

# مدل‌سازی، تحلیل و پیشنهاد یک استراتژی با هدف کاهش اثرات جمینگ بر سیستم‌های کنترل قطار مبتنی بر ارتباطات (CBTC)

مقاله علمی - پژوهشی

\*محمدعلی صنیدیزاده (نویسنده مسئول)، دانشیار، دانشکده مهندسی راه‌آهن، دانشگاه علم و صنعت ایران، تهران، ایران

عاطفه طهماسبی، دانش‌آموخته کارشناسی ارشد، دانشکده مهندسی راه‌آهن، دانشگاه علم و صنعت ایران، تهران، ایران

فرزاد سلیمانی، پژوهشگر پسا دکتری، دانشکده مهندسی راه‌آهن، دانشگاه علم و صنعت ایران، تهران، ایران

\*پست الکترونیکی نویسنده مسئول: sandidzadeh@iust.ac.ir

دریافت: ۱۴۰۴/۰۶/۰۵ - پذیرش: ۱۴۰۴/۱۱/۰۲

صفحه ۹۰-۷۳

## چکیده

هدف اصلی سیستم کنترلی قطار، جلوگیری از برخورد قطارها و خارج نشدن آن‌ها از ریل هست. امروزه کنترل قطار بر پایه ارتباطات، از روش‌های مختلف مخابراتی برای انتقال اطلاعات کنترلی بین قطارها و قطار و کنار خط استفاده می‌کند. با این حال که فناوری اطلاعات و ارتباطات می‌تواند نقش مهمی در پیشرفت صنعت ریلی ایفا کند، اما امنیت اطلاعاتی در این سیستم در مقابل انواع حملات از جمله جمینگ آسیب‌پذیر می‌شود. در این مقاله، امنیت اطلاعاتی سیستم‌های کنترل قطار مبتنی بر ارتباطات (CBTC) بررسی شده است، به طوری که مهاجمی به ارتباطات بین قطارها یا قطار و کنار خط حمله می‌کند و باعث از کار افتادن سیستم‌های CBTC می‌شود. در ادامه، تأثیرات حمله جمینگ بر روی سیستم CBTC بررسی شده و برای مقابله با آن از روش پرش فرکانسی مبتنی بر طیف گسترده جهت ایجاد یک کانال امن برای ارسال سیگنال استفاده شده است و همچنین، محیط انتشار سیگنال موج‌بر نشت در نظر گرفته شده است، چرا که شکاف‌های عرضی موجود بر دیواره‌های موج‌بر نشت می‌تواند سیگنال‌های پایدار با قابلیت ضد تداخلی را فراهم کند؛ بنابراین، با توجه به این که عدم امکان بازگشایی سیگنال کانال و دسترسی به سیگنال، با استفاده از این روش‌ها جرم در رسیدن به هدف ناکام می‌ماند و اثرات آن به حداقل می‌رسد.

واژه‌های کلیدی: امنیت اطلاعات، سیستم‌های کنترل قطار مبتنی بر ارتباطات، پرش فرکانسی طیف گسترده، موج‌بر نشت

## ۱- مقدمه

سیگنالینگ بهره می‌برد. سیستم‌های حمل و نقل ریلی شهری نیز از سیستم‌های سیگنالینگ مرسوم در دنیا استفاده می‌نمایند. سیگنالینگ راه‌آهن مرسوم بر اساس چراغ سیگنال‌های رنگی و تشخیص قطار با کمک مدار راه و محورشمار بوده است این تکنولوژی برای حدود نیم‌قرن گذشته است. تاریخچه استفاده از سیستم‌های سیگنالینگ نشان داده است به‌جز بالا بودن هزینه سیستم‌های کنترلی قطارها، بعد از مدت بسیار کوتاهی، سیستم‌های نصب شده نیاز به تعمیر و نگهداری خواهد داشت

استفاده از سیستم‌های هوشمند کنترل ترافیک در راستای بالا بردن سطح ایمنی، دقت و سرعت در تمامی زمینه‌های حمل و نقل حائز اهمیت است. در این راستا در حمل و نقل ریلی شهری یا متروها به دلیل موقعیت مکانی-زمانی، حساسیت کنترل قطارها برای تردد افراد، بالاتر بوده و مستلزم توجه بیشتر در ارتقا سیستم‌های اجرا شده می‌باشد. در سیستم حمل و نقل ریلی بین‌شهری کشور قالب سیستم‌های کنترل ریلی بر پایه کنترل یک‌طرفه بوده و از سیستم‌های قدیمی یا بسیار قدیمی

سیستم‌های مبتنی بر آن بحث امنیت ارتباطات این شبکه است. از این رو در این مقاله امنیت سایبری سیستم‌های کنترل قطار مبتنی بر ارتباطات CBTC را بررسی خواهیم کرد و برای مقابله با اثرات جمینگ بر سیستم CBTC روش پرش فرکانسی مبتنی بر طیف گسترده را برای ارسال سیگنال انتخاب نموده به طوری که فرکانس موج حامل به طور متوالی و شبه تصادفی عوض می شود در حالی که این توالی برای فرستنده و گیرنده رادیویی شناخته شده است اما برای جمر نامفهوم است و همچنین محیط انتشار سیگنال را موج بر نشت در نظر گرفته زیرا شکاف‌های عرضی موجود بر روی دیواره‌های موج بر نشت می تواند سیگنال‌هایی با خاصیت ضدتداخلی فراهم کند.

## ۲- اصول عملکردی سیستم

برخلاف بسیاری از زمینه‌های تحقیقاتی و توسعه، تشریح جز به جز در سیستم CBTC، به جای دانشگاه توسط صنعت هدایت می شود. علاوه بر این، با توجه به ماهیت بسیار رقابتی صنعت، میزان ادبیات قابل دسترس در این موضوع که به طور آشکار جزئیات اجرایی را مورد بحث قرار دهد، بسیار کم است. در سیستم CBTC، از ارتباطات رادیویی پیوسته و با ظرفیت بالا برای تبادل اطلاعات کنترل قطار بین قطارها و کنارخط استفاده می شود و از ویژگی‌های این سیستم کنترل خودکار قطار، حفاظت خودکار قطار و هدایت خودکار قطار است. قطار به طور مداوم سرعت، جهت و موقعیت جغرافیایی خود را به سمت کنار خط از طریق اتصالات رادیویی می فرستد. بر اساس اطلاعات دریافت شده از تمام قطارهای حاضر در مسیر و علاوه بر آن قابلیت ترمز قطار، مرکز کنترل ترافیک در کنار جاده، حداکثر سرعت و فاصله را برای سفر محاسبه می کند و به قطار می فرستد که در مجموع به عنوان مجوز حرکت شناخته می شود. بر اساس این اطلاعات، تجهیزات ATC در قطار به طور مداوم سرعت قطار را تنظیم می کند و فاصله ایمنی هر قطار را با قطار جلویی خود حفظ می کند. با وجود این مبادله اطلاعات به صورت بلادرنگ، تجهیزات راه آهن مورد استفاده در سیستم‌های معمولی، مانند چراغ سیگنال‌ها و مدارراه‌ها، مورد نیاز نیست و می توانند برداشته شوند. سرعت و مکان یک قطار با استفاده از ترکیبی از دستگاه‌هایی مانند سرعت‌سنج، تاکومتر، فرستنده‌هایی همچون بالیس‌ها، رادار داپلر و سیستم‌های مکان‌یابی مانند سیستم موقعیت‌یابی جهانی تعیین می شود. صحت تعیین مکان، به طور ویژه، بسیار حیاتی

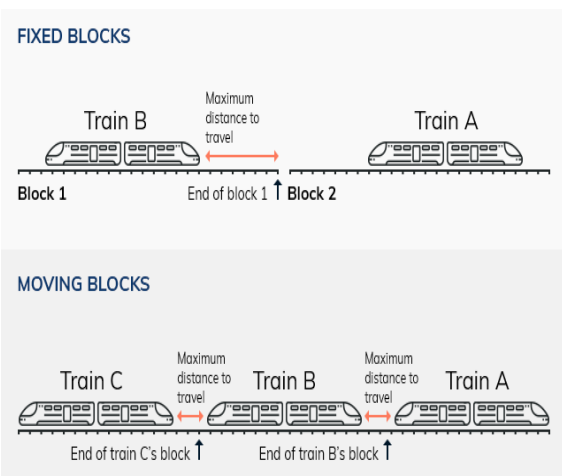
که از لحاظ هزینه بسیار بالا بوده و پس از مدتی این هزینه‌ها از هزینه‌ی اجرای اولیه سیستم، بالاتر خواهد شد. سیستم‌های اجرا شده به دلیل عدم هوشمندی دچار یک حلقه منفی شده و به جای هزینه مداوم برای ارتقا و یا نگهداری مناسب تجهیزات باید این هزینه‌ها صرف خرید تجهیزات تکراری شود. با ایجاد سیستم کنترل بر پایه‌ی ارتباطات CBTC، مدیریت ایمنی در داخل قطار، سرعت و دقت انتقال اطلاعات در ارتباط با دیگر مراکز کنترلی افزایش یافته و همچنین مدیریت محلی در کل سطح شهر ارتقا می‌یابد. در این صورت می‌توان به راحتی کنترل را به صورت دوطرفه انجام داد. در سیستم CBTC با استفاده از ارتباطات رادیویی اطلاعات کنترلی قطار با وضوح بالا و بلادرنگ منتقل می‌شود و همچنین با کاهش فاصله‌ی قطارها، ظرفیت خط افزایش می‌یابد و تجهیزات کنار خط نیز کاهش می‌یابد. در این سیستم، قطارها می‌توانند به طور مداوم وضعیت خود از قبیل موقعیت، سرعت، قابلیت کاهش سرعت و قابلیت افزایش سرعت در میان یکدیگر با ارتباطات بی‌سیم و با سرعت بالا مبادله کنند و بر طبق آن اطلاعات مسیر پیش رو را بهینه طی کنند. تمامی زیر سیستم‌های CBTC باید در برابر خطا ایمن بوده و ضریب اطمینان بالا و قابل قبولی داشته باشند با وجود محاسن زیاد شبکه‌های بی‌سیم در این سیستم‌ها، به دلیل ارتباطات غیر قابل اعتماد بی‌سیم و متحرک بودن قطار، عملکرد کنترل قطار می‌تواند به طور قابل توجهی تحت تأثیر قرار گیرد. مخصوصاً در سیستم‌های حمل و نقل شهری به دلیل این که فضای فیزیکی با محیط عمومی اشتراک دارد، منجر به شرایط بحرانی تری می‌شود برخلاف دیگر زیر ساخت‌های حیاتی که از فضای فیزیکی ایزوله هستند، این موقعیت مکانی خطر را افزایش می‌دهد همان‌گونه که مهاجمان نزدیک به هدف خود می‌توانند به راحتی تداخل‌های زیادی را به وجود آورند. در نتیجه، جمینگ یک مسئله مهم نگران‌کننده برای امنیت سایبری سیستم‌های کنترلی قطار بر پایه‌ی ارتباطات است (Lakshminarayana et al., 2018). زیرا جمینگ می‌تواند CBTC را غیرفعال کند و مزایای آن از جمله کارآمدی انتقالش را خنثی کند. با توجه به مسائل مطرح شده CBTC دارای شرایط سخت برای دسترسی به ارتباطات است و از دست دادن ارتباطات می‌تواند منجر به اختلالات شدید شود. سیستم CBTC با وجود مزایا و امتیازاتی که دارد بدیهی است که یکی از مسائل و چالش‌های در حال حاضر و آینده این استاندارد و

در سیستم CBTC، تعیین موقعیت یک قطار، از مدار راه به آن منتقل شده است (Zhu et al., 2012).

ارتباطات رادیویی به طور کلی غیر قابل اعتماد است. طراحی یک سیستم کنترل قطار قابل اعتماد بر روی یک لینک رادیویی غیر قابل اعتماد یک کار چالش برانگیز است. در سیستم‌های سیگنالینگ معمولی، فاصله بین قطارها با قطار پشتی زیاد است، همان‌طور که در شکل (۱) دیده می‌شود اما در سیستم CBTC، این فاصله مکانی بسیار کوتاه است، از این رو در صورت قطع ارتباط، قطار در آن زمان موقعیت را دریافت نمی‌کند. در این وضعیت، یک روش معمول در سیستم CBTC، اعمال ترمزهای اضطراری است و از آن پس قطار را در حالت دستی هدایت می‌کنند. در بدترین حالت، می‌تواند یک واکنش زنجیره‌ای با قطارهای پشتی ایجاد کند و همه بایستند (Alcala et al., 2011)، (Bu et al., 2014).

فاصله زمان تعلیق قبل از اعمال ترمزهای اضطراری در هر پروژه‌ای متفاوت است، بستگی به عوامل متعدد، از جمله فرکانس پیام‌های کنترل سیستم CBTC دارد. مقدار معمول بین ۵ تا ۱۰ ثانیه است. در مقایسه با سیستم‌های کنترل معمولی قطار، در سیستم CBTC، تعیین موقعیت یک قطار از مدار راه به خود قطار منتقل شده است (Pascoe et al., 2009). این تعیین موقعیت توسط قطار، قابل اطمینان و دقیق‌تر است. پیش از این، موقعیت قطار توسط کنار خط (با کمک یک مدار راه) مستقل از قطار تعیین شده، مشخص می‌شد.

طراحی ایمن مدارهای راه به گونه‌ای است که قطعی مدار راه به معنای حضور یک قطار در ایستگاه تفسیر شده است. اما، در سیستم CBTC، کنار خط برای دستیابی به موقعیت مکانی قطار وابسته است که به ارتباطات رادیویی بستگی دارد (Tazaki et al., 2012).



شکل ۱. بلاک ثابت و بلاک متحرک

است. فرستنده‌ها یا بالیس‌ها نقاط مرجع ثابت نصب شده بین ریل‌ها هستند. هنگامی که یک قطار از روی یک بالیس عبور می‌کند، اطلاعات محل از بالیس به قطار با استفاده از یک آنتن نصب شده در زیر قطار منتقل می‌شود. بین بالیس‌ها موقعیت به طور مداوم با استفاده از اندازه‌گیری مسافت سنج برآورد می‌شود و بر روی صفحه‌نمایش داده می‌شود. هر خطایی در طول مسیر به وجود آید، زمانی که قطار از روی بالیس بعدی می‌گذرد تصحیح می‌شود (Theeg et al., 2009). استاندارد IEEE CBTC توصیه می‌کند که دقت مکان ۵ تا ۱۰ متر باشد. تعدادی از مشکلات مربوط به استفاده از یک سیستم موقعیت یاب جغرافیایی مانند GPS به عنوان ابزار اصلی برای محلی سازی وجود دارد. صحت مکان سیستم‌های جغرافیایی ممکن است به اندازه کافی بالا نباشد، به عنوان مثال برای تشریح قطارهایی که نزدیک به یکدیگر حرکت می‌کنند. همچنین سیگنال‌های ماهواره‌ای قابل اعتمادی در داخل تونل‌ها دریافت نمی‌شود. علاوه بر این، تأمین کنندگان CBTC به طور کلی تمایلی به وابستگی سیستم ندارند که توسط یک شخص خارجی کنترل شود. بنابراین، استفاده از سیستم جغرافیایی در سیستم CBTC معمولاً مکمل است. در سیگنالینگ راه آهن متعارف، مسیرها به بلاک‌هایی تقسیم می‌شوند و مدارها برای تعیین اینکه قطار داخل کدام بلاک است نصب شده‌اند. هر بلاک با یک سیگنال محافظت می‌شود. عوامل مختلف طول بلاک را تعیین می‌کند، از جمله اینکه این خط چه مقدار شلوغ است، حداکثر سرعت مجاز در آن خط، قابلیت ترمز کردن قطارهای مختلف و فاصله دید را برآورد می‌کنند. هنگامی که قطار در داخل یک بلاک است، از آنجا که هیچ روش‌انی و به هنگامی برای تعیین مکان دقیق قطار در داخل بلاک نیست، کل بلاک‌ها به عنوان اشغال شده اعلام می‌شود و سایر قطارها اجازه ورود به آن را ندارند. از آنجا که مرزهای این بلاک‌ها بدون در نظر گرفتن سرعت و قابلیت ترمزی قطار، ثابت است این نوع وضعیت را وضعیت بلاک ثابت می‌نامند (Theeg et al., 2009)، (Pascoe et al., 2009). در مقایسه با وضعیت بلاک متحرک که در سیستم CBTC به کار رفته است، به لطف ارتباطات بلادرنگ بین قطار و کنار خط، موقعیت قطار به طور مداوم به روز می‌شود، در نتیجه منطقه اشغال شده یا بلاک با قطار حرکت می‌کند و نشان‌دهنده محل واقعی آن است. هیچ مرز ثابتی برای بلاک‌های آن وجود ندارد. همان‌طور که در شکل (۱) نشان داده شده است، اجازه می‌دهد تا قطارها به یکدیگر نزدیک‌تر شوند، در مقایسه با سیستم‌های کنترل معمولی قطار،

گره‌ها در همان شبکه یا دستگاه‌های دیگر (مانند ماکروویو و کنترل از راه دور) باشد اما تداخل عمدی معمولاً توسط یک مهاجم که قصد دارد ارتباطات در شبکه را قطع کند و یا مانع ارتباطات شود، انجام می‌شود. مختل کردن می‌تواند در سطوح مختلف، از جلوگیری از انتقال تا انتقال بسته‌های تحریف‌شده در ارتباطات رادیویی انجام شود (Grover et al., 2014).

برای درک بهتر چگونگی حمله یک جمر به شبکه‌های بی‌سیم و نحوه جلوگیری از مختل شدن برای دستیابی به ارتباطات کارآمد، از سه جنبه‌ی مختلف مختل کردن شبکه‌های بی‌سیم مورد بررسی قرار می‌گیرد.

یک شبکه از طریق روش‌های مختلف توسط جمرها مختل می‌شود و برای جلوگیری از مختل شدن شبکه‌ها، مهم است بدانید چگونه آن جمر کار می‌کند. بنابراین در مورد جزئیات انواع مختلف جمرها بحث خواهد شد.

به عنوان مثال جمر غیر واکنشی، واکنشی و همچنین در مورد قرار دادن مطلوب جمرها در شبکه به‌منظور دستیابی به بهترین حالت تداخل در شبکه نیز بررسی‌هایی انجام خواهد شد. اگرچه جمینگ برای شبکه معمولاً یک تهدید بحرانی محسوب می‌شود اما در برخی موارد می‌تواند مفید هم باشد به‌طور مثال در سیستم‌های نظامی برای جلوگیری از استراق سمع، جهت حفظ اطلاعاتشان می‌توانند از آن استفاده کنند (Ma et al., 2023). در این بخش، ابتدا از دیدگاه یک مهاجم، انواع مختلف جمرها بررسی می‌شوند (Pelechrinis et al., 2010) و در نهایت از دیدگاه امنیت اطلاعات، تکنیک‌های مقابله با جمر تجزیه و تحلیل می‌شود.

### ۳-۱- انواع جمر

جمرها گره‌های بی‌سیم مخرب هستند که توسط یک مهاجم کاشته می‌شوند تا دخالت عمدی در یک شبکه بی‌سیم ایجاد کنند. بسته به استراتژی حمله، یک جمر می‌تواند ویژگی‌های یکسان یا متفاوت از گره‌های مشروع در شبکه‌ای که به آن‌ها حمله می‌کند را داشته باشد. اثر مختل کردن یک جمر بستگی به قدرت فرستنده رادیویی، موقعیت و نفوذ آن در شبکه دارد. به جمر ممکن است یک شبکه را به شیوه‌های مختلف متوقف کند. جمینگ می‌تواند به صورت مقدماتی یا پیشرفته باشد برای جمرهای مقدماتی ما آن‌ها رو به دو زیرگروه تقسیم می‌کنیم: غیر واکنشی و واکنشی. آن‌هایی که پیشرفته‌اند نیز به دو نوع

خرابی‌های ارتباطات رادیویی تأخیر در انتقال ایجاد می‌کند که منجر به تأخیر و ضایع کردن بسته اطلاعاتی می‌شود، بنابراین عدم موفقیت در ارتباطات رادیویی برای عملکرد یک سیستم CBTC بسیار حیاتی است. به همین علت سیستم CBTC به‌طور معمول یک محدوده محافظتی ثابت را برای محاسبه فاصله ترمزی ایمن تخصیص می‌دهد. علاوه بر این، سیستم‌های CBTC به‌طور معمول یک روش تشخیص قطار را به‌عنوان جایگزین برای تعیین موقعیت مکانی در صورت قطع ارتباطات رادیویی و همچنین برای قطارهای غیر CBTC که هم‌زمان با قطارهای CBTC کار می‌کنند، استفاده می‌کنند (Pascoe et al., 2009)، که یکی از الزامات استاندارد IEEE CBTC می‌باشد. یک مثال از سیستم‌های CBTC قطار S کپنهاگ است که در آن از محورشمار به‌عنوان جایگزین استفاده می‌شود. مقالات (Bu et al., 2014)، (Zhu et al., 2012)، (Nguyen et al., 2016) این مسائل را مورد بررسی قرار می‌دهند و روش‌های بهبود عملکرد را مورد بحث و بررسی قرار می‌دهند. مقاله (Wang et al., 2015) یک روش کنترل را ارائه می‌دهد که اثرات شکست‌های ارتباطی را بر عملکرد کنترل قطار توضیح می‌دهد و در نتیجه شکاف اطلاعاتی (تفاوت بین آنچه دریافت شده و وضعیت واقعی قطار جلویی) را توصیف می‌کند. مقاله (Sun et al., 2015) پارامترهای لایه دسترسی به رسانه (MAC) با توجه به استاندارد IEEE 802.11 را بهینه‌سازی می‌کند.

### ۳- جمینگ در شبکه‌های مخابراتی

به دلیل گسترش فناوری‌های بی‌سیم، اختلال در شبکه‌های بی‌سیم با توجه به سهولت از بین بردن ارتباطات این شبکه‌ها، یک مشکل عمده تحقیقاتی شده است. برای درک بهتر این مشکل، باید در مورد جزئیات و تکنیک‌های مختلف برای مختل کردن و جلوگیری از اختلال در شبکه‌های بی‌سیم بحث و تجزیه و تحلیل شود. برای رفع این مشکل مکانیزه‌های مختلف مختل کردن، تشخیص و اقدامات مقابله با آن مورد مطالعه قرار می‌گیرد (Wood et al., 2007).

جمینگ با تداخل‌های شبکه معمولی متفاوت است، زیرا جمینگ استفاده عمدی از سیگنال‌های بی‌سیم برای از بین بردن ارتباطات است درحالی‌که تداخل به قطعی ناخواسته اشاره دارد. تداخل غیرعمدی ممکن است ناشی از ارتباطات بی‌سیم بین

حداکثر توان نفوذ را بدون در نظر گرفتن مصرف انرژی صرف کنند. حتی زمانی که جمر یک کانال را در یک زمان مسدود می‌کند، به آن کانال ثابت نمی‌شود و می‌تواند کانال‌های خود را با توجه به قابلیت‌های خاص خود تغییر دهد.

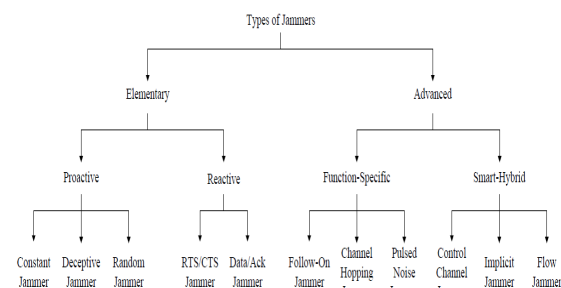
### ۳-۱-۴- جمر ترکیبی هوشمند

به علت قدرت و اختلال مؤثر، آن‌ها را هوشمند می‌نامیم. هدف اصلی این جمر، افزایش اثرات جمینگ در شبکه‌ای است که قصد خراب کردن آن را دارد. علاوه بر این، آن‌ها با ذخیره انرژی از خودشان مراقبت می‌کنند و هر یک از این نوع جمرها را می‌توان هم غیر واکنشی و هم واکنشی اجرا کرد از این رو به آن‌ها ترکیبی گفته می‌شود.

### ۳-۲- روش‌های شناسایی جمر و مقابله با آن

از آنجایی که جمینگ یک حمله بسیار آسیب‌زننده است، تشخیص عامل اثر و مقابله با آن بسیار مهم است. این بخش برخی از این فن‌ها را از لحاظ مدل سیستم، حمله و اندازه‌گیری تشریح می‌کند. در این بخش، ما در مورد طرح‌های موجود برای تشخیص و مقابله با جمر مقدماتی و پیشرفته بحث می‌کنیم. جمر مقدماتی شامل جمرهای غیر واکنشی و واکنشی است. در جمر غیر واکنشی، جمر پهنای باند را شکاف می‌دهد یا خفه می‌کند تا فرستنده عاجز از انتقال باشد. بنابراین، آستانه سنجش حامل را می‌توان برای تشخیص نوع جمر استفاده کرد. هنگامی که جمر تشخیص داده می‌شود، نودها در شبکه می‌توانند منطقه آسیب‌دیده را شناسایی و ترافیک را مجدداً مسیریابی کنند، کانال را تغییر دهند یا عقب‌نشینی مکانی را برای مقابله با این اقدام انجام دهند. تداخل واکنشی که در فرستنده انجام می‌شود می‌تواند با بررسی قدرت سیگنال دریافتی، نسبت سیگنال به نویز و نسبت تحویل بسته‌بندی شناسایی شود. این و بسیاری از معیارهای دیگر برای تشخیص و مقابله با تداخل ابتدایی استفاده شده است.

زیرگروه تقسیم می‌شوند. عملکرد خاص و هوشمند ترکیبی که نشانگر جزئیات طبقه‌بندی دقیق جمرهای مختلف است را می‌توان در شکل (۲) یافت (Grover et al., 2014).



شکل ۲. انواع جمر

### ۳-۱-۱- جمر غیر واکنشی

در این نوع جمر عملیات اختلال رادیویی بر اساس استراتژی از قبل تعریف شده ارسال می‌کند. به عبارت دیگر در این نوع، جمر هیچ اطلاعاتی از کانال هدف ندارد و فقط بر اساس برنامه‌ریزی از پیش تعریف شده عمل می‌کند.

### ۳-۲-۱- جمر واکنشی

در این عملیات اختلال رادیویی بر اساس عملکرد شبکه انجام می‌شود. جمر زمانی که فعالیتی بر روی کانال مورد نظر حس کند، سیگنال اختلال را ارسال می‌کند (Pelechrinis et al., 2010). در این نوع از جمر عملیات مختل شدن شامل دو بخش است که عبارت‌اند از: بخش حس کانال هدف که به عنوان عملیات پیش اختلال در نظر گرفته می‌شود. در این مرحله کانال مورد نظر حس و انتخاب می‌شود. بخش مختل کردن که در این بخش پس از تعیین کانال هدف سیگنال جمینگ بر روی کانال مدنظر ارسال می‌شود.

### ۳-۱-۳- جمر عملکرد خاص

با داشتن یک تابع از پیش تعیین شده اجرا می‌شود. علاوه بر فعال بودن یا واکنش‌پذیری، آن‌ها می‌توانند روی یک کانال کار کنند تا انرژی را ذخیره کنند یا کانال‌های چندگانه را حفظ کنند و

#### ۴- مدل سازی حرکت قطار

می‌شوند و به‌طور بهینه با حداقل زمان مقایسه می‌شود تا کل زمان سفر را به حداقل برسد. معادلات (۱) برای محاسبه مدت زمان فازهای شتاب‌گیری و سرعت ثابت، خلاصی و نیز ترمزگیری قطارها  $(T_1, T_2, T_3)$  و  $(T_4)$ ، در فاز برنامه‌ریزی حرکت قطار و با هدف کمینه کردن کل زمان حرکت قطار ارائه می‌شود.

$$\left\{ \begin{array}{l} T_1 + T_2 + T_3 + T_4 \\ V_1 = V_{init} + \alpha T_1 \\ V_1 = V_{init} + \alpha T_1 \\ V_2 = V_1 + a_{fr} T_3 \\ V_2 + \beta_{ser} T_4 = 0 \\ S_1 = V_{init} T_1 + 0.5 \alpha T_1^2 \\ S_2 = V_1 T_2 \\ S_1 = V_{init} T_1 + 0.5 \alpha T_1^2 \\ S_3 = V_1 T_3 + 0.5 a_{fr} T_3^2 \\ S_4 = V_2 T_4 + 0.5 \beta_{ser} T_4^2 \\ S_1 + S_2 + S_3 + S_4 = S_{remain} \\ 0 < V_2 < V_1 < V_{max} \\ T_1, T_2, T_3, T_4 > 0 \\ \text{Input: } V_{init}, S_{remain}, \alpha, \beta_{ser}, a_{fr} \\ \text{Output: } T_1, T_2, T_3, T_4, V_1, V_2 \end{array} \right. \quad (1)$$

در این معادلات  $V_{init}$  سرعت اولیه می‌باشد و  $V_1$  سرعت ثابت و  $V_2$  سرعت فاز خلاصی می‌باشد و  $S_1, S_2, S_3, S_4$  مسافت‌هایی هستند که طی فازهای مربوطه طی شده‌اند، معادلات محاسبه سرعت و مسافت طی شده در طی این مراحل بر طبق قوانین حرکت نیوتن می‌باشد. معادله چهارم از معادلات (۱) دلالت بر این دارد که قطار هنگام رسیدن به ایستگاه باید بایستد، هنگامی که قطار سفر خود را آغاز می‌کند، سرعت اولیه  $V_{init} = 0$ ،  $S_{remain} = S_{total}$ ، که مجموع فاصله بین دو ایستگاه متوالی است.

توجه کنید که این مدل یک سری جزئیات ظریف را نادیده گرفته است مثلاً شیب یا پیچ مسیر و سریع‌السير بودن قطار که می‌توان به آسانی در آن گنجانده پروفیل شتاب برای طول مسیر حرکت قطار با  $aplan(\tau)$  نشان داده می‌شود (رابطه (۲)).

در هنگام محاسبه‌ی پروفیل سرعت حرکت قطار، شاخص زمان  $(t=0)$  در ابتدای سفر وجود دارد، در موقعیت‌های ویژه قطار

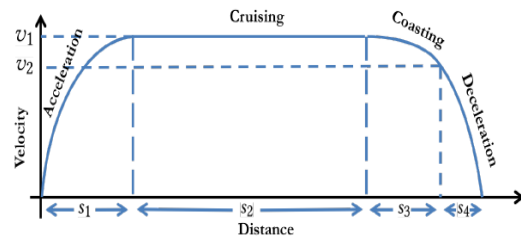
در این بخش یک مدل حرکتی برای قطار طراحی می‌شود و دو فاز برنامه‌ریزی و عملیاتی برای طراحی در نظر گرفته می‌شود. در فاز برنامه‌ریزی یک مسیر هدایت یعنی پروفیل شتاب‌گیری و ترمزگیری و سرعت را قطارها محاسبه می‌کنند که قصد دارند در طول سفر از آن پیروی کنند که پروفیل طراحی شده در شکل (۳) قابل مشاهده است.

در فاز عملیاتی قطارها آن پروفیل طراحی شده را دنبال می‌کنند تا زمانی که یک رویداد غیرطبیعی رخ دهد.

به عنوان مثال، فرض کنید قطار پشتی تا حد امکان به قطار جلویی نزدیک شود یا ارتباطات قطار برای مدت طولانی قطع شود، در این برنامه یک اقدام اصلاحی کوتاه‌مدت انجام می‌شود و پس از آن قطارهای باقی‌مانده مسیر را بر طبق همان پروفیل طراحی‌شده‌ی اولیه حرکت می‌کنند که جزئیات آن در ادامه ارائه خواهد شد.

#### ۴-۱- فاز برنامه‌ریزی

بر اساس (Zhao et al., 2015)، (Wang et al., 2013)، (Zhu et al., 2013)، پروفیل سرعت حرکت قطار به چهار فاز (شتاب‌گیری، سرعت ثابت، خلاصی، ترمزگیری) تقسیم می‌شود. در این جا نیز طبق شکل (۳) فاز اول شتاب‌گیری با  $\alpha$  مشخص می‌شود، فاز دوم قطار سرعت ثابت خود را حفظ می‌کند، فاز سوم قطار هیچ نیروی ترمزی یا ترمز اضطراری را اعمال نمی‌کند، بنابراین کاهش سرعت فقط به علت اصطکاک است که آن را با  $a_{fr}$  نمایش می‌دهند و فاز آخر که ترمزگیری قطار می‌باشد با  $\beta_{ser}$  نمایش داده می‌شود.



شکل ۳. پروفیل سرعت حرکت قطار

مقدار زمان چهار فاز شتاب‌گیری، سرعت ثابت، خلاصی و ترمزگیری قطار به ترتیب با  $T_1, T_2, T_3$  و  $T_4$  نمایش داده

قطارها به طور خودکار به حالت امن برمی گردند و این تضمینی است برای اینکه قطارها باهم برخورد نکنند. در این مقاله فرض می شود که سیگنالینگ *Fall Back* با سیگنالینگ بلاک ثابت مطابقت دارد. در سیستم سیگنالینگ بلاک ثابت، مسیر به بلاک های از پیش تعریف شده تقسیم می شود و قطارها از طریق مدار راه های کنار خط بلاک اشغال شده توسط قطار را تشخیص می دهند. اگر قطار در هر نقطه از بلاک حضور داشته باشد تصور می شود کل بلاک اشغال است علاوه بر این قطار بعدی اجازه ورود به بلاک جلویی را ندارد مگر اینکه فاصله قطارها از مقدار آستانه تعریف شده توسط اپراتور بیشتر باشد. این بلاک ها را با  $i=1,2,\dots$  فهرست می کنیم.  $B_f(t)$  و  $B_l(t)$  شاخص های بلاک های اشغال شده توسط قطارهای جلویی و عقبی را به ترتیب در هر زمان نشان می دهند. فاصله نقطه شروع بلاک  $i$  از مبدأ توسط  $d_i^s$  مشخص می شود. برای ایمنی، قطارها باید با حداقل تعداد بلاک از هم جدا شوند که توسط  $B_{th}$  مشخص شده است.

$$\text{Input} : t, v_1(t), s_1(t), v_f(t), s_f(t). \quad (4)$$

$$\text{Output} : H(t).$$

$$H(t) = 0, \tilde{v}_f = v_f(t), \tilde{v}_l = v_l(t), s_f = \tilde{s}_f(t). \text{ while } \tilde{v}_f \geq 0 \text{ do}$$

$$\tilde{s}_l \leftarrow \tilde{v}_l \Delta t + \frac{1}{2} \beta_{emrg} (\Delta t)^2, \tilde{s}_f \leftarrow \tilde{v}_f \Delta t + \frac{1}{2} \beta_{ser} (\Delta t)^2$$

$$\tilde{v}_l \leftarrow \max(\tilde{v}_l + \beta_{emrg} \Delta t, 0), \tilde{v}_f \leftarrow \tilde{v}_f + \beta_{ser} \Delta t$$

$$H(t) \leftarrow \max(\tilde{s}_f - \tilde{s}_l, H(t)).$$

end

#### ۴-۳- حرکت قطار در طول مرحله عملیاتی

الگوریتم دوم مدل حرکتی قطار به صورت (۵) تعیین می شود. حرکت قطار در الگوریتم دو به طور کامل شرح داده شده است. قبل از توصیف الگوریتم، برخی از نمادهای مورد استفاده در الگوریتم معرفی می شود. زمان با  $t$  مشخص شده است. در هر زمان  $pkt\_rec$  یک متغیر باینری را نشان می دهد که وضعیت ارتباطات را در آن بازه ی زمانی نشان می دهد، یعنی اگر ارتباطات برقرار باشد  $pkt\_rec$  مقدار یک را می گیرد و در صورت قطع ارتباطات مقدار صفر را نشان می دهد. متغیر  $pkt\_loss\_counter$  تعداد از دست دادن ارتباطات متوالی را شمارش می کند. علاوه بر این، ما  $Fixed\_Blk$  را با یک متغیر باینری نشان می دهیم که نحوه عملکرد قطار را مشخص می کند

می تواند با اعمال ترمز اضطراری یا همان  $\beta_{emrg}$ ، بایستد (جایی که  $\beta_{emrg} > \beta_{ser}$  باشد).

$$aplan(\tau) = \begin{cases} \alpha, t \leq \tau \leq t + T_1 \\ 0, t + T_1 < \tau \leq t + T_1 + T_2, \\ a_{ff}, t + T_1 + T_2 < \tau \leq t + T_1 + T_2 + T_3, \\ \beta_{ser}, t + T_1 + T_2 + T_3 < \tau \leq t + T_1 + T_2 + T_3 + T_4 \end{cases} \quad (2)$$

#### ۴-۲- فاز عملیاتی

حرکت قطار را در فاز عملیاتی توصیف می کنیم  $v_1(t), v_f(t), s_1(t), s_f(t), a_l(t), a_f(t)$  شتاب، موقعیت و سرعت قطار جلویی و پشتی را نسبت به مبدأ نشان می دهند. برای سادگی فرض می کنیم قطارها تصمیمات عملیاتی (شتابگیری، سرعت ثابت، خلاصی، ترمزگیری) در بازه های زمانی گسسته، فاصله زمانی بین تصمیمات است. موقعیت و سرعت قطار بر اساس معادلات (۳) به دست می آید.

$$v_i((n+1)\Delta t) = v_i(n\Delta t) + a_i(n\Delta t)\Delta t \quad (3)$$

$$s_i((n+1)\Delta t) = s_i(n\Delta t) + v_i(n\Delta t)\Delta t + \frac{1}{2} a_i(n\Delta t)(\Delta t)^2$$

تصمیمات عملکرد قطار فوق الذکر بستگی به حالت سیگنالینگ قطار دارد که در ادامه توضیح داده می شود. قطارهای CBTC در شرایط عادی از حالت سیگنالینگ بلاک متحرک پیروی می کنند که در آن قطار پشتی هدوی را هر لحظه بر اساس وضعیت حرکت قطار جلویی محاسبه می کند و بر این اساس سرعت خود را تنظیم می کند.  $H(t)$  حداقل فاصله بین دو قطار برای جلوگیری از تصادف است. اگر فاصله بین دو قطار از حداقل فاصله مشخص شده  $H(t)$  کم تر شود قطار پشتی ترمز اضطراری را اعمال می کند. شتاب و سرعت و موقعیت قطار جلویی که با  $s_1(t), v_1(t), a_1(t)$  نشان داده می شود هر لحظه از طریق تجهیزات کنار خط به قطار پشتی اطلاع داده می شود.

بر اساس این اطلاعات قطار پشتی هدوی مناسب را که با  $H(t)$  نشان داده می شود محاسبه می کند. الگوریتم اول مدل حرکتی قطار را می توان به صورت (۴) نوشت. در الگوریتم ارائه شده، در مراحل ۴ تا ۶ این اطمینان را به ما می دهد که اگر قطار جلویی از ترمز اضطراری استفاده کند، قطار پشتی فاصله کافی جهت متوقف کردن قطار و عدم تصادف با قطار جلویی را دارد. برای جبران از دست دادن ارتباطات، اپراتورها اخیراً از حالت سیگنالینگ *Fall Back* استفاده می کنند که در آن

را از دست می‌دهیم بیشتر از  $N$  باشد،  $N$  از قبل توسط اپراتور سیستم تعریف شده است) بلافاصله قطار به حالت بلاک ثابت تغییر حالت می‌دهد. وقتی در حالت بلاک متحرک هستیم قطار پشتی مقدار هدوی مکانی را طبق الگوریتم ۱ محاسبه می‌کند و در خط ۱۵ برنامه بررسی می‌کند که فاصله بین قطارها بیشتر از مقدار هدوی مکانی محاسبه‌شده هست یا خیر. در صورت صحت طبق خط ۱۷ برنامه حرکت خود را مطابق مسیر پروفیل سرعت از پیش برنامه‌ریزی‌شده ادامه می‌دهد؛ اما اگر قطارها نزدیک‌تر از مقدار هدوی محاسبه‌شده نسبت به هم بودند در این حالت نیز بلافاصله به حالت بلاک ثابت (خط ۲۰ تا ۲۴) تغییر حالت می‌دهد. فرض می‌کنیم هر بار که قطار از حالت بلاک متحرک به حالت بلاک ثابت تغییر وضعیت دهد تنها فقط به مدت  $T_{FB}^{MAX}$  زمان دارد تا قبل از بازگشت به حالت بلاک متحرک اطمینان حاصل کند که فاصله بین قطارها به اندازه کافی زیاد شده است.

#### مدل‌سازی کانال ارتباطی بی‌سیم

امروزه قطارها بیشتر از طریق ارتباطات بی‌سیم کار می‌کنند و برخلاف سایر سیستم‌های مخابراتی، در سیستم‌های ریلی تجهیزات کنار خط و قطار از نظر فیزیکی بسیار به هم نزدیک هستند و این موضوع باعث می‌شود یک فضای خوبی برای ارتباط‌گیری از طریق موج‌بر نشت ایجاد شود به این ترتیب اول کارهای قبلی که در زمینه ی موج‌بر نشتی در سیستم‌های ریلی صورت گرفته مورد مطالعه قرار داد و بر اساس آن مطالعات یک مدلی که افت سیگنال انتشار موج داخل موج بر را توصیف کند ارائه می‌شود و در مدل ارائه شده اثرات جمر بررسی می‌شود. قطارهایی که در حال حرکت هستند و با ارتباطات بی‌سیم باهم مرتبط می‌شوند و در نهایت با مرکز کنترل، ایستگاه و قطار ارتباط برقرار می‌کنند؛ یک شکاف هوایی بین قطارهای در حال حرکت و بقیه‌ی زیرساخت‌ها (تجهیزات کنار خط، مرکز کنترل، ایستگاه) وجود دارد. این فضای خالی بین قطار و ایستگاه و مسافران نیز مشترک است و برای عبور ارتباطات از شکاف هوایی خیلی از سیستم‌های قطار تکنولوژی موج‌بر نشت را استفاده می‌کنند که سخت‌افزار موج‌بر را به موازات مسیرهای راه‌آهن نصب می‌کنند بطوریکه موج‌بر همیشه در نزدیکی آنتن‌هایی که بر روی قطار نصب هستند، قرار دارد. جمینگ یک نگرانی گسترده برای دستگاه‌های بی‌سیم است و به‌خوبی

یعنی یک نشان می‌دهد که قطار در حالت بلاک ثابت کار می‌کند و صفر نشان می‌دهد که قطار در حالت بلاک متحرک کار می‌کند.

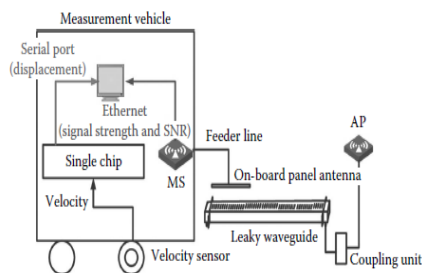
```

(۵)
set t = 0
compute  $A_{plan}(t)$ 
while do  $s_f(t) < s_{tot}$ 
if  $pkt\_rec = 1$  then
set  $pkt\_loss\_counter = 0$ 
 $\hat{s}_l(t) = s_l(t), \hat{v}_l(t) = v_l(t)$ .
else
 $pkt\_loss\_counter = pkt\_loss\_counter + 1$ 
if  $Fixed\_Blk = 0 \& pkt\_loss\_counter = N$ 
 $Fixed\_Blk = 1$ 
 $T_{FB} = T_{FB}^{max}$ 
end
end
if  $Fixed\_Blk = 0$  then
compute  $H(t)$ 
else
set  $a_f(t) = A_{plan}(t)$ 
compute  $v(t + \Delta t)$  and  $s(t + \Delta t)$ 
else
set  $Fixed\_Blk = 1$ 
perform fixed block update
set  $T_{FB} = T_{FB}^{max} - 1$ 
end
else
perform fixed block update
 $T_{FB} \leftarrow T_{FB} - 1$ 
if  $T_{FB} = 0$  Then
set  $Fixed\_Blk = 0$ 
update  $A_{plan}(t)$ 
end
end
set  $t \leftarrow t + \Delta t$ 
end

```

با توصیف خطوط ۴ تا ۱۲ از الگوریتم دو شروع می‌کنیم. در طی هر اسلات زمانی اگر ارتباطات قطار موفقیت‌آمیز باشد. قطار پشتی، اطلاعات جدید را دریافت و به روز رسانی می‌کند. در صورتی که خطای ارتباطاتی رخ دهد همان آخرین اطلاعات دریافت شده است. اگر تعداد دفعات متوالی که داده‌های خود

تجهیزات رادیویی روی قطار را نشان می‌دهد.



شکل ۴. ساختار انتقال اطلاعات موجبر نشت

ساختار موجبر شاید برای ارتباط طولی بین ایستگاه‌ها کافی باشد اما برای ارتباطات بین قطارها باید سطح ارتباطات در خارج از موج بر گسترش یابد و همچنین برای ارتباطات بین تجهیزات کنار خط و قطار نیز به همین شکل مستلزم گسترش ارتباطات خارج از فضای موجبر می‌باشد. بنابراین در سیستم‌های ریلی شکاف‌هایی بر روی سطوح موج بر نشت وارد می‌کنند که از این به بعد موج‌ها نه تنها در داخل فضای موجبر بلکه به بیرون از فضای موجبر نیز هدایت می‌شوند. ساختار موجبر به‌طور موازی و نزدیک مسیره‌های راه‌آهن ساخته شده است.

به دلیل ماهیت نشتی، ارتباطات موجبر نشت کننده، تکرارکننده‌های بی‌سیم را هنگام پشتیبانی از مسافت‌های طولانی‌تر معرفی می‌کند. برای جبران تضعیف سیگنال، تکرار کننده سیگنال را دریافت و تقویت می‌کند و دوباره به ادامه مسیر، سیگنال تقویت شده را ارسال می‌کند. سیگنال‌های نشت یافته در مقایسه با سیگنال‌های داخل محیط موجبر نشت نسبتاً سریع تضعیف می‌شوند زیرا دیگر یک وسیله فیزیکی برای هدایت انتشار آن‌ها در محیط هوای آزاد وجود ندارد بنابراین ارتباطات قطار به‌طور گسترده‌ای از زیرساخت موجبر نشت برای ارسال اطلاعات استفاده می‌کند و عملکرد و مزایای آن در مقالات (Heddebaut et al., 1990)، (Heddebaut, 2008)، (Kawakami et al., 1964)، (Wang et al., 2013) مورد بررسی قرار گرفته است.

در سیستم موج بر نشت، سیگنال نه تنها درون موجبر باقی می‌ماند بلکه در خارج از موجبر نیز نشت می‌کند تا به آنتن قطار برسد. همان‌طور که در شکل (۵) نشان داده شده است، مسیر انتشار موجبر نشتی شامل موارد زیر است.

بررسی شده است (Basar et al., 1983)، (Vo-Huu et al., 2016)، (Strasser et al., 2008). راه‌حل‌هایی از جمله فناوری طیف گسترده برای افزایش مقاومت در برابر جرم‌ها پیشنهاد شده است. به عنوان مثال (Strasser et al., 2008)، (Pickholtz et al., 1982)، (Chang et al., 2012)، (Alnifie et al., 2007) تحقیق و پژوهش کرده‌اند اما کارهای موجود در این زمینه به‌طور عمده بر روی اختلال در فضای آزاد متمرکز شده‌اند. برای تکمیل این تحقیقات در این مقاله زمینه اختلال در فضای موجبر نشت در محیط ارتباطات قطار مطالعه و پژوهش شده است.

همان‌طور که از اسم آن مشخص است تکنولوژی موجبر، موج را هدایت می‌کند و با محدود کردن انتشار آن به یک بعد (برخلاف انتشار موج در سه بعد) قدرت سیگنال را تا مسافت‌های طولانی حفظ می‌کند، همچنین مسیر بین دو کاربر ارتباطی، ثابت است و از این رو اثر محوشدگی را هم به حداقل می‌رساند و انتشار یکنواختی در عبور از کانال دارد، به‌طور مثال هیچ جابجایی بین کاربران وجود ندارد. برای ارسال اطلاعات از طریق موج آزاد، اطلاعات دیجیتالی از سال شده تبدیل به امواج الکترومغناطیسی می‌شوند و از طریق آنتن‌ها منتشر می‌شوند. جایی که سیگنال الکترومغناطیسی آزادانه از فضای هوای آزاد عبور می‌کند، اولاً به علت توسعه فرکانس رادیویی سیگنال به‌طور طبیعی تضعیف می‌شود و دوماً اینکه یک فرستنده رادیویی سیگنال الکترومغناطیسی را بدون توجه به محیط اطرافش ارسال می‌کند. برای محدود کردن این دو ویژگی در موج آزاد موجبر نشت طراحی شده است. به‌طور خلاصه، ارتباطات قطار برای استفاده از این زیرساخت به دو دلیل ایده آل است اول به علت اینکه مسیر حرکت قطار از پیش تعریف شده است و محدود به مسیره‌های ریلی است و زیرساخت ارتباطات نشت نیز نزدیک به مسیره‌های ریلی است، این محدودیت انتشار سیگنال که توسط زیرساخت‌های نشتی وضع شده است برای ارتباطات قطار مناسب است زیرا قطار هرگز از ریل دور نمی‌شود و دوماً این محیط انتشار سیگنال را در مسیر طولانی‌تری نسبت به محیط موج آزاد پشتیبانی می‌کند و چون قطار مسیر طولانی را طی می‌کند از این رو باز موجبر نشت برای آن مناسب‌تر است. ساختار موجبر نشت به‌طور معمول یک سازه فلزی پرشده از هوا است که بین دو کاربر قرار گرفته است. شکل (۴) ارتباط بین موجبر نشت و

موج‌بر تمرکز ما روی اتلاف طولی است که برحسب دسی‌بل و خطی می‌باشد (معادله (۸)).

$$PL = C_{cp \ln g} + \alpha d_l \quad (۸)$$

در فضای آزاد برای ارسال اطلاعات از طریق موج آزاد، اطلاعات دیجیتالی ارسال شده تبدیل به امواج الکترومغناطیسی می‌شوند و از طریق آنتن‌ها منتشر می‌شوند. جایی که سیگنال الکترومغناطیسی آزادانه از فضای هوای آزاد عبور می‌کند، اولاً به علت توسعه فرکانس رادیویی سیگنال به‌طور طبیعی تضعیف می‌شود و دو ما اینکه یک فرستنده رادیویی سیگنال الکترومغناطیسی را بدون توجه به محیط اطرافش ارسال می‌کند. برای محدود کردن این دو ویژگی در موج آزاد موج‌بر نشت طراحی و ارائه شده است.

معادله‌ی مربوط به موج آزاد (۹) را در نظر بگیرید.

$$PL_r = PL_{0,r} + 10\gamma \log_{10}(d_r) + X_r \quad (۹)$$

که در این معادله،  $PL_{0,r}$  نشت از طریق شکاف است و  $X_r$  محو شدن موج آزاد پس از نشت است،  $\gamma$  نیز ضریب افت سیگنال نامیده می‌شود.

حال، معادله (۱۰) را می‌توان بر اساس معادله (۹) نوشت.

$$PL = PL_l + PL_{rptr} + PL_r$$

$$= C_{cp \ln g} + \alpha d_l - C_{rptr} \left[ \frac{d_l}{d_{rptr}} \right] \quad (۱۰)$$

$$+ PL_{0,r} + 10\gamma \log_{10}(d_r) + X_r$$

نسبت سیگنال به نویز یا همان  $SNR$  برای توصیف کیفیت کانال‌های بی‌سیم مورد استفاده قرار می‌گیرد و بر ظرفیت کانال تاثیرگذار است، که از یک مقدار به بالا یک ارتباط قابل اعتمادی برقرار می‌شود.

به طور مثال، قضیه شانون را در نظر بگیرید (رابطه (۱۱)).

$$R < B \log(1 + SNR) \quad (۱۱)$$

پروتکل ارتباطی، پهنای باند ( $B$ ) و نرخ ارسال بیت ( $R$ ) را می‌دهد و  $SNR$  با صرف نظر از نحوه‌ی پردازش سیگنال مشخص می‌کند که امکان برقراری ارتباط موفق وجود دارد یا خیر، بنابراین هدف جمر پایین آوردن  $SNR$  با تزریق نویز یا همان تداخل است که در این صورت می‌شود  $SINR$ ، یعنی نسبت سیگنال به نویز و تداخل است. اگر جمر  $SINR$  را کاهش داد به طوری که ظرفیت کم‌تر از نرخ ارسال داده  $R$  شود، رابطه (۱۲) برقرار خواهد بود.

$$R > B \log(1 + SNR) \quad (۱۲)$$

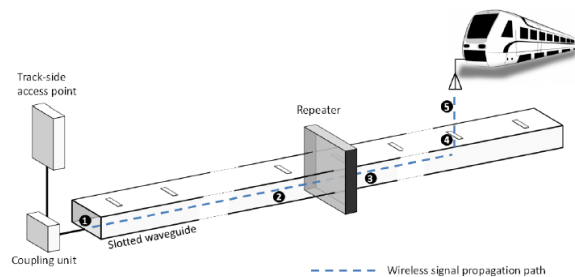
نقطه دسترسی کنار خط (که از طریق ارتباطات سیمی به بقیه زیرساخت‌ها متصل می‌شود)

انتشار سیگنال طولی در طول موج‌بر نشت

برخی از سیگنال‌ها از طریق اسلات‌های طراحی شده نشت می‌شوند.

برای جبران افت سیگنال طولی، تکرارکننده‌های بی‌سیم سیگنال‌ها را تقویت کرده و دوباره ارسال می‌کنند.

انتشار و نشت سیگنال از طریق موج آزاد جهت رسیدن به آنتن تعبیه شده بر روی قطارها



شکل ۵. مسیر انتشار سیگنال در یک موج‌بر نشت

بنابراین، مسیر شامل دو قسمت درونی و بیرونی است، درون موج‌بر در جهت طولی و خارج از موج‌بر در جهت شعاعی که افت سیگنال و فاصله طی شده در جهت طولی با  $PL_L$  و  $d_l$  نمایش داده می‌شود و همچنین در آخر افت سیگنال موج‌بر  $PL$  بر اساس معادله (۶) تعیین می‌گردد.

$$PL = PL_L + PL_{rptr} + PL_r \quad (۶)$$

با طراحی تقویت سیگنال به‌وسیله‌ی تکرارکننده،  $PL_{rptr}$  همیشه منفی است، نشانه منفی تعیین می‌کند که سیگنال به دلیل تکرار شونده تقویت می‌شود و بنابراین، افت سیگنال در مسیر منفی است.  $N_{rptr}$  تعداد تکرارکننده‌ها است که سیگنال از آن عبور می‌کند (معادلات (۷)).

$$\begin{cases} PL_{rptr} = -C_{rptr} N_{rptr} \\ PL_{rptr} = -C_{rptr} \left[ \frac{d_l}{d_{rptr}} \right] \end{cases} \quad (۷)$$

که  $[X]$  سقف مقدار  $X$  است (بزرگ‌ترین عدد صحیحی که از  $X$  بیشتر نباشد) و  $C_{rptr}$  و  $d_{rptr}$  بهره تقویت‌کننده تکرارکننده و فاصله بین تکرارکننده‌ها هستند که  $C_{rptr}$  نسبت قدرت خروجی تکرارکننده به ورودی تکرارکننده است. در سیستم

برخلاف مسیر تداخل جمر که  $PL_{J,R}$  داخل موجبر را تجربه می‌کند، سیگنال اصلی با اتصال سیمی به موجبر تزریق می‌شود و افت سیگنال آن بدین صورت است. پس از استقرار سیستم ارتباطی قدرت جمینگ نسبت به قدرت سیگنال اصلی بستگی به پارامترهای فاصله جمر از موجبر نشت ( $d_{J,wg}$ )، فاصله بین جمر و گیرنده نسبت به فاصله سیگنال اصلی به گیرنده ( $d_{J,R} - d_{S,R}$ ) و نیز تعداد دفعاتی که سیگنال مختل‌کننده با تکرارکننده‌های در طول مسیر نسبت به سیگنال اصلی با آن‌ها برخورد می‌کند، دارد (رابطه (۱۸)).

$$P_J - P_S > PL_{0,R} + 10\gamma \log_{10}(d_{J,wg}) + X_r + \alpha d_{J,R} - C_{rptr} \left[ \frac{d_{J,R}}{d_{rptr}} \right] + \overline{PL}_r + \tau - \left( C_{cp \ln g} + \alpha d_{S,R} - C_{rptr} \left[ \frac{d_{S,R}}{d_{rptr}} \right] + \overline{PL}_r \right) = -C_{cp \ln g} + PL_{0,R} + X_r + 10\gamma \log_{10}(d_{J,wg}) + \tau + \alpha (d_{J,R} - d_{S,R}) - C_{rptr} \left( \left[ \frac{d_{J,R}}{d_{rptr}} \right] - \left[ \frac{d_{S,R}}{d_{rptr}} \right] \right)$$

از آنجا که مسیر حرکت قطار از پیش تعریف شده است و محدود به مسیرهای ریلی است و زیر ساخت ارتباطات نشت نیز نزدیک به مسیرهای ریلی است، این محدودیت انتشار سیگنال که توسط زیر ساخت‌های نشتی وضع شده است برای ارتباطات قطار مناسب است زیرا قطار هرگز از ریل دور نمی‌شود و دوما محیط انتشار سیگنال را در مسیر طولانی‌تری نسبت به محیط موج آزاد پشتیبانی می‌کند. در این حالت، چون قطار مسیر طولانی را طی می‌کند از این رو باز موجبر نشت برای آن مناسب‌تر است اما از طرفی جمر با بهره‌گیری از ساختار موجبر نشت اثرات خودش را در محدوده‌ی بیشتری اعمال می‌کند و این فضای وابستگی به منبع اصلی جمینگ را از بین می‌برد.

### شبیه‌سازی و بررسی نتایج

در این بخش نتایج به دست آمده از این مقاله ارائه شده است. شبیه‌سازی‌ها در محیط متلب انجام شده است. حرکت دو قطار نسبت به هم در طول یک خط مترو شامل چندین ایستگاه در نظر گرفته شده است.

در نتیجه، جمر ارتباط را مختل کرده و  $SINR$  تا زمانی که کم‌تر از مقدار  $\tau$  شود، کاهش می‌یابد (رابطه (۱۳)).

$$\begin{cases} \tau' = 2^{\frac{R}{B}} - 1 \\ SINR < \tau' \end{cases} \quad (13)$$

با توجه به اینکه  $\tilde{P}'_S$  قدرت دریافتی است، رابطه (۱۴) برقرار خواهد بود.

$$SINR = \frac{P'_S}{P'_I + P'_N} < \frac{P'_S}{P'_I} < \tau' \quad (14)$$

مقدار توان جمر  $P'_J$  خیلی بیشتر از توان نویز  $P'_N$  است به همین علت از  $P'_N$  صرف‌نظر می‌کنیم و برحسب دسی‌بل به صورت روابط (۱۵) بازنویسی می‌کنیم.

$$\begin{cases} \tilde{P}_J - \tilde{P}_S > \tau \\ \tilde{P}_J = P_J - PL_{J,R} \\ \tilde{P}_S = P_S - PL_{S,R} \\ P - P > PL - PL + \tau \end{cases} \quad (15)$$

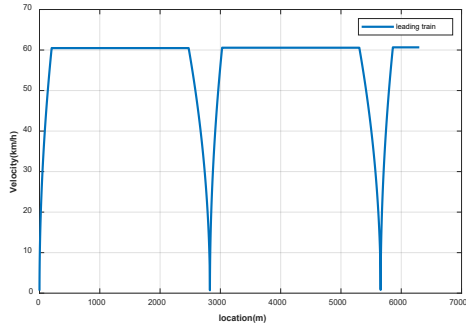
با  $PL_{S,R}$  و  $PL_{J,R}$  جزئیات بیشتر بررسی می‌کنیم، در ابتدا مؤلفه‌ی شعاعی افت سیگنال از موجبر نشت تا آنتن قطار  $PL_r$  بررسی می‌شود زیرا که بر  $PL_{S,R}$  و  $PL_{J,R}$  مؤثر است و در حین حرکت قطار مقدارش ثابت است.

هنگام استفاده از ارتباطات مبتنی بر موجبر نشت در تنظیمات کلی همان‌طور که در معادله ۳۲ مشاهده می‌شود  $PL_r$  به جهت شعاعی  $dr$  و محو شدن  $x_r$  بستگی دارد (معادله (۱۶)). از آنجایی که در سیستم‌های ریلی که موجبر نشت و مسیر حرکت قطار موازی هستند فاصله بین موجبر و گیرنده  $dr$  ثابت است و همچنین  $\sigma = 0$  در نتیجه  $x_r = 0$  است.

$$PL_r = PL_{0,r} + 10\gamma \log_{10}(dr) + x_r \quad (16)$$

$\overline{PL}_r$  مستقل از  $PL_r$  که وابسته به  $dr$  و  $x_r$  باشد، گرفته شده است.  $PL_{J,wg}$  معادل با افت سیگنال در مسیر جمر تا موجبر می‌باشد (روابط (۱۷)).

$$\begin{cases} PL_{J,wg} = PL_{0,r} + 10\gamma \log_{10}(d_{J,wg}) + X_r \\ PL_{J,R} = PL_{J,wg} + \alpha d_{J,R} - C_{rptr} \left[ \frac{d_{J,R}}{d_{rptr}} \right] + \overline{PL}_r \\ PL_{J,R} = PL_{0,r} + 10\gamma \log_{10}(d_{J,wg}) + X_r + \alpha d_{J,R} - C_{rptr} \left[ \frac{d_{J,R}}{d_{rptr}} \right] + \overline{PL}_r \\ PL_{S,R} = C_{cp \ln g} + \alpha d_{S,R} - C_{rptr} \left[ \frac{d_{S,R}}{d_{rptr}} \right] + \overline{PL}_r \end{cases}$$

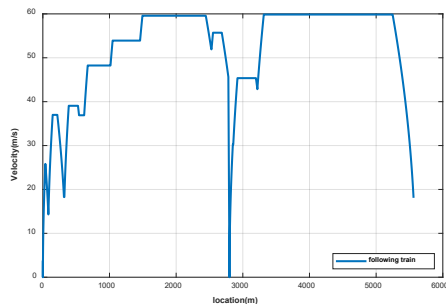


شکل ۶. پروفیل سرعت حرکت قطار جلویی بر حسب موقعیت

یک جمر در فاصله ۰/۲ کیلومتری از مبدأ فرض شده است و به طور مداوم سیگنال مختل کننده را در سراسر محیط شبیه سازی می فرستد، قطار جلویی طبق پروفیل حرکتی تعریف شده به مسیر خود ادامه می دهد.

این در حالی است که به وسیله ی جمر، ارتباطات مختل شده است و قطار پشتی سرعت خود را کم کرده و در نتیجه از حالت بلاک متحرک به حالت بلاک ثابت تغییر وضعیت می دهد تا این که در حالت ایمن تری قرار بگیرد.

در این مدت، اطلاعات مربوط به قطار جلویی، از طریق مدار راه های کنار خط دریافت می گردد و تا زمانی که بلاکی توسط قطاری اشغال باشد طبق برنامه وارد آن بلاک نمی شود (شکل (۷)).



شکل ۷. پروفیل سرعت حرکت قطار پشتی بر حسب مکان

همان طور که در قسمت قبل گفته شده مسافت هر بلاک ۴۰۰ متر است و پس از اینکه ارتباطات وصل گردد به حالت بلاک متحرک برگشته و همان طور که در بخش های قبلی گفته شد قطار نهایت ۳۰ ثانیه می تواند در حالت بلاک ثابت باقی بماند و وقتی به حالت بلاک متحرک بازگردد پروفیل سرعت جدید را با سرعت اولیه جدید و موقعیت جدید محاسبه می کند و به حرکت خود در بلاک متحرک ادامه می دهد (شکل (۸)).

هر قطار حرکت خود را از ایستگاه ۱ شروع می کند و هر دو قطار با فاصله اعزام ۹۰ ثانیه شروع به حرکت می کنند و برای دوره ای چند ثانیه ای در ایستگاه ها توقف می کنند.

### پارامترهای در نظر گرفته شده در این شبیه سازی

پارامترهای حرکت قطار شامل مقدار شتاب ترمزگیری  $\beta_{ser} = -0.4 m/s^2$ ، شتاب گیری  $\alpha = 0.7 m/s^2$ ، مقدار شتاب ترمز اضطراری  $\beta_{emrg} = -1 m/s^2$  و حداکثر سرعت قطار  $v_{max} = 60 km/h$  است. فاصله بین ایستگاه ها ۲٫۸ کیلومتر است. برای وضعیت بلاک ثابت، طول بلاک ۴۰۰ متر تنظیم می شود.

فاصله زمانی بین تصمیمات عملیاتی قطار برابر ۰/۲۵ ثانیه فرض شده است و همچنین فرض می شود که اگر قطع ارتباطات به مدت ۲ ثانیه به طول انجامد، قطار از حالت بلاک متحرک به حالت بلاک ثابت تغییر وضعیت دهد؛ بنابراین  $N = 2/\Delta t = 8$  است؛ یعنی اگر ۸ بار اعلام قطع ارتباطات داشته باشیم این تغییر وضعیت اتفاق می افتد و  $T_{FB}^{max}$  ماکزیمم زمانی است که قطار می تواند در وضعیت بلاک ثابت بماند که به مقدار ۳۰ ثانیه تنظیم شده است.

پارامترهای ارتباطی بی سیم هم با مقادیر زیر تنظیم شده اند. آستانه  $SINR$  برای ارتباط موفق  $\tau = 10 dB$  است. در ارتباطات موج آزاد، افت سیگنال مرجع  $\eta_0$  برابر  $40 dB$  است. پارامترهای شبیه سازی موج بر نشتی، بر اساس استانداردهای  $WR-430$  انتخاب شده است.

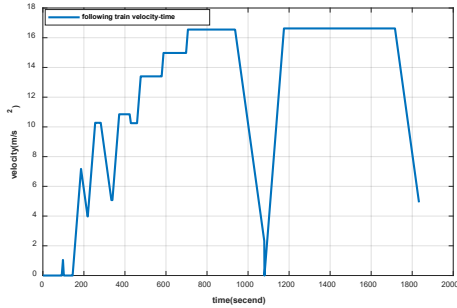
فاصله بین تکرار کننده  $d_{prr}$  برابر  $2/5$  کیلومتر تنظیم شده است. قدرت انتقال سیگنال مجاز  $p_s$  (dBm) و قدرت انتقال سیگنال جیمینگ  $p_r$  (dBm) نامیده می شود.

### بررسی حالت های مختلف در این شبیه سازی

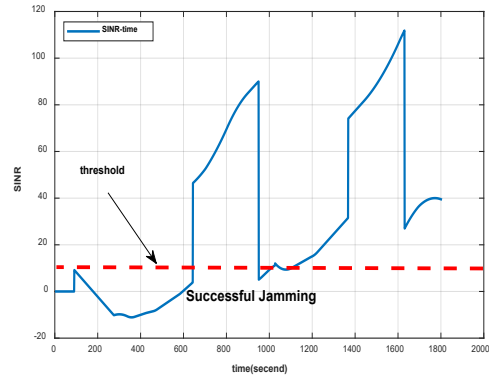
در این شبیه سازی هشت حالت مختلف جهت بررسی اثرات جمر و بررسی روش انتخاب شده برای مقابله با جمر مورد آزمایش قرار گرفته است.

#### حالت اول

در حالت اول یک جمر در موقعیت مشخص در نظر گرفته شده و محاسبه  $SINR$  در آن حالت انجام شده است (شکل (۶)).



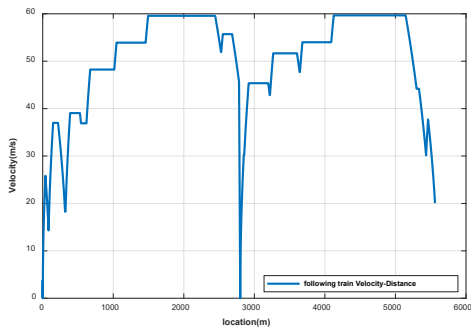
شکل ۱۰. نمودار پروفیل سرعت حرکت بر حسب زمان



شکل ۸. نمودار  $SNIR$  بر حسب زمان

### حالت سوم

در حالت سوم جمر اول در موقعیت مشخص و جمر دوم در موقعیت تصادفی در نظر گرفته می‌شود و بر تعداد مهاجم‌های خود افزوده و علاوه بر مهاجمی که در فاصله ۰/۲ کیلومتری از مبدأ قرار دارد، یک مهاجم دیگر در فاصله ۱ کیلومتری از مبدأ در نظر گرفته شده و به صورت مداوم سیگنال‌های مختل‌کننده از طریق این دو مهاجم انتشار می‌گردد. نتایج به دست آمده در شکل (۱۱) نشان داده شده است.



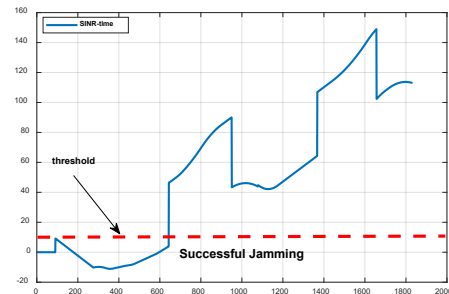
شکل ۱۱. نمودار پروفیل سرعت حرکت قطار بر حسب مکان

نتایج حاصل مربوط به اثرات تعداد جمرها بر مقدار  $SNIR$  و پروفیل حرکت قطار CBTC در شکل (۱۲) ارائه شده است. با اضافه کردن تعداد جمر، اثرات مخرب‌تری بر CBTC وارد شده و تعداد دفعاتی که قطار از حالت بلاک متحرک به بلاک ثابت تغییر حالت می‌دهد، بیشتر می‌شود. چرا که مقدار  $SNIR$  غالباً از مقدار آستانه خود که  $10\text{ dB}$  است کمتر می‌شود.

### حالت دوم

در حالت دوم به تعداد جمرها افزوده شده و دو جمر در موقعیت مشخص در نظر گرفته شده است و پس از آن اثر تعداد جمرها بر روی  $SNIR$  مشاهده می‌شود.

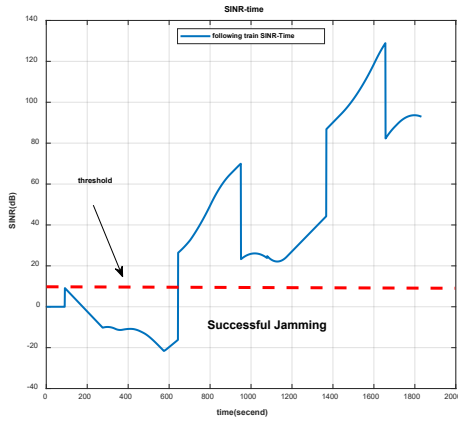
در این حالت با روش پرش فرکانسی طیف گسترده  $FHSS$  با مهاجمی که در فاصله ۰/۲ کیلومتری از مبدأ فرض شده بود و به صورت مداوم سیگنال جمینگ را در سراسر محیط می‌فرستاد، مقابله می‌کنیم و نتایج حاصل از این مقابله را می‌توان بر اساس شکل (۹) نمایش داد.



شکل ۹. نمودار  $SNIR$  بر حسب زمان

در این قسمت ما با روش پرش فرکانسی طیف گسترده اثر جمر را کم کرده و قدرت سیگنال مجاز نسبت به قدرت سیگنال مختل‌کننده افزایش می‌یابد.

بنابراین، مقدار  $SNIR$  از مقدار آستانه خود بیشتر شده و در نتیجه قطار کمتر به حالت بلاک ثابت انتقال یافته و روال طبیعی خود را مطابق با نمودار پروفیل سرعت حرکت تعریف شده پیموده است (شکل (۱۰)).

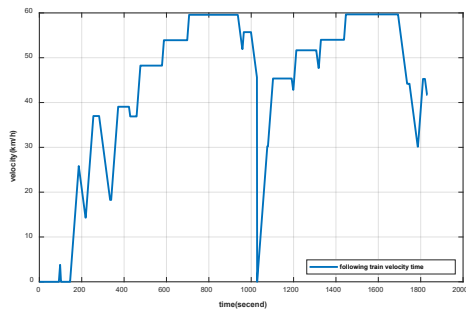


شکل ۱۴. نمودار  $SINR$  بر حسب زمان

در چهار حالت بعدی، نوع کانال را تغییر داده و کانال پرش فرکانسی طیف گسترده فرض شده و اثرات آن بر مقدار  $SINR$  و کاهش زمان سفر و کم کردن اثرات جمر بررسی می‌شود.

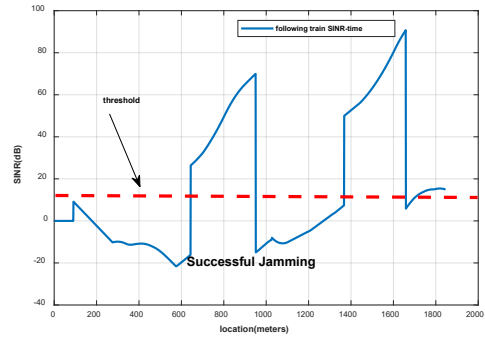
#### حالت پنجم

در حالت پنجم، موقعیت یک جمر را ۰٫۲ کیلومتر از مبدأ و موقعیت جمر دیگر را تصادفی در نظر می‌گیریم. به طوری که همواره سیگنال‌های مختل‌کننده از طریق این دو مهاجم انتشار می‌گردد (شکل (۱۵)).



شکل ۱۵. نمودار پروفیل سرعت حرکت بر حسب زمان

نتایج حاصل از تعیین  $SINR$  بر حسب زمان در این حالت در شکل (۱۶) نمایش داده شده است.



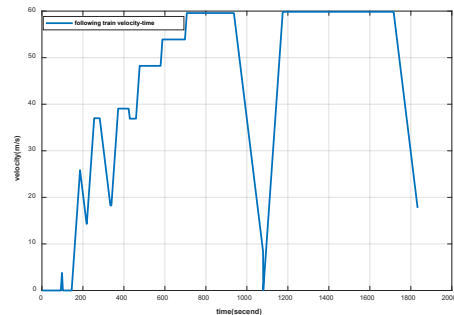
شکل ۱۶. نمودار  $SINR$  بر حسب زمان

#### حالت چهارم

در حالت چهارم نیز جمر اول در موقعیت مشخص و جمر دوم در موقعیت تصادفی در نظر گرفته شده است.

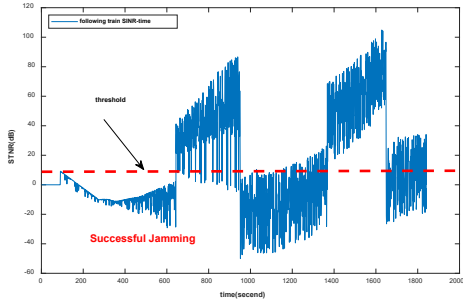
با این تفاوت که برای محاسبه  $SINR$  در هر لحظه موقعیت جمر تصادفی تغییر می‌کند و این آزمایش موقعیت بهینه برای انتخاب محل جمر را به صورتی که اثرگذاری بیشتری بر کاهش  $SINR$  داشته باشد نشان می‌دهد.

در این حالت از پرش فرکانسی طیف گسترده  $FHSS$  برای مقابله با جمر استفاده می‌شود (شکل (۱۳)).

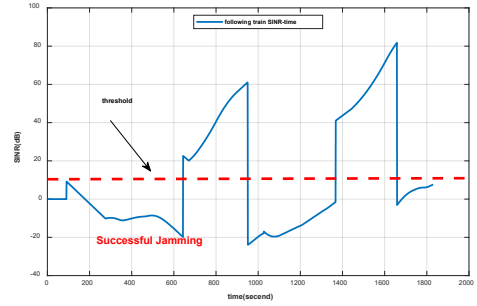


شکل ۱۳. نمودار پروفیل سرعت حرکت بر حسب زمان

روش پرش فرکانسی طیف گسترده در حالتی که دو جمر به سیستم  $CBTC$  حمله کنند و به صورت مداوم سیگنال‌های غیرمجاز را در سراسر محیط شبیه‌سازی انتشار دهند قابل اجرا و استفاده است به طوری که مقدار  $SINR$  ما نسبت به آستانه آن را افزایش می‌دهد و قطار  $CBTC$  سریعاً به حالت عادی خود که همان حالت بلاک متحرک است باز می‌گردد (شکل (۱۴)).

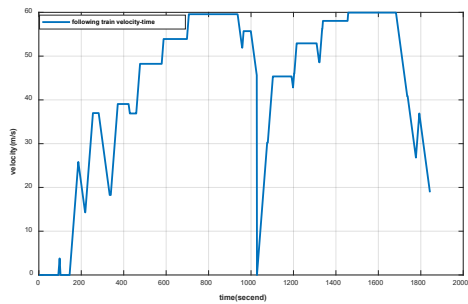


شکل ۱۹. نمودار  $SINR$  بر حسب زمان



شکل ۱۶. نمودار  $SINR$  بر حسب زمان

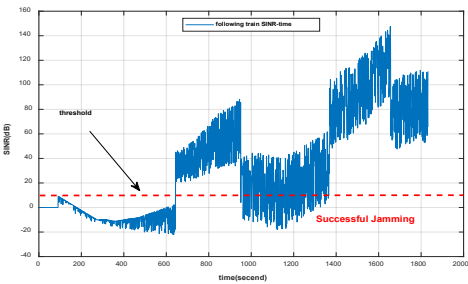
نتایج به دست آمده از این حالت، بیشترین اثرگذاری جمر و بهینه‌ترین موقعیت آن را به ما نشان می‌دهد (شکل (۲۰)).



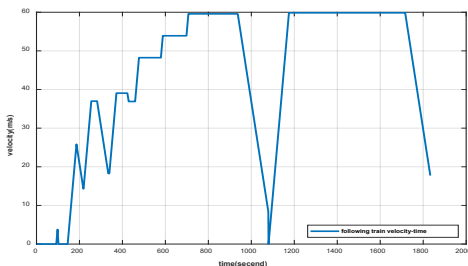
شکل ۲۰. نمودار پروفیل سرعت حرکت بر حسب زمان

### حالت هشتم

پرش فرکانسی طیف گسترده برای این حالت اعمال می‌گردد. نتایج به دست آمده مربوط به این حالت، در شکل (۲۱) و شکل (۲۲) ارائه شده است.



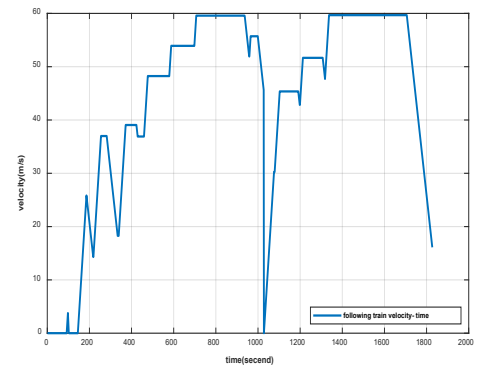
شکل ۲۱. نمودار  $SINR$  بر حسب زمان



شکل ۲۲. نمودار پروفیل سرعت حرکت بر حسب زمان

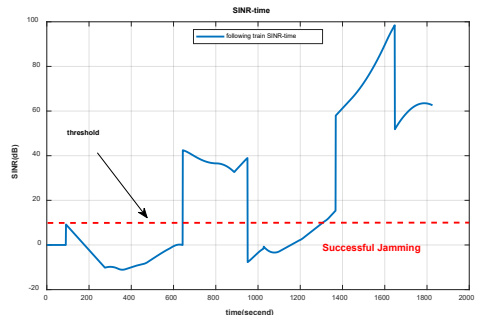
### حالت ششم

روش پرش فرکانسی طیف گسترده در ارتباط با این حالت اعمال می‌شود و نتایج به دست آمده در این حالت، به صورت شکل (۱۷) تعیین می‌گردد.



شکل ۱۷. نمودار پروفیل سرعت حرکت بر حسب زمان

در این حالت، نسبت به حالتی که جمرها در موقعیت ثابت قرار دارند، اثرگذاری کم‌تری حاصل می‌گردد (شکل (۱۸)).



شکل ۱۸. نمودار  $SINR$  بر حسب زمان

### حالت هفتم

در این حالت، یک جمر در فاصله ثابت ۰٫۲ کیلومتری از مبدأ و جمر دوم در هر بار محاسبه مقدار  $SINR$  در یک موقعیت تصادفی در نظر گرفته می‌شود (شکل (۱۹)).

## ۵- نتیجه گیری

-Alnife, G., & Simon, R. (2007). A multi-channel defense against jamming attacks in wireless sensor networks. *In Proceedings of the 3rd ACM Workshop on Qos and Security for Wireless and Mobile Networks*, 95-104.

-Basar, T. (1983). The Gaussian test channel with an intelligent jammer. *IEEE Transactions on Information Theory*, 29(1), 152-157.

-Bu, B., Yu, F. R., & Tang, T. (2014). Performance improved methods for communication-based train control systems with random packet drops. *IEEE Transactions on Intelligent Transportation Systems*, 15(3), 1179-1192.

-Chang, S. Y., Hu, Y. C., & Laurenti, N. (2012). SimpleMAC: A jamming-resilient MAC-layer protocol for wireless channel coordination. *In Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*, 77-88.

-Grover, K., Lim, A., & Yang, Q. (2014). Jamming and anti-jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing*, 17(4), 197-215.

-Heddebaut, M. (2008). Leaky waveguide for train-to-wayside communication-based train control. *IEEE Transactions on Vehicular Technology*, 58(3), 1068-1076.

-Heddebaut, M., Degauque, P., Duhot, D., & Mainardi, J. (1990). IAGO: command control link using coded waveguide. *Journal of Transportation Engineering*, 116(4), 427-435.

-Ma, S., Wang, H., Zhu, L., & Zhang, Q. (2023). Joint security and resilience control in IIoT-based virtual control train sets under jamming attacks. *IEEE Transactions on Vehicular Technology*, 72(9), 11196-11212.

-Kawakami, T., Maruhama, T., Takeya, T., & Kohno, S. (1964). Waveguide communication system for centralized railway traffic control. *IEEE Transactions on Vehicular Communications*, 13(1), 1-18.

-Lakshminarayana, S., Karachiwala, J. S., Chang, S. Y., Revadigar, G., Kumar, S. L. S., Yau, D. K., & Hu, Y. C. (2018). Signal jamming attacks against communication-based train control: Attack impact and countermeasure. *In Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 160-171.

در این مقاله، هشت حالت مختلف به منظور بررسی اثرات جمینگ در نظر گرفته شده و یک استراتژی با هدف کاهش این اثرات ارائه گردید و برای حالت‌های مذکور، مورد آزمایش قرار گرفت. این حالت‌ها را می‌توان به صورت زیر بیان کرد.

-در حالت اول، یک جمر در یک موقعیت مشخص در نظر گرفته شد و محاسبه  $SINR$  انجام گرفت.

-در حالت دوم، به تعداد جمرها افزوده شده و دو جمر در موقعیت مشخص در نظر گرفته شد و در ادامه، اثرگذاری تعداد جمرها بر  $SINR$  مشاهده گردید.

-در حالت سوم، جمر اول در موقعیت مشخص و جمر دوم در یک موقعیت تصادفی در نظر گرفته شد.

-در حالت چهارم، جمر اول در موقعیت مشخص و جمر دوم در موقعیت تصادفی در نظر گرفته شد (با این تفاوت که برای محاسبه مقدار  $SINR$  در هر لحظه، موقعیت جمر به صورت تصادفی تغییر می‌کند).

-برای حالت‌های پنجم تا هشتم، نوع کانال تغییر یافته و کانال پرش فرکانسی طیف گسترده در نظر گرفته شد و اثرات آن بر مقدار  $SINR$ ، زمان حرکت قطارها و همچنین، کم کردن تاثیرگذاری جمینگ مورد بررسی و تحلیل قرار گرفت.

به طور کلی در این مقاله، به منظور مقابله با اثرات جمر دو روش با این شرایط اعمال شد که امکان تغییر وضعیت در انتخاب مدل حرکتی ایمن در شرایط بحرانی از بلاک ثابت به بلاک متحرک تغییر وجود داشته باشد و همچنین، انتخاب کانال از نوع پرش فرکانسی طیف گسترده قدرت جمر را نسبت به سیگنال اصلی کم کند. همچنین، در سیستم مورد نظر با مدل حرکتی انتخاب شده و قابلیت پرش فرکانسی طیف گسترده در ارسال داده موقعیت بهینه جمر با محاسبه  $SINR$  مشخص شد.

با توجه به نتایج به دست آمده از پیاده‌سازی استراتژی ارائه شده، مشاهده شد که این روش موقعیت بهینه را برای انتخاب محل قرارداد جمر، به طوری که تأثیرگذاری بیشتری بر کاهش مقدار  $SINR$  داشته باشد، ارائه می‌دهد.

## ۶- مراجع

-Alcala, C. C., Lin, S., He, R., & Briso-Rodriguez, C. (2011). Design and test of a high QoS radio network for CBTC systems in subway tunnels. *In 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, IEEE, 1-5.

- Vo-Huu, T. D., Vo-Huu, T. D., & Noubir, G. (2016). Interleaving jamming in Wi-Fi networks. *In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 31-42.
- Wood, A. D., Stankovic, J. A., & Zhou, G. (2007). DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks. *In 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 60-69.
- Wang, H., Yu, F. R., Zhu, L., Tang, T., & Ning, B. (2015). A cognitive control approach to communication-based train control systems. *IEEE Transactions on Intelligent Transportation Systems*, 16(4), 1676-1689.
- Wang, H., Yu, F. R., Zhu, L., Tang, T., & Ning, B. (2013). Modeling of communication-based train control (CBTC) radio channel with leaky waveguide. *IEEE Antennas and Wireless Propagation Letters*, 12, 1061-1064.
- Zhao, N., Roberts, C., Hillmansen, S., & Nicholson, G. (2015). A multiple train trajectory optimization to minimize energy consumption and delay. *IEEE Transactions on Intelligent Transportation Systems*, 16(5), 2363-2372.
- Zhu, L., Yu, F. R., Ning, B., & Tang, T. (2013). Communication-based train control (CBTC) systems with cooperative relaying: Design and performance analysis. *IEEE Transactions on vehicular Technology*, 63(5), 2162-2172.
- Zhu, L., Yu, F. R., Ning, B., Tang, T., & Wang, H. (2012). Cross-layer handoff design in communication-based train control (CBTC) systems using WLANs. *In 2012 IEEE Vehicular Technology Conference (VTC Fall)*, IEEE, 1-5.
- Nguyen, K. T., Beugin, J., Berbineau, M., & Kassab, M. (2016). A new analytical approach to evaluate the critical-event probability due to wireless communication errors in train control systems. *IEEE Transactions on Intelligent Transportation Systems*, 18(6), 1380-1392.
- Pascoe, R. D., & Eichorn, T. N. (2009). What is communication-based train control? *IEEE Vehicular Technology Mag.*, 4(4), 16-21.
- Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S. V. (2010). Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications Surveys & Tutorials*, 13(2), 245-257.
- Pickholtz, R., Schilling, D., & Milstein, L. (1982). Theory of spread-spectrum communications-a tutorial. *IEEE Transactions on Communications*, 30(5), 855-884.
- Strasser, M., Popper, C., Capkun, S., & Cagalj, M. (2008). Jamming-resistant key establishment using uncoordinated frequency hopping. *In 2008 IEEE Symposium on Security and Privacy*, (sp 2008), 64-78.
- Sun, W., Yu, F. R., Tang, T., & Bu, B. (2015). Energy-efficient communication-based train control systems with packet delay and loss. *IEEE Transactions on Intelligent Transportation Systems*, 17(2), 452-468.
- Tazaki, T., Li, Z., Sanjo, K., Sakai, K., Shimada, I., & Taoka, H. (2012). Development of CBTC for global markets. *Hitachi Review*, 61(7), 347-375.
- Theeg, G., & Vlasenko, S. (2009). Railway signalling & interlocking. *International Compendium*, 448-449.

# **Modeling, Analyzing, and Proposing a Strategy in Order to Reduce the Effects of Jamming on the Communication Based Train Control (CBTC) Systems**

*Mohammad Ali Sandidzadeh, Associate Professor, Faculty of Railway Engineering,  
Iran University of Science and Technology, Tehran, Iran.*

*Atefeh Tahmasebi, M.Sc., Grad., Faculty of Railway Engineering, Iran University of Science  
and Technology, Tehran, Iran.*

*Farzaad Soleymani, Postdoctoral Researcher, Faculty of Railway Engineering,  
Iran University of Science and Technology, Tehran, Iran.*

**E-mail: sandidzadeh@iust.ac.ir**

Received: September 2025- Accepted: February 2026

## **ABSTRACT**

The main purpose of the train control system is to prevent trains from colliding and derailing. Today, communication-based train control uses various telecommunication methods to transmit control information between trains and the train and the trackside. Although information and communication technology can play an important role in developing the railway industry, information security in this system is vulnerable to various attacks, including jamming. In this paper, the information security of communication-based train control (CBTC) systems is examined, so that an attacker attacks the communication between trains or the train and the trackside and causes the CBTC systems to fail. Next, the effects of jamming attacks on the CBTC system are investigated and to combat it, a frequency hopping spread spectrum method is used to create a secure channel for sending signals. Also, the leaky waveguide signal propagation environment is considered, because the transverse slots on the leaky waveguide walls can provide stable signals with anti-interference capabilities; therefore, given the impossibility of opening the channel signal and accessing the signal, using these methods, the jammer fails to reach the target and its effects are minimized.

**Keywords:** Information Security, Communication-Based Train Control Systems, Frequency Hopping Spread Spectrum, Leaky Waveguide