On the use of Low-Cost IMUs for GNSS Spoofing Detection in Vehicular Applications

James T. Curran[1] and Ali Broumendan[2]

[1]European Space Agency, Noordwijk, The Netherlands
[2]PLAN Group, University of Calgary, Canada

BIOGRAPHIES

James T. Curran received a B.E. in electrical & electronic Engineering and a Ph.D. in telecommunications from the Department of Electrical Engineering, University College Cork, Ireland. He worked as a senior research engineer with the PLAN Group in the University of Calgary, Canada, and as a grant-holder at the Joint Research Center (JRC) of the European Commission (EC), Italy. Curran has recently joined the European Space Agency as a radionavigation engineer at ESTEC in the Netherlands. His main research interests are signal processing, information theory, cryptography, and software defined radio for GNSS.

Ali Broumandan received his Ph.D. degree from the Geomatics Engineering department of the University of Calgary. He is with the PLAN group of the University of Calgary as a senior research associate where his research focuses on GNSS interference mitigation utilizing antenna array processing. Dr. Broumandan has been involved in several industrial research projects focusing on spatial/temporal processing of GNSS channels in dense multipath environments and synthetic antenna array processing.

ABSTRACT

This paper examines the use of low cost IMUs as a means of GNSS spoofing detection. The self-GNSS spoofing scenario is considered, where the holder of a GNSS receiver may shield the antenna from the genuine signals and introduce counterfeit ones to lead the receiver to compute an incorrect PVT. A method of using uncalibrated, low cost inertial measurement units is proposed, which can detect spoofing based on a coherency test between the GNSS and inertial measurements. Results of live testing under vehicular dynamics suggest that reasonable spoofing detection accuracy can be achieved with a time-to-alarm of three minutes.

1. INTRODUCTION

The use of wireless positioning systems, such as GNSS, for the purposes of the monitoring and regulation has risen sharply in recent years. Systems and services such as fleet-management, asset-tracking and pay-as-you-drive insurance have begun to use GNSS as a primary, and sometimes only, positioning sensor. For many of these applications, in particular where the end users are billed or penalized based their location, there is a strong incentive to compromise the GNSS sensor. Unsurprisingly, when such monitoring devices are installed in vehicles, they are typically enclosed in tamper-proof housings, and secured to the vehicle in a tamper-evident manner.

However, it is unavoidable that the GNSS antenna, and in most cases, the device power supply, is exposed to the outside world. In some cases, other vehicle based sensors are also made available to the device via the CAN BUS, including, for example, wheel-tick counters and wheel angle. Because the CAN BUS currently offers no authenticity or security features, inputs delivered are equally vulnerable to spoofing as GNSS. A malicious user may choose to forge both GNSS and vehicle based sensors, in an effort to manipulate the devise estimate of the vehicle position. Although the tamper-proof enclosure might protect the measurement device itself, any measurements, either radio-frequency delivered through an antenna, or digital measurements delivered through the CAN BUS, are exposed. To provide an effective means of spoofing detection, some sensor that can be protected by the tamper-proof enclosure is desirable, an inertial measurement unit (IMU) being a suitable candidate.

Ideally, measurements drawn from the IMU might be compared against GNSS-derived measurements, to provide some consistency check, that could be used to assert whether the GNSS was spoofed or not. One approach might be to project the GNSS measurements onto the same domain as the IMU. For comparison, a 3-axis accelerometer would require a second difference of the GNSS based position, rotated into the body-frame of the IMU, and for the 3-axis gyroscope, this would require a projection of the first difference of the

International Technical Symposium on Navigation and Timing (ITSNT)
14-17 Nov 2017
ENAC, Toulouse, France

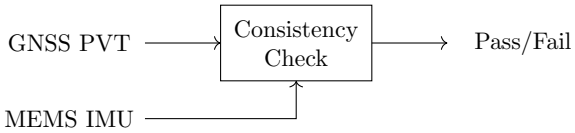


Figure 1: Spoofing detection based on IMU consistency testing

GNSS based position onto a rate of change of heading, and rotated into the body-frame of the IMU.

To perform this comparison, the initial orientation of the IMU would need to be known, and in practice, considering an imperfect IMU, further information is required. Low-cost inertial sensors typically exhibit high measurement noise, and a high uncertainty in measurement bias. For this reason, when used in GNSS-enabled positioning devices, device calibration is typically performed online, by combining GNSS measurements with those of the IMU. Although effective, for navigation purposes, this interaction negates some of the value of the IMU as an independent sensor. When the measurements gained from the IMU are influenced by the GNSS measurements, consistency checking between the IMU and GNSS measurements no longer represents a comparison of independent sensors.

To overcome this problem, some transformation must be found, under which the IMU measurements can be compared with GNSS measurements, such that the comparison is insensitive to both the initial IMU orientation and the IMU measurement biases. In this work, we examine consistency between GNSS and IMU through the norms of the acceleration vectors and rotation rate vectors.

2. SPOOFING SCENARIO

This work explores the use of low cost IMU sensors in the detection of spoofing of GNSS signals for vehicular applications. A typical monitoring receiver is considered, which may be installed in a vehicle for the purposes of monitoring or reporting the vehicle position to some regulatory or commercial entity. It is assumed that the receiver is installed in a tamper-evident enclosure with a single-element GNSS antenna exposed to the sky. One example might be a digital tachographs, such as [1]. As such, it is possible that the holder of the device, who may wish to lead the receiver to compute an incorrect position, might obscure the reception of genuine GNSS signals, and introduce counterfeit ones.

A sporadically operating vehicle is assumed, such that GNSS-based positioning is naturally interrupted between journeys, either because the monitoring receiver is powered down when the vehicle is not in use, or because it is likely to be parked in a GNSS-denied area, such as an underground or roofed parkade or garage. Under these conditions, it is possible that the

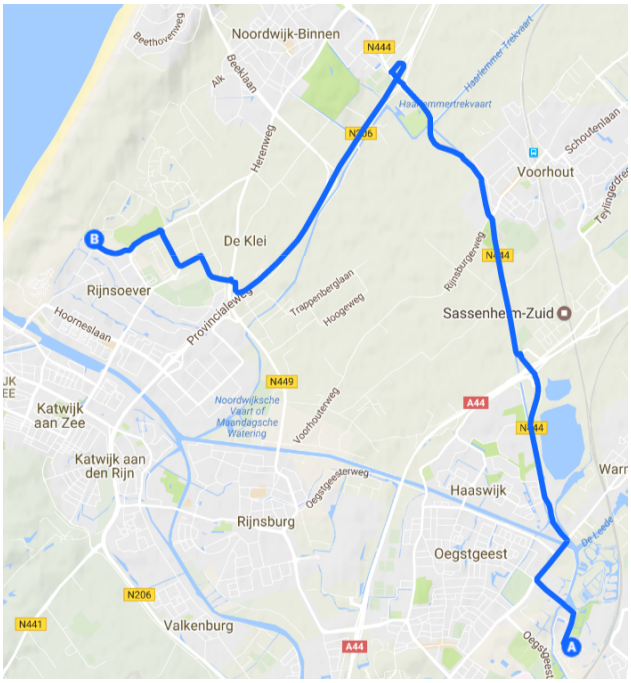


Figure 2: Route taken for each data collection in the campaign. The journey begins in a residential premises at the point denoted 'A', traverses a suburban environment, followed by approximately 4 km of motorway, and finishes in a suburban region, at the location denoted by 'B'.

GNSS antenna is shielded from the genuine signals, and that the counterfeit signals are introduced either before the receiver is switched on, or before the vehicle leaves the GNSS denied area. When counterfeit signals are introduced to the receiver in this way, then spoofing detection mechanisms which monitor signal transients, received power variations, or distortions to the received GNSS signals, are likely to be ineffective. Specifically, in this work, it is assumed that the receiver starts in a spoofed condition, and observes only the counterfeit GNSS signals (and therefore observes no transient from genuine-to-spoofed signals), and retains no useful information or operating states from prior unspoofed operation.

Given the ease with which simple simulator-based GNSS spoofing devices can be constructed, it is clear that a receiver subject to this style of self-spoofing will find it difficult to defend itself using only the information derived from the GNSS antenna. This work explores how the use of low cost IMU sensors, that could be integrated into the GNSS receiver, might enable the detection of spoofing. It is assumed that the inertial sensors are not installed in any specific orientation relative to the vehicle body frame, and that the orientation might be manipulated by the cheating user. Moreover, low-cost MEMS sensors are assumed and that the sensors may exhibit a high bias and gain (scale-factor) uncertainty. The challenge addressed in this work is

that of exploiting this inertial sensor for the purposes of determining whether the GNSS-derived position information is based on the reception of genuine GNSS signals, or whether it is spoofed.

In this work, no attempt is made to calibrate devices using GNSS-derived information. This choice is made in order to *strictly preserve the independence of the IMU*, ensuring that the cheating user cannot influence the detection performance: either by physically manipulating the orientation of the IMU; or by attempting to manipulate the calibration coefficients through spoofed GNSS signals. The IMU is therefore used in a *stateless* manner, where the information contained in each set of measurements is fully independent of previous measurements. The basic idea is illustrated in Figure 1 Given these constraints, it is clear that the use of the IMU as a traditional strap-down system [2]. However, in this particular case, it is not necessary to employ the IMU as a navigation sensor, but rather as a spoofing detection sensor, wherein it can be used in some form of consistency check. To achieve this, some projection of the inertial information must be found that is insensitive to the unknown calibration coefficients. This is discussed further in Section 4.

2.1. State-Of-The-Art

In [3], a formal statistical analysis of the problem of spoofing detection is provided, considering a shipborne GNSS receiver equipped with a high-quality and well-calibrated inertial measurement unit. The work develops a statistical tests capable with well characterized detection and false-alarm rates given some prior knowledge of the inertial measurement unit, it's calibration, and some simplifying assumptions relating to the measurement errors. Among these, are the assumptions that the device is well calibrated, such that the residual measurement errors can be modeled as zero mean Gaussian random variables, and furthermore that the mechanization equations are known, such that the IMU measurements can be reliably transformed to easting and northing, as seen by the GNSS antenna.

Another approach to spoofing detection is presented in [4] and [5] with specific application to aviation navigation. The work focuses on a loose-coupling of GNSS and INS and proposes a spoofing detection test statistic based on the norm of the innovation vector for Kalman filter based GNSS-INS positioning system. In essence the test statistic captures any sudden deviation between the INS and the GNSS trajectories, or any apparent change in the attitude or bias vector for the IMU. In the event of a spoofing attack, any change in the spoofed GNSS trajectory relative to the true trajectory of the aircraft would result in a shift in the distribution of the norm of the innovation vector from central to non-central. Similar to [3], given some assumptions about the measurement errors, a detection and false-alarm rates can be predicted.

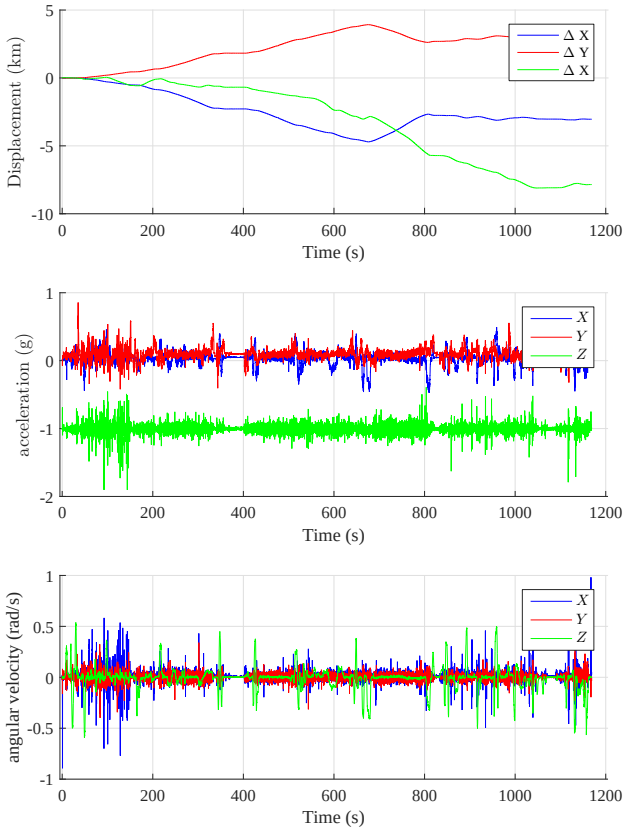


Figure 3: Example of the raw GNSS and IMU measurements showing the delta ECEF GNSS position (top), and the instantaneous IMU acceleration (middle) and angular velocity (bottom).

A different approach to spoofing detection using moderate or low-cost inertial units is presented in [6] and is applied to aircraft. In this case, the proposed approach involves a direct comparison of the absolute vertical acceleration experienced by the inertial sensor, and the equivalent acceleration reported by second-difference of GNSS precise-point position (PPP) solution. This comparison exploits a high precision GNSS trajectory, and requires knowledge of the attitude of the IMU and some level of calibration (including gravity removal). The approach is more heuristic (as is the case in this manuscript) but supports the analysis with extensive experimentation.

We note that in contrast to previous work, the spoofing detection method proposed here does not require knowledge of the IMU attitude (either a priori [3, 6] or derived through online estimation [4, 5], and does not place any requirements on knowledge of IMU biases or (as in [3, 6]) and does not require that they be estimated (as in [4, 5]).

3. DATA COLLECTION

To explore the problem of spoofing detection using inertial measurements, a large set of measurements were collected. Two scenarios were considered: the unspoofed scenario, where the GNSS and IMU data were consistent, and corresponded to the same trajectory; and the spoofed scenario where the GNSS and IMU data were inconsistent, as the GNSS-based PVT did not correspond to the trajectory experienced by the IMU. It is assumed that the spoofing equipment used by the cheating user is perfect, such that the spoofed GNSS PVT is representative of a nominal trajectory, with the exception that it corresponds to a trajectory that is different to the one experienced by the IMU. That is, it exhibits no anomalous features, (i.e. unusual accelerations, rotations etc.), that would otherwise be indicative of spoofing. The unspoofed case was emulated by simply collecting simultaneous GNSS and IMU datasets under nominal vehicular dynamics. The spoofed case was emulated by pairing a series of genuine GNSS measurements with a series of IMU measurements from a different journey.

A data collection campaign was initiated, wherein a short data was collected each day, over 30 days. This dataset consisted of GNSS and inertial measurements taken form a cellular handset, during a 12 km automotive commute including urban, suburban and motorway conditions. The GNSS data included GPS and GLONASS measurements, taken using an iPhone SE which used a Qualcomm WTR1605 RF Transceiver. The GNSS measurements were recorded at a rate of 1 Hz, and the IMU measurements were recorded at a rate of 10 Hz. Both were logged to file for post-processing. Each journey lasted approximately 20 minutes and included speeds ranging from 30 to 110 km/hr. The recorded data was post-processed, up-sampling the GNSS data to 10 Hz, such that each dataset consisted of a 9-dimensional time-series, being: latitude, longitude, altitude, 3D acceleration, and 3D angular velocity. A trace of the route is shown in Figure 2 and an example of the raw measurements recorded is shown in Figure 3.

4. ALGORITHM DESCRIPTION

Under the assumption that the device is installed in the vehicle and only checked periodically for evidence of tampering, this work aims to make no unnecessary assumptions regarding the device installation or calibration. As such, no assumptions about the device orientation or the accelerometer or gyroscope biases are made. The detection of spoofing is based simply on an examination of the consistency between the IMU and the GNSS measurements.

However, to perform some comparison, it is necessary to project the measurements onto a common space. In this case, the GNSS measurements were projected onto equivalent acceleration and angular velocity measurements. To avoid the need to estimate orientation, and under the assumption that the orientation did not change rapidly, a high-pass filter was applied to the acceleration vector, to reject the bias and gravity contribution:

$$A_{\mathrm{IMU}} = \|\alpha_{\mathrm{IMU}} * h_{\mathrm{HP}}\| \tag{1}$$

where α_{IMU} denotes the 3D IMU acceleration vector, and h_{HP} denotes impulse response of a second-order high-pass Butterworth filter with a cut-off frequency of 0.01 Hz. The choice of this filter is somewhat arbitrary, but driven by the constraint that the cutoff is sufficiently high that is rejects any slowly varying biases, and also rejects the gravity contribution even when the attitude changes slowly. At the same time the cutoff must be sufficiently low that it does not reject any of the acceleration and angular velocity measurements that correspond to vehicle motion. The value of 0.01 Hz was chosen following a preliminary experiment, however more thorough analysis is likely necessary to select an appropriate value.

The GNSS based acceleration was found by simply taking the second difference of the earth-centered-earth-fixed (ECEF) position estimates:

$$A_{\mathrm{GNSS}} = \left\|\nabla^2 p_{\mathrm{ECEF}}\right\| F_s^2 \tag{2}$$

where p_{ECEF} denotes the ECEF GNSS based position estimate, A_{GNSS} denotes the 3D GNSS based acceleration estimate, ∇^n denotes the n^{th} difference of the time-series, and F_s denotes the GNSS measurement rate.

The GNSS based angular velocity was computed in a similar manner, assuming that the vehicle only rotates around its z-axis. Firstly, the GNSS based position was transformed into easting and northing (EN) measurements, disregarding the vertical, relative to the first GNSS position in each observation window, and the instantaneous velocity computed as:

$$v^{\mathrm{E}}_{\mathrm{GNSS}} = \nabla p_{\mathrm{E}} F_s \tag{3}$$

$$v^{\mathrm{N}}_{\mathrm{GNSS}} = \nabla p_{\mathrm{N}} F_s \tag{4}$$

The GNSS heading can be calculated as

$$H_{\mathrm{GNSS}} = \mathrm{atan}\left(\frac{v^{\mathrm{E}}_{\mathrm{GNSS}}}{v^{\mathrm{N}}_{\mathrm{GNSS}}}\right) \tag{5}$$

where H_{GNSS} is GNSS based heading information. From this heading measurement, a GNSS based estimate of the angular velocity in the horizontal plane can be computed via:

$$\omega_{\mathrm{GNSS}} = [0\ 0\ \nabla H_{\mathrm{GNSS}} F_s] \tag{6}$$

with a magnitude denoted by $W_{\mathrm{GNSS}} = \|\omega_{\mathrm{GNSS}}\|$. Finally, the norm of the IMU based angular velocities measurements were computed as:

$$W_{\mathrm{IMU}} = \|\omega_{\mathrm{IMU}}\| \tag{7}$$

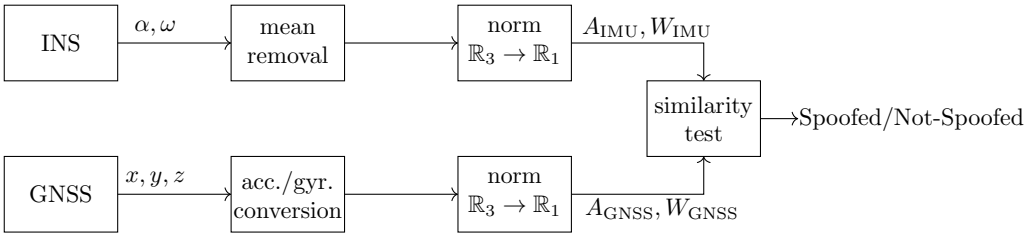


Figure 4: A basic illustration of the spoofing detection scheme, illustrating the flow of measurements from the GNSS receiver and from the IMU, various stages of measurement conditioning and the final measurement consistency check prior to the Spoofed/Not-Spoofed decision.

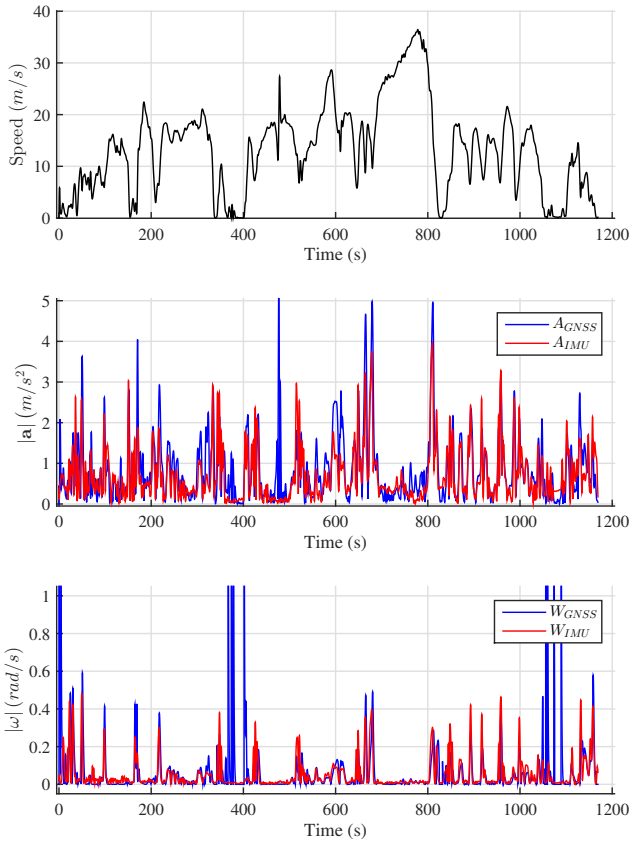


Figure 5: Example of the vehicle speed (top), the norm of the acceleration (middle) and angular velocity (bottom) as computed from the GNSS positions and directly from IMU measurements.

The rate of change of GNSS heading, W_{GNSS} was compared with W_{IMU} for consistency checking. An example of the norm of the acceleration and angular velocity computed from GNSS measurements and directly from the IMU measurements is shown in Figure 5 for a six minute period during one of the recorded datasets.

A clear correlation is evident for periods where the vehicle undergoes some dynamics, however during periods of constant velocity, too few features are present to provide any measurable correlation and the noise present on the IMU and GNSS are uncorrelated. The comparison between the pairs of time series was made by examining the correlation coefficient, defined as the ratio of the sample covariance of the two time series to the product of their sample standard deviations, and is given by:

$$\mathcal{C}(x,y) = \frac{\langle (x - \langle x \rangle_\tau)(y - \langle y \rangle_\tau) \rangle}{\sqrt{\left\langle (x - \langle x \rangle_\tau)^2 \right\rangle \left\langle (y - \langle y \rangle_\tau)^2 \right\rangle}} \tag{8}$$

where $\langle x \rangle_\tau$ denotes the sample average of x over the interval τ. The two correlation coefficients examined in this work are computed as:

$$\rho_\alpha = \mathcal{C}(A_{\text{GNSS}}, A_{\text{IMU}}) \tag{9}$$

$$\rho_\omega = \mathcal{C}(W_{\text{GNSS}}, W_{\text{IMU}}) \tag{10}$$

Examples of these coefficients are shown in Figure 6, discussed in the next section. The final decision statistic computed as the weighted sum of the two coefficients, where κ is a scaler on the interval $(0, 1)$:

$$\rho = \kappa \rho_\alpha + (1 - \kappa)\rho_\omega \tag{11}$$

Finally, the decision as to whether the receiver is spoofed or not is based on a simple threshold test of the devision statistic:

$$\rho \underset{H_1}{\overset{H_0}{\gtrless}} V_T, \tag{12}$$

where the threshold V_T is selected to satisfy some desired detection or false-alarm rate.

5. EXPERIMENTAL RESULTS

The principle of operation of this detection mechanism is that there should exist a reasonable correlation be-

tween the norm of the acceleration as computed from GNSS positions and that measured directly on the IMU and, similarly, there should exist a correlation between the norm of the GNSS derived angular velocity and that measured from the IMU. In the case that the GNSS receiver is experiencing spoofing, then this correlation should not be present.

5.1. Decision Statistic

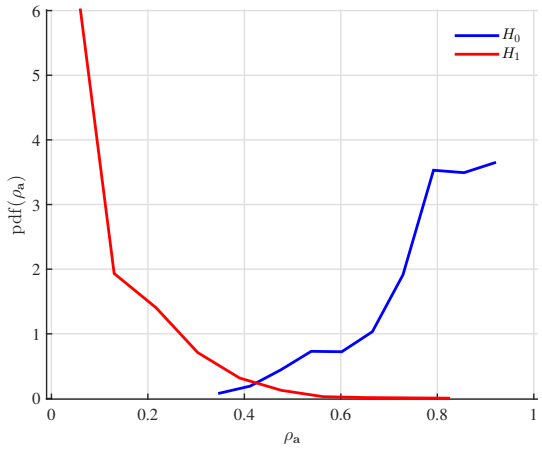
To explore this idea, the correlation between the GNSS and IMU measurements were examined on short samples of data randomly drawn from the datasets. In half of the cases, the GNSS and IMU data were extracted from the same period of a single dataset, such that the GNSS and IMU data were coherent. These cases were assigned to be the 'non-spoofed' hypothesis, and denoted H_0. In the other half of the cases, the GNSS and IMU data were respectively drawn from different datasets and, as a result, the GNSS and IMU were not coherent. There cases were assigned to be the 'spoofed' case, and denoted H_1. Although all of the datasets corresponded to the exact same trajectory, instance-to-instance difference due to traffic and other random influences were expected to result in a decorrelation.

A total of $10,000$ samples were drawn, and the probability density functions of each of the two correlation coefficients, ρ_α and ρ_ω, under each hypothesis, were computed. An example of these measurements, considering an observation period of $\tau = 180$ seconds, is shown in Figure 6. As can be seen, both coefficients offer a reasonable separation between the two hypotheses, although it appears that the acceleration based metric is more specific. It is likely that this is a result of the poor quality of the velocity estimate used in the heading determination, which is based on the first difference of 1 Hz GNSS based position estimates. A higher rate position estimate, or access to a Doppler based velocity estimation would likely improve this. Nonetheless, both metrics exhibit a high likelihood of decorrelation under H_1.

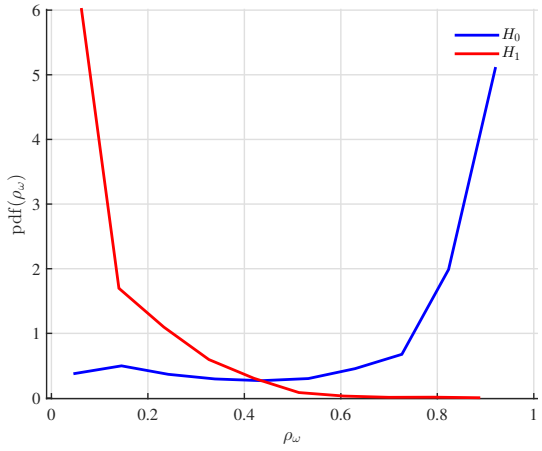
The weighted sum of these two coefficients was then computed for a variety of different weighting coefficients ranging from $\kappa = 0.1$ which was predominantly an acceleration measurement, to $\kappa = 0.9$ which was predominantly a rotation-rate measurement. The probability density function of the combined correlation coefficient is shown in Figure 6 (c) for $\kappa = 0.75$. From inspection it can be seen that the separation of the H_0 and H_1 curves is marginally improved with respect to the two individual coefficients of Figure 6 (a) and (b).

5.2. Spoofing Detection

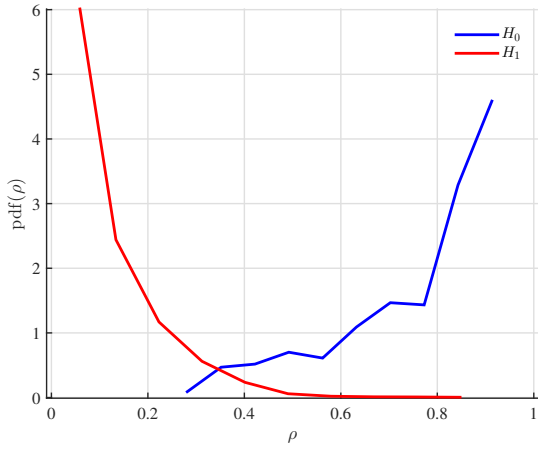
To test the spoofing detection performance of the proposed technique, a total of $100,000$ samples were drawn from the recorded datasets, and the combined



(a) Probability density of the acceleration decision statistic

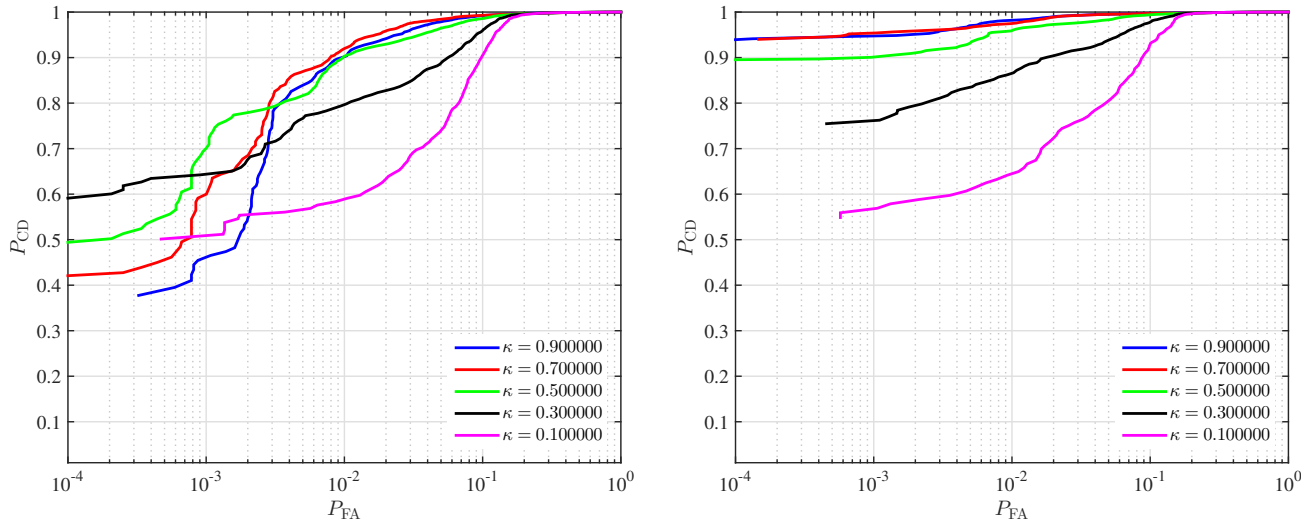


(b) Probability density of the angular velocity decision statistic



(c) Probability density of the combined decision statistic ($\kappa = 0.75$)

Figure 6: Examples of the probability density function of the measured correlation coefficient between the GNSS and IMU based acceleration (a) and angular velocity (b), and the weighted sum of the two correlation coefficients (c), under both the unspoofed (H_0) and spoofed (H_1) hypothesis and given an observatino period of $\tau = 180$ seconds.



(a) ROC curve for observation period of 120 seconds.

(b) ROC curve for observation period of 180 seconds.

Figure 7: Computed receiver operating characteristic curves for the combined decision statistic considering a variety of weighting factors, κ, and two different observation periods, being 120 seconds (a) and 180 seconds (b).

decision statistic, ρ was computed. This was then compared to a threshold to compute the receiver-operating-characteristic (ROC) [7]. A range of weighting coefficient was examined, ranging from $\kappa = 0.1$ to 0.9. Two different observation period were examined, being $\tau = 120$ seconds and $\tau = 180$ seconds. The computed ROC curves are shown in Figure 7. It is apparent that only moderate performance can be achieved for short observation periods. For example, a spoofing detection probability of approximately 0.6, with a false-alarm probability below 10^{-3} can be achieved with a time-to-alarm of 120 seconds. However, the detection performance can be significantly improved by tolerating a higher time-to-alarm for 180 seconds. For example, a detection rate of 0.95 and a false-alarm rate of 10^{-4} can be observed in Figure 7 b. Interestingly, for longer observation periods, the contribution of the gyroscope appears to be less valuable. However, it should be noted that these conclusions are subjective and may change significantly given different IMU performance and/or different vehicular dynamics.

6. CONCLUSION

In terms of spoofing detection performance, seems that the detection accuracy (i.e. the relative rates of correct-detection and false-alarm) in line with what might be demanded by some commercial applications, and so this simple technique might pose a useful barrier against simple simulation-based spoofing. Further work is required to examine how the technique performs when considering current automotive-grade mass-market IMU-enabled GNSS modules, such as the ublox EVA-M8E [8]. It likely that such modules will provide greater precision GNSS measurements, at a higher rate, reducing some of the noise observed in the angular-velocity estimates.

It is important to stress, however, that this barrier is only effective against relatively simple spoofing, and a more sophisticated spoofing device might find means of overcoming it. Specifically, to accommodate the uncertainty in the inertial sensor orientation and calibration, the decision statistic is computed based on the first difference (rotation-rate) and second difference (acceleration) of the GNSS based PVT. As such, the decision statistic is both translation-invariant and rotation-invariant (also, but perhaps less importantly, reflection-invariant).

This implies that any one of an infinite number of candidate trajectories will satisfy the spoofing detection mechanism, provided it can be expressed as a translation and/or rotation of the true trajectory. To successfully spoof the receiver, the cheating user would be forced to produce a set of counterfeit GNSS signals that corresponded to a receiver trajectory that is geometrically similar to the true trajectory. This might require the spoofing device to be equipped with a GNSS receiver, and to perform a real-time generation of the spoofed trajectory based on measurements of the true trajectory (perhaps applying some prescribed translation of the position). By itself, this might already pose a technological complexity barrier against some maliciously motivated users.

However, elaborating on these conclusions, it seems that additional information is required to adequately extend this spoofing barrier. Given that the proposed scheme can only constrain the cheating user in terms of what shape the spoofed trajectory might be, is seems as though consistency checking with prior knowledge of the plausible or possible user trajectories would be

useful. Specifically, an additional consistency check of the GNSS-based position with a map of the road network might help. With this addition, the cheating user would be forced to produce a counterfeit trajectory with similar shape to the genuine trajectory of the vehicle, while also being constrained to select from actual segments of the road network to satisfy this additional map-matching constraint. The spoofed trajectory would need to preserve the shape of the genuine trajectory, such that the spoofed trajectory would be limited to those segments of the road network that had a similar shape to the actual road that is traversed. A sufficiently similar trajectory might not exist, or might appear implausible for other reasons (such as proximity to recent reported positions), thereby effecting a meaningful barrier against spoofing.

One final note is that the proposed work has assumed that the inertial measurement unit, although uncalibrated and installed at an unknown attitude, is nonetheless faithfully reporting the motion it experiences. The assumption that the sensor is impervious to external manipulation is, perhaps, naíve. Recent studies have demonstrated that it may be possible to provoke false measurements in certain kinds of MEMS sensors by exciting them with ultrasonic impulses [9]. Precise manipulation of the reported acceleration has been demonstrated for a wide variety of IMU models, suggesting that the authenticity of reported IMU measurements might not be guaranteed. Although this vulnerability might appear academic, it is possible that it might be operationalised in the future. In light of this development, it might further be necessary to implement some degree of sheilding of the IMU and/or to add some detection mechanism for such an attack (similar to jamming detection systems on the GNSS front-end).

REFERENCES

[1] GeoLoc, "DTCO GeoLoc Guide: Service Information - Tachographs, Telematics abd Services (SI 116279)," 2013, http://www.fleet.vdo.com/,.

[2] D. Titterton and J. Weston, *Strapdown Inertial Navigation Technology (IEE Radar, Sonar, Navigation and Avionics Series)*. The Institution of Engineering and Technology, 2005.

[3] P. F. Swaszek, S. A. Pratz, B. N. Arocho, K. C. Seals, and R. J. Hartnett, "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals," *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014)*, pp. 745–758, September 2014.

[4] C. Tanil, S. Khanafseh, and B. Pervan, "Detecting Global Navigation Satellite System Spoofing Using Inertial Sensing of Aircraft Disturbance," *Journal of Guidance, Control, and Dynamics*, vol. 40, no. 8, pp. 2006–2016, 2017.

[5] ——, "An INS Monitor Against GNSS Spoofing Attacks During GBAS and SBAS-assisted Aircraft Landing Approaches," *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, pp. 2981 – 2990, September 2016.

[6] S. Lo, Y. H. Chen, T. Reid, A. Perkins, T. Walter, and P. Enge, "The Benefits of Low Cost Accelerometers for GNSS Anti-Spoofing," *Proceedings of the ION 2017 Pacific PNT Meeting, Honolulu, Hawaii*, pp. 775–796, May 2017.

[7] J. G. Proakis, *Digital Communications*, 3rd ed., ser. Electrical Engineering Series. McGraw Hill International Editions, 1995, ISBN 0-07-232111-3.

[8] u-blox, "EVA-M8E Miniature Untethered Dead Reckoning Module Data Sheet," uBX-15028061 - R03, www.u-blox.com,.

[9] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks," in *2017 IEEE European Symposium on Security and Privacy (EuroS P)*, April 2017, pp. 3–18.