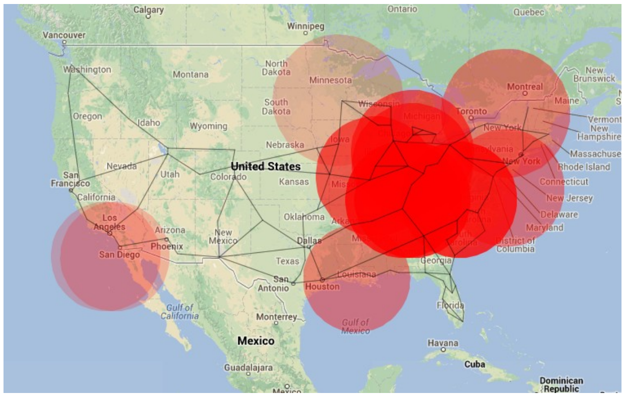

Fig. 3. Level-3 network with different vulnerable areas

find multiple backup paths for every node pair in the network. In order to reduce the overhead of calculating all the paths possible, while at the same time making sure we do not lose survivability to area-based challenges, we need to choose paths from the geographically diverse path sets.

Some may argue that geographical vulnerability should be fixed at network planning phase instead of at routing phase, however, it is not always the case for the following reasons. First, network planning with over-provisioning is a long term process, we still have to design our routing protocol to cope with regional challenges based on current network layout. Second, although sophisticated network planning mechanisms can help reduce the impact to network traffic during area-based challenges, resilient routing is still needed to get around challenged areas quickly and be adaptive to traffic and congestion in the network.

OSPF (Open Shortest Path First) [14] is a link-state interior gateway routing protocol that is a widely used in a single autonomous system. It has become (along with IS-IS) the de facto interior gateway routing protocol. In OSPF, the Dijkstra algorithm is used to calculate the shortest path between a pair of nodes based on link-state information. Every node generates LSA (link state advertisements) that carry the cost of all its links, and floods to the network. To ensure liveness, each node sends HELLO packets to their neighbors over hello interval, which is set as ten seconds by default. If one node does not receive its neighbors' HELLO packets after a hello interval, its adjacency no longer exists and will recalculate the shortest path. This means that if a challenge occurs, the network needs at least a hello interval to detect the challenge and to react in response.

We calculate multiple paths based on the geographic path diversity described in Section II for each node pair in the network. Once we have the multiple paths for each node pair, the question lies in how to choose the paths in different circumstances. In the face of challenges, we consider both challenges with exact information and only estimation. We dedicate one field in the routing header for link failure detection. The *ack request* field is set whenever the packet gets near to the estimated challenge region and enabled for the fast failure detection mechanism. The OSPF protocol usually takes 30-40 seconds to detect the failed area. We use cross-layer information to detect the link failure [15], [16]. We start data transmission using the shortest path. When we detect packet drops that indicate link failure or node failure along the path, we use our path selection algorithm to find the next alternative path. We compare our geo-routing protocol with standard OSPF in terms of both packet delivery ratio and delay. First, we will introduce our path selection algorithm as follows.

A. Single Path Selection Algorithm

We propose the following path selection algorithm to balance the path diversity and stretch given different scales of challenge boundary information. This mechanism will adapt in face of different challenges and is shown as following steps:

Step 1. *Let $\mathcal{P}_a$ be the set of available paths between a given (source, destination) pair, in decreasing order by geo-diversity value, where the number of paths $\mathcal{P}_a$*

Step 2. *If the accurate challenge boundary is known, we use our diversity calculation to route the traffic around the challenge areas, and at this point, the protocol terminates if the path succeeds. If not, it jumps to step 6.*

Step 3. *If the estimated challenge boundary is known, once the traffic gets near those areas, we set the* ack request *field in the routing header to be* true *for fast link failure detection. Then the protocol chooses the nearest geographically diverse path with least path stretch compared to the shortest path.*

Step 4. *If only the existence of challenge is known with no estimation of its boundary, the* ack request *is set to* true *for all the packets sent out for next-hop acknowledgment. This way our protocol can detect challenges in the order of milliseconds*

Step 5. *Once we find that a path is not responding, we switch to the next path with the closest path diversity. This step will be repeated for* pathRetries *times. Once it has been exhausted, we try the largest geo-diversity path in the path cache.*

Step 6. *If all the trials fail, we switch to default OSPF convergence. We can also start the OSPF convergence from the second trial. This way we are able to fall-back to OSPF quickly when all the alternative paths have failed.*

We design this protocol to work under different conditions including both wired and wireless scenarios, with its header inserted between transport and network layer as shown in Figure 4. ResTP [17] is a resilient transport protocol that supports multipath end-to-end transport with application-specific resilience. Our geographical routing protocol takes requirements from ResTP, for example, by providing multiple paths with requested dependability specification. We design our model to calculate one or multiple diverse paths while the challenge simulation is running. For example, when the shortest path stops working due to challenges, we can quickly calculate the diverse path or paths that meets the requirement

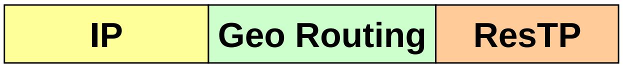

Fig. 4. Geographic routing header encapsulated in the IP header field

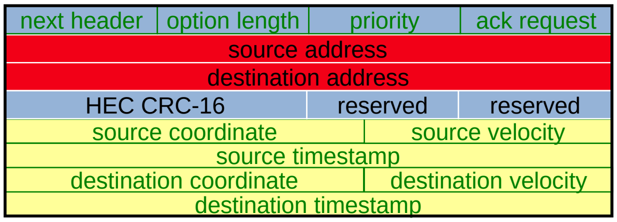

Fig. 5. Geographic routing protocol header

from upper layers. This path can be the next diverse path compared to the shortest path, the largest link-disjoint path, or the largest geo-diverse path depending on the selected mode. This model can also calculate multiple paths with given requirement.

Our geographical routing header is shown in Figure 5. The meaning for each of the fields is shown as follows and some of the fields share similar design with the AeroRP header [18]:

- next header: 8-bit selector, contains the transport layer protocol id
- option length: indicates the length of the following option fields for geo-routing protocol
- priority: packets are able to be differentiated if required
- source node address: 32 bits
- destination node address: 32 bits
- CRC-16: used for header integrity
- source node coordinate: 19 bits
- destination node coordinate: 19 bits
- source node velocity: 13 bits
- destination velocity: 13 bits velocity for the destination node, used when the nodes are mobile
- source timestamp: 32 bits, used to keep track of neighboring node information
- destination timestamp: 32 bits, used to keep track of the neighboring node information for the destination node
- ack request: 8-bit, used to notify the receiver whether to send link-layer acknowledgment

We have implemented two modes for diverse path usage: The first is to select geographically diverse paths on top of the link-disjoint path. For this mode, all the alternative geo-diverse paths we select are also link-disjoint. The second mode is to select geo-diverse paths from the *braided* paths [19]. With the concept of braided paths, there are typically no completely node/link disjoint paths but many partially disjoint alternate paths. This way we relax the restriction of disjoint paths but have more alternative path choices in the case of a sparsely connected network. Therefore, for a densely connected network, we use the mode with link-disjoint path, while for the sparsely connected one, we select our paths based on braided paths. In the meantime, we keep sending HELLO packets from the OSPF protocol. When we discover that the area has recovered from the failure, we begin using the nodes and links that have been previously assumed as failed for transferring packets.

When the transport protocol or application has requested multiple paths, instead of using just one diverse path, we use the number of paths requested by the upper layers. Whenever we have multiple paths, we can either use erasure coding or other mechanism for spreading information across multiple paths [5]. This is desirable, for example, for a real-time service that cannot tolerate the delay of ARQ (automatic repeat request) retransmissions when a path has failed and switched to hot standby. However, this multi-path spreading is beyond the scope of this paper.

IV. Simulation and Experimentation

We use ns-3 [20] as the simulation software to model our geographical routing protocol. For the wired case, we have extended the existing Global Routing ns-3 model by calculating multiple geographical diverse paths to be able to route around the challenged area with a link-layer acknowledgment mechanism. The same mechanism is applicable in wireless mesh networks without nodes mobility. Our protocol is also designed to consider mobility in MANETs (mobile ad hoc networks) using the position and velocity header fields; this simulation and analysis is planned for future work.

A simple example to illustrate path selection with estimated challenge boundaries is shown in Figure 6 as a 4×4 grid mesh topology in which the top-right node sends packets to the bottom-left node with a data rate equal to one packet per second. The CBR (constant-bit rate) traffic selects the shortest path at the beginning, which is shown in Figure 6 (a). At 2.0 s, a challenge comes into the network. Three nodes are influenced by the challenge and the CBR traffic is terminated, as shown in Figure 6 (b). In Figure 6 (c), the traffic tries to use the path with smallest path stretch in all the alternative paths, but this also fails. After *pathRetries*, if the traffic is still blocked, the packet will try the most geo-diverse path. In this simulation, the geo-diversity path works well, as shown in Figure 6 (d). The acknowledgment mechanism is turned on from the beginning, and the failure detection occurs within milliseconds.

We now present simulations using the real world physical topologies including Sprint and Level 3. We only carry out the simulation once for each topology since there is no randomness in the wired network simulation topology. We use CBR traffic sending from each node to all the others with a data rate equal to one packet per second. We choose our challenge duration time as 20 seconds. We start our simulation with one challenge at a time with perfect information of the challenge boundary and one with estimated information. The locations we choose for different challenges come from the flow robustness analysis. We choose the most vulnerable location and the least one. In this paper, we show the results of Sprint L3 network with the given challenged areas and the results for other networks will be included in future work.

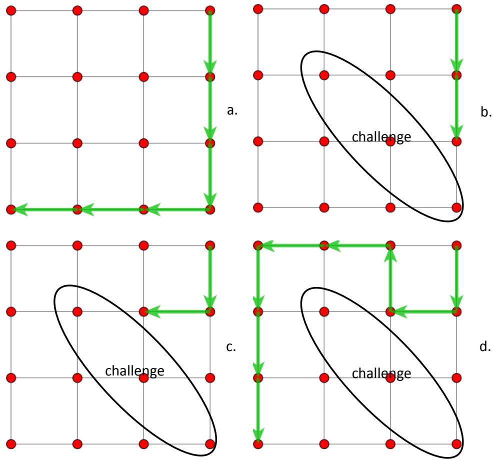

Fig. 6. Geographic routing protocol 4 by 4 grid topology

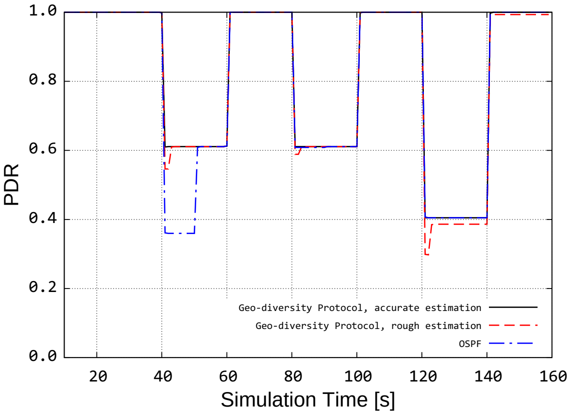

Fig. 7. Sprint packet delivery ratio under area-based challenge

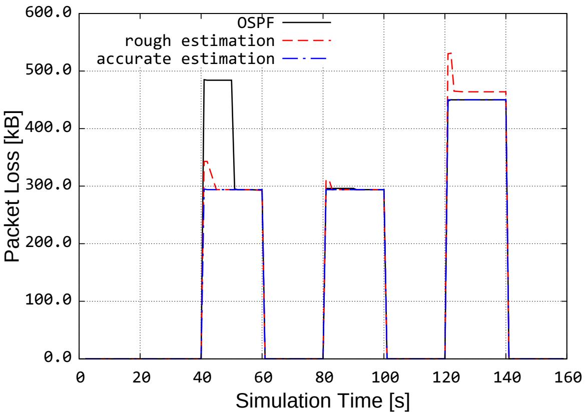

Fig. 8. Sprint packet loss under area-based challenges

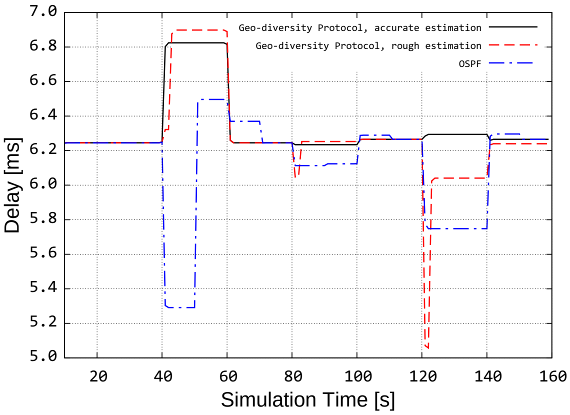

Fig. 9. Sprint network delay under area-based challenges

We compare our results with standard OSPF in terms of PDR (packet delivery ratio) as well as delay.

The PDR for the Sprint network is shown in Figure 7. There are three area-based challenges we have simulated. From 40 to 60 seconds, the challenge occurs around Kansas City, from 80 to 100 seconds in New York City area, while the last challenge occurs at Los Angeles from 120 to 140 seconds. The radius of the challenge areas are all five degrees. We compare the performance of our geographical routing protocol when having exact information of challenge area, estimated information, and standard OSPF. Consider the first challenge in this figure, when the challenge occurs at 40 seconds, the PDR for OSPF drops to below 40% and it takes 10 seconds to converge. In contrast, for the geographical routing protocol with exact challenge boundary information, normal operation is almost instantly restored as shown not excess 300 kB loss at 40 s. For the case that we only have estimated information, it takes about one second to restore normal operation, also a significant improvement over OSPF. We notice that when the challenge is at Los Angeles area, the PDR did not reach exactly 40% at 121 s, we analysed the trace and did not find any additional packet drop around these areas. We believe that it is one simulator inaccuracy in generating packets. We also include the average packet loss for different mechanisms in Figure 8.

The delay analysis is shown in Figure 9. We consider the first case when the challenge happens in the Kansas City area. The reason that OSPF shows lower delay compared to geo-routing is because most of the data packets during the challenge have been dropped and the lost packets are not counted as delay; this is why there is a delay drop for OSPF from 40 to 50 seconds. Around the same time, the estimated case has shown slightly higher delay compared to that with accurate information. This is because that the estimated case is using a more geographically diverse paths which increases the path stretch a bit longer. However, we notice that the difference is only 0.1 second, which is very small in network routing time.

V. Conclusion and Future Work

We have proposed the path geo-diversification mechanism and one global graph resilience metric cTGGD to characterise the geographical diversity for different topologies. We have verified its effectiveness in representing the geographical path diversity of a given topology. We have proposed a network vulnerablility area identification method and verified its effectiveness in identifying vulnerable areas in different topologies. We have also implemented a routing protocol that is able to calculate and choose different geographically diverse paths to meet the requirements from higher layers. We demonstrated its efficiency in routing around the failure area and its improvement in both packet delivery ratio and delay compared to OSPF.

For future work, we will extend the diversity metric to wireless networks. Load balancing is another problem to examine. Whenever we are routing network traffic using alternative paths to get around the challenged areas, we are essentially overloading other links in the network. We will examine different load balancing mechanisms to achieve the best results. We plan to carry out experimentation in a testbed and compare its results with that from the simulation. Another major diversity measure can consider heterogeneous network components, including wired and wireless links, and will be included in future work. We will examine mechanisms to incorporate our geodiverse routing protocol into the current Internet.

Acknowledgment

The authors would like to thank 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] 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.

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

[3] E. K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J. P. G. Sterbenz, "Modelling Communication Network Challenges for Future Internet Resilience, Survivability, and Disruption Tolerance: A Simulation-Based Approach," *Telecommunication Systems*, vol. 52, no. 2, pp. 751–766, 2013.

[4] J. P. Rohrer, A. Jabbar, and J. P. G. Sterbenz, "Path diversification: A multipath resilience mechanism," in *Proceedings of the IEEE 7th International Workshop on the Design of Reliable Communication Networks (DRCN)*, (Washington, DC), pp. 343–351, October 2009.

[5] J. P. Rohrer, A. Jabbar, and J. P. Sterbenz, "Path Diversification for Future Internet End-to-End Resilience and Survivability," *Springer Telecommunication Systems*, 2012.

[6] M. Gardner and C. Beard, "Evaluating Geographic Vulnerabilities in Networks," in *IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*, pp. 1–6, May 2011.

[7] M. Gardner, C. Beard, and D. Medhi, "Avoiding High Impacts of Geospatial Events in Mission Critical and Emergency Networks using Linear and Swarm Optimization," in *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2012 IEEE International Multi-Disciplinary Conference on*, pp. 264–271, March 2012.

[8] J. Liu, X. Jiang, H. Nishiyama, and N. Kato, "Reliability Assessment for Wireless Mesh Networks Under Probabilistic Region Failure Model," *Vehicular Technology, IEEE Transactions on*, vol. 60, pp. 2253–2264, June 2011.

[9] 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.

[10] H.-W. Lee, E. Modiano, and K. Lee, "Diverse routing in networks with probabilistic failures," *IEEE/ACM Transactions on Networking*, vol. 18, pp. 1895–1907, December 2010.

[11] 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 *Proceedings of the 5th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, (Almaty), September 2013.

[12] "ResiliNets Topology Map Viewer." http://www.ittc.ku.edu/resilinets/maps/, January 2011.

[13] A. Atlas and A. Zinin, "Basic Specification for IP Fast Reroute: Loop-Free Alternates." RFC 5286 (Proposed Standard), Sept. 2008.

[14] J. Moy, "OSPF specification." RFC 1131 (Proposed Standard), Oct. 1989. Obsoleted by RFC 1247.

[15] A. Jabbar, J. P. Rohrer, A. Oberthaler, E. K. Çetinkaya, V. Frost, and J. P. G. Sterbenz, "Performance comparison of weather disruption-tolerant cross-layer routing algorithms," in *Proceedings of the 28th IEEE Conference on Computer Communications (INFOCOM)*, (Rio de Janeiro), pp. 1143–1151, April 2009.

[16] A. Jabbar, B. Raman, V. S. Frost, and J. P. G. Sterbenz, "Weather disruption-tolerant self-optimising millimeter mesh networks," in *Proceedings of IWSOS: Third International IFIP/IEEE Workshop on Self-Organizing Systems*, vol. 5343 of *Lecture Notes in Computer Science*, pp. 242–255, Springer, 2008.

[17] J. P. Rohrer, R. Naidu, and J. P. G. Sterbenz, "Multipath at the transport layer: An end-to-end resilience mechanism," in *Proceedings of the IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, (St. Petersburg, Russia), pp. 1–7, October 2009.

[18] J. P. Rohrer, E. K. Çetinkaya, H. Narra, D. Broyles, K. Peters, and J. P. G. Sterbenz, "AeroRP Performance in Highly-Dynamic Airborne Networks using 3D Gauss-Markov Mobility Model," in *Proceedings of the IEEE Military Communications Conference (MILCOM)*, (Baltimore, MD), pp. 834–841, November 2011.

[19] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 5, no. 4, pp. 11–25, 2001.

[20] "The ns-3 network simulator." http://www.nsnam.org, July 2009.