Thesis Defense

CNRS - INPT - UPS - UT1 - UT2J

Monday 13 November 2017
14h30
INP-ENSEEIHT, Salle des thèses

Ahmad Shahrafidz Bin KHALID
Team IRT - IRIT

A Secure Localization Framework of RAIN RFID Objects for Ambient Assisted Living

Jury:
Sylvain GIROUX – *Professeur à l'Université de Sherbrooke, Canada (Rapporteur)*
Abdennaceur KACHOURI – *Professeur à l'Université de Sfax, Tunisie (Rapporteur)*
Beatrice PAILLASSA – *Professeur à l'Université de Toulouse (Examinateur)*
Claude TETELIN – *Chef d'Unité Technique, Centre Nationale de RFID (CNRFID) (Examinateur)*
Fabrice PEYRARD – *Maître de Conférences HDR à l'Université de Toulouse (Directeur)*
Emmanuel CONCHON – *Maître de Conférences à l'Université de Limoges (Co-Directeur)*

Abstract: In parallel with the persistent and constant need of privacy and secrecy of an individual, the objective of this thesis consists of improving the privacy in localizing an object through a new protocol based on the latest version of the RFID second generation passive tag called Gen2V2. The proposed protocol must be able to prevent an object from being identified and located by unauthorized parties. The first contribution of this work is the assessment of the RFID anti collision management. It is performed through the creation of an OMNET++ framework, modelled and built based on the latest RFID standard. It does not require any internal power sources to operate and communicates using the UHF frequency. The Gen2V2 standard provides a list of cryptographical suites that can be used as a method to authenticate a tag and a reader. This new generation of tags is supported by an alliance of manufacturers called RAIN (RAdio frequency IdentificatioN) that promotes the adoption of the Gen2V2. The anti collision management overall performance is then compared with its theoretical value and four of its cryptographical suites namely PRESENT80, XOR, AES128 and cryptoGPS. Among the performances evaluated within the framework is the number of collisions and the duration required to interrogate a group of tags. Note that an addition of a localization functionality within the framework reveals that exchanged messages through wireless channel prior to the authentication can lead to a malicious localization of an object. To increase the localization privacy within AAL application, we propose therefore a second contribution which is a new localization method that is based on the current Gen2V2 standard exchanges by anonymizing the tag identity.

05 61 55 65 10
info@irit.fr

www.irit.fr