Abstract

Due to the weak received power of Global Navigation Satellite System (GNSS) signals, anthropogenic radio frequency interferences could negatively impact GNSS receiver performance. Intentional jamming and spoofing activities are among the most essential dangers, and they are among the most common types of these interferences. Recent studies indicate that modern Android smartphones embedded with GNSS technology can make spoofing attempts. In this work, we provided the results of a test campaign to stress the robustness of such devices to simplistic spoofing attacks and emphasize their actual vulnerability. Our work mainly investigates the effects of jamming and spoofing disturbances on the mass-market positioning and navigation units integrated into smartphones and drones. The tests were performed in an anechoic chamber and open-air conditions with a realistic jammer and spoofer employed to generate disturbances to the GNSS L1 signal transmitted by a signal simulator. Comparative analysis is addressed for the performance of drones and smartphones under intentional disturbances. Additionally, we investigated the impact of a classical spoofing strategy (a straightforward Radio Frequency (RF) attack) on the GNSS raw data observables. We emphasized possible metrics with two synchronized devices in a cooperative framework so that abnormalities are used to detect a simplistic spoofing attack on one of the devices. The remaining part deals with the meaconing simulation of an existing collaborative positioning framework based on the network-based sharing of raw GNSS measurements. The various methods for attacking the framework are outlined, along with the abnormalities that should be investigated to identify an attack in a network of cooperating devices. We demonstrated a new anti-spoofing detection and coping technique in connected COTS GNSS devices. Furthermore, we presented a novel spoofing detection methodology that used the temporal and spatial correlation of the counterfeit signals by applying statistical analysis of GNSS raw data measurements. This suggested approach is applied to devices that include a GNSS unit and provide output GNSS raw data measurements, like Android™ smartphones, since it does not require access to the low signal processing level of the GNSS processor. The proposed technique's vulnerability analysis and validation were carried out in a controlled setting by delivering realistic, false Global Positioning System (GPS) L1/CA RF signals to various Android smartphones. We demonstrate that, under proper conditions, the devices were sensitive to the assaults and that the consequences were obvious through their raw measurements, such as Carrier-to-noise ratio (C/N0), pseudo-range measurements, and position estimates. In

particular, the study demonstrates that the cross-correlation between the C/N0 time series provided by each device about different GNSS satellites increases under spoofing conditions, thus constituting a proper metric to detect the attack.