ارائه روشی جدید و ارزان قیمت برای تولید داده فریب GPS به منظور محافظت از سامانه‌های ناوبری دریایی

امیررضا بازیار[۱]، سید محمدرضا موسوی میرکلایی[۲]، عبدالرضا رحمتی[۳]، مریم معاضدی[۴]

m_mosavi@iust.ac.ir

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

چکیده

سیستم GPS کل جهان را تغییر داده است. این مسئله به ویژه در کاربردهای صنعت دریانوردی، شامل جستجو و نجات صادق است. امنیت و قابلیت اطمینان سیستم GPS در حضور حمله فریب دچار اختلال می‌شود. ازاین‌رو در سال‌های اخیر مطالعه و تحقیق در رابطه با روش‌های مقابله با فریب به یکی از موضوعات مهم تحقیقاتی به ویژه در سامانه‌های ناوبری دریایی، تبدیل شده است. در طراحی روش‌های ضدفریب، یکی از نیازمندی‌های اساسی، تهیه داده‌های فریب واقعی به منظور راست‌آزمایی الگوریتم پیشنهادی است. از طرفی دیگر برای تولید داده‌های فریب واقعی باید دستگاه‌های گران‌قیمت فریبنده تهیه گردد که در اغلب موارد مقدور نمی‌باشد. ازاین‌رو تهیه داده معتبر فریب بدون نیاز به دستگاه فریب‌دهنده، می‌تواند برای مطالعات ضدفریب مفید واقع شود. در این مقاله روشی جدید و ارزان قیمت ارائه شده است که به کمک آن و تنها با استفاده از گیرنده نرم‌افزاری و داده‌های واقعی GPS، مجموعه‌ای از داده‌های فریب معتبر تولید می‌شود. به این ترتیب که در آن با بهره‌گیری از ساز و کار تأخیر و ترکیب، داده فریبی فراهم شده است که در صورت به کاربردن، دستگاه فریب‌دهنده در آنتن ورودی گیرنده هدف در سامانه دریایی ایجاد می‌گردد. پس از شرح الگوریتم تولید فریب، اعتبارسنجی روش پیشنهادی با آزمایش‌های مناسب انجام شده است.

واژگان کلیدی: گیرنده GPS، فریب‌دهنده، سیگنال جعلی، سیگنال معتبر، ناوبری دریایی.

تاریخ دریافت مقاله :	۹۳/۰۸/۰۱
تاریخ پذیرش مقاله :	۹۴/۰۳/۲۴

۱- مقدمه

در چند دهه اخیر مکان‌یابی، ناوبری و سیستم‌های وابسته به سیستم موقعیت‌یاب جهانی[1](GPS) نقش بسزایی در سامانه دریایی ایفا کرده‌اند. در ناوبری دریایی تعیین موقعیت مکانی برای افسر کشتی، هم در دریاهای آزاد و هم در بنادر و راه‌های دریایی پر رفت و آمد بسیار حائز اهمیت است. نیاز به اطلاعات دقیق موقعیتی در مواقعی مانند ورود و خروج کشتی به بندر اهمیت بیشتری پیدا می‌کند. ترافیک کشتی‌ها و دیگر خطرهای احتمالی راه‌های آبی، دقت مانور شناورها و کشتی‌ها، خطر تصادفات را بسیار بیشتر می‌کند. امروزه دریانوردان و اقیانوس‌شناسان به طور فزآینده‌ای از GPS درنقشه‌برداری زیرآب و مکان‌یابی نقاط خطرزا استفاده می‌کنند. همچنین شناورهای ماهی‌گیری نیز به منظور تعیین مکان بهینه ماهی‌گیری و ردیابی مهاجرت ماهی‌ها از این سیستم بهره می‌گیرند [۱].

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. از طرفی دیگر سیستم GPS دارای نقاط ضعفی است که آن را در برابر انواع اختلال‌ها آسیب‌پذیر کرده است. ازاین‌رو امنیت و صحت عملکرد این سیستم‌ها دارای اهمیت ویژه‌ای می‌باشند. هدف از طراحی سیستم‌های امن در سامانه‌های ناوبری، افزایش مقاومت ضعیف‌ترین جزء در برابر حملات قابل پیش‌بینی است [۲]. به‌طور کلی عیوب این سیستم جهانی را می‌توان در عبارات ذیل خلاصه کرد [۳]:

الف) سیستم ناوبری رادیویی.

ب) توان ضعیف سیگنال GPS در سطح زمین.

ج) نرخ به‌روز رسانی ضعیف.

این موارد فرصت و شرایط لازم را برای فریبنده‌ها جهت تولید سیگنال‌های جعلی فراهم می‌آورند، به گونه‌ای که گیرنده هدف در سامانه دریایی متوجه جایگزینی سیگنال توسط فریبنده نمی‌شود. البته سیگنال فریب در حین حمله فریب و پس از آن آثاری به جا می‌گذارد که با بررسی دقیق مشخصه‌های سیگنال قابل شناسایی و جبران‌سازی هستند. در دهه اخیر مطالعات زیادی در رابطه با بررسی سیستم GPS [۳-۷]، تولید فریب [۸-۱۵]، آشکارسازی [۱۳-۲۲] و کاهش فریب [۱۳-۱۷] ارائه شده است. در این مقاله بدون استفاده از سخت‌افزار یا نرم‌افزار اضافی با ساز و کار تأخیر و ترکیب در بیت‌های ناوبری تغییراتی ایجاد کردیم که در نتیجه آن موقعیت گیرنده هدف در سامانه دریایی فریب می‌بینند. در ادامه مقاله ابتدا انواع فریب‌دهنده‌ها را معرفی می‌کنیم. سپس مروری مختصر به فریبنده‌های موفقی که تاکنون ساخته شده‌اند، خواهیم داشت. در بخش بعدی به توضیح روش پیشنهادی می‌پردازیم. پس از آن آزمایشی که جهت بررسی صحت الگوریتم پیشنهادی انجام شده است را شرح می‌دهیم و در نهایت به طور کیفی مقایسه‌ای با کارهای قبلی انجام می‌دهیم.

۲- انواع فریب‌دهنده‌ها

۲-۱- شبیه‌ساز سیگنال GPS

ساده‌ترین نوع فریب استفاده از تقویت‌کننده توان و آنتن به همراه شبیه‌ساز سیگنال GPS است که می‌توانند سیگنال فرکانس رادیویی را به سمت گیرنده هدف در سامانه دریایی منتشر کنند. اساساً سیگنال‌های تولیدی توسط این شبیه‌سازها با سیگنال‌های واقعی GPS مطابق نمی‌باشند، اما اگر توان سیگنال فریب از توان سیگنال‌های معتبر GPS بیشتر باشد، حمله فریب مؤثر خواهد بود [۱۳].

با وجود ساده بودن این روش، مشکلاتی بر سر راه آن قرار دارد. هزینه زیاد برای تهیه و اندازه فیزیکی شبیه‌سازها از مهم‌ترین موانع می‌باشند. در ساده‌ترین حالت ممکن که شبیه‌ساز سیگنال در نزدیکی آنتن گیرنده هدف در سامانه دریایی قرار می‌گیرد، موقعیت قرار گرفتن و استتار شبیه‌ساز از چالش‌های پیش‌رو است [۸]. سهولت در آشکارسازی از عیوب این نوع فریبنده‌ها است. همزمان‌سازی خروجی شبیه‌ساز با سیگنال‌های GPS مجاورش، از مشکلات دیگر است. حمله غیرهمزمان، همانند پارازیت می‌ماند و ممکن است در گیرنده‌های ضعیف موجب از دست رفتن قفل حلقه ردیابی شود، در نتیجه اکتساب مجدد را به گیرنده تحمیل می‌کند.

اکتساب مجدد سوءظن به فریب را افزایش می‌دهد. حتی اگر حمله غیرهمزمان به هر طریقی از دست دادن قفل حلقه ردیابی را جبران کند، تغییرات ناگهانی در تخمین زمان اجتناب‌ناپذیر است. گیرنده هدف با مشاهده جهش

[1] Global Positioning System

بیش از ns ۱۰۰ از حمله فریب آگاه می‌شود [۱۴].

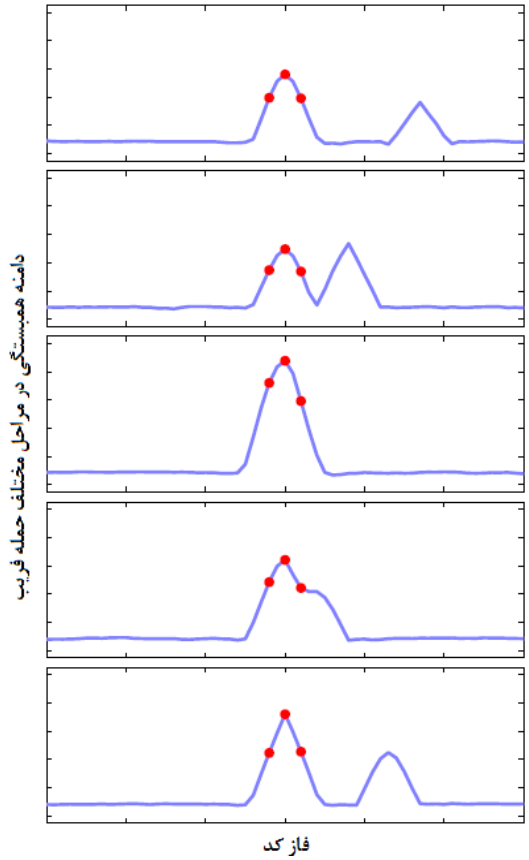
۲-۲- فریب‌دهنده بر اساس گیرنده

سرعت و موقعیت آنتن گیرنده هدف از جمله چالش‌های مطرح شده در تولید حمله فریب موفق است. این اطلاعات برای موقعیت دقیق سیگنال جعلی نسبت به سیگنال حقیقی در آنتن هدف در سامانه دریایی مورد نیاز است. بدون در نظر گرفتن این اطلاعات، حمله فریب به راحتی آشکار می‌شود. این نوع فریب‌دهنده می‌تواند به راحتی در نزدیکی گیرنده هدف قرار گیرد. ابتدا بخش گیرنده در فریب‌دهنده زمان، مکان و موقعیت خودش را با دریافت سیگنال حقیقی GPS تخمین می‌زند، فریبنده متوسط فاز کد، فرکانس حامل و داده ناوبری را به‌طور دقیق بازیابی می‌کند، بعد از آن بیشینه همبستگی سیگنال جدید را با نمونه متعلق به سیگنال واقعی منطبق می‌نماید.

پس از آن با توجه به فاصله اندک نسبت به گیرنده هدف در سامانه دریایی و اطلاعات به‌دست آورده، سیگنال فریب را تولید می‌کند. در شکل (۱) می‌توان نحوه تنظیم شدن بیشینه همبستگی سیگنال فریب با بیشینه نظیرش در سیگنال حقیقی را مشاهده کرد. فریبنده متوسط فاز کد، فرکانس حامل و داده ناوبری را به طور دقیق بازیابی می‌کند. بعد از آن بیشینه همبستگی سیگنال جدید را با نمونه متعلق به سیگنال واقعی منطبق می‌نماید. سپس به‌تدریج توان سیگنال جعلی افزایش می‌یابد. سرانجام سیگنال فریب کنترل نقاط ردیابی شده حلقه قفل تأخیر که بیشینه همبستگی را احاطه می‌کنند، در اختیار می‌گیرد. به دلیل تطابق این سیگنال با نمونه واقعی سیگنال GPS، آشکارسازی این نوع فریب با روش‌های معمول به راحتی امکان‌پذیر نمی‌باشد. با توجه به شکل (۲)، این فریب‌دهنده می‌تواند سیگنالش را با زمان GPS انطباق دهد و توسط مزیت مجاورت با گیرنده هدف، سیگنال جعلی را با سیگنال حقیقی تنظیم کند [۱۲-۱۴].

۲-۳- آرایه‌ای از فریب‌دهنده براساس گیرنده

حمله هماهنگ با بهره‌گیری از چند فریبنده، پیچیده‌ترین و مؤثرترین نوع از فریب است که می‌تواند احتمال آشکارسازی را کاهش دهد.



شکل (۱) کانالی در گیرنده که توسط سیگنال جعلی در کنترل فریب‌دهنده قرار می‌گیرد [۱۳].

در صورت به‌دست آوردن موقعیت آنتن گیرنده هدف و انطباق کامل سیگنال فریب با سیگنال معتبر GPS، روش‌های آشکارسازی فریب همانند زاویه ورود[1](AOA) کم اثر خواهند شد.

هرچند ممکن است انطباق فاز حامل و هماهنگی آرایه‌های فریب فقط برای محدوده بسیار کوچکی که آنتن گیرنده هدف در آن واقع شده است، به‌وجود آید. بنابراین منطقه اثر این نوع فریب‌دهنده بسیار محدود است. علاوه‌براین برخی از محدودیت‌های فیزیکی در مورد قرار دادن آنتن فریب‌دهنده نسبت به آنتن گیرنده هدف وجود دارد. بنابراین تحقق این نوع از فریب‌دهنده‌ها بسیار دشوار است و در بسیاری از موارد با توجه به موقعیت و یا حرکت آنتن گیرنده هدف، غیرممکن است [۱۲-۱۳].

۳- نمونه‌های عملی فریب‌دهنده

در این بخش گزارش‌هایی که فریب‌دهنده را با موفقیت

[1] Angle of Arrival

آزمایش کرده‌اند، مرور خواهند شد. یکی از اولین فریب‌های موفق توسط آقای وارنر و همکارش[1] در سال ۲۰۰۲ گزارش شده است [۷].

ایشان با استفاده از شبیه‌ساز WellNavigate GS720 و تقویت‌کننده سیگنال GPS، سیگنال‌های جعلی را برای فریب دادن گیرنده هدف منتشر ساختند که در آن فاصله موقعیت فریب‌دهنده و گیرنده هدف تقریباً ۹ متر می‌باشد. سیستم گیرنده-فریبنده را که در شکل (۳) نشان داده شده است، آقای هامفریس و همکارانش[2] در سال ۲۰۰۸ ارائه کردند [۱۴]. این دستگاه در واقع توسعه‌یافته گیرنده Cornell GRID می‌باشد [۲۳].

بخش سخت‌افزاری گیرنده این سیستم شامل بخش Zarlink/Plessey GP2015 RF front end به همراه Texas Instruments TMS320C6455 DSP و یک تسهیم‌کننده[3] سیگنال CPLD است. بخش سخت‌افزاری فریبنده شامل تبدیل‌کننده دیجیتال به آنالوگ، ترکیب‌کننده فرکانس، تضعیف‌کننده و آنتن برای منتشر کردن سیگنال می‌باشد. به‌دلیل محدودیت انتشار ناشی از قوانین سازمان ارتباطات فدرال[4] (FCC) آمریکا، این فریب‌دهنده در فضای آزاد آزمایش نشد و از طریق سیگنال‌های ذخیره شده و در فضای بسته صحت عملکرد آن مورد بررسی قرار گرفت.

همان‌طور که قبلاً اشاره شد، شکل (۲) نحوه در اختیار گرفتن کانال توسط این فریب‌دهنده را نشان می‌دهد. قاب بالایی نمایان‌گر تنظیم دقیق نقاط ردیابی شده بر روی بیشینه همبستگی سیگنال حقیقی و نزدیک شدن بیشینه سیگنال جعلی از راست می‌باشد. بعد از این‌که بیشینه جعلی خود را با سیگنال حقیقی تطبیق می‌دهد، به‌تدریج توان سیگنال را افزایش می‌دهد تا کنترل نقاط ردیابی را در اختیار گیرد. ذخیره‌سازی و انتشار تأخیردار همراه با انتقال مکانی سیگنال‌های GPS، راه‌کار آقای پناگیوتیس و همکارش[5] در سال ۲۰۰۸ می‌باشد [۱۵]. برای تأثیر بیشتر در این روش می‌توان از تأخیرهای متغیر برای ماهواره‌های مختلف استفاده کرد. در سال ۲۰۰۹ آقای مونت‌گومری و همکارانش[6] برای آشکارسازی سیگنال فریب، از روش ساده‌ای استفاده کردند [۱۲]. ایشان ابتدا سیگنال‌های معتبر GPS را ذخیره و بعد از انتقال به آزمایشگاه ایزوله نسبت به محیط بیرون[7]، دوباره سیگنال‌های ذخیره شده را منتشر می‌کنند. در این روش، فریبنده بر خلاف ارسال سیگنال معتبر از چندین ماهواره، تمام سیگنال‌های فریب را از یک منبع منتشر نماید.

۴- ساز و کار تأخیر و ترکیب

با توجه به تجربه‌های گذشته که در بخش قبلی گزارش شده‌اند، هنوز ساز و کار ساده و ارزان قیمتی برای ایجاد سیگنال جعلی وجود ندارد و در اغلب موارد برای تولید سیگنال فریب از دستگاه‌های فریبنده با نرم‌افزارهای پیچیده‌ای استفاده می‌شود که تهیه آن‌ها در اغلب موارد مقدور نمی‌باشد. مطالعه و تدبیر در مقاله‌های موجود، راه‌گشای روشی جدید در این زمینه شد تا بتوانیم بدون نیاز به سخت‌افزار یا نرم‌افزار اضافی، سیگنال معتبر فریب را برای انجام مطالعات ضدفریب فراهم کنیم.

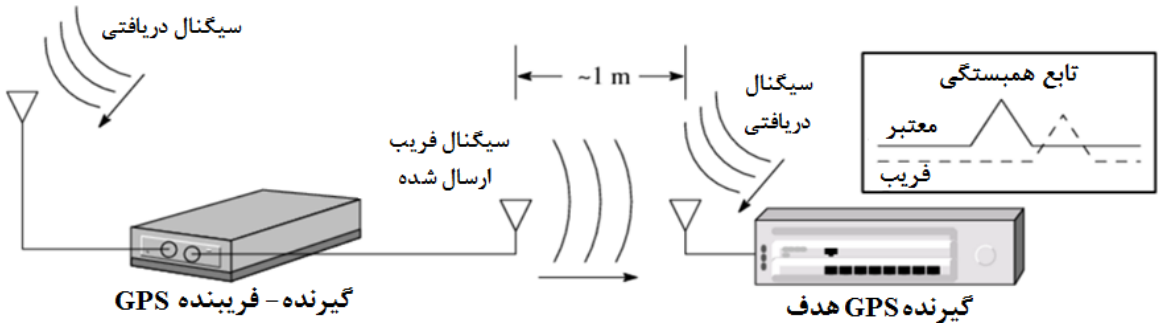
ذخیره‌سازی و تأخیر در سیگنال حقیقی GPS در گذشته بررسی شده است [۱۵]. با گسترش این ایده، به منظور تولید سیگنال جعلی از سیگنال‌های واقعی برای گیرنده نرم‌افزاری، ابتدا از سیگنال معتبر دریافتی به مدت کافی نمونه‌برداری و در فضای حافظه در دسترس ذخیره‌سازی کردیم و پس از ایجاد تأخیر مناسب، آن را برای ترکیب با سیگنال‌های حقیقی GPS منتشر نمودیم.

در حقیقت مفهوم ساز و کار تأخیر و ترکیب به معنای ایجاد سیگنال جعلی توسط ترکیب سیگنال حقیقی و سیگنال تأخیریافته GPS است. سیگنال L1 ارسالی از طریق ماهواره‌های GPS، با رابطه (۱) قابل بیان می‌باشد [۵].

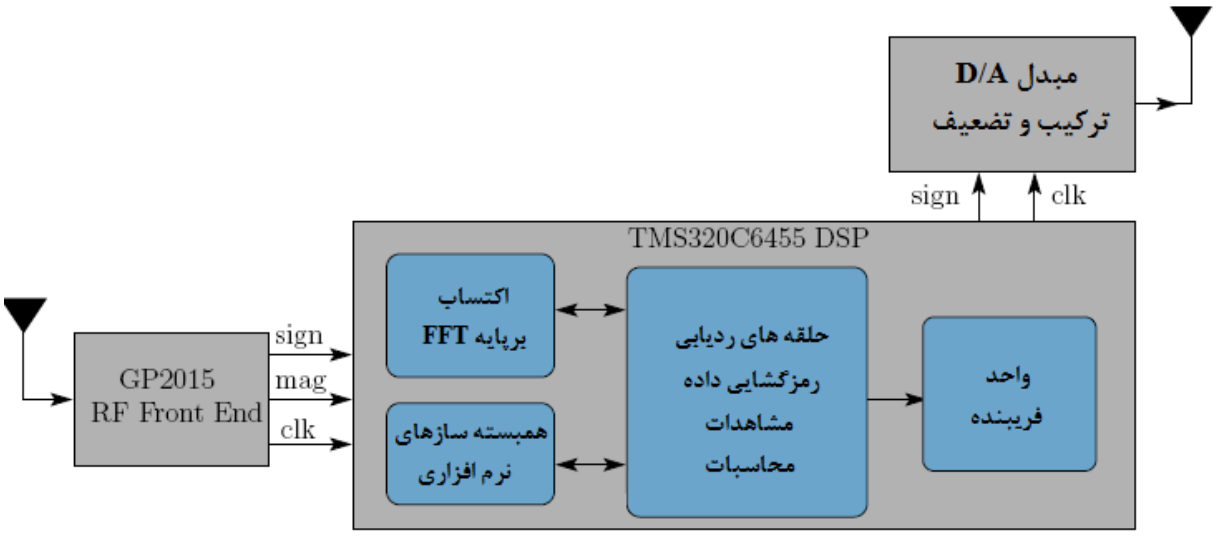
$$S_{L1}(t) = A_P P_i(t) W(t) D_i(t) \cos\left(\omega_{L1}(t+\Delta t)+\varphi_{L1}\right) + A_C C_i(t) D_i(t) \sin\left(\omega_{L1}(t+\Delta t)+\varphi_{L1}\right) \quad (۱)$$

در این رابطه $S_{L1}(t)$ سیگنال تولیدی توسط ماهواره‌های GPS، AP دامنه کد P، Pi(t) کد P iامین ماهواره، W(t) کد رمز شده، Di(t) پیام ناوبری iامین ماهواره، w_{L1} فرکانس

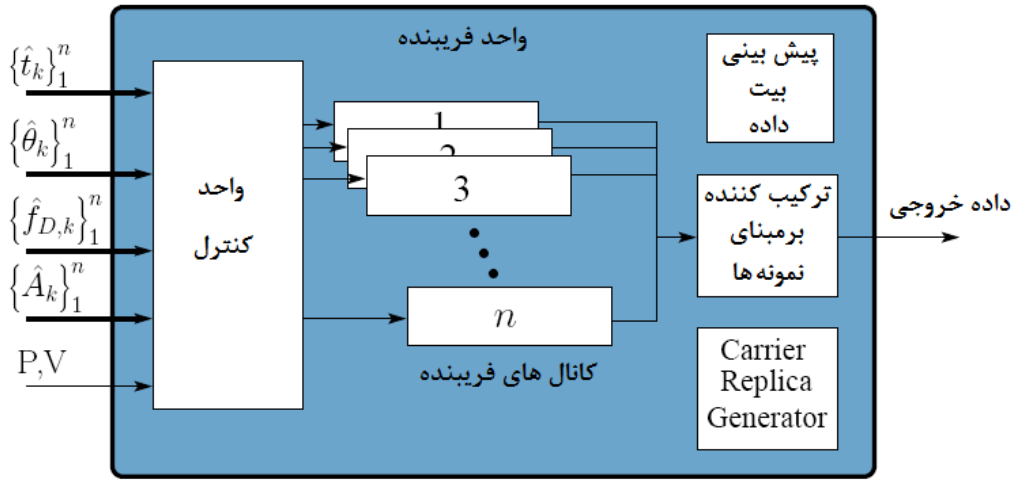
[1] Jon S. Warner and Roger G. Johnston
[2] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner
[3] Multiplexing
[4] Federal Communication Commission
[5] Panagiotis Papadimitratos and Aleksandar Jovanovic
[6] P. Y. Montgomery, T. E. Humphreys and B. M. Ledvina
[7] Outdoor



شکل (۲) نمایش حمله فریب از طریق فریب‌دهنده قابل حمل بر اساس گیرنده [۱۴].



شکل (۳) بلوک دیاگرام گیرنده-فریب‌دهنده [۱۴].



شکل (۴) بلوک دیاگرام فریبنده [۱۴].

زاویه‌ای[1] سیگنال L1، φ_{L1} فاز اولیه سیگنال L1، A_C دامنه کد C/A، Ci(t) کد C/A iامین ماهواره و Δt تأخیر انتشار سیگنال ماهواره می‌باشد. بخش آخر رابطه (۱) که سیگنال قابل بررسی برای گیرنده‌های GPS غیرنظامی می‌باشد، در رابطه (۲) قرار می‌گیرد.

$$S_{L1_{CA}}(t) = A_C C_i(t) D_i(t) \sin\left(\omega_{L1}(t+\Delta t)+\varphi_{L1}\right) \quad (۲)$$

[1] Angular Frequency

حال اگر رابطه (۲) را به‌عنوان سیگنال معتبر در نظر بگیریم، در صورت داشتن نرم‌افزار یا سخت‌افزار آماده فریبنده، سیگنال تأخیری به شکل زیر تولید می‌شود:

$$D_{L1_{CA}}(t) = A_C^D C_i^D(t_D) D_i^D(t_D) \sin\left(\omega_{L1}(t_D + \Delta t_D) + \varphi_{L1}\right) \quad (۳)$$

می‌دانیم در صورت داشتن گیرنده واقعی و انتشار سیگنال تأخیریافته رابطه (۳) توسط فریبنده و با وجود سیگنال واقعی GPS در محیط، مجموع دو سیگنال در ورودی گیرنده واقعی دریافت می‌شود. در نتیجه برای درک عمیق‌تر ساز و کار مورد نظر می‌توان سیگنال جعلی تولیدی در خروجی مبدل آنالوگ به دیجیتال گیرنده هدف را با رابطه (۴) مدل کنیم.

$$C_{L1_{CA}}(t) = A_C^A C_i^A(t_A) D_i^A(t_A) \sin\left(\omega_{L1}(t_A + \Delta t_A) + \varphi_{L1}\right) + A_C^D C_i^D(t_D) D_i^D(t_D) \sin\left(\omega_{L1}(t_D + \Delta t_D) + \varphi_{L1}\right) \quad (۴)$$

در این رابطه $C_{L1_{CA}}(t)$ سیگنال جعلی دریافتی در آنتن گیرنده می‌باشد، بالانویس A بیان‌گر سیگنال معتبر و بالانویس و زیرنویس D گویای سیگنال تأخیریافته هستند. رابطه (۴) در واقع معرف سیگنال نهایی است که گیرنده هدف برای استخراج مختصات مکانی و زمانی آن را پردازش می‌کند. برای تولید این سیگنال ابتدا به ذخیره‌سازی سیگنال معتبر GPS نیاز داریم. سپس سیگنال ذخیره شده را که گویای سیگنال تأخیری می‌باشد، منتشر می‌کنیم که در آنتن گیرنده با سیگنال حقیقی ترکیب می‌شود. در ساز و کار تأخیر و ترکیب دو عامل مؤثر وجود دارد: زمان تأخیر و دامنه سیگنال تأخیریافته. برای این‌که در گیرنده هدف سیگنال تأخیر یافته غالب شود دامنه آن را بزرگ‌تر از سیگنال اصلی در نظر گرفتیم. در بخش بعدی تأثیر عامل زمان تأخیر مورد بررسی قرار می‌گیرد.

با توجه به مطالب گفته شده، مراحل الگوریتم تولید فریب در ساز و کار تأخیر و ترکیب به‌گونه ذیل خلاصه می‌شوند:

الف) ذخیره‌سازی سیگنال معتبر GPS به‌عنوان سیگنال تأخیردار.

ب) انتشار سیگنال ذخیره شده (تأخیردار) برای ترکیب با سیگنال معتبر GPS در آنتن گیرنده.

۵- آزمایش‌ها

در این قسمت نتایج آزمایشگاهی که در سه نوبت انجام شده است، ارائه می‌شوند. ابتدا محدوده زمانی مشخص از سیگنال معتبر GPS را ذخیره می‌کنیم که در هر سه نوبت، این سیگنال ذخیره شده مورد استفاده قرار می‌گیرد. در این آزمایش‌ها سیگنال دریافتی در گیرنده هدف و سیگنال معتبر GPS متناظرش بررسی می‌شوند. نتایج توسط کامپیوتر شخصی با استفاده از گیرنده نرم‌افزاری GPS در نرم‌افزار MATLAB تحلیل می‌شوند [۲۴] و در نهایت نتیجه عملکرد سناریوی طراحی شده برای تولید سیگنال جعلی در راستای محور مختصاتی ENU[1] بیان می‌شوند.

در این آزمایش دامنه کد C/A تأخیردار دو برابر دامنه کد C/A معتبر در سیگنال جعلی می‌باشد ($A_C^D = 2A_C^A$). در نوبت اول بیش از ۲۵۰۰ نمونه از این آزمایش با زمان تأخیر متفاوت انجام شد که در ۲۱ نمونه جواب قانع‌کننده‌ای به‌دست آوردیم. در یکی از نمونه‌های موفق، دو سیگنال جعلی و حقیقی را در حوزه فرکانس بررسی می‌کنیم.

با توجه به شکل (۵)، تغییرات محسوسی در حوزه فرکانسی دو سیگنال مورد نظر دیده نمی‌شود. نتیجه عملیات بخش اکتساب در شکل (۶) قابل مشاهده است. همان‌طور که از شکل مشخص است، سیگنال جعلی ۴ ماهواره از ۶ ماهواره موجود در سیگنال معتبر GPS را با تغییر سطح توان آن‌ها، ردیابی کرده است. در نمونه مورد نظر، توانستیم توسط سیگنال جعلی، موقعیت گیرنده هدف را ۹۷۰ متر مؤثر[2] فریب دهیم.

جدول (۱) جزئیات فریب را در راستای سیستم مختصاتی ENU برای ۲۱ نمونه موفق نشان می‌دهد. ۱۳ و ۱۱۴۰ متر، کم‌ترین و بیش‌ترین مقدار مؤثر فریب گیرنده هدف در این آزمایش می‌باشند. برای بررسی تأثیر تأخیر به شکل (۷) توجه کنید. نقاط مشخص شده در شکل، گویای نمونه‌های موفق فریب هستند. همان‌طور که از شکل نیز مشخص است، میزان زمان تأخیر رابطه مشخصی با مقدار مؤثر فریب ندارد. برای اطمینان از صحت نتایج کسب شده در نوبت اول، آزمایش را در دو نوبت دیگر انجام یافت. در نوبت دوم بیش از ۱۴۰۰ نمونه با زمان تأخیر متفاوت آزمایش شد که توانستیم در ۲۰ نمونه مقدار فریب قابل قبول به‌دست آوریم.

جزئیات فریب در راستای سیستم مختصاتی ENU برای ۲۰

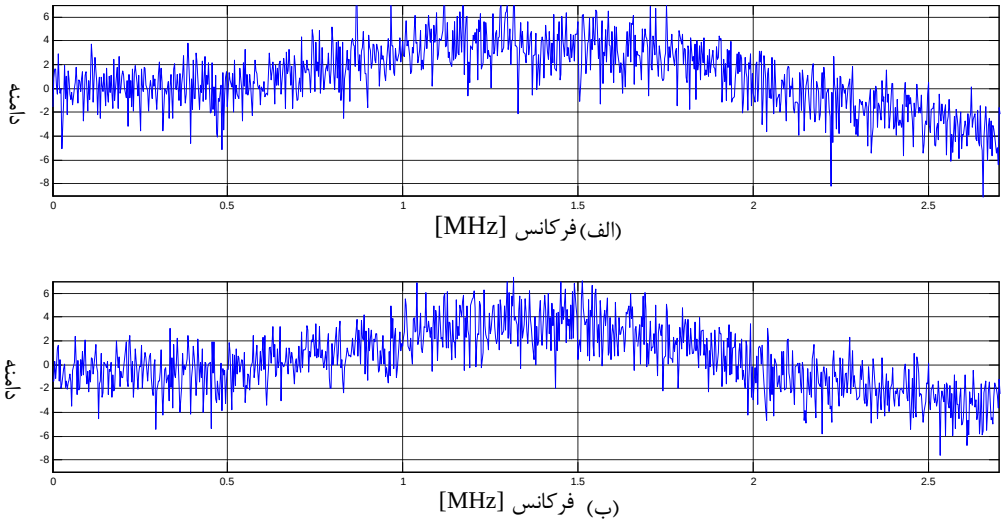
[1] East, North, Up
[2] RMS

نمونه موفق در جدول (۲) قابل مشاهده است. ۴ و ۵۳۲ متر، کمترین و بیشترین مقدار مؤثر فریب گیرنده هدف در این آزمایش می‌باشند. برای بررسی تأثیر تأخیر به شکل (۸) توجه کنید. در نوبت سوم بیش از ۷۵۰ نمونه با زمان تأخیر متفاوت بررسی شد که توانستیم در ۱۹ نمونه جواب قانع‌کننده‌ای به‌دست آوردیم. جزئیات فریب در راستای سیستم مختصاتی ENU برای ۱۹ نمونه موفق در جدول (۳) فراهم شده است.

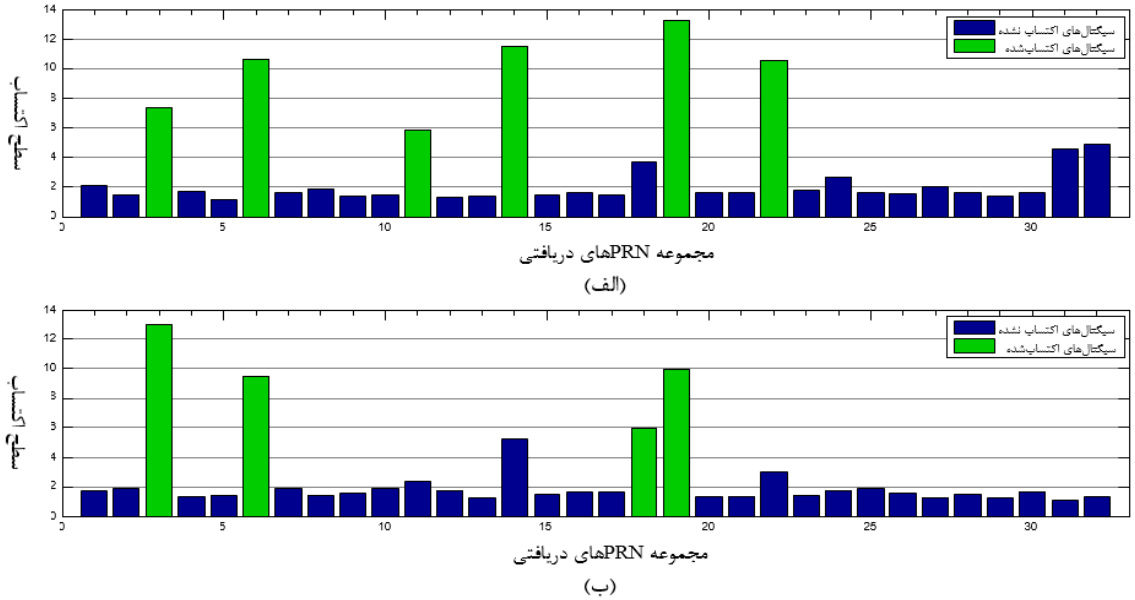
مقادیر ۸ و ۶۰۸ متر، کمترین و بیشترین مقدار مؤثر فریب گیرنده هدف در این آزمایش هستند. برای بررسی تأثیر تأخیر به شکل (۹) توجه کنید.

با دقت در جداول (۱) الی (۳)، متوجه می‌شویم که اثر سیگنال جعلی در هر سه محور مختصاتی ENU یکسان نمی‌باشد. فریب در اکثر موارد بر محور مختصاتی U تأثیر می‌گذارد، به‌عبارت دیگر سیگنال جعلی بیشتر ارتفاع گیرنده هدف را تحت تأثیر قرار می‌دهد.

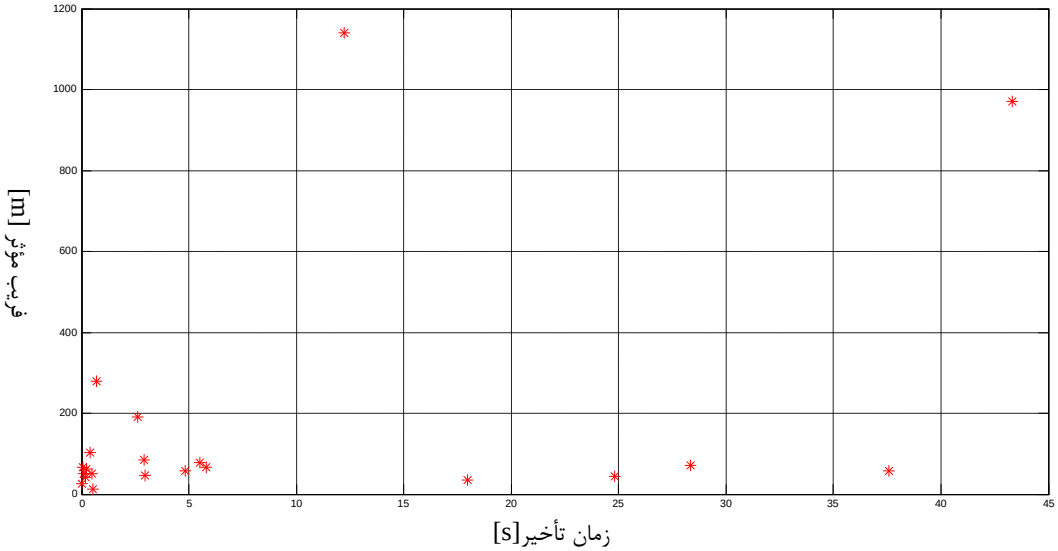
نمونه‌های موفق سه شکل (۷) الی (۹) در شکل (۱۰) جمع‌آوری شده است. کاملاً واضح است که زمان تأخیر با مقدار فریب رابطه مشخصی ندارد. کاهش چشم‌گیر نسبت تراکم فریب موفق قبل از زمان تأخیر ۵ ثانیه به بعد از این زمان، نکته مهم دیگری است که در این شکل نهفته است.



شکل (۵) نمایش حوزه فرکانس (الف) سیگنال حقیقی و (ب) سیگنال جعلی در حوزه فرکانس



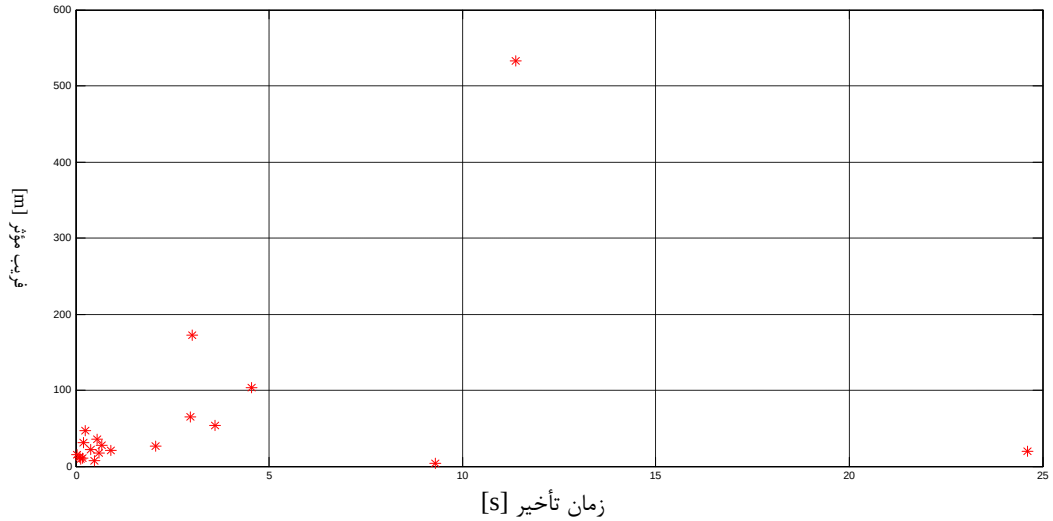
شکل (۶) سطح اکتساب (الف) سیگنال حقیقی و (ب) سیگنال جعلی.



شکل (۷) فریب مؤثر با توجه به تغییرات زمان در آزمایش نوبت اول.

جدول (۱) نتایج حاصل برای سیگنال جعلی در نوبت اول.

زمان تأخیر (میلی‌ثانیه)	خطای فریب در کل	مقدار فریب در مختصات U	مقدار فریب در مختصات N	مقدار فریب در مختصات E
	(متر)			
۱۲۲۵۰	۱۱۴۰	۱۰۵۴	۳۱۶	۲۹۸
۴۳۳۳۰	۹۷۰	۸۹۴	۲۷۶	۲۵۸
۷۰۰	۲۸۰	۲۶۹	۷۸	۷
۲۶۲۵	۱۹۲	۱۸۶	۲۹	۳۷
۴۲۰	۱۰۳	۹۴	۱۶	۳۸
۲۹۰۵	۸۴	۶۹	۲۱	۴۳
۵۵۳۰	۷۷	۴۱	۶۲	۲۲
۲۸۳۶۷	۷۱	۵۳	۳	۴۸
۵۷۲۶۰	۶۷	۱۴	۰	۶۶
۷۰	۶۶	۵۳	۳۶	۱۵
۲۴۵	۶۳	۶۲	۰	۹
۴۸۳۰	۵۸	۵۶	۱۲	۱۰
۳۷۵۹۰	۵۸	۴۱	۳۷	۱۵
۴۹۰	۵۲	۴۹	۶	۱۶
۱۰۵	۵۱	۴۹	۶	۱۴
۲۹۴۰	۴۵	۳۴	۱۵	۲۶
۲۴۸۱۵	۴۴	۳۰	۲۹	۱۳
۲۱۰	۴۱	۴۰	۱۰	۲
۱۷۹۷۲	۳۵	۱۸	۱۹	۲۵
۳۵	۲۵	۲۴	۵	۲
۵۲۵	۱۳	۱۲	۵	۲



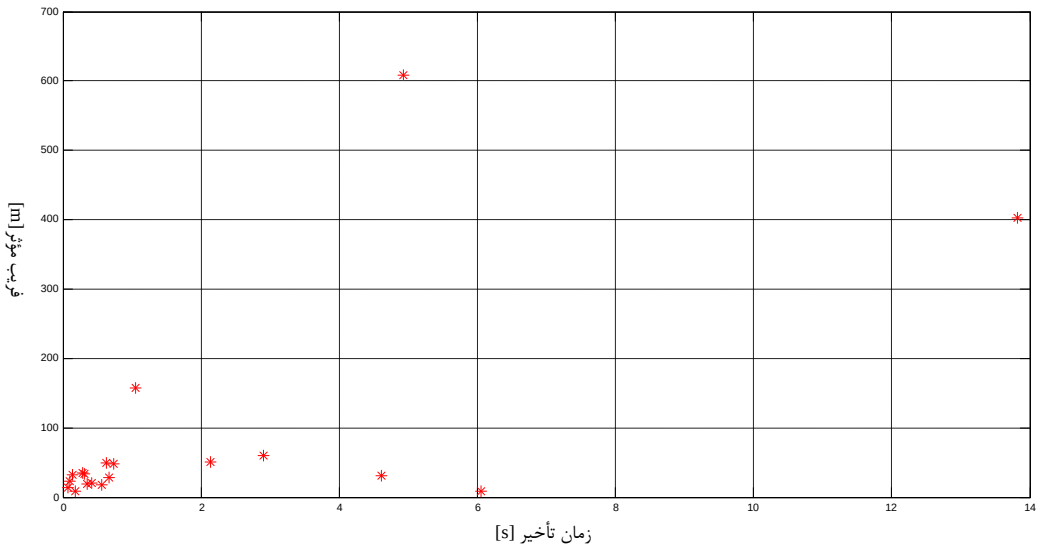
شکل (۸) فریب مؤثر با توجه به تغییرات زمان در آزمایش نوبت دوم.

جدول (۲) نتایج حاصل برای سیگنال جعلی در نوبت دوم.

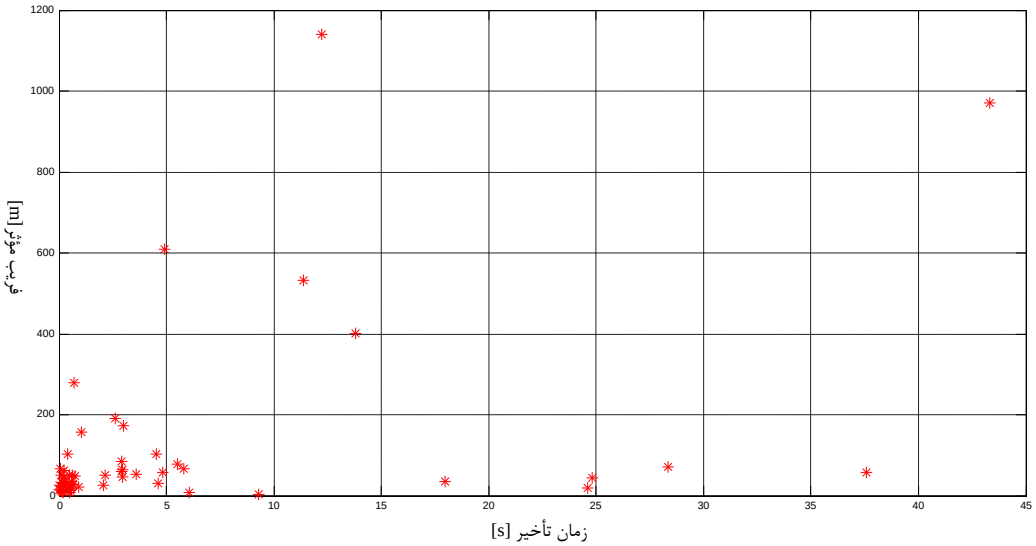
زمان تأخیر (میلی‌ثانیه)	خطای فریب در کل	مقدار فریب در مختصات U	مقدار فریب در مختصات N	مقدار فریب در مختصات E
	(متر)			
۱۱۳۹۲	۵۳۲	۴۹۰	۱۵۱	۱۴۲
۳۰۱۰	۱۷۲	۱۶۲	۴۲	۴۰
۴۵۵۰	۱۰۳	۹۹	۲۱	۲۱
۲۹۷۵	۶۵	۴۴	۳۹	۲۸
۳۶۰۵	۵۳	۱۲	۴۸	۲۱
۲۴۵۰	۴۶	۳۷	۲۱	۱۸
۵۶۰	۳۶	۲۸	۱۸	۱۲
۲۱۰	۳۱	۳۰	۳	۵
۶۶۵	۲۷	۶	۲۱	۱۶
۲۰۶۵	۲۷	۱	۲۳	۱۳
۳۸۵	۲۲	۲۱	۴	۲
۹۱۰	۲۱	۱۹	۷	۵
۲۴۶۲۲	۲۰	۵	۱۷	۱۰
۵۹۵	۱۸	۹	۱۴	۶
۳۵	۱۵	۱۰	۹	۷
۱۰۵	۱۲	۷	۳	۹
۱۷۵	۱۰	۸	۴	۵
۱۴۰	۱۰	۷	۴	۵
۴۹۰	۷	۷	۱	۱
۹۲۹۳	۴	۳	۲	۲

جدول (۳) نتایج حاصل برای سیگنال جعلی در نوبت سوم.

زمان تأخیر (میلی‌ثانیه)	خطای فریب در کل	مقدار فریب در مختصات U	مقدار فریب در مختصات N	مقدار فریب در مختصات E
	(متر)			
۴۹۳۵	۶۰۸	۵۶۱	۱۷۱	۱۶۱
۱۳۸۳	۴۰۲	۳۷۰	۱۱۴	۱۰۸
۱۰۵۰	۱۵۸	۱۵۴	۳۴	۱۰
۲۹۰۵	۶۰	۴۱	۳۵	۲۵
۲۱۳۵	۵۱	۳۹	۱۷	۲۸
۶۳۰	۵۰	۴۶	۱۰	۱۶
۷۳۵	۴۹	۴۶	۱۲	۱۳
۲۸۰	۳۵	۲۹	۱۳	۱۴
۳۱۵	۳۴	۳۰	۱۲	۷
۱۴۰	۳۲	۳۰	۱۱	۲
۴۶۲۰	۳۲	۸	۲۸	۱۳
۶۶۵	۲۸	۲۷	۵	۰
۱۰۵	۲۳	۲	۱۹	۱۴
۴۲۰	۲۱	۱۹	۷	۵
۳۵۰	۲۰	۱۹	۲	۶
۵۶۰	۱۷	۱۶	۵	۱
۷۰	۱۴	۱۱	۵	۸
۱۷۵	۹	۸	۱	۴
۶۰۵۵	۸	۸	۳	۰



شکل (۹) فریب مؤثر با توجه به تغییرات زمان در آزمایش نوبت سوم.



شکل (۱۰) فریب مؤثر با توجه به تغییرات زمان در مجموع سه نوبت.

۶- بررسی نتایج

در بخش قبل ملاحظه کردیم که ساز و کار تأخیر و ترکیب موجب فریب در موقعیت گیرنده هدف می‌گردد. در حقیقت ترکیب مذکور باعث تغییر بیت‌های مقدمه می‌شود که در ابتدای هر زیرقاب پیام ناوبری واقع شده‌اند. بنابراین زیرقاب‌ها تغییر می‌کنند و در نتیجه آن، بیت‌های ناوبری جدیدی تولید می‌شوند.

در بررسی انجام شده بر روی بیش از ۱۰۰ نمونه موفق فریب تولیدی به این نکته دست می‌یابیم که تغییرات ایجاد شده در سیگنال موجب کاهش شبه‌فاصله ماهواره‌ها و همچنین حرکت غیرواقعی مکان ماهواره‌ها می‌شود. دو عامل ذکر شده دلیل فریب در موقعیت گیرنده هدف در سامانه دریایی است. هم‌چنین در نمونه‌های بررسی شده به نکته دیگری پی می‌بریم. تغییرات شبه‌فاصله نسبت به تغییرات مکان ماهواره حدود ۱۰ برابر بیشتر است. این نسبت در حدود ۱۰۰ می‌باشد. با توجه مقادیر بزرگ شبه‌فاصله تغییر ایجاد شده قابل توجه است. بنابراین کاهش چشم‌گیر شبه‌فاصله گواه بر تغییرات بیشتر در ارتفاع گیرنده هدف نسبت به طول و عرض جغرافیایی است.

۷- جمع‌بندی و نتیجه‌گیری

در این مقاله توانستیم با ساز و کار تأخیر و ترکیب در بیت‌های ناوبری تغییراتی ایجاد کنیم که در نتیجه آن موقعیت گیرنده هدف در سامانه دریایی فریب می‌بینند. در اصل این ساز و کار موجب کاهش شبه‌فاصله‌ها و جابه‌جایی غیرواقعی مکان ماهواره‌ها می‌شود. کاهش چشم‌گیر شبه‌فاصله‌ها دلیل قانع‌کننده‌ای برای تغییرات بیش از حد ارتفاع گیرنده هدف است.

نمونه‌های گزارش‌شده در بخش ۳ فریب‌دهنده‌های موفق تولید کرده‌اند که مستلزم وقت و هزینه بالا می‌باشد. همچنین اغلب تکنیک‌های معرفی شده تغییرات حین حمله فریب را نیز بررسی می‌کنند که در این مطالعه فرض کردیم حمله فریب به اتمام رسیده و داده نهایی حاصل شده است. امیدواریم که در آینده الگوریتم مقابله مبتنی بر آشکارسازی و کاهش برای این ساز و کار ساده و ارزان ارائه کنیم.

۸- مراجع

[1] Grant, P. Williams, N. Ward and S. Basker, “GPS Jamming and the Impact on Maritime Navigation”, The General Lighthouse Authorities of the United Kingdom and Ireland, pp.1-12, 2001.

[2] Ferguson N. and B. Schneier, Practical Cryptography, John Wiley & Sons, 2003.

[3] Cheng, X. J., Cao, K. J., Xu, J. N. and Li, B., “Analysis on Forgery Patterns for GPS Civil Spoofing Signals”, The 4th International Conference on Computer Sciences and Convergence Information Technology, pp.353-356, 2009.

[4] Hein, G. W., Kneissl, F., Avila-Rodriguez, J. A. and Wallner, S., “Authenticating GNSS: Proofs Against Spoofs, Part II”, GNSS Magazine, pp.58–63, 2007.

[5] Lo, S., De Lorenzo, D., Enge, P., Akos, D. and Bradley, P., “Signal Authentication, a Secure

Civil GNSS for Today", GNSS Magazine, pp.30-39, 2009.
[6] Juang, J. C., "GNSS Spoofing Analysis by VIAS", Coordinates Magazine, Vol.7, No.1 , pp.11-13, 2011.
[7] Scott, L., "Location Assurance", GPS World, Vol.18, No.7, pp.14-18, 2007.
[8] Warner J. S. and Johnston, R. G., "A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing", Journal of Security Administration, pp. 1-8, 2002.
[9] Tippenhauer, N. O., Popper, C., Rasmussen, K. B. and Capkun, S., "On the Requirements for Successful GPS Spoofing Attacks", The 18th ACM Conference on Computer and Communications Security, pp.75-86,2011.
[10] Nighswander, T., Ledvina, B., Diamond, J., Brumley, R. and Brumley, D., "GPS Software Attacks", Computer Communication Networks—Security and Protection, pp.450-461, 2012.
[11] 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 Satellite Division of The Institute of Navigation, pp.689-712, 2010.
[12] 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 Satellite Division of The Institute of Navigation, pp.1-7, 2009.
[13] Jahromi, A. J., Broumandan, A., Nielsen, J. and Lachapelle, G., "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques", International Journal of Navigation and Observation, pp.1-16, 2012.
[14] 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", The 21st International Technical Meeting of the Satellite Division of The Institute of Navigation, pp.2314-2325, 2008.
[15] Papadimitratos, P. and Jovanovic, A., "GNSS-based Positioning: Attacks and Countermeasures", IEEE Military Communications Conference, pp.1-8, 2008.
[16] Jahromi, A. J., Lin, T., Broumandan, A., Nielsen, J. and Lachapelle, G., "Detection and Mitigation of Spoofing Attacks on a Vector-Based Tracking GPS Receiver", International Technical Meeting of The Institute of Navigation, pp.3-8, 2012.
[17] Nielsen, J., Broumandan, A. and Lachapelle, G., "Spoofing Detection and Mitigation with a Moving Handheld Receiver", GPS World Magazine, Vol. 21, No. 9, pp.27-33, 2010.
[18] White, N. A., Maybeck, P. S. and DeVilbiss, S. L., "Detection of Inter-ference/Jamming and Spoofing in a DCPS-aided Inertial System", IEEE Transactions on Aerospace and Electronic Systems, Vol.34, No.4, pp.1208–1217,1998.
[19] Shepard, D. P. and Humphrey, T. E., "Characterization of Receiver Response to Spoofing Attacks", GPS World, Vol.21, No.9, pp.27–33, 2010.
[20] Jahromi, A. J., Broumandan, A., Nielsen, J. and Lachapelle, G., "GPS Spoofer Countermeasure Effectiveness based on Signal Strength, Noise Power and C/No Observables", International Journal of Satellite Communications and Networking, Vol.30, No.4, pp.181–191, 2012.
[21] 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, 2005.
[22] 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, 2010.
[23] Humphreys, T. E., Psiaki, M. L., Kintner, P. M. and Ledvina, B. M., "GNSS Receiver Implementation on a DSP: Status, Challenges and Prospects", The 19th International Technical Meeting of the Satellite Division of The Institute of Navigation, pp.1-13, 2006.
[24] Borre, K., Akos, D. M., Bertelsen, N., Rinder P. and Jensen, S. H., "A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach", Birkhauser Boston, 2007.