Proceedings Paper:

Nasralla, ZHA, Musa, MOI, El-Gorashi, TEH et al. (1 more author) (2016) Routing Post-Disaster Traffic Floods Heuristics. In: 18th International Conference on Transparent Optical Networks (ICTON 2016). ICTON 2016, 10-14 Jul 2016, Trento, Italy. IEEE . ISBN 9781509014675

https://doi.org/10.1109/ICTON.2016.7550697

Routing Post-Disaster Traffic Floods Heuristics

Zaid H. Nasralla, Mohamed O. I. Musa, Taisir E. H. El-Gorashi and Jaafar M. H. Elmirghani
School of Electronic and Electrical Engineering, University of Leeds, LS2 9JT, United Kingdom
E-mail: {elzhan, el10moi, t.e.h.elgorashi, j.m.h.elmirghani}@leeds.ac.uk

ABSTRACT

In this paper, we present three heuristics for mitigating post-disaster traffic floods. First exploiting the excess capacity, second rerouting backup paths, finally redistributing the whole traffic by rerouting the working and protection paths to accommodate more floods. Using these mitigation approaches can reduce the blocking by up to 30%.

Keywords: core networks, disaster-resilient, post-disaster traffic floods.

1. INTRODUCTION

Disaster-Resilient Networks is a new paradigm in building core networks that can survive with maximum availability after disasters. This topic attracted many research groups recently due to the growing number of disasters around the world. Disasters affects the network infrastructure directly or indirectly depending on the disaster type and impact. In direct impact, it might cause fiber cut or equipment damage, while in the indirect consequences power outages and huge generated traffic due to disasters can be considered.

Recently significant research efforts had focused on mitigating disaster risk through different approaches. Using path protection is the preliminary approach for avoiding fiber cut or intermediate nodes failures as in [1]. Protecting cloud data center was studied in [2], to ensure the availability of service that destined to data centers, by replicating the cloud contents to more than one data center. Building resilient virtual network against disasters studied in [3]. Restoration is a dynamic approach in optical networks which is used to reroute the traffic in case of path failure [4]. Software Defined Network (SDN) is an emerging technology that can be helpful in combating disasters due to its scalability and the centralized operation [5].

Added to failures perspective in building disaster-resilient networks another two dimensions should be addressed which are the energy efficiency and the huge surge amount of traffic generated due to disasters. In previous work [6], we discussed post-disasters traffic floods, which is mainly caused by the enormous amount of data traffic. These floods contains social media traffic, VoIP, user generated videos. This spark rises after disaster and this spark identified by [7, 8] after the Great East Japan Earth Quake and Tsunami. They show that 76% of people tend to use social media during disasters [7]. Whereas in [8], the authors show that the video traffic rises sharply at disasters.

In our previous work [6], we developed a Mixed Integer Linear Programming (MILP) model to simulate the optical core network performance during single node flooding with different flood sizes. Then we studied the four mitigation approaches to serve more floods by exploiting link excess capacity, rerouting, selective traffic filtering and differentiated-services. In this paper, we present three heuristics that mimics the MILP model but in real time. The three approaches are: Floods with Fixed Routing (FFR), Floods with Protection Paths Rerouting (FPPR), and Floods with Working and Protection Paths Rerouting (FWPPR).

The remainder of this paper is organized as follows: in Section 2, the disaster traffic floods heuristics will be explained. Section 3 discuss the results before, finally, the paper is concluded in Section 4.

2. POST-DISASTER TRAFFIC FLOODS HEURISTICS

In this section, we present three heuristics to maximally serve post-disaster traffic floods. We consider an IP over WDM network with multi-hop grooming. Also we assume that all traffic demands are protected using 1+1 protection scheme, where two copies of data are sent over the two physically disjoint paths.

In the default scenario of flooding, the working and protection paths are routed on a predetermined paths. The floods should occupy these lightpaths until they get fully utilized, after which, either they are blocked or new lightpaths are initiated on the same original routes until the link residual capacity gets exploited. In our heuristic, we consider the second case. This scenario has no dynamicity in routing except adding new lightpaths when required.

In the FFR approach heuristic shown in Fig-1, first the algorithm finds the shortest disjoint paths pair between all nodes using Bhandari algorithm [9]. These sorted non-flooding demands are routed on the predetermined working and protection paths. Then it start provision the flooding demands using the same procedure. The algorithm maintains the mutual necessity between the working and protection path; they are either accepted together or blocked together.

In the FPPR, a new dimension of freedom is added by rerouting the protection paths, while the working paths are left without disruption. The heuristic shown in Fig-2 consists of three steps; initially it finds a pair of disjoint paths using Bhandari algorithm then sorts the demands and floods ascendingly. First it starts routing the non-flooding demands by routing working paths and forming an initial routing solution of the corresponding protection paths. Second, it routes the flooding working paths and forms an initial solution by routing their protection paths on the predetermined routes. The third step is to reroute the protection paths for both the non-flooding and flooding demands. It checks whether the initial routing has enough residual capacity or not, if it still has capacity then it uses it, otherwise it attempts to route it using the Routing function which shown in Fig 3. To get a protection path that is link disjoint from the working path, the algorithm removes the working path links from the physical topology then searches for the next best path. If the function fails to route the protection path, the working path route will be deleted and the whole demand will be blocked.

The routing function attempts to route the demand using either a single path if the capacity of the widest path is enough or multipath if the capacity is not enough, otherwise if it fails then the demand is blocked. First it searches for all possible non loop paths between the source and destination. Then it searches for the widest path (which has the maximum bottleneck). After that it will sort the paths in descending order in terms of available path capacity. It checks whether the widest path has enough capacity to accommodate the demand, then it routes it using single path. The function will compromise the number of hops with residual capacity, by searching the minimum hop route that can accommodate the whole demand. If it fails to find a single path, then it will route it using the widest path, after that it will update available capacities and paths residual capacities. Again, it will use the new widest path to accommodate the remaining portion of the demand. Continuing on this process till serving the whole demand or exploiting the available paths. Failing to serve the demand will return a blocking indicator.

Fig. 4 shows the FWPPR heuristic, it consists of two main parts, the first one to route the non-flooding demand while the second loop to route the flooding demands. The reason for routing non-flooding demands first is to prevent the floods from occupying the whole network resources. For the floods, we use our suggested routing function to route both working and protection paths.

```
Algorithm: FFR
Input: Set of Physical Nodes in Network (N),
Set of Physical Links in Network (L),
Set of Flooding Demands(F),
Z: Set of non-flooding demands
Output: Network Blocking Probability
Find a pair of disjoint paths (P1(r), P2(r)) ∀ r ∈ D
Sort Z,F ascendingly
Step 1 : Routing non-flooding demands (Z)
For r in Z
        Route r (working)    on P1(r)
        Route r (protection) on P2(r)
End for
Step 2 : Routing flooding demands(F)
For r in F
      Find residual capacity of P1(r), P2(r) → R1(r), R2(r)
       If v(r) ≤R1(r) & v(r) ≤ R2(r)
          Route r (working)    on P1(r)
          Route r (protection) on P2(r)
       Else Block r
End for
```

Figure 1. FFR Algorithm

```
Algorithm: FPPR
Input: Set of Physical Nodes in Network (N),
Set of Physical Links in Network (L),
Set of Demands (D),
Set of Flooding Demands(F),
Z: Set of non-flooding demands, D=F ∪ Z
Output: Network Blocking Probability
Find a pair of disjoint paths (P1(r), P2(r)) ∀ r ∈ D (Bhandari Algorithm)
Sort D,Z,F ascendingly
Step 1 : Routing Non-flooding demands' Working Path
For r in Z
        Route r on P1(r)
        Form an initial solution by routing r on P2(r)
End for
Step 2 : Routing flooding demands' Working Path
For r in F
     Find residual capacity of P1(r), P2(r) → R1(r), R2(r)
        If v(r) ≤R1(r)
           Route r on P1(r)
           Form an initial solution by routing r on P2(r)
        Else Block r
End for
Step 3 : Rerouting flooding and non-flooding demands' Protection Path
For r in D
      Find residual capacity of (P2(r)) R2(r)
      If v(r) ≤ R2(r)
            Route r on P2(r)
      Else Reroute r using Routing* (Topology, Available Capacity, s, d, v(r))
      If r blocked
         Delete r on P1(r)
End for
```

Figure 2. FPPR Algorithm

```
Routing* Function (Topology, Available Capacity, s, d, rate)
Output: Available Capacity, Blocking
Get all k shortest paths
Calculate hop count h(k)
For i in k:
        Find residual capacity of all paths R(k)
        Calculate R(k)*h(k) product (residual-hop count product)
        Sort R(k) descendingly
        If R(1) ≥ rate
         Sort remaining paths with R > rate based on RxH ascendingly
              Route on the minimum (top) path
              Update capacities
          Break;
        If R(1) < rate
              Route demand on R(1)
              Update capacities (R(1)=0)
              Update demand value(rate=rate-R(1))
End for
```

Figure 3. Routing* Function

```
Algorithm: FWPPR
Input: Set of Physical Nodes in Network (N),
Set of Physical Links in Network (L),
Set of Flooding Demands(F),
Z: Set of non-flooding demands
Output: Network Blocking Probability
Sort Z,F ascendingly
Find a pair of disjoint paths (P1(r), P2(r)) ∀ r ∈ D (Bhandari algorithm)
Step 1: Route the Working and Protection Paths for non-flooding demands
For r in Z
      Route r (working)    on P1(r)
      Route r (protection) on P2(r)
End for
Step 2 : Routing flooding demands' Working and Protection Path
For r in F
       Route r (working) using Routing* (Topology, Available Capacity, s, d, v(r))
       If r blocked
         Break
       Else Delete Working Path Links from physical topology
          Route r (protection)using Routing* (Topology, Available Capacity, s, d, v(r))
             If r blocked
               Delete the working path route
End for
```

Figure 4. FWPPR Algorithm

3. RESULTS AND DISCUSSION

The network performance was evaluated using the NSFNET network that covers the US which is shown in Fig. 5. The NSFET consists of 14 nodes with 21 bidirectional links, and there are five data centers located at nodes (2, 3, 7, 8 and 9).

To simulate the network performance, we apply an incremental flood volumes that range from x2 to x10 in steps of 2. The used traffic matrix is based on the population-factor-distance (PFD) model that considers the US population and the nodes distances.

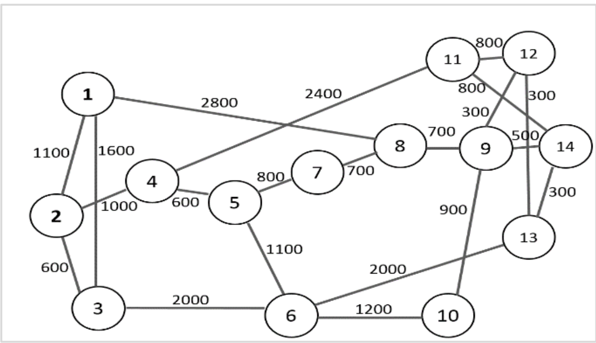

Fig. 5 NSFNET network with link distances in kilometers

Fig. 6 shows the percentages of average served floods for each scenario at each flooding size. We find that FFR is the worst in absorbing floods, because the network does not have the adaptability to change the routing table and stick to the predetermined paths. While FPPR performs better in terms of serving more floods, because rerouting protection paths can free more resources that can be used by floods especially near the flooding node. The last scenario outperforms the first two scenarios. The power point of the FWPPR scenario is that it does not have to use predetermined paths, but instead it can search for all possible paths to route the floods through.

In Fig. 7, we see the nodes performance under the three scenarios. The data center nodes have the worst performance due to the huge amount of traffic they have, although rerouting approaches facilitate absorbing more floods up to 30% in some nodes. In normal nodes, they suffer from blocking under FFR scenario, whereas applying x10 flood volume on these nodes under FPPR and FWPPR, the floods can be absorbed.

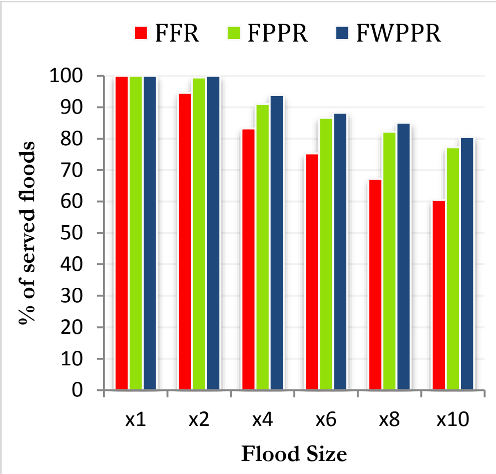

Figure 6. The percentage of average served floods for different flood sizes for three scenarios

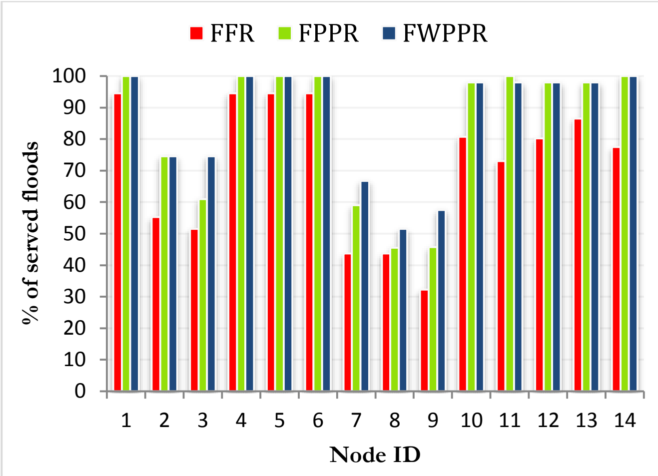

Figure 7. Percentage of average served floods of each node for the three scenarios

4. CONCLUSIONS

In this work, we tackled the problem of post-disaster traffic floods using three mitigation approaches. First by exploiting the excess capacity, then by rerouting protection paths and finally by rerouting working and protection paths. We presented three real time heuristics to simulate the network performance under the traffic floods. The results show that the mitigation approaches can reduce floods blocking by up to 30%.

5. Acknowledgment

The authors would like to acknowledge funding from the Engineering and Physical Sciences Research Council (EPSRC), INTERNET (EP/H040536/1) and STAR (EP/K016873/1). Mr. Zaid H. Nasralla would like to acknowledge the Higher Committee for Education Development-IRAQ (HCED IRAQ) and University of Karbala, for funding his scholarship.

6. References

[1] F. Dikbiyik, A. S. Reaz, M. De Leenheer, and B. Mukherjee, "Minimizing the disaster risk in optical telecom networks," in Optical Fiber Communication Conference, 2012.

[2] S. Ferdousi, F. Dikbiyik, M. F. Habib, and B. Mukherjee, "Disaster-Aware Data-Center and Content Placement in Cloud Networks," Lightwave Technology, Journal of, vol. 30, pp. 2563-2573, 2012.

[3] C. C. Meixner, F. Dikbiyik, M. Tornatore, C.-N. Chuah, and B. Mukherjee, "Disaster-resilient virtual-network mapping and adaptation in optical networks," Optical Network Design and Modeling (ONDM), 2013 17th International Conference on, 2013. pp. 107-112.

[4] F. Xu, T. Das, M. Peng, and N. Ghani, "Evaluation of post-fault restoration strategies in multi-domain networks," Optical Switching and Networking, vol. 9, pp. 147-155, 2012.

[5] K. Nguyen, Q. T. Minh, S. Yamada,"A Software-Defined Networking approach for Disaster-Resilient WANs", Computer Communications and Networks (ICCCN), 2013 22nd International Conference on,2013,p1-5.

[6] Z. H. Nasralla, T. E. El-Gorashi, M. O. Musa, and J. M. Elmirghani, "Routing Post-Disaster Traffic Floods in Optical Core Networks," Optical Network Design and Modeling (ONDM), 2016 20th International Conference on, 2016.

[7] J. Fraustino, L. Brooke, and J. Yan, "Social Media Use during Disasters: A Review of the Knowledge Base and Gaps, Final Report to Human Factors/Behavioral Sciences Division," Science and Technology Directorate, US Department of Homeland Security. College Park, MD, 2012.

[8] P. Baklan, K. Yamori, and Y. Tanaka, "Measure of user behavior before and during disaster congestion," in Advanced Communication Technology (ICACT), 2014 16th International Conference on, 2014, pp. 135-140.

[9] R. Bhandari, "Optimal diverse routing in telecommunication fiber networks", INFOCOM'94. Networking for Global Communications, 13th Proceedings IEEE, 1994, 1498-1508.