Journal of the Civil Engineering Forum, September 2026, 12(3):375-388
DOI 10.22146/jcef.28441
Available Online at https://jurnal.ugm.ac.id/v3/jcef/issue/archive

How Toll Roads Reshape Structural Vulnerability in Primary Road Networks: A Graph Neural Network Learning from Central Java Province

Berlian Kushari[1,2,*], Muhammad Isran Ramli[1], Bambang Bakri[1], Ardy Arsyad[1]
[1]Faculty of Engineering, Hasanuddin University, Makassar, INDONESIA
[2]Faculty of Civil Engineering and Planning, Islamic University of Indonesia, Yogyakarta, INDONESIA
*Corresponding author: bkushari@uii.ac.id

SUBMITTED 1 February 2026 **REVISED** 27 April 2026 **ACCEPTED** 3 May 2026

ABSTRACT The roles of primary road networks in maintaining regional connectivity, supporting economic activities, and enabling emergency response, especially in disaster-prone areas, are well known. Vulnerability analysis of such networks is commonly conducted following disruption-based scenarios, in which external hazards are modeled to disrupt and degrade network performance. This study adopts a different perspective by considering vulnerability as a property that can also arise from the network's own topological structure. In this approach, vulnerability is assumed to exist even prior to external disturbances, and thus is an intrinsic characteristic of the network. To explore this idea, a Graph Neural Network (GNN)-based framework is proposed to learn structural vulnerability directly from network topology. The primary road network of Central Java Province, Indonesia, was used as a case study. The network was modeled as an undirected, weighted graph representing two configurations: without toll roads and with toll road integration. Vulnerability labels at the node level were derived from a series of node removal experiments, capturing efficiency loss, connectivity degradation, and network fragmentation. A Graph Convolutional Network (GCN) model with two GCN layers was then trained to learn patterns associated with structural vulnerability based on node features and graph connectivity. The results indicate that structural vulnerability can be learned as a network property, with the model achieving an accuracy of approximately 82% across both configurations. This performance exceeds that of conventional centrality-based approximations. The findings also show that the inclusion of toll roads reshapes the distribution of vulnerability across the network. This supports the interpretation that toll roads act as structural modifiers by reconfiguring systemic vulnerability rather than simply increasing redundancy.

KEYWORDS Primary road network; Vulnerability; Structural connectivity; Graph Neural Network; Toll roads.

© The Author(s) 2026. This article is distributed under a Creative Commons Attribution-ShareAlike 4.0 International license.

1 INTRODUCTION

Primary road networks are among the most important transportation infrastructures for facilitating regional connectivity, people mobility, and interregional economic as well as logistics functions. In addition, functional road networks are critical for emergency response, evacuation, and post-disaster recovery, particularly in disaster-prone regions such as Indonesia. The significant roles played by road networks justify the evaluation of their vulnerability to disruptions, especially when the disruptions can cause extensive connectivity degradation in the network that is disproportionate to the physical scale of the disruption itself (Jenelius, 2009; Mattsson and Jenelius, 2015; Zhang et al., 2018). In the broader literature, resilience and vulnerability are often discussed together as complementary perspectives on network performance under disruption, although they represent distinct analytical constructs (Zeleke et al., 2026).

Studies on road network vulnerability have long been dominated by assessments that emphasize spatial hazard exposure and selected physical characteristics of network elements, such as flood-prone segments or the length of road sections affected by a disturbance. These approaches are undeniably useful for identifying where disruptions are likely to occur. However, they offer limited insight into how the failure of a single element propagates through the network and alters overall performance, particularly with respect to structural connectivity and topological redundancy. Partly to overcome this gap, graph-theoretical approaches have been increasingly adopted in transportation network studies (e.g. Zhang et al., 2018; Guze, 2019). By representing road systems as graphs that consist of sets of interconnected nodes and edges, these approaches make it possible to explore disruption impacts using topological indicators such as the size of the largest connected component (LCC), average shortest path length (ASPL), and betweenness centrality which are commonly used to evaluate connectivity and efficiency degradation in network vulnerability analysis (Guze, 2019). Therefore, from this perspective, classical graph-theoretic analysis provides a robust starting point for identifying critical components and examining topological fragility in transportation networks.

Using graph-theoretic frameworks, previous studies have demonstrated that the removal or failure of structurally important elements can trigger connectivity degradation that is systemic in nature, even when the underlying physical disruption remains relatively limited, as demonstrated in recent studies on hazard-induced network disruption (e.g. Alizadeh and Dodge, 2025; Seyedi et al., 2025). However, reliance on individual graph-related metrics introduces its own limitations because most of them are locally defined and are not designed to capture higher-order, non-linear interactions that emerge from complex network configurations (Guze, 2019). Moreover, vulnerability assessments based on multiple metrics often require extensive manual interpretation. As a result, the analysis can become difficult to consolidate into a single, coherent view of the system. In many cases, vulnerability is therefore represented as a collection of indicators, rather than as an inherent structural property that can be directly learned from network topology.

Recent developments in artificial intelligence open new possibilities for revisiting these limitations. One important direction is the emergence of Graph Neural Networks (GNNs). Through iterative message-passing and aggregation between neighboring nodes, GNNs can capture complex topological patterns directly from graph-structured data, without requiring all interactions to be explicitly specified. This capability has led to new approaches for analyzing infrastructure networks, including transportation systems, from a topology-driven perspective (Xue et al., 2025).

In transportation-related studies, GNNs have been applied to a wide range of problems, such as traffic prediction, operational optimization, and the analysis of spatio-temporal patterns (Xue et al., 2025). For example, Yu, Lee and Sohn (2020) demonstrated the use of GNN-based models for traffic-related prediction tasks. They have also been used to identify critical components that influence network performance under both normal and disrupted conditions (Xue et al., 2025). Beyond transportation-specific applications, recent studies have explored learning-based approaches, including Graph Convolutional Networks, to identify critical nodes in complex networks (Yu et al., 2020; ReddyPriya et al., 2026). Despite this progress, the use of GNNs to assess structural vulnerability in primary road networks based purely on graph topology remains relatively limited. This becomes particularly relevant when networks undergo structural changes, such as the introduction of toll roads, which alter connectivity patterns and redistribute traffic flows. While such interventions are typically intended to improve efficiency under normal conditions, they may also reshape how failures propagate across the network. For this reason, understanding the structural consequences of major infrastructure interventions can be addressed through vulnerability analyses that combine system-level topological reasoning with graph neural learning.

This study fills the gap by formulating primary road network vulnerability as a learnable structural property. A GNN-based framework is developed to learn structural vulnerability directly from the network's topological representations. To understand how toll roads reshape vulnerability in the road network, two independent network configurations are developed: one without toll roads and one with toll road inclusion. This framework enables an investigation of how such structural modifications reshape the network's vulnerability landscape. The proposed approach is expected not only to provide rich latent representations of the network structure but also to offer a new perspective for planning more resilient infrastructure systems against disaster-induced disruptions.

2 METHODS

Figure 1 summarizes the methods implemented in this study, comprising a series of steps conducted in sequence. These include the construction of graph models of the primary road network to be used as ground truth for learning, the formulation of network structural vulnerability as a learnable problem for GNNs, as well as the development of GNN training programs and the evaluation of model performance. Further details related to the methodology adopted in this study are discussed in the following sections.

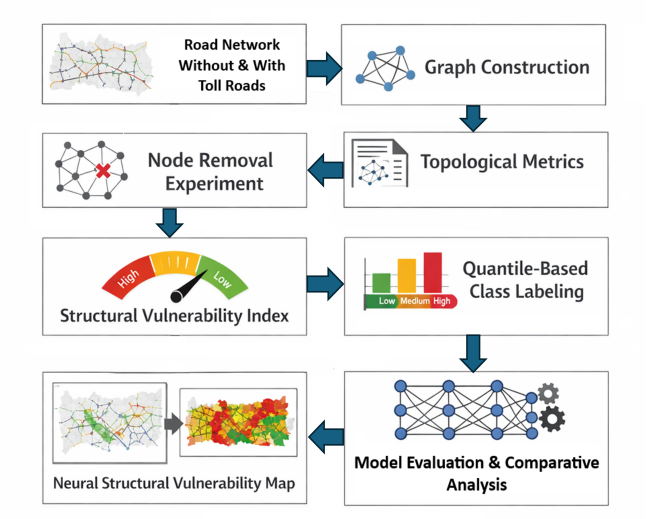


Figure 1. Graph neural methodology for learning structural vulnerability of primary road network.

2.1 Study Area

The study area of this research is Central Java Province, Indonesia, with the primary road network set as the focus of analysis (Figure 2). The network functions as part of the main transportation corridors in Java Is-

land and is frequently exposed to flood and landslide hazards. The Central Java primary road network is composed of a set of national and provincial road sections that serve as primary arterials, collectors, and local roads, connecting the western and eastern regions of Java Island and various national logistics distribution centers. The complex physiographic characteristics of Central Java, ranging from lowland coastal areas to hilly mountainous regions, help to shape this primary road network with an uneven distribution of redundancy.

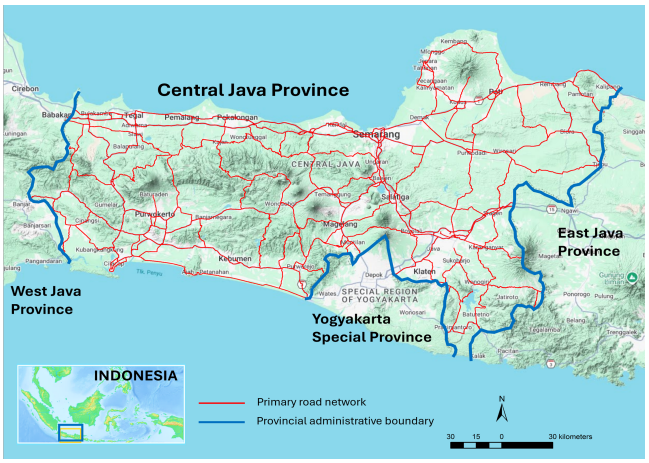


Figure 2. Physiographic conditions of Central Java Province and its primary road network (administrative boundary shown; data sources: Ministry of Public Works and Housing and Central Java Provincial Government; processed using ArcGIS).

2.2 Source of Data

Road network data were obtained from official geodatabase sources, namely the Ministry of Public Works and Housing and the Provincial Government of Central Java, in the form of shapefiles representing the national and provincial road sections designated as the primary road network in Central Java Province. Toll road sections that are part of the Trans-Java Toll Road Network and are located in the province were included in the datasets as a separate layer and were subsequently integrated into the primary road network to form a network model incorporating backbone infrastructure. All spatial datasets were projected to a single coordinate system, Universal Transverse Mercator (UTM) Zone 49S, to ensure geometric precision in distance calculations and graph construction.

2.3 Construction of Network Graphs

All road network representations were modeled as undirected, weighted graphs. An undirected representation was adopted to focus on the structural connectivity of the network rather than traffic flow directionality, which is consistent with the objective of assessing intrinsic structural vulnerability. While this assumption simplifies real-world traffic conditions, it is considered appropriate for capturing topological robustness; however, it may overlook direction-specific effects, such as one-way traffic constraints or asymmetric accessibility that could influence network performance under certain operational scenarios.

As commonly defined in graph theory (e.g. Newman, 2010), a graph G is formulated as shown in Equation (1).

$$G = (V, E, w) \tag{1}$$

where V denotes the union of nodes representing road intersections or functional junctions and E denotes the union of edges representing road sections connecting nodes, and w is a weight function that assigns a geometric length w_e to each edge $e \in E$. This formulation ensures that the shortest path calculations reflect actual travel distance.

To align with the purpose of this study, two graph models were developed using identical construction procedures. The first was the baseline network graph, representing the primary road network without the presence of toll road sections. The second was a graph representing the primary road network with the inclusion of toll road sections. Therefore, the structural difference between the two models originated solely from the presence of toll roads and their access nodes.

The graph construction process begins with generating an initial network from raw GIS road data obtained from official sources. In this representation, nodes correspond to geometric vertices along road centerlines, while edges represent the segments connecting consecutive vertices, as illustrated in Figure 3 (Step 1). However, this direct conversion introduces a number of non-functional nodes, such as curvature points and segmentation artifacts, which do not correspond to actual intersections and may distort the network structure.

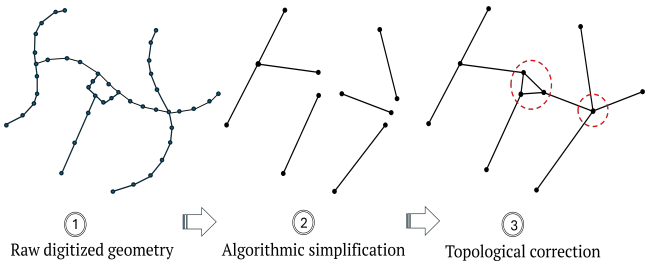


Figure 3. Graph construction workflow from raw GIS data to a topologically consistent network representation. Dashed circles highlight corrected local structures.

To address this issue, a simplification step is applied to remove non-essential elements. Nodes with degree two are iteratively eliminated as a simplification rule,

and their adjacent edges are merged while preserving overall connectivity (Figure 3, Step 2). This step reduces redundant intermediate vertices while retaining nodes that play a meaningful structural role, such as intersections and terminal points.

After simplification, some inconsistencies may still remain due to imperfections in the source data and the transformation process. A final topological correction step is therefore performed to improve structural consistency (Figure 3, Step 3). This includes removing self-loops, verifying connectivity, and correcting node-edge relationships as part of the topological consistency criteria where necessary. The resulting graph provides a cleaner and more reliable representation for subsequent analysis and GNN modeling.

All graph construction and preprocessing steps were implemented using a combination of GIS-based processing (ArcGIS) and Python-based network analysis tools (NetworkX).

2.4 The Construct of Intrinsic Structural Vulnerability as Ground Truth

In this study, structural vulnerability is treated as an intrinsic property of the road network, derived directly from its topology through disruption-based experiments on a graph representation. This approach does not rely on hazard data or traffic conditions. Instead, it focuses on isolating the structural contribution of the network itself, allowing the resulting vulnerability profile to be interpreted as a latent property embedded in the network configuration. The disruption experiments used to derive the network vulnerability profile are described as follows.

2.4.1 Node Removal Experiments

Following standard node removal procedures in network robustness analysis (e.g. Albert et al., 2000), for each node $v \in V$, a removal simulation procedure was conducted, as described in Equation (2).

$$G_{-v} = G \setminus \{v\} \tag{2}$$

The impact of node removal simulations was evaluated by the changes between G and G_{-v} graphs in terms of three main structural indicators, namely (i) network fragmentation, (ii) loss of connectivity, and (iii) loss of network efficiency. Network fragmentation is reflected by changes in the number of connected components due to node removals, while loss of connectivity is defined as the change in the size of the Largest Connected Component (LCC) between the two graphs. Lastly, in a similar manner, loss of network efficiency is evaluated as the change in network efficiency between the G and G_{-v} graphs. The global network efficiency of a graph (Latora and Marchiori, 2001) is adopted in this study and defined as follows Equation (3).

$$\eta(G) = \frac{1}{|V|(|V|-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \tag{3}$$

where $\eta(G)$ denotes the graph global efficiency and d_{ij} denotes the shortest path distance between nodes i and j.

2.4.2 Composite Structural Vulnerability Index

The fragmentation score $F_N(v)$ is defined as the normalized increase in the number of connected components following the removal of node v, reflecting the extent to which the network becomes structurally disconnected. This score is formulated as Equation (4).

$$F_N(v) = \frac{CC(G-v) - CC(G)}{|V| - 1} \tag{4}$$

where $CC(G)$ denotes the number of connected components in the original graph, and $CC(G-v)$ is the number of connected components after removing node v.

The connectivity loss $C_N(v)$ is defined as the relative reduction in the size of the largest connected component, and is formulated in Equation (5).

$$C_N(v) = \frac{LCC(G) - LCC(G-v)}{LCC(G)} \tag{5}$$

where $LCC(G)$ and $LCC(G-v)$ denote the sizes of the largest connected component before and after node removal, respectively.

The efficiency loss $E_N(v)$ is defined as the relative decrease in global network efficiency and is formulated in Equation (6).

$$E_N(v) = \frac{E(G) - E(G-v)}{E(G)} \tag{6}$$

where $E(G)$ represents the global efficiency of the network.

Based on these components, a composite structural vulnerability index $SV(v)$ was calculated according to Equation (7) by integrating the normalized values of $F_N(v)$, $C_N(v)$, and $E_N(v)$.

$$SV(v) = \frac{1}{3}\left(F_N(v) + C_N(v) + E_N(v)\right) \quad (7)$$

The composite structural vulnerability index defined in Equation (7) is developed in this study as an integrative measure of network-level structural degradation. Rather than adopting a single existing metric, the index combines three complementary components—fragmentation, connectivity loss, and efficiency loss—which are widely used indicators in graph-based network analysis. The equal weighting scheme is adopted to avoid introducing subjective bias and to maintain a balanced representation of these structural effects. This formulation allows the index to capture multiple dimensions of structural vulnerability in a unified manner. Since each component is normalized within the range [0,1], the resulting index $SV(v)$ also lies within [0,1]. A value close to 0 indicates that the removal of node v has minimal impact on network structure, while a value close to 1 indicates a highly critical node whose removal significantly disrupts connectivity and efficiency. In this sense, the proposed index represents an intrinsic measure of structural vulnerability associated with each node, reflecting its role in maintaining the integrity of the network.

2.4.3 Vulnerability Classification

Having the Composite Structural Vulnerability Index calculated for each node, the next step was to classify the measured values into three vulnerability classes, namely low, medium, and high vulnerability. The classification was conducted using a quantile-based approach by partitioning the distribution of index values into three groups with a relatively balanced number of nodes. The quantile approach was selected to ensure a relative representation of vulnerability based on the internal structure of the network without relying on an arbitrary threshold.

Let $SV(v)$ denote the composite structural vulnerability index associated with node v, and let Q_{33} and Q_{66} denote the 33rd and 66th percentiles of its distribution. The classification rule is defined as Equation (8).

$$C(v) = \begin{cases} 0, & SV(v) \le Q_{33} \\ 1, & Q_{33} < SV(v) \le Q_{66} \\ 2, & SV(v) > Q_{66} \end{cases} \quad (8)$$

where $C(v)$ denotes the vulnerability class associated with node v, corresponding to low (0), medium (1), and high (2) vulnerability. This classification enables the identification of the most structurally vulnerable nodes in the context of the network configuration being analyzed, as well as supports consistent comparison of vulnerability among nodes within the same network system.

2.5 Node Features Representation

Each node in the network was represented by a vector of structural features consisting of its degree (defined as the number of directly connected neighboring nodes), betweenness centrality, closeness centrality, an articulation node indicator, as well as the loss of network efficiency due to node removal. These features were selected to represent the local topological characteristics and the structural role of the node in the network, under both normal and disrupted conditions. All features were normalized prior to the neural learning process to ensure scale consistency and learning stability. It is to be noted that the composite node vulnerability index was not included in this feature representation because it functions as the learning target derived from network-level responses, not as an intrinsic structural feature of nodes.

2.6 GNN Architecture and Learning Protocol

The GNN model was implemented as a Graph Convolutional Network (GCN) model (Kipf and Welling, 2016) with two graph convolution layers, using the PyTorch Geometric framework. A two-layer GCN architecture was selected due to its ability to integrate node features and capture non-linear structural patterns beyond those represented by individual graph metrics.

The model input is defined as a node feature representation matrix $X \in R^{|V|\times F}$, where F denotes the number of node features. Each node is characterized by structural attributes including degree, betweenness centrality, closeness centrality, articulation indicator, and efficiency loss.

These features were subsequently propagated through the two graph convolution layers (GCNConv) with Rectified Linear Unit (ReLU) activation, as described in Equation (9) to (11), enabling the model to capture higher-order topological interactions. Dropout was implemented as a regularization mechanism to reduce the risks of overfitting. The outputs of the final convolution layer were mapped into vulnerability classes using a Softmax function to produce class probability distributions.

$$H^{(1)} = \sigma\big(\text{GCNConv}(X, A)\big) \quad (9)$$

$$H^{(2)} = \sigma\big(\text{GCNConv}(H^{(1)}, A)\big) \quad (10)$$

$$Z = \text{Softmax}(WH^{(2)}) \quad (11)$$

with H denoting a hidden layer, A denoting the adjacency (neighborhood) matrix, σ denoting the ReLU ac-

tivation function, and Z denoting class probabilities. The GCNConv operation follows the normalized graph convolution formulation proposed by Kipf and Welling (2016).

The ground truth vulnerability labels are derived from node removal experiments based on changes in global efficiency and connectivity, and are subsequently discretized into three classes using a quantile-based scheme.

The model is trained separately for the without-toll-road and with-toll-road network configurations using identical hyperparameters to ensure a fair comparison. Training is performed using the Adam optimizer (Kingma and Ba, 2017) with a categorical cross-entropy loss function and a learning rate of 0.01. The model is trained for up to 200 epochs with early stopping based on validation loss. The dataset is split into training and testing subsets using a stratified sampling scheme to preserve class proportions. Model weights are initialized using Xavier initialization (Glorot and Bengio, 2010).

2.7 Model Evaluation

GNN model performance was evaluated using overall accuracy, as well as precision, recall, and F1-scores for each vulnerability class. In addition, a confusion matrix was used to describe misclassification patterns across classes. Beyond predictive evaluation, node latent embeddings were extracted from the final hidden layer and further analyzed to study the structural representations learned by the model and to uncover the landscape of structural vulnerability within the network.

2.8 Experiment Design of Two Controlled Networks

The experiment was designed as two controlled structural worlds, in which the without-toll-road and with-toll-road networks were analyzed using fully identical GNN architectures and training protocols. Vulnerability labels of each network were constructed independently based on structural disruption experiments to ensure that no information leakage occurred between scenarios. With this design, all differences in learning outcomes and classification results can be directly attributed to topological transformations induced by the inclusion of toll road sections in the primary road network. Therefore, this study positions GNN not only as a predictive model but also as a diagnostic instrument for interpreting the structural consequences of large-scale infrastructure interventions.

2.9 Comparative Analysis

To provide a comparative reference, a simple baseline classification was constructed using betweenness centrality (BC), which is a classical graph-theoretic measure of node importance. Let $G = (V, E)$ denote the road network graph. For each node $v \in V$, the betweenness centrality is defined as Equation (12).

$$BC_v = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{12}$$

where σ_{st} is the number of the shortest paths between nodes s and t, and $\sigma_{st}(v)$ is the number of those paths passing through node v.

Given that the available centrality values were associated with edge endpoints, node-level centrality was approximated by averaging the values of all incident edges, as defined in Equation (13).

$$\widetilde{BC}_v = \frac{1}{k_v} \sum_{e \in E(v)} BC_{v,e} \tag{13}$$

where $\varepsilon(v)$ denotes the set of edges connected to node v, and k_v is its degree.

The aggregated centrality values were then partitioned into three classes using a quantile-based scheme similar to that described in Section 2.4.3. The resulting BC-based vulnerability classes $C^{\mathrm{BC}}(v)$ were subsequently compared with the ground truth vulnerability classes $C(v)$, which were derived from node removal experiments. The classification accuracy is defined as Equation (14).

$$\text{Accuracy} = \frac{1}{|V|} \sum_{v \in V} \delta\big(C^{BC}(v), C(v)\big) \tag{14}$$

where $\delta(.)$ is the Kronecker delta function, which equals 1 if the predicted and actual classes are identical and 0 otherwise.

3 RESULTS

This section reports the results of the GNN learning on structural vulnerability of the primary road network in Central Java Province under two network configurations, namely networks without toll roads and with toll road inclusion (network with backbone infrastructure). The results include network characteristics, the construction of structural vulnerability ground truth, GNN model performance, and the spatial distribution of vulnerability resulting from neural learning.

3.1 Characteristics of the Networks without and with Toll Roads

Figure 4 depicts the graph representation of the primary road network in Central Java Province that was constructed and verified to have full connectivity, consistent node–edge relationships, and no self-loops.

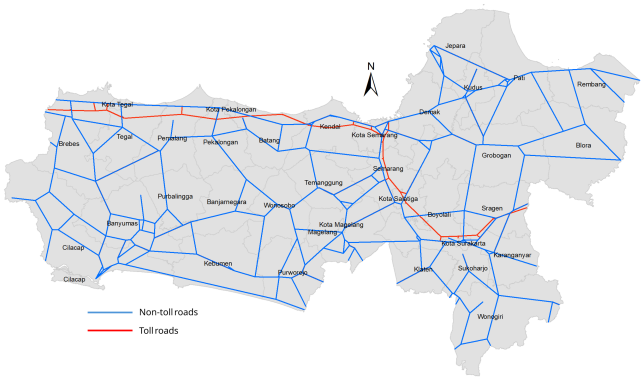


Figure 4. Graph representation of the primary road network in Central Java Province (processed using ArcGIS).

Two configurations of the primary road network were constructed as undirected, weighted graphs. Basic characteristics of these two graphs are shown in Table 1. From Table 1, both graphs form a single connected component, indicating full connectivity at the scale of the primary road network. Model 2 (the with-toll-road model) has a larger number of nodes and edges compared to Model 1 due to the integration of toll road sections and their associated access nodes. Model 2 exhibits a slightly lower global efficiency compared to Model 1, although it has a larger network size.

Table 1. Basic characteristics of the graphs representing the primary road network

Characteristics	Model 1	Model 2
Description	Without toll roads	With toll roads
Nodes	205	250
Edges	269	330
Connected Component	1	1
Global efficiency	0.1332	0.1270

3.2 Ground Truth Construction and Intrinsic Structural Vulnerability

Intrinsic structural vulnerability at the node level was represented by the composite structural vulnerability index, which was used as the ground truth for GNN learning. These vulnerability labels were derived from node-removal-based structural analysis; therefore, the GNN model is trained to learn and approximate the structural response of this conventional approach. The statistical distribution of the index values for the two network configurations is shown in Table 2.

Table 2. Statistics of the intrinsic structural vulnerability index

Model	Nodes	Minimum	Average	Maximum
1	205	0.0000	0.1186	0.7324
2	250	0.0000	0.1137	0.7189

The vulnerability index values were subsequently classified into three classes using quantile-based partitioning. The resulting class distribution is reported in Table 3. As shown in Table 3, the class distributions for both models are relatively even, indicating the stability of the quantile partitioning scheme.

Table 3. Distribution of structural vulnerability class

Model	Low Vulnerability Nodes	Medium Vulnerability Nodes	High Vulnerability Nodes
1	68	67	70
2	83	84	83

Visualization of the boxplots (Figure 5) shows a strongly skewed distribution in both network configurations, with only a few nodes exhibiting much higher vulnerability values than the rest. This is reflected in the low median values (0.0308 and 0.0358) compared to the means (0.1186 and 0.1137), indicating the presence of structurally critical nodes. Compared to the network without toll roads, the toll-integrated network exhibits slightly lower mean vulnerability, while maintaining a similarly skewed distribution. The dispersion of values remains comparable between the two configurations, although the toll-integrated network shows a tendency toward more localized high-value observations. The slightly lower average value in the toll-integrated network suggests that toll road integration does not uniformly reduce structural vulnerability, but rather reshapes its distribution across the network. In quantitative terms, the average structural vulnerability decreases from 0.1186 to 0.1137, corresponding to a reduction of approximately 4.1%. This indicates that

the inclusion of toll roads leads to a measurable shift in the vulnerability landscape, characterized by redistribution rather than uniform improvement.

Table 4. Development of model accuracy during GNN training under two network configurations

Epoch	Model 1 (without toll roads)		Model 2 (with toll roads)	
	Loss	Accuracy	Loss	Accuracy
0	1.1000	0.3268	1.1453	0.3320
40	0.8910	0.5756	0.9266	0.6120
80	0.7310	0.6537	0.8158	0.6920
120	0.5226	0.7805	0.6006	0.7560
160	0.4242	0.8049	0.4917	0.8120
200	0.3678	0.8293	0.4546	0.8240

The results, as reflected in the aggregate statistics (Table 2), class distribution (Table 3), and boxplot representation (Figure 5), consistently indicate that the network exhibits a heterogeneous structural behavior, in which vulnerability is not evenly distributed but concentrated in a limited number of structurally critical nodes. While most nodes contribute minimally to overall structural degradation, a small subset of nodes plays a disproportionately important role in maintaining connectivity and efficiency. This suggests that the intrinsic vulnerability of the network is governed by localized structural dependency rather than uniform redundancy.

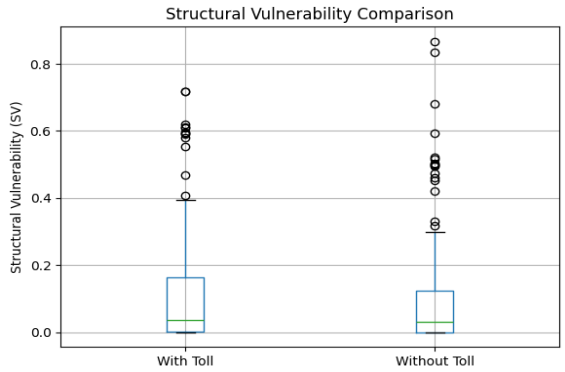


Figure 5. Boxplot summary statistics of structural vulnerability of the primary road network without toll roads and with toll roads.

3.3 Performance of the GNN model

The GNN model was independently trained for Model 1 and Model 2 using an identical architecture and identical hyperparameters. Table 4 reports the development of model accuracies during two independent training processes, each lasting for 200 epochs.

With node feature matrices having dimensions of 205 × 4 and 250 × 4, and with 205 and 250 vulnerability labels, respectively, both models exhibit comparable convergence patterns during the learning process. Model 1 achieved a final accuracy of 82.93%, while Model 2 achieved 82.40%. These results show that the GNN model is capable of learning structural vulnerability classes consistently under both network configurations, despite differences in network topology introduced by toll road integration. In machine learning applications, model performance is generally evaluated relative to baseline methods and convergence behavior rather than against a fixed error threshold, as acceptable performance depends on the characteristics of the dataset and the learning task (Bishop and Nasrabadi, 2006; Goodfellow et al., 2016). It should be noted that among the five structural indicators computed during node removal experiments, efficiency loss was used only for ground-truth construction and was not included in the node feature vector during GNN training.

A pair of confusion matrices (Figure 6) further illustrates the classification performance of the GNN model for both network configurations. The dominance of values along the main matrix diagonal indicates a high level of agreement between predicted vulnerability classes and the ground truth labels across the three vulnerability categories.

In addition to the GNN-based classification, a baseline approach based on betweenness centrality (BC) was evaluated for both network configurations. Using a quantile-based classification scheme as outlined in Section 2.9, the BC-based approach achieved an accuracy of approximately 55.6% for the network without toll roads and approximately 53.8% for the network with toll roads.

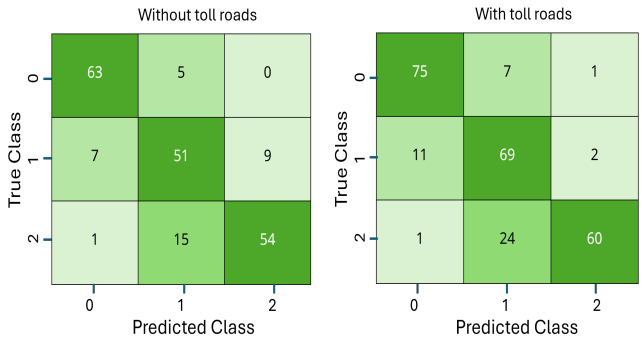


Figure 6. Confusion matrices of GNN learning results under Model 1 (left side) and Model 2 (right side).

A comparison between the baseline and the proposed model is presented in Table 5. The results indicate that the GNN model achieves substantially higher accuracy than the centrality-based baseline across both network configurations.

Table 5. Comparison between baseline and GNN performance under two network configurations

Model	Without Toll Roads	With Toll Roads
Betweenness Centrality (quantile)	55.6%	53.8%
GNN (proposed)	82.9%	82.4%

3.4 Spatial Distribution of Neural Vulnerability

The spatial distribution of network vulnerability learned by the GNN model was analyzed by projecting the predicted vulnerability class of each node back onto the geographic coordinates of the primary road network. This projection enables visual examination of vulnerability patterns under the two network configurations (Model 1 and Model 2). Figure 7 (left part) shows the spatial distribution of the neural vulnerability classes under Model 1 (network without toll roads). Nodes with high neural vulnerability are observed along a number of main interregional connecting corridors, with a relatively distributed pattern across the primary road network.

The influence of integrating toll road sections into the network on the distribution of vulnerability classes as learned by the GNN model is shown in Figure 7 (right part). Under this configuration (Model 2), the pattern of neural vulnerability exhibits a noticeable shift in the clustering of vulnerable nodes compared to Model 1.

To obtain a more detailed spatial perspective, Figure 8 and 9 present a comparison of neural vulnerability distributions along two main corridors of the network, namely the Pantura–Brebes–Semarang corridor and the Semarang–Surakarta corridor, respectively. These detailed visuals allow a clearer observation of differences in the spatial configuration of vulnerable nodes between Model 1 and Model 2. In particular, the toll-integrated network (Model 2) exhibits a more concentrated clustering of high-vulnerability nodes along key segments, whereas in Model 1 the vulnerable nodes appear more dispersed across the corridor. This suggests that the introduction of toll roads tends to reorganize the spatial distribution of vulnerability, shifting it toward more localized structural dependencies rather than evenly distributed network influence.

4 DISCUSSION

4.1 Vulnerability as an Intrinsic Structural Property

This study aimed to answer the main question of whether the vulnerability of primary road networks can be understood as an intrinsic structural property embedded within network topology, and whether this property can be learned directly from graph representations without relying on additional information such as hazard exposure or operational inputs. The results show that intrinsic structural vulnerability at the node level can be learned by a Graph Neural Network (GNN) model using only the structural features and graph adjacency relationships. These findings strengthen arguments in the network science literature stating that the failure of elements with specific roles can cause systemic connectivity degradation that is disproportionate to the physical scale of the disruptions (Albert et al., 2000; Crucitti et al., 2006; Guze, 2019). In the context of transportation networks, these findings are consistent with the results of previous works (see e.g. Jenelius, 2009; Mattsson and Jenelius, 2015; Zhang et al., 2018; Lu et al., 2021) which show that network

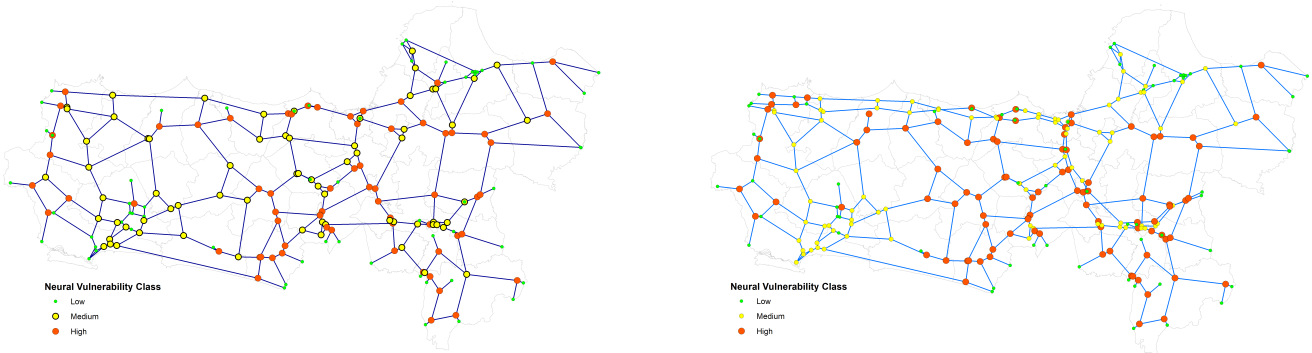


Figure 7. Spatial distribution of neural vulnerability classes for the primary road networks without toll roads (left) and with toll road integration (right) (processed using ArcGIS).

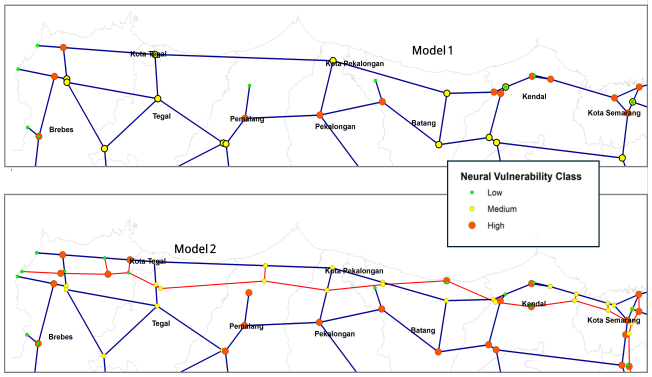


Figure 8. Spatial distribution of neural vulnerability classes along the Pantura-Brebes-Pekalongan-Semarang corridor for Model 1 (top) and Model 2 (bottom); (processed using ArcGIS).

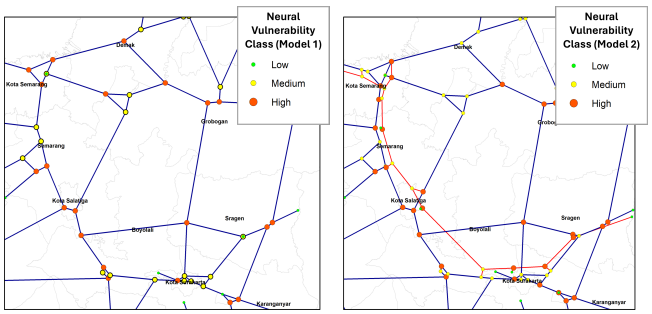


Figure 9. Spatial distribution of neural vulnerability classes along the Semarang-Surakarta corridor for Model 1 (left) and Model 2 (right); (processed using ArcGIS).

vulnerability is not only determined by hazard exposure. In addition, it is also a result of the topological configuration and structural redundancy of the network itself. While accessibility-based approaches provide valuable insights into performance degradation under specific disruption scenarios (Henke et al., 2024), they do not fully capture the structural conditions that predispose a network to systemic fragility. This study therefore complements such approaches by focusing on vulnerability as an intrinsic property of network topology.

Unlike classical graph-theoretic approaches that rely on manual interpretation of various metrics, such as the LCC, ASPL, or betweenness centrality (Guze, 2019), the GNN-based approach proposed in this study enables vulnerability to be learned as an integrated latent representation. In this way, vulnerability is no longer understood as an aggregation of local and independent indicators, but as a systemic property that emerges from non-linear interactions among nodes within the network.

In this study, the road network is represented as a graph in which nodes correspond to physical intersections or junctions, and edges represent road segments. While origin–destination movements in real transportation systems may occur along any point of a road segment, the graph abstraction represents these movements through paths connecting nodes. The focus on node-based vulnerability is therefore intended to capture structurally critical points whose removal can significantly alter global connectivity and efficiency. In this context, node removal serves as a proxy for structural disruption, enabling the analysis of how failures propagate through the network topology. Nevertheless, link-based representations provide a complementary perspective, particularly for capturing segment-specific or direction-dependent characteristics, and are identified as a potential direction for future research.

4.2 GNN Model Accuracy in Structural Vulnerability Learning

The GNN model developed in this study reached classification accuracy levels of approximately 82% for both network configurations, namely networks without and with toll road sections. This value should not be interpreted as a maximum achievable performance, but rather as the result obtained under the current modeling scope. In the context of machine learning, this accuracy score is not meant to compete with model optimization studies or operational prediction tasks, but rather to demonstrate the capability of the model to learn structural representations from latent and abstract targets. The vulnerability labels learned by the model did not originate from direct empirical observation, but were instead derived from graph-based disruption experiments that represent network responses to node failures. Learning targets, therefore, contain inherent structural ambiguity, which leads to non-decisive decision boundaries. Under such conditions, an accuracy level of around 82% reflects the model's success in capturing latent topological patterns, rather than indicating a limitation of the model itself.

The comparison with the centrality-based baseline further highlights the limitation of classical graph-theoretic metrics in representing structural vulnerability. Although betweenness centrality captures certain aspects of node importance, its performance remains limited (approximately 54–56%) and does not improve across different network configurations.

In contrast, the GNN model achieves consistently high accuracy (approximately 82%) in both without-toll and with-toll scenarios. This consistency suggests that structural vulnerability cannot be sufficiently explained by local node importance alone, but rather emerges from higher-order interactions within the network topology. The ability of the GNN model to integrate structural features through message-passing mechanisms enables it to capture these interactions, allowing vulnerability to be interpreted as a system-level property rather than a purely metric-based attribute.

It is worth noting that this neural learning process was conducted entirely using structural features, explicitly excluding the composite vulnerability index as well as any hazard-related information from the node representation. This methodological decision was consciously made for two reasons: to avoid target leakage and to deliberately limit the predictive ceiling. Accordingly, the obtained outcomes, namely the accuracy represents a trade-off between pure structural learning and predictive performance. The consistent accuracy levels produced by the two learning processes applied to networks with and without toll roads demonstrate a high degree of stability in the face of changes in network topology.

The consistent performance observed under both network configurations further highlights the role of GNNs as effective representation learning frameworks for graph-based complex systems (Kipf and Welling, 2016; Hamilton et al., 2017; Wu et al., 2021). More broadly, this finding aligns with the growing adoption of machine learning techniques for infrastructure and geospatial vulnerability assessment (Olii et al., 2025). While previous studies have primarily focused on susceptibility modelling using environmental and spatial variables, the present study extends this learning paradigm by demonstrating that latent structural vulnerability can be learned directly from road network topology through graph neural networks. This also supports recent applications of GNNs in transportation and infrastructure networks (Sant'Ana da Silva et al., 2023; Xue et al., 2025).

4.3 Transformation of the Vulnerability Landscape due to Toll Road Integration

An examination of the spatial distribution of neural vulnerability reveals clear differences between the two network configurations (without and with toll roads). In the absence of toll roads, a dispersed pattern of nodes classified as highly vulnerable is observed. This is due to their tendency to be present along several major interregional corridors. Rather than concentrating on a few locations, vulnerability in this configuration is spread across multiple connecting routes. In contrast, a different pattern is observable when toll roads are introduced. In this configuration, vulnerable nodes show a stronger tendency to cluster within specific parts of the network. A shift toward a more centralized vulnerability structure is therefore captured. This pattern shift suggests that toll road integration alters how vulnerability is spatially organized within the primary road network system. From a broader network perspective, this observation aligns with findings in the transportation vulnerability literature (Mattsson and Jenelius, 2015; Wang et al., 2017; Lin and Lin, 2022; Redzuan et al., 2022), which indicate that increases in connectivity and traffic flow concentration are often accompanied by greater dependence on a limited set of structurally important nodes. The present study offers an additional insight that large-scale structural interventions, such as toll road development, can generate distinct vulnerability landscapes, even when their primary motivation is to enhance overall network performance.

4.4 Toll Roads as Structural Modifiers in the Primary Road Network

Viewed collectively, the results of neural learning and spatial analysis suggest that the inclusion of a toll road system within a primary road network can be interpreted as the introduction of a structural modifier. In this sense, toll roads actively modify topological connections between nodes and redistribute structural roles across the network, rather than merely functioning as infrastructure additions. As a result, changes in connectivity and redundancy extend beyond local improvements and influence the network as a whole. From an infrastructure engineering standpoint, there have been calls for more systemic and structure-aware frameworks for conducting infrastructure evaluation, beyond the considerations of capacity expansion or efficiency gains (e.g. Taylor, 2017; Bergantino et al., 2024). By using the GNN model as a structural diagnostic tool, this study responds to this call by highlighting the need for assessments that also account for the long-term structural implications of infrastructure interventions on road network vulnerability. The findings demonstrate that the structural consequences of such interventions can be explicitly interpreted through changes in the vulnerability landscape learned by the GNN model.

Building on this interpretation, the identification of structurally critical nodes provides insight into potential strategies for improving network robustness. From a structural perspective, interventions that enhance redundancy around these nodes—such as introducing alternative connections or strengthening link diversity—may reduce the concentration of vulnerability. This suggests that infrastructure development should be approached with structural awareness, where new elements, including toll roads, are evaluated not only for their direct functional benefits but also for their capacity to redistribute structural dependency and mitigate intrinsic network vulnerability.

4.5 Methodological Implications, Limitations, and Future Directions

Methodologically, this study shows that GNNs can function as instruments for structural analysis of infrastructure networks. This is beyond their conventional role as purely predictive tools. As demonstrated

in this study, this approach provides an integrated representation capable of capturing non-linear topological interactions that are difficult to represent using individual metrics in classical graph-based methods.

This study, however, has several limitations that should be noted. Although this choice was methodologically intentional, the features considered in the GNN learning process were purely structural, excluding spatial, operational, or temporal dimensions. As a result, the vulnerability discussed in this study is explicitly framed as structural vulnerability. In addition, the analysis is based on a node-centric representation of the network, which may not fully capture link-specific characteristics such as directional flow or segment-level conditions. Secondly, while the comparison with a centrality-based baseline provides initial evidence of the model's capability, the results should be interpreted within the scope of this study, which is limited to a single case and a specific set of structural features. These limitations define the scope of the present analysis and simultaneously open opportunities for future research. Future studies may integrate additional dimensions or test the generalizability of the proposed framework on road networks in other regions to further enhance the understanding of the relationships between network structure, infrastructure interventions, and system vulnerability.

5 CONCLUSION

This study demonstrates that structural vulnerability in road networks is not uniformly reduced by infrastructure expansion, but instead undergoes redistribution following the integration of toll roads. While the average structural vulnerability shows a slight decrease, the overall distribution remains highly skewed, indicating the persistence of structurally critical nodes. These findings suggest that network modifications may alter the configuration of vulnerability without eliminating it. The main contribution of this study lies in framing structural vulnerability as an intrinsic and learnable property of the network, derived purely from graph topology. By integrating graph-theoretic indicators with a Graph Neural Network (GNN) approach, the study demonstrates how higher-order structural interactions can be captured beyond traditional centrality-based metrics, providing a new perspective for understanding intrinsic structural road network vulnerability. Nevertheless, the findings should be interpreted within the scope of this study, which is limited to a single regional case and a structural representation of the network. Future research may extend this framework by incorporating directional, spatial, or temporal dynamics, as well as applying the approach to other regions to further evaluate its generalizability.

DISCLAIMER

The authors declare no conflict of interest.

REFERENCES

Albert, R., Jeong, H. and Barabási, A.-L. (2000), 'Error and attack tolerance of complex networks', *Nature* **406**(6794), 378–382.
URL: *https://doi.org/10.1038/35019019*

Alizadeh, D. and Dodge, S. (2025), 'Disaster vulnerability in road networks: A data-driven approach through analyzing network topology and movement activity', *International Journal of Geographical Information Science* **39**(5), 1035–1056.
URL: *https://doi.org/10.1080/13658816.2024.2411001*

Bergantino, A., Gardelli, A. and Rotaris, L. (2024), 'Assessing transport network resilience: Empirical insights from real-world data studies', *Transport Reviews* **44**(4), 834–857.
URL: *https://doi.org/10.1080/01441647.2024.2322434*

Bishop, C. and Nasrabadi, N. (2006), *Pattern Recognition and Machine Learning*, Springer.

Crucitti, P., Latora, V. and Porta, S. (2006), 'Centrality measures in spatial networks of urban streets', *Physical Review E* **73**(3), 036125.
URL: *https://doi.org/10.1103/PhysRevE.73.036125*

Glorot, X. and Bengio, Y. (2010), Understanding the difficulty of training deep feedforward neural networks, *in* Y. Teh and M. Titterington, eds, 'Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics', Proceedings of Machine Learning Research, Chia Laguna Resort, Sardinia, Italy, pp. 249–256.
URL: *https://proceedings.mlr.press/v9/glorot10a.html*

Goodfellow, I., Bengio, Y. and Courville, A. (2016), *Deep Learning*, MIT Press, Cambridge, MA.

Guze, S. (2019), 'Graph theory approach to the vulnerability of transportation networks', *Algorithms* **12**(12), 270.
URL: *https://doi.org/10.3390/a12120270*

Hamilton, W., Ying, Z. and Leskovec, J. (2017), Inductive representation learning on large graphs, *in* I. e. a. Guyon, ed., 'Advances in Neural Information Processing Systems', Curran Associates, Inc.
URL: *https://proceedings.neurips.cc/paper/2017/hash/5dd9db5e033da9c6fb5ba83c7a7ebea9-Abstract.html*

Henke, I., Troiani, G. and Pagliara, F. (2024), 'An analysis of the vulnerability of road networks in response to disruption events through accessibility indicators specification', *Transportation Planning and Technology* **47**(5), 628–655.
URL: *https://doi.org/10.1080/03081060.2024.2329650*

Jenelius, E. (2009), 'Network structure and travel patterns: Explaining the geographical disparities of road network vulnerability', *Journal of Transport Geography* **17**(3), 234–244.
URL: *https://doi.org/10.1016/j.jtrangeo.2008.06.002*

Kingma, D. and Ba, J. (2017), 'Adam: A method for stochastic optimization'. arXiv:1412.6980.
URL: *https://arxiv.org/abs/1412.6980*

Kipf, T. and Welling, M. (2016), 'Semi-supervised classification with graph convolutional networks', *arXiv preprint arXiv:1609.02907* .
URL: *https://arxiv.org/abs/1609.02907*

Latora, V. and Marchiori, M. (2001), 'Efficient behavior of small-world networks', *Physical Review Letters* **87**(19), 198701.
URL: *https://doi.org/10.1103/PhysRevLett.87.198701*

Lin, J. and Lin, W. (2022), 'Transportation system vulnerability assessment considering environmental impact', *Journal of Advanced Transportation* **2022**, 1–12.
URL: *https://doi.org/10.1155/2022/8711894*

Lu, Q., Xu, P. and Zhang, J. (2021), 'Infrastructure-based transportation network vulnerability modeling and analysis', *Physica A: Statistical Mechanics and its Applications* **584**.
URL: *https://doi.org/10.1016/j.physa.2021.126350*

Mattsson, L.-G. and Jenelius, E. (2015), 'Vulnerability and resilience of transport systems – a discussion of recent research', *Transportation Research Part A: Policy and Practice* **81**, 16–34.
URL: *https://doi.org/10.1016/j.tra.2015.06.002*

Newman, M. E. J. (2010), *Networks: An Introduction*, Oxford University Press, Oxford.

Olii, M. R., Nento, S., Doda, N., Olii, R. S. N., Djafar, H. and Pakaya, R. (2025), 'Transformation of geospatial modelling of soil erosion susceptibility using machine learning', *Journal of the Civil Engineering Forum* **11**(2), 217–232.
URL: *https://doi.org/10.22146/jcef.19581*

ReddyPriya, M. et al. (2026), 'Integrating machine learning techniques for critical node identification in complex networks', *Scientific Reports* **16**(1), 8929.
URL: *https://doi.org/10.1038/s41598-026-40778-y*

Redzuan, A. et al. (2022), 'Road network vulnerability based on diversion routes to reconnect disrupted road segments', *Sustainability* **14**(4), 2244.
URL: *https://doi.org/10.3390/su14042244*

Sant'Ana da Silva, E., Pedrini, H. and Santos, A. d. (2023), 'Applying graph neural networks to support decision making on collective intelligent transportation systems', *IEEE Transactions on Network and Service Management* **20**(4), 4085–4096.
URL: *https://doi.org/10.1109/TNSM.2023.3257993*

Seyedi, I. et al. (2025), 'Structural vulnerability assessment in urban transport networks: A network-wide geometric approach using gromov-wasserstein'.
URL: *https://arxiv.org/abs/2510.24306*

Taylor, M. (2017), *Vulnerability Analysis for Transportation Networks*, Elsevier, Amsterdam.

Wang, J. et al. (2017), 'Research on the robustness of interdependent networks under localized attack', *Applied Sciences* **7**(6), 597.
URL: *https://doi.org/10.3390/app7060597*

Wu, Z. et al. (2021), 'A comprehensive survey on graph neural networks', *IEEE Transactions on Neural Networks and Learning Systems* **32**(1), 4–24.
URL: *https://doi.org/10.1109/TNNLS.2020.2978386*

Xue, J. et al. (2025), 'Data science in transportation networks with graph neural networks: A review and outlook', *Data Science for Transportation* **7**(2), 10.
URL: *https://doi.org/10.1007/s42421-025-00124-6*

Yu, B., Lee, Y. and Sohn, K. (2020), 'Forecasting road traffic speeds by considering area-wide spatio-temporal dependencies based on a graph convolutional neural network (gcn)', *Transportation Research Part C: Emerging Technologies* **114**, 189–204.
URL: *https://doi.org/10.1016/j.trc.2020.02.013*

Yu, E.-Y. et al. (2020), 'Identifying critical nodes in complex networks via graph convolutional networks', *Knowledge-Based Systems* **198**, 105893.
URL: *https://doi.org/10.1016/j.knosys.2020.105893*

Zeleke, Y., Tira, M. and Scaini, C. (2026), 'Resilience of road networks to natural hazards: A systematic literature review', *Transportation Engineering* **23**, 100420.
URL: *https://doi.org/10.1016/j.treng.2026.100420*

Zhang, J., Wang, S. and Wang, X. (2018), 'Comparison analysis on vulnerability of metro networks based on complex network', *Physica A: Statistical Mechanics and its Applications* **496**, 72–78.
URL: *https://doi.org/10.1016/j.physa.2017.12.094*

[This page is intentionally left blank]