Vulnerability assessment of large-scale urban road network under emerging disinformation attacks

Yangyang Meng[a], Xiaofei Zhao[b], Xiaotong Xu[a] and Wei Ma[a,c*]

[a]Department of Civil and Environmental Engineering, The Hong Kong Polytechnic University, Kowloon, Hong Kong; [b]Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong; [c]Research Institute for Sustainable Urban Development, The Hong Kong Polytechnic University, Kowloon, Hong Kong

ARTICLE HISTORY
Compiled April 1, 2025

ABSTRACT
Transportation Cyber-Physical Systems (TCPS) are facing an emerging cyber threat from disinformation attacks that can manipulate individual cognition and behaviors, potentially making urban transportation vulnerable. Traditional studies on road network vulnerability have primarily focused on physical attacks like node or link removal, with little attention to disinformation attacks. To fill this gap, this study introduces a novel disinformation attack mode for road TCPS. It hacks navigation applications by strategically modifying the link cost information, thereby affecting drivers' routing decisions. Crucially, this attack mode leaves the physical topology of TCPS-based road networks unchanged, impacting only the cyber layer's information. Additionally, intriguing link metrics, like the partial derivative of total travel time to link flow, are introduced to identify attack targets. On this basis, we design multi-strategy disinformation attacks to assess road network vulnerability. The proposed research framework, validated by San Francisco's large-scale urban road network, reveals that disinformation attacks on just 0.12% of links could cause an annual city-wide economic loss of $79.26 million in the worst-case scenario. This study offers a unique viewpoint on road network vulnerability, emphasizing the vital need for TCPS cybersecurity to ensure urban transportation's reliability and resilience.

KEYWORDS
Vulnerability assessment; disinformation attacks; large-scale road network; transportation cyber-physical system

1. Introduction

The development goals of smart and sustainable cities are intensifying the need for intelligent, green, and resilient transportation solutions (Chow et al. 2015). In the digital 3.0 era, Transportation Cyber-Physical Systems (TCPS) (Deka et al. 2018; Dey, Fries, and Ahmed 2018) are emerging as a promising paradigm for next-generation transportation systems (Zhu, Qu, and Ma 2023). TCPS seamlessly integrate physical and cyber infrastructures, facilitating the collection, processing, and analysis of real-time data for intelligent transportation system management. However, TCPS remains vulnerable to various cybersecurity threats, including hacktivism, data poisoning attacks, deepfake manipulations, and malicious applications of generative artificial intel-

*Corresponding author: Wei Ma. Email: wei.w.ma@polyu.edu.hk

ligence, all of which can severely compromise urban transportation system operations (Pundir et al. 2022). Consequently, conducting comprehensive vulnerability assessments of TCPS-based road networks against potential cyberattacks is essential for ensuring the continued reliability, resilience, and sustainability of urban transportation infrastructure.

Nowadays, the emergence of digital media and technological advancements has led to a unique and emerging cybersecurity threat in the form of disinformation. Disinformation refers to the false information deliberately spread to deceive people. Traditional cyberattacks are mainly technical, targeting computer systems, networks and data, while Disinformation attacks are psychological and information-based, aiming at exploiting our cognitive biases and emotional reactions. Disinformation is a form of cognitive hacking (Vagan, Golovianko, and Gryshko 2018). Recent widespread disinformation campaigns targeting the U.S. presidential election, Brexit, and COVID-19 vaccination have spotlighted the disinformation attack as an emerging and significant cybersecurity threat (Pathak, Srihari, and Natu 2021; Jamalzadeh et al. 2022). Disinformation detrimentally affects multiple domains, encompassing societal, political, economic, and psychological aspects. The Global Risks Report 2023 has added *misinformation and disinformation* as a new risk. In the contemporary digital landscape characterized by instantaneous information dissemination, the rapid proliferation of zero-cost rumors and the increasing prevalence of conversational AI technologies have amplified the potential impact of disinformation attacks, necessitating heightened attention and vigilance. However, the existing research on disinformation attacks remains nascent, with a predominant focus on social media (Shu et al. 2020; Freelon and Wells 2020).

When disinformation attacks target urban critical infrastructure, the collective decisions of individuals can significantly affect the system's operation. The real examples in recent years, such as the hacked power systems (Raman et al. 2020; Peng et al. 2020) and the suspicious packages on airplanes (Jamalzadeh et al. 2022), prove that disinformation attacks on urban infrastructure can be highly harmful and pose significant risks. Concerning disinformation on the road network, we recall the 2020 experiment Google Maps Hacks by a German artist, who used 99 smartphones to trick Google Maps into detecting fake traffic jams, exposing vulnerabilities in digital navigation systems. This classic case demonstrates that cyberattacks do not always involve directly hacking systems; instead, they can exploit digital algorithms to create real-world disruptions. Additionally, other cases, such as Fort Lee lane closure scandal and Students Hack Waze demonstrate that disinformation attacks can manipulate users' driving routing to cause inefficient traffic management, unnecessary detours and increased congestion. Evidence suggests that while the evolution of next-generation transportation systems brings numerous advantages, it paradoxically amplifies the vulnerability of road TCPS to disinformation attacks. Consequently, some scholars have begun to make tentative explorations into this emerging issue. With false traffic alerts, road signs and store discount notifications, Waniek et al. (2021) set up two disinformation attack scenarios on drivers and discussed the impact of these attacks on streets. Spana and Du (2022) revealed the optimal perturbation for the information sent to vehicles in a coordinated routing scheme to alleviate traffic congestion. Jamalzadeh et al. (2024) assessed the impacts of weaponized disinformation on multi-commodity critical infrastructure networks. Alvisi et al. (2024) demonstrates the potential for traffic congestion induced by disinformation through adversarial attacks targeting traffic map providers. Similarly, Khameneh, Barker, and Ramirez-Marquez (2025) investigates the effects of disinformation on service disruptions in transportation operations, highlighting its sub-

stantial impact on the reliability of transport infrastructure. Furthermore, Jamalzadeh et al. (2025) introduces an approach to address the uncertainties arising during disinformation campaigns, which pose significant risks to infrastructure networks. The preceding remark highlights the susceptibility of road networks to information-based attacks, yet research on the vulnerability of road TCPS to disinformation attacks remains significantly limited.

The vulnerability of a system pertains to its susceptibility to performance degradation experienced following perturbations, whether from deliberate attacks or unintentional damage (Jenelius and Mattsson 2015). This concept captures the extent to which the system's functionality is compromised when faced with adverse conditions or malicious activities (Gu et al. 2020; Hassan et al. 2022). Currently, the conventional research on road network vulnerability primarily centers on the physical layer, with simulation often depicting interruptions or failures through targeted attacks on specific network elements, such as nodes or links. Prior research has extensively examined the impacts of diverse disruptive events on road network vulnerability, encompassing extreme weather conditions, natural disasters, accidents, terrorist activities, and operational incidents (Singh et al. 2018; Calvert and Snelder 2018; Cats and Jenelius 2018). However, contemporary discourse regarding emerging cybersecurity threats targeting road networks remains inadequately comprehensive. The target selection in vulnerability assessment typically involves ranking the importance of nodes or links (Jenelius, Petersen, and Mattsson 2006; Zeng 2020; Chen et al. 2024). Additionally, the attack modes exhibit diverse characteristics, ranging from random to strategically deliberate patterns, and can be classified as either static or dynamic in nature (Liu, Shi, and Tan 2021; Vivek and Conner 2022). At present, popular vulnerability assessment methods primarily rely on approaches such as topology analysis, data-driven models, scenario planning, system dynamics and optimization techniques (Jenelius and Mattsson 2015; Gu et al. 2020; Hassan et al. 2022). In summary, traditional studies on road network vulnerability have heavily relied on node or link removal methods. Such methods fundamentally change the network's physical structure, proving detrimental to its sustainable development.

Meanwhile, there is a growing research trend focusing on the vulnerability of road transportation networks to cyberattacks (Serdar, Koç, and Al-Ghamdi 2022). Existing studies (Feng et al. 2018; Lin et al. 2018; Yang et al. 2021; Wang et al. 2021; Sun, Luo, and Chen 2023; Zhu et al. 2023) investigate the issue by integrating fields like cybersecurity, information science, data protection, and advanced machine learning methodologies, including deep learning techniques. While historical cyberattacks on road transportation systems have primarily targeted computational infrastructure, emerging disinformation attacks represent a distinct threat paradigm that exploits cognitive biases through strategically manipulated information. As a novel research topic, vulnerability assessment of road TCPS to such attacks has not yet been explored.

Real-world cases have demonstrated the tangible impact of disinformation on urban traffic conditions. With the increasing prevalence of IoT devices in modern transportation systems, the likelihood of such disinformation attacks ranges from medium to high. Figure 1 serves as a visual representation of the motivation behind this study. The TCPS-based road network features two interconnected layers: (a) the physical layer with intersections, segments, and sensors like signal lights and cameras; and (b) the cyber layer including communication systems, navigation apps, and digital infrastructure. A bidirectional flow of data and information between these two layers forms a closed-loop system. In such a road network, it is assumed that drivers rely on information provided by navigation apps to make driving decisions, and they remain

unaware of any information manipulation or perturbation in the system. As shown in Figure 1(c), the reference driving time for an origin-destination (OD) provided by Google Maps is 19 minutes in a normal case, while it displays 14 minutes after the app is hacked. Drivers with similar travel demands may be drawn to choose this route, potentially leading to traffic overload. In this study, we refine the attack target from the path to the individual segment, to more accurately assess road network vulnerability against disinformation attacks. During the attacks, the road network's physical topology does not change, but the information provision from the cyber layer does. The contributions of this study are summarized as follows:

(1) A novel disinformation attack mode is proposed, involving the simulation of hacking navigation apps by modifying link cost information on critical segments to manipulate drivers' routing decisions.
(2) Multiple disinformation attack strategies, including target identification strategies and target attack strategies, are devised to assess the TCPS-based road network's vulnerability in various scenarios.
(3) A case study on a large-scale urban road network is implemented, and counter-intuitive results are obtained.
(4) Differences between emerging disinformation attacks and traditional physical attacks are discussed from various perspectives.

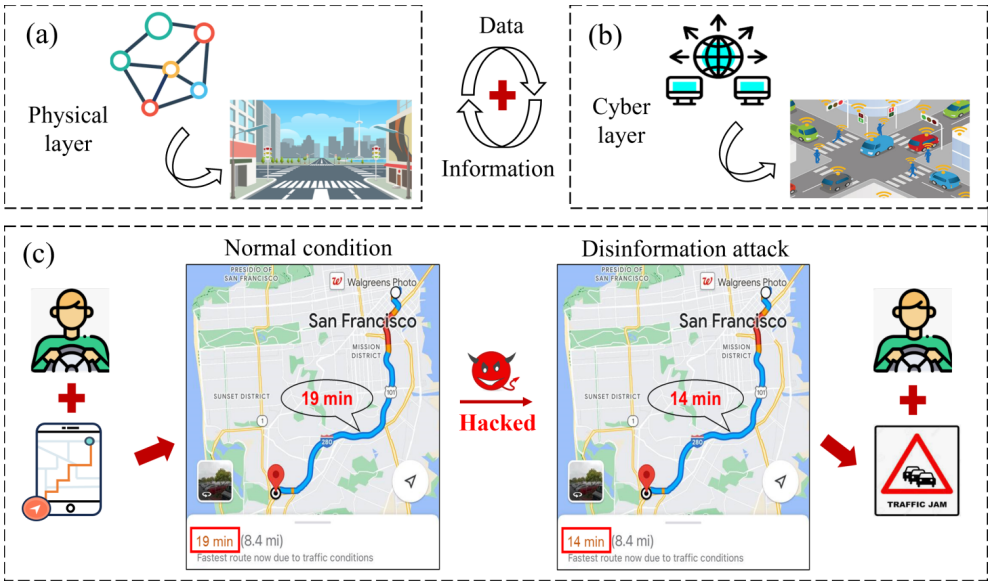


Figure 1. The conceptual representation of disinformation attack on road TCPS.

2. Methodology

The overall research framework of this study is shown in Figure 2. Using the open-source datasets, traffic flow assignment and weighted complex road network modeling are conducted. Subsequently, multiple target identification strategies and target attack strategies are proposed to conduct disinformation attacks. The secondary traffic flow assignment is executed, and the road network performance is evaluated both before and after attacks. Finally, the vulnerability of the TCPS-based road network to

disinformation attacks is quantitatively assessed. Detailed descriptions of the specific algorithms and models involved are provided below.

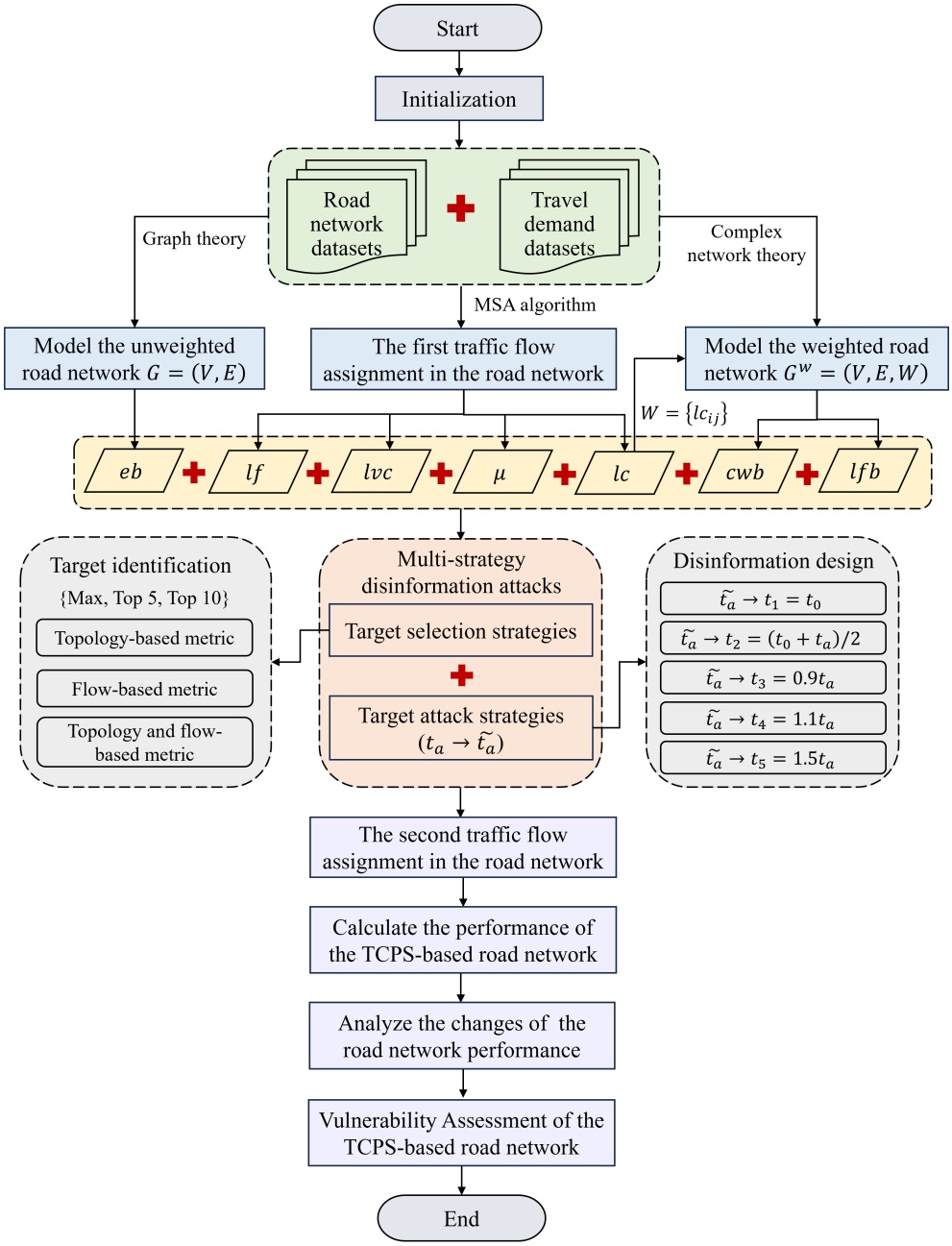


Figure 2. The overall research framework.

2.1. *Traffic flow assignment*

In reality, travelers usually choose routes that best serve their self-interests, typically seeking to minimize travel-related costs like travel time or expenses. Therefore, this study employs the Wardrop Equilibrium (User Equilibrium, UE) (Wardrop 1952) for traffic assignment based on two key assumptions: the shortest path principle and the

assumption that drivers have perfect knowledge of link travel time. Consequently, every route used between an origin (O) and destination (D) has equal and minimal travel time. In the UE-based traffic assignment framework, multiple shortest paths refer to the set of paths with the same minimum travel cost between OD pairs under equilibrium conditions. Here, Beckmann mathematical planning model (Beckmann, McGuire, and Winsten 1956) is adopted for traffic flow assignment and the mathematical expression is as follows:

$$\min \quad Z(X) = \sum_a \int_0^{x_a} t_a(\omega) d(\omega) \tag{1}$$

$$\text{s.t.} \quad \sum_p f_p^{rs} = q_{rs}, \quad \forall_{r,s} \tag{2}$$

$$f_p^{rs} \geq 0, \quad \forall_{p,r,s} \tag{3}$$

$$x_a = \sum_r \sum_s \sum_p f_p^{rs} \delta_{pa}^{rs}, \quad \forall_a \tag{4}$$

Equation (1) shows the minimum value of the objective function and (2) - (4) are the constraint conditions of the model. Among them, (2) represents that the total traffic flow $\sum_p f_p^{rs}$ between origin r and destination s equals the overall OD flow q_{rs}, reflecting flow conservation. Equation (3) indicates that the flow f_p^{rs} on path p meets the non-negative constraint, while (4) defines the link flow x_a as the sum of the path flows for all (r, s) pairs through link a, using the link-path correlation variable δ_{pa}^{rs}. δ_{pa}^{rs} is binary (0-1), indicating 1 when path p includes link a and 0 otherwise.

As shown in Equation (5), the impedance c_p^{rs} of path p is the total of link impedance along it, with $t_a(x_a)$ as the link performance function. The Bureau of Public Roads (BPR) function for travel time calculation is shown in Equation (6). It involves link cost t_a, free-flow travel time t_0, traffic volume x_a and traffic capacity c_a, with the calibration parameters α and β.

$$c_p^{rs} = \sum_a t_a(x_a) \delta_{a,p}^{rs} \quad \forall_{p,r,s} \tag{5}$$

$$t_a = t_0(1 + \alpha(\frac{x_a}{c_a})^\beta) \tag{6}$$

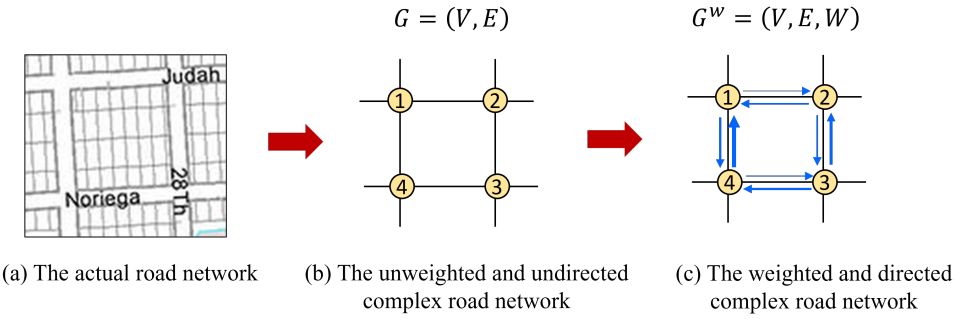
In this study, the MSA (Method of Successive Average) algorithm (Sheffi and Powell 1982; Boyles, Lownes, and Unnikrishnan 2023) is used to solve the Beckmann function model. As one of the link-based algorithms, MSA gradually approaches equilibrium by continuously iterating the assigned flow of each road segment. AEC (average excess cost) is chosen as the convergence criterion. The iteration will stop when the maximum number of iterations is 100 or the AEC reaches the value of 1e-3.

We further validate the robustness of the numerical analysis in the traffic flow assignment model. The assignment process considers multiple parameters, including link attributes, OD multipliers, the BPR function, and turn penalties. To enhance the model's reliability, we integrate network data and commuting datasets from San Francisco. Using software tools such as TransCAD and AequilibraE, we perform network parameter calibration and traffic flow assignment. Furthermore, we validate the

resulting travel times and average speeds against open-source datasets from Waze and TomTom, ensuring the technical accuracy and reliability of the results. This comprehensive calibration and validation process demonstrates the robustness of the parameters utilized in the traffic flow assignment. The detailed implementation of this work is discussed in our previously published study (Xu et al. 2024).

2.2. *Weighted complex road network modeling*

Currently, existing studies have demonstrated that urban road networks are inherently complex systems, integrating structural, functional, and dynamic elements that evolve continuously (Zeng 2020; Ando et al. 2021; Xu et al. 2022; Guo, Zhao, and Gao 2024). The structural complexity primarily arises from the network topology, which is characterized by multiple hierarchical levels, high connectivity, and redundancy. Functional complexity is reflected in the mixed traffic flow, highly fluctuating traffic demand, and the diverse transportation service objectives. Dynamic complexity pertains to the nonlinear effects of traffic congestion, human rerouting decisions, as well as the influences of weather and time. Therefore, based on graph theory and complex network theory, we build a complex road network model $G = (V, E)$, where $V = \{v_i, i = 1, 2, \ldots, N\}$ is the node set and $E = \{e_{ij}, i, j = 1, 2, \ldots, N, i \neq j\}$ is the link set. The nodes and links represent the intersections and road segments in the actual road network, respectively. If two nodes $\langle i, j \rangle$ are adjacent, there is a connected link and $e_{ij} = 1$, otherwise $e_{ij} = 0$.



(a) The actual road network (b) The unweighted and undirected complex road network (c) The weighted and directed complex road network

Figure 3. The schematic representation of weighted complex road network modeling.

A weighted and directed urban complex road network model $G^w = (V, E, W)$ can be constructed based on the link cost results derived from the UE assignment. $W = \{w_{ij}, i, j = 1, 2, \ldots, N, i \neq j\}$ is the weight set. Figure 3 illustrates the construction principle of G and G^w, where (a) is the actual road network, (b) is the unweighted and undirected complex road network G and (c) is the weighted and directed complex road network G^w. The weight w_{ij} is the link cost, and a thicker representation of a link signifies a longer travel time associated with that link.

2.3. *Disinformation attack strategies*

2.3.1. Target identification strategies

Target identification is the first critical step in disinformation attack strategies. This part involves meticulously determining the road network's most critical links that could be potential focal points for an attack. It emphasizes pinpointing links with

the most significant impact on the overall network. Uniquely, we propose a multi-faceted approach to evaluating link importance, considering both structural position and functional usage through metrics based on three perspectives: topology-based, flow-based and a combined topology-flow approach.

(1) Topology-based metric

We utilize edge betweenness centrality (eb) in complex networks to effectively measure the influence of edges across the entire network (Freeman 1977; Kermanshah and Derrible 2017). This metric focuses on determining how often an edge serves as a critical link on the shortest path between two nodes, as delineated in Equation (7). eb_k is the betweenness centrality of the edge k, $\sigma(i,j)$ is the total number of the shortest paths from node i to node j, and $\sigma(i,j|k)$ is the number of the shortest paths from node i to node j that pass through edge k.

$$eb_k = \sum_{i,j,k \in V} \frac{\sigma(i,j|k)}{\sigma(i,j)} \tag{7}$$

(2) Flow-based metric

Traffic congestion is influenced by factors such as speed limits, traffic density, actual travel speeds, traffic volume, and traffic capacity (Loder et al. 2019). Based on the UE assignment, we can derive key metrics such as link flow (lf), link cost (lc) and link volume over capacity ratio (v/c ratio, denoted as lvc). Besides, the total travel time (TTT) of the road network can be obtained using Equation (8). We can further obtain μ, the partial derivative of TTT to link flow, as shown in Equation (9). μ_k represents the marginal cost of travel on link k. That includes both the direct effect on the link itself and the indirect effect on other users who are delayed due to the increased congestion on the link k. A higher μ means that the link is more critical, and the network performance is more sensitive to the flow changes on this link. Based on traffic flow data, we can employ four metrics, namely lf, lc, lvc and μ, to identify the most critical target.

$$TTT = \sum_k x_k t_k(x_k) \tag{8}$$

$$\mu_k = \frac{\partial TTT}{\partial x_k} = t_k(x_k) + x_k \frac{\partial t_k(x_k)}{\partial x_k} \tag{9}$$

(3) Topology and flow-based metric

Combining eb with G^w, we introduce the metric of link cost weighted betweenness (cwb). As shown in Equation (10), cwb_k is the link cost weighted betweenness of the edge k, $\sigma^w(i,j)$ is the total number of the shortest (i,j)-paths in G^w, and $\sigma^w(i,j|k)$ is the number of those shortest paths passing through the edge k in G^w.

$$cwb_k = \sum_{i,j,k \in V} \frac{\sigma^w(i,j|k)}{\sigma^w(i,j)} \tag{10}$$

Additionally, we propose a link flow-based betweenness (lfb) measure based on eb

and lf, which combines the topological structure of the network with the participation rate of the segment. The participation rate of a segment is defined as the proportion of link flow relative to the total OD demand within the road network. The lfb of link k can be calculated using Equation (11), where eb_k and $\widehat{lf}_k$ represent the eb and $\widehat{lf}$ of link k respectively. $\widehat{lf}$ can be obtained by the max-min normalization of lf, and z is the total OD demand of the road network.

$$lfb_k = \frac{\widehat{lf}_k * eb_k}{z} \tag{11}$$

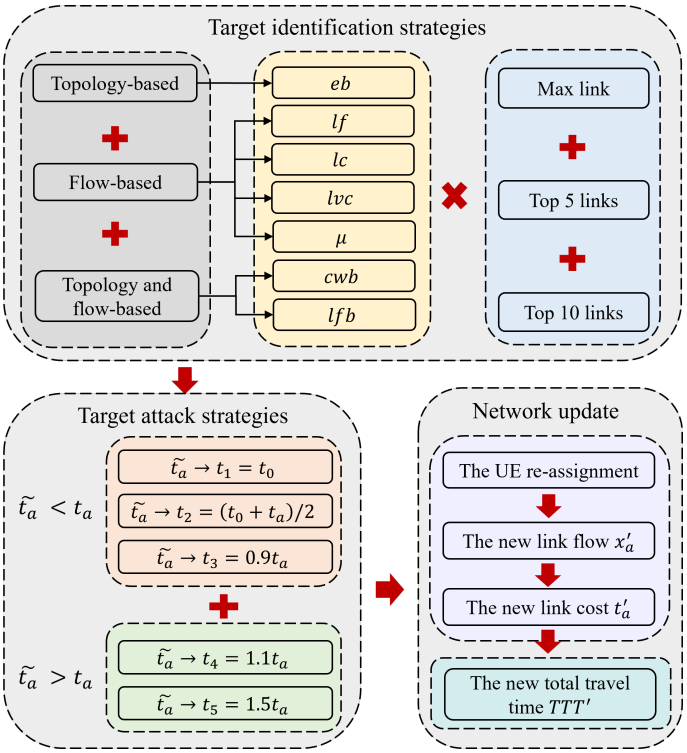


Figure 4. The multi-strategy disinformation attacks on the road network.

As shown in Figure 4, we put forward seven metrics, namely eb, lf, lc, lvc, μ, cwb, and lfb, to measure link importance from three perspectives. Based on these metrics, all the links in the network are ranked in descending order. Subsequently, the link information corresponding to the maximum value (max or the top 1), the top 5, and the top 10 in each metric's ranking can be extracted. By identifying these critical links using their unique IDs, the potential targets for disinformation attacks can be systematically pinpointed.

2.3.2. Target attack strategies

Based on target identification strategies, we next delve into the disinformation design and multimode target attack strategies. In the scenario of this study, link travel time is a crucial factor influencing the drivers' routing. Therefore, the disinformation fed to drivers mainly focuses on the information regarding link cost. It is important to note

that this study focuses on the profound effects of subtle information perturbations at the cyber layer on the entire road TCPS. In addition, the disinformation attacks in our study are assumed to be short-lived and imperceptible. We further assume that traffic management systems have not detected these perturbations in time and that drivers are unaware of the changes. Analogous to adversarial attacks on traffic signal control systems (Qu, Tang, and Ma 2023), information-based attacks on communication systems and navigation apps are equally feasible. Given the high incidence of road congestion, we choose to implement disinformation attacks during peak urban commuting hours.

Guided by UE principles, the disinformation attacks can be executed based on the following inference. For a given link, if its link impedance after attacks is lower than its original value t_a, this link has become more accessible to traverse in the next assignment, potentially leading to increased traffic. Conversely, if the impedance of an attacked link rises above t_a, it will attract less traffic flow. According to the BPR function in Equation (6), the minimum link impedance under the free-flow condition is t_0. Meanwhile, navigation apps typically provide an estimate of the maximum travel time, which is often set at 1.5 times the reference value to create a buffer for variability. It needs to be noted that this value is based on heuristic rules commonly observed in real-world navigation systems. Given this, we alter the impedance information of selected links to a specific constant $\widetilde{t_a}$ to simulate the hacking of navigation apps. Then, the driver's perception and cognition of travel time will change in their routing. Eventually, the road network stabilizes into a new equilibrium state after the secondary UE assignment. Thus, the new x'_a, t'_a and TTT' can also be obtained. What needs illustration is that t'_a is still obtained by the BPR function using x'_a, including those attacked links' cost.

Specifically, we design five unique information perturbations to simulate disinformation attacks by modifying the impedance t_a of the targeted links. Five functions, denoted as $Attack_i(l)$ where $i = 1, ..., 5$ and l is a link ID, are defined in Equation (12), and $t_1, t_2, \ldots, t_5$ represent the modified impedance values. These functions return the modified impedance $\widetilde{t_a}$ based on the original impedance t_a. The impedance t_a and the free-flow time t_0 of a specific link l are denoted as $t_a(l)$ and $t_0(l)$, respectively. Figure 4 also illustrates the degree of attack on the targeted link under various information perturbations. On the one hand, the link impedance $\widetilde{t_a}$ is modified to t_1, t_2 and t_3 respectively, which is lower than the original value t_a. On the other hand, the impedance $\widetilde{t_a}$ is modified to t_4 and t_5 respectively, which is larger than t_a. The detailed target attack strategies are described in Algorithm 1.

$$
\begin{aligned}
t_1 &= Attack_1(l) = t_0(l) \\
t_2 &= Attack_2(l) = (t_0(l) + t_a(l))/2 \\
t_3 &= Attack_3(l) = 0.9t_a(l) \\
t_4 &= Attack_4(l) = 1.1t_a(l) \\
t_5 &= Attack_5(l) = 1.5t_a(l)
\end{aligned}
\tag{12}
$$

Overall, the multi-strategy disinformation attacks involve the establishment of seven distinct metrics, the application of three varying targeted link counts, and the deployment of five unique information designs. There is a total of $7 \times 3 \times 5 = 105$ simulation experiments, and each combination of these parameters represents a distinct attack mode.

Algorithm 1 Target attack strategies

Require: G is the road network, **eb** is a list of key-value pairs, with each key being a link ID l and each value the eb of that link. **lf**, **lc**, **lvc**, $\boldsymbol{\mu}$, **cwb** and **lfb** are defined similarly.

Ensure: The UE re-assignment results, including x'_a, t'_a and TTT'.

```
for each metric m in {eb, lf, lc, lvc, μ, cwb, lfb} do
    Sort the elements in m in descending order based on m.values.
    Max ← Extract the target link based on the max in the ranking.
    Top5 ← Extract the target links based on the top 5 in the ranking.
    Top10 ← Extract the target links based on the top 10 in the ranking.
    for i ← 1, ..., 5 do
        for strategy s ∈ {Max, Top5, Top10} do
            for each link l in s do
                In G, set link l's impedance t_a(l) to t̃_a = Attack_i(l)
            end for
            Record the traffic flow re-assignment results using UE.
        end for
    end for
end for
```

2.4. *Road network performance and vulnerability metrics*

The overall service level of a road network is primarily evaluated through its performance metrics. In this study, the road network's overall OD demand does not change before or after the attacks. Considering the travel expenses and preferences of the driver, the road network's performance Q is defined as the total travel time (TTT) (Ganin et al. 2017; Angelelli et al. 2021; Qu, Tang, and Ma 2023), as expressed in Equation (13). This approach captures both the direct costs and time efficiency of travel while aligning with the drivers' decision-making criteria. It offers a holistic and user-centric metric to evaluate the network's effectiveness.

$$Q = TTT = \sum_k x_k t_k(x_k) \tag{13}$$

The vulnerability (V) of the road network is characterized by the extent to which network performance is altered in response to attacks. This conceptualization captures the network's sensitivity to disinformation-induced disruptions. V is calculated as Equation (14), where $Q_0 = TTT_0$ represents the normal network performance, and $Q' = TTT'$ denotes the performance after attacks. As a complex system, the road network exhibits heterogeneous responses to diverse attacks, reflecting differing levels of vulnerability. A higher value of V for a specific attack mode indicates greater system vulnerability to that particular attack typology.

$$
\begin{aligned}
V &= \frac{\Delta Q}{Q} \times 100\% \\
&= \frac{Q' - Q_0}{Q_0} \times 100\% \\
&= \frac{TTT' - TTT_0}{TTT_0} \times 100\%
\end{aligned} \tag{14}
$$

3. Study area and datasets

3.1. *Study area*

San Francisco Road Network (SFRN) is selected as the subject for the case study. San Francisco, a metropolitan city situated on the central coast of California, USA, is renowned as the commercial, financial, and cultural hub of Northern California. The road network in San Francisco is well-developed and comprehensive, featuring multiple road types for diverse traffic needs. However, San Francisco faces significant traffic congestion challenges. According to the INRIX 2022 Global Traffic Scorecard, congestion in SFRN is ranked as the 7th worst in the United States and 15th globally.

3.2. *Datasets*

The datasets utilized in this study comprise the road network and travel demand. The underlying road network topology is extracted from OpenStreetMap. The node file contains general intersections (Node_type = 0) and centroids (Node_type = 1). The link file includes key road segment information such as Capacity (vehicle/hour), Length (km), Free_speed (km/h), Lanes, and Link_type. The values of Link_type, ranging from 1 to 5, are associated with motorway, trunk, primary, secondary and tertiary, respectively. Besides these general road segments, other links are connectors. For San Francisco, the free speed of connectors is set at 5 km/h (Xu et al. 2024). There are 4,986 nodes (including 194 centroids) and 18,002 links (including 8,418 general road segments) in SFRN.

The original urban travel demand datasets are derived from the Longitudinal Employer-Household Dynamics Origin-Destination Employment Statistics (LODES), published by the U.S. Census Bureau. These data represent average daily urban commuting patterns for the workforce during peak hours. The average daily OD distribution between blocks of San Francisco in 2019 is derived from the total number of jobs in the LODES7 datasets and visualized in Figure 5. Based on a unified dataset from our previous research (Xu et al. 2024), the corresponding link attributes and OD multiplier for San Francisco can be obtained. The total number of OD pairs in the SFRN is 25,657, with a total travel demand of 299,276. To estimate the number of vehicles, the travel demand is multiplied by a coefficient of 0.6, reflecting a more realistic representation of vehicular traffic (Xu et al. 2024). Subsequently, the adjusted travel demand datasets are utilized as input for UE assignment.

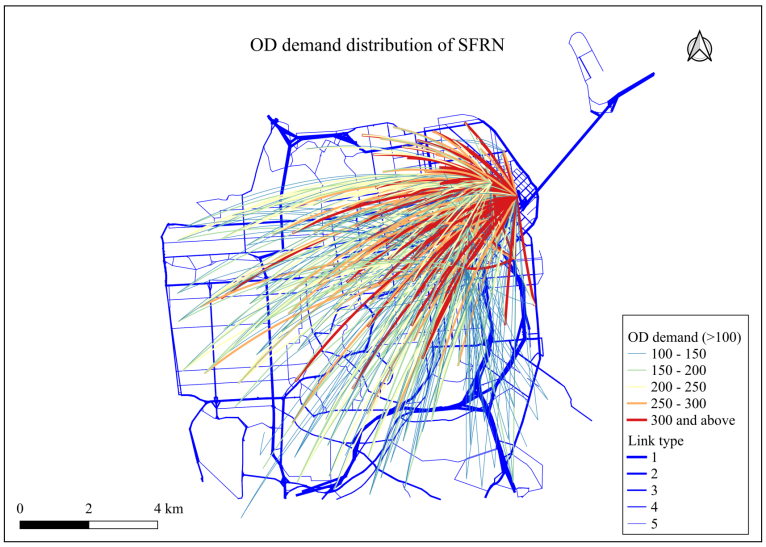


Figure 5. The OD distribution of SFRN.

4. Numerical results analysis

4.1. *Traffic assignment and link importance ranking under normal conditions*

For SFRN, the calibration parameters in the BPR function are set to $\alpha = 0.5$ and $\beta = 2$ accoring to our previous research (Xu et al. 2024). Using the UE assignment model and the available datasets, the traffic flow assignment under normal conditions can be derived. Here, we use *lvc* to visualize the first assignment results, which is shown in Figure 6. Additionally, TTT_0 is 40,040.53 h and the Vehicle Kilometers Travelled ($VKMT$) amounts to 1,090,200.43 km. Thus, the average speed can be determined as $VKMT/TTT_0 = 27.23$ km/h.

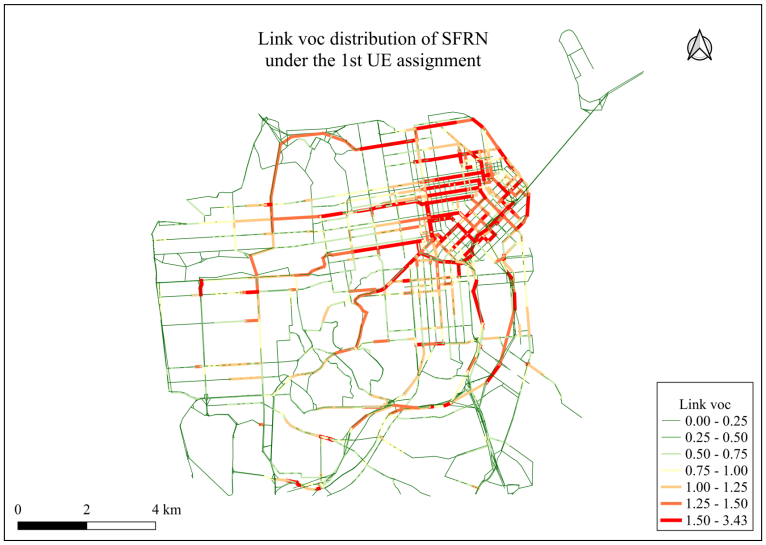
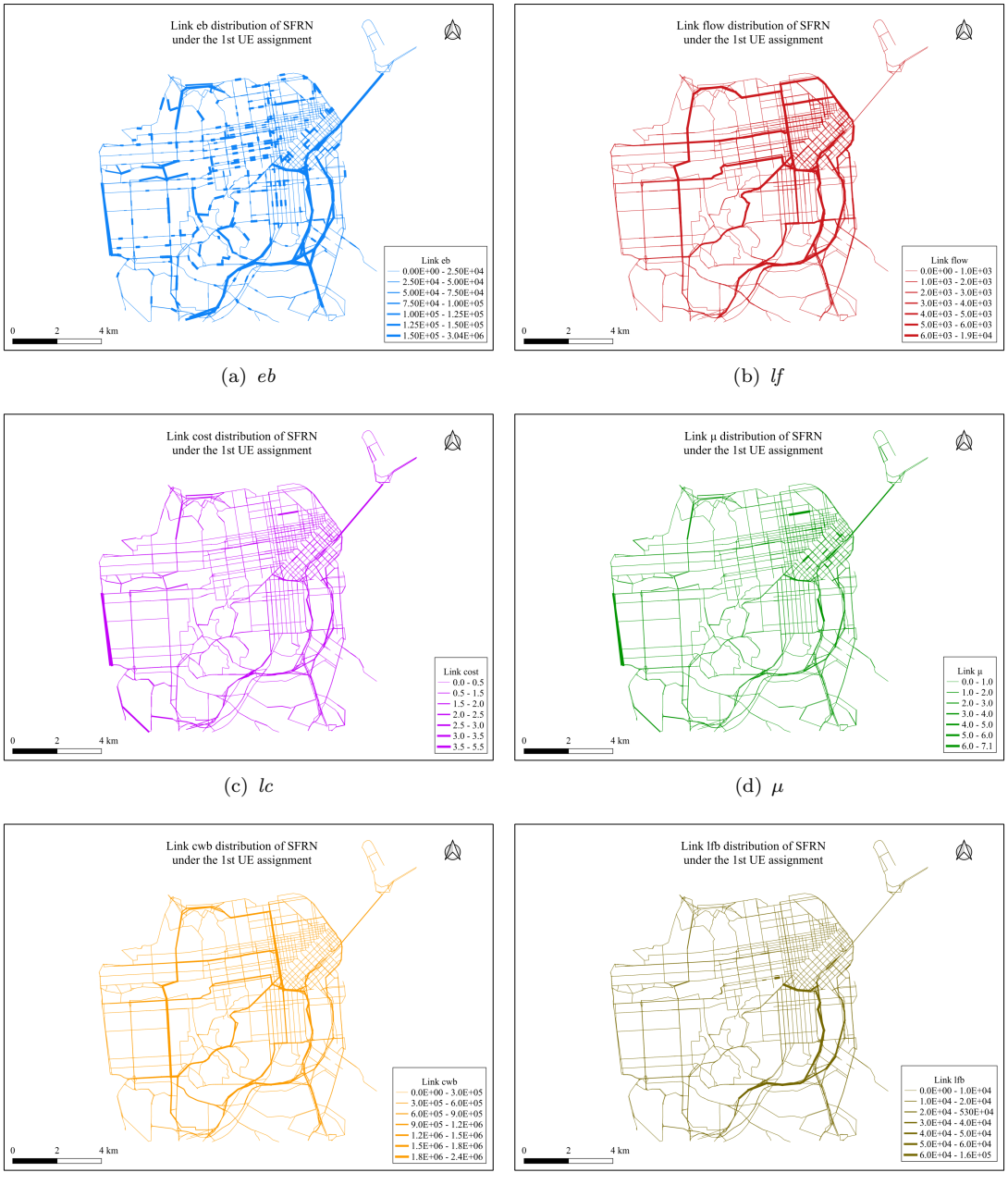


Figure 6. The first UE assignment results visualized with *lvc*.

Based on the methodology outlined in Section 2.3.1, the eb, lf, lc, μ, cwb and lfb distributions of SFRN can be obtained, as visualized in Figure 7. Despite variations in link ranking across different metrics, the visual similarities between lc and μ suggest a close alignment in how these metrics evaluate and rank network links. Subsequently, disinformation attacks are conducted based on these link ranking results.



(a) eb (b) lf

(c) lc (d) μ

(e) cwb (f) lfb

Figure 7. The first UE assignment results visualized with eb, lf, lc, μ, cwb and lfb.

4.2. *Performance measurement of the SFRN under disinformation attacks*

After the disinformation attack, we can finally acquire the updated network performance Q'. Figure 8 presents the calculation results of Q' under multi-strategy disinformation attacks. The subfigures 8(a), 8(b), and 8(c) correspond to the TTT distributions for three different attack counts (max, top 5 and top 10), respectively. Each subfigure uses a consistent legend to facilitate clear comparison.

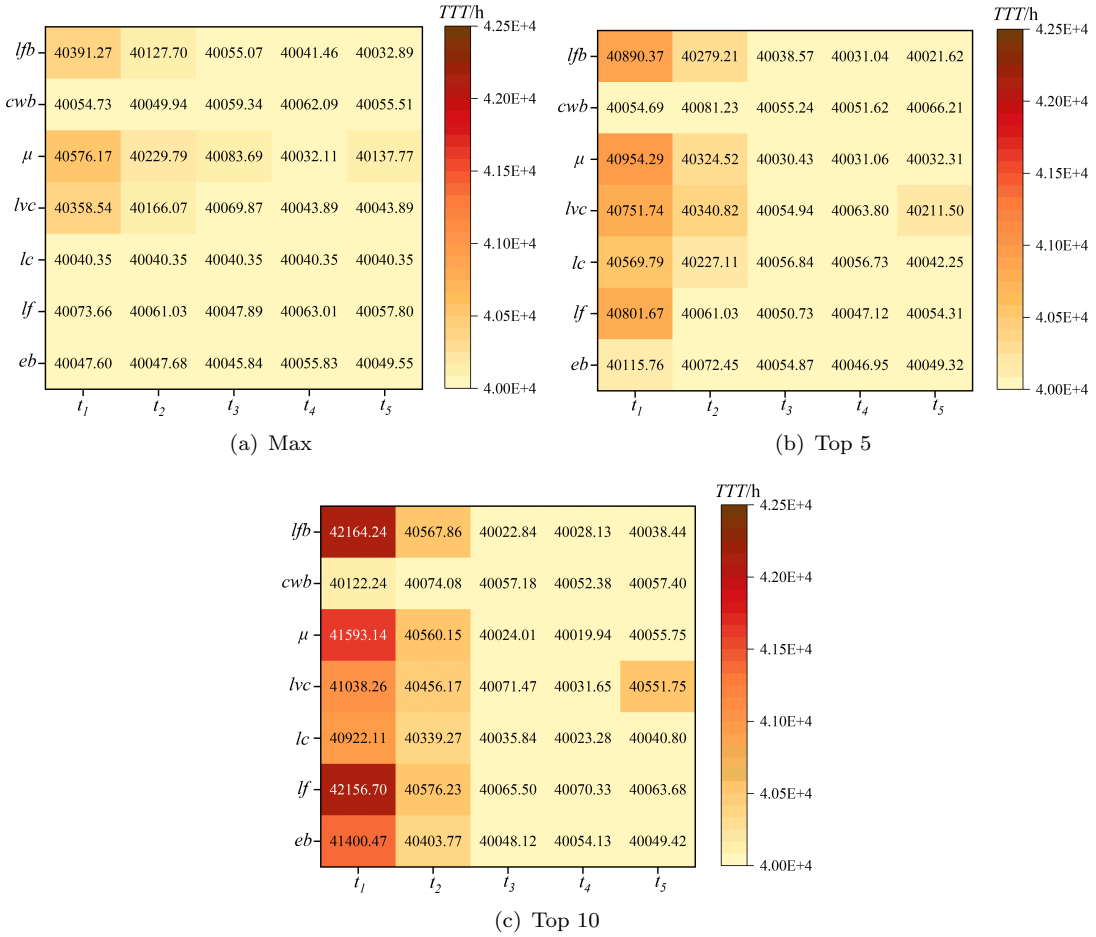


Figure 8. The calculation results of Q' under different disinformation attacks.

In a side-by-side comparison, the values of Q' progressively increase as the number of attacked links rises, indicated by the figures' darkening color. There seems to be a positive correlation between the number of attacked links and TTT. Meanwhile, vertical comparisons reveal that the variations in Q' at t_1 and t_2 are markedly more pronounced than those observed at t_3, t_4 and t_5. Specifically, when the link impedance is maliciously modified to free-flow time (t_1), Q' reaches its maximum value of 42,164.24, which is 5.3 % higher than the original value of 40,040.53. The road network is more vulnerable to disinformation attacks when the link impedance is reduced. Furthermore, $lvc_{\max}$, $\mu_{\max}$ and $lfb_{\max}$ in subfigure 8(a) show greater sensitivity to changes in link cost. In contrast, cwb_{top5} and cwb_{top10} in subfigures 8(b) and 8(c) exhibit the least sensitivity. μ, lfb, and lf demonstrably exert greater impacts on Q' relative to other metrics. The formula of Q' emphasizes the importance of link flow (x_a) as an

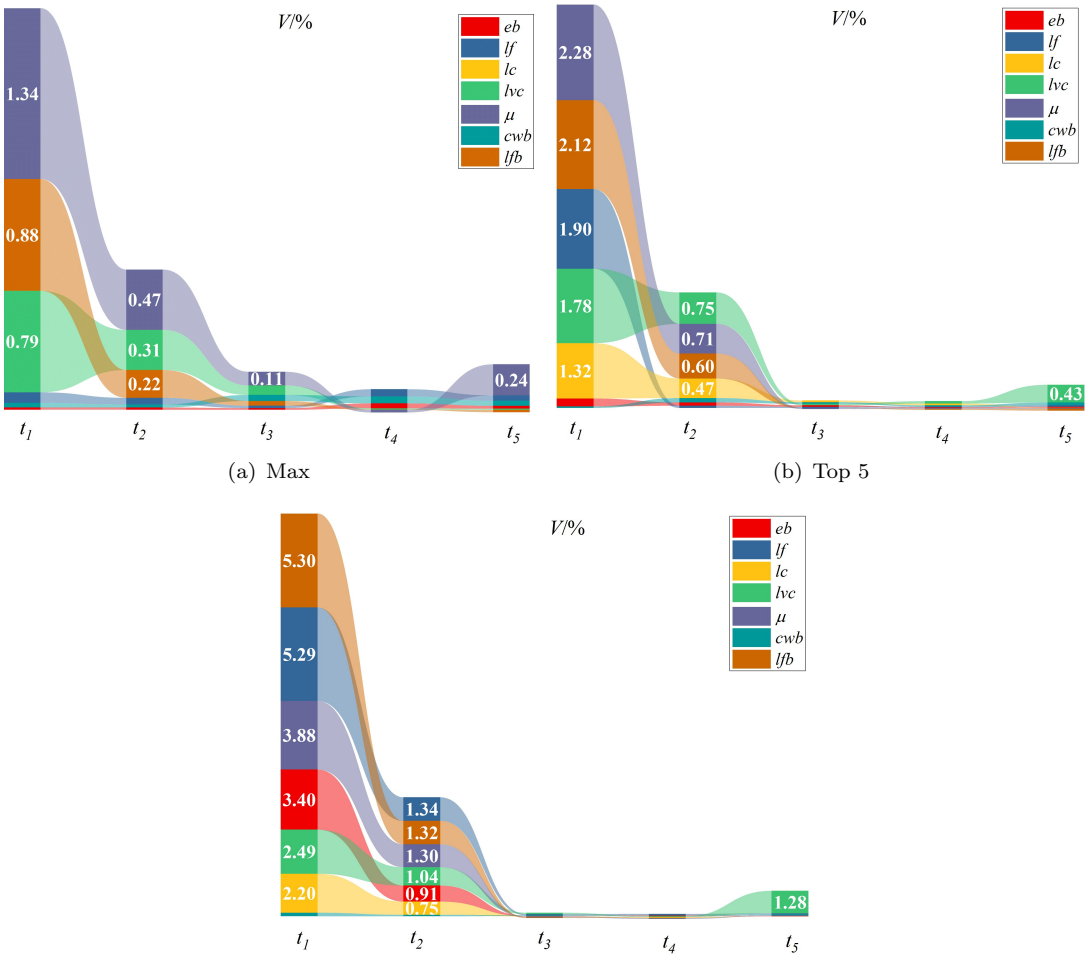
essential independent variable.

Moreover, despite the road network showing highly similar distributions under lc and μ after the initial assignment, the impact of μ on Q' in the max, top 5, and top 10 attack modes is more pronounced than that of lc. Additionally, when the top 5 and top 10 links are targeted across seven metrics, the minimum values of Q' predominantly occur at $t_3 = 0.9t_a$ or $t_4 = 1.1t_a$. This pattern holds for all metrics except for the maximum value of Q' under the cwb_{max} attack, which uniquely peaks at t_4. The observed phenomena suggest that for the link importance metrics eb, lf, lc, lvc, μ and lfb, a smaller variation in $|t_a - \widetilde{t_a}|$ (specifically, the absolute value of the difference between t_a and $\widetilde{t_a}$) results in lesser impacts on TTT.

4.3. *Vulnerability assessment of the SFRN under disinformation attacks*

Figure 9 displays the computed results of V for multi-strategy disinformation attacks, ranging from t_1 to t_5. In the max-attack mode, the metrics μ, lfb and lvc hold the most significant influence on V, contributing 1.338 %, 0.876 %, and 0.795 % respectively. Specifically, in the top 5-attack mode, the indicators μ, lfb, and lf emerge as the most significant, while in the top 10-attack mode, this order shifts to lfb, lf, and μ. This adjustment underscores the dynamic nature of their impacts in different operational contexts. The peak value of V observed in lfb_{top10} stands at 5.304 %. Generally, when μ and lfb are chosen as the link metrics, the resulting values of V are typically higher compared to those derived from other indicators.

As shown in Table 1, the average value $\overline{V}$ is computed as the mean of V. For the scenarios t_1 and t_2, $\overline{V}$ holds the top and second positions respectively. Overall, t_5 is third in its effect on V, while V records minimal values in scenarios t_3 and t_4. The findings validate our initial assumption that lowering the link cost of a specific road segment increases its attractiveness to drivers, which can potentially worsen congestion and heighten the road network's vulnerability. Besides, for t_1, t_2 and t_5, the increase in the number of attacked links, transitioning from max to top 10, leads to a significant rise in TTT' and a more crowded road network. Furthermore, $V > 0$ indicates higher total travel costs, which is detrimental to the overall efficiency of the road system. Given that Table 1 shows predominantly positive values for V across most scenarios, this highlights the road network's susceptibility to attacks. The occurrence of $V < 0$ can be explained by understanding that an increase in t_a leads to significant congestion on certain links. This, in turn, encourages drivers to avoid these congested areas, resulting in a reduction of TTT after UE assignment. It's essential to note that the highest absolute value noted in the occasional negative instances of V is only 0.051%. The above analysis underscores the increased vulnerability of the entire network to disinformation attacks, especially when t_a is modified to match the free-flow cost.



(a) Max (b) Top 5

(c) Top 10

Figure 9. The calculation results of V under multiple disinformation attacks.

Table 1. The calculation results of $\overline{V}$ under various disinformation attacks.

$\overline{V}$	Max	Top 5	Top 10
t_1	0.449%	1.376%	3.252%
t_2	0.157%	0.394%	0.962%
t_3	0.043%	0.021%	0.015%
t_4	0.020%	0.016%	-0.001%
t_5	0.048%	0.070%	0.205%

5. Discussions

5.1. *Economic loss caused by disinformation attacks*

While disinformation attacks may currently represent a few isolated incidents, the growing dependence on navigation technologies and traffic data suggests that such attacks could become increasingly frequent in the future. Quantifying the impact of disinformation attacks in terms of economic losses offers valuable insights for policymakers and urban planners, enabling them to better understand the potential eco-

nomic consequences and prioritize effective mitigation strategies. Therefore, building on the results of disinformation attacks obtained in this study, we further delve into the economic repercussions of citywide traffic congestion induced by such attacks.

Urban traffic is crucial for economic growth, but congestion incurs substantial direct economic costs (Arnott and Small 1994; Jayasooriya and Bandara 2017), particularly in terms of lost productivity. The INRIX 2022 Global Traffic Scorecard report reveals that in San Francisco, traffic congestion caused an average delay of 97 hours and a loss of $1,642 per driver, totaling $2.6 billion in citywide costs. Next, we will compare this study's data with INRIX statistics for an in-depth examination. Given an average of 250 working days per year, the calculation of the average annual lost time per driver involves dividing the total daily lost hours by the number of drivers and then multiplying by 250. This approach enables us to precisely quantify the ratio of annual hours lost to disinformation attacks versus normal delays. Besides, the vulnerability assessment has uncovered a critical insight: altering the link cost from t_a to t_1 exerts the greatest effect on the road network's vulnerability. Here, we focus on examining the delay and economic loss resulting from the t_1 attack, as detailed in Table 2. ΔTTT denotes the lost hours, and V signifies the network vulnerability. γ represents the delay experienced by each driver following the attacks. $\delta = \gamma/97 \times 100\,\%$ quantifies the fraction of each driver's delay during t_1 attack relative to INRIX data. The INRIX indicates that congestion costs San Francisco $2.6 billion. Multiplying this by the factor δ allows for an estimation of the productivity loss L.

Table 2. The lost hours and economic losses of SFRN under the disinformation attacks of t_1.

Attack mode	Link metrics	ΔTTT /hours	V	γ/hours	δ	L/million USD
Max	*eb*	7.25	0.018%	0.010	0.010%	0.270
	lf	33.31	0.083%	0.046	0.048%	1.243
	lc	0.00	0.000%	0.000	0.000%	0.000
	lvc	318.19	0.795%	0.443	0.457%	11.874
	μ	535.82	1.338%	0.746	0.769%	19.996
	cwb	14.38	0.036%	0.020	0.021%	0.536
	lfb	350.91	0.876%	0.489	0.504%	13.095
Top 5	*eb*	75.41	0.188%	0.105	0.108%	2.814
	lf	761.32	1.901%	1.060	1.093%	28.411
	lc	529.44	1.322%	0.737	0.760%	19.758
	lvc	711.38	1.777%	0.990	1.021%	26.547
	μ	913.94	2.283%	1.272	1.312%	34.106
	cwb	14.34	0.036%	0.020	0.021%	0.535
	lfb	850.02	2.123%	1.183	1.220%	31.721
Top 10	*eb*	1,360.11	3.397%	1.894	1.952%	50.757
	lf	2,116.35	5.286%	2.946	3.038%	78.978
	lc	881.76	2.202%	1.228	1.266%	32.905
	lvc	997.91	2.492%	1.389	1.432%	37.240
	μ	1,552.78	3.878%	2.162	2.229%	57.947
	cwb	81.89	0.205%	0.114	0.118%	3.056
	lfb	2,123.89	5.304%	2.957	3.048%	79.259

Here, the metric μ is selected as an instance to demonstrate. The vulnerability under the max, top 5 and top 10 attacks is 1.338%, 2.283% and 3.878%, respectively. Each driver will experience yearly delays of 0.769%, 1.312% and 2.229%, leading to economic losses for the city of $20.00 million, $34.11 million and $57.95 million, respectively. Meanwhile, only 0.012%, 0.059%, and 0.119% of general links are subjected to attacks. According to Table 2, in the most severe scenario, targeting only 0.12% of links can result in 2.96 hours of yearly delay per driver, leading to an economic loss of $79.26 million for the city. The above analysis demonstrates that disinformation

attacks targeting a small number of critical links can significantly amplify the road network's vulnerability, resulting in substantial economic losses for the city. Consequently, implementing effective defensive strategies is crucial to mitigate the adverse impacts of disinformation attacks and ensure urban transportation system resilience.

5.2. *Emerging disinformation attacks vs traditional physical attacks*

As discussed in the Introduction, existing studies on road network vulnerability have primarily focused on traditional physical attack methods, specifically the removal of nodes or links. In contrast, this study offers fresh insights into disinformation attacks targeting large-scale urban road networks. Here, we examine the distinctions between the two types of attacks through four key aspects:

(i) *Research motivation.* In the current era of information explosion, emerging disinformation attacks on road TCPS by deliberately spreading misleading information to manipulate drivers psychologically, highlighting vulnerabilities in intelligent transportation systems. Compared with traditional physical attacks, the disinformation attack is a new form of information-based cyberattack.

(ii) *Attack target.* Disinformation attacks aim to influence drivers' cognition and behaviors, where route choices are influenced by misinformation on navigation apps. In contrast, traditional physical attacks focus on disrupting the physical topology of the road network, impacting network performance by removing nodes or links. The physical topology remains unchanged throughout the disinformation attacks, while it undergoes substantial changes during the physical attacks.

(iii) *Target identification.* A new metric (μ, the partial derivative of TTT to x_a) is proposed to identify attack targets, supplementing conventional indexes used in traditional physical attacks. μ encompasses both direct travel time (direct effect) and marginal congestion effect (indirect effect), carrying significant implications for road network optimization and pricing mechanisms. This study reveals that metric μ significantly impacts road network vulnerability, indicating that it is a more effective tool for identifying targets than other commonly used metrics.

(iv) *Attack strategy.* In contrast to traditional physical attacks that simulate massive disruptions like natural disasters, epidemics, accidents or terrorist activities, the disinformation attacks in this study involve minor modifications to link cost information, rendering them less obvious and harder to detect through intuition, i.e. disinformation attacks are implemented quickly in a short period of time. And the truth is that such seemingly insignificant disinformation has a detrimental effect on the road system and urban economy.

In short, emerging disinformation attacks described in this study are novel in the aforementioned aspects when compared to traditional physical attacks. Given the rapid progress and sustainable development of road TCPS, how vulnerable large-scale urban road networks are to disinformation attacks is a specific field of research that requires immediate concern.

5.3. *Policy implications*

This study highlights the significant negative impacts of disinformation attacks, particularly on drivers' route choices. First, false information can create unsafe driving conditions by leading drivers to take incorrect detours or encounter unexpected con-

gestion, requiring heightened vigilance and caution. Second, disinformation increases travel time and fuel consumption, resulting in higher economic costs, especially in densely populated urban areas. Lastly, frequent disinformation attacks may erode trust in navigation tools, prompting drivers to seek alternative, potentially less efficient methods. To mitigate these risks, several management and prevention strategies are proposed:

(i) *Driver awareness and education.* Raising driver awareness is a crucial first step in mitigating the impact of disinformation attacks. Educating drivers about the nature of these attacks and their potential influence on navigation tools can help them recognize and respond to anomalies. Awareness campaigns can equip drivers with the knowledge to identify anomalies or biases in routing recommendations. Besides, promoting the use of multiple navigation platforms for cross-verification can enhance the reliability of routing decisions.

(ii) *Enhancements to traffic management systems.* Traffic management systems should harness advanced technologies, such as AI-driven algorithms, to detect suspicious traffic patterns and validate data through multiple sources, including GPS signals, roadside sensors, and camera feeds. Verified real-time traffic updates can be delivered to drivers via dynamic information signs or broadcast systems, circumventing potentially compromised digital platforms. Additionally, developing robust emergency routing strategies is crucial for effectively redirecting traffic during an attack, ensuring minimal disruption to the transportation network.

(iii) *Security improvements for navigation platforms.* Enhancing the cybersecurity of navigation platforms is crucial for mitigating vulnerabilities to disinformation attacks. This involves implementing strong encryption protocols to secure data transmission between navigation systems and vehicles, preventing signal manipulation. Moreover, establishing redundant communication channels can further strengthen system resilience, ensuring continuity and reliability even in the face of potential attacks.

(iv) *Policy and regulatory interventions.* Policy and regulatory frameworks are essential in mitigating the risks of disinformation attacks. Implementing stringent regulations for traffic data collection, processing, and sharing is critical to standardizing and securing the ecosystem. Mandating regular security audits of traffic management and navigation systems can help identify and address vulnerabilities proactively. Furthermore, enforcing strict legal penalties can deter malicious activities, ensuring accountability and compliance.

By integrating these strategies, the transportation ecosystem can enhance its resilience to disinformation attacks, safeguarding network functionality and promoting more secure and reliable urban mobility systems.

6. Conclusions and future works

In this study, we propose a novel disinformation attack framework for large-scale road networks, designed to manipulate drivers' cognition and behavior by altering the displayed link cost information on navigation applications. To evaluate the vulnerability of urban road networks, multiple disinformation attack strategies are developed and analyzed. The proposed framework is applied to the San Francisco road network, leading to the following main conclusions:

(i) Several key metrics (*eb*, *lf*, *lc*, *lvc*, μ, *cwb*, and *lfb*) are introduced to identify target links for disinformation attacks. In particular, μ, the partial derivative of total travel time with respect to link flow, is innovatively proposed, considering the marginal cost. These metrics result in different rankings of links, with the notable exception of a strong correlation observed between the results of μ and *lc*.

(ii) The road network's performance deteriorates proportionally with the increase in the number of attacked links. The network performance suffers more with malicious link cost changes at t_1 and t_2 compared to t_3, t_4 and t_5. Moreover, vulnerability assessment findings reveal that μ and *lfb* have more significant impacts compared to other metrics. In attack modes t_1, t_2 and t_5, the road network's congestion increases with the rising number of attacked links. The network's highest vulnerability occurs when t_a is modified as t_1, denoting free-flow cost.

(iii) Overall, the road network demonstrates greater vulnerability when the link cost is modified to a smaller value. In the most severe scenario, targeting merely 0.12 % of the links could add 2.96 hours of delay per driver annually and cost the city $79.26 million. Compared to traditional physical attacks, the road network's vulnerability to emerging disinformation attacks is more sophisticated and nuanced, underscoring the need for increased vigilance and proactive measures.

This work reveals how drivers' thoughts and actions are manipulated in TCPS-based urban road networks, and it indicates that emerging disinformation attacks on a few critical links greatly disrupt road network performance. To ensure the security, reliability, and sustainability of TCPS, it is crucial to focus more on cyberattacks, particularly within vital urban road infrastructures. This study offers a fresh perspective and valuable references in this regard. However, it has certain limitations. Firstly, the disinformation attacks proposed in this study are applicable to other urban road networks, prompting future research to explore variations among different cities confronting such threats. Secondly, the UE model has certain limitations in capturing the temporal dynamics of traffic flow and network behavior, and dynamic traffic assignment(DTA) model has the potential to further enrich analysis in future research. Thirdly, the study employs multi-strategy static and greedy attacks by simultaneously targeting specific links. The next step will be to investigate the impacts of dynamic disinformation attacks on urban road network vulnerability. Lastly, this study delves into the vulnerability of road infrastructure under diverse disinformation attacks, with future endeavors aimed at exploring detection methods and resilience enhancement strategies against such cyberattacks. These strategies encompass encryption, secure communication protocols, data verification technologies, and other measures designed to augment the road systems' capacity to withstand disinformation attacks, thereby bolstering their reliability and resilience.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 72304126), grants from the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. PolyU/25209221 & PolyU/15206322), and a grant from the Research Institute for Sustainable Urban Development (RISUD) at the Hong Kong Polytechnic University (Project No. P0038288), and a grant from the

Otto Poon Charitable Foundation Smart Cities Research Institute (SCRI) at the Hong Kong Polytechnic University (Project No. P0043552). The authors would like to thank the editors and reviewers for their valuable comments and suggestions.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Alvisi, Lorenzo, John Bianchi, Sara Tibidò, and Maria Vittoria Zucca. 2024. "Weaponizing Disinformation Against Critical Infrastructures." .

Ando, Hiroe, Michael Bell, Fumitaka Kurauchi, K. I. Wong, and Kam-Fung Cheung. 2021. "Connectivity Evaluation of Large Road Network by Capacity-Weighted Eigenvector Centrality Analysis." *Transportmetrica A: Transport Science* 17 (4): 648–674. https://doi.org/10.1080/23249935.2020.1804480.

Angelelli, E., V. Morandi, M. Savelsbergh, and M.G. Speranza. 2021. "System Optimal Routing of Traffic Flows with User Constraints Using Linear Programming." *European Journal of Operational Research* 293 (3): 863–879. https://doi.org/10.1016/j.ejor.2020.12.043.

Arnott, Richard, and Kenneth Small. 1994. "The Economics of Traffic Congestion." *American Scientist* 82 (5): 446–455.

Beckmann, Martin J., Charles B. McGuire, and Christopher B. Winsten. 1956. *Studies in the Economics of Transportation*. Cowles Commission for Research in Economics.

Boyles, Stephen D., Nicholas E. Lownes, and Avinash Unnikrishnan. 2023. *Transportation Network Analysis*. version 0.91 ed., Vol. I.

Calvert, Simeon C., and Maaike Snelder. 2018. "A Methodology for Road Traffic Resilience Analysis and Review of Related Concepts." *Transportmetrica A: Transport Science* 14 (1-2): 130–154. https://doi.org/10.1080/23249935.2017.1363315.

Cats, Oded, and Erik Jenelius. 2018. "Beyond a Complete Failure: The Impact of Partial Capacity Degradation on Public Transport Network Vulnerability." *Transportmetrica B: Transport Dynamics* 6 (2): 77–96. https://doi.org/10.1080/21680566.2016.1267596.

Chen, Zhichao, Changjiang Zheng, Tongtong Tao, and Yanyan Wang. 2024. "Reliability Analysis of Urban Road Traffic Network under Targeted Attack Strategies Considering Traffic Congestion Diffusion." *Reliability Engineering & System Safety* 248: 110171. https://doi.org/10.1016/j.ress.2024.110171.

Chow, Andy H.F., W.Y. Szeto, David Z.W. Wang, and S. Travis Waller. 2015. "Quantitative Approaches to Resilience in Transport Networks." *Transportmetrica A: Transport Science* 11 (9): 751–753. https://doi.org/10.1080/23249935.2015.1087231.

Deka, Lipika, Sakib M. Khan, Mashrur Chowdhury, and Nick Ayres. 2018. "Transportation Cyber-Physical System and Its Importance for Future Mobility." In *Transportation Cyber-Physical Systems*, 1–20. Elsevier.

Dey, Kakan, Ryan Fries, and Shofiq Ahmed. 2018. "Future of Transportation Cyber-Physical Systems – Smart Cities/Regions." In *Transportation Cyber-Physical Systems*, 267–307. Elsevier.

Feng, Yiheng, Shihong Huang, Qi Alfred Chen, Henry X. Liu, and Z. Morley Mao. 2018. "Vulnerability of Traffic Control System Under Cyberattacks with Falsified Data." *Transportation Research Record* 2672 (1): 1–11. https://doi.org/10.1177/0361198118756885.

Freelon, Deen, and Chris Wells. 2020. "Disinformation as Political Communication." *Political Communication* 37 (2): 145–156. https://doi.org/10.1080/10584609.2020.1723755.

Freeman, Linton C. 1977. "A Set of Measures of Centrality Based on Betweenness." *Sociometry* 40 (1): 35. https://doi.org/10.2307/3033543.

Ganin, Alexander A., Maksim Kitsak, Dayton Marchese, Jeffrey M. Keisler, Thomas Seager, and Igor Linkov. 2017. "Resilience and Efficiency in Transportation Networks." *Science Advances* 3 (12): e1701079. https://doi.org/10.1126/sciadv.1701079.

Gu, Yu, Xiao Fu, Zhiyuan Liu, Xiangdong Xu, and Anthony Chen. 2020. "Performance of Transportation Network under Perturbations: Reliability, Vulnerability, and Resilience." *Transportation Research Part E: Logistics and Transportation Review* 133: 101809. https://doi.org/10.1016/j.tre.2019.11.003.

Guo, Mingxue, Tingting Zhao, and Ziyou Gao. 2024. "Pre-Disaster Resource Allocation Based on Network Topology and Flow Features." *Transportmetrica A: Transport Science* 1–24. https://doi.org/10.1080/23249935.2024.2344631.

Hassan, Sitti Asmah, Hamizah Amalina Amlan, Nor Eliza Alias, Mariyana Aida Ab-Kadir, and Nur Sabahiah Abdul Sukor. 2022. "Vulnerability of Road Transportation Networks under Natural Hazards: A Bibliometric Analysis and Review." *International Journal of Disaster Risk Reduction* 83: 103393. https://doi.org/10.1016/j.ijdrr.2022.103393.

Jamalzadeh, Saeed, Kash Barker, Andrés D. González, and Sridhar Radhakrishnan. 2022. "Protecting Infrastructure Performance from Disinformation Attacks." *Scientific Reports* 12 (1): 12707. https://doi.org/10.1038/s41598-022-16832-w.

Jamalzadeh, Saeed, Kash Barker, Andrés D. González, Sridhar Radhakrishnan, and Elena Bessarabova. 2025. "Infrastructure Network Protection under Uncertain Impacts of Weaponized Disinformation Campaigns." *Physica A: Statistical Mechanics and its Applications* 660: 130365. https://doi.org/10.1016/j.physa.2025.130365.

Jamalzadeh, Saeed, Lily Mettenbrink, Kash Barker, Andrés D. González, Sridhar Radhakrishnan, Jonas Johansson, and Elena Bessarabova. 2024. "Weaponized Disinformation Spread and Its Impact on Multi-Commodity Critical Infrastructure Networks." *Reliability Engineering & System Safety* 243: 109819. https://doi.org/10.1016/j.ress.2023.109819.

Jayasooriya, S.A.C.S., and Y.M.M.S. Bandara. 2017. "Measuring the Economic Costs of Traffic Congestion." In *2017 Moratuwa Engineering Research Conference (MERCon)*, Moratuwa, Sri Lanka, May, 141–146. IEEE.

Jenelius, Erik, and Lars-Göran Mattsson. 2015. "Road Network Vulnerability Analysis: Conceptualization, Implementation and Application." *Computers, Environment and Urban Systems* 49: 136–147. https://doi.org/10.1016/j.compenvurbsys.2014.02.003.

Jenelius, Erik, Tom Petersen, and Lars-Göran Mattsson. 2006. "Importance and Exposure in Road Network Vulnerability Analysis." *Transportation Research Part A: Policy and Practice* 40 (7): 537–560. https://doi.org/10.1016/j.tra.2005.11.003.

Kermanshah, Amirhassan, and Sybil Derrible. 2017. "Robustness of Road Systems to Extreme Flooding: Using Elements of GIS, Travel Demand, and Network Science." *Natural Hazards* 86 (1): 151–164. https://doi.org/10.1007/s11069-016-2678-1.

Khameneh, Ramin Talebi, Kash Barker, and Jose Emmanuel Ramirez-Marquez. 2025. "A Hybrid Machine Learning and Simulation Framework for Modeling and Understanding Disinformation-Induced Disruptions in Public Transit Systems." *Reliability Engineering & System Safety* 255: 110656. https://doi.org/10.1016/j.ress.2024.110656.

Lin, Jie, Wei Yu, Nan Zhang, Xinyu Yang, and Linqiang Ge. 2018. "Data Integrity Attacks Against Dynamic Route Guidance in Transportation-Based Cyber-Physical Systems: Modeling, Analysis, and Defense." *IEEE Transactions on Vehicular Technology* 67 (9): 8738–8753. https://doi.org/10.1109/TVT.2018.2845744.

Liu, Jie, Zhenwu Shi, and Xianyu Tan. 2021. "Measuring the Dynamic Evolution of Road Network Vulnerability to Floods: A Case Study of Wuhan, China." *Travel Behaviour and Society* 23: 13–24. https://doi.org/10.1016/j.tbs.2020.10.009.

Loder, Allister, Lukas Ambühl, Monica Menendez, and Kay W. Axhausen. 2019. "Understanding Traffic Capacity of Urban Networks." *Scientific Reports* 9 (1): 16283. https://doi.org/10.1038/s41598-019-51539-5.

Pathak, Archita, Rohini K. Srihari, and Nihit Natu. 2021. "Disinformation: Analysis and Identification." *Computational and Mathematical Organization Theory* 27 (3): 357–375. https://doi.org/10.1007/s10588-021-09336-x.

Peng, Rui, Hui Xiao, Jianjun Guo, and Chen Lin. 2020. "Defending a Parallel System against a Strategic Attacker with Redundancy, Protection and Disinformation." *Reliability Engineering & System Safety* 193: 106651. https://doi.org/10.1016/j.ress.2019.106651.

Pundir, Amit, Sanjeev Singh, Manish Kumar, Anil Bafila, and Geetika J. Saxena. 2022. "Cyber-Physical Systems Enabled Transport Networks in Smart Cities: Challenges and Enabling Technologies of the New Mobility Era." *IEEE Access* 10: 16350–16364. https://doi.org/10.1109/ACCESS.2022.3147323.

Qu, Ao, Yihong Tang, and Wei Ma. 2023. "Adversarial Attacks on Deep Reinforcement Learning-based Traffic Signal Control Systems with Colluding Vehicles." *ACM Transactions on Intelligent Systems and Technology* 14 (6): 1–22. https://doi.org/10.1145/3625236.

Raman, Gururaghav, Bedoor AlShebli, Marcin Waniek, Talal Rahwan, and Jimmy Chih-Hsien Peng. 2020. "How Weaponizing Disinformation Can Bring down a City's Power Grid." *PLOS ONE* 15 (8): e0236517. https://doi.org/10.1371/journal.pone.0236517.

Serdar, Mohammad Zaher, Muammer Koç, and Sami G. Al-Ghamdi. 2022. "Urban Transportation Networks Resilience: Indicators, Disturbances, and Assessment Methods." *Sustainable Cities and Society* 76: 103452. https://doi.org/10.1016/j.scs.2021.103452.

Sheffi, Yosef, and Warren B. Powell. 1982. "An Algorithm for the Equilibrium Assignment Problem with Random Link Times." *Networks* 12 (2): 191–207. https://doi.org/10.1002/net.3230120209.

Shu, Kai, Amrita Bhattacharjee, Faisal Alatawi, Tahora H. Nazer, Kaize Ding, Mansooreh Karami, and Huan Liu. 2020. "Combating Disinformation in a Social Media Age." *WIREs Data Mining and Knowledge Discovery* 10 (6): e1385. https://doi.org/10.1002/widm.1385.

Singh, Prasoon, Vinay Shankar Prasad Sinha, Ayushi Vijhani, and Neha Pahuja. 2018. "Vulnerability Assessment of Urban Road Network from Urban Flood." *International Journal of Disaster Risk Reduction* 28: 237–250. https://doi.org/10.1016/j.ijdrr.2018.03.017.

Spana, Stephen, and Lili Du. 2022. "Optimal Information Perturbation for Traffic Congestion Mitigation: Gaussian Process Regression and Optimization." *Transportation Research Part C: Emerging Technologies* 138: 103647. https://doi.org/10.1016/j.trc.2022.103647.

Sun, Ruixiao, Qi Luo, and Yuche Chen. 2023. "Online Transportation Network Cyber-Attack Detection Based on Stationary Sensor Data." *Transportation Research Part C: Emerging Technologies* 149: 104058. https://doi.org/10.1016/j.trc.2023.104058.

Vagan, Terziyan, Mariia Golovianko, and Svitlana Gryshko. 2018. "Industry 4.0 Intelligence under Attack : From Cognitive Hack to Data Poisoning." In *Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures*, Vol. 51 of *NATO Science for Peace and Security Series - D: Information and Communication Security*, 110–125. IOS Press.

Vivek, Skanda, and Hannah Conner. 2022. "Urban Road Network Vulnerability and Resilience to Large-Scale Attacks." *Safety Science* 147: 105575. https://doi.org/10.1016/j.ssci.2021.105575.

Wang, Yue, Esha Sarkar, Wenqing Li, Michail Maniatakos, and Saif Eddin Jabari. 2021. "Stop-and-Go: Exploring Backdoor Attacks on Deep Reinforcement Learning-Based Traffic Congestion Control Systems." *IEEE Transactions on Information Forensics and Security* 16: 4772–4787. https://doi.org/10.1109/TIFS.2021.3114024.

Waniek, Marcin, Gururaghav Raman, Bedoor AlShebli, Jimmy Chih-Hsien Peng, and Talal Rahwan. 2021. "Traffic Networks Are Vulnerable to Disinformation Attacks." *Scientific Reports* 11 (1): 5329. https://doi.org/10.1038/s41598-021-84291-w.

Wardrop, J G. 1952. "Road Paper. Some Theoretical Aspects of Road Traffic Research." *Proceedings of the Institution of Civil Engineers* 1 (3): 325–362. https://doi.org/10.1680/ipeds.1952.11259.

Xu, Dongwei, Yongdong Wang, Peng Peng, Lei Lin, and Yi Liu. 2022. "The Evaluation of the Urban Road Network Based on the Complex Network." *IEEE Intelligent Transportation Systems Magazine* 14 (3): 200–211. https://doi.org/10.1109/MITS.2021.3049351.

Xu, Xiaotong, Zhenjie Zheng, Zijian Hu, Kairui Feng, and Wei Ma. 2024. "A Unified Dataset for the City-Scale Traffic Assignment Model in 20 U.S. Cities." *Scientific Data* 11 (1): 325. https://doi.org/10.1038/s41597-024-03149-8.

Yang, Jingjing, Yuchun Guo, Yishuai Chen, Yongxiang Zhao, and Naipeng Li. 2021. "Vulnerability Analysis of Road Network under Information Pollution Attacks in VANET." In *2021 IEEE Global Communications Conference (GLOBECOM)*, Madrid, Spain, December, 1–6. IEEE.

Zeng, Yu. 2020. "Evaluation of Node Importance and Invulnerability Simulation Analysis in Complex Load- Network." *Neurocomputing* 416: 158–164. https://doi.org/10.1016/j.neucom.2019.05.092.

Zhu, Lyuyi, Kairui Feng, Ziyuan Pu, and Wei Ma. 2023. "Adversarial Diffusion Attacks on Graph-based Traffic Prediction Models." *IEEE Internet of Things Journal* 1–1. https://doi.org/10.1109/JIOT.2023.3290401.

Zhu, Lyuyi, Ao Qu, and Wei Ma. 2023. "Cybersecurity Challenges in AI-enabled Smart Transportation Systems." In *Handbook on Artificial Intelligence and Transport*, Chapters, 567–595. Edward Elgar Publishing.