نشریه پژوهش‌های مهندسی صنایع در سیستم‌های تولید

نشریه پژوهش‌های مهندسی صنایع در سیستم‌های تولید

IERPS

ISSN: 2345-2269

سال هفتم، شماره پانزدهم، پاییز و زمستان ۱۳۹۸، صفحه ۲۵۵-۲۷۱

www.ier.basu.ac.ir

DOI: 10.22084/ier.2020.19334.1860

ارائه الگوریتم جستجوی ممنوعه جهت حل مسئله مکانیابی-حمله- حفاظت تسهیلات بحرانی در شرایط عدم‌تقارن اطلاعات

معصومه مسی بیدگلی[1*]، جاوید جوزدانی[2]

۱. استادیار، گروه مهندسی صنایع، دانشکده فنی و مهندسی گلپایگان

۲. استادیار، گروه مهندسی صنایع، دانشکده فنی و مهندسی گلپایگان

اطلاعات مقاله

تاریخچه مقاله:

دریافت ۱۳۹۸/۳/۱۸

پذیرش ۱۳۹۸/۱۰/۲۶

کلمات کلیدی:

حمله به شبکه

مکانیابی تسهیلات پوششی

حفاظت

الگوریتم جستجوی ممنوعه

اطلاعات نامتقارن

خلاصه

اکثر فعالیت‌های تروریستی که طی دو دهه گذشته به وقوع پیوسته است مبتنی بر اطلاعات دقیق انجام گرفته‌اند که منجر به ایجاد اختلال در فعالیت‌های اساسی کشور شده و خسارات گسترده‌ای را به‌همراه داشته است و ازاین‌رو این موضوع تهدیدی برای زیرساخت‌های عمومی می‌باشد. گسترش چشمگیر چنین فعالیت‌هایی، لزوم برای مکانیابی صحیح و حفاظت از این زیرساخت‌ها به‌منظور افزایش پایایی تسهیلات برای ارائه خدمات را نشان می‌دهد. در چنین شرایطی، بازی استکلبرگی بین طراح سیستم و مهاجم شکل می‌گیرد که طی آن بازیکنان بر اساس اطلاعاتی که از رقیب خود در اختیار دارند، در تلاشند تا با پیش‌بینی و پاسخگویی به استراتژی انتخابی رقیب، ریسک تصمیم‌گیری خود را کاهش دهند. به‌دلیل ارزش بالای اطلاعات و در اختیار نداشتن اطلاعات دقیق و صحیح در شرایط تضاد منافع، در این تحقیق برآنیم تا با مدل‌سازی مسئله مکانیابی-حمله-حفاظت در شرایط عدم‌تقارن اطلاعات و با فرض امکان حملات جزئی، به‌صورت یک مدل برنامه‌ریزی دوسطحی به بررسی مزایا و ریسک‌های ناشی از نادیده گرفتن عدم‌تقارن اطلاعات توسط طراح سیستم بپردازیم. با توجه به منطقی نبودن زمان حل روش کروش-کان-تاکر در مسائل بزرگ، در این تحقیق الگوریتم جستجوی ممنوعه‌ای مبتنی بر هش ارائه می‌نماییم و با محاسبه معیارهایی همچون منطقی بودن موزون و مستقیم، کارایی و اثربخشی الگوریتم پیشنهادی را با اجرای الگوریتم بر روی تعدادی مسئله نمونه تولیدشده به‌صورت تصادفی نشان می‌دهیم.

۱- مقدمه

طی دهه‌های گذشته، مکانیابی صحیح و حفاظت مناسب از زیرساخت‌های اساسی جهت کاهش خسارات ناشی از حمله به این تسهیلات و افزایش پایایی تسهیلات برای ارائه خدمات موردتوجه دولت‌ها قرار گرفته است. تغییر شکل حملات تروریستی از کشتارهای دسته‌جمعی به سمت ایجاد اختلال در عملکرد تسهیلات زیرساختی مثل شبکه‌های تأمین آب و برق و ... اهمیت طراحی صحیح این نوع تسهیلات را نشان می‌دهد. حمله به برج‌های مخابراتی (در افغانستان) و مرکز آمبولانس (در ایرلند شمالی) دو نمونه مهم از مسئله طی سال‌های گذشته هستند. نیروگاه‌های برق، پل‌ها و راه‌های ارتباطی مهم، نیروگاه‌های هسته‌ای، پست‌های حفاظت از محیط‌زیست برای جنگلبانان، پرسنل کلیدی و مواردی از این قبیل می‌توانند نمونه‌های دیگری از زیرساخت‌های حیاتی یک کشور باشند، که ممکن است موردحمله قرار بگیرند و ازاین‌رو مکانیابی و حفاظت از آن‌ها باید به‌درستی و به‌صورتی بهینه انجام بگیرد.

مکان‌یابی تسهیلات رقابتی همچون شعب بانک‌ها، رستوران‌های زنجیره‌ای و مواردی از این قبیل و اتخاذ استراتژی‌های حفاظتی برای حفظ مشتریان در شرایط ورود رقبای جدید، نمونه دیگری از مسئله

* نویسنده مسئول: معصومه مسی بیدگلی

تلفن: ۰۳۱-۵۷۲۴۰۰۶۵؛ پست الکترونیکی: bidgoli_m2000@yahoo.com

موردمطالعه در دنیای رقابتی امروزه است. از سوی دیگر، مکانیابی تسهیلات امدادرسانی و اضطراری و حفاظت از آن‌ها در مناطق حادثه‌خیز که ممکن است به‌واسطه بلایای طبیعی و حوادث غیرمنتظره، فعالیت آن‌ها مختل شود نمونه‌ای از این مسئله است. مکان‌یابی این نوع از تسهیلات، تصمیم استراتژیکی است که به‌طور مستقیم، موفقیت عملیات امداد و نجات را تحت تأثیر قرار می‌دهد. قرارگیری محل تسهیلات در نزدیکی محل‌های حادثه‌خیز از اهمیت زیادی (ازنظر زمان پاسخ‌گویی) برخوردار است. از سوی دیگر، نزدیکی بیش‌ازاندازه به این نقاط، خطر تخریب و ایجاد اختلال در عملیات پشتیبانی از نقاط تقاضا را در پی دارد. این موضوع، اهمیت مسئله را روشن‌تر می‌سازد.

در تمامی موارد مذکور، با نوعی بازی استکلبرگ ایستایی روبرو هستیم که از یک‌سو دولت‌ها و نیروهای امنیتی به‌عنوان طراح سیستم، نقش بازیکن پیشرو را بر عهده دارند و در مقابل مهاجم به سیستم که به‌عنوان پیرو فعالیت می‌کند. در این بازی، طراح سیستم به‌دنبال مکانیابی تسهیلات و شناسایی و حفاظت از تسهیلات مهم‌تر (که با احتمال بیشتری موردحمله قرار می‌گیرند) با کمترین هزینه (مکانیابی میانه) و یا بیشترین میزان پوشش مشتریان در ارائه خدمات (مکانیابی پوششی) است و از سوی دیگر، مهاجم در پی تخریب تسهیلات و ایجاد بیشترین اختلال ممکن در عملکرد آن‌ها و دسترس‌پذیریشان در شرایطی است که منابع محدودی برای حمله در اختیار دارد.

در بسیاری از موارد، تصمیم‌گیری‌ها در زمینه مکانیابی، حفاظت و حمله در شرایطی صورت می‌گیرد که حداقل یکی از بازیکنان (مهاجم و یا طراح سیستم) به‌دلیل در اختیار نداشتن اطلاعات کاملی از رقیب، ناگزیر است تا بر اساس تخمین‌هایی که در اختیار دارد، تصمیمات خود را اتخاذ نماید. این عدم‌تقارن اطلاعات، مزایا و ریسک‌هایی را برای هر یک از تصمیم‌گیرندگان، نسبت به حالت بازی با اطلاعات کامل، در پی دارد که ضروری است بررسی کاملی در این زمینه صورت گیرد. در این تحقیق، به مطالعه مسئله مکانیابی تسهیلات و حفاظت از آن‌ها در شرایط حمله با اطلاعات نامتقارن پرداخته شده است.

کشور ما در منطقه‌ای استراتژیک واقع شده است که به‌دلیل ذخایر فراوان و موقعیت استراتژیکی ویژه، همواره در معرض تهدید قرار داشته است. با توجه به اینکه حملات تروریستی طی سال‌های گذشته، شکل ساختاریافته‌ای به خود گرفته است و پیچیدگی‌های بیشتری نسبت به گذشته دارد، لازم است تا به‌منظور مقابله با این نوع از تحرکات و تهدیدات و افزایش ضریب امنیت تسهیلات مهم، برنامه‌ریزی‌های دقیق‌تری در زمینه طراحی و برنامه‌ریزی و هم‌چنین حفاظت از این تسهیلات صورت گیرد. در صورت پیاده‌سازی نتایج این تحقیق، می‌توان از بسیاری از هزینه‌های ناشی از مکانیابی نادرست این تسهیلات اجتناب کرد و آسیب‌های مادی و تأثیرات روانی ناشی از عدم حفاظت مناسب از این تسهیلات در شرایط تهاجم را تا حد امکان کاهش داد.

در تحقیق حاضر، اهداف زیر دنبال می‌شوند:

(۱) مدل‌سازی مسئله مکان‌یابی تسهیلات در شرایط امکان وجود حمله به شبکه برای حالتی که بازیکنان اطلاعات کاملی از یکدیگر ندارند.

(۲) مطالعه مزایا و ریسک ناشی از عدم‌تقارن اطلاعات برای بازیکنان فعال در سطوح مختلف مسئله و بررسی تأثیر افزایش دقت تخمین پارامترها بر پیامد نهایی بازیکنان

ساختار مقاله حاضر به این صورت است که ابتدا مرور کاملی بر ادبیات موضوع ارائه می‌شود. در بخش سوم، مدل دوسطحی مناسبی برای مسئله در شرایط عدم‌تقارن اطلاعات ارائه می‌شود و در بخش چهارم الگوریتم جستجوی ممنوعه‌ای برای حل این مدل دوسطحی توسعه داده می‌شود. اعتبارسنجی الگوریتم و بررسی کارایی و اثربخشی این الگوریتم در زیربخش پنجم موردبررسی قرار می‌گیرد و مزایا و ریسک‌های ناشی از منظور کردن تأثیر عدم‌تقارن اطلاعات بر تصمیمات اتخاذ شده محاسبه می‌شود. در نهایت، نتایج حاصل از این تحقیق و شکاف‌های تحقیقاتی موجود در این حوزه ارائه می‌شود.

۲- مرور ادبیات

برنامه‌ریزی امنیتی و حفاظت از زیرساخت‌های حیاتی، انجمن تحقیق در عملیات را بر آن داشته است تا گستره وسیعی از مدل‌های حمله را طی سال‌های اخیر توسعه دهند. اصطلاح حمله به اقدامات حساب‌شده و دقیقی از تلاش برای تخریب یا آسیب‌رسانی به یک یا چند عنصر از یک زیرساخت یا سیستم خدماتی با هدف تخریب عملکرد کلی سیستم، اطلاق می‌شود. اسمیت [۱] در مقاله‌اش بیان کرده است که مدل‌ها و الگوریتم‌های حمله می‌توانند به‌طور مؤثری عناصر حیاتی شبکه را بدون نیاز به روش‌های شمارش کامل، شناسایی کنند و به‌منظور شناخت مزایای حفاظت از شبکه، با مدل‌های تقویت و حفاظت، ترکیب شوند. در این رابطه، به‌منظور پیش‌بینی سناریوی بدترین حالت با بیشترین میزان تخریب‌های ممکن در تدارک خدمات، آسیب‌پذیری‌ها از دیدگاه مهاجم شناسایی می‌شود. این تحلیل با دقت به تسهیلات خاصی که در سناریوی بدترین حالت، توسط مهاجم موردحمله قرار می‌گیرند، اشاره می‌کند. بعد از اینکه این تسهیلات شناسایی شدند، طراح سیستم می‌تواند طرح حفاظتی برای کمینه کردن بدترین تخریب‌ها و اختلال‌ها پیشنهاد دهد.

حوزه مدل‌های حمله می‌تواند به دو گروه عمده تقسیم شود: حمله به شبکه و حمله به تسهیلات. در مسائل مرتبط با دسته دوم، هدف تخریب توسط مهاجم، تسهیلات یا گره‌های عرضه‌ای هستند که به مجموعه‌ای از مشتریان، خدماتی را ارائه می‌کنند. کمان‌هایی که بین این نقاط عرضه و تقاضا ارتباط برقرار می‌کنند، موردحمله قرار نمی‌گیرند. بااین‌وجود، مسائل دسته اول، به‌طور گسترده‌تر و باسابقه طولانی‌تری موردمطالعه قرار گرفته است. اولین مدل‌ها در راستای حمله به تسهیلات، در تحقیق چارچ و همکارانش [۲] مشاهده می‌شود که در آن محققین به مطالعه تخریب‌هایی در شبکه‌های عرضه/تقاضا از نوع میانه یا پوششی پرداخته‌اند. این محققین، دو مدل از دیدگاه مهاجم را با این فرض که p تسهیل موجود به مشتریان خدمات ارائه

می‌کنند، فرمول‌بندی کرده‌اند. در مسئله میانه با r حمله، به‌دنبال بیشینه‌سازی مسافت کل وابسته به تقاضا از طریق حمله مهاجم به r تسهیل از p تسهیل است و مشتریان تسهیلات مختل‌شده باید مجدداً به‌منظور دریافت خدمات، به تسهیلات آسیب‌ندیده اختصاص داده شوند. در مسئله پوششی با r حمله، هدف مهاجم، تعیین r تسهیل از بین p تسهیل موجود است که اگر تخریب شوند، بیشترین میزان کاهش در تقاضای مشتریان پوشش داده‌شده را به همراه خواهند داشت. به‌راحتی قابل‌مشاهده است که مسئله میانه با r حمله و مسئله پوششی با r حمله به ترتیب متضاد مسائل شناخته‌شده p-میانه و بیشینه پوشش هستند. چارچ و همکارانش [۲] نیز مرور کاملی بر مدل‌های حمله‌ای که قبل از سال ۲۰۰۴ منتشر شده است، انجام دادند.

۲-۱- مروری بر مدل‌های حفاظت-حمله

برای دولت‌ها امکان حفاظت از کلیه تأسیسات مهم به‌منظور تأمین امنیت کامل آن‌ها وجود ندارد. ماری و همکارانش [۳] به محدودیت‌هایی اشاره می‌کنند که ممکن است دامنه اقدامات حفاظتی قابل پیاده‌سازی را محدود نماید. بااین‌وجود، حفاظت یا تقویت زیرمجموعه‌ای از یک زیرساخت یا سیستم خدماتی در برابر اقدامات مختل‌کننده می‌تواند جایگزین مناسبی برای طراحی مجدد کامل این سیستم به‌منظور کمینه کردن عواقب بعد از حمله باشد. اسکاپارا و چارچ [۴] اضافه کردن گارد امنیتی، فنس‌کشی و حصارکشی، دوربین‌های نظارتی و ارتباطات مخابراتی تقویت‌شده را ازجمله اقدامات حفاظتی ممکن در برابر یک مهاجم برمی‌شمارند. حفاظت می‌تواند احتمال از دست رفتن یک تسهیل یا اجزا (دارایی‌های مهم و حیاتی) شبکه را کاهش دهد و یا اینکه تا حد امکان کاملاً از تخریب آن‌ها جلوگیری نماید. دامنه وسیعی از تحقیقاتی که به بررسی این موضوع در مفاهیم شبکه و حمله به تسهیلات پرداخته‌اند را می‌توان در مقاله اسنایدر و همکارانش [۵] مشاهده کرد. این مدل‌های حفاظت-حمله (یا تقویت-حمله) حاصل، به‌منظور شناسایی دارایی‌های مهمی که حفاظت از آن‌ها عملکرد سیستم را بعد از حمله تا حد امکان حفظ می‌کند، مورداستفاده قرار می‌گیرند. میزان حفاظت یا از طریق محدودیت بودجه و یا محدودیت تعداد تسهیلاتی که می‌توانند در برابر حمله دشمن تقویت شوند، قابل‌محاسبه است.

وجود دو بازیکن در این مدل‌ها، که تحت عنوان طراح سیستم و مهاجم شناخته می‌شوند، ساختار برنامه‌ریزی دوسطحی را طلب می‌کند. نام دیگری که برای این نوع از مسائل معمولاً مورداستفاده قرار می‌گیرد، بازی استکلبرگ ایستای پیشرو-پیرو است. یک مسئله برنامه‌ریزی دوسطحی، حالت خاصی از بهینه‌سازی چندسطحی با دو سطح یا دو بخش است که یکی از آن‌ها نقش پیشرو را دارد و دیگری در نقش پیرو، بر اساس تصمیمات پیشرو، طرح‌های موردنظرش را انتخاب می‌کند. در یک مسئله حفاظت-حمله دوسطحی، تصمیمات مرتبط با حفاظت و مکان‌یابی یا طراحی شبکه در مسئله سطح بالا اتخاذ می‌شود، درحالی‌که در مسئله سطح پایین، به‌منظور تعیین تأثیر مخرب‌ترین حمله برای یک استراتژی حفاظت و مکان‌یابی یا طراحی شبکه، مدل حمله مورداستفاده قرار می‌گیرد. نمونه‌هایی از این نوع مدل‌سازی می‌تواند در مقالات زیر که به ترتیب زمانی مرتب شده‌اند، مشاهده شود:

اوهانلی و همکارانش [۶] مسئله حفاظت از مکان‌های اکولوژیک حیاتی را برای حالتی که با محدودیت بودجه جهت محافظت مواجهیم، مطالعه کردند. در این حالت، طراح سیستم تلاش می‌کند تا از مکان‌های مهم اکولوژیکی در برابر حملات دشمن که به دنبال تخریب زیرمجموعه‌ای از مکان‌های حفاظت نشده است، محافظت نماید. این محققین مدل برنامه‌ریزی دوسطحی عدد صحیحی را توسعه دادند که مبتنی بر مدل مسئله پوششی با r حمله ارائه‌شده توسط چارچ و همکارانش [۲] است و به دنبال کمینه کردن بیشترین میزان از بین رفتن گونه‌هایی است که در اثر حمله به زیرمجموعه محدودی از مکان‌های حفاظت‌نشده از بین می‌روند.

چارچ و اسکاپارا [۷] حفاظت از تسهیلات را با مدل مکان‌یابی میانه در شرایط حمله ترکیب کردند و مسئله مکان‌یابی میانه در شرایط حمله با فرض تقویت تسهیلات را موردبررسی قرار دادند. اسکاپارا و چارچ [۸] نوع دیگری از مسئله مکان‌یابی میانه با r حمله و تقویت تسهیلات را که تحت عنوان مسئله بیشینه پوشش با محدودیت‌های تقدم-تأخیر شناخته می‌شود، موردمطالعه قرار دادند. اسکاپارا و چارچ [8] مدل برنامه‌ریزی دوسطحی را برای مسئله مکان‌یابی میانه با r حمله و تقویت تسهیلات ارائه کردند و این مدل را با استفاده از الگوریتم شمارش ضمنی که بر روی یک درخت جستجو اعمال شده است، حل کردند.

اسمیت و لیم [۹] مروری جامع بر تحقیقات فزاینده انجام‌گرفته در حوزه مسائل حمله به شبکه سه مرحله‌ای را انجام دادند که در آن‌ها اپراتور شبکه، با افزایش ظرفیت‌ها، کاهش هزینه‌های جریان یا دفاع از عناصر شبکه قبل از اینکه مهاجم اقدامی صورت دهد، شبکه را تقویت می‌کند. اسکاپارا و چارچ [۴] گونه دیگری از مسئله مکان‌یابی میانه با r حمله و تقویت تسهیلات را با این فرض که تسهیلات دارای محدودیت ظرفیت هستند، موردمطالعه قرار دادند و مدل برنامه‌ریزی سه سطحی را برای این مسئله ارائه کردند. آکسن و همکارانش [۱۰] مسئله حفاظت از تسهیلات را برای یک شبکه عرضه/تقاضای از نوع میانه و برای حالتی که بودجه حفاظت محدود است و ظرفیت تسهیلات قابل‌افزایش است، حل کردند.

لوسادا و همکارانش [۱۱] حفاظت ناقص (جزئی) از تسهیلات با ظرفیت نامحدود را با فرض اینکه زمان ریکاوری تسهیلات بعد از حمله غیرصفر باشد برای شبکه خدمات از نوع میانه و در افق زمانی چند پریودی موردمطالعه قرار دادند. لیبراتور و همکارانش [۱۲] مسئله مکان‌یابی میانه با r حمله و تقویت تسهیلات را برای حالت تصادفی موردبررسی قرار دادند. کاپنرا و اسکاپارا [۱۳] مسئله حمله چند سطحی برای تعیین تخصیص بهینه منابع حفاظتی در یک شبکه کوتاه‌ترین مسیر را موردبررسی قرار دادند که به‌دنبال افزایش قابلیت اطمینان شبکه در برابر مهاجمی است که توانایی تخریب کمان‌ها و

گره‌های محافظت‌نشده شبکه را دارد. روبوردو و همکارانش [۱۴]، الگوریتم شاخه و برشی جهت حل مسئله مکانیابی میانه با r حمله و تقویت تسهیلات ارائه کردند. محمودجانلو و همکارانش [۱۵]، مدلی سه سطحی ارائه دادند که در مسئله مکانیابی میانه با r حمله، پوشش کاملی جهت حفاظت از تسهیلات ایجاد می‌کند.

خلاصه‌ای از مطالعات انجام‌گرفته در این حوزه در جدول ۱ نمایش داده شده است.

جدول (۱): مروری بر تحقیقات موجود در حوزه مسائل حفاظت-حمله

نویسنده	حفاظت		حمله		نوع اطلاعات	توضیح
	کامل	جزئی	کامل	جزئی		
او هانلی و همکارانش [۶]	×		×		اطلاعات کامل	مسئله حفاظت از مکان‌های اکولوژیکی مهم با هزینه محافظت محدود
اکسن و همکارانش [۱۰]	×		×		اطلاعات کامل	مسئله حفاظت از تسهیلات برای یک شبکه عرضه/تقاضای و برای حالتی که بودجه حفاظت محدود است و ظرفیت تسهیلات قابل‌افزایش است.
لوسادا و همکارانش [۱۱]		×	×		اطلاعات کامل	حفاظت ناقص (جزئی) از تسهیلات با ظرفیت نامحدود را با فرض اینکه زمان ریکاوری تسهیلات بعد از حمله غیرصفر باشد برای شبکه خدمات و در افق زمانی چند پریودی
کاپنرا و اسکاپارا [۱۳]	×		×		اطلاعات کامل	تعیین تخصیص بهینه منابع حفاظتی در شبکه کوتاه‌ترین مسیر به‌طوری‌که مقاوم بودن در مقابل حملات مهاجم به گره‌ها و کمان‌هایی از شبکه است که محافظت نشده است.
روبوردو و همکارانش [۱۴]	×		×		اطلاعات کامل	ارائه الگوریتم شاخه و برش جهت حل مسئله مکانیابی میانه با r حمله و تقویت تسهیلات
محمودجانلو و همکارانش [۱۵]	×		×		اطلاعات کامل	مدلی سه سطحی مسئله مکانیابی میانه با r حمله با پوشش کامل تسهیلات

۲-۲- مروری بر مدل‌های مکان‌یابی-حمله و طراحی شبکه-حمله

در این نوع از مدل‌های حمله، طراح شبکه یا سیستم (مدافع)، نقش رهبر را در بازی استکلبرگ بر عهده دارد و در مورد ساختار سیستم که ممکن است یک زیرساخت شبکه‌ای یا یک سیستم عرضه/تقاضا از نوع پوششی یا میانه باشد، تصمیم‌گیری می‌کند. مهاجم (در نقش پیرو) در تلاش است تا طرح حمله‌ای را به کار بگیرد که تا بیشترین میزان ممکن به این شبکه صدمه وارد کند. تحقیق بر روی این نوع از مدل‌های حمله، جدید و محدود است. یکی از تحقیقات صورت گرفته در زمینه طراحی شبکه-حمله، مقاله‌ای است که توسط اسمیت و همکارانش [۹] ارائه‌شده است که ساخت کمان با بودجه محدود و حمله ناقص به کمان در یک شبکه چندمحصولی را موردبررسی قرار می‌دهد. لیم و اسمیت [۱۶] لایه طراحی را به این مسئله برنامه‌ریزی دوسطحی خطی اضافه کردند. مدل حاصل، مدلی سه سطحی است که در آن ابتدا مدافع، شبکه‌ای می‌سازد که هر کمان از این شبکه، هزینه ساخت ثابت، بیشینه ظرفیت و سود واحد جریان مشخصی دارد. سپس مهاجم، مجموعه‌ای از کمان‌ها را موردحمله قرار می‌دهد و در سطح سوم، مدافع مجموعه جریان‌ها در طول شبکه باقیمانده را به‌گونه‌ای تعیین می‌کند که سود پس از حمله‌اش بیشینه شود. تابع هدف مسئله سطح بالا، ترکیب موزونی از سود جریان‌های قبل و بعد از حمله منهای هزینه‌های ساخت کمان است. نکته متمایزکننده مدل ایشان این است که توابع هدف مدافع و مهاجم یکسان نیستند. تابع هدف مدافع، ترکیب وزنی سودهای خالص قبل و بعد از حمله را شامل می‌شود، درحالی‌که مهاجم، صرفاً به‌دنبال کمینه کردن سود خالص پس از حمله است.

در حوزه شبکه‌های کوتاه‌ترین مسیر، اولین مسئله طراحی شبکه-حمله توسط برمن و گاویوس [۱۷] موردمطالعه قرار گرفت که در آن پیشرو و پیرو به ترتیب ایالت و تروریست هستند. ایالت، k مکان تسهیلات پاسخگویی اضطراری را بر روی یک شبکه شامل چند شهر تعیین می‌نماید و در مورد میزان کل منابع حفاظتی بیرون از شبکه تصمیم‌گیری می‌کند. این مقدار، احتمال موفقیت‌آمیز بودن حمله یک تروریست به یک شهر را مشخص می‌کند. هر چه این منابع بیشتر باشد، احتمال موفقیت حمله بیشتر خواهد بود. فرض می‌شود تروریست اطلاعات دقیقی در مورد مکان تسهیلات پاسخگویی انتخاب‌شده توسط ایالت را داشته باشد. به‌دنبال محاصره یک شهر توسط تروریست، منابع از نزدیک‌ترین تسهیل پاسخگویی از طریق کوتاه‌ترین مسیر در شبکه بین آن تسهیل و شهری که موردحمله قرار گرفته است، ارسال می‌شود. هدف تروریست، بیشینه کردن زیانی است که به‌صورت حاصل‌ضرب تأخیر در ارسال منابع موردنیاز و میانگین آسیب در شهر موردحمله قرار گرفته، محاسبه می‌شود. از سوی دیگر، تابع هدف ایالت، کمینه‌سازی مجموع این زیان و هزینه کل باز کردن تسهیلات پاسخگویی و نصب منابع حفاظتی است. این مسئله، در ابتدا برای حالتی با یک تسهیل پاسخگویی (k=1) و سپس برای چند تسهیل حل می‌شود. در مقاله دیگری، برمن و همکارانش [۱۸] این فرض را که تروریست اطلاعات کاملی درباره مکان تسهیلات دارد را از مدل حذف کردند. این موضوع به یک بازی حرکت همزمان بین دو بازیکن منجر می‌شود که تعادل نش آن با استفاده از روش‌های عددی قابل‌محاسبه است. به دلیل دشواری بازی حاصل، جواب‌ها تنها برای حالت k=1 قابل حصول است.

در حوزه مسائل مکان‌یابی-حمله، تنها دو مقاله چاپ شده در ادبیات موضوع موجود است. اولین مقاله، کاری است که توسط اوهانلی و چارچ [۶] ارائه شده است و یک سیستم عرضه/تقاضا از نوع بیشترین پوشش را بررسی می‌کند. مدافع در این سیستم باید در مورد انتخاب مکان حداکثر p تسهیل از بین مجموعه‌ای از مکان‌های کاندید که در معرض حمله توسط یک مهاجم هوشمند هستند، تصمیم‌گیری نماید. این مدل دوسطحی که از مدل بیشترین پوشش الهام گرفته است، برای اولین بار توسط چارچ و ریول [۱۹] معرفی شد. این محققین مدل بیشترین پوشش را با مکانیابی پوششی با r حمله، ترکیب کردند و در این مسئله، مکان‌های تسهیلات با پیش‌بینی اثر این مکان‌ها بر مخرب‌ترین الگوی حمله به‌کارگرفته‌شده توسط مهاجم، تعیین می‌شوند. به این شیوه، چیدمان قبل از حمله‌ای برای مکان تسهیلات می‌تواند حاصل شود که نسبت به بدترین زیان‌های وارد شده از سوی مهاجم، دارای قابلیت اطمینان بیشتری است. این مسئله حاصل، مسئله حمله- مکان‌یابی بیشترین پوشش نامیده می‌شود و به‌صورت یک برنامه عدد صحیح آمیخته دوسطحی فرموله می‌شود. الگوریتم دوسطحی مبتنی بر روش‌های تجزیه برای برنامه عدد صحیح آمیخته دوسطحی به کار گرفته شده است که طی آن، مسئله اولیه به دو مسئله مجزا از هم، یعنی مسئله سطح بالا (به‌عنوان مسئله اصلی) و مسئله سطح پایین (به‌عنوان زیرمساله)، شکسته می‌شود و این دو مسئله به‌صورت متوالی حل می‌شوند. دومین تحقیقی که به مطالعه مسئله مکان‌یابی-حمله پرداخته، توسط برمن و همکارانش [۲۰] انجام گرفته است. این محققین یک مسئله p-میانه بیشینه پوشش دفاعی تحت شرایط حمله به یک کمان را موردبررسی قرار داده‌اند. این مهاجم، به‌منظور اینکه بتواند تا حدامکان پوشش مشتریان را کاهش دهد، با دقت یکی از کمان‌های شبکه را قطع می‌کند. این مدافع، از سوی دیگر، در تلاش است تا پس از تخریب این کمان، پوشش مشتریان را بیشینه نماید. در این تحقیق، به‌جای استفاده از یک مدل برنامه‌ریزی دوسطحی، مسائل پیشرو و پیرو به‌طور متوالی و با استفاده از سه الگوریتم فراابتکاری حل می‌شود.

خلاصه‌ای از مطالعات انجام‌گرفته در این حوزه در جدول ۲ نمایش داده شده است.

جدول (۲): مروری بر تحقیقات انجام گرفته در حوزه مسائل مکانیابی-حمله

نویسنده	مکانیابی و طراحی شبکه			حمله		نوع اطلاعات	توضیح
	طراحی شبکه	میانه	پوششی	کامل	جزئی		
برمن و گاویوس [۱۷]	×			×		اطلاعات کامل	اولین مسئله طراحی شبکه-حمله، در حوزه شبکه‌های کوتاه‌ترین مسیر
برمن و همکارانش [۱۸]	×			×		اطلاعات ناقص مهاجم	به دلیل دشواری بازی همزمان حاصل، جواب‌ها تنها برای حالت تک تسهیلی قابل حصول است.
اوهانلی و چارچ [۶]			×	×		اطلاعات کامل	حمله به یک سیستم عرضه/تقاضا از نوع بیشترین پوشش
برمن و همکارانش [۲۰]			×	×		اطلاعات کامل	استفاده از سه الگوریتم فراابتکاری حل به‌جای استفاده از مدل دوسطحی

۳-۲- مسئله مکان‌یابی-حفاظت و حمله

بازی مدافع-مهاجم که به بررسی مسائل مکان‌یابی-حمله و حفاظت از تسهیلات می‌پردازد، در سه مقاله قابل‌مشاهده است: (۱) آکسن و همکارانش [۱۰] برای یک مسئله p-میانه، (۲) آکسن و آراس [۲۱] برای یک مسئله مکان‌یابی تسهیلات با شارژ ثابت و (۳) کئی آیسی و همکاران [۲۲] برای یک مسئله شبکه خدمات از نوع بیشینه پوشش برای تسهیلات با شارژ ثابت.

در دو مقاله اول، لازم است مدافع، در مورد میزان ظرفیت اولیه و میزان افزایش ظرفیت موردنیاز پس از حمله در تسهیلات، به‌منظور برآوردن تقاضای کل مشتریان در زمان به‌کارگیری بدترین طرح حمله از سوی مهاجم ، تصمیم‌گیری نماید. می‌توان گفت که تصمیمات مکان‌یابی تسهیلات مدافع، لایه‌ای به مسئله حمله-حفاظتی که توسط آکسن و همکارانش [۱۰] ارائه شده است، اضافه می‌کند. در هر سه این مقالات، تصمیمات مرتبط با حمله و حفاظت از تسهیلات بر پایه همه یا هیچ اتخاذ می‌شود. این موضوع به این معنی است که نه برای حمله و نه حفاظت، فرض امکان حمله یا حفاظت جزئی منظور نشده است. درحالی‌که آکسن و همکارانش [۱۰] و کئی آیسی و همکارانش [۲۲]، محدودیت بودجه‌ای برای هزینه‌های حفاظت از تسهیلات لحاظ کرده‌اند، آکسن و آراس [۲۱] این محدودیت را، مستقیماً در تابع هدف مدافع در مسئله سطح بالا اضافه کرده‌اند.

اکبری جعفرآبادی و همکاران [۲۳]، مسئله مکانیابی میانه با r حمله سه سطحی را مطالعه کردند. اخیراً ژانگ و همکارانش [۲۴] مسئله مکانیابی میانه با r حمله با تقویت زنجیره تأمین غیرمتمرکز را موردبررسی قرار دادند. فتح‌الهی‌فرد و حاجی‌آقائی کشتلی [۲۵]، مسئله دوسطحی دوهدفه‌ای برای حمله جزئی با در نظر گرفتن سیستم‌های دفاعی متفاوت را فرموله کردند.

علی اکبریان و همکارانش [۲۶]، برای اولین بار مسئله مکانیابی تحت شرایط حمله را روی سیستم‌های سلسله مراتبی موردمطالعه قرار دادند. هدف این مسئله این است که به‌منظور کاهش اثرات تخریب، تسهیلات بحرانی سیستم‌های خدماتی تقویت شوند. تسهیلات تقویت‌شده در برابر حمله آسیب‌پذیر نیستند. اخیراً فرقانی و همکاران [۲۷] مسئله مکانیابی میانه سلسله مراتبی را با فرضیات متفاوتی

موردمطالعه قرار دادند. در مقاله اول، در هر سطح از سیستم تعداد مشخصی از تسهیلات موردحمله قرار می‌گیرد درصورتی‌که در مقاله دوم، بر اساس محدودیت بودجه، تسهیلات سطوح مختلف موردحمله جزئی قرار می‌گیرند. علاوه بر این در مقاله اول، جهت حفاظت از تسهیلات، در فاز طراحی سیستم، تسهیلات تقویت می‌شوند درصورتی‌که در دومین مقاله، تقاضای مشتریان از طریق دو استراتژی برونسپاری و تخصیص مجدد برآورده می‌شود.

خلاصه‌ای از مطالعات انجام‌گرفته در این حوزه و شکاف تحقیقاتی موجود، در جدول ۳ نمایش داده شده است.

جدول (۳): مروری بر تحقیقات موجود در زمینه مکانیابی-حفاظت-حمله

مقالات	مکانیابی		حفاظت		حمله		اطلاعات	
	میانه	پوششی	کامل	جزئی	کامل	جزئی	نامتقارن	متقارن
اسکاپارا و چارچ [۸]	×		×		×			×
اسکاپارا و چارچ [۴]	×		×		×			×
کئی آیسی و همکارانش [۲۲]		×	×		×			×
اکسن و همکارانش [۱۰]	×		×		×			×
اکسن و اراس [۲۱]	×		×		×			×
بریچا و نورلفاث [۲۸-۳۰]	×		×		×			×
لی براتور [۱۲]	×		×		×			×
تحقیق حاضر		×	×			×	×	

مقالات	اطلاعات	
	نامتقارن	متقارن
اسکاپارا و چارچ [۸]		× مسئله مکان‌یابی میانه با r حمله و تقویت تسهیلات
اسکاپارا و چارچ [۴]		× توسعه مسئله مکان‌یابی میانه با r حمله و تقویت تسهیلات با فرض محدودیت ظرفیت برای تسهیلات
کئی آیسی و همکارانش [۲۲]		× شبکه با حداکثر پوشش با شارژ ثابت
اکسن و همکارانش [۱۰]		× بررسی مسائل p-میانه
اکسن و اراس [۲۱]		× با شارژ ثابت
بریچا و نورلفاث [۲۸-۳۰]		×
لی براتور [۱۲]		× مسئله مکان‌یابی میانه با r حمله و تقویت تسهیلات برای حالت تصادفی
تحقیق حاضر	×	

همان‌طور که مشاهده می‌شود، فرض عدم‌تقارن اطلاعات در بازی‌های استکلبرگ موردمطالعه قرار گرفته در مسئله موردبررسی تا کنون لحاظ نشده است. نوآوری‌های مسئله موردمطالعه نسبت به تحقیقات پیشین عبارتند از:

(۱) در این تحقیق فرض عدم‌تقارن اطلاعات بین مهاجم و مدافع موردبررسی قرار گرفته است و

(۲) حمله از نوع جزئی است.

به‌منظور مطالعه مسئله مذکور، در زیربخش بعدی، مدل برنامه‌ریزی دوسطحی ارائه می‌شود.

۳- مدل دوسطحی برای مسئله مکان‌یابی –حفاظت– حمله برای شبکه‌های از نوع پوششی

در تعریف این مسئله فرض شده است که تعداد $|J_1|$ تسهیل عملیاتی به مشتریانی با تقاضای d_i که در $|I|$ منطقه مختلف مستقر شده‌اند،سرویس‌دهی می‌کنند. ازآنجایی‌که مهاجم به دنبال حداقل کردن میزان پوشش سرویس با تعداد r حمله به تسهیلات محافظت نشده می‌باشد، طراح سیستم به‌دنبال بیشینه کردن میزان پوشش خدمات پس از حمله از طریق پیاده‌سازی یک یا تعداد بیشتری از اقدامات زیر است:

۱- مکان‌یابی مجدد تسهیلات موجود

۲- استقرار تسهیلات جدید در تعدادی از $|J_2|$ مکان کاندید و

۳- حفاظت از برخی تسهیلات موجود و جدید که آن‌ها را در مقابل هر نوع حمله‌ای شکست‌ناپذیر می‌کند.

۳-۱. مفروضات تحقیق

(۱) مسئله در شرایط قطعی موردمطالعه قرار گرفته است. به این معنا که کلیه پارامترهای مربوط به مسئله در زمان تصمیم‌گیری، مشخص و در طول دوره تصمیم‌گیری مقادیر آن‌ها ثابت است.

(۲) حمله از نوع جزئی است. یعنی متناسب با میزان بودجه، تسهیلات موردحمله قرار می‌گیرند و میزان تخریب تسهیلی که موردحمله قرار گرفته است می‌تواند بین ۰ و صددرصد باشد.

(۳) حفاظت از نوع باینری است. یعنی یا از تسهیلی حفاظت نمی‌شود و یا اگر حفاظت شد، موردحمله قرار نمی‌گیرد.

(۴) تصمیم‌گیری بین بازیکنان با اطلاعات کامل انجام نمی‌گیرد. یعنی دو بازیکن در هنگام تصمیم‌گیری درک یکسانی از اطلاعات یکدیگر ندارند.

(۵) تصمیم‌گیری بین دو بازیکن فقط در یک مرحله انجام می‌گیرد و بازی انجام شده، پویا نیست.

(۶) مکانیابی از نوع پوششی است. به این معنی که طراح سیستم به‌دنبال یافتن مکان‌هایی برای تسهیلات زیربنایی موردنظر است که بیشترین میزان پوشش خدمات برای مشتریان را به همراه داشته باشد.

(۷) پوشش موردبررسی از نوع پوشش جزئی است.

پوشش خدمات را می‌توان با استفاده از مفهوم پوشش تدریجی که در تحقیق برمن و همکاران [۳۱] معرفی شده است، مدل‌سازی کرد، که در آن پوشش یک منطقه مشتری، کامل است تنها درصورتی‌که فاصله بین منطقه این مشتری و یکی از تسهیلات، از حد پایین R_1 کوچک‌تر باشد و هنگامی‌که این فاصله از حد بالای $R_2 > R_1$ بزرگ‌تر

می‌شود، میزان پوشش به‌تدریج به مقدار صفر کاهش می‌یابد. همان‌طور که در مقاله برمن و همکاران [۳۱] اشاره شده است، ایده پوشش تدریجی می‌تواند برخلاف ایده "همه یا هیچ" که در مدل بیشینه پوشش کلاسیک توسط چارچ و ریول [۱۲] ارائه شده است، تقریب خوبی در برخی از کاربردهای زندگی واقعی باشد. بر اساس این مدل، زمانی که فاصله کوچک‌تر یا مساوی با مقدار آستانه R است، پوشش کامل است و ناگهان افت می‌کند و در صفر باقی می‌ماند. در مدل حاضر، تابع نزولی خطی بین R_1 و R_2 در نظر گرفته شده است که در آن سطح پوشش جزئی خدمات (a_{ij})، برای زمانی که فاصله بین منطقه مشتری i و تسهیل قرارگرفته در مکان j برابر با c_{ij} است، به‌صورت زیر محاسبه می‌شود:

$$a_{ij} = \begin{cases} 1, & c_{ij} \le R_1 \\ \dfrac{R_2 - c_{ij}}{R_2 - R_1}, & R_1 \le c_{ij} \le R_2 \\ 0, & c_{ij} > R_2 \end{cases}$$

فرض می‌شود زمانی‌که یک منطقه مشتری، توسط چندین تسهیل به‌صورت جزئی، تحت پوشش قرار می‌گیرد، پوشش نهایی می‌تواند با در نظر گرفتن حداکثر مقدار پوشش جزئی هر تسهیل به‌دست آید. این به این معنی است، زمانی که R_1 و R_2 برای هر تسهیل یکسان هستند، پوشش حاصل از طریق نزدیک‌ترین تسهیل به یک منطقه مشتری به‌دست می‌آید.

ازآنجاکه طراح سیستم، تصمیمات خود را با پیش‌بینی تصمیم مهاجم در مورد تخریب برخی از تسهیلات اتخاذ می‌کند، لذا این وضعیت می‌تواند با یک مدل برنامه‌ریزی دوسطحی فرموله شود. مسئله سطح بالا به طراح سیستم متعلق می‌باشد که نقش رهبر بازی را بر عهده دارد، درحالی‌که مسئله سطح پایین به مهاجمی متعلق است که نقش پیرو را دارد. قبل از ارائه مدل برنامه‌ریزی دوسطحی، پارامترهای استفاده‌شده در مدل را معرفی می‌کنیم:

شاخص مجموعه‌ها:

I: مجموعه مناطق مشتریان

J_1: مجموعه‌ای از مکان‌های موجود

J_2: مجموعه‌ای از مکان‌های کاندید

$J = J_1 \cup J_2$: مجموعه مکان‌های موجود و کاندید برای تسهیلات

پارامترها:

d_i: تقاضای مشتری منطقه $i \in I$

g_{jk}: هزینه تغییر مکان یک تسهیل از مکان $j \in J_1$ به مکان $k \in J_2$

f_j: هزینه باز کردن تسهیل جدید در مکان $j \in J_2$

h_j: هزینه حفاظت از تسهیلات جدید یا موجود در مکان j

b: بودجه در دسترس برای طراح سیستم

r: بیشترین تعداد تسهیلاتی که مهاجم می‌تواند به آن حمله کند.

a_{ij}: برداشت طراح سیستم از میزان پوشش جزئی منطقه مشتری $i \in I$ توسط تسهیل قرارگرفته در مکان $j \in J_1$

$\bar{a}_{ij}$: برداشت مهاجم از میزان پوشش جزئی منطقه مشتری $i \in I$ توسط تسهیل قرارگرفته در مکان $j \in J_1$

متغیرهای تصمیم‌گیری:

Y_j: اگر تسهیلی در مکان $j \in J_1$ قرارگرفته باشد، مقدار یک و در غیر این صورت، مقدار صفر می‌گیرد.

X_{jk}: اگر تسهیل موجود در مکان $j \in J_1$ به مکان $j \in J_2$ منتقل شود، مقدار یک و در غیر این صورت، مقدار صفر می‌گیرد.

S_j: تسهیل واقع در مکان $j \in J_1$ توسط مهاجم، بین صفر تا صددرصد تخریب می‌شود.

P_j: اگر تسهیل واقع در مکان $j \in J_1$ حفاظت شود، مقدار یک و در غیر این صورت، مقدار صفر می‌گیرد.

V_i: کسری از تقاضای منطقه مشتری iام بعد از حمله

$\bar{V}_i$: برداشت مهاجم از کسری از تقاضای منطقه مشتری iام بعد از حمله

در این مدل، بازیکن سطح پایین با توجه به برداشت خود از پارامترهای میزان پوشش جزئی، درصد تقاضای پوشش داده شده از هر مشتری توسط طراح سیستم را در قالب مقادیر $\bar{V}_i$ تخمین می‌زند و از سوی دیگر، طراح سیستم با توجه به اطلاعات دقیقی که از این پارامتر دارد مقادیر دقیق V_i را به دست می‌آورد. این تفاوت سطح اطلاعات بین دو بازیکن باعث می‌شود که دو بازیکن به نتایج متفاوتی دست یابند. با توجه به اینکه فرض می‌شود، طراح سیستم علاوه بر مقادیر دقیق پارامتر میزان پوشش جزئی، از مقادیر تخمینی پارامتر مذکور توسط مهاجم به سیستم اطلاعات کاملی دارد، سعی در انتخاب بهترین محل‌های ممکن برای تسهیلات و میزان پوشش هر تسهیل دارد.

به یاد داشته باشید که اگر تسهیل موجودی در مکان $j \in J_1$ قرار گرفته باشد و یا تسهیل جدیدی در منطقه $j \in J_2$ افتتاح شود و یا تسهیل موجودی به مکان $j \in J_2$ منتقل شود، آنگاه $Y_j = 1$ می‌شود. مدل دوسطحی مربوط به مسئله پوششی مکان‌یابی_حفاظت_حمله به‌صورت زیر توصیف می‌شود:

$$\max_{X,Y,P} Z_{sys} = \sum_{i \in I} d_i V_i \qquad (۰)$$

$$(۱)$$

$s.t.$

$$a_{ij}(Y_j - S_j) \le V_i, \qquad i \in I, j \in J$$

$$(1 - Y_j) = \sum_{k \in J_2} X_{jk}, \qquad j \in J_1 \qquad (۲)$$

$$\sum_{j \in J_1} X_{jk} \le Y_k, \qquad k \in J_2 \qquad (۳)$$

$$\sum_{j \in J_2} f_j (Y_j - \sum_{k \in J_1} X_{kj}) + \sum_{j \in J_1} \sum_{k \in J_2} g_{jk} X_{jk} + \sum_{j \in J} h_j P_j \le b \qquad (۴)$$

$$P_j \le Y_j, \qquad j \in J \qquad (۵)$$

$$P_j, Y_j \in \{0,1\},\ 0 \le V_i \le 1, \qquad i \in I, j \in J \qquad (۶)$$

$$X_{jk} \in \{0,1\}, \qquad j \in J_1, k \in J_2 \qquad (۷)$$

$$\min_{S,V} Z_{att} = \sum_{i \in I} d_i \bar{V}_i \qquad (۸)$$

$$(۹)$$

$s.t.$

$$\bar{a}_{ij}(Y_j - S_j) \le \bar{V}_i, \qquad i \in I, j \in J$$

$$S_j \le Y_j - P_j, \qquad j \in J \qquad (۱۰)$$

$$\sum_{j \in J} S_j \le r \qquad (۱۱)$$

$$0 \le \bar{\bar{V}}_i \le 1, \qquad i \in I \qquad (۱۲)$$

$$0 \le S_j \le 1, \qquad j \in J \qquad (۱۳)$$

در مدل بالا، روابط (۰) تا (۷) مسئله سطح بالا مربوط به طراح سیستم و روابط (۸) تا (۱۳) مسئله سطح پایین مربوط به مهاجم را می‌سازند. در مسئله سطح بالا، تابع هدف (۰) به دنبال بیشینه کردن پوشش کل خدماتی پس از حمله است. محدودیت‌های (۲) و (۳)، رابطه بین متغیر مکان Y_j و متغیر تغییر مکان X_{jk} را نشان می‌دهد. به‌ویژه، اولین مجموعه محدودیت‌ها تضمین می‌کند که اگر یک تسهیل از مکان $j \in J_1$ به مکان دیگری نظیر $k \in J_2$ نقل‌مکان کند، آنگاه، متغیر مکان Y_j مقدار صفر می‌گیرد. مجموعه محدودیت‌های دوم بیان می‌کند که اگر تسهیلی به مکان $k \in J_2$ نقل‌مکان کند، آنگاه $Y_k = 1$ خواهد شد. توجه داشته باشید که این محدودیت‌ها در صورتی معتبر هستند که هیچ تسهیلی به مکان $k \in J_2$ نقل‌مکان نکند (یعنی سمت چپ رابطه، صفر است) و هیچ تسهیل جدیدی در سایت $k \in J_2$ افتتاح نشود (یعنی سمت راست آن یک باشد). محدودیت (۴) اطمینان حاصل می‌کند که هزینه کل طراح سیستم از بودجه در دسترس تجاوز نکند. اولین عبارت در قسمت چپ این نامساوی نشان‌دهنده هزینه افتتاح تسهیل جدید است درحالی‌که عبارات دوم و سوم، به‌ترتیب نشان‌دهنده هزینه‌های نقل‌مکان و حفاظت می‌باشند. محدودیت (۵) نشان می‌دهد که اگر تسهیلی افتتاح نشده باشد، حفاظت نمی‌شود. محدودیت‌های باینری بر متغیرهای مکان Y_j و متغیرهای حفاظتی P_j در محدودیت (۶) و بر متغیر نقل‌مکان X_{jk} در محدودیت (۷) اعمال شده‌اند.

در مدل سطح پایین، تابع هدف (۸) مشابه تابع هدف طراح سیستم است، اما مفهوم بهینه‌سازی کاملاً مخالف است. در واقع مهاجم قصد دارد میزان پوشش سرویس‌دهی پس از حمله را تا حد امکان کاهش دهد. محدودیت‌های (۹) تضمین می‌کنند که هر منطقه مشتری با نزدیک‌ترین تسهیلی که موردحمله توسط مهاجم قرار نگرفته است، پوشش داده می‌شود. توجه داشته باشید که اگر منطقه مشتری i بتواند توسط تسهیلات متعددی سرویس دریافت نماید، پوشش نهایی که با متغیر V_i نمایش داده می‌شود، برابر با حداکثر پوشش جزئی آن تسهیل قرار داده می‌شود. به‌عبارت‌دیگر، این منطقه مشتری از نزدیک‌ترین تسهیل خدمت دریافت می‌کند. محدودیت‌های (۱۰)، شرایط منطقی هستند که از حمله مهاجم نه‌تنها به تسهیلاتی که اصلاً وجود ندارند یا به مکان دیگری منتقل شده‌اند، بلکه هم‌چنین به تسهیلاتی که موردحفاظت طراح سیستم می‌باشند، جلوگیری می‌کند. محدودیت (۱۱) بیان می‌کند که مهاجم، حداکثر به r تسهیل می‌تواند حمله کند. محدودیت‌های (۱۲) و (۱۳) تضمین می‌کنند که متغیرهای پوشش V_i و *متغیرهای حمله* S_j بین صفر و یک مقدار می‌گیرند و حمله از نوع جزئی است.

به تعداد $2|J| + |J_1||J_2|$ متغیر باینری و $2|J| + 1$ محدودیت در سطح بالای مدل دوسطحی که در بالا معرفی شد و در مسئله سطح پایین به تعداد $|I| + |J|$ متغیر پیوسته و $(|I| + 1)|J| + |I| + 1$ محدودیت دارد.

۴- روش‌های پیشنهادی برای حل مدل دوسطحی

۴-۱- روش کروش-کان-تاکر

سینها و همکارانش [۳۲] مروری بر کلیه روش‌های حل مسائل برنامه‌ریزی دوسطحی انجام داده‌اند. بر اساس تحقیقی که ایشان انجام داده‌اند، در شرایطی که مسئله سطح پایین، مسئله‌ای محدب باشد، می‌توان با استفاده از شرایط کروش-کان-تاکر، مسئله دوسطحی را به یک مسئله تک‌سطحی تبدیل کرد. در این روش، با به دست آوردن شرایط کروش-کان-تاکر مربوط به مسئله بهینه‌سازی سطح پایین و اضافه کردن این شرایط به‌عنوان محدودیت به مسئله سطح بالا، به یک مسئله برنامه‌ریزی تک‌سطحی دست می‌یابیم که می‌توان از کلیه الگوریتم‌های بهینه‌سازی موجود در ادبیات، برای حل این مسئله استفاده کرد. مسئله بیشینه‌سازی زیر را در نظر بگیرید:

$$Max\ Z = f(x_1, x_2, \dots, x_n) \qquad (۱۴)$$

$$s.t.\ \ g_i(x_i) \le b_i, \qquad \forall\, i = 1, \dots m \qquad (۱۵)$$

شرایط کروش-کان-تاکر مربوط به این مسئله عبارتست از:

$$\nabla f(x) = \sum_{i=1}^{m} \lambda_i \times \nabla g_i(x_i) \qquad (۱۶)$$

$$[\lambda_i \times (\nabla g_i(x_i) - b_i)] = 0 \qquad \forall\, i = 1, \dots m \qquad (۱۷)$$

$$g_i(x_i) - b_i \le 0 \qquad \forall\, i = 1, \dots m \qquad (۱۸)$$

$$\lambda_i \ge 0 \qquad \forall\, i = 1, \dots m \qquad (۱۹)$$

با توجه به محدب بودن مسئله سطح پایین، می‌توان این محدودیت‌ها را به مسئله سطح بالا اضافه کرد. با جایگزینی مسئله سطح پایین با شرایط کروش-کان-تاکر، تعدادی محدودیت غیرخطی به مدل اضافه خواهد شد.

مسئله تک‌سطحی حاصل در نرم‌افزار گمز کدنویسی شده و با استفاده از سالور سیپلکس، مسائل نمونه حل شده است. هفت دسته مسئله با تعداد متفاوتی از نقاط تقاضا، تعداد مکان‌های موجود برای تسهیل و تعداد مکان‌های جدید برای تسهیلات بحرانی به‌صورت تصادفی تولید شده‌اند. میزان تقاضای پوشش داده شده بعد از حمله به شبکه از دیدگاه طراح سیستم و مهاجم به سیستم در جدول ۴ نمایش داده شده است.

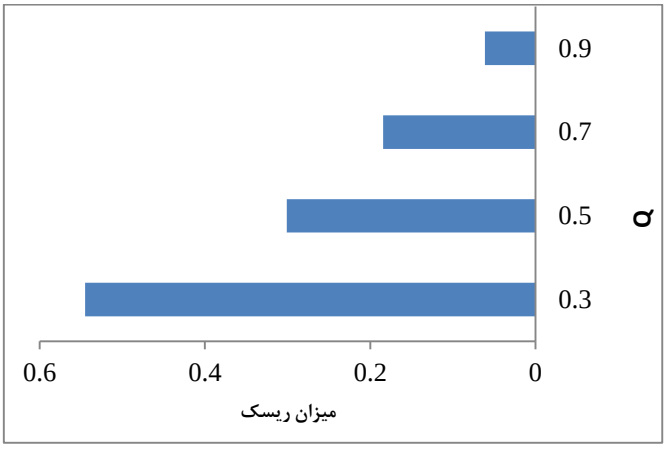
در این جدول مسئله به ازاء مقادیر متفاوت Q محاسبه شده است. Q، درصد دقتی است که براساس آن، مهاجم پارامترهای مربوط به طراح سیستم را تخمین می‌زند.

جدول (۴): مقادیر پوشش نقاط تقاضا از دیدگاه طراح سیستم و مهاجم در شرایط عدم‌تقارن اطلاعات

$\|I\|-\|J_1\|-\|J_2\|$	Q=0.3		Q=0.5		Q=0.7		Q=0.9	
	از دیدگاه مهاجم	از دیدگاه طراح سیستم	از دیدگاه مهاجم	از دیدگاه طراح سیستم	از دیدگاه مهاجم	از دیدگاه طراح سیستم	از دیدگاه مهاجم	از دیدگاه طراح سیستم
۱۰-۴-۲	۱۷۱۷۲,۳	۱۷۱۷۲,۳	۲۸۶۲۰	۲۸۶۲۰,۶	۴۰۰۶۸,۹	۴۰۰۶۸,۹	۵۱۵۱۷,۳	۶۴۳۷۹
۱۵-۴-۲	۱۷۵۰۳,۷	۲۵۶۱۷,۷	۲۹۱۷۲,۸	۴۲۶۹۶,۶	۴۰۸۴۲	۵۹۷۷۴,۸	۵۲۵۱۱,۱	۷۶۸۵۳,۳
۲۰-۷-۳	۴۷۲۶۴	۵۰۲۶۰	۷۸۷۷۳,۸	۸۲۵۶۰	۱۱۰۲۸۲	۱۱۰۲۸۲,۸	۱۴۱۷۹۲,۲	۱۱۰۲۸۲,۸
۲۵-۷-۳	۵۸۶۲۷	۶۲۶۶۷	۹۷۷۱۲,۹	۱۰۴۴۴۵,۱	۱۳۶۷۹۸,۱	۱۴۶۲۲۳,۱	۱۷۵۸۸۳,۳	۱۷۵۸۸۳,۲
۳۰-۷-۳	۷۱۱۱۴,۱	۷۱۱۴	۱۱۸۵۲۳,۵	۱۱۸۵۲۳,۵	۱۶۵۹۳۲,۹	۱۶۵۹۳۲,۱	۲۱۳۳۴۲,۳	۲۱۳۳۴۲,۳
۳۰-۱۰-۵	۷۹۷۲۸,۲	۷۹۷۲۸,۱	۱۳۲۸۸۰,۲	۱۳۲۸۸۰,۳	۱۸۶۰۳۲,۳	۱۸۶۰۳۲,۳	۲۳۹۱۸۴,۴	۱۸۶۰۳۲,۳
۵۰-۱۵-۷	۱۴۵۶۲۵,۵	۱۴۵۶۲۵,۵	۲۴۲۷۰۳	۲۴۲۷۰۳,۹	۳۳۹۷۹۳	۳۳۹۷۹۳	۴۳۶۸۷۶,۶	۴۳۶۸۷۶,۶

۴-۲- بررسی مزایا و ریسک مدل‌سازی مسئله با اطلاعات نامتقارن در مقایسه با اطلاعات متقارن

میزان ریسک ناشی از تصمیم‌گیری نادرست در شرایط در اختیار نداشتن اطلاعات کافی از پارامترهای مسئله توسط مهاجم در شکل ۱ نمایش داده شده است. همان‌طور که در این شکل قابل‌مشاهده است، به هر میزان مهاجم، دقت کمتری در تخمین اطلاعات به خرج دهد، ریسک تصمیم‌گیری نادرست به میزان بیشتر افزایش خواهد یافت. این موضوع، اهمیت در اختیار داشتن اطلاعات صحیح و دقیق حین تصمیم‌گیری توسط مهاجم را تأیید می‌کند.



شکل (۱): میزان ریسک تصمیم‌گیری ناشی از در اختیار نداشتن اطلاعات

در شرایطی که مهاجم اطلاعات کاملی از میزان پوشش جزئی نقاط تقاضا توسط هر یک از تسهیلات مستقرشده در اختیار ندارد، بی‌توجهی به این موضوع از سوی طراح سیستم می‌تواند منجر به اتخاذ تصمیمات غیربهینه از سوی طراح سیستم در زمینه انتخاب مکان مناسب برای تسهیلات بحرانی و سطح حفاظت بهینه برای هر یک از این تسهیلات شود. لذا در نظر گرفتن عدم‌تقارن اطلاعات از سوی طراح سیستم می‌تواند مزایایی به همراه داشته باشد که با I% نشان داده می‌شود. I%، درصد تغییر در میزان تابع هدف سطح بالا در شرایطی است که عدم‌تقارن اطلاعات منظور می‌شود و به‌صورت زیر محاسبه می‌شود: مسئله سطح بالا با استفاده از مقادیر d_i حل می‌شود. این به این معناست که طراح سیستم، با این فرض که مهاجم نیز همین اطلاعات را در اختیار دارد، در مورد مکان تسهیلات و میزان حفاظت از هر تسهیل در حالت بهینه برنامه‌ریزی می‌کند. سپس مهاجم، با استفاده از مقادیر تخمینی $\bar{d}_i$، تسهیلاتی را موردحمله قرار می‌دهد که امکان خدمات‌رسانی به نقاط تقاضا توسط طراح سیستم را حتی‌الامکان کاهش دهد. در نهایت، میزان پوشش واقعی نقاط تقاضا بعد از حمله، توسط تسهیلات با استفاده از مقادیر واقعی d_i محاسبه می‌شود. این مقدار، میزان پوشش واقعی نقاط تقاضا را در شرایطی که مهاجم هیچ‌گونه عدم‌تقارن اطلاعاتی را در نظر نگیرد، در اختیار ما قرار می‌دهد. این مقدار را با $z_{u,1}$ نشان می‌دهیم.

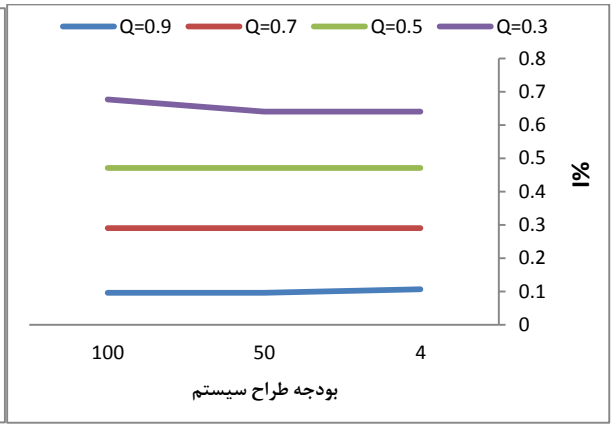
$z_{u,2}$ نیز بهترین مقدار تابع هدف حاصل برای مسئله سطح بالا با در نظر گرفتن فرض عدم‌تقارن اطلاعات برای مسئله است. بر اساس توضیحات ارائه‌شده داریم:

$$\%I = \left|\frac{z_{u,2}-z_{u,1}}{z_{u,1}}\right| \times 100 \qquad (۲۰)$$

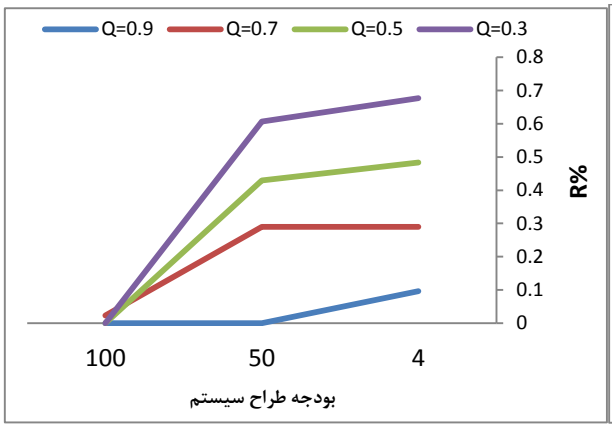
از سوی دیگر، در طول مدل‌سازی مسئله، فرض شد طراح سیستم، از مقادیر تخمین‌زده شده توسط مهاجم برای پوشش جزئی، یعنی $\bar{d}_i$، اطلاعات دقیقی در اختیار دارد (Q'=1). Q'، درصد دقتی است که طراح سیستم از مقادیر تخمین‌زده‌شده توسط مهاجم در اختیار دارد.در دنیای واقع ممکن است این فرض صحیح نباشد و طراح سیستم نیز براساس تخمین‌های نادرستی از مهاجم تصمیم‌گیری نماید. در این صورت، این کمبود اطلاعات منجر به ریسک در تصمیم‌گیری برای طراح سیستم خواهد شد که با $\%R$ نشان داده می‌شود و به‌صورت زیر محاسبه می‌شود: در ابتدا فرض می‌کنیم، طراح سیستم با دقتی کمتر از ۱۰۰٪، می‌تواند پیش‌بینی‌های مهاجم از میزان پوشش جزئی نقاط تقاضا توسط هر تسهیل را حدس بزند. در این حالت، مسئله سطح بالا حل می‌شود و مکان‌های مناسب برای تسهیلات و میزان حفاظت بهینه برای هر یک از تسهیلات به‌دست می‌آید. سپس طرح بهینه حمله به تسهیلات با استفاده از d_i تعیین می‌شود. فرض کنید میزان پوشش نقاط تقاضا توسط تسهیلات در این شرایط، $Z_{u,3}$ باشد. حال با این فرض که طراح سیستم از مقادیر پارامترهای تخمین‌زده شده توسط مهاجم کاملاً اطلاع دارد، مجدداً مسئله را حل می‌کنیم و مقدار بهینه تابع هدف برای مسئله سطح بالا در این حالت را با $z_{u,4}$ نمایش می‌دهیم. با این توضیحات، مقدار $\%R$ با استفاده از رابطه زیر محاسبه می‌شود:

$$\%R = \left|\frac{z_{u,4}-z_{u,3}}{z_{u,4}}\right| \times 100 \qquad (۲۱)$$

شکل‌های ۲ و ۳، مزایا و ریسک‌های حاصل از یکی از مسائل نمونه را برای مسئله موردمطالعه، به ازاء مقادیر متفاوت بودجه و دقت تخمین پارامترهای طراح سیستم توسط مهاجم نمایش می‌دهد.



شکل (۳): مزایای در نظر گرفتن فرض عدم تقارن اطلاعات



شکل (۲): ریسک در نظر گرفتن فرض عدم تقارن اطلاعات

مشاهده می‌شود که مسئله با اطلاعات نامتقارن درصورتی‌که بودجه بیشتری به حمله تخصیص داده شود (زمانی‌که b کاهش می‌یابد) و زمانی‌که مهاجم، پارامترهای طراح سیستم را با دقت کمتری تخمین می‌زند (زمانی‌که Q' کاهش می‌یابد)، می‌تواند بهتر از مدل‌های با اطلاعات متقارن، شرایط واقعی را فرموله کند. بنابراین اگر طراح سیستم بداند که مهاجم نمی‌تواند پارامترها را به‌درستی تخمین بزند، او باید دانش بهتری درباره مهاجم به دست بیاورد و بودجه بیشتری جهت حفاظت از سیستم در اختیار بگیرد.

۴-۳- الگوریتم جستجوی ممنوعه جهت حل مدل دوسطحی پیشنهادی

با توجه به نمونه‌های حل شده توسط روش تک سطحی کردن مدل دوسطحی پیشنهادی با استفاده از شرایط کروش-کان-تاکر مشاهده می‌شود که با افزایش ابعاد مسئله و زیاد شدن تعداد متغیرهای تصمیم‌گیری مسئله، این روش نمی‌تواند در زمانی منطقی به جواب دقیق دست یابد. در چنین شرایطی، استفاده از الگوریتم‌های ابتکاری و فراابتکاری می‌تواند راهگشا باشد. الگوریتم جستجوی ممنوعه یکی از الگوریتم‌های فراابتکاری شناخته شده‌ای است که در مسائل بهینه‌سازی پیچیده توانسته است از خود عملکرد خوبی نشان دهد. نمونه‌هایی از کاربرد موفق این الگوریتم در حوزه مسائل مکانیابی میانه و مسائل مکانیابی با هزینه شارژ ثابت را می‌توان در سان[۳۳]، آراس و آکسن [۳۴] و آراس و همکاران [۳۵] مشاهده کرد.

در این تحقیق، الگوریتم جستجوی ممنوعه‌ای را که آکسن و آراس [۳۶] برای حل مسئله مکانیابی-حفاظت-حمله برای مسائل مکانیابی میانه ارائه کرده‌اند را برای مسئله مکانیابی-حفاظت-حمله با فرض مکانیابی پوششی و عدم‌تقارن اطلاعات توسعه می‌دهیم. الگوریتم پیشنهادی، از تابع هشی استفاده می‌کند که از بررسی جواب‌های تکراری در طول اجرای الگوریتم جلوگیری می‌نماید.

۴-۳-۱- ارائه کدینگ مناسب برای جواب مسائل سطوح بالا و پایین

پنج نوع حرکت در هر تکرار از الگوریتم اتفاق میفتد:

جدول (۵): انواع حرکات انجام گرفته در الگوریتم جستجوی ممنوعه

نوع حرکت	توضیح حرکت
1-Drop	یکی از تسهیلات باز، بسته می‌شود.
1-Add	یک تسهیل حفاظت شده یا حفاظت نشده در یکی از مکان‌های کاندیدی که تسهیلی در آن واقع نشده است، باز می‌شود.
1-Flip	وضعیت یک تسهیل باز شده از نظر حفاظت تغییر داده می‌شود.
1-Swap-Int	وضعیت حفاظتی دو تسهیل باز شده در دو وضعیت حفاظتی مخالف هم، با یکدیگر جابجا خواهند شد.
1-Swap-Ext	یک تسهیل در یکی از مکان‌های کاندیدی که تسهیلی در آن قرار نگرفته است، باز خواهد شد و یکی از تسهیلاتی که در حال حاضر باز هستند، بسته خواهد شد. تسهیل بازشده جدید ممکن است حفاظت شده یا حفاظت نشده باشد.

p: تعداد تسهیلات بازشده در جواب فعلی

π: تعداد تسهیلات حفاظت شده در جواب فعلی

$p-\pi$: تعداد تسهیلاتی است که باز شده است اما حفاظت نشده است

و

$m-p$: تعداد مکان‌های کاندید در دسترس می‌باشد.

ستون چهارم جدول ۶، بیشترین تعداد جواب‌های همسایه‌ای که می‌تواند با استفاده از نوع حرکت برای جواب فعلی σ_t تولید شود را نشان می‌دهد. این تعداد برای حرکت 1-Swap-Ext بر ضریبی که نسبت اندازه همسایگی ($RNS \geq 1$) نامیده می‌شود و فضای جستجو شده واقعی را کوچک می‌کند، تقسیم می‌شود. اگر $p > 1$ و هم‌چنین $\pi > 1$ باشد، آنگاه کمتر از تعداد ممکن برای حرکات 1-Swap-Ext بر روی σ_t انجام می‌شود. انتخاب اینکه کدام‌یک از این حرکات انجام بگیرد تصادفی است. یادآوری می‌کنیم که در طول یک تکرار الگوریتم، به تعداد بیشترین اندازه همسایگی از هر حرکت طی جستجوی همسایگی 1-Swap-Ext اجرا خواهد شد.

جدول (۶): انواع حرکات در الگوریتم جستجوی ممنوعه پیشنهادی

نوع حرکت	بر روی p تأثیر دارد؟	بر روی π تأثیر دارد؟	بزرگترین اندازه همسایگی
1-Drop	بله	ممکن است	$2(\|J\|-p)$
1-Add	بله	ممکن است	p
1-Flip	خیر	بله	p
1-Swap-Int	خیر	خیر	$\pi(p-\pi)$
1-Swap-Ext	خیر	ممکن است	$\begin{cases}\lceil 2p(\|J\|-p)/RNS\rceil, & p>1 \\ 2(\|J\|-1) & \text{در غیر صورت، این}\end{cases}$

۴-۳-۲- نمایش جواب و مقداردهی به آن

به‌منظور نمایش جواب‌های مسئله سطح بالا از رشته‌ای از ارقام سه‌گانه ۰، ۱ و ۲ استفاده می‌کنیم. ۰ نشان‌دهنده تسهیلاتی است که بسته است (هنوز باز نشده است)، ۱ نشان‌دهنده تسهیلاتی است که باز شده‌اند اما حفاظت نشده‌اند و ۲ نشان‌دهنده تسهیلاتی است که حفاظت می‌شوند. نمونه‌ای از رشته جواب برای $|J|=10$ در شکل زیر نمایش داده شده است که در آن تسهیلات ۱، ۳، ۵ و ۸ تسهیلات باز شده‌اند که از بین آن‌ها تسهیلات ۵ و ۸ حفاظت شده‌اند. این رشته از اعداد می‌تواند به‌صورت عددی در مبنای ۳ در نظر گرفته شود که می‌تواند به یک عدد اعشاری منحصربه‌فرد تبدیل شود. این تبدیل، یک نگاشت یک‌به‌یک بین همه طرح‌های مکانیابی-حفاظت موجه و غیرموجه مربوط به طراح سیستم و مجموعه اعداد صحیح مثبت در بازه $[0,3^{|J|}-1]$ است. فرض کنید σ نمایشی از جواب مسئله سطح بالا باشد که در آن وضعیت jامین تسهیل با سلول j برای $j=1,\ldots,|J|$ نشان داده شده است.

شماره تسهیل	1	2	3	4	5	6	7	8	9	10
وضعیت	1	0	1	0	2	0	0	2	0	0
	1×3^9	0×3^8	1×3^7	0×3^6	2×3^5	0×3^4	0×3^3	2×3^2	0×3^1	0×3^0
مقدار هش	$1\times3^9+1\times3^7+2\times3^5=22.374$									

شکل (۴): نمایشی از یک جواب مسئله سطح بالا در الگوریتم جستجوی ممنوعه و مقدار هش مربوطه

عدد صحیح اعشاری مربوط به این راه‌حل به‌عنوان مقدار هش شناخته می‌شود و با استفاده از تابع هش زیر محاسبه می‌شود:

$$Hash(\sigma)=\sum_{j=1}^{|J|} Cell_j \times 3^{|J|-j} \quad (۲۲)$$

تابع هش فوق یک طرح مکانیابی- حفاظت را می‌گیرد و یک عدد صحیح را برمی‌گرداند که در یک لیست هش ذخیره می‌شود. این لیست، حافظه موردنیاز و محاسبات مربوط به چک کردن این‌که آیا جواب ساخته شده جدید در لیست، قبلاً در حافظه ذخیره‌شده است یا نه را کاهش می‌دهد. اگر مقدار هش جواب فعلی ($hash_{cur}$) را بدانیم، مقدار هش جواب همسایه جدید ($hash_{neigh}$) می‌تواند در زمان $O(1)$ محاسبه شود. فرمول‌های موردنیاز برای محاسبه این مقدار برای هر یک از انواع حرکت‌ها در الگوریتم موردبررسی در جدول ۷ نمایش داده شده است.

جدول (۷): فرمول‌های مورد نیاز برای حرکات در الگوریتم مورد بررسی

نوع حرکت	اندیس تسهیل ۱	اندیس تسهیل ۲	فرمول $hash_{neigh}$
1-Drop	j	-	$hash_{cur} + cell_j \times 3^{\|J\|-k}$
1-Add	-	k	$hash_{cur} - cell_k \times 3^{\|J\|-j}$
1-Flip	j	-	$hash_{cur} + 3^{\|J\|-j}$, اگر $cell_j$ در جواب σ یک باشد. $hash_{cur} - 3^{\|J\|-j}$, درغیراینصورت
1-Swap-Int	j	k	$hash_{cur} + 3^{\|J\|-j} - 3^{\|J\|-k}$, اگر $cell_j$ در جواب σ دو باشد.
1-Swap-Ext	j	k	$hash_{cur} + cell_j \times 3^{\|J\|-j} - cell_k \times 3^{\|J\|-k}$

تابع هش و لیست هش پیشنهادی، کمک می‌کند تا از افتادن در دور و گیر کردن در جواب بهینه محلی جلوگیری شود. در این حالت، الگوریتم حل دقیق برای مسئله حمله مهاجم به ازاء هر طرح مکانیابی- حفاظت به‌دست‌آمده برای طراح سیستم، تنها یک‌بار اجرا می‌شود و اثربخشی الگوریتم افزایش می‌یابد. در لیست هش پیشنهادی، نه‌تنها مقدار هش بلکه تابع هدف Z_{sys} برای جواب فعلی σ و نوع هر یک از جواب‌های تولید شده در هر تکرار الگوریتم (جواب فعلی یا جواب همسایه) نیز در این لیست ذکر می‌شود. مقدار هش هر جواب جدید در لیست هش مرتب‌شده از ابتدا و انتهای لیست جستجو می‌شود. اگر این مقدار در این لیست یافت شد، Z_{sys} مربوطه اصلاح می‌شود و با بهترین جواب همسایه که تاکنون یافت شده است، مقایسه می‌گردد. اگر چنین مقدار هشی در طول لیست یافت نشد، مقدار Z_{sys} مربوط به جواب جدید، در ابتدا محاسبه می‌شود و سپس همراه با مقدار هش مربوط به آن در موقعیت مناسب در لیست قرار داده می‌شود. بعد از اینکه جستجوی همسایگی تکمیل شد، بهترین جواب همسایه به‌عنوان جواب فعلی جدید در نظر گرفته می‌شود و فیلد مربوط به نوع این جواب در لیست هش از جواب همسایه به جواب فعلی تغییر داده می‌شود. حفظ ترتیب صعودی مقادیر هش در طول لیست، به‌منظور حفظ اثربخشی روش جستجوی دوسطحی مورداستفاده الزامی است.

t : شمارنده تکرارهای الگوریتم

τ: شمارنده تکرارهای متوالی که طی آن‌ها بهترین جواب یافت شده تاکنون بهبود نیابد.

σ_t: جواب فعلی در تکرار t

σ_t^{neigh}: یک جواب در همسایگی σ_t

σ_t^{best}: بهترین جواب یافت شده در همسایگی σ_t

$MOVES$: مجموعه انواع حرکات برای ساختن جواب همسایه

Obj_t: مقدار تابع هدف طراح سیستم (Z_{sys}) در جواب فعلی σ_t

Obj_{neigh}: مقدار تابع هدف طراح سیستم در جواب همسایه σ_t^{neigh}

Obj_{best}: مقدار تابع هدف طراح سیستم در بهترین جواب همسایه σ_t^{best}

Obj^*: مقدار هدف طراح سیستم در بهترین جواب یافت شده تاکنون

جدول (۸): پارامترهای استفاده‌شده در نمونه‌های تولیدشده

۱: تا زمانی‌که شرط $t \le Max\_Iter$ و $\tau \le Max\_Nonimp\_Iter$ برقرار است کارهای زیر را تکرار کنید:

۲: $Obj_{best} \leftarrow \infty$

۳: برای هر نوع حرکت $k \in MOVES$، کارهای زیر را تکرار کنید:

۴: برای هر جواب همسایه موجه σ_t^{neigh} از نوع k کارهای زیر را تکرار کنید:

۵: با استفاده از $hash_{cur}$ مقدار $hash_{neigh}$ را محاسبه کنید.

۶: اگر σ_t^{neigh} در لیست هش، پیشتر به عنوان جواب فعلی ثبت شده است، آنگاه

۷: این جواب را کنار بگذارید و با σ_t^{neigh} بعدی ادامه بدهید.

۸: درغیراینصورت اگر σ_t^{neigh} در لیست هش به عنوان جواب همسایه ثبت شده باشد، آنگاه

۹: Obj_{neigh} را مجددا محاسبه نمایید.

۱۰: در غیراینصورت

۱۱: جواب بهینه مساله مهاجم را بر اساس Obj_{neigh} و با استفاده از نرم‌افزار سیپلکس محاسبه نمایید.

۱۲: براساس جواب بهینه این مساله، Obj_{neigh} را برای σ_t^{neigh} محاسبه نمایید.

۱۳: در لیست هش، σ_t^{neigh} را به همراه Obj_{neigh} و $hash_{neigh}$ به عنوان جواب همسایه ثبت کنید.

۵. اعتبارسنجی الگوریتم پیشنهادی

به‌منظور ارزیابی کارایی الگوریتم‌های حل پیشنهادی، تعدادی مسئله تصادفی مسیریابی در شرایط حمله به شبکه ایجاد می‌شود. به‌منظور ارزیابی کارایی الگوریتم، ده مسئله به‌صورت تصادفی تولید می‌شود. مقادیر پارامتر d_i به مقادیر $\overline{d_i}$ وابسته‌اند که Q، نشان می‌دهد که تخمین‌های توزیع‌کننده تا چه میزان دقیق است. بر این اساس اطلاعات نمونه‌های آزموده‌شده در جدول ۸ خلاصه شده‌اند.

پارامتر	d_i	$\overline{d_i}$	Q	f_j	h_j	r و b
مقدار	$U[5000,20000]$	$U\ (d_i.Q, d_i.(2-Q))$	۰٫۷	$U[120000,150000]$	$U[20000,60000]$	متناسب با مسئله تعریف شده

شکل (۵): شبه کد الگوریتم جستجوی ممنوعه توسعه داده شده

جهت مقایسه و ارزیابی الگوریتم حل پیشنهادی، الگوریتم با استفاده از نرم‌افزار مطلب ۲۰۱۲a کدنویسی شده است و بر روی رایانه اینتل پنتیوم ۴ با CPU، ۳٫۰۵ گیگاهرتز و حافظه ۵۱۲ مگابایت اجرا شده است.

نتایج حاصل از حل نمونه‌های تصادفی مختلف با استفاده از الگوریتم پیشنهادی در دو حالت با در نظر گرفتن عدم‌تقارن اطلاعات و بدون در نظر گرفتن عدم‌تقارن اطلاعات، از دیدگاه معیارهای منطقی بودن مستقیم و موزون برای مسئله سطح بالا (مسئله طراح سیستم) در جدول ۹ و از دیدگاه میانگین و بهترین برازندگی سطح بالا در جدول ۱۰ به ازاء دقت تخمینی معادل $Q = 0.6$ نشان داده شده است.

جدول (۹): مقایسه نتایج حاصل از حل مدل دو سطحی توسط الگوریتم جستجوی ممنوعه براساس منطقی بودن

شماره مسئله	معیار منطقی بودن مستقیم		معیار منطقی بودن وزنی	
	با در نظر گرفتن عدم‌تقارن اطلاعات	بدون در نظر گرفتن عدم‌تقارن اطلاعات	با در نظر گرفتن عدم‌تقارن اطلاعات	بدون در نظر گرفتن عدم‌تقارن اطلاعات
۱۰-۴-۲	۰٫۶	۰٫۳	۲۲۳	۴۱۵
۱۵-۴-۲	۰٫۲	۰٫۶	۲۱٫۸	۹۸۵
۲۰-۷-۳	۰٫۴	۰٫۴	۵۵٫۵	۶۸۱
۲۵-۷-۳	۰٫۳	۰٫۳	۸۲٫۷	۳۰۵٫۳
۳۰-۷-۳	۰٫۸	۰٫۲	۲۷۶	۶۶۲
۳۰-۱۰-۵	۰٫۹	۰٫۵	۱۹۰٫۲	۱۰۵۵
۵۰-۱۵-۷	۰٫۷	۰٫۵	۳۷۵٫۳	۷۶۸
۸۰-۲۰-۱۵	۰٫۹	۰٫۶	۱۹۸٫۲	۴۹۵
۱۲۰-۲۳-۱۵	۰٫۸	۰٫۶	۱۵۶٫۴	۲۳۷
۲۰۰-۲۵-۱۷	۰٫۹	۰٫۴	۱۲۰٫۴	۶۸۲٫۴

همان‌طور که در جدول (۹) مشاهده می‌شود، الگوریتم جستجوی ممنوعه توسعه داده‌شده برای حل مسائل حمله به شبکه با اطلاعات نامتقارنی با ابعاد متفاوت، قابل‌استفاده هستند و نتایج نسبتاً منطقی صرف‌نظر از ماهیت فضای حل در اختیار قرار می‌دهند. از سوی دیگر در شرایطی که دو بازیکن اطلاعات کاملی در مورد یکدیگر ندارند، می‌توانند این عدم‌تقارن اطلاعات را در تصمیم‌گیری‌های خود در نظر بگیرند یا اینکه بدون در نظر گرفتن این فرض تصمیم‌گیری نمایند. بر اساس نتایج حاصل از در نظر گرفتن فرض عدم‌تقارن اطلاعات یا لحاظ نکردن این فرض در تصمیم‌گیری توسط طراح سیستم، مشاهده می‌شود که میزان خدمات داده‌شده توسط طراح سیستم به نقاط تقاضا در شرایطی که این فرض را در نظر می‌گیرد، به‌طور قابل‌ملاحظه‌ای افزایش می‌یابد و این امر اهمیت در اختیار داشتن اطلاعات درست و دقیق از رقیب را در مسئله موردبررسی نشان می‌دهد.

مقایسه جواب‌های حاصل از الگوریتم جستجوی ممنوعه پیشنهادی با جواب‌های حاصل از روش کروش-کان-تاکر، اثربخشی الگوریتم فراابتکاری پیشنهادی نسبت به کروش-کان-تاکر را نمایش می‌دهد.

جدول (۱۰): مقایسه نتایج حاصل از حل مدل دو سطحی توسط الگوریتم جستجوی ممنوعه بر اساس برازندگی سطح بالا

شماره مسئله	میانگین برازندگی مسئله سطح بالا در الگوریتم جستجوی ممنوعه		بهترین برازندگی مسئله سطح بالا در الگوریتم جستجوی ممنوعه		برازندگی مسئله سطح بالا در روش کروش-کان-تاکر
	با در نظر گرفتن عدم‌تقارن اطلاعات	بدون در نظر گرفتن عدم‌تقارن اطلاعات	با در نظر گرفتن عدم‌تقارن اطلاعات	بدون در نظر گرفتن عدم‌تقارن اطلاعات	
۱۰-۴-۲	۳۶۱۴۸	۱۲۱۶۵	۳۶۹۳۴	۱۰۹۲۰	۳۶۹۳۴
۱۵-۴-۲	۵۶۰۶۲	۳۱۷۴۵	۵۶۱۱۳	۳۳۷۵۹	۵۶۱۱۳
۲۰-۷-۳	۷۷۴۷۶	۴۵۸۵۶	۷۷۷۱۴	۴۷۷۱۷	۸۰۵۶۳
۲۵-۷-۳	۸۷۴۲۶	۶۰۱۴۱	۸۷۶۷۹	۵۸۹۲۱	۹۱۰۲۳
۳۰-۷-۳	۱۱۲۱۱۰	۷۵۱۹۵	۱۱۳۶۶۰	۷۰۵۱۹	۱۲۵۳۶۸
۳۰-۱۰-۵	۱۱۴۹۵۰	۵۶۸۳۱	۱۱۵۷۴۰	۶۱۷۷۱	۱۲۶۰۳۲,۳
۵۰-۱۵-۷	۱۷۰۵۴۹	۷۰۴۳۲	۱۷۲۳۷۲	۷۹۹۶۴	۱۷۶۰۰۴
۸۰-۲۰-۱۵	۲۶۳۶۲۲	۹۵۰۰۸	۲۶۷۰۳۰	۱۱۲۲۱۱	-
۱۲۰-۲۳-۱۵	۳۹۸۰۲۳	۱۵۳۲۷۵	۴۰۲۴۶۸	۱۸۱۲۵۵	-
۲۰۰-۲۵-۱۷	۶۲۵۴۹۷	۲۹۹۱۱۸	۶۳۲۵۶۴	۲۸۲۵۴۶	-

جهت نمایش اثربخشی الگوریتم در ابعاد بزرگ، نتایج حاصل از الگوریتم جستجوی ممنوعه مبتنی بر لیست هش پیشنهادی با نتایج حاصل از الگوریتم جستجوی ممنوعه پایه بدون در نظر گرفتن لیست هش در مسائل نمونه مقایسه شد و نتایج حاصل در جدول ۱۱ نمایش داده شده است. همان‌طور که مشاهده می‌شود، استفاده از لیست هش، اثربخشی الگوریتم جستجوی ممنوعه را برای مسائل موردمطالعه افزایش داده است.

لیست هش مورداستفاده در الگوریتم پیشنهادی، حافظه موردنیاز و محاسبات مربوط به چک کردن این‌که آیا جواب ساخته شده جدید در لیست، قبلاً در حافظه ذخیره‌شده است یا نه را کاهش می‌دهد. هم‌چنین مقدار هش جواب همسایه جدید می‌تواند در زمان کوتاه‌تری محاسبه شود.

تابع هش و لیست هش پیشنهادی، کمک می‌کند تا از افتادن در دور و گیر کردن در جواب بهینه محلی جلوگیری شود. در این حالت، الگوریتم حل دقیق برای مسئله حمله مهاجم به ازاء هر طرح مکانیابی-حفاظت به‌دست‌آمده برای طراح سیستم، تنها یک‌بار اجرا می‌شود و اثربخشی الگوریتم افزایش می‌یابد. حفظ ترتیب صعودی مقادیر هش در طول لیست نیز یکی دیگر از دلایل اثربخشی الگوریتم پیشنهادی است.

همان‌طور که در جدول ۱۲ مشاهده می‌شود، الگوریتم جستجوی ممنوعه پیشنهادی می‌تواند مسئله را در زمان بسیار کوتاه‌تری نسبت به روش کروش-کان-تاکر و روش جستجوی ممنوعه پایه حل نماید.

جدول (۱۱): مقایسه نتایج حاصل از حل مدل دو سطحی توسط الگوریتم جستجوی ممنوعه پیشنهادی و پایه

شماره مسئله	میانگین برازندگی مسئله سطح بالا در الگوریتم جستجوی ممنوعه		بهترین برازندگی مسئله سطح بالا در الگوریتم جستجوی ممنوعه	
	جستجوی ممنوعه پیشنهادی	جستجوی ممنوعه پایه	جستجوی ممنوعه پیشنهادی	جستجوی ممنوعه پایه
۱۰-۴-۲	۳۶۱۴۸	۲۲۳۹۸	۳۶۹۳۴	۲۴۵۶۰
۱۵-۴-۲	۵۶۰۶۲	۴۱۵۶۰	۵۶۱۱۳	۴۲۳۵۰
۲۰-۷-۳	۷۷۴۷۶	۶۷۴۲۰	۷۷۷۱۴	۶۶۳۱۰
۲۵-۷-۳	۸۷۴۲۶	۸۰۲۰۰	۸۷۶۷۹	۸۰۸۸۰
۳۰-۷-۳	۱۱۲۱۱۰	۹۸۳۵۰	۱۱۳۶۶۰	۹۹۲۱۰
۳۰-۱۰-۵	۱۱۴۹۵۰	۹۵۲۳۰	۱۱۵۷۴۰	۹۶۵۸۰
۵۰-۱۵-۷	۱۷۰۵۴۹	۱۵۶۳۰۰	۱۷۲۳۷۲	۱۵۹۸۴۰
۸۰-۲۰-۱۵	۲۶۳۶۲۲	۲۳۵۰۰۰	۲۶۷۰۳۰	۲۳۷۸۲۰
۱۲۰-۲۳-۱۵	۳۹۸۰۲۳	۳۵۳۲۷۵	۴۰۲۴۶۸	۳۶۰۵۶۰
۲۰۰-۲۵-۱۷	۶۲۵۴۹۷	۵۹۸۳۰۰	۶۳۲۵۶۴	۶۰۰۲۸۰

جدول (۱۲): زمان محاسباتی کروش-کان-تاکر، جستجوی ممنوعه پایه و جستجوی ممنوعه توسعه داده شده

شماره مسئله	$\|I\|$	۱۰	۱۵	۲۰	۲۵	۳۰	۳۰	۵۰	۸۰	۱۲۰	۲۰۰	۲۰۰	۴۰۰
	$\|J_1\|$	۴	۴	۷	۷	۷	۱۰	۱۵	۲۰	۲۳	۲۵	۴۰	۵۰
	$\|J_2\|$	۲	۲	۳	۳	۳	۵	۷	۱۵	۱۵	۱۷	۲۰	۳۰
جستجوی ممنوعه پیشنهادی	زمان (ثانیه)	۱,۲	۴,۴	۸,۹	۱۰,۶	۱۱,۲	۲۸	۲۹,۶	۴۷,۴	۴۹,۷	۶۴,۶	۶۷.۸	۹۴.۹۲	۱۰۴.۴
جستجوی ممنوعه پایه	زمان (ثانیه)	۳	۵,۵	۱۳	۲۲	۳۰	۴۲	۴۵,۵	۶۵,۳	۹۵,۵	۱۲۶,۴	۲۶۰,۴	۳۳۶,۴	۴۵۳,۷
کروش-کان-تاکر	زمان (ثانیه)	۰,۸	۰,۶	۰,۷	۰,۷	۳,۹	۵	۲۱	۷۱	۳۶۰۰	>۷۰۰۰	>۱۰۰۰۰	>۱۰۰۰۰	>۱۰۰۰۰
	گپ	۰	۰	۰	۰	۰	۰	۰	۰	٪۳	۴.۳٪	۲۰٪	۳۴%	۳۲٪

۶. جمع‌بندی و نتیجه‌گیری

در این تحقیق مدلی دوسطحی برای مسئله مکانیابی-حفاظت-حمله برای تسهیلات حیاتی با فرض عدم‌تقارن اطلاعات و امکان حملات جزئی پیشنهاد شد و برای حل این مسئله، از روش کروش-کان-تاکر و هم‌چنین الگوریتم جستجوی ممنوعه‌ای مبتنی بر لیست هش جهت جلوگیری از بررسی جواب‌های تکراری استفاده شد. نتایج حاصل از حل مسائل نمونه با استفاده از روش‌های پیشنهادی، لزوم در نظر گرفتن فرض عدم‌تقارن اطلاعات در تصمیم‌گیری توسط رقبا زمانی که دو بازیکن درک یکسانی از اطلاعات یکدیگر ندارند را تأیید می‌کند. تحقیق حاضر می‌تواند از جنبه‌های متفاوتی توسعه یابد: (۱) در این تحقیق، صرفا عدم‌تقارن اطلاعات موردبررسی قرار گرفت. درصورتی‌که اطلاعات بازیکنان از یکدیگر مقادیر تصادفی باشند و بازیکنان بر اساس توابع توزیع احتمالی، پارامترهای رقیب را حدس بزنند لازم است بازی‌های با اطلاعات ناکامل که تحت عنوان بازی‌های بیزین شناخته می‌شوند برای این نوع از مسائل توسعه داده شوند. (۲) در برخی از موارد، بازیکنان از ابتدا شناخت کاملی از بازیکن رقیب ندارند اما به مرور زمان و در طول تکرارهای متوالی بازی، اطلاعات وی تکمیل می‌شود. در نظر گرفتن فرایند یادگیری در طول بازی می‌تواند یکی از توسعه‌های جالب مدل موجود جهت استفاده در شرایط واقعی باشد.

مراجع

[1] Smith, J. C. (2010). Basic interdiction models. *Wiley Encyclopedia of Operations Research and Management Science*.

[2] Church, R. L., Scaparra, M. P., Middleton, R. S. (2004). "Identifying critical infrastructure: the median and covering facility interdiction problems", *Annals of the Association of American Geographers*, 94(3): 491-502.

[3] Murray, A. T., Matisziw, T. C., Grubesic, T. H. (2007). "Critical network infrastructure analysis: interdiction and system flow", *Journal of Geographical Systems*, 9(2): 103-117.

[4] Scaparra, M. P., & Church, R. (2012). "Protecting supply systems to mitigate potential disaster: a model to fortify capacitated facilities", *International Regional Science Review*, 35(2): 188-210.

[5] Snyder, L. V., Scaparra, M. P., Daskin, M. S., Church, R. L. (2006). "Planning for disruptions in supply chain networks", In *Models, methods, and applications for innovative decision making* (pp. 234-257). INFORMS.

[6] O'Hanley, J. R., Church, R. L. (2011). "Designing robust coverage networks to hedge against worst-case facility losses", *European Journal of Operational Research*, 209(1): 23-36.

[7] Church, R. L., Scaparra, M. P. (2007). "Protecting critical assets: the r- interdiction median problem with fortification", *Geographical Analysis*, 39(2): 129-146.

[8] Scaparra, M. P., & Church, R. L. (2008). "A bilevel mixed-integer program for critical infrastructure protection planning", *Computers & Operations Research*, 35(6): 1905-1923.

[9] Smith, J. C., Lim, C., Sudargho, F. (2007). "Survivable network design under optimal and heuristic interdiction scenarios", *Journal of global optimization*, 38(2): 181-199.

[10] Aksen, D., Piyade, N., Aras, N. (2010). "The budget constrained r-interdiction median problem with capacity expansion", *Central European Journal of Operations Research*, 18(3): 269-291.

[11] Losada, C., Scaparra, M. P., O'Hanley, J. R. (2012). "Optimizing system resilience: a facility protection model with recovery time", *European Journal of Operational Research*, 217(3): 519-530.

[12] Liberatore, F., Scaparra, M. P., Daskin, M. S. (2011). "Analysis of facility protection strategies against an uncertain number of attacks: The stochastic R-interdiction median problem with fortification", *Computers & Operations Research*, 38(1): 357-366.

[13] Cappanera, P., Scaparra, M. P. (2011). "Optimal allocation of protective resources in shortest-path networks", *Transportation Science*, 45(1): 64-80.

[14] Roboredo, M. C., Pessoa, A. A., Aizemberg, L. (2019). "An exact approach for the r-interdiction median problem with fortification", *RAIRO: Recherche Opérationnelle*, 53(2): 505-516

[15] Mahmoodjanloo, M., Parvasi, S. P., Ramezanian, R. (2016). "A tri-level covering fortification model for facility protection against disturbance in r-

attacks", *Computers & operations research*, 64, 210-224.

[27] Forghani, A. & Dehghanian, F. & Salari, M. & Ghiami, Y. (2020). "A bi-level model and solution methods for partial interdiction problem on capacitated hierarchical facilities". *Computers & Operations Research* 114. 104831.10/1016/j.cor2019/10483.

[28] Bricha, N., & Nourelfath, M. (2013). "Critical supply network protection against intentional attacks: A game-theoretical model", *Reliability Engineering & System Safety*, 119: 1-10.

[29] Bricha, N., Nourelfath, M. (2014). "Extra-capacity versus protection for supply networks under attack", *Reliability Engineering & System Safety*, 131: 185-196.

[30] Bricha, N., Nourelfath, M. (2015). "Protection of warehouses and plants under capacity constraint", *Reliability Engineering & System Safety*, 138: 93-104.

[31] Berman, O., Krass, D., & Drezner, Z. (2003). "The gradual covering decay location problem on a network", *European Journal of Operational Research*, 151(3): 474-480.

[32] Sinha, A., Malo, P., Deb, K. (2017). "A review on bilevel optimization: From classical to evolutionary approaches and applications", *IEEE Transactions on Evolutionary Computation*, 22(2): 276-295.

[33] Sun, M. (2006). "Solving the uncapacitated facility location problem using tabu search", *Computers & Operations Research*, 33(9): 2563-2589.

[34] Aras, N., & Aksen, D. (2008). "Locating collection centers for distance-and incentive-dependent returns", *International Journal of Production Economics*, 111(2): 316-333.

[35] Aras, N., Aksen, D., Tanuğur, A. G. (2008). "Locating collection centers for incentive-dependent returns under a pick-up policy with capacitated vehicles". *European Journal of Operational Research*, 191(3): 1223-1240.

[36] Aksen, D., Aras, N. (2013). "A matheuristic for leader-follower games involving facility location-protection-interdiction decisions". *In Metaheuristics for Bi-level Optimization* (pp. 115-151). Springer, Berlin, Heidelberg.

interdiction median problem", *Computers & Industrial Engineering*, 102: 219-232.

[16] Lim, C., Smith, J. C. (2007). "Algorithms for discrete and continuous multicommodity flow network interdiction problems", *IIE Transactions*, 39(1): 15-26.

[17] Berman, O., Gavious, A. (2007). "Location of terror response facilities: A game between state and terrorist", *European Journal of Operational Research*, 177(2): 1113-1133.

[18] Berman, O., Gavious, A., & Huang, R. (2010). "Location of response facilities: a simultaneous game between state and terrorist", *International Journal of Operational Research*, 10(1): 102-120.

[19] Church, R., ReVelle, C. (1974). "The maximal covering location problem", *Papers in regional science*, 32(1): 101-118.

[20] Berman, O., Drezner, T., Drezner, Z., Wesolowsky, G. O. (2009). "A defensive maximal covering problem on a network", *International Transactions in Operational Research*, 16(1): 69-86.

[21] Aksen, D., & Aras, N. (2012). "A bilevel fixed charge location model for facilities under imminent attack", *Computers & Operations Research*, 39(7): 1364-1381.

[22] Keçici, S., Aras, N., & Verter, V. (2012). "Incorporating the threat of terrorist attacks in the design of public service facility networks", *Optimization Letters*, 6(6): 1101-1121.

[23] Akbari-Jafarabadi, M., Tavakkoli-Moghaddam, R., Mahmoodjanloo, M., & Rahimi, Y. (2017). "A tri-level r-interdiction median model for a facility location problem under imminent attack". *Computers & Industrial Engineering*, 114: 151-165.

[24] Zhang, X. Y., Zheng, Z., Cai, K. Y. (2017). "A fortification model for decentralized supply systems and its solution algorithms", *IEEE Transactions on Reliability*, 67(1): 381-400.

[25] Fard, A. M. F., Hajiaghaei-Keshteli, M. (2018). "A bi-objective partial interdiction problem considering different defensive systems with capacity expansion of facilities under imminent attacks", *Applied Soft Computing*, 68: 343-359.

[26] Aliakbarian, N., Dehghanian, F., Salari, M. (2015). "A bi-level programming model for protection of hierarchical facilities under imminent

IERPS Journal of Industrial Engineering Research in Production Systems

ISSN: 2345-2269

Journal of Industrial Engineering Research in Production Systems

Autumn and Winter 2020, Volume 7., No. 15., pp. 255-271
www.ier.basu.ac.ir

DOI: 10.22084/ier.2020.19334.1860

A Tabu-Search Algorithm for Location-Interdiction-Protection Problem Under Asymmetric Information

M. Mesibidgoli[1*], J. Jozani[2]

[1, 2] Department of Industrial Engineering, Golpaigan University, Iran

ARTICLE INFO

***Article history*:**

Received 8 June 2019
Accepted 16 January 2020

***Keywords*:**

Network Interdiction
Covering Facility Location Protection
Tabu search algorithm
Information asymmetry

ABSTRACT

Most of the terrorist activities that have taken place over the past two decades have been based on accurate information, which has led to disturbances in the security and some extensive damages and it is a major threat to public and government infrastructures. The dramatic expansion of such activities has shown the necessity and importance of the correct location and protection of these infrastructures in order to reduce the damage caused by the attack to increase the reliability of facilities for providing services. In such cases, a Stachelberg game is formed between the system designer and the attacker. Due to the high value and the lack of accurate information in the context of confliction, in this research, we are going to model the location-interdiction-protection problem under asymmetric information as a bi-level programming model and explore the advantages and risks of neglecting the information asymmetry in decision-making. In order to solve the suggested bi-level model, two solution methods are proposed. At first, Karush-Kuhn-Tucker conditions are used to convert the model to a single level model.Then for large size problems, we develop a matheuristic which searches the solution space of the upper level problem according to tabu search principles, where a hash function calculates and records the hash values of all visited solutions for the purpose of avoiding cycling, and resorts to a CPLEX based exact solution technique to tackle the lower level problem. Test results show efficiency and effectiveness of the proposed heuristic algorithm.

* Corresponding author. M. Mesibidgoli
Tel.: 031-57240065; E-mail address: bidgoli_m2000@yahoo.com