Paper ID: 65195
student

IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Advances in Space-based Navigation Systems, Services, and Applications (6)

Author: Ms. Antonia Russo
University Mediterranea of Reggio Calabria, Italy, antonia.russo@unirc.it

Prof. Gianluca Lax
University Mediterranea of Reggio Calabria, Italy, lax@unirc.it

A-POSTERIORI PRIVACY-PRESERVING TRACING MECHANISM EXPLOITING SATELLITES TO PREVENT FRAUDULENT POSITIONING

Abstract

Positioning tracing mechanisms are a relevant asset to enable location-based services (LBSs) and location-aware functionalities. Even if LBSs provide enhanced functionalities in various domains (e.g., healthcare, marketing, agriculture), several vulnerabilities expose users to the risk of violating their privacy or using their position improperly. Consequently, tracing mechanisms should offer privacy-preserving features. One interesting challenge comes from the concept of alibi. Consider the case of a person who is suspended for a crime that occurred in a given place at a given time. This person can defend against this accusation if she/he can prove afterwards to an authorized party, such as the court, to have been in another place at the crime time. Usually, people who witness that the user was in a different place give an alibi to the user. However, users could leverage information stored in advance by themselves to prove a-posteriori to have been in a specific position at a certain time. Clearly, we should be sure about the reliability of the self-declared user's location to prevent fraudulent positioning. Moreover, the stored information should be suitably handled to avoid that the user's position is known by unauthorized parties (privacy issue). In this paper, we address these two problems by guaranteeing both the integrity of the information declared by the user related to her/his position and preserving privacy. In the proposed solution, the user receives from a trusted party apparently random information depending on her/his position by the Global Navigation Satellite Systems (GNSS). The user elaborates the data received about her/his position and publishes the processed data in a repository suitably designed in a form that does not compromise privacy and guarantees data integrity. When users want to prove a-posteriori to have been in a specific position at a certain time, they disclose a secret to allow for the reading of the information stored on that repository. Then, the trusted party is able to elaborate the read data and verify that the position declared by the user is reliable with a probability higher than p, where p can be as high as desired.