Indonesian Journal of Electrical Engineering and Computer Science
Vol. 20, No. 2, November 2020, pp. 845~853
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v20.i2.pp845-853

Robustness metrics for optical networks

Noor Aishah Zainiar[1], Farabi Iqbal[2], ASM Supa'at[3], Adam Wong Yoon Khang[4]
[1,2,3]School of Electrical Engineering, Universiti Teknologi Malaysia, Malaysia
[4]Faculty of Electrical and Electronic Engineering Technology, Universiti Teknikal Malaysia Melaka, Malaysia

Article Info

Article history:

Received Feb 10, 2020
Revised Apr 12, 2020
Accepted Apr 26, 2020

Keywords:

Centrality metrics
Functional metrics
Optical networks
Robustness metrics
Structural metrics

ABSTRACT

Telecommunication networks are vulnerable towards single or simultaneous nodes/links failures, which may lead to the disruption of network areas. The failures may cause performance degradation, reduced quality of services, reduced nodes/links survivability, stability, and reliability. Therefore, it is important to measure and enhance the network robustness, via the use of robustness metrics. This paper gives an overview of several robustness metrics that are commonly used for optical networks, from the structural, centrality and functional perspectives.

Corresponding Author:

Farabi Iqbal,
School of Electrical Engineering,
Universiti Teknologi Malaysia,
81310 Johor Bahru, Malaysia.
Email: alfarabi@utm.my

1. INTRODUCTION

The study based on robustness is carried out to provide significant insight into the potential damage towards optical network and to support the future communication needs. Robustness is the ability to maintain performance under adverse conditions [1], making it possible to sustain the network efficiency and reliability without performance degradation against the effect of random failures [2] or predicted failures [3]. Robustness also provides a qualitative estimation of reliability when analyses are performed in standard conditions [4]. Robustness metrics are methods or approach to measure and indicate the network performance under certain conditions such as uncertainty, expected conditions or range of scenarios [5]. It is important to have a good understanding of robustness and expressing it quantitatively. Under specific scenarios, robustness metrics can represent various network parameters, though there might be other variations that would not be captured by such approach [6]. Network robustness has drawn many attentions in recent years where the failure of many real-world network causes economic losses in the past [7]. Network robustness can be defined and measured in many ways [8, 9], and there are many ways to achieve communication networks robustness, e.g., by planning the network based on users' requirements, the network physical and logical designs, network configurations, hardware installations and ongoing maintenance.

Optical networks serve as the backbone infrastructure for modern telecommunication networks where it offers to solve many problems in terms of network performance and quality of services and provides enormous data transmission capacities for various important services. Optical networks exchange terabytes of information in a second, thus offer high bandwidth [10]. By providing high data rates, any failure in the optical networks can cause loss of data which in turn will cause revenue loss and loss of sensitive information [11]. There are many network components of which their failure can cause the failure of node or link connection such as switches, optical fibers, and network transceivers. It is of utmost importance that the robustness and survivability is considered as an important aspect of role in ensuring that our optical networks

are as reliable as possible, to mitigate the failure of network services in various failure scenarios [12]. Thus, defining reliable network is vital against any network failures especially for those networks supporting mission critical services [13, 14]. An optical network consists of a number of nodes and fiber links, and some network nodes may be more vital in ensuring network connectivity and acceptable level of network services, compared to other network nodes. Hence, suitable metrics are needed to evaluate the robustness [7] of these nodes and fiber links. In this paper, we review several robustness metrics that are often used in the context of optical networks. Section 2 discusses works that are related to this paper, Section 3 describes the network robustness, Section 4 describes various types of robustness metrics, and Section 5 concludes the paper.

2. RELATED WORKS

Unwanted network failures can cause loss of significant amount for voice and data traffic [15]. Especially when new technologies are being developed, new concerns were also raised [16]. For example, when the network environment become more vulnerable, network operators must respond correspondingly "to maintain the network survivability from any failure risks in the future. The scientific communities believed that optical networks are highly exposed to massive failures and disruptions, mainly caused by natural disasters or human intervention [3, 17]. Researchers have studied how to provide network protections without degrading the network performance. However, whether these measures can properly evaluate the network robustness and which aspects of network robustness these measures can evaluate are still an open question [7].

Robustness metrics can be defined as classical metrics and contemporary metrics [18, 19]. Both classical and contemporary approach are useful for analyzing network connectivity under node/link removals. Heuristic algorithms were proposed in [20] for optimizing four robustness metrics, namely the algebraic connectivity, the effective resistance, the average edge betweenness, and efficiency in order to study the robust growth through generalized meshes. Three categories of robustness metrics were discussed in [1, 21], namely the structural, centrality and dynamic/functional metrics. Structural metrics is based on graph theory, centrality metrics is based on node/link importance and functional metric is related to the quality of services in the established connections [1, 18, 22]. Robust networks can be identified by relating to metrics used under simulated failure scenarios [18]. These (multiple) failures can be either static or dynamic [1, 22]. Static failures are one-off, affecting one or more elements at any given moment, while dynamic failures have a temporal dimension and can further be classified as targeted, epidemic or cascading multiple failures [1, 22]. The temporal evolution in telecommunication network and its connectivity have rapidly increase over time which introduce large size of disturbance and failures. There are four (4) real backbone over temporal sequence of nodal interactions studied in [23] with twenty metrics to measure the robustness and the trends.

Vulnerabilities are defined as the weakness in any network that can be exposed to being attacked or harmed. Vulnerabilities cause low reliability performance requirements, massive disruptions of services, security breaches or attacks, high data transfer rate but with poor configurations, low quality of services, poor disaster-resilience and survivability. Defending networks against vulnerabilities provides network survivability, where survivability can be defined as the ability of maintaining a tolerable quality of service and meet essential requirements when network failures occur [13, 24, 25]. There are two common approaches in ensuring network survivability, which are protection and restoration [24, 26]. Protection involves reserving backup resources before any failure can take place [26], while restoration utilizes unoccupied network resources are not pre-reserved to overcome failures [26]. Resilience in networks (ResiliNets) [27] merge several strategies, disciplines and principles to enhance network survivability and resiliency. ResiliNets axioms provide systematic resilience and comprises a strategy named D2R2+DR mainly used in inner control loop for a system to rapidly adapt to challenges and attacks maintaining an acceptable service level, and in outer control loop for longer term system evolution.

3. ROBUSTNESS METRICS

A common problem in addressing network robustness is what aspect or method should be considered for improving the network robustness. Different metric leads to different notion of robustness notion, since the main purpose of these different metrics is to assert alternative understanding of network robustness. Robustness metrics are used for stability, where the measured quality not necessarily be affected by changing conditions [28]. We consider that robustness metrics can be divided into three main categories, namely structural metrics, centrality metrics and functional metrics.

3.1. Structural metrics

Structural metrics are the most well-known metrics which focus on classical graph analysis and properties. They explain the network stability, vulnerability of network, absence of network or even reliability of the network when some links or nodes are removed from the network topology [1]. To identify the robustness of networks, the measures should be sensitive to changes in networks. The node degree describes the number of neighbours a node has. Moreover, the links that on average connected to the node is known as average nodal degree. The bigger the average nodal degree, the network is said to become more robust. [22]. More connections can be established when the average nodal degree is said to be robust but can lead to a great number of failures if a node with a high nodal degree fails. Node degree also has limited measurements for network robustness since it depends on how the nodal degree is spread over the graph [29].

The edge connectivity of a network is the number of edges whose removal disconnects the network. A k-edge-connected graph suffers disconnection only after k or more edges are removed. A MILP shielding method was proposed in [30] for critical links between geographical or general failure models to increase the edge connectivity of node pair. The proposed method is used to minimize the shielding cost and guarantee the source-destination pair connection. Another approach is to equip the network and its nodes with some methods to rearrange the network resources and services on a partially damaged network to mitigate disasters. [27] introduced swarm intelligence distributed algorithms, that focus on the devices' ability to recover network roles such as gateway or relay, automatically selects its roles, to maximize the end-to-end performance.

Algebraic connectivity is defined as the measure of breaking to network into different network components. If higher number of link or node failures can be survived before the network becomes disconnected, there is a higher chance that network is more robust [1, 31]. [32] proposed survivability based on algebraic connectivity for analyzing network cost and traffic loss. The proposed approach is analysed on three different schemes with different ratios, namely unprotected, shared path protection and 1+1 protected, leading to reduced traffic loss and improved robustness in topological features [31].

Reliability Polynomials (G) stated in [30] are based on the notion of graph connectivity to define the network robustness. The authors explained that all-terminal reliability has always a polynomial, thus it is easier to measure efficiently certain areas for all-terminal reliability. Every all-terminal reliability has its own roots and bounded. The authors proposed that node reliability of any connected graph has nonreal root, unbounded and the closure of the collection of node roots is the whole networks which node reliability identify the difference of the real root of node reliability and all-terminal reliability.

In [33] proposed a metric called the Minimum Total Failure Removals (MTFR) to quantify the network robustness by defining a single failure can cause a failure to all nodes as a Total Failure. The author discussed the failures from the removal of nodes and edges in the networks as Node-MTFR and Edge-MTFR respectively which disrupted the interdependency between power grid and communication networks. The results using the proposed metric are said to be interdependent if the state of network A dependent on the state of network B and vice versa. The result of unidirectional dependencies can be solved in polynomial time. However, the bidirectional dependencies result in failing the network communications.

Path diversity metrics and enhanced analytical resilience network describe in [34] to measure network resilience with unpredictable environment. The authors explained a path diversity features to assess vulnerability by measuring similarities for links and nodes using graph. The path diversity features aim to determine the aggregation of path diversities from a selected set of paths with a given node pair. Lastly, the authors geographical diversity through predicted distances between node pairs is crucial to measure the parameter to model area-based challenges. In [35] addressed the vulnerability level of geographical networks to natural disasters or human-made disasters. The authors proposed a Worse-Case Cut metric in bipartite graph by modelling the physical topology in which links and nodes are geographically located on a plane. The result of the disaster shown in a vertical line in a bipartite graph by discarding all the intersected links. Mixed Integer Linear Programming (MILP) model is created to determine the Worse-Case cut that intersected the links, and lower bound model is created to find the worst-case cut in a bipartite graph.

Physical topology design of optical networks is said to be NP-hard problem and normally solved by using heuristics or metaheuristics method. In order to improve network performance [36] and cost, the authors [37] presented p-Gabriel graphs heuristics-based with three different physical topologies of backbone networks. The authors chose to use Barabási-Albert (BA) method to create the networks since BA is weak against attacks in node but robust in random node failures. The proposed methods with the scenarios are correspond with the defined failure strategies which are Random removal and Degree-based removal. After a node is removed, the size of the largest connected component of the remaining network is calculated. The results explained that p-Gabriel produced robust networks in BA method. Symmetry ratio metric as discussed in [38] is to identify the robustness of network against targeted attack on nodes. The metric introduced is to define that the normal and abnormal circumstances are treated as less or more to the attacker.

3.2. Centrality metrics

Centrality Metrics are defined to classify which properties in the network can be central or important. Furthermore, centrality metrics assist in differentiate information very quick, prevent failures and defending any breakdown in the network [1, 22]. These metrics are also explained that the centralization of network as a measure of how much central node is in relation among other nodes. The main element of a network is centralization. The centralization is to identify differences between the centrality of the most central node and other nodes. In general, if the network has more nodes with similar centrality values, the network is more vulnerable when the centrality metrics are used in order to select the best centrality [22].

Betweenness centrality is a measure that is linked to the number of paths and flow in the network [39]. A specified node will get the shortest paths after they are counted while travelling. A connected node with small number of other nodes is then said to be has a high betweenness centrality. Previous research believed that the nodes are act as bridges between groups of other nodes has high betweenness centrality [1]. When a link that connected to a node with the highest betweenness centrality is removed, it will interrupt the flow of the topologies or graph or reroute it through a longer direction. This is where the betweenness centrality metrics are addressed to evaluate the changes in and therefore be used to identify the critical locations that may directly, or indirectly connected to the high betweenness values. The neighbourhood of the bridges between the nodes that have high betweenness values may also disrupted if any link is removed or break [28, 39]. [23] studied the Chilean Internet Backbone after the disaster hits the Chile. The authors proposed an efficient in determining the right place to add links in the network to prevent any single node or link failure, which is indirectly enhance the network robustness. The metrics used are edge betweenness centrality, the number of links cut sets and node Wiener impact (NWI) which applied in biconnected backbone networks. Therefore, the authors have proposed Variable Neighborhood Search Meta-Heuristic to add extra links until it reaches network robustness.

In [33] proposed random-walk betweenness centrality. In general, the random-walk betweenness of a vertex i is equal to the number of times that a random walk starting at s and ending at t passes through i along the way, averaged over all s and t. This is suitable for a network because until it finds its target, the information will move about randomly. However, it also includes many paths that are not optimal. Therefore, we can consider the random-walk betweenness and the shortest-path betweenness are two different methods that have their own advantages. One with the idea of not knowing where it is going while the other have the capabilities of knowing precisely its target. They can be useful in some real-world situations while others, can still be utilized but not significantly. Moreover, it may be beneficial to compare the prediction of the measures to differentiate them better in the recent cases as we need to explore more about the mode of information propagation in the network to produce a substantial assessment about them both.

Closeness centrality is also having the same criteria as betweenness centrality, which is linked with the number of paths. The centrality of the node is determined by how near a node is to the other nodes. Some previous research defined closeness centrality is to measure the mean distance from the node to all other nodes [6]. To be exact, it is based on the closest distance or path between a specified node and all other nodes [1]. The most important in closeness centrality is which node is close to all the other nodes when certain conditions are required in the network which is much faster than other non-close nodes [1, 39].

Discriminative Closeness centrality [35] as addressed by the authors explained the shortest paths length in the graph between different vertices. The paper discussed not only on a general term of addressing the discriminative closeness centrality, but the paper explained distance-based network indices which include discriminative closeness, discriminative path length, average discriminative eccentricity and discriminative vertex connectivity. The authors used random and exact algorithms to proposed and analyse the metric's indices. Moreover, the authors measure the proposed metrics with real-world applications by link prediction to indicate the likelihood of the vertices. The results using random algorithm produced a very precise estimation value of average discriminative path length and average discriminative eccentricity.

In Degree centrality, a node may be alone, but mostly a node has neighbours surrounding it which is vital for measurement of its centrality. It is the simplest measure for centrality of the node and identified by the number of neighbours connected to a node. Previous research believed that the node is to become the most significant if the degree is very high. However, if a node with high nodal degree is failed, consequently it might affect the overall network connections [1]. A redundancy network is presented in [37] to maintain the survivability of the networks against the large-scale failures which may result in connectivity issues of any nodes of the networks. The redundancy is use for backup resources which by mean to improve fault tolerance whenever the primary resources is unavailable due to the disaster. Another similar approach but with new method is presented in [40] to identify ways in reducing the network failures. The method applied immunization strategies to determine the total number of affected connections. Two methods are presented by using heuristic-based link prioritization; one is built in betweenness centrality concept and another is link criticality to improve the network resilience.

3.3. Functionality metrics

Availability is associated with reliable network that the probability of network operations or network services will be ready at any time [25] since network traffic and communication in optical networks deal with high data transfer rate have complex network infrastructure [30]. Path Geodiversity considered in [41] is to enhance the Availability in the network services and believed to be disaster resilient. The authors discussed the value of Distance (D) has related to geodiversity, which assumes that a disjoint pair or routing paths is defined for each source-destination pair of nodes, and must be separated by a minimum distance, D. The authors addressed the problem using arc-based formulation in non-linear programming model and proposed Integer Liner Programming (ILP) model heuristic-based with the replacement of non-linear limitations. Two networks are used to evaluate the results. The first network is set to a realistic network design test and second network is used in large-scale DWDM networks. Therefore, the solutions to improve the performance are defined between the non-ILP based heuristic and ILP based heuristic. Next, [42] studied the relationship between fragility of existing Internet and the notion of maximum flow reliability. The study focused on availability of connections with the existing simultaneous nodes and link failures and proposed path diversification metrics to instantly apply on the both node pairs in improving network resilience. The proposed algorithm is choosing the best subset of available paths to reduce failures and maximally diverse the connection. The authors concluded the proposed metrics are correlated to both graph theories and survivability of networks.

The average two-terminal reliability (ATTR) [43, 44] is defined as the probability on connectivity that focuses on a node pair which are randomly selected. ATTR is the number of node pairs in every connected component divided by the total number of node pairs in the network. ATTR also gives the fraction of node pairs that are connected to each other. At failure scenarios, the higher the average two-terminal reliability is, the higher the robustness is [1]. Failure Rate (FR) is vary over time as it is defined as the number of failures encountered and predicted for a network component by a total number of components' operating time [14]. Mean Time To Repair (MTTR) is described as the time required to recover and maintenance repair for the failures. It mainly involves repairing hardware devices [45]. Mean Time Between Failures (MTBF) is the mean time expected between failures, measured in hours. For constant failure rate systems, MTBF is the inverse of the Failure Rate. The failure rate of MTBF should be as low as possible, especially for mission critical systems [14, 45]. Mean Time to Failure (MTTF) is the mean time expected before the first failure of a network component. It is meant to be the mean over a long period of time and many units. MTTF is non-repairable system in measuring reliability [14, 45]. Failure in Time (FIT) is another way of reporting MTBF. It produces a report that show a total number of expected failures per billion hours of operation for a network component.

Functional metrics which are also known as Dynamic Metrics [1] are used to measure the network performance which produce varies response to failure during the simulation or real-time network events. Moreover, functional metrics are more focus on the Quality of Service (QoS) parameters (e.g., packet loss, throughput, jitter, delay) of the successful connections. Quantitative robustness metrics are defined that determined the number of blocked connections [19, 29]. It is analysed how an impairment of any possible situations such as in static random, static target, dynamic epidemical, or dynamic periodical can affect the established connections. This metric helps to determine the number of blocked connections in every time step they are analysed [29]. To differentiate the topologies that may not have the same number of connections that should have been established in the same time step, this metrics will play its role in each time step to identify the blocked connections. In [29] the metrics analysed on how an impairment of any possible situations such as in static random, static target, dynamic epidemical, or dynamic periodical can affect the established connections. To differentiate the topologies, this metric will play its role in obtaining the normalized values of average shortest path length, where normalizing the values will correspond the magnitude of increase or decrease of the average shortest path length.

In [27] reviewed problems on large-scale failures in backbone networks with a time varying probabilistic model. The probabilistic model is to determine the survivability of the network and prevent disruption effect. In [42] proposed a scheme to provide protection method from any impact of disaster, estimates the probability of failure, and reroute the traffic if the traffic has potential to fail. In [46] has proposed polynomial-time algorithms in order to detect all the spatially-close segments [47] or different fibers due to high risk in simultaneously failing of network connections. The research mainly focuses on the closeness of each node and link. The authors have also proposed exact algorithm also can be used to identify small number spatially-close fibers groups and measure network robustness. Additionally, the authors [3] taking the importance of geographical information of nodes and links which also consists of the notion of time and a risk profile of the area in embedded network. In [24] proposed reliability-sustainable survivability (RSS) scheme to recover any disrupted services or even no failure in post-disasters event but the reliability decreases beyond expected threshold. The scheme uses a heuristic algorithm and mixed integer

linear programming (MILP) model to conduct routing and distribution of resources respectively. Each link is organized in bidirectional with allocated with bandwidth capacity on every direction. Meanwhile node is given full wavelength conversion capability. A connection for a node pair is organized with a single path with different scenarios, some will experience wavelengths before a disaster and disrupt the communication between the node pair. RSS is believed to achieve performance satisfaction in providing reliable connection and recover any required traffic flow and prevent connection loss.

Preventive Rerouting Threshold [7] is to enhance the protection models and promote adaptability in providing efficiency of the network communications. The authors addressed that any path has a high failure probability than the value of PRT will cause a problem to any other path that has lower PRT value. Therefore, the authors suggested the PRT to provide rerouting of the available path that has the least probability value in failure. The proposed metric helps to reduce huge potential damage on the path since the rerouting helps to indicate the impacted area that will cause failure. In [39] has further discussed on the PRT and provide self-adapting rerouting parameters by deploying average failure probability from lowest to highest failure rate in various scenarios. The network topologies are studied under the Multiprotocol Label Switching (MPLS) [48] networks and with four different locations. The adaptabilities in using PRT increase the efficiency of network and reduced the number of failure connections compared without using PRT. The PRT has provide the self-adaptive protection in selecting the best path by rerouting against the failure areas.

Preprovisioning reserves dedicated-link-protected wavelengths on each of the link for future connection. [23] proposed preprovisioning algorithm to define complexity when the traffic increases and more connections soon to arrive. The algorithm exploited the use of three metrics in order to provide protection and backup reprovisioning. The metrics used in this paper are Connection Setup Time (ST), Protection Switching Time (PST) and lastly Availability. The use of ST in this paper was to segregate the primary path and one or more paths that are assigned to be the backup paths should receive a request to initiate connection. PST is used to switch from primary path to any backup path if any node or link from the primary path is failed. The authors proposed Excess Capacity (EC) method to improve the PST and availability to reserve capacity and reduce the connection ST with mixed-protection schemes and the results show availability performance is better than PST and ST from preprovisioning for any network capacity. Re-provisioning provide recovery method for post-disaster event since the optical networks are exposed with multiple failures and large-scale threats. In [47] discussed that there are two important elements need to be considered in guarantee the network connectivity and maximizing traffic flow. [49] uses three disaster re-provisioning schemes that focus on connection rerouting and block degradation of bandwidth. The three re-provisioning schemes are no-degradation provisioning (NDR), degradation-as-needed re-provisioning (DAN) and fairness-aware degradation re-provisioning (FAD). The mixed integer linear program (MILP) is used for these three-disaster scheme applied on two mesh topologies. The authors considered three performance measures to investigate the network survivability, i.e.; the connection loss ratio (CLR), traffic loss ratio (TLR) and fairness factor (FF). Results show that DAN and FAD achieved optimal CLR performance without rerouting but CLR improved with the use of NDR scheme and rerouting method. The three re-provision schemes can increase the TLR performance on FF with rerouting method on the available connections.

In [36] explained risk is the expected value of undesirable result from any event. The author proposed Disaster Risk-Aware Provisioning (D-RAP) to improve the Service Level Agreement (SLA) in minimizing penalty paid made by the network operator to the customers in case of disaster. The Risk defined as R to identify the elements that contributes the risk analysis and state the Disaster Risk-Aware Provisioning with Integer Linear Programming approach for 1+1 dedicated protection. The paper has also discussed the probability of a disaster that are disaster-dependent in order to measure the probability level of the damage. The authors used NSFNet topology and assumed fiber links are close to highways with the US seismic hazard map. The connections are provisioned over link-disjoint primary and backup path with 1+1 protection. In [30] studied the network survivability in static network planning. The authors used Disaster Risk-Aware Provisioning to reduce from the state has existing failures into the state of no failure case. The probabilistic risk model is introduced to define loss or penalty based on given set of possible disasters, in which focus only the physical locations of the network devices and the distances of defined disaster. Number of protection path can also be extended to more than two [50].

4. CONCLUSION

In this paper had discussed the importance of robustness in optical networks, especially in improving reliability and survivability of the network. This paper has discussed the overview of the robustness metrics in optical networks which mainly focus on structural, centrality and functional metrics. Various robustness metrics can be developed in the future in the context of optical networks.

ACKNOWLEDGEMENTS

This work was supported by Ministry of Higher Education Malaysia (MOHE) and the administration of Universiti Teknologi Malaysia through Institute Grant vote number 05G27.

REFERENCES

[1] D. F. Rueda, E. Calle and J. L. Marzo, "Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements," *Journal of Network and Systems Management*, vol. 25, no. 2, pp. 269-289, 2017.
[2] A. Beygelzimer, G. Grinstein, R. Linsker and I. Rish, "Improving network robustness," in *Proceedings of the International Conference on Automatic Computing (ICAC'04)*, pp. 322-323, 2004.
[3] F. Iqbal and F. Kuipers, "Spatiotemporal risk-averse routing," *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKKSHPS)*, pp. 395-400, 2016.
[4] E. Aguilera, R. Lucena, S. Ca´rdenas, M. Valca´rcel, E. Trullols and I. Ruisa´nchez, "Robustness in qualitative analysis: A practical approach," *TrAC Trends in Analytical Chemistry*, vol. 25, no. 6, pp. 621-627, 2006.
[5] C. McPhail, H. R. Maier, J. H. Kwakkel et.al "Robustness metrics: How are they calculated, when should they be used and why do they give different results?" *Earth's Future*, vol. 6, no. 2, pp. 169-191, 2017.
[6] J. Liu, M. Zhou, S. Wang and P. Liu, "A comparative study of network robustness measures," *Frontiers of Computer Science*, vol. 11, no. 1, pp. 568-584, 2017.
[7] J. L. Marzo and E. Calle, *Robustness against large-scale failures in communications networks: A simulation approach*, Budapest: Universitat de Girona, 2017.
[8] M. Manzano, E. Calle and D. Harle, "Quantitative and qualitative network robustness analysis under different multiple failure scenarios," *Int. Congress on Ultra Modern Telecom. & Control Systems & Workshops*, 2011.
[9] N. K. Olver, "Robust network design," Doctoral dissertation, McGill University Library 2010.
[10] K. Kaushik, "Application to determine optimized path for network robustness," *Conference: 4th International Conference on Image Processing and Pattern Recognition (IPPR 2018)*, pp. 159-167, 2018.
[11] R. Ramaswami, K. N. Sivarajan and G. H. Sasaki, *Optical networks*, USA: Morgan Kaufmann, 2010.
[12] D. R. B. Ara´ujo and C. J. A. Bastos-Filho, "Robustness of physical topologies of optical networks created by variants of gabriel graphs," In *2017 IEEE 18th International Conference on High Performance Switching and Routing (HPSR)*, pp. 1-6, 2017.
[13] X. Zhang, X. Wang, X. Jiang and S. Lu, "Degree of network damage: A measurement for intensity of network damage," In *2014 19th European Conference on Networks and Optical Communications*, pp. 140-146, 2014.
[14] C. Panda, S. N. Patro, P. K. Das and P. K. Gantayat, "Node reliability in WDM optical network," *IJCSI International Journal of Computer Science Issues*, vol. 9, no. 2, pp. 315-320, 2012.
[15] L. Hoang, M. Pontecorvi, R. Dathathri, G. Gill, B. You, K. Pingali and V. Ramachandran, "A round-efficient distributed betweenness centrality algorithm," In Proceedings of the 24th Symposium on Principles and Practice of Parallel Programming, pp. 272-286, 2019.
[16] U. Demsar, O. Spatenkova and K. Virrantaus, "Centrality measures and vulnerability of spatial networks," in *Proceedings of the 4th International Conference on Information Systems for Crisis Response and Management, ISCRAM*, 2007.
[17] J. L. Marzo, S. G. Cosgaya, N. S. Kapov, C. Scoglio and H. Shakeri, "A study of the robustness of optical networks under massive failures," *Optical Switching and Networking*, vol. 31, pp. 1-7, 2019.
[18] Manzano, M., Marzo, J. L., Calle, E., and Manolovay, A. "Robustness analysis of real network topologies under multiple failures scenarios," *2012 17th European Conference on Networks and Optical Communication (NOC)*, pp. 1-6, 2012.
[19] W. Ellens and R. E. Kooij, "Graph measures and network robustness," *arXiv preprint arXiv:1311.5064*, 2013.
[20] X. Yang, Y. Zhu, J. Hong, L.-X. Yang, Y. Wu and Y. Y. Tang, "The Rationality of Four Metrics of Network Robustness: A Viewpoint of Robust Growth of Generalized Meshes," *PloS one*, vol. 11, no. 8, pp. 1-13, 2016.
[21] B. Mukherjee and F. Dikbiyik, "Recent advances in (optical) network survivability," in *2012 Asia Communications and Photonics Conference (ACP)*, pp. 1-2, 2012.
[22] D. F. Rueda, "Geographical Interdependent Robustness Measures in Transportation Networks," Universitat de Girona, 2018.
[23] F. Dikbiyik, L. Sahasrabuddhe, M. Tornatore and B. Mukherjee, "exploiting excess capacity to improve robustness of WDM mesh networks," *IEEE/ACM Transactions on Networking*, vol. 20, no. 1, pp. 114-124., 2011.
[24] N. H. Bao, G. Q. Su, Y. K. Wu, M. Kuang and D. Y. Luo, "Reliability-sustainable network survivability scheme against disaster failures," In *2017 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 334-337, 2017.
[25] A. P. Snow and S. Agarwal, "Towards an optimal network survivability reporting threshold," *Telecommunications Policy Research Conference (TPRC)*, 2004.
[26] A. Bhandari and J. Malhotra, "A review on network survivability in optical networks," *International Journal of Engineering Research and Applications*, vol. 5, no. 12, pp. 97-101, 2015.
[27] T. Gomes, J. Tapolcao, C. Esposito, *et al.*, "A survey of strategies for communication networks to protect against large-scale natural disasters," In *2016 8th international workshop on resilient networks design and modeling (RNDM)*, pp. 11-22, 2016.

[28] A. H. Dekker, "Simulating network robustness for critical infrastructure networks," 28th Australasian Computer Science Conference, vol. 38, no. 5, pp. 59-67, 2005.
[29] M. M. Castro, "Metrics to Evaluate Network Robustness in Telecommunication Networks," Doctoral dissertation, Universitat de Girona, 2011.
[30] J. Brown, L. Mol, "On the roots of the node reliability polynomials," *Networks*, vol. 68, no. 3, pp 238-246, 2016.
[31] "Network topology analysis - graph properties that matter," vol. 52, no. 3-4, pp. 5-12, 2017.
[32] G. A. Virgin and M. Sangeetha, "Performance evaluation of survivability in optical networks design based on graph theory by using OPNET," *International Journal of Pure and Applied Mathematics*, vol. 116, no. 15, pp. 449-455 2017.
[33] M. Parandehgheibi, E. Modiano, "Robustness of interdependent networks: The case of communication networks and the power grid," In *2013 IEEE Global Communications Conference (GLOBECOM)*, pp. 2164-2169 2013.
[34] Sterbenz, James PG, et al. "Evaluation of network resilience, survivability, and disruption tolerance: Analysis, topology generation, simulation, and experimentation," *Telecommunication systems*, vol. 52, no. 2, pp. 705-736, 2013.
[35] M. H. Chehreghani, A. Bifet and T. Abdessalem, "Discriminative distance-based network indices with application to link prediction*," The Computer Journal*, vol. 61, no. 7, pp. 998-1014, 2018.
[36] N. A. Ismail, S.M. Idrus, R.A. Butt, F. Iqbal, A.M. Zin and F. Atan, "Dedicated protection scheme for optical networks survivability," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 3, pp. 1047-105, 2019.
[37] F. Dikbiyik, A. S. Reaz, M. D. Leenheer and B. Mukherjee, "Minimizing the disaster risk in optical telecom networks," *Optical Fiber Communication Conferenc*, pp. 1-3, 2012.
[38] J. S. Silvero, "Robustness Against Large-Scale Failures in Communications Networks," Girona, España, 2012.
[39] S. M. Al-Shehri, P. Loskot, T. Numanoglu and M. Mert, "Common metrics for analyzing, developing and managing telecommunication networks," *arXiv preprint arXiv:1707.03290*, Cornell University, United Kingdom, 2017.
[40] A. Izaddoost, "Dynamic probabilistic network protection in large-scale failure scenarios," Doctoral dissertation, University of Ontario Institute of Technology, 2015.
[41] A. d. Sousa, T. Gomes, R. Girao-Silva and L. Martins, "Minimizing of the network availability upgrade cost with geodiverse routing for disaster resilience," *Int. W. Resilient Networks Design & Modeling (RNDM)*, 2017.
[42] A. Izaddoost and S. S. Heydari, "Enhancing network service survivability in large-scale failure scenarios," *Journal of Communications and Networks*, vol. 16, no. 5, pp. 534-547, 2014.
[43] M. Manzano, J. L. Marzo, E. Calle and A. Manolova, "Robustness analysis of real network topologies under multiple failure scenarios," *2012 European Conference on Networks and Optical Communications (NOC)*, 2012.
[44] M. F. Habib, M. Tornatore, F. Dikbiyik and B. Mukherjee, "Disaster survivability optical communication networks survivability: a complete survey," *Computer Communications*, vol. 36, no. 6, pp. 630-644, 2013.
[45] Advantech B+B SmartWorx, "MTBF, MTTR, MTTF, FIT Explanation of Terms," *in Network Infrastructure Whitepapers, Technical Learning & Support Center* 2014. [Online]. Available: http://advantech-bb.com/mtbf-mttr-mttf-fit-explanation-terms.
[46] F. Iqbal, S. Trajanovski and F. Kuipers, "Detection of spatially-close fiber segments in optical networks," *2016 12th International Conference on the Design of Reliable Communication Networks (DRCN)*, pp. 95-102, 2016.
[47] M.W. Ashraf, S.M. Idrus, and F. Iqbal, "Maximally spatial-disjoint lightpaths in optical networks", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, no. 2, pp. 733-740, 2018.
[48] N. H. Bao, F. Habib, M. Tornatore, C. U. Martel and B. Mukherjee, "Global versus essential post-disaster re-provisioning in telecom mesh networks," *Journal of Optical Communications and Networking*, vol. 7, no. 5, pp. 392-400, 2015.
[49] F. Iqbal, J. van der Ham and F. Kuipers, "Multi-layer routing Technology-aware multi-domain multi-layer routing", *Computer Communications*, vol. 62, pp. 85-96, 2015.
[50] M, Alhihi, M, R, Khosravi, H, Attar and M, Samour, "Determining the optimum number of paths for realization of multi-path routing in MPLS-TE networks," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 15, no. 4, pp. 1701-1709, 2017.

BIOGRAPHIES OF AUTHORS

Noor Aishah Zainiar received the B.S.C.S degree in data communication and networking from UiTM Jasin, Melaka, Malaysia in 2018 and the Master degree in computer networking from UiTM, Shah Alam, Selangor, Malaysia in 2019. She is currently pursuing her Ph.D. degree in electrical engineering in UTM. Her research interests include network robustnes and interdependent networks.

Farabi Iqbal is a senior lecturer in the school of electrical engineering at Universiti Teknologi Malaysia, where he has been a faculty member since 2009. He holds a M.Eng. in Electronics and Telecommunications from Universiti Teknologi Malaysia, and a Ph.D. in Optical Networking from Delft University of Technology, The Netherlands. His main research interests revolve around network routing, resiliency and optimization.

Abu Sahmah Mohd Supa'at was born in Johor Bahru, Malaysia, in 1963. Hereceived the Ph.D. degree from Universiti Teknologi Malaysia (UTM), Johor Bahru, Malaysia, in 2004. He has taught various subjects and involved in a variety of research projects in the field of optical fibers, free space optic, visible free space optic and PLC, and photonic devices. He is currently a Professor and the Chairman of Research Alliance in Innovative Engineering UTM.

Adam Wong Yoon Khang was born in Miri district of Sarawak, Malaysia, in 1982. He received his PhD in Telecommunication Engineering from University Teknologi Malaysia in 2018. He then joined Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka (UTeM) as a Senior Lecturer. At UTeM, he is a research member at Center for Telecommunication Research and Innovation. His current research interests are Internet of Things, Hybrid Optical Wireless, simulation optimization, ad hoc network and passive optical network.