مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال ششم، شماره ۲، تابستان ۱۳۹۴؛ ص ۱۰۴-۹۷

ارائه راهکار مقابله با حمله فریب تأخیری در سامانه ناوبری GPS با استفاده از فیلتر تطبیقی

مریم معاضدی[۱]، محمدرضا موسوی میرکلائی[۲*]، پیوند تیموری[۳]، امیررضا بازیار[۴]

۱- دانشجوی دکتری ۲- استاد ۳- دانشجوی کارشناسی‌ارشد ۴- کارشناس‌ارشد ، دانشگاه علم و صنعت ایران

(دریافت: ۹۳/۰۴/۲۰، پذیرش: ۹۴/۰۴/۰۷)

چکیده

سیگنال‌های GPS غیرنظامی رمز نشده و پیش‌بینی‌پذیر بوده و سطح توان پایینی دارند. ازاین‌رو در برابر تداخلات مخرب از جمله فریب بسیار آسیب‌پذیرند. در این مقاله برای نخستین بار از فیلتر تطبیقی با پاسخ ضربه با طول محدود بر اساس الگوریتم حداقل میانگین مربعات خطا، به منظور کاهش خطای فریب تأخیری و دستیابی به سری زمانی بدون تداخل استفاده شده است. برخلاف روش‌های موجود برای مقابله با فریب، راهکار ارائه شده نیازی به تغییر سخت‌افزاری و ساختاری در گیرنده GPS ندارد. سیگنال ورودی فیلتر تطبیقی، مقادیر شبه‌فاصله داده فریب GPS در بخش موقعیت‌یابی است. ایده اصلی استفاده از فیلتر تطبیقی تخمین سیگنال تداخل و کم کردن آن از سیگنال ورودی (ترکیب سیگنال معتبر و جعلی) است که در نتیجه آن در خروجی نهایی فیلتر سیگنال معتبر باقی می‌ماند. در این مقاله از معیار مجذور متوسط مربعات خطا (RMS) به منظور ارزیابی الگوریتم پیشنهادی بهره گرفته شد. دو سری داده فریب شبیه‌سازی و اندازه‌گیری برای ارزیابی الگوریتم پیشنهادی به‌کار رفته‌اند. نتایج شبیه‌سازی نشان می‌دهند که راهکار ارائه شده به طور میانگین می‌تواند خطای داده فریب آزمایشگاهی را ۹۵ درصد و خطای داده اندازه‌گیری را ۸۱ درصد جبران نماید.

کلید واژه‌ها: الگوریتم‌های جست‌وجوگرایانه، الگوریتم حداقل میانگین مربعات خطا، فریب تأخیری، فیلتر تطبیقی.

Introducing Countermeasure Approach against Delay Spoof Attack in GPS using Adaptive Filtering

M. Moazedi, M. R. Mosavi*, P. Teymoori, A. R. Baziar
Iran University of Science and Technology
(Received: 11/07/2014; Accepted: 28/06/2015)

Abstract

The civilian GPS signals are unencrypted, predictable and low power ones. Therefore, they are vulnerable to destroyer interfaces such as spoofing. In this paper, in order to reduce spoofing effect and achieve time series without interface, an adaptive filter with finite impulse response based on Least Mean Square (LMS) algorithm has been used for the first time. Contrary to the previous methods, proposed approach needs no extra hardware and structural change in GPS receiver. Input signal of utilized adaptive filter is pseudo-range data in navigation section. The principle of using adaptive filter to eliminate interference is obtaining an estimate of interfering signal and subtracting that from the corrupted signal. Therefore, what remains at final output is the authentic signal. In this paper, root mean square (RMS) criteria is used to validate the proposed method. Simulation results show that the proposed approach can neutralize laboratory interface effects average up to 95 percent and measurement spoofing effect in average of 81 percent.

Keywords: Adaptive Filter, Delay Spoof, Searching Methods, LMS Algorithm.

* Corresponding Author E-mail: m_mosavi@iust.ac.ir

۱. مقدمه

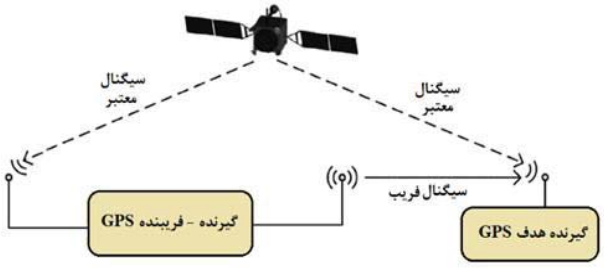
کاربرد سامانه‌های بی‌سیم که برای موقعیت‌یابی، ناوبری و هم‌زمانی نیازمند GPS هستند، روزبه‌روز در حال افزایش است. وابستگی شدید سامانه‌های مختلف به GPS سبب گشته از سال ۲۰۰۰ میلادی تحقیقات عمده‌ای به حفاظت از آن معطوف شود. برخلاف سیگنال‌های GPS نظامی، سیگنال‌های GPS غیرنظامی حفاظت شده (رمز شده) نیستند.

سیگنال‌های GPS به دلیل طی نمودن مسافت طولانی از ماهواره‌ها تا زمین، در سطح زمین توانی کم و در حدود 10^{-16} وات دارند. ازاین‌رو این سیگنال‌ها در برابر حملاتی چون انسداد، جمینگ و فریب آسیب‌پذیرند. در مورد حمله انسداد و جمینگ، گیرنده قادر به تولید اطلاعات موقعیت‌یابی نخواهد بود و بنابراین از حمله آگاه است. اما در شرایط فریب، گیرنده تحت تداخل عمدی قرار گرفته و از وجود حمله اطلاع دارد و در نتیجه اطلاعات موقعیت‌یابی و زمانی اشتباه تولید می‌کند [۱]. ازاین‌رو حمله فریب به مراتب خطرناک‌تر از انسداد و جمینگ است.

تولید حمله فریب را می‌توان به سه دسته کلی فریب ساده، متوسط و پیچیده تقسیم‌بندی نمود [۳-۱]. در فریب ساده، شبیه‌ساز سیگنال GPS که در پایانه ورودی گیرنده قرار دارد از سیگنال معتبر کپی‌برداری می‌نماید. سیگنال فریب تولیدی نسبت به سیگنال اصلی دامنه بزرگ‌تری دارد و هم‌زمان نیست. در نتیجه گیرنده تجاری ارزان قیمت، توسط این روش به سادگی فریب داده می‌شود [۲]. نوع متوسط فریب، فریبنده بر اساس گیرنده است که در این مورد فریبنده از یک گیرنده GPS به همراه آنتن فرستنده سیگنال تداخل تشکیل شده است. همان‌طور که در شکل (۱) مشاهده می‌شود، در روش دوم فریبنده سیگنال معتبر را دریافت نموده و پس از اعمال تغییرات لازم سیگنال جدید با مختصات جعلی را به سمت گیرنده هدف می‌فرستد. دو نوع کلی فریب تأخیری و هم‌زمان برای این دسته از حمله فریب وجود دارد و تشخیص آن به مراتب سخت‌تر از فریب نوع اول است [۱].

در نوع سوم تولید فریب که فریب پیچیده نامیده می‌شود، باید مختصات مرکز آنتن گیرنده هدف با دقت بالا برای فریبنده مشخص بوده و گیرنده قادر به ایجاد هم‌زمانی دقیق فاز کد و فرکانس حامل سیگنال فریب و معتبر باشد. کارایی این روش تولید فریب به مراتب بیشتر از دو روش قبلی است. محقق نمودن فریب پیچیده در برخی موارد به علت متحرک بودن گیرنده یا هندسه خاصی آن، دور از دسترس است [۳].

تاکنون روش‌های زیادی به منظور مقابله با فریب مطرح شده‌اند که می‌توان آن‌ها را در دو دسته کلی تشخیص و کاهش فریب طبقه‌بندی نمود [۷-۳]. در این مقاله روشی جدید برای جبران خطای ناشی از حمله فریب با استفاده از فیلتر تطبیقی[1] در گیرنده‌های تک‌فرکانسه GPS پیشنهاد شده است.



شکل ۱. فریبنده براساس گیرنده [۱].

در ادامه ابتدا برخی روش‌های کاهش فریب به اختصار شرح داده می‌شوند. در بخش سوم مروری بر فیلترهای FIR و الگوریتم‌های تطبیقی خواهید داشت. بخش چهارم و پنجم به معرفی راهکار ارائه شده به منظور کاهش فریب تأخیری با استفاده از فیلترهای تطبیقی اختصاص دارند و در نهایت در بخش ششم آزمون‌های انجام شده بر روی داده‌های آزمایشگاهی و اندازه‌گیری به منظور اعتبارسنجی راهکار پیشنهادی بررسی می‌شوند.

۲. روش‌های پیشین به منظور کاهش خطای فریب

در این بخش برخی از روش‌های مهم کاهش فریب آمده است. خنثی نمودن کامل سیگنال معتبر توسط سیگنال فریب کار بسیار سختی بوده و تنها زمانی که اطلاعات بسیار دقیقی از موقعیت نسبی مرکز فاز آنتن هدف و فریبنده موجود باشد، امکان‌پذیر است. اغلب، این اطلاعات به صورت دقیق در دسترس نیست و علی‌رغم موفقیت‌آمیز بودن حمله فریب نشانه‌ای از سیگنال معتبر باقی می‌ماند که می‌تواند برای شناسایی و کاهش فریب مورد استفاده قرار گیرد [۷-۱].

کاهش فریب از طریق ردیابی سیگنال معتبر: در این روش ابتدا گیرنده نسخه دیجیتال خروجی بخش RF را در حافظه بافر ذخیره می‌نماید. سپس یکی از سیگنال‌های در حال ردیابی GPS توسط گیرنده را به صورت محلی تولید و از سیگنال بافرشده حذف می‌نماید. در نهایت گیرنده ردیابی را با PRN همان سیگنال بر روی داده‌های بافر شده انجام می‌دهد. در این روش گیرنده نیازمند کانال‌های بیشتری برای ردیابی هر دو سیگنال اصلی و فریب است. ازاین‌رو پیاده‌سازی آن پیچیدگی سخت‌افزاری و پردازشی گیرنده را افزایش می‌دهد.

کاهش فریب از طریق گیرنده چند آنتنه و هدایت صفر: در گیرنده‌های چند آنتنه با استفاده از روش‌های پردازش آرایه‌ای می‌توان خطای فریب را کاهش داد. بنابراین گیرنده پس از تشخیص جهت سیگنال جعلی، با هدایت سیگنال صفر به سمت منبع تولید فریب آثار خطرناک آن را خنثی می‌نماید. اگر از یک گیرنده N آنتنه استفاده شود، یک آنتن از گیرنده به عنوان مرجع انتخاب و مرکز

[1] Adaptive Filter

دستگاه مختصات روی آن نقطه در نظر گرفته می‌شود. با فرض وجود یک فریبنده تک آنتنه، حاصل نمونه‌برداری از ترکیب سیگنال معتبر و فریب دریافتی در آنتن‌های گیرنده هدف مانند رابطه (۱) است.

$$r(nT_s)=\begin{bmatrix} r_1(nT_s) \\ \vdots \\ r_N(nT_s) \end{bmatrix}=\sum_{m=1}^{N_{Auth}} a_m\sqrt{P_m^a}\,F_m^a(nT_s)+ b\sum_{q=1}^{N_{Auth}}\sqrt{P_q^s}\,F_q^s(nT_s)+\eta(nT_s) \quad (۱)$$

که در آن، $r(nT_s)$ برداری با اندازه N×1 شامل نمونه سیگنال‌های دریافتی در N آنتن گیرنده است. P_m^a و P_q^s به ترتیب توان سیگنال معتبر m ام و فریب qام هستند. تابع f بیان‌گر فرکانس داپلر سیگنال معتبر و فریب در زمان nT_s و بردار $\eta(nT_s)$ نویز سفید اضافه شونده است. بنابراین اگر برداری مانند f^H با اندازه N×1 موجود باشد که در رابطه (۲) صدق کند، می‌توان سیگنال فریب را از سیگنال اصلی حذف نمود. ازاین‌رو اعمال بردار بهره f^H به سیگنال‌های نمونه‌برداری شده، منجر به رابطه (۳) می‌شود [۸].

$$f^H b=0\,,\|f\|=1 \quad (۲)$$

$$s(nT_s)=f^H r(nT_s)=\sum_{m=1}^{N_{Auth}} f^H a_m\sqrt{P_m^a}\,F_m^a(nT_s)+b\sum_{q=1}^{N_{Auth}} f^H\sqrt{P_q^s}\,F_q^s(nT_s)+\eta(nT_s) \quad (۳)$$

که در آن، $F_q^a(nT_s)$ و $F_m^s(nT_s)$ به ترتیب ترکیبی از بیت‌های موقعیت‌یابی دریافتی و رشته کد C/A مربوط به سیگنال‌های معتبر qام و فریب sام هستند. در مرجع [۹] از شیوه گیرنده چند آنتنه تحت عنوان روش McDowell به منظور کاهش فریب استفاده شده است. در این روش گیرنده برای محاسبه بردار بهره نیازمند پردازش روی تمام نسخه‌های دریافتی سیگنال معتبر و جعلی است. ازاین‌رو به شکل قابل توجهی نیازهای سخت‌افزاری و پردازشی گیرنده را افزایش می‌دهد. در مرجع [۸] از گیرنده دو آنتنه که پیچیدگی محاسباتی پایینی دارد، برای حذف سیگنال فریب استفاده شده است. در این روش گیرنده با محاسبه همبستگی متقابل بین سیگنال‌های دریافتی از دو آنتن قادر به استخراج ویژگی‌های فضایی سیگنال فریب است.

بررسی صحت استقلال موقعیت در گیرنده[۱] (RAIM): سیگنال‌های فریب به طور مؤثر سبب تولید شبه فاصله جعلی در گیرنده GPS می‌شوند. اگر در یک اندازه‌گیری متوالی در لحظه‌ای از زمان فریب ایجاد شود، مکان‌یابی یکپارچه نبوده و در لحظه ایجاد فریب موقعیت نامعقول جعلی تولید می‌گردد [۱۰]. روش توسعه‌یافته RAIM گزارش نیز شده است[۳] که توانایی آشکارسازی و ممانعت از اندازه‌گیری‌های نامعقول را دارد. الگوریتم مقابله با فریب RAIM به عنوان یک روش ضدفریب در سطح حل معادلات موقعیت‌یابی به کار می‌رود. این روش تنها زمانی کاربرد دارد که یک یا دو اندازه‌گیری جعلی در بین چندین اندازه‌گیری معتبر وجود داشته باشد. در گزارشی با محاسبه ضریب VIAS[۲]، قابلیت روش RAIM را برای گیرنده‌ای نشان داده شده که در معرض حمله فریب قرار گرفته است[۱۱].

روش‌هایی که در بالا معرفی شدند، از پر کاربردترین روش‌ها در خصوص کاهش فریب هستند. همان‌طور که از توضیحات استنباط می‌شود، این روش‌ها پیچیدگی سخت‌افزاری و نرم‌افزاری زیادی به گیرنده تحمیل می‌نمایند. در مقایسه با روش‌های مذکور، روش پیشنهادی در این مقاله علاوه بر سادگی در پیاده‌سازی سخت‌افزاری و برنامه‌نویسی نرم‌افزاری قابلیت ردیابی سریع تغییرات ورودی، عدم ایجاد تأخیر در محاسبه خروجی را به همراه دارد و فضای حافظه زیادی را اشغال نمی‌کند.

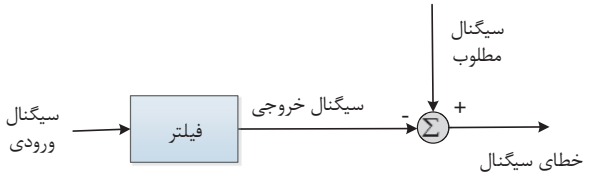
۳. مروری بر فیلترهای FIR و تطبیقی

کلمه فیلتر در حوزه زمان دلالت بر سامانه‌ای دارد که با پردازش نمونه‌های وزن‌دار و تأخیر یافته ورودی طبق قواعدی معین خروجی را تولید می‌کند. قواعد معینی مشخص کننده نوع فیلتر هستند. فیلتر در حوزه فرکانس نیز سامانه‌ای است که بر اساس ویژگی‌های مطلوب خروجی، بازه فرکانسی مشخصی را عبور می‌دهد و بقیه را حذف می‌کند. به طور خلاصه، از فیلترها به منظور تغییر سیگنال ورودی به گونه‌ای که سیگنال مطلوب در خروجی حاصل گردد، استفاده می‌شود [۱۲].

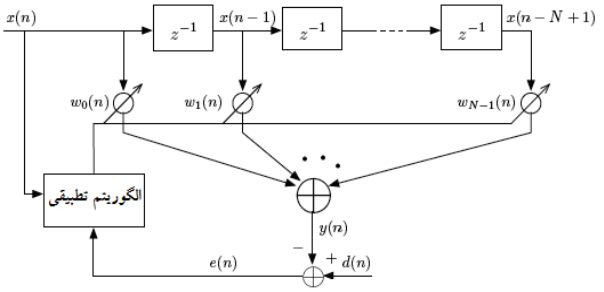
در شکل (۲) نمودار بلوکی کلی فیلترهایی که در مسائل مختلف به منظور تخمین سیگنال مطلوب استفاده می‌شوند، نمایش داده شده است [۱۲]. نکته مهم در اینجا تنظیم وزن‌های فیلتر به گونه‌ای است که بتوان بالاترین تطبیق بین خروجی فیلتر و خروجی مطلوب را ایجاد نمود. برای دستیابی به این منظور از الگوریتم بهینه‌سازی تابع هدف[۳] استفاده می‌شود که می‌تواند به دو صورت آماری[۴] یا قطعی[۵] تعریف شود. از جمله توابع هدف آماری که بیشتر در مسائل حذف سیگنال مزاحم کاربرد دارند، می‌توان به تابع MSE[۶] اشاره نمود که بهینه‌سازی آن از نوع کمینه نمودن است. معمول‌ترین ساختار در پیاده‌سازی فیلترهای تطبیقی، ساختار تراگذار[۷] است که در شکل (۳) مشاهده می‌شود و در آن x(n) مبین ورودی، y(n) خروجی و d(n) سیگنال مطلوب است. در این فیلتر y(n) با ترکیب نمونه‌های وزن یافته ورودی تولید می‌گردد. $W_i(n)$ وزن‌های فیلتر است که با زمان تغییر می‌نمایند. ساختار تراگذار معرفی شده برای فیلتر تطبیقی از نوع ساختارهای غیر بازگشتی است که برای محاسبه خروجی سازوکار بازخوردی ندارد. فیلتر به‌کار رفته در هسته ساختار شکل (۳) فیلتر FIR[۸] است.

[1] Receiver Autonomous Integrity Monitoring
[2] Vulnerability Index Against Spoofing

[3] Performance Function
[4] Stochastic
[5] Deterministic
[6] Mean Square Error
[7] Transversal
[8] Finite Impulse Response



شکل ۲. ساختار کلی یک فیلتر تطبیقی [۱۲].



شکل ۳. نمودار بلوکی فیلتر تراگذر [۱۲].

فیلتر FIR بر خلاف IIR[1] در حوزه زمان پاسخ ضربه با طول محدود دارد. رابطه (۴) معادله تفاضلی فیلتر IIR بازگشتی است (شکل (۴)).

$$y(n) = \sum_{i=0}^{N-1} a_i(n)x(n-i) + \sum_{i=0}^{M-1} b_i(n)y(n-i) \qquad (۴)$$

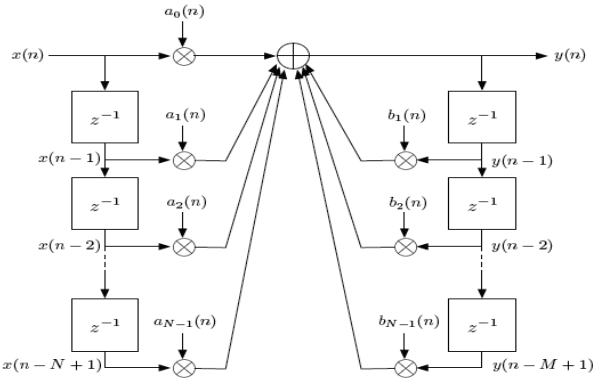
کاربرد فیلترهای IIR به دلیل طول عمر نامحدود و عدم امکان تنظیم وزن، در فیلترهای تطبیقی با محدودیت مواجه است. استفاده از فیلترهای IIR در فیلترهای تطبیقی می‌تواند موجب ناپایداری سامانه شود. علاوه‌براین اعمال تابع هدف MSE به فیلتر IIR منجر به تولید حداقل‌های محلی متعدی می‌شود. با توجه به شکل (۵)، فیلترهای FIR ساختار غیر بازگشتی دارند و ناپایدار نیستند. علاوه بر این با توجه به اینکه اعمال تابع هدف MSE به فیلتر FIR منجر به تنها یک مقدار حداقل می‌شود، الگوریتم قادر است به سرعت و بدون احتمال گیر افتادن در حداقل‌های محلی، کمینه مطلق را پیدا کند.

ازاین‌رو در فیلترهای تطبیقی به جای استفاده از فیلترهای IIR به عنوان هسته فیلتر، از فیلترهای FIR استفاده می‌شود و طراحان به منظور تنظیم وزن‌های فیلتر FIR از الگوریتم‌های تطبیقی بهره می‌گیرند. الگوریتم‌های تطبیقی در واقع روش‌های کاوش‌گر تکرار شونده هستند. از جمله این روش‌ها می‌توان به الگوریتم‌های SD[2]، MSE، LMS و نیوتن اشاره کرد [۱۳ و ۱۴].

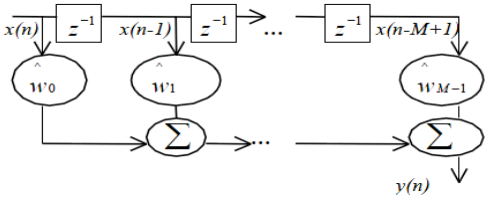
تحقق‌پذیری روش‌های LMS[3] و MSE به‌دلیل سادگی‌شان نسبت به سایر روش‌ها بیشتر است. همان‌طور که در بخش چهارم توضیح داده خواهد شد، روش LMS به عنوان تخمینی از الگوریتم MSE، پیچیدگی محاسباتی و فضای حافظه مورد نیاز را تا حد زیادی کاهش داده و بنابراین قابلیت استفاده در کاربردهای بلادرنگ را نیز دارد و از این لحاظ در کاربرد حاضر نسبت به MSE اولویت دارد [۱۵].

۴. استفاده از فیلترهای تطبیقی به منظور کاهش تداخل

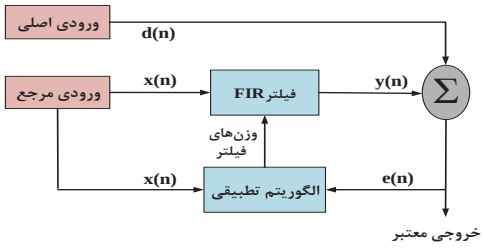
همان‌طور که در بخش قبل گفته شد، استفاده از فیلتر تطبیقی به عنوان یکی از روش‌های حذف تداخل از سیگنال مخرب محسوب می‌شود. وقتی سیگنال به تداخل (نویز، چند مسیری[4]، فریب و غیره) آغشته می‌شود، با استفاده از فیلتر تطبیقی می‌توان سیگنال مطلوب را از تداخل تفکیک کرد. در واقع فیلتر تطبیقی، فیلتر دیجیتالی خود اصلاح‌گری است که وزن‌های آن با توجه به حداقل شدن تابع هزینه (تابعی از خطا) تنظیم می‌گردد. تابع هزینه معمولاً به صورت تفاضل خروجی فیلتر و سیگنال مطلوب تعریف می‌شود. همان‌طور که در شکل (۶) مشاهده می‌گردد، فیلتر تطبیقی یک سامانه بازخورددار شامل دو ورودی اصلی[5] d(n) و مرجع[6] x(n)، یک خروجی معتبر، فیلتر FIR و الگوریتم تطبیقی به منظور تنظیم وزن‌های فیلتر FIR است. در ادامه این بخش هر یک از اجزای فیلتر تطبیقی توضیح داده می‌شود.



شکل ۴. ساختار فیلتر IIR [۱۲].



شکل ۵. ساختار فیلتر FIR در حوزه Z [۱۲].



شکل ۶. نمودار بلوکی فیلتر تطبیقی پیشنهادی.

۴-۱. ورودی‌های فیلتر تطبیقی

سیگنال‌های مرجع و اصلی با اندازهN، ورودی‌های فیلتر هستند.

[1] Infinite Impulse Response
[2] Steepest Decent
[3] Least Mean Square
[4] Multi-path
[5] Primary
[6] Reference

سیگنال d(n) طبق رابطه (۵)، ترکیبی از سیگنال‌های مطلوب S(n) و تداخل x'(n) است. ورودی x(n) نیز فقط شامل تداخل است. به منظور حذف تداخل از سیگنال اولیه و دستیابی به سیگنال مطلوب در خروجی فیلتر تطبیقی، باید شروط (۵) تا (۸) در مورد x(n)، x'(n) و S(n) برقرار باشند.

$$d(n) = S(n) + X'(n) \quad (۵)$$

$$E[S(n)X'(n-k)] = 0 \quad (۶)$$

$$E[S(n)X(n-)] = 0 \quad (۷)$$

$$E[X(n)X'(n-k)] = p(k) \quad (۸)$$

به طور خلاصه عبارت‌های بالا به این معنا هستند که جزء سیگنال مطلوب موجود در ورودی اصلی نباید با جزء تداخل ورودی اصلی و نیز ورودی مرجع همبستگی داشته باشد، اما جزء تداخل سیگنال اصلی و ورودی مرجع با هم همبسته بوده و تابع همبستگی آن‌ها p(k) باشد.

۴-۲. فیلتر FIR

همان‌طور که در بخش سوم توضیح داده شد فیلتر FIR که با نام تمام صفر نیز شناخته می‌شود، به دلیل انطباق‌پذیری بالا، پایداری و سادگی در پیاده‌سازی، در این کاربرد مورد استفاده قرار می‌گیرد. خروجی فیلتر FIR از رابطه (۹) به‌دست می‌آید.

$$y(n) = \sum_{i=0}^{M-1} W_i(n)X(n-i) \quad (۹)$$

۴-۳. الگوریتم تطبیقی

تابع خطا که برای تنظیم وزن‌های فیلتر FIR به‌کار می‌رود، مطابق رابطه (۱۰) به‌دست می‌آید. اگر تابع هزینه E طبق رابطه (۱۱) به صورت متوسط مربعات خطا (MSE)، تعریف گردد، کمینه‌سازی تابع هزینه به روش مستقیم منجر به معادلات وینر- هوپ می‌شود که در رابطه (۱۲) بیان شده است.

$$e(n) = d(n) - y(n) = S(n) + x'(n) - y(n) \quad (۱۰)$$

$$E = {}^{1}/_{N} \sum_{n=0}^{N-1} e^2(n) \quad (۱۱)$$

$$\sum_{l=0}^{M-1} W_i(n) r_{xx}(i-l) = 2r_{dx}(i)\ , i = 0, \dots, M-1 \quad (۱۲)$$

در رابطه (۱۲)، $r_{xx}(i)$ تابع خودهمبستگی ورودی مرجع و $r_{dx}(i)$ تابع همبستگی متقابل بین ورودی مرجع و اصلی است. این رابطه منجر به M معادله خطی می‌شود که با حل آن‌ها می‌توان M وزن بهینه مربوط به فیلتر FIR را در زمان n به‌دست آورد. اگر روابط (۸-۵) برقرار باشند، سیگنال S(n) تحت تأثیر فیلتر FIR قرار نمی‌گیرد. ازاین‌رو حداقل شدن E به معنای حداقل شدن x'(n)-y(n) است. هرقدر x'(n) با x(n) همبستگی بیشتری داشته باشد، مقدار x'(n)-y(n) به صفر نزدیک‌تر خواهد بود. بنابراین جزء تداخل موجود در سیگنال اصلی در خروجی فیلتر FIR ظاهر شده و فیلتر عملکرد بهتری خواهد داشت. در مقابل، اگر x'(n) با x(n) همبستگی نداشته باشد، E[d(n)x(n-k)]=0 می‌گردد و طبق رابطه (۱۲) ورودی d(n) به خروجی راه می‌یابد، در نتیجه خروجی بدون تغییر باقی می‌ماند.

چون در الگوریتم MSE نیاز به محاسبه تابع خودهمبستگی سیگنال مرجع و نیز تابع همبستگی متقابل سیگنال اولیه و مرجع می‌باشد، کلیه نمونه‌ها از ابتدای شروع به‌کار الگوریتم تا لحظه حال مورد نیاز است و بنابراین در کاربردهای بلادرنگ نمی‌توان از این روش استفاده کرد. ازاین‌رو با توجه به استاتیک بودن سیگنال ورودی از الگوریتم LMS به عنوان تخمینی از الگوریتم MSE، به منظور تخمین وزن‌های فیلتر FIR استفاده می‌گردد. در روش LMS استفاده از شیوه گرادیان نزولی به منظور کمینه‌سازی تابع هزینه منجر به رابطه بازگشتی (۱۳) برای تنظیم وزن‌های فیلتر FIR می‌شود.

$$W_i(n) = W_{i-1}(n) + \mu e(n)X(n-i) \quad (۱۳)$$

μ در رابطه (۱۳) گام پیشرفت[1] الگوریتم را مشخص می‌کند که در واقع تعیین‌کننده سرعت همگرایی الگوریتم است. انتخاب مقادیر بزرگ برای گام پیشرفت سبب همگرایی سریع الگوریتم می‌گردد، اما در مواردی نیز ناپایداری سامانه را به‌دنبال خواهد داشت. اگر M طول فیلتر و P_X توان سیگنال مرجع باشد، برای اطمینان از پایدار ماندن سامانه μ در بازه $0 < \mu < \frac{1}{10MP_x}$ انتخاب می‌گردد که طول فیلتر یکی از پارامترهای قابل تنظیم آن است. MDL کمینه طول فیلتر است که نیازهای مسئله را برآورده می‌سازد و از رابطه (۱۴) به‌دست می‌آید.

$$MDL(M) = -L(\theta) + \frac{1}{2} M \ln N \quad (۱۴)$$

که در آن، N طول سیگنال ورودی است. مقداری از M که منجر به حداقل شدن رابطه (۱۴) می‌شود، بیانگر طول بهینه فیلتر FIR است.

۵. راهکار ضد فریب پیشنهادی با استفاده از فیلتر تطبیقی

همان‌طور که در بخش اول مطرح شد، ساده‌ترین نوع فریب، فریب تأخیری است. در این نوع فریب، سیگنال اصلی به همراه نمونه تأخیر یافته آن به سمت گیرنده هدف فرستاده می‌شود. در اینجا فرض بر این است که سیگنال اولیه و مرجع (ورودی‌های فیلتر تطبیقی) ترکیبی از سیگنال معتبر و نمونه تأخیر یافته آن هستند. در گزارشی با استفاده از فیلتر تطبیقی، تداخل چند مسیری از سیگنال معتبر حذف شده است [۱۶]. با توجه به اینکه تأثیر تداخلات فریب تأخیری و چند مسیری در خروجی همبسته‌گرهای گیرنده یکسان است، می‌توان این ایده را نیز در خصوص حذف تداخل فریب به‌کار گرفت. همان‌طور که در بخش قبل توضیح داده شد، فیلتر تطبیقی دارای دو ورودی اصلی و مرجع می‌باشد که ورودی اصلی ترکیبی از سیگنال مطلوب و تداخل است. ورودی مرجع جزء تداخل به تنهایی می‌باشد. در مورد سیگنال‌های GPS جزء تداخل به تنهایی در

[1] Step Size

دسترس نیست و ترکیب آن با سیگنال معتبر در اختیار است. بنابراین در روش پیشنهادی به جای استفاده از جزء تداخل، در ورودی مرجع از سیگنال معتبر آغشته به فریب استفاده می‌شود. بنابراین روابط (۸-۵) به صورت جزئی برقرارند. سیگنال‌های ورودی اصلی و مرجع به ترتیب مطابق روابط (۱۶ و ۱۷) می‌باشند.

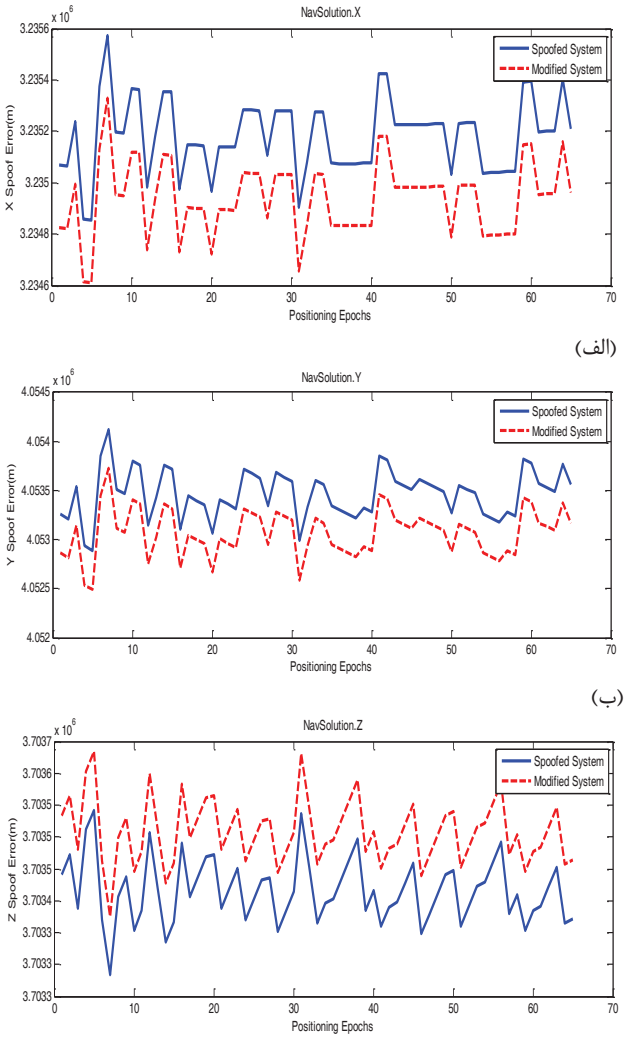
$$d(n) = S(n) + X_{spoof}(n) \quad (16)$$

$$r(n) = S'(n) + X'_{spoof}(n) \quad (17)$$

در این روابط، S(n) و S'(n) سیگنال‌های معتبر هستند (که در حالت کلی با توجه به ساختار سیگنال‌های GPS با هم همبستگی ندارند) و Xspoof و X'spoof سیگنال‌های فریب هستند که با هم همبستگی دارند که هر دو نمونه تأخیر یافته سیگنال معتبر هستند. در واقع آنچه در خروجی فیلتر FIR ظاهر می‌شود، بخشی از سیگنال ورودی d(n) است که با جزئی از سیگنال ورودی r(n) همبستگی دارد و جزء همسان[1] نامیده می‌شود. با کسر نمودن جزء همسان از سیگنال d(n) جزئی از سیگنال ورودی d(n) در خروجی فیلتر تطبیقی کلی ظاهر می‌گردد که با سیگنال ورودی r(n) همبستگی ندارد و جزء ناهمسان[2] را تشکیل می‌دهد.

۶. نتایج و بحث

کارایی روش پیشنهادی با استفاده از دو مجموعه داده فریب آزمایشگاهی و اندازه‌گیری سنجیده شده است. در تولید فریب تأخیری در نوع آزمایشگاهی سیگنال تداخل که در واقع نمونه تأخیر یافته سیگنال معتبر با دامنه بزرگ‌تر است در سطح فرکانس میانی با سیگنال معتبر ترکیب می‌شود. ازاین‌رو سیگنال متداخل عملکرد گیرنده را در بخش همبسته‌گیری و موقعیت‌یابی تحت تأثیر قرار می‌دهد. در تولید داده‌های فریب اندازه‌گیری، فریبنده سیگنال معتبر را دریافت و ذخیره نموده و با تأخیر و دامنه معین به سمت گیرنده هدف ارسال می‌کند. بنابراین سیگنال تأخیر یافته هم‌زمان با سیگنال‌های لحظات بعدی به گیرنده هدف می‌رسد و سبب ایجاد تداخل در این سیگنال‌ها می‌شود. این نوع نحوه تولید تداخل تولید فریب از طریق تأخیر و ترکیب نامیده می‌شود [۱۷]. فیلتر پیشنهادی در گیرنده نرم‌افزاری GPS در بخش موقعیت‌یابی به داده‌های فریب تأخیری آزمایشگاهی و اندازه‌گیری اعمال شد. به این نحو که خروجی بخش موقعیت‌یابی در سطح شبه فاصله به عنوان ورودی به فیلتر پیشنهادی وارد می‌شود، فیلتر جزء تداخل را از سیگنال معتبر جدا کرده و پس از بازیابی شبه فاصله‌های معتبر معادلات موقعیت‌یابی با استفاده از آن‌ها به منظور دستیابی به مختصات مکانی صحیح حل می‌شوند. نتایج اعمال الگوریتم بر روی چهار مجموعه داده شبیه‌سازی به صورت خلاصه در جدول (۱) آمده است. با توجه به اینکه خطای اندازه‌گیری کمتر از ۱ متر است، مقادیر خطای گزارش شده ناشی از حمله فریب هستند. در تمام موارد داده‌های ورودی اصلی و مرجع با عدد ۱۰۰۰ نرمالیزه شده و نیز اندازه فیلتر FIR برابر ۴ در نظر گرفته شده است. لازم به ذکر است که در طراحی فیلتر تبادل مناسبی بین گام پیشرفت و سرعت همگرایی الگوریتم در نظر گرفته شده و فیلتر مورد بحث در کاربردهای بلادرنگ نیز می‌تواند مورد استفاده قرار گیرد. مطابق جدول (۱)، حداقل کاهش فریب در الگوریتم پیشنهادی ۸۸ درصد، حداکثر کاهش فریب برابر ۹۸ درصد و متوسط کاهش فریب ۹۵ درصد است. همچنین به منظور راست‌آزمایی مطمئن‌تر، الگوریتم کاهش فریب بر روی داده‌های فریب اندازه‌گیری ۴، ۶ و ۸ ثانیه اعمال گشته و نتایج آن در جدول (۲) ذکر شده است. همان‌طور که در جدول (۲) مشاهده می‌شود، راهکار ارائه شده خطای RMS ناشی از فریب تأخیری داده‌های اندازه‌گیری را حداقل ۵۵ درصد و حداکثر تا ۹۶ درصد و به طور متوسط ۸۱ درصد جبران نموده است. علت پایین‌تر بودن درصد کاهش خطای موقعیت‌یابی داده‌های اندازه‌گیری نسبت به داده‌های آزمایشگاهی این است که داده‌های اندازه‌گیری علاوه بر تداخل فریب به تداخلات فرکانس بالای محیطی نیز آلوده شده‌اند. به منظور بررسی اثرگذاری الگوریتم در گیرنده GPS، نتایج ناوبری برای داده‌های فریب نمونه در سه بعد قبل و بعد از اعمال الگوریتم در شکل (۷) آمده است.



شکل ۷. نتایج مکان‌یابی داده تأخیری ۴ ثانیه با فریب ۴۷۸ متر: (الف) بعد طول، (ب) بعد عرض و (ج) بعد ارتفاع

[1] Coherent Component
[2] Incoherent Component

همان‌طور که در شکل مشاهده می‌شود، نتایج ناوبری داده‌های فریب قبل و بعد از اعمال الگوریتم نشان دهنده این موضوع است که کلیه نمونه‌ها پس از اعمال الگوریتم در هر بعد انتقال مکانی یکسانی دارد و این موضوع نشأت گرفته از ماهیت داده‌های استاتیک در دسترس می‌باشد که با تأخیر زمانی ثابت به کلیه نمونه‌ها اعمال شده است.

جدول ۱. حداکثر کاهش فریب در مورد هر مجموعه داده اصلی

داده فریب	خطای فریب قبل از اعمال الگوریتم (متر)	خطای فریب بعد از اعمال الگوریتم (متر)	متوسط درصد کاهش فریب
مجموعه داده اول	۱۰۳	۱۲	۸۸
مجموعه داده دوم	۱۹۲	۷	۹۶
مجموعه داده سوم	۱۱۴۰	۲۵	۹۸
مجموعه داده چهارم	۹۷۰	۹	۹۸

جدول ۲. نتایج کاهش فریب بر روی داده‌های اندازه‌گیری.

میزان تأخیر داده فریب (ثانیه)	زمان شروع (ثانیه)	قبل از اعمال الگوریتم			بعد از اعمال الگوریتم			درصد کاهش
		RMS	ΔH	ΔEN	RMS	ΔH	ΔEN	
۴	۴۰	۱۵۷	۱۳۳	۸۴	۶	۲	۶	۹۶
	۶۵	۴۷۸	۳۱۳	۳۶۲	۲۹	۱۱	۲۷	۹۴
۶	۴۹	۱۱۳	۴۳	۱۰۵	۵۱	۵۱	۴	۵۵
	۴۵	۲۶۳	۲۰۵	۱۶۵	۵۶	۳۸	۴۲	۷۹
۸	۵۳	۱۷۸	۱۴۷	۱۰۱	۵۶	۳	۵۵	۷۰
	۷۱	۴۵۶	۴۴۰	۱۲۰	۳۹	۳۹	۳	۹۲

۷. نتیجه‌گیری

در این مقاله یک فیلتر تطبیقی بر اساس الگوریتم LMS به منظور تخمین و حذف خطای فریب سیگنال GPS پیشنهاد شد. این الگوریتم در بخش ناوبری گیرنده GPS و بر روی پارامتر شبه فاصله اعمال شده است و می‌تواند در کاربردهای بلادرنگ به‌کار گرفته شود. فیلتر تطبیقی یک تجزیه کننده سیگنال است که قادر است بخش همسان و ناهمسان سیگنال ورودی را از هم جدا کند. بخش همسان که خروجی فیلتر FIR می‌باشد، از ورودی اصلی کم شده و بخش ناهمسان را در خروجی فیلتر کلی تولید می‌نماید که همان سیگنال معتبر است. راست‌آزمایی روش پیشنهادی بر روی دو مجموعه داده فریب GPS در دو صورت آزمایشگاهی و اندازه‌گیری انجام شد و نتایج کارآیی مطلوب الگوریتم را بر هر دو مجموعه داده نشان داد.

۸. مراجع

[1] Humphreys, T. E.; Ledvina, B. M.; Psiaki, M. L. "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer"; In Proc. of the ION GNSS Meeting 2008, 2314-2325.

[2] Montgomery, P. Y.; Humphreys, T. E.; Ledvina, B. M. "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defence Against a Portable Civil GPS Spoofer"; In Proc. of ION Int. Technical Meeting of the Institute of Nav. 2009, 124-130.

[3] Ledvina, B. M.; Bencze, W. J.; Galusha, B.; Miller, I. "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers"; In Proc. of ION Int. Technical Meeting of the Satellite Division 2010, 698-71.

[4] Jahromi, A. J.; Broumandan, A.; Nielsen, J. "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques"; Int. J. Nav. Observ. 2012, 1-16.

[5] Amiri, A. A.; Mosavi, M. R.; Rezaee, M. J.; Hoseinzaeh, N. "Introduce a Neural Network Based Technique for GPS Anti-Spoofing"; Sharif Con. of Future Electronics 2013, 15-17.

[6] Mosavi, M. R.; Nasrpooya, Z.; Rezaee, M. J.; Abedi, A. A.; "Introduce a GPS Anti-Spoofing Technique Based on Kalman Filter"; The 6th Con. of Electronic War, 2013.

[7] Baziar, A. R.; Moazedi, M.; Mosavi, M. R., Ghaffari, Z. "A Novel Technique for GPS Spoofing Detection Based on Pseudo-range Measurements in Order to Protection of Marine Navigation Systems"; Iranian J. Marine Tech. 2014, 1, 8-21.

[8] Daneshmand, S.; Jahromi, A. J.; Broumandan, A.; Lachapelle, G. "A Low Complexity GNSS Spoofing Mitigation Technique using a Double Antenna Array"; GPS World Magazine 2011, 22, 44-46.

[9] McDowell, C. E. "GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling"; US Patent 7,250,903, 2007.

[10] Kuusniemi, H.; Wieser, A.; Lachapelle, G.; Takala, J. "User-level Reliability Monitoring in Urban Personal Satellite-

Navigation"; IEEE Trans. on Aerospace and Electronic Systems 2007, 43, 1305-1318.

[11] Juang, J. C. "GNSS Spoofing Analysis by VIAS"; Coordinates Magazine 2011, 7, 11-13.

[12] Farhang-Boroujeny, B. "Adaptive Filters: Theory and Applications"; 2nd Ed. John Wiley & Sons, Ltd, 2013.

[13] Wang, X. "Method of Steepest Descent and Its Applications"; IEEE Microwave Wireless Components Letter 2008, 12, 24-26.

[14] Charalambous, C.; Conn, A. R. "An Efficient Method to Solve the Minimax Problem Directly"; J. Num. Anal. 1978, 15, 162-187.

[15] Zhang, L. ; Li, K.; Bai, E. "New Extension of Newton Algorithm for Nonlinear System Modelling using RBF Neural Networks"; IEEE Trans. on Automatic Control 2013, 58, 2929 – 2933.

[16] Linlin, G.; Shaowei, H.; Chris, R. "Multipath Mitigation of Continuous GPS Measurements using an Adaptive Filter"; GPS Solutions 2000, 4, 19-30.

[17] Baziar, A. R.; Mosavi, M. R.; Rahmati, A.; Moazedi, M. "A Novel and Low-Cost Technique for Generating GPS Spoofing in Order to Protection from Marine Navigation Systems"; Iranian J. of Marine Tech. 2014, 1, 1-12.