Improving Spatial Transformation-Based Privacy in Location-Based Systems

Eric Majidian, Aidan Jacobs, Dr. Subhasish Mazumdar
New Mexico Institute of Mining and Technology

Abstract
It has been previously proposed that user location privacy can be preserved through the use of space-filling curves such as the Hilbert curve. However, it has also been shown that a system whose security is dependent solely on the Hilbert curve is still vulnerable to attack.

We have proposed and explored a number of methods to address these vulnerabilities. Our aim is to find which of these methods, possibly in conjunction with other future work, yield substantial enhancements in privacy guarantees for the user in the context of location-based services.

Methods of Attack
A location-based server is needed to resolve user queries. The server is provided with an encoded map, which contains the cell values of points of interest (POIs) in the system and the encrypted category, sub-category, etc. of each point of interest.

When a user queries the system, the user’s location is encoded and sent to the location-based server along with his or her encrypted query.

An adversary who has infiltrated the location-based server may be able to decode the user’s location and query through the following methods:

- Decode POIs by analysing patterns in the category distribution within the encoded map, and
- Using these POIs, reconstruct the curve on which the user’s location is encoded.

Replication and Rotation Method
A curve with a significant number of empty cells is easier to reconstruct than one which has little sparsity. Fake points of interest can be added to empty cells to reduce sparsity, but must be distributed in a manner that makes them indistinguishable from the real points of interest.

This method reduces sparsity by replicating and rotating the set of real points of interest at 90°, 180°, and 270° before superimposing each set onto the original curve. User queries are also replicated and rotated for each set, resulting in four potential user locations per query.

The L1 Pattern
Applying an offset to the encoded cell values of users and points of interests can make it more difficult for an adversary to decode their locations.

On the traditional curve, the order of the curve must be increased in order to accommodate the offset cells, resulting in a large amount of sparsity (see Replication and Rotation Method).

The L1 pattern is a variant of the traditional Hilbert curve, shown in Figure 3 (Liu, 2004). Unlike the traditional Hilbert curve, the L1 pattern begins and ends in the center of the grid. Thus, offset cells that would normally be pushed off of the traditional curve simply wrap around the L1 pattern.

Balancing the Category Tree
The category distribution in the encoded map can be normalized by adding fake points of interest until each category tree is indistinguishable from another. This makes it much more difficult for an adversary to identify points of interest by analysing the category distribution.

A user is required to query within the lowest subcategory level. Therefore, fake points of interest within fake subcategories will never be returned to a real user.

If these fake points of interests are never queried, however, an adversary will be able to identify and discard them. Thus, fake users must query these points occasionally, increasing overhead on the system.

Conclusion
The methods discussed above are capable of limiting or eliminating the threats posed by an adversary who has infiltrated the location-based server. However, balancing the category tree and applying the "Replication and Rotation Method" both increase the amount of overhead on the system while the L1 pattern appears to be advantageous only when an offset is applied to the grid.

References
