Private-MP

Privacy-Preserving Max-Pressure Control Based on Mobile Edge Computing

Tan, Chaopeng; Rinaldi, Marco; Zeng, Yikai; Wang, Meng; Van Lint, Hans

DOI
10.1109/MT-ITS68460.2025.11223553

Publication date
2025

Document Version
Final published version

Published in
2025 9th International Conference on Models and Technologies for Intelligent Transportation Systems, MT-ITS 2025

2025 9th International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS) | 979-8-3315-8063-6/25/$31.00 ©2025 IEEE | DOI: 10.1109/MT-ITS68460.2025.11223553

Private-MP: Privacy-Preserving Max-Pressure Control based on Mobile Edge Computing

Chaopeng Tan
Chair of Traffic Process Automation
Technische Universität Dresden, Dresden
& *Department of Transport and Planning*
Delft University of Technology, Delft
chaopeng.tan@tu-dresden.de

Marco Rinaldi
Department of Transport and Planning
Delft University of Technology
Delft, The Netherlands
m.rinaldi@tudelft.nl

Yikai Zeng
Chair of Traffic Process Automation
Technische Universität Dresden
Dresden, Germany
yikai.zeng@tu-dresden.de

Meng Wang
Chair of Traffic Process Automation
Technische Universität Dresden
Dresden, Germany
meng.wang@tu-dresden.de

Hans van Lint
Department of Transport and Planning
Delft University of Technology
Delft, The Netherlands
j.w.c.vanlint@tudelft.nl

***Abstract*—Max-pressure (MP) control has proven effective at stabilizing network queues and improving traffic throughput in large-scale urban road networks. However, conventional MP controllers based on connected vehicle (CV) data face two critical limitations: network stability diminishes when connected vehicle (CV) penetration rates are low, and significant privacy concerns arise when utilizing individual vehicle data. To address these challenges, this paper proposes a novel Private-MP controller that fuses data from both fixed-location detectors and CVs in an architecture of mobile edge computing. To fully safeguard CV privacy, including macro-route information and micro-trajectory information, Private-MP employs a privacy-preserving mechanism that combines homomorphic encryption with an adaptive randomized response strategy. Simulation studies on a network with five intersections showed that despite some increases in average vehicle delay due to privacy protection, Private-MP still ensures a more robust performance on average vehicle delay than CV-based MP in low penetration rate scenarios and outperforms traditional detector-based MP control while improving fairness among connected and non-connected vehicles.**

***Index Terms*—Max-pressure control, connected vehicle, data fusion, privacy preservation, mobile edge computing, fairness**

I. Introduction

Real-time traffic signal control at the network level presents substantial challenges due to the dynamic, complex, and large-scale nature of urban transportation systems. While centralized methods theoretically allow the optimization of global performance metrics across all intersections, they often rely on large-scale, high-dimensional optimization problems that are computationally expensive to solve in real time [1], [2]. As a result, centralized solutions can become inefficient or infeasible in practice, especially in dynamic traffic environments. In contrast, Max-pressure (MP) control has emerged as a promising alternative, offering a decentralized mechanism wherein each intersection independently determines signal timings based on local real-time traffic state information, e.g., vehicle counts [3] or average travel time [4]. This approach effectively alleviates communication and computational bottlenecks, making MP both simple to implement and highly effective at stabilizing network queues.

Concurrently, advancements in connected vehicle (CV) technologies have made it possible to collect highly detailed vehicle-level data (e.g., position, speed, queue length) in real time, thereby enhancing the responsiveness and accuracy of MP controllers [5]–[7], e.g., [5] proposed position-weighted MP (PWMP) that uses the weighted position of vehicles for pressure calculation and [6] proposed delay-based MP (D-MP) that uses vehicle delay in the last horizon for pressure calculation. However, exclusive reliance on vehicle-level data introduces two major concerns. First, CV-based control approaches become unreliable when the CV penetration rate is low since temporally and spatially sparse data can lead to performance degradation and potential instability in control decisions [8], [9]. Second, it can raise substantial privacy issues, as the granularity of these data may expose sensitive information about individual drivers' behavior and their travel patterns [10]. For example, by linking the data-sharing behaviors of vehicles at different intersections, the travel routes of vehicles can be easily restored.

To address the above concerns, this paper proposes Private-MP, a novel framework for privacy-preserving MP control under a Mobile Edge Computing (MEC) architecture utilizing both CV data and detector data. The major contribution is three-fold:

- By fusing CV data with fixed-location detector information, the proposed data-fusion MP control without considering privacy ensures more stable performance at low CV penetration rates compared to CV-only MP controllers and provides a more comprehensive view of

The authors would like to acknowledge the financial contribution of the EU Horizon Europe Research and Innovation Programme, Grant Agreement No. 101103808 ACUMEN.

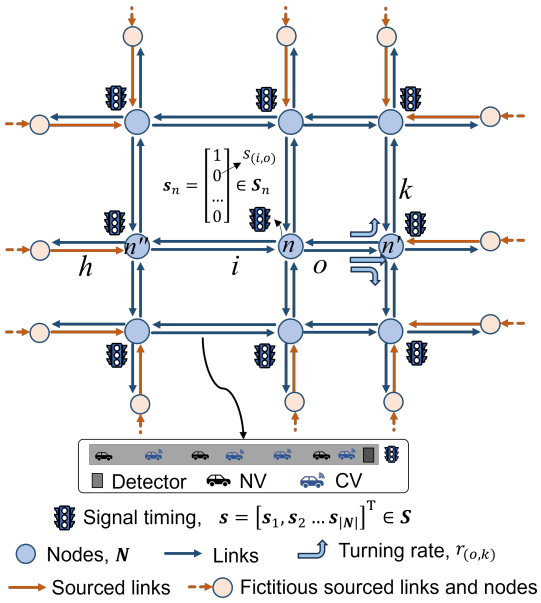

Fig. 1. Network definition.

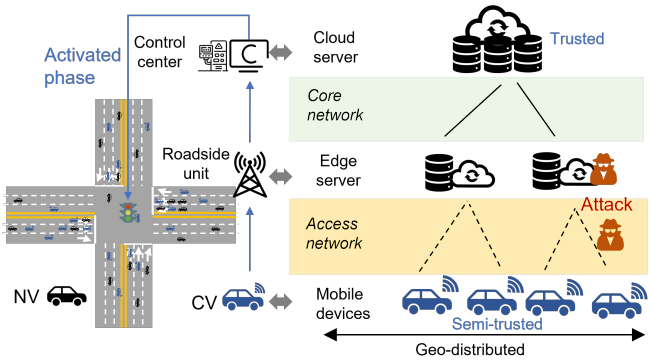

Fig. 2. Mobile edge computing architecture.

traffic conditions than detector-only MP controllers.

- We propose a privacy-preserving mechanism in MEC architecture that incorporates homomorphic encryption and adaptive randomized response to comprehensively protect CV data in both macro-route and micro-trajectory levels.
- Evaluation results demonstrated that data-fusion MP effectively reduces vehicle delays under various penetration rate scenarios, consistently outperforming single-data-source MP controllers. The cost of the privacy-preserving mechanism of Private-MP is the increased vehicle delay, but it still outperforms single-data-source MP controllers at low penetration rates while improving fairness.

II. Preliminaries

A. Network definitions

Given a signalized network modeled as in Fig. 1, let $\mathcal{N}$ be the set of signalized intersections (nodes), indexed by n. The set of movements for a node n is denoted by $\mathcal{M}_n$, where each movement is indexed by a pair of incoming and outgoing links, e.g., (i, o). The upstream node connecting to the incoming link i of node n is indicated by n'' and the downstream node connecting to the outgoing link o of node n is indicated by n'. Traffic demands are introduced from fictitious source links (no physical length) connected via fictitious source nodes $\mathcal{F}$; consequently, these source links have infinite jam densities. We write $\mathcal{M}_{\mathcal{N}}$ and $\mathcal{M}_{\mathcal{F}}$ for the sets of movements at all real and fictitious nodes, respectively. Let $\boldsymbol{s}$ represent the overall signal vector, composed of $\boldsymbol{s}_n$ for each node n. For movement (i, o), the binary variable $s_{(i,o)}$ indicates green phase activation, i.e., $s_{(i,o)} = 1$ if green and $s_{(i,o)} = 0$ otherwise. At any fictitious node, its sole movement is always green. The set $\boldsymbol{S}$ denotes all feasible signal states with respect to signal phase constraints. $r_{(i,o)}$ denotes the turning ratio of the movement (i, o) regarding link i. On the incoming link of movement (i, o), let $\mathcal{J}^{cv}_{(i,o)}$ be the sets of CVs indexed by j, having sizes $z^{cv}_{(i,o)}$. It is assumed that fixed-location detectors, e.g., loop detectors, are deployed near the stopline of each link to capture the traffic volume of each movement per minute, i.e., the resolution of the vast majority of fixed-location detectors in reality.

B. Mobile edge computing architecture

A great advantage of MP control is its decentralized nature, where each intersection relies solely on local traffic state information, making it inherently scalable. However, when employing CV data for MP control, processing large-scale network-level CV data on traditional cloud servers can impose heavy computational burdens and cause network bottlenecks, leading to delays in data processing and signal decision making. To mitigate these issues, this study utilizes MEC technology [11], which brings computation and storage closer to the point of need—such as near signalized intersections—to reduce latency and enhance real-time processing capabilities.

The proposed MEC architecture, as shown in Fig. 2, consists of three layers:

- Mobile devices: CVs that are capable of processing and storing their trajectory data in real time, which share data with nearby edge servers via wireless networks like 5G.
- Edge server: Local computational nodes near intersections (e.g., within roadside units) that collect and locally process CV data, then forward aggregated information to the cloud server.
- Cloud server: Located at the traffic signal control center, this server coordinates geo-distributed edge servers and manages public traffic data (e.g., fixed-location detector data in this study)

While MEC significantly enhances real-time processing by reducing latency, it also introduces privacy challenges when used in applications in CV environments. CV data, particularly location information, is highly sensitive. We assume that CVs are curious but honest, meaning they follow communication protocols while attempting to glean as much information as

possible from received messages [10]. Although the cloud server, managed by government-operated traffic control centers, is considered trustworthy, the roadside placement of edge servers makes them vulnerable to intrusion. Consequently, this MEC architecture faces critical privacy risks: adversaries may compromise edge servers to steal processed or stored data, and wireless transmissions (e.g., 5G) may be intercepted.

III. Methodology

A. Data-fusion MP controller

In this section, we propose a data-fusion MP controller utilizing fixed-location detector data and CV data.

Traditionally, based on flow conservation, the store-and-forward queuing model can be used to derive the traffic dynamics on each incoming link i of the network [3], [12], [13] as below:

$$z_{(i,o)}(t+1) = z_{(i,o)}(t) + a_{(i,o)}(t) - d_{(i,o)}(t), \tag{1}$$

where $z_{(i,o)}(t)$ denotes the number of vehicles of movement (i,o) at decision step t; $a_{(i,o)}(t)$ denotes the arrival vehicles and $d_{(i,o)}(t)$ denotes the departure vehicles,

$$a_{(i,o)}(t) = e_{(i,o)}(t) + \sum_{(\forall h,i)\in\mathcal{M}_{n''}} r_{(i,o)} d_{(h,i)}(t), \tag{2}$$

$$d_{(i,o)}(t) = \min\{z_{(i,o)}(t), s_{(i,o)}(t) c_{(i,o)}(t)\}. \tag{3}$$

where $e_{(i,o)}(t)$ denotes the exogenous arrivals on the source link and $c_{(i,o)}$ denotes the saturated flow rate of movement (i,o). For source links, $\sum_{(\forall h,i)\in\mathcal{M}_{n''}} r_{(i,o)} d_{(h,i)}(t) = 0$ due to the absence of the upstream intersection, while for non-source links, $e_{(i,o)}(t) = 0$.

In (1)-(3), $s_{(i,o)}(t)$ is the known signal decision at decision step t, $c_{(i,o)}(t)$ can be regarded as a known constant, and $r_{(i,o)}$ and $e_{(i,o)}(t)$ can be easily calibrated by historical detector data (or updated at regular sampling periods) as below:

$$e_{(i,o)}(t) = \bar{\lambda}_{(i,o)} T \quad \text{for source links}, \tag{4}$$

$$r_{(i,o)}(t) = \bar{\lambda}_{(i,o)} / \sum_{(i,\forall o)\in\mathcal{M}_n} \bar{\lambda}_{(i,o)}, \tag{5}$$

where $\bar{\lambda}_{(i,o)}$ is the average flow rate collected by fixed-location detectors and T is the decision step length. Thus, the number of vehicles $z_{(i,o)}(t)$, including CVs and non-connected vehicles (NVs), can be estimated by (1) based on fixed-location detector data.

Regarding each CV j of movement (i,o), we use $\tau_j(t)$ to denote its link travel time at the decision moment t:

$$\tau_j(t) = t - t_j^0, \tag{6}$$

where t_j^0 is the moment when CV j entered the link.

Then, the data-fusion MP controller is written as below:

$$\boldsymbol{s}^*(t) = \arg\max_{\boldsymbol{s}\in\boldsymbol{S}} \sum_{n\in\mathcal{N}} \Big(\sum_{\forall(i,o)\in\mathcal{M}_n} s_{(i,o)}(t) c_{(i,o)} \big(\phi_{(i,o)}(t) - \sum_{(o,\forall k)\in\mathcal{M}_{n'}} r_{(o,k)}(t)\phi_{(o,k)}(t)\big)\Big), \tag{7}$$

where the inner parentheses compute the difference in traffic state between the incoming link and outgoing link for the movement (i,o). Multiplied by the corresponding saturation flow rate $c_{(i,o)}$ is the pressure of the movement. $\phi_{(i,o)}(t)$ is the traffic state of movement (i,o) used for pressure calculation and

$$\phi_{(i,o)}(t) = z^{nv}_{(i,o)}(t) + \sum_{j\in\mathcal{J}^{cv}_{(i,o)}} \tau_j(t)/\bar{\tau}_{(i,o)}. \tag{8}$$

In (8), $z^{nv}_{(i,o)}$ denotes the number of NVs and

$$z^{nv}_{(i,o)} = \max\{z_{(i,o)} - z^{cv}_{(i,o)}, 0\}; \tag{9}$$

$\bar{\tau}_{(i,o)}$ is the free-flow link travel time, which is a known constant calculated as link length divided by speed limits. In two extreme cases: (i) if all vehicles are CVs, then $z^{nv}_{(i,o)} = 0$, the proposed MP controller becomes a complete CV-based MP controller; (ii) if no vehicle is CV, then it becomes the original MP based on queue information, i.e., Q-MP [3].

B. Threat Model

In this section, we introduce how the proposed data-fusion MP works under the MEC architecture and analyze the CV privacy information that needs to be protected. Then, the potential attacks are outlined.

When entering a link, CVs record and store the moment t_j^0. At the decision moment t, CVs compute their link travel time τ_j based on (6) and shares τ_j and its turning intention (i.e., left turn, straight through, or right turn encoded in a certain way) with the roadside unit using wireless transmission. Receiving CV data from all movements, roadside unit calculates $\sum_{j\in\mathcal{J}^{cv}_{(i,o)}} \tau_j(t)$ and $\sum_{j\in\mathcal{J}^{cv}_{(i,o)}} 1$ (i.e., $z^{cv}_{(i,o)}$) per movement and share the sum values to the traffic signal control center. Upon receiving the sum values, the traffic signal control center computes the traffic state of each movement based on (8) and makes signal decisions for each intersection based on the proposed data-fusion MP controller, i.e., (7).

During the process, CVs share three types of data with the roadside unit: link travel time, vehicle counts, and turning intention. Although link travel time hides the detailed location and speed information of the vehicle to some extent, it is still sensitive information about individual vehicles. Vehicle counts reflect whether or not a vehicle is communicating at an intersection, which, combined with turning intention, can be exploited to reconstruct complete travel routes. Given the MEC framework, both the wireless communication channels and the edge servers are susceptible to unauthorized access. Consequently, we identify three primary attack types:

- **Interception attack.** Wireless transmissions may be intercepted by adversaries, compromising the confidentiality of transmitted data.
- **Sniffing attack.** External attackers or system entities might clandestinely monitor and extract data stored on edge servers.
- **Inference attack.** By correlating data from the same mobile device over time, adversaries might infer vehicle trajectories or routes.

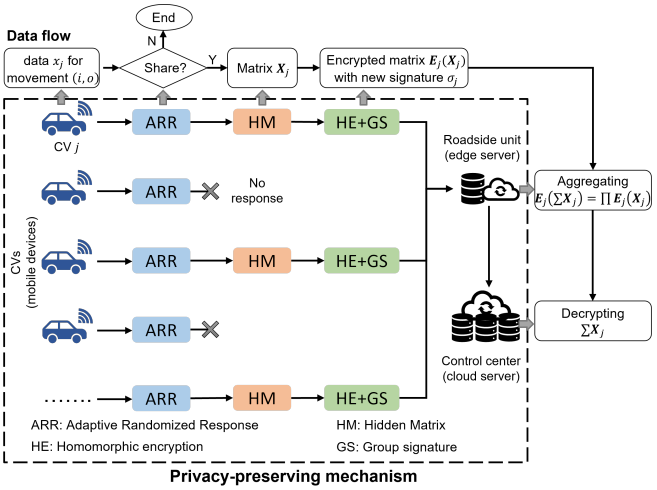

Fig. 3. The proposed privacy-preserving mechanism.

C. Privacy-preserving mechanism

The proposed privacy-preserving mechanism is presented in Fig. 3. Before sharing the private data x_j (note that $x_j = \tau_j$ when calculating $\sum_{j \in \mathcal{J}^{cv}_{(i,o)}} \tau_j(t)$ and $x_j = 1$ when calculating $z^{cv}_{(i,o)}$) and its turning intention, each CV j follows *adaptive randomized response* strategy to determine whether to share its data with a certain probability. For those CVs choosing to share data at the current decision step, the *hidden matrix* approach is adopted to generate a matrix containing all movements, thus protecting their movement information. Then *homomorphic encryption* and *group signature* techniques are used to encrypt the hidden matrix with a new signature for each time data sharing, protecting specific CV data while ensuring anonymity and unlinkability. Upon receiving the encrypted matrix from CVs, the roadside unit aggregates these matrices and shares the aggregated matrix with the control center, which will finally decrypt the aggregated matrix using the private key of homomorphic encryption and apply it for data-fusion MP at the corresponding intersection.

1) Adaptive randomized response: Even when CV data is encrypted, adversaries can still implement **inference attacks** to infer the CV route by analyzing its communication patterns with roadside units. To counter this, we propose an *adaptive randomized response* strategy requiring that:

- Sharing requirement. Each CV j independently decides whether to share data at intersection n based on an intersection-dependent probability P^n_j. The decision of each CV is only related to its own decision at the last intersection, reducing the frequency of communication as well as the computational cost, which is suitable for mobile edge computing architectures.
- Privacy requirement. The probability that a CV shares data at both consecutive intersections does not exceed P^p. It determines the strength of privacy protection against inference attacks. It can be understood as allowing a proportion P^p of CVs to share data at two consecutive intersections.
- Data requirement. Each intersection requires no less than a proportion P^d of CVs to share data. This is to satisfy the data requirements for CV-based MP control. The requirements of different controllers may vary.

Then, P^n_j of CVs has two cases: 1) the CV shares data at the last intersection and we let $P^n_j = P^{n,1}_j$ (case 1); 2) the CV does not share data at the last intersection and we let $P^n_j = P^{n,2}_j$ (case 2). For case 1 CVs, to satisfy the privacy requirement, we have

$$P^{n,1}_j \leq P^p. \tag{10}$$

We consider a steady state where the proportion of CVs that shared data in the previous intersection is P^d, that is, roughly P^d of CVs are in case 1 and the remaining $1 - P^d$ is in case 2. The overall proportion of CVs sharing data at the current intersection, P^n, should satisfy the data requirement:

$$P^n = P^d P^{n,1}_j + (1 - P^d) P^{n,2}_j \geq P^d. \tag{11}$$

In summary, we have

$$P^n_j = \begin{cases} P^p & \text{for case 1 CVs,} \\ P^d(1 - P^p)/(1 - P^d) & \text{for case 2 CVs,} \end{cases} \tag{12}$$

where we take the equal sign to maximize both data and privacy utility.

2) Hidden Matrix: To protect the turning intention, i.e., movement, of those CVs deciding to share data, a hidden matrix approach is proposed. For a CV j deciding to share x_j of movement (i,o) at node n, it generates a matrix $\boldsymbol{X_j}$ containing dimensions of all movements as

$$\boldsymbol{X_j} = [x^1_j, x^2_j, \cdots, x^{|\mathcal{M}_n|}_j]^\top = [0, \cdots, x_j, \cdots, 0]^\top \tag{13}$$

where the matrix $\boldsymbol{X_j}$ has all values of 0 except for the movement (i,o). Note that using a hidden matrix alone doesn't really protect the movement of CVs, since we can easily infer it given the index of the non-zero value in the matrix. However, when combined with homomorphic encryption, even if the adversary performs an **interception attack** and a **sniffing attack** to obtain the matrix, it is not possible to determine the non-zero value from the ciphertext matrix, thus protecting the movement of CVs.

3) Homomorphic encryption with group signature: After implementing the hidden matrix, those CVs deciding to share data further use a homomorphic encryption technique, i.e., Paillier cryptosystem in this study with a group signature technique to further encrypt the matrix to be shared while ensuring its data is unlinkable when communicating with roadside units.

The Paillier cryptosystem supports additive homomorphism [14]. Specifically, a trusted authority, i.e., the traffic signal control center in our study, generates a Paillier key pair. The public key is $PK = (b, g)$, and the corresponding private

key is sk. Then, for any plaintexts m_1 and m_2, with their encryptions defined as

$$c_1 = E(m_1; r_1) = g^{m_1} \cdot r_1^b \bmod b^2, \tag{14}$$

$$c_2 = E(m_2; r_2) = g^{m_2} \cdot r_2^b \bmod b^2, \tag{15}$$

the product of the ciphertexts is given by

$$c_1 \cdot c_2 \bmod n^2 = E(m_1 + m_2; r_1 \cdot r_2), \tag{16}$$

where r_1 and r_2 are random values. This property enables the roadside unit to compute the sum of data across vehicles by multiplying the corresponding ciphertexts.

A group signature scheme is set up by a group manager who generates a group public key GPK [15]. Each CV j is issued a private group signing key GSK_j. The group signature provides the following properties:

- **Anonymity:** The signature does not reveal the identity of the signer.
- **Unlinkability:** Even if the same vehicle signs messages at different times, the signatures cannot be linked.

The specific encryption and signing process is introduced as follows. For each element x_j^i of the matrix $\boldsymbol{X_j}$, the CV computes the ciphertext

$$c_j^i = E_{PK}(x_j^i; r_j^i) = g^{x_j^i} \cdot {r_j^i}^b \bmod b^2, \tag{17}$$

where r_j^i is a fresh random value for each encryption. The encrypted matrix is then $\boldsymbol{c_j} = [c_j^1, c_j^2, \cdots, c_j^{|\mathcal{M}_n|}]^\top$. To ensure both authentication and unlinkability, the CV signs the encrypted matrix using its group signing key. The signature is computed on a hash of the ciphertext vector:

$$\sigma_j = \text{GS.Sign}(GSK_j, H(\boldsymbol{c_j})), \tag{18}$$

where $H(\cdot)$ is a cryptographic hash function. Fresh randomness is used in each signing operation so that signatures generated at different time instants remain unlinkable.

Each CV j transmits the pair $(\boldsymbol{c_j}, \sigma_j)$ to the roadside unit. Upon receipt, the roadside unit performs the following:

1) **Verification:** The group signature σ_j is verified using the group public key GPK. A valid signature confirms that the ciphertext originates from a legitimate group member without revealing the vehicle's identity.
2) **Aggregation:** Utilizing the homomorphic property of Paillier encryption, the roadside unit can aggregate the data. For example, the aggregate encryption for the i-th component from multiple vehicles is computed as

$$C_{\text{sum}}^i = \prod_j c_j^i \bmod n^2 = E_{PK}\left(\sum_j x_j^i; \prod_j r_j^i\right). \tag{19}$$

Note that, since fresh randomness is used for each encryption and signature, ciphertexts at different time instants are statistically independent, thus the roadside unit or any adversary cannot link $\boldsymbol{c_j}(t)$ with $\boldsymbol{c_j}(t+1)$, thereby preserving privacy.

After aggregating $\boldsymbol{C}_{\text{sum}} = [C_{sum}^0, C_{sum}^1, \cdots, C_{sum}^{|\mathcal{M}_n|}]^\top$, The roadside unit then transmits the aggregated ciphertext $\boldsymbol{C}_{\text{sum}}$ to the traffic signal control center. At the traffic signal control center, the private key sk is used to decrypt the aggregated ciphertext. Specifically, the control center computes

$$\sum_j x_j^i = D_{sk}(C_{\text{sum}}^i), \tag{20}$$

thus obtaining $\sum_j x_j$. Specific to data-fusion MP control, $\sum_j x_j$ can be $\sum_{j \in \mathcal{J}_{(i,o)}^{cv}} \tau_j(t)$ and $z_{(i,o)}^{cv}$ in (8) for each movement (i, o).

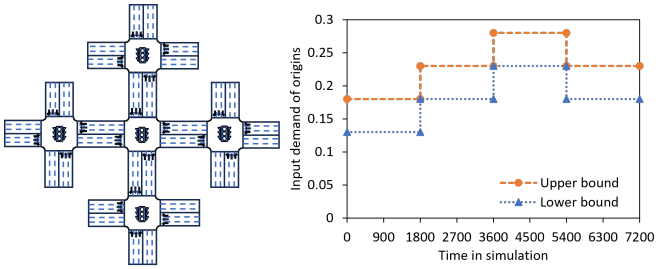

Fig. 4. Simulation at a toy network.

IV. Evaluation

As shown in Figure 4, the proposed Private-MP control is evaluated in a SUMO simulation network with five signalized intersections. Each intersection consists of four links and each link comprises three lanes for different turning directions, i.e., left turn, straight through, and right turn. The turn ratios for the straight-through and left-turn directions are centered at 0.55 and 0.25, respectively, accompanied by deviations following a normal distribution. The input demand at source links varies over time and is taken as a random number sampled uniformly in the given upper and lower bounds. Overall, the total demand of the network showed a gradual increase and then a decrease during the two-hour simulation.

Three benchmark methods are tested:

- Q-MP: the original MP controller proposed by [3], which uses the number of vehicles in movements for pressure calculation. This method uses only fixed-location detector data.
- CV-MP: a variant of Data-fusion MP uses CV data only, which does not consider the privacy issues of CVs.
- DF-MP: the proposed data-fusion MP controller utilizing both fixed-location detector data and CV data, which does not consider the privacy issues of CVs.
- Private-MP: the proposed MP controller utilizing both fixed-location detector data and CV data, where the privacy of CVs is protected by the proposed privacy-preserving mechanism under the MEC architecture. The parameter P^d for data requirement in the adaptive randomized response strategy is set as 0.5.

The results of the four benchmark methods tested at various penetration rates ranging from 0.1 to 0.9 are shown in Fig. 5(a). Compare Q-MP (based solely on fixed-location detector data) and CV-MP (relying exclusively on CV data). At lower CV penetration rates, the limited CV sample size of CV-MP

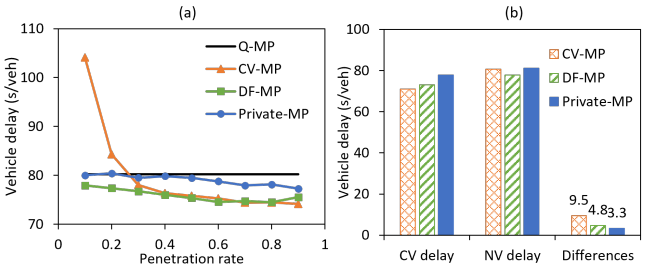

Fig. 5. Evaluation results: (a) average vehicle delay (s/veh) at different penetration rates and (b) fairness between CVs and NVs at 0.5 penetration rate.

can lead to higher vehicle delays. However, as the penetration rate increases, CV-MP benefits from more detailed traffic information provided by CVs, thereby surpassing Q-MP in terms of delay reduction. By combining the reliable volume information of fixed-location detectors with the granular, real-time information provided by CVs, DF-MP effectively reduces delays under various penetration scenarios, consistently outperforming Q-MP and CV-MP. This dual-data strategy addresses the limitations faced by methods that rely on a single data source, ensuring robust performance even when the CV penetration rate is low. As for Private-MP, it further employs a privacy-preserving mechanism in which the proposed adaptive randomized response strategy leads to less available CV data. As a result, its performance is degraded compared to DF-MP. However, it can be noted that it still outperforms Q-MP at various penetration rates. Besides, it also still achieves more robust performance in low penetration rate scenarios compared to CV-MP. This highlights the practical value of Private-MP, as it safeguards the private information of CVs by sacrificing only the limited utility of non-privacy protection methods while still outperforming traditional single-source data methods at low penetration rates.

The results of Fig. 5(b) reveal that, in scenarios where CVs constitute 50% of the traffic, the CV-MP results in the greatest disparity in delays between CVs and NVs due to its exclusive reliance on CV data. In contrast, DF-MP enhances fairness by integrating both CV and fixed-location detector data. This fusion provides a more comprehensive understanding of traffic conditions, leading to a reduction in the delay gap between CVs and NVs to half of that observed under CV-MP. Furthermore, Private-MP incorporates a privacy-preserving mechanism that utilizes only a subset of CV data. While this approach safeguards CV privacy, it further decreases the delay difference between CVs and NVs compared to DF-MP. These findings collectively highlight that employing data fusion techniques can significantly mitigate fairness issues at intersections. Moreover, implementing privacy-preserving measures, while beneficial for protecting user data, can further enhance fairness.

V. Conclusion and Future Work

This study proposed a Private-MP controller for real-time network traffic signal control while preserving CV privacy. By fusing fixed-location detector data and CV data, Private MP addresses the problem of destabilization of CV-based MP control in low penetration rate scenarios, outperforms detector-based MP control, and effectively improves fairness between CVs and NVs. Under a mobile edge computing architecture, the proposed privacy-preserving mechanism integrates homomorphic encryption and group signature techniques to protect CV data from interception, sniffing, and inference attacks, where an adaptive randomized response and a hidden matrix approach are further proposed to enhance protection.

Future work includes 1) further analyzing the effectiveness of the proposed privacy-preserving mechanism and its impact on computational and transmission efficiency, 2) theoretically demonstrating the ability of the proposed Private-MP to stabilize road network queues, and 3) testing the effectiveness of the method in more abundant scenarios.

References

[1] H. Yan, F. He, X. Lin, J. Yu, M. Li, and Y. Wang, "Network-level multiband signal coordination scheme based on vehicle trajectory data," *Transportation Research Part C: Emerging Technologies*, vol. 107, pp. 266–286, 2019.

[2] H. Wang, M. Zhu, W. Hong, C. Wang, G. Tao, and Y. Wang, "Optimizing signal timing control for large urban traffic networks using an adaptive linear quadratic regulator control strategy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 1, pp. 333–343, 2020.

[3] P. Varaiya, "Max pressure control of a network of signalized intersections," *Transportation Research Part C: Emerging Technologies*, vol. 36, pp. 177–195, 2013.

[4] P. Mercader, W. Uwayid, and J. Haddad, "Max-pressure traffic controller based on travel times: An experimental analysis," *Transportation Research Part C: Emerging Technologies*, vol. 110, pp. 275–290, 2020.

[5] L. Li and S. E. Jabari, "Position weighted backpressure intersection control for urban networks," *Transportation Research Part B: Methodological*, vol. 128, pp. 435–461, 2019.

[6] H. Liu and V. V. Gayah, "A novel max pressure algorithm based on traffic delay," *Transportation Research Part C: Emerging Technologies*, vol. 143, p. 103803, 2022.

[7] X. Wang, Y. Yin, Y. Feng, and H. X. Liu, "Learning the max pressure control for urban traffic networks considering the phase switching loss," *Transportation Research Part C: Emerging Technologies*, vol. 140, p. 103670, 2022.

[8] C. Tan, Y. Ding, K. Yang, H. Zhu, and K. Tang, "Connected vehicle data-driven robust optimization for traffic signal timing: Modeling traffic flow variability and errors," *arXiv preprint arXiv:2406.14108*, 2024.

[9] C. Tan, Y. Cao, X. Ban, and K. Tang, "Connected vehicle data-driven fixed-time traffic signal control considering cyclic time-dependent vehicle arrivals based on cumulative flow diagram," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[10] C. Tan and K. Yang, "Privacy-preserving adaptive traffic signal control in a connected vehicle environment," *Transportation research part C: emerging technologies*, vol. 158, p. 104453, 2024.

[11] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–465, 2017.

[12] T. Le, P. Kovács, N. Walton, H. L. Vu, L. L. Andrew, and S. S. Hoogendoorn, "Decentralized signal control for urban road networks," *Transportation Research Part C: Emerging Technologies*, vol. 58, pp. 431–450, 2015.

[13] M. W. Levin, J. Hu, and M. Odell, "Max-pressure signal control with cyclical phase structure," *Transportation Research Part C: Emerging Technologies*, vol. 120, p. 102828, 2020.

[14] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*. Springer, 1999, pp. 223–238.

[15] H. Huang, Y. Wu, F. Xiao, and R. Malekian, "An efficient signature scheme based on mobile edge computing in the NDN-IoT environment," *IEEE Transactions on Computational Social Systems*, vol. 8, no. 5, pp. 1108–1120, 2021.