Designing and evaluating next generation of resilience receivers

The use of GNSS services is becoming a key element for a wide range of applications in our daily lives. Mass-market applications such as sports tracking or user guidance, liability-critical applications such as banking and telecommunication time synchronization, and safety critical services such as aviation and automotive-related solutions, all rely on GNSS. The huge growth experimented during the last decade puts GNSS in the target of attackers.

The Galileo program is working in future enhanced services, complementing the Galileo Open Service with Navigation Message Authentication (NMA) and providing signal authentication through the Commercial Service signals. These new features will improve GNSS applications performance and reduce the likelihood of successful attacks to GNSS. However, these Galileo services still require a step to be completed on the user-side algorithms to successfully exploit them. In this context, the European Commission launched the Navigation Authentication through Commercial Service-Enhanced Terminal (NACSET) project, started in early 2017 and ending after summer 2018, aiming at investigating and implementing different assisted and standalone techniques to detect and mitigate thus improving the resilience at user-level.

NACSET has developed a user terminal based on a high-end multi-GNSS receiver that is able to track E1/L1 signals as well as E6-B/C signals for data and signal authentication. The terminal is equipped with a set of elements to be exploited by the protection techniques. At hardware level, these elements are: An integrated Chip Scale Atomic Clock (CSAC), an Inertial Measurement Unit (IMU), and a high-end dual antenna. At processing level, the NACSET user terminal implements data and signal attack detectors based precise clock bias monitoring, signals angle of arrival, and signal and data authentication.

Among all the implemented features, there are three that stand out and are the focus of this paper: Firstly, the use of the IMU measurements not only to improve the solution robustness in harsh conditions and dead-reckoning, but also to detect incoherent navigation with respect to the GNSS data; secondly, the implementation of an anti-replay solution aiming at protecting the users against zero-delay Secure Code Estimate-Replay (SCER) attacks based on the analysis of the signal unpredictable symbols; and thirdly, the generation of positioning error bounding solution considering the anti-spoofing indicators abovementioned, together with other consistency checks available in the terminal.

The proposed IMU technique follows a hybrid approach which combines the GNSS data with INS acceleration data obtained from the IMU measurements within a tightly coupled Kalman filter to obtain a navigation solution. The approach followed is to process the IMU acceleration and gyroscope measurements in the propagation step within the Kalman filter used for the PVT. While a solution using the GNSS measurements is given when the update step of the Kalman filter is done, solutions just using IMU information are produced at higher rate in the propagation step of the filter. The outputs of the fusing PVT algorithm are used for spoofing detection purposes using heuristic models based on statistical analyses of the residuals. This is a novel approach since typically loosely-coupled and decoupled options are proposed for the identification of navigation incoherencies between GNSS and IMU and full coupling are mainly

used for improving the navigation solution. This feature will be tested using real IMU information combined with real and coherent GNSS measurements as well as spoofed signals.

Anti-replay solution is mainly designed to address zero-delay SCER (Security Code estimation and replay) attacks. This is a type of replay attack where an attacker estimates and rebroadcasts the original signal with a zero or almost negligible delay, taking control of the tracking loop and gradually modifying the signal. The NACSET terminal implements a method that takes advantage of the existence of unpredictable bits and symbols in the navigation thanks to NMA cryptographic information provided through the SIS. In order to conduct a zero-delay SCER attack on a signal containing NMA data, the attacker shall predict the unknown symbols with minimal or none information. The technique is based on the analysis of the signal correlation loss caused by the imperfect estimation of the signal chips corresponding to the mentioned unpredictable symbols. The first step for the detection is the execution of the NMA authentication, once correct checking of the navigation. Afterwards, the selection of a subset of the signal chips corresponding to the NMA unpredictable symbols is done in order to perform a correlation and determine whether correlation peaks are nominal or not. Different subsets of chips can be selected for the correlation. These subsets may be chosen according to different criteria: fixed subsets, random subsets or based on a statistical analysis. For the NMA solution required, Galileo OSNMA definition is used as reference for the implementation.

A key differentiator of the NACSET terminal is the capability to integrate the outputs of every implemented protection measure for the computation of a secure PVT. This feature is split into two stages: The first stage is focused on determining the probability of being under a spoofing attack. In order to calculate this probability, a statistical Bayesian approach is proposed to weight and merge the contributions received from the different techniques. Once the spoofing probability figure is obtained, in the second stage it is integrated with information from the PVT computation (i.e. residuals, navigation data accuracy, measurements quality…) in an error bounding generator algorithm based on a generalization of the Isotropy-based Protection Level (IBPL) solution applicable to sequential estimation processes which provides a Protection Level for a given Target Integrity Risk (TIR).

For the performance assessment of the proposed techniques, the NACSET project experimentation platform can mimic the Galileo infrastructure and SIS, including OSNMA, where signals are simulated using the Spirent's GSS9000 signal generator and threat simulator available at the Joint Research Centre (JRC) and a dedicated spoofer has been developed for the SCER attack execution. A dedicated campaign will be carried out combining the different features herein mentioned in nominal user conditions (open-sky/urban and static/kinematic) to analyse the probability of false alarm (PFA) and fine tune the algorithms configuration and sensitivity. Once nominal tests are completed, a second phase activating different threats and attacks in the simulator will be conducted for similar user conditions. It includes carrying out simulations of spoofing, meaconing and SCER attacks to demonstrate the successful detection of the threat and measure relevant aspects for the user i.e. time to alert, impact on navigation solution, and overall reliability of the combined techniques and correct bounding of the protection levels generated.

This paper will present in detail the novel anti-spoofing techniques herein introduced, providing a theoretical description of the algorithms (GNSS/IMU tight coupling anti-spoofing, antireplay, consistency checks, and spoofing error bounding solution). The results obtained during the experimentation activities in nominal and under attack conditions. The tests and conclusions will

be focused on assessing the most reliable and valuable techniques and parameters for the attack detection, as well as providing conclusions and suggestions for future receiver evolutions.