

تشخیص و مکان‌یابی تقویت‌کننده‌های غیرمجاز در شبکه‌های سلولی مبتنی بر تحلیل آماری مقاوم داده‌های

Drive Test

محمدحسین حق‌دادی^۱، سجاد میرجلیلی^۲ و پارسا شفیعی یکتا^۳

^۱ دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران

چکیده

استقرار خودسرانه و غیرمجاز تقویت‌کننده‌های سیگنال (Unauthorized Repeaters) در شبکه‌های سلولی، یکی از چالش‌های امنیتی و کیفیتی عمده برای اپراتورهای تلفن همراه محسوب می‌شود. این تجهیزات با تزریق نویز و ایجاد تداخل مخرب، منجر به آلودگی پایلوت، کاهش ظرفیت سلول و تخریب شاخص‌های کلیدی عملکرد (KPIs) می‌گردند. روش‌های متداول تشخیص، اغلب متکی بر تجهیزات گران‌قیمت پایش طیف یا تحلیل‌های زمان‌بر میدانی هستند. در این مقاله، یک چارچوب خودکار و داده‌محور برای تشخیص و مکان‌یابی این تجهیزات با استفاده از داده‌های استاندارد Drive Test ارائه شده است. رویکرد پیشنهادی از یک مدل انتشار دو-مسیره (Dual-Path) برای شبیه‌سازی دقیق برهم‌نهی سیگنال‌ها بهره می‌برد. هسته اصلی الگوریتم، یک روش تشخیص ناهنجاری آماری مقاوم (Robust Statistical Anomaly Detection) است که با استفاده از آزمون Z-Score اصلاح‌شده و تخمین گرهای مقاوم (میان و MAD)، اثر پوشش ناهنجاری را خنثی می‌کند. در نهایت، خوشه‌بندی فضایی DBSCAN و تخمین گر مرکز جرم وزن‌دار، موقعیت جغرافیایی تقویت‌کننده‌ها را استخراج می‌نماید. ارزیابی عملکرد روش بر روی شبکه شبیه‌سازی شده شهر تهران، نرخ تشخیص ۱۰۰ درصد و میانگین خطای مکانی کمتر از ۳۵۰ متر را نشان می‌دهد که بیانگر کارایی بالای روش در سناریوهای عملیاتی است.

۱ مقدمه

پوشش دهی "نرمال" استفاده می‌شوند را منحرف می‌کنند. چالش اصلی، ایجاد یک خط پایه مقاوم بدون دانش قبلی از مکان تقویت‌کننده‌هاست.

۲. **مکان‌یابی فضایی:** پس از تشخیص ناهنجاری، باید مکان تقویت‌کننده از اندازه‌گیری‌های پراکنده فضایی استخراج شود. این کار نیازمند تکنیک‌های تحلیل فضایی است که بتوانند با داده‌های نویزی و الگوهای اندازه‌گیری نامنظم کار کنند.

۳. **مقیاس‌پذیری:** روش تشخیص باید برای محیط‌های شهری بزرگ با ده‌ها ایستگاه پایه و هزاران نقطه اندازه‌گیری مقیاس‌پذیر باشد.

۴. **محدودیت منابع:** اپراتورهای شبکه به راهکارهایی نیاز دارند که با زیرساخت جمع‌آوری داده Drive Test موجود کار کنند. روش‌هایی که به تجهیزات تخصصی یا فرآیندهای دستی نیاز دارند، مقرون‌به‌صرفه نیستند.

۲-۱ نوآوری‌ها و دستاوردهای پژوهش

این مقاله یک رویکرد نوین آماری-مکانی را پیشنهاد می‌کند که ویژگی‌های متمایز آن عبارتند از:

• **مدل‌سازی فیزیکی دقیق:** استفاده از مدل انتشار دو-مسیره و ترکیب توان در حوزه خطی برای شبیه‌سازی دقیق اثر تقویت‌کننده بر RSSI.

توسعه روزافزون شبکه‌های سلولی نسل چهارم و پنجم (4G/5G) و نیاز کاربران به پوشش دهی پیوسته، منجر به پدیده‌ای به نام نصب خودسرانه تکرارکننده‌های سیگنال (Repeaters) شده است. این تجهیزات سیگنال دریافتی از ایستگاه پایه (BTS) را تقویت و مجدداً در محیط منتشر می‌کنند. اگرچه هدف ظاهری نصب این تجهیزات بهبود پوشش دهی محلی است، اما عدم هماهنگی آن‌ها با طرح فرکانسی شبکه منجر به چالش‌های فنی جدی می‌شود.

۱-۱ بیان مسئله و ضرورت پژوهش

تقویت‌کننده‌های غیرمجاز با عملکرد به صورت Amplify-and-Forward ساده، علاوه بر سیگنال مفید، نویز محیطی را نیز تقویت می‌کنند که منجر به افزایش سطح نویز (Noise Rise) در سمت گیرنده می‌شود. از سوی دیگر، این تجهیزات با ایجاد پوشش دهی کنترل نشده، مکانیزم‌های مدیریت منابع رادیویی و فرآیند Handover را مختل می‌سازند.

چالش‌های کلیدی تشخیص و مکان‌یابی:

۱. **آلودگی خط پایه:** تقویت‌کننده‌های غیرمجاز خود توزیع سیگنال محلی را تغییر داده و همان آماره‌هایی (میانگین و انحراف معیار) که برای تعریف

- **آمار مقاوم (Robust Statistics):** جایگزینی معیارهای میانگین و انحراف معیار کلاسیک با میان و انحراف مطلق میانه (MAD) برای جلوگیری از اثر "پوشش ناهنجاری" (Masking Effect).
- **زنجیره پردازش خودکار:** تلفیق تشخیص ناهنجاری سیگنال با خوشه‌بندی فضایی DBSCAN برای حذف خودکار مشاهدات پرت (Outliers) و کاهش نرخ هشدار غلط.
- **ارزیابی واقع‌گرایانه:** شبیه‌سازی محیط شهری تهران با در نظر گرفتن پارامترهای سایه‌افکنی (Shadowing) و عدم قطعیت محیطی.

۲ مروری بر کارهای پیشین

تشخیص منابع سیگنال غیرمجاز، یک مسئله شناخته شده در صنعت مخابرات است. رویکردهای موجود را می‌توان به سه دسته اصلی تقسیم کرد.

۱-۲ روش‌های لایه فیزیکی و سخت‌افزار-محور

رویکردهای سنتی معمولاً متکی بر تجهیزات تخصصی فرکانس رادیویی (RF) برای اسکن منابع فرستنده غیرمجاز هستند.

۱-۱-۲ اسکن RF و تحلیل طیف

اپراتورهای شبکه اغلب تیم‌های میدانی مجهز به آنالایزرهای طیفی قابل حمل و آنتن‌های جهت‌دار را برای شناسایی منابع تداخل مستقر می‌کنند. با اندازه‌گیری چگالی انرژی طیفی در باندهای فرکانسی Uplink، مهندسان می‌توانند "افزایش کف نویز" (Noise Floor Rise) مشخصه تقویت‌کننده‌های Amplify-and-Forward را شناسایی کنند. سپس از تکنیک‌های مکان‌یابی جهتی مانند تخمین زاویه ورود (Angle of Arrival - AoA) با استفاده از آرایه آنتن برای مثلث‌بندی مکان فیزیکی دستگاه استفاده می‌شود.

محدودیت‌ها: این فرآیند نیروبر است، نیازمند سخت‌افزار گران‌قیمت (مانند اسنایفرهای دستی یا دستگاه‌های نوع Stingray) بوده و واکنشی است نه پیشگیرانه—معمولاً فقط پس از شکایت مشتریان فعال می‌شود.

۲-۱-۲ تحلیل پیشروی زمانی (Timing Advance - TA)

در شبکه‌های LTE و GSM، ایستگاه پایه (eNodeB) تأخیر رفت و برگشت به دستگاه کاربر را اندازه می‌گیرد تا زمان‌بندی انتقال را تنظیم کند، که به آن پیشروی زمانی (TA) گفته می‌شود. چون تقویت‌کننده‌ها تأخیر پردازشی (معمولاً ۵-۱۰ میکروثانیه) وارد کرده و مسیرهای انتشار سیگنال را طولانی‌تر می‌کنند، همبستگی بین TA اندازه‌گیری شده و فاصله فیزیکی واقعی را مخدوش می‌سازند. مطالعات اخیر پیشنهاد کرده‌اند که آمار TA برای تشخیص "باندهایی" از کاربران که به نظر دورتر از شعاع سلول ظاهر می‌شوند، پایش شود.

محدودیت‌ها: روش‌های مبتنی بر زمان‌بندی نیازمند همگام‌سازی دقیق و دسترسی به داده‌های سیگنالینگ سطح پایین هستند که اغلب در لاگ‌های استاندارد Drive Test در دسترس نیستند.

۲-۲ پایش معیارهای عملکرد شبکه

برای اجتناب از بازدیدهای میدانی، اپراتورها شاخص‌های کلیدی عملکرد (KPI) را در مرکز عملیات و نگهداری پایش می‌کنند.

۱-۲-۲ تشخیص افزایش نویز صعودی

یک علامت اولیه تقویت‌کننده‌های غیرمجاز، افزایش قابل توجه کف نویز صعودی در گیرنده ایستگاه پایه است. تقویت‌کننده‌ها نویز حرارتی را همراه با سیگنال مفید تقویت می‌کنند و نسبت سیگنال به تداخل و نویز (SINR) را برای همه کاربران در سلول تخریب می‌کنند. الگوریتم‌هایی که جهش‌های ناگهانی و پایدار در توان کل باند پهن دریافتی (RTWP) را تشخیص می‌دهند، معمولاً به عنوان هشدار خط اول استفاده می‌شوند.

۲-۲-۲ تشخیص ناهنجاری Handover

تقویت‌کننده‌ها اغلب پوشش‌دهی "بیش از حد" (Overshoot) ایجاد می‌کنند، جایی که سیگنال یک سلول عمیقاً در قلمرو سلول همسایه منتشر می‌شود. این منجر به شکست‌های مکرر Handover، جابجایی‌های سریع (Ping-Pong) و تداخل می‌شود.

۳-۲ روش‌های داده‌محور و یادگیری ماشین

پژوهش‌های اخیر دانشگاهی به سمت تشخیص خودکار داده‌محور با استفاده از یادگیری ماشین حرکت کرده‌اند.

۱-۳-۲ کاهش آزمون‌های رانندگی (MDT) و جمع‌سپاری

استانداردهای مدرن MDT (Minimization of Drive Tests) را تعریف می‌کنند، جایی که گوشی‌های کاربران به صورت خودکار اندازه‌گیری‌های سیگنال را به شبکه گزارش می‌دهند. پژوهش‌ها استفاده از این مجموعه داده‌های عظیم برای ساخت "نقشه‌های محیط رادیویی" (REMs) را بررسی می‌کنند. ناهنجاری‌ها در این نقشه‌ها—جایی که قدرت سیگنال از پیش‌بینی‌های تئوری تجاوز می‌کند—به عنوان منابع تداخل احتمالی علامت‌گذاری می‌شوند.

۲-۳-۲ مکان‌یابی مبتنی بر خوشه‌بندی

الگوریتم‌های خوشه‌بندی فضایی برای مکان‌یابی منابع تداخل اهمیت یافته‌اند. با در نظر گرفتن نمونه‌های سیگنال پر قدرت به عنوان نقاط فضایی، الگوریتم‌هایی مانند DBSCAN می‌توانند به طور مؤثر خوشه‌های تداخل واقعی را از نویز اندازه‌گیری تصادفی جدا کنند.

۴-۲ تمایز روش پیشنهادی

روش ارائه شده در این پژوهش، محدودیت‌های اسکن سخت‌افزاری را با اتکال انحصاری به داده‌های استاندارد RSSI Drive Test حل می‌کند. این یک روش **بدون نظارت** (Unsupervised) است که بدون نیاز به داده آموزشی پاک و تنها با اتکا به مدل انتشار فیزیکی و تخمین‌گرهای آماری مقاوم، قادر به شناسایی و مکان‌یابی ناهنجاری‌ها است.

۳ مدل سیستم و فرمول‌بندی مسئله

۱-۳ توپولوژی شبکه

شبکه مورد مطالعه شامل مجموعه‌ای از ایستگاه‌های پایه $B = \{b_1, \dots, b_M\}$ در یک ناحیه جغرافیایی $Area \subset \mathbb{R}^2$ است. توان دریافتی در هر نقطه x تابعی از فاصله تا BTS، بهره آنتن‌ها و مدل انتشار محیطی است.

۲-۳ مشخصات تقویت کننده های غیر مجاز

تقویت کننده های غیر مجاز معمولاً دارای ویژگی های زیر هستند:

- **بهره تقویت:** معمولاً ۵۰-۸۰ دسی بل، کافی برای تقویت قابل توجه سیگنال
- **محدوده پوشش:** تأثیر در شعاع ۵۰۰-۱۰۰۰ متری از تقویت کننده
- **مکان نصب:** معمولاً در فاصله ۳۰۰-۶۰۰ متری از BTS خدمت دهنده برای دریافت سیگنال ورودی کافی
- **عملکرد:** تقویت و ارسال مجدد در همان فرکانس (Amplify-and-Forward)

۳-۳ مدل انتشار و ترکیب سیگنال

برای مدل سازی دقیق محیط شهری، از مدل تجربی Cost-231 Hata استفاده می شود که برای محیط های شهری در بازه فرکانسی ۱۵۰۰-۲۰۰۰ مگاهرتز مناسب است:

$$PL(d) = 46.3 + 33.9 \log_{10}(f) - 13.82 \log_{10}(h_b) + (44.9 - 6.55 \log_{10}(h_b)) \log_{10}(d) + C_m \quad (1)$$

که در آن $PL(d)$ تلفات مسیر بر حسب دسی بل، f فرکانس بر حسب مگاهرتز، h_b ارتفاع آنتن ایستگاه پایه، d فاصله بر حسب کیلومتر و C_m ضریب تصحیح محیط شهری (معمولاً ۳ دسی بل) است.

توان دریافتی در دستگاه تلفن همراه با استفاده از معادله انتقال Friis محاسبه می شود:

$$P_r = P_t + G_t + G_r - PL(d) \quad (2)$$

که در آن P_r توان دریافتی، P_t توان ارسال BTS (معمولاً -۴۳ dBm برای LTE)، G_t بهره آنتن فرستنده (۱۰-۱۸ dBi برای آنتن های سکتوری)، و G_r بهره آنتن گیرنده (۰ dBi برای دستگاه های تلفن همراه) است.

۱-۳-۳ فیزیک ترکیب سیگنال چندمسیره

نکته کلیدی در حضور تقویت کننده، دریافت سیگنال از دو مسیر مجزا است:

۱. مسیر مستقیم (Direct Path): $BTS \rightarrow UE$

۲. مسیر تقویت شده (Repeater Path): $BTS \rightarrow Rep \rightarrow UE$

چون اختلاف طول مسیر ($\Delta d > \lambda$) منجر به اختلاف فاز تصادفی می شود، امواج به صورت **غیرهمدوس** با یکدیگر ترکیب می گردند. لذا جمع جبری مقادیر dBm نادرست بوده و باید ابتدا توان را به حوزه خطی (میلی وات) تبدیل کرد:

$$P_{total}^{(mW)} = P_{direct}^{(mW)} + P_{repeater}^{(mW)} \quad (3)$$

و سپس به حوزه لگاریتمی بازگشت:

$$P_{rx}(dBm) = 10 \log_{10} \left(10^{\frac{P_{dir}}{10}} + 10^{\frac{P_{rep}}{10}} \right) + \mathcal{N}(0, \sigma_{shadowing}^2) \quad (4)$$

جمله آخر ($\mathcal{N}(0, \sigma^2)$) اثر سایه افکنی لگ-نرمال محیط را با $\sigma = 4$ دسی بل مدل سازی می کند. انتخاب معیار RSSI به جای RSRP دلیل فنی دارد: تقویت کننده های ساده کل پهنای باند (شامل نویز و تداخل) را تقویت می کنند، لذا RSSI به عنوان شاخص انرژی طیفی کل، حساسیت بالاتری نسبت به سیگنال های مرجع دارد.

۴ روش پیشنهادی

الگوریتم پیشنهادی طی یک فرآیند پنج مرحله ای، داده های خام Drive Test را پردازش کرده و مختصات جغرافیایی تقویت کننده ها را استخراج می کند.

۱-۴ نمای کلی معماری سیستم

سیستم تشخیص از پنج ماژول اصلی تشکیل شده است:

۱. **ماژول تولید شبکه:** ایجاد توپولوژی BTS و تقویت کننده های شبیه سازی شده.
۲. **ماژول شبیه سازی انتشار:** مدل سازی انتشار سیگنال با استفاده از Cost-231 Hata.
۳. **ماژول شبیه سازی Drive Test:** تولید اندازه گیری های RSSI در یک شبکه منظم.
۴. **ماژول تشخیص:** پیاده سازی تشخیص ناهنجاری آماری و خوشه بندی.
۵. **ماژول تجسم:** ایجاد نقشه های تعاملی و گزارش های اعتبارسنجی.

جریان داده از اندازه گیری های خام RSSI شروع شده، از مرحله پیش پردازش (نرمال سازی و فیلتر حساسیت) عبور کرده، سپس وارد هسته تشخیص می شود که شامل محاسبه باقی مانده، آزمون آماری مقاوم، و خوشه بندی فضایی است. خروجی نهایی، لیستی از مکان های تخمینی تقویت کننده ها همراه با امتیاز اطمینان هر یک است.

۲-۴ گام ۱: تولید نقشه مبنا (Baseline)

ابتدا با استفاده از پارامترهای مهندسی شبکه (مکان BTS، توان، سمت آنتن و تیلت)، نقشه پوشش تئوری شبکه بدون حضور تقویت کننده ها محاسبه می شود. این نقشه به عنوان مرجع مقایسه عمل می کند.

۳-۴ گام ۲: محاسبه باقی مانده ها (Residuals)

برای هر نقطه اندازه گیری i ، اختلاف توان اندازه گیری شده (P_{meas}) و توان پیش بینی شده (P_{pred}) محاسبه می شود:

$$r_i = P_{meas}^{(i)} - P_{pred}^{(i)} \quad (5)$$

در حضور تقویت کننده، توزیع r_i دارای Positive Skewness خواهد بود.

۴-۴ گام ۳: تشخیص ناهنجاری با آمار مقاوم

۱-۴-۴ مسئله اثر پوشش

چالش اساسی در تشخیص تقویت کننده ها، آلودگی خود مجموعه داده به ناهنجاری هاست. اگر از میانگین و انحراف معیار کلاسیک برای تعیین آستانه استفاده شود:

۱. عدم نیاز به تعیین تعداد خوشه‌ها از پیش
۲. فیلتر خودکار نقاط پرت منفرد (کاهش هشدار غلط)
۳. توانایی یافتن خوشه‌ها با شکل دلخواه
۴. پشتیبانی از خوشه‌ها با چگالی‌های متفاوت

۴-۶ گام ۵: مکان‌یابی با مرکز جرم وزن‌دار

مکان نهایی تقویت‌کننده با میانگین‌گیری وزن‌دار از مختصات جغرافیایی نقاط خوشه محاسبه می‌شود. نقاطی که شدت ناهنجاری بالاتری دارند (Z-Score) بزرگتر، در تعیین مکان نهایی وزن بیشتری دارند:

$$\hat{lat}_{repeater} = \frac{\sum_{i \in C} Z_i \cdot lat_i}{\sum_{i \in C} Z_i} \quad (10)$$

$$\hat{lon}_{repeater} = \frac{\sum_{i \in C} Z_i \cdot lon_i}{\sum_{i \in C} Z_i} \quad (11)$$

که در آن C مجموعه نقاط ناهنجار در خوشه و Z_i امتیازهای اطمینان (وزن) هستند. این رویکرد وزن‌دهی باعث می‌شود نقاط با شواهد قوی‌تر سهم بیشتری در تخمین مکان داشته باشند.

۴-۷ تحلیل پیچیدگی محاسباتی

کارایی محاسباتی الگوریتم برای پردازش شبکه‌های بزرگ مهم است. جدول ۱ پیچیدگی زمانی هر مرحله را نشان می‌دهد.

جدول ۱: پیچیدگی محاسباتی مراحل الگوریتم

مرحله	پیچیدگی	زمان معمول
تولید توپولوژی	$O(N_{BTS})$	> 1 ثانیه
شبیه‌سازی اندازه‌گیری	$O(N_p \times N_{BTS})$	۵-۱۰ ثانیه
محاسبه باقی‌مانده	$O(N_p \times N_{BTS})$	۳-۵ ثانیه
خوشه‌بندی DBSCAN	$O(N_a^2)$	> 1 ثانیه
تجسم نتایج	$O(N_p)$	۲-۳ ثانیه
کل زنجیره	-	۱۰-۲۰ ثانیه

که در آن N_p تعداد نقاط اندازه‌گیری (معمولاً ۲۵۰۰-۳۰۰۰)، N_{BTS} تعداد ایستگاه‌های پایه (۱۰-۲۰)، و N_a تعداد نقاط ناهنجار (معمولاً > 100) است. مرحله شبیه‌سازی و محاسبه باقی‌مانده غالب‌ترین بخش محاسباتی هستند، اما با پیچیدگی خطی نسبت به تعداد نقاط، قابل مقیاس‌پذیری برای شبکه‌های بزرگ هستند.

۵ شبیه‌سازی و ارزیابی عملکرد

۵-۱ سناریوی شبیه‌سازی

کارایی روش پیشنهادی با شبیه‌سازی بخشی از شبکه شهر تهران (ناحیه ۵ در ۵ کیلومتر) ارزیابی شده است. ناحیه جغرافیایی انتخاب شده (۳۵° ۷۲۰ - ۳۵° ۷۵۸ E، ۵۱° ۵۰ - ۵۱° ۵۴ E) یک محیط شهری متراکم را نمایش می‌دهد که شامل مناطق مسکونی، تجاری و صنعتی است.

$$z_i^{naive} = \frac{r_i - \bar{r}}{\sigma_r}, \quad \bar{r} = \frac{1}{N} \sum r_i, \quad \sigma_r = \sqrt{\frac{1}{N} \sum (r_i - \bar{r})^2} \quad (6)$$

سیگنال‌های قوی تقویت‌کننده باعث افزایش مصنوعی \bar{r} و σ_r می‌شوند که آستانه تشخیص ($z_{threshold}$) را بالا برده و همان ناهنجاری‌ای را که باید شناسایی شود، پنهان می‌کنند (پدیده پوشش ناهنجاری).

۴-۲ راه‌حل: تخمین گرهای مقاوم

برای رفع این مشکل، از تخمین گرهای مقاوم استفاده می‌شود که نسبت به مقادیر پرت حساسیت ندارند:

۱. **مرکز توزیع:** به جای میانگین، از میانه (پایدار در برابر ناهنجاری‌های شدید) استفاده می‌شود:

$$\mu_r = \text{median}(\{r_1, \dots, r_N\}) \quad (7)$$

۲. **مقیاس نوسان:** انحراف معیار تنها از سمت منفی توزیع تخمین زده می‌شود (چون تقویت‌کننده‌ها فقط باقی‌مانده‌های مثبت ایجاد می‌کنند):

$$\sigma_{robust} = \sqrt{\frac{1}{|N_{neg}|} \sum_{r_i < \mu_r} (r_i - \mu_r)^2} \quad (8)$$

۴-۳ آزمون آماری

با استفاده از این تخمین گرهای پاک، امتیاز ناهنجاری محاسبه می‌شود:

$$Z_i = \frac{r_i - \mu_r}{\sigma_{robust}} \quad (9)$$

نقاطی که $Z_i > \theta$ (معمولاً $\theta = 2.5$) و $r_i > r_{min}$ (مثلاً ۱۲ دسی‌بل) به عنوان کاندیدای تقویت‌کننده علامت‌گذاری می‌شوند. این رویکرد، تشخیص بدون نیاز به داده آموزشی پاک را ممکن می‌سازد.

۴-۵ گام ۴: خوشه‌بندی فضایی با DBSCAN

برای حذف نویزهای تک‌نقطه‌ای و شناسایی هسته اصلی تقویت‌کننده، نقاط کاندید وارد الگوریتم DBSCAN (Density-Based Spatial Clustering of Applications with Noise) می‌شوند. این الگوریتم بر اساس چگالی نقاط عمل کرده و خوشه‌ها را بر اساس اتصال چگالی تعریف می‌کند:

- **نقطه هسته (Core Point):** نقطه‌ای که حداقل $MinPts$ همسایه در شعاع ϵ داشته باشد
- **نقطه مرزی (Border Point):** نقطه‌ای در شعاع ϵ یک نقطه هسته ولی خود کمتر از $MinPts$ همسایه دارد
- **نقطه نویز:** نقطه‌ای که نه هسته است و نه مرزی

برای این کاربرد، پارامترها به صورت زیر تنظیم می‌شوند:

- شعاع همسایگی: $\epsilon = 300$ متر (متناسب با برد تقویت‌کننده)
- حداقل نقاط: $MinPts = 3$

مزایای DBSCAN برای تشخیص تقویت‌کننده:

۱-۱-۵ پیکربندی شبکه

شبکه شبیه‌سازی شده شامل ۱۰ ایستگاه پایه در یک آرایش شش ضلعی با فاصله بین سایت‌ها ۱ کیلومتر است. برای شبیه‌سازی واقع‌گرایانه، تغییرات تصادفی به پارامترهای شبکه اعمال شده است:

- ارتفاع آنتن: ۳۰ متر با تغییرات $\pm 10\%$
- توان ارسال: ۴۵ dBm با تغییرات ± 2 dB
- بهره آنتن: ۱۵ dBi با تغییرات ± 1 dBi

سه تقویت‌کننده غیرمجاز به صورت تصادفی در فواصل ۳۳۰-۶۶۰ متری از ایستگاه‌های خدمت‌دهنده نصب شده‌اند. این فاصله انتخاب شده تا اطمینان حاصل شود که تقویت‌کننده سیگنال ورودی کافی برای عملکرد مؤثر دریافت می‌کند.

پارامترهای کلیدی شبیه‌سازی در جدول ۲ آورده شده است.

جدول ۲: پارامترهای پیکربندی شبیه‌سازی

پارامتر	مقدار
تعداد ایستگاه‌های پایه (eNodeB)	۱۰ سایت
فرکانس حامل	۱۸۰۰ مگاهرتز
توان ارسال BTS	۴۶ دسی‌بل میلی‌وات
بهره تقویت‌کننده غیرمجاز	۵۰ دسی‌بل
انحراف معیار سایه‌افکنی (σ)	۴ دسی‌بل
دقت شبکه اندازه‌گیری	۱۰۰ متر

۲-۵ تحلیل نتایج

نتایج حاصل از اجرای الگوریتم برای تشخیص ۳ تقویت‌کننده کاشته شده در جدول ۳ خلاصه شده است. روش پیشنهادی موفق به کشف هر سه مورد بدون هیچ‌گونه تشخیص غلط (False Positive) شده است.

جدول ۳: عملکرد تشخیص و دقت مکانی الگوریتم

خطای مکانی (m)	حداکثر Z-Score	تعداد نقاط خوشه
۲۸۷	۲.۷	۱۴
۴۱۲	۸.۵	۹
۳۵۱	۳.۶	۱۱
۳۵۰	۴.۶	۳.۱۱

میانگین خطای مکانی ۳۵۰ متر بدین معناست که تیم‌های میدانی به جای جستجوی کل شهر، تنها نیاز به جستجوی یک محدوده کوچک (در حد دو بلوک شهری) دارند که کارایی عملیاتی را به شدت افزایش می‌دهد.

۳-۵ تحلیل حساسیت پارامترها

کارایی الگوریتم به پارامترهای کلیدی زیر وابسته است:

- آستانه Z-Score (θ):** مقادیر پایین‌تر (مثلاً ۰.۲) نرخ تشخیص را افزایش می‌دهند اما هشدارهای غلط بیشتری تولید می‌کنند. مقدار $\theta = 2.5$ تعادل مناسبی ارائه می‌دهد.
- دقت شبکه اندازه‌گیری:** کاهش فاصله شبکه از ۱۰۰ به ۵۰ متر، خطای مکانی را تا ۳۰٪ کاهش می‌دهد اما تعداد نقاط اندازه‌گیری را ۴ برابر افزایش می‌دهد.
- بهره تقویت‌کننده:** تقویت‌کننده‌های با بهره کمتر از ۴۰ دسی‌بل ممکن است در سایه شدید محیطی پنهان شوند. سیستم برای بهره‌های ۵۰+ دسی‌بل بهینه شده است.
- پارامترهای DBSCAN:** افزایش ϵ خوشه‌ها را ادغام می‌کند، در حالی که کاهش آن ممکن است یک تقویت‌کننده را به خوشه‌های متعدد تقسیم کند.

۶ بحث و تحلیل

۱-۶ محدودیت‌های روش پیشنهادی

با وجود موفقیت سیستم در محیط شبیه‌سازی، چالش‌هایی برای پیاده‌سازی در دنیای واقعی وجود دارد:

- محیط شبیه‌سازی شده:** این پروژه از داده‌های مصنوعی به جای اندازه‌گیری‌های واقعی استفاده می‌کند. در حالی که مدل‌های انتشار و ویژگی‌های نویز واقع‌گرایانه هستند، شرایط میدانی واقعی ممکن است پیچیدگی‌های اضافی داشته باشند.
- مدل انتشار ساده‌شده:** مدل Cost-231 Hata یک محیط شهری متوسط را نمایش می‌دهد. عوامل خاص سایت مانند ارتفاع ساختمان‌ها، تغییرات توپوگرافی و مورفولوژی شهری خاص به صورت جداگانه مدل‌سازی نشده‌اند که ممکن است در داده‌های واقعی منجر به هشدارهای غلط مثبت شود.
- انواع تقویت‌کننده:** الگوریتم برای تقویت‌کننده‌های ساده -Amplify and-Forward and-Forward بهینه شده است. تقویت‌کننده‌های پیچیده‌تر با تبدیل فرکانس، تغییر زمان یا کنترل بهره تطبیقی ممکن است ویژگی‌های سیگنال متفاوتی نشان دهند.
- چگالی اندازه‌گیری:** دقت تشخیص به چگالی و توزیع اندازه‌گیری‌های Drive Test بستگی دارد. مناطق با اندازه‌گیری‌های پراکنده ممکن است دقت مکان‌یابی کمتری داشته باشند.

۲-۶ ملاحظات عملیاتی برای استقرار

برای استقرار این سیستم در شبکه تجاری، موارد زیر باید در نظر گرفته شود:

- کالیبراسیون پارامترها:** آستانه‌ها باید بر اساس محیط خاص شبکه (شهری، متراکم، حومه، روستایی) تنظیم شوند. یک دوره کالیبراسیون اولیه با داده‌های واقعی ضروری است.
- پایش مستمر:** به جای کمپین‌های پراکنده Drive Test، داده‌های MDT مستمر می‌توانند برای تشخیص تقویت‌کننده‌های تازه نصب شده استفاده شوند.

• **تأیید میدانی:** حتی با مکان‌یابی خودکار، تأیید نهایی و حذف توسط تیم‌های میدانی لازم است. سیستم زمان جستجو را کاهش می‌دهد اما آن را حذف نمی‌کند.

۳-۶ مقایسه با روش‌های جایگزین

جدول ۴ مقایسه‌ای کیفی بین روش پیشنهادی و رویکردهای موجود ارائه می‌دهد.

جدول ۴: مقایسه کیفی روش‌های تشخیص تقویت‌کننده

ویژگی	اسکن RF	تحلیل TA	روش پیشنهادی
نیاز به سخت‌افزار	بله	بله	خیر
دقت مکان‌یابی	عالی	متوسط	خوب
مقیاس‌پذیری	ضعیف	خوب	عالی
هزینه عملیاتی	بالا	متوسط	پایین
نرخ هشدار غلط	پایین	متوسط	پایین
پوشش شبکه	موردی	کامل	کامل

۷ نتیجه‌گیری و کارهای آتی

۱-۷ خلاصه دستاوردها

این پژوهش یک سامانه داده‌محور و مقرون‌به‌صرفه برای تشخیص و مکان‌یابی تقویت‌کننده‌های غیرمجاز در شبکه‌های سلولی ارائه کرد. نوآوری‌های کلیدی عبارتند از:

- **مدل‌سازی فیزیکی دقیق:** پیاده‌سازی ترکیب سیگنال دو-مسیره غیرهمدوس در حوزه خطی، که نسبت به مدل‌های جبری ساده، دقت بالاتری در پیش‌بینی اثر تقویت‌کننده دارد.
- **آمار مقاوم برای خط پایه آلوده:** استفاده از میانه و انحراف معیار نیمه‌منفی برای غلبه بر اثر پوشش ناهنجاری، که امکان تشخیص بدون داده‌های آموزشی پاک را فراهم می‌کند.
- **خوشه‌بندی فضایی هوشمند:** ادغام DBSCAN برای فیلتر خودکار نقاط پرت و کاهش نرخ هشدار غلط به صفر در شبیه‌سازی.
- **عملکرد قابل اعتماد:** دستیابی به نرخ تشخیص ۱۰۰٪ با میانگین خطای مکانی ۳۵۰ متر، که برای استقرار عملیاتی کافی است.

۲-۷ مسیرهای توسعه آتی

برای ارتقای این سیستم و آماده‌سازی برای استقرار تجاری، مسیرهای تحقیقاتی زیر پیشنهاد می‌شود:

۱-۲-۷ ادغام چندمنبعی (Multi-Source Fusion)

ترکیب داده‌های RSSI با معیارهای دیگر می‌تواند دقت را بهبود بخشد:

- **پارامترهای Timing Advance:** تأخیر اضافی ناشی از تقویت‌کننده می‌تواند برای فیلتر هشدارهای غلط استفاده شود.
- **الگوهای Handover:** تحلیل آماری لاگ‌های Handover برای تشخیص ناهنجاری‌های پوشش.
- **داده‌های RTWP:** افزایش نویز صعودی به عنوان یک شاخص تأییدی.

۲-۲-۷ یادگیری عمیق برای الگوشناسی پیشرفته

شبکه‌های عصبی کانولوشنی (CNN) می‌توانند الگوهای فضایی پیچیده را در نقشه‌های پوشش یاد بگیرند:

- آموزش یک شبکه CNN برای طبقه‌بندی نقشه‌های حرارتی RSSI به "پاک" و "آلوده به تقویت‌کننده".
- استفاده از شبکه‌های U-Net برای تقسیم‌بندی دقیق مناطق تحت تأثیر.
- یادگیری انتقالی با داده‌های واقعی برای کاهش نیاز به برچسب‌گذاری دستی.

۳-۲-۷ اعتبارسنجی با داده‌های واقعی

گام بعدی حیاتی، آزمایش روش بر روی داده‌های Drive Test واقعی از یک اپراتور تجاری است:

- همکاری با اپراتور برای دسترسی به لاگ‌های Drive Test تاریخی.
- مقایسه با موارد شناخته شده تقویت‌کننده‌های حذف شده.
- تنظیم دقیق آستانه‌ها برای محیط‌های مختلف (شهری، حومه، روستایی).

۴-۲-۷ توسعه به سمت شبکه‌های 5G

معماری 5G چالش‌ها و فرصت‌های جدیدی ارائه می‌دهد:

- سلول‌های کوچک متراکم (Dense Small Cells) الگوهای پوشش پیچیده‌تری ایجاد می‌کنند.
- Beamforming پویا، مدل‌سازی انتشار را پیچیده‌تر می‌سازد.
- گزارش‌های اندازه‌گیری با وضوح بالاتر (5G NR) اطلاعات بیشتری برای تحلیل فراهم می‌کند.

۳-۷ کلام پایانی

تقویت‌کننده‌های غیرمجاز تهدیدی پایدار برای کیفیت و امنیت شبکه‌های سلولی هستند. این پژوهش نشان داد که با ترکیب مدل‌سازی فیزیکی دقیق، آمار مقاوم و تحلیل فضایی، می‌توان یک سامانه کارآمد برای تشخیص خودکار توسعه داد که به جای تجهیزات گران‌قیمت، بر روی داده‌های موجود شبکه متکی است. نتایج شبیه‌سازی نوید پتانسیل بالای این رویکرد را برای استقرار عملیاتی می‌دهند.