A Performance and Resilience Analysis of the South African National Research and Education Network (SANReN)

Alexander White
whtale015@myuct.ac.za
Computer Science Department,
University of Cape Town

Kerry-Lynn Whyte
whyker001@myuct.ac.za
Computer Science Department,
University of Cape Town

Nicolas Wise
wsxnic001@myuct.ac.za
Computer Science Department,
University of Cape Town

1. Introduction

National Research and Education Networks (NRENs) are foundational to data-driven research, offering the high-speed, high-capacity infrastructure required for large-scale collaboration [10, 22]. In South Africa, the South African National Research and Education Network (SANReN) enables high-speed, reliable connectivity between South African research and education institutions, supports data-intensive collaboration, facilitates access to global research networks, and provides advanced services like cloud computing, remote instrumentation, and cybersecurity support [10, 22, 27]. As reliance on SANReN grows, so does the need for resilience against technical faults and cyber threats [10].

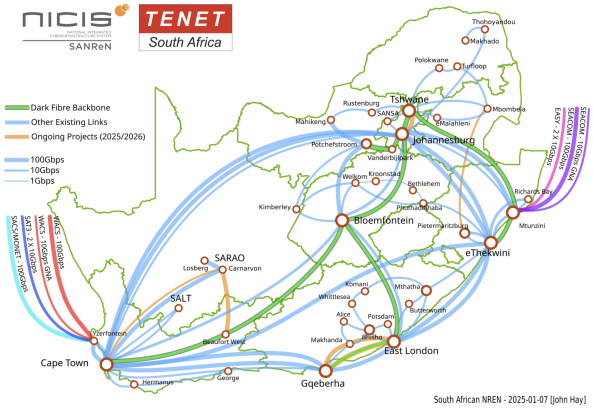

Figure 1: SANReN Network backbone diagram [26]

Traditional analyses of SANReN have focused on logical metrics like latency and packet loss but fail to capture deeper structural vulnerabilities such as redundancy gaps and fragmentation risks [30]. Çetinkaya et. al [6] show that graph-theoretic approaches are more suitable for evaluating network resilience. This project proposes an integrated framework combining spectral graph theory, centrality measures, and core resilience analysis to uncover and evaluate these hidden weaknesses. **Spectral metrics** are used to quantify fragmentation [9, 28], **centrality measures** identify critical nodes that may act as bottlenecks or points of failure, and **core resilience** metrics measure how deeply nodes are embedded within the network's structure [4]. Using NS-3 simulations, the project assesses how SANReN's topology performs under failure scenarios and explores possible structural improvements through repeatable and scalable testing of how the existing and proposed SANReN topologies respond to node failures and attacks. Full definitions and methodological details are provided in Section 2.

1.1. Problem Statement

Despite major upgrades, including 10 and 100 Gbps nodes, SANReN faces persistent infrastructural and topological challenges [3, 10]. For example, despite the difference in distance, transfers from Johannesburg to Cape Town and Johannesburg to Washington are the same speed due to local saturation [23].

The demand for SANReN is growing: the Gross Enrolment rate for South African universities rose 7.1% from 2021 to 2022 [5]. SANReN must future-proof its design to meet this growing demand [3]. Even though network transfers are secured by Globus, SANReN faces security vulnerabilities since cyber threats are constantly evolving [12].

The network's physical topology faces structural limitations including long link distances, poor rural connectivity, circuitous routing in regions such as Cape Town, and single-node dependencies—that constrain its resilience and performance [24].

1.2. Research Questions

This research evaluates the resilience of SANReN's topology. It aims to identify vulnerabilities, test improvements through simulation, and propose data-driven design changes to enhance network reslience by answering the following questions:

(a) To what extent can spectral graph theory and core resilience analysis quantitatively evaluate the structural resilience of SANReN topology - including node criticality, node centrality, and connectivity - and how effectively can these methods inform the design of a more resilient network topology?
(b) To what extent can spectral graph theory together with centrality measures be used to quantitatively identify known vulnerabilities to cyber attacks and network failures — such as critical node dependencies, bottlenecks, and potential points of fragmentation - in SANReN's backbone architecture?
(c) To what extent can spectral graph metrics — such as algebraic connectivity and spectral radius — along with centrality measures, inform the design of more resilient topologies that outperform SANReN's current structure under failure and attack scenarios?
(d) How does the diagnostic performance of the *Spectral Graph Model* (based on Laplacian eigenvalue analysis) compare to that of the *Core Resilience Model* in accurately diagnosing redundancy weaknesses and structural vulnerabilities in SANReN's physical topology under simulated node failure scenarios?

2. Background

2.1. Key Concepts

2.1.1. Network Resilience Network resilience refers to a network being able to maintain suitable levels of connectivity and functionality when subjected to failures or targeted attacks [30]. **Global resilience** refers to a network's ability to preserve overall connectivity and function during large-scale disruptions, often evaluated through topological or performance-based measures [31]. **Structural resilience**, in contrast, captures how the network topology handles localised failures and fragmentation [34].

2.1.2. Logical and Physical topologies The logical topology defines the path data takes through a network—regardless of physical connections—and highlights routing dependencies and bottlenecks [7]. The physical topology describes the physical infrastructure such as fibre cables and switches. It enables realistic network resilience analysis as it considers geographic constraints, physical distances, and infrastructure placement — all of which affect latency, redundancy, and vulnerability to failures [6].

2.1.3. Laplacian Matrix The Laplacian matrix captures overall network connectivity and is essential in assessing structural resilience [4]. The adjacency matrix $A(G)$ encodes edge connections: $a_{ij} = 1$ if nodes i and j are connected, and 0 otherwise, with $a_{ii} = 0$.

The **Laplacian matrix** is computed as [4]:

$$L(G) = D(G) - A(G)$$

where $D(G)$ is the diagonal **degree matrix**, with entries d_{ii} equal to the degree of node v_i.

The **normalised Laplacian matrix** enables comparisons between topologies of different sizes and structures. It extends the basic Laplacian by adjusting for node degree, so that it can accurately compare nodes regardless of how many connections they have [4]. It is defined as:

$$L_{norm}(G)(i,j) = \begin{cases} 1, & \text{if } i = j \text{ and } d_i \neq 0 \\ -\frac{1}{\sqrt{d_i d_j}}, & \text{if } i \text{ and } j \text{ are connected} \\ 0, & \text{otherwise} \end{cases}$$

where d_i and d_j are the degrees of nodes i and j. This matrix is widely used in resilience analysis due to its ability to normalise structural properties.

2.1.4. Spectral Metrics Spectral metrics provide quantitative measures of global network resilience. They are derived from the eigenvalues of the Laplacian matrix.

(1) **Eigenvalues** provide a mathematical method of quantifying network connectivity and resilience. Let M be a symmetric matrix and I the identity matrix of order n. Eigenvalues are the roots of the characteristic polynomial:

$$\det(M - \lambda I) = 0$$

For Laplacian matrices, eigenvalues range from 0 to 2:

$$0 = \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$$

A large number of eigenvalues equal to 1 may suggest structural redundancy (particularly in a meshed toplogy), typically arising from nodes with highly similar neighbourhoods [2].

Eigenvalues approaching 2 are characteristic of nearly bipartite structures. Although not inherently problematic in small quantities, a concentration of eigenvalues near 2 points to weak internal cohesion, with fewer loops or triangles to absorb failures [2]. Such networks are structurally less robust and more prone to disintegration under targeted attack.

(2) **Eigenvalue Spectrum** The overall spread and clustering of the eigenvalue spectrum can reveal how evenly resilience is distributed throughout the network. A tightly clustered spectrum typically indicates a well-balanced and resilient topology, while a widely spread distribution may expose disparities and potential weak [29].

The set of eigenvalues $\{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ defines the **spectrum** of M.

(3) **Multiplicity** indicates the how connected the network is. Multiplicity refers to the number of zero eigenvalues and corresponds directly to the number of disconnected components [4]. A single zero eigenvalue indicates that the network is fully connected, whereas multiple zeros signify fragmentation into isolated sub-graphs — a clear indicator of poor resilience. Therefore, monitoring how multiplicity changes after simulated failures allows us to diagnose weak points in the network.

(4) **Algebraic Connectivity**, a(G), captures the connectivity of graphs in a broader spectrum than average node degree. As networks evolve, a(G) provides a sensitive measure of how well network connectivity is maintained after failures or attacks. a(G) is the second smallest eigenvalue of the Laplacian spectrum, λ_2 [19].

If $\lambda_2 > 0$, the network is connected[4]. A larger value of λ_2 indicates a more resilient network — it is harder to disconnect and has better while a smaller λ_2 suggests lower resilience and a higher risk of the network fragmentation under failure [4].

A high λ_2 reflects strong overall connectivity and good fault tolerance, while a low λ_2 indicates structural weak points and a greater chance of the network fragmentation.

(5) The **Spectral Radius** reflects how tightly connected a network is and reveals a network's vulnerability to fragmentation. The spectral radius is the absolute value of the largest eigenvalue,

$$|\lambda|$$

of the Laplacian matrix. The combination of the spectral radius with the distribution of eigenvalues in the Normalised Laplacian spectrum provides a visual indicator of network vulnerability. In particular, the spread and clustering of these eigenvalues under attack scenarios reveals how easily a network fragments [29].

2.1.5. Centrality Metrics Centrality metrics help identify critical nodes in a network.

(1) **Betweenness centrality** measures how often a node occurs on shortest paths, highlighting key connector nodes [11].
(2) **Closeness centrality** illustrates how quickly a node can reach other nodes [21].
(3) **Degree centrality** indicates the number of direct connections a node has to other nodes [21].

2.1.6. Models Various synthetic geographic graph models can be constructed to represent topologies, based on the node locations of physical topologies [6]. Gabriel graphs connect nodes based on proximity where an edge is drawn between two nodes if no other node lies within the circle whose diameter is the line segment connecting those two nodes [6]. Geometric threshold graphs are spatial graph models where edges exist between nodes if their distance is below a defined threshold [6]. Both models are effective in modelling mesh-like topologies [6].

The **Spectral Model** applies the Laplacian matrix to assess global network resilience [29]. The model provides a complementary resilience perspective (global versus structural resilience) and can be used to simulate and evaluate failure scenarios which is useful in identifying redundancy weaknesses and informing improved topological designs [6].

The **Core Resilience Model** identifies structurally embedded nodes using k-core decomposition. This reveals hierarchical layering and node importance beyond traditional centrality measures. A k-core is a maximal subgraph where each node has at least k connections. Decomposition iteratively removes nodes with a degree less than k, uncovering the network's layered structure. A node's *core number* is the highest k for which it remains in the k-core, reflecting its structural depth and resilience.

Core strength is the minimum number of neighbours that must be removed to reduce a node's core number, while *core influence* measures a node's impact on the core numbers of its neighbours. The *Core Influence-Strength (CIS)* metric, defined as the average core strength of the top $r\%$ most influential nodes provides a measure of network resilience. The *Maximise Resilience by K-Core (MRKC)* algorithm enhances resilience by iteratively reinforcing vulnerable nodes through strategic additions of nodes or edges [16].

2.1.7. Network Simulation Network simulation utilises mathematical models to represent network component and protocol behaviour [15]. By executing discrete events over simulated time, it allows researchers to test networks under failures, congestion, or attack conditions [14]. Simulation supports repeatable, controlled experimentation and enables the analysis of performance and resilience.

NS-3 is an open-source simulation software providing scalability and stress-testing of topological models [**?**]. Events are executed sequentially in simulated time which allows researchers to test network behaviour under varying conditions in a repeatable and modular manner.

2.2. Additional Related Work

Previous studies of NRENs have highlighted the value and limitations of topological evaluation. Salie [25] identified high delays in SANReN affecting Cape Town and Gqeberha caused by circuitous routing and geographic isolation. However, the study is largely descriptive, lacking simulation, graph-theoretic metrics, or structural modelling.

Beyond SANReN-specific works, Çetinkaya et al. [4, 8] and Lee et al. [18] illustrated that physical topologies often follow transport corridors, creating critical points of vulnerability. Logical topologies, though efficient, concentrate traffic through high-centrality nodes, introducing single points of failure [7]. Therefore, modelling both layers is essential for understanding the effects of node failures or attacks. A resilient design must reduce reliance on central logical nodes and increase redundancy in the physical layer.

Traditional graph metrics have proven inadequate for assessing resilience—especially across networks of different sizes or evolving structures [4]. Research has shifted toward spectral graph theory, to evaluate connectivity, fragmentation, and structural weakness [4, 28]. Shatto and Çetinkaya [28] show that mesh-like topologies (such as SANReN) are best modelled with Gabriel graphs.

Core resilience analysis complements spectral metrics by identifying structurally vital nodes overlooked by traditional measures. Laishram et al. [16] proposed k-core decomposition and the MRKC algorithm to improve resilience. Networks with higher Core-Influence Strength (CIS) values demonstrated greater resilience. Though promising, these methods remain underused in SANReN analysis. Metrics such as k-core, modularity, and edge betweenness could reveal bottlenecks in SANReN's support of high-bandwidth collaboration, especially in isolated regions [32, 35].

Simulation tools like NS-3 provide control and reproducibility but are complex and outdated [14]. Still, they are used for link performance and data centre protocol tests [1, 20]. Though NS-3 is used in SDN and data centre resilience testing [17, 33], it remains unused for SANReN. Given SANReN's growing data needs, stress-testing its topology with these tools is essential.

3. Procedures and Methods

3.1. Methodological Overview

This project utilises theoretic graph modelling of SANReN, spectral and core resilience model analysis, as well as stress testing through

simulation. The following are the primary concepts for the project's different research streams:

(1) **Topology Reconstruction:** Constructing graph-based representations of SANReN's physical and logical topologies using publicly available data from SANReN's website, direct consultation with SANReN personnel, and synthetic modelling where necessary.
(2) **Resilience Evaluation:** Applying centrality, spectral and core resilience metrics to identify weaknesses in the physical topology and benchmark SANReN's resilience.
(3) **Stress Testing:** Evaluating the resilience of SANReN's current and proposed topologies under simulated failure and attack scenarios using NS-3 for network simulation.

Topology data will be accessed from the backbone structures published on SANReN's website as well as from SANReN itself. The project will be developed and tested on a MacBook Air M2 (8GB RAM, 500GB SSD) and a MacBook Pro with a Core i5 processor (8GB RAM, 256GB SSD). While these machines lack high-power GPUs, their capacity is sufficient for lightweight simulations required by the scope of this project.

3.2. Applying Spectral and Core Resilience Analysis to SANReN to Identify Structural Properties and to Propose a More Resilient Topology

This stream investigates SANReN's core structural properties by utilising a combined approach leveraging spectral graph theory and core resilience analysis.

3.2.1. Topology Reconstruction This research stream starts with the generation of a representative topology model of SANReN, using Geometric Threshold graph models, as proposed by Cetinkaya et al. for graphing star-like structures [6]. An example of this representation can be seen in Figure 2.

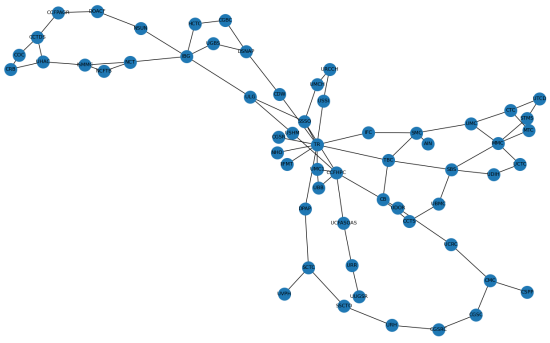

Figure 2: Representative Model of Cape Town's Physical SANReN Topology.

3.2.2. Resilience Evaluation The resilience evaluation will begin with the application of spectral analysis. This involves computing the Laplacian Matrix and eigenvalues to assess connectivity, redundancy and fragmentation. Connectivity will be evaluated using algebraic connectivity. Redundancy will be examined by observing the number and density of eigenvalues clustered around 1 [28], as this clustering suggests the presence of multiple overlapping paths and substructures that can serve as backups in case of failure. Fragmentation will be assessed by evaluating the eigenvalue multiplicity of the zero eigenvalue as a higher multiplicity implies greater fragmentation and weaker structural cohesion.

In parallel, core resilience analysis, as proposed by Laishram et al. [16]. This analysis applies k-core decomposition to derive the network's nodes core numbers and core influence. These metrics will then be used to compute the network's Core Influence-Strength (CIS) metric to quantify the network's overall resilience.

3.2.3. Stress Testing To simulate failures, nodes will be ranked based on core resilience metrics, specifically core strength and core influence. Targeted attacks will be simulated by sequentially removing the top-ranked nodes. After each removal, metrics such as algebraic connectivity, eigenvalues, and core resilience metrics will be recomputed to assess how connectivity, fragmentation, and resilience degrades. These changes will be visualised through comparative plots, such as algebraic connectivity versus number of nodes removed, to illustrate the network's response under attack.

Based on the results of the spectral and core resilience analyses, along with the failure simulations, critical vulnerabilities such as high-risk nodes, single points of failure, and fragmented regions will be identified. These will be mapped to SANReN's topology to identify areas for improvement. Resilience enhancement techniques will be applied through strategies such as reinforcing core and vulnerable nodes, adding redundant links, or applying the MRKC algorithm [16]. These interventions will be applied iteratively, with each iteration evaluated using the same resilience metrics. The most robust iteration will be selected and proposed as an improved, resilience-optimised SANReN topology.

The proposed methodology addresses the research question by combining spectral graph theory and core resilience analysis to evaluate SANReN's layered structure and structural resilience properties. Spectral analysis, via the Laplacian matrix, enables assessment of connectivity, redundancy, and fragmentation, offering a deeper insight into SANReN's structural properties. Core resilience analysis evaluates node centrality and criticality providing a broader resilience measure. Failure simulations validate these metrics by removing top-ranked nodes and observing how resilience deteriorates. Finally, iterative topology improvements guided by these analyses and the MRKC algorithm demonstrate how these methods can effectively inform the design of a more resilient SANReN topology.

3.3. Using Spectral Metrics and Centrality Measures to Diagnose Network Vulnerabilities and Inform the Redesigning of Resilience-Oriented Topologies

This research stream will investigate the extent to which spectral graph metrics and centrality measures can accurately diagnose structural vulnerabilities in SANReN's backbone topology and propose the design of a more resilient topology.

3.3.1. Topology Reconstruction This study begins by constructing graph representations of the logical and physical topologies of SANReN using real-world data and synthetic graph models such as the Gabriel graph. These abstractions enable the analysis of structural properties such as connectivity and redundancy using spectral and centrality-based methods that are needed to identify vulnerabilities and inform resilience-oriented redesign.

3.3.2. Resilience Evaluation Once the graphs have been constructed the topologies will then be represented as Laplacian and normalised Laplacian matrices to enable spectral analysis. A series of experiments will then be conducted in which key spectral metrics (algebraic connectivity, spectral radius, and eigenvalue spread) along with centrality measures (degree, closeness, betweenness), are computed to assess network connectedness, identify bottlenecks, and evaluate redundancy. Algebraic connectivity will be computed as this provides a sensitive measure of how well network connectivity is maintained after failures/cyberattacks [4]. In addition, the spectral radius and the eigenvalue distribution of the normalised Laplacian spectrum - will be computed and analysed in combination to indicate vulnerability. Centrality measures will be computed to identify critical nodes in the network that may be single points of failure [4].

3.3.3. Stress Testing Following metric computation, the experimental phase will simulate both random and targeted node failures, where nodes are removed based on either random selection or their structural importance. Simulations will be implemented using NS-3 to provide controlled experimentation under various failure conditions, provide empirical evidence of how SANReN's structure responds to disruptions and informing the design of more resilient topological configurations [13]. The resulting changes in spectral properties—such as eigenvalue convergence and zero-eigenvalue multiplicity—will be tracked to assess fragmentation and resilience loss.

To evaluate the resilience of SANReN's current topology under failures and attacks, these outcomes will be compared with alternative topologies such as more meshed ones under identical failure scenarios. Metric outcomes will be visualised using spectral distribution plots, centrality heatmaps, and connectivity graphs as quantifiable evidence as to how specific node removals impact network integrity. These visualisations will enable the extent to which known structural vulnerabilities can be identified as well as the extent to which these metrics can inform the design of more resilient topologies to be assessed. The findings will be utilised to inform final topology redesign and be validated through further NS-3 simulations to ensure practical relevance for real-world application.

3.4. Comparing Spectral and Core Resilience Models for Structural Vulnerability Detection in SANReNs

This research stream will evaluate and compare the diagnostic performance of the Spectral Graph Model and the Core Resilience Model in identifying redundancy vulnerabilities and structural weaknesses in SANReN's physical topology. The core objective is to assess how accurately and reliably each model identifies critical nodes under simulated failure scenarios. The analysis is grounded in a comparative framework, where the outputs of both models are evaluated in parallel against controlled node failure experiments to determine their diagnostic **sensitivity**, **accuracy**, and **robustness**.

3.4.1. Topology Reconstruction & Model Application This research stream begins by reconstructing SANReN's physical topology using publicly available documentation and modelling techniques such as the Gabriel graph. Both models are then independently applied to the same baseline graph. The Spectral Graph Model computes the Laplacian and normalised Laplacian matrices and extracts key spectral metrics including algebraic connectivity, spectral radius, and eigenvalue distribution [4]. In contrast, the Core Resilience Model performs k-core decomposition and onion layering to compute core numbers, core strength, and the composite Core Influence-Strength (CIS) metric [2]. Each model produces a ranked list of structurally critical nodes based on its internal logic.

3.4.2. Simulated Failures & Results Analysis Simulated node failures are then introduced in two phases: random removals and targeted attacks based on the critical nodes identified by each model. The effects of these removals are measured in terms of how sharply key structural metrics degrade. Diagnostic sensitivity is evaluated by observing how early a model detects structural decline as nodes are incrementally removed. Accuracy is measured by the severity of network degradation following the removal of nodes identified as critical by each model. Diagnostic robustness is assessed by how consistently each model performs across different failure types—random versus targeted. The degradation curves of both models are plotted and compared to determine which model responds more effectively under stress, enabling a quantifiable and interpretable assessment of diagnostic effectiveness.

3.5. System Validation and Sanity Checks

The procedures will be validated using a triangulated approach to ensure its accuracy, reliability, and practical relevance. First, resilience metrics such as algebraic connectivity and Core Influence-Strength (CIS) will be tested on synthetic graphs with known topological properties—such as being mesh-like—to verify that the system produces expected outputs under controlled conditions. These tests provide a foundational check on metric correctness. Second, NS-3 simulations will be assessed for plausibility by comparing the observed degradation patterns with theoretical expectations; for example, confirming that the removal of high-centrality nodes in a star graph causes immediate fragmentation.

Third, outputs from the system—including topology reconstructions, critical node identification, and resilience rankings—will be reviewed by technical staff from SANReN. Their insights will verify that the models align with SANReN's real-world configuration and known vulnerabilities. Finally, the proposed topological improvements will be benchmarked against the existing SANReN structure under identical simulated failure scenarios. Measurable gains in resilience metrics will be used as evidence that the system not only performs correctly but also supports practical and interpretable network enhancement.

3.6. Theoretical Contribution

This project includes a mathematical component through the application of graph theory to network resilience modelling. By applying these metrics to physical network design—rather than solely logical overlays—it contributes a novel application of theoretical analysis to infrastructure modelling.

3.7. Expected Challenges

Expected challenges include achieving high fidelity in modelling SANReN's complex topology and managing memory constraints when running large-scale simulations. To address these, the project will consult regularly with SANReN to validate model accuracy and ensure alignment with real-world infrastructure. Graph models will be designed to balance realism and computational feasibility, while the simulation framework will be modularised to allow targeted scenario testing without overloading system resources.

4. Anticipated Outcomes

4.1. System

The system consists of an integrated Python toolkit developed using libraries such as NetworkX and NumPy to model SANReN's physical and logical topologies which enables graph-based network representations to be constructed, the computation of spectral and core resilience metrics, and the integration of simulation using NS-3.

Key features include the use of Laplacian and normalised Laplacian matrices for spectral analysis, centrality metrics to identify critical nodes and potential bottlenecks, and core resilience metrics to capture rich resilience data. The combination of these metrics guides the evaluation of SANReN's vulnerability and the effectiveness of topological improvements under stress conditions.

A major design challenge faced was unifying multiple analytical components into a coherent, modular pipeline that is accurate and scalable. The proposed approach balances computational feasibility with structural realism by aligning synthetic models with SANReN's known physical constraints and validating resilience outcomes based on repeatable simulation conditions.

4.2. Research

The research aims to assess the applicability and effectiveness of spectral graph theory and core resilience metrics in uncovering structural weaknesses and guiding the development of more resilient network topologies for SANReN. It is anticipated that spectral metrics will accurately reveal critical node vulnerabilities and potential fragmentation points in the current network structure. Centrality metrics will identify nodes that act as key connectors or potential bottlenecks in data flow. In addition, core resilience metrics will highlight structurally vital nodes that may not be detected using conventional centrality measures.

Evidence that the research problem has been addressed will include accurate detection of weaknesses, measurable improvements in resilience metrics after topological modifications, and validated performance gains under simulated failures or attacks as well as demonstrable improvements in resilience metrics following topological changes based on structural weakness analyses. Ultimately, the project will evaluate whether these combined analytical frameworks offer a practical basis for enhancing SANReN's resilience and performance.

4.3. Expected Impact

The project will deliver a reusable software toolkit for evaluating and improving the resilience and performance of SANReN and other NRENs. It will be able to identify structural vulnerabilities and propose topological changes that improve fault tolerance and scalability. These insights will support SANReN's mission to enable high-speed, reliable research collaboration, while contributing to broader efforts in designing resilient large data and research transfer infrastructures for under-resourced or geographically constrained regions.

4.4. Key Success Factors

Success will be measured by the project's ability to deliver both theoretical insights and practical, scalable tools that enable SANReN to future-proof its infrastructure. Evaluation will focus on three criteria: accuracy (metrics must reliably identify known vulnerabilities, supported by simulation results), improvement (proposed topologies should show measurable gains in resilience under simulated failures and targeted attacks) and efficiency (tools must support timely, modular simulation for networks of SANReN's scale).

5. Ethical, Professional and Legal Issues

This project does not involve human participants or the collection of personal or sensitive data, and thus does not require ethics clearance. All data used is either publicly available from SANReN documentation or obtained through direct consultation with SANReN representatives. The research relies solely on open-source tools, such as NS-3, for modelling and simulation, and does not interact with or affect any real-world infrastructure. All code and models developed will be released under an open-source license, with appropriate attribution to third-party libraries and data sources. Any intellectual contributions will be shared transparently, and all publications resulting from the project will adhere to principles of academic integrity and responsible research conduct.

6. Project plan

6.1. Risks

The project identifies key risks such as limited access to SANReN data, computational resource constraints, and tool compatibility issues. Each risk is paired with targeted mitigation, monitoring, and management strategies to minimise disruption. Refer to APPENDIX A - RISKS.

6.2. Timeline

The project timeline spans from early research and proposal submission in April to final report delivery in September. Key milestones include SANReN topology reconstruction, spectral and core resilience analysis, targeted failure simulations, proposed topology improvement, results analysis and the final report submission. Refer to APPENDIX B - TIMELINE.

6.3. Project Resources

The project will be implemented in Python, using NetworkX for graph construction and resilience analysis, with NumPy and SciPy for matrix computations. Matplotlib will visualise key metrics, while NS-3 will simulate targeted attacks and evaluate SANReN's connectivity, redundancy, and fragmentation through discrete-event network simulations. The data sources for the project will include publicly available SANReN topological data as well as private topology data obtained from SANReN. All development and testing will primarily be carried out on personal laptops.

6.4. Milestones

The projects milestones begin with the literature review and proposal submission. Midway milestones involve topology generation, metric computation, and simulation setup, followed by testing the existing and proposed topologies under various conditions. The final phase focuses on analysis, reporting, and the submission of a comprehensive final report and codebase in September. Refer to APPENDIX C - MILESTONES.

6.5. Deliverables

6.5.1. System Deliverables (Software Tools and Scripts) The project will deliver Python-based tools built with NetworkX, NumPy, and SciPy to model SANReN's physical and logical topologies. These will include modules for spectral analysis (algebraic connectivity, spectral radius) and core resilience (k-core, core strength, CIS). The system will integrate with NS-3 to simulate failure conditions and assess whether proposed topologies outperform SANReN's current topology.

6.5.2. Analysis and Research Deliverables Deliverables will include graph representations of SANReN's current and proposed topologies, with comparative evaluations using centrality, spectral, and core resilience metrics. Results will be visualised through plots and resilience curves under attack scenarios and core influence distributions. The research will conclude with a final report outlining topological enhancements that are evidenced by quantitative resilience improvements.

6.5.3. Evaluation and Documentation Deliverables A final report will document the project's methodology, findings, and recommendations. All simulation files, result logs, and visualisations will be provided to ensure reproducibility, alongside supporting materials such as literature reviews, code documentation, and slides.

6.6. Work Allocation

The project is divided into three interconnected research streams based on the four research questions. Nicolas will investigate question (a) following the procedure outlined in (3.2), Kerry-Lynn will investigate question (b) and (c) following the procedure outlined in (3.3), and Alexander will investigate question (d) following the procedure outlined in (3.4).

References

[1] Leonardo Alberro, Felipe Velázquez, Sara Azpiroz, Eduardo Grampin, and Matías Richart. 2022. Experimenting with Routing Protocols in the Data Center: An ns-3 Simulation Approach. *Future internet* 14 (10 2022), 292–292. https://doi.org/10.3390/fi14100292

[2] Anirban Banerjee and Jürgen Jost. 2009. Spectral Characterization of Network Structures and Dynamics. *Dynamics On and Of Complex Networks* (2009), 117–132. https://doi.org/10.1007/978-0-8176-4751-3_7

[3] Sajitha Bashir. 2020. Connecting Africa's Universities to Affordable High-Speed Broadband Internet: What Will it Take? https://openknowledge.worldbank.org/entities/publication/c9dc3411-3b35-55b0-a6ba-da8b91d1fa90

[4] Egemen K. Çetinkaya, Mohammed J.F Alenazi, Justin P. Rohrer, and James P.G. Sterbenz. 2012. Topologyc connectivity analysis of internet infrastructure using graph spectra. *2012 IV International Congress on Ultra Modern Telecommunications and Control Systems* (10 2012). https://doi.org/10.1109/icumt.2012.6459764

[5] Natalie Cowling. 2024. South Africa: gross tertiary school enrollment ratio. https://www.statista.com/statistics/1261626/south-africa-gross-tertiary-school-enrollment-ratio/

[6] Egemen K. Çetinkaya, Mohammed J.F Alenazi, Yufei Cheng, Andrew M. Peck, and James P.G Sterbenz. 2014. A comparative analysis of geometric graph models for modelling backbone networks. *Optical Switching and Networking* 14 (06 2014), 95–106. https://doi.org/10.1016/j.osn.2014.05.001

[7] Egemen K. Çetinkaya, Mohammed J.F Alenazi, and James P.G Sterbenz. 2013. Network design and optimisation based on cost and algebraic connectivity. *2013 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)* 14 (2013), 193–200. https://doi.org/10.1109/ICUMT.2013.6798426

[8] Egemen K. Çetinkaya, Mohammed J. F. Alenazi, Andrew M. Peck, Justin P. Rohrer, and James P. G. Sterbenz. 2015. Multilevel resilience analysis of transportation and communication networks. *Telecommunication Systems* 60 (03 2015), 515–537. https://doi.org/10.1007/s11235-015-9991-y

[9] Miroslav Fiedler. 1973. Algebraic connectivity of graphs. *Czechoslovak Mathematical Journal* 23 (1973), 298–305. https://doi.org/10.21136/cmj.1973.101168

[10] Michael Foley. 2016. The Role and Status of National Research and Education Networks (NRENs) in Africa. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/233231488314835003/the-role-and-status-of-national-research-and-education-networks-nrens-in-africa

[11] Linton C. Freeman. 1977. A set of measures of centrality based on betweenness. *Sociometry* 40, 1 (1977), 35–41.

[12] Globus. 2025. Go beyond data Globus Compute. https://www.globus.org

[13] Lewis Golightly, Paolo Modesti, and Victor Chang. 2023. Deploying Secure Distributed Systems: Comparative Analysis of GNS3 and SEED Internet Emulator. *Journal of cybersecurity and privacy* 3 (08 2023), 464–492. https://doi.org/10.3390/jcp3030024

[14] Jose Gomez, Elie F. Kfoury, Jorge Crichigno, and Gautam Srivastava. 2023. A survey on network simulators, emulators, and testbeds used for research and education. *Computer Networks* 237 (12 2023), 1–42. https://doi.org/10.1016/j.comnet.2023.110054

[15] James F. Kurose and Keith W. Ross. 2017. *Computer Networking: A Top-Down Approach* (7 ed.). Pearson, Boston, MA.

[16] Ricky Laishram, Ahmet Erdem Sariyüce, Tina Eliassi-Rad, Ali Pinar, and Sucheta Soundarajan. 2018. Measuring and Improving the Core Resilience of Networks. In *Proceedings of the 2018 World Wide Web Conference* (Lyon, France) *(WWW '18)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 609–618. https://doi.org/10.1145/3178876.3186127

[17] Bob Lantz, Brandon Heller, and Nick McKeown. 2010. A network in a laptop: rapid prototyping for software-defined networks. In *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*. 1–6.

[18] Hyeongjik Lee, Seonkoo Jeong, and Kwanghee Lee. 2023. The South Korean case of deploying rural broadband via fiber networks by implementing universal service obligation and public-private partnership based project. *Telecommunications Policy* 47, 3 (2023), 102506. https://doi.org/10.1016/j.telpol.2023.102506

[19] William Liu, Harsha Sirisena, Krzysztof Pawlikowski, and Allan McInnes. 2009. Utility of algebraic connectivity metric in topology design of survivable networks. *UC Research Repository (University of Canterbury)* 4 (10 2009), 131–138. https://doi.org/10.1109/drcn.2009.5340016

[20] Marco Mezzavilla, Marco Miozzo, Michele Rossi, Nicola Baldo, and Michele Zorzi. 2012. A lightweight and accurate link abstraction model for the simulation of LTE networks in ns-3. *CiteSeer X (The Pennsylvania State University)* (10 2012), 55–60. https://doi.org/10.1145/2387238.2387250

[21] Mark Newman. 2010. *Networks: An Introduction.* Oxford University Press.

[22] Izuchukwu Azuka Okafor, Smart Ikechukwu Mbagwu, Terkuma Chia, Zuwati Hasim, Echezona Ejike Udokanma, and Karthik Chandran. 2022. Institutionalizing Open Science in Africa: Limitations and Prospects. *Frontiers in Research Metrics and Analytics* 7 (04 2022). https://doi.org/10.3389/frma.2022.855198

[23] Kasandra Pillay, Johann Hugo, Thuso Bogopa, Manqoba Shabalala, Thokozani Khwela, and Ajay Makan. 2024. SANReN's 100 Gbps Data Transfer Service: Transferring data fast! (11 2024), 765–769. https://doi.org/10.1109/scw63240.2024.00109

[24] Luqmaan Salie. 2021. An analysis of internet traffic flow in SANReN using active and passive measurements. (2021).

[25] L. Salie. 2021. *An Analysis of Internet Traffic Flow in SANReN Using Active and Passive Measurements.* Master's thesis. University of Cape Town, Faculty of Science, Department of Computer Science. http://hdl.handle.net/11427/36058 Accessed March 2025.

[26] SANRen. [n. d.]. South African NREN Backbone – SANReN. https://www.sanren.ac.za/backbone/

[27] SANReN. 2019. SANReN (the network the group). https://www.sanren.ac.za/relationships/

[28] Tristan A. Shatto and Egemen K. Çetinkaya. 2017. Spectral Analysis of Backbone Networks Against Targeted Attacks. In *DRCN 2017 - Design of Reliable Communication Networks; 13th International Conference*. 1–8.

[29] Tristan A. Shatto and Egemen K. Çetinkaya. 2017. Variations in graph energy: A measure for network resilience. *2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM)* (2017), 1–7. https://doi.org/10.1109/RNDM.2017.8093019

[30] James PG Sterbenz, David Hutchison, Egemen K Çetinkaya, Abdul Jabbar, Justin P Rohrer, Marcus Schöller, and Paul Smith. 2010. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer networks* 54, 8 (2010), 1245–1265.

[31] James PG Sterbenz, David Hutchison, Egemen K Çetinkaya, Abdul Jabbar, Justin P Rohrer, Marcus Schöller, and Paul Smith. 2010. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks* 54, 8 (2010), 1245–1265.

[32] Brian Tierney, Brandon Heller, Matthew Tierney, Guojun Jin, and Jason Lee. 2011. *A Case for Network Performance Measurement for End-to-End Application Throughput.* Technical Report LBNL-4950E. Lawrence Berkeley National Laboratory. https://digital.library.unt.edu/ark:/67531/metadc845229/m2/1/high_res_d/1028919.pdf Available via UNT Digital Library.

[33] Klaus Wehrle, Mesut Günes, and James Gross. 2010. *Modeling and tools for network simulation.* Springer Science & Business Media.

[34] Jian Wu, Mauricio Barahona, Yong-Jie Tan, and Hong-Zhong Deng. 2011. Spectral measure of structural robustness in complex networks. *IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics* 41, 6 (2011), 1244–1252.

[35] Ellen W. Zegura, Kenneth L. Calvert, and Michael J. Donahoo. 1997. A Quantitative Comparison of Graph-Based Models for Internet Topology. *IEEE/ACM Transactions on Networking* 5, 6 (Dec. 1997), 770–783. https://doi.org/10.1109/90.650143 Available from IEEE Xplore.

Appendix A – Risks

Table 1: Risk Management Strategy with Impact Ratings

Risk	Mitigation	Monitoring	Management	Impact
Limited access to SANReN infrastructure data	Utilise synthetic Gabriel graphs based on known SANReN points of presence.	Track SANReN publications and consult with SANReN bi-weekly for topology updates.	Use only validated synthetic models (e.g., Gabriel graphs). Document assumptions and mention limitations in final report.	6
Insufficient computing resources for simulation/emulation	Use lightweight tools such as NS-3. NS-3 supports scripting for scalable networks. Keep tests modular.	Monitor CPU and memory usage during test runs. Time each simulation/emulation iteration.	Request UCT lab access. Downscale scenarios (e.g., simulate only Cape Town) while preserving analytical integrity.	7
Inaccurate or oversimplified topology representation	Triangulate using SANReN diagrams, literature, and PoP data.	Regular validation checkpoints; cross-reference latest SANReN statistics.	Acknowledge modelling limitations. Perform sensitivity tests across synthetic topologies.	9
Tool/library compatibility issues (NS-3 and Python)	Use stable versions. Track tools via Git version control.	Run regular integration tests; keep backup branches.	Switch tools as needed (e.g., from NS-3 to Mininet). Modularise workflows to isolate issues.	7
Missed milestones/deadlines	Assign balanced tasks aligned with member strengths. Allow buffer time.	Weekly team meetings, Kanban tracking, supervisor check-ins.	Redistribute tasks if needed. Implement buffer weeks. Consult supervisor on deadline extensions.	6
Unexpected errors in metric computation or simulation runs	Start with small topologies; validate using known benchmarks.	Review logs and outputs for anomalies at each stage.	Isolate faulty components. Switch metrics/tools. Narrow scope to validated components.	9

Appendix B – Timeline

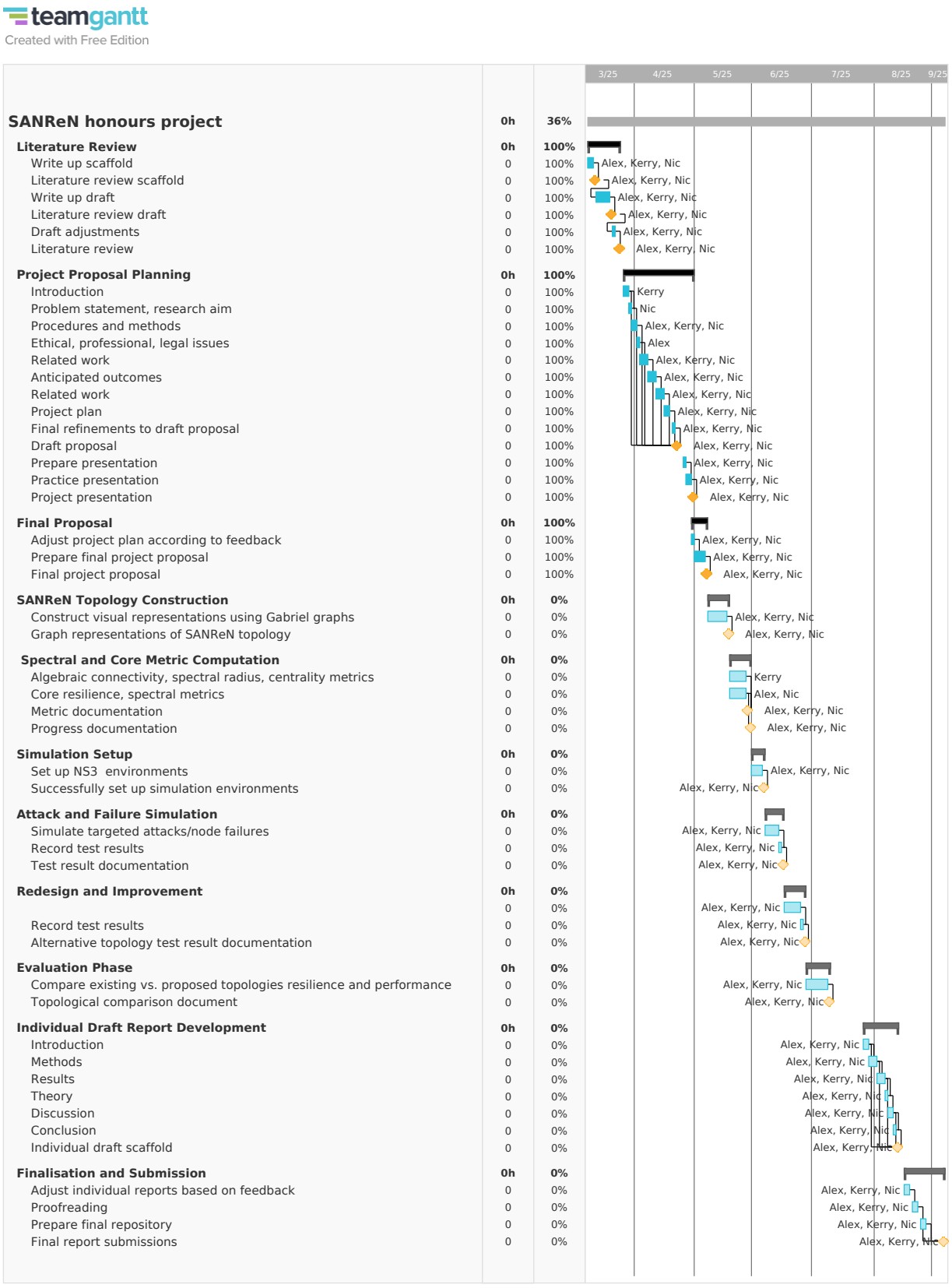

Figure 3: Project timeline

Appendix C – Milestones

Milestone	Expected Date	Description
M1: Literature Review	Completed	Summary of foundational graph theory, SANReN and NREN research.
M2: Proposal Full Draft Due	24 April	Submit the project proposal draft.
M3: Proposal Presentations	25 April - 2 May	Present the project to board of Computer Science Staff.
M4: Final Project Proposal	6 May	Submit our final project proposal.
M5: SANReN topology generation	12 May	Graph-based reconstruction of SANReN using NetowrkX, NumPy and Matplotlib libraries.
M6: Metric computation	28 May	Compute spectral, core resilience and centrality metrics.
M7: Progress documentation	29 May	Illustrate progress made in the project.
M8: Simulation environments	5 June	Successfully setup NS3 simulation environments.
M9: Targeted Simulation Attacks	16 June	Simulate node/link failures and observe resulting changes in core-resilience, centrality and spectral metrics.
M10: Redesign and improvement	26 June	Redesign and re-simulate alternative topologies and record results and improvements.
M11: Analyse results	8 July	Compare existing and proposed topologies metric results and map results back to SANReN to propose and justify and improved topology.
M12: Draft Final Report	13 August	Combine analysis, visualisation, and findings into complete report as well as refactor code and report document.
M13: Finalise Report	5 September	Submit final report and code.