# Mobility Data Anonymization by Obfuscating the Cellular Network Topology Graph

Eduardo Baena Martinez, Michal Ficek, Lukas Kencl
Faculty of Electrical Engineering
Czech Technical University in Prague
Prague, Czech Republic
{baenaedu,michal.ficek,lukas.kencl}@fel.cvut.cz

*Abstract*—**Studies of cellular-network data, comprising analyses of user movements across the network, are becoming increasingly popular with the rise of new services based on user behavior and geographic location. Such data might contain, for example, timestamped lists of IDs of cells a user was registered to. If coupled with the cell locations, confidential to the operator, this would enable reconstruction of user trajectories across the regions covered. It is vital to preserve privacy of this data for all parts involved (users, operators) while enabling open sharing of the data to foster research and development of new findings, services and technologies based on mining of this data. Thus, we pose the problem of obfuscating entire cellular-network topologies while retaining some of the analytical value of the user data. To this end, we adopt multiple obfuscation methods based on different topology-graph distortions, and analyze their performance using simulated scenarios.**

## I. Introduction

Contemporary mobile technologies easily allow the collection of information about user location and behavior. Such information is often used to provide personalized services or for other commercial, monitoring or optimization purposes [1]. Mobile operators show a growing interest to share this kind of data with third party partners in order to obtain profitable knowledge by mobility mining techniques [2]–[4]. However, the use of mobility data has compromised privacy of users who can be identified effortlessly based on the most common places they stay [5]. Besides, mobile operators sharing their location registers are risking sensitive and strategic information such as the map of Base Station (BS) placements, used as reference to determine the users position.

The main motivation of this work is to enable sharing of cellular-network tracking data without revealing the real positions of the BSs, thus avoiding network identification and helping to preserve users' privacy. We use two methods of obfuscating the network topology by distorting the placements of BS while preserving the structural and statistical properties. We evaluate the extent of such topology transformation from the perspectives of reversibility and property-preservation.

Mobility data can be represented by Cell-ID tracking [4], a timestamped history of cells the users visited over a particular time period, conforming a set of trajectories. Usually, such trajectories are anonymized by means of changing the coordinates of trajectory point [6], however, we propose to apply the original trajectory description over an obfuscated network topology, thus avoiding exposure of the real BS placements.

We represent the network topology as a planar graph and use the Voronoi tessellation [7] to approximate cellular network radio coverage. The neighborhood of the cells is captured by the Delaunay triangulation [7], the dual graph of Voronoi tessellation. We call such triangulation, together with a vector of positions of the graph nodes, a Cellular Network Topology Graph (CTG) (for details see Section III). The obfuscated CTG is called OCTG. A naïve approach to generate an OCTG might be to apply linear transformations (translation, rotation, and reflection) to the original CTG. However, these operations can be easily reverted and the true BS placements can be found if the real geographical positions of only two nodes are exposed (or guessed). Instead, we propose the OCTG to be a new planar embedding with different positions of the nodes, but similar statistical properties when compared to the original CTG. These properties are related to edge-length distribution and the distances between corresponding nodes in the CTG and the OCTG, respectively.

In this paper we discuss the possibility of an OCTG to meet the following:

*(i) OCTG Properties:*

- The OCTG preserves triangulation, planarity and cell neighborhood of the CTG.
- The coordinates of corresponding nodes in the OCTG are not close to the real CTG's nodes.

*(ii) Consistency of tracking data applied over the OCTG when compared to the original CTG:*

- Distance traveled by users is preserved.
- Geographical closeness, i.e., the relative distance between moving users along their path, is preserved.
- The shape of users' trajectories is preserved.

## II. Related work

*Location privacy* [8] is currently widely discussed due to the fast spread of mobile networks and positioning systems.

One of the main concerns regards the user's identity privacy, since its vulnerability has been shown to be surprisingly high [5]. Among the proposals to anonymize this data we find obfuscation by manipulation (cloaking) of the tracking record [6], which implies processing of each single location query. Anonymity-preserving publishing of personal mobility data [9] can be realized by adding dummy events or locations.

978-1-4673-3122-7/13/$31.00 ©2013 IEEE

A formal framework to evaluate and measure the anonymization procedures for mobility data has been presented [10].

Spatial $k$-anonymity [11] is a concept of location privacy, where the obfuscated user locations or trajectories cannot be identified beyond the set of other $k-1$ users. The majority of systems use a centralized architecture [12], in which a trusted entity (anonymizer) acts as a proxy updating actual user locations. In a decentralized architecture [13], each device alone or by cooperation with others makes the transformation to avoid exact identification.

In contrast to the anonymization concepts in [10], where every tracking record is altered, we consider the cellular network topology to be the principal identification reference element in all tracking systems. Thus, when such topology is distorted, a hypothetical attacker cannot recognize which network or geographical location the users are being tracked over. Consequently, the users' identity privacy is also preserved.

## III. Cellular Network Topology Model

A cellular network topology is represented by a set of points in the plane, $P = \{p_1, p_2, ..., p_n\},\ p_i \in \mathbb{R}^2$, which correspond to the real, geographical locations of the Base Stations (BS). Each BS hosts an antenna[1] that serves an area approximated by a *Voronoi tessellation* [7] cell $V(p_i)$, a set of points in the plane closer to the *nucleus* $p_i$ than to any other point $p_j$. Each BS's coverage thus corresponds to exactly one Voronoi cell.

To model handovers between cells in the network, let us consider a dual graph to Voronoi tessellation: the nodes of this new graph are the Voronoi cells nuclei and an edge between two nodes exists if and only if the corresponding Voronoi cells share a common edge. Such graph is called a *Delaunay triangulation* [7]. All its planar-embedding faces except the exterior face are triangles. Edges in the Delaunay triangulation for a point set $P = \{p_1, p_2, ..., p_n\}$ can be represented by an adjacency matrix $A \in \{0,1\}^{n \times n}$, where $A_{i,j} = 1$ if and only if there exists an edge between points $p_i$ and $p_j$ such that $i \neq j$, and $A_{i,j} = 0$ otherwise. Such a matrix represents possible handovers between the cells in the network.

### A. Cellular Network Topology Graph

We define the *Cellular Network Topology Graph* (CTG) as a pair $(P, A)$, where $P$ stands for Base Stations coordinates and $A$ is the adjacency matrix given by the Delaunay triangulation for the point set $P$. Such description of a cellular network topology is unique for a given point set $P$, which stems from properties of Delaunay triangulation [7]. The CTG allows for straight-line planar drawing, simply by joining points $P$ according to the adjacency matrix $A$, which is a principal visualization of network topology (see Fig. 1). Without loss of generality we assume that the CTG is 3-connected[2]. A subset of nodes that form the convex hull (CH, the outer face) of the nodes $P$ in a CTG will be denoted $CH$.

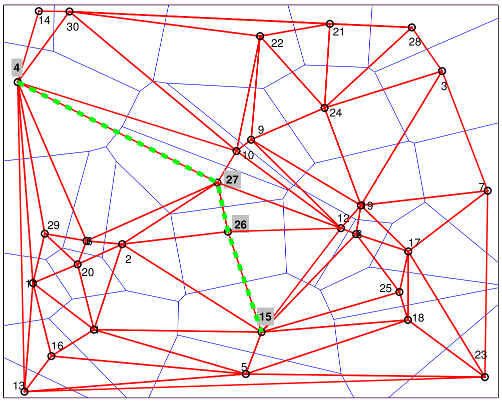


Fig. 1. Cellular Network Topology Graph. Black circles represent BSs, blue lines define Voronoi cells, red lines stand for Delaunay triangulation, green dashed line shows a sample path S={4,27,26,15}.

### B. User Mobility over a Cellular Network Topology Graph

User's movement within the network is usually captured in tracking data by a timestamped sequence of BSs they have been attached to. More formally, tracking data consist of a finite, time-ordered series of BSs transitions: $\mathbb{S} = \{(s_1, t_1), (s_2, t_2), \ldots, (s_l, t_l)\}$. Since this work focuses solely on spatial dimension of users' movement, we further use only the BSs transitions and omit the temporal dimension.

We define a *path* of $l$ steps made by a user $u$ over a particular CTG $(P, A)$, denoted $S_l^u = \{s_1, \ldots, s_l\}$, as a sequence of $l$ BSs identifiers $s_i \in \{1, \ldots, n\}$ in which

*a)* every two succeeding identifiers differ, i.e.,

$$\forall k < l : s_k \neq s_{k+1}, \text{ and} \tag{1}$$

*b)* transition is made only between neighbor BSs:

$$\forall k < l : A_{s_k, s_{k+1}} = 1. \tag{2}$$

Let $T(S_l^u)$ denote a *trajectory* of user's movement over the CTG $(P, A)$, simply defined as a sequence of BSs positions according to the BSs identifiers in the path $S_l^u = \{s_1, \ldots, s_l\}$:

$$T(S_l^u) = \{p_{s_1}, p_{s_2}, \ldots, p_{s_l}\}. \tag{3}$$

We define the *length* of a user's trajectory $T(S_l^u)$ as a sum of edge lengths $e_i = \|p_{s_i}, p_{s_i+1}\|$ (where $\|p_{s_i}, p_{s_i+1}\|$ denotes the Euclidean distance) within the trajectory:

$$L(T(S_l^u)) = \sum_{i=1}^{l-1} e_i. \tag{4}$$

## IV. Obfuscation of Cellular Network Topology

By *obfuscation* we mean a one-time process that avoids easy identification of a cellular network topology by a potential attacker while preserving the analytical value of the represented information, such as neighbor relations between BSs, distances, or user trajectories shape and length. Obfuscation is a cellular network topology transformation leading to a similar graph, but with different BSs positions (see e.g. Fig. 2).

More formally: a graph is planar if it can be drawn in the plane without edge crossings, and if all its faces except the exterior face are triangles, then it is a triangulation. Two graphs

[1] For simplicity, we assume that each BS has only one omnidirectional antenna, covering the 360° radius.

[2] In a 3-connected graph there do not exist any two nodes whose removal disconnects the graph. Most communication graphs have 3-connected planar subgraph [14].

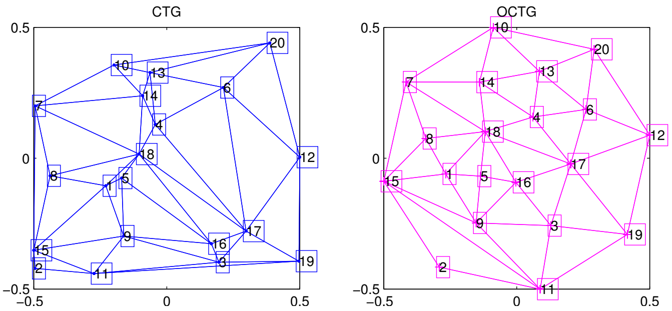


Fig. 2. Example of a random CTG with 20 nodes and one possible OCTG (created by the FDOA method using a circular convex hull, see Section V)

are isomorphic if there exists a one-to-one correspondence between their vertices such that the corresponding edges link corresponding vertices. Our objective is, given a CTG $(P, A)$, to generate a straight-line planar drawing of a triangulated isomorphic graph, called *Obfuscated Cellular Network Topology Graph (OCTG)* $(P', A')$, such that $\forall i : p'_i \in P' \neq p_i \in P$, $A' = A$ and the isomorphism given by a bijection $f : P \to P'$, $f(p_i) = p'_i$. Paths, trajectories, and the convex hull over the OCTG are denoted $S'$, $T'$, and $CH'$ respectively.

### A. Obfuscation objectives

The objectives we place on the obfuscation process and the resulting OCTG are twofold. Firstly, the CTG graph-related properties such as nodes correspondence and their and neighborhood relationship must be preserved. Secondly, the straight-line planar drawing of the OCTG must be different enough when compared to the CTG, yet the analytical value of studying user trajectories over the OCTG should be similar to when trajectories are examined over the original CTG. A detailed description of the characteristics of the CTG we want to change or preserve in the OCTG is as follows:

*1) The neighbor relationship between nodes is preserved:* To enable study of user' mobility over the OCTG, the paths description over the CTG and the OCTG must be identical ($S^u_l = S'^u_l$). Therefore, neighbor relationship between BSs (handovers between cells) must remain intact in the OCTG.

*2) Distribution of distances between corresponding nodes is uniform:* A natural measure of the obfuscation process performance could be the distance between corresponding nodes in the CTG and the OCTG — the higher the distance between corresponding nodes, the higher the degree of obfuscation. However, this would make a poor measure because even a simple Euclidean translation can result in high but identical distances between the corresponding nodes. We therefore consider the *distribution of distances* between corresponding nodes a better measure. A well obfuscated OCTG should have the distances uniformly distributed on an interval that corresponds to the maximal distance of any two CTG points.

*3) Length of users' trajectories is preserved:* Let us consider a trajectory $T(S^u_l)$ over the CTG and a corresponding trajectory $T'(S'^u_l)$ over the OCTG, i.e., $S^u_l = S'^u_l$. We define a ratio of trajectories length as follows:

$$RTL = \frac{L(T'(S'^u_l))}{L(T(S^u_l))}. \tag{5}$$

A value of $RTL$ close to 1 means that the length of the trajectory over the OCTG, i.e., the distance traveled by the user, is preserved.

*4) Shape of users' trajectories is preserved:* Given corresponding trajectories $T(S^u_l)$ and $T'(S'^u_l)$, we use a Procrustes distance $D(T, T')$ [15] as a *dissimilarity measure* of trajectories shape. Procrustes distance $D(A, B)$ is a minimal least-squares distance between corresponding sets of $n$ points $A \in \mathbb{R}^2$, $B \in \mathbb{R}^2$ that can be achieved by Euclidean similarity transformations (scaling, translation, rotation and reflection) of the point set $B$. The Procrustes distance $D(T, T')$ close to 0 means that the shape of the trajectory over the OCTG, i.e., the direction of user's movement along the path, is preserved.

*5) Distance between users who follow different paths is preserved:* Studies of human mobility often involve geographical closeness of network users during a particular time extent. Let us consider two users $u$ and $v$ taking different paths over the CTG with the same number of steps $l$: $S^u_l \neq S^v_l$ where $S^u_l = (s^u_1, s^u_2, \dots, s^u_l)$ and $S^v_l = (s^v_1, s^v_2, \dots, s^v_l)$. Ideally, the distance between users in the OCTG after each step on the same paths should be close to the distance measured over the CTG. To express such characteristics, we compute a vector of distance ratios:

$$\vec{d} = \left( \frac{\|p'_{s^u_1}, p'_{s^v_1}\|}{\|p_{s^u_1}, p_{s^v_1}\|}, \frac{\|p'_{s^u_2}, p'_{s^v_2}\|}{\|p_{s^u_2}, p_{s^v_2}\|}, \dots, \frac{\|p'_{s^u_l}, p'_{s^v_l}\|}{\|p_{s^u_l}, p_{s^v_l}\|} \right). \tag{6}$$

If all elements of the vector $\vec{d}$ are close to 1 then the geographical closeness between users $u$ and $v$ is preserved.

## V. Methods

To obfuscate the network, the positions of BSs (nodes) in the OCTG need to be changed from the positions in the CTG in such a way that the operation cannot be easily inferred and thus reverted by a potential attacker. Should the OCTG generation method rely only on the Euclidean similarity transformations (scaling, translation, rotation and reflection) of the CTG, or even their arbitrary linear combination, a backward transformation from the OCTG to the CTG is possible by means of Procrustes analysis [16] if the attacker has only three exact BS positions in the original CTG. Therefore, we consider such transformations vulnerable and apply two different methods to generate an OCTG that do not rely on them. The first method is a simple randomization of BS positions in a given CTG's, while the second one is based on planar graph drawing.

**Randomization Method (RM)**: The randomization method randomly changes positions of the CTG nodes while it preserves its convex hull and planarity of the resulting drawing.

**Algorithm** *Randomization Method (RM)*

```
(∗ Input: CTG $(P, A)$ ∗)
(∗ Output: OCTG $(P', A')$ ∗)
Initialize: Let $P' = P$ and $A' = A$.
$\forall p'_i \notin CH'$: $p'_i \leftarrow$random point from the interior of a
    convex polygon given by the neighboring nodes of $p'_i$.
```

The Randomization Method has linear complexity $O(|P'|)$.

**Force Directed Obfuscation Algorithm (FDOA)**: We generate an OCTG using a modification of a force directed algorithm proposed by Plestenjak [17]. Plestenjak's algorithm generates a straight-line planar drawing of an arbitrary 3-connected planar graph whose convex hull is given as an input. Our modification consists of superimposition of the two planar drawings (the CTG and the OCTG) according to their convex-hulls shape, after the run of Plestenjak's algorithm. Such a simple transformation enables direct CTG and OCTG comparison.

```
Algorithm Force Directed Obfuscation Algorithm (FDOA)
(* Input: CTG (P,A), positions of nodes in the $CH'$ *)
(* Output: OCTG $(P', A')$ *)
1. Initialize: Place nodes of the $CH'$. Place the rest of the
   nodes ($p' \notin CH'$) in the center of mass of the $CH'$. Let
   $A' = A'$.
2. for $iter \leftarrow 1$ to number of iterations
3.         $\forall p'_i \in P'$ set a resultant force $F_i = 0$.
4.         $\forall p'_i, p'_j$ such that $A'_{ij} = 1$ calculate attractive and
           repulsive forces $F_i = F_i + F_{ij}, F_j = F_j - F_{ij}$,
           where $F_{ij} = (n/\pi)^{-1/2}\|p'_i, p'_j\|^3$.
5.         $\forall p'_i \notin CH'$ move node according to the resultant
           force $p'_i = p'_i + \min(|F_i|, cool(iter))F_i/|F_i|$.
6. Scale P' such that $\max_{i,j}(\|p'_i, p'_j\|) = \max_{k,l}(\|p_k, p_l\|)$.
7. Superimpose P' to have common center of mass with P.
```

We use the total number of $2 \cdot |P'|$ iterations and a cooling function $cool(iter)$ in the algorithm, as proposed in [17]. Computational complexity of the FDOA is linear in the number of vertices and edges, i.e. $O(|P'| + \sum_i \sum_j A'_{i,j})$.

## VI. Performance evaluation

### A. Simulation setup

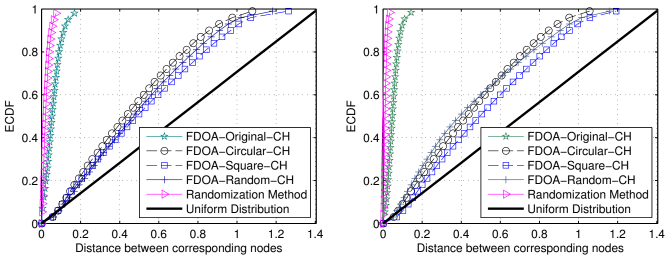
We have simulated 100 CTG's for each of 100 and 500 number of nodes. The BS positions in the CTG were uniformly distributed in a unit square (1x1). To study the effect of a different convex hull shape on the resulting OCTG, we have generated OCTGs for four different $CH'$ shapes:

- Original CH: convex hull remain identical, $CH' = CH$.
- Circular CH: nodes of $CH'$ are mapped onto a regular $|CH|$-sided polygon which is inscribed in a unit square (an example of using this variant can be seen in Fig. 2).
- Square CH: nodes of $CH'$ are mapped onto a regular division of a unit square border.
- Random CH: nodes of $CH'$ are mapped onto a randomly generated convex $|CH|$-sided polygon.

To simulate trajectories followed by users we randomly select 20 distinct shortest paths in the CTG of length of 8 and 14 steps for the CTG with 100 and 500 nodes, respectively. Results presented in the next section represent an average of a total number of 100 OCTGs for each number of nodes (100, 500) and each method (RM and each of FDOA variants).

### B. Results

In this section we show how the objectives described in Section IV-A are achieved by the presented methods.



(a) 100 nodes

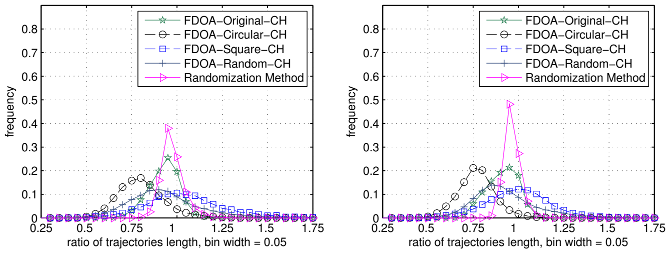
(b) 500 nodes

Fig. 3. Empirical Cumulative Distribution Function (ECDF) of distances between corresponding nodes of CTG and OCTG per method, compared to the ideal uniform distribution ($y = x/\sqrt{2}$). The RM and FDOA-Original-CH methods exhibit the poorest anonymization, being far from the uniform CDF.

*1) The neighbor relationship between nodes is preserved:* The neighborhood relationship between the nodes in the CTG is preserved in the OCTG by definition — OCTG is a graph isomorphic to the CTG. Both presented methods of CTG obfuscation alter only the planar drawing of the graphs.

*2) Distribution of distances between corresponding nodes is uniform:* As shown in Fig. 3, the distributions for the different methods follow a similar shape quite close to the ideal uniform distribution, independently of the number of nodes, except for the FDOA-Original-CH and the Randomization Method, for which corresponding node distances are concentrated within the interval (0,0.2) (indicating that most nodes of the OCTG are quite close to those of the CTG). From the anonymity perspective these two OCTGs are not very protected since a potential attacker could discover that the real BS positions are enclosed within a certain perimeter of OCTG nodes and approximately reconstruct the location data. At the same time, though, fitting the FDOA OCTG into a different convex hull (Circular, Square, Random) than the input CTG likely includes some rotation of the original graph, which contributes to the (desired) uniformity of the node distance distribution but could also be considered a vulnerability. However, with the highly differing CH, the rotation is difficult to identify (see Fig. 2).

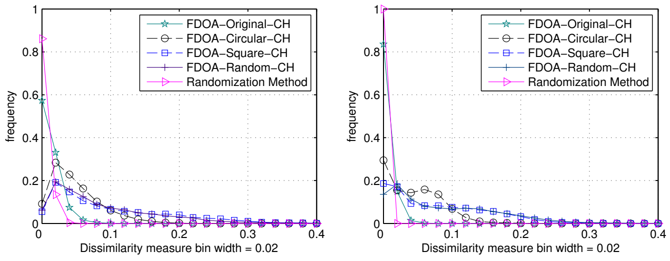
*3) Length of users' trajectories is preserved:* Fig. 4 shows that the RM and the FDOA-Original-CH methods preserve the length of users' trajectories well — the distribution of the Ratio of Trajectories Length (RTL) has a mean value approximately 1. The RM method is advantageous in its smaller standard deviation, a "higher peak" in the graph. The Random and Square variants of the FDOA method still



(a) 100 nodes

(b) 500 nodes

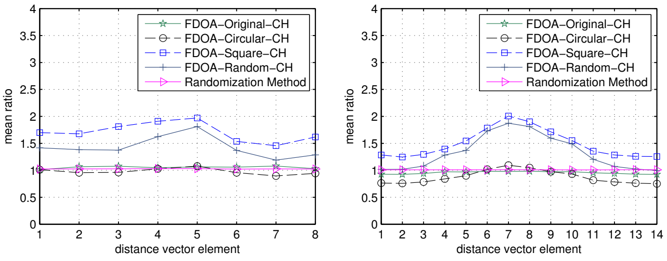
Fig. 4. Histogram of the Ratio of Trajectories Length. As the number of nodes grows, the FDOA methods lose accuracy in preserving trajectories length.



(a) 100 nodes

(b) 500 nodes

Fig. 5. Histogram of dissimilarity measures of shape of trajectories. Values close to 0 indicate better shape preservation.



(a) 100 nodes

(b) 500 nodes

Fig. 6. Vector of mean distance ratios between users following different paths. Values close to 1 indicate better distance preservation.

preserves the mean RTL value of 1, but their standard deviation is much higher, resulting in more inaccurate trajectory length preservation. The last FDOA variant (Circular) achieves shorter trajectories length (around $3/4$ of their original size).

*4) Shape of users' trajectories is preserved:* Graphs in Fig. 5 show that the shape of users' trajectories is better preserved by the RM and FDOA-Original-CH methods. These yield even better performance in networks with more nodes.

*5) Distance between users who follow different paths is preserved:* Geographical closeness between users is better preserved if the shape of the CH in the OCTG is similar to the one in the CTG, see Fig. 6. Therefore, the RM method and the FDOA-Original-CH perform best wrt. this objective. The FDOA-Square-CH and the FDOA-Random-CH differ the most from the original CTG topology and thus yield worse results. The differences in distances are higher in the middle of the path, which is caused by the shape of the CH that "stretches" the OCTG in the corners of the simulation reference frame.

## VII. Conclusion

We have presented a new paradigm in the location-privacy field, mobile network topology obfuscation, thus establishing a new way to anonymize mobility data for the purpose of sharing, while avoiding identification of the mobile network.

Only a single transformation of a given network topology is needed to share anonymized mobility data of all users. As important characteristics of the mobility data are preserved, such transformation is widely useful for large-scale behavior analysis of mobile network users - identifying work-commute distances, size of communities, segmenting users by speed of movement, space-time behavior models or user proximity analyses, without revealing identities or locations. It can be foreseen to be used in such widely different tasks as urban planning, network capacity planning, advertising, virus spread mitigation or disaster prevention. Data analysis can now easily be outsourced to third parties without privacy risks.

To this end, we applied and evaluated two different topology obfuscation methods. Unsurprisingly, the degree of anonymity according to our criteria (Section IV-A) is compromised inversely to the level of analytical accuracy of the obfuscated user trajectories. Those methods that preserve the statistical mobility properties most accurately, Randomization Method and FDOA-Original-CH, present the lowest degree of anonymity, exhibiting a skewed non-uniform distribution of distances between corresponding nodes. On the other hand, FDOA-Circular-CH, even if shortening the trajectories, is the best in the sense of balance between accuracy and anonymity.

Results obtained with the FDOA methods are highly influenced by the choice of convex hull. They could possibly be improved by weighting of the nodes in the actual FDOA process - we leave this for future experimentation. The selection of methods tested in this work is by no means exhaustive and we plan to compare them to other planar drawing methods (e.g. Rahman [18]). Final valuation of this approach should come with application to a CTG of a real mobile network topology - and evaluation of the resulting OCTG.

## References

[1] L. Barkhuus and A. Dey, "Location-based services for mobile telephony: a study of users' privacy concerns," in *Proc. Interact*, 2003, pp. 709–712.

[2] Nokia Research Center, "Nokia mobile data challenge," 2011, [Online]. Available: http://research.nokia.com/page/12000.

[3] France Telecom-Orange, "Orange 'data for development' open data challenge," 2012, [Online]. Available: http://www.d4d.orange.com/home.

[4] K. Dufková *et al.*, "Active gsm cell-id tracking: "where did you disappear?"," in *Proc. ACM MELT*. ACM, 2008, pp. 7–12.

[5] H. Zang and J. Bolot, "Anonymization of location data does not work: a large-scale measurement study," in *Proc. MobiCom*. ACM, 2011, pp. 145–156.

[6] C. A. Ardagna *et al.*, "Location privacy protection through obfuscation-based techniques," in *Proc. IFIP WG 11.3 DBsec*. Springer-Verlag, 2007, pp. 47–60.

[7] F. Aurenhammer, "Voronoi diagrams — a survey of a fundamental geometric data structure," *ACM Comput. Surv.*, vol. 23, no. 3, pp. 345–405, 1991.

[8] K. Rechert *et al.*, "Assessing location privacy in mobile communication networks," in *Proc. ISC*, 2011, pp. 309–324.

[9] F. Bonchi *et al.*, "Trajectory anonymity in publishing personal mobility data," *SIGKDD Explor. Newsl.*, vol. 13, no. 1, pp. 30–42, 2011.

[10] R. Shokri *et al.*, "A unified framework for location privacy," in *Proc. PETS 2010*, 2010, pp. 203–214.

[11] L. Sweeney, "k-anonymity: a model for protecting privacy," *Int. J. Uncertain. Fuz.*, vol. 10, pp. 557–570, 2002.

[12] P. Kalnis *et al.*, "Preventing location-based identity inference in anonymous spatial queries," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 12, pp. 1719–1733, 2007.

[13] G. Ghinita *et al.*, "Prive: anonymous location-based queries in distributed mobile systems," in *Proc. WWW*. ACM, 2007, pp. 371–380.

[14] M. B. Chen, C. Gotsman, and C. Wormser, "Distributed computation of virtual coordinates," in *Proc. SCG*. ACM, 2007, pp. 210–219.

[15] M. B. Stegmann and D. D. Gomez, "A brief introduction to statistical shape analysis," University of Denmark, DTU, Tech. Rep., 2002.

[16] J. C. Gower and G. B. Dijksterhuis, *Procrustes Problems*. OUP Oxford, 2004.

[17] B. Plestenjak, "An algorithm for drawing planar graphs," *Softw. Pract. Exper.*, vol. 29, pp. 973–984, 1999.

[18] M. S. Rahman, S.-I. Nakano, and T. Nishizeki, "Box-rectangular drawings of plane graphs," in *WG*, 1999, pp. 250–261.