UNIVERSITY OF LEEDS

This is a repository copy of *Routing Post-Disaster Traffic Floods in Optical Core Networks*.

White Rose Research Online URL for this paper:
http://eprints.whiterose.ac.uk/97769/

Version: Accepted Version

Proceedings Paper:
Nasralla, ZHA, El-Gorashi, TEH, Musa, MOI et al. (1 more author) (2016) Routing Post-Disaster Traffic Floods in Optical Core Networks. In: ONDM 2016 Conference Proceedings. 20th International Conference on Optical Network Design and Modeling, 09-12 May 2016, Cartagena, Spain. IEEE , pp. 1-5. ISBN 9781467399883

https://doi.org/10.1109/ONDM.2016.7494055

© 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Reuse
Unless indicated otherwise, fulltext items are protected by copyright with all rights reserved. The copyright exception in section 29 of the Copyright, Designs and Patents Act 1988 allows the making of a single copy solely for the purpose of non-commercial research or private study within the limits of fair dealing. The publisher or other rights-holder may allow further reproduction and re-use of this version - refer to the White Rose Research Online record for this item. Where records identify the publisher as the copyright holder, users can verify any specific terms of use on the publisher's website.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

White Rose
university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Routing Post-Disaster Traffic Floods in Optical Core Networks

Zaid H. Nasralla, Taisir E. H. El-Gorashi, Mohamed O.I. Musa and Jaafar M. H. Elmirghani
School of Electronic and Electrical Engineering, University of Leeds, LS2 9JT, United Kingdom

***Abstract*-The increasing number of disasters around the world calls for a new direction in building the networks; this direction is known as disaster-resilient networks. In this paper, we consider the effect of post-disaster traffic on the core network performance. We evaluate the network blocking during single node flooding with different flood sizes. Then we study four mitigation approaches to maximally serve the traffic floods using the excess capacity, traffic filtering, rerouting and Differentiated-Services. The results show that the studied approaches reduce blocking by 50% in the worst cases.**

Keywords—disaster-resilient; traffic-floods; core network

I. Introduction

The current rapidly growing reliance of society on communication networks in all aspects of life necessitates continuous service availability. This availability could be maintained by building a reliable and resilient network. To maintain this reliability and combat failures, there are two types of connection recovery which are either proactive by deploying backup paths or reactive by reprovisioning the connections dynamically to new paths [1].

The Boston bombing in 2013 suggested a new issue that might affect the communication networks during disasters which is capacity exhaustion. This issue is relatively different from the previously studied considerations in building disaster-resilient networks. In this case the infrastructure is not affected physically but the heavy traffic on the network causes capacity exhaustion. This heavy traffic is a consequence of mobile networks' semi-shutdown [2] and the huge surge of data traffic at the scene.

This problem has been expected to rise since the introduction of the new applications and services that most people tend to use to investigate what is going on during disasters, as indicated in [3], which shows that two thirds of people use social media during disasters and post-disasters times. In [4], the authors make a survey to record the user behavior during large size disasters, and they found that 95% of users make phone calls and 76% post information on social media. Added to social media, the news agencies and governmental websites also got attraction through warnings and precautions broadcast. In [5], the authors show the spark raise in popularity in video traffic in both types; the real time video streaming (TV breaking news) and video streaming (user generated videos) after the Great East Japan Earth Quake and Tsunami.

The backbone of different access networks, including the broadband and cellular one, is the optical core network. The core network is the middleware between the access and the data centers and is responsible for delivering the data between them. In disaster situation, the core should handle this huge traffic in order not to violate the Service Level Agreement (SLA).

The core network capacity can't be upgraded instantaneously, because provisioning new lightpaths requires manual configuration and installing new fibers requires a long period. Alternative reactive solutions should be adopted to accommodate the huge traffic. This solution is known as dynamic networking where the network can reprovision the lightpaths automatically according to the available capacity to accommodate the traffic [6]. Software-Defined Networks (SDN) are considered to be a dynamic networking approach.

In [7, 8], the authors exploited the excess capacity for new connection pre-provisioning and backup re-provisioning by developing a Mixed-Integer Linear Programming (MILP) and a heuristic. During traffic fluctuation and growth, the algorithm starts free protection resources to be used by newly arrived connection requests, and then starts re-provisioning protection paths with less availability protection schemes. So during disasters as the network suffers from resources degradation, it will be efficient to use such an algorithm to serve more traffic. In our previous work [9] we have investigated reducing blocking probability using traffic scheduling for advance reservation demands. This approach will allow delaying a portion of the floods until the surge passes.

In this paper, we have studied network capacity exhaustion with different post-disaster traffic floods volumes. We have evaluated the network by applying incremental traffic volumes on a single node (a disastrous node) and measure the blocking probability. Also we have studied four approaches to maximize the served traffic and reduce the blocking probability. In the first approach, we suggest using Selective Traffic Filtering approach to filter out less priority traffic during disasters. The second scenario is to reroute backup paths that pass through the flooded node to free flooded node resources, while in the third approach, we suggest to reroute the working and protection paths in the whole network to accommodate more floods. Finally, we suggest using the Differentiated Services (Diff-Serv) approach, where the network should provide protection for high SLA traffic and eliminate protection for low SLA traffic. The network benchmarking had been done for the five scenarios to show how much traffic floods have been absorbed and how much has been blocked.

The remainder of this paper is organized as follows: in Section II, the disaster traffic floods scenario and mitigation approaches will be explained, Section III will present the MILP model for the floods and mitigation approaches. Section IV discuss the results before, finally, the paper is concluded in Section V.

II. DISASTER TRAFFIC FLOODS SCENARIOS

In the post-disaster phase, a flooded node does not have the global view of the network, so it will attempt to distribute floods using its excess capacity to satisfy the maximum amount of traffic floods. If it fails then it will block the enduring or queue it. In such a case, the users will experience drops and long delays.

We will consider the normal case and alternative approaches that attempt to minimize the blocking. In these approaches, we introduce the rerouting, protection resources violation and traffic filtering that can help to absorb more floods.

A. Floods with Fixed Routing (FFR):

In the normal operation, the routing table is predetermined for the working and protection paths. In the case of increasing the traffic demands, the traffic floods will follow the same paths for each source-destination predetermined path. The traffic floods can be served using the allocated capacity plus the link residual capacity. If the capacity of the links gets fully utilized, then the floods will be blocked.

B. Floods with Selective Traffic Filtering (FSTF):

In this scenario, we suggest reducing the flood by filtering out the less important traffic. During disasters there is important traffic that should be served, such as the Voice over IP (VOIP), social media web sites, news agencies and governmental videos. On the other hand, we can find that file sharing, gaming and Video-on-Demand (VoD) traffic demands are less important and can be filtered out for a short time till the flood surge passes.

One of the issues in this scenario is how to filter out VoD traffic while allowing VOIP traffic and both of them use the Real-Time Protocol (RTP). Deep packet inspection and port filtering can be used to filter special types of traffic while allowing other types to be served.

C. Floods with Protection Paths Rerouting (FPPR):

To satisfy the huge floods, we suggest reprovisioning the protection paths that pass through the flooded node. Reprovisioning the protection paths away from the flooded node will free more capacity that can be filled by the floods without affecting the working traffic.

D. Floods with Working and Protection Paths Rerouting (FWPPR):

To serve more traffic floods, a dynamic approach is required to reprovision resources accordingly. So, next we will introduce a rerouting approach for both working and protections paths with multi-rate splitting. Here the operator has the ability to reroute everything in the network to accommodate more floods. In this scenario, we allow for multi-rate splitting as well, where the demand can be routed using multipath when it is required till the capacity is exploited.

E. Floods with Rerouting and Differentiated Services (FRDS):

In this scenario, we suggest a hybrid approach that mixes the rerouting with Diff-Serv. In Diff-Serv, the traffic is classified into protected and best-effort requests. For the protected type which is represented by high SLA commitment traffic, we keep the 1+1 protection, while for low SLA availability traffic we cancel the protection paths. Removing protection paths for low class traffic demands can free more resources that can be used to serve more traffic floods while keeping the protection for the high class traffic.

III. MILP MODEL FOR DISASTER TRAFFIC FLOODS

In this section, we present a MILP model to maximally serve traffic floods and reduce the traffic blocking and provision resources for the working and protection resources. We consider an IP over WDM network with opaque architecture, which is shown in Fig.-1. Also multi-hop grooming will be used where the traffic is groomed at each intermediate node, and in this configuration the logical topology will be the same as the physical topology. We use such a configuration to reduce model complexity without affecting the expected results.

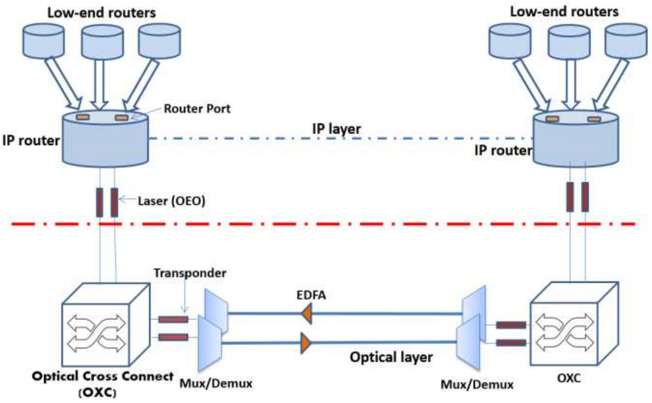

Fig. 1 The IP over WDM network architecture

We assume all traffic classes are protected using 1+1 dedicated path protection. In dedicated path protection, the working and protection paths should be path-disjoint.

First we design a network to accommodate the traffic plus the protection traffic, considering 1+1 means that two copies of the traffic is sent along the working and protections paths, and in the case of working path failure the destination node will switch to protection path copy. Nonetheless, the working and protection traffic (of different demands) can be multiplexed on the same wavelength.

The core network capacity should be provisioned to satisfy the maximum bandwidth requirements and commit the SLA. The SLA targets that should be met are the delay, jitter, availability and loss. Realistically, we consider the network capacity double the busy hour traffic.

The model is based on a node-link formulation, with the objective of maximizing the served traffic floods with min-hop paths for IP over WDM network architecture. The constraints are the primitive constraints for network design and routing. We add a binary parameter to represent the flooded node and another parameter to represent the flood size.

In Table-I, the parameters and variables definition.

Table I: MILP parameters and variables

Parameters:	
λ^{sd}	Traffic demand from node s to node d
Z_{mn}	Number of fibers in link(m , n)
f^{s}	Binary indicator , set if node s is flooded
F^{sd}	Represents the flood volume from node s to node d
W	The number of wavelengths in a fiber
B	Capacity of each wavelength
Variables:	
Δ^{sd}	The actual demand between node s and d , accounting for floods
$\widetilde{\Delta}^{sd}$	The protection traffic of a demand between node s and d , accounting for floods
w_{mn}^{sd}	The number of primary wavelength channels for demand (s, d) that traverse link (m, n)
$\widetilde{w}_{mn}^{sd}$	The number of backup wavelength channels for demand (s, d) that traverse link (m , n)
b_{mn}^{sd}	Binary equivalent of w_{mn}^{sd} , equals 1 if it has a value greater than zero.
$\tilde{b}_{mn}^{sd}$	Binary equivalent of $\widetilde{w}_{mn}^{sd}$, equals 1 if it has a value greater than zero.
w_{mn}	The total number of wavelengths on a physical link (m, n)
δ^{sd}	Binary variable indicate whether the request is served ($\delta^{\mathrm{sd}} = 1$) or not ($\delta^{\mathrm{sd}} = 0$)
γ^{sd}	Binary variable indicate whether the protection path for demand is provisioned ($\gamma^{sd} = 1$) or not ($\gamma^{\mathrm{sd}} = 0$)

The model is defined as follows:
Maximize:

$$\sum_{s\in N}\sum_{d\in N}\delta^{\mathrm{sd}} + \sum_{s\in N}\sum_{d\in N}\gamma^{sd} - \sum_{m\in N}\sum_{n\in Nm_m} w_{mn} \qquad (1)$$

$$\sum_{n\in N_m}(w_{mn}^{sd} - w_{nm}^{sd}) = \begin{cases} \Delta^{sd} & m = s \\ -\Delta^{sd} & m = d \\ 0 & m \neq s \neq d \end{cases} \qquad (2)$$
$$\forall\, s, d, m \in N$$

$$\sum_{n\in N_m}(\widetilde{w}_{mn}^{sd} - \widetilde{w}_{nm}^{sd}) = \begin{cases} \widetilde{\Delta}^{sd} & m = s \\ -\widetilde{\Delta}^{sd} & m = d \\ 0 & m \neq s \neq d \end{cases} \qquad (3)$$
$$\forall\, s, d, m \in N$$

Constraints (2) and (3) represent the flow conservation constraints, where the overall traffic, including the floods, is served between source and destination. The constraint itself accounts for the possibility that some demands can be blocked depending on the overall network situation. This is represented by the total traffic definition that is given by equations (4) and (5).

$$\Delta^{sd} = \delta^{sd}\lambda^{sd}F^{sd}f^{s}/B \qquad (4)$$
$$\forall\, s, d, \in N$$

$$\widetilde{\Delta}^{sd} = \gamma^{sd}\lambda^{sd}F^{sd}f^{s}/B \qquad (5)$$
$$\forall\, s, d, \in N$$

$$\sum_{s\in N}\sum_{d\in N}(w_{mn}^{sd} + \widetilde{w}_{mn}^{sd}) \leq W\, Z_{mn} \qquad (6)$$
$$\forall\, m \in N\,, n \in N_m$$

Constraint (6) ensures that the total number of primary and protection wavelengths on a physical link (m, n) do not exceed the available number of wavelengths on that link.

$$w_{mn} = \sum_{s\in N}\sum_{d\in N}\left(w_{mn}^{sd} + \widetilde{w}_{mn}^{sd}\right) \qquad (7)$$
$$\forall\, m \in N\,, n \in N_m$$

Equation (7) calculates the total number of used wavelengths on the physical link (m, n).

$$u w_{mn}^{sd} \geq b_{mn}^{sd} \qquad (8)$$
$$\forall\, m \in N\,, n \in N_m$$

$$w_{mn}^{sd} \leq M b_{mn}^{sd} \qquad (9)$$
$$\forall\, m \in N\,, n \in N_m$$

$$u\, \widetilde{w}_{mn}^{sd} \geq \tilde{b}_{mn}^{sd} \qquad (10)$$
$$\forall\, m \in N\,, n \in N_m$$

$$\widetilde{w}_{mn}^{sd} \leq M \tilde{b}_{mn}^{sd} \qquad (11)$$
$$\forall\, m \in N\,, n \in N_m$$

Constraint (8) and (9) maps the variable w_{mn}^{sd} to its binary equivalent b_{mn}^{sd}, while constraints (10) and (11) perform the same functionality between the variables $\widetilde{w}_{mn}^{sd}$ and $\tilde{b}_{mn}^{sd}$. M is a sufficiently big number, (10000 used in the model) and (u =10)

$$b_{mn}^{sd} + \tilde{b}_{mn}^{sd} \leq 1 \qquad (12)$$
$$\forall s, d, m \in N, n \in N_m$$

Constraint (12) ensures that the primary and backup paths are path- disjoint.

$$\delta^{sd} = \gamma^{sd} \qquad (13)$$
$$\forall s, d \in N$$

Constraint (13) ensures that if a request is blocked, then its protection path is also blocked.

For the FFR scenarios, the routes are allocated statically by setting the variables (b_{mn}^{sd} *and* $\tilde{b}_{mn}^{sd}$) to their corresponding minimum hop paths.

For the FSTF scenario, the only change is to change the blocking binary variables (δ^{sd} *and* γ^{sd}) to be fraction numbers that range between 0 and 1, to allow for an optimal partial demand blocking.

For the FPPR scenario, the protection paths can be rerouted so the only change in the model is to allow $\tilde{b}_{mn}^{sd}$ to be decided by the model, while not changing the working paths by setting b_{mn}^{sd} to a predetermined value as a parameter.

For the FWPPR scenario, the working and protection paths can be rerouted, which is represented by the general case of the model where (b_{mn}^{sd} *and* $\tilde{b}_{mn}^{sd}$) are both variables.

In previous scenarios, whenever a working demand get blocked its protection path will be blocked as well according to constraint (14), but for the FRDS scenario, the case is different. So we change the equality to:

$$\gamma^{sd} \leq \delta^{sd} \qquad (14)$$
$$\forall s, d \in N$$

IV. Performance Evaluation and Results

We evaluate the models using the NSFNET network which is shown in Fig.2. The NSFNET covers the US and consists of 14 nodes and 21 bidirectional links. Also there are five data centers located at nodes (2, 3, 7, 8 and 9). We used the traffic matrix, which is based on the population-factor-distance (PFD) modelling, that considers the US population and the nodes distances [10]. Also, for traffic types it adopts the cisco VNI forecast [11].

To investigate the network performance, we apply incremental flood volumes (x2, x4, x6, x8 and x10) on a single node at a time and measure the percentage of served traffic flood for the five proposed scenarios.

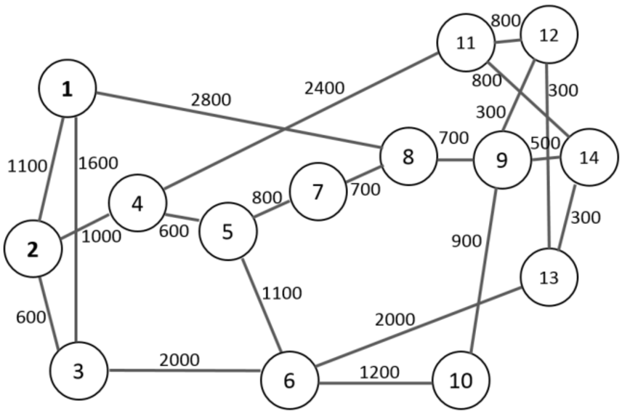

Fig. 2 NSFNET network with link distances in kilometers

Fig.3 shows the percentage of average served floods for different flood sizes for the five suggested scenarios. It is obvious that for floods of up to double the traffic size it can be absorbed fully for all scenarios including the FFR, while for other flood sizes the network starts blocking demands due to capacity exhaustion. The mitigation approaches performs better than normal scenario, as they can absorb more floods and reduce the blocking. FRDS outperforms other scenarios, as the blocking does not exceed 8% for x10 whereas FFR has 33% of blocking.

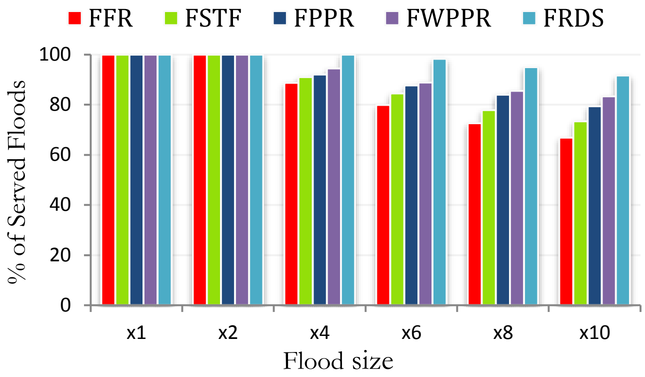

Fig. 3 the percentage of average served floods for different flood sizes for the five scenarios

In the FFR approach, the fixed routing imposed on the floods stops the possibility of rerouting, leading to blocking whenever the floods exploit the available capacity. For the FSTF scenario, the network will block the online gaming, file sharing and VoD that accounts 40% of the whole traffic [10] to allow other important traffic to be served. Eventually, instead of blocking the whole demand it will serve a portion of the demand until the network gets fully utilized.

In FPPR and FWPPR, the percentage of the served traffic is better than the previous two approaches because they reroute and redistribute the traffic in the network for better network utilization and less blocking. In FPPR, the working traffic will not be disrupted while the protection paths will be re-provisioned, whereas in FWPPR, everything will be disrupted to reconfigure the new routes for the working and protection traffic unless SDN technology is deployed. In SDN, the centralized controller will reroute the whole traffic demands in the network to reduce blocking, as the controller has the global view of the network.

Obviously, the FRDS has the ability to eliminate protection resources for a portion of the working traffic. So, 70% of traffic will be served as a best-effort and left to the IP layer restoration service while 30% of traffic is protected in order not to violate the SLA. The elimination of these protection resources will free resources that will be occupied by the floods.

Fig.4 shows the percentage of the average blocked floods of each node for the five scenarios. We see that low traffic nodes (1, 4, 5 and 6) do not suffer from any blocking, while data center nodes blocking exceed 60%.

Fig.5 compares the worst case and the ultimate mitigation approach when the flood volume is x10 of the normal average traffic volume. The FRDS can improve the flood absorption by more than 50%. This value is clearly notable in Fig.6 which shows how node 8, as an example, behaves when increasing the flood size from x1 to x10.

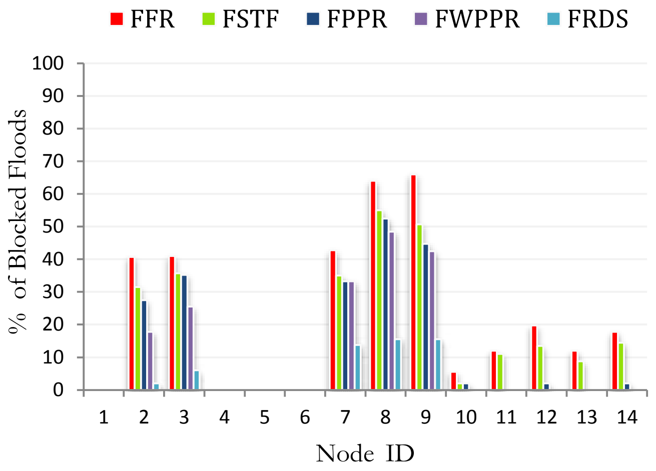

Fig. 4 percentage of average blocked floods of each node for the five scenarios

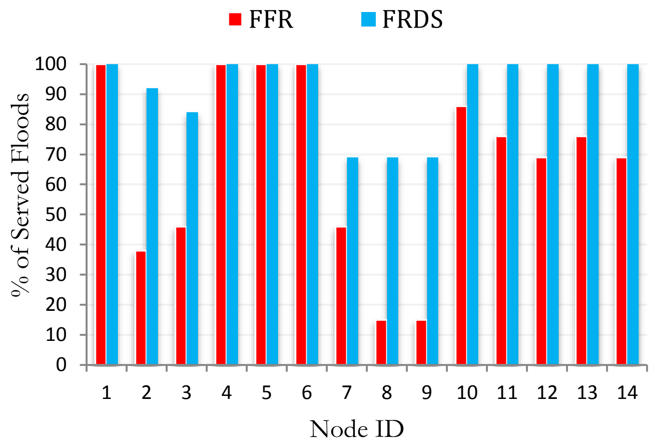

Fig. 5 percentage of served floods for FFR vs. FRDS

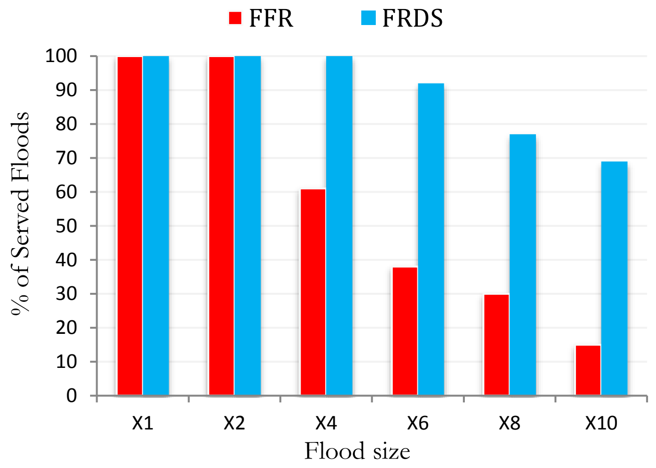

Fig. 6 percentage of served floods at node 8 for FFR vs. FRDS

V. CONCLUSION

In this work we pinpoint a new issue in disaster resilient networks. In specific, we tackled the post-disaster traffic floods in core networks. We have reviewed the possible sources for such a problem. Then we have evaluated the optical network performance under disaster traffic floods and studied how much blocking it will incur. We studied four mitigation scenarios; STF, rerouting and Diff-Serv to absorb the floods. Our approaches can be implemented by ISPs by either adopting one single approach or by combining multiple approaches depending on their existing technologies. The results show that the mitigation approaches can reduce blocking from 66% up to 15% in the worst cases.

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). Zaid H. Nasralla would like to acknowledge his PhD scholarship awarded by the Higher Committee for Education Development in Iraq (HCED) and the University of Karbala.

REFERENCES

[1] M. F. Habib, M. Tornatore, F. Dikbiyik, and B. Mukherjee, "Disaster survivability in optical communication networks," Computer Communications, 2013.

[2] N. UNGERLEIDER. (2013). WHY YOUR PHONE DOESN'T WORK DURING DISASTERS—AND HOW TO FIX IT. Available: http://www.fastcompany.com/3008458/tech-forecast/why-your-phone-doesnt-work-during-disasters-and-how-fix-it

[3] 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.

[4] 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.

[5] K. Fukuda, M. Aoki, S. Abe, Y. Ji, M. Koibuchi, M. Nakamura, et al., "Impact of Tohoku earthquake on R&E network in Japan," in Proceedings of the Special Workshop on Internet and Disasters, 2011, p. 1.

[6] J. M. Simmons, "Optical network design and planning", Springer, 2014.

[7] F. Dikbiyik, M. Tornatore, and B. Mukherjee, "Exploiting Excess Capacity, Part II: Differentiated Services under Traffic Growth," Networking, IEEE/ACM Transactions on, vol. 23, pp. 1599-1609, 2015.

[8] F. Dikbiyik, M. Tornatore, and B. Mukherjee, "Exploiting excess capacity for survivable traffic grooming in optical backbone networks," Journal of Optical Communications and Networking, vol. 6, pp. 127-137, 2014.

[9] Z. H. Nasralla, T. E. El-Gorashi, M. O. Musa, and J. M. Elmirghani, "Energy-Efficient Traffic Scheduling in IP over WDM Networks," in Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on, 2015, pp. 161-164.

[10] K. Hinton, "Traffic modelling for the core network," in GreenTouch Confidential, Feb. 2013.

[11] C. V. N. Index, "Forecast and Methodology, 2014-2019 White Paper, May 27, 2013.