Benefits of Multi-Topology Routing during Geographically Correlated Failures

M. Todd Gardner\(^a\), Rebecca May\(^a\), Cory Beard\(^a\), Deep Medhi\(^{a,b,*}\)

\(^a\)University of Missouri–Kansas City, Kansas City, MO, USA
\(^b\)Indian Institute of Technology–Guwahati, India

Abstract

During large geographic events in networks, the routing churn that occurs has been shown to cause significant impacts in routing stabilization following the event. This work is an extension of earlier work that proposed a set of algorithms that is based on Multi-Topology Routing (MTR) for pre-planning for geographically correlated failures. Thus, in the event of a failure, our approach, Geographic MTR, switches to virtual topologies that reduce the impact of routing changes that can result in dropped connections until new link state and shortest path trees can be established.

Two algorithms are used to generate virtual topologies, Geographic Coverage MTR (gcMTR) and Geographic Targeted MTR (gtMTR). The first method, gcMTR, is to create virtual topologies taking a network wide coverage approach. In addition to the circular coverage approach presented earlier, we offer a hexagonal approach that provides significantly better coverage. gtMTR is a targeted approach that can be used in anticipation of a specific event where knowledge of that event exists. The third algorithm described in this work specifies a way to detect a geographic event and select a topology to use. We also explore other methods of detecting and predicting geographic events for the purpose of topology selection, recognizing that additional information like weather forecasts or political events may lead to future geographic events.

We evaluated our approach on two network topologies and observed that the number of connections that are dropped during a geographic event can be reduced significantly, thereby reducing the impact to the non-affected part of the network. Analysis of topology size versus disaster size, topology location versus disaster location, and general density of the topology is performed. Finally, a simulation model of a large network is used to study the effects of geographically correlated failures both with gcMTR and using default topologies. This provides a way to assess the gains of using MTR to mitigate the impacts of large scale geographic impacts.

Keywords: Future Internet, Internet Trustworthiness, Architecture, Prototype, Geo-Distributed Networks, Network Virtualization

1. Introduction

Large scale geographical events such as natural disasters, major weather events, and geo-political events can significantly disrupt network services. Thus, efforts to reduce or minimize disruptions is desirable since such events are also when disaster response data is needed and when users want to inform their friends and families about their whereabouts. Therefore, it is imperative to create robust network functionalities.

From a network perspective, when geographically-correlated events occur, several problems surface. These range from slow convergence of the routing protocols due to congestion due to overloaded links caused from rerouting traffic affected by the event. Furthermore, such events cause stability issues during the transient period. An important issue is how basic link-state interior gateway protocols (IGP) such OSPF and IS-IS that are commonly deployed in large networks are affected and what can be done to increase throughput during a major event. In [5] and [1], the authors explore the tradeoff between routing stability and convergence speed in link state protocols. Disruptive outages in networks tend to cause multiple link state advertisements (LSA) to be flooded across the routing area and the routers to perform multiple shortest path calculations and therefore have long convergence times. Flapping can occur if link information is propagated through the network too quickly. To prevent flapping, hold down timers are used which slows convergence times [5]. This highlights the tradeoff between convergence speed and routing stability. In addition, major disruptions can cause large numbers of traffic flows to be interrupted or rerouted to other links causing congestion [1].

Another concern during geographical events is that the failures may not occur at one instance. The outages may cascade, moving through the geographic area with the event or subsequent outages are caused as a side effect of the initial outage, like congestion. In [24], Sterbenz, et. al. discusses several examples of major events where cascading outages were an issue. Earthquakes can have aftershocks that cause cascading outages. Floods can cause cascading outages as floodwaters penetrate different geographic areas. Even political situations can escalate and spread across a geographic region. Frequently, routing protocols will attempt to reroute with little knowledge that the paths that are selected are also vulnerable [24] or that the paths...
go around the edges of the disaster area.

In this work, we propose to use a preemptive reconfiguration approach through Multi-Topology Routing (MTR) [18, 17] to improve network performance during a major geographically correlated event. Basic OSPF and IS-IS protocols have been now extended with MTR functionality. Thus, our MTR-based approach is intended to improve network throughput compared to basic link-state protocols in order to isolate parts of the network affected by a geographic event. Using our mechanism, the network is less disruptive to existing traffic and the routing convergence time delay due to the basic link-state protocol can be avoided. More specifically, we use Multi-Topology Routing (MTR) to protect against the problems associated with geographically correlated failures. Briefly, in the MTR framework, we create a series of topologies that can be useful to mitigate potentially disruptive events in the network.

The general effect is that once the geographic event is detected, rapidly move the trunk of the shortest path tree (SPT) away from the affected area in that topology. This isolates a region from the rest of the network and limits the impact that disruption in that part of the network can have on the whole network. To understand why MTR is needed for geographic failures in networks, an understanding of what happens during link or node failures in link-state routing protocols is necessary. First, detection of a link or node state change (like an outage) occurs. Next, routers affected by the change will create LSA’s and send them to their neighbors. This information will be flooded across the routing area till all routers have the same link state database. If database changes occurred, each router independently calculates the shortest path tree to all nodes based on the new database.

If multiple outages occur, like a geographic event, several things can happen that negatively impact the above restoration process. First, where multiple links are involved, links may exhibit repeated and intermittent failures causing link flapping behavior [1]. This behavior typically causes frequent routing changes and that leads to routing instability. If the outages are significant, multiple LSAs will be flooded across the network causing shortest path first (SPF) calculations to run repeatedly at each node. This is commonly referred to as SPF Throttling and can lead to longer convergence times. A significant impact of route instability is that traffic paths may also become unstable and impacted severely [1]. Long RouterDeadInterval intervals impact convergence times during major outages.

In this work, we show using simulation that the RouterDeadInterval directly impacts the time required to re-establish traffic across a network during a large geographic failure. Given that the reduction of this timer setting increases routing instability, a method to switch to a stable routing tree quickly is desirable to avoid significant traffic disruption during these events. We show that this can be achieved using MTR.

Several schemes to improve convergence times and/or improve route stability have been proposed through the years. Modification of OSPF (or IS-IS) timers is the primary way proposed to prevent link or route flapping behavior. Hello timers and Router Dead Interval timers can be extended to dampen flapping behavior. In addition, the interval between successive SPF calculations (SPF hold down timer) can be adjusted to prevent repeated SPF calculations. Clearly, increasing these timers will delay convergence times. These methods are discussed in detail in a number of works including [1] [5] [4].

Improving outage detection times have also been proposed to improve stability and convergence times [5]. This is the most productive if hardware means of detecting outages can be used instead of strictly relying on reducing the Hello timer. False alarms can also cause link flapping and other instability. Additional information may also be available that could improve geographic outage detection times, like weather information or political events.

Incremental SPF (iSPF) has been proposed as a way to reduce SPF processing at the routers [12]. The idea behind iSPF is to incrementally change the shortest path tree when link or node changes occur near the leaves of the tree. Performance improvements due to iSPF are discussed in both [1] [5]. The algorithms we propose take advantage of iSPF efficiencies.

In [11], one of the interesting observations of the impact of Hurricane Sandy is that the major internet providers moved the majority of the traffic away from New York City during the event. The goal was not to eliminate internet access for the New York City area, but to reduce the possible impact the hurricane was having on traffic that was passing through the New York City area. We propose to use MTR to quickly move traffic from a vulnerable geographic region.

There have been several concepts to modify routing to accommodate disaster planning. In [8], Hanson et al. proposed a method of using routing layers to isolate areas of a network. The idea is similar to our work, except that they do not propose using Multi-Topology Routing to accomplish it. Instead they utilize the ability to segment networks into areas using protocols (like OSPF) that can have multiple areas. Their methods require that routing area be pre-configured for possible geographic events. We felt this was not flexible enough for robust disaster planning. In the next section, we see the same authors went on to propose using MTR to re-route around individual nodes or links. In [13], the authors use a novel hill-climbing algorithm to assign link weights such that the link utilization is maintained at a level so that in the event of a disaster re-routing does not overload links causing congestion. While this is useful for network provisioning, it does not necessarily prevent the routing churn caused by large geographic events.

Several local IP fast re-routing methods have been proposed that are summarized in [22]. In general, the router that detects the outage reroutes locally. There are also methods where the packet carries information about the network elements that are to be avoided. These include the not-via methods as described in [20] and others like Localized On-Demand Link State Routing in [19]. These methods are good for a small number of link or node failures, but the mechanisms in these methods either do not support large numbers of correlated node/link failures or the methods do not scale well enough to support large scale outages.

In our MTR-based approach, we create multiple alternate topologies starting from the default topology where link
weights are pre-determined in such a way that in the event of a geographic failure, the routing paths created moves away from a vulnerable geographic region. In particular, we propose a method to compute the link weights so that the path selection attempts to avoid an affected region. While the MTR-based approach has been used for network resilience [3, 2, 9], our approach considers a geographic vulnerability as the driver for how to determine weights that can be used in MTR. This paper extends our earlier conference paper [6] in a number of ways: 1) we present two different ways to generate alternate topologies, one based on circular coverage and the other based on hexagonal coverage, 2) we include additional analysis on assessing improvements based on our approach, 3) we also include simulation results using the OPNET [15] simulation tool to show gain during a transient period.

The rest of the paper is organized as follows. We start with an overview of MTR in Section 2. We then present the two algorithms, geMTR and gtMTR, for our geographic MTR approach in Section 3. An illustrative example using a 5 × 5 grid topology is presented in Section 4. Two real-world topologies, one moderate-size and the other large, were analyzed in Section 5, followed by OPNET-based simulation studies Section 6. A concluding discussion is presented in Section 7.

2. Multi-Topology Routing: An Overview

Multi-topology Routing (MTR) was originally proposed to enhance traffic engineering in link state protocols like OSPF [18]. The concept was to allow different classes of traffic to use different topologies to cross the network. Traffic that requires higher Quality of Service could use a lower latency path than other traffic. It was soon discovered that MTR could be used for other purposes, like fault tolerant routing.

MTR utilizes the link weights used during shortest path calculation to create a virtual topology, setting link weights for links that will not participate in a particular topology very high compared with other links. In OSPF, the distribution of this additional link weight information is accomplished using the LSA. The Type of Service (TOS) field in the LSA is redefined as the MT-ID field. This provides link weight information for each topology to all of the routers in the network. A default (non-modified weighting) topology is required to be maintained.

In the IP packets to be routed, the Differentiated Services Code Point (DSCP) field is used to note which topology is to be used for that packet. The router can look up the topology ID for that packet, check the shortest path tree (SPT) for that topology, and forward the packet based on that SPT.

MTR can also be used for fault tolerance routing. Concepts for implementing MTR for fault tolerance have been described by several authors including Menth and Martin [14], Cicic [2], and Scheffel, et al. [21], and Kvalbein, Hanson, et al. [10]. Alternative topologies are used in these works primarily to protect against single link or node failure. In [2], Cicic defines a legal topology with the following three criteria. All restricted links are attached to an isolated node and non-isolated node. The links between two isolated nodes are isolated. And the non-isolated nodes have no isolated links. Using an algorithm to create the topologies from this criteria, they are able to minimize the number of topologies.

Scheffel, et al. [21] took an optimization approach to creating topologies. They created a binary integer linear program (BILP) to create topologies that had the goal of being able to mitigate single link failures with a given number of topologies. The objective was to minimize path distance.

In both works, once a link outage occurs the detecting node is responsible for finding a topology where the failed link is isolated. The packet can then be rerouted around the failed node or link. We refer to this as local rerouting based on MTR.

3. The Geographic Multi-Topology Routing Approach

With the goal of reducing the impact that a geographic event can have on a network, our approach is different than these approaches (and any other approaches we have seen). The topologies created here are intended to avoid routing (other than local routing) in a specific geographic area. The topology creation algorithm increases link weights around a specific geographic location with a specific radius. This has the affect of pushing the SPT away from the vulnerable area and only allowing leaves of the SPT to exist in the vulnerable area. The weighting algorithm decreases linearly from 100 at the avoided location till the radius boundary and then the weights are set to 1. Other weighting algorithms have been tested (such as exponential decrease). Linear weighting with a boundary at the radius seems to perform well. The advantage of using high (but not infinite) weights is that the SPT will try to avoid the vulnerable area using it only if no other route is available. Multiple topologies are then created with different geographic locations.

Once topologies are created several options exist to select a topology and transition to that topology.

- Individual routers may choose the topology based on the early link state information that arrives at that router. A set of criteria to govern the selection of a topology that is not the default topology is presented.
- A protocol could be created separately from the routing protocol that has the responsibility of detecting geographic events rapidly and notifying routers in the network of the topology change. This would allow routing timers to be maintained at traditional stable levels.
- Network administrators may preemptively select a topology based on situational information that exists. This could be a significant weather forecast, declining political situation, or other large scale events that are known prior to the impact to the network. Preemptively select a topology based on situational information that exists. This could be a significant weather forecast, declining political situation, or other large scale events that are known prior to the impact to the network.
3.1. Topology Creation Algorithm, gcMTR, gtMTR

There are two methods to create multiple topologies presented here that include the Geographic Coverage Multi-Topology Routing (gcMTR) approach and a Geographic Targeted Multi-Topology Routing approach (gtMTR). In gcMTR, N topologies are created, each that can avoid a geographic area in a network. If these topologies are distributed accordingly, they will provide coverage against most geographic events.

The gtMTR approach uses existing knowledge about specific events to build a topology that targets a specific geographic area. Targets could include natural disasters that have a likely location (like an earthquake fault line or area frequently impacted by hurricanes), geo-politically vulnerable areas, or other anticipated geographic impacts. This enables network planners to anticipate certain geographic impacts. Notations used here are:

- $G(V,E)$: Network Graph with nodes $V$ and edges $E$ (links)
- $N$: number of topologies required gcMTR or gtMTR
- $V_i$: center of vulnerable area $i$
- $R$: radius of any vulnerable area
- $T_i$: MTR Topology $i$
- $D_{ij}$: the distance between $V_i$ for $T_i$ and the closest point on link $j$. 
- $W_{ij}$: the Link Weight on link $j$ for $T_i$.

Algorithm 1 (gcMTR) creates a set of topologies that provide coverage across a network to protect against a variety of geographic events. Function `genCoveragePlan` generates locations to avoid based on a coverage plan that can be configured for a specific network. Algorithm 2 (gtMTR) utilizes knowledge about a particular type of an event to create topologies specifically designed for a certain event. Function `genTargetList` generates locations to avoid based on a custom list of predefined geographic event locations. The function `Norm` normalizes the maximum weight (at $V_i$) to 100.

Algorithm 1 Create Coverage Topologies - gcMTR

\[
\begin{array}{l}
\text{for all } i \text{ in } N \text{ do} \\
\quad V_i \leftarrow \text{genCoveragePlan}(i) \\
\text{for all } j \text{ in } K \text{ links do} \\
\quad \quad \text{if } D_{ij} < R \text{ then} \\
\quad \quad \quad W_{ij} \leftarrow \text{Norm}(MaxD_{ij} - D_{ij}) \\
\quad \quad \text{else} \\
\quad \quad \quad W_{ij} \leftarrow 1 \\
\quad \text{end if} \\
\text{end for} \\
\text{end for}
\end{array}
\]

The results in the following sections show that the greatest gain for gMTR methods occurs when the topology vulnerable area is well matched to the actual geographic event both in size and location. Therefore if the event center was in a non-covered area, it is likely that the topology chosen would not be a good match for the event. In Fig. 1, a grid pattern is used to lay out the circles. The circle packing in square method of coverage is shown using the Cost266 network from the Survivable Network Design Library (SNDlib 1.0) [16]. It is easily shown that coverage of circles in a square is $\pi/4$ (78.5%).

A more efficient method of coverage would be to use a hexagonal approach. It is well known that the highest coverage of circle packing is possible using a hexagonal approach with a coverage of $\pi/(2 \sqrt{3})$ (90.7%). The coverage difference using this approach is shown in Fig. 2. It is noted that even with this coverage approach, an event near the intersection of the hexagons is still not necessarily a good match to a given topology vulnerable area. A possible solution would be to overlay another hexagonal pattern of topologies on the existing, shifting the centers to align with the intersection of the hexagons. The topology with the center closest to the event center would still be chosen.

3.2. Topology Selection and Use

As mentioned at the beginning of Sect. 3, there are multiple operational concepts related to the selection of a topology.

3.2.1. LSA Method

As OSPF (or other IGP) detects link and node failures via hardware methods and Hello protocol, LSAs are generated and flooded across the routing area notifying the other routers of the link and node failures. Each router will use a set of criteria to enter MTR mode and note a Geographically Correlated Event $E_V$.

![Figure 1: Circular Topology Coverage Pattern](image-url)
The proposed criteria are shown here:

1. More than 2 nodes or more than 3 non-adjacent links are out of service simultaneously within radius $R$. These devices form the basis of the geographic event with its center at the geographic mean of the failed nodes or links AND
2. Geographic center of the geographic event is within $R$ distance of any $V_i$

This set of criteria allows for considerable flexibility in topology creation algorithms including overlapping coverage algorithms. If overlapping coverage is used, better fitting topologies should exist. The criteria also allow for a no MTR mode option that may be desired for certain geographic locations. It is assumed that all routers in the routing area are using the same algorithm (gcMTR or gtMTR). In addition, all routers would use the same topologies and topology selection criteria. Routing loops would be possible only during the time between when the first router has changed topologies to the time when the last router changes topologies. One of the disadvantages of this approach is that the RouterDeadInterval is still used for notification.

3.2.2. Geographic Detection Protocol

This approach overlays a protocol that monitors the network using other methods and when the above criteria are met, the protocol notifies the routers to switch to a different topology. The advantage of this approach is that faster switching could be accomplished since it is not as reliant on the RouterDeadInterval, assuming other accurate and faster methods are used to detect router or link failures.

3.2.3. Situational Awareness

Perhaps the most promising use for this technology involves the flexibility of humans that have an awareness of events in the different geographic areas of the network helping with the decision making process. The advantage with this approach is that a preemptive switch to a different topology is possible, lessening the impact of the proposed event significantly. Preemptive switch to a different topology is possible, lessening the impact of the proposed event significantly.

Certain types of large geographic events can actually spread, causing routers near the edges to fail later than the routers near the center of the event. This could be the case with certain weather events like hurricanes or even political instability. In this case, the impact to the routing in the network is more significant as route stability is further delayed. We tested this situation using simulation, as is reported in Sect. 6.

Regardless of the operational concept chosen, to achieve fast switching during the event, it would be required that routers maintain SPTs for all topologies that could be used. In order to minimize processing at the routers a couple of approaches could be used. First, the calculation of not-in-use topologies should be prioritized lower than the in-use topology. Second, it may not be required that the not-in-use topologies be calculated as often as the in-use topology. If there were $k$ topologies and we assume a period of $t$ default topology SPT calculations before not-in-use topologies SPTs are calculated, that would be $k/t$ SPT additional calculations for every normal SPT calculation. Since, it is well known that Dijkstra shortest path algorithm has $O(n \log(n) + e)$ complexity, where $n$ is the number of nodes and $e$ is the number of edges (links), the overall complexity would only increase at the worst linearly with the number of topologies.

Definition 1. $(EV_k, P_k, T_k)$ is an Geographically Correlated Event meeting MTR mode criteria that is centered at point $P_k$ with topology selected $T_k$.

Algorithm 3 Select Topology

if Geographically Correlated Outage Occurs, $<EV_k, P_k, 0>$ then

$V_{dist} \leftarrow \infty$

$T_k \leftarrow 0$

for all $j$ in $N$ Topologies do

if $D_{jk} < V_{dist}$ then

$V_{dist} \leftarrow D_{jk}$

$T_k \leftarrow j$

end if

end for

$<E_k, P_k, 0 > \leftrightarrow <E_k, P_k, T_k >$

end if

4. Illustrative Example

To illustrate our approach, we now use a $5 \times 5$ grid topology on the topology generation algorithms (1 and 2).

4.1. $5 \times 5$ Grid Network

Fig. 3a shows a $5 \times 5$ grid with default topology (all link weights are one). The link weights are shown in green. The SPT source node is 4. When geographic events occur, we assume several nodes in an area are disabled. This may affect the default SPT in a minimal way as Fig. 3b shows; only routing to nodes 20 and 21 was affected when nodes 10, 11, 15, 16 were deleted. Fig. 3c shows the topology generated when the vulnerability point is $V_i = (22, 57)$ with a radius of $R = 20$. The topology moves the vulnerable point to the leaves of the tree.
Figure 3: Grid5 Network, SPT Source = 4, SPT links are solid, non-SPT links are dashed. Link weights are shown. (a) Grid5 Default Topology (b) Network with nodes surrounding (22, 57) with radius $R = 20$ deleted (c) Topology created with $V_i = (22, 57)$ with radius $R = 20$ (d) Network with nodes surrounding (40, 24) with radius $R = 20$ deleted (e) Topology created with $V_i = (40, 24)$ with radius $R = 20$

However, when nodes 1, 2, 6, 7 are deleted, Fig. 3d shows that routing to 10, 11, 12, 15, 16, 17, 20, 21, 22 is affected by the SPT change. Clearly, the location of the vulnerability with respect to the main part of the default SPT affects the impact of the outage. Fig. 3e shows the $5 \times 5$ grid with a topology generated with a vulnerability point at $V_i = (40, 24)$ with a radius of $R = 20$.

5. Analysis on Moderate and Large Topologies

To conduct our analysis of the Geographic Multi-Topology Routing algorithms, two networks were chosen. The first network is the Cost266 network shown in Fig. 4 from the Survivable Network Design Library (SNDlib 1.0) [16]. It is moderate size network topology with 37 nodes and 56 links. The second network is the AT&T Layer 1 topology generated by Sterbenz, et al. [23] and available at [7]. Fig. 5 shows this large physical layer topology with 383 nodes and 483 links.

Two metrics are computed and analyzed. These include:

1. **Percentage of Dropped Connections ($\% \text{Drop}$)**. This is the percentage of all paths ($P_K$) used to implement $K$ demands that are interrupted immediately following the geographic event at $t = 0$ as shown in (1). This does not include demands disconnected because a node at either end of the demand was disabled by the event.

   \[
   \% \text{Drop} = \frac{P_K - P_{K_{t=0}}}{P_K} \tag{1}
   \]

2. **Average path length ($L(P_K)$)**. This is the average length of paths ($P_K$) used to implement $K$ demands.

During simulation, we look at the time to re-establish services interrupted by the geographic event, referred to here as convergence time. The gMTR Gain is defined as the convergence time $\times$ the bit rate interrupted with the default topology, giving us the effective amount of information not lost by using the selected topology as opposed to the default.

For the Cost266 network, SPTs were generated from all nodes as Dijkstra algorithm sources and the results averaged. The services are defined as the connection from the source to all other nodes. For the ATT L1 network, SPTs were generated from a selection of 30 nodes as Dijkstra’s algorithm sources that were spread across the network. The 30 largest metropolitan areas were chosen. The SPTs were created from the source to all sites in the ATT L1 network.

5.1. Cost266 Network

In the Cost266 network, a series of topologies in a circular pattern and in a hex pattern were created to provide coverage plans for that network. Fig. 4a shows a hex pattern of 6 locations ($V_i$) used to create the hex coverage topologies. The closest ($V_i$) to the event center is the selected topology. Fig. 4b shows the Cost266 network Default Topology (all link weights $= 1$). For illustrative purposes, the SPT source in the figures is Lisbon. Three geographic events were created for evaluation as shown in Table 1. These were loosely based on possible disaster scenarios.

Fig. 4c shows the SPT with a Lisbon source after event 2. Amsterdam, Dusseldorf, and Brussels and all associated links were removed in this event. Fig. 4d shows the SPT with new link weights created by the selected topology using London as the SPT source.
a source. The selected topology was 1 with a $V_i$ located at (1,51.0).

Table 2 shows the improvements gained by using a selected topology that was similar to the actual event. Generally, it was noted that if the event disconnects a major part of the default SPT, the improvements were significantly better than if the event was located in the leaves of the SPT. Event 2 disrupted the default path that crossed northern Europe. The circular topology that was selected routed connections around this area and improved the number of disconnected services significantly. Interestingly, the hex topologies performed better than the circular topologies with the exception of Event 2.

Table 3 shows the average path distance prior to the event and after the event using the default topology, and after the event using selected circular or hex topology. The distance was shortest during the default topology having more routing options than during the event or selected topology, the additional path length was not substantial.

<table>
<thead>
<tr>
<th>Event Number</th>
<th>X Location</th>
<th>Y Location</th>
<th>Radius</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.2</td>
<td>47.2</td>
<td>3.5</td>
</tr>
<tr>
<td>2</td>
<td>5.0</td>
<td>52.5</td>
<td>3.0</td>
</tr>
<tr>
<td>3</td>
<td>18.0</td>
<td>47.0</td>
<td>4.0</td>
</tr>
</tbody>
</table>

Table 2: Cost266 Evaluation - %Drop During Event

<table>
<thead>
<tr>
<th>Event</th>
<th>Circular Topology</th>
<th>Hex Topology</th>
<th>Default Topology</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4.33%</td>
<td>0.00%</td>
<td>10.93%</td>
</tr>
<tr>
<td>2</td>
<td>1.64%</td>
<td>17.56%</td>
<td>20.67%</td>
</tr>
<tr>
<td>3</td>
<td>3.32%</td>
<td>0.00%</td>
<td>7.03%</td>
</tr>
</tbody>
</table>

Table 3: Cost266 Evaluation - Average Path Length (Hops)

<table>
<thead>
<tr>
<th>Event</th>
<th>Pre-Event</th>
<th>Post-Event</th>
<th>Post-Event</th>
<th>Post-Event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Default</td>
<td>Circular</td>
<td>Hex</td>
<td>Hex</td>
</tr>
<tr>
<td>1</td>
<td>3.657</td>
<td>3.769</td>
<td>3.714</td>
<td>4.097</td>
</tr>
<tr>
<td>2</td>
<td>3.662</td>
<td>3.918</td>
<td>3.913</td>
<td>4.063</td>
</tr>
<tr>
<td>3</td>
<td>3.578</td>
<td>3.669</td>
<td>3.615</td>
<td>3.883</td>
</tr>
</tbody>
</table>

5.2. ATT L1 Network

In the ATT L1 network, 8 topologies were created to provide a circular and hex coverage plan for that network. Fig. 5a shows the circular pattern of 8 locations ($V_i$) and radii ($R_i$) used to create the coverage topologies. For brevity, we show details only for the circular topologies but the hex topologies used are shown in Fig. 6.

Fig. 5b shows the ATT L1 network Default Topology (all link weights = 1). The SPT source in the figures is New York. Four geographic events were created for evaluation as shown in Table 4. These were loosely based on possible disaster scenarios.

Table 4: ATT L1 Geographic Events

<table>
<thead>
<tr>
<th>Event Number</th>
<th>X Location</th>
<th>Y Location</th>
<th>Radius</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-89.5</td>
<td>36.6</td>
<td>3.8</td>
</tr>
<tr>
<td>2</td>
<td>-78.6</td>
<td>34.0</td>
<td>4.0</td>
</tr>
<tr>
<td>3</td>
<td>-119.7</td>
<td>35.6</td>
<td>4.0</td>
</tr>
<tr>
<td>4</td>
<td>-90.0</td>
<td>40.0</td>
<td>3.5</td>
</tr>
</tbody>
</table>

Table 5: ATT L1 Evaluation - %Drop During Event

<table>
<thead>
<tr>
<th>Event</th>
<th>Circular Topology</th>
<th>Hex Topology</th>
<th>Default Topology</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>27.00%</td>
<td>1.83%</td>
<td>22.94%</td>
</tr>
<tr>
<td>2</td>
<td>0.28%</td>
<td>0.86%</td>
<td>12.66%</td>
</tr>
<tr>
<td>3</td>
<td>2.79%</td>
<td>1.15%</td>
<td>4.26%</td>
</tr>
<tr>
<td>4</td>
<td>1.26%</td>
<td>0.58%</td>
<td>20.53%</td>
</tr>
</tbody>
</table>

5.3. Sensitivity to Event Size, Node Density, & Location

One of the areas of interest is how sensitive these methods are to events that are not located directly on a topology from
Figure 4: Cost266 Network, SPT Source = Lisbon, SPT links are solid, non-SPT links are dashed. Link weights are shown. (a) Topology Coverage Plan (b) Default Topology (c) Event Scenario 2, Location = (5, 52.5) Radius = 3.0. (d) Selected Topology with V = (1.0, 51.0), Radius = 4.25

Figure 6: ATT L1 Network, Hex Topology Coverage Plan

Table 6: ATT L1 Evaluation - Average Path Length (Hops)

<table>
<thead>
<tr>
<th>Event</th>
<th>Pre-Event Default</th>
<th>Post-Event Default</th>
<th>Post-Event Circular</th>
<th>Post-Event Hex</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14.378</td>
<td>14.956</td>
<td>15.272</td>
<td>16.302</td>
</tr>
<tr>
<td>3</td>
<td>13.022</td>
<td>12.898</td>
<td>13.082</td>
<td>13.252</td>
</tr>
<tr>
<td>3</td>
<td>14.391</td>
<td>14.743</td>
<td>15.878</td>
<td>15.133</td>
</tr>
</tbody>
</table>

a location or size perspective and how sensitive these methods are to the density of nodes in a topology. The first test to evaluate this was to change the location of all 4 events in the ATT network to locations west and east relative to the center of the topology by 50%, 100%, and 200% of the selected topology radius. Fig. 7 shows the Drop% using both the default topology and selected topology when the event center is not aligned with the topology center. The results were as one would expect. The selected topology performed well when the event was centered where the topology is centered. As the event drifts away from the center of the topology, the performance degrades approaching the performance of the default topology.

The second test varied the topology size of all 4 events in the ATT network from 25% to 200% of the event radius. Fig. 8 shows the average percentage of connections dropped using both the default topology and selected topology when the event size is not aligned with the topology size. When the topology size is between 100% and 200% of the event size, the performance of gMTR is good. Performance degrades quickly outside those bounds. We also looked at the performance when the average number of nodes in a topology is varied. Fig. 9 shows the average number of nodes per topology versus Drop%. This was done by reducing the topology size and event size concurrently. Fig. 8 and Fig. 9 are very similar. This leads to some interesting observations. First, there is definitely a practical lower
bound on the number of nodes per topology. It appears to be near 4. The upper bound is related to the portion of the entire network that is covered by a single topology. As the topology covered more than 70 out of 383 nodes (approximately 18%), the performance approached default performance. That would imply that a single topology should not cover more than approximately 15% to 20% of an entire network.

6. Simulation Study

To better understand the convergence process used by OSPF and gains that are possible using gMTR, a simulation study was conducted on the ATT L1 network. The goal of the simulation was to see how quickly traffic that was interrupted by a geographic event was restored using the OSPF routing protocol in a large network. The simulation was built using OPNET [15]. All 383 nodes were built using a Cisco 12000 series router as the model. All of the ports were set up to use OSPF routing. The network was connected as per the ATT topology using 10 Mb point-to-point Ethernet connections.

Two scenarios were constructed. The first was a single pair of demands between Pittsburgh, PA and Salt Lake City, UT. The demands were constant bit rate (UDP) approximately 32 kB/s. The second scenario was a full mesh of demands between 12 cities. These are listed in Table 7. In both scenarios, a large geographic outage was scheduled to occur at approximately 200 seconds into the simulation. The outage is the same as is de-
In the simulation, the gMTR topology that was used is topology 3 as shown in Fig. 5d. This is the selected topology using Algorithm 3. Link weights in the topology were set manually for the simulation.

In all cases, the demand traffic does not start until approximately 100 sec. This is to allow the routing protocols to initially converge prior to transmission. The traffic noted at approximately 50 sec is routing protocol traffic. In all cases, except where noted the HelloInterval was set to the default of 10 sec and RouterDeadInterval was set to 40 sec.

### Table 7: ATT L1 Simulation - Multiple Demand Cities

<table>
<thead>
<tr>
<th>City</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>New York, NY</td>
<td>Washington, DC</td>
</tr>
<tr>
<td>Atlanta, GA</td>
<td>Miami, FL</td>
</tr>
<tr>
<td>Chicago, IL</td>
<td>Dallas, TX</td>
</tr>
<tr>
<td>Minneapolis, MN</td>
<td>Pittsburgh, PA</td>
</tr>
<tr>
<td>Salt Lake City, UT</td>
<td>Seattle, WA</td>
</tr>
<tr>
<td>San Francisco, CA</td>
<td>Los Angeles, CA</td>
</tr>
</tbody>
</table>

#### 6.1. Single Demand Simulation

Fig. 10-13 demonstrate how MTR would work with a known outage occurring in the region surrounding Chicago, IL. This is depicted in 5e. In Fig. 10 we see the traffic path used by the default topology prior to the event at 200 sec. This path is through Chicago. The traffic path used by the default topology after the event occurs is also shown, going through Kansas City, MO. In Fig. 11, the throughput is shown for the demand. It is easy to see the 40 second interruption in traffic when the outage occurs.

Fig. 12 shows the selected topology path that is used. The path takes a wide route around the topology 3 as shown in Fig. 5a. Finally, as expected Fig. 13 shows the un-interrupted traffic flow through the outage.

To further explore the influence of the RouterDeadInterval in the convergence time, additional tests were conducted. This test was run with a HelloInterval of 2 seconds and RouterDeadInterval of 10 seconds. As is shown in Fig. 14, the convergence time was reduced from 40 seconds to approximately 10
seconds, which follows the RouterDeadInterval settings. This confirms the relationship between the settings for the RouterDeadInterval and the convergence time in OSPF.

It raises the question of why one would not just reduce the RouterDeadInterval in OSPF to achieve faster convergence times? As was pointed out in Section 1, reduction of the OSPF RouterDeadInterval timer reduces the stability of OSPF and can cause flapping. The methods described here both reduce convergence and are stable.

6.2. Multiple Demand Simulation

Fig. 15 - 21 demonstrates how OSPF would function with a large geographic outage near Chicago, IL prior to and after gMTR is implemented as is depicted in Fig. 5e. In Fig. 15 we see multiple traffic paths used by the default topology prior and after the event at 200 seconds. Prior to the event, much of the traffic from Pittsburgh and New York that is destined to Seattle and San Francisco traverses Chicago. After the event, the traffic shifts to a more southerly route through St. Louis.

Figure 16 shows the received traffic at Salt Lake City from the other 11 sites using the default topology during the event. It is interesting to note progression through the event. At 200 seconds, the traffic that crosses Chicago is lost. At approximately 230 seconds, the traffic that was rerouted around Chicago is restored. The final level is the original traffic minus the traffic that was terminated at Chicago. Figure 17 shows the throughput on the Bridgeton, MO (near St. Louis, MO) to Columbia, MO link. This is the link that would have acquired much of the rerouted Chicago traffic. The increase in traffic is noted at approximately 240 seconds. Finally Fig. 18 shows the traffic demands between Salt Lake City and Dallas, Chicago, Pittsburgh. The demand traffic reacts as expected during this event.

After gMTR is implemented, Figure 19 shows the differences in demand paths. It is interesting to note the wide path around the chosen gMTR topology that is used, steering the traffic as far south as Dallas. It is apparent that using gMTR, a margin of error is implemented in case the outage is not exactly as predicted. In addition, much of the traffic is moved away from the edges of the events as opposed to the default topologies which tends to flow around the event.

Fig. 20 shows the received traffic at Salt Lake City post-gMTR implementation during the event. When the event occurs, the only change that occurs is the loss of the traffic associated with the Chicago node. This illustrates the reduction of churn in the network when using gMTR.

Although this simulation has presented these outages as a single event, it is unlikely that in real life they would present as a single event. Cascading outages that are geographically correlated have been documented and are discussed in Section 1. It is useful to investigate the harm caused by cascading outages. A cascading outage was constructed by allowing the Chicago node to fail at 200 seconds and the remaining nodes related to that geographic outage to fail 260 seconds. This caused the interesting (but predictable) results between nodes Minneapolis and Pittsburgh shown in Fig. 21. The traffic flow was inter-
Figure 18: Traffic Using Default Topology between Salt Lake City, UT and a) Dallas, TX b) Chicago, IL c) Pittsburgh, PA

Figure 19: Multiple Demand Showing Pre-outage and Post-outage Paths Using Selected Topology

Figure 20: Receive Traffic at Salt Lake City, UT using Selected Topology

Figure 21: Demand Traffic Between Pittsburgh, PA and Minneapolis, MN during Cascading Failure

ruptured initially at 200 seconds, restored at approximately 240 seconds, and failed again at 260 seconds, and finally restored at approximately 300 seconds. This illustrates the benefits of using gMTR to provide a stable path for traffic that avoids the geographic area.

7. Conclusion

This work has demonstrated that Multi-Topology Routing (MTR) can be used to improve performance of routing during large geographic events like natural disasters. These improvements are achieved by maintaining additional topologies created by increasing link weights in specific areas of the network. This has the effect of pushing the trunk of the Shortest Path Tree out of the region of highest impact, preventing disruption of much of the traffic during the event.

Multiple topologies can be created to anticipate multiple events in a network. When this is done, a topology is selected when it is apparent that a geographic event has occurred. The traffic is moved to the new SPT quickly and the impact of the event is minimized. Essentially, the amount of network churn is reduced during the geographic event.

Clearly the key to improving routing performance during geographic events is to have knowledge of that event and be able to act on that event prior to the rerouting process used by OSPF which is constrained by several timers intended to provide more stability in the routing algorithm. The RouterDeadInterval and HelloInterval are key timers that can directly influence not only the convergence time in the network but also the stability in the network. By using fast detection or forecasting techniques and switching to known stable SPT, the convergence time can be minimized using OSPF.

Three algorithms were proposed. Two algorithms gcMTR and gtMTR provided methods to create alternate topologies in both a network wide coverage approach and targeted approach that can be used to anticipate a specific event, where knowledge of that event exists. gcMTR is implemented using a circular and hexagonal approach. The third algorithm specifies a way to detect a geographic event and select a topology to use. A discussion is included of operational models that can be used to detect geographical events.

During evaluation, it was discovered that the number of dropped connections is typically significantly better if a selected topology is used. The exception to this is if the condition exist where (1) the event does not disrupt a significant branch of the default SPT and (2) the selected topology does not fit well with the event from a location perspective. We explored this further by modifying the distance that the event oc-
curs from the center of the topology and by modifying the size of the event compared to the radius of the topology. Although not unexpected, the results emphasize the importance of the algorithm and parameter selection. One interesting observation is that there appears to be practical bounds related to topology size and distribution. If a topology does not contain more than approximately 4 nodes, the performance degrades to default and if a single topology covers a significant portion of the overall network the performance also suffers. These are intuitive observations and testing here provides a guide during implementation of topologies. Hex configurations of topologies tended to outperform circular configurations in the networks tested here. The better coverage and more optimal locations of topology centers is likely the reason. More research in the distribution of topologies is needed to determine the optimum configuration and number of topologies that should be supported.

Simulation was used to investigate the effects of geographic outages in networks using OSPF without gMTR and with gMTR. Convergence times, defined as the time to restore traffic flows after the event, are analyzed using default settings for HelloInterval and RouterDeadInterval timers in OSPF. The settings are then modified to understand the relationship between the timers and convergence times. Finally, a cascading geographic failure was simulated to show the impact of these types of failures.

Since there is not a large body of research in this area, there are significant opportunities for future research. We plan to implement these algorithms in simulation to assess how they perform in a more lifelike setting. Generating efficient coverage topologies that optimize for size, number, and location of the topologies is needed. Optimizing the frequency of calculating SPTs for not-in-use topologies is also an interesting extension of this work.

Acknowledgments

This research is supported in part by the National Science Foundation under grant Nos. CNS-0916505 and CNS-1217736, and by the Federal Aviation Administration under Cooperative Agreement No. 11-G-0182. The authors would like to thank the KU Resilinets Group (J. Sterbenz and Y. Cheng) for assistance with the ATT L1 network and general conversations about this work.

References