Two New Intelligent Methods for Detecting and Cancelling Spoofing Effects on GPS Receivers

Mohammad Reza Mosavi[1]*, Mohammad Javad Rezaei[2], Nima Hosseinzadeh[3], Ramin Ali Kiaamiri[4]
1,2,3,4- Iran University of Science and Technology
(Reccive: 2013/11/20, Accept: 2014/05/26)

Abstract

One of the goals of spoofing nowadays is to provide the GPS receiver a fake signal. This way, the receiver will produce misleading time and position problems. This paper proposes two new methods for detecting and cancelling spoofing in GPS receivers. These anti-spoofing methods use Kalman filter and recurrent neural network to mitigate spoofing effects on GPS receivers. These methods are also used as an adaptive reduction factor to overcome spoofing effects. The performance of proposed method is analyzed in presence of spoofing signals. Experimental results show that the average pseudo-range RMS error improvement is 45% and 65% for Kalman filter based method and recurrent neural networks based method, respectively.

Keywords:

Spoofing, Pseudo-range, Recurrent Neural Networks, Kalman Filter, Differential GPS.

***Corresponding Author Email:** M_Mosavi@iust.ac.ir

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"

سال دوم، شماره ۱، بهار ۱۳۹۳، ص ۸۱-۷۱

ارائه روش‌های هوشمند برای آشکارسازی و مقابله با سیگنال فریب در گیرنده‌های GPS

سید محمدرضا موسوی[1*]، محمدجواد رضائی[2]، نیما حسین‌زاده[3]، سید رامین‌علی کیاامیری[4]

۱- استاد دانشکده مهندسی برق دانشگاه علم و صنعت ایران، ۲- دانشجوی دکتری مهندسی برق دانشگاه علم و صنعت ایران.

۳- فارغ‌التحصیل کارشناسی مهندسی برق دانشگاه علم و صنعت ایران، ٤- دانشجوی کارشناسی ارشد مهندسی برق دانشگاه آزاد واحد تهران جنوب.

(دریافت: ۹۲/۰۸/۲۹ ، پذیرش: ۹۳/۰۳/۰۵)

چکیده

امروزه فریب از مهم‌ترین و خطرناک‌ترین تهدیدهای پیش روی گیرنده‌هایGPS است که اطلاعات نادرست به گیرنده می‌دهد و مشکلاتی را در محاسبات زمانی و مکانی ایجاد می‌کند. مقابله با فریب از امور مهم در تحقیقات حوزه GPS می‌باشد. در این مقاله دو روش برای آشکارسازی و جبران اثر سیگنال فریب ارائه می‌شود. ابزارهای پیش‌بینی‌شده برای رسیدن به هدف، فیلتر کالمن و شبکه عصبی بازگشتی می‌باشند که از تخمین‌گرهای ساده و قابل پیاده‌سازی روی پردازنده‌های ارزان‌قیمت به حساب می‌آیند. الگوریتم‌های پیشنهادی هم‌چنین از یک ضریب کاهشی تطبیقی برای جبران اثر فریب استفاده می‌نمایند. نتایج شبیه‌سازی روی داده‌های واقعی استخراج‌شده از یک گیرنده تک‌فرکانسه GPS نشان می‌دهند که الگوریتم‌های پیشنهادی مبتنی بر فیلتر کالمن و شبکه عصبی بازگشتی در آشکارسازی وقوع فریب کاملاً موفق می‌باشند و می‌توانند اثر فریب را، به ترتیب به میزان ۴۵ و ۶۵ درصد جبران نمایند. نظر به این‌که داده‌های دریافتی هر یک ثانیه به‌روز می‌شوند، هردو الگوریتم به‌صورت بلادرنگ عمل می‌نمایند.

واژه‌های کلیدی: سیگنال فریب، شبه‌فاصله، شبکه‌های عصبی، فیلتر کالمن، GPS تفاضلی

۱. مقدمه

امروزه گیرنده‌های GPS[1] کاربردهای نظامی و غیرنظامی بسیاری دارند و به‌طور روزمره در بسیاری از وسایل مورد استفاده قرار می‌گیرند، از این‌رو بررسی تهدیدهای احتمالی و رفع آن‌ها از مهم‌ترین موارد پیش‌رو است. استفاده از گیرنده‌های GPS در حوزه‌های گوناگون نظامی و غیرنظامی موجب شده تا تحقیقات زیادی در زمینه‌های انحصاری نمودن و سوءاستفاده از این سیستم در کشورهای مختلف انجام شود. ایجاد مانع[2] در مسیر سیگنال GPS، اختلال[3] و فریب[4] سه نمونه از این تلاش‌ها می‌باشند [۱-۴].

از بین حملات ذکرشده در بند پیشین، فریب به دلیل پنهانی بودن ماهیتش، خطرناک‌ترین حمله به شمار می‌رود. سیگنال فریب امروزه از مهم‌ترین تهدیدهای پیش‌روی گیرنده‌های GPS می‌باشد که مشکلاتی را در محاسبات GPS ایجاد می‌کند. این سیگنال می‌تواند برای منحرف کردن گیرنده‌های دشمن و نیز ایجاد اختلال در آن‌ها، به‌کار گرفته شود. بنابراین، تشخیص و مقابله با چنین سیگنالی، چه در دفاع و چه در حمله امری بسیار مهم می‌باشد [۵].

به‌طور کلی روش‌های مقابله با سیگنال فریب به دو دسته روش‌های رمزنگاری و روش‌های غیررمزنگاری تقسیم می‌شوند. روش‌های رمزنگاری پیچیده بوده و عمدتاً نیاز به تغییر ساختار GPS دارند. از این‌رو به‌کارگیری این روش‌ها با مشکلات بسیاری همراه است. اما روش‌های غیررمزنگاری نسبت به روش‌های رمزنگاری ساده‌تر می‌باشند.

این روش‌ها که عبارت‌اند از آشکارسازی سیگنال نشانه، شکل‌دهی پرتو چندآنتنه و بررسی صحت استقلال گیرنده، نیاز به تغییر ساختار GPS ندارند و صرفاً بر اساس مشخصات سیگنال دریافتی، به آشکارسازی و جبران اثر فریب می‌پردازند.

1. Global Positioning System
2. Blocking
3. Jamming
4. Spoofing

* رایانامه نویسنده پاسخگو: M_Mosavi@iust.ac.ir

عـدم نیـاز به تجـهیزات گـران‌قیـمت ویژگی دیـگر روش‌هـای غیر رمـزنگاری مـی‌باشد. امـا سـه روش ذکرشده در بـالا بـه تـرتیب از کاستـی‌هایی نظـیر پیچیـدگی پـردازش، نیـاز بـه گیرنده‌های چند آنتنه و نیاز به گیرنده‌های دوفرکانسه رنج می‌برند [۶-۸].

از مـتداول‌تـرین ابـزارهای پـیش‌بینی، مـی‌توان به فیلتر کالمن [۹-۱۲] و شبکه عصبی [۱۲-۱۵] اشاره کرد. این ابزارها علاوه‌بر دارا بودن خاصیت پیش‌بینی، خودتصحیح نیز می‌باشند و از این‌رو ابزارهای مناسبی برای آشکارسازی و جبران سیگنال فریب به‌شمار می‌روند. به دلیل ویژگی‌های ذکرشده در بالا و نیز قابلیت پیاده‌سازی الگوریتم‌های مبتنی بر فیلتر کالمن و شبکه عصبی روی پردازنده‌های دیجیتال ارزان‌قیمت، در این مقاله دو الگوریتم آشکارسازی و جبران سیگنال فریب مبتنی بر این دو ابزار پیش‌نهاد شده است. این الگوریتم‌ها از داده‌های شبه‌فاصله یک سیستم مبتنی بر GPS تفاضلی[1] بهره می‌گیرند.

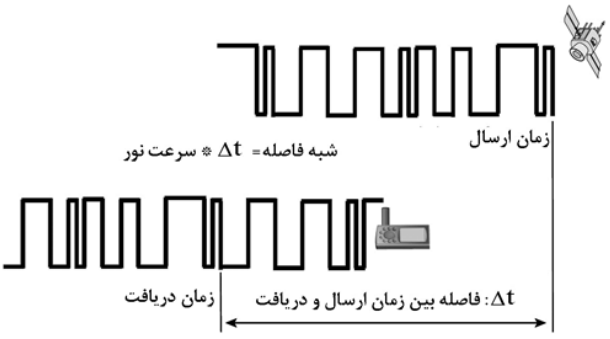
ساختار مقاله پیش‌رو به این صورت است که در ادامه و در بخش بعد، مفاهیم مرتبط با GPS شرح داده می‌شوند. بخش‌های بعدی نیز به‌ترتیب به بررسی سیگنال فریب، معرفی روش‌های مقابله با فریب، بحث پیرامون فیلتر کالمن، شبکه‌های عصبی بازگشتی، ارائه الگوریتم‌های پیشنهادی برای حل مسئله و نتایج شبیه‌سازی اختصاص خواهند داشت. در پایان نیز، نتیجه‌گیری بیان خواهد شد.

۲. مفاهیم مرتبط با GPS

در الگوریتم‌های پیشنهادی (برای آشکارسازی و جبران فریب) از مفاهیمی چون شبه‌فاصله و GPS تفاضلی، بهره گرفته شده است. از آنجایی که آشنایی با این مفاهیم برای درک بهتر بخش‌های آتی ضروری می‌باشد، این بخش به معرفی مفاهیم شبه‌فاصله و GPS تفاضلی می‌پردازد.

۱.۲. شبه‌فاصله

در بخش‌های بعدی، شبه‌فاصله را به عنوان مرجع آشکارسازی فریب به کار خواهیم برد، لذا آشنایی با طریقه محاسبه آن لازم و ضروری است. فاصله بین ماهواره و گیرنده را که به کمک اندازه‌گیری تاخیر در دریافت سیگنال به‌دست می‌آید، شبه‌فاصله گویند. روش اندازه‌گیری بدین صورت است که ماهواره، کد شبه‌تصادفی را تولید و ارسال می‌کند. گیرنده نیز کد مشابهی را تولید می‌نماید. اندازه‌گیری تاخیر Δt کدهای شبه‌تصادفی (گیرنده و ماهواره) توسط یک آشکارساز همبسته انجام می‌گیرد. به محض انطباق کدهای گیرنده و فرستنده، تأخیر حلقه اندازه‌گیری، محاسبه شده و با ضرب کردن آن در سرعت نور، شبه‌فاصله به‌دست می‌آید. یک قاعده کلی برای دقت اندازه‌گیری در روش شبه فاصله، ۱٪ دوره تناوب کد دریافتی است. در شکل ۱ چگونگی محاسبه شبـه‌فاصـله، به نمایش گذاشته شده است [۱، ۲].

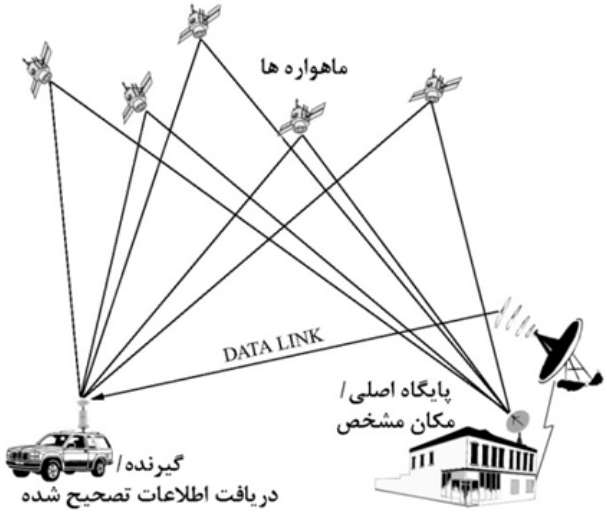


شکل۱. نحوه محاسبه شبه‌فاصله.

۲.۲. GPS تفاضلی

برای مقابله با برخی از خـطاها و بالا بردن دقت سیستم موقعیت‌یابی، می‌توان از روش GPS تفاضلی استفاده کرد. در این روش که در شکل ۲ ساختار آن به نمایش گذاشته شده است، یک گیرنده در نقطه‌ای با موقعیت دقیق و معلوم قرار می‌گیرد. این گیرنده با استفاده از سیگنال‌های دریافتی از ماهواره، موقعیت خود را به‌دست آورده و با موقعیت واقعی مقایسه می‌کند.

با این کار، خطای سیستم به‌دست می‌آید و به دنبال آن، اطلاعات لازم برای تصحیح خطا در این نقطه محاسبه و برای دیگر گیرنده‌های GPS موجود در محل، ارسال می‌گردد. گیرنده‌ها نیز با



شکل۲. ساختار GPS تفاضلی.

1. Differential GPS

دریافت سیگنال تصحیح، محاسبات خود را اصلاح می‌کنند. با این روش می‌توان دقت موقعیت‌یابی ساکن و نیز دقت موقعیت‌یابی متحرک را بهبود بخشید [۳].

۳. فریب در GPS

اعلام گزارشی در سال ۲۰۰۱ از سوی وزارت حمل‌ونقل آمریکا مبنی بر آسیب‌پذیری زیرساخت حمل‌ونقل این کشور به تهدیدهای سیستم‌های ناوبری سبب جلب توجه بیش از پیش محققان به مسئله فریب در سیستم‌های ناوبری، شد. در آن زمان تحقیقات کمی در این حوزه انجام شده بود. بدین ترتیب این مسئله سبب شد که آزمایشگاه‌هایی در چند دانشگاه معتبر دنیا به صورت تخصصی در زمینه فریب و روش‌های مقابله با آن، مشغول به تحقیق شوند [۵].

"فریب و گمراهی" هر دو از جمله حملات فعال محسوب می‌شوند. فریب از نوع حملات فعال نقاب‌دار، و گمراهی (گونه خاصی از فریب) از نوع حملات فعال بازخوانی است. درحمله گمراهی، سیگنال‌های ناوبری تسخیر شده و دوباره روی فرکانس دریافت‌شده ارسال می‌شوند که این عمل سبب اختلال در گیرنده شده و در نتیجه، مختصات اشتباه به گیرنده داده می‌شود. درحالی که فریب (مطابق شکل۳) ارسال سیگنال‌هایی با ساختار مشابه با سیگنال‌های ناوبری اصلی برای تحت کنترل گرفتن حلقه ردیابی گیرنده است [۶].

در میان انواع حمله‌ها، فریب به عنوان خطرناک ترین دخالت عمدی در نظر گرفته شده است که به‌موجب آن، گیرنده GPS با ردیابی سیگنال های جعلی فریب می خورد. حمله فریب از حمله جمینگ خطرناک تر است، زیرا گیرنده نمی تواند حمله فریب را تشخیص بدهد. فریب به دلیل این که مخفیانه می باشد، حمله ای بسیار ظریف‌تر نسبت به حملاتی نظیر ایجاد مانع در برابر سیگنال و یا جمینگ است. به‌طور کلی، فریب حمله‌ای پنهانی است که در آن فریب‌دهنده با تولید سیگنالی جعلی شبیه به سیگنال اصلی، گیرنده را در اندازه‌گیری مکانی و زمانی گمراه می‌کند. مطالعات در مورد واکنش انواع گیرنده‌های GPS در مقابل تهدیدهای سیگنال فریب نشان می‌دهد که چنین حمله‌ای بر اندازه‌گیری‌های گیرنده، اثرات بسیار مخربی دارد [۷].

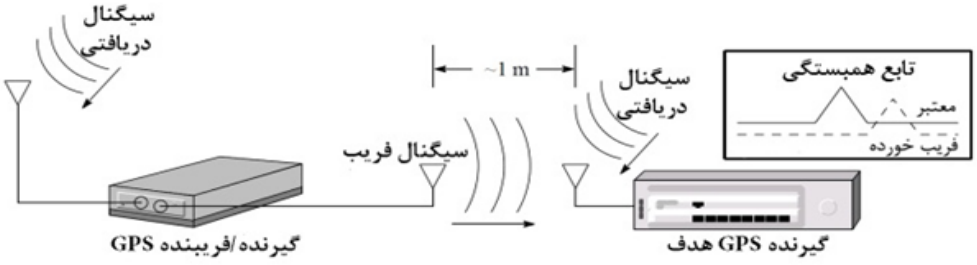
حملات فریب به سه دسته اصلی ساده، متوسط و پیچیده تقسیم‌بندی می‌شوند. در حملات ساده، یک شبیه‌ساز سیگنال‌های ناوبری، سیگنال‌های جعلی را با توان بالا به سمت گیرنده هدف ارسال می‌کند. شناسایی این حمله به‌راحتی امکان‌پذیر است چرا که هیچ همزمانی بین سیگنال‌های جعلی و سیگنال‌های اصلی وجود ندارد. در حملات سطح متوسط، فریب‌دهنده سیگنال‌های جعلی را به‌صورت همزمان‌شده با سیگنال‌های اصلی ارسال می‌کند. مسئله همزمانی موجب می‌شود که امکان شناسایی این حمله کاهش یابد [۸].

در حملات سطح پیچیده، حمله شامل شبکه‌ای از فریب‌دهنده‌ها می‌گردد. این عمل سبب می‌شود هم محتویات سیگنال‌های ناوبری دوباره ارسال شوند و هم اینکه حمله توزیع فضایی داشته باشد و از طریق آنتن‌های چندگانه قابل شناسایی نباشد. از آنجایی که تا کنون حملات سطح متوسط، عملکرد موفقی داشته‌اند، امروزه اکثر تحقیقات در حوزه این دسته از حملات بوده و توجه کمتری به حملات پیچیده می‌شود. شکل ۴ نمونه‌ای از نحوه اعمال فریب متوسط را به نمایش گذاشته است.

۱.۳. آشکارسازی و مقابله با سیگنال فریب

متاسفانه به دلیل پیچیدگی نحوه ایجاد سیگنال فریب و هوشمند بودن آن، روش‌های خیلی زیادی برای مقابله با آن وجود ندارد و روش‌های مقابله، به دو دسته روش‌های رمزنگاری و روش‌های غیررمزنگاری محدود می‌شوند.

روش‌های رمزنگاری تکیه بر کدهای امنیتی غیرقابل پیش‌بینی دارند که در سیگنال‌های ناوبری قرار داده می‌شوند. برای حمله به گیرنده‌های تجهیزشده با این روش‌ها، فریبنده یا باید بتواند کد



شکل۳. ساختار فریب متوسط.

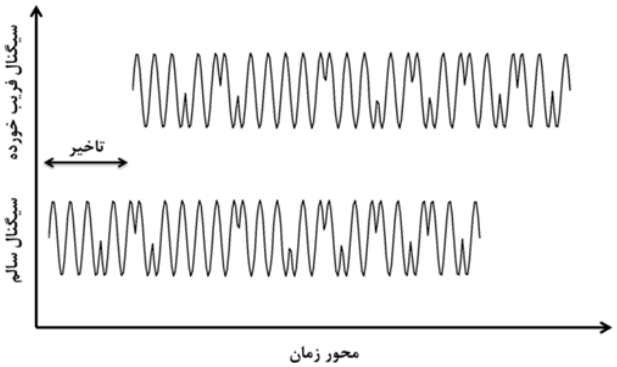
امنیتی را پیش‌بینی کند و یا اینکه سیگنال‌ها را ذخیره و دوباره ارسال نماید. سه روش ضدفریب مبتنی بر رمزنگاری وجود دارد: نخست، روش کدهای امنیتی طیف گسترده (SSSC[1]) که در آن، کدهای امنیتی در میان کدهای L1C[2] ارسال می‌شوند. هنگام ردگیری کدهای L1C، گیرنده می‌تواند زمان ارسال SSSC بعدی را پیش‌بینی کند، ولی نمی‌تواند دنباله و محتویات آن را پیش‌بینی نماید.

با دریافت یک SSSC، گیرنده نمونه‌های پیش‌روی آن را در حافظه ذخیره می‌کند. بعد از مدتی کلیدهای رمزنگاری همراه با پیام‌های ناوبری ارسال می‌شوند. گیرنده با دریافت کلید، SSSC را رمزگشایی می‌کند و از آن و نمونه‌های ذخیره‌شده همبستگی می‌گیرد. اگر همبستگی از یک مقدار آستانه پایین‌تر باشد، یک حمله فریب را شناسایی می‌کند. روش دوم، روش اعتبارسنجی پیام‌های ناوبری (NMA[3]) است که در این روش، از امضای دیجیتال بر روی پیام ناوبری غیرنظامی (CNAV[4]) استفاده می‌شود. ساختار پیام-های CNAV قابل گسترش هستند. از این‌رو نیازی به تغییر شکل پیام‌ها نمی‌باشد. روش سوم، همبستگی کد P(Y) گیرنده‌های دوگانه می‌باشد که در آن، یک گیرنده در محل ایمنی قرار می‌گیرد و کدهای C/A و L1 را دنبال می‌نماید.

این گیرنده از رابطه فاز و زمان بین کدهای C/A و کدهای P(Y) استفاده می‌کند تا کدهای P(Y) را ایزوله و نمونه‌های خام یا تخمینی از کدهای W رمزشده را روی یک شبکه ایمن ارسال نماید. گیرنده دوم که هدف، حفاظت از آن است، همبستگی P(Y) استخراج شده را با نمونه‌ها یا کدهای W دریافت‌شده از گیرنده اول محاسبه می‌کند و اگر زیر یک آستانه مشخص باشد یک حمله فریب شناسایی می‌شود [۵-۸].

در روش‌های غیررمزنگاری، نه از کدهای امنیتی و نه از یک ارتباط جانبی استفاده می‌شود. این روش‌ها عموماً تکیه بر مشاهده تغییرات ویژگی‌های مختلف سیگنال دریافتی دارند. برخی از روش‌های غیررمزنگاری بر اساس به‌کارگیری دو یا چند آنتن بنا نهاده شده‌اند.

به‌کارگیری آنتن‌های متعدد، هزینه‌های سیستم را افزایش می‌دهد. از این‌رو روش‌هایی که تکیه بر یک آنتن دارند، بیشتر مورد توجه قرار می‌گیرند. به‌طور کلی اجرای یک یا چند مورد از اقدامات



شکل۴. مقایسه سیگنال سالم و فریب‌خورده دریافت‌شده توسط گیرنده.

زیر برای آشکارسازی سیگنال‌های GPS مشکوک به حمله فریب، لازم است:

مشاهده توان سیگنال GPS: این اقدام شامل مشاهده و ثبت مقدار متوسط توان سیگنال می‌باشد. مقدار مشاهده‌شده با مقدار مورد انتظار مقایسه می‌شود. اگر مقدار اندازه‌گیری در سیگنال مشاهده‌شده از حد آستانه‌ای از پیش‌تعیین‌شده تجاوز کند، زنگ خطری از فریب برای کاربر به صدا در می‌آید.

مشاهده تغییرات توان سیگنال GPS: در این اقدام، مقدار توان سیگنال دریافتی گیرنده، در هر زمان اندازه‌گیری و ثبت شده و با مقدار ثبت‌شده در زمان قبل مقایسه می‌شود. تغییرات زیاد در این اندازه‌ها می‌تواند نشان‌دهنده وجود فریب باشد. بدین ترتیب به کاربر هشداری در رابطه با احتمال وقوع فریب داده می‌شود.

مشاهده تغییرات شبه‌فاصله: در گیرنده‌های GPS، شبه‌فاصله برای مکان‌یابی به‌کار می‌رود، هرگونه تغییرات بزرگ و پیش‌بینی نشده در اندازه آن می‌تواند دلیل بر وجود فریب باشد.

ثبت اختلاف زمانی: گیرنده‌های GPS ساعت‌های نسبتاً دقیقی دارند. با استفاده از اطلاعات زمانی می‌توان از صحت سیگنال‌های دریافتی اطلاع پیدا کرد. در صورت وجود اختلاف زمانی زیاد بین ساعت گیرنده و ساعت ماهواره، می‌توان احتمال وجود فریب را داد، اما این مسئله باید با دقت بیشتر بررسی گردد.

مشاهده کدهای شناسایی ماهواره و تعداد سیگنال ماهواره‌های دریافتی: مشاهده هرگونه اختلاف در کد ماهواره‌ها یا مشاهده ماهواره مشکوک می‌تواند دلیل بر وجود فریب باشد. روش‌های اشاره شده در بالا به همراه روش‌های دیگر غیررمزنگاری و همچنین روش‌های رمزنگاری برای آشکارسازی و مقابله با فریب به‌کار می‌روند. اما انتخاب روش مناسب بستگی به زمان در اختیار،

1. Spread Spectrum Security Code
2. L1 Civilian
3. Navigation Message Authentication
4. Civil Navigation Message

مقدار هزینه قابل قبول، حجم پردازش قابل قبول و البته داده‌های در دسترس برای پردازش، دارد. این مقاله تغییرات شبه‌فاصله را به عنوان شاخص وجود فریب برمی‌گزیند و از ابزارهای فیلتر کالمن و شبکه عصبی بازگشتی برای آشکارسازی فریب به کمک این شاخص و جبران اثر فریب بر شبه‌فاصله، بهره می‌گیرد.

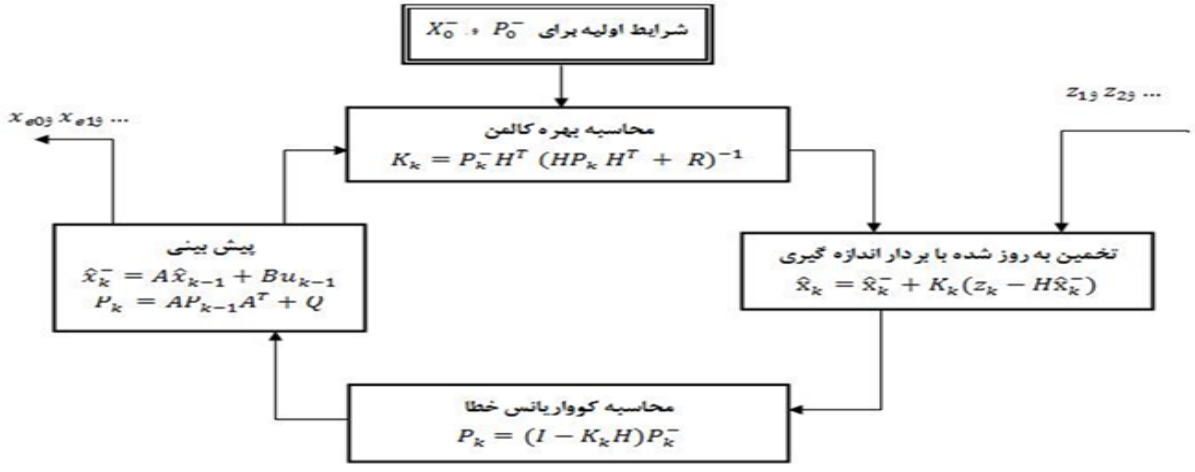
۴. فیلتر کالمن

یکی از شناخته‌شده‌ترین و پرکاربردترین ابزارهای ریاضی موجود، که می‌توان از آن در تخمین و محاسبه فرآیندهای اتفاقی در اندازه‌گیری‌های محیط‌های نویزی استفاده کرد، ابزاری است که تحت عنوان فیلتر کالمن شناخته می‌شود. نام فیلتر کالمن پس از آنکه رادولف کالمن مقاله مشهور خود، که یک راه‌حل بازگشتی برای مسئله فیلترینگ خطی داده‌های گسسته بود را منتشر کرد، بر این ابزار نهاده شد. فیلتر کالمن مجموعه‌ای از معادلات و روابط ریاضی است که به عنوان یک تخمین‌گر بهینه با خاصیت پیش بینی و تصحیح عمل می‌کند و این عمل با کمینه کردن کوواریانس خطا انجام می‌شود [۹]. از مزیت‌های این فیلتر، آن است که محاسبه را برای حالت های مختلف زمانی اعم از گذشته، حال و آینده امکان‌پذیر می‌سازد. در فیلتر کالمن معادلات حالت سیستم و مقادیر اندازه‌گیری در اختیار می‌باشند و از دو دسته معادله به نام معادلات به‌هنگام‌سازی زمانی و به‌روزرسانی اندازه‌گیری استفاده می‌شود. شیوه کار فیلتر کالمن در شکل ۵ آمده است.

فیلتر کالمن یک فرآیند را با استفاده از بازخورد (فیدبک) کنترلی تخمین می‌زند. فیلتر، حالت فرآیند را در یک زمان پیش‌بینی و سپس بازخورد را به صورت یک اندازه‌گیری (از نوع نویزدار) دریافت می‌کند. معادلات به‌هنگام‌سازی زمانی را می‌توان به صورت معادلات پیش‌بینی کننده نیز در نظر گرفت. این درحالی است که معادلات به‌روزرسانی اندازه‌گیری به عنوان معادلات تصحیح‌گر در نظر گرفته می‌شوند. مشخص است که الگوریتم تخمین نهایی، یک الگوریتم پیش‌بینی- تصحیح برای حل مسئله‌های عددی است و فیلترکالمن با استفاده از معادلات به‌هنگام‌سازی زمانی و به‌روزرسانی اندازه‌گیری، تخمینی بهینه از حالت بعدی به ما می‌دهد. بعد از هر بار به‌هنگام‌سازی زمان و اندازه‌گیری، فرآیند با استفاده از تخمین حالت پسین قبلی تکرار می‌شود. بازگشتی بودن، یکی از بهترین ویژگی‌های فیلتر کالمن است. این موضوع پیاده‌سازی عملی این فیلتر را بسیار امکان‌پذیرتر از پیاده‌سازی فیلتری که بر روی تمام داده‌ها به صورت مستقیم برای هر مرحله تخمین اجرا می‌شود، می‌گرداند. در این حالت، فیلتر کالمن به صورت بازگشتی تمام تخمین و پیش بینی کنونی را تنها با استفاده از اطلاعات حالت قبلی انجام می‌دهد [۱۰-۱۲].

۵. شبکه های عصبی بازگشتی

یک شبکه عصبی هوشمند شامل مجموعه‌ای از نرون‌ها (گره‌ها) است که به یک شکل خاص به هم متصل شده‌اند. هر گره، حاصل سیگنال‌های رسیده به خود را به شکل وزن‌دار جمع می‌کند و یک وزن خروجی را به دیگر گره‌ها می‌برد. اتصال و جهت بین لایه‌های مختلف، نوع شبکه را مشخص می‌کند و در نتیجه، به روش آموزش مناسب اشاره می‌نماید. در میان معماری‌های موجود، می‌توان شبکه پرسپترون چندلایه (MLP[1])، شبکه‌های مبتنی بر توابع پایه‌ای شعاعی (RBF[2]) و شبکه‌های بازگشتی را مثال زد [۱۲].

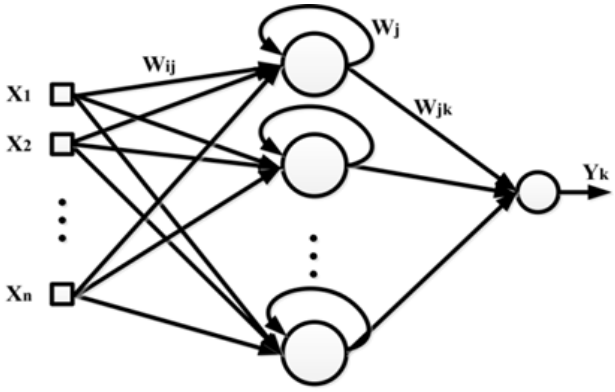


شکل۵. الگوریتم کلی فیلتر کالمن

1. Multi-Layer Perceptron
2. Radial Basis Function

شبکه MLP معمول‌ترین شبکه عصبی است که روش آموزش ساده و پیاده‌سازی مستقیمی نیز دارد. برای شبکه‌های MLP، سیگنال‌ها از لایه ورودی به سمت خروجی‌ها در یک جهت پخش می‌شوند. بنابراین عمل‌های حافظه‌ای یا شبکه‌های پویا را نمایش نمی‌دهد.

شبکه RBF را می‌توان به عنوان یک شبکه مستقیم در نظر گرفت که از عمل‌های پایه‌ای در لایه‌های پنهان خود در مقایسه با فعال‌سازی Sigmoid در شبکه‌های معمولی MLP استفاده می‌کند. هر گره خروجی وزن‌های جمع‌شده از همه نرون‌های پنهان را جمع می‌کند. بنابراین نرون‌های پنهان فقط به شکل غیرخطی ورودی‌ها را از فضای ورودی به یک فضای جدید با یک پارامتر ثابت تبدیل، نگاشت می‌دهند. شبکه‌های عصبی بازگشتی (مطابق شکل۶)، دارای یک یا چند فیدبک از یک لایه مشخص هستند و برخلاف شبکه‌های MLP معمولی، می‌توانند الگوهای موقتی را به خاطر عمل حافظه‌ای متن ورودی‌ها تشخیص دهند. از این‌رو برای حل مسئله پیش‌بینی مناسب می‌باشند. روش انتخاب ورودی‌ها و تابع‌های هدف در این شبکه‌ها، بر سرعت پاسخ‌دهی شبکه، تاثیر چشم‌گیری دارد و به صورت کاملا دلخواه وابسته به اولویت‌بندی (دقت یا سرعت) می‌باشد. با توجه به ویژگی‌های فوق، در این مقاله، شبکه عصبی بازگشتی برای



شکل۶. نمونه‌ای از شبکه‌های عصبی بازگشتی

حل مسئله پیش‌بینی و به‌منظور آشکارسازی و جبران سیگنال فریب به‌کار گرفته شده است [۱۳-۱۵].

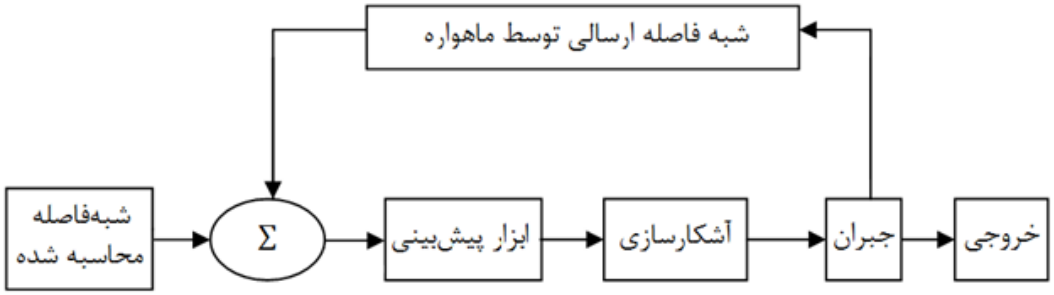
۶. الگوریتم‌های آشکارسازی و جبران فریب

در بحث مقابله با سیگنال فریب، ابتدا باید وجود فریب را آشکار کنیم و در مرحله بعد در صورت وجود فریب، آن را جبران نماییم. در این مقاله با استفاده از ابزارهایی به نام‌های فیلتر کالمن و شبکه عصبی بازگشتی که در بخش‌های قبل به تفصیل به آن پرداخته شد، می‌خواهیم روشی برای آشکارسازی و جبران سیگنال فریب ارائه نماییم. روش‌های پیشنهادی بر پایه بهره‌گیری از داده‌های شبه‌فاصله یک سیستم مبتنی بر GPS تفاضلی بنا نهاده شده‌اند.

ایستگاه‌های GPS تفاضلی برای افزایش دقت و کاهش خطای گیرنده‌ها به‌وجود آمده‌اند. ایستگاه‌های GPS تفاضلی با فرستادن سیگنال تصحیح، به افزایش دقت گیرنده کمک می‌کنند. اگر GPS تفاضلی مورد حمله سیگنال فریب قرار بگیرد، کیفیت سیگنال تصحیح کاهش پیدا خواهد کرد. از آنجایی که مکان ایستگاه‌های GPS تفاضلی شناخته‌شده و ثابت می‌باشند، معمولاً گیرنده‌های محدوده تحت پوشش آن‌ها مورد حمله‌های فریب قرار می‌گیرند. در این مقاله فرض بر این است که یک گیرنده مبتنی بر GPS تفاضلی مورد حمله فریب قرار گرفته است.

اساس کار این مقاله بر مقایسه مقدار شبه‌فاصله اندازه‌گیری‌شده و اطلاعات محاسبه‌شده GPS تفاضلی است که به عنوان ورودی ابزار پیش‌بینی (فیلتر کالمن یا شبکه عصبی بازگشتی) عمل می‌کند. در این مرحله، وظیفه ابزار پیش‌بینی، آشکارسازی وجود فریب است. در صورتی که وجود فریب تشخیص داده شود در مرحله جبران‌سازی، شبه فاصله جبران‌شده محاسبه خواهد شد. در شکل ۷ شمایی کلی از الگوریتم پیشنهادی، قابل مشاهده است.

در مرحله آشکارسازی، با شبه‌فاصله و مفاهیم مربوط به آن سروکار داریم. بنابراین ابتدا نگاهی به روابط این حوزه می‌اندازیم و



شکل۷. الگوریتم آشکارسازی و جبران فریب

سپس نحوه بهره‌برداری از این روابط را برای آشکارسازی وجود فریب، شرح می‌دهیم. شبه‌فاصله در حالت کلی مطابق رابطه ۱ بیان می‌شود.

$$\rho(k) = r(k) + cB(k) + I(k) + T(k) + w(k) \quad (۱)$$

که در این رابطه، $r(k)$ مبین فاصله بین ماهواره تا گیرنده، $B(k)$ مبین خطای ساعت گیرنده، c مبین سرعت نور، $I(k)$ مبین خطای تأخیر یونسفر و $T(k)$ مبین خطای تروپسفر می‌باشند. $w(k)$ نیز بیانگر نویز اندازه‌گیری گیرنده و از نوع نویز سفید گاؤسی است. نرخ تغییرات شبه‌فاصله را می‌توان با استفاده از مقایسه شبه‌فاصله در دو بازه زمانی متوالی به دست آورد:

$$\delta\rho(k) = \rho(k) - \rho(k-1) \quad (۲)$$

$$\rho\delta(k) = \delta r(k) + \delta cB(k) + \delta I(k) + \delta T(k) + \delta w(k) \quad (۳)$$

اگر سیگنال GPS مورد فریب قرار گیرد، در مقدار شبه‌فاصله، تغییر ایجاد می‌شود. این تغییر در نرخ تغییرات شبه‌فاصله اثر می‌گذارد. اگر فواصل زمانی بین اندازه‌گیری‌ها به اندازه کافی کم باشد، خطاهای یونسفری، تروپسفری و ساعت گیرنده قابل چشم‌پوشی هستند. از آنجایی که ایستگاه GPS تفاضلی، اطلاعات درست مکانی ایستگاه و مدار ماهواره را در اختیار دارد، می‌تواند فاصله بین ماهواره و گیرنده را محاسبه کند. اکنون شاخص $z(k)$ را مطابق رابطه ۴ تعریف می‌کنیم:

$$z(k) \cong \delta\rho(k) - \delta r(k) \quad (۴)$$

$$z(k) = \delta\rho(k) - (|R_s(k) - R_u(k)| - |R_s(k-1) - R_u(k-1)|) \quad (۵)$$

که در آن، Rs مبین بردار مکان ماهواره و Ru مبین بردار مکان گیرنده است. در حالت عدم حضور فریب، با چرخش ماهواره به دور محور زمین، مقدار شبه فاصله و بردار مکان ماهواره تغییر می‌کند. اگر مکان گیرنده را در محل ایستگاه و آن را ثابت فرض کنیم، مقدار $z(k)$ تقریبا نزدیک صفر خواهد شد. حال اگر به سیستم، سیگنال فریب اعمال شود، این نظم در سیستم از بین می‌رود و مقدار $z(k)$ مخالف صفر می‌گردد. در این مقاله از این ایده و روند برای تشخیص زمان اعمال سیگنال فریب و مقدار آن استفاده می‌کنیم؛ به این ترتیب که $z(k)$ را به عنوان ورودی شبکه عصبی در نظر می‌گیریم. بعد از تعلیم این شبکه و با توجه به اینکه از این شبکه برای پیش‌بینی حالت بعد استفاده می‌کنیم، مقدار $z(k)$ پیش‌بینی‌شده در خروجی شبکه عصبی ظاهر می‌شود. حال کافیست با تعیین یک مقداری خاص برای $z(k)$ که آن‌را حد آستانه می‌نامیم، زمان وقوع و مقدار سیگنال فریب را تعیین نماییم.

اما برای فیلتر کالمن، معادلات حالت و اندازه‌گیری را با فرض اینکه حرکت کاربر حرکت شتابدار با شتاب ثابت باشد، می‌نویسیم:

$$X_{k+1} = A_k + V_k = \begin{bmatrix} 1 & \Delta & \Delta^2/2 \\ 0 & 1 & \Delta \\ 0 & 0 & 1 \end{bmatrix} X_k + V_k \quad (۶)$$

$$Z_k = HX_k + W_k \quad (۷)$$

در روابط فوق، X_k مبین بردار حالت فرآیند و A مبین ماتریس انتقال حالت است که از نوشتن معادلات حرکت شتابدار ثابت به‌دست می‌آید. Δ مبین فاصله زمانی بین دو اندازه‌گیری است. V_k و W_k نیز به ترتیب مبین بردارهای نویز حالت و نویز اندازه‌گیری بوده و H مبین ماتریس ارتباط ایده‌آل بین بردار اندازه‌گیری و حالت معادل، $[1\ 0\ 0]$ می‌باشد. حال با داشتن معادلات حالت و اندازه‌گیری می‌توانیم حلقه کالمن را تشکیل دهیم و یک پارامتر جدید به عنوان خروجی برای آشکارسازی فریب تعریف نماییم. این پارامتر را که باقیمانده شبه‌فاصله می‌نامیم به صورت رابطه (۸) تعریف می‌کنیم:

$$v = [z(k) - H\hat{x}_k^-] \quad (۸)$$

تغییرات شبه‌فاصله ناشی از حرکت ماهواره‌ها در v باقی نمی‌ماند و از این‌رو می‌توان یک حد آستانه آشکارسازی فریب تعیین کرد. این حد آستانه به‌صورت تجربی به‌دست می‌آید. اگر مقدار v از حد آستانه بیشتر باشد نشان می‌دهد که فریب وجود دارد.

پس از انجام مرحله آشکارسازی اگر به وجود فریب پی برده شود باید جبران‌سازی صورت پذیرد. همان‌طور که مشاهده شد، اگر گیرنده‌ای تحت حمله فریب قرار گیرد، نرخ تغییرات شبه‌فاصله‌اش افزایش می‌یابد. این نرخ تغییرات می‌تواند با استفاده از اختلاف بین مقدار اندازه‌گیری‌شده و مقدار پیش‌بینی‌شده در فیلتر کالمن یا شبکه عصبی جبران گردد. در واقع این اختلاف همان اثری است که سیگنال فریب بر سیستم گذاشته است و برابر است با:

$$\delta\rho_{comp}(k) = \delta\rho(k) - \alpha z(k) \quad (۹)$$

که در آن، α ضریبی است که به صورت تجربی به‌دست آمده است. این ضریب متناسب با خطای شبه‌فاصله، تغییر می‌کند. از آنجایی که فیلتر کالمن و شبکه عصبی بازگشتی نمی‌توانند تغییرات

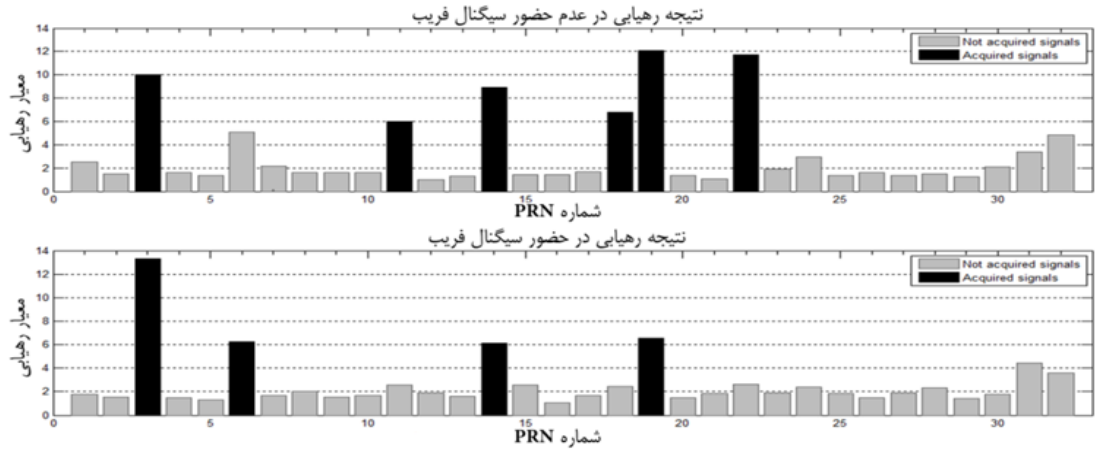
زیاد (به‌ویژه در مدت زمان طولانی) را دنبال کنند، در الگوریتم‌های پیشنهادی برای حذف و کاهش اثر فریب، قبل از اعمال الگوریتم، این ضریب تضعیف را درنظر گرفتیم تا به کمک فیلتر کالمن و شبکه عصبی آمده و به کاهش اثر فریب بپردازد.

۷. نتایج شبیه‌سازی

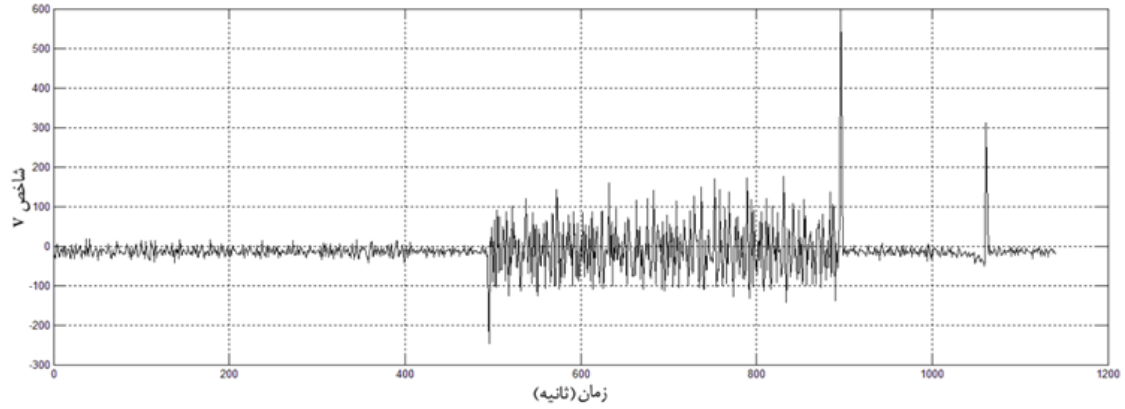
جمع‌آوری داده‌های مورد نیاز برای شبیه‌سازی به‌وسیله یک گیرنده تک‌فرکانسه GPS و یک گیرنده GPS برنامه‌محور، انجام شد.

داده‌های استخراج‌شده، شامل اندازه‌گیری شبه‌فاصله، فاز حامل و مکان دوازده ماهواره می‌باشند. فریب نیز به صورت هوشمند برای مثال به داده‌های ۵۰۰ تا ۹۰۰ اعمال گردید. همان‌طور که قبلاً ذکر شد، فریب نوع متوسط با ایجاد تأخیر در سیگنال دریافتی گیرنده ایجاد می‌شود. اثر این تأخیر در ماهواره‌های شناسایی‌شده در بخش رهیابی (مطابق شکل ۸) و نیز در مقادیر شبه فاصله ظاهر می‌شود. همان‌طور که در شکل ۸ مشاهده می‌شود، پس از اعمال فریب، سه ماهواره معتبر کنار رفته و یک ماهواره نامعتبر افزوده شده است. نحوه اعمال فریب، به این صورت بود که ابتدا یک مقدار معین به شبه‌فاصله اولین داده هدف، افزوده شد و سپس این مقدار، متناسب با تغییرات شبه‌فاصله افزایش و یا کاهش یافت. در روشی دیگر می‌توان به‌جای افزایش پله‌ای مقدار شبه‌فاصله اولین داده هدف، افزایش تدریجی شبه‌فاصله را جایگزین نمود.

پس از شبیه‌سازی الگوریتم‌های پیشنهادی، مشاهده شد که این الگوریتم‌ها علاوه بر این‌که بلادرنگ عمل می‌کنند (با توجه به به‌روز-رسانی داده‌های دریافتی در هر یک ثانیه)، در فاز آشکارسازی نیز کاملاً موفق عمل می‌نمایند. بر اساس توضیحات داده‌شده در بخش قبل، در این مرحله از رابطه ۸ بهره گرفته شد و نمودار مقدار V بر حسب زمان ترسیم گردید که این نمودار در شکل ۹ آمده است. از روی شکل ۹ می‌توان دریافت که در فاصله بین داده‌های ۵۰۰ تا ۹۰۰، یعنی زمان اعمال فریب، نمودار دارای آشفتگی بیشتری می‌باشد که آشکار کننده وجود فریب است. لازم به ذکر است که به



شکل۸. نتیجه بخش رهیابی گیرنده درحضور و عدم حضور فریب

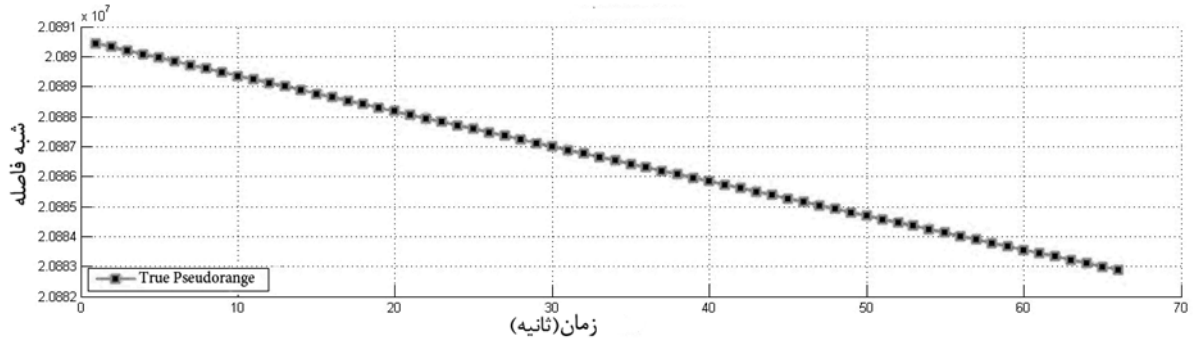


شکل۹. نتیجه مرحله آشکارسازی سیگنال فریب

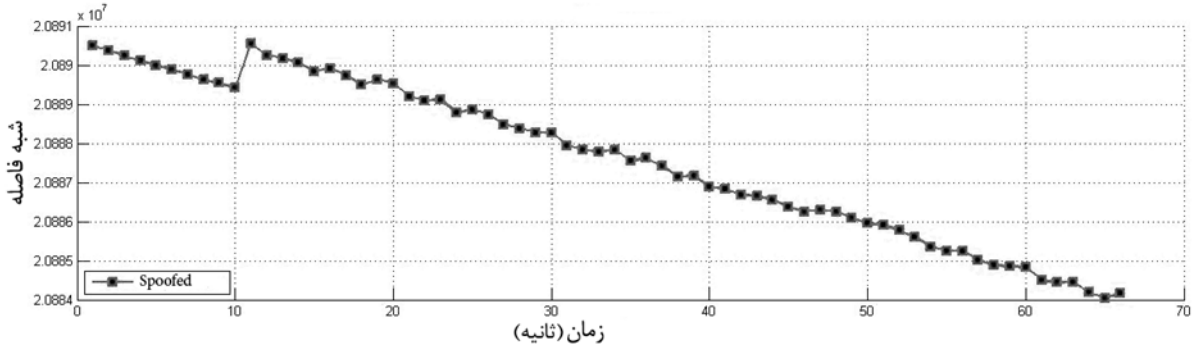
دلیل تشابه نتایج این بخش برای هر دو روش پیشنهادی، به نمایش یک نمودار اکتفا شده است.

برای بررسی اثربخشی الگوریتم‌های جبران‌سازی، مقدار موثر خطای شبه‌فاصله به عنوان معیار ارزیابی [۱۶]، قبل و بعد از جبران‌سازی محاسبه شد. نتایج نشان می‌دهند که الگوریتم مبتنی بر فیلتر کالمن توانسته اثر فریب را به میزان ۴۵ درصد جبران نماید. شکل‌های ۱۰، ۱۱ و ۱۲ به ترتیب شبه‌فاصله بدون فریب، شبه‌فاصله فریب داده‌شده و شبه فاصله جبران‌شده را بر حسب زمان و با حفظ رابطه زمانی نشان می‌دهند. همان‌طور که در شکل ۱۰ مشاهده می‌شود، برای حالتی که فریبی اعمال نشده است، در نمودار تغییرات شبه‌فاصله بر حسب زمان، هیچ‌گونه شکستگی و یا پرشی وجود ندارد؛ در حالی که مطابق با شکل ۱۱، برای حالتی که فریب اعمال شده است، نمودار تغییرات شبه‌فاصله بر حسب زمان، یک جهش پله‌ای در لحظه اعمال فریب را به نمایش می‌گذارد.

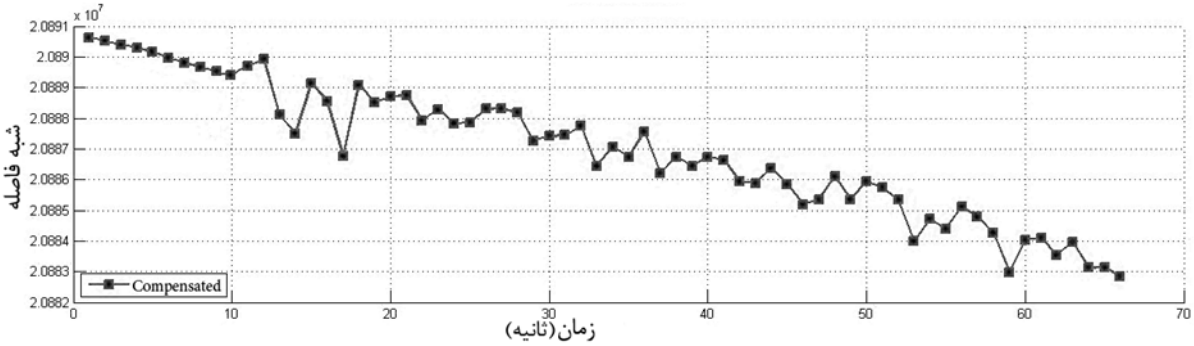
نتایج حاصل از اعمال الگوریتم مبتنی بر شبکه عصبی بر روی سیگنال فریب‌خورده، حاکی از جبران ۶۵ درصدی اثر فریب



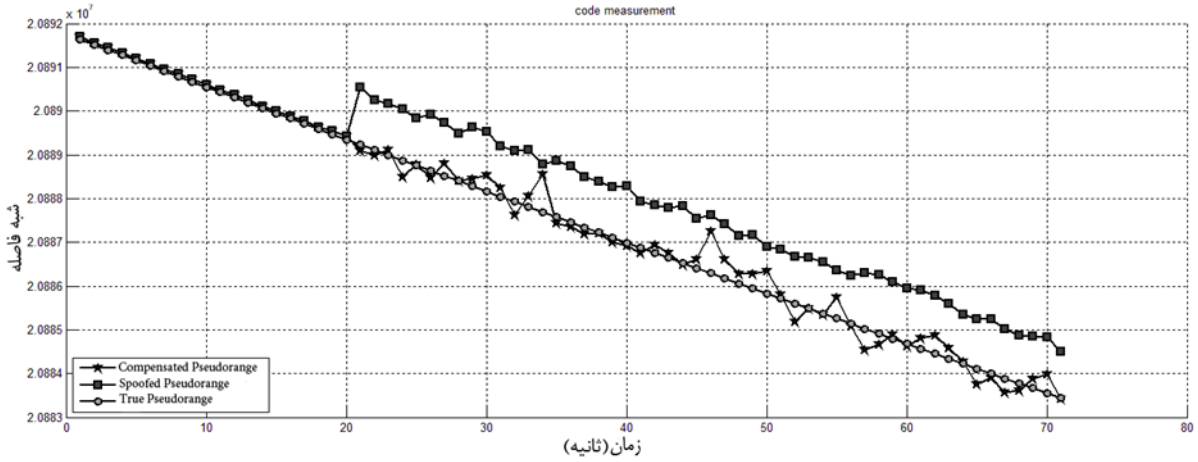
شکل۱۰. شبه‌فاصله بدون فریب



شکل۱۱. شبه‌فاصله فریب داده‌شده.



شکل۱۲. شبه‌فاصله جبران‌شده به کمک فیلتر کالمن



شکل ۱۳. شبه‌فاصله در حالات مختلف، برای روش مبتنی بر شبکه عصبی

می‌باشد. بنابراین، روش دوم نسبت به روش نخست، کارایی نسبتاً بهتری در فاز جبران‌سازی از خود نشان می‌دهد. اندازه‌گیری‌های شبه‌فاصله برای حالات عادی، فریب‌داده‌شده و جبران‌شده برای الگوریتم مبتنی بر شبکه عصبی در شکل ۱۳ قابل مشاهده می‌باشد. همان‌طور که از نتایج شبیه‌سازی برمی‌آید ویژگی الگوریتم‌های ارائه‌شده در این مقاله این است که مستقل از شناسایی یا عدم شناسایی فریب در بخش‌های رهیابی و ردیابی گیرنده، صرفاً با کمک داده‌های شبه‌فاصله به آشکارسازی و جبران فریب می‌پردازد.

۸. نتیجه‌گیری

در این مقاله ابتدا مسئله فریب و روش‌های مقابله با آن شرح داده شد. سپس فیلتر کالمن و شبکه عصبی بازگشتی به عنوان دو ابزار کارا برای حل مسائل پیش‌بینی مورد بررسی قرار گرفتند. از آنجایی که این ابزارها در عین سادگی، کارایی قابل قبولی در حل مسئله پیش‌بینی دارند، برای استفاده در الگوریتم مقابله با فریب، مورد توجه قرار داده شدند. الگوریتم‌های پیشنهادی این مقاله، علاوه‌بر داشتن قابلیت به‌کارگیری هم‌زمان برای چندین ماهواره، می‌توانند در تولید کد تصحیح ایستگاه‌های GPS تفاضلی نیز به‌کار روند. این الگوریتم‌ها که از اطلاعات شبه‌فاصله برای آشکارسازی و جبران استفاده می‌کنند، دارای سرعت پاسخ‌دهی بالایی بوده و با توجه به به‌روزرسانی داده‌ها در هر یک ثانیه، به‌صورت بلادرنگ عمل می‌نمایند. هم‌چنین الگوریتم‌های پیشنهادی، قابل پیاده‌سازی روی پردازنده‌های ارزان‌قیمت می‌باشند. نتایج شبیه‌سازی اعمال این الگوریتم‌ها به داده‌های واقعی، نشان‌دهنده موفقیت کامل آن‌ها در آشکارسازی فریب و قابلیت جبران ۴۵ درصدی و ۶۵ درصدی اثر فریب، به ترتیب برای روش‌های مبتنی بر فیلتر کالمن و شبکه عصبی هستند.

۹. مراجع

[1] N. A. White, P. S. Maybeck and S. L. Devilbiss, "Detection Interference, Jamming and Spoofing in a DGPS-Aided Inertial System," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 34, No. 4, 1998, pp. 1208-1217.

[2] S. Amiri, M. A. Dalir, and H. Talaiee, "GPS Signal Simulation in Intermediate Frequency (IF)," *Journal of Space Science and Technology*, Vol. 5, No.3, 2012, pp. 33-40.

[3] M. R. Mosavi, A. Nakhaei and Sh. Bagherinia, "Improvement in Differential GPS Accuracy using Kalman Filter," *Journal of Aerospace Science and Technology*, Vol. 7, No. 2, 2010, pp. 69-80.

[4] M. R. Mosavi, "Comparing DGPS Corrections Prediction using Neural Network, Fuzzy Neural Network, and Kalman Filter," *Journal of GPS Solutions*, Vol. 10, No. 2, 2006, pp. 97-107.

[5] K. Wesson, M. Rothlisberger and T. E. Humphreys, "Practical Cryptographic Civil GPS Signal Authentication," *Journal of Navigation*, Vol. 59, No. 3, 2012, pp. 177-193.

[6] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," *Proceedings of 21st International Technical Meeting of the Satellite Division of the Institute of Navigation*, USA, 2008, pp.2314 -2325.

[7] M. H. Jin, Y. H. Han, H. H. Choi, C. Park, M. B. Heo and S. J. Lee, "GPS Spoofing Signal Detec-

tion and Compensation Method in DGPS Reference Station," *Proceedings of 11th International Conference on Control, Automation and Systems*, Korea, 2011, pp. 1616-1619.

[8] L. Scott, "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems," *Proceedings of 16th Int. Technical Meeting of the Satellite Division of The Institute of Navigation*, USA, 2003, pp. 1543-1552.

[9] Z. Lin, C. Habin and Z. Natong, "Anti-Spoofing Extended Kalman Filter for Satellite Navigation Receiver," *Inside GNSS*, Vol. 4, No. 2, 2009, pp. 40-46.

[10] R. G. Brown and P. Y. C. Hwang, *Introduction to Random Signals and Applied Kalman Filtering with Matlab Exercises*, John Wiley & Sons, 4th ed., 2012.

[11] M. R. Mosavi, N. Hosseinzadeh, R. Kiaamiri and M. J. Rezaei, "A New Kalman Filter Based Method for GPS Anti-Spoofing," *Proceedings of 11th Conference of Iranian Aerospace Society*, Iran, 2013.

[12] M. R. Mosavi, "A Comparative Study Between Performance of Recurrent Neural Network and Kalman Filter for DGPS Corrections Prediction," *IEEE Conference on Signal Processing*, China, Aug. 31-4 Sep. 2004, pp. 356-359.

[13] M. R. Mosavi, "Recurrent Polynomial Neural Networks for Enhancing Performance of GPS in Electric Systems," *Journal of Wireless Sensor Network*, Vol. 1, No. 2, 2009, pp. 95-103.

[14] M. R. Mosavi, "Estimation of Pseudo-Range DGPS Corrections using Neural Networks Trained by Evolutionary Algorithms," *Journal of Review of Electrical Engineering*, Vol. 5, No. 6, 2010, pp. 2715-2721.

[15] R. Kiaamiri, M. R. Mosavi, M. J. Rezaei and N. Hosseinzadeh, "A New Neural Networks Based Method for GPS Anti-Spoofing," *Proceedings of Sharif Conference on Future Electronics*, Iran, 2013, pp. 25-28.

[16] M. R. Azarbad and M. R. Mosavi, "A New Method to Mitigate Multipath Error in Single-Frequency GPS Receiver based on Wavelet Transform," *Journal of GPS Solutions*, 2013 (DOI 10.1007/s10291-013-0320-1).