Privacy in Mobile Communications

Valtteri Niemi
Nokia Research Center, Radio Systems laboratory
University of Turku
Department of Mathematics and Statistics
Helsinki, Finland
valtteri.niemi@nokia.com

Abstract

Context information helps in providing better service to the mobile user but it can also be used in ways that are not necessarily in the best interest of the user, e.g. people can be tracked and their habits can be learnt. Therefore, access to personal information requires certain amount of trust on the mobile service provider; at minimum the service provider should not leak the context information to untrusted third parties. In summary, both trust and privacy issues are most relevant for mobile context-aware services.

A mobile device that a person is carrying almost continuously provides a good platform for learning that person's context. Indeed, for instance, modern smartphones include several sensors that provide context information either directly or indirectly: e.g. a GPS receiver provides directly location information, an accelerometer provides a little bit more indirect information about the type of movement of the person carrying the device, and a microphone could collect audio samples that provide more indirect information about the general surroundings of the person.

There are several strategies how the privacy-sensitive context information could be protected. One possibility is to keep the (exact) context information locally in the device and use it to enhance the service locally. Another option is to minimize the amount of the context information that is provided to the service. Both of these strategies have the downside that it may be difficult for service providers to improve their service as they would not learn enough about service users. Another strategy is to try to make sure that only trusted services can obtain information about the user.

Still another strategy could be found in a direction where the context information and information about the user's true identity are separated from each other. The context information alone is often sufficient for improving the service; e.g. for providing information about the traffic conditions it is much more relevant to know where a person is, and where she is going than knowing who the person is. On the other hand, it is often the case that, in addition to the current context, also the context history of the person is relevant for the service, and obtaining a context history of a person is typically sufficient for being able to identify her/him.

In this talk we briefly go through various privacy protection technologies that try to follow the strategies listed above. These technologies have been developed by Nokia Research Center, together with collaborators, and also tried out with data from real-life experiments. Examples of technologies are privacy-preserving scheduling, privacy-triggered communication, pseudonym systems, usage control and context-aware policy management.