Abstract
Xin Huang

SENSOR APPLICATION PRIVACY AND SECURITY

Wireless sensor networks (WSNs) have attracted both public and research communities, because they provide a new interface between humans and the environment. The Internet of Things, which is a cloud of WSNs, collects sensor information In order to provide it for Health care, context aware and other applications. This paradigm brings both challenges and opportunities to privacy and security protections. The main challenges are the privacy issues; we introduce several privacy protection technologies. Firstly, an access control centric architecture is proposed. Secondly, PPID and IDA protocols are designed for ID management. The service provider cloud and the ID cloud are unable to obtain the service details, meanwhile, the third party service cloud and service clouds are not able to obtain the user's ID profile. Thirdly, XCAP based indirect privacy protection methods are studied. Enhanced presence authorization policy and privacy filters are used in order to stop indirect privacy leakage. In addition, k-anonymity for location privacy is also utilized and improved. In addition, a privacy degree for a home sensor system is proposed by extending the definition of the general service anonymity degree. The privacy protection strategies of a home sensor system are derived from the home sensor system privacy degree.

On the other side, we study how the sensor cloud can assist a user to authenticate in a convenient and secure way. A sensor-aided password (SAP) is proposed. The advantage is that it is much easier for the user to both create and remember it; meanwhile, it does not violate the strength of the authentication. The architecture of the sensor aided authentication (SAA) for simple authentication is designed based on the SAP that is generated by the features extracted from the sensor cloud.