

Received 30 June 2026, accepted 20 July 2026, date of publication 30 July 2026, date of current version 6 August 2026.

Digital Object Identifier 10.1109/ACCESS.2026.3718222

RESEARCH ARTICLE

Improving Communication Network Availability and Sovereignty

SHAKTHIVELU JANARDHANAN¹, (Graduate Student Member, IEEE), KAUSTUBH PATIL¹,
RITANSHI AGARWAL², (Graduate Student Member, IEEE),
WOLFGANG KELLERER¹, (Fellow, IEEE),
AND CARMEN MAS-MACHUCA², (Senior Member, IEEE)

¹Chair of Communication Networks, Technical University of Munich, 80333 Munich, Germany

²Chair of Communication Networks, University of the Bundeswehr Munich, 85579 Neubiberg, Germany

Corresponding author: Shakthivelu Janardhanan (shakthivelu.janardhanan@tum.de)

This work was supported in part by the Federal Ministry of Research, Technology and Space in Germany (BMFTR) through the Project SUSTAINET-ADVANCE under Grant 16KIS2279 and Grant 16KIS2283; and in part by Bavarian Ministry of Economic Affairs, Regional Development, and Energy as part of the Project “6G Future Lab Bavaria.”

ABSTRACT Network availability is a network’s ability to serve all traffic adequately at any instant. Network sovereignty is the network operator’s ability to reduce dependencies on component manufacturers. Recent geopolitical developments have forced several nations to embrace digital autonomy by promoting indigenous technology, reducing foreign influence, and avoiding excessive reliance on certain manufacturers. Hence, network operators face the new challenge of maintaining high availability and sovereignty. This work aims to guide network operators to assign manufacturers to the nodes in the network cost-effectively, such that both network availability and sovereignty are maximized. A Minimal Cut Set (MCS) of a source-destination pair in a network is the smallest set of components whose failure causes a loss of connectivity between the source-destination pair. In this work, we use MCSs to identify the critical nodes for two purposes. First, we improve network availability by assigning more reliable components to the critical nodes. Second, we improve network sovereignty by assigning different manufacturers to these critical nodes to avoid an overwhelming dependency on a particular manufacturer. Our main contributions are (i) proposing a novel approach based on MCSs to maximize network availability, (ii) proposing the novel Cut Set Diversity (CSD) metric to measure network sovereignty, and (iii) introducing *Iroh*, a Mixed Integer Linear Program (MILP), for the hierarchical optimization of network availability and sovereignty. Furthermore, we compare *Iroh*’s performance with other state-of-the-art methods to maximize network availability and sovereignty. Our results show that *Iroh*’s manufacturer assignment for availability and sovereignty outperforms heuristics, while matching the state-of-the-art optimization methods despite having only a fraction of their computational complexity.

INDEX TERMS Manufacturer assignment, measurement metric, minimal cut sets, network availability, network sovereignty.

I. INTRODUCTION

There are two major concepts discussed in this work: Network availability and network sovereignty.

The associate editor coordinating the review of this manuscript and approving it for publication was Cong Pu¹.

A. NETWORK AVAILABILITY

Network availability is defined as a network’s ability to route all traffic appropriately at a given time instant [1]. It is a traditional dependability attribute that has been an integral part of Service Level Agreements (SLAs). Mission-critical applications like telemedicine, teleoperation, autonomous vehicular communication, smart grids, etc., require guaranteed high levels of availability, around six

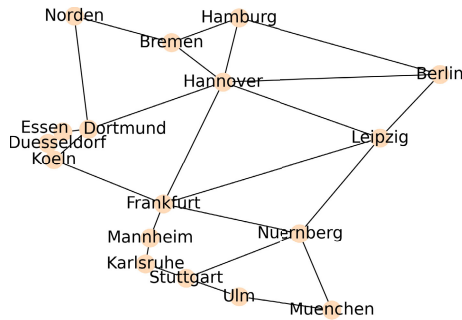


FIGURE 1. Germany_17 topology [4] with 17 nodes and 26 edges. There are 101 simple paths between Munich and Hamburg.

9s, at high data rates of around 100 Mbps [2]. Therefore, next-generation communication networks must have high resilience against failures, attacks, disasters, etc., to guarantee seamless connectivity [3].

There are several simple paths between a source and a destination in a network. For example, in the Germany_17 topology in Fig. 1, there are 101 simple paths between Munich and Hamburg. Therefore, it is necessary for network operators to employ efficient planning strategies to maximize network availability by accounting for all the redundant paths in the network.

B. NETWORK SOVEREIGNTY

Sovereignty is defined as the ability of a governing body to regulate its affairs with absolute control over its people and territory without any external interference [5]. It speaks to a state's independence and autonomy in enforcing the state's best interests within its boundaries. Recently, sovereignty has been extended to the digital world [6] with new interpretations of data, digital, and technological sovereignty. This manuscript focuses on network sovereignty. Network sovereignty is defined as the ability of a network operator to operate a network with minimal dependency on manufacturers to reduce the impact of manufacturer failures [7], [8], [9], [10]. A manufacturer (or a vendor) failure means that all the components from that manufacturer have failed. Manufacturer failures can be caused by several factors.

For instance, natural disasters can cause vendor-specific large-scale network outages. For example, the thunderstorm in Pittsburgh in 2025 caused only T-Mobile services to be down for more than a day [11]. Human error and misconfiguration may also lead to hardware or software issues. Samsung Galaxy Note 7 units exploding [12] in 2016 due to an inherently flawed battery is an example of hardware errors. A software security certificate expiration in Ericsson equipment caused an outage of nearly a day for over 25 million O2 customers in 2018 [13]. Other incidents, like the Verizon outage in 2024 causing iPhone users to be stuck in 'SOS' mode [14], the CrowdStrike outage [15] in 2024, the Telefonica outage in Spain in 2025 due to a

faulty update [16], etc., show that minor software issues can cause severe vendor-specific outages. Security vulnerabilities also cause vendor-specific failures. Examples such as CVE-2021-0275 [17]- a scripting issue affecting Juniper Networks' Junos Operating System (OS), CVE-2013-6026 [18]- a firmware issue allowing backdoor remote access to D-Link, Alpha Networks, and Planex routers, show that these vulnerabilities create a shared threat because all devices from the same manufacturer use the same firmware.

Manufacturer unavailability can also be the result of geopolitical intervention. Several governments are removing outsourced components from their critical infrastructure to ensure digital autonomy [19]. For example, the United States, Spain, England, Germany, etc., have declared their intention to remove Chinese components from their core networks [20]. Similarly, Russia's sovereign RUnet network [21], China's development of Baidu, Youku, etc., replacing popular Google applications [22], and Europe's GAIA-X initiative [23] aim to reduce the dependency on American cloud services, while promoting indigenous technology.

These examples show that excessive dependence on a manufacturer is dangerous. Hence, network operators try to deploy components from different manufacturers. However, such deployments suffer from weak planning, high costs, and interoperability issues. Our goal is to provide network operators with cost-efficient guidelines to assign manufacturers to nodes such that availability and sovereignty are maximized together. Our major contributions are as follows.

- i) Introduce MCS-based availability estimation and its application (Sec. III-A).
- ii) Introduce Cut Set Diversity (CSD) score, a novel metric to measure a network's sovereignty based on its manufacturer assignment (Sec. III-B).
- iii) Formulate the Manufacturer Assignment for Availability and Sovereignty (MAAS) problem and solve it with *Iroh*, our CSD score-based MILP (Sec. IV).
- iv) Compare *Iroh*'s performance with centrality metrics-based heuristics for availability and sovereignty, and state-of-the-art works like *Zohra* [24] for Manufacturer Assignment for Availability (MAA), *Naga* [9], *CSC-ILP* [10], and *DAP* [25] for Manufacturer Assignment for Sovereignty (MAS) (Secs. V and VI).

Note that we evaluate topological structural sovereignty and network availability. We do not look at active data traffic. Hence, we intentionally exclude data plane metrics, routing, cryptography, and security.

II. BACKGROUND AND RELATED WORK

This section summarizes and discusses the relevant state-of-the-art concerning cut sets, centrality metrics, and methods to maximize network availability and sovereignty. Throughout this work, 'manufacturer assignment' refers to the purchasing of network nodes from different manufacturers.

A. MINIMAL CUT SET (MCS)

In this work, the term flow (r) refers to a source-destination ($s - t$) pair with traffic between them, and is represented as $r = (s_r, t_r)$. A flow's cut set is a set of nodes in the network that, when failed, cause the flow to fail. A MCS is a cut set that cannot be further reduced without losing its status as a cut set [26]. For example, in the example topology Germany_17 shown in Fig. 1, for a flow between Muenchen and Norden, (Bremen, Dortmund, Essen) is a cut set while (Bremen, Dortmund) is a MCS. MCSs have been a popular topic of research in fault tree analyses [27], [28], reliability block diagram evaluations [29], [30], [31], decision diagram analyses [32], [33], network reliability studies [34], [35], [36], network sovereignty studies [10], [37], etc.

B. CENTRALITY METRICS

A node's importance in the network can be quantified using centrality metrics. In this work, we consider three traditional centrality metrics- Nodal Degree (ND), Betweenness Centrality (BC), and Closeness Centrality (CC) [38]. A node's ND refers to the number of links associated with it. A node's BC describes how often it is being used in the shortest paths between other nodes. A node's CC describes how close (in hops or link length) it is to other nodes. Along with these three popular centrality metrics, we consider two state-of-the-art centrality metrics- Isolating Centrality (IC) and Entropy Degree Distance Combination (EDDC). IC [39] identifies nodes whose removal most effectively 'isolates' a region of the network. It directly evaluates the impact of node removal on network connectivity, making it apt for detecting critical nodes in the network. It captures global structural vulnerability rather than just local importance. EDDC [40] unifies degree centrality, information entropy, and node distance into a single metric to identify influential nodes in the network. It improves over single-metric approaches by balancing local connectivity (degree), structural diversity (entropy), and global reach (distance) to better understand the critical nodes in the network. The evaluations of the IC and EDDC are as per the original proposals in [39] and [40], respectively. These centrality metrics can be used in availability studies [24] or sovereignty studies [9], [10], [37]. Their application to obtain manufacturer assignments is discussed in Sec. V-A.

C. MAXIMIZING AVAILABILITY IN MULTI-VENDOR NETWORKS

Several techniques aim to optimize network availability, such as adding new links to the network to increase redundancy [41], developing more robust topologies [42], [43], including fault-tolerant protection schemes [44], [45], replacing network components with robust upgrades [46], [47], routing all the flows through a high-availability spine [48], optimization formulations and heuristics [49], [50], [51], geographically diverse routing [52], etc. However,

these techniques do not consider the deployment of multiple manufacturers in the network.

Notably, the authors in [48] aimed to improve network availability by routing the working paths of all the flows through the network's spine. The spine was a reserved subnetwork with very high-availability links. Hence, the working path availability for all the flows was very high. However, this approach requires very high-capacity links in the spine to handle all the traffic in the network, which is infeasible in large networks. Moreover, the Integer Linear Program (ILP) optimization to find the spine links is not scalable. Hence, they propose a heuristic, denoted as the *Spine-H*. Additionally, [48] only considered the working and protection paths for each flow. In this way, *Spine-H* did not use all the redundancy in the network. However, *Spine-H* is evaluated in our current work to compare against our new approach in Sec. VI.

Modern communication networks are built with components that are purchased from different manufacturers. The components' availabilities from different manufacturers may vary according to the cost, subcomponents used, supply chain logistics, and the inherent component design. For example, the authors in [53] report that the failure and recovery rates of devices from different vendors vary by multiple orders of magnitude. Therefore, network operators arrange these components from different manufacturers in their networks such that the flow availabilities in the network are maximized, thereby maximizing network availability.

Previous works discuss interoperability challenges in multi-vendor networks [54], [55], [56]. Our work does not dive deep into these challenges. However, we recognize that standardization is critical to ensuring seamless integration across diverse hardware and software layers. The emergence of disaggregated networks based on OpenROADM [57], disaggregated components [58], and disaggregated cloud architectures as proposed by Deutsche Telekom [59], demonstrates a shift toward flexible, vendor-neutral architectures that replace proprietary monolithic systems with interoperable, standardized components. Similar trends are evident in the mobile sector with open-source initiatives like OpenAirInterface (OAI) [60] and Open5GS [61], which enable the deployment of modular 5G infrastructures. Hence, we rely on the unified standardization efforts to handle the interoperability challenges and direct the focus of this manuscript towards network availability and sovereignty in multi-vendor networks.

However, these works do not consider network availability. To the best of our knowledge, only our previous work [24] addresses the availability of multi-vendor networks. In [24], we discussed the Manufacturer Assignment for Availability (MAA) problem, i.e., finding the best manufacturer assignment to the nodes in the network such that network availability is maximized. Our proposed Non Linear Program (NLP) solution, *Zohra*, assigns manufacturers and finds the optimal paths for each flow in the network given a cost constraint. *Zohra* is also evaluated in our current work to

compare its performance against *Iroh*, the MILP proposed in this work. The comparison is detailed in Sec. VI.

D. MAXIMIZING NETWORK SOVEREIGNTY

Current literature on multi-vendor networks focuses on the modeling [57], interoperability issues [56], network security and trust guarantees [62], and techno-economic analysis [63]. However, they do not study the impact of manufacturer failures. Other works investigate issues in establishing a sovereign infrastructure [20], and propose a hierarchical stacking model to understand the digital capacity of a geographical region [64]. However, they do not quantify or explore solutions to improve sovereignty. Three metrics based on centrality metrics and graph theory to measure a nation's sovereignty with respect to the Submarine Cable Networks (SCNs) were proposed [65]. However, they do not apply to a conventional optical core network with multiple vendors.

Other works study network heterogeneity to improve resilience and sovereignty, i.e., to remove shared vulnerabilities across all the nodes by introducing variations in the nodes in the form of hardware and software configurations [66], [67]. The most notable one, [25], focuses on improving network security and resilience by solving the *Diversity Assignment Problem (DAP)*. *Diversity Assignment Problem-Integer Linear Program (DAP-ILP)* introduces network diversity by changing some nodes to 'variant nodes', which have similar properties as the original nodes, but do not possess the same vulnerabilities. Though *DAP* does not consider a multi-vendor network, it focuses on removing common points of failure and reducing the impact of a mass-exploit of a shared vulnerability by an attacker. Therefore, *DAP* [25] can be seen as a variation of the MAS problem. Hence, *DAP* is evaluated in this manuscript as state-of-the-art and compared in Sec. VI. However, there are two issues in [25]: (i) *DAP* suffers from scalability issues, and (ii) [25] does not quantify the resilience offered by introducing heterogeneity through a metric. In other words, it does not quantify the network's sovereignty.

We have also considered network sovereignty in our previous work. Our papers [69], [70] focus on the impact of multiple manufacturers in Data Center Networks (DCNs) and provide guidelines to DCN operators to improve network sovereignty. We also developed a heuristic denoted as *MCS-H*, based on MCSs in [37] to maximize network sovereignty in core networks. A flow's MCS consists of components that, when failed, cause the flow to fail. If all the components of the MCS are from the same manufacturer, and if that manufacturer is unavailable, then the MCS fails, causing the flow to fail. Therefore, *MCS-H* assigns nodes from a MCS to different manufacturers such that multiple manufacturers need to fail for the flow to fail. The simultaneous unavailability of multiple manufacturers is more unlikely, and hence *MCS-H* provides a good solution for the MAS problem. However, *MCS-H* discussed in [37]

is only a heuristic and hence provides a fast but sub-optimal solution. Moreover, similar to [25] and [37] does not quantify a network's sovereignty.

Our previous work [9] addresses the aforementioned issue by introducing the PSD score metric to measure network sovereignty based on the manufacturer assignment. Each flow in the network can be routed via several paths. The PSD score metric rewards each path based on the degree of manufacturer diversity in its paths. For example, if there are several manufacturers in a path, the failure of any of those manufacturers would cause that path to fail. Therefore, it is advantageous to have fewer manufacturers in a path. It is also advantageous to have multiple paths between the source and destination, with each path having different manufacturers. This would prevent single points of failure. Hence, each path's PSD score is calculated by finding the reciprocal of the number of manufacturers in that path. Consequently, the flow's PSD score is calculated as the sum of the PSD scores of all the paths for that flow. Additionally, we also proposed *Naga*, our MILP formulation, to solve the MAS problem based on the PSD score. However, *Naga* also suffers from scalability issues because there are several flows in a network, with each flow having hundreds of paths. *Naga* overcomes this issue by considering only k shortest paths, where choosing an appropriate k is a challenge. Hence, *Naga* does not use the advantage of all the redundancy in the network to maximize sovereignty. Moreover, if there are several paths with similar lengths, like in a DCN, choosing the appropriate paths is a challenge. However, since *Naga* is still a strong solution to the MAS problem, we evaluate it as state-of-the-art and compare it with our new approach in Sec. VI.

Our work in [10] combats the drawback of *Naga* [9] using MCSs. In [10], we propose the CSC score metric to quantify network sovereignty. Instead of considering a flow's several possible paths, CSC score rewards the diversity in the flow's MCSs. This is based on the same reasoning for the *MCS-H* in [37]. If there are more manufacturers in the MCS of a flow, then the MCS is less likely to fail, making the flow more resilient to manufacturer failures. Each flow has many MCSs. An MCS's CSC score is calculated as the reciprocal of the sum of the manufacturers in that MCS. A flow is only as strong as its weakest MCS. Hence, a flow's CSC score is calculated as the minimum MCS-CSC score across all the MCSs of that flow. We also proposed the *CSC-ILP* [68], an ILP based on the CSC score [10] to solve the MAS problem. *CSC-ILP* is fast and provides a more holistic manufacturer assignment because it considers all the redundancy in the network, unlike *Naga* in [9]. Hence, *CSC-ILP* is also evaluated as state-of-the-art in our current work and compared with our new approach in Sec. VI.

Table 1 differentiates the state-of-the-art based on their primary area of focus, the implementation method, and the extent of holistic optimization considering all the paths in the network. The features discussed in Table 1 are relevant to network availability and sovereignty as discussed in this manuscript. Table 2 lists the advantages, limitations, and

TABLE 1. Comparison of relevant state-of-the-art approaches evaluated in this work.

Feature	[24]	[48]	[9]	[10], [68]	[37]	[25]	[39]	[40]	Current
Denoted as, in this work	<i>Zohra</i>	<i>Spine-H</i>	<i>Naga</i>	<i>CSC-ILP</i>	<i>MCS-H</i>	<i>DAP</i>	IC	EDDC	<i>Iroh</i>
Focusing availability	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Focusing sovereignty	No	No	Yes	Yes	Yes	Subjective	Yes	Yes	Yes
Sovereignty quantified	No	No	PSD score.	CSC score	No	No	No	No	CSD score
Method	NLP	Heuristic	MILP	ILP	Heuristic	MILP	Heuristic	Heuristic	MILP
Considers all network paths	No	No	No	Yes	Yes	Yes	No	No	Yes

TABLE 2. Comparison of state-of-the-art approaches: advantages, limitations, and scalability.

Name	Method	Advantages	Limitations	Scalability
<i>Zohra</i> [24]	NLP	Jointly optimizes manufacturer assignment and routing under a cost constraint; directly addresses availability in multi-vendor networks.	Does not address sovereignty; considers only working and protection paths, not all network redundancy; NLP may converge to local optima.	Moderate — NLP complexity grows with network size; not well suited to large topologies.
<i>Spine-H</i> [48]	Heuristic	Fast execution; routes working paths through a high-availability spine, improving flow availability.	Requires very high-capacity spine links, infeasible for large networks; exploits only working and protection paths; no sovereignty or multi-vendor assignment.	Moderate — heuristic itself is fast, but the underlying ILP for spine selection is not scalable.
<i>Naga</i> [9]	MILP	Introduces the Path Set Diversity (PSD) score to quantify sovereignty; jointly optimizes manufacturer assignment and routing; strong baseline for the MAS problem.	Considers only k shortest paths — choice of k is non-trivial and may omit important paths; does not address availability; suboptimal in dense topologies with many equal-length paths.	Poor — path enumeration per flow grows rapidly; scalability bottleneck in large or dense networks.
<i>CSC-ILP</i> [10], [68]	ILP	Leverages MCSs to capture all network redundancy without path enumeration; Cut Set Coloring (CSC) score provides a holistic sovereignty quantification; faster and more complete than <i>Naga</i> .	Does not address availability; CSC score may not capture worst-case scenarios when MCS sizes vary widely.	Good — MCS-based formulation avoids path enumeration, but ILP complexity can still grow in large networks with many flows and MCSs.
<i>MCS-H</i> [37]	Heuristic	Efficiently distributes MCS nodes across manufacturers to reduce single-vendor failure risk; fast execution; leverages full network redundancy via MCSs.	Sub-optimal: no optimality guarantee; sovereignty is not quantified; does not address availability.	High — heuristic runtime is low; scales to large networks, though solution quality may degrade for complex topologies.
<i>DAP</i> [25]	MILP	Reduces shared vulnerabilities by introducing heterogeneous “variant” nodes; improves resilience against mass exploits of common vulnerabilities; considers all network paths.	Does not model a true multi-vendor network; sovereignty is not quantified; availability is not addressed; focus is on security rather than dependability.	Poor — scalability issues are explicitly acknowledged; MILP complexity limits applicability to small or medium-sized topologies.
IC [39]	Heuristic	Captures global structural vulnerability by identifying nodes whose removal most effectively isolates regions; improves over degree-only metrics.	Purely topological — does not model manufacturer assignments, availability values, or sovereignty directly; requires additional steps to yield practical assignments.	High — centrality computation is polynomial; applicable to large networks, but acts as a pre-processing heuristic rather than a full optimizer.
EDDC [40]	Heuristic	Unifies degree, information entropy, and node distance into a single metric; identifies influential nodes more effectively than single-metric approaches; balances local and global network properties.	Same as IC: topology-only; no direct optimization of availability or sovereignty; assignment decisions require additional logic.	High — metric computation scales polynomially; same limitations as IC when used as a standalone basis for manufacturer assignment.

scalability of the state-of-the-art. In our previous works [9], [10], [37], [58], we advocated for the inclusion of sovereignty as a secondary dependability attribute as outlined in [1]. Our current work goes one step further to combine the MAA and MAS problems to discuss the Manufacturer Assignment for Availability and Sovereignty (MAAS) problem as formulated in Sec. IV.

III. MINIMAL CUT SET (MCS)-BASED AVAILABILITY ESTIMATION AND CUT SET DIVERSITY (CSD) METRIC

This section explains the usage of MCSs in the (i) flow availability estimation for maximizing network availability

and (ii) CSD metric evaluation for maximizing network sovereignty. We use the sample topology in Fig. 2a to explain our novel approaches.

A. MCS-BASED AVAILABILITY ESTIMATION

A Reliability Block Diagram (RBD) is a simple graphical tool that is used to calculate the availability of a system based on its components and their interconnection [71]. For a network flow, the flow’s availability A_f can be evaluated using a RBD based on the nodes in the paths between the source and destination and their interconnection with the links. However, the accurate expression to evaluate A_f is

nonlinear. For example, A_r of the flow from source S to destination T in the sample topology shown in Fig. 2a can be calculated from the flow's RBD shown in Fig. 2b as follows.

$$A_r = A_S \cdot (1 - (1 - A_A)(1 - A_C)) \cdot (1 - (1 - A_B)(1 - A_D)) \cdot A_T, \quad (1)$$

where, A_n is node n 's availability. However, it is infeasible to write linear constraints in an ILP formulation to maximize A_r . This is the major reason for most previous literature, as discussed in Sec. II-C, to consider only the working and backup paths in optimization problems. To overcome the aforementioned infeasibility, we investigate MCSs. Using MCSs in network availability evaluation is common practice [72], [73]. Furthermore, MCSs are also commonly used in establishing bounds for a system's availability [74], [75].

When all the nodes in a flow's MCS fail, the flow fails. Hence, the MCS's availability, A_{MCS} , can be numerically evaluated as the probability that at least one node in the MCS is functional. Each MCS must be perceived as a limitation on A_r , that is, A_{MCS} acts as the upper bound of A_r . For a flow with multiple MCSs, when the weakest MCS with the lowest availability (A_{MCS}^*) is considered, the upper bound is closer to A_r . This hypothesis was tested in our previous work [34], where we correlated A_r for all the flows in several topologies with the availability estimations ($\hat{A}_r = A_{MCS}^*$). A high positive correlation of around 0.9 was observed [34], greatly supporting our hypothesis.

As an example, let us consider the sample topology in Fig. 2a and the flow between S and T . Let the nodes S and T have availabilities of 0.99, A and C have availabilities of 0.9, and B and D have availabilities of 0.8. Then, from Eq. 1, A_{ST} is calculated as 0.9315. The two MCSs for said flow are (A, C) and (B, D) . The MCS is available if at least one node in the MCS is available. This can be modeled as a parallel connection in the RBD and evaluated as,

$$A_{MCS} = 1 - \prod_{n \in MCS} (1 - A_n). \quad (2)$$

Hence, $A_{(A,C)}$ and $A_{(B,D)}$ are calculated as 0.99 and 0.96, respectively. From this example, we see that (B, D) is the weaker MCS with lower availability, and $\hat{A}_r = A_{(B,D)} = 0.96$ it is a closer upper bound to the actual $A_r = 0.9315$.

The high positive correlation between A_r and $\hat{A}_r$, means that improving $\hat{A}_r$ should also improve A_r . Moreover, since $\hat{A}_r$ consists of only one MCS, this availability can be modeled as a linear expression in the logarithmic domain [49] as further explained in Sec. IV-C. This novel approach allows us to maximize for network availability, considering all the MCSs, and in turn considering all the paths in the network. This is the first approach to maximize network availability, leveraging the complete redundancy available in the network.

B. CUT SET DIVERSITY (CSD) METRIC

The Path Set Diversity (PSD) score metric [9] rewards manufacturer diversity across different k -shortest paths for each flow. Since it does not consider all the possible paths,

it does not utilize the redundancy in the network efficiently. The Cut Set Coloring (CSC) score metric [10] rewards manufacturer diversity in the MCS, thereby utilizing the redundancy in the network. However, the CSC score metric performs sub-optimally because it does not consider the manufacturer diversity across different MCSs for a single flow. It only considers the weakest MCS, i.e., the MCS with the lowest MCS-CSC score for evaluation. To overcome the drawbacks of the PSD score metric [9] and CSC score metric [10] we propose a novel Cut Set Diversity (CSD) score metric. It is based on MCSs and it considers the manufacturer diversity across the flow's different MCSs. Let us better understand the CSD metric with the example topology in Fig. 2a.

Let us assume that there is a flow r between source S and destination T . The MCSs of this flow are (A, C) and (B, D) . Let us assume that there are four manufacturers- Yellow (Y), Purple (P), Green (G), and Red (R), from which the network operator can choose to buy the different nodes A , B , C , and D . We assume that S and T are always available and exclude them from the evaluation because if the source or destination fails, the flow fails anyway. Let us consider the two manufacturer assignments- Assignment-1 and Assignment-2, shown in Figs. 2c and 2d.

First, let us calculate the CSC scores [10] for the two assignments. The MCS-CSC score is given by,

$$\text{MCS-CSC score} = \begin{cases} 0, & \text{if } |M_{MCS}| = 1 \\ \frac{|M_{MCS}|}{|MCS|}, & \text{otherwise} \end{cases}, \quad (3)$$

where, $|M_{MCS}|$ and $|MCS|$ denote the number of manufacturers in the MCS and the number of nodes in the MCS, respectively. There are two manufacturers in each MCS of the flow in both assignments. Therefore, both MCSs have the MCS-CSC score of 1 in both assignments. Hence, the Flow-CSC score in both assignments is 1. This means that the CSC score metric ranks both assignments as fully sovereign. Now let us consider various manufacturer failure scenarios to check the performance of the two assignments in Figs. 2c and 2d. Table 3 has the failure scenarios in the first row and shows if the flow survives the corresponding failure scenario for the two assignments in their corresponding rows, respectively. Since there are four manufacturers, Y, P, G , and R , there are four one-manufacturer failures, six two-manufacturer failure combinations, and four three-manufacturer failure combinations, as seen in Table 3. These manufacturer failure combinations are the same regardless of the topology. Hence, if four manufacturers are used for the Germany_17 topology seen in Fig. 1, the failure combinations will remain the same. How the topology handles the manufacturer failures is the crucial difference.

Let us look at Assignment-1's performance. Here, both MCSs have the Y and P manufacturers in them. Therefore, any failure scenario with Y and P failing will cause the MCSs to fail, and consequently the flow to fail. There is one two-manufacturer combination- (Y, P) , and two

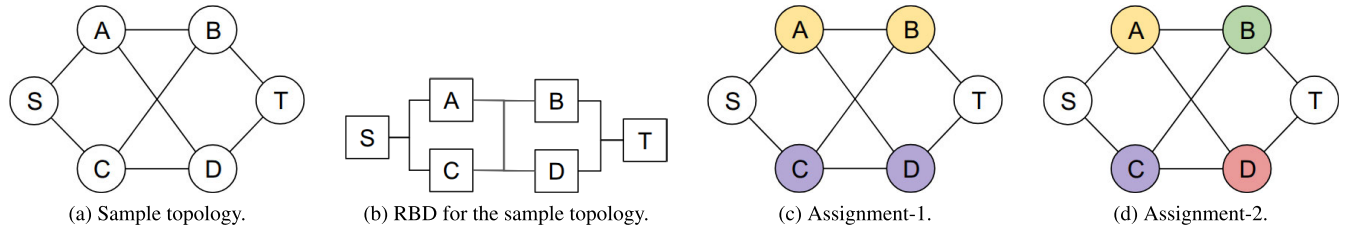


FIGURE 2. Sample topology and its corresponding Reliability Block Diagram (RBD) in Fig. (a) and (b), respectively. Two example manufacturer assignments in Figs. (c) and (d) for the topology shown in Fig. (a) as discussed in Sec. III. The colors, Yellow (Y), Purple (P), Green (G), and Red (R) denote different manufacturers from which the nodes are purchased. The source node *S* and destination node *T* are always available and excluded from the evaluation because if the source or destination fails, the flow fails regardless.

TABLE 3. Manufacturer failure scenarios and their impact on the assignments in Figs. 2c and 2d for the flow from *S* to *T*. Failure scenarios *Y*, *P*, *G*, and *R* correspond to the failures of manufacturers Yellow, Purple, Green, and Red, respectively. Assignment-2 suffers from more failure scenarios than Assignment-1.

	One-manufacturer failures				Two-manufacturer failures						Three-manufacturer failures			
Failure scenario	Y	P	G	R	Y, P	Y, G	Y, R	P, G	P, R	G, R	Y, P, G	Y, P, R	Y, G, R	P, G, R
Assignment-1	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	×	×	✓	✓
Assignment-2	✓	✓	✓	✓	×	✓	✓	✓	✓	×	×	×	×	×

three-manufacturer combinations- (Y, P, G) and (Y, P, R) , that could cause flow failure. On the other hand, for Assignment-2, the first MCS ($MCS_1 = (A, C)$) has the *Y* and *P* manufacturers, while the second MCS ($MCS_2 = (B, D)$) has the *G* and *R* manufacturers. This assignment experiences flow failure when at least one of the MCS fails. Hence, any manufacturer failure in combination with (Y, P) or (G, R) will cause the flow to fail. This is also seen in Table 3. Assignment-2 fails for two two-manufacturer failures- (Y, P) and (G, R) , and all three-manufacturer failures.

Though manufacturer diversity is maximized in both the MCSs in Assignment-2, the diversity across the two MCSs plays a significant disadvantage for Assignment-2. From a qualitative perspective of sovereignty, introducing two more manufacturers in the second MCS creates additional dependency on the two manufacturers, thereby increasing the chances for flow failure. On the other hand, Assignment-1 removes this additional dependency by reusing the same set of manufacturers in both MCSs. Therefore, Assignment-1 is more sovereign than Assignment-2. This shows that having more manufacturers in the network is not always the best solution to improve sovereignty. This counter-intuitive inference also shows that the CSC score metric [10] does not quantify a network's sovereignty accurately. Hence, the new Cut Set Diversity score metric should have the following properties.

- (P1) Maximizing manufacturer diversity inside a MCS to minimize dependencies on a particular manufacturer must be rewarded.
- (P2) Minimizing manufacturer diversity across multiple MCSs for the same flow to exclude additional dependencies must be rewarded.

Based on properties (P1) and (P2), we propose the CSD score metric as follows. The Flow-CSD (CSD_r) score is given by,

$$CSD_r = \sum_{m=1}^{|M|-1} (\omega_m \times |\phi_m(r)|), \quad (4)$$

where $|M|$ is the number of manufacturers available, $|\phi_m(r)|$ is the number of m -manufacturer failure scenarios that flow r can tolerate, and ω_m is the weight assigned to tolerating an m -manufacturer failure. That is, the CSD_r score is defined as the weighted sum of the number of manufacturer failure scenarios that a particular manufacturer assignment can tolerate. The higher the CSD_r score, the higher the sovereignty of the flow. ω_m should be higher for smaller m because it is more important to tolerate the failures of fewer manufacturers, i.e., tolerating 1-manufacturer failures is more important than tolerating 3-manufacturer failures. In order to incorporate this inverse relationship, we assume that the weighting factor ω_m is equal to the reciprocal of m , i.e., $\omega_m = \frac{1}{m}$.

Let us better understand the CSD score metric with the two example manufacturer assignments presented in Figs. 2c and 2d. In Assignment-1, four 1-manufacturer failures, five 2-manufacturer failures, and two 3-manufacturer failures can be tolerated, i.e., $|\phi_1(r)| = 4$, $|\phi_2(r)| = 5$, and $|\phi_3(r)| = 2$. Hence, the CSD_r score for Assignment-1, based on Eq. 4 is obtained as,

$$CSD_r = \left(\frac{1}{1} \times 4\right) + \left(\frac{1}{2} \times 5\right) + \left(\frac{1}{3} \times 2\right) = 7.16. \quad (5)$$

Similarly, in Assignment-2, four 1-manufacturer failures, four 2-manufacturer failures, and no 3-manufacturer failures can be tolerated, i.e., $|\phi_1(r)| = 4$, $|\phi_2(r)| = 4$, and $|\phi_3(r)| = 0$. Hence, the CSD_r score for Assignment-2, based on Eq. 4, is obtained as,

$$CSD_r = \left(\frac{1}{1} \times 4\right) + \left(\frac{1}{2} \times 4\right) + \left(\frac{1}{3} \times 0\right) = 6. \quad (6)$$

From Eqs. 5 and 6, Assignment-1 is more sovereign than Assignment-2. Therefore, our novel CSD score metric evaluates network sovereignty based on manufacturer assignments more accurately than the current state-of-the-art.

In Sec. IV, we employ our approach to maximize network availability (discussed in Sec. III-A) together with our CSD

Algorithm 1 Summary of *Iroh*'s Formulation**Decision Variable:**

$b_{m,n} \in \{0, 1\}, \forall m, n$ (1 if manufacturer m is assigned to node n).

Objectives:

Maximize availability $\mathcal{A}$. (Sec. IV-D1)

Maximize sovereignty $\mathcal{S}$. (Sec. IV-D2)

Constraints:

C1: Single manufacturer assignment. (Eq. 7)

C2: Network cost $\leq$ threshold. (Eq. 8)

Intermediates:

I1: Calculate RBD availability for all MCSs. (Eq. 11, 12)

I2: Identify weakest MCS availability. (Eq. 11, 13)

I3: Map manufacturer combinations per flow. (Eq. 14–20)

I4: Compute weighted CSD score. (Eq. 23)

score metric (discussed in Sec. III-B) to formulate a Mixed Integer Linear Program (MILP), called *Iroh*, to hierarchically maximize network availability and sovereignty.

IV. MANUFACTURER ASSIGNMENT FOR AVAILABILITY AND SOVEREIGNTY (MAAS) AND IROH

We mainly focus on the Manufacturer Assignment for Availability and Sovereignty (MAAS) problem. Given a network topology as a graph G with vertices N and edges E , its expected traffic, the number of manufacturers available ($|M|$), the availability of the nodes from each manufacturer (A_m), and the cost of the nodes from each manufacturer (C_m), the MAAS problem can be stated as follows.

(Q1) What is the best manufacturer assignment to maximize network availability and sovereignty, given a cost threshold?

The MAAS problem aims to assign manufacturers (colors) to nodes in the network (graph). Hence, it can be viewed as a modified graph coloring problem [76], with the major difference being that MAAS has a limitation on the number of manufacturers (colors), while traditional graph coloring problems have infinite colors. In this section, we introduce our Mixed Integer Linear Program (MILP) formulation, called *Iroh* (pronounced *l'ɑi.roʊʊ*, adapted from Japanese, meaning 'color'), to solve the MAAS problem. There are two sections to *Iroh*: (i) maximizing network availability with *Iroh-A*, and (ii) maximizing network sovereignty with *Iroh-S*. *Iroh*'s problem formulation is summarised in Alg. 1 and detailed in the following subsections.

A. INPUT CONSTANTS

Let the network graph G have nodes as vertices N and links as edges E . Let $M = \{0, 1, \dots, |M| - 1\}$ and $|M|$ be the set and the number of manufacturers available, respectively. A flow r is represented by its source s_r and destination t_r , while R represents the set of all the flows in the network. Let U_m be

the unavailability of manufacturer m in the log scale. That is, if manufacturer m has an availability of 0.99, then the unavailability of m is 0.01, while $U_m = \log 0.01 = -2$. Let C_m be the cost of one node from manufacturer m . We assume that the availability of a manufacturer is proportional to the cost of the node from that manufacturer [24], [68]. Let C_T be the maximum cost threshold of the network. The total cost of the network is the sum of the costs of the nodes from the different manufacturers. Let K_r be the set of all MCSs of flow r . Let $k_{r,j}$ be flow r 's j^{th} MCS. Let x be a possible manufacturer combination represented as $x = (x_m | x_m \in \mathbb{Z}_2, m \in M)$, where x_m is the binary notation equal to one if manufacturer m is present in $k_{r,j}$. For example, in the sample manufacturer Assignment-2 in Fig. 2d, $MCS_1 = (A, C)$, has manufacturers Y and P . Hence, $x_Y = 1$, $x_P = 1$, $x_G = 0$, $x_R = 0$. Thus, $x = (1100)$. Similarly, MCS_2 has manufacturers G and R , making $x = (0011)$. Let X be the set of all possible manufacturer combinations. All-zero combinations of x (like $x = (0000)$) are excluded because at least one manufacturer is necessary in a MCS. For example, if $|M| = 2$, then $X = \{(01), (10), (11)\}$.

In a communication network, it is unlikely to have multiple manufacturers failing simultaneously. Therefore, the CSD score metric should prioritize the ability of the network to survive fewer manufacturers failing. This is achieved with w_x , the weighting factor associated with manufacturer combination x . w_x is chosen such that the network is rewarded with a higher CSD score when it can successfully tolerate 1-manufacturer failures, and rewarded less when it can successfully tolerate more unlikely 3-or 4-manufacturer failures. Hence, w_x must be in the range (0,1). In this work, we assume w_x to be the reciprocal of the number of manufacturers present in combination x . w_x is similar to ω in Eq. 4. We also evaluated *Iroh* with different values and functions for the weighting factor. For example, we evaluated $w_x = 0.1^{\sum_{m \in M} x_m}$, $w_x = (0.1 \cdot \sum_{m \in M} x_m)^2$ and other weighting combinations. Due to space constraints, we do not plot the results for these trials. The simplest weight of $w_x = \frac{1}{\sum_{m \in M} x_m}$

consistently gives the best results by focusing on greater rewards for tolerating fewer manufacturer failures for the topologies considered in this work. The user can use different values for w_x as per their requirement. Identifying the optimal w_x applicable to all networks is marked as future work. Table 4 summarizes the constants used in *Iroh*.

B. VARIABLES

For an easier understanding of the following variables summarized in Table 5, consider the example manufacturer Assignment-2 in Fig. 2d. For the flow r between S and T , the following statements are noted. In MCS_1 , nodes A and C are assigned to the zeroth (Y) and first (P) manufacturers, respectively. In MCS_2 , nodes B and D are assigned to the second (G) and third (R) manufacturers, respectively.

TABLE 4. Constants and their symbols in *Iroh*.

Symbols	Constants
$G = (N, E)$	Graph
N	Set of vertices
E	Set of edges
$M = \{0, 1, 2, \dots, M - 1\}$	Set of manufacturers
$ M $	No. of manufacturers
$r = (s_r, t_r)$	Flow = (source, destination)
R	Set of flows
U_m	Unavailability of manufacturer m in the log scale
C_m	Cost of node from manufacturer m
C_T	Network cost threshold
K_r	Set of flow r 's MCSs
$k_{r,j}$	Flow r 's j^{th} MCS
$x = (x_m x_m \in \mathbb{Z}_2, m \in M)$	Possible manufacturer combination
X	Set of all possible manufacturer combinations except all-zero combination
$w_x = \frac{1}{\sum_{m \in M} x_m}$	Weight for a combination x

TABLE 5. Variables and their symbols in *Iroh*.

Symbols	Variables
$b_{m,n}$	Binary variable equal to one if manufacturer m is assigned to node n
$z_{r,j}$	Continuous variable equal to the unavailability of $k_{r,j}$
Z_r	Continuous variable equal to the unavailability of flow r based on MCSs in the logarithmic scale
μ_r	Continuous variable equal to the maximum unavailability out of all $k_{r,j}$ of flow r
$q_{m,r,j}$	Binary variable equal to one if manufacturer m is used in $k_{r,j}$
$f_{x,r,j}$	Binary variable equal to one if combination x is used in $k_{r,j}$
$F_{x,r}$	Binary variable equal to one if combination x is used in flow r
$L_{\tilde{x},r}$	Binary variable equal to one according to $F_{x,r}$ to get all manufacturer combinations for which flow r fails
CSD_r	Continuous variable equal to the CSD score of flow r

- 1) Let the binary variable $b_{m,n}$ be equal to one if manufacturer m is assigned to node n . Hence, only $b_{0,A}, b_{1,B}, b_{2,C}$ and $b_{3,D}$ are one for Assignment-2.
- 2) Let the continuous variable $z_{r,j}$ be equal to the unavailability of $k_{r,j}$, flow r 's j^{th} MCS. This is further explained in Eq. 11.
- 3) Let the continuous variable Z_r be equal to the unavailability of flow r in the logarithmic scale based on MCSs. This is further explained in Eq. 12.
- 4) Let the continuous variable μ_r be the highest unavailability amongst all the MCSs of flow r , i.e., the unavailability of the weakest MCS. This is further explained in Eq. 13.
- 5) Let the binary variable $q_{m,r,j}$ be equal to one if manufacturer m is used in $k_{r,j}$, flow r 's j^{th} MCS. Hence, only $q_{0,r,1}, q_{1,r,1}, q_{2,r,2}$ and $q_{3,r,2}$ are one for Assignment-2.
- 6) Let the binary variable $f_{x,r,j}$ be equal to one if combination x is used in $k_{r,j}$, flow r 's j^{th} MCS. Hence, only $f_{(1100),r,1}$ and $f_{(0011),r,2}$ are one for Assignment-2.
- 7) Let the binary variable $F_{x,r}$ be equal to one if the combination x is used in flow r . Hence, only $F_{(1100),r}$ and $F_{(0011),r}$ are one for Assignment-2.
- 8) The binary variable $L_{\tilde{x},r}$ is set to one for all the manufacturer combinations for which flow r fails. For example, since $F_{(1100),r}$ is equal to one for Assignment-2, any failure combination where m_0 and m_1 fail, causes the flow to fail. Hence, $L_{1100,r}, L_{1101,r}, L_{1110,r}, L_{1111,r}$ are set to one.
- 9) Let CSD_r be equal to the flow's CSD score.

C. PROGRAM FORMULATION

The model-specific constraints are formulated as follows.

- 1) Each node must be assigned to only one manufacturer.

$$\sum_{m \in M} b_{m,n} = 1, \quad \forall n \in N. \quad (7)$$

- 2) Total network cost must not exceed the cost threshold. The cost threshold can be specified by the operator.

$$\sum_{n \in N} \left(\sum_{m \in M} (C_m \times b_{m,n}) \right) \leq C_T. \quad (8)$$

- 3) The MCS's availability A_{MCS} is modeled in a RBD by a parallel connection of all the nodes in the MCS as per Eq. 2. Since Eq. 2 is non-linear, we use the logarithmic scale. The MCS's unavailability U_{MCS} and its logarithm z_{MCS} can be evaluated based on Eq. 2 as a function of the node unavailability u_n and its logarithm U_n as,

$$U_{MCS} = \prod_{n \in MCS} (1 - A_n) = \prod_{n \in MCS} u_n, \quad (9)$$

$$z_{MCS} = \log(U_{MCS}) = \sum_{n \in MCS} U_n. \quad (10)$$

However, node n 's unavailability depends on the manufacturer m , from which n is procured. Hence, applying Eq. 10 to the nodes in $k_{r,j}$, $z_{r,j}$ is obtained as,

$$z_{r,j} = \sum_{n \in k_{r,j}} \left(\sum_{m \in M} (b_{m,n} \times U_m) \right), \quad \forall r \in R, k_{r,j} \in K_r. \quad (11)$$

- 4) The failure of any of the MCSs can cause the flow to fail. Hence, the MCSs can be arranged in series in the RBD to determine an estimate of the flow availability. Hence, we evaluate the Z_r , the unavailability of a flow r in the logarithmic scale, as the sum of all the unavailabilities of flow r 's MCSs in the logarithmic scale.

$$Z_r = \sum_{k_{r,j} \in K_r} z_{r,j} \quad \forall r \in R. \quad (12)$$

- 5) Since the weakest MCS, i.e., the MCS with the lowest availability, is an estimate of the lower bound of the unavailability, this can also be used in the objective to minimize unavailability. Hence, the maximum unavailability out of all of the flow r 's MCSs is stored in μ_r .

$$\mu_r = \max\{z_{r,j} | k_{r,j} \in K_r\} \quad \forall r \in R \quad (13)$$

- 6) Set $q_{m,r,j}$ equal to one if manufacturer m is used in in $k_{r,j}$, flow r 's j^{th} MCS, using the binary 'OR' operator ($\vee$). Modern optimization tools are capable of transforming the binary operators into linear constraints automatically. In this work, we use Gurobi [77], [78], which automates this via "general constraints," while keeping the underlying model a standard MILP using the standard Big-M approach. The Big-M approach acts like a mathematical light switch that converts logical conditions into linear constraints by using a binary variable and a large constant to activate or deactivate a rule [79].

$$q_{m,r,j} = \bigvee_{n \in k_{r,j}} b_{m,n} \quad \forall m \in M, r \in R, k_{r,j} \in K_r. \quad (14)$$

- 7) Set $f_{x,r,j}$ equal to one if manufacturer combination x is used in $k_{r,j}$, flow r 's j^{th} MCS, using the binary 'AND' operator ($\wedge$). $f_{x,r,j}$ can be indirectly set using $q_{m,r,j}$.

$$f_{x,r,j} = \bigwedge_{x_m \in x} (\widetilde{q_{m,r,j}}) \quad \forall r \in R, k_{r,j} \in K_r, x \in X, \quad (15)$$

where

$$\widetilde{q_{m,r,j}} = \begin{cases} q_{m,r,j} & \text{if } x_m = 1 \\ 1 - q_{m,r,j} & \text{if } x_m = 0. \end{cases} \quad (16)$$

For example, if $|M| = 3$ and only the first manufacturer is used in in $k_{r,j}$, i.e., $x = (100)$, then

$$f_{(100),r,j} = q_{0,r,j} \wedge (1 - q_{1,r,j}) \wedge (1 - q_{2,r,j}) = 1. \quad (17)$$

Other values of x like (001, 010, 011, ..) except (100) for the same r and j set $f_{x,r,j}$ to zero. Hence, $f_{x,r,j}$ denotes if the manufacturer combination x is present in $k_{r,j}$.

- 8) Each flow r has many MCSs. It is necessary to keep track of all the manufacturer combinations across all the MCSs of flow r . $F_{x,r}$ is the variable that is set to one if manufacturer combination x is used in flow r . It can be obtained using the binary 'OR' operator ($\vee$) over all the $f_{x,r,j}$ variables for a specific flow r .

$$F_{x,r} = \bigvee_{k_{r,j} \in K_r} f_{x,r,j} \quad \forall r \in R, x \in X. \quad (18)$$

Eq. 18 also removes duplicate entries. For example, consider the example Assignment-1 in Fig. 2c. Here, both the MCSs have the same manufacturers, Y and P . Counting the same manufacturer combination twice for the same flow is redundant. Eq. 18 forces $F_{x,r}$ to one if a manufacturer combination x is used at least once in any of the flow r 's MCSs.

- 9) Set $L_{\tilde{x},r}$ equal to one according to $F_{x,r}$ to get all manufacturer combinations for which flow r fails.

$$F_{x,r} = \bigwedge_{\tilde{x}_m \in \tilde{x}} (L_{\tilde{x},r}) \quad \forall r \in R, \tilde{x} \in X, x \in X, \quad (19)$$

where

$$\tilde{x}_m = \begin{cases} 1 & \text{if } x_m = 1 \\ 1 \text{ or } 0 & \text{if } x_m = 0. \end{cases} \quad (20)$$

For example, consider the Assignment-2 in Fig. 2d. Here, there are four available manufacturers, $|M| = 4$. MCS_1 has the Y and P manufacturers present. Hence, any failure scenario where Y and P fail causes the flow to fail. For example, failure scenarios like (Y, P, G) and (Y, P, R) also lead to flow failure. From Eq. 18, $F_{(1100),r}$ is set to one. Since $L_{\tilde{x},r}$ tracks all failure combinations, $L_{(1100),r}$, $L_{(1101),r}$, $L_{(1110),r}$, and $L_{(1111),r}$ should be set to one. This is achieved by,

$$F_{(1100),r} = L_{(1100),r} \wedge L_{(1101),r} \wedge L_{(1110),r} \wedge L_{(1111),r}, \quad (21)$$

$$1 = L_{(1100),r} \wedge L_{(1101),r} \wedge L_{(1110),r} \wedge L_{(1111),r}. \quad (22)$$

- 10) Set CSD_r equal to flow r 's CSD score.

$$CSD_r = \sum_{x \in X} (w_x \times (1 - L_{x,r})) \quad \forall r \in R, \quad (23)$$

where constant w_x represents the weight for manufacturer combination x , which can be set by the user. Eq. 23 is equivalent to Eq. 4.

D. OBJECTIVES

This work focuses on the hierarchical optimization of network availability and sovereignty. Hence, there are separate objective functions for each.

1) MAXIMIZING NETWORK AVAILABILITY: *IROH-A*

Eqs. 7, 8, 11–13, and their associated variables are sufficient to maximize network availability. We evaluated different objectives to identify the best solution.

(*Iroh-A(1)*) : Minimize the sum of all flow unavailabilities.

$$\min \left(\sum_{r \in R} Z_r \right) \quad (24)$$

(*Iroh-A(2)*) : Minimize the worst-case (highest) flow unavailability.

$$\min \{ \max \{ Z_r | r \in R \} \} \quad (25)$$

(*Iroh-A(3)*) : Minimize the maximum MCS unavailability among all the flows.

$$\min \{ \max \{ \mu_r | r \in R \} \} \quad (26)$$

(*Iroh-A(4)*) : Minimize the sum of all flows' worst-case (highest) MCS unavailabilities.

$$\min \left(\sum_{r \in R} \mu_r \right) \quad (27)$$

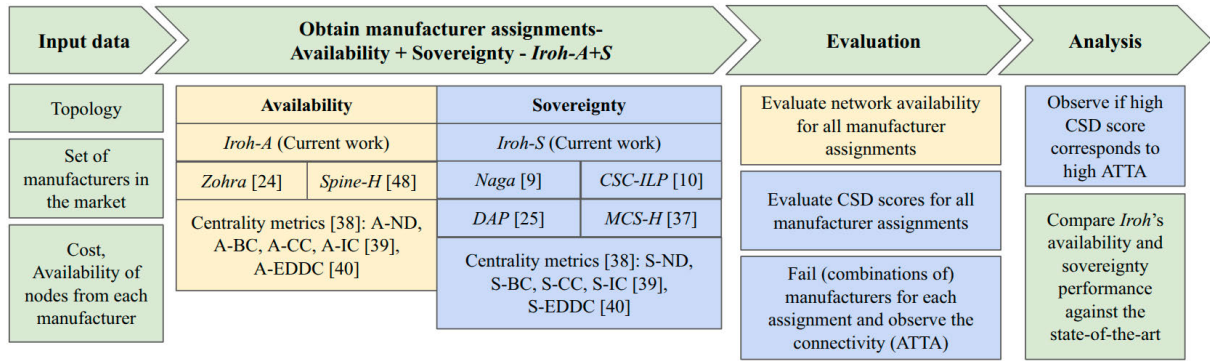


FIGURE 3. Evaluation workflow adopted in this work. The boxes colored in yellow and blue correspond to the Manufacturer Assignment for Availability (MAA) and Manufacturer Assignment for Sovereignty (MAS) problems, respectively. The boxes in green are common to both.

Note that the flows can be prioritized in the objective formulations as per the operator's requirements, thereby awarding more importance to certain flows. In this work, we consider all flows to have equal priority. Based on our experiments discussed in Sec. VI, we found that Objectives (*Iroh-A(3)*) and (*Iroh-A(4)*) in Eqs. 26 and 27 respectively, perform the best in globally improving availability across all the flows. Hence, we combined Objectives (*Iroh-A(3)*) and (*Iroh-A(4)*) sequentially in two ways:

(*Iroh-A(3, 4)*): First objective (*Iroh-A(3)*), then (*Iroh-A(4)*).

(*Iroh-A(4, 3)*): First objective (*Iroh-A(4)*), then (*Iroh-A(3)*).

Only the order of execution (priority) varies between the two new combinations. The results for all six objectives are compared and explained in Sec. VI-B using Fig. 5. Since objective (*Iroh-A(4,3)*) performs the best by maintaining the highest average flow availability and best worst-case flow availability, we use this in the evaluation of the hierarchical optimization.

2) MAXIMIZING NETWORK SOVEREIGNTY: *IROH-S*

Eqs. 7, 8, 14–20, and 23, and their associated variables are sufficient to maximize network sovereignty.

(*Iroh-S*) : Maximize the sum of all the flows' CSD score.

$$\max \left(\sum_{r \in R} CSD_r \right) \quad (28)$$

Similar to the availability objective formulations, the flows can be weighted by the operator to award more importance to certain flows. In this work, we consider all flows to have equal weights. We also tested the max-min approach to maximize the sovereignty of the flow with the lowest sovereignty. This yielded no improvement. Hence, we show the evaluation only for the Objective (*Iroh-S*) in Eq. 28 in Sec. VI.

3) HIERARCHICAL OPTIMIZATION OF AVAILABILITY AND SOVEREIGNTY

To solve the MAAS problem, we use all the constraints mentioned in Sec. IV-C and combine the objectives discussed in Secs. IV-D1 and IV-D2. For network availability optimization, we only consider the updated objective (*Iroh-A(4,3)*).

It is infeasible to combine the objectives for availability and sovereignty in a single weighted multi-objective expression because availability and sovereignty are not measured on the same scale. Normalizing the sovereignty measurement would compromise important information about the worst-case CSD_r. Hence, we adopt a sequential formulation to accommodate both objectives. There are two alternatives to achieve this.

- i) *Iroh-A+S*: First, availability is maximized by objective (*Iroh-A(4,3)*). Then, sovereignty is maximized by *Iroh-S*.
- ii) *Iroh-S+A*: First, sovereignty is maximized by objective *Iroh-S*. Then, availability is maximized by (*Iroh-A(4,3)*).

Table 6 summarizes all the objective functions evaluated in this work. Note that the availability and sovereignty optimizations can work as standalone solutions to the MAA and MAS problems, respectively. The results of the evaluation are discussed in Sec. VI.

V. EVALUATION WORKFLOW

This section explains our workflow as seen in Fig. 3.

- (i) First, the inputs such as the topology, number of manufacturers available, and cost and availability of nodes from the different manufacturers are taken.
- (ii) Then, the MILP formulation described in Sec. IV is evaluated on Python using the Gurobi [77] optimization suite, and the manufacturer assignments are saved for *Iroh-A*, *Iroh-S*, and *Iroh-A+S* as described in Secs. IV-D1, IV-D2, and IV-D3, respectively. Similarly, the state-of-the-art and centrality metrics-based manufacturer assignments are also obtained as discussed in Secs. V-B and V-A.
- (iii) The manufacturer assignments are then evaluated in terms of availability and sovereignty.
 - a) First, the network availability as an aggregate of all the flows' availability is evaluated on Python using RBD evaluation tools [29], [30].
 - b) Second, the network's CSD score as an aggregate of all the flows' CSD scores and the impact of manufacturer failures are evaluated (Sec. V-C).

TABLE 6. Summary of *Iroh*'s objectives, constraints, and intermediate evaluations corresponding to Alg. 1.

Model	Priority of Objectives		Required
	First	Second	
<i>Iroh-A</i> (1)	Minimize sum of all flow unavailabilities (Eq. 24).	None	C1, C2, I1
<i>Iroh-A</i> (2)	Minimize the worst-case flow unavailability (Eq. 25).	None	C1, C2, I1
<i>Iroh-A</i> (3)	Minimize the maximum MCS unavailability among all the flows (Eq. 26).	None	C1, C2, I2
<i>Iroh-A</i> (4)	Minimize the sum of all flows' worst-case MCS unavailabilities (Eq. 27).	None	C1, C2, I2
<i>Iroh-A</i> (3,4)	<i>Iroh-A</i> (3) (Eq. 26).	<i>Iroh-A</i> (4) (Eq. 27).	C1, C2, I2
<i>Iroh-A</i> (4,3)	<i>Iroh-A</i> (4) (Eq. 27).	<i>Iroh-A</i> (3) (Eq. 26).	C1, C2, I2
<i>Iroh-S</i>	Maximize the sum of all the flows' CSD score (Eq. 28).	None	C1, C2, I3, I4
<i>Iroh-S+A</i>	<i>Iroh-S</i> (Eq. 28).	<i>Iroh-A</i> (4,3) (Eq. 27, Eq. 26).	C1, C2, I2, I3, I4
<i>Iroh-A+S</i>	<i>Iroh-A</i> (4,3) (Eq. 27, Eq. 26).	<i>Iroh-S</i> (Eq. 28).	C1, C2, I2, I3, I4

(iv) Finally, we verify if higher CSD scores correspond to higher resilience against manufacturer failures to consolidate the CSD score as a valid metric to measure network sovereignty. Additionally, we compare *Iroh* with the state-of-the-art approaches.

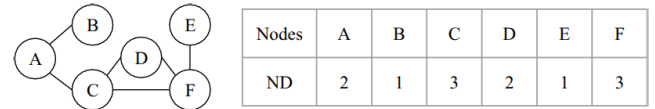
A. APPLICATION OF CENTRALITY METRICS

In this work, we consider three traditional centralities- ND, BC, and CC [38] and two state-of-the-art modern centralities- IC [39] and EDDC [40], as discussed in Sec. II-B. There are two sets of assignments possible for each centrality metric- one for availability and another for sovereignty.

1) CENTRALITY APPLICATION FOR AVAILABILITY

When the main focus is on availability, all the important nodes must be purchased from the manufacturer with the highest availability. We assume a homogeneous assignment to satisfy the cost constraint [24]. For example, consider the nodes in the graph G with ND centrality values as mentioned in Fig. 4. The higher the centrality, the more important the node is. Hence, the nodes are rewritten in descending order of ND as $\{C, F, A, D, B, E\}$. When two nodes have the same ND, they are written in alphabetical order. When there are two manufacturers ($|M| = 2$), the nodes are divided into $M_0 = \{C, F, A\}$ and $M_1 = \{D, B, E\}$. Similarly, if $|M| = 3$, then, $M_0 = \{C, F\}$, $M_1 = \{A, D\}$, and $M_2 = \{B, E\}$. Hence, the most important nodes are purchased from the most available manufacturer.

We assign nearly the same number of nodes to each manufacturer to ensure the cost threshold is obeyed. The assumption of a homogeneous assignment, distributing an approximately equal number of nodes to each manufacturer,

**FIGURE 4.** Example topology and the Nodal Degree (ND) of the nodes.

serves as a heuristic to satisfy cost constraints. In real-world network procurement, high-availability manufacturers typically warrant a higher price. By enforcing a homogeneous distribution of the nodes across the manufacturers, we prevent a monopoly scenario where the budget is exhausted by purchasing the entire network from the most expensive vendor. Hence, this strategy ensures that while critical nodes receive the highest possible protection to maximize network availability within the budget, the overall procurement remains economically feasible while also minimizing an overwhelming dependency on a particular vendor under a capped total expenditure threshold. BC, CC, IC, and EDDC-based assignments also follow the same procedure. The heuristics for availability are marked as A-ND, A-BC, A-CC, A-IC, and A-EDDC, adapted from the heuristics discussed in [24].

2) CENTRALITY APPLICATION FOR SOVEREIGNTY

When the main focus is on sovereignty, an operator would not purchase all the important nodes from the same manufacturer to avoid shared vulnerabilities. Therefore, the nodes of similar importance should be assigned to different manufacturers. For example, in a graph G with vertices V , the nodes are arranged in descending order of their centralities. Then, we assign the nodes with comparable centralities to different manufacturers alternatively. For example, consider the graph G and the ND centrality values mentioned in Fig. 4. The nodes are rewritten in descending order of ND as $\{C, F, A, D, B, E\}$. When two nodes have the same ND, they are written in alphabetical order. When there are two manufacturers ($|M| = 2$), the nodes are divided into $M_0 = \{C, A, B\}$ and $M_1 = \{F, D, E\}$. Similarly, if $|M| = 3$, then, $M_0 = \{C, D\}$, $M_1 = \{F, B\}$, and $M_2 = \{A, E\}$. Hence, nodes of similar importance are distributed across different manufacturers. BC, CC, IC, and EDDC-based assignments also follow the same procedure. The heuristics for sovereignty are marked as S-ND, S-BC, S-CC, S-IC, and S-EDDC, adapted from the heuristics discussed in [9], [10], and [37].

B. IMPLEMENTING OTHER SOLUTIONS FOR COMPARISON

The state-of-the-art on availability and sovereignty is detailed in Secs. II-C and II-D and summarized in Table 1.

Zohra [24] and *Spine-H* [48] are the approaches considered for the MAA problem. Given the topology as a graph, the set of manufacturers, and the cost and availability of nodes from the manufacturers, the NLP in *Zohra* returns the appropriate manufacturer assignment directly. *Zohra* is

implemented as described in [24]. *Spine-H* [48] considered the only link availabilities. It is modified in our work to consider node availability for a fair comparison. The high-availability spine subnetwork is generated as a Minimum Spanning Tree (MST) using Kruskal's algorithm. The nodes of this MST are then arranged in descending order according to their Nodal Degrees (NDs), considering only the links that are in the MST. Then, the most critical nodes are assigned to the manufacturer with the highest availability, while the least critical nodes are assigned to the manufacturer with the least availability, similar to the procedure in Sec. V-A1.

Naga [9], *MCS-H* [37], *CSC-ILP* [10], and *DAP* [25] are the approaches considered for the MAS problem as explained in Sec. II-D. The PSD score-based ILP in *Naga* assigns the least number of manufacturers in each path for each flow in the network to minimize the dependency on particular manufacturers. However, when there are several simple paths between the source and destination, *Naga* considers k -shortest paths. k is a parameter that can be set by the operator. *MCS-H* is a heuristic that tries to assign the nodes in each MCS to different manufacturers to avoid a single point of failure in the MCS. *CSC-ILP* implements the same logic as *MCS-H* using an ILP formulation. *DAP* is an ILP formulation that tries to diversify nodes in the network by using diverse variants of the nodes at different locations in the network. Note that the terminology, 'diverse variants', in *DAP*, is comparable to using different manufacturers in our current work. The implementations of *Naga*, *MCS-H*, *CSC-ILP*, and *DAP* are exactly as described in [9], [25], [37], and [68], respectively.

C. MANUFACTURER FAILURE EVALUATION

We simulate all possible combinations of manufacturer failures to study their impact on the network's connectivity. When a manufacturer fails, all the nodes from the manufacturer fail simultaneously. For example, when there are three manufacturers ($M = \{0, 1, 2\}$), the possible combinations of failures include $\{(0), (1), (2), (0, 1), (1, 2), (0, 2)\}$. The case where all manufacturers fail is not considered. For each combination of failures, the Average Two Terminal Availability (ATTA) of the network is evaluated. ATTA is defined as the percentage of successfully connected source-destination pairs in the network under failure scenarios. A fully sovereign network has 100% ATTA under any failure scenario. However, this is unrealistic.

VI. RESULTS

This section explains our input parameters and the corresponding results. The key findings are summarized in Table 7 and they are supported with explanations in the following subsections.

A. INPUT PARAMETERS

The input parameters in this work are summarized in Table 8. We evaluate four topologies- Abilene, Polska, Germany_17, and Nobel_EU with different numbers of manufacturers

($|M| \in \{2, 3, 4\}$). For each topology, flows between all possible source-destination pairs are considered, except the flows with one-hop paths. The node availabilities from different manufacturers (A_M) vary linearly between 0.85 and 0.95. For example, if there are two manufacturers ($|M| = 2$), then the node availabilities from the manufacturers $m0$ and $m1$ are $A_{m0} = 0.85$ and $A_{m1} = 0.95$. Similarly, if $|M| = 3$, then $A_{m0} = 0.85$, $A_{m1} = 0.9$, and $A_{m2} = 0.95$.

The cost of premium services and components with higher availability is higher than standard services and components with lower availability [80]. For example, the Cisco Catalyst 9300X-48HX switch has an MTBF of 185,420 hours [81], while the Cisco 9606R has an MTBF of 4,113,900 hours [82] at a significantly higher cost. Similarly, Atlassian cloud services offer higher uptime SLAs in higher-priced tiers [83]. Hence, in this work, we assume that a node's availability is directly proportional to its cost [9], [24] to ease our calculations and provide a proof of concept. This assumption does not consider other factors, such as performance, power consumption, etc. The user must change the costs according to their network's requirements. Additionally, we set the cost threshold C_T in Eq. 8 to the numerical average cost to build the network as formulated in Eq. 29.

$$C_T = |N| \times \frac{\sum_{m \in M} C_m}{|M|} \quad (29)$$

B. MAXIMIZING AVAILABILITY

We represent network availability as the distribution of the flows' availabilities using box plots in Fig. 5. The Y and X axes show the flow availability and the various manufacturer assignments as discussed in Secs. IV-D1, V-B, and V-A, for the Germany_17 topology [4] shown in Fig. 1, when four manufacturers are considered ($|M| = 4$). The golden star, horizontal black line inside the box, and the small circles represent the mean, median, and outliers, respectively. *Iroh-A(4)*, *Iroh-A(4,3)*, and *Iroh-A+S* have the highest average flow availability. They also have the highest worst-case availabilities. Note that *Iroh-A(4,3)*, and *Iroh-A+S* are also constructed based on *Iroh-A(4)*. However, all three assignments have minor variations among them according to the objectives employed. These minor variations do not change the network availability, but impact the sovereignty, as discussed in Sec. VI-C.

Iroh-A(4) outperforms *Iroh-A(1)* and *Iroh-A(2)* because *Iroh-A(4)* is more granular, evaluating each flow's worst-case MCS unavailability, whereas *Iroh-A(1)* and *Iroh-A(2)* work more superficially, considering the flow's unavailabilities. *Zohra* [24] is a close second, because *Zohra* focuses on working path availability while *Iroh-A(4)* focuses on overall flow availability.

Moreover, all the approaches that maximize sovereignty have poor network availability. This clearly shows that there is a tradeoff between availability and sovereignty. The centrality metrics-based heuristics also perform poorly.

TABLE 7. Key findings and summary of comparison results listing the best performers in availability and sovereignty based optimizations.

Method	Availability	Sovereignty	Runtime	Remark
Availability-optimized assignments				
<i>Iroh-A(4)</i>	Best	Poor	Fast	Availability-only priority
<i>Iroh-A(4,3)</i>	Best, with highest worst-case availability	Poor	Fast	Availability-only priority with an additional objective to maximize worst-case availability
<i>Iroh-A+S</i>	Best, with highest worst-case availability	Poor	Fast	Availability first, then sovereignty
<i>Zohra</i>	Close 2nd	Poor	Slow	State-of-the-art availability baseline
Sovereignty-optimized assignments				
<i>Iroh-S</i>	Poor	Best	Moderate	Sovereignty-only priority
<i>Iroh-S+A</i>	Poor	Best	Moderate	Sovereignty first, then availability
<i>DAP</i>	Poor	Best	Very slow	Small topologies only; infeasible at scale
<i>CSC-ILP</i>	Poor	Close 2nd	Fast	Large topologies; fast sub-optimal alternative
<i>MCS-H</i>	Poor	Moderate	Fastest	Very large topologies; quick approximation
<i>Naga (k=2)</i>	Poor	Moderate	Moderate	Improves at higher k; ILP may become infeasible
Centrality based heuristics				
Centrality-based	Poor	Poor	Fast	Not recommended for either objective

TABLE 8. List of input options.

Input Parameters	Choices			
Topologies		V	E	Source
	Abilene	11	14	[84]
	Polska	12	18	[4]
	Germany_17	17	26	[4]
	Nobel_EU	28	41	[4]
Number of manufacturers and their corresponding availabilities	2	$A_{m0} = 0.85, A_{m1} = 0.95$		
	3	$A_{m0} = 0.85, A_{m1} = 0.9, A_{m2} = 0.95$		
	4	$A_{m0} = 0.85, A_{m1} = 0.883, A_{m2} = 0.917, A_{m3} = 0.95$		
Node cost	The node cost from a manufacturer is equal to its availability from that manufacturer.			

Hence, network operators must act according to their priorities. If the operator prefers to maximize availability first and then sovereignty, *Iroh-A+S* is the most suitable assignment. All the topologies for all the $|M|$ values follow the same trends as seen in Fig. 5. Additionally, increasing $|M|$ did not impact the network availability significantly.

C. MAXIMIZING SOVEREIGNTY

First, we aim to show that the CSD score is a valid metric. Second, we aim to show that *Iroh-S* and *Iroh-S+A* have the best sovereign manufacturer assignment.

The network's CSD score is represented as the distribution of Flow-CSD scores in Fig. 6 across different numbers of manufacturers ($|M|$) for the Germany_17 topology. *Iroh-S*, *Iroh-S+A*, and *DAP* have the best average and worst-case Flow-CSD scores. Flow-CSD score increases with $|M|$. *CSC-ILP* is a close second. Hence, for a large topology, *CSC-ILP* can be used to reduce computation time. If there is no box (like for *Iroh-A+S*, $|M| = 2$), then the Flow-CSD scores are concentrated at the mean. The assignments focusing on availability first, like *Iroh-A(4,3)* and *Iroh-A+S*, and the centrality metrics-based heuristics have poor CSD scores.

To show the validity of the CSD metric, we need to show that there is a correlation between the CSD score

and the Average Two Terminal Availability (ATTA) under different failure scenarios. Hence, we follow the failure evaluation in Sec. V-C. We show the ATTA results for the Germany_17 topology with four manufacturers ($|M| = 4$) in Fig. 7a, where each line corresponds to a manufacturer assignment. The X axis shows all the manufacturer failure combinations, with the three grey boxes denoting one, two, and three-manufacturer failures, respectively. However, this graph is difficult to compare. Hence, we redraw this graph by rearranging the lines in descending order inside each box for each n -manufacturer failures in Fig. 7b. Fig. 7b does not have X-axis labels because the rearrangement of each line reorders the X axis differently for each line (manufacturer assignment).

Based on Fig. 7b, *Iroh-S*, *Iroh-S+A*, and *DAP* have the best ATTA under failure scenarios. They have identical performance. Hence, *Iroh-S* and its extension *Iroh-S+A* provide the most sovereign manufacturer assignment without the computational complexity of *DAP*. Furthermore, *MCS-H* and *CSC-ILP* maintain high connectivity under one-manufacturer failures, but deteriorate when more manufacturers fail. *Naga* has weaker performance, when a small k value of 2 is considered. *Naga* is expected to improve when k is higher. However, this adds to the complexity, deeming the ILP infeasible at some point. Hence, *MCS-H* and *CSC-ILP* can be used as a quick alternative for very large topologies. The centrality metrics-based heuristics also have poor ATTA even for a one-manufacturer failure, making them unsuitable.

The assignments focusing on availability first, like *Iroh-A(4,3)* and *Iroh-A+S*, show poor ATTA. For example, both *Iroh-A(4,3)* and *Iroh-A+S* have their ATTA dropped to around 20% even for a one-manufacturer failure. This means that they have a very high dependency on a particular manufacturer, making them the least sovereign assignments. Once again, this observation shows that there exists a tradeoff between availability and sovereignty. If the operator prefers to maximize sovereignty first, then *Iroh-S+A* is recommended. The other topologies also follow the same trend.

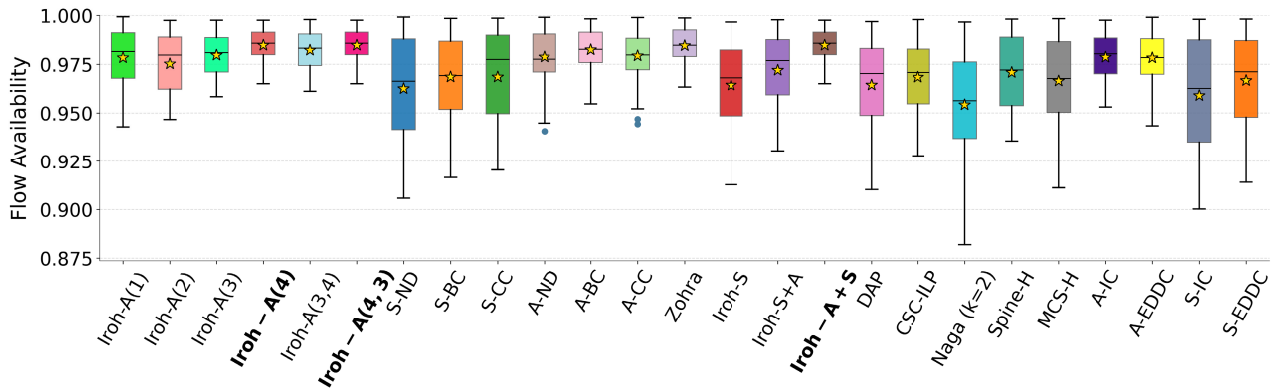


FIGURE 5. Network availability represented as a distribution of all the flow availabilities for Germany_17 with four manufacturers ($|M| = 4$). The golden star, horizontal black line inside the box, and the small circles represent the mean, median, and outliers, respectively. *Iroh-A(4)*, *Iroh-A(4,3)*, and *Iroh-A+S* present the best average flow availability and the highest worst-case availabilities, while *Zohra* is a close second. All the approaches that maximize sovereignty have poor network availability.

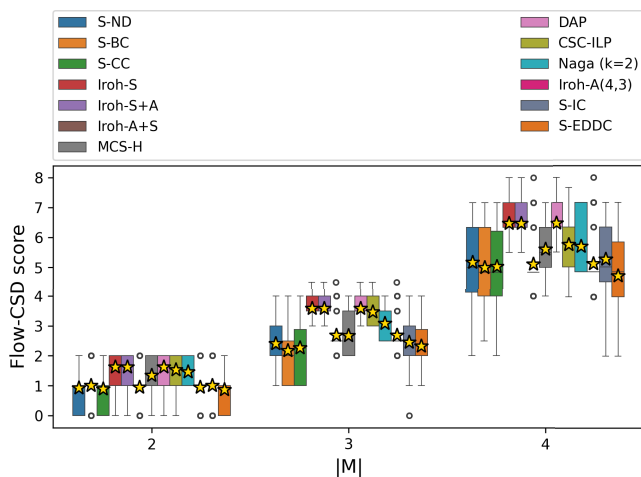


FIGURE 6. Network-CSD score represented as the distribution of Flow-CSD scores across different numbers of manufacturers ($|M|$) for the Germany_17 topology. The golden star, horizontal black line inside the box, and the small circles represent the mean, median, and outliers, respectively. *Iroh-S*, *Iroh-S+A*, and *DAP* have the best average and worst-case Flow-CSD scores. If there is no box (like for *Iroh-A+S*, $|M| = 2$), then most of the flows have their CSD scores close to the mean.

Based on Figs. 6, 7a, and 7b, we can infer the following.

- 1) When CSD score is high, ATTA is also high, and vice versa. Hence, the CSD score metric is a valid metric to quantify network sovereignty.
- 2) *Iroh* shows superior performance at lower complexity compared with the state-of-the-art.

D. ENSURING IROH'S SCALABILITY

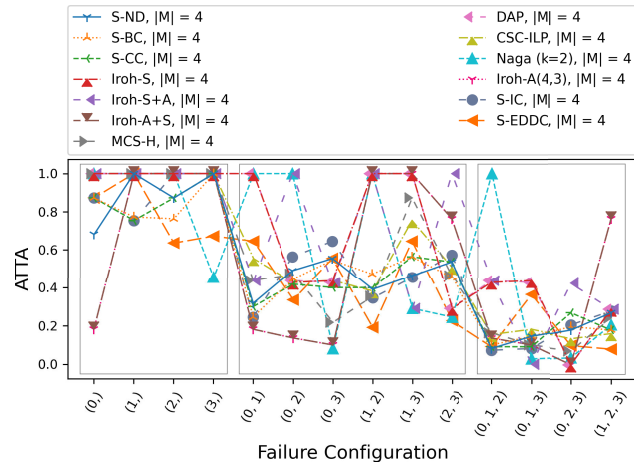
Iroh was evaluated on an AMD Ryzen 7 3700X octa-core processor with 32 GB RAM. For the Germany_17 topology (17 nodes and 26 edges) shown in Fig. 1 with four manufacturers ($|M| = 4$), *Iroh-A* and *Iroh-S* took 1 second and 27 minutes, respectively. For the Nobel_EU topology (28 nodes and 41 edges) with four manufacturers ($|M| = 4$), *Iroh-A* and *Iroh-S* took 5 seconds and 14 hours, respectively. The

lower time required for *Iroh-A* can be attributed to its fewer constraints and intermediate evaluations. Although slower than *Iroh-A*, *Iroh-S* is still significantly faster than *DAP*, as it took over three hours for Germany_17 and crashed out of memory for Nobel_EU.

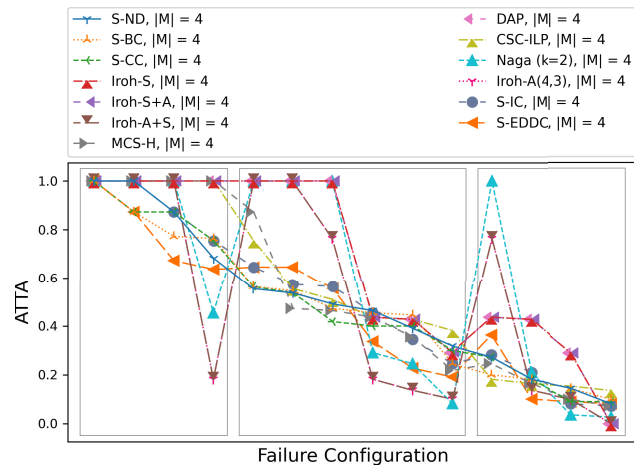
DAP uses a brute force optimization logic, whereas *Iroh-S* uses MCSs to reduce the solution space. Hence, *Iroh* is at least an order of magnitude faster than *DAP*. Moreover, our new work [85] provides a much faster way to evaluate MCSs in a network, enabling faster pre-processing for *Iroh*. *CSC-ILP* and *MCS-H* are faster due to their low complexity, but do not produce optimal results. *Iroh*'s runtime for a larger topology depends on the size and the number of the MCSs for all the source-destination pairs in the network, rather than the actual size of the topology in terms of the number of nodes and edges. Hence, if a very large topology with several nodes is considered, *Iroh* can be sped up by restricting the MCSs to only those that are smaller than a threshold. This is because very large MCSs are unlikely to fail and can be omitted to save on computation time. Furthermore, *Iroh* is a network planning solution. It needs to be run only once, likely on high-performance servers or clusters, to get the optimal manufacturer assignment in the design stage of the network. Therefore, the longer runtimes for *Iroh* for larger topologies with bigger MCSs are not a major concern.

E. CHALLENGES IN PRACTICAL DEPLOYMENT

Though the CSD score metric and *Iroh* are theoretically sound, a practical deployment of nodes in the network based on this study poses challenges. Similar to any multi-vendor network, problems such as interoperability, security, efficient network management, sharing limited performance-related information between different manufacturers, etc., exist [55], [56], [57]. Furthermore, *Iroh* is a static solution. However, a communication network is ever-evolving in terms of traffic, capacity requirements, energy requirements, and manufacturer availability. The temporal variability in



(a) Average Two Terminal Availability (ATTA) vs. failure configurations. For example, configuration (0, 1) means manufacturers 0 and 1 have failed.



(b) Average Two Terminal Availability (ATTA) arranged in descending order, grouped by the number of failing manufacturers. The X-axis represents failure configurations. *Iroh-S*, *Iroh-S+A*, and *DAP* consistently avoid manufacturer dependencies.

FIGURE 7. Comparing *Iroh*'s performance against the state-of-the-art, focusing on sovereignty, for the Germany_17 topology with $|M| = 4$.

TABLE 9. Comparison of the different sovereignty metrics.

Metric	Basis	Advantage	Limitation
CSD (current work)	MCSs	Considers all redundant paths in the network.	For very large networks, the optimization runtime is high.
CSC [10]	MCSs	Considers all redundant paths in the network. Very fast.	The optimization is sub-optimal because it does not consider the manufacturer diversity across MCSs for the same flow.
PSD [9]	k-Shortest Simple Path Sets	Can be tuned to consider only the paths that the flow can potentially use.	It is sub-optimal if the flow is allowed to take a path not included in the considered set because it does not consider all the redundant paths in the network.

such a planning problem needs to be addressed with more formulations that account for the future. We mark this as our future work.

VII. CONCLUSION

Modern Ultra Reliable Low Latency Communication (URLLC) applications need high network availability, while the current global political scene demands stable national networks with minimal external dependencies. Regions like Europe, Africa, and Asia [19], [20], and companies like Amazon, Microsoft, and Google [86] have promised sovereign solutions in the future. Though data, digital, and technology sovereignty have been discussed in detail [6], network sovereignty is yet to be explored.

To the best of our knowledge, we are the first to investigate the tradeoff between cost, availability, and sovereignty. We (i) proposed a new optimization approach to maximize network availability, (ii) proposed the novel Cut Set Diversity (CSD) metric to measure a network's sovereignty based on the manufacturers in the network, (iii) evaluated *Iroh*, our Mixed Integer Linear Program (MILP) to optimize network availability and sovereignty, and (iv) demonstrated *Iroh*'s performance gains in terms of improvements in network availability and sovereignty and reduced computational complexity against other state-of-the-art methods. Additionally, we also discussed how to ensure *Iroh*'s scalability for very large networks. Our major inferences from this work that serve as guidelines are as follows.

- 1) Increasing the number of manufacturers increases sovereignty, but does not necessarily impact availability.
- 2) Network availability can be optimized holistically, considering the complete redundancy in the network by leveraging the relationship between flow availability and Minimal Cut Set (MCS) availability.
- 3) The impact of manufacturer failures can be reduced if diversity is maximized within the MCS and minimized across MCSs of a flow.
- 4) CSD score validly quantifies network sovereignty.
- 5) *Iroh* is a powerful optimization tool that can be used to maximize network availability and sovereignty according to the user's preference- *Iroh-A+S* if availability is prioritized and *Iroh-S+A* if sovereignty is prioritized.
- 6) For very large networks, *Iroh* can be relaxed by discarding very large MCSs.

Table 9 summarizes the different sovereignty metrics to help network operators use the appropriate metric and its corresponding optimization as per the problem at hand. Our current work only considers node manufacturer failures. We intend to extend this work to include link manufacturer failures in the future. Moreover, we assume manufacturer failures to be independent. However, manufacturer failures can be correlated due to several reasons, such as multiple manufacturers from the same country being banned, the unavailability of one manufacturer affecting the supply chain of another manufacturer, subcomponent sharing between manufacturers, etc. Hence, we are currently extending the CSD score metric and *Iroh* to include correlated manufacturer failures. Furthermore, we consider a static network from a graph perspective. In the future, we plan to extend *Iroh*'s formulation to include temporal traffic data and

link capacities and devise adequate congestion control and restoration mechanisms. Additionally, we are interested in extending the CSD metric for multi-domain networks managed by different geographical regions and different networking technologies.

REFERENCES

- [1] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable Secure Comput.*, vol. 1, no. 1, pp. 11–33, Jan. 2004.
- [2] A. Sulta. (2023). *Ultra Reliable Low Latency Communications*. [Online]. Available: <https://www.3gpp.org/technologies/urllc-2022>
- [3] D. Tipper, A. Babay, B. Palanisamy, and P. Krishnamurthy, "Network connectivity resilience in next generation backhaul networks: Challenges and future opportunities," *IEEE Trans. Netw. Service Manage.*, vol. 21, no. 5, pp. 5321–5334, Oct. 2024.
- [4] S. Orlowski, R. Wessälly, M. Pióro, and A. Tomaszewski, "SNDlib 1.0—Survivable network design library," *Networks*, vol. 55, no. 3, pp. 276–286, May 2010.
- [5] J. Bodin, C. Frémont, M.-D. Couzinet, and H. Rochais, *Les six livres de la République*, Chez Jacques du Puys Paris, vol. 6, 1986.
- [6] M. Hellmeier and F. von Scherenberg, "A delimitation of data sovereignty from digital and technological sovereignty," in *Proc. ECIS Res. Papers*, 2023, pp. 1–19.
- [7] J. Edler, "Technology sovereignty: From demand to concept [technologiesouveränität: Von der forderung zum konzept]," Fraunhofer Inst. Syst. and Innov. Res., Karlsruhe, Germany, Tech. Rep. 02/2020, 2020.
- [8] A. Weber, S. Reith, M. Kasper, D. Kuhlmann, J.-P. Seifert, and C. Krauß, "Sovereignty in information technology," Karlsruhe Inst. Technol. (KIT), Inst. Technol. Assessment Syst. Anal. (ITAS), Karlsruhe, Germany, Tech. Rep., 2018.
- [9] S. Janardhanan, M. Samonaki, P. E. Heegaard, W. Kellerer, and C. Mas-Machuca, "Network sovereignty: A novel metric and its application on network design," *IEEE Trans. Rel.*, vol. 74, no. 2, pp. 1–15, Jun. 2025.
- [10] S. Janardhanan, R. Agarwal, W. Kellerer, and C. Mas-Machuca, "How to build a sovereign network?—A proposal to measure network sovereignty," *IEEE Commun. Mag.*, pp. 1–7, 2026.
- [11] A. Hamid. (May 2025). *T-Mobile Customer Says Pittsburgh Outage Was a Reminder That AT&T and Verizon Remain Ahead*. [Online]. Available: https://www.phonearena.com/news/T-Mobile-customer-says-Pittsburgh-outage-was-a-reminder-that-AT-T-and-Verizon-remain-ahead_id170000
- [12] M. Loveridge, G. Remy, N. Kourra, R. Genieser, A. Barai, M. Lain, Y. Guo, M. Amor-Segan, M. Williams, T. Amietszajew, M. Ellis, R. Bhagat, and D. Greenwood, "Looking deeper into the galaxy (note 7)," *Batteries*, vol. 4, no. 1, p. 3, Jan. 2018.
- [13] (2024). *O2 Network Outage*. [Online]. Available: https://www.ofcom.org.uk/siteassets/resources/documents/about-ofcom/bulletins/enforcement-bulletin/all-cases/cw_01235/decision-to-conclude-investigation--o2-net-work-outage?v=321087
- [14] H. M. Varghese and D. Shepardson. (2024). *Verizon Says Resolved Network Disruption; FCC Probing Co's Mobile Network Outage for Thousands of Users in US*. [Online]. Available: <https://www.reuters.com/business/media-telecom/verizons-network-down-thousands-users-downdetector-shows-2024-09-30/>
- [15] B. Fung. (2024). *We Finally Know What Caused the Global Techoutage and How Much It Cost*. [Online]. Available: <https://edition.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html>
- [16] (May 2025). *Telefonica Reestablishes Service in All of Spain After Partial Outage*. [Online]. Available: <https://www.reuters.com/markets/commodities/telefonica-spanish-network-update-causes-partial-communication-s-outage-2025-05-20/>
- [17] (2021). *Vulnerability Details: CVE-2021–0275*. [Online]. Available: <https://www.cvedetails.com/cve/CVE-2021-0275/>
- [18] (2013). *Vulnerability Details: CVE-2013-6026*. [Online]. Available: <https://www.cvedetails.com/cve/CVE-2013-6026/>
- [19] H. Li, X. Yang, H. Li, and X. Yang, "Interpretation of network sovereignty," *Co-governed Sovereignty Netw.: Legal Basis and Its Prototype & Appl. with MIN Archit.*, Springer, pp. 29–60, 2021.
- [20] D. Tipper and P. Krishnamurthy. (Aug. 2022). *Digital Sovereignty and Resilience*. [Online]. Available: <https://ssrn.com/abstract=4178621>
- [21] I. Stadnik, "Internet governance in russia—sovereign basics for independent runet," in *Proc. 47th Res. Conf. Commun., Inf. Internet policy*, 2019, pp. 1–16.
- [22] P. Leskin. (2019). *Here Are All the Major U.S. Tech Companies Blocked Behind China's 'Great Firewall'*. [Online]. Available: <https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5>
- [23] A. Braud, G. Fromentoux, B. Radier, and O. Le Grand, "The road to European digital sovereignty with gaia-X and IDSA," *IEEE Netw.*, vol. 35, no. 2, pp. 4–5, Mar. 2021.
- [24] S. Janardhanan, S. S. Indrasena, and C. Mas-Machuca, "Zohra: Joint routing and manufacturer assignment problem," in *Proc. IEEE Int. Workshop Tech. Committee Commun. Quality Rel. (CQR)*, Oct. 2023, pp. 19–24.
- [25] A. Newell, D. Obenshain, T. Tantilillo, C. Nita-Rotaru, and Y. Amir, "Increasing network resiliency by optimally assigning diverse variants to routing nodes," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 6, pp. 602–614, Nov. 2015.
- [26] A. Rauzy, "Mathematical foundations of minimal cutsets," *IEEE Trans. Rel.*, vol. 50, no. 4, pp. 389–396, 2001.
- [27] E. Ruijters and M. Stoelinga, "Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools," *Comput. Sci. Rev.*, vols. 15–16, pp. 29–62, Feb. 2015.
- [28] R. Patil, "An overview of fault tree analysis (FTA) method for reliability analysis," *J. Eng. Res. Stud.*, vol. 4, pp. 6–8, 2013.
- [29] S. Janardhanan, S. Badnava, R. Agarwal, and C. Mas-Machuca, "PyRBD: An open-source reliability block diagram evaluation tool," in *Proc. IEEE Int. Workshop Tech. Committee Commun. Quality Rel. (CQR)*, Oct. 2024, pp. 19–24.
- [30] S. Janardhanan, Y. Chen, and C. Mas-Machuca, "PyRBD++: An open-source fast reliability block diagram evaluation tool," in *Proc. 15th Int. Workshop Resilient Netw. Des. Model. (RNDM)*, 2025, pp. 1–7.
- [31] S. Janardhanan, Y. Chen, and C. Mas-Machuca, "Leveraging minimal path sets for reliability block diagram evaluation," in *Proc. IEEE Future Netw. World Forum (FNWF)*, Jan. 2026, pp. 1–6.
- [32] Z. Tang and J. Dugan, "Minimal cut set/sequence generation for dynamic fault trees," in *Proc. Annu. Symp. Rel. Maintainability (RAMS)*, 2004, pp. 207–213.
- [33] W. S. Jung, S. H. Han, and J. Ha, "A fast BDD algorithm for large coherent fault trees analysis," *Rel. Eng. Syst. Saf.*, vol. 83, no. 3, pp. 369–374, Mar. 2004.
- [34] S. Janardhanan, A. I. Gomez Ryfka, and C. Mas-Machuca, "Investigating the correlation between minimal cut set and flow availabilities," in *Proc. Würzburg Workshop Next-Generation Commun. Netw. (WueWoWas)*, 2025.
- [35] P.-C. Chang, "A path-based simulation approach for multistate flow network reliability estimation without using boundary points," *Rel. Eng. Syst. Saf.*, vol. 249, Sep. 2024, Art. no. 110237.
- [36] S. Janardhanan, R. Gazzah, W. Kellerer, and C. Mas-Machuca, "How important is that node?" *IEEE Rel. Mag.*, pp. 1–8, 2026.
- [37] S. Janardhanan, Y. M. Ali, R. Agarwal, and C. Mas-Machuca, "Improving network sovereignty—A minimal cut set approach," in *Proc. 24th Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2024, pp. 1–4.
- [38] A. Saxena and S. Iyengar, "Centrality measures in complex networks: A survey," 2020, *arXiv:2011.07190*.
- [39] O. Ugurlu, "Comparative analysis of centrality measures for identifying critical nodes in complex networks," *J. Comput. Sci.*, vol. 62, 2022, Art. no. 101738.
- [40] R. D. Shetty, R. M., K. R. Shetty, and M. T., "Enhanced complex network influential node detection through the integration of entropy and degree metrics with node distance," *Sci. Rep.*, vol. 15, no. 1, p. 31227, Aug. 2025.
- [41] S. Janardhanan, N. Felber, and C. Mas-Machuca, "Evaluating the impact of adding links on network availability and max-flow," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2024, pp. 1–3.
- [42] A. Roy, H. Zeng, J. Bagga, G. Porter, and A. C. Snoeren, "Inside the social network's (datacenter) network," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 4, pp. 123–137, Sep. 2015.
- [43] S. Sinche, O. Polo, D. Raposo, M. Femandes, F. Boavida, A. Rodrigues, V. Pereira, and J. Sá Silva, "Assessing redundancy models for IoT reliability," in *Proc. IEEE 19th Int. Symp. (WoWMoM)*, Jun. 2018, pp. 14–15.
- [44] R. Saeedinia, "Protection switching in communication networks," in *Proc. 16th Eur. Conf. Netw. Opt. Commun.*, Jul. 2011, pp. 20–23.

- [45] C. B. Serna, S. Janardhanan, E. Doğan, A. Sharma, and C. Mas-Machuca, "Dependency analysis of optical access networks on electrical distribution networks," in *Proc. 25th Anniversary Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2025, pp. 1–5.
- [46] S. Janardhanan and C. Mas-Machuca, "Availability modeling and evaluation of switches and data centers," in *Proc. 10th Int. Conf. Dependable Syst. Their Appl. (DSA)*, Aug. 2023, pp. 710–721.
- [47] T. A. Nguyen, D. Min, E. Choi, and T. D. Tran, "Reliability and availability evaluation for cloud data center networks using hierarchical models," *IEEE Access*, vol. 7, pp. 9273–9313, 2019.
- [48] A. Alashaikh, T. Gomes, and D. Tipper, "The spine concept for improving network availability," *Comput. Netw.*, vol. 82, pp. 4–19, May 2015.
- [49] D. A. Schupke and F. Rambach, "A link-flow model for dedicated path protection with approximative availability constraints," *IEEE Commun. Lett.*, vol. 10, no. 9, pp. 679–681, Sep. 2006.
- [50] M. Samonaki, C. B. Serna, and C. Mas-Machuca, "Survivable node-disjoint routing in multi-domain networks," in *Proc. IEEE Int. Conf. Commun.*, May 2023, pp. 4578–4583.
- [51] M. Samonaki and C. Mas-Machuca, "Optimal and reliable routing for multicast sessions in WDM networks," in *Proc. 20th Int. Conf. Design Reliable Commun. Netw. (DRCN)*, May 2024, pp. 115–122.
- [52] A. D. Sousa, D. Santos, and P. Monteiro, "Determination of the minimum cost pair of D-geodiverse paths," in *Proc. 13th Int. Conf. Design Reliable Commun. Netw.*, Mar. 2017, pp. 1–8.
- [53] J. Meza, T. Xu, K. Veeraraghavan, and O. Mutlu, "A large scale study of data center network reliability," in *Proc. Internet Meas. Conf.*, Oct. 2018, pp. 393–407.
- [54] J.-L. Auge, V. Curri, and E. Le Rouzic, "Open design for multi-vendor optical networks," in *Proc. Opt. Fiber Commun. Conf. Exhib. (OFC)*, Mar. 2019, pp. 1–3.
- [55] A. Gabilondo, Z. Fernandez, Á. Martín, R. Viola, M. Zorrilla, P. Angueira, and J. Montalbán, "5G SA multi-vendor network interoperability assessment," in *Proc. IEEE Int. Symp. Broadband Multimedia Syst. Broadcast. (BMSB)*, Oct. 2021, pp. 1–6.
- [56] A. Martínez, M. Yannuzzi, V. López, D. López, W. Ramírez, R. Serral-Gracià, X. Masip-Bruin, M. Maciejewski, and J. Altmann, "Network management challenges and trends in multi-layer and multi-vendor settings for carrier-grade networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2207–2230, 4th Quart., 2014.
- [57] V. Karunakaran, S. K. Patri, S. Zimmermann, A. Autenrieth, and T. Bauschert, "OpenROADM for disaggregated optical networks: Challenges, requirements and evaluation," in *Proc. 24th ITG-Symp. Photon. Netw.*, 2023, pp. 1–5.
- [58] S. Janardhanan, K. Patil, and C. Mas-Machuca, "Open disaggregated network component (ODNC): Network sovereignty at the subcomponent level," in *Proc. IEEE Future Netw. World Forum (FNWF)*, Jun. 2025, pp. 384–390.
- [59] G. Yigit and J. Attwood. (2026). *Deutsche Telekom's Horizontal Telco Cloud (htc) Establishes a New Industry Blueprint for Telco Clouds*. [Online]. Available: <https://www.analysysmason.com/research/content/perspectives/dt-htc-project/>
- [60] N. Nikaein, M. K. Marina, S. Manickam, A. Dawson, R. Knopp, and C. Bonnet, "OpenAirInterface: A flexible platform for 5G research," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 33–38, Oct. 2014.
- [61] (2017). *Open5GS*. [Online]. Available: <https://github.com/open5gs/open5gs>
- [62] A. Banerjee, S. S. Mwanje, and G. Carle, "Trust and performance in future AI-enabled, open, multi-vendor network management automation," *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 2, pp. 995–1007, Jun. 2023.
- [63] R. Romero-Reyes, V. V. Pai, S. Sultana, and T. Bauschert, "Impact of vendor selection on the total cost of ownership of intra-data centre networks," in *Proc. 21st Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2019, pp. 1–4.
- [64] H. Sheikh, "European digital sovereignty: A layered approach," *Digit. Soc.*, vol. 1, no. 3, p. 25, Dec. 2022.
- [65] R. de Oliveira Costa and D. R. Figueiredo, "Evaluating countries' sovereignty from the point of view of the submarine cable network," in *Proc. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, 2025, pp. 924–937.
- [66] Y. Zhang, H. Vin, L. Alvisi, W. Lee, and S. K. Dao, "Heterogeneous networking: A new survivability paradigm," in *Proc. Workshop New Secur. Paradigms*, 2001, pp. 33–39.
- [67] F. Ghawash and W. Abbas, "Leveraging diversity for achieving resilient consensus in sparse networks," *IFAC-PapersOnLine*, vol. 52, no. 20, pp. 339–344, 2019.
- [68] S. Janardhanan, R. Agarwal, W. Kellerer, and C. Mas-Machuca. (2025). *Cut Set Coloring-Integer Linear Program Formulation*. [Online]. Available: <https://mediatum.ub.tum.de/doc/1771766/1771766.pdf>
- [69] S. Janardhanan and C. Mas-Machuca, "Modeling and evaluation of a data center sovereignty," in *Proc. 18th Int. Conf. Design Reliable Commun. Netw. (DRCN)*, Mar. 2022, pp. 1–8.
- [70] S. Janardhanan and C. Mas-Machuca, "Modeling and evaluation of a data center sovereignty with software failures," in *Proc. 6th Int. Conf. Syst. Rel. Saf. (ICSRS)*, Nov. 2022, pp. 233–242.
- [71] K. K. Aggarwal, K. B. Misra, and J. S. Gupta, "Reliability evaluation a comparative study of different techniques," *Microelectron. Rel.*, vol. 14, no. 1, pp. 49–56, Feb. 1975.
- [72] A. Heidari, Z. Amiri, M. A. J. Jamali, and N. Jafari, "Assessment of reliability and availability of wireless sensor networks in industrial applications by considering permanent faults," *Concurrency Comput., Pract. Exper.*, vol. 36, no. 27, p. 8252, Dec. 2024.
- [73] D. Rani Sahu, N. K. Ray, and P. Kumar Tripathy, "MCRel: A minimal cut set-based approach for reliability analysis of sensor-based IIoT," *IEEE Access*, vol. 13, pp. 191906–191923, 2025.
- [74] S. Ghosh and B. Bhattacharya, "A nested hierarchy of second order upper bounds on system failure probability," *Probabilistic Eng. Mech.*, vol. 70, Oct. 2022, Art. no. 103335.
- [75] E. K. Mutar, "Estimating the reliability of complex systems using various bounds methods," *Int. J. Syst. Assurance Eng. Manage.*, vol. 14, no. 6, pp. 2546–2558, Dec. 2023.
- [76] T. R. Jensen and B. Toft, *Graph Coloring Problems*. Hoboken, NJ, USA: Wiley, 2011.
- [77] Gurobi Optimization, LLC. (2026). *Gurobi Optimizer Reference Manual*. [Online]. Available: <https://www.gurobi.com>
- [78] (2026). *Tolerances and User-Scaling*. [Online]. Available: https://docs.gurobi.com/projects/optimizer/en/current/concepts/numericguide/tolerances_scaling.html
- [79] H. P. Williams, *Model Building in Mathematical Programming*. Hoboken, NJ, USA: Wiley, 2013.
- [80] J. Wray. (2021). *The Cost of High Availability*. [Online]. Available: <https://jaredwray.com/blog/the-cost-of-high-availability>
- [81] (2017). *Cisco Catalyst 9300 Series Switches Data Sheet*. [Online]. Available: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html>
- [82] (2017). *Cisco Catalyst 9600 Series Switches*. [Online]. Available: <https://www.cisco.com/site/us/en/products/collateral/networking/switches/catalyst-9600-series-switches/nb-06-cat9600-series-data-sheet-cte-en.html>
- [83] *Atlassian Confluence Pricing*. [Online]. Available: <https://www.atlassian.com/software/confluence/pricing>
- [84] S. Knight, H. X. Nguyen, N. Falkner, R. Bowden, and M. Roughan, "The internet topology zoo," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 9, pp. 1765–1775, Oct. 2011.
- [85] S. Janardhanan, Y. Chen, W. Kellerer, and C. Mas-Machuca, "Fast-MCS: A scalable open-source tool to find minimal cut sets," in *Proc. 17th Int. Conf. Netw. Future (NoF)*, 2026.
- [86] SciDA. (Nov. 2025). *In the Name of Sovereignty*. [Online]. Available: <https://scidaproject.com/2025/11/21/in-the-name-of-sovereignty/>



SHAKTHIVELU JANARDHANAN (Graduate Student Member, IEEE) received the bachelor's degree in electronics and communication engineering from the SSN College of Engineering, India, in 2019, and the Master of Science degree in communication engineering from the Technical University of Munich (TUM), in 2021, where he is currently pursuing the Ph.D. degree with the Chair of Communication Networks. His research interests include modeling and analysis of resilient networks.



KAUSTUBH PATIL received the Bachelor of Engineering (B.E.) degree in electronics engineering from the University of Mumbai, in 2022, and the Master of Science (M.Sc.) degree in communications engineering from the Technical University of Munich, in April 2025. His research interests include modeling, analysis, and planning of resilient communication networks.



WOLFGANG KELLERER (Fellow, IEEE) is a Full Professor at the Technical University of Munich (TUM), heading the Chair of Communication Networks. Before, he was with NTT DOCOMO's European Research Laboratories for over ten years. He currently serves as an Associate Editor for IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT and as an Area Editor for Network Virtualization for IEEE COMMUNICATIONS SURVEYS AND TUTORIALS.



RITANSHI AGARWAL (Graduate Student Member, IEEE) received the Master of Science degree in communications engineering from the Technical University of Munich, Germany, specializing mainly in communication systems, in 2024. In June 2024, she joined the Chair of Communication Networks, University of the Bundeswehr Munich, Germany, as a Research Associate. Her interests include resilient optical access networks and techno-economic communication networks evaluation.



CARMEN MAS-MACHUCA (Senior Member, IEEE) is a Full Professor with the Chair of Communication Networks, University of the Bundeswehr Munich (UniBW), Germany. Her research interests include techno-economic studies, resilient network planning, optimization problems, and optical networks. She is a Guest Editor for IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, *OSA Journal on Optical Communications and Networking*, and *IEEE Communications Magazine*.

...