Context-aware privacy protection in the Internet of Things

Sophie Chabridon and Maryline Laurent
Institut Mines-Télécom, Télécom SudParis — CNRS UMR Samovar
9 rue Charles Fourier, 91011 Évry cedex
Contact: Sophie DOT Chabridon AT telecom-sudparis.eu (replace characters appropriately)
Maryline DOT Laurent AT telecom-sudparis.eu (replace characters appropriately)

Keywords: Internet of Things, Privacy, Context-awareness, Quality of Context (QoC), Distributed Systems, Software Engineering, Middleware.

Research issues: The Internet of Things (IoT) offers promising opportunities for the development of new context-aware software services taking advantage of the unprecedented amount of contextual information that can be collected and shared by IoT devices about their environment [1]. However, it also comes with new challenges regarding the privacy of the users and it is essential to associate with context management the mechanisms offering extrafunctional properties which include quality of context (QoC) and privacy concerns [2, 7].

Although privacy is an old notion, it is still unclear exactly what it means today, especially with the new usages provided by communication and computing technologies [5]. During the collection of context data, anonymization techniques like k-anonymity are often used to protect data from being linked to the user. However, de-anonymization attacks, like those in [6], have demonstrated that such techniques are still not sufficient or safe enough. One issue of current Privacy-Enhancing Technologies (PETs) for context data processing is to cope with the variety of anonymization and data protection mechanisms that should be used in combination along the processing chain, such as differential privacy [3] proposing to use perturbation techniques to make datasets indistinguishable. This calls for new policy languages and techniques and new middleware mechanisms to plug-in relevant mechanisms when required.

In the IoT, the number of connected objects grows in an exponential way. These objects may be sources (or producers) of context supplying information to be transformed and forwarded to a large and changing number of consumers. The routing and the processing of the information is realized through several intermediaries located at different scales. Therefore, with the IoT, context management takes place at different scales (personal network, Internet, clouds) with a strong decoupling between producers and consumers. During the design of the context-aware applications, the designers must be able to express in a contractual way their requirements with regard to contextual information in terms of extrafunctional properties. This will allow applications to better manage their adaptations and reactions during the execution. The requirements must be able to vary during the execution under certain predefined conditions. In a symmetric way, the management system of context has to specify and protect both the QoC expected by applications and the privacy of the users.

Subject: The Master thesis will first investigate software engineering and middleware solutions for proposing design and runtime models for the support of context-aware applications, taking into account privacy. New solutions for privacy management will also be proposed. Finally, it will integrate existing or new mechanisms for managing autonomic systems [4] able to adapt at runtime in order to fulfill the requirements of the new and dynamic applications enabled by the IoT.

References


