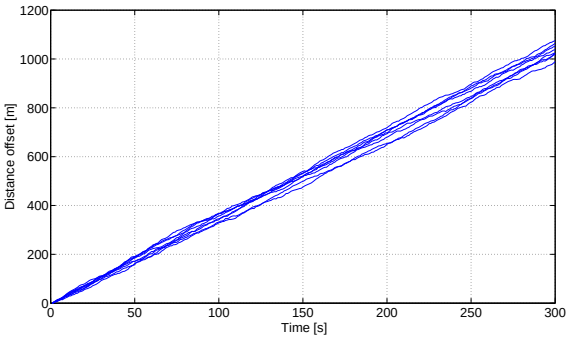

Figure 5: Distance error of inertial mechanisms with Kalman filtering, as a function of the GNSS unavailability period.

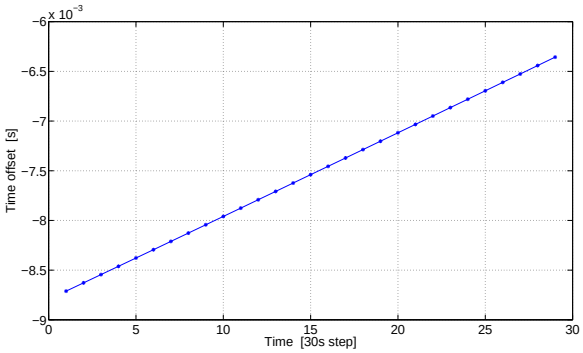

Figure 6: Clock offset for the ASHTECH Z-XII3T receiver, during a 900 sec period with no re-synchronization.

4.2 Clock Offset Test

Each receiver has a clock that is in general imprecise, due to the drift errors of the quartz crystal. If the reception of GNSS signals is disrupted, the oscillator switches from normal to holdover mode. Then, the time accuracy depends only on the stability of the local oscillator [2,6]. The quartz crystals of different clocks run at slightly different frequencies, causing the clock values to gradually diverge from each other (skew error).

A simulation based study [2] of quartz clocks claims that coarse time synchronization can be maintained at *microsecond accuracy* without GPS reception for 350 sec in 95% cases. This means that quartz oscillators can maintain millisecond synchronization for few hours, including random errors and temperature change inaccuracies. Indeed, in such a case, the adversary would need to cause GNSS availability for long periods of time, for example, tens of hours, before being able to mount a relay attack that causes a time offset in the order of tens of milliseconds.

However, without highly stable clocks, mounting attacks against the Clock Offset Test can be significantly easier. This can be the case for a ASHTECH receiver, for which time offset values are shown at successive points in time, each 30 seconds apart, in Fig. 6. We clarify this is not to be perceived as criticism for a given receiver or to be the basis for the suitability of the Clock Offset Test. As explained above, the stability of the receiver clock determines the strength of this test. But the data in Fig. 6, over a period of 900 seconds, exactly demonstrates that for commodity receivers significant instability is observed; time offset values are in the order of ten milliseconds (or slightly less). Consequently, the adversary would need to jam for roughly a couple of minutes, force the receiver to consider as acceptable a time offset of 20 to 32 milliseconds, and thus be mislead by a replay attack as detailed in Sec. 3.

Finally, we note that we do not consider here the case of synchronization by means external to the GNSS system. For example, if the receiver could connect to the Internet and run NTP, it could obtain accurate time. But this would be an infrequent operation (in the order of magnitude of days), thus useful only if highly stable clock hardware were available.

4.3 Doppler Shift Test (DST)

Based on the received GNSS signal Doppler shift, with respect to the nominal transmitter frequency (f_t = 1.575GHz), the receiver can predict future Doppler Shift values. Once lock to GNSS signals is obtained again, predicted Doppler shift values are compared to the ones calculated due to the received GNSS signal. If the latter are different than the predicted ones beyond a threshold, the GNSS signal is deemed adversarial and rejected. What makes this approach attractive is the smooth changes of Doppler shift and the ability to predict it with low, essentially constant errors over long periods of time. This in dire in contrast to the inertial test based on location, whose error grows exponentially with time.

The Doppler shift is produced due to the relative motion of the satellite with respect to the receiver. The satellite velocity is computed using *ephemeris* information and an orbital model available at the receiver. The received frequency, f_r, increases as the satellite approaches and decreases as it recedes from the receiver; it can be approximated by the classical Doppler equation:

$$f_r = f_t \cdot (1 - \frac{v_r \cdot a}{c}) \tag{5}$$

where f_t is nominal (transmitted) frequency, f_r received frequency, v_r is the satellite-to-user relative velocity vector and c speed of radio signal propagation. The product $v_r \cdot a$ represents the radial component of the relative velocity vector along the line-of-sight to the satellite.

If the frequency shift differs from the predicted shift for each visible satellite S_i in the area depending on the data obtained from the almanac (in the case when the navigation history is available), for more than defined thresholds $(\Delta f_{min}, \Delta f_{max})$ or estimated Doppler shift from navigation history differs for more than the estimated shift, knowing the rate (r), the receiver can deem the received signal as product of attack.