Title
Exploiting Social Networks for Sensor Data Sharing with SenseShare

Permalink
https://escholarship.org/uc/item/4919w4vh

Authors
Schmid, Thomas
Srivastava, Mani B

Publication Date
2007-10-10
Exploiting Social Networks for Sensor Data Sharing
with SenseShare

Thomas Schmid, Young Cho, Mani B. Srivastava
Networked and Embedded Systems Lab - http://nesl.ee.ucla.edu

Introduction: Social Networks and Data Sharing

Social Networks

• Social networks create groups and link people together
  Facebook allows you to create a network with your friends and people you
  know.

• Authentication and privacy
  With sophisticated privacy settings, you can select who can see which
  information. For example, you can say that your immediate family can see your
  phone number, but no one else.

• Open APIs for application developers
  Facebook implemented an API to its service. This allows developers to build
  their own applications using the social networks the Facebook users create.

Data Sharing

• Urban Sensing
  Researchers want to collect data by involving people in the process.

• Location sharing
  People want to share their whereabouts with their friends, but not everyone

• Data collection

Problem Description: Privacy and Selective Sharing

• Sharing, but with whom?
  Each individual has his own policies of which data he wants to share with whom. For example, you might want to share your current location with all your family
  members, whereas you don’t want to share this with the general public. Or you might be collecting the data from a small weather station in your backyard and want
  everybody to know about this data. SenseShare and the social network structure of Facebook will make it easy to select to whom you want to share what.

• Trust
  Everybody trusts some people more than others. Thus, you can apply different data filters for different individuals or groups. For example, to your immediate family,
  you give your exact location, whereas to you friends, you only share the current ZIP code, city, or even just country you reside in right now.

• Assurance
  If you share personal information, how can one assure that the people you trust don’t misuse that trust you have in them?

• Water marking
  Can we apply similar techniques as for Digital Rights Management (DRM) in multimedia files for sensor data?

Proposed Solution: SenseShare Architecture

General SenseShare Architecture

Example Clients

• CitySniff
  Small and affordable pollution sensing kit for homes.

• Cell phones
  N80, OpenMoko

• NetCar
  Small computer for a car that logs the different car sensors and
  makes them accessible to the car owner.

• Sensor Networks
  A simple gateway application can expose the collected data
  from a sensor network through the SenseShare architecture.

Facebook

Privacy Manager

Database
e.g. SensorBase

Data
Obfuscater/Changer

Privacy Manager

Database

e.g. SensorBase

Data
Obfuscater/Changer

• Facebook
  This is the main frontend to the SenseShare architecture.
  Facebook provides a rich user interface, as well as an API into
  their social network infrastructure. For example, it is very easy
  to find out if someone is a friend of a user, and to what groups
  or networks a user belongs to. This can be used to provide a rich
  set of privacy options.

• Privacy Manager (PM)
  The PM is the core of the SenseShare architecture. It policies
  who can see what with what kind of resolution, or filters. It
  exploits the rich API provided by Facebook, in order to achieve
  a network of social trust.

• Database
  Currently we are using a simple MySQL database. We plan to
  have a generic data provider, such that the user himself could
  select where his data should be stored.

• Data Obfuscater / Changer / Water Marker
  The SenseShare user will have a choice of applying different
  filters for different users to his data. The filters range from
  adding random noise to measurements, specific location filters,
  to water marking of the outgoing data.