Abstract
To protect civilian Global Positioning System (GPS) users from spoofing, the Air Force Research Lab has developed the chips-message robust authentication (Chimera) signal enhancement for the GPS L1C signal. With Chimera, stand-alone receivers that only have access to the GPS signal will be able to authenticate their received measurements once every 3 min, whereas users with access to an out-of-band source will be able to perform authentication once every 1.5 or 6 s. However, moving receivers typically rely on much faster real-time GPS update rates of 1–20 Hz. In this work, we design a spoofing-resilient filter framework that provides continuous and secure state estimation between Chimera authentication times. By leveraging self-contained sensors on-board the vehicle, such as an inertial measurement unit or wheel encoder, as well as the periodic Chimera authentication, our proposed filter determines how much to rely on the received unauthenticated GPS measurements for state estimation. In this respect, our filter relies more extensively on GPS measurements in order to improve real-time navigation performance and reduce localization errors when GPS signals are authentic, while successfully mitigating spoofing-induced errors during an experienced attack. We experimentally validate our proposed spoofing-resilient filter in a simulated test environment for a ground vehicle model with access to the 3-min Chimera channel, under various simulated spoofing attack scenarios. To the best of the authors’ knowledge, this is the first adaptive filter proposed for Chimera that continuously leverages real-time GPS measurements in a spoofing-resilient manner.

Keywords
adaptive filter, Chimera, GPS, inertial measurement unit, Kalman filter, M-estimation weight function, spoofing mitigation, wheel encoder

1 | INTRODUCTION

Modern society currently relies heavily on the Global Positioning System (GPS) for navigation and precise timing for a wide range of applications, including...
applications within the energy, communication, transportation, and emergency services sectors (Navstar GPS Joint Program Office, 2020). However, because the civilian GPS is currently insecure, with unencrypted, publicly available signal structures, all civilian signals are vulnerable to being spoofed, where an attacker mimics authentic GPS signals to induce a false position or timing solution. Spoofing has not only been demonstrated in academic settings (Psiaki & Humphreys, 2016b; Shepard et al., 2012), but has also been reported in numerous real-world scenarios. A 2019 report from the Center for Advanced Defense Studies documented nearly 10,000 separate GPS spoofing incidents in Russia and its occupied territories, affecting over 1000 civilian maritime vessels (C4ADS Think Tank, 2019). Additionally, in recent years, several GPS “circle spoofing” scenarios have been reported for ships in various parts of the world, including near China, Malaysia, Norway, and Nigeria (Goward, 2020). In a few incidents, ships reported locations that were thousands of miles from their true location and that followed circular trajectories at speeds of 20 knots (Goward, 2020). Furthermore, GPS spoofing is becoming an increasingly accessible form of attack. Past academic demonstrations of spoofing have been performed with $2000 worth of equipment (Psiaki & Humphreys, 2016b). Additionally, with the arrival of inexpensive software-defined radios, available for less than $300 (Getz, 2021; Ossmann, 2022), and open-source software capable of transmitting false GPS signals, spoofing has become inexpensive and significantly easier to perform.

To protect civilian GPS users against spoofing, the Air Force Research Lab (AFRL) has proposed the chips-message robust authentication (Chimera) signal enhancement for the GPS L1C signal (AFRL Space Vehicles Directorate, Advanced GPS Technology, 2019; Anderson et al., 2017). Chimera is the first proposed civilian authentication service for GPS and will be tested on the Navigation Technology Satellite-3 platform to be launched in 2023 (Inside GNSS, 2021). Based on the authentication technique first proposed by Logan Scott (Scott, 2003), the Chimera signal enhancement punctures the L1C spreading code in the pilot channel with encrypted markers. These encrypted markers cannot be predicted beforehand, but can be verified via a digital signature, or a set of marker keys, provided to the user with a short latency. Standalone receivers that only have access to the GPS L1C signal can use the slow watermark channel, which sends marker keys through the L1C data channel once every 3 min, whereas users with access to an out-of-band channel, such as a secure internet connection or an augmentation system, can use the fast watermark channel, which sends marker keys once every 1.5 or 6 s (AFRL Space Vehicles Directorate, Advanced GPS Technology, 2019; Cozzens, 2021). The time duration between consecutive Chimera authentications is referred to as the Chimera epoch (AFRL Space Vehicles Directorate, Advanced GPS Technology, 2019).

However, for both slow and fast watermark channels, the Chimera authentication service is not continuously available. As a result, users who await authentication before relying on GPS measurements will experience a corresponding measurement latency. Moving receivers, such as ground vehicles or unmanned aerial vehicles, typically rely on real-time GPS update rates, which are much faster than the authentication rate provided by Chimera. In particular, moving receivers often utilize GPS update rates of 1–20 Hz, standing in stark contrast with the 6-s fast channel and 3-min slow channel of Chimera. Prior work (Esswein & Psiaki, 2021) has analyzed the errors induced by Chimera authentication delays for a tightly coupled GPS/inertial measurement unit (IMU) filter. The authors observed root-mean-square (RMS) position errors of approximately 10 m for a navigation-grade IMU and over 300 m for a tactical-grade IMU with the Chimera
slow channel, greatly contrasting with RMS position errors of approximately 1.5 m for a GPS update rate of 20 Hz (Esswein & Psiaki, 2021).

Indeed, in designing a state estimation filter with the Chimera enhancement, we observe a trade-off between two key navigation objectives: (1) ensuring navigation security and (2) improving real-time navigation performance. In this work, we design a filter framework that provides a balance between these two objectives, by leveraging the Chimera signal enhancement and the redundancy from additional self-contained information sources to strategically weigh the received GPS measurements for state estimation during the Chimera epoch. In particular, we design our filter to mitigate the effects of GPS spoofing attacks, while enhancing navigation performance when unauthenticated measurements are determined to be trustworthy.

1.1 Related Prior Work

Significant prior research has focused on GPS spoofing detection, with a wide range of proposed techniques, including signal quality and power monitoring (Akos, 2012; Wesson et al., 2017), direction-of-arrival techniques (Bitner et al., 2015; Broumandan & Lachapelle, 2018; Lo et al., 2018), and the use of multiple receiver antennas (Bhamidipati et al., 2019; Bitner et al., 2015). Signal quality monitoring and power monitoring are valuable spoofing detection strategies for standalone receivers, but may have high false alarm rates (FARs) in the presence of multipath or sudden changes in signal power due to the environment. Furthermore, signal monitoring strategies often rely on successful detection at the onset of a spoofing attack (Psiaki & Humphreys, 2016a). As a result, if initial detection fails, these techniques may no longer be able to detect spoofing for the remaining attack duration. Additionally, direction-of-arrival techniques often require special equipment, such as directional antennas, antenna arrays, or multiple antennas.

Oftentimes, moving receivers utilize an additional self-contained sensor for navigation (Mohamed et al., 2019), such as an IMU, which can be readily leveraged for consistency-checking strategies without requiring additional equipment. Furthermore, self-contained sensors, unlike GPS, do not rely on external information sources and are, correspondingly, inherently secure from external jamming or spoofing attacks. In this respect, prior works have also investigated spoofing detection techniques that validate the consistency of the received GPS measurements with odometry measurements from one or more self-contained sensors, such as an IMU or wheel encoder (Broumandan & Lachapelle, 2018; Khanafseh et al., 2014; Tanıl et al., 2017). With the current, unencrypted GPS signal, one limitation of performing odometry-based consistency-checking for spoofing detection is that such sensors will eventually drift because of accumulated errors. As a result, a patient spoofer can circumvent detection by gradually ramping the GPS measurement errors until the total induced spoofing error is comparable to the expected drift errors. However, with a signal authentication scheme such as Chimera, a spoofer is limited to the time duration between Chimera authentications, thereby limiting the extent of error that can be induced without triggering detection, either through odometry-based consistency-checking techniques or because of authentication failure at the end of the Chimera epoch.

Prior work has also focused on designing a spoofing attack method against cryptographically signed GPS data such as Chimera, called secure code estimation and replay (SCER) attacks. In this sophisticated attack model, the spoofer conducts real-time estimation of the unpredictable security codes within the
cryptographically signed GPS signal, creates a counterfeit signal, and rebroadcasts the signal to the victim receiver (Humphreys, 2013). A corresponding detection strategy has also been designed to defend against SCER attacks (Humphreys, 2013). Although the SCER attack method is sophisticated, requiring the adversary to utilize high-gain receiving antennas to successfully carry out the attack (Scott, 2003), this detection strategy is of critical importance to defend against these attacks and to confirm that the Chimera authentication is in fact authentic. Our proposed work is complementary in that we focus on the simpler attack scenario, where the spoofer takes advantage of the window between Chimera authentications, before the user can validate the authenticity of the received GPS signal. Furthermore, our work seeks to go beyond detection to develop a framework for spoofing-resilient state estimation while leveraging Chimera.

Few prior works have performed GPS spoofing mitigation. Prior works include null steering, which seeks to suppress the undesired spoofing signal via spatial filtering techniques (Magiera & Katulski, 2015), as well as scanning of the signal space for an authentic GPS peak once an attack is detected (Jafarnia-Jahromi et al., 2012; Rothmaier et al., 2021). Null steering requires additional equipment such as an antenna array (Magiera & Katulski, 2015), and both spoofing mitigation strategies generally rely on responding to the spoofing attack only upon detection. However, the response time depends on the type of detection method used as well as the false alarm probability threshold chosen for detection, potentially allowing the spoofer to incorporate errors into the navigation solution before an official detection is declared.

1.2 Key Contributions

In this work, we propose a novel, adaptive GPS spoofing-resilient filter to provide continuous and secure state estimation between Chimera authentication times. To the best of the authors’ knowledge, this work provides the first adaptive filter proposed for Chimera that continuously leverages real-time unauthenticated GPS measurements in a spoofing-resilient manner. Furthermore, we experimentally validate our proposed filter framework in a simulated test environment for a ground vehicle model with access to the Chimera slow channel, under various degrees of simulated GPS spoofing attack scenarios. This work is based on our recent conference paper from the 2022 Institute of Navigation International Technical Meeting (Mina et al., 2022).

Our proposed Chimera spoofing-resilient filter framework:

1. leverages the periodic Chimera authentication, once available, as well as the self-contained sensors and vehicle dynamics model, to determine the trustworthiness of a received GPS signal,
2. utilizes a novel weighting scheme for unauthenticated GPS measurements, which extends M-estimation (Huber, 1964), in order to strategically balance between (1) improving real-time navigation performance when a GPS signal is authentic and (2) maintaining resilience against spoofing-induced errors during an experienced attack, and
3. demonstrates better spoofing mitigation performance (i.e., reduced localization errors) than a series of alternative adaptive filters during various degrees of simulated spoofing attacks, while maintaining navigation performance comparable to that of a conventional filter incorporating GPS measurements at a rate of 10 Hz, when the GPS signal is authentic.
1.3 Paper Organization

In Section 2, we provide an overview of the extended Kalman filter (EKF) and M-estimation, which are both used in our proposed method. In Section 3, we outline the details of our proposed spoofing-resilient filter. We describe the tightly coupled filtering framework in Section 4 for a ground vehicle model with access to GPS, IMU, and wheel encoder measurements. Finally, we present our experimental results in Section 5 and provide concluding remarks in Section 6.

2 PRELIMINARIES

2.1 Extended Kalman Filter

Our state estimation framework builds off of the classical EKF, which we outline in this section. Consider the following discrete, nonlinear state transition and measurement model:

\[ x_k = f_k(x_{k-1}, u_k) + w_k \]
\[ z_k = h_k(x_k) + r_k \]

where \( x_k \) denotes the state at index \( k \), \( u_k \) denotes the system input, if any, affecting the state transition, \( z_k \) denotes the received measurement, \( f_k \) and \( h_k \) denote the nonlinear state transition and measurement models, and \( w_k \) and \( r_k \) denote the process noise and measurement noise terms. The process noise and measurement noise terms are frequently modeled as zero-mean white Gaussian noise vectors, where \( w_k \sim \mathcal{N}(0, Q_k) \) and \( r_k \sim \mathcal{N}(0, R_k) \).

Given a sequence of past received measurements \( \{z_1, ..., z_k\} \), an EKF maintains an estimate of the current state \( x_k \), represented as \( \hat{x}_k \), and a corresponding covariance \( \hat{P}_k \) by recursively performing a predict step and an update step. In the predict step, the EKF propagates the previous state estimate and covariance forward by using the state transition model:

\[ \hat{x}_k = f_k(\hat{x}_{k-1}, u_k) \]
\[ \hat{P}_k = F_k \hat{P}_{k-1} F_k^\top + Q_k \]

where \( F_k := \frac{\partial f_k}{\partial x_k} \bigg|_{x_k = \hat{x}_{k-1}, u_k} \) is the Jacobian for the state transition model. Upon receiving a measurement \( z_k \), the EKF then updates the state estimate and covariance through the following update step:

\[ \gamma_k = z_k - h_k(\hat{x}_k) \]
\[ S_k = H_k \hat{P}_k F_k^\top + R_k \]
\[ K_k = \hat{P}_k F_k^\top S_k^{-1} \]
\[ \hat{x}_k = \hat{x}_k + K_k \gamma_k \]
\[ \hat{P}_k = (I - K_k R_k) \hat{P}_k \]
where \( H_k := \frac{\partial}{\partial x_k} \) is the Jacobian for the measurement model, \( \gamma_k \) is the innovation, and \( S_k \) represents the corresponding covariance of the innovation. The innovation term represents the additional information provided by the received measurement \( z_k \), which is unmodeled by the expected measurement as determined from the measurement model and predicted state, i.e., \( h(\bar{x}_k) \).

### 2.2 | M-Estimation

We additionally use M-estimation-based cost functions to strategically weigh the impact of the GPS measurements in the resilient filter state estimate. In this section, we provide an overview of M-estimation, which generalizes maximum likelihood estimation to be robust to outliers or extreme measurements. In particular, consider the following stochastic observation model:

\[
y = g(\beta) + e
\]  

where \( g \) represents a nonlinear function of the design variable \( \beta \) and \( e \) is the stochastic noise impacting our observations \( y \). When each element of the residual error vector \( e_i \) is a zero-mean, Gaussian random variable, i.e., \( e_i \sim \mathcal{N}(0, \sigma^2) \forall i \), and the residuals are independent and identically distributed, then the problem of estimating \( \beta \) is often formulated as follows:

\[
\beta^{LS} = \arg \min_{\beta} \sum_i e_i^2
\]  

where we observe the sum of squared residuals as the cost function to minimize and \( \beta^{LS} \) is referred to as the nonlinear least-squares solution. One drawback of using the cost function in Equation (11) is that the resulting state estimate \( \beta^{LS} \) is sensitive to outliers or extreme observations in \( y \). Thus, in the 1960s, Huber introduced the first notion of an M-estimator to reduce the influence of outliers in regression (Huber, 1964), which minimizes the sum of a more general function \( \Omega \) of the residuals:

\[
\arg \min_{\beta} \sum_i \Omega(e_i)
\]  

where \( \Omega \) is chosen as a symmetric, positive definite function with a unique minimum at 0 and is chosen to increase less rapidly than the least-squares cost function to provide greater robustness to measurement outliers.

M-estimators are often characterized in terms of their score function or influence function, which is the derivative of the cost function with respect to the residual, defined as \( \psi(e'_i) := \frac{\partial}{\partial e_i} \Omega(e_i) \). From the influence function, the M-estimator-based regression problem can be written as a weighted least-squares function, where the weight function is defined as \( w(e_i) := \frac{\psi(e_i)}{e_i} \). In this work, we examine three types of M-estimators, the Huber (Huber, 1964), Tukey (Tukey, 1962), and Hampel (Hampel, 1974) M-estimators, with respective weight functions:

\[
w^{\text{hub}}(e_i) = \begin{cases} 1 & \text{for } |e_i| \leq \tau_a \\ \frac{\tau_a^a}{|e_i|^a} & \text{otherwise} \end{cases}
\]  

(13)
The above M-estimator weight functions are correspondingly plotted in Figure 1 in comparison to the traditional least-squares function. The weight function thresholds $\tau_a$, $\tau_b$, and $\tau_c$ in Equations (13)–(15) are also denoted in Figure 1 and are used to determine the assigned reduced weight of the received measurement residual for robust estimation.

### 3 PROPOSED CHIMERA SPOOFING-RESILIENT FILTER FRAMEWORK

For our resilient filter framework, we perform the same prediction step as the traditional EKF in Equations (3)–(4) to obtain the predicted state and covariance $\left(\bar{x}_k, P_k\right)$. However, for the update step, we separate the set of received measurements into two categories: (1) trusted, self-contained sensor measurements $z^\text{self}_k$ and
and (2) GPS measurements $z_{k}^{gps}$. Thus, at each time step $k$, after the prediction step, we perform the update step in two parts, as outlined in the following two subsections.

### 3.1 Trusted Measurement Update Using Self-Contained Sensor Measurements

For any available self-contained sensor measurements $z_{k}^{self}$, we leverage the fact that these sensors are inherently trustworthy and perform the traditional EKF update as discussed in Section 2.1. Thus, we correspondingly perform the trusted measurement update using the expressions in Equations (5)–(9) with respect to the set of self-contained measurements $z_{k}^{self}$ and obtain an updated state estimate and covariance, which we denote as $(\hat{\chi}_{k}^{self}, \hat{P}_{k}^{self})$.

### 3.2 M-Estimation-Based GPS Measurement Update

After the trusted measurement update, if any GPS measurements $z_{k}^{gps}$ are available, we perform a modified EKF update step on the intermediate state estimate and covariance $(\hat{\chi}_{k}^{self}, \hat{P}_{k}^{self})$. In particular, we first evaluate the GPS measurement innovation and innovation covariance as in Equations (5)–(6), but using only the GPS measurements and evaluating the expected measurement with respect to the intermediate state estimate and covariance obtained after the trusted measurement update:

\[
\gamma_{k}^{gps} = z_{k}^{gps} - h_{k}^{gps}(\hat{\chi}_{k}^{self}) \tag{16}
\]

\[
S_{k}^{gps} = H_{k}^{gps}(\hat{\chi}_{k}^{self})H_{k}^{gps\top} + R_{k}^{gps} \tag{17}
\]

where $h_{k}^{gps}$, $H_{k}^{gps}$, and $R_{k}^{gps}$ represent the nonlinear measurement model, linearized model with respect to $\hat{\chi}_{k}^{self}$, and measurement covariance for the received GPS measurement vector, respectively. The resilient filter maintains a fixed window of the GPS measurement innovations and covariances as in Equations (16)–(17) from the past $N$ time steps. Similar to prior works (Khanafseh et al., 2014; Tanıl et al., 2017), we evaluate a test statistic of the sum of normalized, squared innovations over the window:

\[
q_{k} = \sum_{i=k-N}^{k} (\gamma_{i}^{gps})^{\top} (S_{i}^{gps})^{-1} \gamma_{i}^{gps} \tag{18}
\]

When the received GPS measurements are authentic and follow the nominal distribution with zero-mean Gaussian noise, as modeled in Equation (2), the test statistic $q_{k}$ follows a central chi-squared distribution with $n^{q} := (Nn^{gps})$ degrees of freedom, where $n^{gps}$ represents the number of received GPS measurements. We assume that the spoofer is self-consistent, in order to overcome detection through the use of receiver autonomous integrity monitoring (RAIM), and thereby modifies all GPS measurements in a self-consistent manner to induce the false navigation solution (Psiaki & Humphreys, 2016a). In this respect, we develop a single weighting factor at each time step in order to deweigh the influence of all GPS
measurements, if determined to be inconsistent with the self-contained sensor measurements. Thus, from the test statistic \( q_k \), we evaluate the scalar weighting factor for time step \( k \) as follows:

\[
d_k := w(q_k)
\]  \hspace{1cm} (19)

Here, \( w \) represents a generalization of the M-estimator weight function and outputs a value between 0 and 1, where a smaller value indicates less weight on the received GPS measurements. Indeed, when evaluating the weight function \( w \) in Equation (19), we extend the M-estimator weight functions in Section 2.2 from operating on absolute residuals, which nominally follow a standard normal distribution, to norms of multi-variate standard normal distributions. Note that the square root of the test statistic \( \sqrt{q_k} \) represents the norm of a multi-variate standard normal distribution, because \( q_k \) is a sum of squared, normalized Gaussian innovation vectors under nominal conditions, as shown in Equation (18). As a concrete example, we correspondingly extend the Huber M-estimator weight function as follows:

\[
tw_{\text{hub}}(q_k) = \begin{cases} 
1 & \text{for } p_k \leq \tau'_a \\
\frac{\tau'_a}{p_k} & \text{otherwise}
\end{cases}
\]  \hspace{1cm} (20)

where we use a modified threshold \( \tau'_a \) based on the degrees of freedom of the multi-variate residual. Indeed, notice that, when the number of degrees of freedom \( n^q \) is 1 for the test statistic \( q_k \), the generalized weight function in Equation (20) reduces to the classical definition of the Huber M-estimator weight function in Equation (13). Additionally note that the threshold values for the weight function, based on the norm of the residual vector, can be represented as a confidence level. In particular, we choose the generalized weight function threshold \( \tau' \) to represent the \( \alpha \) quantile, such that we have the following:

\[
P\{p_k \leq \tau'\} = P\{q_k \leq (\tau')^2\} = \alpha
\]  \hspace{1cm} (21)

\[
F((\tau')^2; n^q) = \alpha
\]  \hspace{1cm} (22)

where \( P\{\cdot\} \) represents the probability and \( F(\cdot; n^q) \) represents the cumulative distribution function (CDF) of the chi-squared distribution with \( n^q \) degrees of freedom. Then, we can choose the corresponding threshold value as follows:

\[
\tau' \leftarrow \sqrt{F^{-1}(\alpha; n^q)}
\]  \hspace{1cm} (23)

where \( F^{-1}(\cdot; n^q) \) represents the inverse CDF for the chi-squared distribution with \( n^q \) degrees of freedom. We perform analogous extensions to the Tukey and Hampel M-estimator weight functions to evaluate the corresponding weighting factor in Equation (19).

With the weighting factor \( d_k \) from Equation (19), we inflate the GPS measurement covariance used in the EKF update step, thereby reducing the reliance on GPS measurements during state estimation when the weighting factor becomes
smaller and closer to zero. In particular, we modify the EKF update expressions (Equations (6)–(9)) as follows:

\[
\begin{align*}
\tilde{S}_k &= H_k^{\text{gps}} \hat{p}_k^{\text{gps}} H_k^{\text{gps}^\top} + \frac{1}{d_k} R_k^{\text{gps}} \\
K_k^{\text{gps}} &= \hat{p}_k^{\text{gps}} H_k^{\text{gps}^\top} \tilde{S}_k^{-1} \\
\hat{x}_k^{\text{gps}} &= \hat{x}_k^{\text{self}} + K_k^{\text{gps}} \gamma_k^{\text{gps}} \\
\hat{p}_k^{\text{gps}} &= \left( I - K_k^{\text{gps}} R_k^{\text{gps}} \right) \hat{p}_k^{\text{self}}
\end{align*}
\]

Note that \(d_k\) is a scalar weight between 0 and 1. If \(d_k\) is too close to 0 in value, Equation (25) may become challenging to compute in practice, because of numerical overflows that arise when the inflated covariance is evaluated. Thus, in practice, we only perform the update in Equations (24)–(27) for sufficiently large \(d_k\).

The filter also leverages the periodic Chimera authentication, when available, to increase trust in the received GPS signal. In particular, if the received authentication is successful, the filter chooses \(d_k = 1\) for the first \(N_{\text{chim}}\) GPS measurements, given the recently confirmed authenticity of the received signal, where \(N_{\text{chim}}\) is chosen to correspond to a short duration, e.g., \(\sim 1\) s.

### 3.3 Extending the Spoofing-Resilient Filter Framework to Address GPS Multipath Scenarios

In this work, we focus on developing a spoofing-resilient filtering strategy for the case in which the received authentic GPS measurements are nominal, without degradation from multipath errors. To extend this framework to address multipath-affected GPS measurements, one could leverage the fact that an adept spoofer would spoof all GPS signals in a self-consistent manner, whereas individual multipath errors would lead to inconsistent bias errors in the received GPS measurements. Thus, to address multipath errors, this framework could be extended to include an initial multipath mitigation step, in which one verifies whether the received GPS measurements are self-consistent before performing the spoofing-resilient measurement update. Such an extension of the current framework is left as future work, but for the initial multipath mitigation step, one could utilize prior works on the detection and exclusion of erroneous GPS measurements (Groves, 2013) as well as multipath bias estimation and correction methods (Cheng et al., 2016; Lesouple et al., 2018).

### 4 Tightly Coupled GPS-IMU-Wheel Encoder Filter for a Ground Vehicle Model

We further examine our Chimera spoofing-resilient filter framework for a ground vehicle model. We assume that the vehicle moves horizontally in a local north-east-down (NED) navigation frame of reference, following a Dubins car model. In the trusted measurement update, we use an IMU and wheel encoder as the self-contained sensors. We utilize only one axis of the IMU measurements, which we assume is aligned in the vehicle’s direction of motion. Additionally, we propagate the vehicle state before each measurement update, with IMU updates...
performed at the highest rate every $\delta t^{\text{imu}}$ seconds. We assume that the vehicle receives GPS pseudorange and pseudorange rate measurements from all visible satellites. To simplify the propagation and update equations, we assume that the GPS antenna and IMU are both mounted at the vehicle's center of gravity.

### 4.1 State Overview

The state vector $x = [p^x, p^y, \theta, \dot{\theta}, v, a, b^g, b^a, b^{\text{clk}}, \dot{b}^{\text{clk}}]^\top \in \mathbb{R}^{10}$ consists of the vehicle's two-dimensional position $(p^x, p^y)$, heading $\theta$, heading rate $\dot{\theta}$, linear velocity $v$, linear acceleration $a$, IMU gyroscope and accelerometer biases $(b^g, b^a)$, and receiver clock bias and drift states $(b^{\text{clk}}, \dot{b}^{\text{clk}})$. The vehicle’s position, heading, and heading rate are in the local navigation frame of reference, whereas the linear velocity and acceleration are in the body frame, pointing towards the direction of vehicle motion.

### 4.2 State Propagation Model

At time index $k$, we propagate the vehicle position and heading via a Dubins car model (Thrun et al., 2005):

\[
\begin{bmatrix}
p^x_{k+1} \\
p^y_{k+1} \\
\theta_{k+1}
\end{bmatrix} =
\begin{bmatrix}
p^x_k \\
p^y_k \\
\theta_k
\end{bmatrix} + \delta t^{\text{imu}}
\begin{bmatrix}
v \cos(\theta) \\
v \sin(\theta) \\
\dot{\theta}
\end{bmatrix}
\tag{28}
\]

and we propagate the linear velocity using the linear acceleration, $v_{k+1} = v_k + \delta t^{\text{imu}} a_k$. The IMU bias states are modeled as follows:

\[
\begin{bmatrix}
b^g_{k+1} \\
b^a_{k+1}
\end{bmatrix} =
\begin{bmatrix}
b^g_k \\
b^a_k
\end{bmatrix} + w_k^{b,\text{imu}}
\tag{29}
\]

Here, the IMU bias process noise $w_k^{b,\text{imu}} \sim \mathcal{N}(0, Q^{b,\text{imu}})$, where $Q^{b,\text{imu}}$ is a block diagonal matrix with gyroscope and accelerometer terms, $Q^{b,\text{imu}} = \text{diag}(Q^{b,\text{gyro}}, Q^{b,\text{acc}})$, which we model using bias instability and correlation time parameters from IMU Allan deviation plots, as discussed in Section 4.4. The receiver clock states are modeled through a random walk process:

\[
\begin{bmatrix}
b^{\text{clk}}_{k+1} \\
\dot{b}^{\text{clk}}_{k+1}
\end{bmatrix} =
\begin{bmatrix}
1 & \delta t^{\text{imu}} \\
0 & 1
\end{bmatrix}
\begin{bmatrix}
b^{\text{clk}}_k \\
\dot{b}^{\text{clk}}_k
\end{bmatrix} + w_k^{b,\text{clk}}
\tag{30}
\]

where $w_k^{b,\text{clk}} \sim \mathcal{N}(0, Q^{b,\text{clk}})$. $Q^{b,\text{clk}}$ is modeled using the $h_0$ and $h_2$ power spectral density (PSD) coefficients, which are derived from Allan deviations and converted to units of m and m/s, respectively, based on the speed of light $c$ (Morton et al., 2021):

\[
Q^{b,\text{clk}} = c^2 \begin{bmatrix}
\frac{h_0}{2} \delta t^{\text{imu}} + 2\pi^2 h_2 (\delta t^{\text{imu}})^{\frac{3}{2}}, & 2\pi^2 h_2 (\delta t^{\text{imu}})^{\frac{3}{2}} \\
2\pi^2 h_2 (\delta t^{\text{imu}})^{\frac{3}{2}}, & 2\pi^2 h_2 \delta t^{\text{imu}}
\end{bmatrix}
\tag{31}
\]
4.3 Measurement Model

IMU measurements from the gyroscope and accelerometer are modeled as biased with Gaussian noise with respect to the corresponding true heading rate and linear acceleration as follows:

\[
\begin{align*}
    z^\text{gyro}_k &= \dot{\theta}_k + b^\text{gyro}_k + r^\text{gyro}_k \\
    z^\text{acc}_k &= a_k + b^\text{acc}_k + r^\text{acc}_k
\end{align*}
\]

where \( r^\text{gyro}_k \sim \mathcal{N}(0, R^\text{gyro}) \) and \( r^\text{acc}_k \sim \mathcal{N}(0, R^\text{acc}) \), with Section 4.4 providing more details on modeling \( R^\text{gyro} \) and \( R^\text{acc} \). Wheel encoder measurements of the linear velocity are modeled with additive Gaussian noise \( r^\text{whl}_k \), given by the following:

\[
    z^\text{whl}_k = v_k + r^\text{whl}_k
\]

For each satellite \( i \), the GPS pseudorange \( \rho^i_k \) and pseudorange rate \( \dot{\rho}^i_k \) measurements are modeled as follows:

\[
\begin{align*}
    \rho^i_k &= \sqrt{(p^i_k - x^i_k)^2 + (p^i_k - y^i_k)^2 + (p^i_k - z^i_k)^2} + b^\text{clk}_k + r^\rho^i_k \\
    \dot{\rho}^i_k &= \frac{(p_k - p^i_k) \cdot (\dot{p}_k - \dot{p}^i_k)}{\| p_k - p^i_k \|} + b^\text{clk}_k + r^{\dot{\rho}^i}_k
\end{align*}
\]

where \( p^i_k = [p^i_k, p^i_k, p^i_k]^T \) is the receiver position in the NED frame, \( p^i_k \) is the satellite position in the NED frame, \( r^\rho^i_k \) and \( r^{\dot{\rho}^i}_k \) are additive, white Gaussian noise terms, \( \dot{p}_k \) and \( \dot{p}^i_k \) denote the receiver and satellite velocities in the NED frame, and \( || \cdot || \) denotes the \( l_2 \) norm in Equation (36).

4.4 IMU Noise Covariance Modeling

We model the gyroscope and accelerometer process and measurement noises using the bias instability and random walk parameters, as described by Farrell et al. (2020) and summarized in this section. The process noise covariance is modeled via the bias instability parameter \( B^\text{imu} \) and correlation time \( T^b \), obtained from the IMU Allan deviation plot or datasheet. \( T^b \) is reported in seconds, and \( B^\text{imu} \) is reported in m/s^2 for accelerometers and °/s for gyroscopes. From the velocity and angular randomwalk terms, we obtain the randomwalk PSD \( S^\text{imu}_{\rho} \), which is then converted to the process noise covariance for the IMU bias terms:

\[
S^\text{imu}_{\rho} = \frac{2 \left( B^\text{imu} \right)^2 \ln(2)}{\pi (0.4365)^2 T^b} \quad Q^{\text{imu} \rho} = S^\text{imu}_{\rho} \delta t^\text{imu}
\]

The measurement noise covariance is modeled via the velocity random walk parameters \( N^\text{imu} \), obtained from the IMU Allan deviation plot or datasheet. \( N^\text{imu} \) is reported in m/s^2 for accelerometers and °/s for gyroscopes. From the velocity and angular randomwalk terms, we obtain the randomwalk PSD \( S^\text{imu}_{\rho} \), which is then converted to the IMU measurement covariance:

\[
S^\text{imu}_{\rho} = \left( N^\text{imu} \right)^2 \quad R^\text{imu} = \frac{S^\text{imu}_{\rho}}{\delta t^\text{imu}}
\]
5 | EXPERIMENTAL RESULTS

5.1 | Experimental Setup

We validate our proposed Chimera spoofing-resilient filter in a simulated test environment for the ground vehicle model outlined in Section 4, under various simulated GPS spoofing attack scenarios. We assume that the user has access to the 3-min Chimera slow authentication channel, and we simulate the scenario for two Chimera epochs, i.e., for 6 min in total. The simulated spoofing attack begins 60 s into the second Chimera epoch, i.e., 4 min after the simulation starts.

We assume that the spoofer has perfect knowledge of the vehicle state and gradually ramps the linear acceleration error in the true heading direction of the ground vehicle. We consider five different ramping rates between $10^{-4}$ m/s$^3$ and $10^{-2}$ m/s$^3$ and cap the linear acceleration error at a maximum of 0.1 m/s$^2$. We consider two separate vehicle trajectories, which are depicted in Figure 2, along with various spoofing ramp rates. Both trajectories are simulated using a Dubins car model (Thrun et al., 2005) with Gaussian noise $w^p \sim \mathcal{N}(0, Q^p)$ of covariance $Q^p = 10^{-4}$ m$^2$ added to the vehicle position states $(p^x, p^y)$.

Additionally, we simulate IMU measurements at 100 Hz, wheel encoder measurements at 10 Hz, and GPS pseudorange and pseudorange rate measurements at 10 Hz. We consider two grades of IMUs: a tactical-grade IMU and a micro-electromechanical system (MEMS) IMU (Groves, 2013, Chapter 4). The noise parameters from Section 4.4 for both IMU grades are specified in Table 1.

For the wheel encoder, measurement noise is modeled as $R^{whl} = 0.005$ m$^2$/s$^2$. For the GPS measurements, we simulate satellite positions and velocities using an ephemeris file from June 13, 2022 at 01:50am coordinated universal time. We assume our trajectories begin at the Durand building on the Stanford campus, using an elevation mask of 5°. We set the GPS pseudorange and pseudorange rate measurement covariances to be 36 m$^2$ and 1 m$^2$/s$^2$, respectively. For the receiver

![Figure 2](image-url)  

**Figure 2** Two simulated scenarios of ground vehicle trajectories with different degrees of spoofing attacks (a) Trajectory A (b) Trajectory B

We examine the performance of our Chimera spoofing-resilient filter for different degrees of spoofing attacks. In each case, the error in the GPS measurements is gradually ramped to reflect a corresponding linear acceleration error in the true heading direction of the Dubins car model. The corresponding false trajectories induced by the simulated GPS spoofing attacks are indicated by the red curves, for three of the five tested spoofing attack levels. We assume that the spoofer has perfect knowledge of the vehicle state.
Given the above covariance values, we consider an inflated process noise covariance for our spoofing-resilient filter as \( Q = 3 \cdot \text{diag} \{ Q^p, Q^p, 0.1 \times 10^{-4}, 0.1 \times 10^{-6}, 0.1 \times 10^{-4}, 0.1 \times 10^{-6} \} \). We compare the performance of our filter against other baseline filters, as detailed in Section 5.2. To determine the initial covariance matrix for the tested filters, we ran a conventional EKF with an inflated initial state error for 60 s prior to the start of the trajectory, allowing it to reach a steady-state covariance. We then used this steady-state covariance matrix for initialization of each tested filter.

In total, we have 20 test scenarios, one for each IMU grade, vehicle trajectory, and degree of spoofing attack. For each test scenario, we perform 10 Monte Carlo runs and examine the mean position errors during both authentic GPS conditions and during the spoofing attack. These results are discussed in Section 5.3 and Section 5.4.

### 5.2 Tested and Baseline Filters

For each test scenario, we examine the performance of our proposed Chimera spoofing-resilient filter for three different M-estimator weight functions (Huber, Tukey, and Hampel), with thresholds derived from chi-squared confidence levels, as given in Equation (23). For the Huber weight function, we chose a confidence level of 0.1 to obtain \( \tau_h \); for the Tukey weight function, we chose a confidence level of 0.997 to obtain \( \tau_t \). For the Hampel weight function, we chose confidence levels of 0.3, 0.6, and 0.9 to obtain \( \tau_h, \tau_b, \) and \( \tau_c \), respectively. We use window sizes \( N_{\text{chim}} \) and \( N \) of 15 GPS measurements, corresponding to 1.5 s for a rate of 10 Hz.

Additionally, we compare the performance of our proposed filter with a series of baseline filters:

- **Naive Filter:** This filter executes the classic EKF prediction and update expressions, as described in Section 2.1. In particular, this filter directly incorporates GPS measurements without performing any consistency-checking.
- **Odometry-Only Filter:** This filter only relies on the self-contained sensor measurements, i.e., the IMU and wheel encoder measurements, during the Chimera epoch. At the same time, this filter runs a naive filter in parallel. Upon receiving a successful Chimera authentication, the filter updates its state estimate and covariance to that of the naive filter, before continuing state estimation with odometry-only sensor measurements for the next Chimera epoch.
- **Authentic-GPS-Only Filter:** This filter directly uses GPS measurements only when they are authentic and immediately stops using these measurements at
the start of the spoofing attack, after which it relies only on the self-contained sensors for the remaining duration of the attack. While this filter is likely not realizable, because of the zero-delay response to induced attack errors, it provides an interesting baseline filter for comparison against our framework.

- **Chi-Squared Detector Switching (CSDS) Filter**: This filter relies on GPS measurements until it detects spoofing, using a chi-squared test statistic for the GPS measurements, similar to prior IMU-based innovation monitors (Khanafseh et al., 2014; Tanıl et al., 2016). We initiate the cumulative, chi-squared test statistic $q^\text{csd}_k$ at the beginning of each Chimera epoch. Then, after the statistic accumulates at least $N_{\text{chim}}$ GPS measurements, at each time step, we compare the test statistic to a threshold determined from the inverse CDF and a user-defined FAR for the confidence level, via the conversion in Equation (23). We test this detector for two FARs: $3 \times 10^{-3}$ and $10^{-6}$. If the chi-squared-based detector declares an attack, the filter stops using GPS measurements and only relies on self-contained sensor measurements until the next Chimera authentication time.

- **Kalman Gain Scaling (KGS) Filter**: Extending the CSDS filter, after the first $N_{\text{chim}}$ time steps, this heuristic filter uses the chi-squared statistic to weight the Kalman gain matrix in the GPS measurement update step. In particular, the confidence level associated with the chi-squared test statistic $q^\text{csd}_k$ is obtained via the expression in Equation (22) as $\alpha_k^\text{csd} := F(q^\text{csd}_k; n^q, \text{csd})$, where $n^q, \text{csd}$ represents the number of degrees of freedom of the statistic. This confidence level is used to weight the Kalman gain matrix before the measurement update step is performed with the GPS measurements as $K_k \leftarrow \alpha_k^\text{csd} K_k$.

- **Adaptive Measurement Covariance Estimation (AMCE) Filter**: This filter adaptively estimates the diagonal GPS measurement covariance matrix, based on the innovation for the GPS measurement update. At the start of each Chimera epoch, the filter initializes the diagonal GPS measurement covariance as the nominal covariance outlined in Section 5.1. Then, after $N_{\text{chim}}$ time steps, the filter updates this estimate at each subsequent time step as follows:

$$
\hat{\Sigma}_k = \max \left\{ \epsilon^+, \left( R_k + \gamma_k \gamma_k^\top - H_k R_k H_k^\top \right)_{ii} \right\} 
$$  \hspace{1cm} (39)

$$
\hat{R}_k = (1 - \mu_k) \hat{R}_k + \mu_k R_k 
$$  \hspace{1cm} (40)

$$
\mu_k = \frac{1 - \lambda}{1 - \lambda^{k+1}} 
$$  \hspace{1cm} (41)

where the $(i, i)$ subscript represents the $i$-th diagonal element of the covariance matrix, $\lambda = 0.95$, and $\epsilon^+ = 10^{-6}$. The maximum operation in Equation (39) ensures that the measurement covariance remains positive definite at all time steps.

### 5.3 Monte Carlo Results: Mean Position Estimation Errors Over Time

In Figures 3 and 4, we plot the mean position errors over 10 simulated rollouts for several levels of GPS spoofing attacks with the tactical-grade and MEMS IMU, respectively. In Figure 3, we observe that the odometry-only filter accumulates an average error of 10–30 m during the Chimera epoch when relying on the
FIGURE 3 Mean position estimation errors over time across 10 Monte Carlo runs, for various spoofing attack levels with the tactical-grade IMU and wheel encoder as self-contained sensors (a) Larger spoofing attack ($10^{-3}$ m/s$^3$ ramp rate) with Trajectory A (b) Larger spoofing attack ($5 \cdot 10^{-3}$ m/s$^3$ ramp rate) with Trajectory B (c) Smaller spoofing attack ($10^{-4}$ m/s$^3$ ramp rate) with Trajectory A (d) Smaller spoofing attack ($5 \cdot 10^{-4}$ m/s$^3$ ramp rate) with Trajectory B. The odometry-only filter (periwinkle) accumulates 10–30 m of error during the Chimera epoch, whereas the naive filter (green) accumulates over 400 m of error for the largest attack. The Huber spoofing-resilient filter (purple) and ACME filter (pink) only show marginally better spoofing mitigation than the naive filter in all scenarios, except for the largest attack magnitude, as shown in Figure 3(b). The CSDS filters (orange and lime green) both demonstrate an ability to mitigate the spoofing attack with a significantly lower accumulated error than the naive filter during spoofing, for all but the smallest attack magnitude, as shown in Figure 3(c). The KGS filter (olive) shows improved spoofing mitigation over the CSDS filters; however, the best spoofing mitigation performance is observed for the proposed spoofing-resilient filters with the Tukey and Hampel weight functions (brown and sky blue), with the lowest accumulated average error in each scenario.
tactical-grade IMU, wheel encoder, and vehicle dynamics model. In contrast, as shown in Figure 4, the errors accumulate to 50–200 m for the MEMS IMU. For the naive filter, depending on the level of spoofing attack, we observe that the average errors accumulate to just above 15 m for the smallest attack magnitude with a ramp rate of $10^{-4}$ m/s$^3$ to over 400 m for the largest attack magnitude with a ramp rate of $10^{-2}$ m/s$^3$.

For each case in Figures 3 and 4, we notice that the spoofing-resilient filter with the Huber weight function only performs marginally better than the naive filter, with an accumulated error magnitude comparable to that of the naive filter during the simulated attacks. Thus, on average, the Huber spoofing-resilient filter accumulates larger errors than the odometry-only filter for nearly all spoofing attacks in Figures 3 and 4, except for the smallest magnitude size with a ramp rate $10^{-4}$ m/s$^3$.

We observed similar performance results when utilizing different thresholds for the Huber weight function. Indeed, because of the shape of the Huber weight function, moderate measurement outliers are treated the same as very large outliers, thereby making this filter less resilient to spoofing attacks as compared with the re-descending Tukey and Hampel spoofing-resilient filters. The AMCE filter also accumulates a significant amount of position error during the simulated attacks, exceeding the accumulated error of the odometry-only filter in all cases with the tactical-grade IMU, as shown in Figure 3, and in the larger attack with the MEMS IMU, as shown in Figure 4(a).

The CSDS filters both show an ability to mitigate the spoofing attack, with a significantly lower accumulated error on average than the naive filter for nearly all cases in Figures 3 and 4. We can particularly observe this in the examples in Figures 3(b) and 4(d), when both CSDS filters distinctly stop following the same error growth rate as the naive filter and begin accumulating additional error at slower drift rates, comparable to the rate of error growth observed for the odometry-only filter at the start of the Chimera epoch. Indeed, at this time point, the CSDS filters switch to using only the self-contained sensors and correspondingly reject the spoofed GPS measurements. However, because the CSDS filters rely completely on GPS until the test statistic falls below the FAR threshold, these filters tend to more readily incorporate errors induced by the spoofer at the onset of the attack, leading to a larger overall accumulation of position errors on average than the Tukey and Hampel spoofing-resilient filters as well as the heuristic KGS filter in each case. Indeed, because the KGS filter begins to partially deweight inconsistent GPS measurements earlier than the CSDS filters, we observe better error mitigation with this filter as compared with the switching filters, with smaller average accumulated errors for all cases in Figures 3 and 4. In Figure 3(c), we further notice that the mean position estimation error grows slightly during the first Chimera epoch for the CSDS filter with a FAR of $3\cdot10^{-3}$. This result arises from the fact that 1 of the 10 Monte Carlo simulation runs had a false alarm event and switched to using only the self-contained sensors until the start of the next Chimera epoch, when it began re-accepting GPS measurements because of the successful Chimera authentication.

Interestingly, for the smaller spoofing attack magnitude cases with the MEMS IMU, as shown in Figures 4(c) and 4(d), we observe that the CSDS filters and KGS filter consistently outperform the authentic-GPS-only filter, maintaining similar or smaller average position errors. In this case, the authentic-GPS-only filter immediately stops using the GPS measurements once spoofing starts, and the MEMS IMU and wheel encoder sensors together still lead to a greater position error drift rate as compared with the error growth initially induced by the spoofing attacks. Thus, we observe that these filters acquire an advantage by following...
FIGURE 4 Mean position estimation errors over time across 10 Monte Carlo runs, for various spoofing attack levels with the MEMS IMU and wheel encoder as self-contained sensors (a) Larger spoofing attack (10^{-3} m/s^3 ramp rate) with Trajectory A (b) Larger spoofing attack (10^{-2} m/s^3 ramp rate) with Trajectory B (c) Smaller spoofing attack (10^{-4} m/s^3 ramp rate) with Trajectory A (d) Smaller spoofing attack (5 \cdot 10^{-4} m/s^3 ramp rate) with Trajectory B

The odometry-only filter (periwinkle) accumulates 50–200 m of error during the Chimera epoch, whereas the naive filter (green) accumulates over 400 m of error for the largest attack. Similar to Figure 3, the Huber spoofing-resilient filter (purple) and ACME filter (pink) only exhibit marginally better spoofing mitigation than the naive filter in all scenarios except for the largest attack magnitude, as shown in Figure 4(b). The CSDS filters (orange and lime green) both demonstrate a significantly lower accumulated error than the naive filter for all but the smallest spoofing attack, as shown in Figure 4(c). The KGS filter (olive) shows improved spoofing mitigation over the CSDS filters; however, the best spoofing mitigation performance is observed for the proposed spoofing-resilient filters using the Tukey and Hampel M-estimator weight functions (brown and sky blue), with the lowest accumulated average error in each spoofing scenario.
the smaller-magnitude spoofing attack for a longer time duration. In particular, for the smallest-magnitude attack, as shown in Figure 4(c), the growth of the spoofing-induced errors is less than the error growth incurred by using only the self-contained sensors accumulated from the start of the attack. Consequently, the CSDS and KGS filters largely utilize the spoofed GPS measurements and accumulate less error than the authentic-GPS-only filter in this case. Similarly, as shown in Figure 4(d), we observe that by tracking the spoofed GPS measurements a bit longer (while the errors are relatively small) before rejecting GPS measurements, the CSDS and KGS filters accumulate less error than the authentic-GPS-only filter for this milder attack scenario.

For each scenario in Figures 3 and 4, we observe the best spoofing mitigation performance for the spoofing-resilient filters with the Tukey and Hampel M-estimator weight functions, with the lowest accumulated position errors during the attack. In fact, both spoofing-resilient filters have comparable or even lower accumulated position errors than the authentic-GPS-only filter in each scenario. For each case, we observe that these spoofing-resilient filters utilize the GPS signal while the spoofing-induced errors are small, but still switch away from using the spoofed GPS measurements once the errors grow, even before the CSDS and KGS filters, which follow the error growth trajectory of the naive filter for a longer duration. This effect is particularly noticeable in Figures 3(b) and 4(d). Although the Tukey spoofing-resilient filter consistently outperforms the Hampel spoofing-resilient filter during the spoofing attacks, its conservative use of GPS measurements also results in slightly worse performance (larger mean position errors) than the Hampel spoofing-resilient filter when the GPS signal is authentic, as discussed in more depth in Section 5.4.

5.4 Monte Carlo Results: Mean Position Errors During Authentic and Spoofed Conditions

We next examine the overall mean position errors for each scenario (IMU type, spoofing attack level, and trajectory) and for each filter type. The mean position errors are computed across the 10 Monte Carlo simulations and across time, for both the duration when the GPS signal is authentic as well as the duration of the simulated attack. In Figure 5, we plot the mean position error during authentic conditions on the x-axis and the mean error during the spoofing attack on the y-axis. Figures 5(a) and 5(b) show the Monte Carlo results obtained with the tactical-grade IMU for Trajectories A and B, respectively, whereas Figures 5(c) and 5(d) show results obtained with the MEMS IMU for the two trajectories. At the top of the figure, we include a legend that denotes the results from each filter type with a different color and those for each level of spoofing attack with a different type of plotting marker. The results plotted in Figure 5 are also numerically presented in Table 2.

In each scenario, we notice that the naive filter performs well during authentic-GPS conditions, providing a sub-meter-level average error when using the on-board IMU, wheel encoder, vehicle dynamics model, and authentic GPS pseudorange and pseudorange rate measurements for state estimation. However, during the simulated spoofing attacks, this filter accumulates a significant amount of position error, with an average error of over 100 m for the worst-case attacks. At the same time, we notice that the odometry-only filter is more resilient than the naive filter during spoofing, exhibiting an average error on the order of 10 m (across time and across rollouts) when equipped with the tactical-grade IMU and less than 100 m for the MEMS IMU. As a result, the odometry-only filter accumulates
Mean position estimation errors over 10 Monte Carlo runs during authentic-GPS and spoofing conditions (a) Trajectory A, tactical-grade IMU (b) Trajectory B, tactical-grade IMU (c) Trajectory A, MEMS IMU (d) Trajectory B, MEMS IMU Figures 5(a) and 5(b) show results for the simulated scenarios with the tactical-grade IMU for Trajectories A and B, respectively, and Figures 5(c) and 5(d) show results for the MEMS IMU. The legend at the top denotes the different colors for each tested and baseline filter and the different marker shapes for each level of spoofing attack. We observe that the naive filter (green) performs well when the GPS signal is authentic, but exhibits an average error of over 100 m (across time and Monte Carlo rollouts) during the worst-case spoofing attacks. The odometry-only filter (periwinkle) exhibits increased spoofing resilience, but at the cost of significantly larger average errors when the GPS signal is authentic. The Huber spoofing-resilient filter (purple) and AMCE filter (pink) have only marginally smaller average position errors than the naive filter during spoofing. Both CSDS filters (orange and lime green) show larger errors than the authentic-GPS-only filter (blue) during spoofing when equipped with the tactical-grade IMU, whereas the KGS filter (olive) shows improved spoofing mitigation performance with smaller accumulated errors than the CSDS filters. Our proposed Tukey and Hampel spoofing-resilient filters (brown and sky blue) show the best spoofing mitigation, with a smaller average position error than the other filters during attack conditions. Moreover, the Hampel spoofing-resilient filter maintains position errors comparable to those of the naive and authentic-GPS-only filters during authentic conditions.
<table>
<thead>
<tr>
<th>Filter</th>
<th>IMU</th>
<th>Traj.</th>
<th>Tested Spoofing Acceleration Ramp Rate (m/s²)</th>
<th>10⁻²</th>
<th>5 · 10⁻³</th>
<th>10⁻³</th>
<th>5 · 10⁻⁴</th>
<th>10⁻⁴</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Author. Spoofed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Author. Spoofed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Naive</td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.53</td>
<td>0.49</td>
<td>0.52</td>
<td>0.44</td>
<td>0.5</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.51</td>
<td>0.51</td>
<td>0.51</td>
<td>0.53</td>
<td>0.51</td>
</tr>
<tr>
<td></td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.54</td>
<td>0.52</td>
<td>0.52</td>
<td>0.53</td>
<td>0.52</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.55</td>
<td>0.54</td>
<td>0.55</td>
<td>0.53</td>
<td>0.52</td>
</tr>
<tr>
<td>Odometry Only</td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.54</td>
<td>0.40</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.79</td>
<td>0.79</td>
<td>0.79</td>
<td>0.52</td>
<td>0.79</td>
</tr>
<tr>
<td></td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.54</td>
<td>0.52</td>
<td>0.52</td>
<td>0.53</td>
<td>0.52</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.55</td>
<td>0.54</td>
<td>0.55</td>
<td>0.53</td>
<td>0.52</td>
</tr>
<tr>
<td>Authentic GPS Only</td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.64</td>
<td>0.65</td>
<td>0.61</td>
<td>0.23</td>
<td>0.59</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.88</td>
<td>0.75</td>
<td>0.77</td>
<td>0.26</td>
<td>0.53</td>
</tr>
<tr>
<td></td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.57</td>
<td>0.8</td>
<td>0.63</td>
<td>0.28</td>
<td>0.56</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.59</td>
<td>0.69</td>
<td>0.64</td>
<td>0.27</td>
<td>0.57</td>
</tr>
<tr>
<td>Chi-Squared Detector</td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.53</td>
<td>0.49</td>
<td>0.52</td>
<td>0.13</td>
<td>0.51</td>
</tr>
<tr>
<td>Switching (FAR: 3 · 10⁻³)</td>
<td>MEMS</td>
<td></td>
<td></td>
<td>1.39</td>
<td>0.51</td>
<td>0.51</td>
<td>0.52</td>
<td>1.06</td>
</tr>
<tr>
<td></td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.54</td>
<td>0.52</td>
<td>0.55</td>
<td>0.18</td>
<td>0.54</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.55</td>
<td>0.54</td>
<td>0.55</td>
<td>0.11</td>
<td>0.54</td>
</tr>
<tr>
<td>Chi-Squared Detector</td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.53</td>
<td>0.49</td>
<td>0.49</td>
<td>0.53</td>
<td>0.52</td>
</tr>
<tr>
<td>Switching (FAR: 10⁻⁴)</td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.55</td>
<td>0.52</td>
<td>0.55</td>
<td>0.13</td>
<td>0.53</td>
</tr>
<tr>
<td>Kalman Gain scaling</td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.53</td>
<td>0.48</td>
<td>0.48</td>
<td>0.52</td>
<td>0.51</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.54</td>
<td>0.52</td>
<td>0.55</td>
<td>0.18</td>
<td>0.54</td>
</tr>
<tr>
<td>Spoofing-Resilient (Huber)</td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.53</td>
<td>0.49</td>
<td>0.49</td>
<td>0.53</td>
<td>0.52</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.51</td>
<td>0.51</td>
<td>0.49</td>
<td>0.52</td>
<td>0.51</td>
</tr>
<tr>
<td></td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.54</td>
<td>0.52</td>
<td>0.55</td>
<td>0.43</td>
<td>0.52</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.55</td>
<td>0.53</td>
<td>0.55</td>
<td>0.43</td>
<td>0.54</td>
</tr>
<tr>
<td>Spoofing-Resilient (Tukey)</td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.68</td>
<td>0.62</td>
<td>0.66</td>
<td>0.57</td>
<td>0.61</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.63</td>
<td>0.63</td>
<td>0.65</td>
<td>0.56</td>
<td>0.66</td>
</tr>
<tr>
<td></td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.71</td>
<td>0.68</td>
<td>0.71</td>
<td>0.42</td>
<td>0.65</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.69</td>
<td>0.64</td>
<td>0.67</td>
<td>0.52</td>
<td>0.67</td>
</tr>
<tr>
<td>Spoofing-Resilient (Hampel)</td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.56</td>
<td>0.52</td>
<td>0.52</td>
<td>0.43</td>
<td>0.52</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.53</td>
<td>0.54</td>
<td>0.54</td>
<td>0.41</td>
<td>0.52</td>
</tr>
<tr>
<td></td>
<td>tactical</td>
<td></td>
<td></td>
<td>0.58</td>
<td>0.57</td>
<td>0.58</td>
<td>0.54</td>
<td>0.57</td>
</tr>
<tr>
<td></td>
<td>MEMS</td>
<td></td>
<td></td>
<td>0.58</td>
<td>0.56</td>
<td>0.59</td>
<td>0.61</td>
<td>0.59</td>
</tr>
</tbody>
</table>

Results are also visually plotted in Figure 5. Each scenario is simulated over two Chimera epochs, i.e., 6 min in total. The first Chimera epoch has authentic GPS measurements only, and the erroneous, spoofed GPS measurements begin 60 s into the second Chimera epoch, i.e., 4 min after the simulation starts.
less average position error than the naive filter during spoofing, except when the degree of the spoofing attack is smaller than the amount of drift from the set of odometry sensors on-board the vehicle, as observed for the two smallest spoofing attacks ($5 \cdot 10^{-4}$ m/s$^3$ and $10^{-4}$ m/s$^3$) with the MEMS IMU. However, this increased spoofing resilience of the odometry-only filter occurs at the cost of significantly larger average errors during authentic conditions, because the filter does not utilize the authentic GPS signals to improve its state estimation during the Chimera epoch.

Similar to our observations in Section 5.3, for each scenario in Figure 5, we observe that the Huber spoofing-resilient filter has only marginally smaller average position errors during spoofing as compared with the naive filter. Similarly, we observe that the AMCE filter exhibits significantly larger errors during spoofing, with an error of approximately 20 m or greater for all but the smallest spoofing scenario, while also having larger errors than the naive and authentic-GPS-only filters during authentic conditions.

For the CSDS filter with a FAR of $10^{-6}$, we observe average position errors similar to those of the naive and authentic-GPS-only filters during authentic conditions. However, for the CSDS filter with a FAR of $3 \cdot 10^{-3}$, we occasionally observe larger average errors under authentic conditions, for instances in which a spoofing attack is falsely declared and the filter switches to using only the self-contained sensors. Indeed, the CSDS filter maintains an updated chi-squared statistic at the GPS measurement rate of 10 Hz and tests for spoofing at the same rate, leading to occasional false alarms during authentic conditions, across Monte Carlo simulations. We observe in Figures 5(c) and 5(d) that, during spoofing, both CSDS filters have average position errors comparable to that of the authentic-GPS-only filter when equipped with the MEMS IMU, with an error of 10–20 m; however, during the attack scenarios in Figures 5(a) and 5(b), we observe that the CSDS filters have 2–3 times larger error than the authentic-GPS-only filter when equipped with the tactical-grade IMU.

Additionally, we observe that our proposed Chimera spoofing-resilient filters with the Tukey and Hampel weight functions maintain a lower average position error during spoofing than the other tested filters for nearly every simulated scenario in Figure 5, including the KGS filter. As also observed in Section 5.3, both of these spoofing-resilient filters perform either comparatively well or better than the authentic-GPS-only filter during spoofing. During authentic conditions, the Tukey resilient filter performs slightly worse than the naive and authentic-GPS-only filters, with the position errors being approximately 1.5 times larger on average. However, the Hampel resilient filter only exhibits slightly larger average position errors than the naive and authentic-GPS-only filters during authentic conditions, with the additional error being consistently less than 0.1 m for each scenario. Thus, our results demonstrate that the Tukey and Hampel spoofing-resilient filters not only strategically leverage the received GPS measurements during authentic conditions to improve state estimation during the Chimera epoch, but also successfully mitigate spoofing-induced errors for different degrees of simulated attacks.

6 CONCLUSION

In this work, we proposed a new GPS spoofing-resilient filter framework that provides continuous and secure state estimation between Chimera authentication times. In particular, our spoofing-resilient filter leverages the Chimera authentication information, when available, and the redundancy from additional
self-contained sensors to strategically determine how much trust to assign to the real-time, unauthenticated GPS measurements via an M-estimation-based weighting scheme. In validating our filter in a simulated test environment under various degrees of simulated spoofing attacks, we observed that, with the re-descending Tukey or Hampel M-estimation weight functions, our filter mitigates the effects of each spoofing attack by rejecting the spoofing-induced errors in a timely manner, resulting in a lower overall position error during spoofing as compared with filters that switch away from using GPS once the chi-squared-based detector declares an attack. In addition to demonstrating resilience during each simulated spoofing attack, when the received GPS signal is authentic, our spoofing-resilient filter shows comparable navigation performance, evaluated in terms of mean localization errors, as compared with filters that consistently trust and leverage the GPS measurements. In this respect, our proposed spoofing-resilient filter framework ensures attack resilience by mitigating spoofing-induced errors during various levels of spoofing attacks, while also improving real-time navigation performance when the GPS signal is authentic.

ACKNOWLEDGMENTS

This material is based upon work supported by the AFRL under grant number FA9453-20-1-0002. This material is also based upon work supported by a National Science Foundation (NSF) Graduate Research Fellowship under grant number DGE-1656518. We would like to thank the AFRL and NSF for sponsoring this research. We would also like to thank Bradley Collicott for insightful discussions as well as Shubh Gupta for reviewing this paper.

REFERENCES

C4ADS Think Tank. (2019). Above us only stars: Exposing GPS spoofing in Russia and Syria. https://c4ads.org/reports/above-us-only-stars/  


**How to cite this article:** Mina, T., Kanhere, A., Shetty, A., & Gao, G. (2024). GPS spoofing-resilient filtering using self-contained sensors and Chimera signal enhancement. *NAVIGATION, 71*(2). https://doi.org/10.33012/navi.636