Impact of Nodal Centrality Measures to Robustness in Software-Defined Networking

Tomas HEGR, Leos BOHAC

Department of Telecommunications, Faculty of Electrical Engineering,
Czech Technical University in Prague, Technicka 2, 166 27 Prague, Czech Republic

tomas.hegr@fel.cvut.cz, bohac@fel.cvut.cz

Abstract. *The paper deals with the network robustness from the perspective of nodal centrality measures and its applicability in Software-Defined Networking (SDN). Traditional graph characteristics have been evolving during the last century, and numerous of less-conventional metrics was introduced trying to bring a new view to some particular graph attributes. New control technologies can finally utilize these metrics but simultaneously show new challenges. SDN brings the fine-grained and nearly online view of the underlying network state which allows to implement an advanced routing and forwarding. In such situation, sophisticated algorithms can be applied utilizing pre-computed network measures. Since in recent version of SDN protocol OpenFlow (OF) has been revived an idea of the fast link failover, the authors in this paper introduce a novel metric, Quality of Alternative Paths centrality (QAP). The QAP value quantifies node surroundings and can be with an advantage utilized in algorithms to indicate more robust paths. The centrality is evaluated using the node-failure simulation at different network topologies in combination with the Quality of Backup centrality measure.*

Keywords

Centrality, network robustness, OpenFlow, software-defined networking, topology.

1. Introduction

The concept of Software-Defined Networking (SDN) revealed countless new possibilities in the area of packet forwarding in data networks, packet handling and network security. Even though the concept is oriented to the network control centralization, it does not mean that the network reliability, i.e. provided service availability, is automatically decreased. The view of the events in the network and the online accessibility of the traffic statistics gives a possibility to install forwarding rules (also referred as matching rules) with respect to variety network measures. One of the network areas which can be improved at the flow level is a host-to-host communication reliability, i.e. the installed network path resilience, which is important for mission-critical applications.

In SDN, a host-to-host communication path is, usually, established via installation of engineered rules into network nodes along the path. Considering the OF protocol, these rules are usually installed in a reactive way, when the controller needs every time to evaluate the given traffic pattern. To keep the packet latency low, it is necessary to provide rules as fast as possible. An SDN application has to compute a network path keeping a low latency which can be challenging especially in complex networks. First and very understandable way is to optimize the SDN applications built up to the controller to reach the low latency of the network path computation. Another way is to provide pre-computed measures to these algorithms, and so reduce the problem complexity or increase quality of results.

In this paper, we focus on the path robustness in terms of the aforementioned communication reliability and node failure resilience. It is generally true that path protection is better than path restoration from the latency view. In the OF area of SDN, the protection can be realized via the set of equal matching rules with different execution priority and dissimilar output action. The same can be simply established thanks to the *Group Table* architecture and the *fast failover* feature included in recent versions of the OF specification [7]. In such case, the first forwarding action is executed from a set of actions at which the output port is alive for the particular flow in OF. Since the management of rules itself is demanding, there must be assured proper expressiveness, efficiency and correctness, and it should be utilized an appropriate framework as for example is FatTire [14] by Reitblatt et al.

Although the technical means are already available to implement the protected path, the issue with right path selection in complex networks still remains. This is particularly important in high-demanding low-latency networks where the connection protection is vital. We suggest utilizing a graph centrality measures during the path generation process to solve the issue. The graph centrality concept is well known in graph theory and from the area of social network analysis. In the next sections we present and evaluate new centrality named Quality of Alternative Paths (QAP). The centrality reflects an average fitness of node's alternative paths and thus it can be used not only during the path generation process but also for network analysis. The evaluation of the centrality measure impact to network robustness is done through the node failure simulation together with the another centrality measure called Quality of Backup published by Shavitt and Singer in [18].

2. Related Works

The mechanism of failure recovery was in general extensively investigated from the beginning of the telecommunication age. In the area of SDN and particularly OF, there have been published several papers on this topic in recent years. Beside the FatTire [14] framework, there was presented a runtime system for emulating controller flow installations allowing programmers to implement failure-agnostic code in [8]. The way of handling high controller load during a failure in the network and the appropriate fast restoration algorithm were proposed in [15] by Sharma et al. The authors showed in [17] that using the *Group Table* and two well-known mechanisms of failure recovery, i.e. restoration and protection, the sub-50 ms recovery latency can be achieved at carrier-grade networks. Since the results are encouraging the authors showed in [16] that the OF in-band control, thus utilizing same channel for both control and payload traffic, remains problematic from the latency viewpoint. The optimized controller placement and control-traffic routing can greatly improve the SDN architecture resilience as is presented in [3].

The node degree is one of the basic centrality metrics in graph theory. While it simply shows the node's elementary attribute, it could not encompass all information about the node's surroundings. Therefore, many new metrics were introduced targeting to particular node's attribute such as closeness, betweenness and others [5]. The centrality measures describing network robustness were introduced in [18] where authors describes two new centrality measures, Quality of Backups and Alternative Path Centrality (APC). While QoB is a normalized centrality, APC quantify the topological contribution of a node to the network functionality in graph-individual way. Beyond these robustness centrality measures, even other measures were also as, for example, advanced compound length-constrained Connectivity and Rerouting Centrality (l-CRC) designated for wireless sensor networks [19].

To evaluate the impact of centrality measures to the path robustness, we decided to apply the node failure simulation. This method is well-known, and it was frequently used for describing relations between nodes and graph components in complex networks in famous work [1]. Focusing particularly on network robustness several papers were published by Manzano et al. In [10], the authors present a robustness analysis of real-world network topologies under different failure scenarios. These scenarios are divided into Static and Dynamic node impairments. Likewise, there were published works analyzing contemporary data-center topologies in [9] and in [6]. As the Static random failure test shows to be one of the most useful simulation test it was selected as a counterexample to our targeted static node failure simulation described in section 4.

Topologies for the QAB metric evaluation were chosen from several different networking areas. The random graphs have been obtained using three models Erdos-Renyi [4], Watts and Strogatz as the small-world representative [20] and Barabasi-Albert as the scale-free one [2]. Traditional random graphs have been supplemented with real-world carrier-grade networks accessible at the SDNlib project [13].

3. Centrality Measures

In this section, we describe the graph theory background and two centrality measures. The first is QoB and the second is the newly proposed QAP.

3.1. Graph Theory Background

Every communication network can be represented by a graph $G = (V, E)$ where V is a set of nodes and E is a set of edges. Every pair of two connected nodes are said to be adjacent. A walk of length k between any two nodes $(u, v) \in V$ is a sequence of edges $e_1 e_2 ... e_k$ such that e_i and e_{i+1} are adjacent. If we denote the walk from u to v in k steps as $u \xrightarrow{k} v$ than the distance $\delta(u, v) = \min\{k | u \xrightarrow{k} v\}$ is the length of the shortest path in an unweighted graph. By convention, $\delta(u, v) = \infty$ if there does not exist a walk from u to v and $\delta(u, u) = 0$. If we look for a shortest path from u to w bypassing node v, i.e. the path is not going through the node v, we denote such distance $\delta_v(u, w)$. Both centrality measures involve this vital function.

Moreover, both measures QAP and QoB use specific node sets to express the node centrality. The set of nodes adjacent to node v are called neighbors of node v and similarly $N_G(v) = \{u \in G | (v,u) \text{ or } (u,v) \in E\}$ is named the neighborhood of v. Then the set $C_v = \{u \in G | (v,u) \in E\}$ is the set node v's direct children, thus nodes accessible through v, and the set $P_v = \{u \in G | (u,v) \in E\}$ is the set node v's direct parents. It is clear that in undirected graphs sets P_v and C_v are equal.

3.2. Quality of Backup

The Quality of Backup centrality introduced in [18] quantifies backup efficiency of a given node by examination the cost of re-routing paths from the set of parents to the set of children. The expression Eq. (1) shows the QoB function capturing the backup efficiency:

$$\rho(v) = \frac{\sum\limits_{u \in P_v} \sum\limits_{w \in C_v} \frac{1}{\max\{\delta_v(u,w) - 1, 1\}}}{|P_v| \cdot |C_v|}. \quad (1)$$

QoB describes node's dispensability in the given graph in the normalized way, thus $\rho : V \rightarrow [0,1]$, and so is possible to compare different graphs between each other. If a node with perfect backup $\rho = 1$ fails, the network functionality is not reduced. In this case, neither the network connectivity nor the path lengths in the network are affected. On the contrary if $\rho = 0$ the node has no backup.

3.3. Quality of Alternative Paths

While QoB gives a comprehensive centrality measure in terms of node backup quality using the path lengths, it does not consider number of such alternative paths, thus the number of those paths bypassing the evaluated node. The presented Quality of Alternative Paths centrality is a complementary measure to QoB dealing with this gap. This auxiliary centrality measure provides additional information when analyzing network robustness or generating paths in a network.

The QAP has been inspired by QoB as can be seen in expression Eq. (2). In this expression, it is used a newly defined function α_v which assigns a weight to the connections in $P_v \times C_v$, i.e. the connections between all parent and child nodes. This weight takes into account number of alternative paths and consequently it can be used to prioritize nodes with higher load-balancing potential avoiding bottlenecks in case of the evaluated node failure. The final QAP value is given as the average weight of all alternative paths:

$$\eta(v) = \frac{\sum\limits_{u \in P_v} \sum\limits_{w \in C_v} \alpha_v(u,w)}{|P_v| \cdot |C_v|}. \quad (2)$$

$$\alpha_v(u,w) = \begin{cases} 1 & \text{if } \delta_v(u,w) = 0 \\ \sum\limits_{p \in D} \frac{1}{\delta_v(u,w)} & \text{else} \\ 0 & \text{if } \delta_v(u,w) = \infty \end{cases}. \quad (3)$$

The newly proposed weight function α expressed in Eq. (3) has the following rationale. Every node-disjoint path between the given parent's node and child's node bypassing the examined node contribute to the total weight by the reverse value of the path's length. This is valid if the nodes are connected, else the weight is 0. In case $u = w$, the weight is 1 to keep the proper η average value. In the α expression, only contribution of node-disjoint paths is considered. Such approach gives the number of effective alternative paths, and it prefers better node connectivity. The set of node-disjoint paths between given nodes from P_v and C_v in Eq. (3) is marked as D. An example network is shown in Fig. 1.

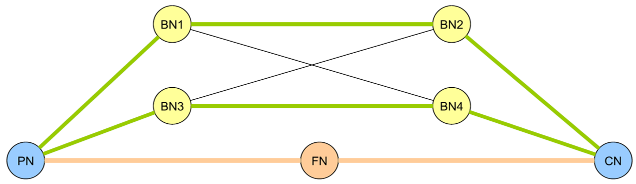


Fig. 1: An example scenario with two node-disjoint paths bypassing node FN between nodes PN and CN going through BN nodes.

The transmission latency is, usually, introduced by interconnecting nodes along the transmission path nowadays. QAP was designed to prefer the shorter length of the path to the number of paths in order to prioritize lower latency. This characteristic is obvious from Fig. 2. In case the parent's node and the child's node are directly connected, the path weight is 1, consequently QAP for all nodes in Full graph reaches 1.

Even though in today's conventional networks links have assigned cost or weight, in QAP we consider only two aforementioned graph properties, number of paths and the path's length, and the application only on unweighted graphs. This can be modified by extending α function by adding an appropriate cost variable according to the chosen network environment.

The basic version of the algorithm for QAP computation is written below in Alg. 1 in form of pseudocode. All failover shortest paths are stored in list marked $\bar{\delta}_v$. These paths are found by BFS algorithm. According to Menger's theorem [11] the minimum vertex cut between two given nodes is equal to the maximum

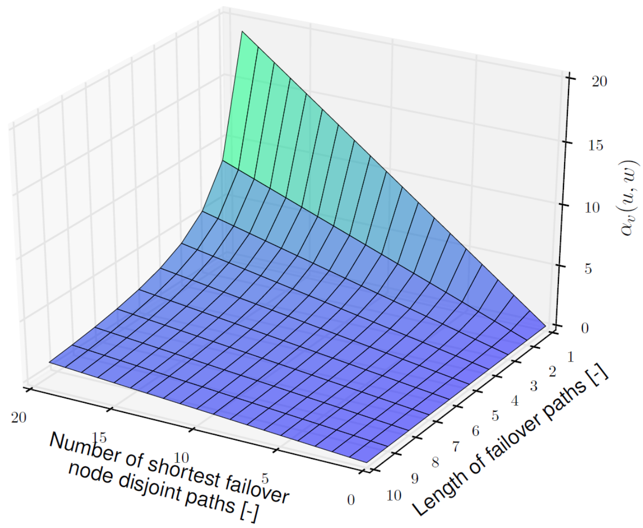


Fig. 2: Model of α_v function showing the relation between lengths and number of shortest failover node-disjoint paths. It shows steep increase of the weight for shorter paths, i.e. preferring shorter paths to number of paths.

number of pairwise node-independent paths between them. This can be done in $O(|V|^3)$. In our approach, the node-disjoint failover paths are found from a set of all shortest failover paths between given nodes by the process of iterative removing most node-intersect paths until no node intersections are present.

Algorithm 1 QAP centrality pseudocode.

function QAP(v,G)
$\eta \leftarrow 0$
for u **in** P_v **do**
$\bar{\delta_v}(u) \leftarrow BFS_v(u, G, allpaths)$
for w **in** C_v **do**
$\bar{\delta_v}(u,w) =$ Find D for w in $\bar{\delta_v}(u)$
if $\delta_v(u,w) = 0$ **then**
$\eta \leftarrow \eta + 1$
else if $\delta_v(u,w) \neq \infty$ **then**
$\eta \leftarrow \eta + |\bar{\delta_v}(u,w)|_{\frac{1}{\delta_v(u,w)}}$
$\eta \leftarrow \frac{\eta}{|P_v||C_v|}$

4. Centrality Evaluation

This section describes the impact of complementary centrality measures QoB and QAP to the network under the static node-failure simulation. Since the usability proof of centrality measures by following all paths in the network during the failure simulation would be exceedingly complex, we decided to apply static failure simulation known from topology robustness tests as was mentioned in section 2. In the evaluation, we use All Terminal Reliability (ATR) [12] as a pointer to the beginning and the end of evaluation interval which described later. We compare network diameter D, average shortest path length δ and total count of all shortest path in the network at both simulation scenarios in the evaluation interval.

Selected topologies and a set of computed classical robustness characteristics is listed in Tab. 1. All topologies were constructed as undirected and unweighted graphs.

The simulations were performed in two different scenarios. The first is Static Random node-failure simulation (RS) which was repeatedly evaluated to reach desired confidence level of 95 %. The second is Targeted Static node failure simulation (TS). The TS simulation is based on the value of QoB and QAP measures. The higher priority is assigned to QoB in TS since it is the preferred path robustness to quality of alternative paths. QAP is used as a complementary criterion. TS simulations were carried out in descending order of QoB and on the second place in ascending order of QAP. This means that nodes are removed from the less-significant one with the worst quality of alternative paths to the best one. We assume that better results of TS in observed graph parameters give a presumption for usability of QoB and QAP in the selection of more resilient paths with higher quality of alternative paths.

The evaluation interval is in this paper defined as the difference in portion of removed nodes at the moment the ATR falls down under 1 for the first time during the node removing process in both scenarios. This means the moment when the evaluated graph is unconnected for the first time during the simulation run. Since RSs were carried repeatedly, we focused on the average portion of removed nodes. All numbers of removed nodes are expressed as the portion of removed nodes to the total number of nodes in the graph.

The comparison of both simulation scenarios was done at the begging of the evaluation interval (RS removed nodes) and in the mid-interval. Even though, it was possible to analyze also the end of the evaluation interval, the results were not relevant in most cases because of the small residual graph size.

An example histogram showing distribution of QAP for the nobel-eu is depicted in Fig. 3. In this particular case, all QAP values are in the range from 0.45 to 0.75. This is because most nodes have similar nodal degree. The colored plot of the topology is shown in Fig. 4, where the colors match to the computed QAP values. The QAP value has no upper bound and can be significantly higher at different topologies.

The results are presented in the form of percentage comparison between TS and RS scenarios at the begging and in the mid-interval. The first part is the diameter comparison depicted in Fig. 5 which is an important graph parameter giving information about

Tab. 1: Main characteristics of constructed graphs. First three are random graphs with 400 nodes and similar average nodal degree close to 12. Their names are as follow: ern400d12 for Erdos-Renyi, swn400d12 for Watts and Strogatz and ban400d12 for Barabasi-Albert. The rest of graphs is based on real-world telecommunication topologies from SNDlib project [13].

Characteristic	ban400d12	ern400d12	swn400d12	geant	germany50	india35	nobel-eu	norway	pioro40
$\|V\|$	400	400	400	22	50	35	28	27	40
$\|E\|$	2379	2381	2400	36	88	80	41	51	89
Diameter	3	4	4	5	9	7	8	7	7
Average shortest path length	2.16	2.68	2.68	2.53	4.05	2.94	3.56	3.13	3.31
StdDev	0.44	0.59	0.58	0.99	1.75	1.25	1.65	1.47	1.48
Average nodal degree	11.90	11.91	12.00	3.27	3.52	4.57	2.93	3.78	4.45
StdDev	22.31	3.53	3.17	1.70	1.05	1.69	0.86	1.19	0.50
Maximum degree	183	27	24	8	5	9	5	6	5
Minimum degree	6	3	4	2	2	2	2	2	4
Edge density	0.03	0.03	0.03	0.16	0.07	0.13	0.11	0.15	0.11
Edge per vertex	5.95	5.95	6.00	1.64	1.76	2.29	1.46	1.89	2.23
Heterogeneity	0.09	0.01	0.01	0.11	0.04	0.06	0.05	0.06	0.02

Tab. 2: Observed moments when the ATR falls below 1 for the first time in the simulation run and the mid-interval between those moments at TS and RS.

Topology	TS removed nodes [%]	RS removed nodes [%]	Mid interval [%]
geant	72.7	28.9 ± 1.9	50.8
germany50	52.1	19.1 ± 1.0	35.6
india35	62.9	32.5 ± 1.6	47.7
nobel-eu	22.2	18.5 ± 1.0	20.3
norway	44.4	29.0 ± 1.1	36.7
pioro40	47.5	33.1 ± 1.3	40.3
ern400d12	74.8	50.2 ± 2.6	62.5
ban400d12	97.8	46.4 ± 3.5	72.1
swn400d12	69.3	53.0 ± 3.3	61.1

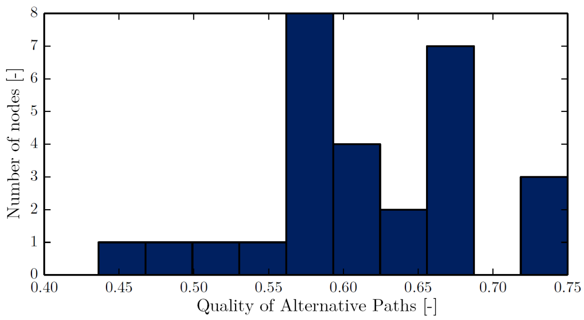


Fig. 3: An example QAP distribution for the nobel-eu topology. Since the topology is not excessive and nodal degree of most nodes is similar the histogram shows low values of QAP up to 0.75.

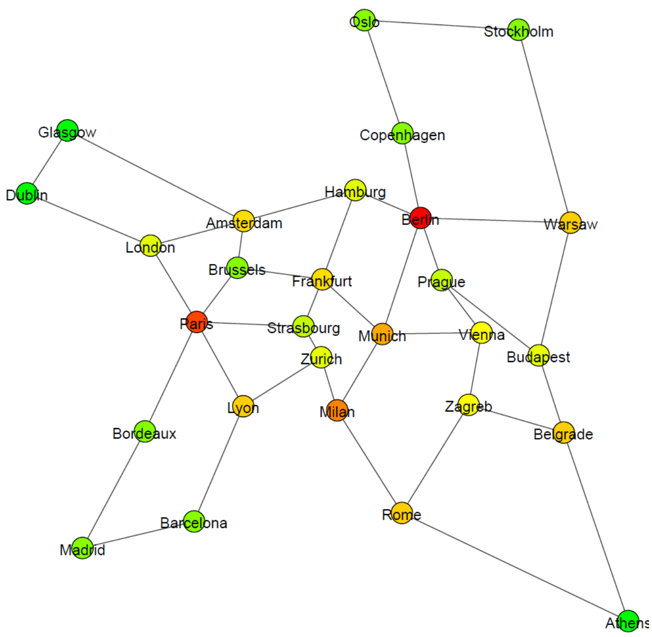
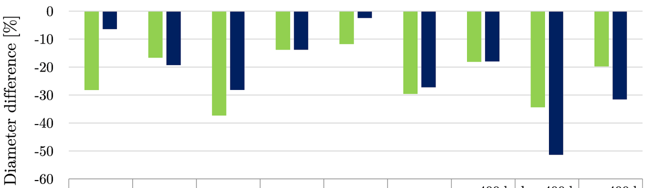


Fig. 4: The plotted nobel-eu topology shows QAP values depicted in Fig. 3. The color range from green to red represents QAP values in range from 0.45 to 0.75.

maximum path lengths in the graph. Results show that the TS scenario gives in almost all cases smaller graph diameter especially at the begging of the interval, where the improvement reaches almost 52 % in case of ban400d12. The state in the mid-interval is unbalanced at real-world showing that engineered topologies are in case removing higher number of unimportant nodes degrade considerably faster.

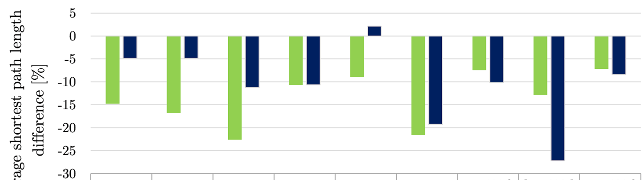
The second observed characteristic is the average shortest path length which gives another information about path lengths to diameter. The results depicted in Fig. 6 almost correlate in many cases with results for di-



	geant	germany 50	india35	nobel-eu	norway	pioro40	ern400d 12	ban400d 12	swn400d 12
D start	-28,2	-16,7	-37,3	-13,8	-11,8	-29,6	-18,1	-34,4	-19,8
D mid	-6,4	-19,3	-28,2	-13,8	-2,4	-27,2	-18,0	-51,4	-31,6

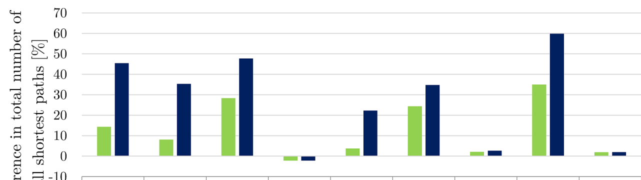
Fig. 5: The bar chart shows a percentage difference in graph diameter between RS and TS for evaluated topologies. The TS shows that diameter at all cases is smaller up to 52 % as in case of ban400d12 in the mid-interval.

ameter. Values reach 23 % shorter paths in case of the india35 topology at the begging of the interval that is lower than the improvement at graph diameter. Higher improvement than india35 reaches again random graph ban400d12 at 27 %. One can observe more significant reduce of improvement in case of randomly generated graphs. This is highly probably due to the different graph structure than at the engineered real-world telecommunication topologies. The improvement drop is most significant at norway network in mid-interval as in the case of diameter.



	geant	germany 50	india35	nobel-eu	norway	pioro40	ern400d 12	ban400d 12	swn400d 12
ASPL start	-14,7	-16,8	-22,6	-10,6	-8,9	-21,6	-7,4	-12,9	-7,1
ASPL mid	-4,8	-4,8	-11,2	-10,6	2,1	-19,2	-10,2	-27,2	-8,4

Fig. 6: The value of average shortest path length shows roughly the same results as in case of diameter. The percentage difference reaches up to 23 % for india35 topology at the beginning of the evaluation interval and 27 % for ban400d12 in the mid-interval.



	geant	germany 50	india35	nobel-eu	norway	pioro40	ern400d 12	ban400d 12	swn400d 12
TSP start	14,3	8,1	28,3	-2,2	3,7	24,4	2,1	34,9	1,9
TSP mid	45,5	35,3	47,8	-2,2	22,3	34,8	2,6	59,8	2,0

Fig. 7: Total number of all shortest paths shows the positive impact of evaluated centrality measures especially in mid-interval. The TS gives in several cases from 30 % to 40 % more paths.

The last characteristic reflecting the impact of QAP is the total number of all shortest paths between all pairs of nodes. Results depicted in Fig. 7 show that the general improvement is predominantly in mid-interval. More paths exist between nodes more possibly the path protection can be implemented. While the improvement for average path lengths for norway network was negative in mid-interval, in case of the total number of all shortest paths is gives more than 22 % better results in the same interval. The opposite trend shows nobel-eu and also random graphs. The total number of paths for TS reaches up to 60 % in case of ban400d12 random graph and keeps above 20 % in half of all real-world topologies.

5. Conclusion

The SDN era brings new possibilities to the network control also covering the path protection by failover mechanism. The application built at top of the SDN controller can now take into account a plethora of statistics and network state information during the generation of forwarding rules for a particular path while preserving it more robust. Moreover, these applications are enabled to use the surplus computing capacity available in data centers and run optimization algorithms to obtain advanced and complex measures there. Such measure can help to construct paths with higher resilience to the node or link failure in complex networks.

In this paper, we suggest using centrality measures for the path protection purpose: Quality of Backup complemented by the newly proposed Quality of Alternative Paths. These centrality measures describe paths bypassing a particular failed network node. The impact of these measures was demonstrated by the method of Static failure simulation.

It was performed random static node-failure simulation and targeted static node-failure simulation taking into account both centrality measures. The simulations were carried out on three different random graphs and six real-world telecommunication topologies. The results show that on undirected and unweighted graphs targeted simulation can give better results up to tens of percent for graph diameter, average path length and also for total number of all shortest paths in case of the massive node failure.

The simulations can be in the future work extended to follow and quantify the impact of centrality measures to every single path between all node pairs. Moreover, the proposed metric can be improved to consider weights of links.

Acknowledgment

This work was supported by Students grants at Czech Technical University in Prague

SGS13/200/OHK3/3T/13 and by grant of Ministry of the interior of the Czech Republic number VG20132015104.

References

[1] ALBERT, R., H. JEONG and A.-L. BARABASI. Error and attack tolerance of complex networks. *Nature*. 2000, vol. 406, iss. 6794, pp. 378–382. ISSN 0028-0836. DOI: 10.1038/35019019.

[2] BARABASI, A.-L. and R. ALBERT. Emergence of scaling in random networks. *Science*. 1999, vol. 286, no. 5439, pp. 509–512. ISSN 0036-8075. DOI: 10.1126/science.286.5439.509.

[3] BEHESHTI, N. and Y. ZHANG. Fast failover for control traffic in Software-defined Networks. In: *2012 IEEE Global Communications Conference (GLOBECOM)*. Anaheim: IEEE, 2012, pp. 2665–2670. ISBN 978-1-4673-0920-2. DOI: 10.1109/GLOCOM.2012.6503519.

[4] BOLLOBAAS, B. *Modern graph theory*. New York: Springer, 1998. ISBN 0-387-98488-7.

[5] BRANDES, U. On variants of shortest-path betweenness centrality and their generic computation. *Social Networks*. 2008, vol. 30, iss. 2, pp. 136–145. ISSN 0378-8733. DOI: 10.1016/j.socnet.2007.11.001.

[6] COUTO, R. S., M. E. M. CAMPISTA and L. H. M. K. COSTA. A reliability analysis of datacenter topologies. In: *2012 IEEE Global Communications Conference (GLOBECOM)*. Anaheim: IEEE, 2012, pp. 1890–1895. ISBN 978-1-4673-0920-2. DOI: 10.1109/GLOCOM.2012.6503391.

[7] OpenFlow 1.2. In: *Open Networking Foundation* [online]. 2011. Available at: `https://www.opennetworking.org`.

[8] KUZNIAR, M., P. PERESINI, N. VASIC, M. CANINI and D. KOSTIC. Automatic failure recovery for software-defined networks. In: *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*. New York: ACM Press, 2013, pp. 159–160. ISBN 978-145032056-6. DOI: 10.1145/2491185.2491218.

[9] MANZANO, M., K. BILAL, E. CALLE and S. U. KHAN. On the Connectivity of Data Center Networks. *IEEE Communications Letters*. 2013, vol. 17, iss. 11, pp. 2172–2175. ISSN 1089-7798. DOI: 10.1109/LCOMM.2013.091913.131176.

[10] MANZANO, M., J. L. MARZO, E. CALLE and A. MANOLOVAY. Robustness analysis of real network topologies under multiple failure scenarios. In: *2012 17th European Conference on Networks and Optical Communications*. Vilanova i la Geltru: IEEE, 2012, pp. 1–6. ISBN 978-1-4673-0949-3. DOI: 10.1109/NOC.2012.6249941

[11] MENGER, Karl. Zur allgemeinen Kurventheorie. *Fundamenta Mathematicae*. 1927, vol. 10, iss. 1, pp. 96–115. ISSN 0016-2736.

[12] NEUMAYER, S. and E. MODIANO. Network Reliability With Geographically Correlated Failures. In: *2010 Proceedings IEEE INFOCOM*. San Diego: IEEE, 2010, pp. 1–9. ISBN 978-1-4244-5836-3. DOI: 10.1109/INFCOM.2010.5461984.

[13] ORLOWSKI, S., R. WESSALY, M. PIORO and A. TOMASZEWSKI. SNDlib 1.0-Survivable Network Design Library. *Networks*. 2009, vol. 55, iss. 3, pp. 276–286. ISSN 0028-3045. DOI: 10.1002/net.20371.

[14] REITBLATT, M., M. CANINI, A. GUHA and N. FOSTER. FatTire: Declarative fault tolerance for software-defined network. In: *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*. New York: ACM Press, 2013, pp. 109–114. ISBN 978-145032056-6. DOI: 10.1145/2491185.2491187.

[15] SHARMA, S., D. STAESSENS, D. COLLE, M. PICKAVET and P. DEMEESTER. Enabling fast failure recovery in OpenFlow networks. In: *2011 8th International Workshop on the Design of Reliable Communication Networks (DRCN)*. Krakow: IEEE, 2011, pp. 164–171. ISBN 978-1-61284-124-3. DOI: 10.1109/DRCN.2011.6076899.

[16] SHARMA, S., D. SAESSENS, D. COLLE, M. PICKAVET and P. DEMEESTER. Fast failure recovery for in-band OpenFlow networks. In: *2013 9th International Conference on the Design of Reliable Communication Networks (DRCN)*. Budapest: IEEE, 2013, pp. 52–59. ISBN 978-1-4799-0049-7.

[17] SHARMA, S., D. STAESSENS, D. COLLE, M. PICKAVET and P. DEMEESTER. OpenFlow: Meeting carrier-grade recovery requirements. *Computer Communications*. 2013, vol. 36, iss. 6, pp. 656–665. ISSN 0140-3664. DOI: 10.1016/j.comcom.2012.09.011.

[18] SHAVITT, Y. and Y. SINGER. Beyond Centrality - Classifying Topological Significance Using Backup Efficiency and Alternative Paths. In: *6th International IFIP-TC6 Networking*

Conference. Atlanta: Springer Berlin Heidelberg, 2007, pp. 774–785. ISBN 978-3-540-72605-0. DOI: 10.1007/978-3-540-72606-7_66.

[19] SITANAYAH, L., K. N. BROWN and C. J. SREENAN. Fault-Tolerant Relay Deployment Based on Length-Constrained Connectivity and Rerouting Centrality in Wireless Sensor Networks. In: *9th European Conference, EWSN 2012.* Trento: Springer Berlin Heidelberg, 2012, pp. 115–130. ISBN 978-3-642-28168-6. DOI: 10.1007/978-3-642-28169-3_8.

[20] WATTS, D. J. and S. H. STROGATZ. *Nature.* vol. 393, iss. 6684, pp. 440–442. ISSN 0028-0836. DOI: 10.1038/30918.

About Authors

Tomas HEGR received his M.Sc. in computer science at the Czech Technical University in Prague in 2012. He participate in teaching activities at the department of telecommunication engineering. His research interests involves industrial networks based on Ethernet and Software-Defined Networking in all research areas.

Leos BOHAC received the M.Sc. and Ph.D. degrees in electrical engineering from the Czech Technical University, Prague, in 1992 and 2001, respectively. Since 1992, he has been teaching optical communication systems and data networks with the Czech Technical University, Prague. His research interest is on the application of high-speed optical transmission systems in a data network.