Archive of SID

چهاردهمین کنفرانس بین المللی انجمن هوافضای ایران
تهران، سازمان پژوهش های علمی و صنعتی ایران، پژوهشکده مخابرات و فن آوری ماهواره، ۱۲ تا ۱٤ اسفند۱۳۹۳
Aero2015P349

کنترل کانال‌ها و انتخاب ماهواره‌های مناسب بعد از آشکارسازی بلادرنگ حمله فریب برای کاهش خطای فریب در گیرنده‌های تک فرکانسه GPS

مریم معاضدی[۱]، امیررضا بازیار[۲]، سید محمدرضا موسوی میرکلایی[۳]
دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، نارمک، تهران، ۱۳۱۱۴-۱۶۸۴۶، ایران

چکیده

امروزه فریب‌دهنده یک تهدید ثابت‌شده برای گیرنده‌های GPS محسوب می‌شود. نتیجه حمله فریب خطاهای بزرگ ناوبری در گیرنده ناآگاه با نتایج زیان‌آور است. به دلیل این‌که سیگنال فریب از سیگنال اصلی تقلید می‌کند، گیرنده متوجه حضور آن نمی‌شود. ازاین‌رو تشخیص و جبران آن سخت‌تر از دیگر اختلال‌های مطرح‌شده برای GPS است. در این تحقیق با فرض در اختیار داشتن آشکارساز فریب بلادرنگ، روشی ابتکاری برای کاهش خطای حمله فریب در گیرنده‌های GPS ارائه خواهد شد که در آن از کنترل کانال‌ها و انتخاب ماهواره‌های مناسب در شروع مرحله ردیابی بهره می‌گیریم. برای این منظور به اطلاعات کانال‌ها و ماهواره‌های قبل از آشکارسازی نیاز است. روند الگوریتم پیشنهادی به این ترتیب است که گیرنده پس از آشکارسازی بلادرنگ حمله فریب، ماهواره‌های جعلی را از نتایج بخش اکتساب حذف می‌نماید و با ماهواره‌های مشترک قبل و بعد از آشکارسازی، روند موقعیت‌یابی را انجام می‌دهد. در واقع با انتخاب ماهواره‌های مناسب برای استخراج پیام ناوبری، از ردیابی ماهواره‌های جعلی توسط گیرنده GPS جلوگیری می‌شود. برای ارزیابی عملکرد روش پیشنهادی بر روی ۱۱ مجموعه داده متفاوت پیاده‌سازی شد. در نهایت با استفاده از این روش بیش از ۸۴ درصد از فریب با میانگین ۹۱/۲۷ درصد کاهش یافته است.

واژه های کلیدی: گیرنده GPS – حمله فریب - الگوریتم ضدفریب - ماهواره جعلی.

مقدمه

مکان‌یابی، ناوبری و دستگاه‌های وابسته به سیستم موقعیت‌یاب جهانی (GPS) جزء جدایی‌ناپذیر زندگی روزمره شده‌اند. اتکا به GPS برای ناوبری و هدایت، به آگاهی روزافزون جهت حفاظت در برابر تداخلات عمدی و غیرعمدی نیاز دارد [۱-۲]. فریب به عنوان خطرناک‌ترین دخالت عمدی در میان انواع تداخل‌ها، شناخته شده است [۳]. همه گیرنده‌های GPS شهری در دسترس عموم، نسبت به فریب بی‌توجه هستند. شکل ۱ مفهوم حمله فریب را به تصویر می‌کشد که در آن کابر GPS مسیر جعلی را می‌پیماید، در حالی که می‌پندارد در حال عبور از مسیر اصلی است. گیرنده GPS که در معرض حمله فریب قرار دارد، دو مجموعه سیگنال اصلی و فریب را همزمان دریافت می‌کند. سیگنال جعلی به گونه‌ای طراحی می‌شود که بر سیگنال اصلی GPS غلبه نموده و کنترل گیرنده ناآگاه را در اختیار گیرد.

با تغییر هر یک از مشخصه‌های سیگنال معتبر GPS امکان ایجاد سیگنال فریب وجود دارد [۴]. از آن جمله می‌توان به تغییر در شبه‌فاصله و موقعیت ماهواره‌ها اشاره کرد. با توجه به حرکت ماهواره‌های GPS در مدارهای مشخص به دور زمین، تغییرات شبه‌فاصله و موقعیت ماهواره در محدوده معینی می‌باشند. بنابراین ایجاد تغییرات زیاد و به‌دور از عرف در آن‌ها موجب سهولت آشکارسازی سیگنال فریب می‌شود. از جمله روش‌های مرسوم برای آشکاسازی این دسته از حملات فریب، بررسی صحت استقلال گیرنده (RAIM) می‌باشد [۵-۶]. روش RAIM، یک دفاع عملی در مقابل خطای اندازه‌گیری شبه‌فاصله در گیرنده GPS است که از طریق فرضیه آماری، خطای اندازه‌گیری شبه‌فاصله را آشکار و آن را از مسئله ناوبری حذف می‌کند. آزمون فرضیه آماری مورد استفاده در RAIM متکی بر روش استاندارد تنظیم احتمال هشدار اشتباه و محاسبه آستانه بر اساس احتمال تشخیص است.

فریبنده با ارسال سیگنال جعلی و بدست گرفتن کنترل نقاط ردیابی‌شده حلقه قفل تأخیر نیز می‌تواند موجب فریب در گیرنده شود. ارزیابی دفاع سیگنال باقی‌مانده، به عنوان روشی بر پایه نظارت بر خرابی ناحیه همبستگی مختلط تعریف می‌شود تا این نوع حمله فریب درجریان را تشخیص دهد. کارآیی این روش به میزان تضعیف سیگنال اصلی GPS، در طول حمله فریب بستگی دارد، مگر در مواردی که فریبنده یک تطبیق فاز در مرکز فاز آنتن گیرنده GPS تولید نماید [۷]. گیرنده‌های بردار پایه نیز در حضور یک سیگنال فریب به محض مشاهده توزیع غیرعادی هر خروجی همبسته‌ساز، آشکارسازی فریب بر روی خروجی‌های همبسته‌ساز عمل می‌کنند. ساختار کاهش فریب نیز اندازه‌گیری‌های محلی را که از فیلترهای حلقه ردیابی می‌آید، نادیده گرفته و از اندازه‌گیری‌های سطح ناوبری استفاده می‌کند. این حالت باقی می‌ماند تا پیک همبستگی فریب دور شود و همبسته‌ساز به فرآیند ردیابی سیگنال اصلی بازگردد [۸].

با تغییر در مجموعه ماهواره‌های قابل مشاهده و به عبارتی معرفی ماهواره جعلی نیز می‌توان موجب انحراف گیرنده GPS از موقعیت معتبر شد [۹]. این روش یکی از نمونه‌های معمول برای تولید فریب است که دانشمندان این حوزه در حال تحقیق برای مقابله با آن هستند [۱۰-۱۴]. از جمله می‌توان به روش پردازش فضایی اشاره کرد [۱۴]. این روش بر این اصل استوار است که اختلاف فاز حامل دو گیرنده نزدیک به هم تابعی از مکان گیرنده است. برای اجرای این روش به داشتن آرایه آنتنی نیاز است که پیچیدگی سخت‌افزاری زیادی را به گیرنده GPS تحمیل می‌کند. در این مقاله نیز این نوع از فریب مد نظر نویسندگان است. در ادامه، ابتدا به تشریح روش ارائه‌شده می‌پردازیم و سپس نتایج پیاده‌سازی الگوریتم پیشنهادی تحلیل و بررسی خواهند شد.

۱- دانشجوی دکتری
۲- فارغ‌التحصیل کارشناسی ارشد
۳- استاد، m_mosavi@iust.ac.ir (نویسنده مخاطب)

www.SID.ir

Archive of SID

کنترل کانال‌ها و انتخاب ماهواره‌های مناسب

عملیات پردازش سیگنال سیستم ناوبری GPS بر پایه ساختار کانالی قرار دارد. شکل ۲ شمای کلی یک کانال از گیرنده GPS را نشان می‌دهد. بعد از ورود سیگنال به کانال بدون توجه به معتبر بودن آن، مرحله پردازش تا انتهای کانال پیش می‌رود. در نتیجه قبل از تخصیص یک کانال به یک ماهواره خاص، گیرنده باید بداند که کدام ماهواره‌ها در حال حاضر قابل مشاهده هستند و از معتبر بودن آن‌ها اطمینان حاصل نماید. هدف از بخش اکتساب یافتن کلیه ماهواره‌های قابل مشاهده و تخمین دو مشخصه فرکانس و فاز کد هر ماهواره است. دقیق‌تر کردن مقادیر تخمین‌های فرکانس و فاز کد ماهواره‌ها و دنبال کردن تغییرات مقادیر این متغیرها وظیفه بخش ردیابی محسوب می‌گردد. به منظور ردگیری صحیح تغییرات فازکد و فرکانس حامل باید مرحله ردیابی به صورت پیوسته انجام شود. چنانچه ردیابی ماهواره‌ای از دست گیرنده خارج گردد، مرحله اکتساب مجدداً برای آن ماهواره انجام می‌شود [۱۵].

یک حمله فریب می‌تواند در هر یک از بخش‌های اکتساب، ردیابی و ناوبری گیرنده GPS رخ دهد [۱۶-۱۸]. در هر صورت، این تغییرات نباید خیلی آنی و به‌دور از عرف باشد تا از آشکارسازی آسان جلوگیری شود. در این مقاله حمله فریب و مقابله با آن در بخش اکتساب انجام می‌گردد. به طور خلاصه روش مقابله به این ترتیب است که گیرنده پس از آشکارسازی بلادرنگ ماهواره‌های جعلی را از نتایج بخش اکتساب حذف می‌نماید. ماهواره‌های جعلی نمونه‌هایی هستند که در حین حمله فریب در مجموعه ماهواره‌های دردید گیرنده قرار می‌گیرند. در این روش، ماهواره‌هایی را که بلافاصله بعد از آشکارسازی حمله فریب ظاهراً در خط دید قرار می‌گیرند، به عنوان ماهواره‌های جعلی در نظر گرفته می‌شوند. با کنار گذاشتن این ماهواره‌ها ادامه روند ردیابی و ناوبری تنها با نمونه‌های معتبری که قبل از آشکارسازی جمله فریب در خط دید بودند، انجام می‌شود.

به عنوان مثال در شکل ۳ نتایج بخش اکتساب سیگنال نمونه GPS در سه مرحله قابل مشاهده است. شکل ۳(الف) مربوط به سیگنال معتبر است. همان‌طور که ملاحظه می‌شود، ماهواره‌های شماره ۳، ۶، ۱۴، ۱۸، ۱۹ و ۲۲ در خط دید هستند. سیگنال جعلی در همان لحظه ارسال می‌شود و مطابق شکل ۳(ب) می‌تواند بعد از کنترل نقاط ردیابی‌شده حلقه قفل تأخیر، در عمل ماهواره ۱۸ را حذف و ماهواره ۳۱ را اضافه کند. ممکن است به نظر برسد که اضافه و کم شدن یک ماهواره تغییرات زیادی در موقعیت گیرنده هدف ایجاد نکند، اما در بخش بعد نشان خواهیم داد که مقدار این تغییرات می‌تواند قابل توجه باشد.

با توجه به مطالب بیان شده، وقتی که فریبنده برای کاهش احتمال آشکارسازی از تغییرات محسوسی استفاده نمی‌کند، می‌توان بعد از آشکارسازی سیگنال فریب، به حافظه گیرنده GPS مراجعه کرده و برای موقعیت‌یابی از ماهواره‌های مشترک قبل و بعد از آشکارسازی فریب استفاده نمود. شکل ۳(ج) گویای نتایج اکتساب نهایی پس از اعمال روش پیشنهادی می‌باشد. کنترل کانال‌ها قبل و بعد از آشکارسازی فریب ما را در انتخاب ماهواره‌های ۳، ۶، ۱۴، ۱۹ و ۲۲ یاری می‌دهد، ولی قادر به بازیابی ماهواره ۱۸ نیست. البته تغییرات آنی سطح اکتساب و افزایش بی رویه مقدار PDOP در دو سیگنال معتبر و فریب از ویژگی‌های این حمله فریب می‌باشد که می‌توانند به عنوان معیاری مناسب برای آشکارسازی حمله فریب مورد استفاده قرار گیرند. لازم به یادآوری است که وجود آشکارساز مطمئن و بلادرنگ از ملزومات موفقیت این روش می‌باشد. برای دو نمونه سیگنال دیگر نتایج بخش اکتساب در هر مرحله در شکل‌های ۴ و ۵ مشاهده می‌شوند.

نتایج شبیه‌سازی

در این بخش ابتدا نحوه شکل‌گیری داده‌های فریب توضیح داده می‌شود، سپس به شرح نتایج شبیه‌سازی و بررسی عملکرد روش پیشنهادی برای گیرنده ایستا می‌پردازیم. بلوک دیاگرام نشان داده شده در شکل ۶ مربوط به سیستم طراحی شده برای تولید فریب است. مطابق روند مشاهده شده در شکل به تولید سیگنال فریب تأخیری با استفاده از سیگنال واقعی جمع‌آوری شده در نرم‌افزار MATLAB پرداختیم.

به طور خلاصه مراحل الگوریتم تولید فریب تأخیری به قرار ذیل است:

۱. دریافت و ذخیره‌سازی سیگنال معتبر جمع‌آوری شده GPS به‌عنوان سیگنال تأخیری.

۲. انتشار سیگنال ذخیره‌سازی‌شده در مرحله قبل برای ترکیب با سیگنال معتبر GPS در آنتن گیرنده.

آزمایش را به تعداد زیاد با تأخیرهای مختلف تکرار کردیم. به ازای تأخیرهای مختلف مقادیر متفاوتی از خطای فریب حاصل شد. ۱۱ نمونه از داده‌های فریب حاصل به صورت اتفاقی انتخاب شدند و روش ضدفریب پیشنهادی بر روی آن‌ها پیاده سازی گردید. در هر از این آزمایش‌ها سیگنال دریافتی در گیرنده هدف و سیگنال معتبر GPS متناظرش به طور دقیق مورد بررسی قرار گرفتند. نتایج به دست آمده توسط کامپیوتر شخصی با استفاده از نرم‌افزار MATLAB تحلیل می‌شوند [۴]. در نهایت میزان انحراف موقعیت گیرنده در اثر سیگنال جعلی در راستای محور مختصاتی ENU (East, North, Up) برای چند نمونه در جدول ۱ بیان شده است.

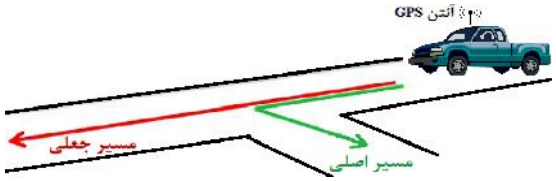
فریب در تمامی مجموعه داده‌ها با ایجاد تأخیر در داده حقیقی GPS ایجاد شده‌است. این مجموعه قادر به فریب گیرنده تک‌فرکانسه GPS از ۵۸ تا ۱۰۴ متر می‌باشد. در طی آزمایشات مختلف، توانستیم بیش از ۸۴ درصد از فریب این مجموعه را کاهش دهیم. جزئیات کامل کاهش فریب توسط اعمال روش توضیح داده شده برای تمام مجموعه داده‌ها درجدول ۲ درج شده‌است. با توجه به نتایج ارائه‌شده در جدول ۲ توانستیم توسط اعمال روش ضدفریب کنترل کانال‌ها و انتخاب ماهواره‌های مناسب، بیش از ۸۴ درصد از فریب ایجاد شده در ۱۱ مجموعه سیگنال جعلی مورد نظر را با میانگین ۹۱/۲۷ درصد کاهش بدهیم. برای نمایش تأثیر سیگنال جعلی و موفقیت روش ضدفریب، خطای ناشی از حمله فریب در سه نمونه از مجموعه داده‌های مورد نظر را قبل و بعد از اعمال الگوریتم ضدفریب پیشنهادی در اشکال ۷-۹ ترسیم شده‌اند. لازم به ذکر است که به دلیل مشابه بودن نتایج حاصل برای سایر داده‌های فریب، گزارش نشده‌اند. حذف چشم‌گیر فریب توسط الگوریتم ضدفریب در این اشکال مشهود می‌باشد.

نتیجه‌گیری

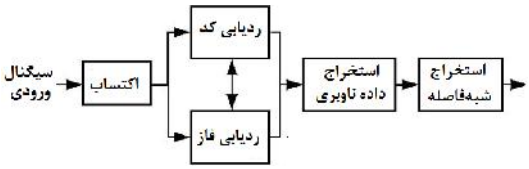
در این مقاله روش ابتکاری و ساده‌ای به منظور کاهش خطای فریب ارائه شد. به منظور عملکرد مناسب این روش نیاز به آشکارساز بلادرنگ وجود دارد تا هر چه سریعتر وجود سیگنال جعلی را اعلام نماید. سپس برای کاهش اثر فریب در گیرنده‌های GPS از کنترل کانال‌ها و انتخاب ماهواره‌های مناسب بهره بردیم. در اصل به کمک اطلاعات صحیح سیگنال معتبر GPS قبل از آشکارسازی، می‌توانیم با انتخاب ماهواره‌های مناسب برای استخراج پیام ناوبری، اثر فریب را کاهش دهیم. عملکرد روش پیشنهادی توسط ۱۱ مجموعه داده فریب متفاوت ارزیابی شد. با استفاده از این روش بیش از ۸۴ درصد از فریب را با میانگین ۹۱/۲۷ درصدی در این مجموعه داده فریب کاهش دادیم.

www.SID.ir

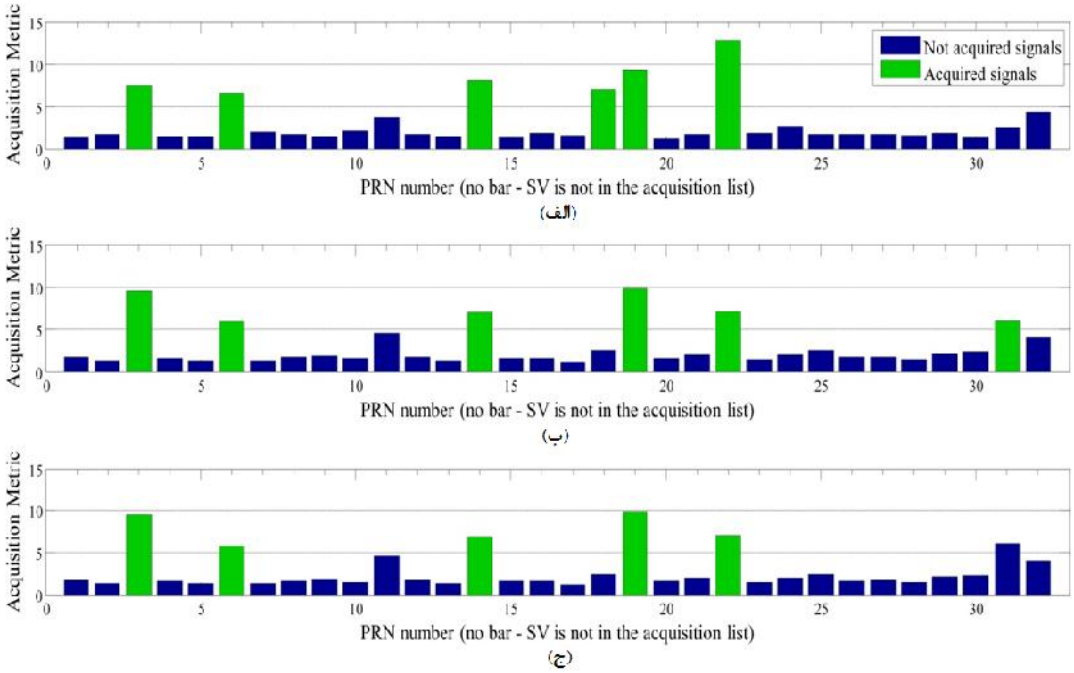
Archive of SID



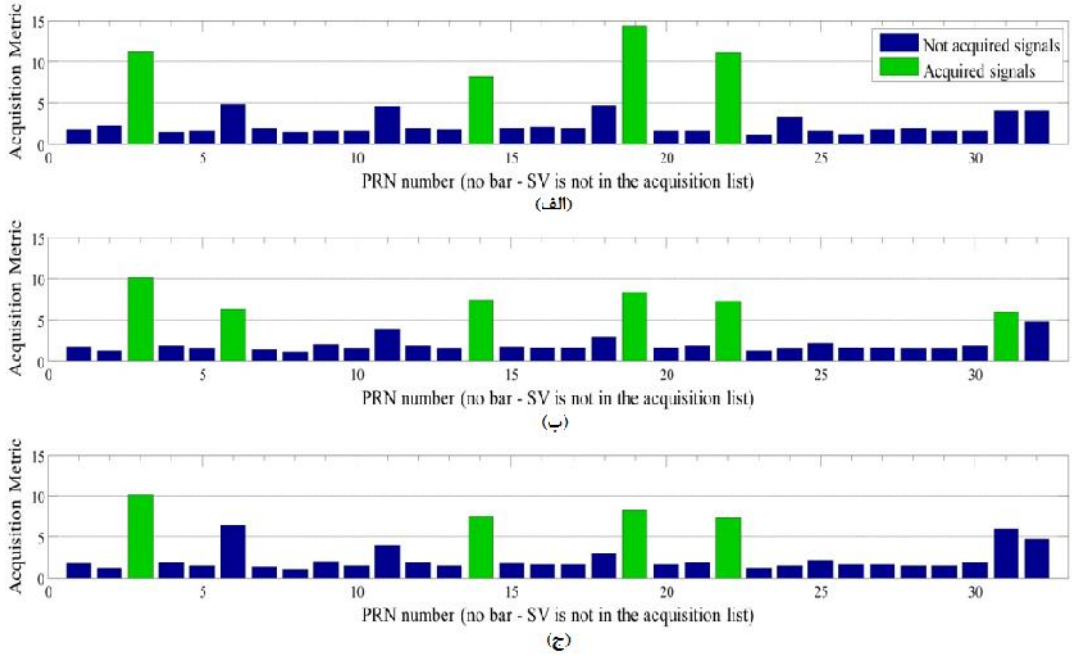
شکل۱- مفهوم کلی حمله فریب.



شکل۲- یک کانال گیرنده GPS.



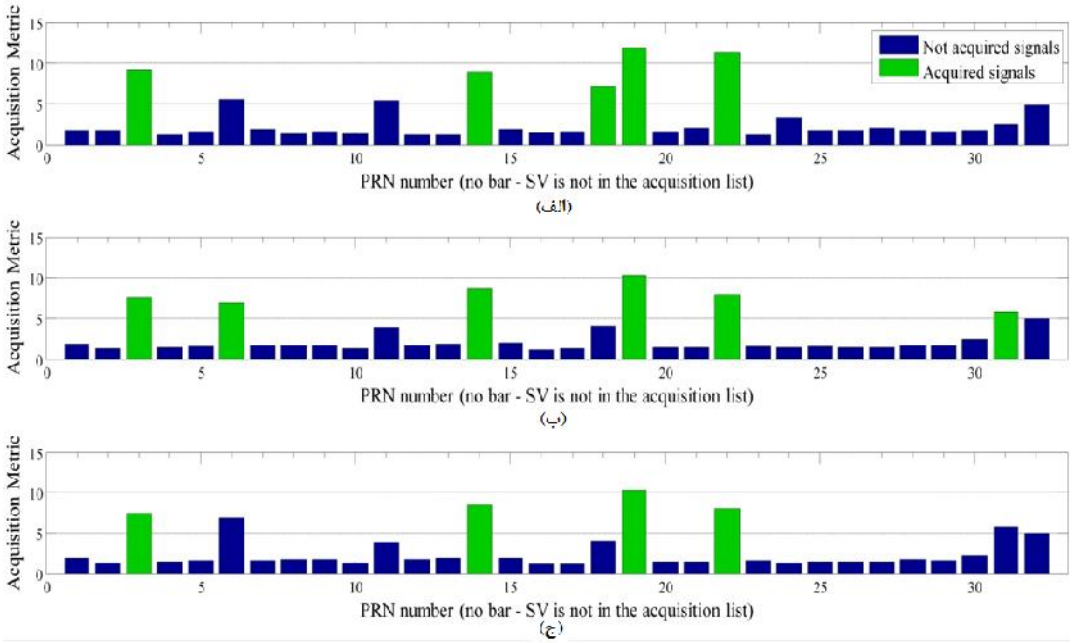
شکل۳- سطح اکتساب سیگنال نمونه اول در (الف) سیگنال حقیقی، (ب) سیگنال فریب و (ج) سیگنال فریب بعد از روش ضدفریب.



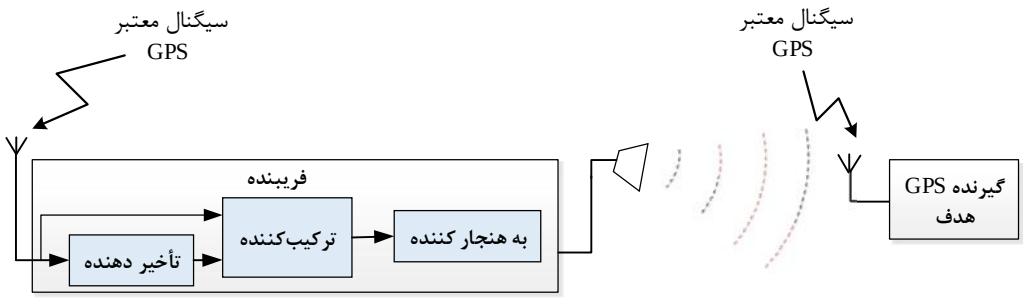
شکل۴- سطح اکتساب سیگنال نمونه دوم در (الف) سیگنال حقیقی، (ب) سیگنال فریب و (ج) سیگنال فریب بعد از روش ضدفریب.

www.SID.ir

Archive of SID



شکل۵- سطح اکتساب سیگنال نمونه سوم در (الف) سیگنال حقیقی، (ب) سیگنال فریب و (ج) سیگنال فریب بعد از روش ضدفریب.



شکل۶- بلوک دیاگرام سیستم تولید فریب.

جدول۱- جزئیات ۱۱ مجموعه داده فریب.

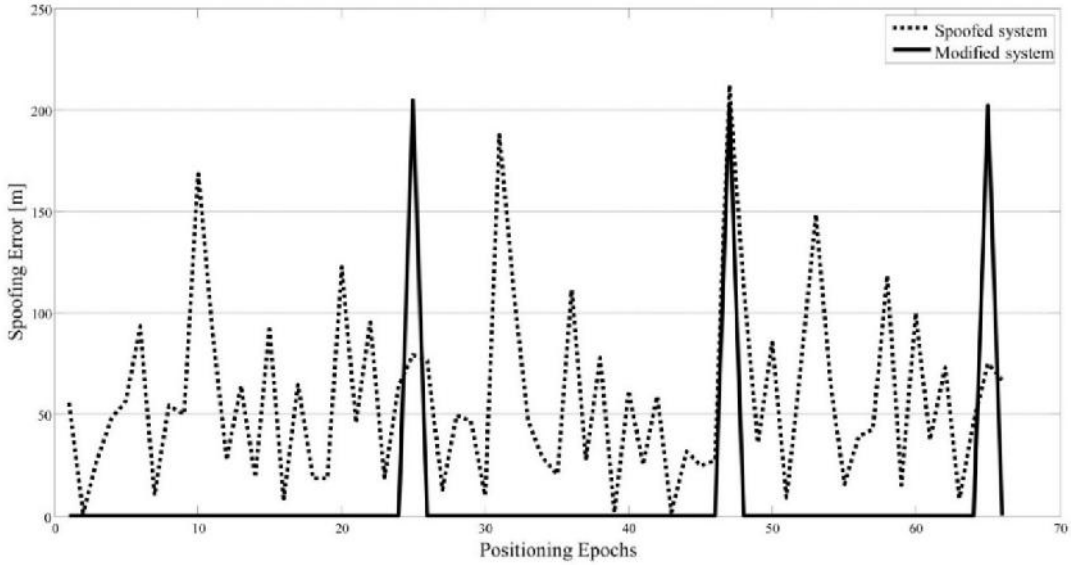
داده‌های فریب	خطا در مختصات E	خطا در مختصات N	خطا در مختصات U	مقدار کل خطای فریب
	(متر)			
مجموعه داده اول	۱۸	۱۸	۵۲	۵۸
مجموعه داده دوم	۱۹	۱۹	۵۴	۶۰
مجموعه داده سوم	۲۰	۱۹	۵۶	۶۲
مجموعه داده چهارم	۲۱	۲۰	۵۷	۶۴
مجموعه داده پنجم	۶	۱۶	۶۹	۷۱
مجموعه داده ششم	۲۲	۵	۷۸	۸۱
مجموعه داده هفتم	۲۲	۴	۷۹	۸۲
مجموعه داده هشتم	۲۲	۴	۸۰	۸۳
مجموعه داده نهم	۲۱	۶	۸۵	۸۸
مجموعه داده دهم	۲۷	۱۱	۸۹	۹۴
مجموعه داده یازدهم	۲۸	۱۶	۹۸	۱۰۴

www.SID.ir

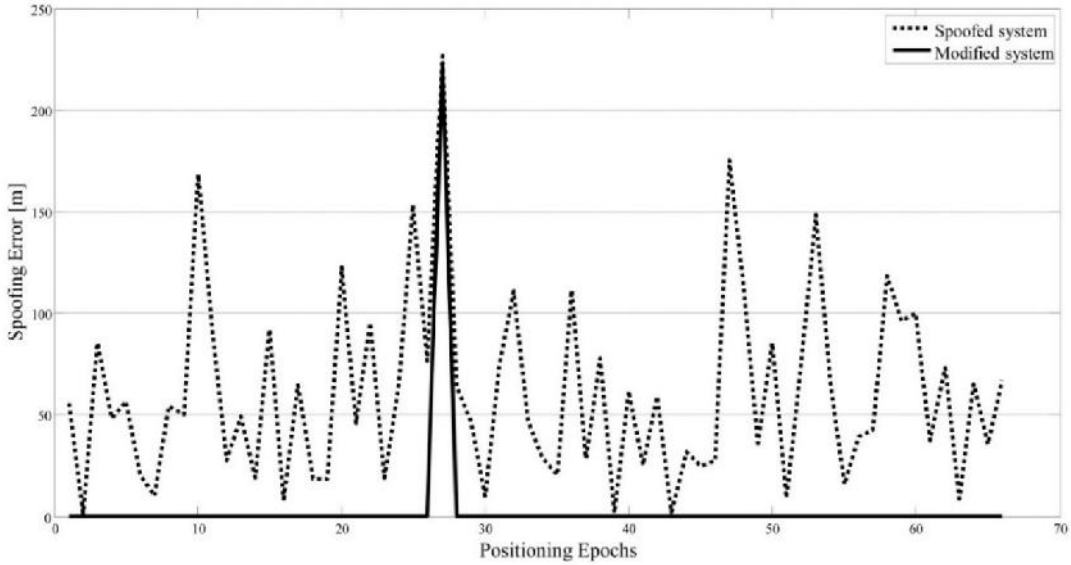
Archive of SID

جدول۲- جزئیات عملکرد روش ضدفریب.

مقدار فریب (متر)												
	۱۰۴	۹۴	۸۸	۸۳	۸۲	۸۱	۷۱	۶۴	۶۲	۶۱	۵۸	متوسط کاهش فریب ٪
درصد کاهش												
	۹۱	۹۳	۹۰	۱۰۰	۹۷	۹۶	۸۴	۸۵	۹۰	۹۴	۸۴	۹۱,۲۷



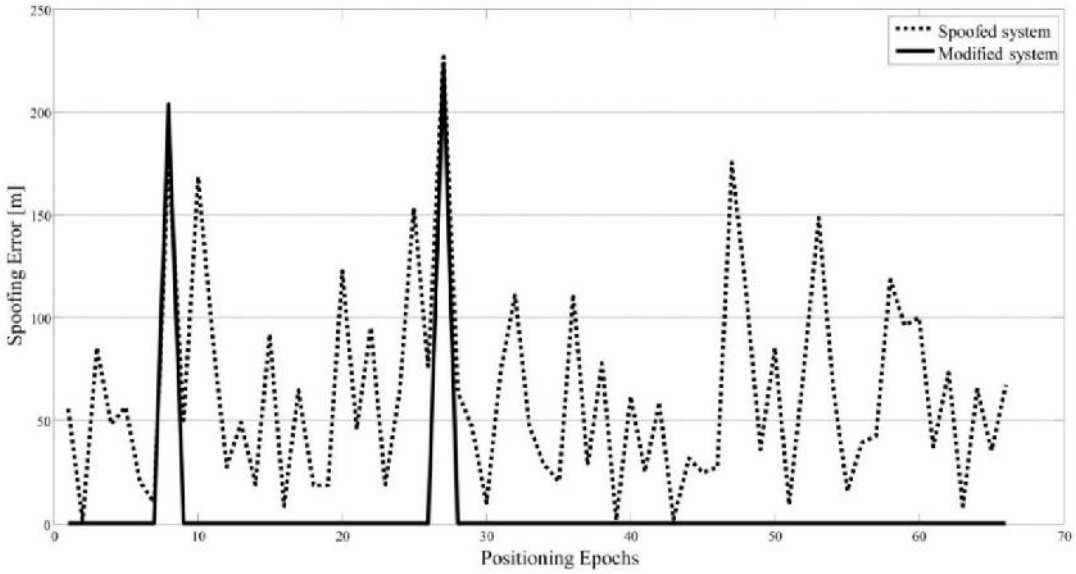
شکل۷- اختلاف موقعیت استخراج‌شده حقیقی و فریب قبل و بعد از اعمال الگوریتم ضدفریب در مجموعه داده اول.



شکل۸- اختلاف موقعیت استخراج‌شده حقیقی و فریب قبل و بعد از اعمال الگوریتم ضدفریب در مجموعه داده دوم.

www.SID.ir

Archive of SID



شکل۹- اختلاف موقعیت استخراج‌شده حقیقی و فریب قبل و بعد از اعمال الگوریتم ضدفریب در مجموعه داده دوم.

مراجع

1. M. R. Mosavi, "Real Time Prediction of GPS Receivers Timing Errors using Parallel-Structure Neural Networks", *Journal of Geoinformatics*, v. 3, n. 3, 2007, pp. 53-61.

2. M. R. Mosavi, S. Azarshahi, I. EmamGholipour and A. A. Abedi, "Least Squares Techniques for GPS Receivers Positioning Filter using Pseudo-range and Carrier Phase Measurements", *Iranian Journal of Electrical and Electronic Engineering*, v. 10, n. 1, 2014, pp.18-26.

3. A. Volpe National Transportation Systems Center Vulnerability Assessment of the Transportation Infrastructure Relying on Global Positioning System. Final Report, 2001.

۴. امیررضا بازیار، سید محمدرضا موسوی، عبدالرضا رحمتی و مریم معاضدی، "ارائه روشی جدید و ارزان قیمت برای تولید داده فریب GPS به منظور محافظت از سامانه‌های ناوبری دریایی"، *مجله دریا فنون، دانشگاه دانشگاه علوم دریایی امام خمینی (ره) نوشهر*، سال اول، شماره اول، ۱۳۹۲، ص۱-۱۲.

5. S. Feng, W. Y. Ochieng, D. Walsh and R. Ioannides, "A Measurement Domain Receiver Autonomous Integrity Monitoring Algorithm", *Journal of GPS Solution*, v. 10, 2006, pp. 85-96.

6. D. P. Shepard and T. E. Humphreys, "Characterization of Receiver Response to Spoofing Attacks", *GPS World*, v. 21, n. 9, 2010, pp. 27–33.

7. K. D. Wesson, D. P. Shepard, J. A. Bhatti and T. E. Humphreys, "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing", *24th International Technical Meeting of the Satellite Division of the Institute of Navigation*, pp. 1-11, Sep. 2011.

8. A. J. Jahromi, T. Lin, A. Broumandan, J. Nielsen and G. Lachapelle, "Detection and Mitigation of Spoofing Attacks on a Vector-Based Tracking GPS Receiver", *International Technical Meeting of the Institute of Navigation*, 2012, pp. 3-8.

9. A. J. Jahromi, "GNSS Signal Authenticity Verification in the Presence of Structural Interference", *Doctoral Dissertation, Department of Geomatics Engineering*, University of Calgary, Alberta, Canada, Sept. 2013.

10. T. E. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing", *IEEE Transactions on Aerospace and Electronic Systems*, v. 49, 2013, pp. 1073-1090.

11. K. D. Wesson, B. L. Evans and T. E. Humphreys, "A Combined Symmetric Difference and Power Monitoring GNSS Anti-Spoofing Technique", *IEEE Global Conference on Signal and Information Processing*, pp. 1-4, Dec. 2013.

12. P. Zalewski, "Real-time GNSS Spoofing Detection in Maritime Code Receivers", *Scientific Journals*, v. 38, n. 110, 2014, pp. 118–124.

۱۳. سید محمدرضا موسوی، امیررضا بازیار و مریم معاضدی، "روشی جدید برای کاهش اثر فریب در گیرنده‌های GPS تک‌فرکانسه مبتنی بر تبدیل موجک"، *مجله رایانش نرم و فن آوری اطلاعات*، دانشگاه صنعتی نوشیروانی بابل، ۱۳۹۳.

14. C. E. McDowell, "GPS Spoofer and Repeater Mitigation System Using Digital Spatial Nulling", *U.S. Patent 7250903 B1*, 31 July 2007.

15. K. Borre, D. M. Akos, N. Bertelsen, P. Rinder and S. H. Jensen, "A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach", *Birkhäuser Boston*, 2007.

16. 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", *21st International Technical Meeting of the Satellite Division of the Institute of Navigation*, 2008, pp. 2314-2325.

17. T. Nighswander, B. Ledvina, J. Diamond, R. Brumley and D. Brumley, "GPS Software Attacks", *Computer Communication Networks-Security and Protection*, 2012, pp. 450-461.

18. D. P. Shepard and T. E. Humphreys, "Characterization of Receiver Response to Spoofing Attacks", *GPS World*, v. 21, n. 9, 2010, pp. 27–33.

www.SID.ir