Uncoupled Accelerometer Based GNSS Spoof Detection for Automobiles using Statistic and Wavelet Based Tests

Andrew Neish, Sherman Lo, Yu-Hsuan Chen, Per Enge – Stanford University

Abstract

Low cost IMUs have shown potential for use in spoof detection of dynamic vehicles. IMUs represent independent sources of measurement that can be corroborated with accelerations derived from GNSS measurements. This work looks at statistical methods used in previous work in aircraft and investigates their use in spoof detection for cars. Although signatures in dynamics for cars are not as strong as they are in aircraft, there is agreement between both sources of measurement. The statistical methods previously used, however, are not yet robust to factors in the automobile environment contributing to false alarms. A method focused on the frequency content using wavelet coherence is introduced that has the potential to greatly simplify the operations necessary to compare acceleration signatures.

I: Introduction

Since GPS became fully operational in 1995, it has become pervasive throughout the world. With billions of receivers in operation around the globe, GPS has enabled the advancement of technologies and infrastructure in virtually all fields. The Department of Homeland Security states that 15 of the 18 critical infrastructure and key resources sectors in the United States rely upon GPS. This reliance on GPS has produced a double-edged sword: while becoming ubiquitous, its vulnerabilities have also become more apparent and ripe for exploitation. GPS signals are received at very low power and the data is a part of a predictable structure sent on an unencrypted channel. These aspects make GPS vulnerable to jamming and spoofing attacks. Personal Protective Devices (PPDs) that are intended to disrupt GPS locally have unintentionally disabled GPS in other systems. This is a cause for great concern in safety of life systems that are dependent upon GPS's position and timing capabilities. Spoofing events have also occurred recently, both seemingly intentional near the Kremlin in Russia and unintentional at the most recent ION GNSS+ in 2017. If users are to continue to rely upon GPS for accurate timing and position, their receivers must be capable of mitigating or detecting spoofing events.

There has been a large push within the GNSS community to create solutions to the problems of spoofing. Some of these have focused on the use of receiver metrics such as Automatic Gain Control (AGC) and C/N_0 [1]. Others have looked at incorporating cryptographic techniques to authenticate the data [2]. There is no one technique that can detect all forms of spoofing attacks, but detection techniques can be developed with the goal to increase the effort required for a spoofer to be successful. A strong, feasible spoof detection method must be low-cost, robust (low false alarm rates and low missed detection rates), and must be capable of detecting spoofing attacks using a steady state method. Many anti-spoofing techniques focus on the transient signs of spoofing leaving them vulnerable to spoofing attacks that are successful in the initial capture of a receiver. This research focuses on a technique that can detect spoofing during the entire duration of a spoofing attack.

In previous work, it was shown that vehicle dynamics can be used to create unpredictable signatures that are never repeated [3]. In the cryptographic world, signatures such as these are known as a "one-time pad". By measuring the accelerations using a low-cost Microelectromechanical Systems (MEMS) Inertial Measurement Unit (IMU), the dynamics measured by this device on board the vehicle were able to be directly verified using the GPS derived accelerations using PPP. The MEMS accelerometer measures specific force in the body frame and the GPS derived accelerations can be represented in the ENU frame with a position solution. Because of this, a rotation to align both frames must be accomplished first. There is no coupling between the MEMS IMU and the GPS measurements so once the alignment was accomplished, the accelerations were compared to verify the validity of the incoming signals. Test statistics, such as mean and variance tests on the differenced accelerations, were developed to scrutinize the authenticity of the incoming GPS signals and an executive monitor (EM) was created to appropriately screen these statistics and flag when there was a suspected spoofing attack.

This paper focuses on the detection techniques involved in the comparison between the accelerometer and the GPS measurements. Previous research looked detection techniques using data collected from an aircraft. This paper will look at applying those techniques to cars as well as introduce another potential detection method using wavelets. The paper is split into the following sections: Section II gives background on how spoofing is detected using inertials; Section III introduces the experiment test setup; Section IV looks at the performance of spoof detection algorithms using statistical tests mean difference and sample variance; Section V looks at the potential wavelets may have in spoof detection; and finally Section VI gives conclusions to this work along with future areas of research.

II: Spoof Detection Using Inertials

The concept of using inertial measurements with GNSS to provide redundancy and spoof detection is very natural. Hence, it is not surprising that several researchers have proposed using inertial for GNSS spoof detection. For example, O'Keefe and Tanil proposed the comparison of inertial to GNSS derived position for spoof detection in automotive and aviation applications, respectively [4][5][6]. This is powerful but also limited as the inertials need to be calibrated with GNSS and high-grade gyroscopes are needed to propagate position without significant error. A more direct comparison is to examine rates (acceleration, rotation rate) derived from inertials and from GNSS. This is more direct as these are the fundamental outputs of the inertial sensor. The benefit of this approach is an infinite observation window and a clearer comparison allowing for a straight-forward safety analysis. A drawback is that reasonable knowledge of vehicle orientation is needed though this is also required for position comparisons. For this paper, we focus on comparing acceleration from MEMS accelerometers and GNSS. These MEMS are readily available in reasonable costs for automotive and other applications.

To have robust implementations of the inertial spoof detection technique, there are three pre-requisites. First, there needs an adequate acceleration signature. By acceleration signature, we mean acceleration profiles that are not easily determined by an attacker. Hence, the acceleration profile should not be easily predictable and have enough variations to make it difficult to precisely guess. Second, we need to be able to compare that signature between the GNSS and accelerometers. The accelerometers are fixed to the vehicle body frame while the GNSS measurements are not aligned with the body. GNSS results are often expressed in inertial and local east north up (ENU) frame. Hence comparison requires that we can properly rotate and align the GNSS axes with those of the accelerometer. Third, robust detection algorithms must be developed to use these comparisons. By robust, we mean that the overall probability of false alerts (P_{fa}) and missed detection (P_{md}) are very low. To do that, we develop different monitors to compare different aspects of the acceleration signature such as different axes or characteristics of the acceleration profile.

This section focuses on the first two requisites – finding adequate acceleration signal for a robust test and processing to align the GNSS and acceleration measurement axes. Acceleration is measured directly by the accelerometer. For GNSS, velocities derived from carrier Doppler are used to get GNSS accelerations.

Acceleration Signature

An acceleration profile that a spoofer cannot precisely guess a priori represents in cryptographic terms, a one-time pad. If a spoofer cannot adequately predict it, we can use the difference between our actual acceleration profile, as determined by the accelerometers, and the spoofed GNSS acceleration to detect the deception. Results from flight shows that there can be many sources of unpredictable acceleration — wind, pilot input to thrust, lowering of the landing gear, etc. [3][7]. Automotive applications should also have difficult to predict components due to bumps, driver inputs, and turns. Along track, cross track and vertical acceleration may all be difficult to predict a priori. This may even be difficult to determine in near real-time even if the driving route is known as an attacker may not easily determine the exact time turns and accelerations are initiated by the driver.

However, for the acceleration profile to be useful, it must have high enough signal relative to the sensor noise and errors induced by our comparison processing. With a reasonable acceleration profile, any spoofing attack without a good estimate of the vehicle acceleration should be detectable. Even a spoofer that can measure the acceleration remotely or relay a measurement of acceleration from an onboard device may be detectable. This is because the spoofer will incur errors and delays that may be detected provided there are high frequency dynamics.

However, there are threats that the technique cannot catch. An attacker with accurate and near real-time knowledge of acceleration can slowly drift the measured position from truth as long as they keep the acceleration error within the allowable detection tolerance. Physical security or complimentary detection techniques may be used to handle these threats.

Axes Alignment

Rotating and aligning the GNSS-derived accelerations with the accelerometer derived accelerations is necessary as they are measured on different reference frames. To make such an alignment requires some knowledge of the orientation of the vehicles as the accelerometer is lined up in the vehicle body frame. There are several ways to derive orientation. Orientation may be derived from a high quality gyroscope and occasional calibrations and updates. Because automobiles have reasonably stable attitudes, drive in defined directions (roads) and frequently stop, calibration may be possible without using GNSS. Another method is to derive coarse orientation from GNSS. The direction of vehicle travel roughly approximates heading. Roll and pitch are harder to estimate accurately with GNSS. The use of GNSS for calibration or orientation is reasonable and does not affect accelerometer measurements. If GNSS is spoofed, this can show up in incorrect accelerations and/or orientation[1].

With orientation known, we rotate the GNSS accelerations to the body axes. This is shown in Equation 1 and 2 where α, β, and γ are the heading, pitch, and roll angles, respectively. As accelerometers measure specific force rather than inertial acceleration, we need to compensate for the gravity force. We can either add the acceleration due to gravity, g, set nominally at 9.81 meters per second squared (m/s^2), to the GNSS up direction or subtract it from the accelerometer z-axis. The former is seen in Equation (1). Then we can calculate an acceleration difference between the accelerometer and GNSS acceleration.

$$\boldsymbol{a}_{GNSS,body-g} = A * \left(\boldsymbol{a}_{GNSS,enu} + \begin{bmatrix} 0 \\ 0 \\ g \end{bmatrix} \right), \boldsymbol{a}_{GNSS,enu} = \begin{bmatrix} a_{gnss,E} \\ a_{gnss,N} \\ a_{gnss,U} \end{bmatrix} \quad 1$$

$$A = \begin{bmatrix} cos(\alpha)cos(\beta) & sin(\alpha)cos(\beta) & sin(\beta) \\ -sin(\alpha)cos(\gamma) + cos(\alpha)sin(\beta)sin(\gamma) & cos(\alpha)cos(\gamma) + sin(\alpha)sin(\beta)sin(\gamma) & -cos(\beta)sin(\gamma) \\ -sin(\alpha)sin(\gamma) - cos(\alpha)sin(\beta)cos(\gamma) & cos(\alpha)sin(\gamma) - sin(\alpha)sin(\beta)cos(\gamma) & cos(\beta)cos(\gamma) \end{bmatrix} \quad 2$$

For our initial analysis, we will use GNSS to provide orientation. Roll is not estimated as this is difficult to estimate with GNSS in an automobile. Heading and pitch may be estimated from the velocity vector and used. Heading is used. Pitch adjustment is sometimes employed. It did not make a significant difference for our test data as no major inclines were encountered.

With adequate acceleration signature and axis alignment, a comparison can be made. Figure 1 shows the vertical acceleration profile from GNSS and a commercial off the shelf (COTS) smartphone accelerometer. The high magnitude relative to errors, high frequency change, the variations from approach to approach makes use of accelerometer comparison for GNSS spoof detection feasible for aircraft approach [3]. Figure 2 shows the resulting acceleration difference between the two sensors.

[1] One could spoof GNSS such that the spoof induced error in orientation compensates for the spoof induced error in acceleration making the spoof more difficult to detect. However, this would be very challenging.

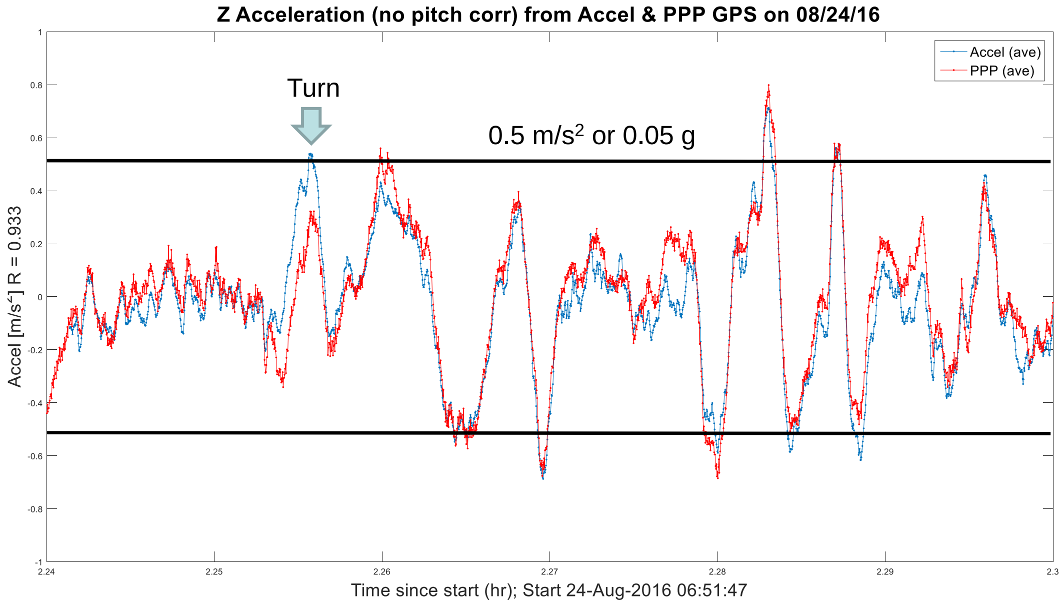


Figure 1. Acceleration (five second exponential averaged) from accelerometer vertical axis (body up) (blue) and precise point positioning (PPP) GNSS (red) versus time from start (hours) for first approach segment of August 24 2016 test flight. R is the correlation coefficient between the GNSS and accelerometer acceleration for the shown segment of flight

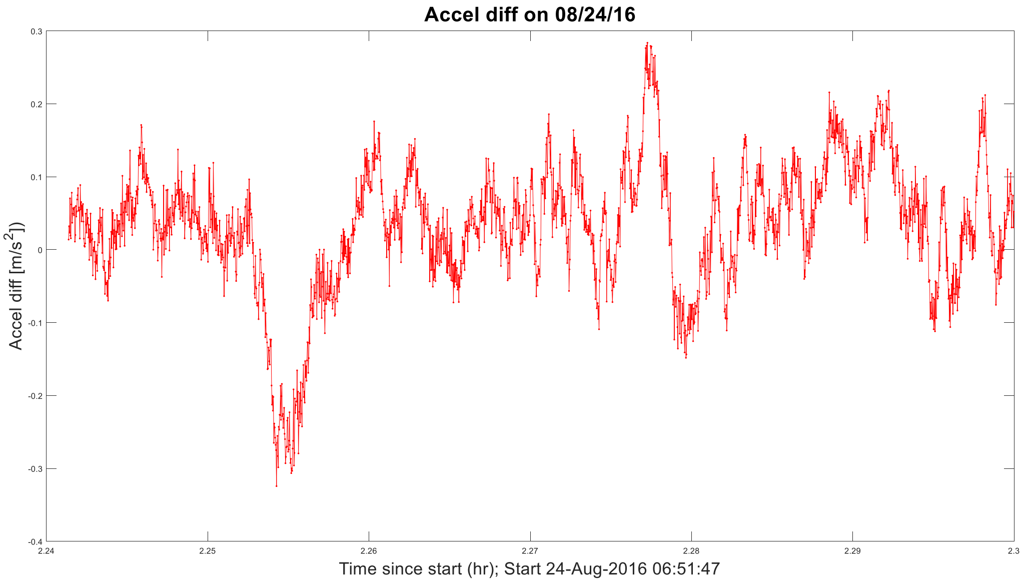


Figure 2. Acceleration difference between GNSS and COTS accelerometer derived vertical acceleration versus time from start (hours) on first approach segment of August 24 2016 test flight

III: Experimental Test Setup

Field experiments were conducted to examine the feasibility of the concept for automotive applications. These tests provide data from a variety of environments experienced by a car and allow us to examine various effects such as the acceleration signature on each axes and unmodeled pitch or roll.

Test Set Up

Our test van was set up with GNSS and several inertial measurement units (IMU) onboard. The GNSS receiver used was a Novatel SPAN with a Novatel pinwheel antenna. Three grades of MEMS IMU were used - specifically COTS smartphone (Galaxy Note 3), automotive (Bosch) and high grade MEMS (Novatel SPAN). Figure 3 shows the test set up and Table 1 shows the data collection rate. As seen in the figure, the IMUs were generally collocated while the GNSS antenna was located on the vehicle roof above the IMU. No moment arm correction was applied in our analysis to adjust for this difference.

Table 1. Update rate of sensor set up

Equipment	Update rate
GNSS velocity	10 Hz
COTS IMU	8 Hz
Auto IMU	200 Hz
SPAN IMU	100 Hz

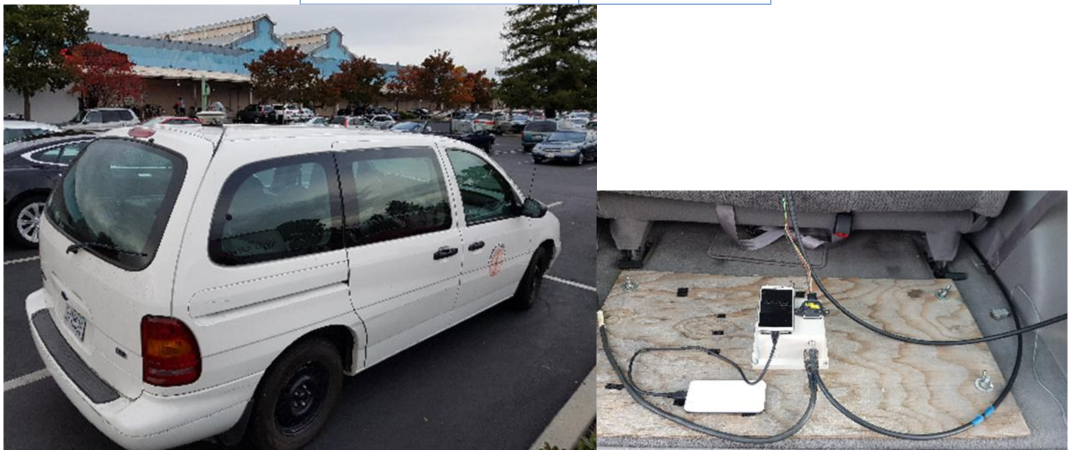


Figure 3. Experimental Set Up for November 2017 Tests. Van with GNSS antenna on roof (left) and IMU (right)

Several drive tests were conducted to cover various conditions from suburban, mixed urban and highway. Figure 4 shows the similar test routes on November 13 and 17, 2017 while Table 2 shows the times of various conditions for those dates. The 11/13 did not have SPAN accelerometer output due to a set up issue. Other tests were conducted prior to obtaining the automotive grade IMU to test the experimental set up.

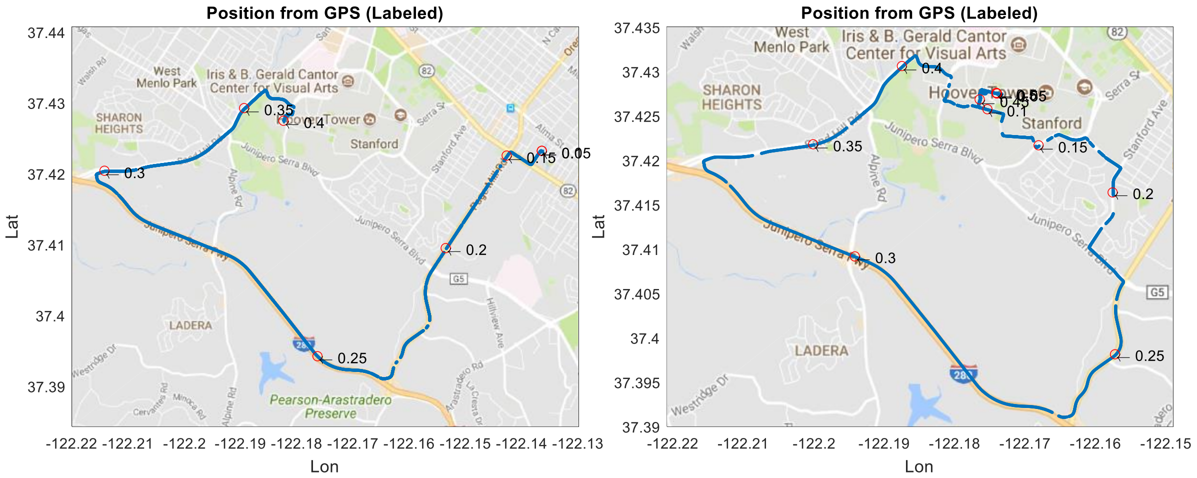


Figure 4. Drive route of November 13 and 17, 2017 test – left and right, respectively.

Table 2. Condition, start and end time from start of November 2017 test drives (in hours from start)

Condition	Start Time 11/13 (hr)	End Time 11/13 (hr)	Start Time 11/17 (hr)	End Time 11/17 (hr)
Suburban (static)	0 hr	0.11 hr	0 hr	0.05 hr
Suburban (light buildings)	0.11 hr	0.2 hr	0.06 hr	0.11 hr
Open suburban & foliage	0.2 hr	0.24 hr	0.11 hr	0.268 hr
Highway	0.24 hr	0.29 hr	0.268 hr	0.325 hr
Open suburban	0.29 hr	0.36 hr (END)	0.325 hr	0.43 hr
Covered suburban			0.43 hr	0.51 hr
Suburban (static)			0.51 hr	0.56 hr (END)

Measured Acceleration

The drive tests accelerations needed to be processed to conduct the comparison. First, orientation needs to be determined so that the GNSS measurements can be rotated into the body axes used by the accelerometers. GNSS velocity was translated into a local ENU frame and then differenced to get acceleration. Heading was estimated using velocity in the north and east direction. The estimate was considered valid only used if speed exceeded 2 miles per hour (2 mph). Otherwise, no heading estimate was provided or used. Pitch could also be estimated from the vertical and horizontal velocities. Second, the measurement times from each instrument needs to be aligned. As the data from each sensor were collected with independent instruments, their time references are generally different. Hence, we had to perform time alignment of the GNSS data to each IMU. The SPAN IMU acceleration was used to perform the alignment as it uses the same reference time as GNSS. We aligned time by aligning the accelerations of each unit to that of the SPAN. As they are collocated, their outputs are similar. By aligning the accelerometer reference time with the SPAN reference time, we are also aligning with the GNSS measurement time. We then perform exponential averaging to the acceleration data. With orientation information, the GNSS accelerations are rotated to the body frame, accounting for gravity. The overall calculation flow is shown in Figure 5.

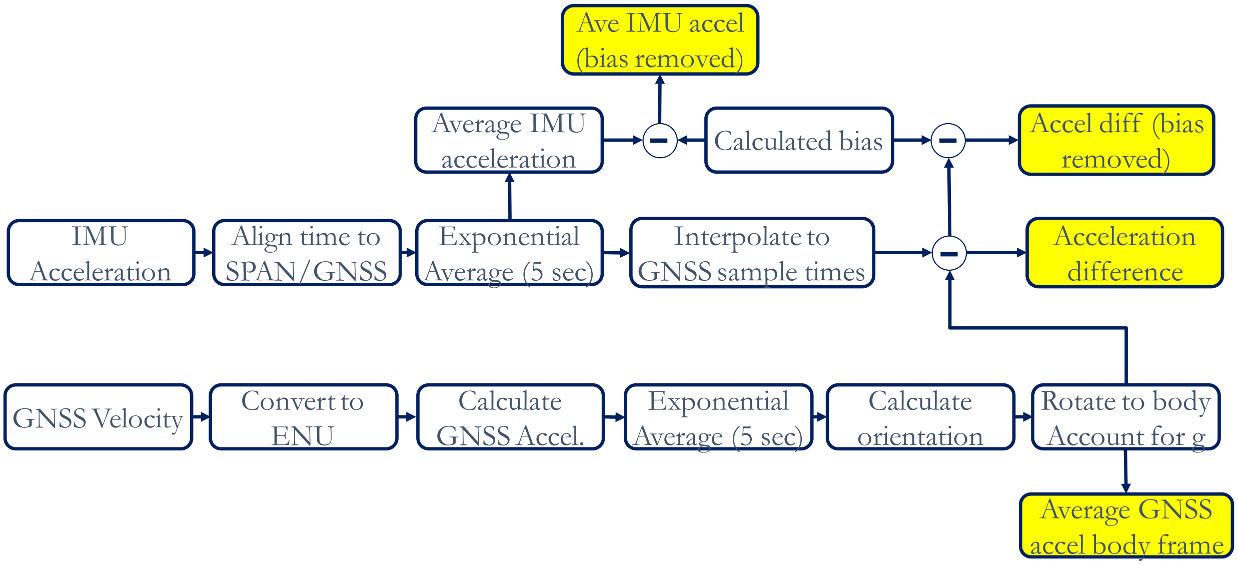

Ave IMU accel (bias removed)
Average IMU acceleration
Calculated bias
Accel diff (bias removed)
IMU Acceleration
Align time to SPAN/GNSS
Exponential Average (5 sec)
Interpolate to GNSS sample times
Acceleration difference
GNSS Velocity
Convert to ENU
Calculate GNSS Accel.
Exponential Average (5 sec)
Calculate orientation
Rotate to body Account for g
Average GNSS accel body frame

Figure 5. Processing flow for raw GNSS, accelerometer to get Acceleration Difference; Yellow indicates final products used

Nominal biases and measurement noise were also measured. Data from the static initial segments of the November drive tests were used to generate the statistics. Statistics for acceleration and acceleration difference of inertial from GNSS are calculated. Statistics for the raw and 5 second exponentially averaged accelerations are made. We typically use the 5 second exponentially averaged accelerations for our comparison as the raw measurements are generally very noisy and hence not good for a sample-by-sample comparison. The static statistical results are later shown in Table 5. The bias calculated then can be removed from the accelerations or acceleration differences

Figure 6 shows a comparison of along-track, cross-track and up acceleration derived from GNSS and MEMS accelerometers during a test drive involving several loops on a garage roof. Both a consumer mass market, commercial off the shelf (COTS) and high end MEMS (SPAN) accelerometer are shown. Overall the accelerometers match well, as they should since they are collocated. GNSS match reasonably on both along-track and cross-track when the accelerometer biases are removed. Hence, these directions seem like reasonable choices for comparison and detection. However, the match is not perfect. In the cross track direction, while the GNSS accelerations generally follow those of the accelerometer, it is often less in magnitude. This is seen again in Figure 7 which shows the result for November 17, 2017 with the addition of a Bosch (AUTO) grade accelerometer. Figure 7 also shows that the vertical acceleration is useful but noisier due to relatively small vertical accelerations experienced by automobiles and poorer GNSS performance in the vertical direction relative to the horizontal direction. Figure 8 shows similar performance results for November 13, 2017.

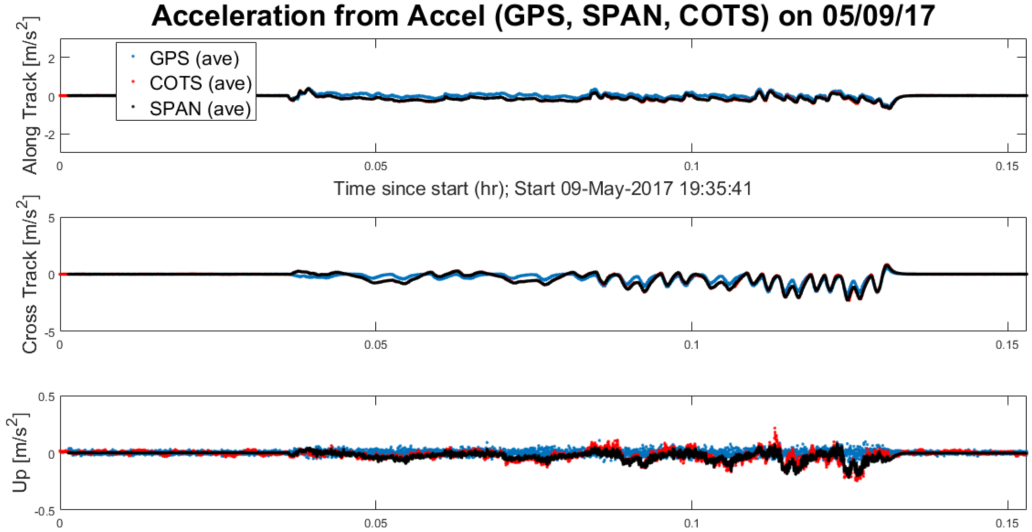


Figure 6. Comparison of GNSS, high end MEMS (SPAN) and consumer MEMS (COTS) acceleration (along track and cross track) during test loops in parking lot, May 9, 2017

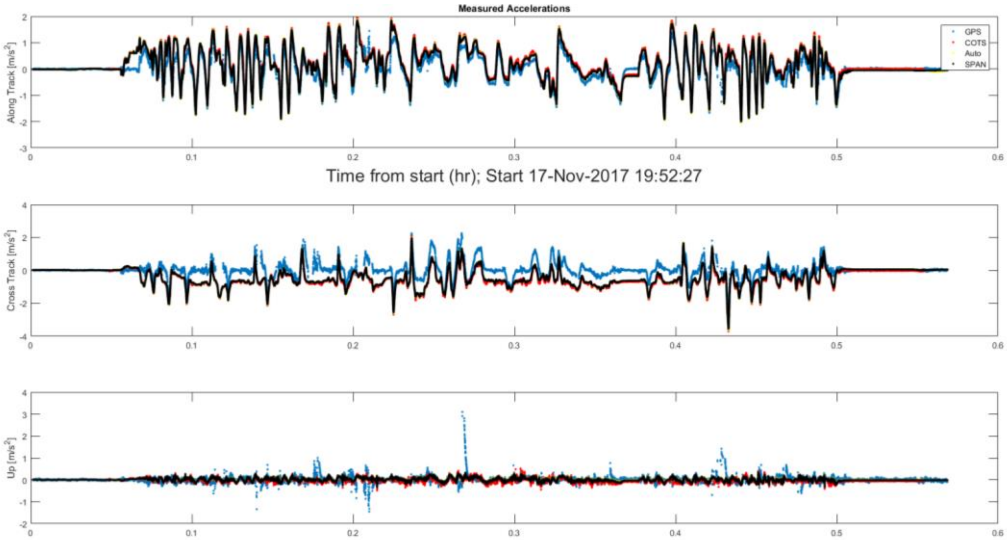


Figure 7. Comparison of GNSS and accelerometer (COTS, Auto, SPAN) measured accelerations on all three axes for November 17, 2017 test drive, accelerometer bias removed

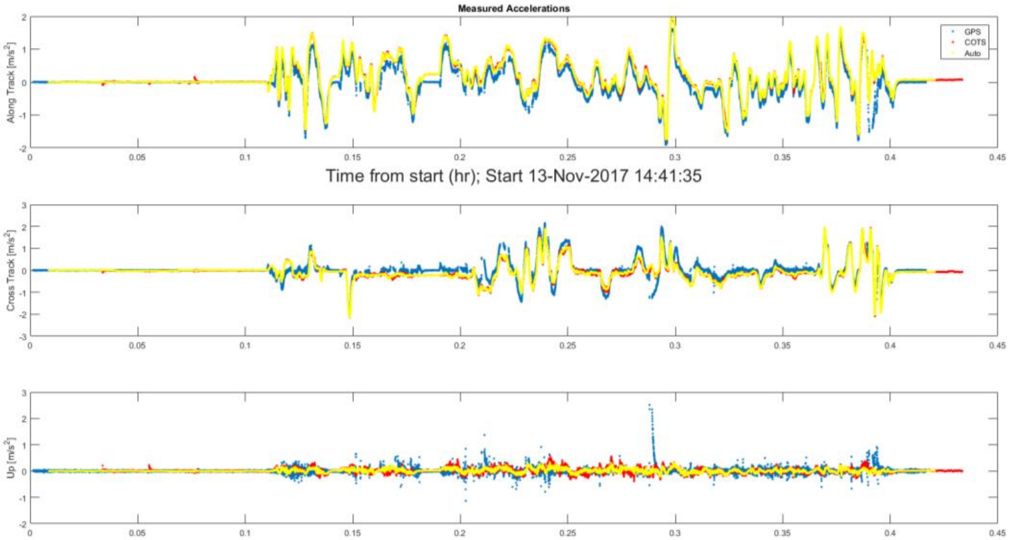


Figure 8. Comparison of GNSS and accelerometer (COTS, Auto) measured accelerations on all three axes for November 13, 2017 test drive, accelerometer bias removed. SPAN accelerometer data not saved

IV: Spoof Detection Using Statistical Tests

While we can observe differences in measured accelerations between GNSS and accelerometer, we need to have clear tests that can detect abnormal behavior with confidence and a low probability of false alert. Individual monitors based on statistical tests are thus developed to examine specific measurement properties that should be consistent between genuine GNSS and accelerometer accelerations. Statistical tests are used because they are straight-forward and their performance can be easily assessed. As spoofed acceleration may result in different inconsistencies, multiple different monitors can be developed. The executive monitor (EM) then synthesizes the results of the individual monitors to provide an indication of spoofing. This design architecture is shown in Figure 9. The design and implementation of the EM is not within the scope of this work. The next two subsections cover the individual monitors and statistical tests in detail.

The architecture shown in Figure 9 is useful for the overall spoof detection as it can help achieve good detection with a very low false alert rate. As detection can result in alerting the user and disrupting service, false alerts are harmful as they make the system unavailable when it otherwise would be. Furthermore, false alerts can lead to distrust of the system, potentially leading users to ignore alerts. Hence, minimizing false alerts is important. It is our belief that a detection system is only useful and not considered a liability if it has very few false alerts (nearly zero) over the course of its life. Since there is generally no spoofing, this means an extremely very low false alert rate. Accomplishing this is not necessarily easy as it can be difficult to distinguish spoofing signatures from natural occurrences. Multipath, scintillation, and other phenomena can be mistaken for spoofing. With proper design and EM, many different independent spoof tests can help minimize false alerts.

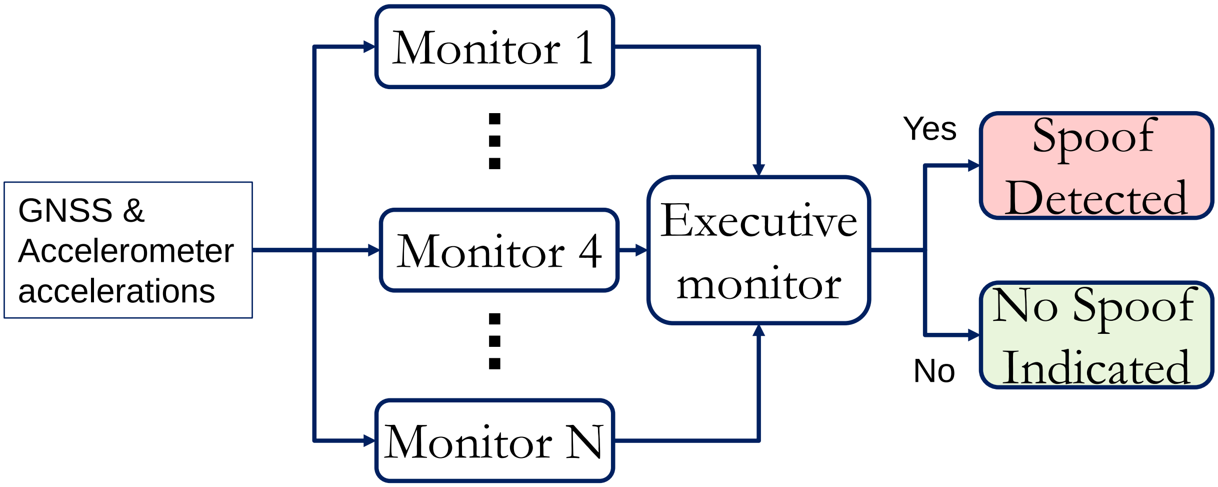


Figure 9. General Spoof Detection Architecture with Executive Monitoring indicating spoofing based on information from various monitors

Test Monitors

Several monitors may be developed for GNSS spoof monitoring as there are multiple possible comparisons of acceleration measurements. The first one examined is difference in acceleration as this is relatively straight-forward. Other characteristics of the acceleration profile can also be used. For example, the rate of acceleration (so-called jerk) changes should be similar. The variation of the acceleration over a time window should also be similar. Additionally, these comparisons can be examined for each axes (along-track, cross-track or vertical). All these should match within error tolerances.

For the initial analysis, the mean and standard deviation of acceleration differences are used for monitor tests. Test statistics, discussed in the next part, are generated for these measurements. The mean acceleration difference (Δa) examines how closely the acceleration from each sensor (GNSS, accelerometer) matches. As a result, accelerometer biases need to be calibrated out as much as possible otherwise they have to be accounted for in the test statistic. Having to accommodate biases weakens the detection capability of the test. The standard deviation of acceleration difference $(\sigma_{\Delta a})$ is calculated over a specified number of samples or time windows. It examines the relative trend between the acceleration measurements. It is less sensitive to a relatively constant bias, such as those resulting from axis misalignment. $\sigma_{\Delta a}$ should be larger than the nominal value when the accelerations between the two sensors are not well matched (i.e. GNSS is spoofed.) As shown later in Figure 6, the trend may be similar but there can be a changing scale or bias error.

Statistical Tests

Standard hypothesis tests are used to develop monitors for the mean and standard deviation of acceleration differences. We are essentially testing between the null hypothesis (H0), “there is no spoofing,” against the alternative hypothesis (H1), ”there is spoofing.” Table 3 shows what this means for each comparison measure. For the acceleration difference (Δa), H0 is that the Δa is zero, within our statistical variation. For the standard deviation test, we examine whether the sample variance, s^2, is consistent with the model variance, $(\sigma_{\Delta a})^2$.

Table 3. Null and Alternative Hypothesis for Each Spoof Monitor Test Statistic

Test	H0 (Null) Hypothesis	H1 (Alt.) Hypothesis
Generally	No GNSS Spoofing	There is GNSS Spoofing
Accel Diff $(\boldsymbol{\Delta a})$	Mean $(\Delta a) = 0$	Mean $(\Delta a) \neq 0$
Std Accel Diff $(\boldsymbol{\sigma_{\Delta a}})$	Sample variance s^2 consistent with $(\sigma_{\Delta a})^2$	s^2 not consistent with $(\sigma_{\Delta a})^2$

The first test statistic, z (mean difference), is shown in Equation 3. It examines the absolute value of mean difference of acceleration $(\bar{y})$ normalized by the model standard deviation, σ. It also accounts for the effect of the maximum nominal bias b. The max function used as the statistic should not be below zero. The statistic should be bounded by a standard normal distribution provided the model standard deviation and bias are representative. Hence, our threshold test is to flag if $z > z_{thres}$. For a 10^{-9} probability of false alert, z_{thres} is 6.11. The second test statistic, χ^2, is shown in Equation 4 with n being the number of samples examined, and s^2 and σ^2 being the sample and model variances, respectively. For the initial analysis, $n = 12$ samples are used to generate the sample variance. The statistic is (central) χ^2 distributed with $(n-1)$ degrees of freedom (dof). Similarly, our threshold test is to flag when $\chi^2 > \chi^2_{thres}$ with χ^2_{thres} being 65.17 for 10^{-9} and dof equal to 11 (since $n = 12$). These thresholds are shown in Table 4. Both statistical tests depend on the model standard deviation, σ, of the acceleration difference. As such, incorrect modeling affects the monitor performance. If σ is too large, then there will be a larger missed detection rate than modeled. Given the steady state nature of the developed spoof detector, this may be acceptable as there are many chances to catch the spoofer. If σ is too small, the false alert rate will be higher than expected. This is the worst outcome as it may lead the user to distrust the system. Because of this, it is better to err on the side of slightly too large. This is shown in Equation 4.

$$z = \frac{max(|\bar{y}| - b, 0)}{\sigma} \qquad 3$$

$$\chi^2 = \frac{(n-1)s^2}{\sigma^2} \qquad 4$$

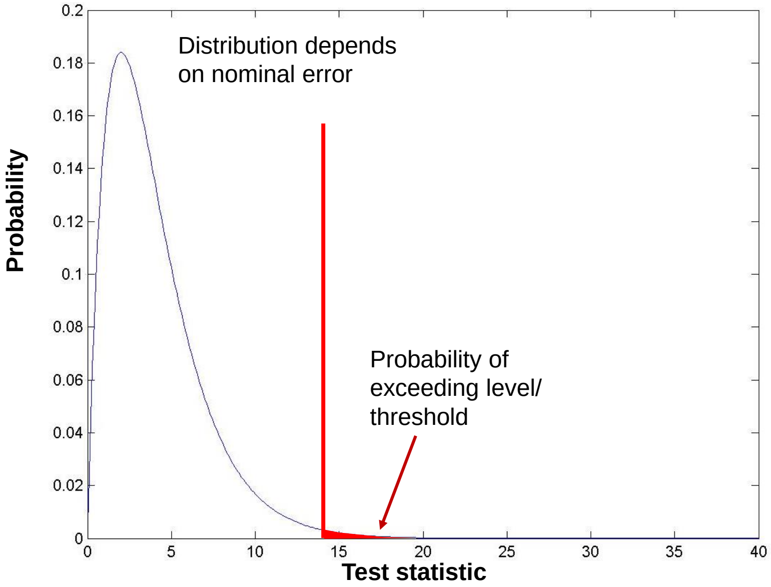


Figure 10. Detection threshold for Test Statistic determined using targeted probability of false alert

Table 4. Test Statistic, Threholds and Rationale

Test	Statistic	Threshold	Rationale
Accel Diff ($\boldsymbol{\Delta a}$)	z (Equation 3)	6.11	z level which has at most a 10^{-9} probability of exceeding
Std Accel Diff ($\boldsymbol{\sigma_{\Delta a}}$)	χ^2 (Equation 4)	65.17	χ^2 level which has only a 10^{-9} probability of exceeding (assuming 11 degrees of freedom)

Acceleration Differences

Calculating acceleration differences requires aligning the measurements and creating matching samples. Typically, the measurements are not taken at the same time. Hence to create the acceleration difference, the inertial accelerations are interpolated to the times of available GNSS samples. This is done after exponential smoothing as shown in Figure 11. The acceleration difference is then calculated on a sample by sample basis. The bias estimate on each accelerometer can be removed with the bias being assumed fixed for the entire drive. This is an assumption and other processing such as zero velocity updates (ZUPT) during stops can be used to update the bias estimate. For the processing shown, the initial bias is calculated prior to the vehicle moving and applied to the acceleration measurements from each axes. No other bias compensation (i.e. ZUPT) is used.

Figure 11 and Figure 12 show the acceleration difference for each axes for two different drives. We examine these differences to determine the most favorable measurements and to develop monitor tests to detect spoofing. Given our test drive data, we can generally use all three axes. However, in the executive monitor, we may want to weigh their results differently due to their different signature (signal) level relative to noise.

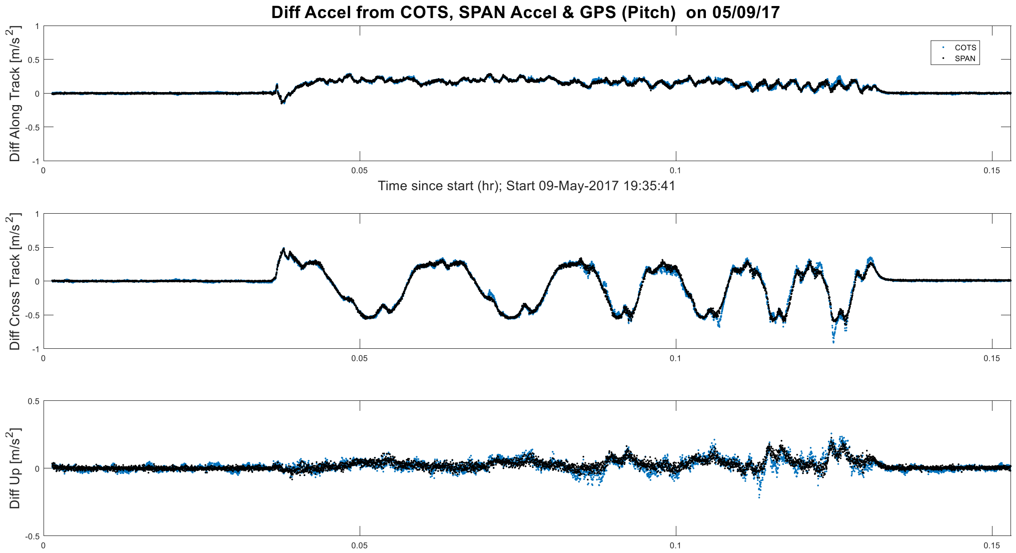


Figure 11. Difference between GNSS and accelerometer (COTS, Auto) measured accelerations on all three axes for May 9, 2017 test drive, accelerometer bias removed (Roof top)

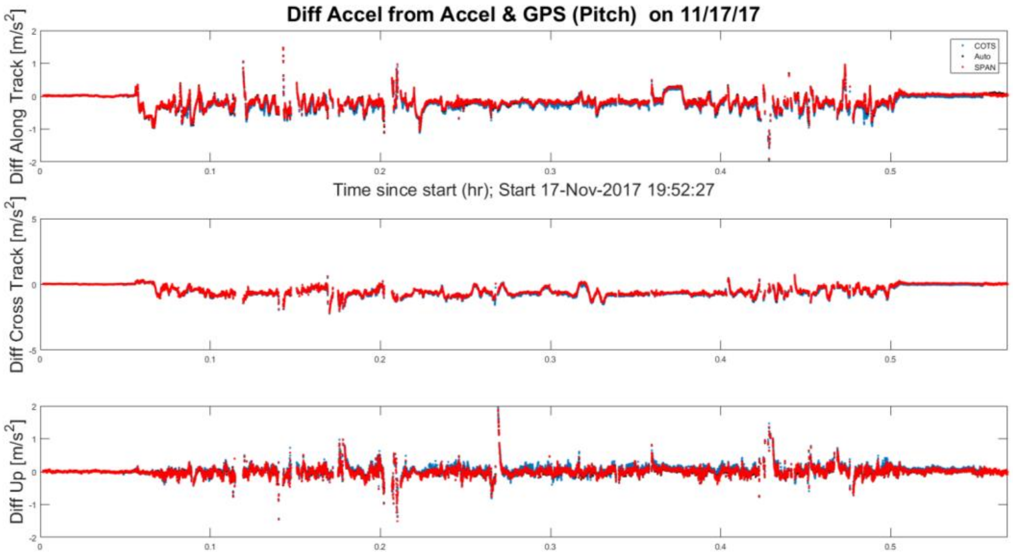


Figure 12. Difference between GNSS and accelerometer (COTS, Auto) measured accelerations on all three axes for November 17, 2017 test drive, accelerometer bias removed (urban, suburban, highway)

Another important difference to note is that automotive applications require a greater allowance for error than aviation. Multipath is much more significant in cars than aircraft and can cause significant error. Indeed, this multipath effect can be seen when comparing Figure 11 and Figure 12. The garage roof top environment for the May 9 test is much more benign in terms of multipath and signal blockages. This is seen in the lower amounts of GNSS drop outs and lower noise levels for acceleration difference. While the nominal (static) sensor noise is similar between aircraft and automobiles, the actual errors experienced should be larger in automobiles and allowances need to be made in the spoof detection algorithms.

Monitor Test Results

The individual monitors compress the acceleration profiles of each sensor into simple spoof indicators or flags. The probabilities of alert and missed detection are tested using nominal (no spoofing) and spoofed conditions. Testing the nominal case is straightforward and is done with the collected data without modification. To test the spoof detection, we do not need to simulate the spoofing signal. We only need to model the effect of the spoofer on the statistical tests – that is, the acceleration resulting from the spoofing signal. Multiple different scenarios can be tested as the spoofer's level of information and processing are not known. For example, our developed MATLAB analysis routine can test different delays as well as acceleration estimation strategies such as repeat back (with delay), extrapolate, extrapolate and smooth and zero acceleration. The last represents a best guess when the attacker has no knowledge of the actual acceleration.

For the results shown, acceleration repeat back spoofer is used. With the acceleration repeat back spoofing, it is assumed that the spoofer generates a GNSS acceleration profile that matches the GNSS output. The only difference is that the spoofer results are delayed as its information is delayed. Other spoofing can be tested such as extrapolated acceleration where the spoofer tries to extrapolate its acceleration information to the present time to account for the delay. This tends to be noisy and smoothing can be employed – hence the extrapolate and smooth strategy. However, our previous analysis has shown the acceleration repeat back to be generally the most effective strategy for the spoofer.

Monitor Performance under Nominal Conditions

Nominal conditions are tested with the collected data. Test statistics are determined using Equation 3 and 4 with 12 samples (~ 1.2 seconds) of data. The threshold is based on model standard deviation and model worst case biases. For the analysis, Table 5 shows these values based on static measurements. It shows the actual bias used to zero mean the static accelerometer data. Table 6 shows the thresholds used and how they are calculated. For the z threshold, the distribution is two sided and so have the probability of false alert is allocated to each side – hence $0.5 * P_{fa}$. The χ^2 distribution is one sided. Figure 13 and Figure 14 show the acceleration difference and standard deviation of acceleration difference test statistic for nominal conditions. Note that the threshold is sometimes exceeded. This should be a rare event but is not. There are several causes. One is GNSS data drop outs which corrupts the calculated GNSS acceleration and its moving average. Another is unmodeled attitude or axes alignment errors. This can add a component of gravity into the accelerometer measurement of the cross track or along track axes. Another is increased measurement noise due to multipath and non-line of sight (NLOS) signals. Another is that GNSS and the accelerometers are not co-located resulting in slightly different measurements. This may increase the difference variations, resulting in larger standard deviation of acceleration difference test statistic. These can all be mitigated. For the first, we eliminate periods around GNSS drop outs. The others are not currently mitigated but we are examining their effects. For example, we will conduct a drive test with co-located GNSS and accelerometer to examine the difference.

Table 5. Model bound statistics for acceleration differences (IMU-GNSS) for all three axes

Equipment	**Bias for 11/17 (m/s^2)**			**Std for 11/17 (m/s^2)**			**Model Bias (m/s^2)**			**Model Std (m/s^2)**		
COTS IMU-GNSS	0.19372	-1.04918	10.25246	0.005	0.004	0.012	0.25	0.25	0.3	0.06	0.06	0.08
Auto IMU-GNSS	0.40589	-1.02410	9.96192	0.005	0.013	0.011	0.25	0.25	0.3	0.06	0.06	0.08

SPAN IMU-GNSS	0.38155 -1.15647 9.75695	0.005 0.013 0.010	0.25 0.25 0.3	0.06 0.06 0.08

Table 6. Test Statistic, Threholds and Calculation where P_{fa} is the probability of false alert

Test	Statistic	Threshold	Calculation (MATLAB)
Accel Diff (Δa)	z (Equation 3)	6.11	*Norminv(* 1-0.5* P_{fa},0,1)
Std Accel Diff ($\sigma_{\Delta a}$)	χ^2 (Equation 4)	65.17	*Chi2inv(1*- P_{fa}, dof) where dof =(number of samples - 1

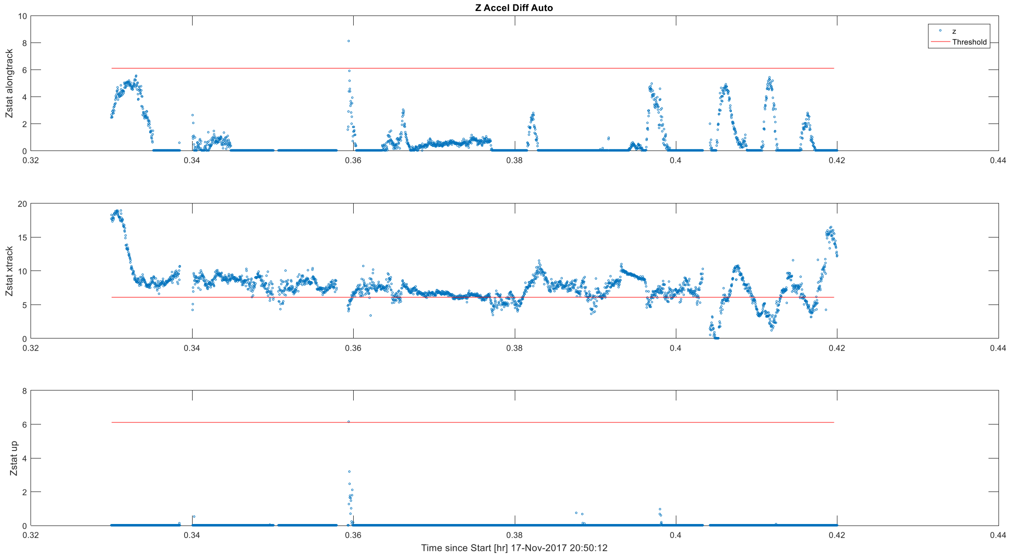


Figure 13. Acceleration difference test statistic (z) vs. Threshold for 3 principal axes, no spoofing November 17, 2017

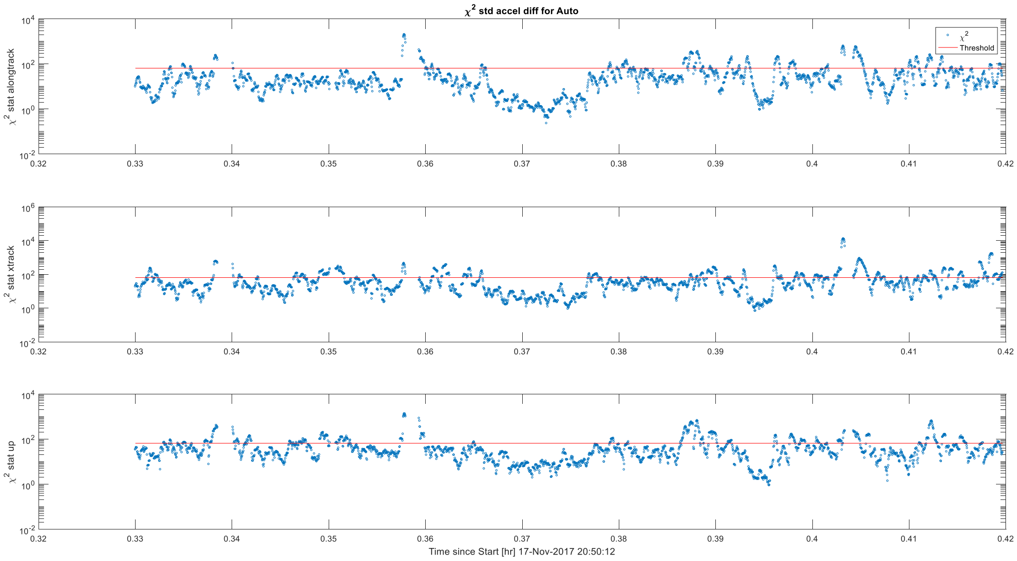


Figure 14. Standard deviation of acceleration difference test statistic (χ^2) vs. Threshold for 3 principal axes, no spoofing November 17, 2017

Monitor Performance under Spoofing Conditions

The ability to defeat the monitor is determined by the acceleration that the spoofer can predict. An unsophisticated spoofer has no knowledge of acceleration and hence its best guess is to assume zero acceleration in most directions, including along track. A sophisticated, worst-case spoofer would accurately know the true acceleration (GNSS or accelerometer, for this analysis, we assume GNSS) with a small delay and could generate a spoofed GNSS exhibiting any acceleration profile. While the spoofer can produce many different acceleration profiles with delayed knowledge of the true acceleration to fool the monitors, repeating back the true acceleration was found to be a good strategy [3]. This is an extreme scenario as the spoofer only cares to spoof the acceleration profile without regard to the actual spoofed position. An actual attack would be constrained by the need to generate the desired spoofed positions at the targeted times.

Figure 15 and Figure 16 show the acceleration difference and standard deviation of acceleration difference test statistic for a replay spoofer with a two second delay. The same thresholds are used as before. Compared with the nominal scenario, the test statistics are exceeded more often as will be shown next.

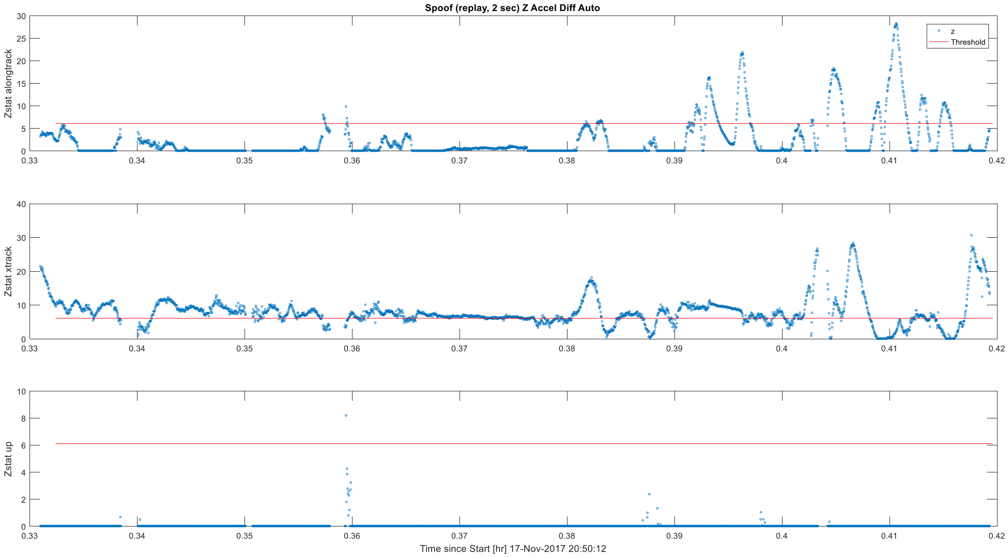


Figure 15. Acceleration difference test statistic (z) vs. Threshold for 3 principal axes, repeat back spoofing with 2 sec delay, November 17, 2017

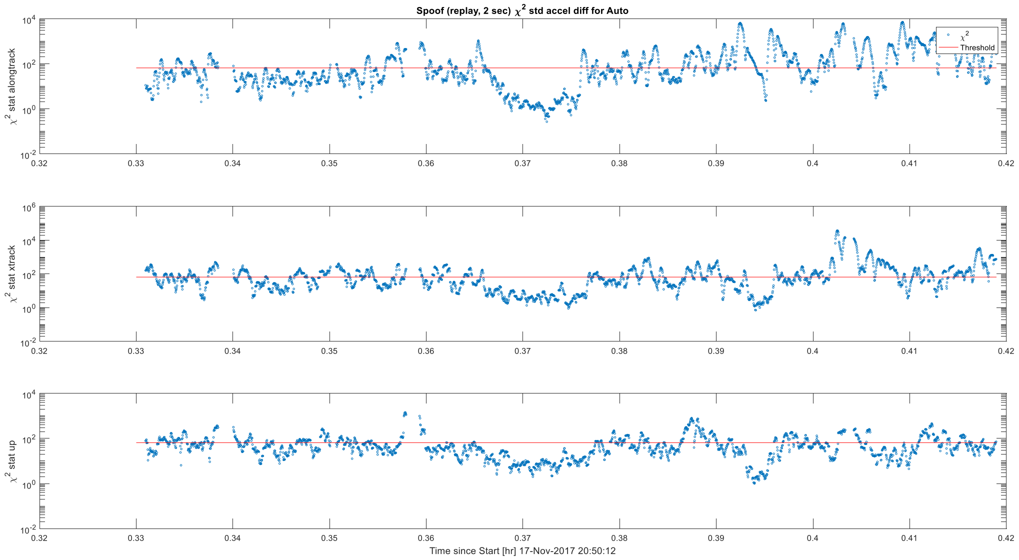


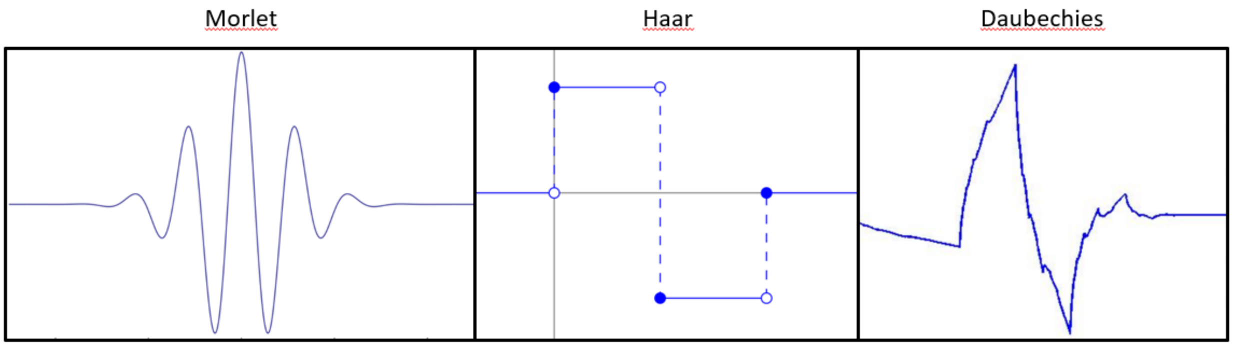
Figure 16. Standard deviation of acceleration difference test statistic (χ^2) vs. Threshold for 3 principal axes, repeat back spoofing with 2 sec delay, November 17, 2017

V: Spoof Detection Using Wavelets

The detection criteria discussed so far has been centered around the numerical values of the measurements made by the accelerometer and GNSS receiver in the time domain. The goal is to use these values to infer a larger pattern in behavior that the accelerometer and GNSS receiver output would agree upon in most cases with non-spoofed GNSS measurements. We have begun to explore the use of another method that focuses on this pattern by looking at the measurements in the frequency domain as well as the time domain. We accomplish this by using wavelets to approximate the waveform created by the data provided from the accelerometer and receiver and compare the waveforms that are generated.

Wavelets were first developed by Haar in the early 1900's and in the late 20th century, their application to denoising and classification problems in areas from economics to voice recognition precipitated their rise to prominence. The time-series measured by both the accelerometer and receiver are non-stationary phenomenon, meaning they do not repeat themselves over time. The advantage of using wavelets to analyze time-series is their ability to estimate the spectral characteristics as a function of time [8]. While the Fourier transform can be used to study the cyclical nature of a time-series, the time information is lost. A windowed Fourier transform (WFT) is an attempt at recovering some of that time dependent information, but complications can arise in the selection of optimal window length making the WFT hard to implement for general problems [9]. In addition to this, the Fourier transform is confined to a basis defined by sines and cosines, whereas there are theoretically an infinite set of basis available for wavelet analysis.

A wavelet is a function that is zero mean and is localized in both the time and frequency space [10]. Figure 17 gives three examples of wavelets: Morlet, Haar, and Daubechies. Similar to elementary phenomena in physics, the ability for a wavelet to discern both time and frequency information for a given time-series is limited by the Heisenberg uncertainty principle. This is to say that for better resolution in the frequency domain, the resolution of the time domain will suffer. Different wavelets have strengths and weaknesses with respect to discerning information in the time and frequency domains.


Morlet

Haar

Daubechies

Figure 17: Morlet, Haar, and Daubechies wavelets

If a wavelet (known as the "mother wavelet") is given by a function, ψ, then a family of wavelets (known as "daughter wavelets") can be derived by scaling and translating the mother wavelet using Equation 5, where s is a scaling parameter, and τ is a translation parameter. The continuous wavelet transform (CWT) is the corollary to the continuous Fourier transform, in that it projects the time series onto the space defined by the family of wavelets. The equation for the CWT is given in Equation 6, where the coefficients are given as $W_{x;\psi}(\tau, s)$, $\langle \quad \rangle$ represents the inner product, and $x(t)$ represents the time-series of interest.

$$\psi_{\tau,s}(t) \coloneqq \frac{1}{\sqrt{|s|}}\psi\left(\frac{t-\tau}{s}\right) \qquad 5$$

$$\mathrm{W}_{x;\psi}(\tau, s) = \langle x, \psi_{\tau,s} \rangle = \int_{-\infty}^{\infty} x(t)\frac{1}{\sqrt{|s|}}\psi^{*}\left(\frac{t-\tau}{s}\right)dt \qquad 6$$

For two separate measurements of stationary phenomena, when the extent of correlation wants to be measured between the two, the spectral coherence is calculated, taking the cross-spectral density between the two waveforms and normalizing them by their auto-spectral densities. Similarly, wavelet coherence is defined in much the same way, as seen in Equation 7, where W_{xy} is the cross-wavelet transform and $|W_x|^2$ is the wavelet power spectrum. The smoothing operator, $\mathcal{S}(\quad)$, is necessary in order to prevent the coherency from being identically one at all times and scales. The value of $R_{xy}(\tau, s)$ is normalized and is always between 0 and 1.

$$R_{xy} = \frac{|\mathcal{S}(W_{xy})|}{\sqrt{\left[\mathcal{S}(|W_x|^2)\mathcal{S}\left(|W_y|^2\right)\right]}} \qquad 7$$

Another useful characteristic of wavelet coherency is that the angle, or phase-difference, between the two waveforms can be calculated using Equation 8.

$$\phi_{xy} = \mathrm{Arctan}\left(\frac{\Im\left(\mathcal{S}(W_{xy})\right)}{\Re\left(\mathcal{S}(W_{xy})\right)}\right) \qquad 8$$

Comparing frequency phenomena in the wavelet domain has several distinct advantages when compared to comparing strictly in the time-domain. Wavelet coherence is bias and scale independent. A series of autoregressive time-series, shown in Figure 18, are compared to demonstrate this key characteristic. The first pair of time-series are identical except for a bias offset, and the second pair of time-series have a scale and bias offset. Their coherency for all scales and time-shifts are identically one as shown by Figure 19. The arrows in the figure represent the phase difference between the time series at different scales and times. This is a crucial feature in the comparison between accelerometer and receiver measurements as accelerometers contain biases and scale factors that would otherwise need to be calibrated and compensated for in time series comparisons. Another constant bias that exists between accelerometer and GNSS velocity derived measurements is the force of gravity, shown in Equation 1.

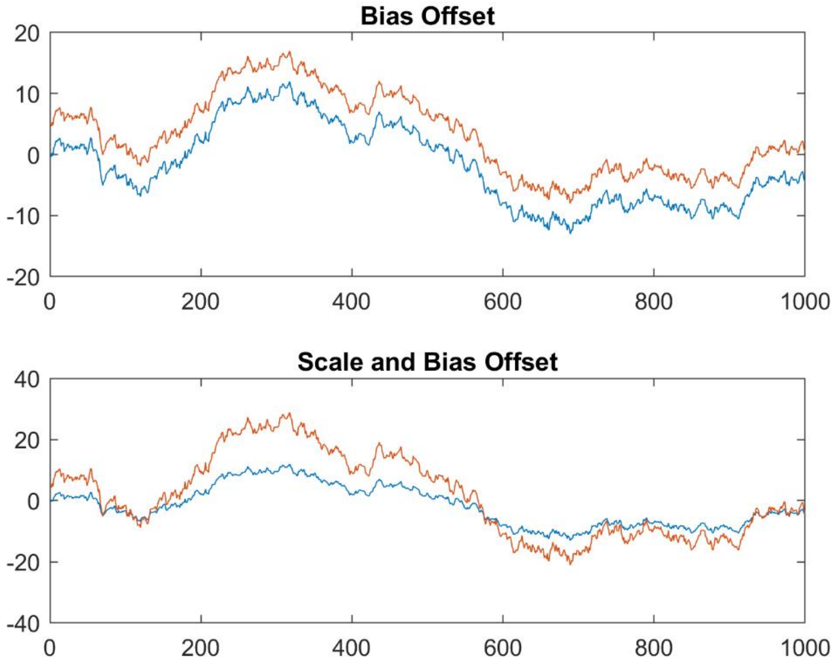


Figure 18: Autoregressive time-series that have identical coherence with zero phase-difference

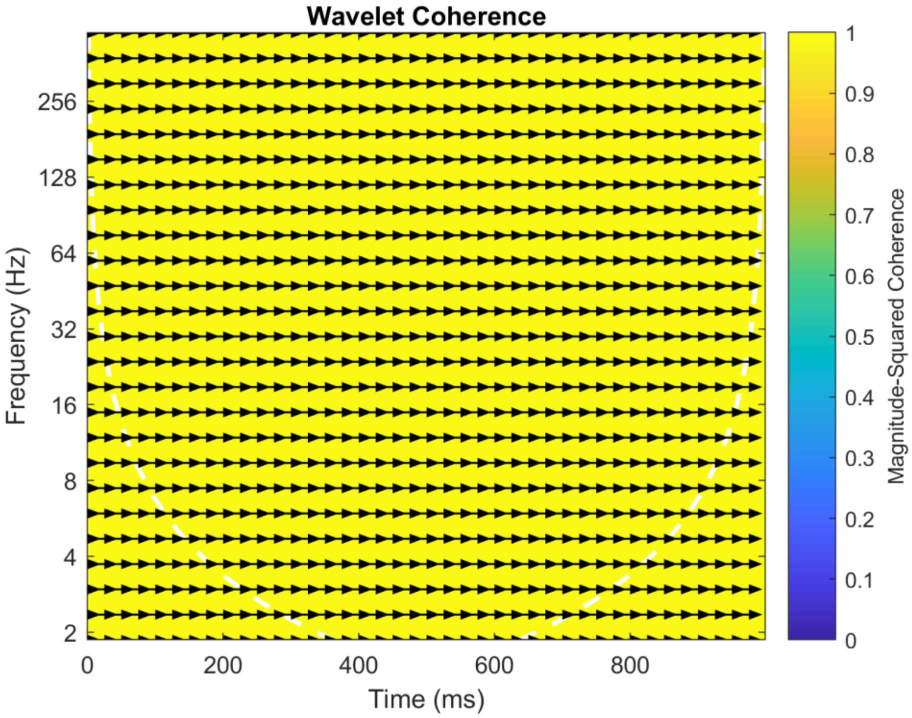


Figure 19: Wavelet coherence between the autoregressive time-series shown in Figure 18

Using the analytic Morse wavelet, the wavelet coherence of the data taken May 9, 2017 was calculated using the horizontal 2D RMS of the accelerometer and GPS outputs, shown in Figure 21. The time series of the data is shown in Figure 6 and the 2D RMS of both the accelerometer and receiver measurements is shown in Figure 20. For reference, the coherence of the 2D RMS accelerometer outputs and spoofed GPS data with a different acceleration profile is shown in Figure 22 and the coherence of spoofed data with 2-second delay is shown in Figure 23.

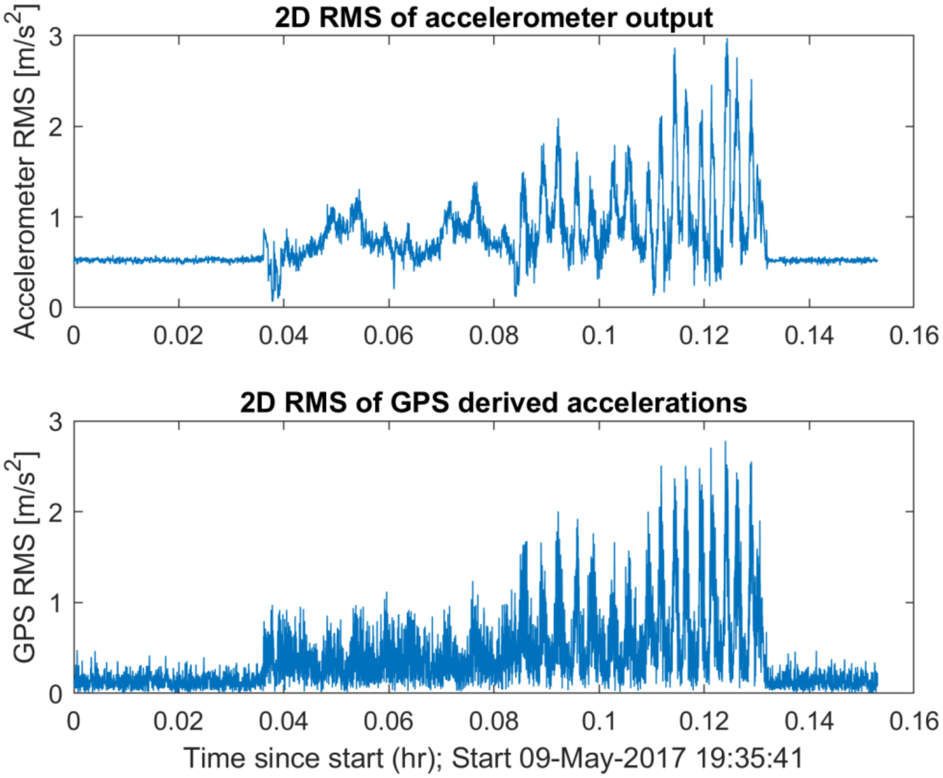


Figure 20: Horizontal 2D RMS of GPS and Accelerometer accelerations

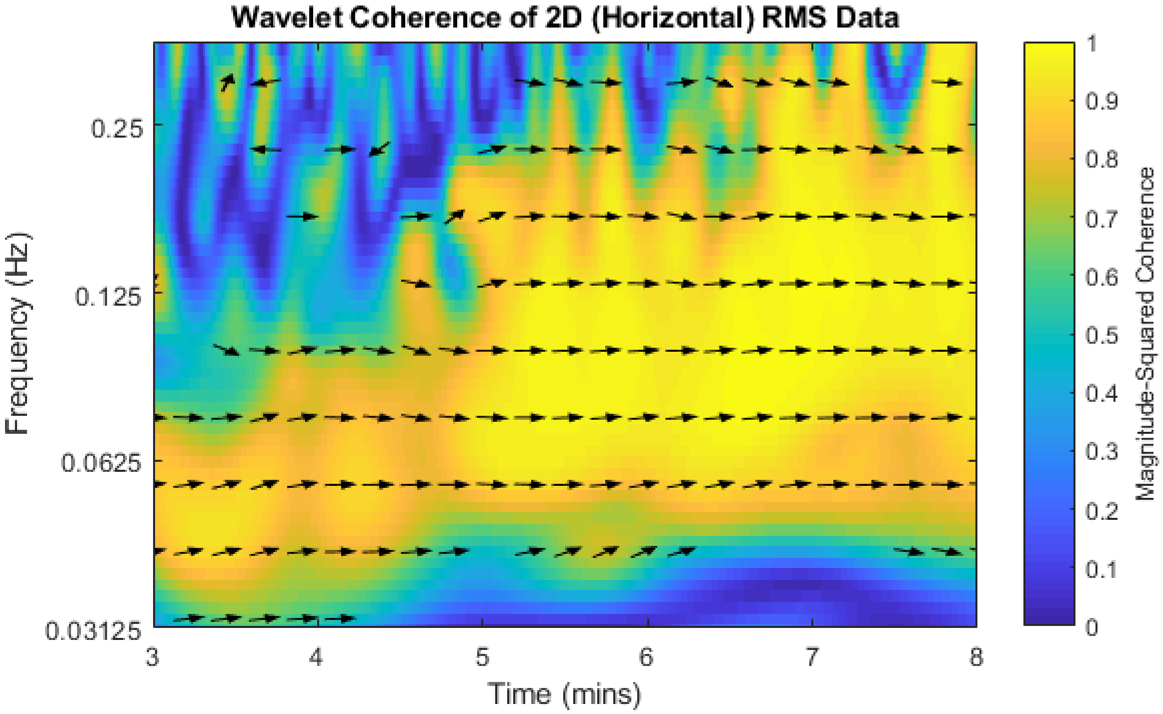


Figure 21: Wavelet Coherence of 2D (Horizontal) RMS Data

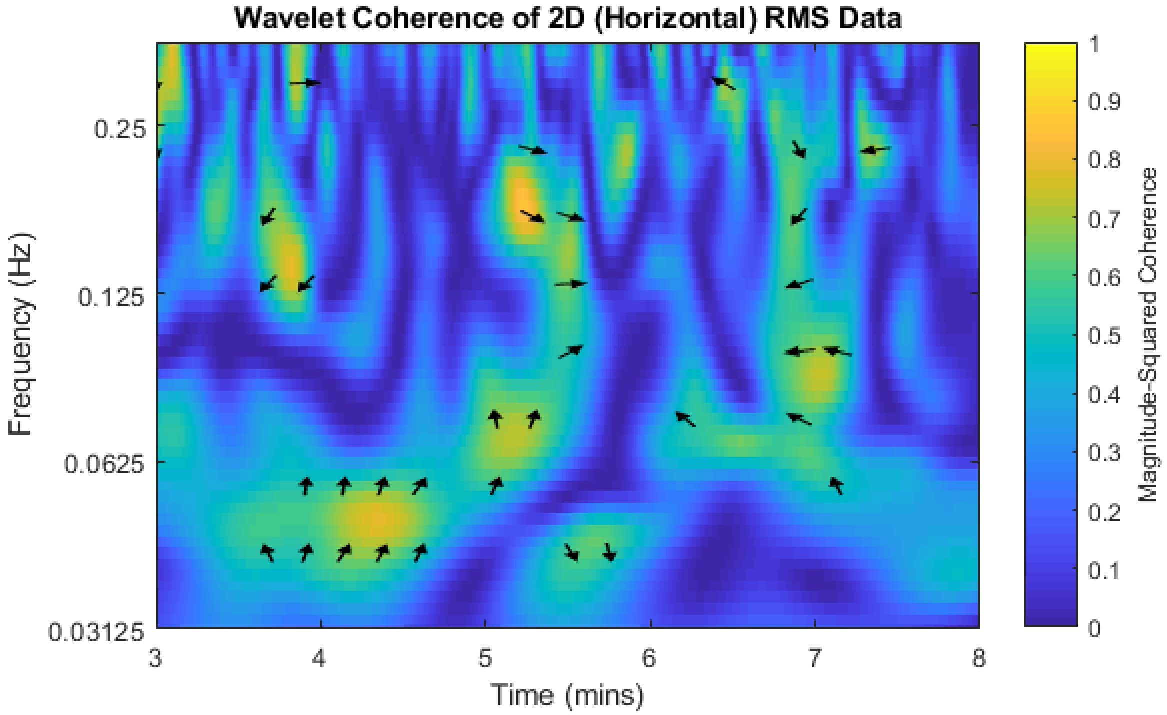


Figure 22: Wavelet Coherence of 2D (Horizontal) RMS Spoofed Data with different acceleration profile

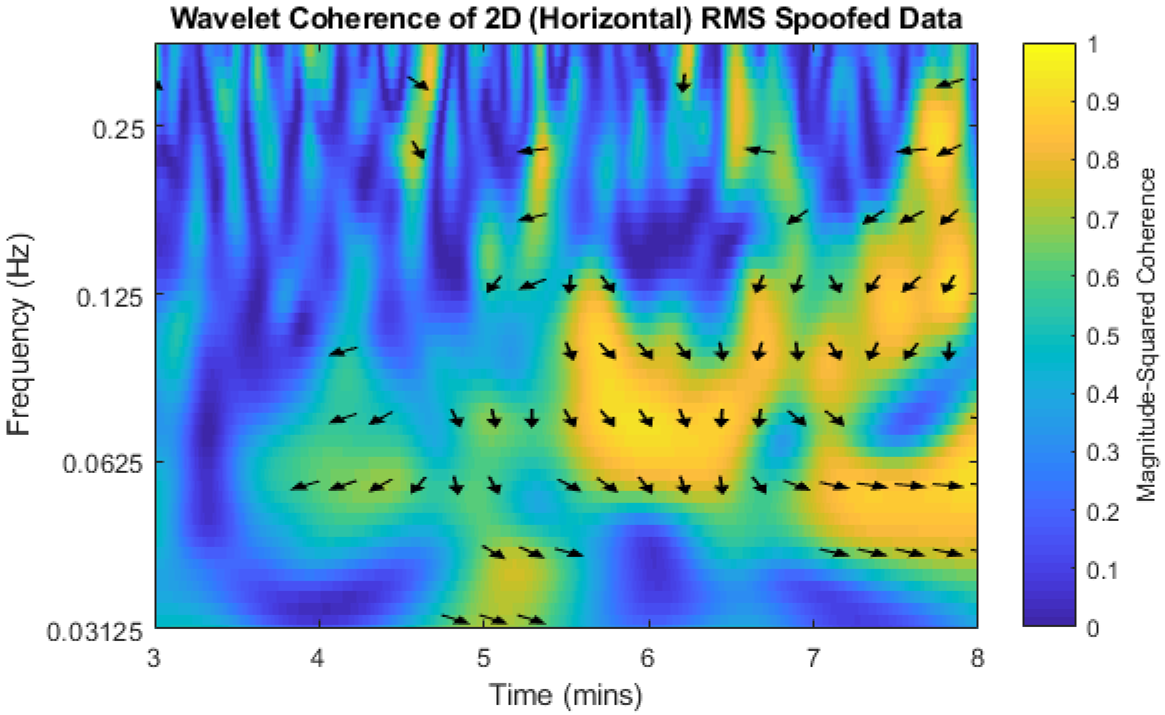


Figure 23: Wavelet Coherence of 2D (Horizontal) RMS Spoofed Data with 2-second delay

In the nominal case without spoofing, within the 0.06Hz range after 3 minutes there is a clear coherence between the accelerometer and GPS data. This begins around the 3-minute mark when the car begins to drive, before which the car is not moving. From preliminary findings, this method shows promising results when the vehicle is in motion. In addition to this, for the spoofed cases, the coherence is far less in the similar frequency range, and the phase offset is significant for the 2-second delay spoofed case. Moreover, this coherence was calculated using the RMS values of the horizontal axes of acceleration without the need to rotate these axes to correct for heading. Further analysis will include a closer look at expected coherence values for specific vehicle applications and the level of confidence in results that can exist in practice from using this technique.

VI: Conclusions and Future Work

Statistical methods that were used in previous research to detect spoofing in aircraft dynamics signatures are more difficult to implement in the case of cars. The results using the statistical tests showed many cases of false alerts and so it is apparent that the model used in deriving the statistical tests must be updated. This model may be made more accurate by incorporating mitigations for effects thought to throw off the current statistical tests. GNSS dropouts must be acknowledged and accounted for as these can sometimes give erroneous acceleration measurements in the receiver. Streets tend to have cross slope for drainage systems. This cross slope means that cars tend to see some of the gravity vector in the cross-track axis of the accelerometer. In this way, better modeling of this effect will be required to properly account for axis-alignment errors between the receiver and accelerometer accelerations. Multipath and non-line of sight signals can contribute to erroneous GNSS acceleration measurements as well as the fact that the GNSS antenna and accelerometer are not co-located.

Wavelets have shown some potential for use in spoof detection. For cars, only the 2D (Horizontal) information between the IMU and receiver were compared as the local vertical axis does not provide much more useful information. For the case of aircraft, this third axis will be added and wavelets will be used to detect the agreement of frequency information of 3D RMS data. Although it may be apparent from observation of the coherence that there exists a method of detecting a spoofing attack, a proper, statistically significant technique of using wavelet coherence and phase to detect cases of spoofing will need to be developed. An executive monitor, similar to the design shown in Figure 9 will then need to be implemented in a way that takes into account the information given by the wavelet coherence monitor.

References

[1] E. G. Manfredini, P. Torino, D. M. Akos, and Y. Chen, "Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers," in *Proceedings of the Institute of Navigation International Technical Meeting*, 2018.

[2] L. Scott, "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems," *Proc. 16th Int. Tech. Meet. Satell. Div. Inst. Navig. (ION GPS/GNSS 2003)*, pp. 1543–1552, 2003.

[3] S. Lo and H. C. Yu, "The Benefit of Low Cost Accelerometers for GNSS Anti-Spoofing," in *Proceedings of the ION 2017 Pacific PNT Meeting*, 2017.

[4] S. Manickam and K. O. Keefe, "Using Tactical and MEMS Grade INS to Protect Against GNSS Spoofing in Automotive Applications," *ION GNSS+ 2016 Conf. Sess. E5*, pp. 1–11, 2016.

[5] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "Kalman Filter-based INS Monitor to Detect GNSS Spoofers Capable of Tracking Aircraft Position," in *Position, Location and Navigation Symposium (PLANS) IEEE/ION*, 2016, pp. 1027–1034.

[6] C. Tanil, P. Martinez Jimenez, M. Raveloharison, B. Kujur, S. Khanafseh, and B. Pervan, “Experimental Validation of INS Monitor against GNSS Spoofing,” in *ION GNSS+ 2018*, 2018.

[7] C. Tanil, S. Khanafseh, and B. Pervan, “An INS monitor against GNSS spoofing attacks during GBAS and SBAS-assisted aircraft landing approaches,” *29th Int. Tech. Meet. Satell. Div. Inst. Navig. ION GNSS 2016*, vol. 4, no. September, pp. 2981–2990, 2016.

[8] L. Aguiar-Conraria and M. J. Soares, “The Continuous Wavelet Transform: A Primer,” p. 40, 2010.

[9] C. Torrence and G. P. Compo, “A practical guide to wavelet analysis,” *Bull. Am. Meteor. Soc.*, vol. 79, no. 1, pp. 61–78, 1998.

[10] M. Farge, “Wavelet Transforms And Their Applications To Turbulence,” *Annu. Rev. Fluid Mech.*, vol. 24, no. 1, pp. 395–457, 1992.