Air-Writing: A Platform for Scalable, Privacy-Preserving, Spatial Group Messaging

iiWAS 2010, Session „Web Applications“
Paris, 9.11.2010 14:00 - 15:30

Alexander Sommer, Sinan Saral (Univ. Vienna)
Rene Mayrhofer (Upper Austria Univ. of Applied Sciences)
Aim: Improved Spatial Messaging

Overview
- System architecture
- Privacy protection
- Preliminary evaluation

Motivation
- Novel aspects
- Use cases

What is Airwriting?
- Based on a simple business model
- Designed as a framework!
- Privacy protecting
- Funny
- Attribute-based messaging
- Marketing
Novel aspects

Privacy

- Privacy protection built into whole architecture
- Anonymous queries possible, even against Internet provider and server operator level

Quality Component

- A business model
- rating message service
What can Air-Writing be used for?

**End Users**

- **general**: creative socializing, promoting art work, business
- **functional**: pick-messages, practical & segmented ads, location based games, tourism, information, events, single-portal

**Scientists**

- **theoretical**: for proposing & analyzing message attributes
- **practical & theoretical**: considering our architecture design if they are building their own
Attributes: basic architectural concept in Air-Writing

- e.g. location, time, emotional state, weather, temperature, etc.
- text and user ID are also attributes

Groups: define a “scope” for communication

- messages sent to group
- group defines the set of mandatory and optional attributes for messages
Client Platforms

- **iPhone, iPad**: currently main client platform
- **Android**: fully featured port
- **J2ME**
Communication Protocol

- **Queries for messages are anonymous:**
  - group ID (as pseudonym), longitude/latitude, area width
  - no client ID in queries
  - distinct query for each group with randomized delays

- **Sending messages with optional log-in**

- **Static HTTP URLs for area lattice to support content distribution networks ⇒ protection against DoS**
Client Privacy and Security Measures

- Clients always query more than they actually need
  - for whole area
  - may use dummy queries for other locations for enhanced privacy
  - may query for groups it is not interested in

- Filters applied locally (time, location, other attributes) to only show relevant messages
  - some attributes checked/enforced by server (e.g. #picks), others on client
  - applications need to be careful about cheating in their use case

- Encryption and decryption of messages with local passwords or other key data (e.g. from QR code tags)
Anonymization of Traces: Results

<table>
<thead>
<tr>
<th>Range [m]</th>
<th>Poll interval [sec]</th>
<th>Overhead</th>
<th>Largest poll</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>700</td>
<td>1000</td>
<td>0</td>
<td>8</td>
<td>3/3</td>
</tr>
<tr>
<td>700</td>
<td>350</td>
<td>19</td>
<td>8</td>
<td>3/3</td>
</tr>
<tr>
<td>400</td>
<td>350</td>
<td>6</td>
<td>6</td>
<td>2/3</td>
</tr>
<tr>
<td>300</td>
<td>350</td>
<td>2</td>
<td>3</td>
<td>1/3</td>
</tr>
<tr>
<td>45</td>
<td>30</td>
<td>14</td>
<td>2</td>
<td>1/3</td>
</tr>
<tr>
<td>200</td>
<td>300</td>
<td>0</td>
<td>3</td>
<td>1/3</td>
</tr>
</tbody>
</table>
Next Steps

What is the next big thing in Air-Writing?

- New attributes
- Mobile web version
- Framework
- Further evaluation (user surveys, further usability studies)
Thank you for your attention!

Slides: http://www.mayrhofer.eu.org/presentations
Later questions: alexander.sommer@gmail.com
                  rene@mayrhofer.eu.org

OpenPGP key: 0xC3C24BDE
7FE4 0DB5 61EC C645 B2F1 C847 ABB4 8F0D C3C2 4BDE