آشکارسازی حمله جعل داده در سیستم ناوبری ترکیبی اینرسی– ماهواره‌ای با آزمون نسبت احتمال حاشیه‌ای

تاریخ دریافت: ۱۴۰۴/۰۳/۱۰
تاریخ پذیرش: ۱۴۰۴/۱۱/۱۲

محسن شادمهری [۱]، رضا محبوبی اسفنجانی [۲]
۱ دانشجوی دکتری، دانشکده مهندسی برق وکامپیوتر، دانشگاه صنعتی سهند، تبریز، ایران
۲ استاد تمام، دانشکده مهندسی برق وکامپیوتر، دانشگاه صنعتی سهند، تبریز ، ایران، mahboobi@sut.ac.ir

چکیده

در ناوبری ترکیبی اینرسی- ماهواره ای (GNSS/INS)، سیستم‌های ناوبری ماهواره‌ای و اینرسی یکپارچه می‌شوند تا دقت سیستم ناوبری ارتقا یابد. اما، در این ترکیب مهاجم می‌تواند داده‌های ناوبری ماهواره‌ای را جعل کند تا موقعیت نادرستی به سیستم ناوبری القا کند. در این مقاله، با استفاده از آزمون نسبت احتمال حاشیه‌ای (MLRT) یک آشکارساز جدید برای حملهٔ جعل داده در سیستم ناوبری ترکیبی GNSS/INS با تزویج سست ارائه می شود. در روش MLRT، برای محاسبهٔ نسبت احتمال، پارامترهای مزاحم تصادفی به جای تخمین، از طریق حاشیه‌سازی حذف می‌شوند و در نتیجه، آزمون در برابر خطاهای مدل‌سازی مقاوم‌تر است. درقیاس با روش های موجود، با استفاده از آزمون نسبت احتمال حاشیه‌ای، نیاز به تعیین آستانه توسط طراح برای آشکارسازی حمله مرتفع می شود. نتایج شبیه‌سازی نشان می‌دهد که در رویکرد پیشنهادی، تاخیر آشکارسازی در برابر یک حمله چالشی که در آن مسیر جعلی به آرامی از مسیر واقعی منحرف می‌شود، نسبت به روش‌های رقیب، بسته به سناریوی حمله تا حدود پنجاه درصد کمتر است.

واژه‌های کلیدی: *ناوبری ترکیبی، جعل داده، آشکارساز حمله، نسبت احتمال حاشیه‌ای.*

Spoofing attack detection in integrated GNSS/INS navigation systems using marginalized likelihood ratio test

Mohsen Shadmehri1, Reza Mahboobi Esfanjani 2
1- Ph.D. Student, Department of Electrical and Computer Engineering, Sahand University of Technology, Tabriz, Iran.
2- Professor, Department of Electrical and Computer Engineering, Sahand University of Technology, Tabriz, Iran.

Abstract
In integrated inertial-satellite navigation (GNSS/INS), complementary characteristics of Global Navigation Satellite System (GNSS) and Inertial Navigation System (INS) are combined with together to enhance navigation acuracy. However, a malicious attacker can spoof satellite navigation data to induce a false position into the victim's navigation system. In this paper, for the case that counterfeit signals bypass signal-based attack detectors employed in the GNSS receiver, a novel spoofing attack detector for loosely coupled GNSS/INS systems is developed using the Marginalized Likelihood Ratio Test (MLRT), in which, instead of estimating nuisance random parameters, they are eliminated through marginalization. Compared to existing approaches, using MLRT removes the need for manually setting a detection threshold and also improves robustness against system model uncertainties. Simulation results in MATLAB demonstrate that, under a challenging attack scenario where the spoofed path gradually diverges from the true one, the proposed approach achieves a shorter detection delay, up to fifty percent compared to rival methods.
Keywords: *integrated GNSS/INS navigation, spoofing, attack detector, marginalized likelihood ratio.*

۱. مقدمه

در ناوبری ترکیبی GNSS/INS، سیستم‌های ناوبری ماهواره‌ای و اینرسی یکپارچه می‌شوند تا ناوبری دقیق‌تری حاصل شود. رایج‌ترین ساختار یکپارچه‌سازی، تزویج سست[1] نامیده می‌شود که در آن، داده‌های ماهواره برای ساخت بردار اندازه‌گیری مکمل برای استفاده در فیلتر تلفیق داده مورد استفاده قرار می‌گیرند. یک فیلتر کالمن خطاهای سیستم ناوبری اینرسی را تخمین می‌زند تا بر اساس آن خطاها تصحیح شوند [۱].

با این وجود، داده‌های سیستم ناوبری جهانی ماهواره‌ای در معرض حملات مخرب قرار دارند. در حملهٔ جعل[2] داده، مهاجم با ارسال سیگنال‌های فریب، گیرنده را گمراه می‌کند تا خروجی ناوبری نادرست تولید شود. مهاجم، سیگنال اصلی را با توان بالاتر تقلید می‌کند تا از آشکارسازهای مخابراتی حمله که در سطح سیگنال در گیرنده عمل می‌کنند، عبور کند [۲]. اخیراً روش‌هایی برای آشکارسازی حملات جعل بر پایه تخمینگرها، خصوصا فیلتر کالمن توسعه یافته‌اند که در سطح داده، ناسازگاری اطلاعات ناوبری ماهواره‌ای و ناوبری اینرسی را به صورت آماری بررسی می‌کنند.

لیو و همکاران، تأثیرات جعل داده در سیستم ناوبری یکپارچه را تحلیل و نشان داده‌اند که خواص آماری نوآوری[3] فیلتر کالمن در هنگام حمله جعل تغییر می‌کند، این واقعیت، استفاده از آزمون‌های آماری برای شناسایی جعل را امکان‌پذیر می‌کند [۳]. این روش بر پایه فیلتر کالمن خطی عمل می‌کند و حساسیت مناسبی به حملات ناگهانی دارد، اما برای حملات آهسته نیازمند به تنظیم پویای آستانه است.

خانافسه و همکاران با استفاده از مفهوم پایش یکپارچگی خودمختار گیرنده (RAIM)، یک آشکارساز جعل توسعه داده‌اند که بر اساس توزیع آماری تخمین‌های فیلتر کالمن عمل می‌کند [۴]. این روش، با محاسبه آزمون ناسازگاری کلی برای چند ماهواره و مقایسه با آستانه، ناسازگاری INS/GNSS را تشخیص می‌دهد که متضمن محاسباتی پیچیده‌تر از روش‌های معمول مبتنی بر نوآوری است.

همچنین، مانش و همکاران در چارچوب RAIM، از اطلاعات دریافتی از ماهواره برای تأیید یکپارچگی داده‌ها استفاده کرده‌اند که مبتنی بر روش فضای پریتی در حوزهٔ تشخیص و جداسازی خطا (FDI) می‌باشد [۵]. این روش بر پایه پردازش خام داده شبه فاصله[4] که با اطلاعات INS ترکیب می‌شود، عمل می‌کند و نسبت به روش‌های نوآوری‌محور، به داده‌های GNSS با نرخ بالا نیاز دارد.

روش پیشنهادی خو و همکاران بر اساس پایش بهره و نوآوری فیلتر کالمن است [۶]. جهش سه برابری واریانس در سیگنال نوآوری به عنوان نشانگر حمله استفاده شده است که برای حملات گذرا مناسب است اما در حملات مداوم حساسیت کمتری دارد. تانیل و همکاران با استفاده از فیلتر کالمن، یک پایشگر برای شناسایی حملات جعل در سیستم ناوبری با تزویج محکم توسعه داده‌اند و سپس، با تحلیل بدترین سناریوی فریب، عملکرد آشکارساز مبتنی بر نوآوری را به صورت نظری

ارزیابی کرده‌اند[۷]. در این روش، معادله حالت شامل بایاس های IMU است و در نتیجه نیاز به مدل‌سازی دقیق این کمیت دارد. ارزیابی بر مبنای حد پایین کرامر- رائو برای بدترین شرایط جعل انجام شده است. در همان چارچوب، لیو و همکاران دو استراتژی را برای شناسایی حمله آهسته از نوع تابع شیب که در آن مقدار جعلی به آرامی زیاد می‌شود، پیشنهاد داده‌اند [۸]. یک روش مبتنی بر میانگین‌گیری از نوآوری فیلتر کالمن و روش دیگر میانگین‌گیری از مشاهدات در یک بازه زمانی است. همچنین، با ادغام استراتژی‌های میانگین‌گیری مذکور، یک روش ترکیبی جدید، به نام "روش پیش‌بینی با نظارت خودکار" معرفی کرده‌اند. روش ترکیبی پیشنهادی از فیلتر کالمن با پنجره متحرک برای کاهش نویز استفاده می‌کند و کارایی آن با معیار تأخیر تشخیص ارزیابی شده است.

لیانگ و همکاران با استفاده از موقعیت حاصل از سیستم ناوبری اینرسی و موقعیت پیش‌بینی‌شده توسط فیلتر کالمن، جعل سیگنال در ناوبری یکپارچه را تشخیص داده‌اند [۹]. در این روش، فرآیند به‌روزرسانی مشاهده در فیلتر، زمانی اجرا می‌شود که داده‌های موقعیت ناوبری معیار تشخیص حمله را برآورده کنند. به عبارتی، در از مکانیزم دروازه برای به‌روزرسانی فیلتر استفاده می‌شود تا مشاهدات مشکوک را حذف کند. در این مرجع، فیلتر کالمن توسعه یافته برای مدل غیرخطی INS/GNSS بکار گرفته شده است.

ژانگ و همکاران یک حسگر اینرسی ثانویه به کار برده‌اند. تخمین اولیه در فیلتر با استفاده از داده‌های این حسگر تصحیح می‌شود تا سیگنال نوآوری بهبود یابد [۱۰]. وای و همکاران با ارزیابی رابطه بین خروجی اینرسی و فرکانس داپلر سیگنال ناوبری، یک آشکارساز حالت دائمی جعل طراحی کرده‌اند که از مشاهدات خام دو سیستم ناوبری و اطلاعات پیشین موقعیت استفاده می‌کند[۱۱].

سکاتو و همکاران یک روش آشکارسازی جعل با استفاده از آزمون نسبت احتمال تعمیم‌یافته (GLRT) ارائه کرده‌اند که ابزاری رایج در نظریه تصمیم‌گیری بهینه است [۱۲]. برای غلبه بر بار محاسباتی سنگین، طرح پیشنهادی با استفاده از ضرب ماتریسی پیاده‌سازی شده است. اما در این روش، عملکرد آشکارسازی به انتخاب آستانه تصمیم‌گیری حساس است که آن را مستعد خطا می‌کند.

آزمون نسبت احتمال حاشیه‌ای (MLRT) به عنوان یک روش جایگزین برای GLRT است که به جای تخمین، پارامترهای مزاحم تصادفی را از طریق حاشیه‌سازی حذف می‌کند و برخلاف آن، نیاز به تنظیم آستانه ندارد و در برابر خطاهای مدل‌سازی مقاوم‌تر است و قابلیت اطمینان سیستم آشکارساز را در عمل افزایش می‌دهد [۱۳]. با وجود مزیت‌های زیاد، تاکنون MLRT در آشکارسازهای جعل در سیستم‌های ناوبری مورد استفاده قرار نگرفته است.

در این مقاله، برای تشخیص جعل دادهٔ ناوبری ماهواره‌ای در سیستم ترکیبی INS/GNSS با تزویج سست، یک روش جدید بر پایه MLRT مطرح شده است. نتایج شبیه‌سازی مقایسه‌ای، مزایای آشکارساز

پیشنهادی را در یک حمله چالش‌برانگیز کـه در آن مسـیر جعلـی بـه آرامـی از مسـیر واقعـی منحـرف می‌شود، نشان می‌دهد.

بـــرای مقایســـهٔ روش‌هـــا، از معیـــار تـــأخیر آشکارسازی، یعنی زمان لازم تا اولـین آشکارسـازی حمله استفاده می‌شود. زمان تشخیص به عنوان یک پارامتر عملکردی مهم آشکارساز مطرح شـده اسـت [۸]. تأخیر بیشتر در شناسایی جعل GNSS، موجب تزریق طولانی‌ترِ خطای موقعیت یا سرعت به حلقـه هدایت و کنترل و در نتیجـه انحـراف پرنـده در اثـر داده‌های آلوده می‌شود.

مقاله به صورت زیر سازمان‌دهی شـده اسـت: در بخش۲، مدل دینامیکی سیسـتم نـاوبری ترکیبـی مدنظر در فضای حالت تشریح می‌شود. در بخـش۳، طرح تشخیص جعل مبتنی بر MLRT ارائه می‌شود. در بخش۴، روش پیشنهادی از طریق شبیه‌سازی بـا روش‌هـای رقیـب مقایسـه مـی‌شـود. بخـش۵ نتیجه‌گیری مقاله است.

۲. مدل دینامیکی ناوبری GNSS/INS

یک سیستم ناوبری متشکل از گیرنـده نـاوبری ماهواره‌ای و واحـد نـاوبری اینرسـی (شـتاب‌سـنج و ژیروسکوپ) با پیکربندی تـزویج سسـت اسـت کـه هدف آن برآورد موقعیـت مـی‌باشـد. بـا اسـتفاده از متغیرهای خطای[۵] نـاوبری، معادلـه حالـت سیسـتم به‌صورت (۱) نوشته می شود [۱۴]:

$$\dot{X}(t) = F(t)\,X(t) + v(t) \qquad (۱)$$

بـردار حالـت سیسـتم خطـا متشـکل از پـنج بـردار ســـــــه‌تـــــــایی بـــــــه فـــــــرم $\left[\ \phi^T\ \ (\delta v^n)^T\ \ (\delta p)^T\ \ \left(\varepsilon^b\right)^T\ \ \left(\nabla^b\right)^T\ \right]^T$ می‌باشد کـه در آن، $\phi = [\phi_E\,,\phi_N\,,\phi_U]^T$ بـردار زوایـای ناهمـاهنگی[۶]، $\delta v^n = [\delta v_E^n\,,\delta v_N^n\,,\delta v_U^n]^T$ بـردار خطای سرعت، $\delta p = [\delta L\,,\delta\lambda\,,\delta H\,]^T$ بردار خطـای موقعیـت، $\varepsilon^b = [\varepsilon_R^b\,,\ \varepsilon_F^b\ ,\varepsilon_U^b\,]^T$ و $\nabla^b = [\nabla_R^b\,,\ \nabla_F^b\ ,\nabla_U^b\,]^T$ بـه ترتیـب، بردارهـای بایـاس جـایرو و شـتاب‌سـنج هستند. نمادهای n و b به ترتیب نمایـانگر چـارچوب ناوبری و چارچوب بدنه هستند؛ زیرنویس‌های N، E و U به ترتیب نشان‌دهنده جهت‌های شمال، شـرق و بالا در دستگاه مختصات ناوبری می‌باشـند. همچنـین، زیرنویس‌های F، R و U به ترتیب بیـانگر جهـت‌هـای جلو، راست و بالا در دستگاه مختصـات بدنـه هسـتند. $v(t)$ نویز فرآیند است که برداری گاوسـی بـا میـانگین صفر و ماتریس کوواریانس $Q(t)$ می‌باشد. ماتریس $F(t)$ به صورت (۲) می‌باشد:

$$F(t) = \begin{bmatrix} F_{11} & F_{12} & F_{13} & -C_b^n & 0_3 \\ F_{21} & F_{22} & F_{23} & 0_3 & C_b^n \\ 0_3 & F_{32} & F_{33} & 0_3 & 0_3 \\ 0_3 & 0_3 & 0_3 & 0_3 & 0_3 \\ 0_3 & 0_3 & 0_3 & 0_3 & 0_3 \end{bmatrix} \qquad (۲)$$

در این رابطه، 0_3 یک ماتریس صفر با ابعاد سـه در سه است. C_b^n ماتریس چرخش از چارچوب بدنه به ناوبری را نشان می‌دهد؛ همچنین، مـاتریس‌هـای F_{ij} ماتریس‌هایی با ابعاد سه در سه به قرار زیرند:

$$F_{11} = (-(w_{ie}^n + w_{en}^n)\times)$$

$$F_{21} = ((C_b^n f^b)\times)$$

$$F_{12} = \begin{bmatrix} 0 & -1/R_{Mh} & 0 \\ 1/R_{Nh} & 0 & 0 \\ \tan L\,/R_{Nh} & 0 & 0 \end{bmatrix}$$

$$F_{13} = \begin{bmatrix} 0 & 0 \\ -w_{ie}\sin L & 0 \\ w_{ie}\cos L + v_E^n\,sec^2\,L\,/R_{Nh} & 0 \\ v_N^n/{R_{Mh}}^2 & \\ -v_N^n/{R_{Nh}}^2 & \\ -v_E^n\tan L\,/{R_{Nh}}^2 & \end{bmatrix}$$

$$F_{22} = (v^n\times)F_{12} - \left((2w_{ie}^n + w_{en}^n)\times\right)$$

$$F_{23} = (v^n \times)\begin{bmatrix} 0 & 0 \\ -2w_{ie}\sin L & 0 \\ 2w_{ie}\cos L + v_E^n\, sec^2\, L\, /R_{Nh} & 0 \end{bmatrix}$$

$$\begin{bmatrix} v_N^n/{R_{Mh}}^2 \\ -v_N^n/{R_{Nh}}^2 \\ -v_E^n \tan L\, /{R_{Nh}}^2 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & -v_N^n\, /{R_{Mh}}^2 \\ v_E^n \sec L \tan L\, /R_{Nh} & 0 & -v_E^n \sec L\ /{R_{Nh}}^2 \\ 0 & 0 & 0 \end{bmatrix}$$

$$F_{32} = \begin{bmatrix} 0 & \frac{1}{R_{Mh}} & 0 \\ \frac{\sec L}{R_{Nh}} & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$F_{33} = (v^n \times)$$

که در آن × نشان دهنده ماتریس پادمتقارن بردار مربوطه است. R_{Mh} و R_{Nh} شعاع‌های خمیدگی عرضی و نصف النهاری به اضافهٔ ارتفاع هستند. $v^n = [v_E^n\ v_N^n\ v_U^n]$ بردار سرعت در دستگاه ناوبری است که از مولفه‌های شرق، شمال و بالا تشکیل شده است. L نشان‌دهنده عرض جغرافیایی است. C_b^n ماتریس چرخش قاب بدنه به فریم ناوبری است (از بالانویس برای نشان دادن چارچوب مرجع استفاده می‌شود). $f^b = [f_R^b\ f_F^b\ f_U^b]$ بردار نیروی ویژه (نیروی مخصوص شتاب‌سنج‌ها) در دستگاه بدنی است که از اجزای راست، جلو و بالا تشکیل شده است. w_{ie} نرخ ثابت چرخش زمین است. w_{ie}^n بردار چرخش زمین (نرخ دوران دستگاه زمینی به دستگاه اینرسی) است که در دستگاه ناوبری محلی به صورت $w_{ie}^n = [\,0\ \ w_{ie}\cos L\ \ w_{ie}\sin L]^T$ تعریف می‌شود. بردار چرخش دستگاه ناوبری نسبت به دستگاه زمین‌مرکز و زمین‌محور در دستگاه ناوبری محلی به صورت بردار زیر نشان داده شده است.

$$w_{en}^n = [-v_N^n/R_{Mh}\ \ v_E^n/R_{Nh}\ \ v_E^n \tan L\, /R_{Nh}]^T$$

بردار مشاهده، تفاوت بین مقادیر سرعت و موقعیت حاصل از INS و GNSS می‌باشد که به صورت (۳) تعریف شده است:

$$Z(t) = H\, x(t) + e(t) \qquad (۳)$$

در این رابطه، $e(t)$ نویز اندازه‌گیری موقعیت‌ها را نشان می‌دهد که یک بردار گاوسی با میانگین صفر و ماتریس کوواریانس $R(t)$ است و $H = [\,0_3\ I_3\ I_3\ 0_3\ 0_3\,]$ ماتریس مشاهده می‌باشد که در آن، I_3 نماد ماتریس همانی سه در سه است. فرض می‌شود که نویز فرآیند، $v(t)$ و نویز اندازه‌گیری، $e(t)$ با یکدیگر همبستگی ندارند.

INS به سیگنال رادیویی وابسته نیست و بر اساس حسگرهای شتاب‌سنج و ژیروسکوپ عمل می‌کند و خطای آن پیوسته و بدون جهش ناگهانی است. در حمله جعل، اندازه‌گیری GNSS به‌آرامی ولی غیر واقعی منحرف می‌شود، اما INS مسیر واقعی حرکت را دنبال می‌کند. این تضاد، امضای آماری حمله است. به جای اتکا به سازگاری درونی GNSS، اختلاف آن با مرجع فیزیکی مستقل INS در (۳) برای آشکارسازی استفاده می‌شود.

مهاجم سیگنال جعلی به گیرنده GNSS ارسال می‌کند تا موقعیتی نادرست تولید کند. مقدار جعل، در مدل اندازه‌گیری به‌صورت جمع‌شونده افزایشی در نظر گرفته می‌شود که بازنمایی دقیقی از حمله‌ی جعل تدریجی در دنیای واقعی است که طی آن مهاجم پس از هم‌فاز شدن با سیگنال‌های اصلی ماهواره‌ای، به‌آرامی زمان یا فاز سیگنال را جابه‌جا می‌کند تا شبه‌فاصله‌ها به‌صورت تدریجی دچار

بایاس شوند. در نتیجه، گیرنده GNSS بدون درک تغییر ناگهانی، به‌صورت نرم از موقعیت واقعی به موقعیت جعلی منتقل می‌شود.

$$A_t = \begin{bmatrix} \Phi_t & 0 \\ 0 & I \end{bmatrix}, \qquad B_v = \begin{bmatrix} I \\ 0 \end{bmatrix},$$
$$B_\theta = \begin{bmatrix} 0 \\ I \end{bmatrix}, \qquad C = [H \quad 0]$$

از آنجایی که در بسیاری از گیرنده‌های GNSS اندازه‌گیری‌های موقعیت و سرعت از کانال‌های پردازشی مجزا (مانند فاز کد برای موقعیت و شیفت داپلر برای سرعت) حاصل می‌شوند، مهاجم قادر است در سطح داده، تنها مشاهدات موقعیت را دستکاری کند بدون اینکه مشاهدات سرعت را تغییر دهد. بسیاری از حملات جعل داده فقط روی شبه‌فاصله (موقعیت) اثر می‌گذارند و فرکانس داپلر را که مبنای محاسبه سرعت است، منحرف نمی‌کنند.

مساله مد نظر، توسعه یک روش پایش مبتنی بر آزمون نسبت احتمال حاشیه‌ای(MLRT) به‌منظور آشکارسازی حمله جعل به گیرنده GNSS در سریع‌ترین زمان ممکن است.

۳. آشکارساز حمله مبتنی بر MLRT

در این بخش، یک آشکارساز جعل جدید که از مفهوم MLRT مبتنی بر فیلتر کالمن استفاده می‌کند، توسعه داده می‌شود و در بخش بعدی با شبیه‌سازی با روش‌های موجود مقایسه می‌شود.

ابتدا، معادلات سیستم ناوبری در (۱) و (۳) به منظور استفاده در الگوریتم، به شکل (۴) گسسته‌سازی می‌شوند:

$$X_{t+1} = \Phi_t X_t + v_t$$
$$Z_t = H X_t + e_t + \vartheta \rho_{t-k} \qquad (۴)$$

که در آن، اندیس t نمایانگر زمان گسسته است و ρ تابع حمله شیب است که در لحظه k آغاز می‌شود. با تعریف کردن بردار حالت افزونه[۷] به صورت $x = [X^T,\ \theta^T]^T$، معادلات (۴) به صورت (۵) بازنویسی می‌شوند:

$$x_{t+1} = A_t x_t + B_v v_t + B_\theta \vartheta \sigma_{t-k}$$
$$y_t = C x_t + e_t \qquad (۵)$$

جایی که، σ تابع پله واحد را نشان می‌دهد و همچنین، e_t نشانگر سیگنال گسسته شده $e(t)$ در معادله (۳) است که نویز اندازه‌گیری موقعیت‌ها را نشان می‌دهد.

توجه کنید که با تعریف متغیر کمکی θ ، با دینامیک $\theta_{t+1} = \theta_t + \vartheta \sigma_{t-k}$ ، بردار حالت افزونه به فرم $x = [X^T,\ \theta^T]^T$ در نظر گرفته شد که متعاقب آن، معادله (۵) حاصل می‌شود. θ در (۵) متغیر انتگرال‌گیر است که نقش آن تبدیل تابع پله به تابع شیب از یک طرف و انتقال عبارت جمع شونده از معادله مشاهده به معادله حالت است تا تئوری مرجع [۱۳] که برای تغییرات ناگهانی از جنس پله در معادله حالت است، در اینجا برای حمله آهسته از جنس شیب به مشاهده قابل استفاده باشد.

ماتریس‌های کوواریانس نویزهای فرآیند و اندازه‌گیری با Q_t و R_tنشان داده می‌شوند. در اینجا، جهش پله‌ای نامعلوم ϑ در زمان نامشخص k رخ می‌دهد، که در این مساله، یافتن زمان جهش k اهمیت دارد.

۱.۳ مبانی MLRT

در آزمون نسبت احتمال (LR)، فرضیه[۸] وقوع جهش با فرضیه عدم جهش مقایسه می‌شود. به عبارتی، فرضیه‌ها عبارتند از: H_0 عدم جهش و $H_1(k,\vartheta)$ وقوع جهش با دامنهٔ ϑ در لحظهٔ k. y^N مجموعه‌ای از اندازه‌گیری‌ها به صورت $y_1, y_2, \dots, y_N$ را نشان می‌دهد. نسبت احتمال لگاریتمی به عنوان آماره[۹] آزمون به صورت (۶) تعریف می‌شود:

$$l_N(k,\vartheta) = 2\log\frac{P(y^N|H_1(k,\vartheta))}{P(y^N|H_0)} \qquad (۶)$$

معادله (۷) بر اساس آماره‌ای که معادله (۶) آن را تعریف کرده است، عمل تخمین زمان وقوع جهش را انجام می‌دهد:

$$\hat{k} = argmax\, l_N(k,\vartheta) \qquad (۷)$$

یعنی، k ای انتخاب می‌شود که آماره (۶) به ازا آن، مقدار بیشینه را داشته باشد؛ به عبارتی، $\hat{k}$ لحظه‌ای است که به احتمال زیاد جهش در آن رخ داده است. توجه کنید که در اینجا ϑ معلوم است و $k = N$ به معنای عدم وقوع جهش است.

چون دامنه‌ی جهش ϑ معمولاً نامعلوم است به جای بیشینه‌سازی روی ϑ، از توزیع احتمال آن طبق (۸) انتگرال می‌گیرند.

$$l_N(k,\vartheta) = 2\log\frac{\int P(y^N|H_1(k,\vartheta))P(\vartheta)\,d\vartheta}{P(y^N|H_0)} \qquad (۸)$$

در مدل خطی-گاوسی، چگالی احتمال، توزیع نرمال است در نتیجه، انتگرال مذکور به‌صورت تحلیلی قابل محاسبه است. این رویکرد برای حذف پارامتر مزاحم نامعلوم ϑ که از روش حاشیه‌سازی[۱۰] استفاده می‌کند، به عنوان آزمون MLR برای آشکارسازی تغییر نامیده می‌شود [۱۵,۱۳].

حمله جعل در (۵) در واقع، یک بایاس تدریجی است که به‌صورت ناسازگاری آماری پیوسته در زمان بروز می‌کند. به عبارتی، با اینکه هر نوآوری به‌تنهایی ممکن است کوچک و غیرمعنادار باشد، اما هم‌بستگی آنها باعث رشد یکنواخت شاخص تصمیم (نسبت احتمال) می‌شود. حمله تدریجی اندازهٔ نوآوری را فوراً افزایش نمی‌دهد، اما توزیع آماری آن را از حالت عادی خارج می‌کند. MLRT تغییر تدریجی توزیع نوآوری را آشکار می‌کند، نه صرفاً مقدار آن را؛ در نتیجه، حتی اگر نوآوری‌ها در محدوده‌ی نویز باشند، احتمال تجمع آنها رشد می‌کند و آزمون از آستانه تصمیم عبور می‌کند.

احتمال وقوع جهش در زمان‌های $k = 1,2,\dots,N$ با استفاده از دو فیلتر محاسبه می‌شود: یک فیلتر کالمن که در زمان به صورت پس‌رو[۱۱] و فیلتر کالمن دوم که در زمان به صورت پیش‌رو[۱۲] اجرا می‌شود. حالت x_t متغیر پنهان در محاسبه انتگرال (۸) است که با حاشیه‌سازی حذف می‌شود، یعنی احتمال مشترک روی x_t کنار زده می‌شود تا احتمال فقط بر روی داده‌های مشاهده‌شده باقی بماند. هر فیلتر کالمن تقریبی از توزیع احتمال شرطی $P(x_N \mid y^N)$ و $P(x_k \mid y_{k:N})$ را که در محاسبه (۸) ظاهر می‌شوند، تولید می‌کند. آزمون MLR این دو تقریب را برای ارزیابی احتمال وقوع تغییر در حالت در لحظه k ترکیب می‌کند.

به عبارتی، MLRT از دو فیلتر پیش‌رو و پس‌رو برای حاشیه‌گیری پارامتر ناشناخته θ استفاده می‌کند. فیلتر پیش‌رو اثر لحظه‌ای را می‌سنجد، فیلتر پس‌رو انحراف تدریجی را تثبیت می‌کند، و ترکیب آنها باعث فعال‌شدن آشکارسازی پس از عبور نرخ تغییر از کران نویز طبیعی سیستم می‌شود.

۲.۳ پیاده سازی MLRT برای آشکارسازی

در پیاده سازی برخط، در زمان فعلی t مقدار $l_t(m)$ برای $m = 1, 2, \dots, t-L$ محاسبه می‌شود. حمله، زمانی اعلام می‌شود که $l_t(m)$ مثبت باشد.

مقدار دهی اولیه:

در لحظهٔ t ، بر مبنای مشاهدات $y^t = \{y_1, y_2, \dots, y_t\}$

$$V^F(0) = 0, \quad D^F(0) = 0$$

اجرای فیلتر کالمن پیشرو:

$$V^F(t) = V^F(t-1) + (\varepsilon_t^F)^T (S_t^F)^{-1} \varepsilon_t^F$$
$$D^F(t) = D^F(t-1) + \log\det S_t^F$$

که در آن،

$$\varepsilon_t^F = y_t - C_t\, \hat{x}_{t|t-1}^F$$
$$S_t^F = C_t\, P_{t|\,t-1}^F\, C_t^T + R_t$$
$$\hat{x}_{t+1|t}^F = A_t\, \hat{x}_{t|t-1}^F + A_t\, P_{t|t-1}^F C_t\, (S_t^F)^{-1}\, \varepsilon_t^F$$
$$P_{t+1|t}^F = A_t \left(P_{t|t-1}^F - P_{t|t-1}^F\, C_t^T\, (S_t^F)^{-1} C_t\, P_{t|t-1}^F\right) A_t^T + B_v\, Q_t\, B_v^T$$

اجرای فیلتر اطلاعات پسرو:

$$(P_{t|t+1}^B)^{-1} = 0 \ , \ \hat{a}_{t|t+1}^B = 0$$
for $i = t, t-1, \dots, t-L+1$
$$\hat{a}_{t|t}^B = \hat{a}_{t|t+1}^B + C_t^T R_t^{-1} Y_t$$
$$(P_{t|t}^B)^{-1} = (P_{t|t+1}^B)^{-1} + C_t^T R_t^{-1} C_t$$
$$F = A_t^T (P_{t|t}^B)^{-1} A_t$$
$$G = F A_t^{-1} B_v (B_v^T A_t^{-T} F\, A_t^{-1} B_v + Q_t^{-1})^{-1}$$
$$\hat{a}_{t-1|t}^B = A_t^T \hat{a}_{t|t}^B$$
$$(P_{t-1|t}^B)^{-1} = F$$

اجرای فیلتر اطلاعات کالمن پسرو:

$P_{t-L|t-L+1}^B$ from the backward information filter

$$\hat{x}_{t-L|t-L+1}^B = P_{t-L|t-L+1}^B\, \hat{a}_{t-L|t-L+1}^B$$
$$V^B(t-L+1) = 0, \quad D^B(t-L+1) = 0$$
for $i = t-L, t-L-1, \dots, 1$
$$V^B(i) = V^B(i+1) + (\varepsilon_i^B)^T (S_i^B)^{-1} \varepsilon_i^B$$
$$D^B(i) = D^B(i+1) + \log\det S_i^B$$

که در آن

$$\varepsilon_i^B = y_i - C_i\, \hat{x}_{i|i+1}^B$$
$$S_i^B = C_i\, P_{i|\,i+1}^B\, C_i^T + R_i$$
$$\hat{x}_{i-1|i}^B = A_i^{-1}\, \hat{x}_{i|i+1}^B + A_i^{-1}\, P_{i|i+1}^B C_i\, (S_i^B)^{-1}\, \varepsilon_i^B$$
$$P_{i-1|i}^B = A_i^{-1} \left(P_{i|i+1}^B - P_{i|i+1}^B\, C_i^T\, (S_i^B)^{-1} C_i\, P_{i|i+1}^B\right) A_i^{-T} + A_i^{-1}\, Q_i\, A_i^{-T}$$

محاسبه پارامتر آشکارسازی

for $m = 1 : t-L$
$$l_t(m) = V^F(t) + D^F(t) - V^F(m) - D^F(m) - V^B(m+1) - D^B(m+1)$$
■

بر اساس فیلترهای مذکور، تخمین‌های هموارشده[۱۳] حالت و ماتریسکوواریانس خطای آن به صورت زیر به دست می‌آید.

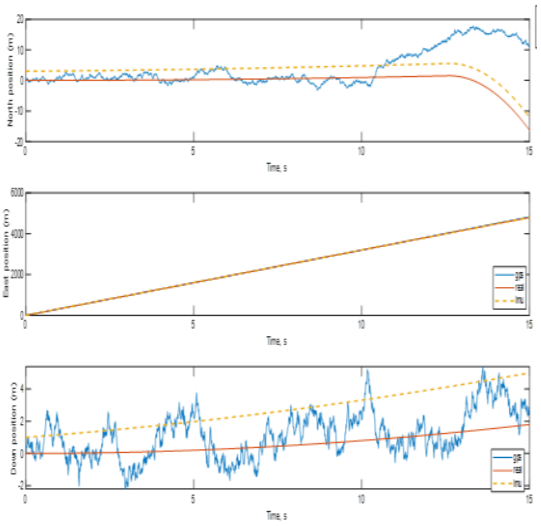
$$P_{t|t} = \left((P_{t|t}^F)^{-1} + (P_{t|t+1}^B)^{-1}\right)^{-1}$$
$$\hat{x}_{t|t} = P_{t|t}\left((P_{t|t}^F)^{-1}\, \hat{x}_{t|t}^F + (P_{t|t+1}^B)^{-1} \hat{x}_{t|t+1}^B\right)$$

۴. شبیه‌سازی آشکارساز

کارایی آشکارساز پیشنهادی با مقایسه عملکرد آن با آشکارسازهایی که از روش‌های GLRT و فیلتر کالمن استفاده می‌کنند، نشان داده می‌شود. اثربخشی روش پیشنهادی از حیث مقدار زمان لازم تا آشکارسازی مورد بررسی قرار می‌گیرد.

داده های حرکتی یک وسیله هوایی شامل ارتفاع ژئودتیک، عرض و طول جغرافیایی، به همراه سرعت‌ها و شتاب‌ها با فرکانس نمونه‌برداری ۱۶۰ هرتز برای INS و ۱ هرتز برای GNSS در اختیار است. این داده‌های از مدل‌های حسگرهای موجود

در Navigation Toolbox نـــــرم‌افـــــزار Matlab اندازه‌گیری می‌شوند. مدت زمان کل شبیه‌سازی ۱۵ ثانیه است و در زمان ۱۰ ثانیه، یک حمله جعـل بـا رشد آهسته اعمال می‌شود. یعنی، از زمان ۱۰ ثانیـه به بعـد، مسـیر جعلـی بـه تـدریج از مسـیر واقعـی منحرف می‌شود. همان‌طـور کـه در شـکل ۱ نشـان داده شده است، مهاجم یک پروفایل جعل شیب‌دار با نرخ ۵ متر بر ثانیه به موقعیـت شـرق و شـمال اضافه می‌کند کـه منجـر بـه انحـراف انـدازه‌گیـری موقعیت GNSS از مسیر واقعی می‌شـود. بـا توجـه بـه محـدوده محـور عمـودی در نمـودار بـالایی شـکل ۱(مولفه شمال) که مقادیر اصلی درحـدود چنـدمتر است، حمله از ثانیه دهم قابل رویت است.



شکل ۱. موقعیت جرکت پرنده در شمال-شرق-پایین و حمله جعل (متر)

توجه کنید که گیرنده GNSS، فقـط داده هـای موقعیت را اشتباه دریافت می‌کند و سرعت‌هـا برابـر با مقدار واقعی اندازه‌گیری مـی‌شـوند. لازم بـه ذکـر است گیرنده GNSS دو نوع مشاهده مسـتقل از هـم تولید می‌کند: مشاهده موقعیت و مشـاهده سـرعت. در این سناریو مهاجم به تدریج مقدار موقعیـت را از مقدار واقعی دور می‌کند. به عبارتی، به جای افزودن یک انحراف ثابت(بایاس)، یک خطای متغیر با زمـان اضافه می‌کند که مقدار آن با نرخ ۵ متر در هر ثانیه زیـاد مـی‌شـود. یعنـی، جعـل داده بـر روی کانـال مشاهده موقعیت به صورت یک تابع شیب، بر حسب زمان است و هیچ تغییری در کانال مشاهده سـرعت اعمال نمی‌شود.

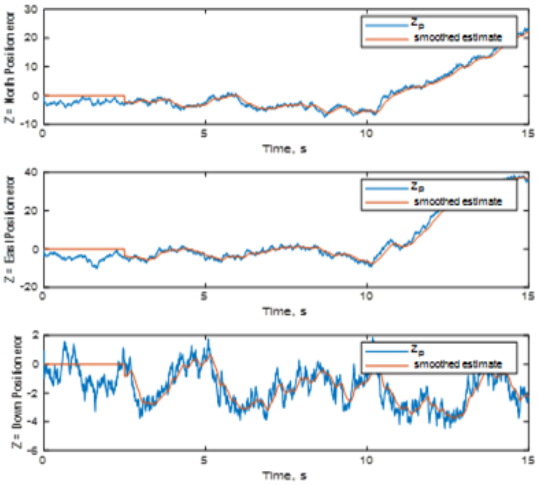
بـا توجـه بـه ویژگـی‌هـای حسـگرها، مقـادیر پارامترهای فیلترها به صورت زیر انتخاب شده‌اند:

$$R = diag\{3.7\ m, 3.7\ m, 6\ m\}^2$$

$$Q = diag\ \{0.005\ {}^{\circ}/\sqrt{h}, 0.005\ {}^{\circ}/\sqrt{h}, 0.005\ {}^{\circ}/\sqrt{h}, 20\ {}^{\mu g}/\sqrt{Hz}, 20\ {}^{\mu g}/\sqrt{Hz}, 20\ {}^{\mu g}/\sqrt{Hz}, 1\ {}^{m}/\sqrt{h}, 1\ {}^{m}/\sqrt{h}, 1\ {}^{m}/\sqrt{h}, 0,0,0,0,0,0\}^2 \times \left(\frac{1}{160}\right)$$

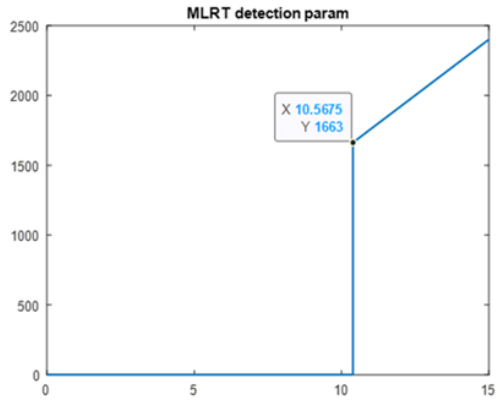
$$P_{-1} = diag\ \{20^{"}, 20^{"}, 180^{"}, 0.1\ {}^{m}/_{s}, 0.1\ {}^{m}/_{s}, 0.1\ {}^{m}/_{s}, 3.7\ m,\ 3.7\ m,\ 6\ m, 0.01\ {}^{\circ}/_{h}, 0.01\ {}^{\circ}/_{h}, 0.01\ {}^{\circ}/_{h}, 100\ \mu g, 100\ \mu g, 100\ \mu g] \times 3\}^2$$

شکل ۲ بخشی از بردار حالت (خطای موقعیت، δp) و تخمین هموارشده آن را در طول زمان نشان می‌دهد. همان‌طور که انتظار می‌رفت، فیلترهـا ایـن متغیرها را به دقت تخمین می‌زنند.



شکل ۲. خطاهای موقعیت (در بردار حالت) و تخمین‌های هموارشده آنها (متر)

شکل۳ پارامتر تشخیص MLRT، $l_t(k)$ را نشان می‌دهد که با تأخیری برابر ۰/۵۶ ثانیه، از صفر به مقدار مثبت تغییر و حمله جعل را آشکار می‌کند.



شکل ۳. پارامتر آشکارسازی l_t

جدول ۱ تأخیر در آشکارسازی روش پیشنهادی را با دو روش کالمن معمولی و GLRT برای سناریوهای مختلف حمله بر حسب ثانیه گزارش می‌کند. برای مقایسه کارایی روش‌ها، از معیار تأخیر آشکارسازی، یعنی زمان اعمال حمله تا آشکارسازی آن استفاده می‌شود. در آشکارساز مبتنی بر نوآوری فیلتر کالمن استاندارد، آستانه تشخیص روی ۲۵.۹ تنظیم شده است به طوری که احتمال هشدار کاذب، 10^{-5} برآورده شود. در روش GLRT، آستانه آشکارسازی معادل با سه برابر واریانس تنظیم شده است. در حمله با شدت ۵، که نتایج آن در ستون سمت چپ گزارش شده است، زمان تشخیص از حدود ۱ با GLRT به حدود ۰/۵ در MLRT رسیده است. روشن است که روش پیشنهادی حملات را با تأخیر بسیار کمتر (تا حدود پنجاه درصد) نسبت به روش‌های رقیب شناسایی می‌کند.

روش MLRT مبتنی بر استفاده از نسبت احتمال است و برخلاف روش مبتنی بر فیلتر کالمن، تصمیم گیری در آن نه بر اساس اندازه نوآوری، بلکه بر مبنای انباشت ناسازگاری آماری در طول زمان انجام می‌شود. در این رویکرد امکان تجمیع شواهد ضعیف اما پیوسته فراهم می‌شود. بنابراین، علت کاهش تأخیر آشکارسازی آن است که در MLRT، به‌جای انتظار برای بزرگ‌شدن مقدار نوآوری، افزایش احتمال بروز خطا به صورت پیوسته پایش می‌شود؛ به‌گونه‌ای که پیش از افزایش محسوس اندازه نوآوری، احتمال وقوع حمله از آستانه تشخیص عبور می‌کند.

در MLRT به‌جای بیشینه‌سازی پارامتر نامعلوم که در GLRT انجام می شود، روی آن حاشیه‌سازی انجام می‌شود. نشان داده شده که اگر خطا کوچک ولی پیوسته باشد، بیشینه‌سازی در GLRT باعث تأخیر در تصمیم می‌شود، اما حاشیه‌سازی در

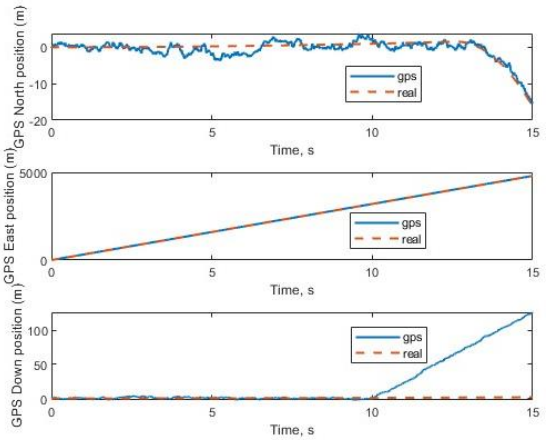
MLRT باعث می‌شود که احتمال حضور خطا به‌صورت تجمعی افزایش یابد [۱۵]. با به‌کارگیری حاشیه‌سازی، وابستگی الگوریتم به تخمین نقطه‌ای پارامترهای نامعلوم حمله حذف می‌گردد. این ویژگی سبب می‌شود تا شواهد ضعیف اما هم‌بسته در طول زمان یکپارچه شوند؛ به گونه‌ای که حتی وقتی که خطای تزریقی هنوز در سطح نویز سیستم پنهان است، انباشت ناسازگاری آماری باعث عبور سریع‌تر آماره از سطح اطمینان شده و حمله در مراحل آغازین کشف می‌گردد.

لازم به ذکر است که در سناریوی شبیه‌سازی این بخش، حداقل نرخ حمله شیب به داده‌های موقعیت (شمال و شرق) که توسط روش پیشنهادی قابل تشخیص است، برابر با ۱/۸ متربرثانیه می باشد که با آزمون و خطا حاصل شده است.

جدول ۱. مقادیر تاخیر آشکارسازی در سناریوهای مختلف حمله (بر حسب ثانیه)

حمله شیب (m/s)	۲	۳	۵
فیلتر کالمن	-	۳/۴	۱/۹
GLRT	۲/۶۳	۱/۵۹	۱/۰۳
MLRT	۲/۵۷	۱/۵۷	۰/۵۶

در آزمایش دوم، مهاجم از ثانیه ۱۰ یک پروفایل جعل شیب‌دار با نرخ ۲۵ متر بر ثانیه فقط به محور سوم موقعیت اضافه می‌کند. شکل ۴، مسیر واقعی و اندازه‌گیری جعل شدهٔ گیرندهٔ GNSS را در این سناریو نشان می‌دهد. این حمله پیچیده با تاخیر حدود ۱/۹۳ ثانیه توسط روش MLRT آشکارسازی می‌شود.



شکل ٤. موقعیت جرکت پرنده در شمال-شرق-پایین و حمله جعل (متر) در آزمایش دوم

۵. نتیجه‌گیری و پیشنهاد

یک روش نوین برای تشخیص حملات جعل با استفاده از MLRT ارائه شد. نتایج شبیه‌سازی نشان داد که آشکارساز پیشنهادی ابزاری کارآمد برای آشکارسازی حملات جعل است و نسبت به روش‌های موجود، تأخیر کمتری در آشکارسازی دارد. بهبود کیفیت آشکارسازی در این روش، ناشی از مقاوم بودن ذاتی الگوریتم MLRT در برابر نامعینی‌ها و مهم‌تر از آن عدم نیاز به تعیین سطح آستانه برای آشکارسازی است که در روش‌های رقیب ضرورت دارد. تطبیق برخط مدل سیستم، خصوصا ویژگی نویزها و نیز تمرکز بر حملات پویا، به‌عنوان زمینه‌ای برای پژوهش‌های آینده پیشنهاد می‌شود.

۵. مراجع

[1] M. Grewal, L. Weill, A. Andrews, Global positioning systems, inertial navigation, and integration, Third edition, John Wiley, 2013.

[2] D. Schmidt, K. Radke, S. Camtepe, E. Foo, M. Ren, “A survey and snalysis of the GNSS spoofing threat and countermeasures,” ACM Computing Surveys, vol. 48, no. 4, pp. 1-31, 2016.

[3] Y. Liu, S. Li, Q. Fu, Z. Liu, “Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system,” Sensors, vol. 18, pp. 131-143, 2018.

[4] S. Khanafseh, N. Roshan, S. Langel, F. Chan, M. Joerger, and B. Pervan, “GPS spoofing detection using RAIM with INS coupling,” in Proceedings of the IEEE/ION Position, Location Navigation Symposium, Monterey, CA, USA, May 2014.

[5] M.R. Manesh, J. Kenney, W.C. Hu, V.K. Devabhaktuni, N. Kaabouch, “Detection of GPS spoofing attacks on unmanned aerial systems,” in Proceedings of the 16th IEEE Annual Consumer Communications and Networking Conference, Las Vegas, NV, USA, January 2019.

[6] R. Xu, M. Ding, Y. Qi, S. Yue, J. Liu, “Performance analysis of GNSS/INS loosely coupled integration systems under spoofing attacks,” Sensors, vol. 18, 4108, 2018.

[7] C. Tanil, S. Khanafseh, M. Joerger, B. Pervan, “An INS monitor to detect GNSS spoofers capable of tracking vehicle position,” IEEE Transactions on Aerospace Electronic Systems, vol. 54, pp. 131-143, 2018.

[8] Y. Liu, S. Li, Q. Fu, Z. Liu, Q. Zhou, “Analysis of Kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system,” IEEE Sensors Journal, vol. 19, pp. 5167-5178, 2019.

[9] W. Liang., K. Li, Q. Li, “Anti-spoofing Kalman filter for GPS/rotational INS integration,” Measurement, vol. 193, 110962, 2022.

[10] L. Zhang, H. Zhao, C. Sun, L. Bai, W. Feng, “Enhanced GNSS spoofing detector via multiple-epoch inertial navigation sensor prediction in a tightly coupled system,” IEEE Sensors Journal, vol. 22, pp. 8633-8647, 2022.

[11] Y. Wei, H. Li, M. Lu, “A steady-state spoofing detection and exclusion method based on raw IMU measurement,” IEEE Sensors Journal, vol. 22, pp. 3529-3539, 2022.

[12] M. Ceccato, F. Formaggio, N. Laurenti, and S. Tomasin, “Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3496-3509, 2021.

[13] F. Gustafsson, “The Marginalize likelihood ratio test for detecting abrupt changes,” IEEE Transactions on Automatic Control, vol. 41, pp. 66-78, 1996.

[14] P. D. Groves, Principles of GNSS, inertial, and multisensor integrated navigation systems, Second edition, Artech House, Boston, USA, 2013.

[15] M. Basseville, and I. V. Nikiforov, Detection of abrupt changes: theory and application, Englewood Cliffs: Prentice Hall, 1991.

پی‌نوشت

1. Loosely Coupled
2. Spoofing
3. Innovation
4. Pseudorange
5. Error-state
6. Misalignment Angles
7. Augmented
8. Hypothesis
9. Statistics
10. Marginalization
11. Backward
12. Forward
13. Smoot