# SCER spoofing attacks on OS-NMA and anti-spoofing protection based on data mining techniques.

SCER (Secure Code Estimation and Replay) spoofing techniques represent a severe threat to modern GNSS systems, even for those providing its users with defense and counteracting methods based on Navigation Message Authentication (NMA). Due to the risk this type of spoofing techniques pose for modern GNSS systems it is essential to characterize in detail the feasibility of such kinds of attacks in realistic contexts, allowing the proposal of additional defense techniques for GNSS users. Although the SCER spoofing attacks are widely covered in the literature, perfect Acquisition and Tracking stages are considered by some of the authors. Moreover, the impact due to a realistic channel response in the spoofer symbol estimation is typically not found.

This paper provides with a detailed review of the impact over SCER spoofers due to errors in the estimation of time delay and Doppler shift. It also considers the channel influence on the spoofer symbol estimation through generative models to adequately characterize the channel behavior for the attacker. The channel modeling step allows approaching the SCER spoofer issue more realistically as time series responses can be simulated and analyzed. This work considers different channel behaviors that may affect future GNSS applications like autonomous cars.

In a second stage, a set of recommendations is derived for GNSS receiver manufacturers. Based on Data Mining techniques, this paper analyzes possible methods to detect the spoofer presence: First, data reduction techniques are considered (PCA). Then, Signal features at the acquisition stage are used to train data mining algorithms covering different classifiers (Neural Networks, decision trees, Gaussian Mixture Models and Support Vector Machines) to help the GNSS users to detect the attack.

Other complementary simple solutions are applied to detect bursting or chirping signals, which can be used by the spoofer to get the victim receiver out of lock before starting the attack. Such initial detection can also be used to provide further inputs to the data mining classifiers, providing an extra contribution to the victim’s protection system. This step may help to reduce the false alarm rates of the protection system (i.e., it is not likely that multipath signals will be preceded by RFI events, although we can expect advance SCER spoofers to try first to blind the victim).

Several signal metrics, combined with the techniques described above, are analyzed providing final users with a set of recommended methods for spoofing protection against SCER attacks on NMA.
A brief introduction is provided to the workbench designed in Python to simulate the SCER attacks on the Galileo OS-NMA. This setup allows the generation of I/Q samples signal records at different stages: at the spoofer receiver input or at the victim receiver input (therefore the structure enables the generation of a SCER satellite spoofed scenario). This workbench allows the benchmarking of different

spoofer estimation techniques and the defense techniques for the victim's receiver. The workbench is highly modular, allowing the quick evaluation of new detection and symbol estimation algorithms.

**Gallardo López F** [1] , Pérez Yuste A [2] , Arbinger C [3]
[1] DLR GfR, UPM, Weßling Bavaria, Germany
[2] UPM, Madrid Madrid, Spain
[3] DLR GfR, Weßling Bavaria, Germany