Covert Control of Surface Vessels via Counterfeit Civil GPS Signals

Jahshan Bhatti and Todd E. Humphreys

Abstract—**An attacker's ability to covertly control a maritime surface vessel by broadcasting counterfeit civil Global Positioning System (GPS) signals is analyzed and demonstrated. The aim of this work is to explore civil maritime transportation's vulnerability to deceptive GPS signals. It is shown that, despite access to a variety of high-quality navigation and surveillance sensors, modern maritime navigation depends crucially on satellite navigation. A simple innovations-based detection framework for GPS deception is developed, and given real-world environmental and attack parameters, the probability of hazardously misleading information (HMI) is minimized within the framework. A covert attack is designed to have a high probability of HMI and is possible because attacker-induced deviations in the vessel's cross-track dynamics can be disguised as the effects of slowly-changing ocean currents. A field experiment confirms the analysis by demonstrating covert control of a 65-m yacht in the Mediterranean Sea.**

Keywords: Navigation security, Maritime navigation, GPS spoofing.

I. Introduction

Surface vessels, from fishing boats to container ships to deep-water oil rigs, depend crucially on Global Positioning System (GPS) signals for navigation, station keeping, and surveillance [1]–[5]. GPS and other Global Navigation Satellite System (GNSS) signals are the primary maritime navigation aid even for vessels actively piloted by human operators, except perhaps under clear conditions in familiar littoral waters. Moreover, as surface craft become more autonomous, the trend is toward increased reliance on GNSS: current autopilot systems, dynamic-positioning systems, and fully unmanned surface vehicles are designed under the assumption that GNSS signals are usually available and trustworthy [2], [4], [6], [7]. Even autonomous underwater vehicles typically depend indirectly, or periodically, on GNSS [8].

Given the fragility of GNSS signals under conditions of signal blockage or jamming, and given that the signals do not penetrate underwater, there is interest in developing GNSS-independent maritime navigation and control systems [2], [9], [10]. Terrain-relative navigation has been successfully employed in autonomous submersibles [9], [10], and could serve as a backup to GNSS for surface vessels. This technique has historically required high-resolution (e.g., m-level) underwater terrain maps, which are available for only a tiny fraction of the seafloor, but recent results indicate that coarser (e.g., 20-m-resolution) ship-based bathymetry maps may be adequate for 10-meter-level positioning, provided sufficient terrain variability [11]. Nonetheless, for the present, terrain-relative navigation does not even appear to be an active research topic for civil surface maritime transportation. What is more, the only widespread radionavigation backup to GNSS, LORAN-C, was abandoned by the U.S. Coast Guard in 2010 [12], and there are no official U.S. plans for a successor. Consequently, one can expect most maritime navigation systems to rely on GNSS for years to come.

By standard practice marine craft are equipped with redundant GNSS units so that one serves as backup if the other experiences a fault. And for extremely critical applications, an entirely GNSS-free positioning system may be available, such as the acoustic positioning system required as a backup to GNSS on dynamically-positioned deepwater drilling vessels [4]. But these fail-safe systems are designed to handle obvious faults or GNSS outages caused by signal blockage or ionospheric effects. They are likely to fail when confronted with a sophisticated and deliberate attacker: outlaws are different from outliers; fraud is different from faults.

A GNSS deception attack, in which counterfeit GNSS signals are generated for the purpose of manipulating a target receiver's reported position, velocity, and time, is a potentially dangerous tool in the hands of a deliberate attacker. While there have been no reports of such attacks performed with malice, convincing demonstrations have been conducted both in the laboratory and in the field with low-cost equipment against a wide variety of GPS receivers [13]–[17]. The key to the success of these so-called GPS spoofing attacks is that, whereas the military GPS waveforms are by design unpredictable and therefore resistant to spoofing [18], civil GPS waveforms—and those of other civil GNSS—are unencrypted, unauthenticated, and openly specified in publicly-available documents [19], [20]. Also, although not entirely constrained by the GNSS signal specifications, the navigation data messages modulating these civil waveforms are highly predictable. The combination of known signal structure and navigation data predictability makes civil GNSS signals an easy target for spoofing attacks.

This paper makes four primary contributions. First, it details the pathways and effects of GNSS deception on maritime navigation and surveillance. Second, whereas maritime transportation's vulnerability to GNSS jamming has been previously established [2], this paper offers the first detailed analysis of the effects of GNSS deception on a surface vessel. Third, it investigates the performance of a spoofing detection framework and optimizes the integrity risk within this framework given a set of possible attack profiles. Fourth, it presents the results of an unprecedented field experiment demonstrating hostile

Authors' address: Department of Aerospace Engineering, The University of Texas at Austin, Austin TX, 78712, Email: (jahshan@utexas.edu), (todd.humphreys@mail.utexas.edu).

control of a 65-m yacht in the Mediterranean Sea.

II. Pathways and Effects of GNSS Deception

This section details the pathways and effects of GNSS deception on maritime navigation and surveillance. Although the focus here and throughout the rest of the paper will be on manned surface vessels, the conclusions apply with some modification to unmanned surface vessels (USVs).

A. GNSS Dependencies of a Modern Integrated Bridge System

1) Compass: The magnetic compass and gyrocompass (a gyroscope designed to be north-seeking by taking advantage of the Earth's rotation) depend weakly on GNSS. A magnetic compass requires knowledge of latitude and longitude to correct for magnetic variation [21]. A gyrocompass requires knowledge of the latitude and speed in the north/south direction to correct for "northing" error [21]. However, outside of the polar regions, position errors on the order of tens of kilometers and velocity errors on the order of meters per second will only cause pointing errors on the order of a degree. Therefore, this paper will neither exploit nor model the weak coupling between GNSS and the compass.

However, with the introduction of the satellite compass [22], [23], which provides both position and three-axis attitude of the ship, the compass could now be strongly dependent on GNSS signals. A common satellite compass configuration is two GPS receivers separated by a 5-10 meter baseline coupled with miniature accelerometers, gyros, and a magnetometer, which can be significantly more attractive than a heavy, power-hungry, and slow-to-calibrate gyrocompass. Despite the satellite compass's heavy dependence on GPS, the dual-antenna configuration is a necessary component for a potent spoofing detector, as will be shown in Sec. VII.

2) Automatic Radar Plotting Aid: The Automatic Radar Plotting Aid (ARPA) is the primary tool used for collision avoidance by the navigator. The ARPA processes and displays the raw radar data in a polar azimuth-range plot, tracks targets, and computes time and distance of closest approach for each target [24]. Without the additional information that sensors like compass, speed log, and GNSS provide, the ARPA can still perform collision-avoidance functions but only display target information in a heads-up mode with relative motion. With compass information, the ARPA can present the radar data in a course-up mode to prevent smearing of the returns during course-change manuevers. Similarly, the ARPA can present the radar data in a "true motion" mode, where the motion is either sea-stabilized by compass and speed log or ground-stabilized by GNSS. Additionally, GNSS information allows the ARPA to compute latitude and longitude for the tracked targets. Therefore, basic collision avoidance with ARPA is possible without GNSS, but advanced convenience features such as ground stabilization and target localization depend on GNSS signals. For example, under a GNSS deception attack with ground stabilization enabled on the ARPA, radar echos from land masses may appear to move when they should be stationary.

3) Automatic Identification System: The Automatic Identification System (AIS) allows ships to communicate their position, heading, and speed in a self-organizing radio network to aid in collision avoidance [21]. A ship's AIS transceiver typically uses a GNSS-based positioning source, although backup sources only used during GNSS failure can be set. However, under a GNSS deception attack, a ship may transmit misleading AIS reports and incorrectly compute the point of closest approach (PCA) to surrounding ships, hindering collision avoidance.

4) Dead Reckoning System: Dead reckoning (DR) is the process of propagating a known position based solely on a ship's course and speed, derived from compass and speed log measurements. An estimated position (EP) corrects a dead-reckoned position based on the best knowledge of the effects of environmental disturbances such as leeway (drift due to wind), rudder offset, and tidal and ocean currents. Typically, the effects of environmental disturbances are lumped together into a velocity error vector, whose angle and magnitude are referred to as set and drift, respectively. The set and drift can be estimated by comparing a dead-reckoned position to a position fix derived from either a GNSS receiver (typically), observations of celestial bodies, or radar and visual bearings [21]. On paper charts, DR would be reset with a position fix at least every hour, or as often as every three minutes, depending on the accuracy required for navigating the surrounding waters. However, in most electronic chart systems, DR is reset once per second since GNSS is nearly always available and reliable [21].

5) Electronic Chart Display and Information System: The Electronic Chart Display and Information System (ECDIS) consolidates the measurements available from various ship sensors and integrates systems such as ARPA, AIS, and DR as shown in Fig. 1 to provide complete situational awareness to the ship's crew [21]. ECDIS is the primary tool for route planning and tertiary to the ARPA and AIS for collision avoidance. However, most ECDIS allow overlaying ARPA and AIS information over the charts and planned route for convenience. In fact, the overlay may be useful in detecting discrepancies between the GNSS and radar signals, but may also confuse a crew unaware of GNSS deception. Nevertheless, when the shore exceeds the range of radar (20 km for low-frequency radar, less for X-band) and there are only a few ships nearby, GNSS deception attacks are not likely to be detected solely with radar. Some electronic chart systems such as the Totem ECDIS allow configuring the position fix interval of the built-in DR and raising an alarm if the position fix exceeds a threshold [25]. In Sec. IV, the probability of hazardously misleading information (HMI) and detection statistic threshold will be computed for a given false-alarm rate and fix interval.

6) Autopilot System: Most ships will typically have a course autopilot, which maintains a prescribed heading through rudder actuation and compass feedback. Some ships will additionally have a speed autopilot, which maintains a prescribed speed through water by varying the engine thrust from speed log feedback. Both autopilot systems do not depend on GNSS directly, however, the course autopilot is typically driven by a higher-level track-keeping system, which

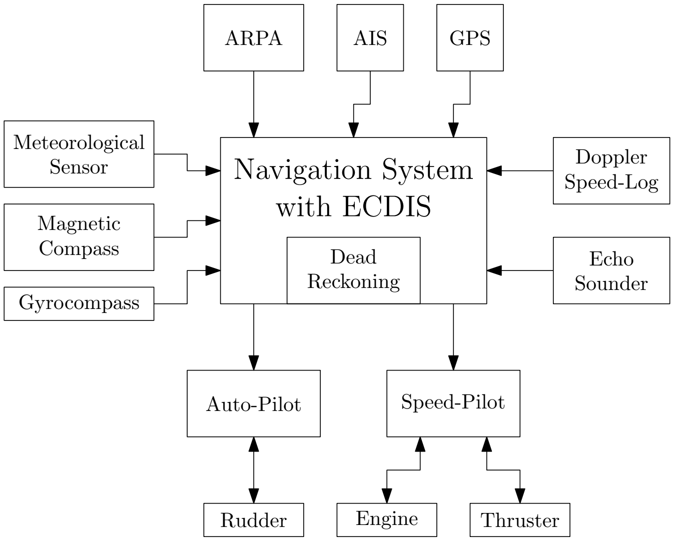


Figure 1. Block diagram showing relationship between sensors, actuators, and the ECDIS on an integrated bridge system.

requires GNSS feedback [26].

7) Others: Sensors which do not have any dependency on GNSS include the speed log, meteorological sensors, sonar, and roll stabilization systems. The modern speed log uses Doppler measurements to compute two axis speed through water. Roll stabilization typically involves a feedback control loop that modulates the rudder or more expensive fins if available [26].

B. Illustrative Example: The Grounding of the Royal Majesty

To appreciate the possible effects of a GPS deception attack on a surface vessel, it is instructive consider the grounding of the 174-meter cruise liner Royal Majesty [27]–[29]. Shortly after the ship departed Bermuda for Boston in June of 1995, the cable connecting its GPS antenna to the unit on the bridge became detached, forcing the GPS unit to transition to a dead-reckoning mode in which the ship's location was extrapolated from the last known good location based solely on gyro compass and water speed measurements. The crew and autopilot, unaware of the transition to DR mode, accepted the position indicated on the radar display's map as truthful even as the ship accumulated a 17 nmi cross-track navigational error. As the ship approached Nantucket, the crew misidentified one buoy and ignored the absence of another. The ship's GPS-based navigation system had performed so utterly reliably in the past that the crew's trust in the ship's displayed position was not shaken even as a lookout sighted blue and white water ahead. Minutes later, the ship ran aground on shoals invisible to its radar system.

In the aftermath of the Royal Majesty grounding, integrated bridge systems were modified to more clearly indicate loss of GPS signals, and redundant GPS units became standard. But neither of these safety upgrades would prevent a repeat of the Royal Majesty grounding, or a similar incident, caused by deliberate, strategic GPS deception because there would be no apparent loss of GPS and because primary and backup GPS units would be equivalently affected. In fact, given the termination of LORAN-C, one could argue that, in the face of such an attack, present-day surface vessels would be less secure than the Royal Majesty.

III. Modeling

Consider a simplified ship dynamics model with a conventional track-keeping guidance system as derived in [26]. A conventional track-keeping system attempts to zero the ship's cross-track position using a proportional-integral (PI) controller wrapped around a course autopilot as shown in Fig. 2.

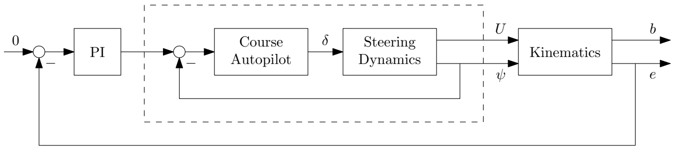


Figure 2. Convetional track-keeping system based on an existing course autopilot system [26].

A. Ship Dynamics

Let the ship's steering dynamics be described by a 1st order Nomoto model,

$$T\dot{r} + r = K\delta + r_{\mathrm{b}},$$

where T is the ship's time constant (s), K is the rudder gain $(1/\mathrm{s})$, δ is the rudder angle (rad), r is the ship's turn rate $(\mathrm{rad}/\mathrm{s})$, and r_{b} is a slowly-varying parameter due to environmental disturbances $(\mathrm{rad}/\mathrm{s})$. The rudder angle δ and rate $\dot{\delta}$ are physically constrained by saturation conditions $|\delta| < \delta_{\max}$ and $\left|\dot{\delta}\right| < \dot{\delta}_{\max}$, respectively, but the controller will be designed such that the rudder angle dynamics will remain linear under typical conditions. The kinematics of the ship are given by

$$\begin{aligned}\dot{\psi} &= r\\ \dot{x} &= U\cos\psi + d_x\\ \dot{y} &= U\sin\psi + d_y,\end{aligned}$$

where U is the ship's speed through water (m/s), d_x and d_y describe errors due to drift caused by slowly-varying environmental disturbances such as ocean currents and wind (m/s), x and y are the ship's northing and easting (m), respectively, and ψ is the ship's heading (rad). Zero heading is defined to be due north with increasing heading clockwise. The environmental disturbance parameters are modeled as a Gauss-Markov process,

$$\begin{aligned}\dot{d}_x &= -\frac{1}{T_d}d_x + v_x\\ \dot{d}_y &= -\frac{1}{T_d}d_y + v_y,\end{aligned}$$

where T_d is the disturbance time constant and v_x and v_y are additive white Gaussian noise (AWGN) sources with intensity σ_d^2 $(\mathrm{m}^2/\mathrm{s}^3)$.

B. Ship Control Law

The ship's course autopilot controls the ship's heading ψ to a desired heading $\psi_{\mathrm{d}} \approx$ constant using a proportional-integral-derivative (PID) control law. In modeling the control laws, the measurements are assumed to be noiseless and continuous since the controller's low bandwidth will filter the high-frequency measurement noise experienced in the real world. The measurements from the gyrocompass and rate-of-turn (ROT) sensor are fed back with a PID law given by

$$\delta\left(t\right) = K_{\mathrm{i}} \int_{0}^{t} \left[\psi_{\mathrm{d}} - \psi\left(\tau\right)\right] d\tau + K_{\mathrm{p}}\left[\psi_{\mathrm{d}} - \psi\left(t\right)\right] - K_{\mathrm{d}} r\left(t\right),$$

where K_{i} is the integral gain, K_{p} is the proportional gain, and K_{d} is the derivative gain. Following the rules of thumb for PID control design of second-order systems in [26, 261], the design parameters are reduced to choosing the natural frequency ω_{n} and relative damping ratio ξ of the closed-loop system. The relative damping ratio is typically chosen in the interval $0.8 \leq \xi \leq 1.0$. The closed-loop bandwidth ω_{b}, defined as

$$\omega_{\mathrm{b}} = \omega_{\mathrm{n}}\sqrt{1 - 2\xi^{2} + \sqrt{4\xi^{4} - 4\xi^{2} + 2}},$$

is chosen such that

$$\frac{1}{T} < \omega_{\mathrm{b}} < \omega_{\delta},$$

where $\omega_{\delta} = \frac{\dot{\delta}_{\max}}{\delta_{\max}}$ is the rudder servo bandwidth. Finally, the PID gains are related to ω_{n} and ξ by

$$\begin{aligned} K_{\mathrm{p}} &= \frac{T}{K}\omega_{\mathrm{n}}^{2} \\ K_{\mathrm{d}} &= \frac{1}{K}\left[2T\xi\omega_{\mathrm{n}} - 1\right] \\ K_{\mathrm{i}} &= \frac{T}{K}\frac{\omega_{\mathrm{n}}^{3}}{10}. \end{aligned}$$

An outer PI control loop for track-keeping is typically wrapped around the course autopilot. In some cases, a human operator in the loop may take the role of the track-keeping, whose control actions can be approximated with a PI controller. The track, typically a rhumb line, can be approximated in the local Cartesian coordinates by a ray, which is parametrized by an angle ψ_0 (rad) and start position x_0 and y_0 (m). Therefore, the along-track and cross-track position, b and e, respectively, are given by

$$\begin{aligned} b &= (x - x_0)\cos\psi_0 + (y - y_0)\sin\psi_0 \\ e &= (y - y_0)\cos\psi_0 - (x - x_0)\sin\psi_0. \end{aligned}$$

Graphically, the relationship between the global and track coordinates are shown in Fig. 3. Under nominal conditions, the measured cross-track position from the GPS receiver is fed back with a PI control law given by

$$\psi_{\mathrm{d}}\left(t\right) = \psi_0 - K_{\mathrm{i}}' \int_{0}^{t} e\left(\tau\right) d\tau - K_{\mathrm{p}}' e\left(t\right),$$

where K_{i}' is the integral gain and K_{p}' is the proportional gain. The gains are chosen so that the inner pointing loop and outer track-keeping loop have some time scale separation, which is typical for marine and aerial vehicles [26], [30]. In that way, $\psi \approx \psi_{\mathrm{d}}$ and the closed-loop cross-track dynamics can be approximated by a first-order system with bandwidth $\omega_{\mathrm{b}}' = UK_{\mathrm{p}}'$, which should be designed to be less than ω_{b}.

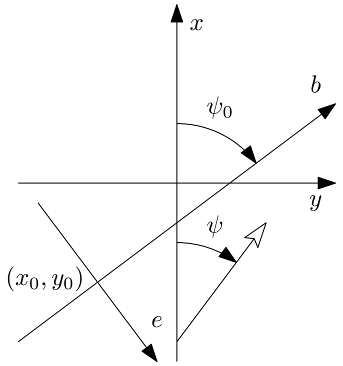


Figure 3. Coordinate systems for ship global position (x, y) and track position (b, e).

C. Spoofer Control Law

In a spoofing attack, the ship's GPS receiver will report the position commanded by the spoofer. To remain covert, the spoofer will typically command positions that are deviations from the ship's true position. Using ship-local coordinates, the deviations can be represented in the along-track and cross-track directions. Clearly, deviations in the cross-track direction will yield an immediate response from the ship's control law. However, the ship will not respond to along-track deviations unless the ship's track changes. An along-track deviation could cause the ship to turn too early or late at a waypoint, which could place the ship onto a trajectory into hazardous waters. Although along-track spoofing is quite dangerous, it requires more planning and knowledge of the ship's route. The sequel will focus on a cross-track spoofing control law that can place the ship covertly onto a cross-track position that the spoofer commands.

In a cross-track spoofing attack, the spoofer generates a GPS signal with the ship's actual along-track position b and a spoofed cross-track position e_{s}. The spoofer-generated cross-track position e_{s} is written as the difference of two parts, the ship's true cross-track position e and a spoofer-induced cross-track modulation e_{m} so that $e_{\mathrm{s}} = e - e_{\mathrm{m}}$. Note, that the spoofer operator must be able to track the ship's position and infer the rhumb line the ship is tracking in order to determine the ship's true cross-track position e. The assumption is not particularly restrictive since many transoceanic ships use a waypoint-based route planning provided by the ECDIS. The waypoints are connected by straight lines, except during track change manuevers, which can be detected by the attacker. A radar system operated by the attacker can determine the ship's true position.

The goal of the attacker is to force the ship to track a spoofer-commanded cross-track position $\bar{e}$ as quickly as possible without being detected. An intuitive heuristic for the covertness constraint limits the magnitude of the spoofer-induced velocity and acceleration for all time

$$
\begin{aligned}
|\dot{e}_{\mathrm{m}}(t)| &\leq v_{\max} \\
|\ddot{e}_{\mathrm{m}}(t)| &\leq u_{\max}.
\end{aligned}
\tag{1}
$$

Solving the minimum-time optimal-control problem posed in (2) yields the cross-track modulation time history $e_{\mathrm{m}}(t)$ that achieves the spoofer's goal.

$$
\begin{aligned}
\min_{u(t)} \quad & t_{\mathrm{f}} \\
\text{s. t.} \quad & \ddot{e}_{\mathrm{m}}(t) = u(t) \\
& e_{\mathrm{m}}(0) = 0, \dot{e}_{\mathrm{m}}(0) = 0 \\
& e_{\mathrm{m}}(t_{\mathrm{f}}) = \bar{e}, \dot{e}_{\mathrm{m}}(t_{\mathrm{f}}) = 0 \\
& (1)
\end{aligned}
\tag{2}
$$

Note that it is assumed that the ship's control law has enough bandwidth to track the cross-track modulation, which can be ensured by choosing sufficiently small $v_{\max}$ and $u_{\max}$. In addition, because of the open-loop nature of the modulation, the ship may not reach the spoofer-desired position due to small errors in the estimated rhumb line and position. A closed-loop feedback control law could be used to compensate for the uncertainty in the ship's position and route, but such a controller would be less covert in a similar manner to unmanned aerial vehicle (UAV) spoofing shown in [17].

IV. Spoofing Detection Framework

The detection framework developed in this paper attempts to minimize the integrity risk I_R for a given continuity risk C_R. This framework borrows concepts from GPS integrity monitoring in aviation applications and the fault-detection literature, which are applied here to the "fraud-detection" problem. As noted by Joerger, fault-detection methods typically tend to focus on minimizing time-to-detect without regard to integrity risk [31]. Typically, the integrity and continuity risk are specified in terms of the probability of hazardously misleading information (HMI) per approach and the false-alarm rate (which is the inverse of the mean time between false alarms M_F), respectively. In the maritime case, an approach represents some leg or legs of a journey such as the final approach to a harbor, where time $t = 0$ indicates the beginning of the approach. In the framework, for each time $t(k) = kT_s$ for integers $k > 0$, a detection test decides between two hypotheses—a null hypothesis H_0 indicating nominal operating conditions, and an alternative hypothesis H_1 indicating a spoofing attack is underway. At the beginning of the approach, the null hypothesis is assumed to be true, and at some later time t_0, a transition to the alternative hypothesis occurs, although a transition is not necessarily guaranteed to occur during the approach. Additionally, if a spoofing attack begins, it is assumed the attack will continue until either hazardous conditions occur or the attack is detected. In this framework, the time between tests T_s is assumed to be constant, and is the primary tuning parameter for the integrity optimization problem. Furthermore, the detection framework is completely separate from the ship's control law, which will accept spoofed measurements at a rate potentially much faster than $1/T_s$. The authors suspect that in practice captains would prefer a detection module that does not interfere with the ship's off-the-shelf controller over a joint control-detection framework with potentially better performance.

The detection statistic $q(k)$ must remain below a threshold in order to assume the null hypothesis. Otherwise, the alternative hypothesis is assumed and the continuity of the approach is broken as the crew attempts to neutralize the potential spoofing threat. The threshold λ satisfies

$$
P(q(k) > \lambda | H_0) = \frac{T_s}{M_F} = C_R T_s
$$

to maintain the prescribed false-alarm rate. Note that the probability distribution of the detection statistic under the null hypothesis, and therefore λ, is independent of the time index k. In integrity monitoring, hazardous conditions occur when the absolute value of the estimation error ϵ exceeds a threshold L (referred to as navigation system error in aviation). In the maritime case, a reasonable value for L may be 1 km, although L must be smaller than the minimum distance that the ship's route clears charted hazards to account for worst-case control error (referred to flight technical error in aviation). Although, the ship may not immediately be in danger if $|\epsilon| > L$, control decisions based on such poor (divergent) estimates will likely cause hazardous conditions. Assuming GPS measurements are continuously available as in the previously developed model for the ship control law, note that under spoofing

$$
\epsilon = e_{\mathrm{s}} - e = -e_{\mathrm{m}}.
$$

Note that if the ship must revert to dead reckoning due to loss of GPS, then the variance of the estimation error will grow without bound and ϵ must be treated as a random variable that is also potentially correlated with the detection statistic q. As previously mentioned, sophisticated spoofing attacks that induce along-track estimation errors to cause the ship to turn early or late in a multi-leg journey are possible to implement, but only cross-track attacks are considered in this analysis.

A "local" HMI event $E(t)$ for $t \geq t_0$ is defined as hazardous conditions under a spoofing attack that has not been detected. Mathematically, $E(t)$ can be expressed as

$$
E(t) = |e_{\mathrm{m}}(t)| > L \wedge \left(\bigwedge_{t_0 < kT_s < t} q(k) < \lambda \right).
$$

Then, the event E that considers if HMI occurred at any time during an approach for a given t_0 is given by

$$
E = \bigvee_{t \geq t_0} E(t).
$$

If the first time hazardous conditions occur under a spoofing attack is given by t_L, then E can be reformulated as

$$
E = \bigwedge_{t_0 < kT_s < t_L} q(k) < \lambda.
$$

All spoofing start times are assumed to be equally likely, and due to the periodic nature of sampling the detection statistic, the probability of HMI is given by

$$
I_R = \int_0^1 P\left(E | t_0 = \beta T_s\right) d\beta.
$$

The detection statistic $q(k)$ is based on the innovation sequence $\nu(k)$ generated by a Kalman filter ingesting infrequent GPS measurements. In order to compute the integrity risk, a simplified model for the Kalman filter is developed to determine the probability distribution of $q(k)$. First, consider the continuous-time ship dynamics model

$$\dot{\eta}(t) = A\eta(t) + Bu(t) + Ev(t),$$

where

$$\begin{aligned}
&\eta = \begin{bmatrix} x & y & d_x & d_y \end{bmatrix}^{\mathrm{T}} \text{ is the state vector,}\\
&A = \begin{bmatrix} 0 & I \\ 0 & -\frac{1}{T_d}I \end{bmatrix}, B = \begin{bmatrix} I \\ 0 \end{bmatrix}, E = \begin{bmatrix} 0 \\ I \end{bmatrix},\\
&u = U\begin{bmatrix} \sin\psi & \cos\psi \end{bmatrix}^{\mathrm{T}} \text{ is the control, and}\\
&v = \begin{bmatrix} v_x & v_y \end{bmatrix}^{\mathrm{T}} \text{ is AWGN with intensity } Q_c = \sigma_d^2 I.
\end{aligned}$$

Similarly, the potentially-spoofed GPS measurements are sampled from

$$z(k) = H\eta(kT_s) - z_{\mathrm{m}}(kT_s) + w(k),$$

where w is discrete AWGN with covariance $R = \sigma_p^2 I$, $H = \begin{bmatrix} I & 0 \end{bmatrix}$, and z_{m} is the spoofer-induced position modulation. Note that this model is similar to the complementary filter used in GPS/INS integration, where the disturbance parameters d_x and d_y are analogous to IMU biases in their modeling as a Gauss-Markov process [32]. By definition, also note that $z_m(t)$ is zero for $t < t_0$. Now, consider the *a priori* and *a posteriori* estimation error of the Kalman filter, $\bar{\epsilon}(k)$ and $\epsilon(k)$, respectively. The innovation $\nu(k)$ at time $t(k)$ is given by

$$\nu(k) = w(k) - z_{\mathrm{m}}(kT_s) - H\bar{\epsilon}(k).$$

The recursion equations for the estimation error's mean and covariances $\bar{P}$ and P are given by

$$\begin{aligned}
\mathbb{E}\left[\bar{\epsilon}(k)\right] &= F\mathbb{E}\left[\epsilon(k-1)\right]\\
\bar{P}(k) &= FP(k-1)F^{\mathrm{T}} + Q\\
\mathbb{E}\left[\epsilon(k)\right] &= (I - K(k)H)\mathbb{E}\left[\bar{\epsilon}(k)\right] - K(k)z_{\mathrm{m}}(kT_s)\\
P(k) &= (I - K(k)H)\bar{P}(k),
\end{aligned}$$

where

$$\begin{aligned}
F &= e^{AT_s},\\
Q &= \int_0^{T_s} e^{A\tau}EQ_cE^{\mathrm{T}}e^{A^{\mathrm{T}}\tau}d\tau,\\
S(k) &= H\bar{P}(k)H^{\mathrm{T}} + R,\\
K(k) &= \bar{P}(k)H^{\mathrm{T}}S^{-1}(k), \text{ and}\\
\mathbb{E}\left[\bar{\epsilon}(0)\right] &= 0.
\end{aligned}$$

In the sequel, it is assumed that the estimation error covariances have reached their steady-state values (which can be found by solving a discrete-time algebraic Riccati equation), and the index k is dropped from P, $\bar{P}$, S, and K. Note that under a spoofing attack, the estimation error and innovation are no longer unbiased.

One choice for the detection statistic is the normalized innovation squared (NIS) given by $q(k) = \nu^{\mathrm{T}}(k)S^{-1}\nu(k)$. NIS is a simple but common statistic used for detecting measurements that are inconsistent with an assumed dynamics and measurement model [32]. However, no claims are made regarding the optimality of NIS for this detection problem. Under H_0, the statistic is distributed as χ^2 with two degrees of freedom. However, under H_1, the statistic is distributed as non-central χ^2 with two degrees of freedom and non-centrality parameter $\delta(k) = \bar{\nu}^{\mathrm{T}}(k)S^{-1}\bar{\nu}(k)$, where

$$\bar{\nu}(k) = -\left(z_m(kT_s) + H\mathbb{E}\left[\bar{\epsilon}(k)\right]\right)$$

is the mean of innovation at index k. Since the innovation sequence is white, each detection test is independent. Varying T_s and $v_{\max}$ from 0.1 m/s to 1 m/s yields the integrity risk shown in Fig. 4.

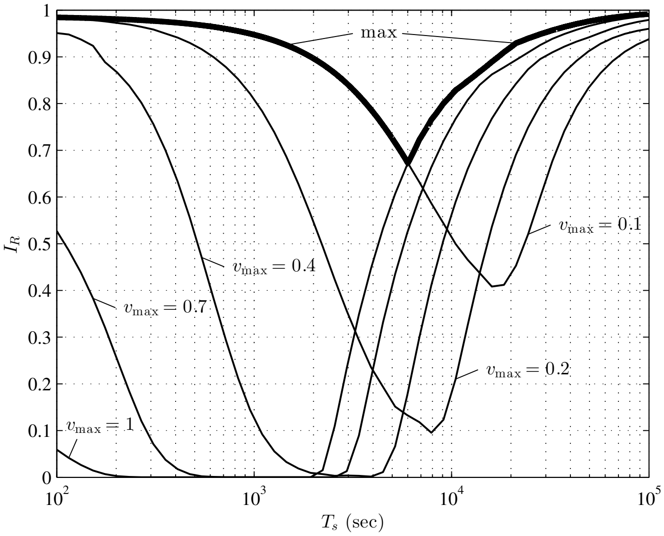


Figure 4. Integrity risk I_R vs. sampling time T_s for various choices of $v_{\max}$. The optimal sampling time $T_s^\star$ that minimizes the worst-case integrity risk is approximately 100 minutes, yielding $I_R^\star \approx 0.6727$. Note that the worst-case attack is given by either $v_{\max} = 0.1$ or 1 m/s. Other parameters are $u_{\max} = 0.03$ m/s^2, $M_F = 1$ month, $\bar{e} \gg L = 3$ km, $\sigma_p = 6$ m, $T_d = 200$ s, and $\sigma_d = 0.02$ m/s$^{1.5}$.

For a particular $v_{\max}$, there is an optimal value for the sampling time T_s that minimizes the integrity risk. Intuitively, if T_s is too small, then $\delta(k)$ and, hence, the probability of detection per test is small. However, if T_s is too large, even though the probability of detection per test is large, hazardous conditions will likely occur before a test is conducted (i.e. $t_L - t_0 \ll T_s$). Given that the crew will not know exactly what $v_{\max}$ and $u_{\max}$ the attacker has chosen, a robust optimizer for the sampling time would be

$$\min_{T_s} \max_{\substack{v_{\max}\in\mathbb{V}\\ u_{\max}\in\mathbb{U}}} I_R,$$

where $\mathbb{V}$ and $\mathbb{U}$ are sets containing reasonable values for the attack parameters. The sets $\mathbb{V}$ and $\mathbb{U}$ will typically contain a bounded subset of real numbers. The framework as presented currently assumes an approach takes an infinite amount of time to allow averaging the integrity risk over a single sample interval T_s. Therefore, $v_{\max}$ is bounded from below assuming the attacker wishes to cause hazardous conditions before the end of a typical approach. In other words, if the average duration of an approach is $\bar{T}_{\mathrm{app}}$, then $v_{\max} \geq L/\bar{T}_{\mathrm{app}} \approx 0.1$ m/s, reasonably assuming a linear relationship between the approach's protection level and average duration. In addition, induced velocities greater than 1 m/s would lead to physically impossible set and drift values that are not captured by the Gauss-Markov disturbance model and break the small control error assumption, placing an upper bound on $v_{\max}$. Lastly, the impact of the acceleration regime of the attack is diminished for large enough T_s since the regime only occurs for a short period of time in the beginning of the attack. Therefore, the integrity risk optimization is not particularly sensitive to the choice of $u_{\max}$, which is fixed to a value of 0.03 m/s^2 for the rest of the analysis. The minimax results for a couple of example scenarios are shown in Figs. 5 and 6.

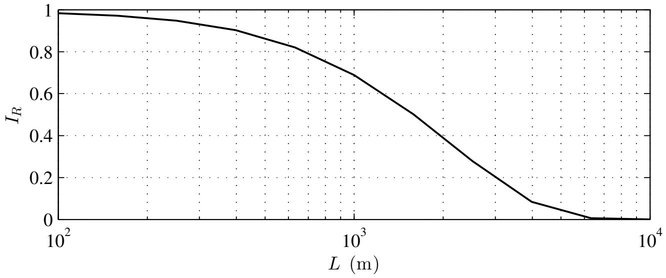


Figure 5. Minimax integrity risk $I_R^{\star}$ vs. the hazardous condition threshold L. For $L \leq 400$ m, the worst-case attack will likely cause HMI since $I_R^{\star} > 0.9$. On the other hand, $L \geq 7$ km maintains an integrity risk near zero for any reasonable attack. Other parameters are set to the values indicated in Fig. 4.

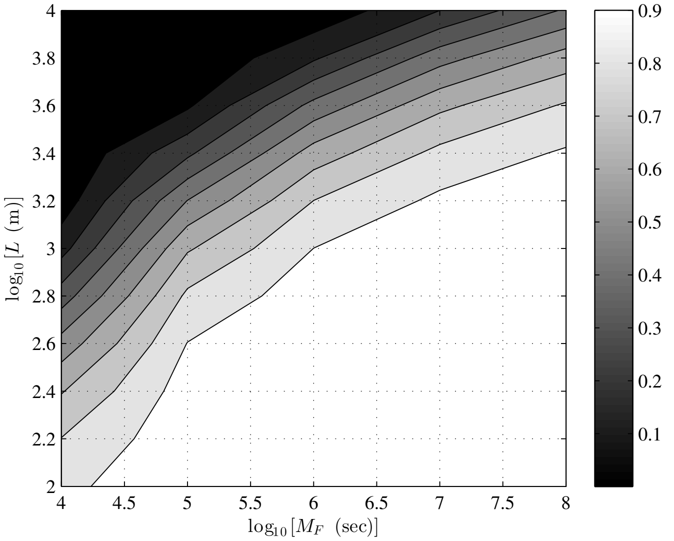


Figure 6. Minimax integrity risk $I_R^{\star}$ vs. L and M_F. Depending on the protection level and continuity risk requirements of the approach, the detection framework will maintain an integrity risk that can be either quite high (white region), in which covert attacks are possible, or quite low (black region). Other parameters are set to the values indicated in Fig. 4.

V. Simulation

The spoofer control law and integrity risk calculation were verified with Monte-Carlo simulations. The simulations take into account the Nomoto ship model, closed-loop ship controller, and open-loop spoofer controller developed in Sec. III. A couple of representative ship trajectories are shown in Fig. 7. The simulation-based integrity risk is determined by counting the number of HMI events over 100 sampling phases per simulation and 20 simulations per attack profile. As shown in Fig. 8, the simulation-based integrity risk for different values of $v_{\max}$ agrees quite well with the values predicted by the theory developed in Sec. IV.

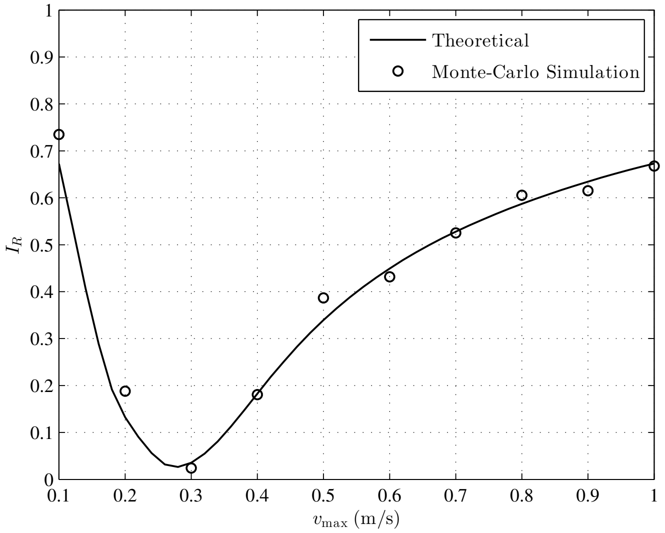


Figure 8. Theoretical vs. simulated integrity risk for different values of $v_{\max}$. Other parameters are set to the values indicated in Fig. 4.

VI. Experiment

Covert control of a marine vessel by GPS spoofing was demonstrated in the Mediterranean sea in the summer of 2013. The authors were invited to conduct the unprecedented experiment aboard the White Rose of Drachs, a 65-meter superyacht. The experimental setup centered on the receiver-spoofer developed at the University of Texas at Austin [17]. The spoofer receives the authentic signals from an antenna placed in the stern. The spoofer transmits the false navigation signals towards the bow, where the ship's GPS antennas are located as shown in Fig. 9.

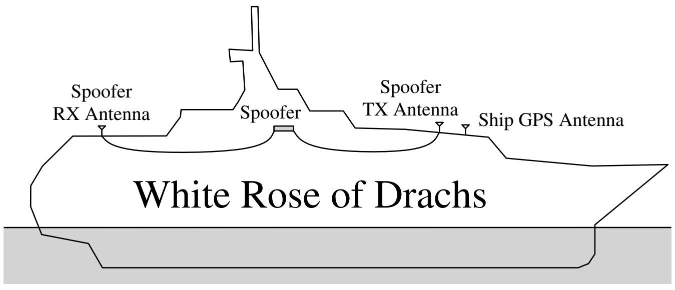
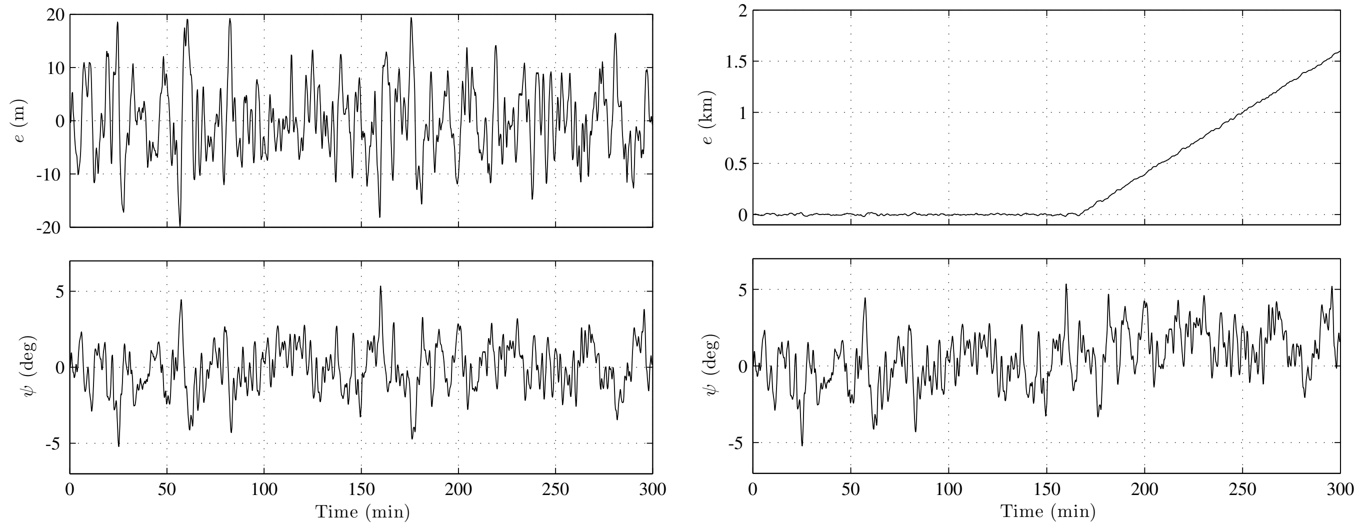


Figure 9. Sketch of the spoofer setup on the White Rose of Drachs.

Once a safe route is established, the captain attempts to maintain the ship's reported position along a series of rhumb lines within some prescribed corridor. Control actions at sea



(a) Case I, no spoofing

(b) Case II, $v_{\max} = 0.2$ m/s

Figure 7. Trajectory resulting from simulation of ship dynamics under nominal conditions and a spoofing attack. Model parameters are given by $T = 39.94$ s, $K = 0.211\ \mathrm{s}^{-1}$, $U = 8.23$ m/s, $K_{\mathrm{p}} = 1.4415$, $K_{\mathrm{i}} = 0.0126$, $K_{\mathrm{d}} = 21.6904$, $K'_{\mathrm{p}} = 0.0028$, $K'_{\mathrm{i}} = 1.8949 \times 10^{-5}$. Other parameters are set to the values indicated in Fig. 4.

are required to maintain course due to disturbances such as wind and ocean currents, which are typically not measured directly. Instead, the disturbance sources are lumped together, and measured indirectly through the GPS. Therefore, a spoofing attack can induce false disturbances, causing the captain to believe the ship is on course, when in reality, the ship is slowly drifting off course. In the aforementioned experiment, a spoofer-induced velocity was introduced in the cross-track direction—at first 0.5 m/s, then increased to 2 m/s, and finally reset to zero. The spoofer-induced acceleration in the first velocity change was $0.03\ \mathrm{m/s^2}$, while for all other changes the acceleration was $0.1\ \mathrm{m/s^2}$. Note that the maximum spoofer-induced velocity and acceleration exceed the limits assumed in Sec. IV in order to reduce the duration of the experiment. As the captain performed typical correction maneuvers to maintain the spoofed trajectory within a ± 200 m corridor, the actual ship's position deviated along a parallel track as shown in Fig. 10 and 11.

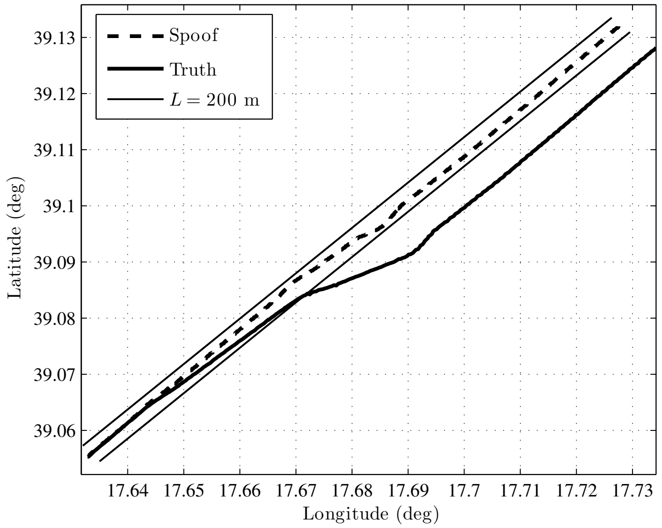


Figure 10. Comparison of the ship's reported position and the ship's actual position during a spoofing attack. The thin solid lines indicate ± 200 m cross-track deviation.

The ship's reported position and heading were logged to a file during the spoofing attack. Unfortunately, the ship's Doppler log was not functional, but the ship's engine throttle control was set to Full Ahead, so the ship's speed through water U is assumed to be a nominal 15 knots. The logged measurements are fed post-facto into the innovations-based spoofing detection framework developed in Sec. IV. In order to determine the optimal sampling time $T_s^\star$ for the experiment, many of the same parameter values indicated in Fig. 4 were used, except $0.5\ \mathrm{m/s} < v_{\max} < 2\ \mathrm{m/s}$ and $L = 200$ m. Even though the ship was traveling in open waters, the narrow corridor was chosen to reduce the time scale of the experiment from hours to minutes, and could potentially represent approaches to harbors with many surrounding hazards. The resulting minimax optimization yields $T_s^\star \approx 250$ s and integrity risk $I_R^\star = 0.8956$ for the worst-case attacks. The first phase of the actual attack, while $|z_{\mathrm{m}}| \leq 200$ m, is a worst-case attack and remains covert with respect to the detection framework. The second phase of the attack is significantly less covert assuming $L = 700$ m, $u_{\max} = 0.1\ \mathrm{m/s^2}$, and $v_{\max} = 2$ m/s, which yields a theoretical integrity risk of $I_R = 0.0067$, although the actual integrity risk is different due to the change in the spoofer-induced velocity in the middle of the attack. The NIS values generated by the detection framework for the experimental data with five different sampling phases are shown in Fig. 12. Recall that the integrity risk computed previously is the marginal risk over uniformly distributed sampling phases. A realization for a particular sampling phase leads to HMI if the associated NIS values never cross the

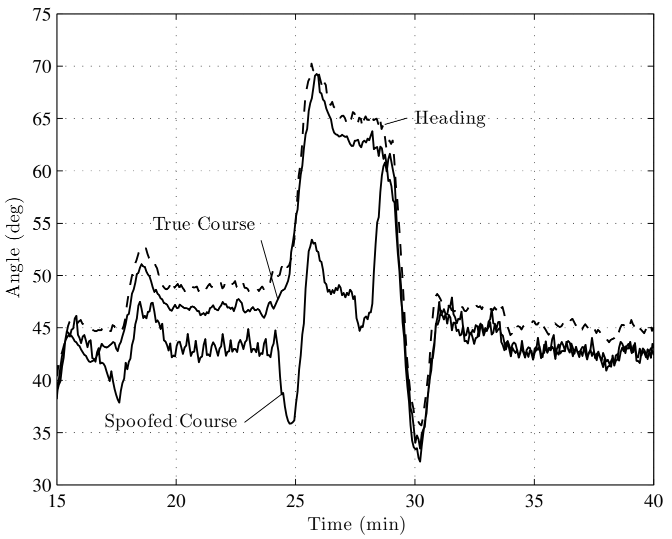


Figure 11. Comparison of the ship's heading, spoofed course, and true course during a spoofing attack. Course is defined as the direction of the ship's velocity over ground vector with respect to North.

detection threshold λ after the spoofing attack begins and before the attack leads to hazardous conditions. The shaded detection regions for the two phases of the attack are indicated in Fig. 12.

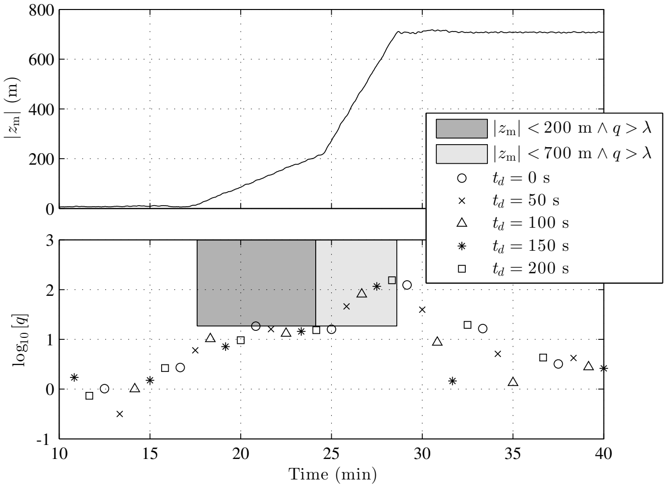


Figure 12. NIS values generated by the detection framework with a sampling time $T_s = 250$ s for the experimental data collected on the White Rose of Drachs during a spoofing attack. NIS time history for five different sampling phases and shaded detection regions are shown.

VII. Strategies for Mitigating Surface Vessel Vulnerability to GNSS Deception

A number of promising methods are currently being developed to defend against civil GNSS deception attacks. These can be categorized as (1) receiver-autonomous signal-processing-oriented techniques, which require no antenna motion or specialized antenna hardware [33]–[37]; (2) receiver-autonomous antenna-oriented techniques, which require antenna motion or specialized antenna hardware [38]–[40]; (3) cryptographic techniques that require signal specification modifications to overlay unpredictable but verifiable modulations on existing or future civil GNSS signals [41], [42]; and (4) techniques that exploit the existing encrypted military signals to offer civil GPS signal authentication for networked GPS receivers [43]–[46]. Among these methods, the dual-antenna technique described in [39] seems an especially promising option for maritime protection because (1) it could be implemented in the near term, and (2) its chief drawbacks relative to the other techniques—larger size and higher cost—are not so critical for marine vessels as they are for handheld devices and small unmanned aerial vehicles, for example. Nonetheless, it will take years before this or other techniques mature and are implemented on a wide scale. Meanwhile, there are no off-the-shelf defenses against GNSS spoofing.

VIII. Conclusions

A detection framework has been developed to detect spoofing attacks in maritime environments based solely on Doppler log, gyrocompass, and potentially-spoofed GPS measurements. Although more sophisticated spoofing detection techniques such as the dual-antenna defense are much more effective, the framework was developed to be easily implementable in ECDIS software currently available on all ships. The framework is based on a dynamics model that captures the essential features of the environmental disturbances such as ocean currents and wind. Although this paper focused on the maritime dynamics model, the framework can be easily applied to an inertial measurement unit or clock model, which both have drift parameters governed by Gauss-Markov processes, but is left for future work. The paper derived the performance of the detection framework, which is captured by the integrity risk or probability of HMI. The sampling time of the framework was optimized by minimizing the maximum integrity risk given a set of possible attack profiles. Just as aviation has developed rigorous integrity risk standards for GPS faults, maritime regulatory authorities can use the detection framework analysis to compute the best possible integrity risk given reasonable values for real-world disturbance and attack parameters and the minimum acceptable continuity risk. Lastly, Monte-Carlo simulations verified the theoretical integrity risk of the detection framework and an unprecedented experiment demonstrated the feasibility of conducting a spoofing attack on an actual vessel.

Acknowledgements

The authors thank the crew of the White Rose of Drachs and her captain, Andrew Schofield, for supporting the GPS spoofing experiment.

References

[1] John A. Volpe National Transportation Systems Center, "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," 2001.

[2] A. Grant, "GPS jamming and the impact on maritime navigation," *Journal of Navigation*, vol. 62, no. 2, 2009.

[3] U. Kroener and F. Dimc, "Hardening of civilian GNSS trackers," in *Proceedings of the 3rd GNSS Vulnerabilities and Solutions Conference*. Krk Island, Croatia: Royal Institute of Navigation, Sept. 2010.

[4] International Marine Contractors Association, "Guidelines for the design and operation of dynamically positioned vessels," 2007, http://www.imca-int.com/media/73055/imcam103.pdf.

[5] M. Thomas, J. Norton, A. Jones, A. Hopper, N. Ward, P. Cannon, N. Ackroyd, P. Cruddace, and M. Unwin, "Global navigation space systems: reliance and vulnerabilities," *The Royal Academy of Engineering, London*, 2011.

[6] M. Caccia, M. Bibuli, R. Bono, and G. Bruzzone, "Basic navigation, guidance and control of an unmanned surface vehicle," *Autonomous Robots*, vol. 25, no. 4, pp. 349–365, 2008.

[7] L. Elkins, D. Sellers, and W. R. Monach, "The autonomous maritime navigation (AMN) project: Field tests, autonomous and cooperative behaviors, data fusion, sensors, and vehicles," *Journal of Field Robotics*, vol. 27, no. 6, pp. 790–818, 2010.

[8] L. Paull, S. Saeedi, M. Seto, and H. Li, "AUV navigation and localization: A review," *Oceanic Engineering, IEEE Journal of*, vol. 39, no. 1, pp. 131–149, 2014.

[9] D. E. Di Massa and W. Stewart Jr, "Terrain-relative navigation for autonomous underwater vehicles," in *OCEANS'97. MTS/IEEE Conference Proceedings*, vol. 1. IEEE, 1997, pp. 541–546.

[10] D. K. Meduna, S. M. Rock, and R. S. McEwen, "Closed-loop terrain relative navigation for auvs with non-inertial grade navigation sensors," in *Autonomous Underwater Vehicles (AUV), 2010 IEEE/OES*. IEEE, 2010, pp. 1–8.

[11] D. Meduna, S. M. Rock, and R. McEwen, "AUV terrain relative navigation using coarse maps," in *Unmanned Untethered Submersible Technology Conference*, 2009.

[12] U.S. Coast Guard; U.S. Department of Homeland Security, "Terminate long range aids to navigation (Loran-C) signal," Federal Register, Jan. 2010.

[13] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS Meeting*. Savannah, GA: Institute of Navigation, 2008.

[14] D. Shepard and T. E. Humphreys, "Characterization of receiver response to a spoofing attack," in *Proceedings of the ION GNSS Meeting*. Portland, Oregon: Institute of Navigation, 2011.

[15] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," in *Proceedings of the ION GNSS Meeting*, 2012.

[16] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146–153, 2012.

[17] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[18] J. J. Spilker, Jr., *Global Positioning System: Theory and Applications*. Washington, D.C.: American Institute of Aeronautics and Astronautics, 1996, ch. 3: GPS Signal Structure and Theoretical Performance, pp. 57–119.

[19] GPS Directorate, "Systems engineering and integration Interface Specification IS-GPS-200G," 2012, http://www.gps.gov/technical/icwg/.

[20] European Union, "European GNSS (Galileo) open service signal in space interface control document," 2010, http://ec.europa.eu/enterprise/policies/satnav/galileo/open-service/.

[21] N. Bowditch, *The American Practical Navigator*. Bethesda, Maryland: National Imagery and Mapping Agency, 2002.

[22] Sperry Marine, "NG Introduces New Technology Satellite Compass System," June 2003, http://www.sperrymarine.com/news/ng-introduces-new-technology-satellite-compass-system.

[23] GPS World staff, "Hemisphere GPS Offers Vector Compass Products for Marine Applications," *GPS World*, Oct. 2012, http://gpsworld.com/hemisphere-gps-offers-vector-compass-products-for-marine-applications.

[24] *Radar Navigation and Maneuvering Board Manual*, 7th ed. Bethesda, Maryland: National Imagery and Mapping Agency, 2001, ch. 5, http://msi.nga.mil/MSISiteContent/StaticFiles/NAV_PUBS/RNM/310ch5.pdf.

[25] "Totem ECDIS and GPS Spoofing," *eNav International*, June 2013, http://www.enav-international.com/news/id5774-Totem_ECDIS_and_GPS_Spoofing.html.

[26] T. I. Fossen, *Guidance and Control of Ocean Vehicles*. New York: John Wiley and Sons, 1994.

[27] National Transportation Safety Board, "Marine accident report: Grounding of the Panamanian passenger ship Royal Majesty on Rose and Crown Shoal near Nantucket, Massachusetts June 10, 1995," National Transportation Safety Board, Tech. Rep., 1997.

[28] M. H. Lützhöft and S. W. Dekker, "On your watch: Automation on the bridge," *Journal of Navigation*, vol. 55, no. 1, pp. 83–96, 2002.

[29] B. Schager, "When technology leads us astray: a broadened view of human error," *Journal of Navigation*, vol. 61, no. 1, p. 63, 2008.

[30] F. Kendoul, "Survey of advances in guidance, navigation, and control of unmanned rotorcraft systems," *Journal of Field Robotics*, vol. 29, no. 2, pp. 315–378, 2012.

[31] M. Joerger and B. Pervan, "Kalman filter-based integrity monitoring against sensor faults," *Journal of Guidance Control Dynamics*, vol. 36, pp. 349–361, 2013.

[32] Y. Bar-Shalom, X. R. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation*. New York: John Wiley and Sons, 2001.

[33] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing module for legacy civil GPS receivers," in *Proceedings of the ION International Technical Meeting*, San Diego, CA, Jan. 2010.

[34] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proceedings of the ION GNSS Meeting*, Portland, OR, 2011.

[35] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/N_0 estimates," in *Proceedings of the ION GNSS Meeting*. Nashville, Tennessee: Institute of Navigation, 2012.

[36] K. D. Wesson, B. L. Evans, and T. E. Humphreys, "A combined symmetric difference and power monitoring GNSS anti-spoofing technique," in *IEEE Global Conference on Signal and Information Processing*, 2013.

[37] K. D. Wesson, T. E. Humphreys, and B. L. Evans, "Receiver-autonomous GPS signal authentication based on joint detection of correlation profile distortion and anomalous received power," 2014, (in preparation).

[38] D. S. D. Lorenzo, J. Gautier, J. Rife, P. Enge, and D. Akos, "Adaptive array processing for GPS interference rejection," in *Proceedings of the ION GNSS Meeting*. Long Beach, CA: Institute of Navigation, Sept. 2005.

[39] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "A multi-antenna defense: Receiver-autonomous GPS spoofing detection," *Inside GNSS*, vol. 4, no. 2, pp. 40–46, April 2009.

[40] A. Broumandan, A. Jafarnia-Jahromi, V. Dehgahanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," in *Proceedings of the IEEE/ION PLANS Meeting*. Myrtle Beach, SC: Institute of Navigation, April 2012.

[41] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navigation, Journal of the Institute of Navigation*, vol. 59, no. 3, pp. 177–193, 2012.

[42] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, 2013.

[43] S. Lo, D. DeLorenzo, P. Enge, D. Akos, and P. Bradley, "Signal authentication," *Inside GNSS*, vol. 0, no. 0, pp. 30–39, Sept. 2009.

[44] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, and T. E. Humphreys, "Civilian GPS spoofing detection based on dual-receiver correlation of military signals," in *Proceedings of the ION GNSS Meeting*. Portland, Oregon: Institute of Navigation, 2011.

[45] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, and T. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2250–2267, 2013.

[46] B. O'Hanlon, M. Psiaki, J. Bhatti, and T. Humphreys, "Real-time spoofing detection using correlation between two civil GPS receiver," in *Proceedings of the ION GNSS Meeting*. Nashville, Tennessee: Institute of Navigation, 2012.