ارائه روشی جدید برای آشکارسازی فریب GPS مبتنی بر اندازه‌گیری شبه‌فاصله به منظور استفاده در سامانه‌های ناوبری دریایی

امیررضا بازیار[۱]، مریم معاضدی[۲]، سید محمدرضا موسوی میرکلایی[۳]، سید زمان غفاری[۴]

m_mosavi@iust.ac.ir

۱- کارشناسی ارشد دانشکده مهندسی برق، دانشگاه علم و صنعت ایران
۲- دانشجوی دکتری دانشکده مهندسی برق، دانشگاه علم و صنعت ایران
۳- استاد دانشکده مهندسی برق، دانشگاه علم و صنعت ایران
۴- کارشناسی ارشد دانشکده مهندسی برق، دانشگاه علم و صنعت ایران

چکیده

امروزه موقعیت‌یابی بر پایه GPS جز جدایی‌ناپذیر سامانه ناوبری دریایی شده است. از این‌رو قابلیت اطمینان و امنیت سیستم GPS برای کاربردهای صنعت دریانوردی از اهمیت بسزایی برخوردار می‌باشد. از طرفی به دلیل این‌که سیگنال‌های GPS مسافت نسبتاً طولانی تا رسیدن به گیرنده طی می‌کنند، سیگنال دریافتی توان پایینی دارد و به شدت در برابر انواع اختلال آسیب‌پذیر است. بنابراین امروزه بحث فریب به عنوان یکی از مهم‌ترین اختلال‌های مطرح‌شده در زمینه GPS، یکی از موضوعات مهم تحقیقاتی به ویژه در سامانه‌های ناوبری دریایی محسوب می‌شود. در این مقاله سعی شده است روش‌های مطرح‌شده برای آشکارسازی فریب را که در گیرنده‌های معمولی تک فرکانسه قابل استفاده‌اند، به طور کامل بررسی گردند. ابتدا روند کلی هر روش را به طور مختصر توضیح داده و سپس چالش‌ها و نقاط ضعف و قوت هر روش مورد مطالعه قرار می دهیم. در نهایت روشی جدید برای شناسایی حمله فریب در سامانه دریایی مبتنی بر اندازه‌گیری شبه‌فاصله پیشنهاد شده و نتایج شبیه‌سازی بیان شوند.

واژگان کلیدی: آشکارسازی، سامانه ناوبری دریایی، شبه‌فاصله، فریب‌دهنده، گیرنده GPS.

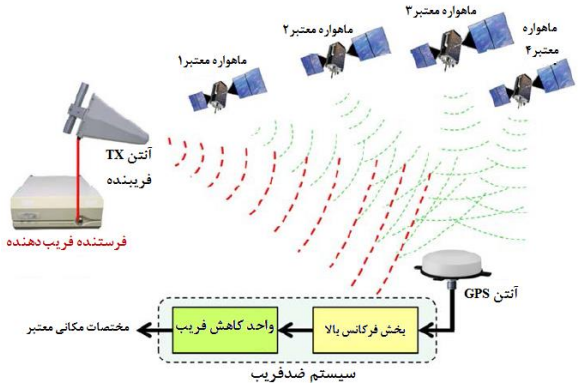
تاریخ دریافت مقاله :	۹۲/۷/۱۲
تاریخ پذیرش مقاله :	۹۳/۸/۱۱

۱- مقدمه

سیستم موقعیت‌یاب جهانی[1] (GPS) که امروزه به‌طور گسترده در کاربردهای دریانوردی و علوم دریایی استفاده می‌شود، هدف جذابی برای بهره‌برداری‌های غیرمجاز در مقاصد مختلف می‌باشد. اتکا به GPS برای ناوبری و هدایت، به آگاهی روزافزون برای حفاظت در برابر تداخلات عمدی و غیرعمدی نیاز دارد. به‌دلیل ضعیف بودن سیگنال‌های GPS دریافتی در سطح زمین یک تداخل کم توان نیز قادر به ایجاد جمینگ یا فریب تا شعاع چندکیلومتری گیرنده کشتی در دریاهای آزاد می‌باشد. تداخل می‌تواند عمدی یا غیرعمدی باشد. فریب سیگنال‌های GPS در راه‌های آبی یکی از مهم‌ترین تداخلات عمدی است که در آن سیگنال جعلی منطبق با ساختار سیگنال‌های GPS و با دامنه‌ی بزرگ‌تر تولید شده، همراه با سیگنال اصلی به سمت گیرنده هدف فرستاده می‌شود. از این‌رو لازم است راه‌کارهای مناسبی برای تشخیص و کاهش فریب در گیرنده هدف در سامانه دریایی به کار گرفته شود. در طول یک حمله فریب ترکیبی از سیگنال معتبر و فریب حضور دارند که در اغلب موارد موجب آسیب دیدن سیگنال معتبر می‌شود. فریبنده برای این‌که بتواند در حین تولید فریب به سیگنال معتبر آسیبی نرساند دو راه دارد: الف) سیگنال مخالف و خنثی‌کننده بسازد و ب) سیگنال معتبر دریافت‌شده را به انحصار خود در آورد.

برای اجرای راه نخست لازم است بردار موقعیت سه بعدی بین گیرنده و فریبنده دقیقاً معلوم باشد و نیز فریبنده بتواند به دقت ۰/۱ نانو ثانیه از تأخیر انتقال و عملیات پردازش خود برسد. برای راه دوم نیز دسترسی فیزیکی به گیرنده لازم است[۱]. با توجه به این‌که هیچ کدام از موارد بالا در عمل به راحتی امکان‌پذیر نیست، با حمله فریب برخی یا همه مشخصات سیگنال معتبر تحت تأثیر قرار می‌گیرند.

میزان تخریب سیگنال معتبر GPS یک فرصت برای تشخیص فریب محسوب می‌شود. از این‌رو با بررسی مشخصه‌های مختلف سیگنال GPS می‌توان به وجود سیگنال فریب در سامانه ناوبری پی برد و با روش‌های مناسب آن را جبران‌سازی نمود. شکل (۱) نحوه ایجاد یک



شکل (۱) شمای کلی یک سیستم ضدفریب [۲].

حمله فریب توسط دستگاه فریبنده در حضور سیگنال‌های معتبر ماهواره‌ها و سیستم مقابله با آن را در حالت کلی نشان می‌دهد [۲].

۲- مروری بر روش‌های آشکارسازی حمله فریب در GPS

در راستای مقابله با فریب دو گام اساسی مطرح می‌گردد: الف) چگونه گیرنده GPS حمله فریب را تشخیص دهد؟ و ب) چگونه گیرنده‌ای که در معرض سیگنال جعلی قرار گرفته است، اطلاعات موقعیت‌یابی صحیح را بازیابی کند؟ مقابله با فریب می‌تواند در هر یک از سطوح گیرنده از جمله بخش بیت داده، اکتساب، ردیابی، استخراج شبه‌فاصله و معادلات موقعیت‌یابی انجام پذیرد. در مرحله آشکارسازی فریب تمرکز بر روی وجوه تمایز سیگنال‌های معتبر و جعلی می‌باشد. روش‌های مختلفی برای آشکارسازی فریب‌های غیرنظامی ارائه شده‌اند که در ادامه به شرح آن‌ها می‌پردازیم.

۲-۱- روش‌هایی بر اساس بررسی توان سیگنال

به‌دلیل وجود فاصله‌ی زیاد بین ماهواره‌ها و گیرنده، سیگنال‌های دریافتی توسط گیرنده بسیار ضعیف و در نتیجه به راحتی تحت تأثیر عوامل محیطی و تداخل‌های توان پایین قرار می‌گیرند. اما در مورد سیگنال جعلی این مسئله صدق نمی‌کند. از این‌رو با بررسی توان سیگنال اصلی و جعلی می‌توان وجود سیگنال فریب را در سناریوهای مختلف تشخیص داد.

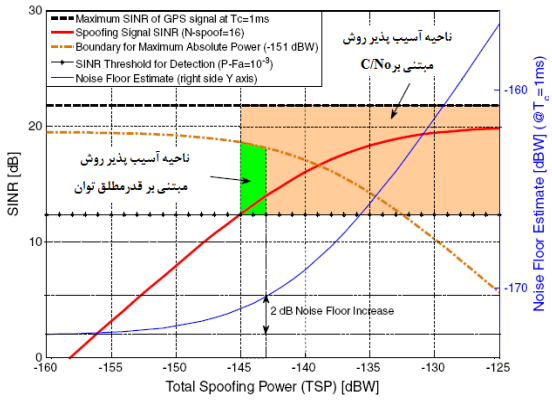
بیشتر گیرنده‌های GPS از نسبت حامل به نویز[2] (C/N_0)

[1] Global Positioning System

[2] Carrier-to-Noise Ratio

به عنوان پارامتری برای سنجش کیفیت سیگنال دریافتی استفاده می‌کنند. در شرایط مناسب جوی[1]، فقط تغییرات یونسفر و حرکت ماهواره‌ها می‌توانند تغییرات هموار تدریجی[2] را در توان سیگنال دریافت‌شده به وجود آورند. درمقابل وقتی توان بزرگ‌تر فریبنده، گیرنده GPS را گمراه می‌کند، ممکن است C/N_0 تغییرات ناگهانی را تجربه کند که نشان‌دهنده حضور سیگنال فریب می‌باشد. گیرنده ضدفریب می‌تواند پی‌درپی C/N_0 را بررسی کند و هر تغییر غیرمعمول را که می‌تواند نشانه‌ای از حمله فریب باشد، جستجو نماید. البته اگر C/N_0 اندازه‌گیری‌شده برای سیگنال فریب ارسال‌شده، در محدوده مجاز C/N_0 معتبر باشد، فریبنده توان بیشتری را با توجه به پیک‌های طبقه نویز محاسبه‌شده تولید و گیرنده را به‌طور موثر گمراه می‌کند [۳].

از آن‌جایی که تلفات مسیر بین فریبنده و گیرنده هدف بسیار متغیر است، تخمین توان ارسالی مورد نیاز برای تحمیل قدرت سیگنال مناسب در گیرنده هدف بسیار سخت می‌باشد. زیرا سطح سیگنال فریب نباید بیش از اندازه از سطح توان معمولی سیگنال‌های معتبر GPS بزرگ‌تر باشد. بنابراین دریافت سیگنال فریبنده با قدرمطلق توان نسبتا زیادتر از سیگنال معتبر مورد انتظار، بیان‌گر راه ساده دیگری برای آشکارسازی حمله فریب در سامانه ناوبری دریایی می‌باشد. شکل (۲) مقایسه‌ای بین محدوده‌های آسیب‌پذیر در برابر فریب را برای گیرنده ضدفریب بررسی‌کننده C/N_0 و گیرنده بررسی‌کننده قدرمطلق توان، فراهم کرده‌است [۲].



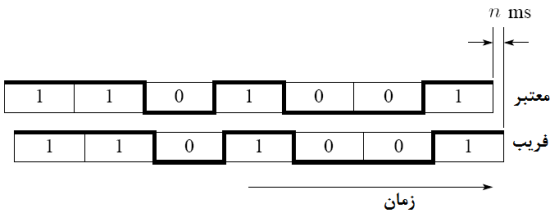
شکل (۲) مقایسه محدوده آسیب‌پذیری C/N_0 در برابر روش‌های بررسی قدرمطلق توان [۲].

[1] Open Sky
[2] Gradual Smooth Changes

منطقه آسیب‌پذیر گیرنده بررسی‌کننده قدرمطلق توان خیلی کمتر از منطقه آسیب‌پذیر گیرنده بررسی‌کننده C/N_0 می‌باشد. به‌علاوه اگر گیرنده قادر به آشکارسازی توان قدرمطلق با دقت بیشتری باشد، می‌تواند به مقدار زیادی بازه آسیب‌پذیری را کاهش دهد. در مقابل پیاده‌سازی روش بررسی‌کننده توان به گیرنده‌ای نیازمند است که توانایی اندازه‌گیری قدرمطلق دامنه سیگنال دریافت‌شده را در سطح صحت قطعی داشته باشد. در این‌صورت پیچیدگی سخت‌افزاری افزایش می‌یابد. محدوده‌ی پویا ی[3] نسبتاً زیاد توان سیگنال GPS، محدودیت دیگری برای عملکرد روش‌های تفکیک دامنه می‌باشد.

۲-۲- تفکیک زمان ورود[4] (TOA)

به این روش در گیرنده‌های تک فرکانسه تأخیر بیت[5] نیز گفته می‌شود. در حالتی که فریبنده به‌عنوان گیرنده باشد، به‌دلیل اینکه هیچ اطلاعات قبلی در مورد بیت‌های داده ناوبری ندارد، ابتدا باید سیگنال‌های GPS دریافت‌شده را کدگشایی[6] و سپس کپی پردازش‌شده‌ای را به‌عنوان سیگنال فریبنده تولید نماید. به این ترتیب یک تأخیر اجتناب‌ناپذیر بین مرزهای بیت داده فریبنده و داده معتبر وجود دارد [۴ و ۵]. در صورتی‌که فریبنده بخواهد داده ناوبری را پیش‌بینی کند، توسط گیرنده هدف قابل تشخیص است. اگر هم بخواهد عین سیگنال دریافتی را با تأخیر ارسال کند، باید به طور پیوسته قفل بیت را بررسی کند (مطابق شکل (۳)). تأخیر بین داده اصلی و فریب را در شرایط حمله فریب بدون پیش‌بینی نشان می‌دهد. اگر تغییر علامت در بیت غیرمعمول رخ دهد، وجود فریب به شرط نبودن اختلال‌های دیگر و ضعیف نبودن سیگنال



شکل (۳) تأخیر رشته داده فریب نسبت به داده اصلی[۵].

[3] Dynamic Range
[4] Time of Arrival
[5] Bit Latency
[6] Decode

گزارش می‌شود [۵]. این روش با چندین محدودیت مواجه است. ساختار قاب[1] اطلاعات GPS مشخص است و شامل بخش‌های مختلف با فرکانس‌های به‌روزرسانی متفاوت می‌باشد. فرکانس به‌روزرسانی بیشتر بخش‌های قاب GPS بسیار کم می‌باشد. بنابراین در صورتی‌که فریبنده اطلاعات GPS را پیش از شروع به ارسال سیگنال‌های جعلی به‌دست آورده باشد، اغلب بیت‌های اطلاعات GPS می‌توانند پیش‌بینی شوند. هم‌چنین در شرایط وجود اختلال‌های دیگر مانند جمینگ، فریبنده می‌تواند بر این دفاع غلبه کند، چون در این شرایط گیرنده از قفل بیت خارج می‌شود.

۲-۳- بررسی سازگاری با دیگر روش‌های ناوبری و موقعیت‌یابی

افزودن اطلاعات از تجهیزات کمکی مانند واحد اندازه‌گیری حرکتی[2] (IMU) می‌تواند به گیرنده هدف برای تفکیک تهدید فریب کمک کند [۶]. علاوه‌براین گیرنده GPS می‌تواند موقعیت استخراج‌شده توسط سیگنال‌های GPS دریافت‌شده را با دیگر روش‌های موقعیت‌یابی و ناوبری به‌دست‌آمده توسط ایستگاه‌های شبکه محلی بی‌سیم[3] (WLAN) یا شبکه‌های موبایل مقایسه کند. بنابراین اگر ناحیه اطمینان روش‌های مختلف فصل مشترکی نداشته باشند، به احتمال قوی امکان وجود فریب وجود دارد.

به‌کاربردن این روش، پیچیدگی سخت‌افزاری و نرم‌افزاری گیرنده GPS را افزایش می‌دهد. حسگرهای IMU به کالیبراسیون قبل از استفاده برای پیشنهادهای موقعیت‌یابی نیاز دارند [۷]. علاوه‌براین تکنولوژی‌های مکان‌یابی بی‌سیم متناوب (مانند شبکه‌های بافت سلولی[4])، معمولاً راه‌حل‌های موقعیت‌یابی را به‌دقت سیگنال‌های GPS ارائه نمی‌دهند. بنابراین اگر یک عدم تطابق کوچک بین موقعیت به‌دست‌آمده توسط فریبنده و موقعیت‌یابی معتبر وجود داشته‌باشد، ممکن است این روش‌ها مفید نباشند. پوشش محدود شبکه‌های بافت سلولی و شبکه‌های WLAN نیز کاربرد این روش را محدود می‌کند.

۲-۴- بررسی سازگاری و تخمین پارامترهای سیگنال ورودی GPS

در این روش ابتدا سیگنال GPS در گیرنده دریافت و ذخیره می‌گردد. گیرنده پس از استخراج مشخصه‌های سیگنال با داده‌های دقیقه قبل مقایسه کرده و در صورت مشاهده هرگونه تغییرات بزرگ و پیش‌بینی‌نشده در اندازه آن‌ها، وجود فریب را اعلام می‌نماید [۸-۱۳]. در سیگنال‌های معتبر GPS، فرکانس داپلر و نرخ تأخیر کد پایدار می‌باشند [۹]. فریبنده کم کیفیت ممکن است نتواند این پایداری را بین فرکانس داپلر و نرخ تأخیر کد حفظ نماید [۱۰]. همین‌طور، اگر خروجی فیلتر حلقه قفل فاز[5] (PLL) و حلقه قفل تأخیر[6] (DLL) سازگار نباشند، گیرنده می‌تواند با موفقیت وجود حمله فریب را آشکار نماید. علاوه‌برآن پیام ناوبری هر ماهواره شامل چندین داده نجومی متناسب با موقعیت ماهواره‌های دیگر GPS می‌باشد. هر ناسازگاری بین این اطلاعات نجومی می‌تواند یک حمله فریب همگام‌نشده[7] را اخطار دهد. پیام ناوبری هر سیگنال PRN شامل اطلاعات زمان GPS نیز می‌باشد. این زمان از ماهواره‌های مختلف GPS که باید سازگار باشند، به‌دست می‌آید. زمان GPS استخراج‌شده از یک فریبنده همگام‌نشده ممکن است با زمان GPS استخراج‌شده از دیگر ماهواره‌ها سازگار نباشد و این امر می‌تواند حضور حمله فریب را اخطار دهد.

در مراجع [۱۱-۱۲] از تخمین‌گر فیلتر کالمن برای پیش‌بینی مشخصات سیگنال لحظه بعد استفاده می‌کنند. در صورت مشاهده اختلاف قابل توجه بین مقادیر اندازه‌گیری و تخمین‌زده‌شده، وجود حمله فریب گزارش می‌گردد. در مرجع [۱۳] وجود فریب با شناسایی ناسازگاری آماری در مشخصات اصلی سیگنال‌های ماهواره‌ها تشخیص داده می‌شود. در فاز آموزش، سیستم ضدفریب مشخصه‌های آماری سیگنال را دریافت می‌کند. در حین حمله فریب، برخی یا همه مشخصات سیگنال از حدود آستانه مجاز تخطی می‌کند که با بررسی مداوم توسط سیستم ضدفریب قابل شناسایی می‌باشد. فزونی مشخصه‌های حدآستانه، پایه‌ای برای انتخاب بر مبنای احتمال حضور حمله فریب است. برای اجرای موفق این روش لازم است اطلاعات سیگنال معتبر GPS قبل از لحظه شروع فریب در دسترس باشد، زیرا در اغلب موارد

[1] Frame
[2] Inertial Measurement Unit
[3] Wireless Local Area Network
[4] Cellular Networks
[5] Phase Locked Loop
[6] Delay Locked Loop
[7] Unsynchronized

پس از اتمام حمله فریب مشخصات سیگنال جعل‌شده در حد آستانه مجاز قرار می‌گیرند.

۲-۵- پردازش فضایی[1] سیگنال‌های دریافتی GPS

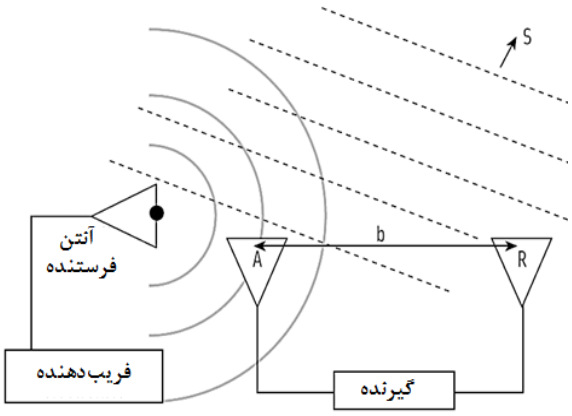
به دلیل محدودیت‌های عملی، معمولاً فرستنده‌های فریب چندین سیگنال جعلی را از یک آنتن می‌فرستند، در حالی که سیگنال‌های معتبر GPS از ماهواره‌های مختلف در مسیرهای گوناگون ارسال می‌شوند. از این‌رو می‌توان روش پردازش فضایی را برای تخمین اثر سه بعدی سیگنال‌های دریافت‌شده و تفکیک سیگنال‌هایی که رابطه فضایی دارند، به کار گرفت. به این روش، تشخیص فریب بر پایه زاویه ورود نیز می‌گویند. برای اجرای روش پردازش فضایی به داشتن آرایه‌ای از آنتن‌ها نیاز است که در ادامه پیاده‌سازی آن به شکل‌های مختلف بررسی می‌گردد.

در مرجع [۱۴] تفاوت فاز بین دو آنتن ثابت‌شده برای حدود یک ساعت اندازه‌گیری می‌شود (مطابق شکل (۴)). با دانستن رفتار آرایه آنتن و مسیر حرکت ماهواره‌ها، تفاوت‌های فاز نظری می‌تواند محاسبه و با تفاوت فازی عملی دیده‌شده توسط آرایه آنتن[2] مقایسه شود تا تهدید فریب آشکار گردد. مشکل اصلی این الگوریتم زمان‌گیر بودن آن است (حدود یک ساعت). علاوه‌برآن، این روش برای عملکرد مناسب به آرایه آنتن کالیبره‌شده با جهت‌گیری مشخص[3] نیاز دارد. مرجع [۱۵] یک ساختار آرایه آنتنی را برای آشکارسازی سیگنال فریب مبتنی بر همبستگی فضایی آن‌ها به کار گرفته است.

این روش می‌تواند سیگنال فریب را با موفقیت آشکار کند و هیچ احتیاجی به آرایه کالیبره‌شده یا دانستن نحوه جهت‌گیری آن ندارد. هم‌چنین، انتشار چندمسیری کارآیی این روش را کاهش نمی‌دهد، زیرا تمام سیگنال‌های فریب در کانال انتشار با مشخصه‌های مشابه، آزمایش می‌شوند. روش تفکیک چندآنتنه پیچیدگی سخت‌افزاری و محاسباتی گیرنده GPS را افزایش می‌دهد، زیرا ناگزیر به استفاده از چندین شاخه آنتن می‌باشد و برای تمیز PRNهای فریب به اکتساب و بررسی هر دو سیگنال فریب و معتبر نیاز دارد. ممکن است یک فریبنده چندآنتنه توانایی مغلوب ساختن روش‌های تفکیک‌پذیر فریبنده چندآنتنه را داشته باشد، هرچند برای تحقق چنین سناریوی فریبنده ماهری، محدودیت‌های عملی بسیاری وجود دارد.در مراجع [۱۶-۱۸]، روش آشکارسازی فریب با یک آرایه آنتن مصنوعی پیشنهاد شده است. مطابق شکل (۵) در این سناریو تک‌آنتن دستی گیرنده GPS در طی مسیر تصادفی حرکت داده می‌شود و یک ساختار آرایه‌ای آنتن مصنوعی[4] شکل می‌دهد.

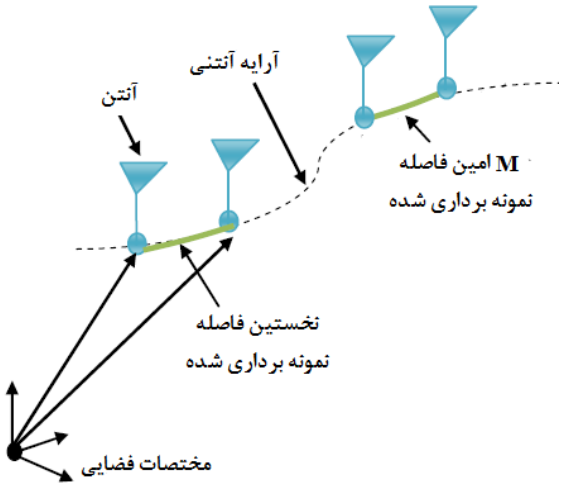
بعد از اکتساب سیگنال‌های PRN مختلف در مجموعه سیگنال دریافتی (هر دو سیگنال معتبر و فریب) و محاسبه همبستگی متقابل بین آن‌ها، سیگنال‌های فریب و معتبر از هم تفکیک می‌گردند. لازم به ذکر است که این روش در محیط‌های چندمسیری نیز عملکرد خوبی دارد، زیرا تمام سیگنال‌های فریبنده مسیر محو شدن[5] یکسانی را تجربه می‌کنند.

ازآن‌جایی‌که از چندآنتن گیرنده استفاده نمی‌کند، پیچیدگی سخت‌افزاری آن در مقایسه با روش‌های پیشنهادی در مراجع [۱۴-۱۵] بسیار کمتر است. با این وجود در شرایطی که فریبنده دامنه و یا فاز سیگنال‌های PRN مختلف را به طرز متفاوتی مدوله می‌کند، چند اصلاح برای موفقیت تفکیک سیگنال‌های جعلی باید اعمال شود.



شکل (۴) شکل هندسی متنوع آنتن برای تک ماهواره و فرستنده نقطه‌ای [۱۴].

[1] Spatial Processing
[2] Antenna Array
[3] Known Array Orientation
[4] Synthetic Array Spoofing Discrimination
[5] Fading Path



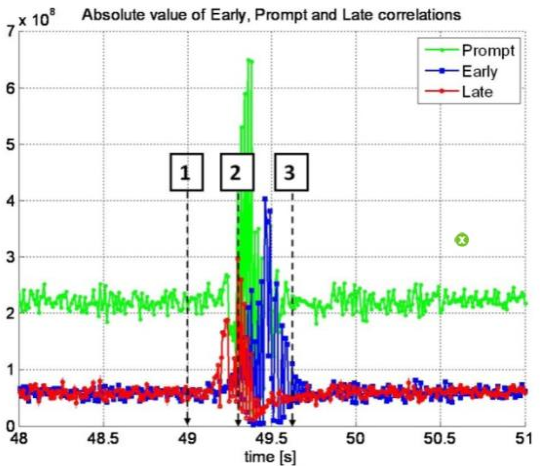
شکل (۵) نمونه‌گیری فضایی برای یک گیرنده GPS دستی در حال حرکت[۱۶].

۶-۲- نظارت بر کیفیت سیگنال[1] (SQM)

این روش‌ها از تحقیقات اولیه در زمینه نظارت بر کیفیت سیگنال و روش‌های آشکارسازی چندمسیری برای حل مشکل فریب استفاده می‌کنند. در گذشته SQM برای بررسی کیفیت پیک همبستگی GPS در محیط‌های محوشدگی و چندمسیری به‌کار گرفته می‌شد [۱۹-۲۱]. نویسنده‌های مراجع [۲۲-۲۴]، روش‌های SQM را برای آشکارسازی حمله فریب بر روی گیرنده‌های متحرک که در شرایط مسیر دید می‌باشند، توسعه داده‌اند. آزمون‌های SQM قادرند قله‌های غیرطبیعیِ نوک تیز سیگنال یا افزایش همبستگیِ قله‌ها را تشخیص دهند و جهت آشکارسازی هر بی‌تقارنی ناهنجار و یا یکسانی پیک‌های روی‌هم‌افتاده GPS که حمله فریبنده تحمیل می‌کند، به‌کار روند. بررسی و تصمیم‌گیری برای حضور یا عدم حضور حمله فریب معمولاً با آزمون‌های فرضیه آماری انجام می‌شود.

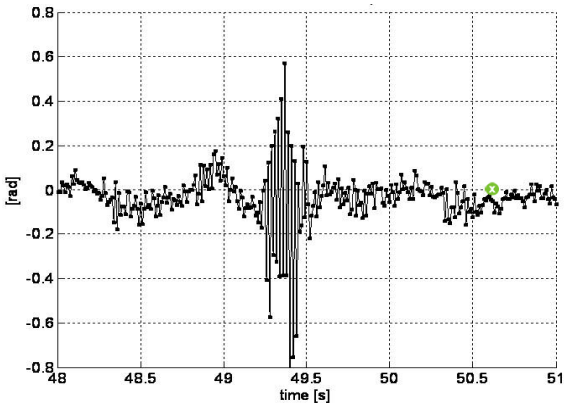
به عنوان نمونه در مرجع [۲۳]، روش SQM در سطح ردیابی کد و حامل پیاده شده است. می‌توان تغییرات ناشی از اعمال فریب را در حلقه ردیابی و خروجی DLL و PLL مشاهده کرد. مقادیر مطلق همبستگی‌های E، L و P در بازه زمانی مشخص در شکل (۶) نشان داده شده است. همان‌طور که از شکل نیز مشخص است خروجی DLL تحت تأثیر حمله فریب به طور غیرخطی تغییر می‌کند. در این لحظات DLL نمی‌تواند سیگنال کنترل فیدبک مناسب را متناسب با تأخیر بین PRN واقعی و کد محلی تولید کند. در نتیجه همزمان‌سازی در این شرایط امکان‌پذیر نبوده و تخریب ناشی از آن برای تشخیص فریب استفاده می‌شود. اثر مشابه در خروجی حلقه PLL نیز قابل مشاهده است. شکل (۷) خروجی حلقه PLL را حین حمله فریب نشان می‌دهد. با وجود یکسان بودن فرکانس سیگنال جعلی و اصلی PLL نمی‌تواند در طول حمله فریب سیگنال فیدبک مناسب ایجاد کند و به ناچار از قفل خارج می‌شود.

یک راه دیگر تشخیص حمله فریب GPS، بررسی توزیع تابع همبستگی است. در شرایط خط دید که فقط سیگنال اصلی و نویز در خروجی همبسته‌ساز وجود داشته باشد، مربع دامنه از خروجی همبسته‌ساز یک توزیع χ^2 با دو درجه آزادی را دنبال می‌کند. اگرچه در طول تداخل سیگنال فریب و اصلی، خروجی همبسته‌ساز نباید یک توزیع χ^2 را دنبال کند، اما پیک همبستگی سیگنال فریب تا حد امکان باید در نزدیکی سیگنال معتبر GPS قرار گیرد. بنابراین سیگنال فریب بر توان خروجی همبسته‌ساز تاثیر می‌گذارد و برهم‌کنش بین سیگنال‌های معتبر و فریبنده به چندین تغییر در دامنه خروجی همبسته‌ساز منجر می‌گردد. این تغییرات موجب انحراف توزیع خروجی همبسته‌ساز از توزیع χ^2 مورد انتظار می‌شوند [۶]. شکل (۸) توزیع میانی خروجی همبسته‌ساز را در حضور و عدم حضور سیگنال‌های فریب مقایسه می‌کند.

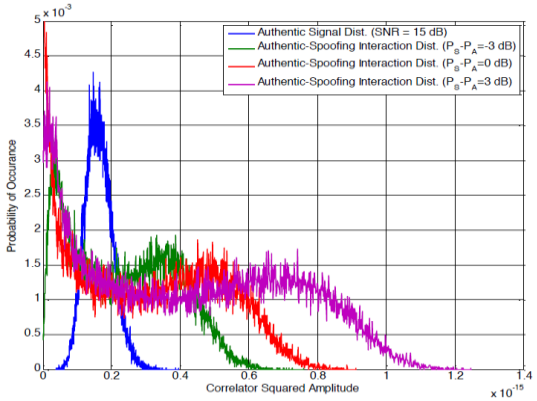


شکل (۶) خروجی حلقه PLL در حین حمله فریب.

[1] Signal Quality Monitoring



شکل (۷) خروجی همبسته‌سازهای E، L و P در DLL.



شکل (۸) توزیع خروجی همبسته‌ساز میانی برای سیگنال‌های اصلی و تداخل سیگنال‌های اصلی و فریب برای توان‌های متفاوت فریب.

همان‌طور که مشاهده می‌شود در حین تداخل سیگنال فریب و اصلی، توزیع خروجی همبسته‌ساز کاملاً با توزیع χ^2 متفاوت است. در حالت کلی روش‌های ضدفریب SQM، روش‌های قدرتمندی برای آشکارسازی حملات فریب می‌باشند. اگرچه ممکن است توانایی تفکیک بین سیگنال‌های فریب و بازتاب‌های چندمسیری را نداشته باشد. هم‌چنین در صورتی که فریبنده بتواند بدون تغییر شکل بیشینه همبستگی سیگنال فریب را تولید کند، این روش نمی‌تواند وجود فریب را تشخیص دهد. برای بهبود کارآیی آن در شرایط مختلف چندین راه‌حل در قالب راهکارهای دیگر بر پایه SQM پیشنهاد شده است که از جمله می‌توان به دفاع سیگنال نشانه و روش بردار پایه و روش ترکیبی اشاره کرد که در بخش‌های آتی بررسی خواهند شد.

۲-۷- ارزیابی دفاع سیگنال باقی‌مانده برای ضدفریب غیرنظامی GPS

دفاع سیگنال باقیمانده[1] (VSD) به عنوان روشی بر پایه نظارت بر خرابی ناحیه همبستگی مختلط تعریف می‌شود. VSD یک دفاع نرم‌افزاری قدرتمند، کم‌هزینه و مستقل است و اندازه یا وزن گیرنده را افزایش نمی‌دهد. کارآیی آن به میزان تضعیف سیگنال اصلی GPS، در طول حمله فریب بستگی دارد [۲۵-۲۷]. اگر همبستگی سیگنال PRN تولیدی با کل سیگنال ورودی گرفته شود یک تابع همبستگی مختلط x در زمان t و تأخیر آفست τ مانند زیر ایجاد می‌گردد:

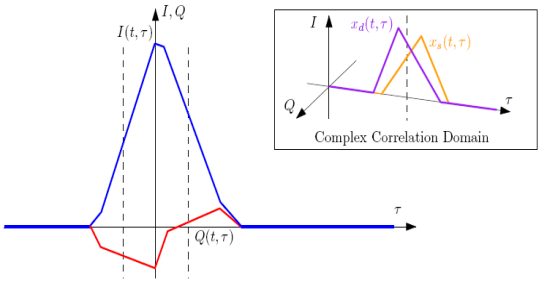
$$x(t,\tau)=x_d(t,\tau)+x_m(t,\tau)+x_s(t,\tau)+n(t,\tau) \qquad (۱)$$

$x(t,\tau)$ برهم نهی چهار جزء همبستگی مختلط، x_d مسیر مستقیم و به عبارتی سیگنال GPS اصلی، x_m جزء چندمسیری، x_s سیگنال فریب و n نویز سفید گوسی اضافه شده است. DLL با سه همبسته‌ساز مختلط (اولیه، میانی و نهایی) برای تعقیب سیگنال بر روی این تابع اجرا می‌شود. بعضی گیرنده‌ها همبسته‌سازهای خیلی بیشتری برای افزایش دقت پیش‌بینی بر روی میزان تخریب تابع همبستگی مختلط تولید می‌کنند. وقتی‌که زنجیره‌ای از تأخیر همبسته‌سازها موجود است، تابع همبستگی مختلط می‌تواند به‌عنوان سیگنال پیوسته زمان در نظر گرفته شود. اگر فرض کنیم سیگنال چندمسیری وجود ندارد، مدل سیگنال فریب $x_s(t,\tau)$ در ناحیه تابع همبستگی مختلط به‌صورت رابطه (۲) خواهد بود.

$$x_s(t,\tau)=(\alpha_s(t)R(\tau-\tau(t))e^{j\theta s(t)})\times I_{spoofing} \qquad (۲)$$

اگر فریبنده سعی کند گیرنده قربانی را با سیگنال جعلی که یک کپی خیلی نزدیک از سیگنال GPS است، فریب دهد، باید $x_s(t,\tau)$ تقریباً با $x_d(t,\tau)$ برابر باشد. تنها تفاوت قابل توجه در این مدل شاخص $1_{spoofing}$ است که رخ دادن فریب را مشخص می‌کند [۲۸]. در شکل (۹) اجزاء مسیر مستقیم و فریب در نظر گرفته شده‌اند. تخریب وابسته به تأخیر به‌دلیل تخریب فاز، وابسته به تأخیر است که در نتیجه آن سیگنال فریب فاز غیرحامل تطبیق داده شده دارد.

[1] Vestigial Signal Defense



شکل (۹) شکل تخریبی که می‌تواند در در تابع $x(t,\tau)$ در طول یک حمله‌ی فریب وجود داشته باشد [۲۹]

در این مورد، تخریب یکسانی در $I(t,\tau)$ و $Q(t,\tau)$ وجود دارد. در نتیجه نوع تخریب نشان‌داده‌شده در این شکل یک فریب منحصربه‌فرد نیست [۲۹].

۲-۸- استفاده از گیرنده GPS ردیابی بردار پایه

گیرنده GPS در مرحله ردیابی بر روی تعقیب بیشینه همبستگی سیگنال اصلی تمرکز دارد. اگر حین حمله فریب بیشینه همبستگی با توان بالاتر خیلی نزدیک به بیشینه سیگنال اصلی نباشد، بر روی فرآیند تعقیب گیرنده تاثیر نخواهد داشت. در حین تداخل که بیشینه همبستگی فریب از سیگنال اصلی منحرف می‌شود، در دامنه همبسته‌ساز خروجی نوسانات سریع رخ می‌دهد. به عبارتی دیگر در طول تداخل همه خروجی‌های همبسته‌ساز اولیه، میانی و انتهایی تغییرات دامنه نسبی را تجربه می‌کنند. با این وجود شکل ایده‌آل بیشینه همبستگی اصلی در طول نوسانات دامنه خروجی همبسته‌ساز خیلی تحت تاثیر قرار نمی‌گیرد. هم‌چنین، روش‌های SQM مطرح‌شده هم قادر به آشکارسازی حمله فریب وقتی‌که دو بیشینه همبستگی بر روی هم قرار دارند، نخواهند بود.

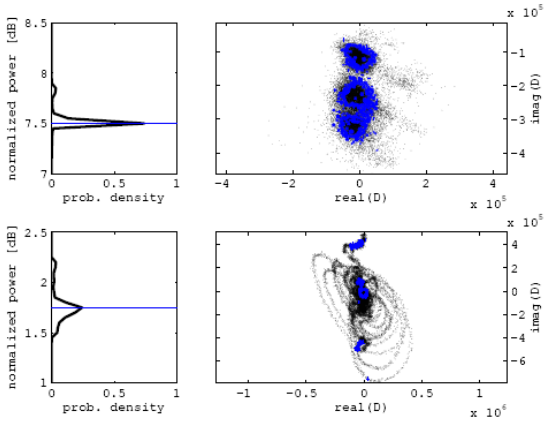
برای حل مشکل در این روش نقاط بیشتری از تابع همبستگی فریب مورد بررسی قرار می‌گیرند. با مطالعه یک میلی‌ثانیه برهم‌کنش سیگنال اصلی و فریب در حین حمله در نقاط مختلف VL, L, P, E, VE تابع همبستگی تغییرات دامنه دیده می‌شود. هم‌چنین با بررسی بیش‌تر مشخص می‌گردد در لحظه t = 0 که دو سیگنال فریب و اصلی منطبق هستند، بیشینه همبستگی حداکثر مقدار خود را دارد و نرخ تغییرات آن کاهش می‌یابد. تابع همبستگی حاصل اعمال فیلتر پایین‌گذر به خروجی همبستگی سیگنال دریافتی با کد تولیدشده محلی می‌باشد.

برای تشخیص وجود فریب خروجی پنج شاخه همبسته‌گر در آزمون فرضیه آماری مورد بررسی قرار می‌گیرد. برای حالت معتبر H0 و برای حالت نامعتبرH1 در نظر گرفته می‌شود. بلوک‌های هیستوگرام بر مبنای میانگین انحراف معیار خروجی همبسته‌سازها تعریف و مقدار آزمون برای خروجی هر شاخه به مدت چند میلی‌ثانیه محاسبه می‌گردد. اگر همه پنج شاخه زیر حد آستانه بودند، H0 و در غیر این‌صورت H1 مورد قبول است. حال اگر فرض H1 صحیح و فریب موجود باشد، تا زمانی‌که همه مقادیر آزمون به ازای همه شاخه‌ها به زیر حدآستانه نرسد، وجود حمله فریب مورد تأیید است [۶].

۲-۹- روش ترکیبی برای تشخیص فریب

در بخش‌های قبل روش‌های بررسی توان و خروجی همبستگی شرح داده شدند. روش‌های بر پایه توان به اختلال‌های دیگر حساس هستند و روش‌های بررسی همبستگی در چندمسیری دچار خطا می‌شوند. در این روش با ترکیب دو روش نام‌برده دقت و صحت اندازه‌گیری بهبود می‌یابد و امکان تشخیص فریب‌های پیچیده با حضور چندمسیری و تفکیک حالت‌های مختلف فراهم می‌گردد. به این ترتیب که فریبنده را بین روش‌های نظارت توزیع تابع همبستگی و توان کل داخل باند[1] قرار می‌دهد. به عبارت دیگر این روش از سخت بودن ایجاد فریبی که بتواند به طور همزمان هر دو مشخصه توان و توزیع همبستگی سیگنال فریب را منطبق با سیگنال اصلی نگه دارد، استفاده می‌کند. روش ترکیبی مستقل از گیرنده بوده و با تغییر اندک برای محدوده وسیعی از گیرنده‌ها قابل پیاده‌سازی می‌باشد. چالش مهم در این روش نیز تفکیک چندمسیری با نویز و فریب می‌باشد. برای بررسی توزیع همبستگی نامتقارنی تابع همبستگی با تفاضل شاخه‌های E و L مورد بررسی قرار می‌گیرد. شکل (۱۰) نتایج ارزیابی را برای دو سناریوی فریب نشان می‌دهد. نمودار بالا مربوط به نتایج توان بالاتر ۱۰ dB و سناریوی دوم مربوط به فریب با توان تطبیق‌یافته حدود ۱/۳ dB است. در نمودارهای سمت راست داخل حاشیه آبی رنگ

[1] In-Band



شکل (۱۰) نمودار توان هنجارشده (چپ) و توزیع تفاضل همبستگی (راست) برای سناریوی فریب با توان بالاتر و جابجایی زمانی (بالا) و سناریوی فریب با توان تطبیق شده و جابجایی مکانی (پایین).

احتمال رخ دادن بالای ۰/۰۰۰۱ را نشان می‌دهند که در نمودارهای سمت راست با خطوط آبی افقی نشان داده شده است [۳].

۳- روش پیشنهادی برای آشکارسازی بلادرنگ حمله فریب در GPS

یکی دیگر از مشخصات قابل بررسی برای آشکارسازی حضور حمله فریب شبه‌فاصله می‌باشد. می‌دانیم که استخراج مختصات مکان و زمان با حل معادلات ناوبری محقق می‌گردد. حل معادلات ناوبری نیز به ازای هر PRN معتبر و بر مبنای مشخصه شبه‌فاصله انجام می‌شود. از طرفی دیگر وجود حمله از هر نوعی که باشد در نهایت منجر به انحراف در مکان نهایی به‌دست‌آمده برای گیرنده نسبت به مقدار واقعی آن می‌گردد که به عنوان فریب شناخته می‌شود. پس می‌توان نتیجه گرفت که عمده اثرگذاری حمله فریب در مقدار شبه‌فاصله مشاهده شود. انتظار می‌رود در حالت عادی که حمله فریب رخ نداده است، تغییرات شبه‌فاصله شیب تندی نداشته باشد. زیرا گیرنده‌های معمولی GPS نمی‌توانند به طور آنی تغییر مکان قابل توجهی بدهند. در نتیجه با مشاهده تغییرات ناهموار در مقدار شبه‌فاصله می‌توان به وجود حمله فریب در گیرنده GPS پی برد. در ادامه مختصری در مورد نحوه‌ی محاسبه شبه‌فاصله در گیرنده GPS شرح می‌دهیم و سپس به ارائه الگوریتم پیشنهادی تشخیص فریب در GPS برای گیرنده ایستا خواهیم پرداخت.

در GPS قدم اساسی دانستن میزان مسافت از گیرنده تا ماهواره است، بنابراین استفاده از روش‌های پیشرفته به منظور محاسبه مسافت امری اجتناب‌ناپذیر است. ایده‌ی اصلی این موضوع براساس معادله سرعت نور در مدت زمان تأخیر استوار است. سیستم GPS بدین صورت کار می‌کند که گیرنده‌ی کاربر مدت زمانی را که طول می‌کشد تا امواج رادیویی از ماهواره به او برسد، اندازه‌گیری می‌کند. بدین ترتیب گیرنده با ضرب زمان اندازه‌گیری‌شده در سرعت نور، مسافت خود را تا ماهواره به‌دست می‌آورد. این کار حداقل باید برای چهار ماهواره مشخص صورت گیرد. با توجه به محاسبات انجام‌شده، این زمان در بازه ۶۵ الی ۸۳ میلی‌ثانیه قرار دارد.

دقت ساعت گیرنده‌های GPS حدود نانو ثانیه می‌باشد. بین کپی کد GPS ایجادشده درگیرنده با اصل کد رسیده از ماهواره اختلاف زمانی وجود دارد. خطای زمانی در هر دو ساعت گیرنده و ماهواره باعث می‌شود که فاصله‌ی اندازه‌گیری‌شده با فاصله هندسی بین ماهواره و گیرنده فرق داشته باشد. گیرنده فاصله خود تا هر ماهواره را با خطای موجود در ساعت خود محاسبه می‌کند. فاصله‌هایی که به این ترتیب محاسبه می‌شوند، دارای خطای زیاد، ولی هماهنگی هستند. به عبارتی دیگر خطا بر روی هر چهار اندازه‌گیری به یک نسبت اثر می‌گذارد. به‌همین جهت به این فاصله‌های غیرواقعی ولی مفید، شبه‌فاصله گفته می‌شود. با توجه به مشخص بودن موقعیت دقیق ماهواره‌ها خطای ناشی از شبه‌فاصله حداقل با حل چهار معادله به‌دست می‌آید. با به‌دست آمدن خطا، می‌توان پارامترهای موقعیت را تعیین و ساعت گیرنده را تصحیح کرد [۳۰].

در گیرنده GPS به منظور افزایش هرچه بیشتر دقت مختصات مکانی گیرنده، فرآیند موقعیت‌یابی برای بازه‌های مختلف زمانی تکرار می‌شود و موقعیت نهایی با میانگین‌گیری از مقادیر محاسبه‌شده در تکرارهای متوالی به دست می‌آید. با بررسی مقادیر شبه‌فاصله در تکرارهای مختلف، مشاهده می‌شود که حداکثر شیب تغییرات شبه‌فاصله بین دو تکرار متوالی موقعیت‌یابی حدود ۳۰۰ کیلومتر است. لازم به ذکر است که این مقدار معادل با مسافتی است که نور در مدت یک ثانیه طی می‌کند. بنابراین در صورتی‌که تغییرات شبه‌فاصله در تکرارهای

متوالی بیشتر از این حد مجاز مشخص شده باشد، می‌توان وجود حمله فریب را تشخیص داد. در بخش بعد نتایج بررسی میزان تغییرات مشخصه شبه‌فاصله بر روی چهار مجموعه داده فریب مورد بررسی قرار گرفته است.

۴- نتایج شبیه‌سازی

در این تحقیق برای بررسی میزان اثرگذاری حمله فریب در مشخصه شبه‌فاصله از سیگنال‌های فریب تولیدشده با ساز و کار تأخیر و ترکیب استفاده کرده‌ایم. فرض می‌کنیم در ابتدا سیگنال GPS معتبر بوده و حمله فریبی رخ نداده است. سپس حمله فریب در لحظه مشخصی اعمال می‌شود و از آن لحظه به بعد در ورودی گیرنده هدف سیگنال فریب اعمال می گردد. در سه نوبت فرآیند تولید داده فریب انجام شد و به منظور ارزیابی روش ارائه‌شده، چهار مجموعه داده مختلف از بین نمونه‌های موجود انتخاب و تغییرات شبه‌فاصله را در آن‌ها مطالعه کردیم.

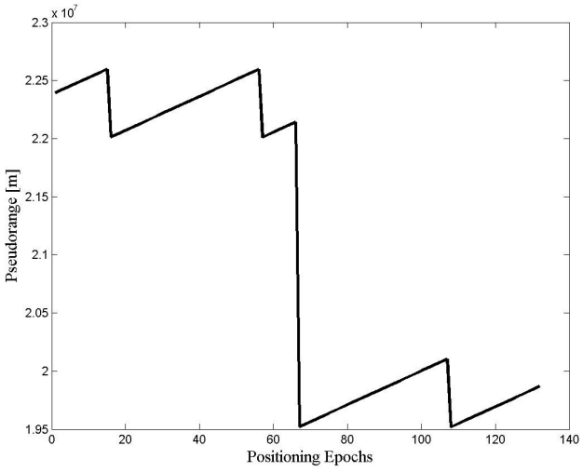
نتایج حاصل‌شده توسط کامپیوتر شخصی با استفاده از نرم‌افزار matlab تحلیل شده‌اند [۳۰]. فریب در مجموعه داده اول با ایجاد تأخیر ۲۶۲۳/۷ ms توسط ساز و کار تأخیر و ترکیب در داده حقیقی GPS ایجاد شده است. این مجموعه قادر به فریب ۱۹۲ متری گیرنده‌ی تک‌فرکانسه می‌باشد. جزئیات تغییرات شبه‌فاصله در این مجموعه در شکل (۱۱) قابل مشاهده است.

فریب در مجموعه داده دوم با ایجاد تأخیر ۶۹۹/۷ ms توسط ساز و کار تأخیر و ترکیب در داده حقیقی GPS فراهم شده است. این مجموعه قادر به فریب ۲۸۰ متری گیرنده‌ی تک‌فرکانسه می‌باشد. جزئیات تغییرات شبه‌فاصله در این مجموعه در شکل (۱۲) قابل مشاهده است. فریب در مجموعه داده سوم با ایجاد تأخیر ۴۳۳۰۸/۵ ms توسط ساز و کار تأخیر و ترکیب در داده حقیقی GPS ایجاد شده است. این مجموعه قادر به فریب ۹۷۰ متری گیرنده‌ی تک‌فرکانسه می‌باشد. جزئیات تغییرات شبه‌فاصله در این مجموعه در شکل (۱۳) قابل مشاهده است. فریب در مجموعه داده چهارم با ایجاد تأخیر ۱۲۲۴۳/۹ ms توسط ساز و کار تأخیر و ترکیب در داده حقیقی GPS تولید شده است. این مجموعه قادر به فریب ۱۱۴۰ متری گیرنده‌ی تک‌فرکانسه می‌باشد. جزئیات تغییرات شبه‌فاصله در این مجموعه در شکل (۱۴) قابل مشاهده است.

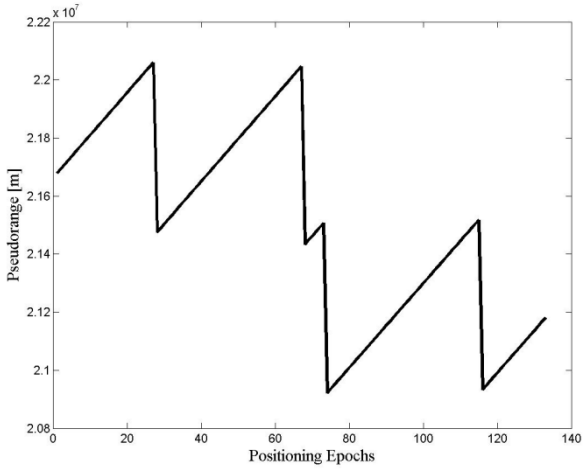
مشاهده می‌شود که در هر چهار نمونه در لحظه اعمال فریب نرخ تغییرات شبه‌فاصله از حد مجاز تخطی کرده است. بنابراین میزان تغییرات شبه‌فاصله می‌تواند معیار مناسبی برای تشخیص حمله فریب در نظر گرفته شود. لازم به ذکر است که برای کارآیی مناسب روش پیشنهادی، لازم است مشخصه شبه‌فاصله برای مدت کافی قبل از شروع حمله فریب در اختیار گیرنده قرار گیرد.

۵- جمع‌بندی و نتیجه‌گیری

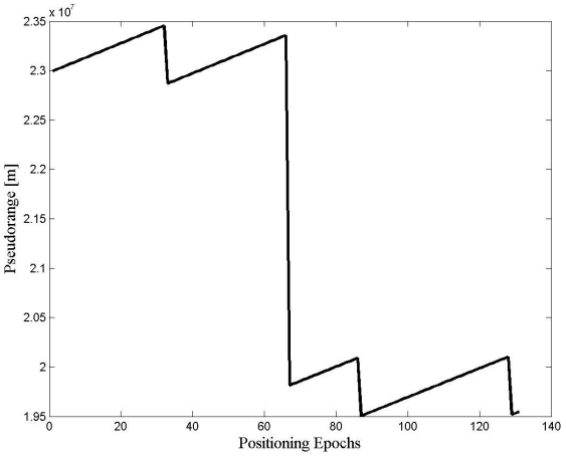
در این مقاله روش‌های مطرح‌شده به منظور آشکارسازی حمله فریب در گیرنده‌های تک فرکانسه غیرنظامی مورد بررسی قرار گرفتند.



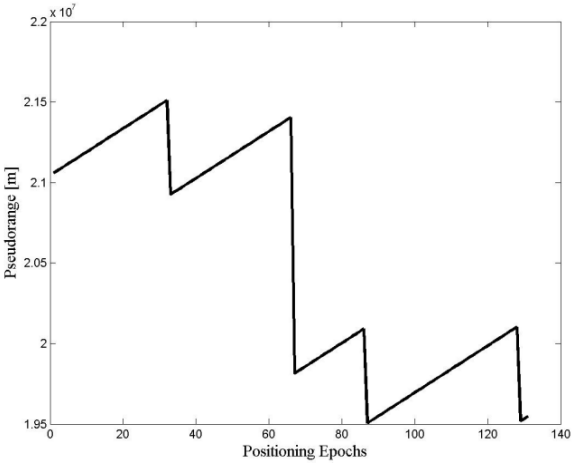
شکل (۱۱) تغییرات شبه فاصله برای مجموعه داده اول.



شکل (۱۲) تغییرات شبه فاصله برای مجموعه داده دوم.



شکل (۱۳) تغییرات شبه فاصله برای مجموعه داده سوم.



شکل (۱۴) تغییرات شبه فاصله برای مجموعه داده چهارم.

اساس همه روش‌ها بر این پایه استوار است که سیگنال معتبر GPS در حضور حمله فریب آسیب می‌بیند. کارآیی این روش‌ها نسبی است و با تغییر شرایط محیطی و نوع حمله فریب تحت تأثیر قرار می‌گیرد. جدول (۱) خلاصه‌ای از مطالب بیان‌شده را در بر می‌گیرد.

روش بررسی توان بر پایه C/No محدوده آسیب‌پذیر بزرگی دارد. روش تشخیص بر پایه قدرمطلق توان به سخت‌افزار اضافه برای اندازه‌گیری دقیق نیاز دارد. به طور کلی اثربخشی روش‌هایی مانند بررسی توان، TOA، بررسی سازگاری که بر پایه تحلیل مشخصات سیگنال دریافتی عمل می‌کنند در صورت استفاده از فریبنده‌های پیچیده و حتی متوسط محدود می‌شود. روش پردازش فضایی راهکار قدرتمندی است و در اغلب موارد می‌تواند بدون خطا فریب را تشخیص دهد، اما به تجهیزات اضافی برای گیرنده نیاز دارد. روش‌های بر پایه SQM تنها در صورت نبود اختلال‌های دیگر موثر هستند، هم‌چنین نمی‌توانند سیگنال اصلی و جعلی را از همدیگر تشخیص دهد و تنها قادرند تخریب مشخصات سیگنال را حین حمله فریب شناسایی کند.

روش VSD مشکل اختلال چندمسیری را حل کرده است. در واقع VSD به‌دنبال به گوشه راندن فریبنده و کاهش فضای احتمالی حمله‌ی آن است. هرچند موثر بودن VSD نیز توسط سختی تمایز بین فریب و چندمسیری محدود می‌شود. روش VB نیز در اغلب موارد موثر است، اما به پردازش‌گرهای اضافی برای بخش ردیابی گیرنده نیاز دارد. روش ترکیبی، دقت و صحت تشخیص فریب را تا حد قابل توجهی بهبود داده است، با این‌وجود در حضور سیگنال‌های چندمسیری اثربخشی آن کاهش می‌یابد. بحث چندمسیری از جمله مهمترین چالش‌های مطرح‌شده در زمینه شناسایی فریب در سامانه‌های ناوبری دریایی می‌باشد. از یک طرف تشابه سیگنال‌های فریب با چندمسیری به محققان در پیدا کردن روش‌های موثر شناسایی و کاهش فریب کمک می‌کند، از طرفی دیگر مشکل تمایز فریب و چندمسیری در اغلب موارد کارآیی روش‌های ارائه‌شده را محدود می‌نماید. نکته آخر این‌که تشخیص وجود فریب قدم اول مقابله با حمله فریب است و بخش اصلی مقابله در کاهش اثر حمله در عملکرد گیرنده هدف می‌باشد.

در این تحقیق روش ساده و موثری برای آشکارسازی حمله فریب مبتنی بر بررسی شبه‌فاصله ارائه شده است. با توجه به ارتباط مستقیم مشخصه شبه‌فاصله با مختصات مکانی حاصل‌شده توسط گیرنده، انتظار می‌رود در حین حمله فریب، مشخصه شبه‌فاصله تغییرات غیرعادی داشته باشد. نتایج آزمایش بر روی چهار مجموعه داده فریب مختلف صحت این ادعا را ثابت می‌کند. لازم به ذکر است که در صورت استفاده از فریب‌دهنده هوشمند برای اعمال سیگنال فریب شبه‌فاصله از مقدار اولیه تا مقدار جعلی نهایی به طور تدریجی تغییر می‌نماید. در این صورت شناسایی حمله فریب با روش پیشنهادی مقدور نخواهد بود. نویسندگان امیدوارند در آینده بتوانند بر مشکل مطرح‌شده غلبه نمایند و سپس روشی نوین برای کاهش حمله فریب بر مبنای این تئوری ارائه دهند.

جدول(۱) مقایسه روش‌های مختلف آشکارسازی فریب GPS.

روش‌های آشکارسازی	مشخصه مورد بررسی	تجهیزات مورد نیاز	مزایا	محدودیت‌ها
بررسی توان سیگنال	توان و دامنه	سخت‌افزار برای اندازه‌گیری توان	سادگی	محدوده بزرگ آسیب‌پذیری و گران بودن تجهیزات در صورت نیاز
TOA	زمان دریافت	ارتقای نرم‌افزاری	پیاده‌سازی آسان	عدم کارآیی در حضور اختلال دیگر و پیش‌بینی TOA توسط فریبنده
سازگاری با دیگر روش‌های ناوبری	نتایج ناوبری	تجهیزات ناوبری غیر GPS	قابلیت اطمینان بالا	هزینه بالا و پوشش محدود تجهیزات دیگر
سازگاری پارامترهای سیگنال ورودی	چندین پارامتر به طور همزمان	ارتقای نرم‌افزاری	هزینه پایین	نیاز به اطلاعات قبل از شروع حمله و عدم کارایی در فریب‌های هماهنگ
پردازش فضایی	جهت ورود سیگنال به گیرنده	آرایه آنتن ویژه و ارتقای نرم‌افزاری	قابلیت اطمینان بالا و عدم نیاز به اطلاعات قبلی	هزینه بالا و عدم کارآیی در چندمسیری و چندآنتنه
SQM	همبستگی	ارتقای نرم‌افزاری و سخت‌افزار اضافه برای نصب آرایه آنتنی	تشخیص آسان	عدم کارآیی در چندمسیری و فریب هوشمند نیاز به اطلاعات قبل از شروع حمله
VSD	همبستگی	ارتقای نرم‌افزاری	امکان تفکیک چندمسیری	عدم کارآیی در فریب هماهنگ
VB	همبستگی	حلقه ردیابی اضافی	دقت تشخیص بالا	هزینه بالا
ترکیبی	همبستگی و توان	ارتقای نرم‌افزاری	قابلیت اطمینان بالا و پیاده‌سازی آسان	کاهش کارآیی در حضور چندمسیری
الگوریتم ارائه‌شده در این مقاله	شبه‌فاصله	ارتقای نرم‌افزاری	سرعت بالای تشخیص پیاده‌سازی آسان	عدم کارآیی در فریب هوشمند و نیاز به اطلاعات قبل از شروع حمله

۶- مراجع

[1] Mosavi, M. R., "Frequency Domain Modeling of GPS Positioning Errors", IEEE Conference on Signal Processing, Vol. 4, pp. 1-4, Nov. 2006.

[2] Jahromi, A. J., Broumandan, A., Nielsen J. and Lachapelle, G., "GPS Spoofer Countermeasure Effectiveness Based on Signal Strength, Noise Power and C/N_o Observables", International Journal of Satellite Communications and Networking, Vol. 30, No. 4, pp. 181-191, June 2012.

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

[4] Lo, S. C., and Enge, P. K., "Authenticating Aviation Augmentation System Broadcasts", IEEE/ION Position, Location and Navigation Symposium, pp. 708-717, 2010.

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

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

[7] Petovello, M. G., "Real-Time Integration of a Tactical-Grade IMU and GPS for High-Accuracy Positioning and Navigation", Doctoral Dissertation, Department of Geomatics Engineering, University of Calgary, Alberta, Canada, 2003.

[8] Warner, J. S., and Johnston, R. G., "GPS Spoofing Countermeasures", Vulnerability Assessment Team, Los Alamos National Laboratory, Vol. 10, pp. 22-30, Dec. 2003.

[9] Moshavi, S., "Multi-User Detection for DS-CDMA Communications", IEEE Communications Magazine, Vol. 34, No. 10, pp. 124-135, Oct. 1996.

[10] Wen, H., Huang, P. Y. R., Dyer, J., Archinal, A. and Fagan, J., "Countermeasures for GPS Signal Spoofing", The 18th International Technical Meeting of the Satellite Division of The Institute of Navigation, pp. 1285–1290, Sep. 2005.

[11] Jin, M. H., Han, Y. H., Choi, H. H., Park, C., Heo, M. B., and Lee, S. J., "GPS Spoofing Signal Detection and Compensation Method in DGPS Reference Station", The 11th International Conference on Control, Automation and Systems, pp. 1616-1619, Oct. 2011.

[12] Papadimitratos, P. and Jovanovic, A. "GNSS-Based Positioning: Attacks and Countermeasures", IEEE Military Communications Conference, pp. 1-8, 2008.

[13] Ochin, E., Dobryakova, L. and Lemieszewski, L. "Design and Analysis of GNSS Antispoofing Algorithms", Scientific Journals Maritime University of Szczecin, pp. 93-101, 2012.

[14] Montgomery, P. Y., Humphreys, T. E. and Ledvina, B. M., "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense Against a Portable Civil GPS Spoofer", Institude of International Technical Meeting of the Institute of Navigation, pp. 1-7, Jan. 2009.

[15] McDowell, C. E., "GPS Spoofer and Repeater Mitigation System Using Digital Spatial Nulling", US Patent 7250903 B1, 2007.

[16] Broumandan, A., Jahromi, A. J., Dehgahanian, V., Nielsen, J. and Lachapelle, G., "GNSS Spoofing Detection in Handheld Receivers Based on Signal Spatial Correlation", IEEE/ION Position, Location and Navigation Symposium, pp. 479-487, April 2012.

[17] Nielsen, J., Broumandan, A. and Lachapelle, G., "GNSS Spoofing Detection for Single Antenna Handheld Receivers", Journal of the Institute of Navigation, Vol. 58, No. 4, pp. 335-344, 2011.

[18] Nielsen, J., Broumandan, A. and Lachapelle, G., "Spoofing Detection and Mitigation with a Moving Handheld Receiver", GPS World Magazine, Vol. 21, No. 9, Sep. 2010.

[19] Phelts, R. E., "Multicorrelator Techniques for Robust Mitigation of Threats to GPS Signal Quality", Doctoral Dissertation, Stanford University, California, 2001.

[20] Mitelman, M. "Signal Quality Monitoring for GPS Augmentation Systems", Doctoral Dissertation, The Department of Electrical Engineering, Stanford University, California, Dec. 2004.

[21] Shepard, D. P., and Humphreys, T. E., "Characterization of Receiver Response to Spoofing Attacks", GPS World, Vol. 21, No. 9, pp. 27-33, 2010.

[22] Ledvina, B. M., Bencze, W. J., Galusha, B. and Miller, I. "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers", The 23rd International Technical Meeting of the Institute of Navigation, pp. 689-712, Jan. 2010.

[23] Cavaleri, A., Motella, B., Pini, M. and Fantino, M., "Detection of Spoofed GPS Signals at Code and Carrier Tracking Level", The 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, pp. 1-6, Dec. 2010.

[24] Pini, M., Fantino, M., Cavaleri, A., Ugazio, S. and Presti, L. L., "Signal Quality Monitoring Applied to Spoofing Detection", The 24th International Technical Meeting of The Satellite Division of the Institute of Navigation, pp. 1-9, Sep. 2011.

[25] Stansell, T., "Location Assurance Commentary", GPS World, Vol. 18, No. 7, pp. 19, July 2007.

[26] Montgomery, P. Y., Humphreys, T. E. and Ledvina, B. M., "A Multi-Antenna Defense: Receiver-Autonomous GPS Spoofing Detection", Inside GNSS, Vol. 4, No. 2, pp. 40-46, March/April 2009.

[27] Scott, L., "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems", The 16th International Technical Meeting of the Satellite Division of the Institute of Navigation, pp. 1542-1552, 2003.

[28] Sahmoudi, M. and Landry, R. J., "Multipath Mitigation Techniques Using Maximum-Likelihood Principle", Inside GNSS, pp. 24-29, 2008.

[29] Mubarak, O. M., and Dempster, A. G., "Analysis of Early Late Phase in Single and Dual Frequency GPS Receivers for Multipath Detection", GPS Solution, Vol. 14, pp. 381-388, 2010.

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