MPC-CSAS: Multi-Party Computation for Real-Time Privacy-Preserving Speed Advisory Systems

Mingming Liu⬤, Long Cheng, Yingqi Gu, Ying Wang⬤, Qingzhi Liu⬤, and Noel E. O'Connor, *Member, IEEE*

Abstract— As a part of Advanced Driver Assistance Systems (ADASs), Consensus-based Speed Advisory Systems (CSAS) have been proposed to recommend a common speed to a group of vehicles for specific application purposes, such as emission control and energy management. With Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) technologies and advanced control theories in place, state-of-the-art CSAS can be designed to get an optimal speed in a privacy-preserving and decentralized manner. However, the current method only works for specific cost functions of vehicles, and its execution usually involves many algorithm iterations leading long convergence time. Therefore, the state-of-the-art design method is not applicable to a CSAS design which requires real-time decision making. In this article, we address the problem by introducing MPC-CSAS, a Multi-Party Computation (MPC) based design approach for privacy-preserving CSAS. Our proposed method is simple to implement and applicable to all types of cost functions of vehicles. Moreover, our simulation results show that the proposed MPC-CSAS can achieve very promising system performance in just one algorithm iteration without using extra infrastructure for a typical CSAS.

Index Terms— Speed advisory systems, multi-party computation, vehicle networks, optimal consensus algorithm.

I. INTRODUCTION

WITH the advances in smart vehicle technologies and Intelligent Transportation Systems (ITS), Intelligent Speed Advisory (ISA) systems have become a critical part of Advanced Driver Assistance Systems (ADASs). For both manually driven and autonomous vehicles, ISA has shown to be able to significantly improve driving safety, sustainability and efficiency [1]–[3].

As a special type of ISA, Consensus-based Speed Advisory Systems (CSAS) aim to recommend a consensus speed to a group of vehicles in a given area [4], [5]. Compared to the cases that asking different vehicles to drive at their own optimal speeds, CSAS make more sense in many practical scenarios. As demonstrated in Fig. 1, cars tend to follow a common speed when possible in highways or special zones in cities, and this can bring some obvious benefits to various types of road users, such as reduced emissions (with less frequent accelerations/decelerations), reduced energy consumption, increased throughput, and increased safety and health [6]–[10].

Mingming Liu is with the School of Electronic Engineering, Dublin City University, Dublin 9, D09 V209 Ireland (e-mail: mingming.liu@dcu.ie).

Long Cheng is with the School of Computing, Dublin City University, Dublin 9, D09 V209 Ireland (e-mail: long.cheng@dcu.ie).

Yingqi Gu is with the Insight Centre for Data Analytics, Dublin City University, Dublin 9, D09 V209 Ireland (e-mail: yingqi.gu@alkermes.com).

Ying Wang is with the Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China (e-mail: wangying2009@ict.ac.cn).

Qingzhi Liu is with the Information Technology Group, Wageningen University & Research, 6708 PB Wageningen, The Netherlands (e-mail: qingzhi.liu@wur.nl).

Noel E. O'Connor is with the School of Electronic Engineering, Dublin City University, Dublin 9, D09 V209 Ireland, and also with the SFI Insight Centre for Data Analytics, Dublin City University, Dublin 9, D09 V209 Ireland (e-mail: noel.oconnor@dcu.ie).

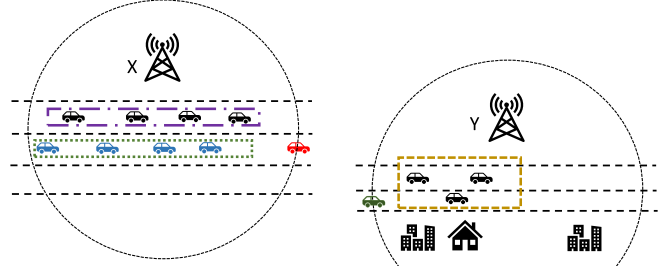Digital Object Identifier 10.1109/TITS.2021.3052840

Fig. 1. An application scenarios of consensus-based speed advisory systems.

Considering the condition that environmental concerns become increasingly compelling, in this article we focus on the design of a CSAS to minimize the emissions for a group of vehicles. In fact, achieving an optimal common speed for the case is not easy. The main reason is that different vehicles are designed to operate optimally at different vehicle speeds and at different loading conditions [5]. Namely, to get an optimal speed, we will have to get all the detailed information of the vehicles in a group, not only the basic information such as the vehicle type, vehicle age and fuel mode, but also the load and the desired time of arrival etc. It is obvious that the data collection process will be complex. More important, due to confidentiality concerns and privacy regulations such as GDPR,[1] nowadays it is not always possible for vehicle owners to share or reveal their data. Therefore, a more practical and privacy-preserving CSAS becomes desirable.

Along this line, our previous work in [5] has attempted to devise an optimal speed for a CSAS in a privacy-preserving manner, namely without revealing in-vehicle information to other vehicles or to infrastructures. Specifically, it is assumed that each vehicle is associated with an emission cost function, and only the implicit information, i.e. derivative values of the cost function at certain speeds are transmitted to a central infrastructure. For simplicity, we refer to the approach proposed in [5] as DP-CSAS (i.e., Derivation based Privacy-preserving CSAS) in the following context.

Although DP-CSAS represents the state-of-the-art approach on privacy-preserving CSAS design, it has two shortcomings:

(i) The proposed optimization model in DP-CSAS is built based on the assumption that the emission cost functions of all vehicles are strictly convex, and thus the derivatives can be calculated. Further, the emission model adopted in [5] is essentially an average-speed model, and the emission only depends on the average-speed of a specific vehicle. This unlikely works for all real cases due to (1) the emission function of a vehicle can also depend on other factors, such as acceleration, road types, weather conditions etc, and (2) some cost functions can be discontinuous and not differentiable.

(ii) DP-CSAS usually requires a relatively large amount of iterations for the algorithm convergence. This makes the optimization

process time costly, and thus the applications of the approach may be limited. For example, as the results reported [5], DP-CSAS takes more than 200 secs to optimize the speed for a group of 40 vehicles. It means that DP-CSAS will not be hard to handle dynamical cases in real time, such as frequent changes of a vehicular network due to frequent check-in and check-out of vehicles in the group, which may require the new optimal consensus speed to be calculated within a few seconds.

To provide a more practical and powerful privacy-preserving CSAS, in this article, we introduce a Multi-Party Computation (MPC) based design approach. Specifically, the proposed method, MPC-CSAS, has several advantages compared to the state-of-the-art DP-CSAS: (1) it is applicable to all emission cost functions; (2) it is simple to implement in real-time without imposing a large communication burden on the existing infrastructures; and (3) it can not only be deployed in a static and strongly connected network, but it can also be extended to deal with weakly and dynamic connectivity conditions in a practical ITS scenario under a certain assumptions. Therefore, we believe that the proposed MPC-CSAS can be applied in many new scenarios where the DP-CSAS method cannot effectively and efficiently take over.

The remainder of this article is organized as follows. In Section II, we introduce the background and the related works of CSAS. We present the system design of MPC-CSAS in Section III. We carry out extensive evaluation of our approach in Section IV and conclude this article in Section V.

II. BACKGROUND AND RELATED WORK

In this section, we briefly introduce the optimization problem of CSAS as well as the related works.

A. CSAS Problem Statement

In this section, we describe an application to design a CSAS for a fleet of vehicles. Specifically, the objective of the CSAS is to recommend a consensus virtual speed to a fleet of Internal Combustion Engine Vehicles (ICEVs) running on the highway so that the overall emissions of the fleet can be minimized if all ICEVs can follow the recommended speed. Full details of this application have been presented in [5]. Here, we briefly review the problem statement for completeness of the context.

We consider a scenario in which a number of ICEVs are driving along a stretch of highway in the same direction. Some users of the ICEVs can decide to participate into the CSAS, that is during their driving period, they wish to use the CSAS to receive a recommend virtual speed in order to reduce the overall emissions on the highway. Each ICEV owner may get some revenue by participating into the CSAS, e.g., tax reduction. Let N denote the number of ICEVs on the highway where the broadcast signal from the CSAS can be received. Each vehicle needs to equip with a specific communication device, which is able to receive the broadcast signal and transmit limited message back to the CSAS and to nearby vehicles. In practice, the broadcast signal from the CSAS can be triggered from a base station facilitated at the road infrastructure, and vehicular communication links can be established using V2V and V2I technologies.

Let $\underline{N} := \{1, 2, \ldots, N\}$ denote the set for indexing the vehicles, and let $s_i(k)$ be the recommend speed of the i'th vehicle at a time slot k. Let $\mathbf{s}(k) := [s_1(k), s_2(k), \ldots, s_N(k)]^T$ be a vector for all $s_i(k)$ at time k. Furthermore, each vehicle i is associated with a cost function $f_i(s_i(k))$ which models the amount of CO_2 emission generated if the vehicle is travelling at the speed $s_i(k)$. According to [5], each cost function is continuous, strict convex and second order differentiable.

In particular, f_i has been adopted as an emission function of s_i in an average speed model in the following form:

$$f_i(s_i) = k\left(\frac{a + bs_i + cs_i^2 + ds_i^3 + es_i^4 + fs_i^5 + gs_i^6}{s_i}\right) \quad (1)$$

where the parameters k, a, b, c, d, e, f, g are constant values and they are defined differently by different types of ICEVs as per the reference [11]. With this in place, the specific problem to be solved can be formulated in the following:

$$\min_{\mathbf{s} \in \mathbb{R}^N} \sum_{i \in \underline{N}} f_i(s_i),$$
$$\text{s.t. } s_i = s_j, \ \forall i \neq j \in \underline{N}. \quad (2)$$

Comment: The ultimate objective of a CSAS is to recommend a virtual consensus speed $\mathbf{s}^*$ to a group of ICEVs. In the DP-CSAS approach, this is done by solving (2) through iterations of $\mathbf{s}(k)$. We note that the recommended speed deem to be a virtual speed, and thus it is not our intention to enforce every driver to follow such a speed, which is the key difference between a CSAS and a platooning system.

B. Related Solutions for CSAS

SAS is a cooperative system which aims to improve energy-efficient and sustainable mobility for vehicles. Different from the conventional approaches such as the works in [1], [2], [12], we focus on the consensus problem of SAS in this work. Although consensus problem can be solved in a variety of ways such as using ADMM [13], our focus is to construct a partially distributed solution which allows to calculate an optimal solution in real time. Moreover, different from the works in CSAS designs [14], [15], we address the optimization problem in a privacy-preserving way without revealing individual cost functions of vehicles.

To the best of our knowledge, only a few papers in the literature have considered the privacy issue of the CSAS. Specifically, the work [16] achieves the consensus over a multi-layer network that no vehicle knows the exact state of other vehicles. Different from that, we focus on protecting the emission cost function of vehicles and our target is to reduce vehicle emissions. The problem studied in the work [5] is the same as ours. However, as we have described, the proposed DP-CSAS has a few shortcomings. In what follows, we will give a brief review of the DP-CSAS solutions.

C. The State of the Art DP-CSAS Solution

The key idea of the DP-CSAS solution in [5] is to find the equivalent Lagrange equations for (2), that is:

$$\frac{\partial\left[\sum_{i=1}^N f_i(s_i(k)) + \lambda_i(s_i(k) - s_j(k))\right]}{\partial s_i(k)} = 0, \ \forall i \neq j \in \underline{N} \quad (3)$$

where λ_i denotes the Lagrange multiplier of the i'th constraint. It is not difficult to derive from (3) that finding the optimal solution of (2) is equivalent to solving the following equation:

$$\sum_{i=1}^N f_i'(s_i) = 0$$
$$s_i = s_j, \ \forall i \neq j \in \underline{N} \quad (4)$$

To solve (4), an iterative feedback scheme has been applied in the form of:

$$\mathbf{s}(k+1) = P(k)\mathbf{s}(k) - \mu \sum_{i=1}^n f_i'(s_i(k))\mathbf{e} \quad (5)$$
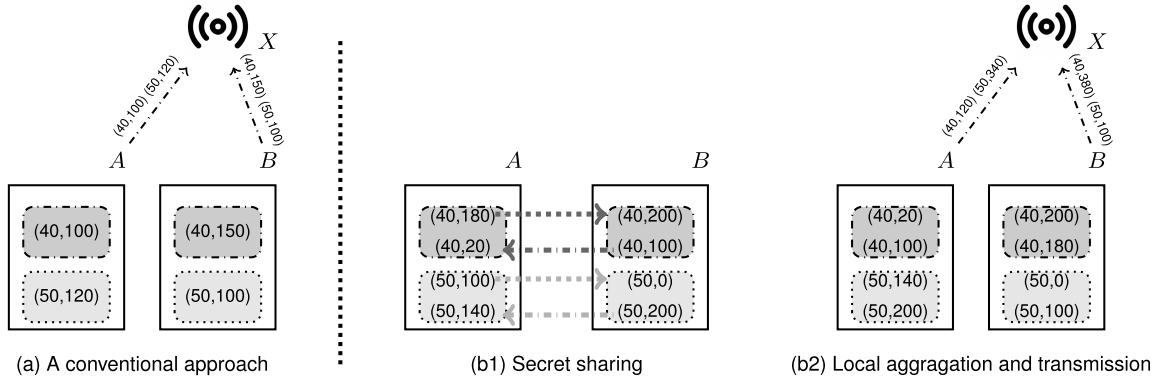
Fig. 2. An example of how to use MPC to consensus-based speed advisory systems.

where $\{P(k)\}_{k\in\mathbb{N}} \subset \mathbb{R}^{N\times N}$ is a uniformly strongly ergodic sequence of row stochastic matrices which can be used to model the connectivity among moving vehicles. $\mathbf{e} \in \mathbb{R}^N$ is a consensus vector with all entries equal to 1. u is a parameter which determines the convergence and stability of the system. It has been proved in [5] that if f_i are strictly convex, continuous, and each f'_i has a strictly positive and bounded growth, i.e. there exist constants $d^i_{\min}$ and $d^i_{\max}$ such that for any $a \neq b$

$$0 < d^i_{\min} \leq \frac{f'_i(a) - f'_i(b)}{a - b} \leq d^i_{\max}, \quad \forall i \in \underline{N}. \tag{6}$$

and when μ is chosen according to

$$0 < \mu < 2 \left(\sum_{i=1}^{n} d^i_{\max} \right)^{-1} \tag{7}$$

then (5) is uniformly globally asymptotically stable at the unique optimal point $\mathbf{s}^* = s^* e$ of the problem (2).

As a concluding remark of this section, we note that the DP-CSAS proposed in [5] leverages the derivative of each cost function f_i, and it requires some strict conditions (Lipschitz condition) on each derivative function f'_i, which might not be practical for cost functions in all ITS applications.

III. THE PROPOSED APPROACH

In this section, we first demonstrate how we can use MPC for privacy-preserving CSAS design with an example. Then, we give the details of our proposed MPC-CSAS.

A. MPC and Its Application to CSAS

Multi-party Computation (MPC) is a cryptographic functionality that allows for secure computation over sensitive data sets [17]. In an MPC protocol, all parties can cooperatively evaluate for some functions, with guarantee that each party can only learn from the output and its own private input. We can construct MPC protocols in different ways, and one of the most commonly used method is the homomorphic secret sharing [18]. In such an approach, the type of the transformation from one algebraic structure into another is kept as the same. Namely, for any kind of manipulation over the original data, there is a corresponding manipulation of the transformed data [19].

To demonstrate how we can apply MPC to the privacy-preserving CSAS design, a simple example with two vehicles, A and B, and a base station X, is illustrated in Fig. 2. For simplicity, we only include emission values of the two vehicles when speeds are 40 and 50km/h. Here, the objective is to find out which speed can achieve a smaller

values. As shown in Fig. 2(a), following a conventional approach, we can ask A and B to send the values of their speed-emission mappings to X. In this condition, the base station can calculate the sum of the mappings at the speed 40 and 50 respectively, and then recommend the better corresponding speed. For instance, X knows that the sum of the mappings is 250 for the speed 40, and 220 for the speed 50, and clearly 50 will be sent to A and B by broadcast. Obviously, the privacy of A and B is not preserved in this method, since the base station knows their private information. In order to protect private information to the infrastructure (i.e., the base station), we can ask B to send its speed-emission mapping information to A to get an optimal speed. However, B will lose its privacy by revealing its value to A in this setup.

To address this issue, an MPC-based approach is demonstrated in Fig. 2 (b). The processing mainly includes three steps as follows:

1) Secret generation: The speed-emission mappings of A and B are split into several shares and some shares should be kept locally. As shown in Fig. 2 (b1), we use two shares for each mapping, that is the mapping (40,100) is split into (40,180) and (40,20). Note that we doubled the original mapping value here, i.e., from 100 to 200 in this example, but this splitting is not unique.

2) Secret sharing: For the secret generated for each speed, A and B share part of them to each other. For example, A shares (40,180) and (50,100) to B, and B shares (40,100) and (50,200) to A. After that, the data located on A and B is demonstrated in Fig. 2 (b2).

3) Local aggregation: A and B aggregate to the local and received speed-emission mappings based on the value of each speed and then send the information to the base station for final speed recommendation. In our example, A sends (40, 120) and (50, 340) to X, and B sends (40, 380) and (50, 100).

After the above three steps, X will know that the emission is 500 for the speed 40, and 440 for the speed 50. Therefore, the two vehicles can get the same speed recommendation (i.e., 50km/h) as the conventional approach shown in Fig. 2(a). Moreover, since both A and B have kept part of their secret locally, they cannot get any information of the original values from each other. Therefore, the privacy of both A and B is well preserved.

Comment: In the above example, for a speed s_i and its emission $f_i(s_i)$, we simply generate two secret values $f^1_i(s_i)$ and $f^2_i(s_i)$ on the emission, and guarantee that the functions f^1_i and f^2_i always meet the condition $f_i(s_i) = 0.5 \times (f^1_i(s_i) + f^2_i(s_i))$ for any s_i. This is consistent with the definition of an MPC protocol, since the transformation of algebraic structure is preserved in the assigned

problem, i.e., $\sum_i f_i(s_i) = 0.5 \times (\sum_i f_i^1(s_i) + \sum_i f_i^2(s_i))$. Therefore, our above operations can achieve the privacy-preserving computation. In contrast, if we generate secrets using another way like $f_i(s_i) = f_i^1(s_i) \times f_i^2(s_i)$, then the computation will be invalid within the MPC scheme. In general, if M secret values need to be generated for each vehicle, then we can have $g(f_i(s_i)) := af_i(s_i) + b = \sum_{h=1}^M f_i^h(s_i)$ for any s_i, where a, b are constants.

B. The MPC Based Privacy-Preserving CSAS

Now we propose the MPC based privacy-preserving CSAS in a formal way by using graph theories. We define an order pair $\mathcal{G} = (V, E)$ as a directed graph for all vehicles in the network. V denotes the set of vertices, or vehicles of the graph $\mathcal{G}$. E is a set of edges, or communication links between vehicles, which are order pairs with two distinctive vertices. In our context, this implies that a communication link between any two vehicles in the network is directional. Let $deg^+(v)$ denotes the outdegree of a vertex $v \in V$, which models the number of vehicles that can receive a signal from the vehicle represented by the vertex v, and let v^+ be the set of vertices of v which it can reach to. Let v^- denote the set of vertices of v which it can receive signal from. We assume that $deg^+(v)$ is known to every vertex v in the network.

With this in place, we claim that for every vehicle, represented by the vertex v in a directed graph $\mathcal{G}$, the MPC based CSAS can preserve privacy for all vehicles in the network if $deg^+(v) >= 1$, $v \in V$. Indeed, if the outdegree can hold for every $v \in V$, then it implies that every vehicle in the network can have at least one neighbour to do the secret sharing part shown in Section III-A, which preserves the privacy of any vehicle by splitting the emission mapping to at least two parts. Now we present the pseudo code of the MPC based privacy-preserving algorithm in the following:

Algorithm 1 MPC-CSAS Privacy-Preserving Algorithm

1: **for** each $i \in \underline{N}$ **do**
2:   Generate a sequence of M pairs of the original speed-emission mappings in a given range of speeds.
3:   Get the outdegree value for vehicle i corresponding to vertex v_i in the graph $\mathcal{G}$, i.e. $deg^+(v_i)$.
4:   **for** $j = 1, 2, \ldots, M$ **do**
5:     Split the mapping into $deg^+(v_i) + 1$ shares.
6:     Reserve one share locally.
7:     Transmit $deg^+(v_i)$ shares to vehicles in the set v_i^+.
8:   **end for**
9:   Aggregate the local received mappings from set v_i^-.
10:   Send the aggregated local mappings to a base station.
11: **end for**
12: Get the best pair index j^* from the base station.
13: Set the recommended speed to the speed in j^*th pair.

---

1) Remark on Network Connectivity: Our proposed Algorithm 1 can be implemented in a batch manner, that is the optimal consensus solution of the problem (2) can be found in just one simple algorithm iteration between vehicles and the base station if the outdegree condition for all vehicles can be satisfied in the network. By definition, a strongly connected graph is a graph which for any two vertices $u, v \in V$, there exists a directed path from $u \rightarrow v$ and $v \rightarrow u$, respectively. This show that the proposed MPC-CSAS algorithm is applicable to strongly connected networks.

On the other hand, vehicular networks are not always static due to various interferences in urban areas. To deal with this challenge, vehicular networks have been modelled using time-varying connectivity graphs in current literature. For instance, in our previous work [5],

a sequence of row-stochastic matrices $\{P(k)\}_{k \in \mathbb{N}} \subset \mathbb{R}^{N \times N}$ has been applied for this purpose. In particular, if $\{P(k)\}$ is a uniformly strongly ergodic sequence as the assumption made in [5], then it implies that every vehicle in the network can communicate to other vehicles over a certain period of time. Roughly speaking, this is equivalent to saying that the resulting connectivity graphs are strongly connected at most time instances [5], which shows the applicability of our proposed algorithm under switching graph topologies. It is worth noting that in most cases we assume that a group of moving vehicles are relatively static and the distance between each car is relatively small so that the V2V communication is achievable among the group. This assumption is consistent with our previous work [5]. However, our proposed solution can be easily extended to cover the case where a group of vehicles can be dynamically clustered and created according to the quality of network connectivity. In such a case, if a vehicle is driving too fast/slow on a road and it cannot receive the message from a given base station, it is still possible for the vehicle to join a different group of vehicles implementing the MPC-CSAS on another stretch of road.

Finally, if a vehicle in a group has weakly connectivity to its neighbouring vehicles, it is still possible for the vehicle to conduct the secret sharing and the local aggregation steps with the base station. In this case, a new service needs to be incorporated into the base station which can be seen as a "dummy" vehicle for the application purpose. Here, the "dummy" vehicle is considered as a software component deployed at a base station, which can assist the weakly connective vehicle for V2V based information exchange. Once this is done, the speed recommendation service, essentially another software component based on the MPC-CSAS algorithm deployed at the base station, can be involved for the final decision making step. From an operational perspective, this setup has flexibility in that it will allow vehicles to conduct a two-step communication with the base station to receive the optimal speed advisory information at different time and place during travelling. We note that although both software components can be deployed at a given base station, the privacy of vehicles' data can still be preserved provided that a security access control based approach is employed at the base station. We shall ignore a further discussion for this aspect in the work as this is beyond the scope of our article.

2) Remark on Network Communication Overheads: In fact, MPC has significant computational overhead and always involves high communication cost in the presence of big data processing [17]. However, for a CSAS case, the domain of vehicle speeds is small. Moreover, getting an absolute optimal speed will make little sense for CSAS. Therefore, we can ask each vehicle to keep a local list of speed-emission mappings in a specified speed range, such as between 30km/h and 120km/h with increasing every 5km/h. In this case, each vehicle will only need to keep 19 speed-emission pairs locally and shares the 19 pairs with another vehicle. If we use integers to represent the speed and emission, the size of the shared information between vehicles is only 152 bytes. Moreover, the data received and processed by a base station will be less than 3KB for a group of 20 vehicles. Obviously, the amount of data to be processed is extremely small in our approach, and the communication and computing time will be approximately 0 for both vehicles and base stations which are with a general hardware configuration. Namely, the overhead of the MPC is negligible. This is also the reason why we call our approach as a real-time solution for privacy preserved CSAS. Specifically, in our simulation environment, we have observed that with inserted timestamps both the data sharing and data aggregation process can be done in less than 5ms.

3) Remark on Practical Implications of Applying the Proposed Methodology: We believe that our current proposed method can be

TABLE I
EMISSION FACTORS FOR SOME CO_2 EMISSION TYPES OF ICEVS
ACCORDING TO [11], WHERE {E, F, G} = 0 AND K = 1

Type	a	b	c	d
R004	2.2606E+3	7.0183E+1	2.9263E-1	3.0199E-3
R005	2.2606E+3	5.9444E+1	2.9263E-1	3.0199E-3
R011	2.5324E+3	1.1834E+2	-4.3167E-1	6.6776E-3
R012	2.5324E+3	1.0340E+2	-4.3167E-1	6.6776E-3
R018	3.7473E+3	1.6774E+2	-8.5270E-1	1.0318E-2
R019	3.7473E+3	1.5599E+2	-8.5270E-1	1.0318E-2
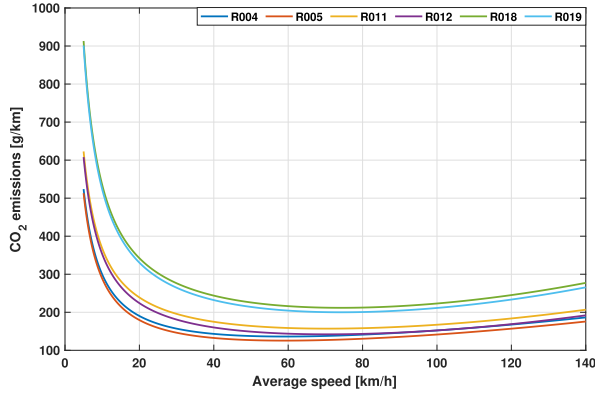
Fig. 3. Different CO_2 emission cost functions in Table I.

easily extended to cope with various setups whilst utilising most up-to-date in-vehicle communication and computing devices as well as roadside traffic infrastructure. Specifically, our proposed approach fits well into the current Mobile Edge Computing (MEC) framework and architecture, where various services can be defined, deployed and implemented at the edge side using for instance REST-based APIs. As we have already commented, our proposed system requires very limited communication and computation overhead (less than 3KB data for 20 vehicles) compared to other existing works in the literature. Given this, we believe that the instantaneity of our system operation in a real world speed advisory scenario is fully operable in current 4G/LTE infrastructures, and will surely be working well in the 5G and beyond 5G network environment.

IV. SUMO SIMULATION AND RESULTS

In this section, we evaluate the performance of Algorithm 1 using SUMO [20].

A. Simulation Setup

In order to illustrate the efficacy of our proposed algorithm, we first adopt the average speed model in (1) for different types of ICEVs with the parameters a, b, c, d, e, f, g, k illustrated in Table I. The resulting emission functions for six types of ICEVs are shown in Fig. 3.

It is clear to see from Fig. 3 that for same emission standard, e.g. Euro 3, increasing engine capacity of the vehicles, i.e. R004, R011 and R018, will also increase the CO_2 amount for a given average speed.

We now perform the following experiments.

1) In the first case, we assume that there are six vehicles, one vehicle in each class as outlined in Table I. Also, we assume that the topology of the vehicular network is static and strongly connected. In particular, each vehicle is assumed to be connected circle-wise, that is vehicle 1 has one neighbour vehicle 2, vehicle 2 has one neighbour vehicle 3, likewise, up to vehicle 6
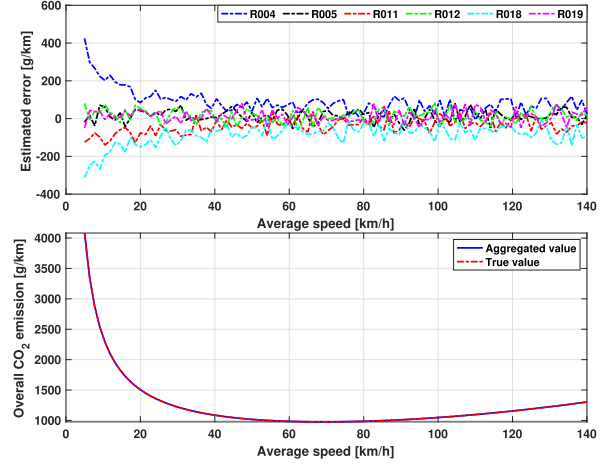

Fig. 4. Local estimated error (upper plot) and aggregated curve seen from the base station (lower plot) for the first case.
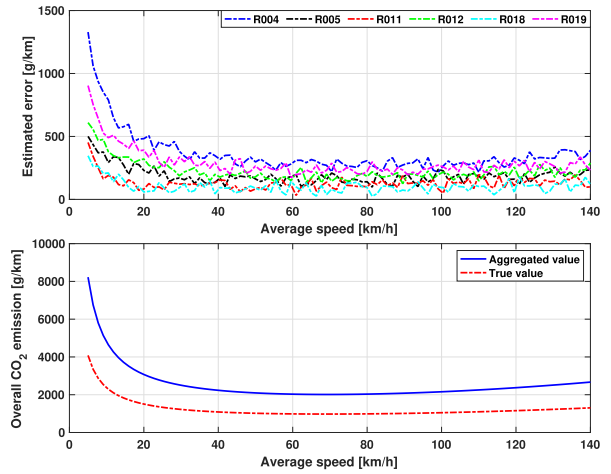

Fig. 5. Local estimated error (upper plot) and aggregated curve seen from the base station (lower plot) for the second case.

which has one neighbour vehicle 1. Finally, we set $M = 100$ which linearly spaces the speed in the range of $[5, 140]$km/h, and with the mapping function $g(f_i(s_i)) = f_i(s_i)$.

2) In the second case, we assume that the system setup is the same to the first case, but with the mapping function $g(f_i(s_i)) = 2 f_i(s_i) + 10$.

3) In the third case, we assume that there are 20 vehicles for each emission type, and the vehicular network is still static and strongly connected, but with $M = 20, 30, \ldots, 100$ with the same mapping function in the second case.

B. Simulation Results

Our simulation results for each individual case study listed above are shown in Figs. 4 - 6, respectively. In Fig. 4, we show that the local estimated error from each vehicle has been different from zero, which indicates that no vehicle can correctly identify other vehicles' cost functions by using the secret sharing mechanisms. However, with a basic mapping function $g(x) = x$, the overall cost function seen from a base station is the same with the ground truth, which demonstrates that the privacy of the overall cost function does not preserve well to a central agent in this case. To improve this, we now impose a new linear mapping function $g(x) = 2x + 10$, and it is clear to show from Fig. 5 that privacy for both local and the central agents have been preserved well by using our proposed algorithm while without affecting the optimal solutions of the original problem.
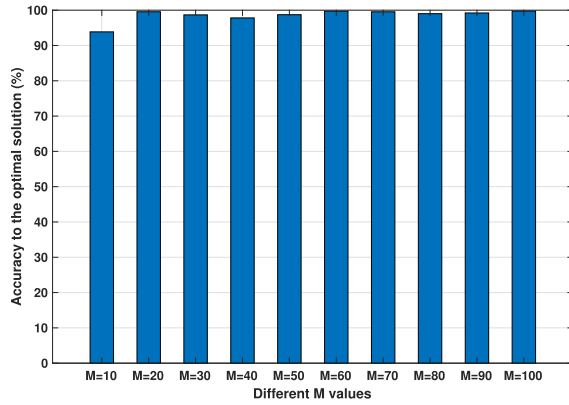
Fig. 6. Accuracy of our proposed method compared to the true optimal solutions with respect to M.

Finally, the results in Fig. 6 compare the accuracy of optimal solutions by using the proposed algorithm with respect to varying values of M within a set. Clearly, when M is chosen as the lowest value in Fig. 6, i.e. with only 10 data points linearly sampled in the given speed range, the algorithm can perform well by reaching to over 90% optimality in simple one algorithm iteration. For other cases shown in the figure, we find out that the accuracy is almost identical and nearly 100% due to the fact that the converged optimal recommended speed is much close to the true optimal value of the original optimization problem. This fact further shows the efficacy to deploy the proposed algorithm in real-time CSAS scenarios, i.e. the value M is not quite sensitive to the accuracy of the optimal solution in our problem. As a final remark, we note that the above simulation results are also applicable to time-varying network having uniformly strongly ergodic property. The stability and convergence of the time-varying graph is guaranteed by our results in [21]. The optimality and consistency of the result is guaranteed by the mechanism of the proposed MPC-CSAS algorithm.

V. Conclusion

In this article, we propose a new design for CSAS based on the MPC protocols, namely MPC-CSAS. We have shown that by using the ideas of secret generation and sharing, users' privacy can be designed and preserved both locally and globally for a CSAS application, that is no other vehicles or a base station in the network can infer the original cost function associated with each vehicle, which may contain a user's critical/sensitive information. We have discussed the applicability and feasibility to deploy the MPC-CSAS with both static and strongly connected network as well as time-varying network which satisfies uniformly strongly ergodic property linked to graph theories. We have validated the efficacy of the proposed algorithm in SUMO simulations. One of the assumptions we made in this article is that a participated vehicle can trust the information received from other vehicles in the network, which may potentially cause security concerns to the participated vehicle. In light of this, we will explore trustiness detection strategies such as how to use blockchain to record trustiness of the involved vehicles as part of our future work. We will also explore how the proposed MPC-CSAS can be adapted to more complex networks for novel scenarios in ITS.

References

[1] N. B. Hounsell, B. P. Shrestha, J. Piao, and M. Mcdonald, "Review of urban traffic management and the impacts of new vehicle technologies," *IET Intell. Transp. Syst.*, vol. 3, no. 4, pp. 419–428, Dec. 2009.

[2] N. Tradisauskas, J. Juhl, H. Lahrmann, and C. S. Jensen, "Map matching for intelligent speed adaptation," *IET Intell. Transport Syst.*, vol. 3, no. 1, pp. 57–66, Mar. 2009.

[3] S. Darbha, S. Konduri, and P. R. Pagilla, "Benefits of V2 V communication for autonomous and connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 5, pp. 1954–1963, May 2019.

[4] Y. Gu, M. Liu, E. Crisostomi, and R. Shorten, "Optimised consensus for highway speed limits via intelligent speed advisory systems," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Nov. 2014, pp. 1052–1053.

[5] M. Liu, R. H. Ordonez-Hurtado, F. Wirth, Y. Gu, E. Crisostomi, and R. Shorten, "A distributed and privacy-aware speed advisory system for optimizing conventional and electric vehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1308–1318, May 2016.

[6] D. Helbing and B. A. Huberman, "Coherent moving states in highway traffic," *Nature*, vol. 396, no. 6713, pp. 738–740, Dec. 1998.

[7] M. Barth, K. Boriboonsomsin, and G. Wu, "The potential role of vehicle automation in reducing traffic-related energy and emissions," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Dec. 2013, pp. 604–605.

[8] M. M. Waldrop, "Autonomous vehicles: No drivers required," *Nature*, vol. 518, no. 7537, pp. 20–23, Feb. 2015.

[9] P. Fernandes and U. Nunes, "Platooning of autonomous vehicles with intervehicle communications in SUMO traffic simulator," in *Proc. 13th Int. IEEE Conf. Intell. Transp. Syst.*, Sep. 2010, pp. 1313–1318.

[10] Y. Gu, M. Liu, M. Souza, and R. N. Shorten, "On the design of an intelligent speed advisory system for cyclists," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2018, pp. 3892–3897.

[11] P. Boulter, T. Barlow, and I. McCrae, "Emission factors 2009: Report 3-exhaust emission factors for road vehicles in the United Kingdom," TRL Limited, Wokingham, Crowthorne, U.K., Tech. Rep. PPR356, 2009.

[12] R. Gallen, N. Hautiere, A. Cord, and S. Glaser, "Supporting drivers in keeping safe speed in adverse weather conditions by mitigating the risk level," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 4, pp. 1558–1571, Dec. 2013.

[13] W. Shi, Q. Ling, K. Yuan, G. Wu, and W. Yin, "On the linear convergence of the ADMM in decentralized consensus optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1750–1761, Apr. 2014.

[14] W. J. Schakel and B. van Arem, "Improving traffic flow efficiency by in-car advice on lane, speed, and headway," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1597–1606, Aug. 2014.

[15] R. H. Ordó nez-Hurtado, W. M. Griggs, K. Massow, and R. N. Shorten, "Intelligent speed advising based on cooperative traffic scenario determination," in *Optimization and Optimal Control in Automotive Systems*. Cham, Switzerland: Springer, 2014, pp. 77–92.

[16] W. Griggs, G. Russo, and R. Shorten, "Leader and leaderless multi-layer consensus with state obfuscation: An application to distributed speed advisory systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 3, pp. 711–721, Mar. 2018.

[17] N. Volgushev, M. Schwarzkopf, B. Getchell, M. Varia, A. Lapets, and A. Bestavros, "Conclave: Secure multi-party computation on big data," in *Proc. 14th EuroSys Conf.*, Mar. 2019, pp. 1–18.

[18] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[19] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1999, pp. 148–164.

[20] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO-simulation of urban MObility," in *Proc. 3rd Int. Conf. Adv. Syst. Simulation (SIMUL)*, 2011, pp. 55–60.

[21] M. Liu, F. Wirth, M. Corless, and R. Shorten, "On the stability and convergence of a class of consensus systems with a nonlinear input," *Automatica*, vol. 86, pp. 205–211, Dec. 2017.

Mingming Liu received the B.E. degree (Hons.) in electronic engineering from the National University of Ireland, Maynooth, in 2011, and the Ph.D. degree from the Hamilton Institute, Maynooth University, in 2015. He was a Senior Post-Doctoral Researcher University College Dublin and also a Data Scientist, an Applied Researcher, and H2020 Project Lead with the IBM Ireland Lab. He is currently an Assistant Professor with the School of Electronic Engineering, Dublin City University. His research interests include control and optimization theories with applications to 5G & IoT, electric vehicles, smart grids, intelligent transportation systems, and smart cities.

Long Cheng received the B.E. degree from the Harbin Institute of Technology, China, in 2007, the M.Sc. degree from the University of Duisburg-Essen, Germany, in 2010, and the Ph.D. degree from the National University of Ireland, Maynooth, in 2014. He was an Assistant Professor with Dublin City University and a Marie Curie Fellow with University College Dublin. He has also worked at organizations such as Huawei Technologies, Germany, IBM Research, Dublin, TU Dresden, and TU Eindhoven. He is currently a Professor with the School of Control and Computer Engineering, North China Electric Power University, Beijing. His research interests include high-performance data analytics, distributed systems, cloud computing, and process mining.

Yingqi Gu received the M.Sc. degree from the School of Engineering, The University of Edinburgh, and the Ph.D. degree in control engineering and decision science from the School of Electrical and Electronic Engineering, University College Dublin. She was a Post-Doctoral Research Fellow with the Insight Centre for Data Analytics, Dublin City University, and the Adjunct Lecturer with Maynooth University. She is currently a Senior Data Scientist with Alkermes plc. Her current research interests include AI & machine learning, control and optimization theories with applications to EVs, intelligent transportation systems, and digital health.

Ying Wang received the B.E. and M.S. degrees in electrical engineering from the Harbin Institute of Technology in 2007 and 2009 respectively, and the Ph.D. degree in computer science from ICT, CAS, Beijing, in 2014. He is currently an Associate Professor with the Institute of Computing Technology (ICT), Chinese Academy of Sciences (CAS). His research interests include computer architecture and VLSI design, specifically memory systems, on-chip interconnects, resilient and energy-efficient architecture, and machine learning accelerators.
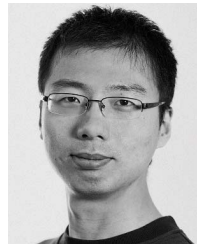
Qingzhi Liu received the B.S. and M.Eng. degrees from Xidian University, China, in 2005 and 2008, respectively, and the M.Sc. *(cum laude)* and Ph.D. degrees from the Delft University of Technology, The Netherlands, in 2011 and 2016, respectively. From 2016 to 2019, he was a Post-Doctoral Researcher with the Eindhoven University of Technology, The Netherlands. He is currently a Lecturer with the Information Technology Group, Wageningen University & Research, The Netherlands. His research interests include the IoTs and artificial intelligence.

Noel E. O'Connor (Member, IEEE) was the Academic Director of DCU's Research and Enterprise Hub on Information Technology and the Digital Society, with the responsibility of coordinating multi-disciplinary ICT-related research across the university. He is currently a Full Professor with the School of Electronic Engineering, Dublin City University (DCU), Ireland. He is also a CEO of the Insight SFI Research Centre for Data Analytics, Ireland's largest SFI-funded research centre. Since 1999, he has published more than 400 peer-reviewed publications, made 11 standards submissions, and filed 7 patents. His research interests include multimedia content analysis, computer vision, machine learning, information fusion and multi-modal analysis for applications in security/safety, autonomous vehicles, medical imaging, the IoT and smart cities, multimedia content-based retrieval, and environmental monitoring. He is a member of the ACM. He is an Area Editor of *Signal Processing: Image Communication* (Elsevier) and an Associate Editor of the *Journal of Image and Video Processing* (Springer).