

## ارائه الگوریتم RAIM بهبود یافته به منظور مقابله با اختلال فریب GPS در سامانه حمل و نقل ریلی

زهرا نقیب<sup>۱</sup>، علی صدر<sup>۲</sup>، سید محمد رضا موسوی میرکلانی<sup>۳</sup> و مریم معاضدی<sup>۴</sup>

<sup>۱</sup> دانشجوی کارشناسی ارشد، دانشکده برق دانشگاه علم و صنعت ایران؛ zahra\_naghib@elec.iust.ac.ir

<sup>۲</sup> استادیار، دانشکده برق دانشگاه علم و صنعت ایران؛ sadr@iust.ac.ir

<sup>۳</sup> استاد، دانشکده برق دانشگاه علم و صنعت ایران؛ m\_mosavi@iust.ac.ir

<sup>۴</sup> دانشجوی دکتری، دانشکده دانشگاه علم و صنعت ایران؛ m\_moazedi@elec.iust.ac.ir

### چکیده

مدیران حمل و نقل ریلی به کمک سیستم های ناوبری مانند GPS می توانند با جام جهان نمایی که به عنوان مرکز کنترل در دفترشان روی یک کامپیوتر نصب شده است، اطلاعات مورد نیاز خود در زمینه نحوه و زمان اجرای ماموریت ها و ایمنی و سلامت تیم های تحت پوشش خود و همچنین ناوگان در حال سیر را به طور مداوم در دسترس داشته باشند، تا در مواقع لازم در حداقل زمان تصمیم گرفته و دستورات لازم را صادر نمایند. از طرفی سیگنال های GPS به دلیل توان کم، در برابر تداخل های ناخواسته یا عمدی بسیار آسیب پذیر هستند و در نتیجه مستلزم روش هایی برای مقابله با تداخل در مسئله ناوبری می باشند. در میان انواع تداخل، فریب خطرناک ترین دخالت عمدی محسوب می شود. از این رو در این مقاله، روش نظارت صحت استقلال گیرنده (RAIM) برای مقابله با فریب به کار گرفته شده است. به طور دقیق تر این روش بر مبنای اندازه های شبه فاصله به تشخیص خطا (FD) می پردازد و بر این فرض استوار است که بیش از یک ماهواره جعلی وجود ندارد. نتایج شبیه سازی بر روی چندین مجموعه داده فریب، موفقیت قطعی آن را نشان می دهد.

**کلمات کلیدی:** نظارت صحت استقلال گیرنده (RAIM)، تشخیص فریب، شبه فاصله، امنیت، ناوگان ریلی.

### مقدمه

سامانه موقعیت یاب جهانی<sup>۱</sup> (GPS) یکی از پرکاربردترین سیستم های تعیین موقعیت ماهواره ای می باشد که امروزه از آن در بسیاری از کاربردهای بسیار دقیق استفاده می شود. با این که روز به روز سیستم های بیشتری به فناوری GPS مجهز می شوند که دقت مکان یابی خوبی دارند، وجود برخی عوامل در دنیای واقعی باعث خطا در موقعیت تخمین زده شده به وسیله GPS می گردد. یکی از این عوامل بروز خطا اختلال عمدی می باشد. به دلیل اینکه توان سیگنالی که به زمین میرسد، حدود 160dBW- می باشد (حدودا 20~30 dB کمتر از سطح نویز حرارتی گیرنده)، به شدت در معرض تداخل های ناخواسته (هارمونیک های ناشی از ایستگاه های انتشار امواج یا سایر منابع) یا عمدی قرار می گیرد [۱].

در میان انواع اختلال، فریب به عنوان خطرناک ترین دخالت عمدی شناخته شده است که به موجب آن، گیرنده GPS با ردیابی سیگنال های جعلی فریب می خورد و گیرنده را با اختلاف زمانی و مکانی از زمان دقیق و مکان فیزیکی واقعی آن ها به تولید اجباری نتیجه اشتباه ناوبری نائل می کند. برای بخش های هوانوردی غیرنظامی، مالی یا حمل و نقل و غیره، حمله فریب می تواند نتایج سنگینی داشته باشد. تولیدکننده فریب با تقلید از سیگنال های GPS معتبر به منظور گمراه کردن گیرنده هدف تلاش می کند و در دو مرحله شامل غلبه بر سیگنال ماهواره ای GPS و سپس ارسال سیگنال فریب انجام می شود. حمله فریب به طور قابل توجهی بیشتر از جَمینگ، گیرنده را تهدید می کند، چون گیرنده هدف از این تهدید آگاه نیست.

به طور کلی فریب GPS به سه دسته تقسیم می شود: ساده (از طریق شبیه سازی سیگنال GPS)، متوسط (از طریق فریب دهنده بر اساس گیرنده) و فریب پیچیده. هر نوع حمله فریب متناسب با روش مورد استفاده و دقت عمل کرد آن محدوده مشخصی به عنوان ناحیه هدف دارد. در مرحله نخست، باید وجود سیگنال فریب تشخیص داده شده و پس از آن به حذف یا کاهش آن اقدام کرد. آسیب پذیری GPS نسبت به فریب را می توان در سه سطح حل ناوبری/موقعیت یابی، بیت داده و پردازش داده بررسی کرد [۲-۴].

از آنجایی که فریبند می تواند شبه فاصله های جعلی در مشاهدات گیرنده ایجاد کند و منجر به PVT<sup>۲</sup> نادرست شود، در این مقاله روشی بر اساس بررسی شبه فاصله ها برای تشخیص فریب به کار گرفته شده است. در مواردی که تعداد شبه فاصله های فریب کم باشد، روش نظارت بر صحت

استقلال گیرنده (RAIM)<sup>۱</sup> قادر به شناسایی فریب است. در ادامه ابتدا به روش‌های تشخیص به اختصار اشاره می‌شود. در بخش سوم، به عملکرد روش RAIM پرداخته خواهد شد. در نهایت در بخش چهارم نتایج شبیه‌سازی برای تشخیص مطرح می‌شود.

### مروری بر روش‌های مقابله با فریب

مقابله با فریب می‌تواند در هر یک از بخش‌های گیرنده از جمله بخش پردازش سیگنال، بخش بیت داده، معادلات موقعیت‌یابی و بخش موقعیت‌یابی (ردیابی، ره‌یابی و استخراج شبه‌فاصله) انجام پذیرد [۵]. عمل تشخیص مستلزم تصمیم‌گیری برای تعیین جعلی بودن سیگنال است. در ادامه برخی از روش‌های موجود برای تشخیص مطرح و به اختصار شرح داده می‌شوند.

بررسی توان سیگنال دریافتی : در شرایط جوی مناسب، تغییرات تدریجی و یکنواخت در توان سیگنال دریافتی<sup>۲</sup> (RSS) مشاهده می‌شود، وجود سیگنال فریب که توان بیشتری دارد، ممکن است جهشی در RSS ایجاد کند که نشان دهنده حضور فریب باشد. بیشتر گیرنده‌های GPS از نسبت حامل به نویز<sup>۳</sup> (C/N<sub>0</sub>) به عنوان پارامتری برای سنجش کیفیت سیگنال دریافتی استفاده می‌کنند.

تنوع الگوی آنتن : این روش بر مبنای اختلاف بین مدل‌های انتشار فرستنده‌ها صورت می‌گیرد. منابع فریب معمولاً فرستنده‌های زمینی هستند که به طور همزمان چند سیگنال PRN را منتشر می‌کنند. در مقابل، سیگنال‌های GNSS معتبر از منابع توزیع شده فضایی یعنی ماهواره‌های GNSS فرستاده می‌شوند. این اختلاف با استفاده از آنتن‌های مختلف با الگوهای دریافت مختلف آشکار می‌شود و با استفاده از تحلیل‌های آماری برای تشخیص حضور سیگنال‌های فریب استفاده می‌شود.

تشخیص فریب بر اساس چند گیرنده : سیگنال‌های فریب را می‌توان با مقایسه اندازه‌های حاصل از گیرنده‌های مختلفی آشکار کرد که از لحاظ جغرافیایی مجزا هستند.

تأخیر بین داده و کد PRN : از این روش با عنوان تفکیک زمان ورود<sup>۴</sup> (TOA) نیز یاد می‌شود. در حالتی که فریب‌دهنده به عنوان گیرنده باشد، به دلیل این که هیچ اطلاعات قبلی در مورد بیت‌های داده ناوبری ندارد، ابتدا باید سیگنال‌های GPS دریافت‌شده را رمزگشایی<sup>۵</sup> کند و سپس کپی پردازش‌شده‌ای را به عنوان سیگنال فریب‌دهنده تولید کند. از این رو یک تأخیر اجتناب‌ناپذیر بین مرزهای بیت داده فریب‌دهنده و داده معتبر وجود دارد. بنابراین در صورتی که انتقال بیت داده ناوبری در لحظاتی از زمان با یک فاصله‌گذاری غیر از ۲۰ ms اتفاق بیافتد، ممکن است حمله فریب‌دهنده ظاهر شود [۶-۷].

نظارت بر کیفیت سیگنال : در گذشته روش‌های SQM برای بررسی کیفیت پیک همبستگی GPS در محیط‌های محوشدگی و چندمسیری به کار گرفته می‌شدند. حملات فریب بر روی یک گیرنده در حال حرکت می‌تواند همانند تأثیرات چندمسیری در نظر گرفته شود و برای هر دو مدل یکسانی تعریف کرد. در نتیجه روش‌های آشکارسازی چندمسیری یک پیشنهاد مناسب برای آشکارسازی فریب می‌تواند باشند. تصمیم‌گیری برای حضور یا عدم حضور حمله فریب معمولاً با آزمون‌های فرضیه آماری انجام می‌شود [۸-۹].

بررسی سازگاری با دیگر روش‌های موقعیت‌یابی : افزودن اطلاعات از تجهیزات کمکی مانند واحد اندازه‌گیری حرکتی<sup>۶</sup> (IMU) می‌تواند به گیرنده هدف برای تفکیک تهدید فریب کمک کند [۱۰]. علاوه‌براین گیرنده GPS می‌تواند موقعیت استخراج‌شده توسط سیگنال‌های GPS دریافتی را با دیگر روش‌های موقعیت‌یابی و ناوبری حاصل از ایستگاه‌های شبکه محلی بی‌سیم<sup>۷</sup> (WLAN) یا شبکه‌های موبایل مقایسه کند. بنابراین اگر ناحیه اطمینان روش‌های مختلف فصل مشترکی نداشته باشند، به احتمال قوی امکان حضور فریب وجود دارد. به‌کاربردن این روش، پیچیدگی سخت‌افزاری و نرم‌افزاری گیرنده GPS را افزایش می‌دهد.

پردازش فضایی : روش تشخیص فریب بر پایه زاویه ورود، روش قدرتمندی محسوب می‌شود. 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 فرستاده می‌شوند. از این رو می‌توان روش پردازش فضایی را برای تخمین اثر سه بعدی سیگنال‌های دریافت‌شده و تفکیک این سیگنال‌ها که رابطه فضایی دارند، به کار گرفت. برای اجرای این روش به داشتن آرایه‌ای از آنتن‌ها نیاز است.

Receiver Autonomous Integrity Monitoring

<sup>2</sup> Received Signal Strength

Carrier-to-Noise Ratio

Time Of Arrival

<sup>5</sup> Decode

<sup>6</sup> Inertial Measurement Unit

<sup>7</sup> Wireless Local Area Network

## RAIM برای مقابله با حمله فریب

RAIM اولین روشی بود که FAA برای تأمین نظارت GPS پذیرفت. این روش از سال ۱۹۹۲ به عنوان بخش اساسی دستگاه‌های الکتریکی هوایی در نظر گرفته شده است. RAIM اساساً برای تشخیص خطای ماهواره‌ای بر مبنای اندازه‌های شبه‌فاصله در ماهواره ایجاد شده است. طرح‌های مختلفی برای RAIM پیشنهاد شده‌اند و معمولاً بر پایه تحلیل باقیمانده‌ها انجام می‌شوند، یعنی اختلاف بین اندازه‌های پیش‌بینی شده و واقعی. الگوریتم‌های RAIM نیاز به حداقل یک درجه افزونگی به منظور تشخیص وجود خطا ( $FD^1$ ) در مجموعه اندازه‌گیری دارند، که با برقراری این شرط، روش RAIM قابل اجرا خواهد بود [۱۱]. به منظور به‌کارگیری این روش برای شناسایی فریب می‌توان سیگنال‌های فریب را خطاهایی برای سیگنال معتبر در نظر گرفت. بنابراین RAIM روشی عملی است که نیاز به سخت افزار پرهزینه ندارد. در این روش فرض بر آن است که بیش از یک ماهواره خطا دار به طور همزمان اتفاق نمی‌افتد. بر این مبنای، در صورت در دسترس بودن RAIM می‌توان تشخیص فریب را برآورد ساخت [۱۲]. بر اساس روش RAIM استاندارد، سیگنال فریب را می‌توان با مقایسه پارامتر آماره<sup>۲</sup> مبتنی بر اندازه‌های شبه‌فاصله با آستانه محاسبه شده با استفاده از روش خی‌دو شناسایی کرد. RAIM وجود سیگنال فریب را در صورتی اعلام می‌کند که آماره بیشتر از آستانه باشد. این روش از حداقل مربعات استفاده می‌کند. حداقل مربعات روشی در آمار است که برای حل دستگاه معادلاتی به کار می‌رود که تعداد معادله‌هایش بیش از تعداد مجهول‌هایش است. بر این اساس، مدل اندازه‌گیری GPS بر اساس رابطه زیر بیان می‌شود [۱۳-۱۹]:

$$y = Gx + e \quad (۱)$$

که در آن

- $y$  با ابعاد  $N \times 1$  مبین بردار اندازه خطی شده است که اختلاف بین اندازه شبه‌فاصله‌های خام و مقدار فاصله مورد انتظار بر اساس مکان ماهواره‌ها و موقعیت اولیه‌ی تخمین‌زده شده برای کاربر می‌باشد؛
- $x$  بردار حالت  $4 \times 1$ ؛
- $G$  ماتریس مشاهدده یا ماتریس طراحی با ابعاد  $N \times 4$  که یک ماتریس ارتباط خطی بین  $x$  و  $y$  است؛
- $e$  بردار خطای اندازه‌گیری ناشی از نویز گیرنده، انتشار موج، ephemeris و ... با ابعاد  $N \times 1$  می‌باشد.

پس از محاسبه ماتریس طراحی، روش حداقل مربعات برای تخمین  $x$  ( $X_{LS}$ ) بر اساس رابطه زیر بدست می‌آید:

$$X_{LS} = (G^T G)^{-1} G^T \cdot y = Ay \quad (۲)$$

$$y_{LS} = Gx_{LS} \quad (۳)$$

در معادله (۵)،  $y_{LS}$  نیز تخمینی از  $y$  است که در محاسبه بردار باقیمانده به کار گرفته می‌شود. بردار باقیمانده که اختلاف بین  $y$  و مقدار تخمین‌زده‌ی آن می‌باشد نهایتاً از رابطه زیر حاصل می‌شود:

$$\varepsilon_{LS} = y - y_{LS} = [I - G(G^T G)^{-1} G^T] e = Se \quad (۴)$$

این پروسه یک تبدیل خطی است که خطای اندازه‌ی فاصله را می‌گیرد و به بردار باقیمانده تبدیل می‌کند. پس از بدست آوردن بردار باقیمانده، از آن برای بدست آوردن مجموع مربعات خطا<sup>۳</sup> (SSE) استفاده می‌شود.

$$SSE = \varepsilon_{LS}^T \varepsilon_{LS} = e^T S^2 e \quad (۵)$$

مجموع مربعات باقیمانده نقش اساسی ملموسی در RAIM مورد بحث بازی می‌کند که از آن جهت بدست آوردن آماره استفاده می‌شود. در سال ۱۹۹۶، پارکسون<sup>۴</sup> اشاره کرده است که می‌توان از رابطه زیر برای بدست آوردن آماره استفاده کرد که نسبتاً غیر حساس به هندسه ماهواره/گیرنده است:

$$test\ statistic = \sqrt{\frac{SSE}{N-4}} \quad (۶)$$

و آستانه مورد نظر برای تصمیم‌گیری را نیز می‌توان از رابطه زیر محاسبه کرد:

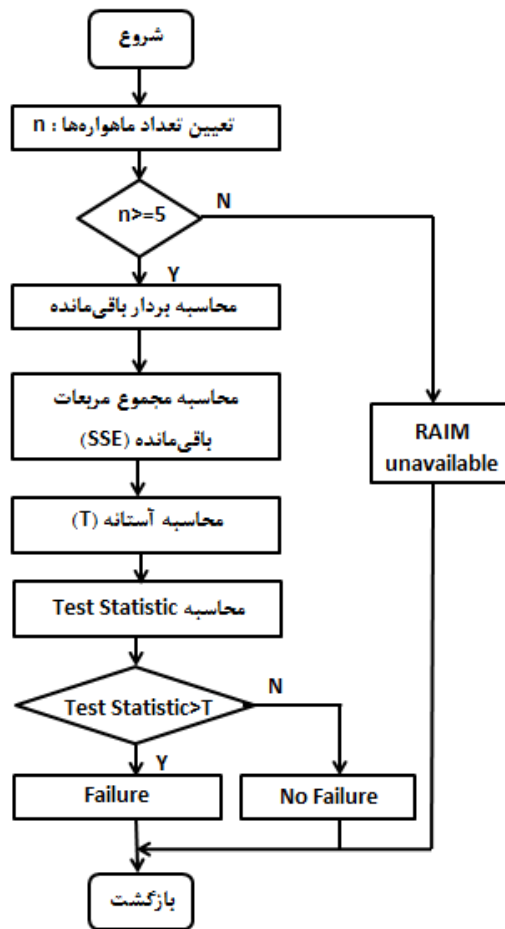
$$threshold = \left[ \frac{F_{N-4}^{-1} (1-P_{FA}) \sigma^2}{N-4} \right] \quad (۷)$$

که در آن

- $F_{N-4}^{-1}$ : معکوس تابع توزیع خی‌دو مرکزی

- $P_{FA}$ : ماکزیمم نرخ هشدار نادرست مجاز
- $\sigma$ : انحراف معیار فرضی خطای اندازه‌گیری

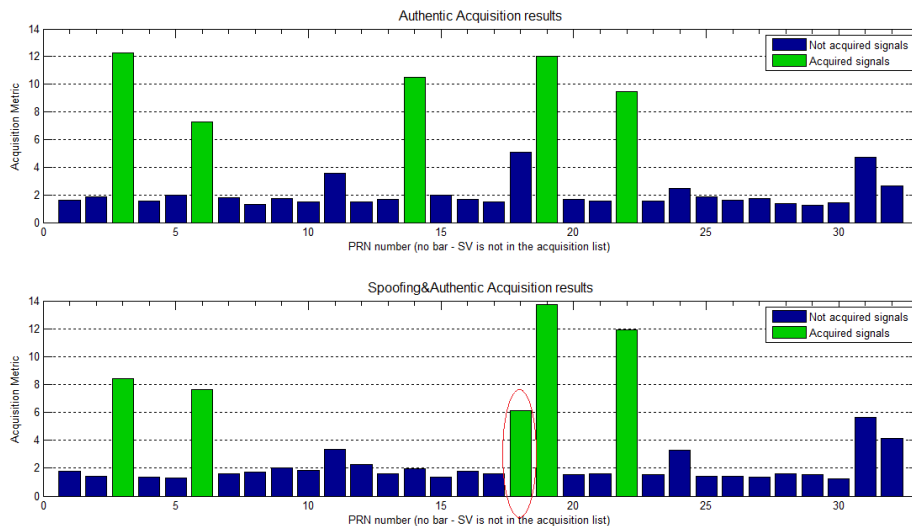
روند روش RAIM با استفاده از باقیمانده شبه‌فاصله در شکل زیر نشان داده شده است.



شکل ۱: فلوچارت تشخیص خطا بر اساس داده‌های باقیمانده شبه‌فاصله.

### بررسی و تحلیل نتایج

الگوریتم پیشنهادی بر روی چندین داده فریب مختلف پیاده‌سازی شد. جزئیات نتایج بدست آمده در این قسمت مطرح شده است. شکل ۲ نتیجه اکتساب ماهواره‌ها را برای داده نمونه تحت آزمایش نشان می‌دهد. همان‌طور که در شکل نیز مشخص است، پس از اعمال فریب یک ماهواره جعلی با PRN ۱۸ اضافه شده است. همچنین سطح اکتساب دیگر ماهواره‌ها نیز تغییر کرده است.



شکل ۲: نتیجه اکتساب ماهواره‌ها برای داده شماره ۱.

جدول ۱ تا ۴ نیز مقادیر بردارهای باقیمانده بدست‌آمده را برای داده‌های تحت آزمون نشان می‌دهد. همانطور که از جداول برمی‌آید، نرم بردار باقیمانده برای داده‌های فریب بیشتر از داده‌های معتبر می‌باشد، که نتیجه‌ی آن تأثیر بر SSE و افزایش آماره می‌باشد. در جدول ۵ نیز مقادیر آماره برای داده‌ها نشان داده شده است. از آنجایی که داده‌های تحت آزمون ۵ ماهواره‌ای هستند، درجه آزادی ۱ دارند و مقدار آستانه برای تمامی آن‌ها با احتمال هشدار نادرست  $\sigma = 4$  و  $0.00055$  بدست آمد. لازم به ذکر است بازه تغییر احتمال هشدار نادرست برای ۵ تا ۱۴ ماهواره قابل دید، مقداری ثابت بین  $10^{-7}$  تا  $10^{-1}$  می‌باشد.

جدول ۱: مقادیر بردار باقیمانده برای داده شماره ۱.

| داده شماره ۱ | شماره PRN (معتبر) | بردار باقیمانده (معتبر) | شماره PRN (فریب) | بردار باقیمانده (فریب) |
|--------------|-------------------|-------------------------|------------------|------------------------|
|              | ۳                 | -۶/۶۴۷۳۱۸۰۱۷            | ۱۹               | -۱۹/۹۵۰۴۰۵۸۹۵          |
|              | ۱۹                | ۳/۱۹۱۱۹۷۸۴۵۶۱           | ۲۲               | ۷/۷۵۹۰۴۸۴۹             |
|              | ۱۴                | -۰/۷۷۶۸۰۷۷۳۲            | ۳                | ۳۵/۲۹۵۸۵۰۲۲۶           |
|              | ۲۲                | -۰/۲۴۹۲۶۲۸۵۱            | ۶                | -۲۰/۸۵۷۶۸۱۴۹۸          |
|              | ۶                 | ۴/۴۸۲۱۸۹۶۸۵             | ۱۸               | -۲/۲۴۶۸۱۱۶۱۲           |
| norm         | ۸,۶۶۷۵۳۵۲۱        |                         | ۴۶,۳۰۴۵۳۱۲۶      |                        |

جدول ۲: مقادیر بردار باقیمانده برای داده شماره ۲.

| داده شماره ۲ | شماره PRN (معتبر) | بردار باقیمانده (معتبر) | شماره PRN (فریب) | بردار باقیمانده (فریب) |
|--------------|-------------------|-------------------------|------------------|------------------------|
|              | ۳                 | ۴/۰۱۵۴۳۹۵۰۶             | ۱۹               | -۱۹/۹۵۰۴۰۵۸۹۵          |
|              | ۱۹                | ۱/۸۵۹۳۴۱۲۴۳             | ۱۴               | ۷/۷۵۹۰۴۸۴۹             |
|              | ۱۴                | ۰/۵۶۶۳۷۰۳۰۶             | ۶                | ۳۵/۲۹۵۸۵۰۲۲۶           |
|              | ۶                 | ۲/۷۷۳۷۷۲۳۴۲             | ۳۱               | -۲۰/۸۵۷۶۸۱۴۹۸          |
|              | ۱۸                | ۰/۰۵۱۳۱۳۹۷۲             | ۲۳               | -۲/۲۴۶۸۱۱۶۱۲           |
| norm         | ۵,۲۵۳۳۹۱۷۹        |                         | ۴۲,۰۴۱۴۶۲۵۸۵     |                        |

جدول ۳: مقادیر بردار باقیمانده برای داده شماره ۳.

| داده شماره ۳ | شماره PRN (معتبر) | بردار باقیمانده (معتبر) | شماره PRN (فریب) | بردار باقیمانده (فریب) |
|--------------|-------------------|-------------------------|------------------|------------------------|
|              | ۳                 | ۴/۵۰۱۵۱۸۶۱۳             | ۲۳               | -۱۹/۹۵۰۴۰۵۸۹۵          |
|              | ۱۹                | ۲/۱۶۰۵۳۱۴۳۳             | ۶                | ۷/۷۵۹۰۴۸۴۹             |
|              | ۶                 | ۳/۰۳۵۲۹۶۲۹۵             | ۱۴               | ۳۵/۲۹۵۸۵۰۲۲۶           |

|      |            |             |             |               |
|------|------------|-------------|-------------|---------------|
|      | ۱۴         | ۰/۵۳۱۰۷۶۴۳۲ | ۱۹          | -۲۰/۸۵۷۶۸۱۴۹۸ |
|      | ۲۳         | ۰/۱۶۳۲۳۲۶۱۲ | ۳۲          | -۲/۲۴۶۸۱۱۶۱۲  |
| norm | ۵,۸۶۹۶۹۱۳۵ |             | ۱۷,۵۴۹۸۴۶۵۹ |               |

جدول ۴: مقادیر بردار باقیمانده برای داده شماره ۴.

| بردار باقیمانده (فریب) | شماره PRN (فریب) | بردار باقیمانده (معتبر) | شماره PRN (معتبر) | داده شماره ۴ |
|------------------------|------------------|-------------------------|-------------------|--------------|
| ۱۸,۹۰۶۱۹۵۸۹۱           | ۲۳               | ۲,۹۱۹۳۳۲۷۳۳             | ۱۹                |              |
| ۶,۵۰۰۸۸۳۲۲۵            | ۱۸               | -۰,۷۱۵۳۶۲۸۵۷            | ۳                 |              |
| ۱۲,۴۴۹۸۶۶۵۲۳           | ۳                | -۶,۰۶۹۵۹۴۱۶۱            | ۱۴                |              |
| -۱۰,۲۷۳۶۰۲۶۴۵          | ۱۴               | -۰,۲۲۰۷۸۰۵۶۱            | ۲۳                |              |
| ۱۴,۵۸۱۵۷۶۵۱۶           | ۱۹               | ۴,۰۹۲۶۰۵۰۰۶             | ۶                 |              |
| ۲۹,۵۴۴۴۴۴۲۷            | ۷,۹۱۴۳۰۴۷۳       |                         | norm              |              |

جدول ۵: مقادیر آماره برای داده‌های معتبر و فریب.

| Test statistic (A) | Test statistic (S) | تعداد ماهواره جعلی | تعداد ماهواره‌های داده معتبر | تعداد ماهواره‌های داده فریب | داده |
|--------------------|--------------------|--------------------|------------------------------|-----------------------------|------|
| ۱۳/۸۱۰۵            | ۱۴/۱۲              | ۱                  | ۵                            | ۵                           | ۱    |
| ۱۳/۱۹۰۴            | ۱۳/۹۳              | ۱                  | ۵                            | ۵                           | ۲    |
| ۱۳/۲۰۵             | ۱۶/۰۱۶             | ۱                  | ۵                            | ۵                           | ۳    |
| ۱۳/۲۷۴             | ۱۹/۰۶۶             | ۱                  | ۵                            | ۵                           | ۴    |

### جمع‌بندی و نتیجه‌گیری

در این مقاله به منظور شناسایی جمله فریب الگوریتم دقیق RAIM مطرح شد که بر اساس باقیمانده شبه‌فاصله با استفاده از روش حداقل مربعات عمل می‌کند. الگوریتم پیشنهادی توسط داده‌های فریب GPS آزموده و نشان داده شد که می‌تواند خطای موجود در اندازه‌ها را تشخیص و با تحلیل باقیمانده شبه‌فاصله‌ها، GPS را در برابر تداخل فریب هشدار دهد. نتایج آزمایش نشان داد که این روش بسیار ساده و عملی برای گیرنده‌های شهری GPS می‌باشد.

### مراجع

- [1] A. Cavaleri, B. Motella, M. Pini, M. Fantino, "Detection of Spoofed Signals at Code and Carrier Tracking Level", 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), pp.1-6, December 2010.
- [2] J. A. Larcom and H. Lio, "Modeling And Characterization of GPS Spoofing", IEEE International Conference on Technologies for Homeland Security (HST), pp.729-734, November 2013.
- [3] J. Liu, M. Lu, X. Cui and Z. Feng, "Theoretical Analysis of RAIM in The Occurrence of Simultaneous Two-Satellite Faults", Vol. 1, pp. 92-97, May 2007.
- [4] K. D. Wesson, D. Shepard and T. E. Humphreys, "Straight Talk on Anti-Spoofing", University of Texas Radio Navigation Laboratory, pp.32-63, January 2012.
- [5] A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen and G. Lachapelle, "GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation", IEEE/ION Position, Location and Navigation Symposium, pp.479-487, April 2012.
- [6] A. Jafarnia-Jahromi, A. Broumandan, L. Nielsen and G. Lachapelle, "GPS Spoofer Countermeasure Effectiveness Based on Signal Strength, Noise Power and C/N<sub>0</sub> Observables", International Journal of Satellite Communications and Networking, Vol.30, No.4, pp.181-191, May 2012.
- [7] B.M. Ledvina, W.J. Bencze, B. Galusha and I. Miller, "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers", Proceedings of the 2010 International Technical Meeting of The Institute of Navigation, pp.689-712, January 2010.

- [8] S.C. Lo and P.K. Enge, "Authenticating Aviation Augmentation System Broadcasts", Proceedings of the IEEE/ION Position Location and Navigation Symposium (PLANS), pp.708–717, May 2010.
- [9] R.E. Phelts, "Multicorrelator Techniques for Robust Mitigation of Threats to GPS Signal Quality", Doctoral Dissertation, Stanford University, California, 2001.
- [10] A.M. Mitelman, "Signal Quality Monitoring for GPS Augmentation Systems", A Dissertation for the Degree of Doctor of Philosophy, The Department of Electrical Engineering, Stanford University, California, December 2004.
- [11] 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", in Proceedings of International Technical Meeting of The Institute of Navigation, pp. 3-8, Jan. 2012.
- [12] X. J. Cheng, K. J. Cao, J. N. Xu and B. Li, "Analysis on Forgery Patterns for GPS Civil Spoofing Signals", in proceedings of the 4<sup>th</sup> International Conference on Computer Sciences and Convergence Information Technology (ICCIT' 09), pp. 353-356, Nov. 2009.
- [13] Y. C. Lee, "A New Improved Raim Method Based on the Optimally Weighted Average Solution (OWAS) Under the Assumption of a Single Fault", Proceedings of the 2006 National Technical Meeting of The Institute of Navigation, pp. 574- 586. January 2006.
- [14] E. Wang, M. Cai and T. Pang, "A Simple and Effective GPS Receiver Autonomous Integrity Monitoring and Fault Isolation Approach", 2012 International Conference on Control Engineering Communication Technology (ICCECT), pp. 657-660. Dec. 2012.
- [15] E. Wang, Sh. Zhang and Z. Zhang, "GPS Receiver Autonomous Integrity Monitoring Approach Based on Pseudorange Residual Message", Software engineering and knowledge engineering, pp. 755-762, Vol. 162. 2012
- [16] K. O'Keefe, G. Lachapelle, A. D. Fazio and D. Bettinelli, "Receiver Autonomous Integrity Monitoring in Urban Vehicle Navigation: The Five Satellite", Journal of Global Positioning System, pp. 157-164, Vpl. 10, No. 2, 2011.
- [17] J. Lio, M. Lu, X. Cui and Z. Feng, "Theoretical Analysis of RAIM in The Occurrence of Simultaneous Two-satellite Faults", Radar, Sonar & Navigation, IET, pp.92-97, Vol. 1, May 2007, 2007
- [18] Y. Zhang, F. Wu and H. Isshiki, "A New Cascade Method for Detecting GPS Multiple Outliers Based on Total Residuals of Observation Equations", Position Location and Navigation Symposium (PLANS), pp. 208-215, April 2012.
- [19] F. Blumrich, "Parametric Study of RAIM Performance Using Nearly Uniformly Distributed Preference Points on the Earth's Surface", 28<sup>th</sup> international conference of the aeronautical science, 2012.