Performance assessment of a communication infrastructure with redundant topology: A complex network approach

Article *in* Computer Networks · March 2023

DOI: 10.1016/j.comnet.2023.109747

Manuel Herrera
University of Cambridge

Manu Sasidharan
University of Cambridge

Ajith Kumar Parlikad
University of Cambridge

Performance assessment of a communication infrastructure with redundant topology: A complex network approach*

Manuel Herrera[a,*], Manu Sasidharan[a], Stephen Cassidy[b], Ajith Kumar Parlikad[a]

[a] *Institute for Manufacturing, Dept. of Engineering, University of Cambridge, 17 Charles Babbage Road, Cambridge CB3 0FS, United Kingdom*
[b] *British Telecomm plc (BT), Adastral Park – Barrack Square, Martlesham Heath, Martlesham, Ipswich IP5 3RE, United Kingdom*

Abstract

The physical assets within a critical infrastructure system are pivotal to its efficient performance and protection and that of other dependent systems. This is particularly the case for communication systems where network protection strategies usually involve asset redundancy. Although such redundancy is well-modelled in the literature, there is a gap in knowledge from a network science perspective in terms of its implications for network modelling and performance assessment. This paper presents a multilayer complex network framework that takes into account the heterogeneity of the redundant infrastructure for realistic network modelling and further analysis, a step change from using a single network model. Key performance indicators (KPIs) for communication networks (i.e., latency and jitter, bandwidth and throughput, queue depth and packet drops) are redefined to evaluate key important features of a long-haul backbone network such as network capacity and average use. In addition, these KPIs are adapted to deal with the aforementioned redundancy and so inform network managers with values defined over a model closer to the real system. The paper

*This research was funded by the EPSRC and BT Prosperity Partnership project: Next Generation Converged Digital Infrastructure, grant number EP/R004935/1.

*Corresponding author
Email address: `amh226@cam.ac.uk` (Manuel Herrera)

analyses the use case of a nationwide core and metro network infrastructure of one of the main UK internet service providers. The results of the analysis of KPIs showcase the advantage of the proposed multilayer complex network framework over the traditional single network model. Critical network elements within different dimensions of a communication network are identified based on their performance for prioritising network management measures.
Keywords: Infrastructure protection, Network modelling, Multilayer networks, Network analytics, Core and metro networks

---

1. Introduction

Communication networks (CNs) are critical infrastructures (CIs) providing services such as telephone communications (point-to-point), radio broadcasting (one-to-many), and internet (many-to-many) [1]. The effective functioning and performance of other CIs such as banking and finance, emergency services, transport, public health, defence and utility networks are dependent on the resilience of the CNs. Moreover, any failure or malfunctioning of CNs may cascade into other CIs. The importance of this error propagation is increasing nowadays given the growing societal dependence on smart devices and systems. While the CNs are a fundamental enabler underpinning the effective response to any emergency situation, the physical CN assets are being exposed to a range of threats and vulnerabilities such as natural events, earthquakes, extreme weather events, and deliberate attacks [2, 3]. For example, the breakdown of communication services hampered the rescue and recovery efforts during Hurricane Katrina (2004) and bombings in London (2005) [4]. More recently, the failure of CNs during the 2022 floods in Australia's New South Wales resulted in widespread disruptions to the banking sector [5]. Additionally, the data system of CNs is also vulnerable on their message transmission processes to the threat of software malfunction and malicious attacks [6, 7]. Consequently, governments worldwide prioritise CN systems and services within the resilience assessment of CIs [8].

The existing approach for characterising the resilience of CIs is varied with much of the literature focusing on key performance indicators (KPIs) to measure their capability and availability. KPIs represent abstractions of complex systems and have been used to objectively compare the performance of the different systems and their components. This is the case for CIs such as energy and performance [9], transport and safety [10], nuclear power and efficiency [11] and urban water management and availability [12]. For CNs, the typical KPIs are associated with network availability and quality of service (QoS) with respect to data traffic [13]. However, other main KPIs are those related to network performance such as data-packets latency [14], bandwidth [15], and data-packets drop and packets not reaching their destination due to queue congestion [16]. These existing KPIs can be expanded by considering the latency (delay in the data-packet transmission) and jitter (variability in such a transmission) or combined. For instance, measures of latency and queue depth can be strong indicators of network problems when such information is combined. Shariati et al [17] used the measure of latency as the KPI for 5G network slicing on optical networks. The throughput was employed alongside latency and jitter by Soos et al [18] to compare the performance of 5G over 4G network. The energy efficiency of CNs have also been monitored as a KPI by Fuentes et al [19]. Ruiz et al [20] introduced QoS-related measures and end-to-end KPI analysis for converged fixed-mobile infrastructure. Kakadia et al [21] dealt with KPIs at various granularity levels for the long-haul backbone infrastructure. They proposed a multilayer network view that can be considered an antecedent to the work presented in this paper. However, the multilayer analysis presented by Kakadia et al was from a telecom system analysis point of view; while this paper presents an approach related to complex network modelling and analysis. In another work, Kakadia and Ramirez-Marquez [22] focused on the quality of experience (QoE) to the end user for estimating the resilience of a mobile network through causal models. Their proposal was such that the higher the resilience of the network infrastructure (radio access, back-haul, core and metro networks), the better the QoS provided to the end user [23]. The interdependence between QoE and QoS in video streaming has been explored by Vaser et al [24].

Many internet service providers (ISPs) worldwide often work with a redundant topology for their physical infrastructure to protect their network. Critical network elements are duplicated, allowing the system to work constantly, with redundancy in assets and resources. While this characteristic has been well investigated in the literature, there is little research done from the complex network analysis perspective with respect to the representation of such a redundant topology. The multilayer complex-network approach proposed within this paper typically generates an innovative solution for network operation and management that cannot be obtained by solving each of the single-layer network design problems sequentially. This provides the opportunity for significant cost savings. A redundant network topology naturally has implications in network protection and resilience, the latter being understood as the capability of the network to maintain an acceptable performance level against both internal perturbations and external disturbances [25]

To the best of our knowledge, the existing approaches in network science for managing and planning the physical infrastructure of a CN are often based on a traditional, single-dimensional approach. This paper, however, focuses on the analysis and synthesis of the redundant topology of network elements that often appear in an actual infrastructure along with other element dimensions that can originate additional information, computing and analysing network KPIs at the element-wise and at the mesoscale level. The aim is to consider a closer representation as possible of the network for creating KPIs that asset managers can use for better-informed decision-making processes on tasks such as network traffic re-routing and prioritising interventions on critical network elements based on their performance.

This paper complements the recent studies that have surveyed the application of a multidimensional approach to CNs [26] and designed the taxonomy for such dimensions [27] by proposing a novel framework for assessing the resilience and performance of a CN through a multilayer complex network representation, decomposition and a consequent data extraction process, taking into account both node redundancy and node router-type role. The main contributions of this paper are as follows: (1) innovative ways for network visualisation via multilayer complex networks; (2) novel redefinition of the main network KPIs relevant for a long-haul backbone network and adaptation to a multidimensional complex network topology, including physical network redundancy; (3) novel multi-view analysis of the network performance.

The remaining paper is as follows. Section 3 introduces a theoretical background of the paper. First, it summarises how a redundant topology of CNs works for its management and protection. This section also discusses the role of multilayer networks in infrastructure systems, particularly in CNs. KPI-based analysis and synthesis framework is discussed in Section 4 alongside a series of CN-relevant KPIs for a long-haul backbone network. Section 5 presents the case study of the redundant network topology of one of the main ISPs in the UK. The paper closes with a series of conclusions and future research in Section 6.

2. Network protection and management

The main aim of network protection strategies is to improve the resilience of the network. This is the purpose of an infrastructure redundant topology. However, it is also necessary to ensure that the identified strategies translate into efficient operation and management of the network. This section presents a list of network protection strategies, along with a brief overview of different planning levels of network management.

Over the years several design solutions have been proposed for ensuring the resilience of CNs [28]. Their aim is to maintain network service even when malfunctions or failures occur. There are two important strategies for CN resilience: restoration and protection.

- Restoration is a reactive resilience mechanism. It arranges new backup connections only after a failure event. To restore a connection, CN nodes learn the network topology that is not affected by the failure. This allows the system to propose a number of candidate-routes (either nodes or links) free of faulty assets. The restoration process continues by selecting a new route and then setting up the backup connections. Although restoration can be easily implemented and offers a high degree of adaptability to any failure scenario, the total response time can take longer than desired if the network intent is a high-speed internet provision.

- Protection is a preventive resilience mechanism. That is, the network is designed to have a number of backup routes able to cope with a range of predefined failures while incurring the minimal cost. The main advantage of protection as a CN resilience strategy is its quick operation since the network backup elements (link/s, path/s) are predefined and the corresponding network assets (e.g. routers, switches and cables) are pre-allocated. Protection inherently has adopted a dual network topology for some or all of the CN assets. The most common protection strategies are the following: $1 + 1$ protection, where the data traffic is duplicated and, then, transmitted through two different routes; $1 : 1$ protection, where the working route uses a backup transmission path although the data traffic travels over only one of the routes; $M : N$ protection, where M protection/backup routes are used to cover N working routes ($M \leq N$). In all cases, the network traffic will only partially load the capacity of each transmission path aiming to make room for traffic spikes.

While a redundant topology is, in principle, intended for protection and resilience design, it contributes to asset management planning at different levels: strategic (service levels, e.g.), tactical (risk and criticality levels, e.g.), and operational (condition and performance levels, e.g.).This translates into short-, medium- and long-term decisions ranging from managing a network element, such as routing stations and cables, to the whole CN. A key aspect of asset management planning is to match the CN performance and service to stakeholder expectations and future demand. Different KPIs are employed to monitor performance and support decision-making at each planning level.

- Strategic: the desired levels of service (including cost, efficiency, quality and reliability) are agreed and the resilience strategies to attain such levels are identified. To this end, a high-level assessment needs to be carried out to understand how the condition and performance of the CN elements affect the service levels. This in turn informs the asset life cycle management plans and the long-term budgetary requirements.

- Tactical: clear criteria are set to monitor when there is a deviation from the intended service levels. An in-depth analysis is carried out to identify the critical network elements and events (e.g. overheating of routing stations, malfunctioning cables) where resilience strategies need to be prioritised to ensure the CN's desired service levels.
- Operational: the intervention levels are set for each network element based on their condition and performance that triggers remedial actions such as a dynamic re-routing. A maintenance needs assessment is conducted on a routine basis and the required interventions are carried out.

3. Multilayer complex networks in infrastructure systems

Complex networks are representations of systems of interconnected elements [29, 30, 31]. Mathematically, complex networks are graphs whose vertices represent physical or virtual items and edges represent the interaction between them [32]. Formally, the elements of a network are called nodes and links; while their graph counterparts are vertices and edges, respectively (we will refer indistinctly to nodes and vertices, and links and edges, over the rest of the paper). A universal way to conduct further analysis of complex networks is by using their mathematical representation as graphs. To this end, the adjacency matrix, $\boldsymbol{A}$, captures the structure of the graph. Let us denote a node set as $\mathcal{V} = \{v_0, v_1, \ldots, v_{n-1}\}$, and the edges between them as $\mathcal{E} = \{e_0, e_1, \ldots, e_{m-1}\}$, such that we have a graph, $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ of n nodes and m edges. $\mathcal{G}$ can be directed or undirected, and supposing it is unweighted. The adjacency matrix is $\boldsymbol{A} = [a_{ij}]$; where $a_{ij} \in \{0, 1\}$, such that when $(i, j) \in \mathcal{E}$, that is, i and j share an edge, $a_{ij} = 1$, else $a_{ij} = 0$. In directed networks, $a_{ij} \neq a_{ji}$, since $(i, j) \neq (j, i)$, however in undirected networks, $a_{ij} = a_{ji}$, such that $\boldsymbol{A}$ is symmetric.

The adjacency matrix plays a fundamental role in almost every complex network analysis. For instance, the computation of centrality metrics to evaluate the connectivity level of the network elements has been shown to be useful to find correlation metrics ascertaining the network structure [33] or to analysing synchronisation phenomena for network supervision and control purposes [34]. In the case of CN, the adjacency matrix gathers the connectivity and communicability of network elements such as switches and router stations, being its properties key for routing, anomaly detection, and other traffic engineering issues [35]. However, complex networks representing real-world systems often come with heterogeneity in their elements, and the relationship between them, that cannot be expressed by a single, 2-dimensional graph.

3.1. Multilayer complex networks in infrastructure systems

The natural heterogeneity associated with any infrastructure system should be taken into account for a closer-to-reality representation of such a system. To this end, this paper proposes multilayer networks as an enriched network modelling of the system. In a multilayer complex network, nodes of different types or properties, are mapped into different complex network layers. Appendix A provides a formal definition of the adjacency matrix of a multilayer complex network and, through it, a closer look to such multilayer complex networks, along with their structure and operation.

Applied multilayer complex network analysis to infrastructure systems has been approached through a generalisation of the common network measures such as centrality metrics and modularity [36]. Additional examples of analysis of multilayer complex networks in infrastructure are diffusion processes to estimate the capacity of transmission of a network [37]. The studies on the dynamics of failure spreading are related to the concept of diffusion (the failure spread / cascading processes) [38], as well as the percolation analysis in networks to estimate topological changes within the infrastructure systems [39, 40]. All these cases revolve around the particularities of a multilayer complex network structure and dynamics.

From the point of view of the application, Milanović et al. [41] focused their work on interconnected infrastructure systems and the challenge of synchronisation between the different layers (or systems) in such system of systems). The problem of allocation of additional network resources on power and CNs have been addressed by [42]. Ulak at al. [43] studied the resilience of power and roadway networks against extreme weather conditions. Pan et al. [44] proposed a review on the network structure for the resilience analysis of transportation infrastructure, including the multilayer complex network approach.

CNs historically work from a multilayer approach [45], as the overall infrastructure can be understood as a network of networks [46]. However, a CN is often related to the classification of their multiple functionality levels and it is approached from a logical point of view rather than that of complex (multilayer) networks [47]. Nevertheless, there are indeed works on CNs and network modelling considering a multilayer approach. Wu et al. [48] focused on CN traffic dynamics from a multilayer network view. Another work to highlight is the social network analysis point of view taken by Socievole et al. [49] for optimal data-traffic re-routing. Still, most of the work involving CNs lie in the interdependence with other infrastructure systems [50].

3.2. The role of a multilayer-aspects approach for communication networks

Within a multilayer complex network representation, *aspects* are groups of layers of different types [51, 52]. The network nodes do not necessarily appear on all layers, but they necessarily appear on at least one layer of each aspect. Hence, the i-th multilayer network aspect is a multilayer network in its own, $\mathcal{M}_i$, made by a particular set of layers of the overall network, $\mathcal{M}_i = (\mathcal{G}_i, \mathcal{C}_i)$. where $\mathcal{G}_i = \{G_{\alpha,i} : \alpha \in \{1, \ldots, M_i\}\}$ is the i-th family of graphs with layers $G_{\alpha,i} = (X_{\alpha,i}, E_{\alpha,i})$. Consequently, addressing the network computations through more than one aspect will enrich any network analysis through a more holistic approach to modelling the network. Figure 1 shows a visualisation of this concept through a set of possible aspects and their division into layers at each aspect. In this case, the CN representation focuses on its redundancy aspect, as it is shown by Figure 1a), and on its node or router-type aspect, Figure 1b).

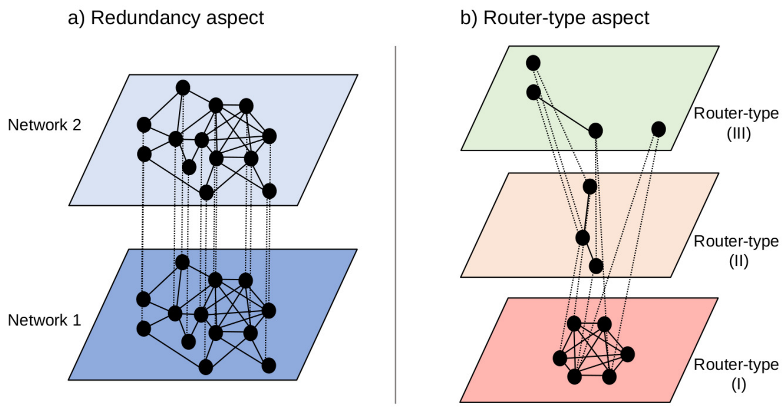


Figure 1: Instances of 2 multilayer network aspects for the same network: a) redundancy aspect - each layer represents redundant nodes - b) node-type aspect - each layer represents nodes of a different type.

The following points explain in more detail the router type and redundancy aspects:

- Redundancy aspect (Figure 1a) comprises of main and backup network layers. The main objective of this aspect is infrastructure resilience and protection. Depending on the protection strategy chosen by the ISP (see Section 2), the use of these two networks may change. One working option is redundancy on the traffic transmission by duplicating the data packets at each network. Another option is to split the volume of data transmission between the two networks to avoid the risk of congestion. The data traffic can keep a balance between the two networks, in regular demand scenarios, but could also be unbalanced in case of a network faces any issues.

- Router-type aspect (Figure 1b) comprises of super or inner-core, regional or outer-core, and metro network layers. The core network encompasses points of presence (PoPs, data centres and buildings for internet exchange) of high-capacity routers with multi-protocol label switching (MPLS) that support faster redirection of data. The inner core has a direct connection to the Internet via a wired or satellite connection. The function of the outer-core network is to enable traffic transit. Nodes at the metro network are large-scale routers supplying internet service to local areas. The main objective of this aspect is the distribution of data packets or network traffic.

After defining the multilayer network aspects, a plausible analysis approach is to proceed with a data extraction process considering such aspects. This paper works in the extraction of knowledge from those data thanks to creating as many data sets to analyse further as the number of layer combinations extracted from the network.

4. KPIs from a multilayer complex network perspective

KPIs are essential tools for measuring and monitoring the performance of CNs. KPIs provide a quantitative way to evaluate network performance and identify areas for improvement. CN asset managers can use KPIs to optimise the performance of their infrastructure, ensure high availability and deliver high-quality service to their users. They are largely used to measure network uptime and downtime, latency, throughput, security and quality of service. The main KPIs for CN management are often based on latency, bandwidth and packet drops. These KPIs have a straightforward expression considering single communication networks. However, in the presence of a redundant topology and within the multilayer network analysis framework, it is necessary to redefine the KPIs taking into account such a structure. Hence, this section considers a multi-aspects approach dealing not only with the redundancy aspect of a CN but also with the router-type aspect, to better analyse the network performance at both levels. The section also proposes new expressions for the KPIs that are able to consider the heterogeneity naturally associated with a multilayer network.

4.1. Latency and jitter

Network latency is the time it takes for a signal to travel from a source node to a destination.

The first approach to latency is its computation through the distance between such nodes. Actually, if a packet travels directly from a node source to a destination, latency should theoretically be the inverse of the signal transmission speed, with a theoretical upper bound being the speed of light through the fibre-optic cables. In practice, this limit is conditional on the material and geometric characteristics of the cables. In addition, the data packets cannot travel directly point-to-point and they need to travel through intermediate network elements. The travel time then will also depend on the condition of such elements, as it can be the case of traffic/link congestion (associated with bandwidth) or the percentage of packets dropped by the system in the route source destination (associated with queue depth/node congestion).

This paper provides a tailored expression to approximate the value of a KPI associated with the latency in a multilayer network case. In this regard, Equation (1) proposes a standard way to compute network latency-related measures at any node. Consider the destination as node v, in a network represented by the graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Then, Equation (1) that gives the average latency at a certain node, v, is:

$$TL(u,v) = \sum_{(w_i,w_j)\in W} d(w_i,w_j) + \sum_{w_i\in W} \left(q(w_i) + p(w_i)\right), \tag{1}$$

where W is the set of nodes belonging to the shortest path between the source node, u, and the destination node, v. That is, $W = \{u, w_1, \ldots, w_i, w_j, \ldots, v\}$. In addition, d is a function of the distance between nodes i and j weighted by the bandwidth of the link (i,j); q is a function of the queue depth at the node $w_i \in W$, and p is a function of the packet processing delay at each node. Equation (1) works with the assumption of a linear relationship between q and p. However, it can be a multiplicative relationship or any other kind of relationship. Other variables such as medium propagation speed are not considered in this equation but could easily be added to it.

The expression of Equation (1) can be straightforwardly extended to handling multilayer networks, considering the latency of data transfer from the source node, $u^{\gamma 1}$, and the destination node, $v^{\gamma 2}$ through the shortest path named $W = W^{(\gamma 1, \gamma 2)}$; where $\gamma 1$ and $\gamma 2$ can be any of $\{\alpha, \beta\}$ layers. This is shown by Equation (2), where the KPI associated with the latency is given by:

$$TL(u^{\gamma 1}, v^{\gamma 2}) = \sum_{(w_i, w_j) \in W} h_{i,j} d(w_i^{\gamma}, w_j^{\gamma}) + \sum_{w_i \in W} (q(w_i^{\gamma}) + p(w_i^{\gamma})) = \sum_{(w_i, w_j) \in W \wedge \gamma i = \gamma j} h'_{i,j} d(w_i^{\gamma i}, w_j^{\gamma j}) + \sum_{(w_i, w_j) \in W \wedge \gamma i \neq \gamma j} h''_{i,j} d(w_i^{\gamma i}, w_j^{\gamma j}) + \sum_{w_i \in W} (q(w_i^{\gamma}) + p(w_i^{\gamma})) \,, \quad (2)$$

where $h_{i,j}$ are the time weights for the link connections, independently of the layer of the connected nodes by the link. In that case, the layer is indicated generically as γ, standing for $\{\alpha, \beta\}$. The second part of Equation (2) makes a distinction between links and interlinks (connecting different layers). Then $h'_{i,j}$ and $h''_{i,j}$ represent different weights in the time estimation depending on whether the links connect nodes at the same layer or from different layers (i.e. interlinks).

From a multilayer approach, an interesting extension of a KPI directly related to latency is to measure the impact of data transmission between different layers on the latency. Equation (3) computes the proportion of the latency time used for such data shift between layers, for the case of having just 2 layers, α and β.

$$TL^{\alpha,\beta}(u^{\gamma 1}, v^{\gamma 2}) = \frac{\sum_{(w_i, w_j) \in W \wedge \gamma i \neq \gamma j} h''_{i,j} d(w_i^{\gamma i}, w_j^{\gamma j})}{TL(u^{\gamma 1}, v^{\gamma 2})}, \quad (3)$$

where $\gamma 1$ and $\gamma 2$ can be any of $\{\alpha, \beta\}$ layers. The weights $h''_{i,j}$ and other equation elements come from the definition of the previous Equation (2).

In addition to the indication about the time proportion in data transmission used for layer exchange, Equation (3) can also be used as an indicator of traffic issues in the network traffic, when it is designed to be used in both layers independently and only go from one layer to another for handling an unexpected traffic anomaly or planned network maintenance. In this regard, the definition of jitter as the variability associated with the computation of latency is key to detecting data traffic anomalies. Although to estimate jitter it is necessary to look into the order of the packets in addition to the latency variability; for anomaly detection purposes, a surrogate measure for jitter is the one based on re-sampling the throughput to estimate both latency and jitter at local and global network levels [53]. The case study in Section 5 will discuss this and adopt this strategy to approximate the concept of jitter through the root mean square (RMS) of the throughput passing every two minutes, rather than directly using the time [54].

4.2. Bandwidth and throughput

While latency is a KPI explaining the transmission speed, bandwidth is about the capacity of transmission. Hence, both KPIs are complementary since an optimal network performance will seek high transmissions as well as high capacities for such transmission. Consequently, high transmission capacity or high bandwidth is associated with a lower risk of traffic congestion over the network. Similarly, it is also associated with data packets that need to be discarded and transmitted again - increasing in latency. The concept of throughput is an experimental measure of successful data transmission from source to destination. Equation (4) computes the network bandwidth as the minimum of the maximum capacity of each cable in such a shortest path, W, between the source node, u, and the destination node, v.

$$B(u,v) = \min_{(w_i,w_j)\in W} \Big\{ b(w_i,w_j) \Big\}, \tag{4}$$

where $W = \{u, w_1, \dots, w_i, w_j, \dots, v\}$ is the set comprising the nodes belonging to the shortest path between u and v. The function $b(w_i, w_j)$ is the bandwidth associated to the cable (w_i, w_j).

Taking into account the multilayer network characteristics, the expression of Equation (4) can be computed by splitting the bandwidth links between links within a layer and the interlinks between layers. This is what Equation (5) shows.

$$B(u^{\gamma 1}, v^{\gamma 2}) = \underset{b(w_i,w_j)}{\arg\min} \Big\{ b(w_i, w_j) : (w_i, w_j) \in W \wedge \gamma i = \gamma j, \\ b(w_i, w_j) : (w_i, w_j) \in W \wedge \gamma i \neq \gamma j \Big\}, \quad (5)$$

The KPI about bandwidth can be expanded to compare the bandwidth of intra-layer links and the bandwidth of interlinks. This is computed by the ratio presented in Equation (6).

$$B^{\alpha,\beta}(u^{\gamma 1}, v^{\gamma 2}) = \frac{B(u^{\gamma 1}, v^{\gamma 2})}{\min_{(w_i,w_j) \in W \wedge \gamma i \neq \gamma j} \{b(w_i, w_j)\}}, \quad (6)$$

Other combinations of interest based on the bandwidth KPI are those coming from the ratios of bandwidths and observed measures of throughput. This performance measure provides information about link congestion. Such a ratio can also be computed at the interlinks to estimate the congestion when data is transmitted between layers.

4.3. Queue depth and packets-drop

Network bandwidth is also related to the likelihood of packets-drop to account for situations where the data transmitted exceeds a set bandwidth or the capacity of the queue at each point of presence (PoP) of the network, defined in Section 3.1. Queue depth is closely related to the important concepts of network efficiency and downtime.

Equation (7) proposes a standard way to compute the average queue depth at any node in the shortest path from the node source u to the destination v. As introduced above, the set of nodes in the shortest path is W. Note that Equation (7) uses the average as a statistical indicator of the queue depth over the path. However, it is possible to change such a function by others such as the maximum, which explains the risk of packet drop and downtime. In practice, it is possible to use both average and maximum queue depth to have a clear overview of the network performance.

$$Q(u,v) = \frac{\sum_{w_i \in W} q(w_i)}{n_W}, \tag{7}$$

where n_W is the number of nodes on the path W.

Equation (7) can be divided into membership of nodes in network layers. Under this consideration, it is possible to work with Equation (8) for a general case of a network with M layers.

$$Q(u^{\gamma 1}, v^{\gamma 2}) = \frac{1}{M} \sum_{\gamma j} \frac{\sum_{w_i \in W^{\gamma j}} q(w_i)}{n_j}, \tag{8}$$

where γj represents the j-th layer, n_j is the number of nodes on W for γj.

Among other possible combinations of interest for this KPI, it highlights the ratio of queue depths between layers. For the case of having 2 layers, α and β, this information is expressed by the Equation (9)

$$Q^{\alpha,\beta}(u^{\gamma 1}, v^{\gamma 2}) = \frac{\sum_{w_i \in W^{\alpha}} q(w_i)/n_{\alpha}}{\sum_{w_j \in W^{\beta}} q(w_j)/n_{\beta}}, \tag{9}$$

where W^{α} and W^{β} is the number of nodes belonging to the layers α and β, respectively, on the path W. The number of nodes at each layer is expressed by n_{α} and n_{β}, also for layers α and β, respectively.

5. Core and metro networks: case-study

The paper works with the case study of the long-haul backbone infrastructure of one of the major ISP in the UK. Particularly, the open system interconnect (OSI) level 3 (network level) that organises and transmits data through multiple networks. Other OSI levels [55] such as level 1 (physical level) and 2 (data-link level) are indirectly involved in the case study. The proposal can benefit OSI level 4 (transport), ensuring reliable data traffic management. The analysis revolves around a network comprising 206 PoPs - 8 of them are related to super router stations, and 18 to regional router stations. Both of the stations are big hubs. The remaining 180 PoPs are related to metro router stations that are closer to the final user via a subsequent metro access network, the analysis of which is out of the scope of this paper. The maximum (aggregated) bandwidth capacity is 400 GB for super and regional router stations, and 100 GB for metro router stations. The case-study network also comprises 722 fibre-optic tubes of cable aggregations. Since the case study presents a redundant topology, the network elements are equally distributed in 2 network layers: core-aln-1 and core-aln-2, mirroring the topology from one to another (almost perfectly). Figure 2 presents the overall network layout, where fibre-optic tubes are network links and PoPs are the network nodes, classified into super-router stations, regional-router stations, and metro-router stations.

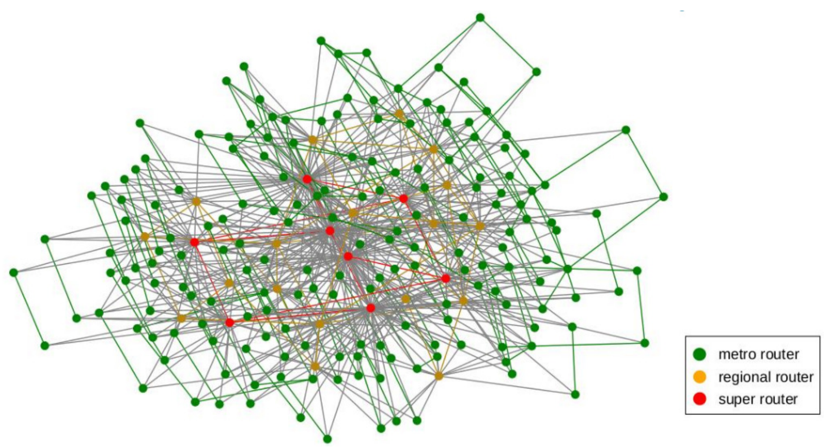
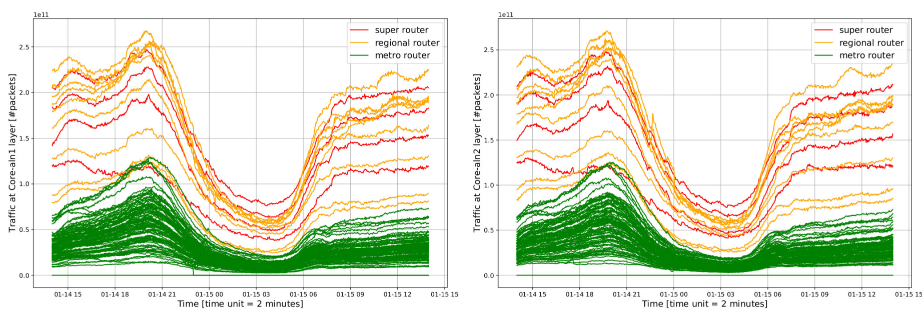


Figure 2: Core and metro networks. Representation in Flatland.

From a redundancy aspect point of view, the network is composed of two network layers: Core-aln-1 and Core-aln-2, as mentioned earlier. Both networks have 103 nodes; Core-aln-1 has 309 links and Core-aln-1 has 310. The number of interlinks connecting nodes from one network to another is 103, as expected by the number of nodes at each network layer. Figure 3 presents the traffic at each node of the network. Particularly, Figure 3a shows the traffic at each node of the network Core-aln-1 and Figure 3b at each node of the network Core-aln-2. The overall similarity between these two figures is due to the strategy of a complete balance of traffic load between them. This is in line with a 1 : 1 protection strategy where the data transmission has a backup path that is only used in case of necessity, and so, the backup network is regularly used to carry extra data traffic. Figure 3 shows a strategy in which the data traffic management seeks a balance of traffic load distribution between both networks. The data is taken at a 2min interval for a typical day, from 14:00 until 14:00 the next day. The traffic demand appears to have an increasing trend during the day to peak at night. After the first hour of the day, from 01:00, the data traffic descends quickly to get back to increasing from 06:00 am onward.



(a) Traffic network distribution at each PoP for a typical day at core-aln-1

(b) Traffic network distribution at each PoP for a typical day at core-aln-2

Figure 3: Traffic network distribution at each PoP for a typical day at core-aln-1 and core-aln-2

Figure 4 represents the same network elements of the network model of Figure 2, however, the network representation emphasises the redundancy aspect of the networks. To this end, Figure 4 comes with the network nodes classified by their type (or aspect) as they were in the previous representation. This information is enriched by the visualisation of the average data traffic passing by each network node, which is proportional to the node size in the network representation.

Computing the KPI associated with the latency from the redundancy aspect of a multilayer network, it is possible to get the time in the latency due to data transmission exchange from one layer to another, following Equation (3). The

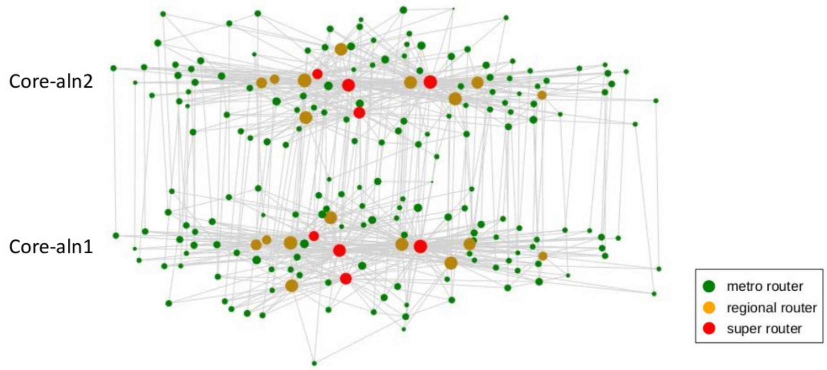


Figure 4: Core and metro networks. Redundancy aspect. Node size is proportional to their average traffic.

proportion of traffic evolution on one layer and the other is used to point out when an anomaly happens, as is the case of Figure 5. This anomaly is due planed network maintenance and shows a lack of traffic load balance between the two networks, with the time series of data presenting a high variability during the duration of such anomaly (approx. between 22:30 and 00:30). The anomaly has been further reproduced using a stochastic-based network simulation. The aim of this simulation is to compare the benefits of the redundant topology at dealing with an anomaly at the same router where the anomaly was detected in real data. The anomaly is based on a router disruption during the time units 25 to 50, out of the 100 time units of the total simulation. This video shows the results of the simulation for a single topology: Link Video 1. This video shows the results of the simulation for a redundant topology: Link Video 2. The comparison of both simulations clearly shows how the anomaly on a single topology propagates from the affected router to others easier than when the anomaly happens in a redundant topology. Further details on the simulation process can be found at [56, 57].

Table 1 shows the results of the computation of the proposed KPI: RMS for the throughput variation (RMS-TV as a related measure to jitter), throughput, and load. The KPI approach is based on the redundancy aspect and the

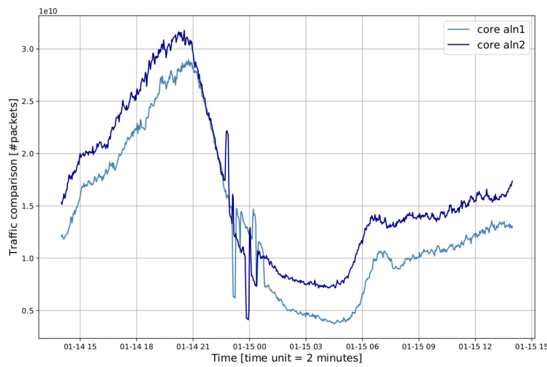


Figure 5: Core and metro networks. Redundancy aspect. Traffic anomaly at a network node, with intensive re-routing activity from one layer to another.

consequent duplicity of network elements. Table 1 presents the value computed for each network layer and the comparison between both the layers, using the Equations (2) and (3) for RMS-TV, Equations (5) and (6) for throughput, and Equations (8) and (9) for packet drops. The results confirm the high traffic load balance that the ISP reached in the distribution of data between the 2 networks, as the ratio Core-aln1 / Core-aln2 computed at Table 1 is close to one. The Core-aln2 network has the maximum RMS-TV, and so jitter, in spite of having a similar throughput as of Core-aln1 network. The results of the ratio Core-aln1 / Core-aln2 can inform the decision about traffic routing aiming to target a particular load balance between these two networks.

In contrast to the 1 : 1 redundancy presented in Figure 4, Figure 6 is a multilayer complex network representation based on the node heterogeneity regarding the operational aspect. Here, super-router PoPs made a network layer representing the inner-core network of the infrastructure. While the regional-router PoPs are at a more external level of the core network, it still remains within the definition of the core network. In this case, regional-router nodes make a network layer of nodes connecting between themselves but also to nodes at the inner-core and metro networks. The metro-router PoPs are the layer representing the metro network of the infrastructure within this case study. The router-type aspect highlighted by Figure 6 shows how the metro network nodes

Table 1: Summary statistics of the KPIs considering the redundancy aspect of core and metro networks.

		Core-aln1	Core-aln2	Core-aln1 / Core-aln2
RMS-TV	max	66.60	68.06	1.37
(GB)	mean	18.60	18.53	1.01
	min	3.43	3.71	0.92
Throughput	max	78.85	78.80	1.00
(GB)	mean	43.01	43.19	1.02
	min	14.73	14.57	1.03
Load	max	54.29	54.37	0.99
(%)	mean	32.33	32.54	0.99
	min	11.83	11.79	1.00

make a network sparsely connected to other nodes at the same level but densely connected to nodes of the regional-router layer. Still, there is a significant number of metro nodes directly connected to the super-router layer.

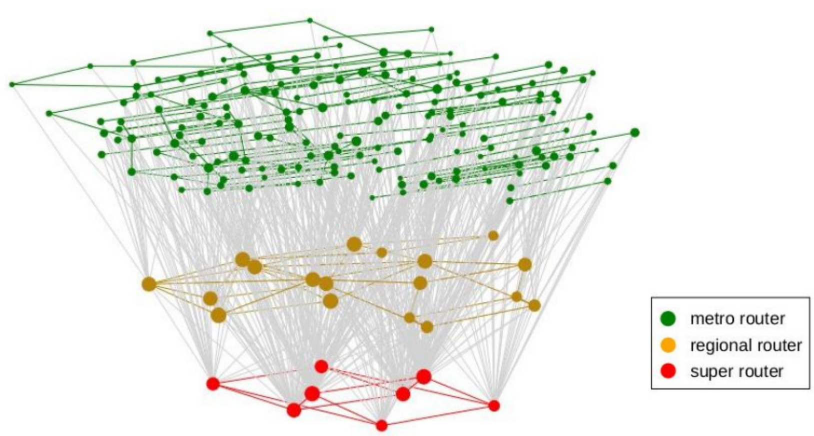


Figure 6: Core and metro networks. Router-type aspect. Node size is proportional to their average traffic.

Table 2 presents a similar analysis to those conducted for Table 1 but revolving around the KPIs considering the router-type aspect. The results show that the regional router layer has the highest throughput and RMS-TV in comparison to the super and metro router layers. On the other hand, the load of the metro router layer reaches a capacity of 94%, which is 1.77 times more than the regional router layer. From a network management perspective, this means that the assets within the regional router layer need to be prioritised for protection measures over super-router and metro-router when investing in resilience schemes for the CN as they have the highest throughput and RMS-TV (and so jitter). The load of the metro router layer also needs to be taken into consideration as the results show that it can lead to larger queue depths and consequent packet drops. Overall, the network layers associated with higher KPI values should be closely monitored; particularly, in relation to inter-layer traffic between one router-type to and another. This traffic can be associated with high costs if such a layer shift implies a change in the technology used.

Table 2: Summary statistics of the KPIs considering the router-type aspect of core and metro networks.

		Super	Regional	Metro	Metro/Regional	Regional/Super
RMS-TV	max	48.74	55.80	24.15	0.43	1.14
(GB)	mean	31.29	37.49	11.79	0.31	1.20
	min	15.04	12.72	3.79	0.30	0.85
Throughput	max	200.36	212.12	94.01	0.44	1.06
(GB)	mean	136.30	134.14	29.71	0.22	0.98
	min	56.66	47.60	5.90	0.10	0.84
Load	max	50.09	53.03	94.01	1.77	1.06
(%)	mean	34.08	33.54	29.71	0.88	0.98
	min	14.16	12.00	5.90	0.42	0.85

Table 3 shows the top 10 nodes / PoPs ranked by their contribution to the KPIs given in Table 1, with their location marked in Figure 7. Identifying these PoPs allows extracting information about their criticality across KPIs. In addition, Table 3 specifies the router type at each PoP (in parenthesis at the side of each PoP name) for a better understanding of the KPI impact on the network traffic.

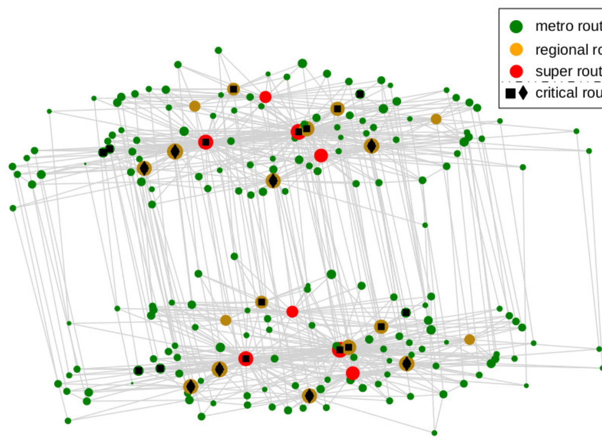


Figure 7: Core and metro networks. Redundancy aspect. Marked top critical nodes in black squares and diamonds.

Table 3: Critical PoPs with respect to the maximum values of their KPIs. Redundancy aspect of core and metro networks.

Ranking	RMS-TV	Throughput	Load
1	router-r1 (R)	router-r1 (R)	router-r1 (R)
2	router-r2 (R)	router-r3 (R)	router-r2 (R)
3	router-r3 (R)	router-r2 (R)	router-r3 (R)
4	router-r4 (R)	router-r4 (R)	router-r4 (R)
5	router-r5 (R)	router-s1 (S)	router-m1 (M)
6	router-s1 (S)	router-r5 (R)	router-s1 (S)
7	router-s2 (S)	router-s2 (S)	router-m2 (M)
8	router-r6 (R)	router-r6 (R)	router-m3 (M)
9	router-r7 (R)	router-s3 (S)	router-r5 (R)
10	router-m1 (M)	router-r7 (R)	router-s2 (S)

This level of network visibility across the multiple layers enables asset managers to prioritise the protection of those nodes that are critical to the CN performance. In this case, the criterion is to work only with the KPI maxima, since their values are those having a more direct impact on any further critical assessment. Given the strong relationship between the traffic load, as Table 1 shows, the ranking presented in Table 3 does not vary from the PoPs of one network layer to the other. The critical nodes identified within the CN are majorly from the regional router layer when considering the KPIs of jitter (approximated by RMS-TV) and throughput. Even though the load carried by the metro-route layer was the highest in comparison to other layers (see Table 2), the critical nodes from load perspective presented in Table 1 highlights the variability. For instance, half of the top 10 critical nodes from a traffic load perspective are from the regional router layer, followed by the metro router and super router. Particularly, the regional router nodes of router-r1, router-r2, router-r3 and router-r4 (see their position, marked in black diamonds, in Figure 7) are to be prioritised for any preventive maintenance to ensure that the current levels of system performance continue.

The network analysis and visualisation have been approached using Python 3, particularly using the NetworkX library [58]. The library Pandas [59, 60] has been key for data wrangling on selecting subsets of the database and computing the KPI equations. The multilayer is depicted by shifting the coordinates of the layers after their identification and subsequent node classification and labelling. To complete the analysis on the redundancy aspect of the network topology, we run a network simulation using a developed software adapted from the “anx” Python package proposed by [56].

6. Conclusions

Communication networks are a critical enabler to the economic and social development of a nation. As technology continues to evolve and user demands rise, CNs are becoming increasingly complex resulting in the potential for failure. It is important to address the resilience issues in the computing, control and management of communication networks to ensure they remain reliable and available [61]. The resilience of the communication networks is critical to maintaining network availability and performance, even when faced with unexpected failures such as natural disasters, cyber-attacks, or system failures. The computing, control and management of communication networks are critical components to ensuring network resilience. While control refers to the processes and protocols used to manage and maintain the network, management refers to the resources required to operate and support the network. Hardware failure is one of the significant resilience issues in computing. Network components such as routers, switches and servers can fail due to hardware malfunctions, power outages or environmental factors. Redundant hardware components can ensure that if one component fails, another will take over without any disruption to the network. On the other hand, software bugs and errors can cause computing-related network failures, which can lead to downtime and service interruptions. Cyber security threats such as malware, viruses and hackers can compromise the network's integrity and availability. Robust security measures such as firewalls, intrusion detection systems, and access controls, must be implemented. Finally, management is a key resilience issue, as the human factor can impact network performance and availability. Effective management practices, such as regular monitoring, maintenance and testing, can help ensure that the network remains resilient. For instance, the results of the case study presented earlier show that the routers r1-r4 can be prioritised for management interventions.

This paper proposes a novel analysis approach for the communication network performance assessment of core and metro networks with a redundant topology. To this end, a multilayer complex network modelling and data extraction process is proposed.

The main contributions of this paper are the following:

- A redefinition of the KPIs for a multilayer complex network topology. This includes the analysis of network topologies specifically tailored for protection issues, such as the 1 : 1 strategy.

- A combined multidimensional/multilayer analysis of the network structure, splitting the network into dimensions corresponding to its redundant and router-type aspects alongside the combination of such dimensions.

- A framework based on a multilayer complex network model to support the creation of novel KPIs related to how the traffic moves from one aspect to another or within the various dimensions of a given aspect. This helps the monitoring and control of traffic load balances, the traffic that is moving from one layer to another (with the corresponding possible costs if that also means a change in the network technology), and the rapid identification and classification of any network traffic issue.

The paper also formalises the KPI equations for computing latency, bandwidth, and queue depth. Such a formalisation in equations comes twofold. Firstly, for a single network, in which such KPIs are expressed in equations related to the shortest paths enabling point-to-point communication, for any node of the network. Second, the paper includes the novelty of formalising the KPI computation for the case of multilayer networks. This is by considering the general case of having multiple multilayer network aspects, and therefore the KPI interpretations and possible re-combinations. The results show the variation in the contribution of different network elements and layers towards the CN performance. However, the regional router layer is found to be critical to the CN's performance.

As CNs continue to evolve and become increasingly complex, it is essential to prioritise network resilience to ensure that they remain reliable and available to users. Future research will focus on working with a generalisation of multilayer networks, developing the analysis around the concept of hypergraphs. Hypergraphs do not constrain the definition of a link to be one-to-one but many-to-many nodes. In addition, the dynamics on multilayer complex networks will be explored to better understand the evolution of the network performance and the network resilience assessment over time. Moreover, the proposed approach will be expanded to identify the vulnerable assets within the network for prioritising network security measures. It will also be tested in 5G and future 6G topologies, accounting for their heterogeneity through the multilayer model and their highly dynamic environment through the dynamics on, and of, these networks.

Data access statement

Additional data related to this publication contain network traffic on the BT core and metro network, but these data cannot be released publicly. The data contain confidential information, protected by a non-disclosure agreement with BT. This data can be made available, subject to a non-disclosure agreement.

References

[1] S. Haykin, Communication systems, John Wiley & Sons, 2008.

[2] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. De Sousa, A. Iossifides, R. Travanca, J. André, 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), IEEE, 2016, pp. 11–22.

[3] J. Rak, R. Girão-Silva, T. Gomes, G. Ellinas, B. Kantarci, M. Tornatore, Disaster resilience of optical networks: State of the art, challenges, and opportunities, Optical Switching and Networking 42 (2021) 100619.

[4] Z. El Khaled, H. Mcheick, Case studies of communications systems during harsh environments: A review of approaches, weaknesses, and limitations to improve quality of service, International journal of distributed sensor networks 15 (2) (2019) 1550147719829960.

[5] P. Harrison, How we rebuild our network after natural disaster strikes, Telstra Fundation (2022).
URL `http://shorturl.at/jqNRU`

[6] S. H. Conrad, R. J. LeClaire, G. P. O'Reilly, H. Uzunalioglu, Critical national infrastructure reliability modeling and analysis, Bell Labs Technical Journal 11 (3) (2006) 57–71.

[7] S. Neumayer, G. Zussman, R. Cohen, E. Modiano, Assessing the vulnerability of the fiber infrastructure to disasters, IEEE/ACM Transactions on Networking 19 (6) (2011) 1610–1623.

[8] U. C. Office, Resilient communications, Tech. rep., Her Majesty's Government (2013).

[9] Y. Li, R. García-Castro, N. Mihindukulasooriya, J. O'Donnell, S. Vega-Sánchez, Enhancing energy management at district and building levels via an EM-KPI ontology, Automation in Construction 99 (2019) 152–167.

[10] M. Sasidharan, M. E. Torbaghan, Risk-informed sustainable asset management of railway tracks, Infrastructure Asset Management 8 (1) (2020) 25–35.

[11] W. Zhao, H. Yu, L. Tian, X. Li, G. Yan, Nuclear power project performance management system research based on the KPIs, in: International Conference on Nuclear Engineering, Vol. 57793, American Society of Mechanical Engineers, 2017, p. V001T01A003.

[12] D. K. Gidion, J. Hong, M. Z. Adams, M. Khoveyni, Network DEA models for assessing urban water utility efficiency, Utilities policy 57 (2019) 48–58.

[13] A. Slalmi, H. Chaibi, A. Chehri, R. Saadane, G. Jeon, Toward 6G: Understanding network requirements and key performance indicators, Transactions on Emerging Telecommunications Technologies 32 (3) (2021) e4201.

[14] V. Bobrovs, S. Spolitis, G. Ivanovs, Latency causes and reduction in optical metro networks, in: Optical Metro Networks and Short-Haul Systems VI, Vol. 9008, International Society for Optics and Photonics, 2014, p. 90080C.

[15] N. Jay, N. Rotman, B. Godfrey, M. Schapira, A. Tamar, A deep reinforcement learning perspective on internet congestion control, in: International Conference on Machine Learning, PMLR, 2019, pp. 3050–3059.

[16] M. Cociglio, G. Fioccola, G. Marchetto, A. Sapio, R. Sisto, Multipoint passive monitoring in packet networks, IEEE/ACM Transactions on Networking 27 (6) (2019) 2377–2390.

[17] B. Shariati, L. Velasco, J.-J. Pedreno-Manresa, A. Dochhan, R. Casellas, A. Muqaddas, O. G. de Dios, L. L. Canto, B. Lent, J. E. L. de Vergara, S. López-Buedo, F. Moreno, P. Pavón, M. Ruiz, S. K. Patri, A. Giorgetti, F. Cugini, A. Sgambelluri, R. Nejabati, D. Simeonidou, R.-P. Braun, A. Autenrieth, J.-P. Elbers, J. K. Fischer, R. Freund, Demonstration of latency-aware 5G network slicing on optical metro networks, J. Opt. Commun. Netw. 14 (1) (2022) A81–A90.

[18] G. Soós, D. Ficzere, P. Varga, Z. Szalay, Practical 5G KPI measurement results on a non-standalone architecture, in: Noms 2020-2020 IEEE/IFIP network operations and management symposium, IEEE, 2020, pp. 1–5.

[19] M. Fuentes, J. L. Carcel, C. Dietrich, L. Yu, E. Garro, V. Pauli, F. I. Lazarakis, O. Grøndalen, O. Bulakci, J. Yu, et al., 5G new radio evaluation against IMT-2020 key performance indicators, IEEE Access 8 (2020) 110880–110896.

[20] M. Ruiz, M. Richart, A. Castro, L. Velasco, End-to-end KPI analysis in converged fixed-mobile networks, in: 2020 22nd International Conference on Transparent Optical Networks (ICTON), IEEE, 2020, pp. 1–4.

[21] D. Kakadia, J. Yang, A. Gilgur, Overview of ip transport network architectures—backhaul, metro, and core network, in: Network Performance and Fault Analytics for LTE Wireless Service Providers, Springer, 2017, pp. 103–135.

[22] D. Kakadia, J. E. Ramirez-Marquez, Quantitative approaches for optimization of user experience based on network resilience for wireless service provider networks, Reliability Engineering & System Safety 193 (2020) 106606.

[23] C. Natalino, S. Ristov, L. Wosinska, M. Furdek, Functional Metrics to Evaluate Network Vulnerability to Disasters, Springer International Publishing, Cham, 2020, pp. 47–62. doi:10.1007/978-3-030-44685-7_2.
URL https://doi.org/10.1007/978-3-030-44685-7_2

[24] M. Vaser, S. Forconi, QoS KPI and QoE KQI relationship for LTE video streaming and VoLTE services, in: 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, IEEE, 2015, pp. 318–323.

[25] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, P. Smith, Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines, Computer Networks 54 (8) (2010) 1245–1265.

[26] M. Kivelä, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, M. A. Porter, Multilayer networks, Journal of Complex Networks 2 (3) (2014) 203–271.

[27] T. G. Crainic, B. Gendron, M. R. A. Kazemzadeh, A taxonomy of multilayer network design and a survey of transportation and telecommunication applications, European Journal of Operational Research 303 (1) (2022) 1–13.

[28] D. Tipper, Resilient network design: challenges and future directions, Telecommunication Systems 56 (1) (2014) 5–16.

[29] R. Albert, A.-L. Barabási, Statistical mechanics of complex networks, Reviews of Modern Physics 74 (1) (2002) 47.

[30] F. Menczer, S. Fortunato, C. A. Davis, A first course in Network Science, Cambridge University Press, Singapore, 2020.

[31] M. Herrera, M. Pérez-Hernández, A. Kumar Parlikad, J. Izquierdo, Multi-agent systems and complex networks: Review and applications in systems engineering, Processes 8 (3) (2020) 312.

[32] B. Bollobás, Modern graph theory, Vol. 184, Springer Science & Business Media, Springer-Verlag New York, 1998.

[33] N. Meghanathan, Correlation coefficient analysis of centrality metrics for complex network graphs, in: Computer Science On-line Conference, Springer, 2015, pp. 11–20.

[34] F. A. Rodrigues, Network centrality: an introduction, in: A mathematical modeling approach from nonlinear dynamics to complex systems, Springer, 2019, pp. 177–196.

[35] W. Jiang, Graph-based deep learning for communication networks: A survey, Computer Communications 185 (1) (2022) 40–54.

[36] C. Rahmede, J. Iacovacci, A. Arenas, G. Bianconi, Centralities of nodes and influences of layers in large multiplex networks, Journal of Complex Networks 6 (5) (2018) 733–752.

[37] S. Gomez, A. Diaz-Guilera, J. Gomez-Gardenes, C. J. Perez-Vicente, Y. Moreno, A. Arenas, Diffusion dynamics on multiplex networks, Physical review letters 110 (2) (2013) 028701.

[38] M. De Domenico, C. Granell, M. A. Porter, A. Arenas, The physics of spreading processes in multilayer networks, Nature Physics 12 (10) (2016) 901–906.

[39] S. Osat, A. Faqeeh, F. Radicchi, Optimal percolation on multiplex networks, Nature Communications 8 (1) (2017) 1540.

[40] Z. Mahabadi, L. Varga, T. Dolan, Network properties for robust multilayer infrastructure systems: A percolation theory review, IEEE Access 9 (2021) 135755–135773.

[41] J. V. Milanović, W. Zhu, Modeling of interconnected critical infrastructure systems using complex network theory, IEEE Transactions on Smart Grid 9 (5) (2018) 4637–4648.

[42] J. Banerjee, A. Sen, C. Zhou, On auxiliary entity allocation problem in multi-layered interdependent critical infrastructures, in: International Conference on Critical Information Infrastructures Security, Springer, 2016, pp. 25–37.

[43] M. B. Ulak, L. M. Konila Sriram, A. Kocatepe, E. E. Ozguven, R. Arghandeh, Resilience characterization for multi-layer infrastructure networks, IEEE Intelligent Transportation Systems Magazine (2021) 1–13.

[44] S. Pan, H. Yan, J. He, Z. He, Vulnerability and resilience of transportation systems: A recent literature review, Physica A: Statistical Mechanics and its Applications 581 (2021) 126235.

[45] R. Casellas, R. Martínez, R. Vilalta, R. Muñoz, Control, management, and orchestration of optical networks: evolution, trends, and challenges, Journal of Lightwave Technology 36 (7) (2018) 1390–1402.

[46] G. D'Agostino, A. Scala, Networks of networks: the last frontier of complexity, Vol. 340, Springer, 2014.

[47] M. Kantor, E. Biernacka, P. Boryło, J. Domżał, P. Jurkiewicz, M. Stypiński, R. Wójcik, A survey on multi-layer ip and optical software-defined networks, Computer Networks 162 (2019) 106844.

[48] J. Wu, C. Pu, L. Li, G. Cao, Traffic dynamics on multilayer networks, Digital Communications and Networks 6 (1) (2020) 58–63.

[49] A. Socievole, E. Yoneki, F. De Rango, J. Crowcroft, Ml-sor: Message routing using multi-layer social networks in opportunistic communications, Computer Networks 81 (2015) 201–219.

[50] M. M. Danziger, A.-L. Barabási, Recovery coupling in multilayer networks, Nature communications 13 (1) (2022) 1–8.

[51] H. Zhang, C.-D. Wang, J.-H. Lai, S. Y. Philip, Modularity in complex multilayer networks with multiple aspects: A static perspective, in: Applied Informatics, Vol. 4, SpringerOpen, 2017, pp. 1–29.

[52] Z. Hammoud, F. Kramer, Multilayer networks: aspects, implementations, and application in biomedicine, Big Data Analytics 5 (1) (2020) 1–18.

[53] X. Zhang, H. Yin, D. O. Wu, H. Huang, G. Min, Y. Zhang, SSL: A surrogate-based method for large-scale statistical latency measurement, IEEE Transactions on Services Computing 13 (5) (2017) 958–968.

[54] T. N. Minhas, M. Fiedler, P. Arlos, Quantification of packet delay variation through the coefficient of throughput variation, in: Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, 2010, pp. 336–340.

[55] M. M. Alani, OSI Model, Springer International Publishing, Cham, 2014, pp. 5–17. doi:10.1007/978-3-319-05152-9_2.

[56] V. Likic, K. Shafi, Battlespace mobile/ad hoc communication networks: Performance, vulnerability and resilience, in: Data and Decision Sciences in Action: Proceedings of the Australian Society for Operations Research Conference 2016, Springer, 2018, pp. 303–314.

[57] M. Herrera, Y. Proselkov, M. Pérez-Hernández, A. K. Parlikad, Mining graph-fourier transform time series for anomaly detection of internet traffic at core and metro networks, IEEE Access 9 (2021) 8997–9011.

[58] A. Hagberg, P. Swart, D. S Chult, Exploring network structure, dynamics, and function using networkx, Tech. rep., Los Alamos National Lab.(LANL), Los Alamos, NM (United States) (2008).

[59] T. pandas development team, pandas-dev/pandas: Pandas (Feb. 2020). doi:10.5281/zenodo.3509134.
URL https://doi.org/10.5281/zenodo.3509134

[60] Wes McKinney, Data Structures for Statistical Computing in Python, in: Stéfan van der Walt, Jarrod Millman (Eds.), Proceedings of the 9th Python in Science Conference, 2010, pp. 56 – 61. doi:10.25080/Majora-92bf1922-00a.

[61] D. Hutchison, J. P. Sterbenz, Architecture and design for resilient networked systems, Computer Communications 131 (2018) 13–21.

[62] R. Gallotti, M. Barthelemy, The multilayer temporal network of public transport in great britain, Scientific Data 2 (1) (2015) 1–8.

[63] A. Modarresi, J. Symons, Modeling technological interdependency in IoT-A multidimensional and multilayer network model for smart environments, in: 2019 11th International Workshop on Resilient Networks Design and Modeling (RNDM), IEEE, 2019, pp. 1–7.

[64] Y.-Y. Cao, R.-R. Liu, C.-X. Jia, B.-H. Wang, Percolation in multilayer complex networks with connectivity and interdependency topological structures, Communications in Nonlinear Science and Numerical Simulation 92 (2021) 105492.

Appendix A. Adjacency matrix and multilayer networks

The adjacency matrix of a multilayer network, $\boldsymbol{A}$, is a diagonal block-matrix composition of adjacency matrices, one per network layer of the multilayer network, named supra-adjacency matrix. This matrix represents the internal structure existing at each layer, or block of such a matrix, and also the interrelationship between layers (through the elements out of such diagonal blocks). A multilayer network encompasses M interdependent networks such that it creates the pair $\mathcal{M} = (\mathcal{G}, \mathcal{C})$; where $\mathcal{G} = \{G_\alpha : \alpha \in \{1, \ldots, M\}\}$ is a family of graphs $G_\alpha = (X_\alpha, E_\alpha)$, called layers of $\mathcal{M}$, and $\mathcal{C} = \{E_{\alpha,\beta} \subseteq X_\alpha \times X_\beta; \alpha, \beta \in \{1, \ldots, M\}, \alpha \neq \beta\}$ is the set of interconnections between nodes of different layers, G_α and G_β. The adjacency matrix of each layer, G_α, is $\boldsymbol{A}^{[\alpha]} = \left(a_{ij}^{\alpha}\right) \in \mathbb{R}^{N_\alpha \times N_\alpha}$; where N_α is the number of nodes in X_α and $a_{ij}^{\alpha} = 1$ if node i is linked to node j in G_α; otherwise $a_{ij}^{\alpha} = 0$. The definition of a weighted adjacency matrix is straightforward by considering w_{ij}^{α} instead of 1 in the definition above. For instance, weights in the adjacency matrix can represent CN features such as throughput or number of data packets in queue. The inter-layer adjacency matrix for $E_{\alpha,\beta}$ is $\boldsymbol{A}^{[\alpha,\beta]} = \left(a_{ij}^{\alpha\beta}\right) \in \mathbb{R}^{N_\alpha \times N_\beta}$; where N_α is the number of nodes in X_α and N_β is the number of nodes in X_β. In this case, $a_{ij}^{\alpha\beta} = 1$ if (i, α) is linked to (j, β); taking the value 0 otherwise. In a multilayer context for CNs, an inter-layer adjacency matrix includes the representation of the connectivity of router stations of different types and/or belonging to different (sub-)networks. Equation (A.1) represents a general expression of a supra-adjacency matrix.

$$\tilde{A} = \left(\begin{array}{c|c|c|c} A^{[1]} & A^{[1,2]} & \dots & A^{[1,M]} \\ \hline A^{[2,1]} & A^{[2]} & \dots & A^{[2,M]} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline A^{[M,1]} & A^{[M,2]} & \dots & A^{[M]} \end{array}\right) \tag{A.1}$$

The concept of multilayer networks is a generalisation of a number of specific cases of interrelation between networks. For instance, layers of temporal networks could represent the evolution of network structure and dynamics [62]. Multidimensional networks have layers representing node dimensions, one per feature measured at the nodes [63]. Interdependent networks have layers representing a collection of networks and their connections [64]. There are other types of multilayer networks. In terms of redundant topology perfectly mirroring one network topology to another, the multilayer network representation becomes the particular case of a multiplex network. Multiplex networks have the property of all the layers having the same nodes. that is, a graph representing a multiplex network is such that $X_1, \dots, X_M = X$ and $E_{\alpha,\beta} = \{(x, x); x \in X\}$ for $1 \leq \alpha \neq \beta \leq M$.

Glossary

This is a section with the commonly used names and acronyms.

- BT: British Telecomm plc.
- CI: Critical infrastructure

- CN: Complex network
- ISP: Internet service provider
- KPI: Key performance indicator
- OSI: Open Systems Interconnection model
- PoP: Point of presence
- QoE: Quality of experience
- QoS: Quality of service
- RMS: Root mean square (of the throughput)
- RMS-TV: Root mean square for the throughput variation