2015 International Conference on Computing, Networking and Communications (ICNC), Workshop on Computing, Networking and Communications (CNC)

Admission Control in Flow-Aware Multi-Topology Adaptive Routing

Jerzy Domżał, *Member, IEEE*, Robert Wójcik, *Member, IEEE*,
Dawid Kowalczyk, Piotr Gawłowicz, Piotr Jurkiewicz, Andrzej Kamisiński

***Abstract*—Flow-Aware Multi-Topology Adaptive Routing (FAMTAR) is a new mechanism which provides the ability to use multiple paths between two points in a network. When the primary path becomes congested, a new path is found and used. However, when all possible paths are congested, new flows are still accepted on one of the congested paths which degrades the observed quality of service. Therefore, in this paper, two admission control mechanisms for FAMTAR are presented and analyzed. The main goal of the algorithms is to restrict new flows' access to congested paths and force them to wait for resources to become available. We propose two different methods to determine whether an available path for a new flow is congested or not. Moreover, we propose a mechanism which assures the transmission of selected flows (e.g. emergency calls) through paths with minimum total delay. The presented analysis shows the advantages of the introduced proposals and allows to estimate the potential gain from using these mechanisms.**

***Index Terms*—Flow-Aware Multi-Topology Adaptive Routing; Flow-Aware Networks; Quality of Service; Admission Control; Congestion Control**

I. Introduction

Internet traffic grows every year significantly. Such trend is also observed in corporate and even private networks where e.g. cloud services become more and more popular. It is predicted that total IP traffic will increase over threefold from 2012 to 2017, reaching 120 exabytes (10^{18} bytes) per month in 2017 [1]. It is very important to ensure proper transmission quality for selected traffic, e.g. for streaming traffic, where too many packet drops or too long delays are not acceptable. Operators usually decide to increase the total capacity of links in their networks rather than to implement quality of service (QoS) mechanisms. Based on the transmission history it is quite easy to estimate the necessary capacities of links. Usually, it is planned that the available throughput should not be consumed totally.

In IP networks, traffic between source and destination nodes is usually sent through one path selected by the routing protocol. Although it is possible to use multi-path transmissions, mechanisms that allow it are usually complex. Therefore, in most cases operators use only two-path load balancing or, like in MPLS, they configure multi-path routing statically, which can be inefficient. In MPLS, usually historical traffic statistics are collected over time and used to determine paths for packets [2]. From time to time large amount of traffic needs to be sent between two nodes in a network. As a result, a path or paths selected for transmission of traffic between such nodes may be congested for a prolonged period. At the same time, other resources may be available and they could be used to send that burst of traffic quicker.

Flow-Aware Multi-Topology Adaptive Routing (FAMTAR) [3] is a mechanism which allows for automatic multi-path transmission in a network. It operates based on measurements performed periodically for each link. When the value of the observed parameter, e.g. the available throughput, exceeds its border value, the cost of such a link is increased to the predefined high value and the link is considered as congested. As a result, the routing protocol tries to find new paths for flows which normally would transmit their traffic through the congested link.

In this paper, we propose and analyze two admission control mechanisms for FAMTAR which limit the number of flows being processed when all paths to the destination node are congested. In the first proposal new flows are rejected when packets are to be forwarded on a congested link. This solution is simple and based on concept used in Flow-Aware Networks (FAN) [4], [5]; however, may be inefficient as traffic is blocked in core. In the second solution, we observe the total cost of a path at the border router and if it exceeds the threshold value, new flows are rejected immediately and not forwarded to the core. Moreover, we define a method to reserve original paths for certain special flows to provide them with best possible quality and availability.

This paper is organized as follows. Section II describes the FAMTAR mechanism. In Section III, the proposed admission control algorithms for FAMTAR are introduced. In Section IV, the results of selected simulation experiments of the admission control algorithms for FAMTAR are presented. Section V concludes the paper.

II. Flow-Aware Multi-Topology Adaptive Routing

The Flow-Aware Multi-Topology Adaptive Routing enables multi-path transmission in IP networks. It was first presented in [3] and analyzed in [6]. Similar concept was also presented in [7] for FAN [8]. In FAMTAR, similarly to currently popular SDN's and other architectures [9], it is assumed that traffic is sent based on flows. Flows can be identified in several ways. We decided to use five fields from packet headers: source and destination addresses, source and destination ports and an

J. Domżał, R. Wójcik, D. Kowalczyk, P. Gawłowicz, P. Jurkiewicz, A. Kamisiński are with the Faculty of Computer Science, Electronics and Telecommunications, Department of Telecommunications, AGH University of Science and Technology, Al. Mickiewicza 30, 30-059 Kraków, Poland (e-mail: domzal@kt.agh.edu.pl).

978-1-4799-6959-3/15/$31.00 ©2015 IEEE

identifier of the transport protocol. The tests results of FAN router where the same method for flow identification is used are presented in [10].

One of the main assumptions of FAMTAR is constant monitoring of traffic in all links in a network. Routers periodically estimate e.g. volume of traffic or delay in outgoing links and if the received values exceed acceptable threshold (max_th) such links are considered as congested. The cost of the congested link is then changed to the predefined high value. The measurements are conducted locally and we do not need to broadcast results to entire network. When the value of the observed parameter drops below the lower threshold (min_th), the cost of such a link is changed again to its previous, original value. After any change of a link cost, a routing protocol performs standard updates in all nodes in the domain.

When the first packet of a new flow arrives at a router, the flow identifier is added to the Flow Forwarding Table (FFT). That packet is routed according to the current routing table state. Routing information (outgoing interface, gateway) for that flow is then remembered in the FFT entry and any further packets of that flow are forwarded according to the routing information stored there. It means that the outgoing interface is selected from the FFT and not from the routing table. Such an operation ensures that packets of a particular flow are always sent through the same path, even when routing table changes. The FFT also stores the arrival time of the last packet for each flow. To keep the FFT as small as possible, the flow identifier is removed from the FFT when the flow inactivity exceeds the fixed threshold. The functionality described above makes the FFT act similarly to a route cache.

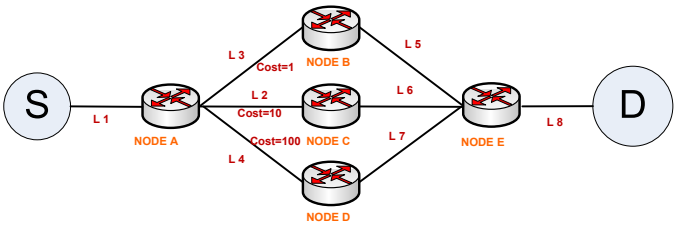

Fig. 1. Traffic service in a network with FAMTAR

Traffic service in a network with FAMTAR is illustrated with the support of Fig. 1. Assume that 100 flows need to be sent from S to D. Firstly, considering given link costs, a routing protocol, e.g. OSPF, selects the lowest-cost path: L1-L3-L5-L8. The throughputs in all links are monitored by the respective routers. The min_th and max_th thresholds are set to e.g. 0.7 and to 0.9, respectively. Also, let us assume that 10 flows are enough to cross the max_th threshold. It means that first 10 flows will be accepted on the primary path. Their traffic will be transmitted through this path based on the FFT content. Next 10 flows will be accepted on the path composed of links L1-L2-L6-L8, because the cost of L2 is greater than cost of L3 and lower than cost of L4. Further 10 flows will be accepted on the path L1-L4-L7-L8. In this moment, the network is fully congested. However, there are 70 flows which want to begin the transmission. Based on the basic FAMTAR assumptions, they will be accepted on the primary path, i.e., L1-L3-L5-L8. This will slow down transmission of 10 flows accepted there first. In this path the available bandwidth will have to be shared by 80 flows. As a result, it may be impossible to establish a voice or video streaming connections. Such a situation is unfavorable in the network. To solve such a problem, usually the admission control algorithms are used. In this paper, we propose two admission control approaches which efficiently deal with the mentioned problem. Also, we define a method to reserve original paths for certain special flows to provide them with best possible quality and availability.

III. Admission Control for FAMTAR

The main goal of the admission control algorithms presented in this section is to restrict new flows' access to congested paths and force them to wait for resources to become available.

The first proposal, called *local AC* is simple and straightforward. It assumes that a router does not accept new flows if they are to be forwarded via a port from which a congested link originates. Therefore, if the routing table indicates an outgoing link, but this link is congested, the packet is dropped and the flow is not added to the FFT. As a result, links in the network are protected against overloading. It needs to be noted that by implementing such a mechanism, less traffic will be served than in the basic FAMTAR. However, with high probability, all accepted traffic will be served with good quality. This approach is very simple, yet it has one disadvantage. Packets may travel through the whole network only to be rejected before entering a bottleneck link. As a result, some bandwidth is unnecessarily consumed which decreases resources available for other transmissions.

The second proposal, called *global AC*, solves the problem described above. In this solution, the FAMTAR routers check the cost of the current path to the destination node in the routing table. If this cost is greater than a predefined maximum path cost, new flows are rejected. As a result, new flows are blocked in the first router on its possible path to minimize the total amount of wasted traffic. Moreover, when there are transit nodes in a network (nodes which do not introduce new traffic), those nodes do not need to provide the admission control functionality. For example, in Fig. 1, a network where only two nodes generate traffic is presented. In such a network the *global AC* algorithm needs to be implemented only in node A and node E. Such a network comprises five nodes; nodes A and E are the border routers (with admission control functionality) whereas nodes B, C and D are the core routers (admission control functionality is not required).

To improve transmission of emergency traffic in a network we also propose an additional mechanism which can be used with both admission control algorithms described above. In this mechanism, it is assumed that the original routing table, i.e., the one when all the links in a network are not congested, is saved in routers' memory. When a router receives the first packet of a special flow it selects the outgoing interface

for this flow based on the original routing table. It ensures that such special flows, which may be e.g. emergency flows, are always accepted immediately on the shortest path, which may be critical to ensure proper performance for such flows. The special flows can be marked by using, e.g. the DSCP (differentiated services code point) field in a packet header. Similar concept was presented for FAN in [11]. In this method, the Static Router Configuration method was employed which assumes that emergency calls are established to emergency centres with statically assigned network addresses. In such a case, which can also be used for FAMTAR, routers need to be configured to treat flows with certain destination addresses as special.

In the following section we present the results of simulation experiments conducted for the IP network and compare them with the ones obtained for such a network with basic FAMTAR and with FAMTAR with two versions of the admission control algorithms.

IV. Performance analysis

In this Section, the results of simulation experiments carried out in the ns-2 simulator are presented. We observed transmission parameters such as: received data, delay, packet loss or the number of flows. The examined network topology is presented in Fig. 2. This is the US backbone network as provided by the SNDlib project [12] (name of the data set: janos-us-ca). The capacity of each link in the network was set to 100 Mbit/s and the delay was set to 1 ms. The results are presented in Fig. 3 and 4 and Tab. I - II for pure IP, basic FAMTAR, FAMTAR with *localAC* and for FAMTAR with *globalAC*.

In the first experiment, TCP traffic was generated in node 0 (Vancouver) and was destined to node 38 (Montreal). 240 simulation runs were performed to observe the parameters listed in Tab I. The duration of each simulation run was set to 250 seconds. The number of background elastic flows activated by node 0 was changed from 200 to 1200 to observe the impact of different volume of traffic on transmission parameters in the network. The traffic was generated with the Pareto distribution for calculating the volume of traffic to be sent by each elastic flow (FTP connections): the mean size of each TCP flow was set to 4 MB and the Pareto shape factor was set to 1.5. The packet size was set to 1000 bytes. The exponential distribution for generating the time intervals between beginnings of transmissions of the TCP flows was used. The flows were sent from the beginning of the simulation run with the mean interval equal to 0.2 s. Additional traffic was generated from the beginning of the simulation between nodes 10-13, 9-12 and 7-11. This traffic consumed 60% of the available bandwidth in these links and was generated to simulate background traffic in these key links. In other links in the network around 40% of the available bandwidth was consumed by background traffic.

In the 70th second we also generated one UDP flow from node 0 to node 38 with the rate of 100 kbit/s and with the packet size of 100 bytes. This flow was treated as an emergency call. It means that it should be accepted as quickly as possible and its packets forwarded via the best possible path. The capacity of access links (with FIFO queues) was set to 1 Gbit/s. The buffers in routers were sized to 1000 packets which is a reasonable value for the analyzed links. The min_th and max_th thresholds in all the links were set to 0.7 and 0.9, respectively. It means that around 80% of the link capacity can be consumed in a link during normal transmission. 95% confidence intervals were calculated by using the Student's t-distribution.

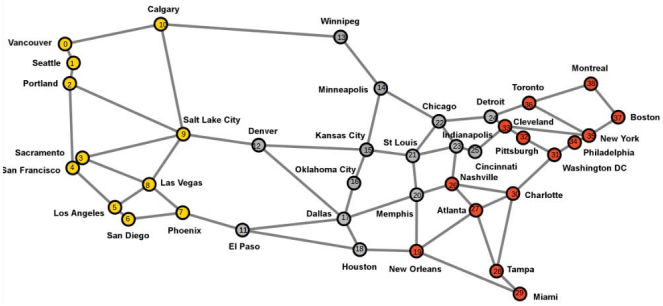

Fig. 2. Network topology - US backbone network

In the second experiment a similar UDP traffic was generated. The results are presented in Fig. 3 and in Tab. II. The inter-arrival times of flows were generated using exponential distribution with mean interval equal to 0.2 s. The volume of traffic to be sent by each UDP flow was generated by Pareto distribution: the mean size of each flow was set to 4 MB and the Pareto shape factor was set to 1.5. Exponential distribution was also used to generate flow rates with mean value equal to 500 kbit/s. The packet size was set to 1000 bytes. As in the previous experiment, an additional traffic was generated from the beginning of the simulation between nodes 10-13, 9-12 and 7-11. This traffic consumed 60% of available bandwidth in these links and was generated to simulate background traffic in these key links. In other links in the network around 40% of available bandwidth was consumed by background traffic. In the 70th second, one additional UDP flow begun to transmit traffic from node 0 to node 38 with rate equal to 100 kbit/s and with packet size equal to 100 bytes. This flow was treated as an emergency call.

The simulation results confirm that the FAMTAR mechanism ensures significantly better transmission parameters than pure IP. For both TCP and UDP traffic much more traffic is sent while packet losses are reduced. For TCP traffic mean packet delay is slightly greater in comparison to IP network. However the differences are not significant. For UDP traffic FAMTAR minimizes mean packet delay. FAMTAR's superiority grows with the increasing volume of traffic. For TCP traffic, the *localAC* or *globalAC* algorithms additionally minimize packet losses and delays. For UDP transmissions, delays are similar in each case of the analyzed FAMTAR network. However, *globalAC* significantly reduces packet losses. This is the effect of the path selection mechanism, which can reject new flows on entering the domain.

Obviously, when FAMTAR with *localAC* or *globalAC* is

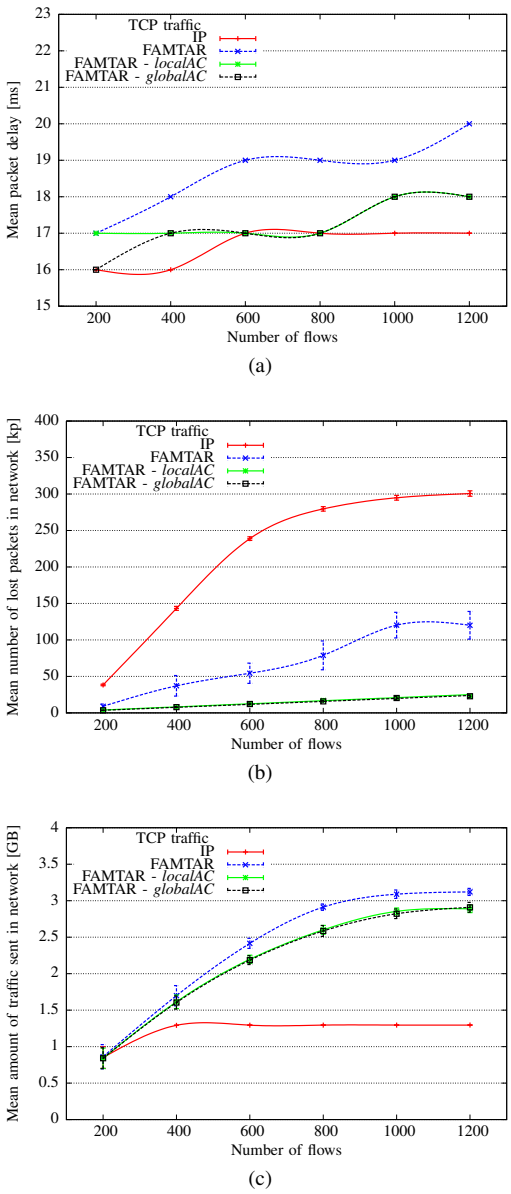

Fig. 3. FAMTAR transmission performance in a network with TCP flows.

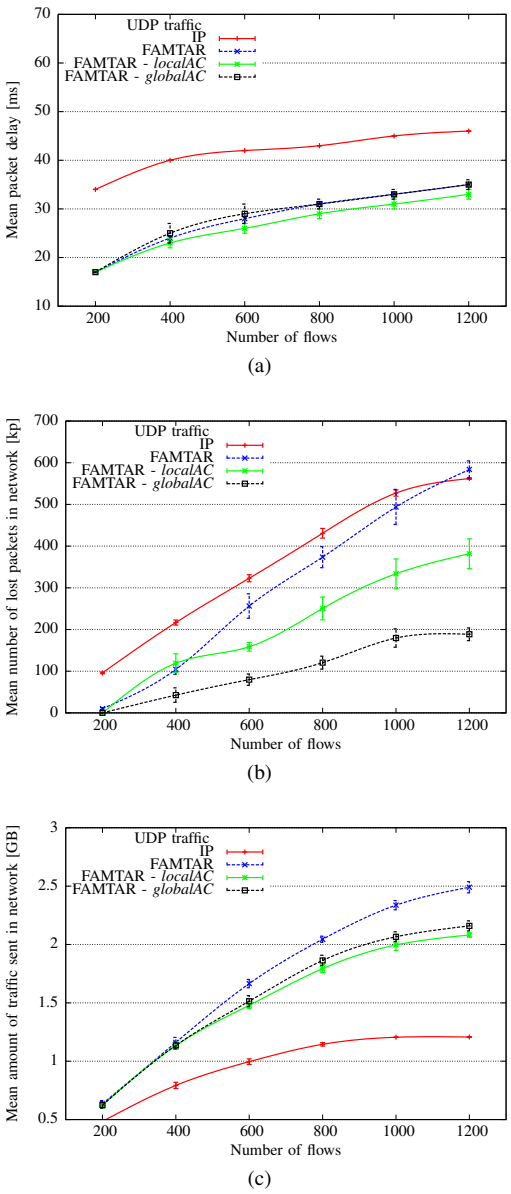

Fig. 4. FAMTAR transmission performance in a network with UDP flows.

used, the amount of traffic sent in the network is lower in comparison to basic FAMTAR. This is the effect of blocking some flows when paths are congested. However, the differences are not significant and still much more traffic is sent than in the basic IP network. Moreover, due to the limitation of the flow number served, better transmission parameters are observed. In Tab. I and in Tab. II, one can see that in FAMTAR with admission control the number of flows in links 10-13, 9-12 and 7-11 is similar, while in basic FAMTAR or original IP, significantly more flows are served in node 10. It is also worth to note that in FAMTAR with or without admission control, paths are a bit longer than in the original IP network: the mean number of hops is greater. However, it does not have any observable negative impact on transmission parameters. Both versions of the admission control algorithms also decrease the acceptance delay for emergency calls, which is an important advantage of the proposed approaches.

The results presented in this section are consistent with our predictions and show that the proposed admission control algorithms ensure favorable transmission parameters.

V. Conclusion

Flow-Aware Multi-Topology Adaptive Routing provides multi-path transmission of traffic in the IP network. As shown in this paper, it is possible to significantly increase the amount of data sent in a network, especially when unexpected traffic needs to be served. As a result, the transmission costs can be minimized while proper transmission parameters are still ensured.

In this paper, three admission control mechanisms for FAMTAR are presented. The *localAC* and the *globalAC* allow

TABLE I
NETWORK PERFORMANCE COMPARISON FOR TCP TRAFFIC

Parameter	**IP**	**FAMTAR without admission control**	**FAMTAR with *localAC***	**FAMTAR with *globalAC***
Data sent [GB]	1.47 ± 0.01	3.23 ± 0.04	2.91 ± 0.05	2.93 ± 0.07
Data received [GB]	1.29 ± 0.01	3.12 ± 0.05	2.89 ± 0.05	2.91 ± 0.07
Packets dropped in core [10^3]	300.64 ± 3.74	120.09 ± 18.96	22.76 ± 1.64	22.80 ± 1.76
Number of flows in node 7	0	20.19 ± 6.48	15.71 ± 1.59	15.08 ± 2.05
Number of flows in node 9	0	77.95 ± 25.48	14.98 ± 1.58	16.26 ± 2.32
Number of flows in node 10	470.49 ± 7.67	167.70 ± 33.13	16.75 ± 1.50	16.31 ± 1.28
Mean packet delay [ms]	17 ± 1	20 ± 1	18 ± 1	18 ± 1
Mean hop number	11	12.80 ± 0.10	13.16 ± 0.06	13.01 ± 0.18
Mean acceptance delay of emergency call [ms]	25 ± 5	27 ± 4	17 ± 5	18 ± 4

TABLE II
NETWORK PERFORMANCE COMPARISON FOR UDP TRAFFIC

Parameter	**IP**	**FAMTAR without admission control**	**FAMTAR with *localAC***	**FAMTAR with *globalAC***
Data sent [GB]	3.32 ± 0.04	3.32 ± 0.04	3.32 ± 0.04	3.32 ± 0.04
Data received [GB]	1.21 ± 0.01	2.49 ± 0.05	2.08 ± 0.02	2.16 ± 0.04
Packets dropped in core [10^3]	562.13 ± 2.01	583.84 ± 20.62	381.79 ± 35.80	188.57 ± 15.30
Number of flows in node 7	0	43.89 ± 1.38	46.51 ± 1.80	49.57 ± 2.96
Number of flows in node 9	0	60.34 ± 4.77	49.23 ± 3.04	52.33 ± 2.96
Number of flows in node 10	201.07 ± 2.41	104.18 ± 5.41	53.64 ± 2.89	55.06 ± 4.07
Mean packet delay [ms]	46 ± 1	35 ± 1	33 ± 1	35 ± 1
Mean hop number	11	14.59 ± 0.10	15.03 ± 0.15	14.84 ± 0.32
Mean acceptance delay of emergency call [ms]	788 ± 366	384 ± 290	49 ± 47	42 ± 19

to minimize the packet delay and packet losses in a network. They also ensure that much more traffic can be served in a network in comparison to classical IP. The *globalAC* allows to obtain better results, especially for UDP traffic. The superiority of *globalAC* comes from the fact that packets are discarded before they enter the network. This solution requires path cost lookup for new flows instead of checking the congestion status of the outgoing link on which *localAC* is based. The former requires careful link's cost planning so that FAMTAR does not confuse an uncongested path with high basic cost with a congested one. The additional mechanism proposed for both admission control algorithms ensures that special traffic such as e.g. emergency calls is immediately accepted in the network with FAMTAR on the best available path.

The admission control algorithms for FAMTAR proposed in this paper meet the requirements of modern networks and may be used in the Future Internet.

ACKNOWLEDGEMENTS

The research was carried out with the support of the project "Flow-Aware Multi-Topology Adaptive Routing" founded by the National Centre for Research and Development in Poland under the LIDER programme.

REFERENCES

[1] CISCO, "Cisco Visual Networking Index: Forecast and Methodology, 2012–2017," 2013, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf.

[2] S. Lahoud, G. Texier, and L. Toutain, "FATE: a polynomial time framework for flow allocation in MPLS-TE networks," in *The 14th IEEE Workshop on Local and Metropolitan Area Networks. LANMAN 2005*, pp. 1–6.

[3] R. Wojcik, J. Domzal, and Z. Dulinski, "Flow-aware multi-topology adaptive routing," *IEEE Communications Letters*, vol. 18, no. 9, pp. 1539–1542, Sept. 2014.

[4] A. Kortebi, S. Oueslati, and J. Roberts, "Cross-protect: implicit service differentiation and admission control," in *IEEE HPSR 2004*, Phoenix, USA, Apr. 2004.

[5] J. Domzal, R. Wojcik, A. Jajszczyk, V. Lopez, J. Hernandez, and J. Aracil, "Admission control policies in flow-aware networks," in *11th International Conference on Transparent Optical Networks, 2009. ICTON '09.*, June 2009, pp. 1–4.

[6] R. Wojcik, J. Domzal, Z. Dulinski, P. Gawlowicz, and D. Kowalczyk, "Performance evaluation of Flow-Aware Multi-Topology Adaptive Routing," in *IEEE CQR International Workshop*, Tucson, USA, May 2014.

[7] J. Domzal, "Intelligent Routing in Congested Approximate Flow-Aware Networks," in *IEEE Globecom 2012*, Anaheim, USA, December 2012.

[8] S. Oueslati and J. Roberts, "A new direction for quality of service: Flow-aware networking," in *NGI 2005*, Rome, Italy, April 2005.

[9] R. Wójcik and A. Jajszczyk, "Flow Oriented Approaches to QoS Assurance," *ACM Comput. Surv.*, vol. 44, no. 1, pp. 5:1–5:37, Jan. 2012.

[10] J. Domzal, J. Dudek, P. Jurkiewicz, L. Romanski, and R. Wojcik, "The cross-protect router: implementation tests and opportunities," *IEEE Communications Magazine*, vol. 52, no. 9, pp. 115–123, Sept. 2014.

[11] A. Jajszczyk and R. Wojcik, "Emergency Calls in Flow-Aware Networks," *IEEE Communications Letters*, vol. 11, pp. 753–755, Sept. 2007.

[12] S. Orlowski, R. Wessaly, M. Pioro, and A. Tomaszewski, "SNDlib 1.0 — Survivable Network Design Library," in *NET*, vol. 55, May 2010, pp. 276–286.