

## ارائه مدلی جهت تحلیل حملات تسخیر گره در الگوریتم‌های مکان‌یابی جدا از محدوده و معیار جدیدی جهت مسئله مرزی

سیدصابر بنی‌هاشمیان<sup>۱</sup>، فضل‌اله ادیب‌نیا<sup>۲\*</sup>، مهدی آقا صرام<sup>۳</sup>

<sup>۱</sup>دانشجوی دکتری، دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، s.banihashemian@stu.yazd.ac.ir

<sup>۲</sup>نویسنده مسئول، دانشیار دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، fadib@yazd.ac.ir

<sup>۳</sup>دانشیار دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، mehdi.sarram@yazd.ac.ir

### چکیده

تاکنون الگوریتم‌های جدا از محدوده متعددی جهت تخمین مکان در شبکه‌های حسگر بی‌سیم پیشنهاد شده است. در این الگوریتم‌ها فرض شده است که شبکه عاری از هرگونه خطا و داده غلط و مخرب است. در این مقاله مدلی جهت تحلیل حملات و داده‌های مخرب در الگوریتم‌های مکان‌یابی جدا از محدوده ارائه شده است و سپس به کاربرد آن در ارزیابی و مقایسه الگوریتم‌های مکان‌یابی جدا از محدوده مطرح *DV-Hop*، *LSVM* و *ELM* پرداخته شده است. داده‌های مخرب ممکن است توسط گره‌های لنگر مخرب و یا گره‌های حسگر تسخیر شده، تولید شوند. مقاومت این الگوریتم‌ها در برابر حمله تسخیر گره با یکدیگر مقایسه و تحلیل شده است. نتایج نشان می‌دهد که اگرچه *DV-Hop* در شرایط عادی خطای مکان‌یابی کمتری نسبت به سه الگوریتم دیگر دارد اما در صورت وجود حمله تسخیر گره لنگر و حسگر، به ترتیب، *ELM* و *LSVM* دارای خطای مکان‌یابی کمتری هستند. همچنین در این مقاله، معیار جدیدی جهت بررسی و مقایسه مسئله مرزی در الگوریتم‌های مکان‌یابی جدا از محدوده، پیشنهاد شده است. نتایج شبیه‌سازی الگوریتم‌های مکان‌یابی نشان می‌دهد که *LSVM* در مقایسه با دیگر روش‌های مکان‌یابی جدا از محدوده، در مسئله مرزی دارای کارایی بهتری است.

### کلیدواژه

مکان‌یابی، شبکه حسگر بی‌سیم، جدا از محدوده، حمله تسخیر گره، مسئله مرزی.

### مقدمه

به دلیل محدودیت‌های حسگرها در هزینه، اندازه، مصرف انرژی، محیط بکارگیری (بطور مثال سیستم موقعیت‌یاب جهانی در برخی مکان‌ها در دسترس نیست) و نوع توزیع آنها (بطور مثال گره‌های حسگر ممکن است به صورت تصادفی در محیط پراکنده شوند)، اغلب حسگرها مکان خودشان را نمی‌دانند. الگوریتم‌های مکان‌یابی در شبکه‌های حسگر بی‌سیم این قابلیت را برای گره‌ها فراهم می‌آورد که مکان خود را با کمک تعدادی گره با مکان مشخص به نام لنگر<sup>۴</sup> یا دیده‌بان<sup>۵</sup> تخمین بزنند. گره‌های با اطلاعات مکانی نامشخص، گره‌های غیر-لنگر یا معمولی نامیده می‌شوند و مکان‌شان توسط الگوریتم مکان‌یابی تخمین زده می‌شود. فرآیند مکان‌یابی جهت تخمین موقعیت مکانی گره‌های معمولی شامل دو مرحله است:

- مرحله جمع‌آوری اطلاعات: در این مرحله اطلاعاتی از قبیل مسافت<sup>۶</sup>، اتصال و زاویه بین گره‌ها و همچنین مکان گره‌های

شبکه حسگر بی‌سیم<sup>۱</sup>، فناوری جدیدی است که هم‌اکنون تحقیقات گسترده‌ای در حوزه آن در حال انجام است. پیشرفت‌های اخیر در حوزه ارتباطات بی‌سیم و الکترونیک، این امکان را فراهم نموده است تا حسگرهایی آچندکاره با هزینه و انرژی مصرفی پایین، ساخته شوند که از نظر اندازه کوچک بوده و در فواصل کوتاه، قادر با ارتباط با هم باشند [۱]. قابلیت خود-مکان‌یابی<sup>۲</sup> یک خصوصیت مطلوب در شبکه‌های حسگر بی‌سیم است. در کاربردهای نظارت محیطی مانند رصد آتش و نظارت بر کیفیت آب و کشاورزی، داده اندازه‌گیری شده بدون اطلاع از مکان آن داده، بی‌فایده خواهد بود. همچنین تخمین مکان برای کاربردهای متعدد دیگری مانند تشخیص نفوذ، نظارت بر ترافیک جاده‌ای و نظارت بر سلامت نیز می‌تواند مفید باشد.

<sup>۴</sup> anchor  
<sup>۵</sup> beacon  
<sup>۶</sup> distance

<sup>۱</sup> wireless sensor networks  
<sup>۲</sup> self-localization  
<sup>۳</sup> sensors

شده است که داده مورد استفاده در مکان یابی، عاری از خطا بوده و هیچ حمله ای در شبکه وجود ندارد. همچنین در روش های امن سازی پیشنهادی [۸-۱۵]، هیچ گونه تحلیلی در مورد میزان تاثیر داده های مخرب در دقت مکان یابی نشده است. از طرف دیگر روش های پیشنهادی قادر به حذف مهاجمان از فرآیند مکان یابی به صورت کامل نیستند. الگوریتم های مکان یابی نیز مانند سایر اجزا و پروتکل های شبکه، می توانند توسط مهاجمان در معرض تهدید قرار گیرند. به بیانی دیگر مهاجمان می توانند باعث عملکرد نادرست این الگوریتم ها شوند. با توجه به اهمیت حمله تسخیر گره در بین انواع حملات دیگر، در اینجا حمله تسخیر گره بررسی شده است. به عنوان مثال در روش های جدا از محدوده و چندپرشه، اگر یک گره لنگر مخرب، مکان خود را غلط اعلام کند و یا یک گره حسگر مخرب، تعداد پرش را کاهش و یا افزایش دهد، این عمل موجب استفاده از داده های غلط در مکان یابی می شود. یکی از اهداف این مقاله بررسی تاثیر داده های غلط بر روی دقت مکان یابی با استفاده از مدل سازی حمله است. نتایج این تحقیق می تواند در کارهای آتی جهت امن سازی الگوریتم های مکان یابی در مقابل حمله تسخیر گره، استفاده شود. نوآوری بعدی این مقاله، ارائه یک معیار جدید جهت بررسی میزان تاثیر مسئله مرزی در الگوریتم های مکان یابی در شبکه های حسگر همگن<sup>۱۴</sup> است. مسئله مرزی یک موضوع مهم در مکان یابی بوده و تاکنون به صورت محدود [۱۶] بررسی شده است. روش استفاده شده در [۱۶] نمی تواند برای مقایسه کارایی الگوریتم های مکان یابی در مسئله مرزی بکار گرفته شود در آن مسئله مرزی به صورت کامل و دقیق مورد بررسی قرار نگرفته است. همچنین در [۱۹] تنها بر روی لایه آخر تمرکز نموده و امکان مقایسه در لایه های دیگر ممکن نیست. ساختار مقاله به این شکل است که در بخش بعدی به مرور کارهای پیشین پرداخته می شود. در بخش سوم، مدل حمله و معیارهای لازم جهت بررسی و تحلیل آن، پیشنهاد می گردد. در بخش بعدی نتایج حاصله از شبیه سازی ارائه می شود و در پایان نتیجه گیری نهایی آمده است.

### پیشینه تحقیق

تران و همکاران [۱۶] الگوریتمی به نام LSVM پیشنهاد دادند. مکان یابی در این الگوریتم تنها براساس اطلاعات تعداد پرش انجام می شود. این الگوریتم ساده بوده و به هیچ گونه سخت افزار مسافت یاب و یا ابزار متحرک کمکی مورد استفاده در بسیاری از روش های دیگر، نیاز ندارد. همچنین LSVM براساس ماشین

لنگر جمع آوری می شود [۲]. مسافت بین همسایه ها می تواند براساس شدت [۳]، زمان رسیدن و اختلاف زمانی رسیدن [۴] سیگنال دریافتی، اندازه گیری شود. مسافت بین گره های چندگانه می تواند توسط DV-Hop [۴] یا DV-distance [۴] اندازه گیری شود.

- مرحله محاسبه مکان: در این مرحله موقعیت مکانی گره با استفاده از اطلاعات جمع آوری شده در مرحله قبل محاسبه می شود.

روش های مکان یابی براساس معیارهای مختلفی تقسیم بندی می شوند. در یک تقسیم بندی آنها به دو دسته مبتنی بر گره<sup>۱۵</sup> و مبتنی بر ایستگاه کاری<sup>۱۶</sup> تقسیم می شوند [۵، ۶]. در دسته اول، خود گره حسگر مکان خود را محاسبه می کند ولی در دسته دوم، ایستگاه کاری<sup>۱۷</sup> یا گره هایی که ایستگاه کاری به آنها اعتماد دارد، مکان گره های حسگر را محاسبه می کند. براساس اینکه جهت مکان یابی از لنگرهای در دسترس مستقیم استفاده شود یا خیر، روش های مکان یابی به دو دسته مکان یابی یک پرشه<sup>۱۸</sup> و مکان-یابی چندپرشه<sup>۱۹</sup> تقسیم بندی می شوند. در دسته اول گره های معمولی تنها با کمک لنگرهای همسایه در محدوده یک پرش، مکان یابی می شوند، در حالی که در دسته دوم از لنگرهای دورتر نیز استفاده می شود. از نظر نوع داده های مورد استفاده، روش های مکان یابی به دو دسته مبتنی بر محدود<sup>۲۰</sup> و جدا از محدوده<sup>۲۱</sup> تقسیم می شوند. در روش های مبتنی بر محدود، مسافت یا زاویه بین گره ها در مرحله جمع آوری اطلاعات اندازه گیری می شود در حالی که در روش های جدا از محدوده، نیازی به این اندازه گیری نیست و از تعداد پرش جهت تخمین مکان استفاده می شود.

به منظور مقاوم سازی الگوریتم های مکان یابی در برابر حملات نیز تعدادی روش پیشنهاد شده است [۸-۱۵]. اما بیشتر این روش ها جهت امن سازی الگوریتم های مبتنی بر محدود، پیشنهاد شده است و امنیت در روش های مکان یابی چندپرشه جدا از محدوده یک چالش اصلی است [۱۳]. از طرف دیگر این روش های امن سازی به طور کامل قادر به حذف تاثیر مهاجمان از فرآیند مکان یابی نیستند و بنابراین میزان تاثیر حملات بر روی این الگوریتم ها نیز می تواند به عنوان معیاری جهت ارزیابی آنها مطرح شود.

همچنین کارایی روش های مکان یابی جدا از محدوده مانند DV-Hop، LSVM، NN و ELM [۴، ۱۶، ۱۷، ۱۸] فقط در شرایط عادی (عدم حمله) مطالعه شده است. در تحقیقات قبلی، فرض

<sup>۱۱</sup> multi-hop  
<sup>۱۲</sup> range-based  
<sup>۱۳</sup> range-free  
<sup>۱۴</sup> isotropic

<sup>۱۵</sup> node-centric  
<sup>۱۶</sup> infrastructure-centric  
<sup>۱۷</sup> base station  
<sup>۱۸</sup> one-hop

بدست می‌آید. این مقاله مسئله مکان‌یابی را با استفاده از شدت سیگنال حل می‌کند.

سو-این و همکاران [۱۸] روش‌های هوش محاسباتی را در مکان‌یابی بکار گرفتند و نتایج حاصله از آنها را با هم مقایسه کردند. همچنین، از ماشین یادگیری بی‌نهایت<sup>۱۸</sup> (ELM) برای حل مسئله مکان‌یابی استفاده کردند تا از مزیت آموزش سریع این ماشین بهره ببرند. چاواراسیا و همکاران [۲۰] بیان کردند که شبکه از دو دسته گره معمولی و لنگر تشکیل شده است. گره‌های لنگر به سیستم موقعیت‌یاب جهانی مجهز هستند. الگوریتم مکان‌یابی آنها به سه مرحله تخمین مسافت، تخمین مکان و تبدیل مختصات تقسیم می‌شود.

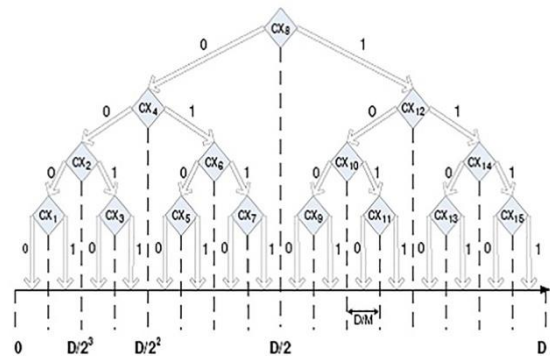
افضل و همکارش [۲۱] الگوریتم مکان‌یابی مبتنی بر آموزش برای شبکه‌های حسگر بی‌سیم سیار پیشنهاد دادند که عملکرد این الگوریتم براساس اطلاعات اتصال است. یان و همکاران [۲۲] تخمین مکان با استفاده از کرنل حداقل مربعات جزئی، پیشنهاد دادند. در روش پیشنهادی آنها، از تابع کرنل برای تعریف اطلاعات اتصال میان گره‌ها استفاده شده و سپس مدلی برای مکان‌یابی میان گره‌ها براساس حداکثر واریانس ایجاد می‌شود. این مدل و تعداد پرش میان گره‌ها با مکان ناشناخته و گره‌های لنگر برای تخمین مکان استفاده می‌شود. بنی‌هاشمیان و همکاران [۲۳] یک الگوریتم مکان‌یابی جدا از محدوده مبتنی بر شبکه عصبی، پیشنهاد کردند. این الگوریتم مکان‌یابی، از روش بهینه‌سازی (Particle swarm optimization) PSO جهت بهینه‌سازی نرون‌های شبکه عصبی استفاده می‌کند. احمدی و همکاران [۲۴] از هر دو روش دسته‌بندی و رگرسیون استفاده کردند. در روش آنها، برای کاهش اثرات نوسانات شدت سیگنال دریافتی، ابتدا دسته‌بند نزدیک‌ترین همسایه (KNN) برای انتخاب نزدیک‌ترین لنگرها به هدف استفاده می‌شود. سپس مکان‌یابی با کمک درخت رگرسیون و با استفاده از لنگرهای انتخابی انجام می‌شود.

یون و همکاران [۲۵] یک روش مکان‌یابی هوشمند ارائه نمودند که از شدت سیگنال دریافتی از گره‌های لنگر استفاده می‌کند. در این مقاله دو طرح با روش فازی و شبکه عصبی ارائه شده است. میلی‌وبرویچ و همکارانش [۲۶] جهت حل مشکل عدم قطعیت شدت سیگنال دریافتی و خطای مکان‌یابی، یک روش مکان‌یابی مبتنی بر مجموعه فازی پیشنهاد دادند که FRORF نامیده می‌شود. این روش سیگنال‌های لنگر را که به وسیله یک ناحیه از فضای مکان‌یابی که احتمال قرار گرفتن گره حسگر در

بردار پشتیبان<sup>۱۵</sup> است و در این مقاله به گونه‌ای از آن، استفاده شده که جهت مکان‌یابی مناسب بوده و در عین حال خطای مکان‌یابی در یک حد قابل قبولی باشد. این روش مکان‌یابی به صورت توزیعی است و همچنین از نظر منابع پردازشی و ارتباطی کارآمد است. همچنین، مسائل سوراخ-پوششی<sup>۱۶</sup> و مسئله مرزی<sup>۱۷</sup> را به صورت مناسب، بررسی می‌کند. در این روش، گره‌ها در یک مکان جغرافیایی با ابعاد  $[0, D] * [0, D]$  که  $D > 0$  توزیع می‌شوند. گره‌های حسگر به دو مجموعه  $M-1$  کلاسی تقسیم می‌شوند:

مجموعه  $M-1$  کلاس  $\{CX_1, CX_2, \dots, CX_{M-1}\}$  برای بعد  $x$  که هر کلاس  $CX_i$  شامل گره‌هایی با  $X \geq i \frac{D}{M}$  است. مجموعه  $M-1$  کلاس  $\{CY_1, CY_2, \dots, CY_{M-1}\}$  برای بعد  $y$  که هر کلاس  $CY_i$  شامل گره‌هایی با  $Y \geq i \frac{D}{M}$  است.

سپس برای هر کلاس، یک ماشین بردار پشتیبان، آموزش دیده و از ضرایب بدست‌آمده آن، جهت مکان‌یابی استفاده می‌شود. جهت مکان‌یابی، مجموعه‌ای از ماشین‌های بردار پشتیبان مانند شکل ۱ استفاده می‌شود.



شکل ۱. درخت تصمیم با  $m=4$

چترجی [۱۷]، یک الگوریتم مکان‌یابی مبتنی بر اتصال چندپرشه و با کمک شبکه عصبی فیدفوروارد چندلایه گرادیان توام<sup>۱۸</sup> پیشنهاد کرده است. در این روش ابتدا گره‌های سردسته فاصله خود با یکدیگر را براساس تعداد پرش بدست آورده و سپس اطلاعات جمع‌آوری شده را به همراه مکان خود به یک سردسته ارسال می‌کنند. سردسته با استفاده از اطلاعات دریافتی، یک مدل شبکه عصبی را آموزش داده و سپس این مدل را جهت تخمین مکان گره‌های حسگر بکار می‌برد. گره‌های حسگر با استفاده از وزن‌ها و بایاس‌های بدست آمده، مکان خود را در شبکه تخمین می‌زنند. این شبکه عصبی دو خروجی دارد که بر اساس این دو خروجی، کلاس مکانی گره در محور  $x$  و محور  $y$

<sup>۱۸</sup> conjugate

<sup>۱۹</sup> Extreme learning machine

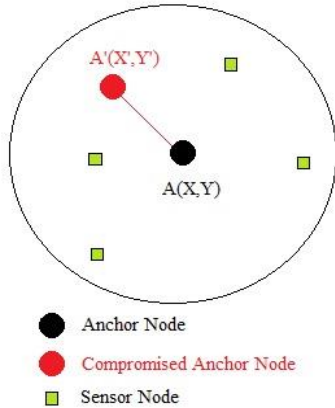
<sup>۲۰</sup> Received Signal Strength

<sup>۱۵</sup> support vector machine

<sup>۱۶</sup> coverage-hole

<sup>۱۷</sup> border

توضیح خواهیم داد. در این نوع از حمله، مهاجم پس از تسخیر گره لنگر مکانی غلط را به شبکه ارسال می کند. این اطلاعات مکانی غلط در الگوریتم های مکان یابی استفاده شده و باعث می گردد که گره های حسگر مکان خود را اشتباه تخمین بزنند. به عنوان مثال در شکل ۲، گره لنگر A که در مکان واقعی  $(x, y)$  قرار دارد، اطلاعات مکانی غلط  $(x', y')$  را درون شبکه ارسال کرده و باعث می شود که گره های حسگر یک موقعیت مکانی غلط را برای خود تخمین بزنند.



شکل ۲. حمله تسخیر گره دیده بان

در DV-Hop، هر گره لنگر یک پیام شامل فیلد مکان گره لنگر و فیلد تعداد پرش با مقدار اولیه صفر، در شبکه ارسال می کند. هر گره دریافت کننده آن پیام، حداقل فاصله تعداد پرش تا هر لنگر را در حافظه خود نگهداری می کند. پیام های دیگر مربوط به یک لنگر خاص، با تعداد پرش بزرگ تر به عنوان اطلاعات قدیمی در نظر گرفته شده و نادیده گرفته می شوند. پیام های با فیلد مقدار پرش کمتر، با افزایش فیلد مقدار پرش، دوباره در شبکه همه پخش می گردد. در مرحله دوم، هر گره لنگر  $i$ ، میانگین اندازه پرش را با استفاده از معادله (۱) تخمین می زند.

$$\text{hopsize}_i = \frac{\sum_{j \neq i} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{\sum_{j \neq i} h(A_i, A_j)} \quad (1)$$

که  $(x_i, y_i)$  و  $(x_j, y_j)$  مختصات گره لنگر  $i$  و  $j$  بوده و  $h(A_i, A_j)$  تعداد پرش بین گره لنگر  $i$  و  $j$  می باشد. سپس هر گره لنگر  $i$ ، اندازه پرش خود را در شبکه ارسال می کند. پس از دریافت اندازه پرش هر گره لنگر  $i$ ، گره های حسگر اندازه پرش را در تعداد پرش ضرب نموده و فاصله خود تا گره لنگر  $i$  را تخمین می زنند. در ادامه، گره های حسگر با استفاده از روش multilateration و با کمک فاصله های تخمینی خود با گره های لنگر، موقعیت مکانی خود را تخمین می زنند. حال فرض کنید یک گره لنگر مخرب  $k$  با مختصات مکانی  $(x_k, y_k)$ ، که عضوی از مجموعه  $m$  لنگر

آن بیشتر است، ایزوله می کند. این روش در دسته روش های مکان یابی جدا از محدوده و مبتنی بر ناحیه، قرار می گیرد. زائو و همکاران [۲۷] الگوریتمی برای شبکه های حسگر سه بعدی پیشنهاد داده اند. این الگوریتم به صورت توزیع شده بوده و هزینه بکارگیری آن اندک است. لیو و همکاران [۲۸] نسخه بهبود یافته الگوریتم DV-Hop پیشنهاد داده اند که از تصحیح اندازه پرش برای کاهش خطاهای اندازه گیری استفاده شده است. همچنین این الگوریتم اثر خطاهای اندازه گیری فاصله را کاهش می دهد.

### مدل پیشنهادی حمله

الگوریتم های جدا از محدوده چند پرش به شدت در برابر حملات تاثیر پذیر هستند. چون اطلاعات مکان یابی هم می تواند توسط گره های لنگر در مرحله اعلان مکان و هم گره های حسگر در مرحله تعیین تعداد پرش، تغییر یابد. یکی از اهداف این مقاله، مطالعه تاثیر حملات بر روی الگوریتم های مکان یابی جدا از محدوده و چند پرش است. در این نوع از الگوریتم ها، اطلاعات مکانی توسط گره های لنگر در شبکه، همه پخش شده و این اطلاعات پرش به پرش توسط گره های حسگر به یکدیگر منتقل می شود. الگوریتم مکان یابی، پس از دریافت این اطلاعات، با استفاده از اطلاعات مکانی و تعداد پرش بکار گرفته شده، مکان یک گره حسگر را تخمین می زند. به منظور بررسی و تحلیل حملات بر روی دقت روش های مکان یابی، به مدل سازی حمله و تشریح تاثیر آن بر روی الگوریتم های مکان یابی DV-Hop [۴]، LSVM [۱۶]، NN [۱۷] و ELM [۱۸] خواهیم پرداخت. منظور از حمله در اینجا، حمله تسخیر گره است که در آن مهاجم می تواند با تسخیر گره، اطلاعات ذخیره شده در حسگر را بدست آورده و با تغییر کارکرد گره، آن را دوباره درون شبکه بکار گیرد. دو نوع حمله تسخیر گره لنگر [۲۹] و تسخیر گره حسگر [۲۹] مورد بررسی قرار می گیرد.

تعدادی فرض جهت این مدل سازی در نظر گرفته شده است. نخست فرض شده است که گره های حسگر و لنگر دارای محدوده ارتباطی یکسانی هستند. همچنین فرض شده که مکان گره ها، ثابت بوده و تغییری در توپولوژی شبکه رخ نمی دهد. در این مدل هیچ فرضی در مورد امن بودن اطلاعات درون گره های لنگر و حسگر نشده است. به عبارتی دیگر، یک مهاجم می تواند با تسخیر یک گره لنگر و یا یک گره حسگر اطلاعات درون آن را تسخیر نماید.

### مدل حمله تسخیر گره لنگر

در این قسمت به بررسی و مدل سازی حمله تسخیر لنگر پرداخته و تاثیر آن را بر روی الگوریتم های مکان یابی [۴]، [۱۶]، [۱۷]، [۱۸]

<sup>۲۳</sup> Sensor node Compromise

<sup>۲۱</sup> node compromise attack

<sup>۲۲</sup> Beacon Compromise

بدین ترتیب حمله تسخیر گره لنگر باعث می‌شود اندازه پرش در گره لنگر  $i$  از معادله (۴) محاسبه شده و مقدارش تغییر یابد. با تغییر اندازه پرش مهاجم می‌تواند بر روی multilateration تاثیر گذاشته و سبب تخمین مکانی غلط در گره‌های حسگر شود. در الگوریتم LSVM [۱۶]، مختصات مکانی غلط می‌تواند در مرحله آموزش ماشین‌های بردار پشتیبان استفاده شود. این عمل می‌تواند منجر به کلاس‌بندی غلط در مرحله مکان‌یابی شود.

$$hopsizet_i = \frac{\sum_{j \neq i, j \neq k \in K} \sqrt{(x_i - x_j)^2 + (y_i + y_j)^2} + \sum_{k \in K} \sqrt{(x_i - x'_k)^2 + (y_i - y'_k)^2}}{\sum_{j \neq i} h(A_i, A_j)} \quad (2)$$

$$= \frac{\sum_{j \neq i, j \neq k \in K} \sqrt{(x_i - x_j)^2 + (y_i + y_j)^2}}{\sum_{j \neq i} h(A_i, A_j)} + \frac{\sum_{k \in K} \sqrt{(x_i^2 + x_k'^2 - 2x_i x_k' + y_i^2 + y_k'^2 - 2y_i y_k')}}{\sum_{j \neq i} h(A_i, A_j)} \quad (3)$$

$$= \frac{\sum_{j \neq i, j \neq k \in K} \sqrt{(x_i - x_j)^2 + (y_i + y_j)^2}}{\sum_{j \neq i} h(A_i, A_j)} + \frac{\sum_{k \in K} \sqrt{(x_i - x_k)^2 + z^2 - 2z(x_i - x_k) + (y_i - y_k)^2 + w^2 + 2w(y_i - y_k)}}{\sum_{j \neq i} h(A_i, A_j)} \quad (4)$$

مختصات مکانی  $(x_i, y_i)$ ، به کلاس  $c$  بعد  $x$  (و یا بعد  $y$ ) با استفاده از رابطه  $x_i \leq c \left(\frac{D_x}{N_x}\right) < (c-1) \left(\frac{D_x}{N_x}\right)$  (یا  $y_i \leq j \left(\frac{D_y}{N_y}\right) < (j-1) \left(\frac{D_y}{N_y}\right)$ ) انجام می‌شود.

در دو الگوریتم NN [۱۷] و ELM [۱۸]، مهاجم با اجرای حمله تسخیر گره لنگر، موجب تغییر در کلاس مکانی نمونه‌های آموزش می‌شود. به عبارت دیگر تغییر در داده‌های آموزش می‌تواند منجر به آموزش غلط شبکه عصبی شود.

به عنوان مثال گره لنگر  $A$  با مکان واقعی  $(x, y)$  به کلاس  $x_{cA} = \left\lfloor \frac{x * N_x}{D_x} \right\rfloor$  و  $y_{cA} = \left\lfloor \frac{y * N_y}{D_y} \right\rfloor$  روی بعد  $x$  و  $y$  منصوب می‌شود. با ارائه مکان نادرست  $(x'_i, y'_i) = ((x_i + z), (y_i + w))$  توسط گره لنگر مخرب  $i$  که  $|z| > 0$  و  $|w| > 0$ ، گره لنگر مخرب  $i$  به کلاس مکانی متفاوتی مانند (۶) و (۷) منصوب می‌شود. کلاس مکانی غلط یک گره لنگر مخرب می‌تواند منجر به کلاس‌بندی اشتباه کلاس‌های مکانی گره‌های حسگر در مرحله مکان‌یابی شود.

$$C_{i'}^x = \left\lfloor \frac{(x_i + z) * N_x}{D_x} \right\rfloor = \left\lfloor \frac{x_i N_x + z N_x}{D_x} \right\rfloor = \left\lfloor \frac{x_i N_x}{D_x} \right\rfloor + \left\lfloor \frac{z N_x}{D_x} \right\rfloor \Rightarrow C_{i'}^x + \left\lfloor \frac{z N_x}{D_x} \right\rfloor \leq C_{i'}^x \leq C_i^x + \left\lfloor \frac{z N_x}{D_x} \right\rfloor + 1 \quad (6)$$

$$C_{i'}^y = \left\lfloor \frac{(y_i + w) * N_y}{D_y} \right\rfloor = \left\lfloor \frac{y_i N_y + w N_y}{D_y} \right\rfloor = \left\lfloor \frac{y_i N_y}{D_y} \right\rfloor + \left\lfloor \frac{w N_y}{D_y} \right\rfloor \Rightarrow C_{i'}^y + \left\lfloor \frac{w N_y}{D_y} \right\rfloor \leq C_{i'}^y \leq C_i^y + \left\lfloor \frac{w N_y}{D_y} \right\rfloor + 1 \quad (7)$$

تسخیر شده  $K = \{k_1, k_2, \dots, k_m\}$  می‌باشد، اطلاعات مکانی نادرست  $(x'_k, y'_k) = ((x_k + z), (y_k + w))$  را در شبکه ارسال نماید که  $|z| > 0$  اختلاف میان مختصات مکانی واقعی و مختصات مکانی غلط اعلام شده بر روی محور  $x$  و  $|w| > 0$  اختلاف میان مختصات مکانی واقعی و مختصات مکانی غلط اعلام شده بر روی محور  $y$  است. بنابراین معادله (۱) به صورت (۲)، (۳) و (۴) تغییر می‌کند.

در دو الگوریتم NN [۱۷] و الگوریتم ELM [۱۸]، از اطلاعات مکانی جمع‌آوری شده و فاصله تعداد پرش بین گره‌های لنگر جهت آموزش شبکه عصبی استفاده می‌شود. در این دو الگوریتم، اطلاعات جمع‌آوری شده برای آموزش به صورت (۵) است.

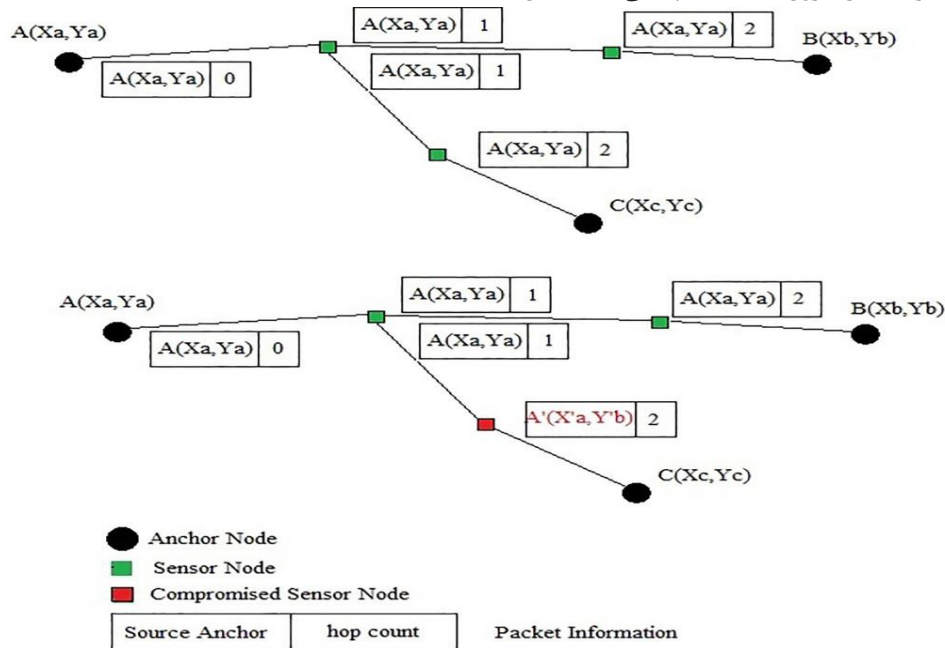
$$\begin{pmatrix} h(S_1, S_1) & h(S_1, S_2) & \dots & h(S_1, S_k) & : & x_{1c} & y_{1c} \\ h(S_2, S_1) & h(S_2, S_2) & \dots & h(S_2, S_k) & : & x_{2c} & y_{2c} \\ \vdots & \vdots & \dots & \dots & \dots & \vdots & \vdots \\ h(S_i, S_1) & h(S_i, S_2) & \dots & h(S_i, S_k) & : & x_{ic} & y_{ic} \\ \vdots & \vdots & \dots & \dots & \dots & \vdots & \vdots \\ h(S_k, S_1) & h(S_k, S_2) & \dots & h(S_k, S_k) & : & x_{kc} & y_{kc} \end{pmatrix} \quad (5)$$

که  $h(S_i, S_j)$  تعداد پرش کوتاه‌ترین مسیر بین دو گره لنگر  $S_i$  و  $S_j$  است و  $x_{ic}$  و  $y_{ic}$  کلاس مکانی متناظر با گره لنگر  $i$  روی محورهای  $x$  و  $y$  است. برای تعیین کلاس مکانی گره لنگر  $i$ ، محیط بکارگیری در محور  $x$  به  $N_x$  خانه مجازی و محیط بکارگیری در محور  $y$  به  $N_y$  خانه مجازی تقسیم می‌شود. بنابراین، تمامی فضای بکارگیری به صورت  $(N_x \times N_y)$  خانه کوچک مجازی تقسیم‌بندی می‌شود. انتصاب گره لنگر  $i$  با

### مدل حمله تسخیر گره حسگر

ترتیب گره حسگر مهاجم می تواند مختصات غلط و یا تعداد پرش جعلی را تولید کرده و در کار الگوریتم مکان یابی اختلال ایجاد کند. لازم به ذکر است که تولید مختصات مکانی جعلی توسط گره های حسگر مخرب در فرآیند مکان یابی الگوریتم های NN، ELM و SVM، تاثیر بی ندارد. زیرا هر گره لنگر، خودش مختصات مکانی خود را به یک گره لنگر سردسته (بدون دخالت گره های حسگر) ارسال کرده و گره لنگر سردسته مختصات مکانی لنگرها را در مرحله آموزش ابزار کلاس بندی، استفاده می کند.

در حمله تسخیر گره حسگر، یک گره حسگر تسخیر شده ممکن است داده بسته های Hello، که توسط یک لنگر ارسال شده، را تغییر دهد (بسته Hello در مرحله ابتدایی جهت تعیین تعداد پرش توسط گره های لنگر تولید و در شبکه ارسال می شود). به عنوان مثال گره حسگر مهاجم، با دریافت پیام یک گره لنگر، ممکن است نسبت به تغییر مختصات مکانی آن گره لنگر اقدام کرده و یا فیلد تعداد پرش بسته دریافتی را کاهش دهد و سپس بسته Hello تغییر یافته را درون شبکه همه پخش کند. بدین

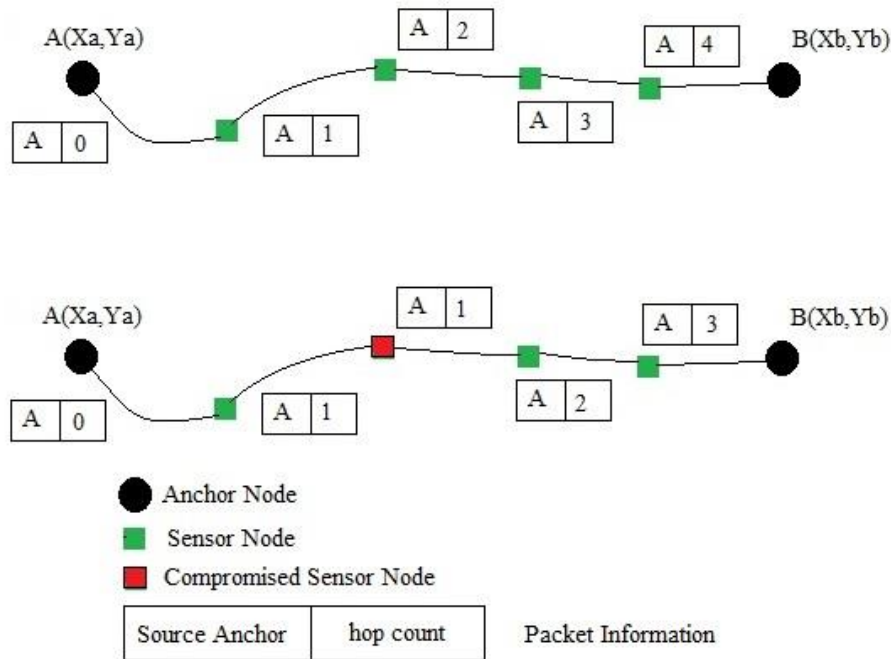


شکل ۳. حمله تسخیر گره لنگر به وسیله تغییر اطلاعات مکانی

تعداد پرش در عملکرد مکان یابی اختلال ایجاد کند. به عبارت دیگر، گره حسگر مهاجم مقدار فیلد تعداد پرش بسته Hello دریافت شده را دست کاری کرده و آن را به گره های بعد از خود ارسال می کند. گره حسگر مهاجم می تواند مقدار فیلد تعداد پرش را افزایش و یا کاهش دهد. در صورت افزایش مقدار فیلد تعداد پرش، این احتمال وجود دارد مسیر دیگری توسط گره های بعدی (شامل گره های حسگر و گره های دیده بان)، به عنوان کوتاه ترین مسیر به گره دیده بانی که مقدار فیلد تعداد پرش بسته Hello آن تغییر پیدا کرده، انتخاب شود. در این مقاله، ما تنها بر روی کاهش مقدار فیلد تعداد پرش، متمرکز شده ایم. در این نوع حمله، یک گره حسگر مهاجم می تواند مقدار فیلد تعداد پرش بسته Hello مربوط به یک گره لنگر A را مانند شکل ۴ کاهش می دهد.

در حمله نوع اول یک گره حسگر مهاجم مانند شکل ۳ می تواند اطلاعات مکان ارسال یک گره لنگر را تغییر دهد. در الگوریتم مکان یابی DV-Hop گره های دیده بانی که این اطلاعات را دریافت می کنند، از اطلاعات غلطی استفاده کرده که این باعث محاسبه اندازه پرش غلط در گره های لنگر و در نتیجه تخمین غلط مکان در گره های حسگر می شود. در برخی از گره های لنگر که مختصات مکانی صحیح دریافت کرده اند از معادله (۱) به منظور تعیین اندازه پرش استفاده می شود. گره دیده بانی که مختصات مکانی غلط دریافت نموده، از معادله (۴) استفاده می کند که باعث محاسبه اندازه پرش غلط می شود.

در حمله نوع دوم، گره حسگر مهاجم، مقدار فیلد تعداد پرش بسته Hello برخی از لنگرها را تغییر می دهد. در این نوع حمله، گره حسگر مهاجم سعی می کند با کاهش و یا افزایش مقدار فیلد



شکل ۴. حمله تسخیر گره لنگر به وسیله تغییر فیلد تعداد پرش

میانگین خطای مکان‌یابی به کار گرفته شده است. الگوریتم NN [۱۷] با یک شبکه عصبی شامل تابع فعال‌سازی  $\text{tansigmoidal}$  در لایه پنهان و تابع فعال‌سازی خطی در لایه خروجی، پیاده‌سازی شده است. در ادامه به شرح پارامترها و معیار ارزیابی خواهیم پرداخت.

### پارامترها و معیار ارزیابی کارآیی

در این بخش تاثیر حمله تسخیر گره حسگر و لنگر بر روی الگوریتم‌های DV-Hop، LSVM، NN و ELM شبیه‌سازی و ارزیابی شده است. در این شبیه‌سازی‌ها هر دو نوع حمله تسخیر گره، به صورت جداگانه مطالعه شده است. در حمله تسخیر گره حسگر، گره حسگر به تغییر مقدار فیلد تعداد پرش در یک پیام اقدام می‌کند و در حمله تسخیر گره لنگر، گره لنگر تسخیر شده، اطلاعات مکانی غلط را در شبکه پخش می‌کند. در این شبیه‌سازی‌ها، میزان خطای مکان‌یابی بر حسب پارامترهای مختلفی بررسی نموده و نتایج بدست آمده تحلیل می‌گردد. خطای مکان‌یابی یک گره اختلاف میان مکان تخمین زده شده با مکان واقعی آن گره است. هرچه این اختلاف کمتر باشد، دقت مکان‌یابی بیشتر است.

در تنظیم اولیه، تعداد ۲۵۶ گره در یک محیط ۵۰ در ۵۰ مترمربع بکار گرفته شده است. محدوده ارتباطی پیش‌فرض ۷ متر در نظر گرفته شده که این محدوده ارتباطی برای کلیه گره‌های حسگر و لنگر یکسان است. همچنین شبکه عاری از خطا

فرض کنید که گره لنگر  $i$ ، فاصله‌های تعداد پرش تغییر یافته  $h'_{k_1}, h'_{k_2}, \dots, h'_{k_m}$  که  $h_{k_i} \neq h'_{k_i}$ ، از  $m$  گره لنگر شامل  $K = \{k_1, k_2, \dots, k_m\}$  دریافت کند. بنابراین گره لنگر  $i$  در الگوریتم DV-Hop، اندازه پرش را با استفاده از معادله (۸) محاسبه می‌کند.

$$\text{hopsiz}_i = \frac{\sum_{j \neq i} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{\sum_{j \neq i, j \in K} h(A_i, A_j) + \sum_{k \in K} h'(A_i, A_k)} \quad (8)$$

در الگوریتم‌های NN، LSVM و ELM، اندازه پرش بین گره لنگر  $i$  و گره لنگر  $k$  به  $h'(S_i, S_k)$  تغییر یافته و در نتیجه اطلاعات جمع‌آوری شده برای آموزش در این الگوریتم‌ها به صورت (۹) تغییر می‌کند.

$$\begin{bmatrix} h(A_1, A_1) & h(A_1, A_2) & \dots & h(A_1, A_k) & : & C_1^x & C_1^y \\ h(A_2, A_1) & h(S_2, S_2) & \dots & h(A_2, A_k) & : & C_2^x & C_2^y \\ \vdots & \vdots & \dots & \dots & \dots & \vdots & \vdots \\ h(A_i, A_1) & h(A_i, A_2) & \dots & h'(A_i, A_k) & : & C_i^x & C_i^y \\ \vdots & \vdots & \dots & \dots & \dots & \vdots & \vdots \\ h(A_k, S_1) & h(A_k, A_2) & \dots & h(A_k, A_k) & : & C_k^x & C_k^y \end{bmatrix} \quad (9)$$

### شبیه‌سازی

جهت شبیه‌سازی الگوریتم‌های [۴، ۱۶، ۱۷، ۱۸] از نرم‌افزار متلب استفاده شده است. در شبیه‌سازی این الگوریتم‌ها فرض شده که محیط بکارگیری به شکل مربع است. به عبارت دیگر  $N_x = N_y$  و  $D_x = D_y$  جهت بررسی الگوریتم‌ها، معیار

در رخداد حمله تسخیر گره لنگر تغییر محسوسی در خطای مکان یابی الگوریتم های NN و ELM مشاهده نمی شود. در الگوریتم SVM، به غیر از مورد تعداد گره های کم (۱۹۶ گره حسگر) رفتار ثابتی مشاهده می شود و این نشان می دهد که در رخداد حمله، افزایش تعداد گره ها تاثیری بر دقت مکان یابی ندارد. در الگوریتم DV-Hop خطای مکان یابی ابتدا کاهش و سپس با یک شیب اندک، افزایش می یابد.

می توان گفت که در رخداد حمله تسخیر گره لنگر، تعداد گره های حسگر در خطای مکان یابی تاثیر چندانی ندارد. علت این امر این است که خطای ناشی از حمله، به دلیل وجود گره های لنگر مخرب است و تعداد گره های حسگر تاثیری بر این عامل ندارد.

#### تعداد گره های متفاوت و حمله تسخیر گره حسگر

شکل ۶ تاثیر حمله تسخیر گره حسگر را بر روی الگوریتم های مکان یابی نشان می دهد. تعداد کل گره ها (شامل گره های حسگر و لنگر) ۱۹۲، ۲۵۶، ۳۲۰ و ۳۸۴ عدد است که از بین آنها تعداد ۳۰ عدد گره تسخیر شده اند. در میان الگوریتم های مورد بررسی، الگوریتم DV-Hop نتایجی بسیار ضعیف تری از سه الگوریتم دیگر دارد. در این الگوریتم متوسط خطای مکان یابی در رخداد حمله نسبت به حالت بدون حمله تا ۶ برابر افزایش یافته است. البته همان گونه که مشاهده می شود با رسیدن تعداد گره ها به ۳۸۴ عدد، این اختلاف به ۵ برابر کاهش می یابد. حمله تسخیر گره حسگر کمترین تاثیر را بر روی الگوریتم ELM دارد هر چند افزایش تعداد گره ها تاثیر چندانی بر کاهش خطای مکان یابی ندارد. در دو الگوریتم SVM و NN با افزایش تعداد گره ها، میانگین خطای مکان یابی به میزان اندکی کاهش می یابد.

فرض شده و بسته های ارسالی توسط تمام گره های درون محدوده ارتباطی گره فرستنده، دریافت می شود. پارامترهای اولیه شبیه سازی به صورت جدول ۱ است.

جدول ۱. پارامترهای اولیه شبیه سازی

پارامتر	مقدار
محیط بکارگیری	۵۰*۵۰ متر مربع
تعداد کل گره های حسگر (با گره های لنگر)	۲۵۶
تعداد گره های دیده بان	۶۴
محدوده ارتباطی گره	۷ متر
تعداد گره های حسگر تسخیر شده	۰
تعداد گره های لنگر تسخیر شده	۰
تعداد اجرا برای هر شبیه سازی	۵۰

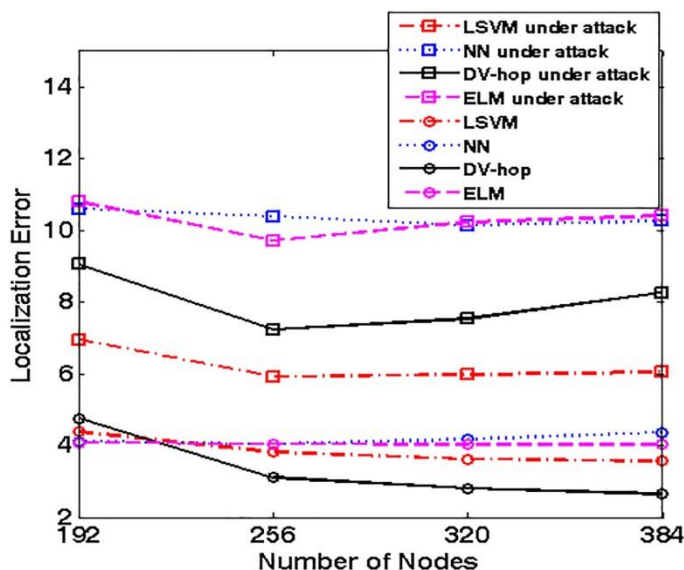
هر شبیه سازی ۵۰ بار تکرار شده و در هر تکرار، گره های حسگر و لنگر به صورت تصادفی در محیط پخش شده اند.

#### نتایج شبیه سازی

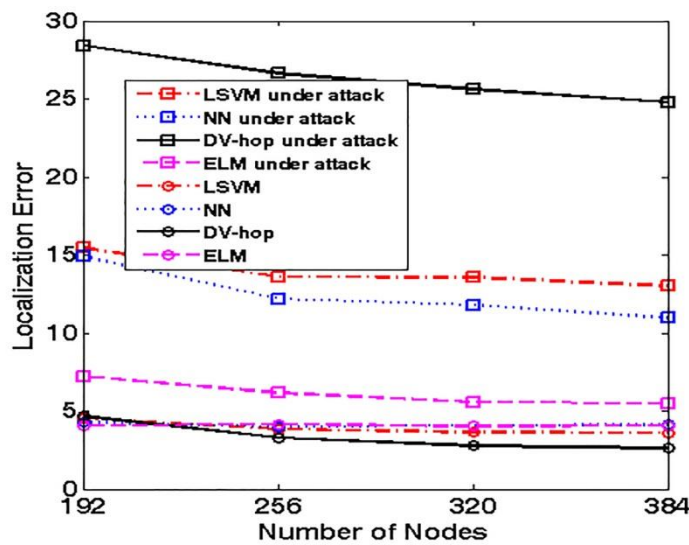
در این قسمت تاثیر پارامترهای گوناگون بر روی نتایج شبیه سازی الگوریتم های مذکور نشان داده شده است.

#### تعداد گره های متفاوت و حمله تسخیر گره لنگر

شکل ۵ تاثیر تسخیر گره لنگر را بر روی الگوریتم مکان یابی نشان می دهد. در این شبیه سازی تعداد گره های لنگر تسخیر شده ۲۰ و تعداد کل گره ها (شامل لنگرها و حسگرها) به صورت متفاوت ۱۹۲، ۲۵۶، ۳۲۰ و ۳۸۴ در نظر گرفته شده است. نتایج شبیه سازی نشان می دهد که با افزایش تعداد گره ها در حالت عادی، دقت مکان یابی الگوریتم های SVM و DV-Hop اندکی کاهش می یابد. با این حال، در الگوریتم های NN و ELM، تفاوت تعداد گره ها تاثیر چندانی بر دقت مکان یابی ندارد.



شکل ۵. تاثیر تعداد گره ها بر روی حمله تسخیر گره لنگر

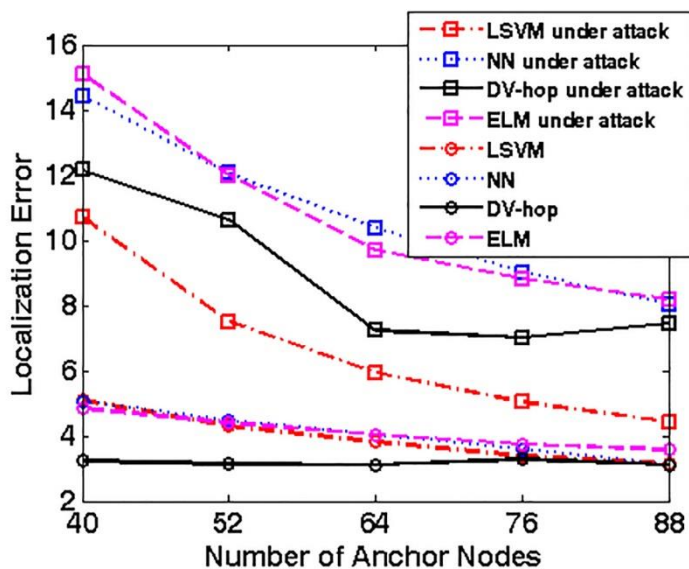


شکل ۶. تاثیر تعداد گره‌ها بر روی حمله تسخیر گره حسگر

لنگرها، میانگین خطای مکان‌یابی در الگوریتم‌های مکان‌یابی کاهش یابد که در شکل ۷ هم این کاهش مشاهده می‌شود. البته همان‌گونه که مشاهده می‌گردد الگوریتم SVM عمل کرد بهتری نسبت به الگوریتم‌های DV-Hop، NN و ELM دارد. در هنگام رخداد حمله تسخیر گره لنگر این الگوریتم دارای خطای مکان‌یابی کمتری نسبت به سایر الگوریتم‌های بررسی شده دارد. با این حال مشاهده می‌شود که در تمامی الگوریتم‌ها با افزایش تعداد گره‌های لنگر، از تاثیر حمله تسخیر گره‌های لنگر تا حد زیادی کاسته شده و می‌توان گفت که در صورت زیاد بودن تعداد گره‌های لنگر، حمله تسخیر گره لنگر به میزان زیادی خنثی می‌شود.

#### تعداد لنگرهای متفاوت و حمله تسخیر لنگر

در این بخش تاثیر تعداد گره‌های لنگر بر دقت مکان‌یابی ارزیابی می‌شود. برای این ارزیابی، تعداد گره‌های لنگر ۴۰، ۵۲، ۶۴، ۷۸ و ۹۰ در نظر گرفته شده است که از این تعداد، ۳۰ عدد گره، تسخیر شده است. نتایج به‌دست آمده در شکل ۷ نشان داده شده است. در حالت عادی و بدون وجود لنگر مهاجم، افزایش تعداد گره‌های لنگر تاثیر چندانی بر روی الگوریتم DV-Hop ندارد و در عین حال با افزایش تعداد گره‌های لنگر، دقت مکان‌یابی الگوریتم‌های SVM، NN و ELM اندکی بهبود می‌یابد. در صورت وجود حمله، انتظار می‌رود که با افزایش تعداد گره‌های



شکل ۷. تاثیر تعداد گره‌های لنگرهای بر روی حمله تسخیر لنگر

## تعداد گره‌های حسگر تسخیر شده و حمله تسخیر گره حسگر

گره حسگر بیشترین مقاومت را خواهد داشت. نتایج حاصله به صورت خلاصه در جدول ۲ بیان شده است.

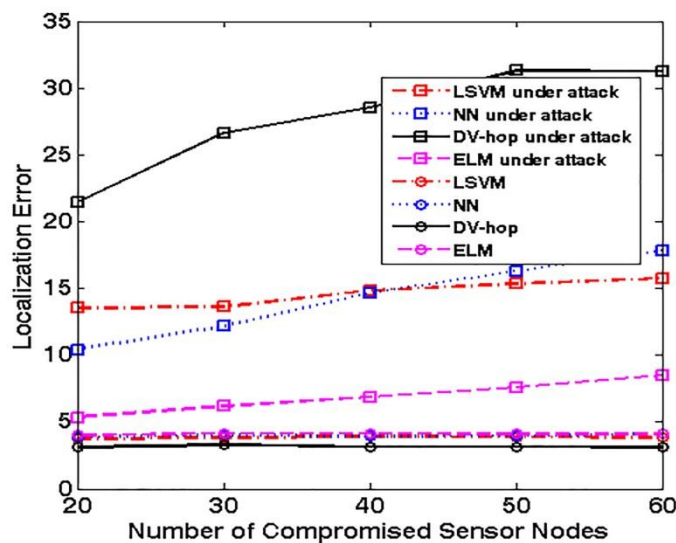
به طور کلی می‌توان گفت الگوریتم SVM از حمله تسخیر گره لنگر، کمترین تاثیر را می‌پذیرد. زیرا الگوریتم SVM از ماشین‌های بردار پشتیبان آموزش داده شده، ساخته می‌شود. در هنگام آموزش هر کدام از ماشین‌های بردار پشتیبان، گره‌های لنگر بر اساس موقعیت مکانی خود به دو کلاس تقسیم می‌شوند (به شکل ۱ مراجعه شود). در حمله تسخیر گره لنگر، گره‌های لنگر مخرب مکان خود را غلط اعلام می‌کنند ولی چون تعداد گره‌های عادی بیشتر است، از تاثیر آنها کاسته می‌شود.

در بین الگوریتم‌های بررسی شده، الگوریتم ELM کمترین تاثیر را از حمله تسخیر گره حسگر می‌پذیرد. حمله تسخیر گره حسگر باعث می‌شود برخی صفت‌های داده ورودی اشتباه شود. این الگوریتم در محیط نویزدار دارای عمل کرد بهتری است [۳۰].

نتایج بدست آمده نشان می‌دهد کارایی الگوریتم شبکه عصبی NN در حالتی که داده ورودی غلط باشد و یا حالتی که کلاس داده اشتباه باشد، کاهش پیدا می‌کند.

الگوریتم DV-Hop بیشترین تاثیر را از حمله تسخیر گره حسگر می‌پذیرد چون گره‌های حسگر مهاجم می‌توانند با تغییر تعداد پرش بر روی محاسبه اندازه پرش تاثیر بگذارند. علت تاثیر بیشتر حمله تسخیر گره حسگر نسبت به حمله تسخیر گره لنگر در این الگوریتم، این است که در حمله تسخیر گره حسگر، اطلاعات تعداد بیشتری از گره‌های لنگر توسط حسگرهای مخرب، تغییر می‌یابد.

شکل ۸ میانگین خطای مکان‌یابی برای تعداد گره‌های حسگر تسخیر شده متفاوت نشان می‌دهد. همانگونه که می‌توان دید افزایش تعداد گره‌های تسخیر شده موجب افزایش خطای مکان‌یابی می‌شود. البته این تاثیر در الگوریتم‌های مختلف، متفاوت است. در الگوریتم DV-Hop میانگین خطای مکان‌یابی نسبت به سه الگوریتم دیگر در صورت رخ دادن حمله تسخیر گره حسگر با اختلافی محسوس بیشتر بوده و در عین حال با افزایش تعداد گره حسگر تسخیر شده، این اختلاف نمایان تر خواهد شد. به بیان دیگر عمل کرد الگوریتم DV-Hop در برخورد با حمله تسخیر گره حسگر نسبت به سه الگوریتم دیگر ضعیف تر است. مشاهده می‌گردد که الگوریتم NN، در صورت تسخیر ۲۰ گره حسگر، عملکرد بهتری نسبت به SVM دارد اما با افزایش تعداد گره‌های حسگر تسخیر شده، میانگین خطای مکان‌یابی بیشتر می‌شود. در صورتی که تعداد گره‌های حسگر تسخیر شده، بیشتر از ۴۰ باشد، دقت مکان‌یابی آن نسبت به SVM کمتر خواهد شد. در الگوریتم SVM، رفتار پایدارتری در صورت افزایش تعداد گره‌های حسگر تسخیر شده، مشاهده می‌گردد و با افزایش تعداد گره‌های حسگر تسخیر شده، میانگین خطای مکان‌یابی افزایش کمی خواهد داشت. در میان این الگوریتم‌ها، الگوریتم ELM کمترین تاثیرپذیری را از حمله تسخیر گره حسگر خواهد داشت و این نشان می‌دهد این الگوریتم نسبت به حمله تسخیر



شکل ۸. تاثیر حمله تسخیر گره حسگر با تعداد گره‌های حسگر تسخیر شده متفاوت

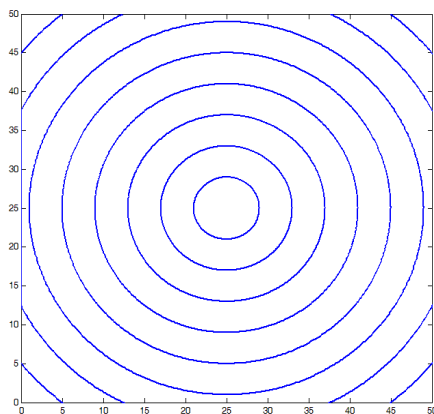
جدول ۲. نتایج تاثیر حمله بر روی الگوریتم‌های مکان‌یابی

ELM	NN	LSVM	DV-op	
کاهش اندک خطای مکان‌یابی	کاهش اندک خطای مکان‌یابی	عدم تاثیر	عدم تاثیر	تاثیر افزایش تعداد گره‌های حسگر در حمله تسخیر گره لنگر
کاهش متوسط خطای مکان‌یابی- تاثیرپذیری کمتر از حمله نسبت به سایر الگوریتم‌ها	کاهش متوسط خطای مکان‌یابی	کاهش متوسط خطای مکان‌یابی	کاهش متوسط خطای مکان‌یابی در رخداد حمله نسبت به حالت بدون حمله از ۶ برابر به ۵ برابر	تاثیر افزایش تعداد گره‌های حسگر در حمله تسخیر گره‌های حسگر
کاهش	کاهش	کاهش	کاهش	تاثیر افزایش تعداد لنگرها در حمله تسخیر گره لنگر
افزایش خطای مکان‌یابی- تاثیرپذیری کمتر از حمله نسبت به سایر الگوریتم‌ها	افزایش خطای مکان‌یابی	افزایش جزئی در خطای میانگین مکان‌یابی	افزایش بیشتر میانگین خطای مکان‌یابی نسبت به سه الگوریتم دیگر	تاثیر افزایش تعداد گره‌های حسگر تسخیر شده در حمله تسخیر گره حسگر

خطای مکان‌یابی بیشتر می‌گردد. این رفتار در هنگام حمله مشخص‌تر است.

جدول ۳. متوسط تعداد گره‌ها در هر بخش در سه شبیه‌سازی با تعداد ۲۵۶، ۳۲۰ و ۳۸۴ گره حسگر

۳۸۴ گره حسگر	۳۲۰ گره حسگر	۲۵۶ گره حسگر	
۶.۱۲	۴.۴۲	۲.۲۶	بخش ۱
۱۷.۸۴	۱۴.۲۶	۱۰.۴۴	بخش ۲
۳۲.۴۴	۲۳.۹۰	۱۸.۹۲	بخش ۳
۴۳.۶۶	۳۵.۰۶	۲۵.۳۴	بخش ۴
۵۶.۵۸	۴۵.۱۲	۳۳.۸۸	بخش ۵
۶۹.۱	۵۵.۰۸	۴۱.۳۴	بخش ۶
۵۵.۶۸	۴۴.۳۰	۳۴.۴۴	بخش ۷
۲۴.۴۸	۲۰.۶۲	۱۴.۰۴	بخش ۸
۵.۱۰	۴.۲۴	۲.۳۴	بخش ۹



شکل ۹. تقسیم بندی محیط بکارگیری [۵۰\*۵۰] به بخش‌های ۴ متری

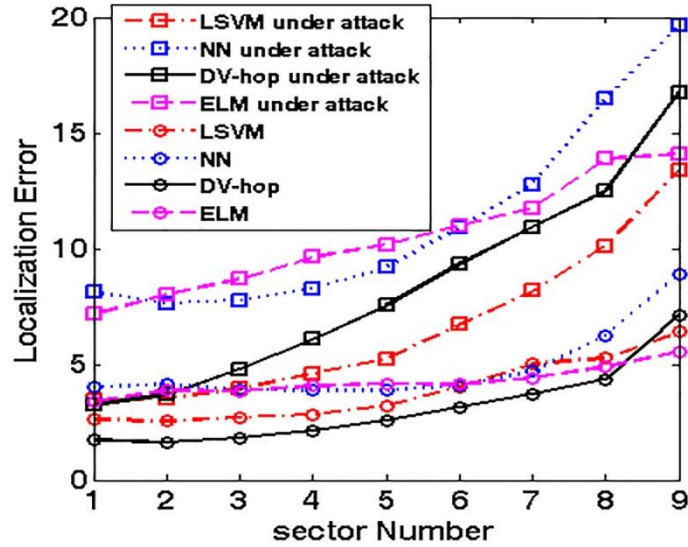
## معیار و بررسی مسئله مرزی

در این بخش به تحلیل و بررسی مسئله مرزی در الگوریتم‌های مکان‌یابی در دو حالت بدون حمله و با حمله تسخیر گره لنگر، خواهیم پرداخت. در مسئله مرزی، هر چه گره‌های حسگر به لبه محیط بکارگیری، نزدیک‌تر باشند، دارای خطای بیشتری در هنگام تخمین مکان هستند. ابتدا مسئله مرزی در سه شبکه مختلف بررسی شده است. تعداد گره‌های حسگر ۲۵۶، ۳۲۰ و ۳۸۴ عدد در نظر گرفته شده است. تعداد گره‌های لنگر تسخیر شده ۲۰ عدد فرض شده است. سایر پارامترها مشابه جدول ۱۱ است. به منظور ارزیابی مسئله مرزی، محیط بکارگیری به بخش‌های دایره‌ای شکل از مرکز تقسیم شده و میانگین خطای مکان‌یابی گره‌های حسگر واقع در آن بخش، به عنوان خطای مکان‌یابی آن بخش در نظر گرفته شده است. در این شبیه‌سازی مرکز بخش‌ها (۲۵، ۲۵) و فاصله میان دو بخش متوالی ۴ متر در نظر گرفته شده است. شکل ۹ تقسیم‌بندی این بخش‌ها را نشان می‌دهد.

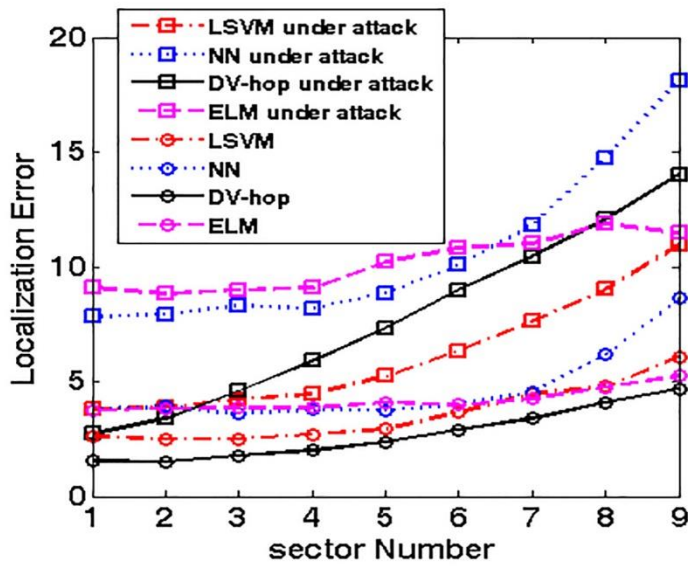
جدول ۳ متوسط تعداد گره‌های هر بخش در سه شبیه‌سازی مذکور را نشان می‌دهد. همان‌گونه که مشاهده می‌شود تعداد گره‌ها در بخش‌های آخر کمتر است و دلیل این اختلاف، کمتر بودن مساحت این بخش‌ها نسبت به سایر بخش‌ها است. نتایج بدست آمده در شکل ۱۰، ۱۱ و ۱۲ نشان داده شده است. همان‌گونه که مشاهده می‌شود تنها در شبیه‌سازی اول (در شکل ۱۰) با ۲۵۶ گره، در بخش آخر جهشی نسبت به بقیه بخش‌ها ملاحظه می‌شود که این امر به دلیل وجود تعداد کم گره‌ها در این بخش می‌باشد. در سایر بخش‌ها رفتاری متعادل مشاهده می‌گردد. به عبارت دیگر هر چه از مرکز بکارگیری دورتر شویم

حالی است که در حالت معمول و بدون وجود حمله، الگوریتم DV-hop دارای خطای مکان یابی کمتری است.

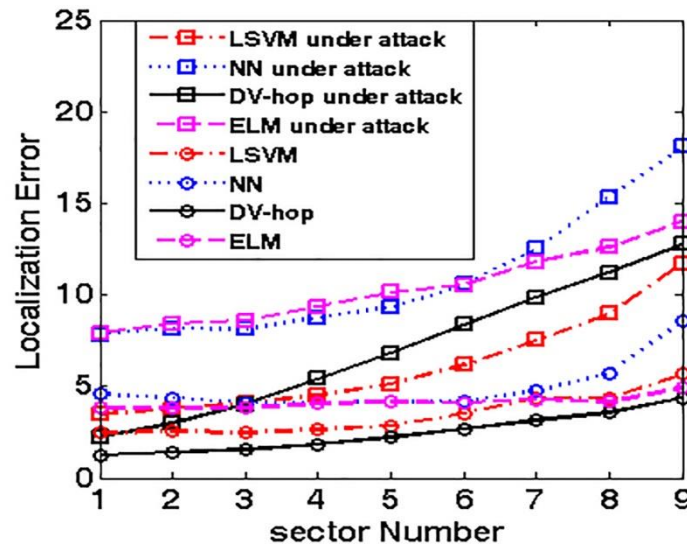
از طرف دیگر مشاهده می شود که الگوریتم SVM در هنگام حمله عملکرد بهتری نسبت به سه الگوریتم دیگر دارد این در



شکل ۱۰. تاثیر مسئله مرزی در صورت وجود و عدم وجود حمله در شبکه های با تعداد ۲۵۶ گره



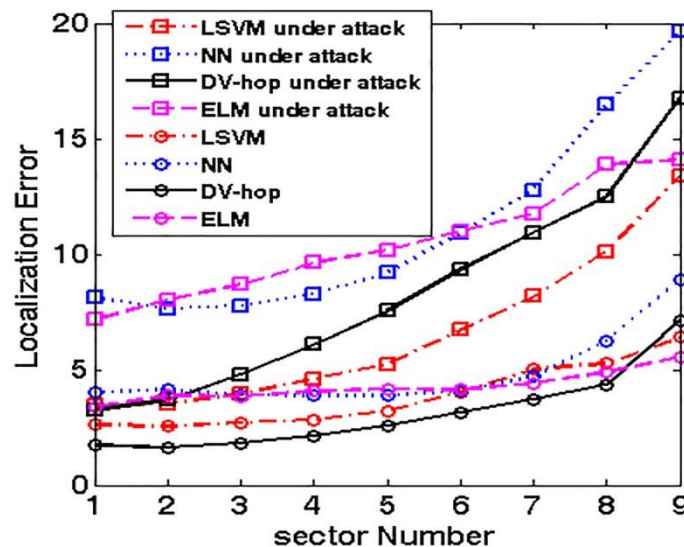
شکل ۱۱. تاثیر مسئله مرزی در صورت وجود و عدم وجود حمله در شبکه های با تعداد ۳۲۰ گره



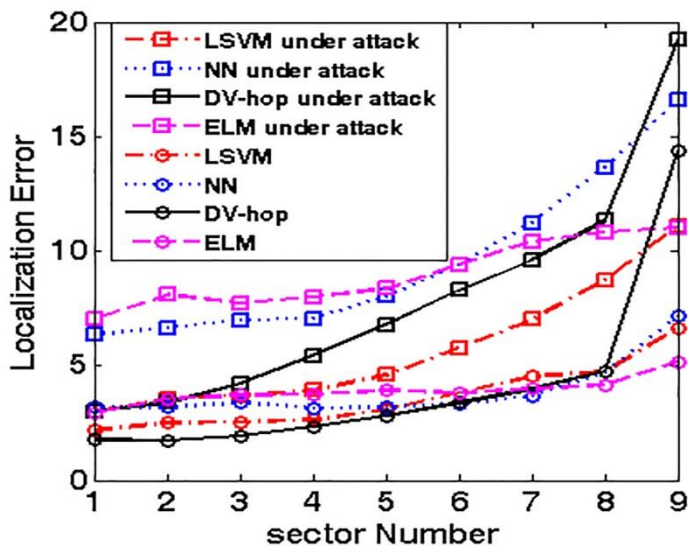
شکل ۱۲. تاثیر مسئله مرزی در صورت وجود و عدم وجود حمله در شبکه‌ای با تعداد ۳۸۴ گره

تعداد گره‌های لنگر در کاهش میزان خطای مکان‌یابی در بخش‌های بیرونی تاثیر گذاشته و خطای مکان‌یابی در این بخش‌ها کاهش می‌یابد. این مسئله در الگوریتم LSVM واضح‌تر است. از طرف دیگر مشاهده می‌گردد که در حالتی که تعداد گره‌های لنگر برابر ۸۸ بوده و حمله وجود ندارد، چهار الگوریتم دارای متوسط خطای مکان‌یابی نزدیک به هم هستند و در عین حال در بخش‌های داخلی DV-Hop عملکرد بهتری از نظر میزان خطای مکان‌یابی دارد.

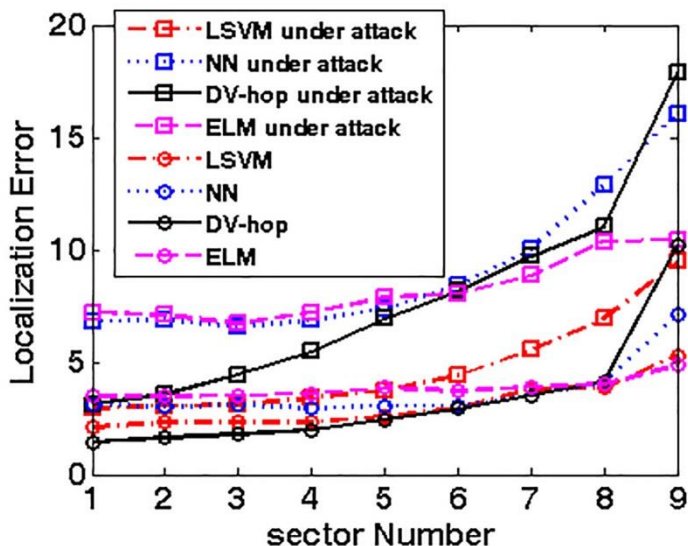
برای بررسی بیشتر مسئله مرزی، تاثیر تعداد گره‌های لنگر هم بر روی این مسئله، مطالعه شده است. بدین منظور در سه شبیه‌سازی متفاوت، از ۲۵۶ گره موجود، به ترتیب ۶۴، ۷۶ و ۸۸ گره به عنوان گره لنگر در نظر گرفته شدند. متوسط تعداد گره‌ها در هر بخش در جدول ۴ نشان داده شده است. در بخش‌های ابتدایی و انتهایی به دلیل مساحت کوچک‌تر این بخش‌ها، تعداد متوسط گره در آنها نیز کمتر است. نتایج این شبیه‌سازی در شکل‌های ۱۳، ۱۴ و ۱۵ نشان داده شده است. همان‌گونه که مشاهده می‌شود در صورت وجود حمله، افزایش



شکل ۱۳. تاثیر مسئله مرزی در صورت وجود و عدم وجود حمله در شبکه‌ای با تعداد ۶۴ گره دیده‌بان



شکل ۱۴. تاثیر مسئله مرزی در صورت وجود و عدم وجود حمله در شبکه‌ای با تعداد ۷۶ گره دیده‌بان



شکل ۱۵. تاثیر مسئله مرزی در صورت وجود حمله و عدم وجود حمله در شبکه‌ای با تعداد ۸۸ گره دیده‌بان

جدول ۴. متوسط تعداد گره‌ها در هر بخش در سه شبیه‌سازی با تعداد ۷۶، ۶۴ و ۸۸ گره دیده‌بان

۸۸ گره دیده‌بان	۷۶ گره دیده‌بان	۶۴ گره دیده‌بان	
۲.۵۸	۲.۶	۲.۲۶	بخش ۱
۸.۶۴	۸.۹۴	۱۰.۴۴	بخش ۲
۱۶.۴۴	۱۷	۱۸.۹۲	بخش ۳
۲۲.۲۲	۲۴.۶۰	۲۵.۳۴	بخش ۴
۲۹.۶۰	۳۱.۸۰	۳۳.۸۸	بخش ۵
۳۶.۸۰	۳۷.۷۲	۴۱.۳۴	بخش ۶
۲۷.۹۶	۳۲.۷۲	۳۴.۴۴	بخش ۷
۱۲.۰۶	۱۳.۲۸	۱۴.۰۴	بخش ۸
۲.۷۰	۲.۳۴	۲.۳۴	بخش ۹

جدول ۵. خلاصه نتایج تاثیر حمله بر روی مسئله مرزی در الگوریتم‌های مختلف مکان‌یابی

ELM	NN	LSVM	DV-Hop	
تغییر اندک خطای مکان‌یابی در نواحی مرزی	عدم تغییر خطای مکان‌یابی در نواحی مرزی	عدم تغییر خطای مکان‌یابی در نواحی مرزی - میانگین خطای مکان‌یابی کمتر در نواحی بیرونی نسبت به سه الگوریتم دیگر	کاهش خطای مکان‌یابی در نواحی مرزی - میانگین خطای مکان‌یابی کمتر در نواحی مرکزی نسبت به سه الگوریتم دیگر	تاثیر افزایش گره‌های حسگر در حمله تسخیر گره لنگر
کاهش خطای مکان‌یابی در نواحی مرزی	کاهش خطای مکان‌یابی در نواحی مرزی	کاهش خطای مکان‌یابی در نواحی مرزی - میانگین خطای مکان‌یابی کمتر در نواحی بیرونی نسبت به سه الگوریتم دیگر	کاهش خطای مکان‌یابی در نواحی مرزی - میانگین خطای مکان‌یابی کمتر در نواحی مرکزی نسبت به سه الگوریتم دیگر	تاثیر افزایش تعداد لنگرها در حمله تسخیر لنگر

مرزی و در صورت وجود حمله تسخیر گره لنگر، الگوریتم LSVM عملکرد بهتری در مقایسه با سه الگوریتم دیگر دارد و این در حالی است که عملکرد الگوریتم DV-Hop در صورت عدم وجود حمله از نظر متوسط خطای مکان‌یابی در گره‌های مرزی بهتر است.

در آینده قصد داریم روش جدیدی برای مقابله با حمله تسخیر گره در الگوریتم‌های مکان‌یابی پیشنهاد گردد و با کمک مدل پیشنهادی، حمله تسخیر گره و همچنین حملات نوع دیگر مورد ارزیابی قرار گیرد.

## مراجع

- [1] C.Y. Chong and S. Kumar, "Sensor networks: Evolution, opportunities, and challenges," Proceedings of the IEEE, vol. 91, pp.1247-1256, 2003.
- [2] G. Han, H. Xu, T.Q. Duong, J. Jiang and T. Hara, "Localization algorithms of wireless sensor networks: a survey," Telecommunication Systems, pp.1-18, 2013.
- [3] F. Yaghoubi, A.A. Abbasfar and B. Maham, "Energy-efficient RSSI-based localization for wireless sensor networks," IEEE Communications Letters, vol. 18(6), pp. 973-976, 2014.
- [4] D. Niculescu and B. Nath, "Ad hoc positioning system (APS)," In Proceedings of Global Telecommunications Conference, pp. 2926-2931, 2001.
- [5] S. Capkun, M. Cagalj and M. Srivastava, "Securing localization with hidden and mobile base stations," In Proceedings of 25th IEEE Conference on Computer Communications, pp.1-10, 2006.
- [6] S. Capkun, K. Rasmussen, M. Cagalj and M. Srivastava, "Secure Location Verification with Hidden and Mobile Base Stations," IEEE

## نتیجه‌گیری

امن‌سازی الگوریتم‌های مکان‌یابی، موضوع مهمی در شبکه‌های حسگر بی‌سیم است. اگرچه تاکنون تعدادی الگوریتم جهت امن‌سازی مکان‌یابی پیشنهاد شده است، ولی تعداد محدودی از این الگوریتم‌ها مناسب مکان‌یابی‌های جدا بر محدوده بوده و هیچ‌کدام برای الگوریتم‌های چندپرشه پیشنهاد نشده‌اند. همچنین این الگوریتم‌های امن‌سازی به‌طور کامل نمی‌توانند داده‌های مخرب تولید شده توسط گره‌های مهاجم را در هنگام محاسبه مکان، حذف کنند.

در این مقاله، به بررسی تاثیر حملات تسخیر گره حسگر و لنگر بر روی الگوریتم‌های مکان‌یابی جدا از محدوده و چندپرشه پرداخته شد. بدین منظور چهار الگوریتم مطرح DV-Hop، NN، LSVM، و ELM با یکدیگر شبیه‌سازی و مقایسه شدند. در ابتدا، مدل حملات تسخیر گره حسگر و لنگر ارائه شد و سپس به تشریح اثرات این حملات بر هر کدام از الگوریتم‌ها پرداختیم.

سپس به شبیه‌سازی و ارزیابی تاثیر این حملات بر روی متوسط خطای مکان‌یابی پرداخته شد. نتایج بدست آمده نشان می‌دهد که در هنگام حمله تسخیر گره لنگر، الگوریتم LSVM عملکرد بهتری از نظر خطای مکان‌یابی نسبت به سه الگوریتم دیگر دارد و DV-Hop در مقابل این نوع حملات ضعیف‌تر است. به عبارت دیگر مهاجمان تاثیر مخرب بیشتری بر روی فرآیند مکان‌یابی در الگوریتم DV-Hop می‌گذارند. در حمله تسخیر گره حسگر، الگوریتم ELM کمتر از حمله تاثیر می‌پذیرد و اختلاف خطای مکان‌یابی در حالت حمله و بدون حمله از سایر الگوریتم‌ها کمتر است. دو الگوریتم LSVM و NN عملکرد مشابه و تا حدودی بهتر از DV-Hop داشته و متوسط خطای مکان‌یابی در این دو الگوریتم نزدیک به هم است. به طور خلاصه می‌توان گفت که الگوریتم ELM در حمله تسخیر گره حسگر و الگوریتم LSVM در حمله تسخیر گره لنگر عملکرد بهتری دارند. از طرف دیگر در گره‌های

- [19] S.S. Banihashemian, F. Adibnia, and M.A. Sarram, "Proposing a measurement criterion to evaluate the border problem in localization algorithms in WSNs," *Computing*, vol. 100, pp.1-22, 2018.
- [20] V. Chaurasiya, N. Jain and G. Nandi, "A novel distance estimation approach for 3D localization in wireless sensor network using multidimensional scaling," *Information Fusion*, vol. 15, pp. 5-18, 2014.
- [21] S. Afzal and H. Beigy, "A localization algorithm for large scale mobile wireless sensor networks: a learning approach," *J Supercomputing.*, vol. 69, pp. 98-120, 2014.
- [22] X. Yan, Z. Yang, A. Song, W. Yang, Y. Liu, and R. Zhu, "A Novel Multihop Range-Free Localization Based on Kernel Learning Approach for the Internet of Things," *Wireless Personal Communications*, vol. 87(1), pp.269-292, 2016.
- [23] S.S. Banihashemian, F. Adibnia and M.A. Sarram, "A New Range-Free and Storage-Efficient Localization Algorithm Using Neural Networks in Wireless Sensor Networks," *Wireless Personal Communications*, Published Online: 2 Sep. 2017.
- [24] H. Ahmadi, F. Viani, A. Polo and R. Bouallegue, "An improved anchor selection strategy for wireless localization of WSN nodes," In *IEEE Symposium on Computers and Communication (ISCC)*, pp. 108-113, 2016.
- [25] S. Yun, J. Lee, W. Chung, E. Kim and S. Kim, "A soft computing approach to localization in wireless sensor networks," *Expert Systems with Applications*, vol. 36, pp. 7552-7561, 2009.
- [26] A. Velimirovic, G. Djordjevic, M. Velimirovic and M. Jovanovic, "Fuzzy ring-overlapping range-free (FRORF) localization method for wireless sensor networks," *Computer Communications*, vol. 35, pp. 1590-1600, 2012.
- [27] X. Zhao, X. Zhang, Z. Sun and P. Wang, "New Wireless Sensor Network Localization Algorithm for Outdoor Adventure," *IEEE Access*, vol. 6, pp.13191-13199, 2018.
- [28] Y. Liu, and Y. Zhang, "A better range-free localization algorithm in wireless sensor networks," In *International Symposium on Computer, Consumer and Control (IS3C)*, pp. 132-135, 2016.
- [29] A. Boukerche, H. Oliveira, E. Nakamura and A. Loureiro, "Secure localization algorithms for wireless sensor networks," *IEEE Commun. Mag.*, vol. 46, pp. 96-101, 2008.
- [30] G.B. Huang, D.H. Wang and Y. Lan, "Extreme learning machines: a survey," *International Journal of Machine Learning and Cybernetics*, vol. 2(2), pp. 107-122, 2011.
- Transactions on Mobile Computing, vol. 7, pp. 470-483, 2008.
- [7] G. Han, J. Jiang, C. Zhang, T.Q. Duong, M. Guizani and G.K. Karagiannidis, "A survey on mobile anchor node assisted localization in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 18(3), pp. 2220-2243, 2016.
- [8] S. Jha, S. Tripakis, S.A. Seshia and K. Chatterjee, "Game theoretic secure localization in wireless sensor networks," In *International Conference on the Internet of Things (IOT)*, pp. 85-90, 2014.
- [9] Z. Li, W. Trappe, Y. Zhang and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," In *Proceedings of the 4th international symposium on Information processing in sensor networks*, pp. 12, 2005.
- [10] D. Wang, J. Wan, M. Wang and Q. Zhang, "An MEF-Based Localization Algorithm against Outliers in Wireless Sensor Networks," *Sensors*, vol. 16(7), p.1041, 2016.
- [11] Y. Zhang, W. Liu, W. Lou and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE J. Select. Areas Commun.*, vol. 24, pp. 247-260, 2006.
- [12] R. Garg, A. Varna and M. Wu, "An Efficient Gradient Descent Approach to Secure Localization in Resource Constrained Wireless Sensor Networks," *IEEE Trans. Inform. Forensic Secur.*, vol. 7, pp. 717-730, 2012.
- [13] Y. Zeng, J. Cao, J. Hong, S. Zhang and L. Xie, "Secure localization and location verification in wireless sensor networks: a survey," *J Supercomputing.*, vol. 64, pp. 685-701, 2013.
- [14] P. Li, X. Yu, H. Xu, J. Qian, L. Dong and H. Nie, "Research on Secure Localization Model Based on Trust Valuation in Wireless Sensor Networks," *Security and Communication Networks*, vol. 2017, 2017.
- [15] H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang and A. Xia, "Securing DV-Hop localization against wormhole attacks in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, pp. 22-35, 2015.
- [16] D. Tran and T. Nguyen, "Localization in Wireless Sensor Networks Based on Support Vector Machines," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, pp. 981-994, 2008.
- [17] A. Chatterjee, "A Fletcher-Reeves Conjugate Gradient Neural-Network-Based Localization Algorithm for Wireless Sensor Networks," *IEEE Trans. Veh. Technol.*, vol. 59, pp. 823-830, 2010.
- [18] C. So-In, S. Permpol, and K. Rujirakul, "Soft computing-based localizations in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 29, pp.17-37, 2016.