Modern Cryptography
Term Project Proposal

Privacy-Aware Indoor Location Sensor Networks

20082114
Choi, Im-sung

1. Introduction

Sensor network technology promises a vast increase in automatic data collection capabilities through efficient deployment of tiny sensing devices. Arrays of sensors could be deployed alongside roads to monitor traffic patterns or inside buildings to sense contextual information for adaptive computing services. In particular, there is great interest in indoor location tracking systems, which determine the position of users for indoor location-based services.

While indoor location sensor networks offer great benefits to users, they also exhibit significant potential for abuse like privacy concerns. A common approach addresses privacy concerns at the database or location server layer; after data has been collected. For instance, privacy policies govern who can use an individual's data for which purposes [1, 2, 3]. Furthermore, data perturbation [4] or anonymity mechanism [5, 6] provide access to data without disclosing privacy sensitive information.

2. Objectives

These approaches solve the privacy concerns partly, but data is difficult to protect once it is stored on a system and these approaches don't address the risks that an adversary circumvents the location server and directly collects data from the location tracking system.

Because user cannot trust databases and locations servers, and user only need to trust the sensor networks itself, we think that these privacy concerns problems should be addressed at the sensor networks level.

3. Expected Result

We discuss privacy risks and attacks for the indoor location sensor networks and propose our idea that cloaks location information to preserve anonymity.

4. Project Schedule

3~6 weeks	Review location sensor networks
7 week	Mid-term
8~9 weeks	Describe possible privacy concerns in location sensor networks
10~11 weeks	Survey existing approaches to address privacy concerns
12~13 week	Propose our solution and evaluation
14 week	Make the term project report and Prepare presentation
15 week	Final-term

Reference

[1] Marc Langheinrich, "A privacy awareness system for ubiquitous computing environments," In *4th International Conference on Ubiquitous Computing*, 2002.

[2] Einar Snekkenes, "Concepts for personal location privacy policies," In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pages 48–57, ACM Press, 2001.

[3] Sastry Duri, Marco Gruteser, Xuan Liu, Paul Moskowitz, Ronald Perez, Moninder Singh, and Jung-Mu Tang, "Framework for security and privacy in automotive telematics," In *2nd ACM International Worksphop on Mobile Commerce*, 2002.

[4] Rakesh Agrawal and Ramakrishnan Srikant, "Privacy preserving data mining," In *Proc. of the ACM SIGMOD Conference on Management of Data*, pages 439–450. ACM Press, May 2000.

[5] Pierangela Samarati, "Protecting Respondents' Identities in Microdata Release," *IEEE Transactions on Knowledge and Data Engineering*, 13(6), 2001.

[6] Latanya Sweeney, "Achieving k-Anonymity Privacy Protection Using Generalization and Suppression," *International Journal on Uncertainty, Fuzziness and Knowledgebased Systems*, 10(5):571–588, 2002.