# Prometheus: Distributed Management of Geo-Social Data

Nicolas Kourtellis, Joshua Finnis, Paul Anderson, Jeremy Blackburn, Adriana Iamnitchi
Department of Computer Science and Engineering, University of South Florida, Tampa, FL
[nkourtel, jfinnis, paanders, jhblackb, anda]@cse.usf.edu

## 1. Introduction

Many of today's internet services, such as online social networks and collaborative tools, collect a vast amount of social information about the interactions between their users. Ubiquitous GPS and Bluetooth-enabled mobile devices generate yet another layer of social data through finding location and collocation of users which is in turn used by location-based services such as Loopt or Google Latitude. These services allow for socially-aware applications which can use social data to infer preferences, trust between individuals, and incentives for resource sharing. However, existing applications use social information collected only from their own social contexts. Using social information from only one source is subject to higher bootstrap costs, is naturally restricted to the application domain, and can be misleading (e.g., friendship in Facebook).

The centralized nature of these services invokes major privacy concerns and raises awareness of the need for users to have control over the storage and access of their own social information. We present Prometheus, a socially-aware peer-to-peer infrastructure that decentralizes the social information of users to user-selected trusted peers, and allows users to:

- Report social information from multiple sources through a set of 'social sensors' that can be developed for any service or application with relevant social data.
- Control the storage of their social information by defining trusted peers and using public-key infrastructure (PKI) cryptography.
- Control the access of their social data from applications that request complex geo-social inferences, using user-specified access control lists.

## 2. Prometheus Architecture

Prometheus runs on top of a DHT-based overlay formed by resources contributed by users. Social information is represented as a weighted, directed multigraph where nodes correspond to users and edges correspond to social activities or ties connecting two users. The activities are described with a label (e.g., "hiking") and a weight that specifies the intensity of the activity.

The social information is decentralized onto peers as partial social graphs, such that no single peer stores the entire graph. A user's social information is stored on user-chosen *trusted peers* that have socially-based incentives to remain online and manage the user's data. Incoming social information from social sensors is disseminated via group communication to all trusted peers responsible for storing the relevant data of a user. Applications use social inference requests to access social data; the trusted peers are responsible for fulfilling these requests, using user-specified access control lists and PKI for authorization and verification. The software components of Prometheus needed to provide these functionalities are shown in Figure 1.

## 3. Demonstration of Prometheus

The attendees experimenting with our system will be able to choose either registering with Prometheus as new users or selecting one of the existing users already inserted in a social graph. With a laptop we will visualize a) the distribution of users onto system peers they trust to store and manage their social information, b) how each peer's partial social graph changes with incoming social information (e.g., collocation) reports from the social sensors running on mobile devices available for testing, and c) how complex inference requests are serviced when social data from multiple users (and consequently peers) are needed to fulfill them.

We plan to demonstrate how two socially-aware mobile applications can utilize the Prometheus infrastructure to access social data by submitting complex inference requests for social information. The first mobile application decides whether to allow an incoming call to ring or go to voicemail by determining if the user's current social context is appropriate (e.g., at the conference, a user's social context is "work"). A phone call from outside the work context will be silenced. The second application allows a user to find and invite other users with a shared interest (such as in hiking), to a common activity (such as a hiking weekend excursion). The application queries the system to find other users linked with the user with the particular activity edge and a minimum weight. The application can request users of more than one social hop away from the user. This might lead to a traversing of multiple peers to find the social data of users not directly connected to the user submitting the request.

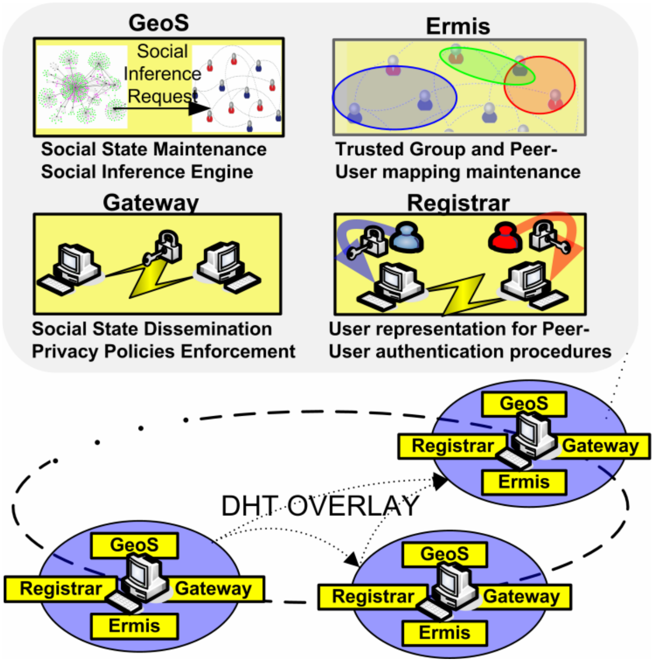

**Figure 1: Each peer in the Prometheus overlay runs four components: Ermis, Gateway, GeoS and Registrar.**

## Acknowledgments

This research was supported by the National Science Foundation under Grant No.CNS-0831785.