Transportation Research Part C 191 (2026) 105848

Contents lists available at ScienceDirect

Transportation Research Part C

journal homepage: www.elsevier.com/locate/trc

Private-MP: Privacy-Preserving Max-Pressure control based on heterogeneous data fusion

Chaopeng Tan [a,b,*], Marco Rinaldi [b], Yikai Zeng [a], Meng Wang [a], Keshuang Tang [c,*], Hans van Lint [b]

[a] Chair of Traffic Process Automation, Technische Universität Dresden, Hettnerstraße 3, Dresden, 01069, Germany
[b] Department of Transport and Planning, Delft University of Technology, Gebouw 23, Stevinweg 1, Delft, 2628 CN, The Netherlands
[c] The Key Laboratory of Road and Traffic Engineering of the Ministry of Education, College of Transportation Engineering, Tongji University, No. 4800, Cao'an Road, Shanghai, 201804, China

ARTICLE INFO

Keywords:
Max-pressure control
Connected vehicle
Data fusion
Privacy preservation
Mobile edge computing

ABSTRACT

Max-pressure (MP) control has proven effective at stabilizing network queues and improving traffic throughput in large-scale urban road networks. However, conventional connected-vehicle (CV)-based MP controllers face two critical limitations: in low-CV-penetration scenarios, their performance and practical stability may be compromised by sparse observations, and significant privacy concerns arise when utilizing individual vehicle data. To address these challenges, this paper proposes a novel data-fusion MP (DF-MP) controller that fuses data from both fixed-location detectors and CVs within a mobile edge computing architecture. To protect CV privacy, including macro-route information and micro-trajectory information, a privacy-preserving mechanism that combines homomorphic encryption, group signatures, hidden-matrix encoding, and a newly proposed adaptive randomized response strategy is further integrated with DF-MP to form Private-MP. Theoretical analysis shows that the proposed DF-MP and Private-MP controllers can stabilize network queues under the fusion framework, while the privacy-preserving mechanism of Private-MP limits disclosure to the movement-wise aggregate information required for control under the stated threat model. Simulation studies on a real-world network with 28 intersections show that Private-MP outperforms traditional detector-based MP control and remains more robust than CV-based MP at low penetration rates. At the same time, the performance loss caused by privacy protection remains small: compared with DF-MP, the increase in average vehicle delay of Private-MP is generally within 4%.

1. 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 (Yan et al., 2019; Wang et al., 2020). As a result, centralized solutions can become inefficient or infeasible in practice, especially in dynamic traffic environments. In contrast, Max-pressure (MP) control, also commonly referred to as Backpressure control

* Corresponding authors.
E-mail addresses: tantantan951122@gmail.com (C. Tan), m.rinaldi@tudelft.nl (M. Rinaldi), yikai.zeng@tu-dresden.de (Y. Zeng), meng.wang@tu-dresden.de (M. Wang), tang@tongji.edu.cn (K. Tang), cj.w.c.vanlint@tudelft.nl (H. van Lint).

https://doi.org/10.1016/j.trc.2026.105848
Received 29 December 2025; Received in revised form 29 April 2026; Accepted 1 July 2026
Available online 6 July 2026

in the literature, 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 (Varaiya, 2013; Zaidi et al., 2016). This approach effectively alleviates communication and computational bottlenecks, making MP simple to implement. MP control is demonstrated to offer long-term queue stability and optimal throughput, which ensures its efficiency when the traffic flow is within the admissible demand regions (Varaiya, 2013).

Existing MP control research can be categorized into two streams: variants of MP control and extensions of MP control. The latter focuses on extending MP control to a wider range of signal control applications, such as arterial signal coordination (Xu et al., 2024; Ahmed et al., 2025), transit signal priority (Xu et al., 2022; Ahmed et al., 2024; Tan et al., 2025b), perimeter control (Liu and Gayah, 2024), and pedestrian friendly signals (Liu et al., 2024), which are outside the scope of this study and will not be discussed further.

Research on variants of MP control explores the use of different traffic state measures for pressure calculation. Early studies used aggregated traffic state information that conventional fixed-location detectors could acquire as inputs. For instance, the early Q-MP proposed by Varaiya (2013) uses queue length, which is essentially the number of vehicles on the link due to the assumption of the point queue model, for pressure calculation. Such queue length information of the internal links can be estimated by store-and-forward models when vehicle arrivals from the external links are known. As Q-MP assumes infinite queue capacities for stability analysis that deviates from the real world, Gregoire et al. (2014) proposed Capacity-Aware MP to incorporate link capacity constraints, but its impact on road network stability has not been proved. Related studies have also considered max/back-pressure control with estimated queue lengths and enhanced queue-based MP formulations under more practical traffic conditions (Li et al., 2021; Zoabi and Haddad, 2026). Nevertheless, due to the real-time fluctuation of the turning ratio, there are inevitable errors in the estimation of the queue length based on fixed-location detectors (Yao and Tang, 2019), and these errors will keep accumulating, leading to the failure of MP control.

Recent advances in connected vehicle (CV) technologies have made it possible to collect highly detailed vehicle trajectory data (e.g., position, speed, queue length) in real time, thereby enhancing traffic state estimation (Zheng and Liu, 2017; Cao et al., 2021; Tan et al., 2025e) and traffic signal control (Yao et al., 2019; Tan et al., 2025a,c; Wang et al., 2024; Tan et al., 2024) for more responsiveness and accurate of urban traffic management. MP control has also evolved from utilizing aggregated detector data to employing vehicle trajectory data. Li and Jabari (2019) proposed a position-weighted MP that uses the weighted position of vehicles for pressure calculation. On the basis of position-weighted MP, Wang et al. (2022) employed reinforcement learning to assign distinct weights to stopped and moving vehicles for optimized performance, i.e., learning-curve-based MP. Nevertheless, these studies only account for the instantaneous spatial distribution of vehicles while neglecting vehicle delays, which may cause excessive delays on minor roads with shorter queues. Therefore, some studies explored time-cumulative vehicle states for MP control. Wu et al. (2018) proposed to use the head-of-line delay as a traffic state for MP control, which can reduce delays for short queues, thus improving fairness. Mercader et al. (2020) used average travel time for pressure calculation, termed TT-MP, which has been validated in field tests. A later work conducted experimental studies on MP control based on travel time delays (Zoabi and Haddad, 2025). Liu and Gayah (2022) proposed a delay-based MP that uses vehicle delay in the last horizon for pressure calculation, and in a later study, they also used the total delay of vehicles (Liu and Gayah, 2023), though the network queue stability is unproven in the latter study. Most recently, Tan et al. (2026) proposed to use the real-time link travel time of CVs for pressure calculation, i.e., CV-MP, which pioneered the theoretical proof of network stability of MP control in partially CV environments.

However, exclusive reliance on vehicle trajectory data introduces two major concerns. First, CV-based control approaches become unreliable when the CV penetration rate is low, since temporally and spatially sparse CV data can lead to performance degradation and potential instability in control decisions (Tan et al., 2026). 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 (Tan and Yang, 2024; Tan et al., 2025d; Wang and Yang, 2024). 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 aforementioned issues, this paper first proposes a data fusion MP control (DF-MP) scheme that integrates complementary CV data with fixed-location detector data. This complementarity entails that in high-penetration scenarios, CV data provides more accurate pressure measures for MP control, while in low-penetration scenarios, detector data still offers reliable pressure measures. Subsequently, we introduce a novel framework, Private-MP, which integrates multiple privacy protection techniques within a Mobile Edge Computing (MEC) architecture. This framework enables privacy-preserving MP control, thereby safeguarding the security of macro-micro vehicle information. The major contribution is threefold:

- By fusing CV data with fixed-location detector information, the proposed DF-MP control ensures more robust performance at low CV penetration rates compared to CV-only MP controllers and provides a more accurate representation of traffic conditions than detector-only MP controllers.
- We propose a privacy-preserving mechanism in MEC architecture for MP control, i.e., Private-MP, which protects CV data in both macro-route and micro-trajectory levels.
- We rigorously prove the stability of DF-MP and Private-MP in road network queues, which is the most important theoretical property of MP-based algorithms, and demonstrate the privacy protection capabilities of Private-MP.

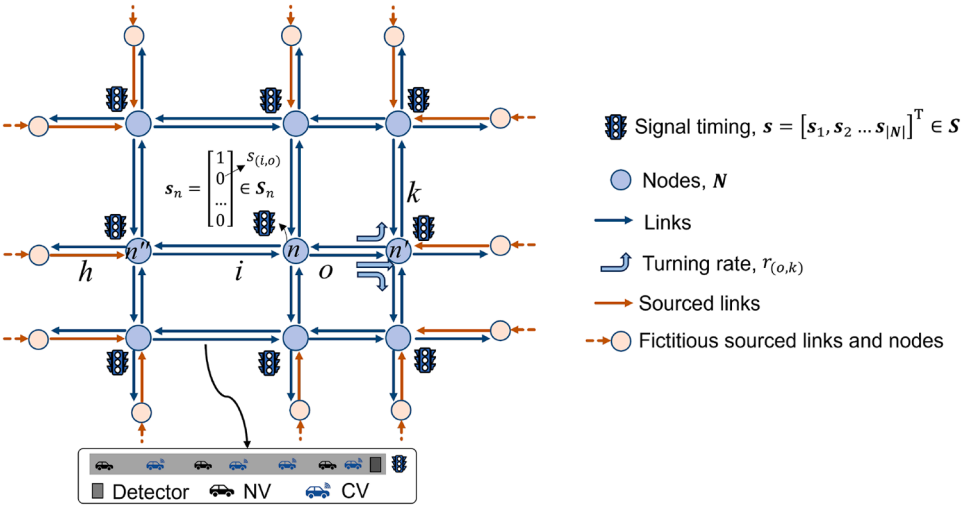

Fig. 1. Network definition.

2. Preliminaries

2.1. Network definitions

We use the notation convention as in Tan et al. (2026). 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^u, and the downstream node connecting to the outgoing link o of node n is indicated by n^d. Traffic demands are introduced from fictitious source links (no physical length) connected via fictitious source nodes $\mathcal{F}$. We write $\mathcal{M}_{\mathcal{N}}$ and $\mathcal{M}_{\mathcal{F}}$ for the sets of movements at all real and fictitious nodes, respectively. In practice, real links have limited length and a finite jam density. By contrast, a fictitious source link has no physical extent and is represented as a point queue at the source node. We assume this queue has infinite jam density; thus, its length can grow without bound. The inflow and outflow for both fictitious and real links remain finite because of the minimum time headway between vehicles.

Let $\boldsymbol{s}$ represent the overall signal vector, composed of $\boldsymbol{s}_n$ for each node n. For movement (i, o), the binary variable $s_{(i,o)}(t)$ indicates green phase activation at moment t, i.e., $s_{(i,o)}(t) = 1$ if green and $s_{(i,o)}(t) = 0$ 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 at moment t and $\boldsymbol{r} \in \mathbb{R}^{|\mathcal{M}_{\mathcal{N}}| \times |\mathcal{M}_{\mathcal{N}}|}$ denotes a matrix containing all turning ratios $r_{(i,o)}(t)$. On the incoming link of movement (i, o), let $\mathcal{J}^{cv}_{(i,o)}(t)$ be the sets of CVs at moment t indexed by j, with size $z^{cv}_{(i,o)}(t)$. The corresponding set of all vehicles, including CVs and non-CVs (NVs), is denoted by $\mathcal{J}_{(i,o)}$ with size $z_{(i,o)}$. It is assumed that low-resolution fixed-location detectors, e.g., loop detectors, are available to provide aggregated flow/count measurements for each movement over a reporting interval. In this study, we do not restrict the framework to a specific detector layout; the key assumption is that only coarse aggregated detector data are available.

2.2. 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, 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 (Abbas et al., 2017; Chen and Qiu, 2021; Wang et al., 2023).

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)

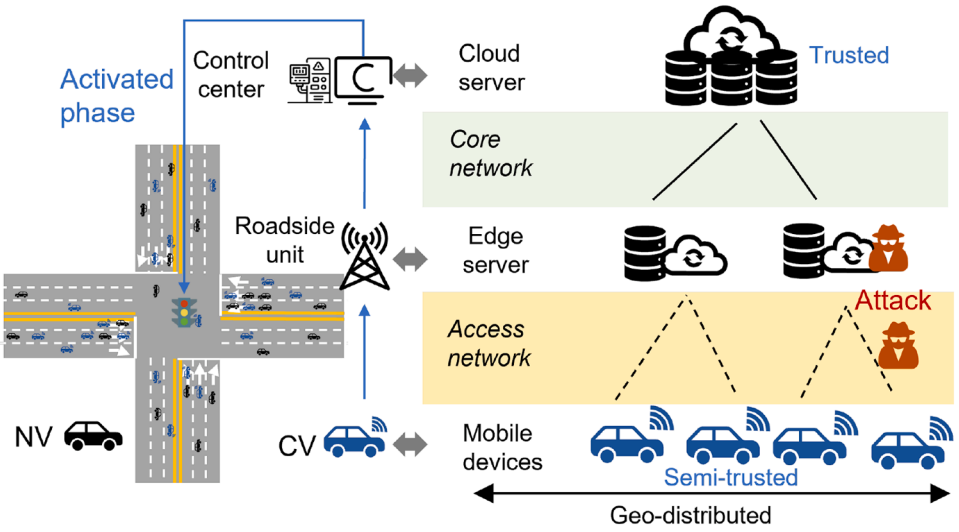

Fig. 2. Mobile edge computing architecture.

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 (Tan and Yang, 2024). 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 may be intercepted.

3. Data-fusion MP

In this section, we first briefly recall two MP control based on single data sources, i.e., detectors and CVs, respectively. Then, the proposed DF-MP is introduced to fuse detector data and CVs.

3.1. Single-data-source MP

The original MP control method, namely the basic queue-based MP in Varaiya (2013) and its weighted-queue extension, calculates movement pressure based on the number of vehicles. In its basic form, the movement weight is given by the upstream queue minus the weighted downstream queue. The same paper further proposes a weighted-queue extension that uses link-length-based weighting to account for heterogeneous link lengths. In this study, we adopt this weighted formulation and write the controller as follows:

$$s^*(t) = \arg\max_{s\in S} \sum_{n\in\mathcal{N}} \Big(\sum_{\forall(i,o)\in\mathcal{M}_n} s_{(i,o)}(t) c_{(i,o)} \big(\frac{z_{(i,o)}(t)}{L_i} - \sum_{(o,\forall k)\in\mathcal{M}_{n^d}} r_{(o,k)}(t) \frac{z_{(o,k)}(t)}{L_o} \big) \Big), \tag{1}$$

where $z_{(i,o)}(t)$ denotes the number of vehicles and $r_{(i,o)}$ denotes the turning ratio of movement (i,o), respectively. L_i denotes the link length. The inner parentheses compute the difference in traffic state between the incoming link and outgoing link for the movement (i,o). The movement pressure is calculated by multiplying the traffic-state difference by the corresponding saturation flow rate $c_{(i,o)}$. The factor $1/L_i$ is introduced to reflect heterogeneous link lengths in a simple manner and to assign relatively higher priority to shorter links, which are generally more vulnerable to spillback and spillover. For simplicity, we hereafter refer to this weighted queue-based implementation as Q-MP.

A major advantage of Q-MP is that it can be applied under conventional traffic detection conditions, as $z_{(i,o)}(t)$ can be easily estimated using loop detector data deployed at intersections. 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 (Varaiya, 2013) as below:

$$z_{(i,o)}(t+1) = z_{(i,o)}(t) + a_{(i,o)}(t) - d_{(i,o)}(t), \tag{2}$$

where $z_{(i,o)}(t)$ denotes the number of vehicles (i.e., the queue, as the spatial vehicle distribution is ignored) of movement (i,o) at time step t. $a_{(i,o)}(t)$ denotes the arrival vehicles and $d_{(i,o)}(t)$ denotes the departure vehicles, i.e.,

$$a_{(i,o)}(t) = e_{(i,o)}(t) + \sum_{(\forall h,i)\in\mathcal{M}_{n^u}} r_{(i,o)} d_{(h,i)}(t), \tag{3}$$

$$d_{(i,o)}(t) = \min\{z_{(i,o)}(t), s_{(i,o)}(t) c_{(i,o)}\}. \tag{4}$$

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, we have the arrival vehicles from other links $\sum_{(\forall h,i)\in\mathcal{M}_{n^u}} r_{(i,o)} d_{(h,i)}(t) = 0$ due to the absence of the upstream intersection, while for non-source links, the exogenous arrivals $e_{(i,o)}(t) = 0$. In Eq. (2)-(4), $s_{(i,o)}(t)$ 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 calibrated by historical detector data (or updated at regular sampling periods) as below:

$$e_{(i,o)}(t) = \bar{\lambda}_{(i,o)} T \quad \text{for source links,} \tag{5}$$

$$r_{(i,o)} = \frac{\bar{\lambda}_{(i,o)}}{\sum_{(i,\forall o)\in\mathcal{M}_n} \bar{\lambda}_{(i,o)}}, \tag{6}$$

where $\bar{\lambda}_{(i,o)}$ is the average flow rate collected by fixed-location detectors and T is the decision horizon. Thus, the number of vehicles $z_{(i,o)}(t)$, including CVs and NVs, can be estimated by Eq. (2) based on fixed-location detector data. However, as indicated by Eq. (2)–(6), the estimation of $z_{(i,o)}(t)$ is inherently subject to systematic modeling errors. These errors mainly arise because the turning ratios are approximated by average values rather than the true time-varying turning behavior, the exogenous arrivals are represented by average rates rather than realized short-term arrivals, and the store-and-forward model neglects the detailed within-link spatial distribution of vehicles. Since $z_{(i,o)}(t)$ is updated recursively over time, such approximation errors may propagate and accumulate, ultimately degrading the performance of MP-based control and, in severe cases, compromising network stability.

These issues become even more critical in the low-resolution detector setting considered in this study, where measurements are available only as aggregated counts at the detector reporting interval (e.g., 60 s). In this case, the arrival and departure terms can only be refreshed when new detector data becomes available, while the queue state between two detector updates must be inferred using the last interval arrival rate, the signal state, and the store-and-forward dynamics. As a result, the state estimation becomes less responsive to short-term traffic fluctuations, and the mismatch between the estimated and actual queue lengths can be further amplified. Moreover, even if queue lengths were estimated accurately, Q-MP still has an inherent limitation in that it ignores vehicle delay. At intersections with significant demand imbalances, this may lead to excessive delay for shorter queues, because the controller tends to allocate green time repeatedly to longer queues.

Recent advances in CV technologies have facilitated the development of MP control by providing detailed vehicle trajectories. Rather than using the number of vehicles, CV-MP (Tan et al., 2026) uses the link travel time of CVs for pressure calculation, which captures vehicle delays. Regarding each CV j of movement (i, o), $\tau_j(t)$ is used to denote its link travel time at the decision moment t:

$$\tau_j(t) = t - t_j^0, \tag{7}$$

where t_j^0 is the moment when CV j entered the link. Then, CV-MP (Tan et al., 2026) applies as follows:

$$\boldsymbol{s}^*(t) = \arg\max_{\boldsymbol{s}\in\boldsymbol{S}} \sum_{n\in\mathcal{N}} \Big(\sum_{\forall(i,o)\in\mathcal{M}_n} s_{(i,o)}(t) c_{(i,o)} \big(\tau^{cv}_{(i,o)} - \sum_{(o,\forall k)\in\mathcal{M}_{n^d}} r_{(o,k)}(t) \tau^{cv}_{(o,k)}\big)\Big), \tag{8}$$

where

$$\tau^{cv}_{(i,o)} = \sum_{j\in\mathcal{J}^{cv}_{(i,o)}} \frac{\tau_j(t)}{\bar{\tau}_{(i,o)}}$$

and $\bar{\tau}_{(i,o)}$ is the free-flow link travel time of the corresponding movement.

Although CV-MP has been shown to outperform Q-MP in overall network performance, achieving lower vehicle delays and fewer spillbacks (Tan et al., 2026), its effectiveness critically depends on sufficiently informative CV observations. When CV penetration is low, sparse CV trajectories may leave some links or movements unobserved for extended periods, causing CV-MP to miss the corresponding traffic pressure. As shown by Tan et al. (2026), the stability of CV-only-based MP control in imperfect CV environments requires that a congested movement be effectively observed before spillover occurs; otherwise, the absence of pressure information may lead to queue starvation and ultimately destabilize the network (see Theorem 5 in Tan et al. (2026)).

3.2. Proposed DF-MP

To overcome the aforementioned limitations of both detector-based and CV-based MP control, this study proposes a data-fusion-based MP control framework, termed DF-MP, that jointly exploits detector data and CV data. Different from conventional MP formulations that use queue length or vehicle counts, DF-MP adopts link travel time as the traffic state measure. Compared with CV-MP, which uses travel time of CV observations only, the proposed DF-MP further fuses the travel times of NVs inferred from loop detector data. In this way, DF-MP can provide a more robust and comprehensive characterization of traffic conditions, especially when CV observations are sparse.

Since the detectors are assumed to be low-resolution to make the proposed method applicable to a wider range of real-world environments, the following assumptions are made for travel-time estimation based on detector data: i) due to the traffic dynamics based on the store-and-forward model, vehicles on the links are assumed to be queues with no spatial variation within the link; ii) the queues are assumed to accumulate at the downstream end of links (i.e., near the stopline) in a point-queue sense, so that a simplified analytical approximation of total delay can be constructed from the queue estimate and the arrival rate. It should be clarified that these assumptions align with those of Varaiya (2013), who assumed infinite link length, employed the number of vehicles on the link as a queuing metric to demonstrate stability, and derived traffic dynamics using the store-and-forward model.

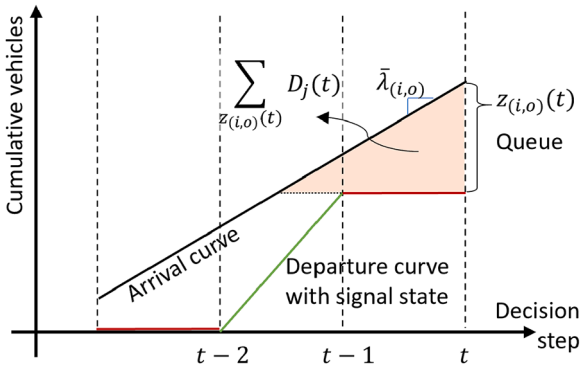

Fig. 3. The total delay estimated by detector data.

Given these assumptions, the total travel time of all vehicles, i.e., $\tau_{(i,o)}$, can be estimated as

$$\tau_{(i,o)}(t) = \sum_{j=1}^{z_{(i,o)}(t)} \left(\bar{\tau}_{(i,o)} + D_j(t)\right) \tag{9}$$

where D_j denotes the delay of vehicle j. Here, the vehicle link travel time is decomposed into the free-flow travel time $\bar{\tau}_{(i,o)}$ and the delay $D_j(t)$.

Since low-resolution detectors provide only aggregated counts at discrete reporting times, the detailed arrival pattern within each detector reporting interval cannot be directly observed. We therefore approximate arrivals over the detection range as uniform within each detector update interval, using an average arrival rate $\bar{\lambda}_{(i,o)}$ obtained from the most recent detector measurement. Importantly, the detector reporting interval is not the same as the MP decision interval. Although $\bar{\lambda}_{(i,o)}$ is refreshed only when new detector data becomes available, the queue length, delay, and travel-time estimates are updated at every decision step using the current traffic state and signal timing information. For example, if detectors report every 60 seconds while MP decisions are made every 15 seconds, the same detector-based arrival rate is used within the 60-second reporting interval, but the queue and delay estimates are still recalculated every 15 seconds.

Accordingly, at each decision step t, the queue length $z_{(i,o)}(t)$ is first obtained from Eq. (2). Given this queue estimate and the latest available $\bar{\lambda}_{(i,o)}$, the real-time delay is approximated using a triangular-area formulation (Webster, 1958), as illustrated in Fig. 3. This local approximation allows the detector-based term to serve as a lightweight and dynamically updated surrogate for real-time MP control under low-resolution detector settings, rather than as an exact physical delay model.

$$\sum_{j=1}^{z_{(i,o)}(t)} D_j(t) = \frac{z_{(i,o)}(t)^2}{2\bar{\lambda}_{(i,o)}} \tag{10}$$

Then, the expected total travel time of NVs is estimated as

$$\tau^{nv}_{(i,o)}(t) = (1-p)\tau_{(i,o)}(t) = (1-p)\left(z_{(i,o)}(t)\bar{\tau}_{(i,o)} + \frac{z_{(i,o)}(t)^2}{2\bar{\lambda}_{(i,o)}}\right) \tag{11}$$

where p is the average penetration rate of CVs. Specifically, we assume that the average penetration rate p of the network is known, as this parameter can be readily obtained based on the historical detector data and CV counts observed over time.

Fusing the total travel time of NVs estimated by detector data and the total travel time of CVs, the DF-MP is written as follows:

$$\boldsymbol{s}^*(t) = \arg\max_{\boldsymbol{s}\in\boldsymbol{S}} \sum_{n\in\mathcal{N}} \left(\sum_{\forall(i,o)\in\mathcal{M}_n} s_{(i,o)}(t) c_{(i,o)} \left(\phi_{(i,o)}(t) - \sum_{(o,\forall k)\in\mathcal{M}_{nd}} r_{(o,k)}(t)\phi_{(o,k)}(t)\right)\right), \tag{12}$$

where $\phi_{(i,o)}(t)$ actually denotes the total link travel time of the movement by data fusion and

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

A significant advantage of DF-MP lies in its ability to overcome the limitations of single-data-source MP methods by fusing detector data with CV data. Compared to Q-MP, the CV information in DF-MP provides more reliable travel time observations, reducing the impact of cumulative estimation errors in detector-based traffic-state approximation. Compared to CV-MP, DF-MP avoids control failures caused by missing CV data in low-penetration-rate scenarios by relying on point detector data. This complementarity is particularly important because the detector data considered here are low-resolution aggregated measurements with limited temporal resolution, whereas CV data provide finer and more up-to-date travel-time observations. Moreover, MP control determines the signal decision by comparing the pressure values of competing movements and activating the one with the maximum pressure. Hence,

the controller is more sensitive to whether the adopted state measure can reasonably preserve the relative ordering of movement congestion levels than to whether it provides an exact physical delay value. This makes the MP framework relatively robust to moderate approximation errors in the detector-side surrogate, while the fusion with real-time CV observations further mitigates such errors. In Section 5, we will further prove that DF-MP can still stabilize network queues. In two extreme cases: (i) if all vehicles are CVs, then we have $\tau^{nv}_{(i,o)} = 0$ as $1 - p = 0$ and the proposed MP controller becomes a complete CV-based MP controller; (ii) if no vehicle is CV, then it becomes a detector-based travel-time MP controller that relies only on detector data and considers vehicle delay factors. The same detector-based controller is also the $p = 0$ case of Private-MP in Section 4, since no CV information is available and the privacy mechanism does not affect the control input.

Remark 1 (Confidence coefficient of estimates by detectors)**.** In practice, if the average accuracy $0 \le \gamma \le 1$ of the estimates of $z_{(i,o)}$ is pre-evaluated, an accuracy-related confidence coefficient ϱ_γ, e.g., $\varrho_\gamma = \gamma^2$, can be introduced for the final estimate of $\phi_{(i,o)}$, i.e.,

$$\phi_{(i,o)}(t) = \varrho_\gamma \frac{\tau^{nv}_{(i,o)}(t)}{\bar{\tau}_{(i,o)}} + \sum_{j \in \mathcal{J}^{cv}_{(i,o)}} \frac{\tau_j(t)}{\bar{\tau}_{(i,o)}}. \tag{13}$$

This is because, in comparison, the travel time estimated by the detector is significantly affected by the accuracy of the queue length estimate, while the CV travel time observation is relatively accurate. In the final travel time estimate, we enhance the influence of the CV observation by introducing this confidence coefficient.

4. Private-MP

As discussed above, although CV data can enhance traffic management through detailed vehicle trajectories, they also raise substantial privacy concerns. Macroscopic routes may reveal personal travel patterns, while microscopic trajectory-related quantities may expose sensitive driving behavior. Therefore, on the basis of DF-MP, we further propose Private-MP, a privacy-aware extension that protects both macro-route and micro-trajectory information of CVs while still providing the movement-wise aggregate statistics required by MP control.

Before introducing the technical details, we briefly summarize the idea of Private-MP in plain terms. The goal of Private-MP is not to hide all system information, but to ensure that the controller only receives the movement-wise aggregate quantities required for pressure calculation, rather than individual vehicle data. To this end, Private-MP combines three standard privacy-preserving building blocks, additively homomorphic encryption, group signatures, and hidden-matrix encoding, with a new adaptive randomized response (ARR) strategy proposed in this paper. The standard building blocks protect the content of uploaded messages, while ARR reduces the chance that repeated uploads can be linked into a vehicle route. Since ARR also reduces the amount of shared CV data, the detector-based component of DF-MP is used to compensate for the resulting loss of usable CV observations.

4.1. Threat model

When entering a link, CVs record and store the moment t^0_j. At the decision moment t, CVs compute their link travel time τ_j based on Eq. (7). For MP control, the system only needs to obtain, for each movement, the aggregate of shared travel-time contributions. However, if vehicles directly upload their individual link travel times and turning intentions, an observer may combine these pieces of information across intersections to infer sensitive trajectory information. Therefore, the design objective of Private-MP is to let the controller obtain only the movement-wise aggregates required by Eq. (12), while limiting disclosure of individual vehicle data under the considered threat model.

During the process, CVs share two types of information with the roadside unit: link travel time and turning intention. Although link travel time does not explicitly reveal the full trajectory, it is still sensitive information about individual vehicles. Combined with turning intention, it may 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 consider a semi-honest setting with the following parties:

- **Vehicles:** All vehicles are honest and do not collude or leak their secret keys.
- **Edge servers:** Adversary $\mathcal{A}_{\text{edge}}$ may fully observe and control all edge servers. It sees all data stored on edge servers.
- **Cloud server:** Adversary $\mathcal{A}_{\text{cloud}}$ controls the cloud server. It follows the protocol (semi-honest) but attempts to infer additional information.
- **External eavesdropper:** A network adversary sees all messages on the communication channels but cannot modify them.

The adversarial goals include recovering individual $\tau_j(t)$ beyond what is implied by aggregate movement statistics, reconstructing the route of a particular vehicle over the network, or recovering the specific turning movement at a given node and time. To address these threats while still preserving the movement-wise aggregate information required by MP control, Private-MP combines several privacy-preserving building blocks, which are introduced next.

4.2. Privacy-preserving building blocks

This subsection introduces the building blocks used in Private-MP. Additionally, homomorphic encryption, group signatures, and hidden-matrix encoding are standard privacy-preserving tools, while the adaptive randomized response (ARR) strategy is the new

component proposed in this paper. For the standard tools, we only retain the properties needed by the protocol; more technical definitions can be moved to Appendix A.

4.2.1. Standard privacy-preserving tools

Additively homomorphic encryption.. We use an additively homomorphic encryption scheme

$$\mathsf{HE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}), \tag{14}$$

where pk and sk denote the public key and secret key, respectively. The scheme has the property that ciphertexts can be aggregated without decryption:

$$\mathsf{Enc}(pk, m_1) \circ \mathsf{Enc}(pk, m_2) = \mathsf{Enc}(pk, m_1 + m_2), \tag{15}$$

where m_1 and m_2 are plaintext messages, and $\circ$ denotes the ciphertext-side aggregation operation corresponding to plaintext addition. Thus, the edge server can compute movement-wise sums directly on ciphertexts, while only the cloud holding the secret key sk can decrypt the aggregated result. In Private-MP, this property is used to aggregate encrypted travel-time contributions without revealing the individual values. Any additively homomorphic cryptosystem can be used here, e.g., the Paillier cryptosystem (Paillier, 1999).

Group signatures.. We use a group signature scheme

$$\mathsf{GS} = (\mathsf{GS.Setup}, \mathsf{GS.Join}, \mathsf{GS.Sign}, \mathsf{GS.Verify}, \mathsf{GS.Open}), \tag{16}$$

where gpk denotes the group public key. This mechanism is used to ensure that uploaded messages come from authorized vehicles while preventing ordinary verifiers from linking a valid upload to a specific vehicle identity. In Private-MP, the protocol only uses two properties of GS: *authenticity* (to reject invalid uploads) and *anonymity/unlinkability* (to reduce identity leakage from message authentication) (Bellare et al., 2003; Perera et al., 2022).

Hidden-matrix encoding. For each node n, let $\mathcal{M}_n$ denote the set of all possible movements. For a vehicle j contributing a private value x_j to movement $(i, o) \in \mathcal{M}_n$, we define a hidden vector

$$\boldsymbol{X}_j^n = [x_j^1, x_j^2, \dots, x_j^{|\mathcal{M}_n|}]^\top = [0, \dots, x_j, \dots, 0]^\top \in \mathbb{Z}^{|\mathcal{M}_n|}, \tag{17}$$

where $|\mathcal{M}_n|$ is the number of possible movements at node n. This vector can be written as

$$\boldsymbol{X}_j^n = \mathsf{HM}(n, (i, o), x_j). \tag{18}$$

Only the entry corresponding to movement (i, o) is non-zero. By itself, this encoding does not hide the movement, because the non-zero position reveals it. In Private-MP, it is therefore always combined with encryption:

$$\boldsymbol{C}_j^n = \mathsf{Enc}(pk, \boldsymbol{X}_j^n),$$

where $\boldsymbol{C}_j^n$ denotes the encrypted hidden vector of vehicle j at node n. In this way, the protocol can aggregate movement-wise contributions without exposing individual turning intentions in plaintext (Tan and Yang, 2024).

4.2.2. Adaptive randomized response

Even if CV data are encrypted, an adversary may still infer a vehicle's macro route by linking its repeated uploads across intersections. To reduce this risk, we propose an *adaptive randomized response* (ARR) strategy. ARR is designed to satisfy the following three requirements:

- **R1 Sharing requirement.** Each CV independently decides whether to share data at intersection n based on an intersection-dependent probability. The decision depends only on whether it shared at the previous intersection, which keeps the rule lightweight and suitable for MEC implementation.
- **R2 Privacy requirement.** The probability that a CV shares data at two consecutive intersections does not exceed P^p. This parameter controls route-linkage risk.
- **R3 Data requirement.** Each intersection requires that at least a proportion P^d of CVs share data on average, in order to support CV-enhanced MP control.

For each vehicle j, node n, and time t, we denote the realized sharing decision by

$$b_{j,n,t} \sim \mathsf{ShareProb}(j, n, t), \tag{19}$$

where $b_{j,n,t} \in \{0, 1\}$ indicates whether vehicle j shares data at node n and time t. The decision $b_{j,n,t}$ is sampled according to an ARR strategy parameterized by a sharing probability $P_j^n \in [0, 1]$, whose value depends on whether the vehicle shared at the previous intersection.

$$P_j^n = \begin{cases} P^p, & \text{if the vehicle shared data at the previous intersection,} \\ \dfrac{P^d(1 - P^p)}{1 - P^d}, & \text{if the vehicle did NOT share data at the previous intersection.} \end{cases} \tag{20}$$

Steady state of ARR.. To show that such a strategy can satisfy requirements **R1–R3**, we model the sharing decision as a two-state Markov chain, where S_j denotes that CV j shares data and N_j denotes that it does not share data. Under this design, the conditional probabilities are

$$\Pr(S_j^n \mid S_j^{n-1}) = P_j^{n,1}, \tag{21}$$

$$\Pr(N_j^n \mid S_j^{n-1}) = 1 - P_j^{n,1}, \tag{22}$$

$$\Pr(S_j^n \mid N_j^{n-1}) = P_j^{n,2}, \tag{23}$$

$$\Pr(N_j^n \mid N_j^{n-1}) = 1 - P_j^{n,2}. \tag{24}$$

Requirement **R2** implies $P_j^{n,1} \le P^p$.

Let $\pi = [\pi_S,\ \pi_N]$ denote the long-run proportions of sharing and non-sharing states. In steady state,

$$\pi = \pi T_{ARR} \quad \text{and} \quad T_{ARR} = \begin{bmatrix} P_j^{n,1} & 1 - P_j^{n,1} \\ P_j^{n,2} & 1 - P_j^{n,2} \end{bmatrix}. \tag{25}$$

Solving $\pi = \pi T_{ARR}$ together with $\pi_S + \pi_N = 1$ gives

$$\pi_S = \frac{P_j^{n,2}}{P_j^{n,2} + 1 - P_j^{n,1}}, \quad \pi_N = \frac{1 - P_j^{n,1}}{P_j^{n,2} + 1 - P_j^{n,1}}. \tag{26}$$

To satisfy **R3**, we set $\pi_S = P^d$ in steady state. To maximize data utility under **R2**, we take $P_j^{n,1} = P^p$. Substituting these into (26) yields

$$P_j^{n,2} = \frac{P^d(1 - P^p)}{1 - P^d}. \tag{27}$$

Therefore, the ARR strategy for each CV j is

$$P_j^n = \begin{cases} \Pr(S_j^n \mid S_j^{n-1}) = P^p, & \text{if } S_j^{n-1}, \\ \Pr(S_j^n \mid N_j^{n-1}) = \dfrac{P^d(1 - P^p)}{1 - P^d}, & \text{if } N_j^{n-1}, \end{cases} \tag{28}$$

with steady-state overall sharing level $\pi_S = p^d$ and $\pi_N = 1 - p^d$.

Since $P_j^{n,2}$ must be a probability, we require

$$P^p \in \left[\max\left(0, \frac{2P^d - 1}{P^d}\right),\ 1\right], \quad 0 < P^d < 1. \tag{29}$$

The above derivation shows that the proposed ARR strategy satisfies the three requirements by construction: P^d determines the steady-state sharing level required for control, while P^p limits the probability of consecutive sharing required for privacy. A useful interpretation is that P^d mainly controls the average amount of CV information available to the controller, while P^p mainly controls the persistence of consecutive sharing. Thus, the former is more directly related to control performance, whereas the latter is more directly related to route-linkage risk.

4.3. Proposed privacy-preserving mechanism

With the above building blocks in place, we now describe how Private-MP operates in one control cycle. The key idea is that vehicles do not reveal their individual travel times or turning intentions directly; instead, they contribute encrypted movement-wise values that can be aggregated and then used for MP control.

Recall that DF-MP requires CVs to provide movement-wise travel-time contributions for pressure calculation. The proposed privacy-preserving mechanism is presented in Fig. 4. It consists of three components: **C1** – adaptive randomized response (ARR), **C2** – hidden matrix (HM), and **C3** – homomorphic encryption with group signature (HE + GS). These components are selected according to the structure and requirements of MP control. Since the pressure calculation only requires movement-wise additive aggregates, the hidden matrix is used to encode movement-specific contributions, while homomorphic encryption is used because the required aggregation operation is addition. Meanwhile, ARR controls how many CVs contribute to the aggregate and therefore directly affects the effective observation rate used by the controller. Reducing CV sharing helps protect macro-route privacy, but it also lowers the amount of usable CV information. In a CV-only controller, this would increase the risk of sparse-observation failure on congested movements. By contrast, the proposed data-fusion structure compensates for this privacy-induced reduction through detector data, thereby allowing privacy protection and robust MP control to be achieved jointly.

For each node n, time t, and vehicle j:

1. **C1 – Adaptive Randomized Response:** Vehicle j samples

   $$b_{j,n,t} \in \{0, 1\}$$

   according to $\mathsf{ShareProb}(j, n, t)$. If $b_{j,n,t} = 0$, it does not upload data at (n, t).

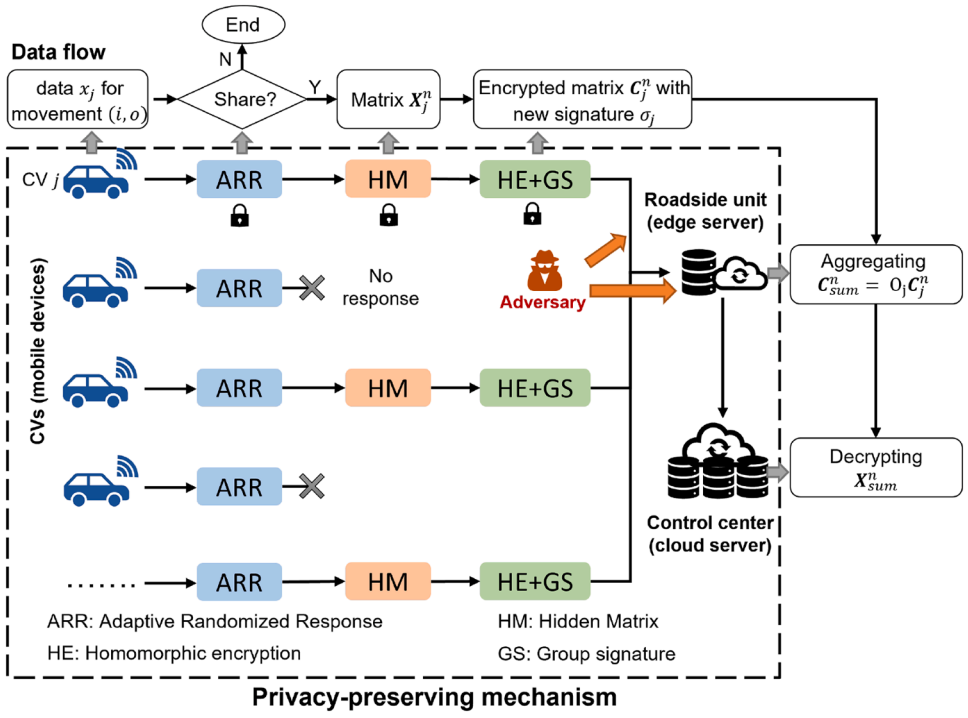

Fig. 4. The proposed privacy-preserving mechanism with **C1** – ARR, **C2** – HM, and **C3** – HE + GS.

2. **C2 – Hidden Matrix Encoding:** If $b_{j,n,t} = 1$, vehicle j computes

$$\boldsymbol{X}_j^n(t) = \mathsf{HM}(n,(i,o),x_j) \in \mathbb{Z}^{|\mathcal{M}_n|},$$

where all entries are 0 except the one corresponding to movement (i,o), which is set to x_j.

3. **C3 – Homomorphic Encryption and Group Signature:** Vehicle j encrypts $\boldsymbol{X}_j^n(t)$ element-wise under pk:

$$\boldsymbol{C}_j^n(t) = \mathsf{Enc}(pk, \boldsymbol{X}_j^n(t)).$$

It then computes a group signature

$$\sigma_j^n(t) \leftarrow \mathsf{GS.Sign}\big(gsk_j, (\boldsymbol{C}_j^n(t), n, t)\big)$$

and sends $(\boldsymbol{C}_j^n(t), \sigma_j^n(t))$ to the edge server at node n.

Upon receiving all messages at (n,t), the edge server first verifies each signature via

$$\mathsf{GS.Verify}(gpk, (\boldsymbol{C}_j^n(t), n, t), \sigma_j^n(t)),$$

then aggregates the ciphertexts homomorphically (entry-wise):

$$\boldsymbol{C}_{\text{sum}}^n(t) = \bigcirc_{j:b_{j,n,t}=1} \boldsymbol{C}_j^n(t),$$

and finally forwards $\boldsymbol{C}_{\text{sum}}^n(t)$ to the cloud control center. When many ciphertexts are aggregated, $\bigcirc_j c_j$ denotes the iterated homomorphic operation over the vehicle index set j.

The cloud control center holds the secret key sk and decrypts

$$\boldsymbol{X}_{\text{sum}}^n(t) \leftarrow \mathsf{Dec}(sk, \boldsymbol{C}_{\text{sum}}^n(t)),$$

obtaining the aggregated movement statistics, which are used by DF-MP (denoted *Private-MP*) at the corresponding intersection, since

$$\{\boldsymbol{X}_{\text{sum}}^n(t)\}_{(i,o)} = \sum_{b_{j,n,t}=1,\, j\in\mathcal{J}_{(i,o)}^{cv}} x_j(t) = \sum_{b_{j,n,t}=1,\, j\in\mathcal{J}_{(i,o)}^{cv}} \tau_j(t). \tag{30}$$

During the protocol, the cloud never receives individual ciphertexts $\boldsymbol{C}_j^n(t)$.

4.4. Private-MP controller

The steady-state result of ARR directly changes the control input of Private-MP. Under DF-MP, a proportion p of vehicles are represented by CV observations on average. Under Private-MP, however, only a proportion pP^d of vehicles are represented in the

shared CV sample in steady state. Therefore, the detector-side compensation term must cover the traffic not represented in the shared CV sample, including both NVs and CVs that do not upload under ARR. For notational consistency, we still denote this term by $\tau^{nv}_{(i,o)}$, although under Private-MP it should be interpreted more generally as the detector-based compensation for the unobserved portion of traffic:

$$\tau^{nv}_{(i,o)}(t) = (1 - p \cdot P^d)\left(z_{(i,o)}(t)\bar{\tau}_{(i,o)} + \frac{z_{(i,o)}(t)^2}{2\bar{\lambda}_{(i,o)}} \right). \tag{31}$$

This expression shows that the privacy requirement directly changes the effective traffic-state input used by the controller through the factor P^d. In particular, reducing CV sharing improves macro-route privacy but also lowers the amount of usable CV information. The detector-based component compensates for this reduction and prevents the controller from becoming overly sensitive to sparse CV observations.

Accordingly, the final signal decision of Private-MP is made by applying the same DF-MP structure to the privacy-aware effective input:

$$\boldsymbol{s}^*(t) = \arg\max_{\boldsymbol{s}\in\boldsymbol{S}} \sum_{n\in\mathcal{N}} \Big(\sum_{\forall(i,o)\in\mathcal{M}_n} s_{(i,o)}(t) c_{(i,o)} \big(\phi^{\text{private}}_{(i,o)}(t) - \sum_{(o,\forall k)\in\mathcal{M}_{n^d}} r_{(o,k)}(t) \phi^{\text{private}}_{(o,k)}(t) \big) \Big), \tag{32}$$

where

$$\phi^{\text{private}}_{(i,o)}(t) = \frac{\tau^{nv}_{(i,o)}(t)}{\bar{\tau}_{(i,o)}} + \sum_{b_{j,n,t}=1,\, j\in\mathcal{J}^{cv}_{(i,o)}} \frac{\tau_j(t)}{\bar{\tau}_{(i,o)}}. \tag{33}$$

Note that the MP control itself involves only additive aggregation for pressure calculation and a final maximization over feasible phases. In Private-MP, the main aggregation step, i.e., the computation of total shared CV travel time per movement, is carried out at the edge server in encrypted form, while the cloud only performs lightweight post-decryption operations together with the detector-based compensation term. This MEC architecture avoids frequent raw-data interaction between massive mobile devices and the cloud, while remaining compatible with the privacy-preserving protocol above.

5. Stability and privacy analysis

This section summarizes the two analytical properties most relevant to the paper: queue stability and privacy protection. For readability, we only keep the main idea of the stability proof in the main text, while the detailed derivation is moved to Appendix B. The privacy analysis is presented focusing on what each party can observe and what remains protected under the stated threat model.

5.1. Network queue stability

In terms of control policy, Private-MP is essentially DF-MP with a smaller effective CV sample and a correspondingly larger detector-side compensation term. Therefore, the two controllers share the same stability argument, and it is sufficient to analyze DF-MP.

We first state the main result and then sketch its proof.

Proposition 1 (Stability of DF-MP and Private-MP). *Given the admissible demand region $\boldsymbol{\Lambda}$, if the exogenous demand $\lambda \in \boldsymbol{\Lambda}^{\text{int}}$, then DF-MP and Private-MP can strongly stabilize the traffic network queues.*

The proof follows the standard Lyapunov-drift framework used in the MP literature (Li and Jabari, 2019; Tan et al., 2026). In particular, if there exist constants $0 < K < \infty$ and $0 < \epsilon' < \infty$ such that

$$\mathbb{E}^{\rho(t)}\left(\frac{\mathrm{d}V(\boldsymbol{\rho}(t))}{\mathrm{d}t} \right) \le K - \epsilon' \mathbb{E}\left(\sum_{(i,o)\in\mathcal{M}_{F\cup N}} z_{(i,o)}(t) \right), \tag{34}$$

then the network queues are strongly stable.

As in the literature, the admissible demand region is

$$\boldsymbol{\Lambda} = \{ \lambda \mid \lambda \preceq (\boldsymbol{I} - \boldsymbol{r})\boldsymbol{c}\bar{\boldsymbol{s}}, \exists \bar{\boldsymbol{s}} \in \boldsymbol{S}^{co} \}, \tag{35}$$

and for any $\lambda \in \boldsymbol{\Lambda}^{\text{int}}$, there exists $\epsilon > 0$ such that

$$\lambda - (\boldsymbol{I} - \boldsymbol{r})\boldsymbol{c}\bar{\boldsymbol{s}} \preceq -\epsilon \mathbf{1}. \tag{36}$$

The key difference from existing CV-MP proofs is that DF-MP uses a *composite* pressure measure rather than a pure CV-based one. For $(i,o) \in \mathcal{M}_N$, its traffic state can be written as

$$\phi_{(i,o)}(t) = (1-p) z_{(i,o)}(t) + \left(\frac{1-p}{2\bar{\lambda}_{(i,o)}\bar{\tau}_{(i,o)}} \right) z_{(i,o)}(t)^2 + \tau^{cv}_{(i,o)}(t). \tag{37}$$

This motivates a different Lyapunov construction from that of CV-MP.

Specifically, we define the composite weight

$$\varphi_{(i,o)}(x,t)=\begin{cases}0, & x=0,\\ \theta_1+\theta_2 z_{(i,o)}(t)+\theta_3\tau_{(i,o)}(x,t), & x\in(0,L_i],\end{cases} \tag{38}$$

with $\theta_1=1-p$, $\theta_2=(1-p)/(2\bar{\lambda}_{(i,o)}\bar{\tau}_{(i,o)})$, and $\theta_3=p$, and introduce the Lyapunov function

$$V(\boldsymbol{\rho}(t))\equiv\frac{1}{2}\sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}}\int_0^{L_i}\int_0^{L_i}\big(\varphi_{(i,o)}(x,t)+\varphi_{(i,o)}(x',t)\big)\rho_{(i,o)}(x,t)\rho_{(i,o)}(x',t)\,\mathrm{d}x'\mathrm{d}x +\frac{1}{2}\sum_{(i,o)\in\mathcal{M}_F}\rho_{(i,o)}(t)^2. \tag{39}$$

This Lyapunov function matches the fused pressure structure in (37); this is the main technical difference from the existing CV-MP stability proof.

The corresponding MP policy can be written in matrix form as

$$\boldsymbol{s}^*(t)=\arg\max_{\boldsymbol{s}\in\boldsymbol{S}}\boldsymbol{\phi}^\top(\boldsymbol{I}-\boldsymbol{r})\boldsymbol{c}\,\boldsymbol{s}. \tag{40}$$

Using the continuity equations and the boundedness properties of $\varphi_{(i,o)}(x,t)$, the Lyapunov drift can be upper-bounded by

$$\mathbb{E}^{\boldsymbol{\rho}(t)}\left(\frac{\mathrm{d}V(\boldsymbol{\rho}(t))}{\mathrm{d}t}\right)\le K+\mathbb{E}^{\boldsymbol{\rho}(t)}\big[\boldsymbol{\phi}^\top\big(\boldsymbol{\lambda}-(\boldsymbol{I}-\boldsymbol{r})\boldsymbol{c}\,\boldsymbol{s}^*\big)\big], \tag{41}$$

where K is a finite constant independent of the control action.

Because $\boldsymbol{s}^*$ maximizes $\boldsymbol{\phi}^\top(\boldsymbol{I}-\boldsymbol{r})\boldsymbol{c}\,\boldsymbol{s}$ over $\boldsymbol{S}$, and $\boldsymbol{\lambda}$ lies in the interior of the admissible region, (36) implies

$$\mathbb{E}^{\boldsymbol{\rho}(t)}\big[\boldsymbol{\phi}^\top\big(\boldsymbol{\lambda}-(\boldsymbol{I}-\boldsymbol{r})\boldsymbol{c}\,\boldsymbol{s}^*\big)\big]\le-\epsilon\,\mathbb{E}^{\boldsymbol{\rho}(t)}\big(\boldsymbol{\phi}^\top\mathbf{1}\big). \tag{42}$$

Moreover, for real movements $(i,o)\in\mathcal{M}_N$, we have $\phi_{(i,o)}(t)\ge(1-p)z_{(i,o)}(t)$, while for fictitious source movements $(i,o)\in\mathcal{M}_F$, $\phi_{(i,o)}(t)=z_{(i,o)}(t)$. Hence there exists $\epsilon'>0$ such that

$$\mathbb{E}^{\boldsymbol{\rho}(t)}\left(\frac{\mathrm{d}V(\boldsymbol{\rho}(t))}{\mathrm{d}t}\right)\le K-\epsilon'\mathbb{E}\left(\sum_{(i,o)\in\mathcal{M}_{F\cup N}}z_{(i,o)}(t)\right). \tag{43}$$

By the sufficient condition in (34), DF-MP strongly stabilizes the network queues. The same argument applies to Private-MP, because ARR only changes the effective CV sample size and the detector-side compensation term, but not the fused MP structure itself. The full derivation is provided in Appendix B.

A final remark is that this result is established for the detector–CV fusion framework. It does not directly imply the same guarantee for CV-only MP controllers under partial and heterogeneous penetration. In particular, Tan et al. (2026) showed that the effective admissible region of CV-MP may shrink in imperfect CV environments, whereas the fusion framework here avoids this issue because detector data still provides usable pressure information for every movement.

5.2. Privacy protection analysis

We next discuss the privacy meaning of Private-MP from the viewpoint of traffic operations. The central question is not whether all information is hidden, but rather what each party can observe and whether the disclosed information is limited to what is needed for control.

We first note that the privacy analysis relies on the standard security properties of the building blocks introduced in Section 4. Specifically, we assume that the adopted additively homomorphic encryption scheme is semantically secure (e.g., IND-CPA secure), and that the group signature scheme provides authenticity, anonymity, and unlinkability in the standard sense (Bellare et al., 2003; Paillier, 1999; Perera et al., 2022). These assumptions imply that uploaded values cannot be read in plaintext by unauthorized parties, and that two valid uploads cannot be directly linked to the same vehicle identity through the signature itself.

Under these assumptions, Private-MP protects two levels of information. First, it protects *micro-trajectory information*, namely the individual travel-time contribution and turning intention uploaded by a CV at a node. Second, it protects *macro-route information*, namely the possibility of linking repeated uploads across intersections into a vehicle route.

From the perspective of the different parties in the system, the privacy effect of Private-MP can be summarized as follows.

(1) Edge servers and external eavesdroppers do not see plaintext vehicle data. Vehicles upload encrypted movement-wise vectors rather than plaintext travel times or turning intentions. Therefore, although an edge server or eavesdropper may observe that a message is transmitted at a node-time, it does not learn the plaintext travel-time value or the movement choice of the uploading vehicle.

(2) The cloud receives only movement-wise aggregates. The edge server aggregates encrypted uploads before forwarding them. After decryption, the cloud obtains only the movement-wise sums required for pressure calculation, rather than individual uploads. Thus, the control center learns the aggregate traffic-state information needed by MP control, but not the individual CV trajectories that generated it.

(3) GS unlinkability and ARR jointly reduce route linkage. Even when the message content is protected, route inference may still arise if uploads at consecutive intersections can be connected. Here the group signature scheme already helps, because each valid

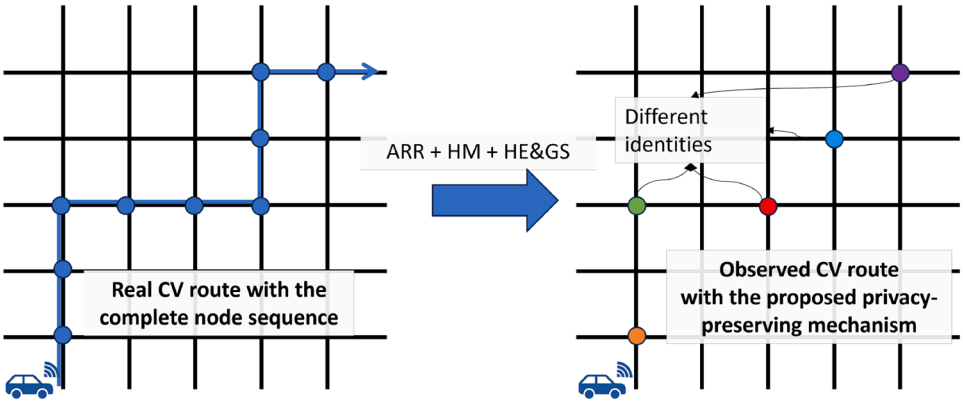

Fig. 5. Illustration of macro-route protection in Private-MP.

upload is verified as coming from an authorized vehicle without revealing which vehicle it is. From the adversary's point of view, each upload can therefore be viewed as coming from a new anonymous sender, rather than from a directly identifiable vehicle.

However, anonymized uploads may still be linked indirectly through their timing and travel-time consistency. This is where ARR becomes important. By reducing the frequency of data sharing, ARR decreases the number of consecutive observable points generated by the same vehicle, and therefore lowers the chance that an adversary can associate them through travel-time patterns. In steady state, the probability of two consecutive sharings is

$$\Pr(S, S) = P^d P^p, \tag{44}$$

and more generally, the probability of Y consecutive sharings is

$$\Pr(\underbrace{S, \ldots, S}_{Y \text{ times}}) = P^d (P^p)^{Y-1}. \tag{45}$$

Thus, decreasing P^p directly suppresses long sharing sequences and reduces the chance that a vehicle can be tracked across intersections.

Fig. 5 illustrates this intuition. From the adversary's viewpoint, the trajectory of one physical vehicle is no longer observed as a continuous line of uploads. Instead, it is broken into sparse and disconnected anonymous points. The unlinkability of the group signature removes direct identity continuity, and ARR further reduces the number of observable points that might be associated through travel-time consistency.

(4) Private-MP does not remove all metadata leakage. Some metadata remain observable under the stated threat model, including node-time upload activity, the number of uploads at a node-time, and the final movement-wise aggregates revealed to the cloud. Therefore, the privacy guarantee of Private-MP should be understood as follows: under the stated assumptions, the mechanism protects individual trajectory-related values and reduces route-linkage risk, while limiting disclosure to the aggregate information required for control and unavoidable metadata. Table 1 summarizes the role of each component in the overall mechanism. In particular, the standard cryptographic building blocks protect the content of uploaded messages, while ARR reduces route-linkage risk by limiting repeated uploads across intersections. At the same time, some metadata, such as node-time activity and final movement-wise aggregates, remain observable under the stated threat model.

An important operational point is that this privacy enhancement remains compatible with MP control because the detector-based term compensates for the CV information lost through ARR. In other words, privacy protection does not act only as an external wrapper; it is coordinated with the data-fusion controller so that reduced CV sharing does not create the sparse-observation instability risk that may arise in CV-only control.

6. Evaluation

As shown in Fig. 6, the proposed Private-MP control is evaluated in a SUMO simulation of a real-world urban road network in Lianyungang City, Jiangsu Province, China. The network comprises 28 signalized intersections (nodes for signal control) with various lane configurations. For instance, nodes 23 and 24 are T-intersections, nodes 11 and 14 have channelized right-turn lanes, and nodes 17 and 18 have shared-use lanes. The signal phase, composed of movements, is provided by the local traffic authority, including the mechanism of alternating release of incoming links used at small intersections, e.g., nodes 7 and 8, and the NEMA-based release of opposite straight or left turns used at main roads, e.g., nodes 6 and 11. The total input demand varies during the simulation period, undergoing a significant increase and decrease to simulate peak periods in the real world. The peak flow reaches nearly 1.6 times the off-peak flow. It should be noted that the demand profile is not directly taken from observed field demand; instead, it is intentionally amplified in the simulation to stress-test the controllers under challenging conditions and to better reveal their differences near the network performance limit.

Table 1
Summary of threats, exposed data, protection tools, and residual leakage in Private-MP.

Threat	Exposed data	Protection tool	Residual leakage
Edge-server compromise	Encrypted uploads at node (n,t)	HE over HM encoding + GS	Node/time activity, number of uploads at a node-time, and ciphertext traffic remain observable; plaintext individual values are hidden without sk.
External eavesdropper	Wireless transmissions	HE over HM encoding + GS	Message timing and size metadata remain visible; plaintext travel-time values and turning intentions are hidden.
Route linkage across intersections	Repeated anonymous uploads across nodes/times	ARR + GS	Upload occurrence is intentionally reduced, but node/time upload activity is not fully hidden.
Cloud-side inference	Aggregated movement statistics	Edge-side aggregation (cloud receives only aggregates)	The cloud learns only movement-wise aggregates needed by control, but not individual uploads.
Turning-intention inference	Movement-specific aggregate contributions	HE over HM encoding + edge-side aggregation	Aggregate movement totals are revealed after decryption; individual turning intentions are hidden from edge servers, eavesdroppers, and from the cloud at the individual level.

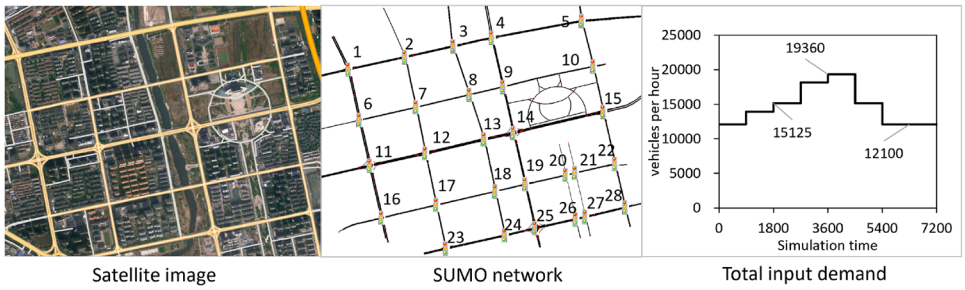

Fig. 6. Real-world network with 28 signalized intersections.

In the simulation, low-resolution detectors are assumed to be installed near the stopline and at an upstream position given by the minimum of the lane length and 250 m. These detectors update every 60 s and provide the number of vehicles that passed during the previous 60 s. Accordingly, the arrival and departure terms in the store-and-forward model are updated every 60 s. While the signal control decision is made every 15 s, the queue state between two detector updates is inferred using the last interval arrival rate and the signal state.

For fairness, we distinguish between queue-length-based and travel-time-based MP baselines under the sensing assumptions adopted in this paper. Under the low-resolution detector setting considered here, the detectors provide only aggregated flow/count information rather than direct high-resolution travel-time measurements. Moreover, in the travel-time-based MP literature we are aware of, travel time is typically assumed to be directly available from CV data or advanced sensing setups, rather than estimated online from only low-resolution aggregated detector counts. Therefore, instead of attempting to reproduce these methods under mismatched sensing assumptions, we use the detector-only special case of the proposed framework (i.e., DF-MP with $p = 0$) as a detector-based travel-time MP baseline.

Five benchmark methods, including the proposed ones, are tested:

- **Q-MP**: the detector-based queue-length MP controller by Varaiya (2013), which uses the number of vehicles (weighted by the link length) in movements for pressure calculation, i.e., Eq. (1). The number of vehicles is estimated by fixed-location detector data.
- **Detector-MP**: a detector-based travel-time MP controller corresponding to the proposed DF-MP with $p = 0$, i.e., the special case where no CV information is available, and the pressure is calculated only from detector-based travel-time approximation.
- **CV-MP**: a CV travel time-based MP controller by Tan et al. (2026), which relies on CV data only and does not consider the privacy issues of CVs, i.e., Eq. (8).
- **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, i.e., Eq. (12).
- **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. Unless otherwise specified, for the adaptive randomized response strategy, P^d is taken as 0.5 and P^p is taken as 0.2, indicating that at least 50% CVs will contribute to signal control while the probability of a CV sharing data at both consecutive intersections does not exceed 20%.

For all methods, the signal decision step length is 15 s, and a 3-s yellow time is inserted for phase transition. The following metrics are used to evaluate the performance of different MP controllers:

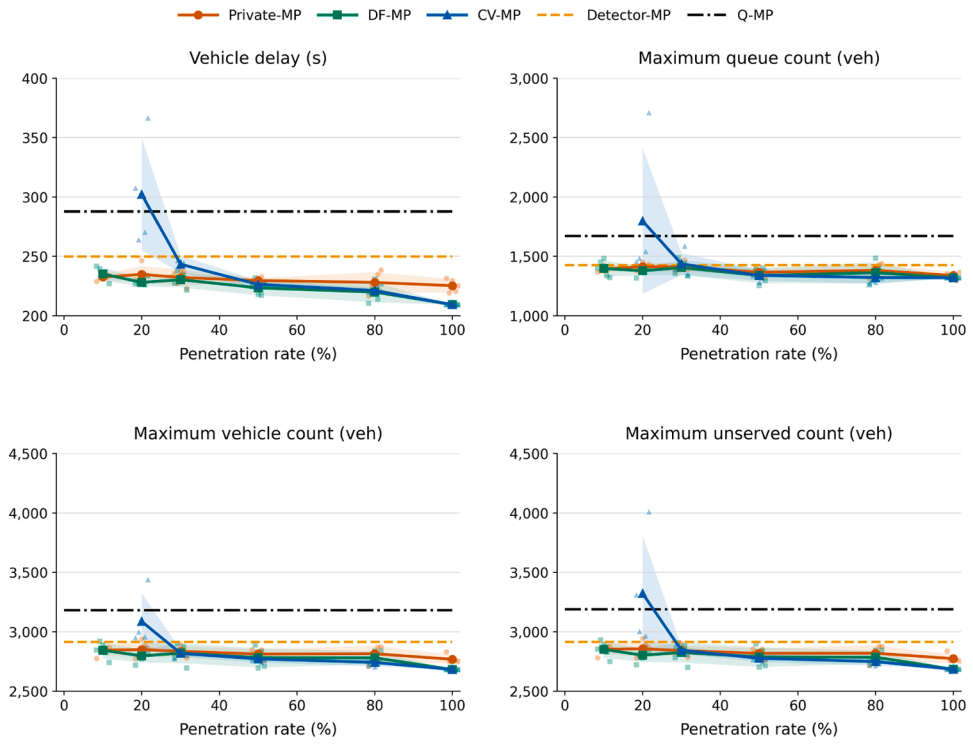

Fig. 7. Overall performance of MP controllers at various penetration rates.

- *Average vehicle delay* (s/veh): the average control delay of vehicles, including waiting time outside the network due to spillover.
- *Queue count* (veh): The real-time number of queuing vehicles on the network. Under the same traffic demand, fewer queuing vehicles indicate smoother traffic flows.
- *Vehicle count* (veh): The real-time number of vehicles on the network. Under the same traffic demand, a smaller number of vehicles indicates a stronger road network carrying capacity.
- *Unserved count* (veh): The unserved vehicle is defined as the number of vehicles that are loaded but have not completed their trips, including both the vehicles currently inside the network and the spillover vehicles that are unable to enter the road network due to downstream congestion. Therefore, when the unserved count is close to the vehicle count, the spillover component is small or negligible; by contrast, when the unserved count is significantly larger than the vehicle count, this indicates substantial spillover outside the network. The lower the unserved count, the higher the throughput capacity of the controller, as more vehicles are served given the same traffic load.

We can also use the maximum queue count, the maximum spillover count, and the maximum unserved count to evaluate the overall performance of the controller during the whole simulation.

6.1. Overall performance at various penetration rates

In this section, we evaluate the performance of five MP controllers at various penetration rates, as shown in Fig. 7. The results for each penetration rate are the average of five repeated experiments with different random seeds. To ensure a fair comparison, we fix both the random seed for SUMO demand generation and the random seed for CV sampling, so that DF-MP and Private-MP are evaluated on the same underlying CV sample; for Private-MP, the privacy-induced selective sharing process is then applied on top of this common sample. For Q-MP and Detector-MP, they only rely on fixed-location detector data, and thus, the results for different penetration rates are the same. For CV-MP, when the penetration rate is 0.1, it fails to stabilize the network queue due to the sparsity of CV observations, showing remarkable vehicle delays, maximum queue count, and maximum unserved count. In this case, most movements do not have any CV observations most of the time, which does not meet the *necessary condition of CV-MP stability* proved in Tan et al. (2026). Therefore, we will not discuss this result further here.

Comparing the Detector-MP baseline (i.e., DF-MP at 0% CV penetration rate) to Q-MP, we can find that, even relying only on detector data, Detector-MP using estimated travel time to calculate pressure outperforms Q-MP using the queue length in terms of vehicle delay, queue count, and unserved count. Specifically, the vehicle delay was reduced by 13.2%. This can be attributed to the fact that the estimated travel time takes into account the cumulative delay of vehicles, which improves the delay fairness across movements compared to Q-MP, leading to better overall performance of the network. These results highlight the benefit of using a travel-time-based pressure metric even under detector-only conditions.

As the CV penetration rate increases, DF-MP performs better on the evaluation metrics overall. This is because more CVs provide more reliable travel-time observations, thereby reducing the impact of detector-side estimation errors and improving the movement-state approximation. Compared to Q-MP, the reduction of average delay by DF-MP increases from 13% to 27% as the penetration rate rises. Regarding CV-MP, in low-penetration-rate scenarios, the increase in CV has a much stronger effect because CV-MP relies entirely on CV observations. By contrast, for DF-MP, the detector data already provide a stable baseline, so the additional benefit of CV data is more moderate but still positive. These results indicate that DF-MP leverages the advantages of both CV and detector data through fusion: at low penetration rates, it achieves more reliable performance than CV-MP by relying on detector data, while at higher penetration rates, it further benefits from richer CV observations.

This comparison also provides an empirical interpretation of the impact of the detector-side travel time approximation introduced in Eq. (11). Detector-MP (i.e., DF-MP at 0% CV penetration) relies entirely on the detector-based travel-time approximation, whereas at 100% CV penetration DF-MP coincides with CV-MP and uses directly observed CV travel-time information, with the detector-based compensation term vanishing. Therefore, the performance gap between Detector-MP and DF-MP/CV-MP at 100% penetration can be interpreted as an empirical indication of the loss associated with the detector-side approximation under detector-only operation. At the same time, the monotonic improvement of DF-MP as the penetration rate increases shows that this approximation error is progressively mitigated as richer CV information becomes available through fusion.

Private-MP is essentially the same as DF-MP, except that Private-MP only requires a proportion P^d of CVs to share data for privacy concerns. Therefore, the effective CV penetration rate of Private-MP is reduced relative to that of DF-MP. Results show that DF-MP consistently outperforms Private-MP across penetration rates. Nevertheless, the gap between the two remains relatively small (less than 4% on average delay in most of the cases), which demonstrates that the proposed privacy-preserving mechanism achieves privacy protection at only a limited performance cost. This result also indicates that, although privacy protection reduces the amount of shared CV data, the detector-fusion design effectively prevents a pronounced performance degradation under low-penetration conditions.

The results for maximum queue size, maximum number of vehicles, and maximum number of unserved vehicles all show similar trends, so we will not repeat them here.

6.2. Detailed network performance

In Fig. 8, we present the detailed network performance, i.e., real-time vehicle count, unserved count, and vehicle time loss distribution, for three typical penetration rates. Across different penetration rates, the performance of Q-MP and Detector-MP remains unchanged, as they rely on detector data only.

When the CV penetration rate is only 20%, due to the randomness and sparsity of CV observations, CV-MP, relying on CV only, experiences a substantial increase in unserved count compared to the detector-based controllers. There is a significant discrepancy between the vehicle count and the unserved count of CV-MP, indicating that vehicles continue to overflow onto the network boundary. Under these circumstances, the CV-MP has become ineffective, and the network has become unstable. This observation is consistent with Tan et al. (2026), which pointed out that, at low penetration rates, spillover may occur when CV observations fail to satisfy the necessary condition for stability, i.e., when a congested movement is not effectively observed by any CV before spillover occurs. By contrast, Q-MP, Detector-MP, DF-MP, and Private-MP, which utilize detector data, all maintain the stability of the road network. Among them, DF-MP and Private-MP, which further fuse CV data, perform better than Detector-MP and Q-MP, because detector data still provides usable pressure information even when no CV is present on a congested movement, while the available CV observations further improve the travel-time estimate. The vehicle time loss distribution at 20% penetration shows the same pattern: DF-MP and Private-MP yield lower central values and lighter upper tails than the single-source baselines, whereas CV-MP exhibits a noticeably heavier upper tail.

When the penetration rate increases to 50%, the performance of CV-MP improves markedly, and the network can be stabilized as well. In this case, CV-MP becomes clearly better than Q-MP and Detector-MP, but it is still slightly inferior to DF-MP. Private-MP remains close to DF-MP, although it performs slightly worse because its privacy-preserving mechanism reduces the amount of shared CV data. The vehicle count, unserved count, and time loss distribution all show that the fusion-based controllers remain the best-performing methods, while the gap between CV-MP and the fusion-based methods becomes smaller than that at 20% penetration.

At 100% CV penetration, DF-MP and CV-MP coincide by definition, since all vehicles are CVs and the detector-based compensation term vanishes. Under this condition, the two controllers produce the same performance and significantly outperform Q-MP and Detector-MP. Private-MP still performs worse than DF-MP because only a half proportion of CVs share data under the privacy mechanism, but it remains substantially better than the detector-only baselines. The corresponding vehicle time loss distributions are consistent with these observations: DF-MP and CV-MP achieve the most concentrated and lowest-loss distributions, whereas Q-MP shows the heaviest tail.

These results confirm that DF-MP and Private-MP combine the advantages of detector and CV data, achieving better results than MP controllers with a single data source over a wider range of penetration scenarios. In particular, detector data provide a stable baseline at low penetration rates, while richer CV observations further improve the performance as the penetration rate increases.

6.3. Sensitivity analysis for privacy parameters

We validate the proposed strategy by analyzing how key consecutive-sharing probabilities vary with the data requirement P^d and the privacy parameter P^p in the adaptive randomized response strategy. These privacy parameters are not chosen independently of the controller, since stronger privacy protection reduces the effective CV sample available for control and therefore increases the

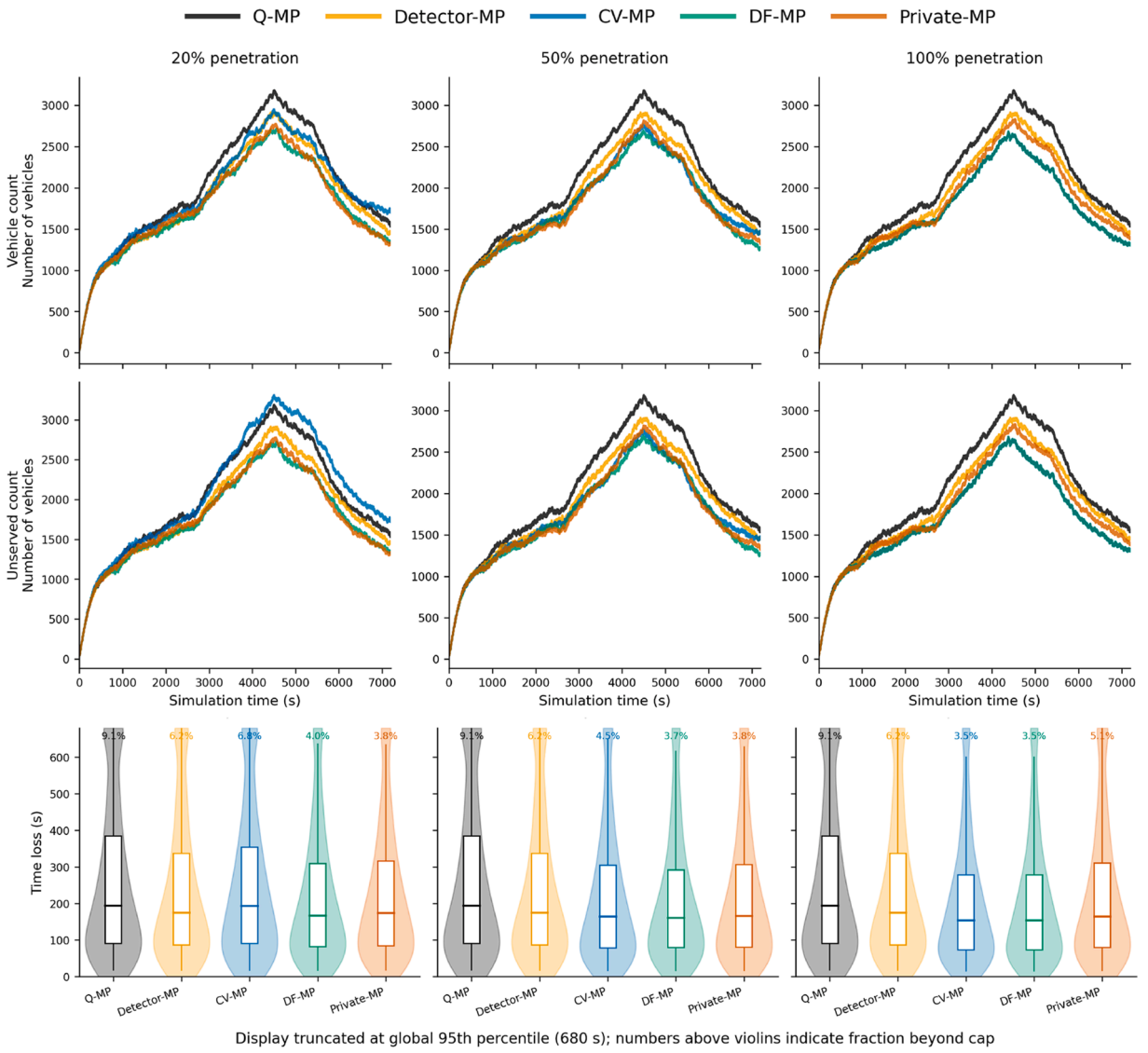

Fig. 8. Detailed network performance of MP controllers for three typical penetration rates.

importance of detector-data compensation. Let $\pi_S = P^d$ be the steady-state sharing proportion and $\pi_N = 1 - P^d$ be the non-sharing proportion. Then we can derive the CV proportion of two consecutive sharings $\Pr(S, S)$, two consecutive not-sharings $\Pr(N, N)$, and three consecutive sharings $\Pr(S, S, S)$:

$$\Pr(S,S) = \Pr(S^{n-1})\Pr(S^n \mid S^{n-1}) = \pi_S \cdot P_j^{n,1} = P^d\, P^p. \tag{46}$$

$$\Pr(N,N) = \Pr(N^{n-1})\Pr(N^n \mid N^{n-1}) = \pi_N \cdot (1 - P_j^{n,2}) = 1 - 2P^d + P^d\, P^p. \tag{47}$$

$$\Pr(S,S,S) = \Pr(S^{n-2})\Pr(S^{n-1} \mid S^{n-2})\Pr(S^n \mid S^{n-1}) = \pi_S\, (P_j^{n,1})^2 = P^d\, (P^p)^2. \tag{48}$$

We sweep (P^d, P^p) over the feasible region (29) and plot heatmaps with contour lines (step 0.1) for the above three critical probabilities, as shown in Fig. 9. $\Pr(S, S)$ increases monotonically with both P^d and P^p. Contours slope upward; larger P^p raises the risk of consecutive sharings and thus inference attacks. $\Pr(N, N)$ decreases linearly with P^d and increases linearly with P^p. For large P^d, maintaining high $\Pr(N, N)$ requires high P^p, which conflicts with the goal of suppressing $\Pr(S, S)$. $\Pr(S, S, S)$ convex in P^p; high P^p accelerates the growth of long sharing sequences. Appendix C suggests the determination process for privacy parameters.

To further examine the practical privacy–performance trade-off, Fig. 10 reports both the average vehicle delay and the realized consecutive-sharing probability under different privacy-parameter settings. When P^p is fixed at 0.2, increasing P^d reduces vehicle delay noticeably, indicating that the control performance benefits from a larger average CV participation rate. By contrast, when P^d is

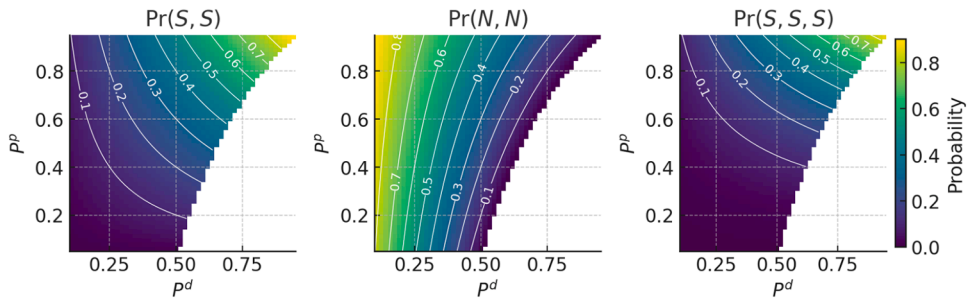

Fig. 9. Sensitivity heatmaps (with 0.1-spaced contours): the CV proportion of two consecutive sharings $\Pr(S,S)$, two consecutive not-sharings $\Pr(N,N)$, and three consecutive sharings $\Pr(S,S,S)$.

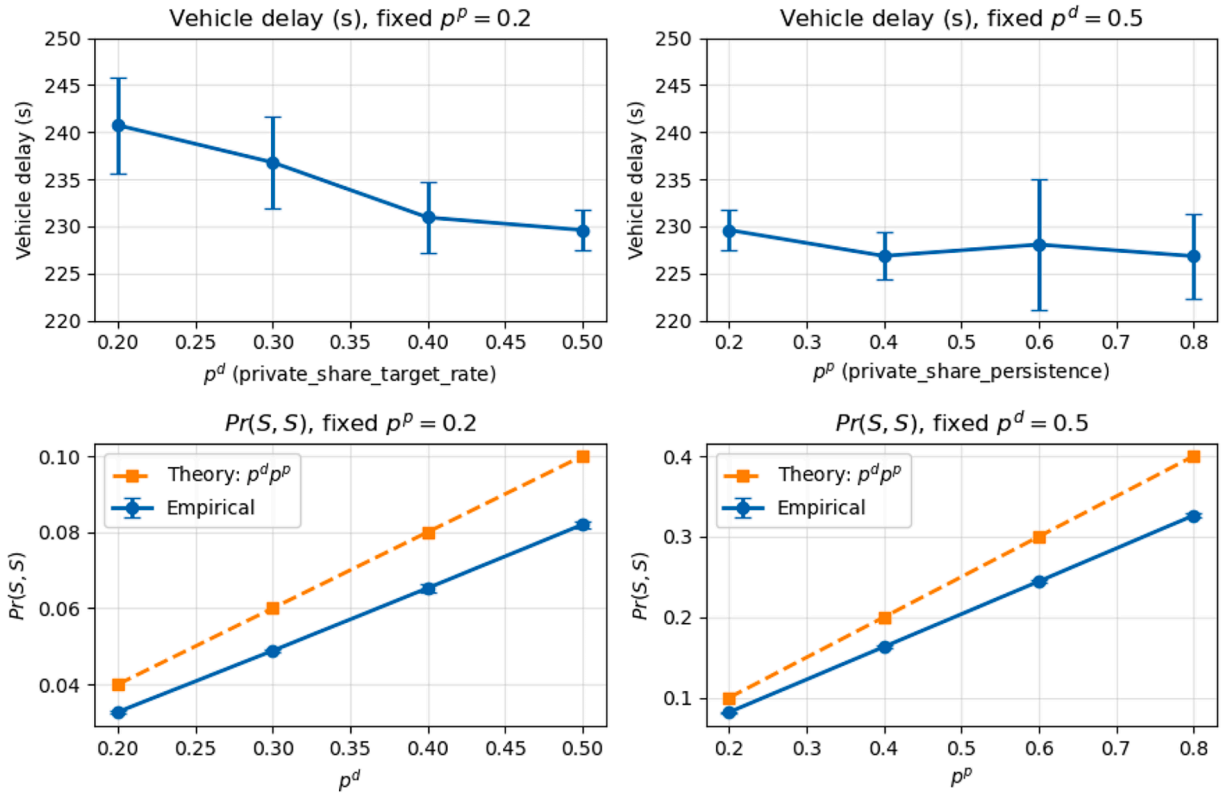

Fig. 10. Sensitivity of control performance and realized consecutive-sharing probability under different privacy parameters.

fixed at 0.5, varying P^p causes only limited changes in delay. This suggests that, under the tested conditions, the control performance is more sensitive to the average amount of shared CV information than to the persistence of consecutive sharing.

The bottom row of Fig. 10 further shows that the empirical $\Pr(S,S)$ follows the same monotonic trend as the theoretical value $P^d P^p$, although it is slightly lower in magnitude. This gap is mainly due to finite-horizon simulation, stochastic traffic loading, and boundary effects, whereas the theoretical result is derived under the steady-state assumption. Overall, these results indicate that P^d is the dominant privacy-related parameter from the control-performance perspective, while the detector-based component helps maintain relatively stable performance even when privacy protection reduces the amount of shared CV data.

7. Conclusion and future work

This study proposed Private-MP, a privacy-aware max-pressure controller for real-time network traffic signal control in mixed detector–CV environments. By fusing fixed-location detector data and CV data, Private-MP overcomes the sparse-observation problem that may affect CV-only MP control at low penetration rates, while also outperforming conventional detector-based MP control. Under a mobile edge computing architecture, the proposed privacy-preserving mechanism combines additively homomorphic encryption, group signatures, hidden-matrix encoding, and the newly proposed adaptive randomized response strategy, so that the controller only

receives movement-wise aggregate information required for pressure calculation while reducing the exposure of individual micro-trajectory and macro-route information. The analytical results show that Private-MP preserves the core queue-stabilizing property of MP control under the fusion framework, and that its privacy mechanism limits disclosure to aggregate control inputs and unavoidable metadata under the stated threat model.

The evaluation results show that: 1) at low CV penetration rates, CV-only MP may fail in practice because some congested movements are not effectively observed by any CV, leading to large delays and spillovers, whereas DF-MP and Private-MP avoid this issue by relying on detector-based information as a robust reference; 2) when no CV data are available, DF-MP degenerates into a detector-based travel-time MP controller (Detector-MP), which outperforms Q-MP because the pressure metric reflects cumulative delay rather than queue length only; 3) as the CV penetration rate increases, DF-MP achieves further performance gains because richer CV observations improve the travel-time estimate, while the detector-fusion structure keeps the controller robust across penetration levels; 4) at full CV penetration, DF-MP and CV-MP become identical by definition, whereas at intermediate penetration rates, the fusion-based controllers remain the best-performing methods overall; 5) compared with DF-MP, Private-MP incurs only a limited performance loss, with the average-delay increase remaining small (no more than 4%) in most cases, which indicates that meaningful privacy protection can be achieved at a modest control cost; and 6) the sensitivity analysis further shows that the control performance is more sensitive to the average sharing level P^d than to the consecutive-sharing parameter P^p, while the detector-based component helps maintain stable operation even under stronger privacy settings.

Future research will extend the current work in three main directions. First, the performance of MP control strategies will be investigated in mixed-traffic scenarios where connected autonomous vehicles (CAVs) and human-driven vehicles operate together. In such settings, CAVs' advanced environmental perception capabilities, such as cooperative sensing, LiDAR-based object detection, and vehicle-to-everything (V2X) communication, can be exploited to improve traffic state monitoring accuracy (Chen et al., 2022; Deng et al., 2025), thus improving MP control performance. Second, privacy protection mechanisms will be expanded to address the unique challenges of data sharing in CAV environments. This will involve safeguarding not only the information of CAVs themselves but also that of other vehicles within their perception range, ensuring an optimal balance between privacy and data utility (Aoki, 2024). Finally, the influence of CAV platooning (Liu et al., 2019; Li et al., 2024) on MP control effectiveness will be explored, focusing on how coordinated vehicle formations affect control stability and operational efficiency under various traffic densities.

CRediT authorship contribution statement

Chaopeng Tan: Writing – original draft, Visualization, Validation, Methodology, Investigation, Formal analysis, Data curation, Conceptualization; **Marco Rinaldi:** Writing – review & editing, Validation, Supervision, Project administration, Methodology, Funding acquisition; **Yikai Zeng:** Writing – original draft, Validation, Methodology, Formal analysis; **Meng Wang:** Writing – review & editing, Visualization, Supervision, Methodology; **Keshuang Tang:** Writing – review & editing, Validation, Resources, Data curation; **Hans van Lint:** Writing – review & editing, Supervision, Project administration, Funding acquisition.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the authors used ChatGPT in order to improve the language. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Acknowledgment

Keshuang Tang would like to acknowledge the financial support of the National Key Research and Developmentrogram, Grant/Award Number: 2023YFE0209300. Chaopeng Tan, Marco Rinaldi, and Hans van Lint would like to acknowledge the financial support of the EU Horizon Europe Research and Innovation Programme, Grant Agreement No. 101103808 ACUMEN.

Data availability

Data will be made available on request.

Appendix A. Technical details of standard privacy-preserving tools

This appendix provides additional technical details of the standard privacy-preserving tools used in Private-MP.

A.1. Additively homomorphic encryption

We use an additively homomorphic encryption scheme

$$\mathsf{HE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}), \tag{A.1}$$

where $\mathsf{KeyGen}(1^\lambda)$ is the key-generation algorithm that, on input security parameter λ, outputs a public/secret key pair (pk, sk); $\mathsf{Enc}(pk, m)$ encrypts plaintext m under the public key; and $\mathsf{Dec}(sk, c)$ decrypts ciphertext c under the secret key.

The scheme supports addition in the encrypted domain:

$$\mathsf{Enc}(pk, m_1) \circ \mathsf{Enc}(pk, m_2) = \mathsf{Enc}(pk, m_1 + m_2), \tag{A.2}$$

where $\circ$ denotes the ciphertext-side aggregation operation corresponding to addition in the plaintext space. When many ciphertexts are aggregated, we write

$$\bigcirc_j c_j \tag{A.3}$$

for the iterated homomorphic operation over the vehicle index set j.

In Private-MP, this property allows the edge server to compute movement-wise aggregated ciphertexts without learning the individual values. We assume that HE is IND-CPA secure in the standard sense. Any additively homomorphic cryptosystem can be used here, e.g., the Paillier cryptosystem (Paillier, 1999).

A.2. Group signatures

We use a group signature scheme

$$\mathsf{GS} = (\mathsf{GS.Setup}, \mathsf{GS.Join}, \mathsf{GS.Sign}, \mathsf{GS.Verify}, \mathsf{GS.Open}), \tag{A.4}$$

where:

- $\mathsf{GS.Setup}(1^\lambda)$ outputs a group public key gpk and a group manager secret key $gmsk$;
- GS.Join is the enrollment protocol through which a vehicle obtains a personal signing key gsk_j;
- $\mathsf{GS.Sign}(gsk_j, m)$ generates a group signature σ on message m;
- $\mathsf{GS.Verify}(gpk, m, \sigma)$ checks whether σ is valid;
- $\mathsf{GS.Open}(gmsk, m, \sigma)$ reveals the signer identity when necessary.

In Private-MP, group signatures are used to ensure that uploaded ciphertexts come from authorized vehicles, while ordinary verifiers cannot link a valid upload to a specific vehicle identity. We assume that GS provides authenticity, anonymity, and unlinkability against probabilistic polynomial-time (PPT) adversaries in the standard sense (Bellare et al., 2003; Perera et al., 2022).

A.3. Hidden-matrix encoding

For each node n, let $\mathcal{M}_n$ denote the set of all possible movements. For a vehicle j contributing a private value x_j to movement $(i, o) \in \mathcal{M}_n$, we define a movement-wise vector

$$\boldsymbol{X}_j^n = [x_j^1, x_j^2, \dots, x_j^{|\mathcal{M}_n|}]^\top = [0, \dots, x_j, \dots, 0]^\top \in \mathbb{Z}^{|\mathcal{M}_n|}, \tag{A.5}$$

which can be written as

$$\boldsymbol{X}_j^n = \mathsf{HM}(n, (i, o), x_j). \tag{A.6}$$

Only the entry corresponding to movement (i, o) is non-zero.

By itself, this encoding does not hide the movement, because the non-zero position reveals it. In Private-MP, it is therefore always used together with encryption:

$$\boldsymbol{C}_j^n = \mathsf{Enc}(pk, \boldsymbol{X}_j^n).$$

This allows movement-wise aggregation without exposing individual turning intentions in plaintext (Tan and Yang, 2024).

Remark 2. The role of hidden-matrix encoding in Private-MP is not to provide confidentiality by itself, but to structure each vehicle contribution in a movement-wise form compatible with encrypted aggregation.

Appendix B. Detailed proof of network queue stability

This appendix provides the detailed derivation omitted from the main text for Proposition 1. We first recall the standard stability definitions and sufficient condition, then introduce the composite Lyapunov function tailored to DF-MP, and finally provide the full drift analysis.

B.1. Preliminary definitions

Definition 1 (Traffic network stability (Neely, 2010; Li and Jabari, 2019; Tan et al., 2026)). A traffic network is strongly stable under a traffic signal policy if the total queues remain finite in the long term:

$$\limsup_{T\to\infty} \frac{1}{T} \int_0^T \mathbb{E}\left(\sum_{(i,o)\in\mathcal{M}_{\mathcal{F}\cup\mathcal{N}}} z_{(i,o)}(t) \right) \mathrm{d}t < \infty. \tag{B.1}$$

In density form,

$$z_{(i,o)}(t) = \begin{cases} \rho_{(i,o)}(t), & \text{if } (i,o) \in \mathcal{M}_{\mathcal{F}}, \\ \int_0^{L_i} \rho_{(i,o)}(x,t)\mathrm{d}x, & \text{if } (i,o) \in \mathcal{M}_{\mathcal{N}}, \end{cases} \tag{B.2}$$

where $\rho_{(i,o)}$ denotes the traffic density of movement (i,o).

For fictitious source movements $(i,o) \in \mathcal{M}_{\mathcal{F}}$, queues can grow without bound. By contrast, for real-link movements $(i,o) \in \mathcal{M}_{\mathcal{N}}$, queues are bounded by physical storage capacity. Hence, network instability is reflected by the unbounded growth of source-link queues, typically caused by spillback and spillover.

Lemma 1 (Sufficient condition for traffic network stability (Neely, 2010; Li and Jabari, 2019; Tan et al., 2026)). *Consider a Lyapunov function $V(\boldsymbol{\rho}(t)) \geq 0$ with $V(\boldsymbol{\rho}(t)) = 0$ if and only if $\boldsymbol{\rho}(t) = 0$. If there exist constants $0 < K < \infty$ and $0 < \epsilon' < \infty$ such that*

$$\mathbb{E}^{\boldsymbol{\rho}(t)}\left(\frac{\mathrm{d}V(\boldsymbol{\rho}(t))}{\mathrm{d}t}\right) \leq K - \epsilon'\mathbb{E}\left(\sum_{(i,o)\in\mathcal{M}_{\mathcal{F}\cup\mathcal{N}}} z_{(i,o)}(t)\right) \tag{B.3}$$

for all $t \geq 0$ and $\boldsymbol{\rho}(t)$, then the stability condition (B.1) holds.

The proof of Lemma 1 follows directly by integrating both sides of (B.3) and rearranging the terms; see Li and Jabari (2019), Tan et al. (2026) for details.

Definition 2 (Admissible demand region (Wang et al., 2022; Tan et al., 2026)). Given the turning-ratio matrix $\boldsymbol{r}$ and the feasible signal-state polyhedron $\boldsymbol{S}$, the admissible demand region is

$$\boldsymbol{\Lambda} = \{\lambda \mid \lambda \preceq (\boldsymbol{I} - \boldsymbol{r})\boldsymbol{c}\bar{\boldsymbol{s}},\ \exists \bar{\boldsymbol{s}} \in \boldsymbol{S}^{co}\}, \tag{B.4}$$

where λ is the vector of average exogenous demands, $\boldsymbol{S}^{co}$ is the convex hull of $\boldsymbol{S}$, $\boldsymbol{c}$ is the diagonal matrix of saturation flow rates, and $\boldsymbol{I}$ is the identity matrix.

For any $\lambda \in \boldsymbol{\Lambda}^{\text{int}}$, there always exists a constant $\epsilon > 0$ such that

$$\lambda - (\boldsymbol{I} - \boldsymbol{r})\boldsymbol{c}\bar{\boldsymbol{s}} \preceq -\epsilon\mathbf{1}. \tag{B.5}$$

B.2. Continuity equations and node flow relations

Recall that for each movement $(i,o) \in \mathcal{M}_N$, we denote by $\rho_{(i,o)}(x,t)$ the traffic density at position x on the upstream link i associated with vehicles heading toward the downstream link o. This density depends on both the spatial coordinate x along the link and the time t. For movements $(i,o) \in \mathcal{M}_F$, corresponding to fictitious source links without physical length, we write the density as $\rho_{(i,o)}(t)$, which is independent of x.

By applying the conservation of vehicles with continuity equations, we obtain

$$\frac{\mathrm{d}\rho_{(i,o)}(t)}{\mathrm{d}t} = \lambda_{(i,o)}(t) - q^{\text{out}}_{(i,o)}\left(s^{\text{out}}_{(i,o)}(t)\right), \qquad (i,o) \in \mathcal{M}_F, \tag{B.6}$$

$$\frac{\partial\rho_{(i,o)}(x,t)}{\partial t} = -\frac{\partial q_{(i,o)}(x,t)}{\partial x}, \qquad x \in (0, L_i),\ (i,o) \in \mathcal{M}_N, \tag{B.7}$$

where $q_{(i,o)}(x,t)$ is the flow rate at position x and time t along incoming link i for vehicles destined to o, $\lambda_{(i,o)}(t)$ is the exogenous demand rate, $q^{\text{out}}_{(i,o)}(s^{\text{out}}_{(i,o)}(t))$ denotes the outflow from link i at time t, $s^{\text{out}}_{(i,o)}(t)$ is the corresponding downstream control state, and L_i is the length of link i. For fictitious movements $(i,o) \in \mathcal{M}_F$, we assume that the downstream control is always active, i.e., $s^{\text{out}}_{(i,o)}(t) \equiv 1$.

At the boundaries of an incoming link for any movement $(i,o) \in \mathcal{M}_N$, the dynamics specialize to

$$\frac{\partial\rho_{(i,o)}(0,t)}{\partial t} = -\frac{\partial q_{(i,o)}(0,t)}{\partial x} = q^{\text{in}}_{(i,o)}\left(s^{\text{in}}_{(i,o)}(t)\right) - q_{(i,o)}(0,t), \qquad x = 0, \tag{B.8}$$

$$\frac{\partial\rho_{(i,o)}(L_i,t)}{\partial t} = -\frac{\partial q_{(i,o)}(L_i,t)}{\partial x} = q_{(i,o)}(L_i,t) - q^{\text{out}}_{(i,o)}\left(s^{\text{out}}_{(i,o)}(t)\right), \qquad x = L_i, \tag{B.9}$$

where $q^{\text{in}}_{(i,o)}(s^{\text{in}}_{(i,o)}(t))$ is the inflow entering link i at time t, and $s^{\text{in}}_{(i,o)}(t)$ is the corresponding upstream control state.

Coupling between adjacent links is captured by expressing the node flows $q^{\text{in}}_{(i,o)}$ and $q^{\text{out}}_{(i,o)}$ as

$$q^{\text{out}}_{(i,o)}\left(s^{\text{out}}_{(i,o)}(t)\right) = \min\left\{c_{(i,o)}\, s_{(i,o)}(t),\ \mu_{(i,o)}(t)\right\}, \tag{B.10}$$

$$q^{\text{in}}_{(i,o)}\left(s^{\text{in}}_{(i,o)}(t)\right) = \sum_{(\forall h,i)\in\mathcal{M}_{n'}} r_{(i,o)}(t)\, \min\left\{c_{(h,i)}\, s_{(h,i)}(t),\ \mu_{(h,i)}(t)\right\}, \quad \text{if } (i,o) \in \mathcal{M}_{\mathcal{N}}, \tag{B.11}$$

where $c_{(i,o)}$ is the saturation flow rate of movement (i,o) at the stop line (i.e., at $x = L_i$), and $\mu_{(i,o)}(t)$ is the effective serviceable demand rate. The term $\mu_{(i,o)}(t)$ depends on both the upstream density on link i and the downstream density on link o, and effectively corresponds to the minimum between upstream sending capability and downstream receiving capacity at time t. In this way, $\mu_{(i,o)}(t)$ guarantees that the discharge flow is simultaneously constrained by vehicle availability upstream and storage limitations downstream. The parameter

$r_{(i,o)}(t)$ denotes the turning ratio associated with movement (i,o) at time t. We use n'' to denote the upstream neighboring node that connects to link i, with movements indexed by (h,i). Eqs. (B.10) and (B.11) thus describe the node-level traffic flow dynamics, which are governed by the signal control state $s_{(i,o)}(t)$ for each movement $(i,o) \in \mathcal{M}_{F\cup N}$. Finally, note that in practical implementations of MP control, the explicit value of $\mu_{(i,o)}(t)$ is not required, as it does not directly appear in the control law; instead, $\mu_{(i,o)}(t)$ is introduced for the purpose of stability analysis.

B.3. Composite pressure and Lyapunov function

For DF-MP, the pressure term for movements $(i,o) \in \mathcal{M}_{\mathcal{N}}$ is

$$\phi_{(i,o)}(t) = \frac{\tau^{nv}_{(i,o)}(t)}{\bar{\tau}_{(i,o)}} + \sum_{j\in\mathcal{J}^{cv}_{(i,o)}} \frac{\tau_j(t)}{\bar{\tau}_{(i,o)}} = (1-p) z_{(i,o)}(t) + \left(\frac{1-p}{2\bar{\lambda}_{(i,o)}\bar{\tau}_{(i,o)}}\right) z_{(i,o)}(t)^2 + \tau^{cv}_{(i,o)}(t). \tag{B.12}$$

The first term corresponds to a detector-based queue term, the second to a detector-based cumulative-delay term, and the third to the CV travel-time term.

Assuming the CV indicator β_j satisfies $\Pr(\beta_j = 1) = p$ and is independent of the real-time link travel time, we have

$$\mathbb{E}\Big(\tau^{cv}_{(i,o)}(t)\Big) = \mathbb{E}\left(\sum_{j\in\mathcal{J}^{cv}_{(i,o)}} \frac{\tau_j(t)}{\bar{\tau}_{(i,o)}}\right) = \mathbb{E}\left(\sum_{j\in\mathcal{J}_{(i,o)}} \beta_j \frac{\tau_j(t)}{\bar{\tau}_{(i,o)}}\right) = \mathbb{E}(\beta_j)\,\mathbb{E}\left(\sum_{j\in\mathcal{J}_{(i,o)}} \frac{\tau_j(t)}{\bar{\tau}_{(i,o)}}\right) = p\,\mathbb{E}\Big(\tau^{a}_{(i,o)}(t)\Big), \tag{B.13}$$

where $\tau^{a}_{(i,o)}(t)$ denotes the total link travel time of all vehicles.

Hence, in density form,

$$\mathbb{E}\big(\phi_{(i,o)}(t)\big) = \mathbb{E}\Big(\theta_1 z_{(i,o)}(t) + \theta_2 z_{(i,o)}(t)^2 + \theta_3 \tau^{a}_{(i,o)}(t)\Big) = \mathbb{E}\left(\int_0^{L_i} \big(\theta_1 + \theta_2 z_{(i,o)}(t) + \theta_3 \tau_{(i,o)}(x,t)\big)\rho_{(i,o)}(x,t)\,\mathrm{d}x\right), \tag{B.14}$$

where

$$\theta_1 = 1-p, \qquad \theta_2 = \frac{1-p}{2\bar{\lambda}_{(i,o)}\bar{\tau}_{(i,o)}}, \qquad \theta_3 = p.$$

Accordingly, we define the composite Lyapunov function used in the proof.

Definition 3 (Composite Lyapunov function)**.** Given the density state $\boldsymbol{\rho}(t)$, define

$$V(\boldsymbol{\rho}(t)) \equiv \frac{1}{2} \sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} \int_0^{L_i}\int_0^{L_i} \big(\varphi_{(i,o)}(x,t) + \varphi_{(i,o)}(x',t)\big)\rho_{(i,o)}(x,t)\rho_{(i,o)}(x',t)\,\mathrm{d}x'\mathrm{d}x + \frac{1}{2}\sum_{(i,o)\in\mathcal{M}_F} \rho_{(i,o)}(t)^2, \tag{B.15}$$

where

$$\varphi_{(i,o)}(x,t) = \begin{cases} 0, & x = 0, \\ \theta_1 + \theta_2 z_{(i,o)}(t) + \theta_3 \tau_{(i,o)}(x,t), & x \in (0, L_i]. \end{cases} \tag{B.16}$$

Then $\varphi_{(i,o)}(x,t) \geq 0$, which ensures that $V(\boldsymbol{\rho}(t)) \geq 0$ and $V(\boldsymbol{\rho}(t)) = 0$ if and only if $\boldsymbol{\rho}(t) = 0$.

B.4. Auxiliary bounds and derivation of the upper bound

For any $(i,o) \in \mathcal{M}_{\mathcal{N}}$, assume that the travel-time weight satisfies

$$0 \leq \tau_{(i,o)}(x,t) \leq \tau^{\max}_{(i,o)} < \infty, \qquad \tau_{(i,o)}(0,t) = 0, \qquad \left|\frac{\partial \tau_{(i,o)}(x,t)}{\partial t}\right| \leq \dot{\tau}^{\max}_{(i,o)} < \infty.$$

Since real links have finite length and finite inflow/outflow due to the minimum headway constraint, there exist constants $z^{\max}_{(i,o)}$ and $\dot{z}^{\max}_{(i,o)}$ such that

$$0 \leq z_{(i,o)}(t) \leq z^{\max}_{(i,o)} < \infty, \qquad \left|\frac{\partial z_{(i,o)}(t)}{\partial t}\right| \leq \dot{z}^{\max}_{(i,o)} < \infty.$$

Define

$$\varphi^{\max}_{(i,o)} := \theta_1 + \theta_2 z^{\max}_{(i,o)} + \theta_3 \tau^{\max}_{(i,o)}, \qquad \dot{\varphi}^{\max}_{(i,o)} := \theta_2 \dot{z}^{\max}_{(i,o)} + \theta_3 \dot{\tau}^{\max}_{(i,o)}.$$

Then

$$0 \leq \varphi_{(i,o)}(x,t) \leq \varphi^{\max}_{(i,o)} < \infty, \qquad \varphi_{(i,o)}(0,t) = 0,$$

and

$$\left|\frac{\partial \varphi_{(i,o)}(x,t)}{\partial t}\right| \leq \dot{\varphi}^{\max}_{(i,o)} < \infty.$$

Using the same reasoning as in Lemma 2 of Tan et al. (2026), there exist constants $\rho^{\max}_{(i,o)}$, $q^{\max}_{(i,o)}$, and $\dot{q}^{\max}_{x,(i,o)}$ such that

$$0 \le \rho_{(i,o)}(x,t) \le \rho^{\max}_{(i,o)} < \infty, \tag{B.17}$$

$$0 \le q_{(i,o)}(x,t) \le q^{\max}_{(i,o)} < \infty, \tag{B.18}$$

$$\left|\frac{\partial q_{(i,o)}(x,t)}{\partial x}\right| \le \dot{q}^{\max}_{x,(i,o)} < \infty. \tag{B.19}$$

These imply

$$\int_0^{L_i}\int_0^{L_i} \rho_{(i,o)}(x,t)\rho_{(i,o)}(x',t)\,\mathrm{d}x'\mathrm{d}x \le (L_i\rho^{\max}_{(i,o)})^2, \tag{B.20}$$

$$\int_0^{L_i} \varphi_{(i,o)}(x,t)\rho_{(i,o)}(x,t)\,\mathrm{d}x \le \varphi^{\max}_{(i,o)} L_i \rho^{\max}_{(i,o)}, \tag{B.21}$$

$$\int_{0_+}^{L_{i-}} -\frac{\partial q_{(i,o)}(x',t)}{\partial x'}\,\mathrm{d}x' \le q^{\max}_{(i,o)}, \tag{B.22}$$

$$\int_{0_+}^{L_{i-}} -\varphi_{(i,o)}(x',t)\frac{\partial q_{(i,o)}(x',t)}{\partial x'}\,\mathrm{d}x' \le \varphi^{\max}_{(i,o)} L_i \dot{q}^{\max}_{x,(i,o)}. \tag{B.23}$$

We next derive uniform upper bounds for the terms δ_0, δ_3, δ_4, δ_5, and δ_6.
For δ_0, we have

$$\begin{aligned}
\delta_0 &= \mathbb{E}^{\rho(t)}\left(\sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}}\int_0^{L_i}\int_0^{L_i}\frac{\partial\varphi_{(i,o)}(x,t)}{\partial t}\rho_{(i,o)}(x,t)\rho_{(i,o)}(x',t)\,\mathrm{d}x'\mathrm{d}x\right)\\
&\le \mathbb{E}^{\rho(t)}\left(\sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}}\int_0^{L_i}\int_0^{L_i}\left|\frac{\partial\varphi_{(i,o)}(x,t)}{\partial t}\right|\rho_{(i,o)}(x,t)\rho_{(i,o)}(x',t)\,\mathrm{d}x'\mathrm{d}x\right)\\
&\le \sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} \dot{\varphi}^{\max}_{(i,o)}(L_i\rho^{\max}_{(i,o)})^2 =: K_0.
\end{aligned} \tag{B.24}$$

Since $q^{\mathrm{out}}_{(i,o)}(s^{\mathrm{out}}_{(i,o)}(t)) \ge 0$, $\varphi_{(i,o)}(L_i,t) \ge 0$, $q_{(i,o)}(0,t) \ge 0$, and $\rho_{(i,o)}(x,t) \ge 0$, it follows that

$$-\delta_3 = -\sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} \mathbb{E}^{\rho(t)}\left(q^{\mathrm{out}}_{(i,o)}(s^{\mathrm{out}}_{(i,o)}(t))\int_0^{L_i}\varphi_{(i,o)}(L_i,t)\rho_{(i,o)}(x,t)\,\mathrm{d}x\right) \le 0, \tag{B.25}$$

$$-\delta_4 = -\sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} \mathbb{E}^{\rho(t)}\left(q_{(i,o)}(0,t)\int_0^{L_i}\varphi_{(i,o)}(x,t)\rho_{(i,o)}(x,t)\,\mathrm{d}x\right) \le 0. \tag{B.26}$$

For δ_5, we obtain

$$\begin{aligned}
\delta_5 &= \sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} \mathbb{E}^{\rho(t)}\left(q_{(i,o)}(L_i,t)\int_0^{L_i}\big(\varphi_{(i,o)}(x,t)+\varphi_{(i,o)}(L_i,t)\big)\rho_{(i,o)}(x,t)\,\mathrm{d}x\right)\\
&\le \sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} 2q^{\max}_{(i,o)}\varphi^{\max}_{(i,o)}L_i\rho^{\max}_{(i,o)} =: K_1.
\end{aligned} \tag{B.27}$$

For δ_6, we have

$$\begin{aligned}
-\delta_6 &= -\sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} \mathbb{E}^{\rho(t)}\left(\int_0^{L_i}\int_{0_+}^{L_{i-}}\big(\varphi_{(i,o)}(x,t)+\varphi_{(i,o)}(x',t)\big)\rho_{(i,o)}(x,t)\frac{\partial q_{(i,o)}(x',t)}{\partial x'}\,\mathrm{d}x'\mathrm{d}x\right)\\
&= \sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} \mathbb{E}^{\rho(t)}\left(\int_0^{L_i}\varphi_{(i,o)}(x,t)\rho_{(i,o)}(x,t)\left(\int_{0_+}^{L_{i-}}-\frac{\partial q_{(i,o)}(x',t)}{\partial x'}\,\mathrm{d}x'\right)\mathrm{d}x\right)\\
&\quad+\sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} \mathbb{E}^{\rho(t)}\left(\int_0^{L_i}\rho_{(i,o)}(x,t)\left(\int_{0_+}^{L_{i-}}-\varphi_{(i,o)}(x',t)\frac{\partial q_{(i,o)}(x',t)}{\partial x'}\,\mathrm{d}x'\right)\mathrm{d}x\right)\\
&\le \sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}}\left(q^{\max}_{(i,o)}\varphi^{\max}_{(i,o)}L_i\rho^{\max}_{(i,o)}+\varphi^{\max}_{(i,o)}L_i^2\dot{q}^{\max}_{x,(i,o)}\rho^{\max}_{(i,o)}\right) =: K_2.
\end{aligned} \tag{B.28}$$

Therefore, the above terms are uniformly bounded by constants K_0, K_1, and K_2.

B.5. Detailed proof of proposition 1

For stability analysis, fictitious source links are also included in the controller. Thus

$$\phi_{(i,o)}(t) = \begin{cases} z_{(i,o)}(t), & (i,o) \in \mathcal{M}_{\mathcal{F}}, \\ (1-p)z_{(i,o)}(t) + \left(\frac{1-p}{2\bar{\lambda}_{(i,o)}\bar{\tau}_{(i,o)}}\right) z_{(i,o)}(t)^2 + \tau^{cv}_{(i,o)}(t), & (i,o) \in \mathcal{M}_{\mathcal{N}}. \end{cases} \tag{B.29}$$

In matrix form,

$$\boldsymbol{s}^*(t) = \arg\max_{\boldsymbol{s}\in\boldsymbol{S}} \boldsymbol{\phi}^\top (\boldsymbol{I}-\boldsymbol{r})\boldsymbol{c}\,\boldsymbol{s}. \tag{B.30}$$

Proof. By applying the Leibniz integral rule and the product rule to Definition 3, and replacing $\partial\rho_{(i,o)}(x,t)/\partial t$ by $-\partial q_{(i,o)}(x,t)/\partial x$ using (B.7), the Lyapunov drift can be decomposed as

$$\mathbb{E}^{\rho(t)}\left(\frac{\mathrm{d}V(\boldsymbol{\rho}(t))}{\mathrm{d}t}\right) = \eta + \delta_0 + \delta_1 - \delta_2 - \delta_3 - \delta_4 + \delta_5 - \delta_6, \tag{B.31}$$

where the terms correspond exactly to the source-link dynamics, time variation of the weight, inflow and outflow contributions, and boundary/interior terms generated by the integrations.

Using the bounds in Section B.4, we obtain

$$\delta_0 \le \sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} (\theta_2 \dot{z}^{\max}_{(i,o)} + \theta_3 \dot{\tau}^{\max}_{(i,o)})(L_i \rho^{\max}_{(i,o)})^2 = K_0, \tag{B.32}$$

$$-\delta_3 \le 0, \tag{B.33}$$

$$-\delta_4 \le 0, \tag{B.34}$$

$$\delta_5 \le \sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} 2q^{\max}_{(i,o)}(\theta_1 + \theta_2 z^{\max}_{(i,o)} + \theta_3 \tau^{\max}_{(i,o)}) L_i \rho^{\max}_{(i,o)} = K_1, \tag{B.35}$$

$$-\delta_6 \le \sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} \left[q^{\max}_{(i,o)}(\theta_1 + \theta_2 z^{\max}_{(i,o)} + \theta_3 \tau^{\max}_{(i,o)}) L_i \rho^{\max}_{(i,o)} + (\theta_1 + \theta_2 z^{\max}_{(i,o)} + \theta_3 \tau^{\max}_{(i,o)}) L_i^2 q^{\max}_{x,(i,o)} \rho^{\max}_{(i,o)} \right] = K_2. \tag{B.36}$$

Therefore,

$$\mathbb{E}^{\rho(t)}\left(\frac{\mathrm{d}V(\boldsymbol{\rho}(t))}{\mathrm{d}t}\right) \le K_0 + K_1 + K_2 + \eta + \delta_1 - \delta_2. \tag{B.37}$$

Using the node flow relations (B.10)–(B.11), the remaining terms can be rearranged into

$$\begin{aligned} \eta + \delta_1 - \delta_2 &= \mathbb{E}^{\rho(t)}\big(\boldsymbol{\phi}^\top \big(\lambda - (\boldsymbol{I}-\boldsymbol{r})\min\{\boldsymbol{\mu}, \boldsymbol{c}\boldsymbol{s}^*\}\big)\big) \\ &= \eta_1 + \eta_2, \end{aligned} \tag{B.38}$$

where

$$\eta_1 = \mathbb{E}^{\rho(t)}\big(\boldsymbol{\phi}^\top \big(\lambda - (\boldsymbol{I}-\boldsymbol{r})\boldsymbol{c}\boldsymbol{s}^*\big)\big), \tag{B.39}$$

$$\eta_2 = \mathbb{E}^{\rho(t)}\big(\boldsymbol{\phi}^\top \big(\boldsymbol{c}\boldsymbol{s}^* - \min\{\boldsymbol{\mu}, \boldsymbol{c}\boldsymbol{s}^*\}\big)\big). \tag{B.40}$$

For η_2, using the boundedness of source-link effective service and real-link densities, there exists a finite constant K_3 such that

$$\eta_2 \le \sum_{(i,o)\in\mathcal{M}_{\mathcal{F}}} \rho^{\mu}_{(i,o)} c_{(i,o)} + \sum_{(i,o)\in\mathcal{M}_{\mathcal{N}}} (\theta_1 + \theta_2 z^{\max}_{(i,o)} + \theta_3 \tau^{\max}_{(i,o)}) L_i \rho^{\max}_{(i,o)} c_{(i,o)} = K_3. \tag{B.41}$$

Hence

$$\mathbb{E}^{\rho(t)}\left(\frac{\mathrm{d}V(\boldsymbol{\rho}(t))}{\mathrm{d}t}\right) \le K_0 + K_1 + K_2 + K_3 + \eta_1. \tag{B.42}$$

By the MP maximization property,

$$\boldsymbol{\phi}^\top (\boldsymbol{I}-\boldsymbol{r})\boldsymbol{c}\,\boldsymbol{s}^* = \max_{\boldsymbol{s}\in\boldsymbol{S}} \boldsymbol{\phi}^\top (\boldsymbol{I}-\boldsymbol{r})\boldsymbol{c}\,\boldsymbol{s} = \max_{\bar{\boldsymbol{s}}\in\boldsymbol{S}^{co}} \boldsymbol{\phi}^\top (\boldsymbol{I}-\boldsymbol{r})\boldsymbol{c}\,\bar{\boldsymbol{s}} \ge \boldsymbol{\phi}^\top (\boldsymbol{I}-\boldsymbol{r})\boldsymbol{c}\,\bar{\boldsymbol{s}}. \tag{B.43}$$

Combining this with (B.5) gives

$$\eta_1 \le \mathbb{E}^{\rho(t)}\big(\boldsymbol{\phi}^\top \big(\lambda - (\boldsymbol{I}-\boldsymbol{r})\boldsymbol{c}\bar{\boldsymbol{s}}\big)\big) \le -\epsilon\, \mathbb{E}^{\rho(t)}(\boldsymbol{\phi}^\top \mathbf{1}). \tag{B.44}$$

Finally, for real movements $(i,o) \in \mathcal{M}_{\mathcal{N}}$,

$$\phi_{(i,o)}(t) = (1-p)z_{(i,o)}(t) + \left(\frac{1-p}{2\bar{\lambda}_{(i,o)}\bar{\tau}_{(i,o)}}\right) z_{(i,o)}(t)^2 + \tau^{cv}_{(i,o)}(t) \ge (1-p)z_{(i,o)}(t), \tag{B.45}$$

while for fictitious movements $(i,o) \in \mathcal{M}_{\mathcal{F}}$, $\phi_{(i,o)}(t) = z_{(i,o)}(t)$. Therefore there exists $\epsilon' > 0$ such that

$$\mathbb{E}^{\rho(t)}\left(\frac{\mathrm{d}V(\boldsymbol{\rho}(t))}{\mathrm{d}t}\right) \le K - \epsilon' \mathbb{E}\left(\sum_{(i,o)\in\mathcal{M}_{\mathcal{F}\cup\mathcal{N}}} z_{(i,o)}(t)\right), \tag{B.46}$$

where $K = K_0 + K_1 + K_2 + K_3$. By Lemma 1, the network is strongly stable. Since Private-MP preserves the same fused MP structure and only changes the effective CV sample through ARR, the same argument applies to Private-MP. □

C. Determination of privacy parameters

In practical applications, the steady-state sharing proportion P^d is determined by the CV data requirement P_{MP} of the MP controller. Given the actual CV penetration rate p in the network, the data requirement imposes the constraint

$$P^d \geq \frac{P_{MP}}{p}. \tag{C.1}$$

Feasibility requires $P_{MP}/p \leq 1$. From (46), the privacy constraint $\Pr(S,S) \leq \alpha$ translates into

$$P^p \leq \frac{\alpha}{P^d}. \tag{C.2}$$

In addition, the Markov-chain feasibility bound (29) requires

$$1 \geq P^p \geq L(P^d) \triangleq \max\left(0, \frac{2P^d - 1}{P^d}\right), 0 < P^d < 1. \tag{C.3}$$

Since $\Pr(S,S) = P^d P^p$ increases monotonically with both P^d and P^p, minimizing $\Pr(S,S)$ subject to the constraints (C.1)–(C.3) yields:

1. Choose the smallest feasible P^d:

$$P^{d\star} = \frac{P_{MP}}{p}. \tag{C.4}$$

2. Compute the feasibility lower bound for P^p:

$$L^\star = L(P^{d\star}) = \max\left(0, \frac{2P^{d\star} - 1}{P^{d\star}}\right). \tag{C.5}$$

3. Choose the smallest P^p allowed by both the privacy cap and the feasibility bound:

$$P^{p\star} = \max\left(0, 2 - \frac{p}{P_{MP}}, \min\left(1, \frac{\alpha p}{P_{MP}}\right)\right). \tag{C.6}$$

Remark 3 (Feasible α and P_{MP})**.** A feasible $P^{p\star}$ exists if and only if

$$\frac{\alpha}{P^{d\star}} \geq L^\star \Longleftrightarrow \alpha \geq P^{d\star} L^\star = \max\left(0, 2\frac{P_{MP}}{p} - 1\right). \tag{C.7}$$

If (C.7) is violated, no (P^d, P^p) pair can simultaneously satisfy the data requirement, privacy cap, and Markov feasibility; one must either relax α or increase p (or reduce P_{MP}).

References

Abbas, N., Zhang, Y., Taherkordi, A., Skeie, T., 2017. Mobile edge computing: a survey. IEEE Internet Things J. 5 (1), 450–465.

Ahmed, T., Liu, H., Gayah, V.V., 2024. Occ-mp: a max-pressure framework to prioritize transit and high occupancy vehicles. Transp. Res. C: Emerg. Technol. 166, 104795.

Ahmed, T., Liu, H., Gayah, V.V., 2025. C-MP: A decentralized adaptive-coordinated traffic signal control using the max pressure framework. Transp. Res. B: Methodol. 200, 103308. https://doi.org/10.1016/j.trb.2025.103308

Aoki, S., 2024. Privacy, security, and reliability for urban ambient sensing with sensor-rich autonomous vehicles. IEEE Internet Things Mag. 7 (2), 114–118.

Bellare, M., Micciancio, D., Warinschi, B., 2003. Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions. In: International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 614–629.

Cao, Y., Tang, K., Sun, J., Ji, Y., 2021. Day-to-day dynamic origin–destination flow estimation using connected vehicle trajectories and automatic vehicle identification data. Transp. Res. C: Emerg. Technol. 129, 103241.

Chen, H., Qiu, T.Z., 2021. Distributed dynamic route guidance and signal control for mobile edge computing-enhanced connected vehicle environment. IEEE Trans. Intell. Transp. Syst. 23 (8), 12251–12262.

Chen, X., Yin, J., Tang, K., Tian, Y., Sun, J., 2022. Vehicle trajectory reconstruction at signalized intersections under connected and automated vehicle environment. IEEE Trans. Intell. Transp. Syst. 23 (10), 17986–18000.

Deng, Y., Cao, Q., Ren, G., Wu, C., Zhang, S., 2025. Reconstructing fully-sampled vehicle trajectories with fragmented observations from connected and automated vehicles. Expert Syst. Appl. 270, 126401.

Gregoire, J., Qian, X., Frazzoli, E., De La Fortelle, A., Wongpiromsarn, T., 2014. Capacity-aware backpressure traffic signal control. IEEE Trans. Control Netw. Syst. 2 (2), 164–173.

Li, D., Zhu, F., Wu, J., Wong, Y.D., Chen, T., 2024. Managing mixed traffic at signalized intersections: an adaptive signal control and CAV coordination system based on deep reinforcement learning. Expert Syst. Appl. 238, 121959.

Li, L., Jabari, S.E., 2019. Position weighted backpressure intersection control for urban networks. Transp. Res. B: Methodol. 128, 435–461.

Li, L., Okoth, V., Jabari, S.E., 2021. Backpressure control with estimated queue lengths for urban network traffic. IET Intell. Transp. Syst. 15 (2), 320–330.

Liu, H., Gayah, V.V., 2022. A novel max pressure algorithm based on traffic delay. Transp. Res. C: Emerg. Technol. 143, 103803.

Liu, H., Gayah, V.V., 2023. Total-delay-based max pressure: a max pressure algorithm considering delay equity. Transp. Res. Rec. 2677 (6), 324–339.

Liu, H., Gayah, V.V., 2024. N-MP: A network-state-based max pressure algorithm incorporating regional perimeter control. Transp. Res. C: Emerg. Technol. 168, 104725.

Liu, H., Gayah, V.V., Levin, M.W., 2024. A max pressure algorithm for traffic signals considering pedestrian queues. Transp. Res. C: Emerg. Technol. 169, 104865.

Liu, H., Lu, X.-Y., Shladover, S.E., 2019. Traffic signal control by leveraging cooperative adaptive cruise control (CACC) vehicle platooning capabilities. Transp. Res. Part C: Emerg. Technol. 104, 390–407.

Mercader, P., Uwayid, W., Haddad, J., 2020. Max-pressure traffic controller based on travel times: an experimental analysis. Transp. Res. C: Emerg. Technol. 110, 275–290.

Neely, M., 2010. Stochastic network optimization with application to communication and queueing systems. Springer Nature.

Paillier, P., 1999. Public-key cryptosystems based on composite degree residuosity classes. In: International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 223–238.
Perera, M. N.S., Nakamura, T., Hashimoto, M., Yokoyama, H., Cheng, C.-M., Sakurai, K., 2022. A survey on group signatures and ring signatures: traceability vs. anonymity. Cryptography 6 (1), 3.
Tan, C., Cao, Y., Ban, X., Tang, K., 2024. Connected vehicle data-driven fixed-time traffic signal control considering cyclic time-dependent vehicle arrivals based on cumulative flow diagram. IEEE Trans. Intell. Transp. Syst. 25 (8), 8881–8897.
Tan, C., Ding, Y., Yang, K., Zhu, H., Tang, K., 2025a. Connected vehicle data-driven robust optimization for traffic signal timing: modeling traffic flow variability and errors. IEEE Trans. Intell. Transp. Syst. .
Tan, C., Liu, H., Sun, D., Rinaldi, M., van Lint, H., 2025b. Transit-MP: transit-prioritized max-pressure control in sparse connected vehicle environments. arXiv preprint arXiv:2511.00309 .
Tan, C., Sun, D., Liu, H., Rinaldi, M., van Lint, H., 2026. CV-MP: Max-pressure control in heterogeneously distributed and partially connected vehicle environments. Transp. Res. B: Methodol. 204, 103387. https://doi.org/10.1016/j.trb.2025.103387
Tan, C., Wang, Q., Liang, J., Yang, K., 2025c. A connected vehicle-based contextual stochastic optimization model for real-time traffic signal timing. IEEE Trans. Intell. Transp. Syst. 26 (11), 20162–20175.
Tan, C., Yang, K., 2024. Privacy-preserving adaptive traffic signal control in a connected vehicle environment. Transp. Res. Part C: Emerg. Technol. 158, 104453.
Tan, C., Yao, J., Tang, K., Liang, J., Yin, G., 2025d. Privacy-preserving cycle-based arrival profile estimation based on cross-company connected vehicles. IEEE Trans. Consum. Electron. 71 (2), 6167–6182.
Tan, C., Yao, J., Zhu, H., Tang, K., 2025e. Robust estimation of traffic arrival rates at signalized intersections with sparse internet of vehicles. IEEE Internet Things J. 12 (19), 40146–40158.
Varaiya, P., 2013. Max pressure control of a network of signalized intersections. Transp. Res. C: Emerg. Technol. 36, 177–195.
Wang, H., Zhu, M., Hong, W., Wang, C., Tao, G., Wang, Y., 2020. Optimizing signal timing control for large urban traffic networks using an adaptive linear quadratic regulator control strategy. IEEE Trans. Intell. Transp. Syst. 23 (1), 333–343.
Wang, Q., Yang, K., 2024. Privacy-preserving data fusion for traffic state estimation: a vertical federated learning approach. Transp. Res. C: Emerg. Technol. 168, 104743.
Wang, X., Jerome, Z., Wang, Z., Zhang, C., Shen, S., Kumar, V.V., Bai, F., Krajewski, P., Deneau, D., Jawad, A., et al., 2024. Traffic light optimization with low penetration rate vehicle trajectory data. Nat. Commun. 15 (1), 1306.
Wang, X., Li, J., Ning, Z., Song, Q., Guo, L., Guo, S., Obaidat, M.S., 2023. Wireless powered mobile edge computing networks: a survey. ACM Comput. Surv. 55 (13s), 1–37.
Wang, X., Yin, Y., Feng, Y., Liu, H.X., 2022. Learning the max pressure control for urban traffic networks considering the phase switching loss. Transp. Res. C: Emerg. Technol. 140, 103670.
Webster, F.V., 1958. Traffic signal settings. Technical Report.
Wu, J., Ghosal, D., Zhang, M., Chuah, C.-N., 2018. Delay-based traffic signal control for throughput optimality and fairness at an isolated intersection. IEEE Trans. Veh. Technol. 67 (2), 896–909.
Xu, T., Barman, S., Levin, M.W., 2024. Smoothing-MP: a novel max-pressure signal control considering signal coordination to smooth traffic in urban networks. Transp. Res. C: Emerg. Technol. 166, 104760.
Xu, T., Barman, S., Levin, M.W., Chen, R., Li, T., 2022. Integrating public transit signal priority into max-pressure signal control: methodology and simulation study on a downtown network. Transp. Res. C: Emerg. Technol. 138, 103614.
Yan, H., He, F., Lin, X., Yu, J., Li, M., Wang, Y., 2019. Network-level multiband signal coordination scheme based on vehicle trajectory data. Transp. Res. C: Emerg. Technol. 107, 266–286.
Yao, J., Tan, C., Tang, K., 2019. An optimization model for arterial coordination control based on sampled vehicle trajectories: the STREAM model. Transp. Res. Part C: Emerg. Technol. 109, 211–232.
Yao, J., Tang, K., 2019. Cycle-based queue length estimation considering spillover conditions based on low-resolution point detector data. Transp. Res. Part C: Emerg. Technol. 109, 1–18.
Zaidi, A.A., Kulcsár, B., Wymeersch, H., 2016. Back-pressure traffic signal control with fixed and adaptive routing for urban vehicular networks. IEEE Trans. Intell. Transp. Syst. 17 (8), 2134–2143.
Zheng, J., Liu, H.X., 2017. Estimating traffic volumes for signalized intersections using connected vehicle data. Transp. Res. C: Emerg. Technol. 79, 347–362.
Zoabi, R., Haddad, J., 2025. An experimental study on max-pressure traffic controller based on travel time delays. Transp. Res. C: Emerg. Technol. 175, 105070.
Zoabi, R., Haddad, J., 2026. Enhanced queue-based max-pressure traffic signal control. Transp. Res. C: Emerg. Technol. 186, 105538.