Privacy-preserving carpooling

Ulrich Matchi Aïvodji, Sébastien Gambs, Marie-José Huguet, Marc-Olivier Killijian

Privacy-preserving carpooling*

Ulrich Matchi Aïvodji[1,2], Sébastien Gambs[3], Marie-José Huguet[1,4], Marc-Olivier Killijian[1]

[1] Université de Toulouse, LAAS-CNRS, F-31400 Toulouse, France
{umaivodj, killijian, huguet}@laas.fr
[2] Université de Toulouse, Paul Sabatier, F-31062 Toulouse, France
[3] Université de Rennes 1 - Inria / IRISA, Rennes, France
sebastien.gambs@irisa.fr
[4] Université de Toulouse, INSA, F-31400 Toulouse, France

Keywords: *Carpooling, Multi-modal routing, Privacy enhancing technologies, Secure multi-party computation, Distributed algorithms.*

1 Introduction

Mobility has always been an important aspect of human activities. Nowadays problems of congestion in urban areas due to the massive usage of cars, last-minutes travel needs and progress in information and communication technologies encourage the rise of new transport modes. Among those are carpooling services, which let car owners share the empty seats of their cars with other travellers having the same travel direction.

In a carpooling scenario, illustrated in Figure 1, we have a driver and a pedestrian, each with an origin and a destination. The driver is looking for a passenger and is willing to take a detour in order to pick him up while the pedestrian is looking for an itinerary in which he may use carpooling.

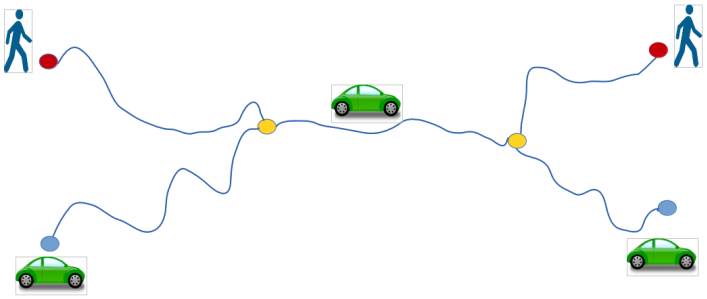

Figure 1: Illustration of a carpooling scenario

The objective of the carpooling service is to find for both of them a pick-up and drop-off location and optimal itineraries for their journeys.

Most of current systems for carpooling have two main limitations. The first one is related to the real time consideration. In fact, until now, to plan theirs journeys, pedestrians have to choose among

*This work is partially supported by the ANR French project AMORES (ANR-11-INSE-010) and the INRIA Project Lab CAPPRIS (Collaborative Action on the Protection of Privacy Rights in the Information Society)

a list of itineraries predefined by the driver. In addition there is no consideration of the time taken by pedestrians in public transportation and additional walking time. However recent works [1], have considered this issue and proposed methods to solve it using a centralized solution. The second problem is precisely with the respect to the centralized nature of this infrastructure. Indeed, actual carpooling services rely on centralized platforms in charge of collecting and storing sensitive data from carpooling users and computing itineraries. This situation could lead to important damages to the privacy of users. For instance, malicious individuals can use sensitive data (like location) stored on the centralized platform to cause a privacy breach [2]. For example malicious individuals can learn their Points Of Interest (POIs), compute their mobility models to infer their future movements or even de-anonymize them in another geolocated dataset.

The aim of this paper is to promote a new approach of carpooling implementation relying on a distributed platform and privacy enhancing technologies.

2 Privacy-preserving carpooling

To guarantee the protection of the privacy of users, we want to ensure these three desiderata:

- The location data (origin and destination) of each user is private.
- The computation of itineraries is distributed (and not centralized).
- Collaboration between different users relies on secure multi-party computation techniques.

The secure multi-party computation (SMPC) is a set of cryptographic techniques used to compute a function depending of the inputs of several parties in a distributed manner, so that only the result of the computation is revealed and the inputs of each party remain secret [3]. Yao first defined the two-party comparison problem now known as Yao's Millionaires' problem and developed a provably secure solution [4] for this problem. Since this seminal work, a lot of works have been done in the field of secure computation. The SMPC can occur in tasks as simple as coin-tossing and broadcast, and as complex as electronic voting, electronic auctions, electronic cash schemes, contract signing, anonymous transactions, and private information retrieval schemes.

We use a specific instance of SMPC called Private Set Intersection (PSI). PSI allows different parties to securely compute the intersection of their entries sets without revealing any other information [3]. Our implementation of private set intersection (PSI) protocols is based on oblivious polynomial evaluations and interpolations [5]. The main idea of this technique is to represent a set as a polynomial, the elements of the set as its roots and evaluate this polynomial homomorphically. An homomorphic encryption scheme is an encryption scheme that allows certain algebraic operations to be carried out on the encrypted plaintext, by applying an efficient operation to the corresponding ciphertext [3]. Our solution also relies on several shortest path algorithms in multi-modal transport graph with time-dependency consideration [1]. We particularly consider isochrones algorithms that compute, given a starting location and a method of travel (walking, biking, public transit, driving), all reachable locations within a given amount of time.

Our solution can be formalized as follow: let X be the pedestrian, Y the driver and G a multi-modal graph.

Sketch of protocol Secure computation protocol for carpooling

1: X : Computes P_x and D_x, corresponding to his potential pick-up and drop-off locations
2: Y : Computes P_y and D_y, corresponding to his potential pick-up and drop-off locations
3: X and Y : Compute $I{=}P_x \cap P_y$ and $J{=}D_x \cap D_y$ using PSI. Let C_{xi} (respectively C_{y_i}) and C_{xj} (respectively C_{y_j}) be the cost of a pick-up location in I for X (respectively Y) and the cost of a drop-off location in J for X (respectively Y)
4: X and Y : Get all paths T_{ij} between I and J and navigable by car
5: X : Computes for each T_{ij} a score S_{ij}^X according to $C_{xi}{+}T_{ij}{+}C_{xj}$
6: Y : Computes S_{ij}^Y according to $C_{y_i}{+}T_{ij}{+}C_{y_j}$
7: X and Y : Get the best path T_{ij} that is the one maximizing the value of $S_{ij}^X + S_{ij}^Y$. By doing so they also get the pick-up point i and the drop-off point j

By using this protocol we have the guarantee that locations of each participant are kept private.

Finally we have proposed a global architecture to implement our solution in real-world. This architecture is based on the publish/subscribe model. Let Bob be a driver candidate for a carpooling scenario and Alice the pedestrian.

Real world scenario Use case example

1: *Alice* : Subscribes to the topic *Carpooling*
2: *Bob* : Publishes on the same topic as soon as he is ready for a carpooling.
3: *Alice* : Launches the protocol mentioned previously with *Bob* as soon as she gets the notification's message.
4: *Alice* and *Bob* : Get pick-up and drop-off locations
5: *Alice* : Can repeat the scenario with others drivers until she finds a configuration that satisfies her time constraints.

Our protocol also solves the problem of the static nature associate to carpooling services with using of publish/subscribe model that aims the driver to find a new passenger on the fly.

3 Experiments

In this section, we present the experiments that we have conducted to evaluate the efficiency of our solution. Tests have been performed on 50 randomly generated instances of carpooling problem in Toulouse city. We have implemented two versions of distributed carpooling algorithms that differ in the way the sets P_x, P_x, D_x and D_y are computed. In the first version (iso-iso) these four sets are obtained with isochrones algorithms on both driver and pedestrian side while in the second version (iso-A*) P_x and D_x are obtained with isochrones and P_y and D_y with A* in order to minimize the detour taken by the car. Isochrones limit's has been fixed to 30 minutes [1] with 1 minute step which allows to stop as soon as a solution is found. A* computes the shortest path (origin-destination) with an average speed of 30 km/h. The set of vertices labeled by both A* and isochrones defines potential carpooling locations set. Results in Table 1 show that the gap between the carpooling cost in distributed and centralized approach is acceptable and that distributed approach takes significantly more time than centralized approach.

This increase in time observed in distributed approach is due to the PSI protocol. PSI execution

[1] This 30-minutes limit condition ensures for the relevant graph, the existence of a carpool solution

	average cost (s)	average runtime (s)
Centralized	2295.78	2.75
Distributed iso-iso	2629.40	12.34
Distributed iso-astar	2733.80	19.06

Table 1: Cost and runtime analysis

time increases polynomially with the size of the input data. However, the PSI runtime is expected to drop significantly due to recent advances in homomorphic encryption [6].

4 Conclusion

In this paper, we have proposed a secure protocol enabling users to interact in a private and trusted way to run a carpooling service. The protocol has solved the problem of dynamism associated to current carpooling services. Our future works will integrate many-to-many aspects in our protocol such as a pedestrian can use more than one car during his journeys. Our results show that the use of the implemented privacy enhancing technologies can help solve carpooling problem while respecting users privacy with appreciable results compared to centralized approach. However, some progress need to be done to reduce the global running time in order to make this approach usable in real-time applications.

We are also ambitious to extend the multi-party secure computation techniques used in this paper to others mobility problems including goods transportation in which different companies want to collaboratively manage the transportation of their raw material and goods in order to reduce costs and without disclosing their private information such as limited resources.

References

[1] A. Bit-Monnot and C. Artigues and M.J. Huguet and M.O. Killijian, "Carpooling: the 2 Synchronization Points Shortest Paths Problem", *Proceedings of the 13th Workshop on Algorithmic Approaches for Transportation Modelling, Optimization, and Systems*, 150–163 (2013).

[2] S. Gambs and M.O. Killijian and D.P. Cortez and M. Nunez, "Show Me How You Move and I Will Tell You Who You Are", *Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, 34–41 (2010).

[3] Y. Lindell and B. Pinkas, "Secure Multiparty Computation for Privacy-Preserving Data Mining", *IACR Cryptology ePrint Archive*, 197 (2008).

[4] A. C. Yao, "How to generate and exchange secrets", *Proceedings of the 27th IEEE Symposium on Foundations of Computer Science*, 162–167 (1986).

[5] "Practical Private Set Intersection Protocols with Linear Complexity", *Proceedings of the 14th International Conference, FC 2010, Tenerife, Canary Islands, January 25-28*, 143–159.

[6] C. Aguilar-Melchor and J. Barrier and L. Fousse and M.O. Killijian, "Private Information Retrieval for Everyone", *Cryptology ePrint Archive, Report 2014/1025.*