Privacy-Preserving Fair Meeting Point Agreement

Mohamed Taoufiq Damir, Gizem Akman
Kuan Eeik Tan, Philip Ginzboorg, Sampo Sovio, Valtteri Niemi

[1] University of Helsinki
[2] Huawei Technologies

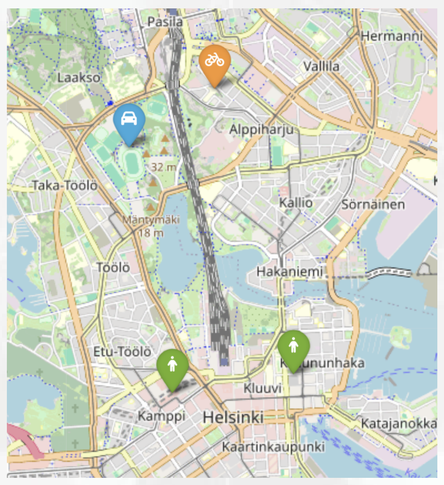
[1] mohamed.damir@helsinki.fi, [1] valtteri.niemi@helsinki.fi
, [1] gizem.akman@helsinki.fi, [2] kuan.eeik.tan@huawei.com, [2] sampo.sovio@huawei.com,
[2] philip.ginzboorg@huawei.com

The Problem

n parties want to agree on a meeting location.

Our aim is to propose a privacy-preserving meeting point protocol, while taking into account the following requirements:

1. The meeting location should be fair and convenient.
2. The parties' initial locations should not be revealed to each other or anybody else.
3. The meeting location should be revealed only to the parties and no one else.
4. Recommend an Estimated Time of Meeting.
5. Support dynamical scenarios, i.e., adding and removing participants, ETM changes.
6. The participants are honest-but-curious.
7. No *trusted third party*.



Towards a Fair Meeting Point

Given a set of locations, possible strategies to define a fair meeting point include:

1- Finding a point minimizing the maximum distance to all locations.
2- Finding a point minimizing the sum of distances to the given locations.
3- Finding the point minimizing the sum of the squares of distances from the given locations.

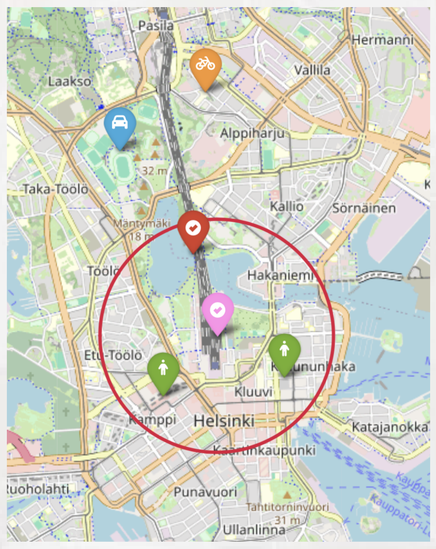
In the case of Euclidean distance, method (3) is achieved by the centroid, and it is the most efficient (computationally). For more fairness, we use the weighted centroid of the locations' set $(x_1,x_2,\cdots,x_n)$ with the weights $(w_1,w_2,\cdots,w_n)$ defined by

$$C = \frac{w_1x_1 + w_2x_2 + \cdots + w_nx_n}{w_1 + w_2 + \cdots + w_n},$$

where the weights are proportional to the participants' speed.

Towards a Convenient Meeting Point

- The participants use MPC to compute an initial point, i.e., the weighted centroid.
- Define a circle $\mathcal{C}$ around C with radius proportional to the slowest participant.
- Get a list of potential meeting points in $\mathcal{C}$, e.g., locally or by using an LBS+obfuscation.
- Run a privacy-preserving voting protocol, e.g., participants assign a score to each location, then use MPC to sum the scores.
- The ETM is the maximal ETA among all the participants, e.g., a privacy-preserving Dutch auction protocol can be used here.



Dynamic Navigation

Our protocol satisfies the following dynamic features:

- The protocol checks periodically, i.e., for some period Δ, if the participants ETA is still less than the group ETM, if not, ETM is updated in a PP way.
- The meeting point can be updated if someone changes their location, the price is to reveal their location change δ.
- When the number of participants joining or leaving is one or two, the meeting place does not change. The meeting point can be updated in a privacy-preserving way if the number of joining/leaving participants is at least three.

Performance Analysis

We delegate collective computations to a group admin, e.g., the participant who initiated creating the group. Thus, the worst case communication overhead is given at the admin level. The following Table 1 illustrates the operations on the group admin's side.

Table 1 – The number of sent messages by the group leader per protocol phase (the case of n users)

Phase	**Number of Messages**
Centroid computation	n
Determining the circle	0
Choosing potential points	2
Travel distance and time	1
Ranking the meeting points	0
Sum of votes	n
The estimated time of meeting	1
Total	$2n+4$

Computational cost: In the case of $n = 3$, the average total time for the protocol is 0.8 s. This includes the time taken by the LBS to send the candidate locations.

Security Analysis

Assuming the following adversarial model:

- The participants, the server, and LBS are assumed to be honest-but- curious.
- the participants are assumed to have a pre-established pairwise secure channel

Our protocol achieves the following security properties:

- **The Meeting Point Secrecy**: The meeting point is only known to par- participants by the end of the protocol.
- **The ETM secrecy**: The ETM is only revealed to the participants over the secure group channel.
- **The preference-privacy**: For k candidate locations, each participant votes for their favourite location in a privacy-preserving way.
- **The Location Privacy:** The weighted centroid is computed without revealing the initial locations. However, the centroid C may leak some information about a participant's location X. The information leakage can be estimated by

$$\mathcal{L}(X \to C) = \frac{P_m(X|C)}{P_m(X)},$$

where $P_m(X|C) = \sum_{c\in C} P(c) \max_{x\in X} P(x|c)$, and $P_m(X) = \max_{x\in X} P(x)$.

There is an unavoidable vulnerability, that is when one of the parties is compromised, then the meeting point and the ETM are revealed to the adversary. However, the participants' locations are still not compromised even if the adversary compromised a number ($\leq n-2$) of participants .