Research Reports on Computer Science
https://ojs.wiserpub.com/index.php/RRCS/

Research Article

Network Design for Silent Link User Equilibrium

Xu Chen[1], Zeguan Wu[2], Xuan Di[1*]

[1]Department of Civil Engineering and Engineering Mechanics, Columbia University, New York, USA
[2]Department of Industrial Engineering and Operations Research, Columbia University, New York, USA
E-mail: sharon.di@columbia.edu

Received: 2 January 2022; **Revised:** 22 February 2023; **Accepted:** 2 March 2023

Abstract: Connected vehicles (CVs) are anticipated to improve road safety and travel efficiency in a transportation system. However, the deployment of CV technologies in transportation networks can lead to privacy issues, as the communication among CVs can expose vehicles' location information. To address this issue, we introduce a privacy protection method named "silent link" to transportation networks and propose a silent link user equilibrium (SLUE) framework to study the impact of privacy protection countermeasures on network flow. A theoretical analysis regarding existence and uniqueness conditions of SLUE is provided. The proposed SLUE facilitates privacy-oriented network design to achieve optimal levels of privacy for CVs. Accordingly, a bi-level network optimization problem is formulated for the design of silent links in transportation networks. Numerical examples are demonstrated using the Braess and Sioux Falls networks.

***Keywords*:** location privacy, silent link, user equilibrium

1. Introduction

Connected vehicle (CV) technologies are developed in an intelligent transportation system for safer and more efficient driving environments. By exchanging basic safety messages (BSM) via dedicated wireless communication [1] with other vehicles (i.e., vehicle-to-vehicle) or with roadside infrastructure (i.e., vehicle-to-infrastructure), drivers can become aware of road conditions that they may not have been able to foresee. The shared information and data among CVs can help policymakers and road planners analyze how to make roads safer and less congested. This, in turn, can provide travelers with a better experience and reduce total travel cost in a mobility ecosystem. The great potentials of CV technologies have enabled a variety of safety-critical applications [2, 3].

Despite the fact that the BSM contains no personal identifying information, the standard-based open communication among vehicles may significantly compromise travelers' location privacy [4, 5]. This is because the packet of data in safety applications contains information related to vehicles' state and predicted paths, which could be used by a malicious global listener to reconstruct privacy-sensitive information, such as complete commuting routes of target drivers. Therefore, it is crucial for stakeholders such as government agencies, automakers, and researchers to develop effective privacy protection techniques prior to a large-scale deployment of CVs in transportation networks. To do so, it is essential to thoroughly investigate traveler decisions, anti-tracking countermeasures, and network equilibrium to develop effective privacy protection techniques.

DOI: https://doi.org/10.37256/rrcs.2120232295

1.1 *Related works*

Privacy protection techniques have been widely applied in transportation modeling [6-10] and real-time tracking [11]. Protection methods include anonymity [12] spatial and temporal cloaking [13] and dummy information [14, 15]. However, these methods may lead to over-protecting issues and reduce the efficiency of communication via BSMs among CVs. Mix-zone [16, 17] and SLOW (silence at low speeds) [4] are proposed to achieve a balance between efficient communication and message eavesdropping. To avoid exchanging messages among vehicles with invariant pseudonym identifications (i.e., public-key certificate), the mix-zone approach designates physical areas; e.g., a highway resting area, where all vehicles collectively enter radio silence and change their pseudonym identifications. This paper applies the silence mechanism to transportation networks where each link can be treated as a silent area. Location privacy is protected when vehicles navigate silent links and vehicles make their route choice (i.e., the next-go-to link) on nodes. Existing work mainly focuses on empirical studies to understand the impact of privacy protection methods. Buttyán et al. [4] investigates the relationship between vehicles' speed and the length of silent period. Xin et al. [18] leverages the simulation data to study how silent strategies dynamically affect the real-time travel flow regarding different network topologies and demand levels. Chow [19] discusses the privacy of providers and users when they share the data [20, 21] in transportation services. Some studies utilize optimization tools to facilitate the design of anti-tracking countermeasures. Freudiger et al. [22] uses vehicle-tracked probability as a privacy metric and studies the optimization on mix-zone deployment. Sun et al. [23] investigates how to minimize the total number of mixed zones. This work incorporates location privacy into network user equilibrium and measures the network-level privacy of CVs. Having such an integrated modeling framework is of great importance as it helps understand the impact of anti-tracking countermeasures and investigate the interaction between these measures and network equilibrium through game-theoretic analysis.

1.2 *Contributions of our paper*

Our contributions include:

(1) We introduce a privacy protection technique (i.e., silent links) into transportation networks and formulate the privacy-based network user equilibrium, i.e., silent link user equilibrium (SLUE), which in turn facilitates the optimal design of privacy protection.

(2) We provide a theoretical analysis of solution properties for SLUE. Numerical examples on the Braess and Sioux Falls networks are demonstrated to understand the equilibrium.

(3) We investigate a bi-level network design problem regarding the deployment of silent links. On the upper level, road links are chosen to be silent or not in order to minimize the probability of all vehicles being tracked. On the lower level, SLUEs are formulated according to the choice of silent links.

The rest of the paper is organized as follows: In Section 2, we introduce a privacy metric to transportation networks and formulate SLUE. Theoretical analysis is provided. In Section 3, we propose a bi-level network design problem based on SLUE. Section 4 concludes the paper.

2. SLUE

In this section, we utilize traffic flow to model the privacy metric of silent links in network user equilibrium [24, 25]. Notations are demonstrated first: A road network is denoted as $\mathcal{G} = \{\mathcal{N}, \mathcal{L}\}$. $\mathcal{N}$ is the node set and $\mathcal{L}$ is the link set. x_{ij}^d represents the traffic flow on link (i, j) with destination d, $d \in \mathcal{N}_D$. $\mathcal{N}_D$ is the destination set.

2.1 *Link-node based formulation*

In a single-mode network, traffic flow on each link is divided into several destination-based flows under the link-node formulation. A destination-based scalar named potential π_i^d, $i \in \mathcal{N}$, $d \in \mathcal{N}_D$ is also defined for each node in the network, which represents the minimum travel cost from the node to the destination. At user equilibrium, we have the following nonlinear complementarity conditions:

[user equilibrium (UE) – nonlinear complementarity problem (NCP)]

$$0 \le [\pi_j^d + c_{ij} - \pi_i^d] \perp x_{ij}^d \ge 0, \forall (i,j) \in \mathcal{L},\ d \in \mathcal{N}_D, \tag{1}$$

$$0 \le \left[\sum_{j:(i,j)\in\mathcal{L}} x_{ij}^d - \sum_{k:(k,i)\in\mathcal{L}} x_{ki}^d - q_i^d \right] \perp \pi_i^d \ge 0, \forall i \in \mathcal{N},\ i \ne d,\ d \in \mathcal{N}_D. \tag{2}$$

where $c_{ij} = t_{ij}(x_{ij})$, $t_{ij}(x_{ij})$ is link travel time and x_{ij} is the aggregate traffic flow where $x_{ij} = \Sigma_d x_{ij}^d$.

2.2 *Link cost specification*

In this section, we specify link cost regarding the privacy. To measure travelers' privacy level, we first introduce an entropy-based privacy metric [16, 26, 27] using the link flow distribution.

Definition 2.1. The link flow distribution, denoted as p_{ij}^d, is the proportion of the link flow x_{ij}^d to the total link flow $\Sigma_{d\in\mathcal{N}_D} x_{ij}^d$. Mathematically,

$$p_{ij}^d = \frac{x_{ij}^d}{\Sigma_{d\in\mathcal{N}_D} x_{ij}^d}, \forall d \in \mathcal{N}_D, (i,j) \in \mathcal{L}. \tag{3}$$

p_{ij}^d is also called anonymity probability [27], which is interpreted as the probability of travelers to destination d identified by an attacker from all travelers in link (i, j).

Note that p_{ij}^d satisfies: $\forall d \in \mathcal{N}_D, (i,j) \in \mathcal{L}$,

$$0 \le p_{ij}^d, \tag{4}$$

$$1 \ge p_{ij}^d. \tag{5}$$

The denominator in the definition of the link flow distribution (3) can be zero if the total link flow is zero. To avoid $\frac{0}{0}$, we introduce p_{ij}^d into the complementarity formulation as a variable [24, 28]. Denote $\lambda_{ij}^{d+}, \lambda_{ij}^{d-}$ as the multipliers for constraints defined in (4) to (5), respectively. Accordingly, we have the following complementarity conditions: $\forall d \in \mathcal{N}_D, (i,j) \in \mathcal{L}$,

$$0 \le p_{ij}^d \perp \sum_d x_{ij}^d \cdot p_{ij}^d - x_{ij}^d + \lambda_{ij}^{d+} - \lambda_{ij}^{d-} \ge 0, \tag{6}$$

$$0 \le p_{ij}^d \perp \lambda_{ij}^{d+} \ge 0, \tag{7}$$

$$0 \le 1 - p_{ij}^d \perp \lambda_{ij}^{d-} \ge 0. \tag{8}$$

Definition 2.2. The link flow privacy metric, denoted as m_{ij}, is the entropy of the link flow distribution [27]. Mathematically,

$$m_{ij} = \sum_d -p_{ij}^d ln(p_{ij}^d), \forall d \in \mathcal{N}_D, (i,j) \in \mathcal{L}. \tag{9}$$

m_{ij} is interpreted as the amount of information that an attacker needs to identify travelers to different destinations in the link flow. In a trivial case where $|\mathcal{N}_D| = 1$, i.e., all travelers have the same destination $d \in \mathcal{N}_D$, the probability of the attacker identifying travelers to destination d is 1 and the amount of information that the attacker needs is $m_{ij} = 0$.

Proposition 1. Given the number of destinations $|\mathcal{N}_D| = k \ge 1$, the link flow privacy metric satisfies: $\forall (i,j) \in \mathcal{L},\ 0 \le m_{ij} \le ln(k)$, and when $m_{ij} = ln(k)$, $x_{ij}^{d_1} = \ldots = x_{ij}^{d_k}$, i.e., it is hardest to identify travelers when travelers to different destinations are evenly distributed in the link flow.

Proof. We first look at inequality: $0 \le m_{ij}$. Because $0 \le p_{ij}^{d_l} \le 1$, we have $ln(px_{ij}^{d_l}) \le 0$. Accordingly, $0 \le -p_{ij}^{d_l} ln(p_{ij}^{d_l})$. $0 \le m_{ij}$ thus holds.

Next, we look at $m_{ij} \le ln(k)$. We reformulate m_{ij} as $\mathcal{F}(p_{ij}^{d_1}, \ldots, p_{ij}^{d_k}, \gamma) = \sum_l -p_{ij}^{d_l} ln(p_{ij}^{d_l}) + \gamma(\sum_l p_{ij}^{d_l} - 1)$ where γ is the Lagrange multiplier. Therefore, we have:

$$\frac{\partial \mathcal{F}}{\partial p_{ij}^{d_l}} = -ln(p_{ij}^{d_l}) - 1 + \gamma = 0.$$

Accordingly, $p_{ij}^{d_1} = \ldots = p_{ij}^{d_k} \equiv e^{\gamma - 1}$. It means travelers to different destinations are evenly distributed in the link flow, i.e., $p_{ij}^{d_1} = \frac{1}{k}$, $l = 1, \ldots, k$. We substitute $p_{ij}^{d_1}$ with $\frac{1}{k}$ and get $m_{ij}^* = ln(k)$ where $m_{ij} \le m_{ij}^*$. Therefore, $m_{ij} \le ln(k)$ holds and when $m_{ij} = ln(k)$, we have $x_{ij}^{d_1} = \ldots = x_{ij}^{d_k}$.

Proposition 2. Given the number of travelers to each destination $x_{ij}^d \equiv \overline{x}$ where $\overline{x}$ is a positive constant, the link flow privacy metric increases as the number of destinations increases. In other words, the more destinations are involved on a link, the harder to trace one car.

Proof. Assume there are k destinations, i.e., $|\mathcal{N}_D| = k$, and the link flow metric is calculated as $m_{ij} = -\sum_{l=1}^{k} p_{ij}^{d_l} log(p_{ij}^{d_l})$. Because $x_{ij}^{d_l} \equiv \dot{x}$, $l = 1, \ldots, k$, we have $m_{ij} = ln(k)$. If we add a destination d_{k+1} with flow $\dot{x}$ and the new link flow distribution $p_{ij}^{*d_l}$, $l = 1, \ldots, k+1$ is equal to $\frac{1}{k+1}$. Accordingly, we have $m_{ij}^* = ln(k+1) > m_{ij}$. Therefore, the more destinations are involved on a link, the harder to trace one car.

Note that the silent link method is protecting travelers from being traced by the attacker and the proposed privacy metric is actually measuring the degree to which travelers' privacy is protected. Therefore, the protected privacy of travelers should be deducted from the generalized link cost. Mathematically, the generalized link cost is reformulated as:

$$\tilde{c}_{ij} = c_{ij} - I_p y_{ij} m_{ij}, \ \forall (i, j) \in \mathcal{L}, \tag{10}$$

where,

I_p: the coefficient of protected privacy on a link and $I_p > 0$.

y_{ij}: binary variable, indicating whether link $(i, j) \in \mathcal{L}$ is silent or not. When $y_{ij} = 0$, the link is not silent and the privacy of travelers is not protected. Therefore, the generalized link cost is the link travel time. When $y_{ij} = 1$, the link is silent and the protected privacy is deducted from the generalized link cost.

2.3 *SLUE formulation*

Summarizing equations (1), (2), (6) to (8), and (10), the equilibrium can be formulated as:

[SLUE − NCP]

$$0 \le [\pi_j^d + \tilde{c}_{ij} - \pi_i^d] \perp \pi_{ij}^d \ge 0, \forall (i, j) \in \mathcal{L}, \ d \in \mathcal{N}_D, \tag{11}$$

$$0 \le \left[\sum_{j:(i,j)\in\mathcal{L}} x_{ij}^d - \sum_{k:(k,i)\in\mathcal{L}} x_{ki}^d - q_i^d \right] \perp \pi_i^d \ge 0, \forall i \in \mathcal{N}, \tag{12}$$

$$0 \le p_{ij}^d \perp \sum_d x_{ij}^d \cdot p_{ij}^d - x_{ij}^d + \lambda_{ij}^{d+} - \lambda_{ij}^{d-} \ge 0, \forall (i, j) \in \mathcal{L}, \tag{13}$$

$$0 \le p_{ij}^d \perp \lambda_{ij}^{d+} \ge 0, \tag{14}$$

$$0 \le 1 - p_{ij}^d \perp \lambda_{ij}^{d-} \ge 0. \tag{15}$$

Equation (11) captures route choice for travelers. Equation (12) shows the flow conservation in the network. Equation (13) defines the link flow distribution. Equations (14) and (15) define the lower and upper bound of the link flow distribution, respectively.

2.4 *Existence and uniqueness*

Proposition 3. The existence and uniqueness of SLUE hold if the following conditions are satisfied:

1. $t_{ij}(x_{ij}) - \alpha_{ij} y_{ij} m_{ij}(x_{ij}) > 0,\ \forall (i,j) \in \mathcal{L}$

2. $\partial (t_{ij}(x_{ij})) / \partial x_{ij}^d - \partial (\alpha_{ij} y_{ij} m_{ij}(x_{ij})) / \partial x_{ij}^d > 0,\ \forall (i,j) \in \mathcal{L},\ d \in \mathcal{N}_D$

Proof. To prove the existence of the equilibrium, we need to show that the Jacobian of the variational inequalities satisfies that $J + J^T$ is positive definite. Denote that

$$g_{ij}^d(x, \pi) = \pi_j^d + t_{ij}\left(\sum_{d \in \mathcal{N}_D} x_{ij}^d\right) - \alpha_{ij} y_{ij} m_{ij}(\mathbf{x}) - \pi_i^d, \tag{16}$$

$$h_i^d(x) = \sum_{j:(i,j) \in \mathcal{L}} x_{ij}^d - \sum_{k:(k,i) \in \mathcal{L}} x_{ki}^d - q_i^d. \tag{17}$$

We then have

$$J + J^T = \left[\frac{\partial g}{\partial x} + \left(\frac{\partial g}{\partial x}\right)^T\right], \tag{18}$$

$\forall v^T = (v_1^T, \ldots, v_{|\mathcal{L}|}^T) \in \Re^{|\mathcal{L}| \cdot |\mathcal{N}_D|}$, where each $v_k^T \in \Re^{|\mathcal{N}_D|}$, then

$$v^T \left(\frac{\partial g}{\partial x} + \left(\frac{\partial g}{\partial x}\right)^T\right) v = \sum_k v_k^T v^T \left(\frac{\partial g_{i_k j_k}}{\partial x_{i_k j_k}} + \left(\frac{\partial g_{i_k j_k}}{\partial x_{i_k j_k}}\right)^T\right) v_k. \tag{19}$$

$\frac{\partial g}{\partial x} + \left(\frac{\partial g}{\partial x}\right)^T$ is positive definite (PD) if and only if when each $\frac{\partial g_{i_k j_k}}{\partial x_{i_k j_k}} + \left(\frac{\partial g_{i_k j_k}}{\partial x_{i_k j_k}}\right)^T$ is PD. According to Facchinei and Pang [29], the Jacobian has to be PD in nonnegative orthant since the link-node flows and potentials are all nonnegative by definition. Arbitrarily choose a vector $v = \{v_{ij}^d\} \in \mathcal{R}_+^{|\mathcal{N}_D|}$, then $v^T \left(\frac{\partial g_{i_k j_k}}{\partial x_{i_k j_k}} + \left(\frac{\partial g_{i_k j_k}}{\partial x_{i_k j_k}}\right)^T\right) v = \Sigma_m \Sigma_n v_m \left(\frac{\partial g_{i_k j_k}}{\partial x_{i_k j_k}^{d_n}} + \frac{\partial g_{i_k j_k}}{\partial x_{i_k j_k}^{d_m}}\right) v_n$. It is positive only when each $\frac{\partial g_{i_k j_k}}{\partial x_{i_k j_k}^{d_n}} + \frac{\partial g_{i_k j_k}}{\partial x_{i_k j_k}^{d_m}}$ is positive, which is equivalent to that each $\frac{\partial g_{i_k j_k}}{\partial x_{i_k j_k}^{d_n}}$ is positive and thus holds under Proposition 3.

2.5 *Numerical examples*

In this section, we present equilibrium results on the Braess network. We use the Bureau of Public Roads (BPR) function as the travel time function on links, $t_{ij}(x_{ij}) = t_{ij}^0 \left[1 + A\left(\frac{x_{ij}}{\text{Capacity}}\right)^B\right]$. In this paper, we simplify the function as $t_{ij}(x_{ij}) = a_{ij} + b_{ij}(x_{ij})$. [SLUE – NCP] is solved using the PATH solver. We use the Braess network with multiple origin-destination (OD) pairs to demonstrate the existence of Braess paradox. The parameters are in Table 1. Figures 1(a) and 1(c) show that adding the link (2,3) does not increase the total travel cost, which means that there is no Braess paradox. However, when link (1,2) is silenced (Figure 1(d)), the total travel cost increases to 73.4162, indicating the existence of the Braess paradox.

Table 1. Mean parameters on the Braess network

(a) Parameters in travel time function

link	a	b	α
(1,2)	2	5	$2/ln3$
(1,3)	10	2	$2/ln3$
(2,3)	2	0.1	0
(2,4)	30	1	0
(3,4)	10	1	0

(b) OD demand

OD	Demand
(1,2)	1
(1,3)	1.5
(1,4)	1.5

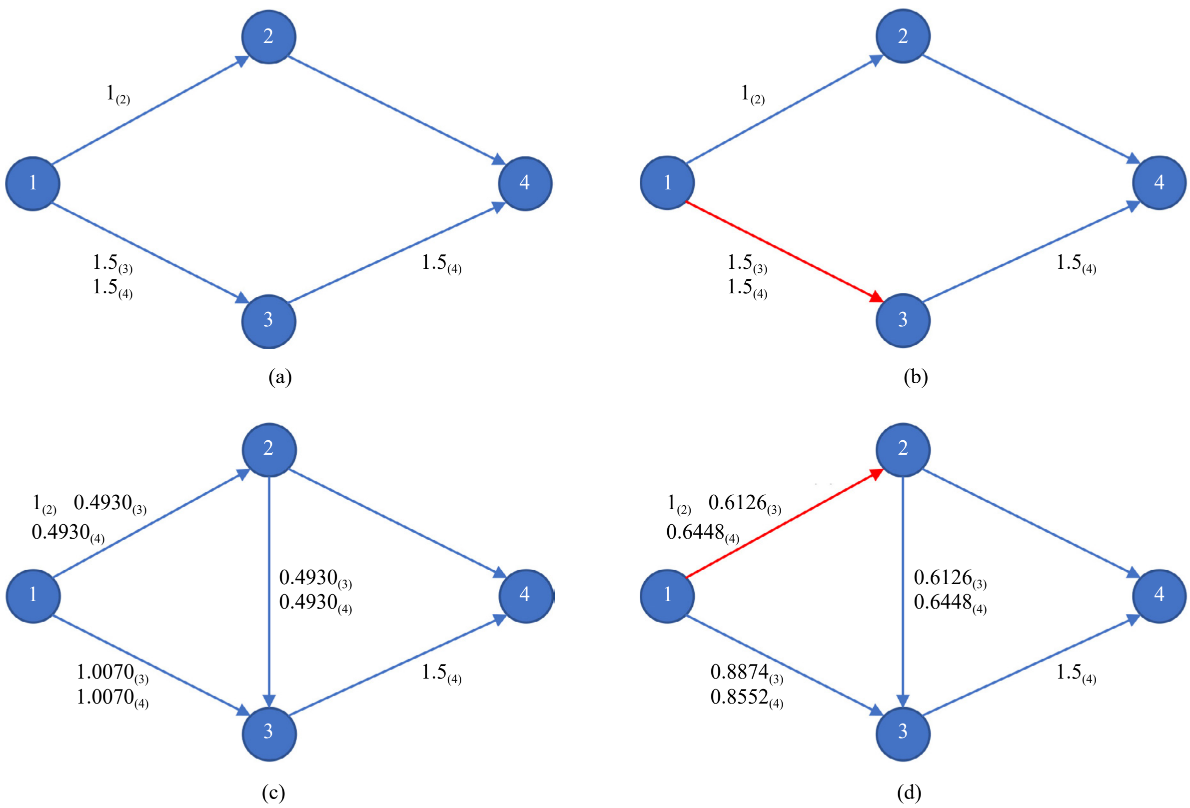

Figure 1. The existence of Braess paradox: (a) Total travel cost is 72.25; (b) Total travel cost is 72.25 and link (1,3) is silenced; (c) Total travel cost is 71.2641; (d) Total travel cost is 73.4162 and link (1,2) is silenced

3. Bi-level network design

In this section, we propose a bi-level network design model to study how a city planner can maximize the total privacy level for travelers by silencing links and how the city planner affects user equilibrium.

3.1 *Problem formulation*

On the upper level, a city planner makes the decision about which links to silence to maximize travelers' privacy level. The decision variable of the city planner is: $\mathbf{y} \in \{0,1\}^{|\mathcal{L}|}$ where $\mathbf{y} = [y_{ij}]$, $\forall(i,j) \in \mathcal{L}$ and the binary variable y_{ij} indicates whether link (i,j) is silent ($y_{ij} = 1$) or not ($y_{ij} = 0$). The objective function of the city planner is formulated as: $z(\mathbf{y}) = \sum_{(i,j)\in\mathcal{L}} y_{ij} m_{ij}$. Note that the privacy metric mij depends on route choice in SLUE. We then reformulate the upper level as:

$$[\mathbf{SLUE-NDP}]\max_{\mathbf{y}} z(\mathbf{y},\mathbf{m}), \tag{20}$$

where $\mathbf{m}=[m_{ij}],\ \forall(i,j)\in\mathcal{L}$. On the lower level, SLUE is formulated when the city planner makes the decision about which links to silence. Given the decision of the city planner **y**, we have:

$$[\mathbf{SLUE-NCP(y)}]\mathbf{m}=\mathbf{m}(\mathbf{y};\mathbf{x}). \tag{21}$$

We also add a budget constraint to the network design for the city planner. Mathematically,

$$\mathbf{A}^{\mathbf{T}}\mathbf{y}\le b, \tag{22}$$

where $\mathbf{A}=[a_{ij}]^T,\ \forall(i,j)\in\mathcal{L},\ a_{ij}$ represents the construction and operation cost of silencing link (i, j) and b is the city planner's budget. Note that the city planner should not silence a link unoccupied by any traveler, i.e., $x_{ij} = 0 \to y_{ij} = 0$. We reformulate it as an indicator constraint:

$$\mathbf{y}\le M\cdot\mathbf{x}, M>10^5. \tag{23}$$

Summarizing (20), (21), (22) and (23), we have the following network design problem (NDP):

$$\begin{aligned}&[\mathbf{SLUE-NDP}]\\&\max_{\mathbf{y}} z(\mathbf{y};\mathbf{m})\\&s.t.\\&[\mathbf{SLUE-NCP(y)}]\mathbf{m}=\mathbf{m}(\mathbf{y};\mathbf{x})\\&\mathbf{A}^{\mathbf{T}}\mathbf{y}\le b,\ \mathbf{y}\le M\cdot\mathbf{x},\ \mathbf{y}\in\{0,1\}^{|\mathcal{L}|}.\end{aligned} \tag{24}$$

3.2 *Solution approach*

To solve the bi-level network design problem [30, 31], we decompose it into two parts: choosing silent links on the upper level and obtaining the equilibrium in SLUE on the lower level. In step 1, we initialize the city planner's decision as $\mathbf{y} = \mathbf{y}^{(0)}$. In step 2, given silent links on the upper level, we solve [**SLUE_NCP**(**y**)] and get the equilibrium solution **m** = **m**(**y**; **x**). In step 3, we apply the branch and bound algorithm to solve a binary integer programming [**SLUE_NDP**(**m**)] for the city planner. The solution is denoted as $\mathbf{y} = \mathbf{y}^{(1)}$. In step 4, we repeat steps 2 to 3 until $\left|\mathbf{y}^{(n+1)}-\mathbf{y}^{(n)}\right|\le\epsilon$ where $\epsilon=10^{-4}$.

3.3 *Numerical examples*

We plot the traffic flow on the Braess network in Figure 2. Figure 2(a) shows the equilibrium with no silent links. The right one shows the link flow when (1,3) is silenced (marked in green). When our silent link method is applied to the network, the system will shift to a new user equilibrium as shown in Figure 2(b), where the silent link is marked green. More travelers switch from link (1,2) to link (1,3), from which they can get access to the silent link in this network and thus enhance their privacy level.

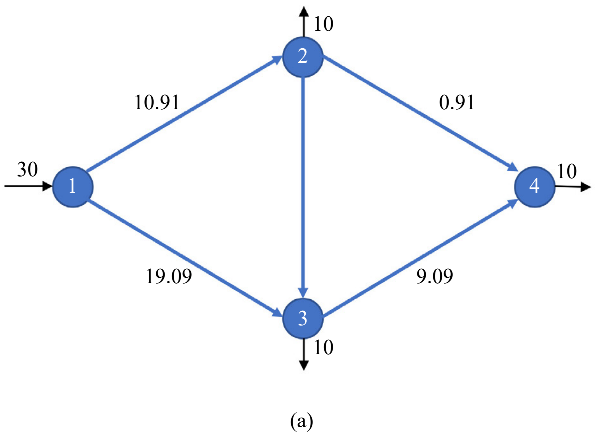

Figure 2. Braess network

To demonstrate the performance of our method, we apply the bi-level network design problem to a larger size network (Sioux Falls network) with 24 nodes and 76 links. The topology of the network, node indexes, link indexes, and the link performance functions are downloadable from GitHub (https://github.com/bstabler/TransportationNetworks). The total travel demand is 1,800. Figure 3 demonstrates the traffic flow on the Sioux Falls network. The x-axis represents the link index 1, ..., 76 and the y-axis denotes the traffic flow on each link in SLUE. The optimal number of silent links in the network is 6 (link index: 6, 24, 34, 59, 63, 72). The running time of solving the bi-level problem in GAMS [32] is 32.83 s.

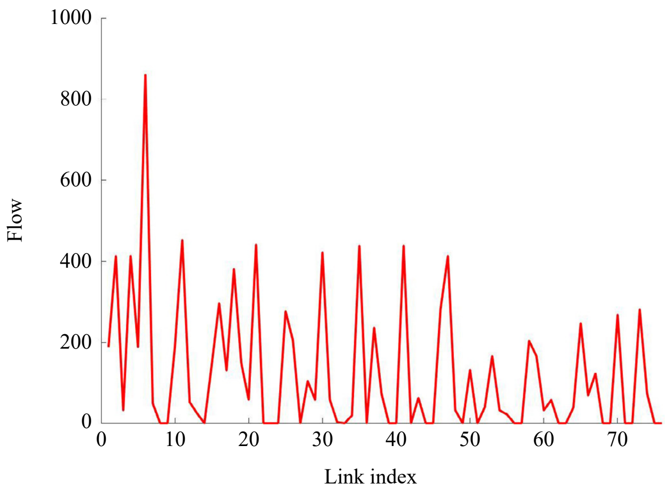

Figure 3. Sioux Falls network

4. Conclusions

In a network of CV, location privacy protection conflicts with safety applications. On one hand, vehicles locations need to be obfuscated as much as possible for privacy, while on the other hand, availability of location information is crucial for safety applications such as forward collision warning systems. Striking a balance of network privacy and safety is of critical importance for real-life deployment of CV systems. Existing literature is limited in both theory and practice.

In this paper, we address the issue with a new privacy metric based on traffic user equilibria. This metric can evaluate privacy levels of a transportation network, capturing the inherent connection between the privacy level endogenous to a transportation network and equilibrium patterns therein. We further proposed a new privacy protection method named "Silent Link." From the network equilibrium perspective, vehicles running on silenced links experience a reduced generalized cost, leading to a shift in equilibrium patterns. The new privacy metric and silent link method are integrated into a network design framework for the purpose of designing and optimizing the choices of Silent Links.

Conflict of interest

The authors declare that there is no conflict of interest.

References

[1] U.S. Department of Transportation. *Connected vehicle basics*. https://www.its.dot.gov/cv_basics/index.htm. [Accessed 15th March 2021].

[2] Hartenstein H, Laberteaux LP. A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*. 2008; 46(6): 164-171. https://doi.org/10.1109/MCOM.2008.4539481

[3] Di X, Shi R. A survey on autonomous vehicle control in the era of mixed-autonomy: From physics-based to AI-guided driving policy learning. *Transportation Research Part C: Emerging Technologies*. 2021; 125: 103008. https://doi.org/10.1016/j.trc.2021.103008

[4] Buttyán L, Holczer T, Weimerskirch A, Whyte W. SLOW: A practical pseudonym changing scheme for location privacy in VANETs. In: *2009 IEEE Vehicular Networking Conference (VNC)*. Tokyo, Japan: IEEE; 2009. p.1-8. https://doi.org/10.1109/VNC.2009.5416380

[5] Meinrenken CJ, Shou Z, Di X. Using GPS-data to determine optimum electric vehicle ranges: A Michigan case study. *Transportation Research Part D: Transport and Environment*. 2020; 78: 102203. https://doi.org/10.1016/j.trd.2019.102203

[6] Mokbel MF, Chow CY, Aref WG. The new casper: Query processing for location services without compromising privacy. In: *Proceedings of the 32nd International Conference on Very Large Data Bases.* Seoul, Korea: VLDB Endowment; 2006. p.763-774. https://dl.acm.org/doi/abs/10.5555/1182635.1164193

[7] Ban X, Gruteser M. Mobile sensors as traffic probes: addressing transportation modeling and privacy protection in an integrated framework. In: Mao B, Tian Z, Huang H, Gao Z. (eds.) *Traffic and Transportation Studies 2010*. Kunming, China: American Society of Civil Engineers; 2010. p.750-767. https://doi.org/10.1061/41123(383)72

[8] Sun Z, Zan B, Ban XJ, Gruteser M. Privacy protection method for fine-grained urban traffic modeling using mobile sensors. *Transportation Research Part B: Methodological*. 2013; 56: 50-69. https://doi.org/10.1016/j.trb.2013.07.010

[9] Gonder J, Burton E, Murakami E. Archiving data from new survey technologies: enabling research with high-precision data while preserving participant privacy. *Transportation Research Procedia*. 2015; 11: 85-97. https://doi.org/10.1016/j.trpro.2015.12.008

[10] Aïvodji UM, Gambs S, Huguet MJ, Killijian MO. Meeting points in ridesharing: A privacy-preserving approach. *Transportation Research Part C: Emerging Technologies*. 2016; 72: 239-253. https://doi.org/10.1016/j.trc.2016.09.017

[11] Gruteser M, Liu X. Protecting privacy, in continuous location-tracking applications. *IEEE Security & Privacy*. 2004; 2(2): 28-34. https://doi.org/10.1109/MSECP.2004.1281242

[12] Sweeney L. *k*-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*. 2002; 10(05) :557-570. https://doi.org/10.1142/S0218488502001648

[13] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking. In: *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*. New York, United States: ACM; 2003. p.31-42. https://doi.org/10.1145/1066116.1189037

[14] Kido H, Yanagisawa Y, Satoh T. An anonymous communication technique using dummies for location-based services. In: *ICPS'05. Proceedings. International Conference on Pervasive Services, 2005*. Santorini, Greece: IEEE; 2005. p.88-97. https://doi.org/10.1109/PERSER.2005.1506394

[15] Pingley A, Zhang N, Fu X, Choi HA, Subramaniam S, Zhao W. Protection of query privacy for continuous location based services. In: *2011 Proceedings IEEE INFOCOM*. Shanghai, China: IEEE; 2011. p.1710-1718. https://doi.

org/10.1109/INFCOM.2011.5934968
[16] Beresford AR, Stajano F. Location privacy in pervasive computing. *IEEE Pervasive Computing*. 2003; 2(1): 46-55. https://doi.org/10.1109/MPRV.2003.1186725
[17] Freudiger J, Raya M, Félegyházi M, Papadimitratos P, Hubaux JP. Mix-zones for location privacy in vehicular networks. In: *Proceedings of the First International Workshop on Wireless Networking for Intelligent Transportation Systems (Win-ITS), 2007*. Vancouver, Canada: ACM; 2007. p.1-7. http://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Akth%3Adiva-35531
[18] Xin W, Moonam HM, Petit J, Whyte W. Towards a balance between privacy and safety: microsimulation framework for assessing silence-based pseudonym-change schemes. *Transportation Research Record*. 2019; 2673(2): 71-84. https://doi.org/10.1177/0361198119825833
[19] Chow J. *Informed urban transport systems: Classic and emerging mobility methods toward smart cities*. Netherlands: Elsevier; 2018. https://doi.org/10.1016/C2016-0-02361-6
[20] He Y, Chow JY, Nourinejad M. A privacy design problem for sharing transport service tour data. In: *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC)*. Yokohama, Japan: IEEE; 2017. p.1-6. https://doi.org/10.1109/ITSC.2017.8317692
[21] He BY, Chow JY. Optimal privacy control for transport network data sharing. *Transportation Research Part C: Emerging Technologies.* 2020; 113: 370-387. https://doi.org/10.1016/j.trc.2019.07.010
[22] Freudiger J, Shokri R, Hubaux JP. On the optimal placement of mix zones. In: Goldberg I, Atallah MJ. (eds.) *Privacy Enhancing Technologies. PETS 2009*. Lecture Notes in Computer Science, vol 5672. Springer, Berlin, Heidelberg; 2009. https://doi.org/10.1007/978-3-642-03168-7_13
[23] Sun Y, Zhang B, Zhao B, Su X, Su J. Mix-zones optimal deployment for protecting location privacy in VANET. *Peer-to-Peer Networking and Applications*. 2015; 8: 1108-1121. https://doi.org/10.1007/s12083-014-0269-z
[24] Di X, Ma R, Liu HX, Ban XJ. A link-node reformulation of ridesharing user equilibrium with network design. *Transportation Research Part B: Methodological*. 2018; 112: 230-255. https://doi.org/10.1016/j.trb.2018.04.006
[25] Di X, Ban XJ. A unified equilibrium framework of new shared mobility systems. *Transportation Research Part B: Methodological*. 2019; 129: 50-78. https://doi.org/10.1016/j.trb.2019.09.002
[26] Diaz C, Seys S, Claessens J, Preneel B. Towards measuring anonymity. In: Dingledine R, Syverson P. (eds.) *Privacy Enhancing Technologies. PET 2002*. Lecture Notes in Computer Science, vol 2482. Springer, Berlin, Heidelberg; 2003. p.54-68. https://doi.org/10.1007/3-540-36467-6_5
[27] Serjantov A, Danezis G. Towards an information theoretic metric for anonymity. In: Dingledine R, Syverson P. (eds.) *Privacy Enhancing Technologies. PET 2002*. Lecture Notes in Computer Science, vol 2482. Springer, Berlin, Heidelberg; 2003. p.41-53. https://doi.org/10.1007/3-540-36467-6_4
[28] Chen X, Di X. A unified network equilibrium for e-hailing platform operation and customer mode choice. *ArXiv* [Preprint] 2022. Version 2. https://arxiv.org/abs/2203.04865v2
[29] Facchinei F, Pang JS. (eds.) *Finite-dimensional variational inequalities and complementarity problems*. New York: Springer Science & Business Media; 2007. https://doi.org/10.1007/b97543
[30] Di X, Liu HX, Ban XJ. Second best toll pricing within the framework of bounded rationality. *Transportation Research Part B: Methodological*. 2016; 83: 74-90. https://doi.org/10.1016/j.trb.2015.11.002
[31] Chen X, Di X. Ridesharing user equilibrium with nodal matching cost and its implications for congestion tolling and platform pricing. *Transportation Research Part C: Emerging Technologies*. 2021; 129: 103233. https://doi.org/10.1016/j.trc.2021.103233
[32] Ferris M. *GAMS/NLPEC Solver Manual*. GAMS Development Corporation; 2009.