تعیین استراتژی بهینه تخصیص منابع مالی با هدف حفاظت سیستم قدرت در برابر خرابکاری‌های عمدی مبتنی بر تئوری بازی

رضا غفارپور[1]

۱- استادیار- دانشکده مهندسی برق- دانشگاه جامع امام حسین (ع)-تهران- ایران

rghaffarpour@ihu.ac.ir

چکیده: **در سال‌های اخیر، افزایش انگیزه‌های اقدامات خرابکارانه علیه سیستم‌های قدرت از یک‌سو و محدودیت تخصیص منابع مالی در حفاظت از این زیرساخت‌ها از سوی دیگر، لزوم برنامه‌ریزی بهینه این منابع را بیش‌ازپیش مورد توجه قرار داده است؛ تا درصورت رخداد حوادث احتمالی آینده، صدمات وارده و متعاقباً میزان خاموشی‌های مشترکین حداقل گردد. طراحان اقدامات خرابکارانه اغلب به‌عنوان بازیگرانی کاملاً باهوش و استراتژیک، آن‌دسته از وقایع را مورد هدف قرار می‌دهند که به‌دلیل احتمال وقوع بسیار کم در روند طراحی حفاظت سیستم مدنظر قرار نمی‌گیرند تا بدین وسیله حداکثر خسارت ممکن را به سیستم وارد آورند. در این پژوهش یک طرح جدید مبتنی بر تئوری بازی به‌صورت یک رقابت حذفی با حاصل صفر به‌منظور هدفمندسازی تخصیص منابع مالی به‌خدمت گرفته می‌شود. در این مقاله، دو الگوریتم تخصیص بودجه در مقابل تهدیدات عمدی نسبت به خطوط و پست‌های انتقال پیشنهاد شده‌است. در الگوریتم اول، تخصیص میزان ثابتی بودجه سالیانه به خطوط و پست‌های انتقال به منظور دست‌یابی به بهترین شرایط قابلیت‌اطمینان سیستم فرمول‌بندی می‌شود؛ درحالی‌که به‌کمک الگوریتم دوم بودجه لازم و نحوه تخصیص آن برای دستیابی به سطح از پیش تعیین شده‌ای از خاموشی مشترکین در مقابل استراتژی نامشخص افراد خرابکار محاسبه می‌شود. مدل پیشنهادی در محیط نرم‌افزارهای MATLAB (اجرای الگوریتم‌های بهینه‌سازی تک‌هدفه پرنده فاخته و چندهدفه ژنتیک با مرتب‌سازی نامغلوب) و GAMS (محاسبه شاخص قابلیت اطمینان سیستم پس از عملکردتوسط مدل پخش‌بار بهینه) حل شده‌است. نتایج کارایی تکنیک پیشنهادی را در تخصیص بهینه بودجه محافاظتی و افزایش شاخص امنیت تأمین انرژی الکتریکی تأیید می‌کند.**

واژه های کلیدی: **تئوری بازی، امنیت انرژی، پخش‌بار بهینه، الگوریتم پرنده فاخته، الگوریتم ژنتیک نامغلوب**

تاریخ ارسال مقاله: ۱۳۹۶/۰۳/۰۵

تاریخ پذیرش مشروط مقاله: ۱۳۹۷/۰۲/۰۳

تاریخ پذیرش مقاله: ۱۳۹۷/۰۵/۰۸

نام نویسنده‌ی مسئول: دکتر رضا غفارپور

نشانی نویسنده‌ی مسئول: تهران- بزرگراه بابایی-دانشگاه جامع امام حسین (ع)

۱- مقدمه

مسئله امنیت سیستم‌های قدرت به‌عنوان یکی از زیرساخت‌هایی که دارای نقشی حیاتی در پایداری اجتماعی و رشد اقتصادی کشورها است، همواره تحت تأثیر تهدیدات مختلفی چون حوادث طبیعی، تهدیدات تصادفی و عوامل نوظهور بوده است. در کنار این عوامل، محافظت از سیستم‌های قدرت در برابر تهدیدات خرابکارانه یکی دیگر از مواردی است که در سال‌های اخیر مورد توجه پژوهشگران در حوزه امنیت سیستم‌های قدرت قرار گرفته است [۱]. افراد خرابکار همواره سعی در اتخاذ تاکتیک‌هایی به‌منظور انهدام تأسیسات مهم و شریان‌های حیاتی کشور داشته‌اند تا از این طریق سیستم‌های حفاظتی کشور مورد نظر را دچار خدشه و با صرف حداقل سرمایه بیشترین خاموشی را به آن تحمیل نمایند. لذا ضروری است که به‌طور سالیانه میزانی از سرمایه ملی صرف حفاظت سیستم‌های قدرت در مقابل چنین اقداماتی گردد تا در صورت رخداد حوادث احتمالی آینده، صدمات وارده به زیرساخت‌ها و میزان خاموشی‌های سیستم حداقل گردد. اما محدودیت تخصیص اعتبارت به بخش حفاظت سیستم‌های قدرت تأییدی است بر ضرورت استفاده بهینه از منابع تخصیصی که در این پژوهش به این مهم پرداخته خواهد شد.

برای رسیدن به این هدف، تجزیه و تحلیل آسیب‌پذیری سیستم‌های قدرت نقش مهمی در توسعه صنعت برق ایفا می‌کند [۲] و [۳]. در سیستم‌های قدرت با ساختار سنتی، امنیت سیستم از طریق روش‌های به‌خوبی تثبیت‌شده‌ای تأمین می‌شود که عمدتاً معیارهایی برای هدایت و راهنمایی تصمیم‌گیرندگان در مورد نحوه سازماندهی عملیات‌های پیشگیرانه، پاسخ و بازگردانی سیستم پس از وقوع یک رخداد (شکست) معمول هستند. به‌عنوان مثال، معیار [۴] N-1 و معیار ریسک بالا [۵] که امروزه به‌طور گسترده‌ای مورد استفاده قرار می‌گیرد ازجمله این معیارها در صنعت برق می‌باشند. این معیارها می‌توانند اختلالات و قطعی‌های ناشی از حوادث و یا وقایع تصادفی در طبیعت را کنترل کنند. ازلحاظ تکنیکی، این روش‌ها مجموعه‌ای از وقایع بابیش‌ترین احتمال اختلال در سیستم را شناسایی و با آن‌ها مقابله می‌کنند.در این میان با هدف صرفه‌جویی‌های اقتصادی، شرکت‌های برق معمولاً رویدادهایی با احتمال‌های وقوع به اندازه کافی کم را نادیده می‌گیرند.

اگرچه، با افزایش طیف گسترده‌ای از انگیزه‌های تهدیدات خرابکارانه،سیستم‌های قدرت به‌عنوان یکی از مهم‌ترین زیرساخت‌های حیاتی کشورها تبدیل به یکی از اهداف مهم خرابکاران شده‌است [1][۱]، [۶]. در نتیجه، چارچوب سنتی امنیتی سیستم‌های قدرت در حال روبروشدن با چالش عظیمی هستند؛ چراکه گردانندگان وقایع خرابکارانه اغلب بازیگرانی کاملاً باهوش و استراتژیک هستند. آن‌ها می‌توانند آن دسته از وقایع با احتمال کم که سیستم در مقابل آن‌ها محافظت‌شده نیست، ولی درعین‌حال موجب آسیب جدی به سیستم قدرت شوند، را مورد هدف قرار دهند.

برخی از محققان مشکلات امنیتی شبکه‌های قدرت را به‌منظور ارائه روش‌های نوین حفاظتی در بخش تولید و انتقال مورد مطالعه قرار داده اند [۷] و [۸]. در این پژوهش‌ها، سعی برکشف معیارهای آسیب‌پذیری جدیدی از سیستم بوده است. در [۹] نویسندگان در مرحله اول مسئله اقدامات خرابکارانه در سیستم‌های قدرت را فرمول‌بندی کردند؛ که در آن طراحان آسیب‌های عمدی سعی بر حداکثرسازی قطعی بارها داشته‌اند. در [۱۰]، نویسندگان مدل ارائه‌شده در [۹] رابه یک مسئله برنامه‌نویسی دوسطحی انعطاف‌پذیرتر تعمیم دادند. علاوه‌برآن، [۱۱] مسائل موجود در مراجع [۹]، [۱۰] را به یک مدل برنامه‌نویسی دوسطحی عددصحیح مختلط تبدیل کرده و یک روش حل نوین ارائه داده‌اند. با توجه به مراجع[۹]- [۱۱]، می‌توان مشاهده کرد که در بستر جدید که در آن برنامه‌ریزان وقایع خرابکارانه وارد بازی می‌شوند، سیستم‌های قدرت سنتی مقاوم و مستحکم نیز ممکن استآسیب‌پذیر ظاهر شوند.

اخیراً، نظریه بازی برای طراحی استراتژی‌های بهینه جهت محافظت از سیستم‌های قدرت الکتریکی در برابر اقدامات خرابکارانه استفاده شده است. تئوری بازی ارائه‌شده در[۱۲] شرکت‌کننده‌گان در بازار را بازیکنانی کاملاً استراتژیک تلقی می‌کند. این نظریه با موفقیت برای بسیاری از رشته‌های کاربردی علوم ازجمله اقتصاد[۱۳]،[۱۴]، علوم سیاسی [۱۵]، و نظامی [۱۶]، [۱۷] اعمال شده است؛ که در آن چندین بازیگر با اهداف مختلف می‌توانند به رقابت بپردازند و با هر یک از دیگران بازیگران تعامل برقرار کنند. در [۱۸]، نویسندگانیک مدل بازی استاتیک با دو بازیکن با حاصل‌جمع صفر را برای مطالعه استراتژی محافظت از شبکه‌های قدرت الکتریکی در برابر حملات خصمانه پیشنهاد کرده‌اند. در این مدل، به‌طور هم‌زمان، مدافعان یک استراتژی با بودجه محدود را برای حفاظت از هر یک از عناصر سیستم‌های قدرت به‌کار می‌گیرند و خرابکاران یک هدف برای تخریب انتخاب می‌کنند. این یک تلاش اولیه برای حفاظت از سیستم قدرت در برابر حملات هدفمند است که در آن نظریه بازی یک بعد جدید برای پاسخ‌های بالقوه ممکن ارائه می‌دهد.

در این مطالعه، هدف ارائه یک چارچوب جامع بازی است که علاوه‌بر مدل بازی استاتیک ارائه‌شده در [۱۸] شامل چندین نسخه جدید دینامیکی در یک چهارچوب جامع ترکیبی نیز می‌شود. در مرحله بعد، تئوری مدیریت ریسک برای تجزیه‌وتحلیل چارچوب معرفی و بر این مبنای روش پیشنهادی، استراتژی قابل‌اعتماد جدیدی برای محافظان تشریح می‌شود. همچنین در مقاله حاضر فرمول‌بندی [۱۸] برای تهدید همزمان چند هدف نیز بسط داده شده است. علاوه بر آن بر خلاف پژوهش‌های گذشته، دو الگوریتم با اهداف متفاوت برای دستیابی به استراتژی‌های قابل‌اعتماد برای دو مسئله حافظتی زیر ارائه خواهد شد:

۱) هنگامی که محافظان دارای یک بودجه محدود هستند، چگونه

بودجه را برای استقرار یک استراتژی قابل‌اعتماد اختصاص دهند؟

۲) هنگامی که محافظان می‌خواهند ارزش ازدست‌رفته خود را (میزان خاموشی) به یک مقدار مورد انتظار محدود کنند، به‌منظور دستیابی به یک استراتژی حفاظتی قابل‌اعتماد نیازمند چقدر بودجه هستند؟

نوآوری‌های مهم ارائه‌شده در پژوهش حاضر در مقایسه با مطالعات گذشته به‌شرح زیر است:

- فرمول‌بندی عوامل تهدیدزا برای امنیت سیستم قدرت و عملکرد حافظان سیستم بر مبنای نظریه بازی با حاصل صفر تحت یک چهارچوب جدید ترکیبی (استاتیکی- دینامیکی).
- تعریف یک استراتژی قابلیت اطمینان جدید برای تعیین حداکثر زیان بدبینانه تحت هرگونه تهدیدات نامشخص عمدی و طبیعی.
- تعریفدو استراتژی بازی متفاوت برای محافظان که با توجه به میزان اهمیت شبکه توسط بهره‌بردار قابل استفاده هستند.
- اعمال روش پیشنهادی به پست‌های انتقال.
- بکارگیری یک الگوریتم بهینه‌سازی دوهدفه NSGAII که می‌تواند بامشخص‌نمودن سری نقاط بهره‌برداری در هر یک از استراتژی‌های پیشنهادی، در تعیین بهینه حد نهایی بودجه و یا قابلیت اطمینان موردنیاز کارآمد باشد.

پس از مقدمه، در بخش دوم، خلاصه‌ای از تهدیدات حاضر برای سیستم‌های قدرت بیان می‌شود. در بخش سوم، استراتژی بازی برای محافظان و همچنین افراد شرکت‌کننده در اقدامات خرابکارانه و تهدیدات عمدی نسبت به سیستم‌های قدرت تعیین و سپس چهارچوب بازی تعریف خواهد شد. در بخش چهارم، الگوریتم تخصیص بودجه پیشنهادی به‌عنوان تابع هدف مسئله تعریف می‌شود. در ادامه در بخش پنجم، با استفاده از مدل پیشنهادی، شبیه‌سازی‌های موردنظر در محیط متلب و بر روی یک سیستم نمونه استاندارد اجرا خواهد شد و نتایج به‌دست‌آمده مورد بررسی قرارمی‌گیرد. در بخش ششم، نتیجه حاصل از این پژوهش بیان می‌شود.

۲- نگاهی به تهدیدات علیه سیستم‌های قدرت

تهدید عبارت‌است از دلیل بالقوه‌ای از یک حادثه خواسته یا ناخواسته که ممکن است منجر به به‌خطرافتادن سیستم قدرت شود. معمولاً این تهدیدات در چهار دسته تقسیم‌بندی می‌شوند. تهدیدات طبیعی، تهدیدات تصادفی، تهدیدات نوظهور و تهدیدات عمدی.

در دو دهه اخیر روند صعودی خاموشی‌هایی که توسط تهدیدات طبیعی و تصادفی به‌وجود آمده‌اند، بیش‌ترین توجه را به‌خود جلب می‌کند. در رابطه با تهدیدات عمدی و تهدیدات نوظهور، درسال‌های قبل از ۱۹۹۸، هیچ خاموشی رخ نداده استتعداد بسیار اندکی خاموشی گزارش شده است. اما پس از این سال تهدیدات عمدی و سایر تهدیدات نوظهور به‌عنوان دلایل خاموشی‌ها، مطرح شده‌اند. در سال‌های اخیر، تهدیدات عمدی مانند هک و تهدیدات سایبری و هم‌چنین تهدیدات نوظهور مانند اثرات متقابل سایر زیرساخت‌ها، موجب بروز خاموشی‌های بسیاری شده‌اند. اگرچه تهدیدات مرسوم (سنتی) هنوز دلیل بیشترخاموشی‌ها هستند، اما با توجه به رشد چشم‌گیر خاموشی‌های ناشی از تخریب‌های عمدی، باید به این دسته از تهدیدات غیرمتعارف توجه کافی شود.دسته‌بندی این نوع از تهدیدات به‌همراه توضیحات مرتبط و اثرات ممکن هر یک از آن‌ها بر سیستم قدرت، در جدول (۱) ارائه شده است.

۳- چهارچوب بازی در خرابکاری‌های عمدی

در این بخش مدل ابتدائی مدافع-مهاجم سیستم‌های قدرت ارائه شده در [۱۸] به‌منظور استفاده وسیع‌تر بهبود می‌یابد. در مدل ارائه‌شده، محافظان دارای بودجه محدود برای حفاظت از سیستم قدرت هستند. افراد تهدیدکننده سیستم نیز قابلیت انهدام کامل اهداف با اندازه‌های متفاوت را دارند. فرض می‌شود که ترکیبی از عناصرسیستم قدرت را می‌توان به‌عنوان یک هدف مشترک درنظر گرفت [۱۸]. بنابراین در اینمدل، یک واقعه خرابکارانه موفقیت‌آمیز که منجر به شکست هدف شود، منتهی به ازدست‌رفتن یک یا چندی از تأسیسات می‌شود. قبل ازاستقرار یک استراتژی حفاظتی، فرض می‌شود که $X_j >= 0$ نرخ مورد

جدول (۱): دسته‌بندی تهدیدات عمدی

		تهدیدات فیزیکی
آسیب‌های عمدی	تعریف	عملی تند و شدید برای ایجاد ترس و وحشت در میان مردم با اهداف مذهبی، سیاسی، اقتصادی یا ایدئولوژیک که شامل تخریب زیرساخت‌های فیزیکی و صدمه‌زدن به کارکنان سیستم قدرت می‌باشد.
	اثرات	ازدست‌رفتن کارایی و عملکرد سیستم قدرت.
جنگ	تعریف	آسیب نظامی به سیستم با هدف متوقف‌کردن عملکرد آن.
	اثرات	ازدست‌رفتن کارایی و عملکرد بخشی یا کل سیستم قدرت.
خرابکاری	تعریف	فعالیتی مجرمانه موثر بر تولید، انتقال و توزیع توان مانند دزدیدن مس و ملزومات خطوط انتقال.
	اثرات	ازدست‌رفتن کارایی و عملکرد بخشی از سیستم قدرت.
		تهدیدات انسانی
تهدیدات داخلی	تعریف	سوءاستفاده یکی از کارمندان که به اطلاعات سازماندهی سیستم قدرت دسترسی دارد، از آسیب-پذیری سیستم به‌منظور زیان‌رساندن به آن.
	اثرات	ازدست‌رفتن کارایی و عملکرد بخشی از سیستم قدرت.
		تهدیدات سایبری
بدافزارها	تعریف	نرم‌افزارهایی که برای مختل‌کردن عملیات، کسب اطلاعات و یا کسب دسترسی غیرمجاز به‌کارمی‌روند و به‌منظور آسیب‌رساندن به سیستم طراحی شده‌اند.
	اثرات	ازبین‌بردن وظعیت مطلوب سیستم قدرت و متوقف-

		کردن عملکرد آن.
هک کردن	تعریف	هک‌کردن سیستم سایبری و کنترل سیستم قدرت به‌منظور آسیب‌رساندن به آن.
	اثرات	ازدست‌رفتن کارایی و عملکرد بخشی از سیستم.

انتظار ازدست‌دادن شیء j ام است؛ یعنی اگرعنصر j مورد آسیب واقع شده باشد، خسارت وارده مساوی با X_j برای یک ساعت خاموشی خواهد شد. با فرض آن‌که T_j برابر بامدت زمان موردنیاز برای احیاء و بازگردانی کامل هدف j بر حسب ساعت (h) باشد، مجموع از دست-رفتن مورد انتظار برای عنصربدون حفاظت j با y_j معرفی می‌شود که به صورت $y_j = X_j.T_j$ می‌تواند محاسبه شود.

۳-۱- فرمول‌بندی محافظت سیستم

با فرض یک سیستم قدرت شامل N عنصر از جمله ژنراتورها، خطوط انتقال، تجهیزات پست، ترانسفورماتورها و غیره، محافظان نیازمند اتخاذ یک تصمیم درمورد چگونگی تخصیص بودجه محدود R_0 خود برای حفاظت از N عنصر هستند. هر عنصر i دارای یک تابع حفاظت $p_i(c_i)$ به‌شرح زیر است [18]:

$$0 \le p_i(c_i) \le 1 \qquad (۱)$$

که در آن c_i بودجه اختصاص‌داده‌شده برای حفاظت عنصر i است. تابع $p_i(c_i)$ در (۱) نشان‌دهنده احتمال یک تخریب عمدی موفقیت-آمیز به عنصر i است. برای مثال، اگر c_i برابر 0 باشد، هیچ بودجه‌ای برای عنصردرنظر گرفته‌نشده‌است؛ بنابراین،احتمال انهدام عنصر i برابر ۱ است. وقتی c_i افزایش می‌یابد، $p_i(c_i)$ متناظر با آن باید کاهش می‌یابد. بدین‌معنا که متوقف ساختن کامل عملکرد عنصر سخت‌تر می‌شود. بر این اساس، $p_i(c_i)$ را می‌توان به‌صورت یک تابع کاهشی پیوسته فرمول‌بندی کرد. محافظ ان بودجه را در میان N عنصراز سیستم قدرت اختصاص می‌دهند. حفاظت کلی سیستم را می‌توان به-صورت بردار تابع حفاظت زیر شرح داد:

$$P = (p_1, p_2, p_3, ..., p_N) \qquad (۲)$$

علاوه بر این، شرکت‌های الکتریکی معمولا ظرفیت بازیابی و احیای پایه و محدودی برای تعمیر و نگهداری خرابی هر عنصر دارند. t_i^{base} مدت‌زمان لازم برای تعمیرعنصر i است؛ هنگامی‌که هیچ بودجه‌ای برای بازیابی [۱۸] صرف نشده باشد.اگرمحافظان سیستم بودجه‌ای برای بازیابی اختصاص دهند، زمان تعمیر و احیا t_i کاهش خواهد یافت،یعنی:

$$t_i = t_i^{\text{base}} \times f_i(c_{\text{recovery}}) \qquad (۳)$$

که در آن $f_i(c_{\text{recovery}})$ یک تابعپیوسته کاهشی است و c_{recovery} یک متغیر برای تخصیص بودجه برای بازیابی می‌باشد. زمان بازیابی را می‌توان به‌صورت تقریبی به شرح زیر فرمول‌بندی کرد:

$$T_i = \sum_{i=1}^{N} t_i^{\text{base}} \times f_i(c_{\text{recovery}}) \qquad (۴)$$

با فرض بودجه کل محافظان برابر با R_0 واستراتژی آن‌ها برابر با $c = (c_1, c_2, c_3, ..., c_N)$، به سادگی می‌توان معادله زیربه‌دست آورد:

$$\sum_{i=1}^{N} c_i + c_{\text{recovery}} = R_0 \qquad (۵)$$

که در آن $c_i \ge 0$، $c_{\text{recovery}} \ge 0$ و N نشان‌دهنده تعداد المان‌های سیستم است.

۳-۲- فرمول‌بندی تخریب عمدی

با فرض آن‌که افراد خرابکار می‌توانند به‌صورت موفقیت‌آمیزی به یک هدف متشکل از n عناصر صدمه بزنند، درحالی‌که n توسط قابلیت آنها محدود شده است؛ برای یک هدف متشکل از n عنصر، تعداد کل حالات اهداف بالقوه (M) می‌تواند به‌صورت زیرمحاسبه گردد [۱۸].

$$M = \binom{N}{n} = \frac{N!}{n!(N-n)!} \qquad (۶)$$

استراتژی موردنظر خرابکارانرا می‌توان به شکل یک بردار احتمالات به‌صورت q تشکیل داد. q_j احتمال متناظر با حالتی است که هدف j مورد آسیب قرار گیرد:

$$q = (q_1, q_2, ..., q_M) \qquad (۷)$$

$$0 \le q_j \le 1, \qquad j = 1, ..., M \qquad (۸)$$

$$\sum_{j=1}^{M} q_j = 1 \qquad (۹)$$

۳-۳- چارچوب جامع بازی

۳-۳-۱- رقابت حذفی بین محافظان و مهاجمان

در یک حمله عمدی، تعامل بین محافظان و افراد خرابکاررا می‌توان به‌عنوان یک بازی دو نفره با حاصل‌جمع صفر درنظرگرفت. به‌این‌معنا که، میزان سودعواملی که قصد صدمه‌زدن به سیستم را دارند برابر ضررمحافظان است که "حذفی" بین آن‌ها نامیده می‌شود. بازی‌های مجموع‌صفر بازی‌هایی هستند که ارزش بازی در طی بازی ثابت می‌ماند وسود یک بازیکن با زیان بازیکن دیگر همراه است. بر این اساس، سودافراد خرابکار (یا همان ضررمحافظان) را طبق نظریه بازی حذفی می‌توان به صورت زیر تعریف کرد:

$$L = \sum_{j=1}^{M} L_j(\text{c},\text{q}) = \sum_{j=1}^{M} q_j.U_j(c) \qquad (۱۰)$$

که در اینجا، q_j احتمال آن است که عنصر j مورد هدف قرار گیرد و $U_j(c)$ ضررمورد انتظار تحت استراتژی محافظتی c است. برای آسیب به هدف j، که تنها شامل یک عنصر منفرد است:

$$U_j(c) = p_j(c_j).y_j \quad (11)$$

اگر هدف آسیب بیش از ۱ المان از سیستم باشد، یعنی $n>1$، مسئله بسیار پیچیده می‌شود؛ چرا که باید احتمال متناظر باوضعیتی که تنها یک زیرمجموعه از هدف نیز خراب شده باشد، را نیز درنظر گرفت. به‌طور کلی می‌توان گفت که اگر هدف j شامل n المان (یعنی $i_1 \dots i_n$) مورد هدف قرار گیرد، زیان $U_j(c)$ محافظان به شکل زیر قابل‌تعریف است.

$$\begin{aligned} U_j(c) &= p_{i_1}(c_{i_1}) \dots p_{i_n}(c_{i_n}).y\{i_1 \dots i_n\} \\ &+ p_{i_1}(c_{i_1}) \dots p_{i_{n-1}}(c_{i_{n-1}}) \\ &\times\left(1-p_{i_n}(c_{i_n})\right).y\{i_1 \dots i_{n-1}\}+\dots \\ &+ p_{i_2}(c_{i_2}) \dots p_{i_n}(c_{i_n}) \\ &\times\left(1-p_{i_1}(c_{i_1})\right).y\{i_2 \dots i_n\}+\dots \\ &+ p_{i_1}(c_{i_1}) \dots \left(1-p_{i_2}(c_{i_2})\right) \dots \\ &\left(1-p_{i_n}(c_{i_n})\right) y\{i_1\} \end{aligned} \quad (12)$$

که $U_j(c)$ مجموع بخش‌های $C_n^n + C_n^{n-1} + \dots + C_n^1 = 2^n - 1$ است. درطول یک دوره $y\{s\}$ مقداری ثابت فرض می‌شود. پس از اتمام دوره درنظرگرفته شده حاضر، محافظان باید استراتژی خود را منطبق با $y\{s\}$ جدید تغییر دهند.

هدف اصلی این تحقیق اتخاذ استراتژی کلی c است که در آن جدای از چگونگی بازی افراد خرابکار q، رقابت حذفی L که همان زیان‌های وارده به محافظان است، به یک میزان حداقل محدود گردد. بدین‌منظور لزوم بر آن است که در ابتدا رابطه‌ی میان طرفین بازی تشریح گردد. مبتنی‌بر تئوری بازی [۱۹]، رابطه‌ی میان آن‌ها می‌تواند به وضعیت‌های متفاوتی تقسیم شود. در بخش بعدی این وضعیت‌ها شرح داده خواهد شد و سپس در یک چارچوب جامع ادغام می‌گردند.

۳-۳-۲- انواع مدل بازی میان مهاجمان و محافظان

۱) مدل بازی استاتیک [۱۸]: در مدل بازی استاتیک فرض بر آن است که عوامل خرابکار اطلاعی درباره‌ی استراتژی محافظان ندارند؛ یعنی به‌طور هم‌زمان، مدافعان از استراتژی c جهت محافظت (طرح اختصاص بودجه برای N عنصر در سیستم قدرت) و عوامل خرابکاراز استراتژی q به‌منظور طراحی یک برنامه خرابکارانه، بهره می‌برند.

۲) مدل بازی دینامیک (پویا): در واقعیت افرادی که قصد صدمه به سیستم را دارندمی‌توانند از روش‌های مختلفی به منظور کسب اطلاعات لازم درباره‌ی حافظت سیستم‌های قدرت یا همان استراتژی محافظان و همچنین زمان دقیق تغییر این استراتژی استفاده کنند. در این مدل افراد خرابکار می‌توانند استراتژی محافظان c را ببینند و استراتژی q را برای آغاز عملکرد یک تخریب عمدی در آن دوره اتخاذ نمایند.

۳) تعدد بازی‌ها: مدل‌های بازی استاتیک و دینامیک دو نمونه حدی از تئوری بازی هستند که در آن‌ها فرض بر آن است که افراد خرابکارکاملاً بی‌اطلاع و یا دارای اطلاعات کامل نسبت به استراتژی محافظان هستند. گاهی اوقات خرابکاران می‌توانند تنها بخشی از استراتژی را بدانند و بر اساس این‌که آن‌ها تا چه میزان از استراتژی آگاهی دارند، می‌توان وضعیت‌های متعددی را فرض نمود. به‌منظور تسهیل آنالیز، یک مدل بازی جامع در قسمت بعد معرفی می‌شود.

۳-۳-۳- مدل بازی جامع

۱) آنالیز چارچوب: در مدل ایستا، ریسک بالایی در مقابل استراتژی‌آسیب به سیستم وجود دارد. با افزایش اطلاعات اخذشده درباره‌ی استراتژی حفاظت از سیستم توسط افرادی که تاحدودی از استراتژی محافظان آگاهی دارند، این ریسک افزایش می‌یابد و درنهایت در مدل پویا به ۱۰۰٪ می‌رسد. با توجه به تئوری مدیریت ریسک [20]، به‌ازای هر استراتژی که توسط محافظان بازی می‌شود، همیشه یک حداکثر زیان برای محافظان تحت آن استراتژی نیز وجود دارد. حداکثر میزان آسیب یک وضعیت بدبینانه است. برای مثال اگر فرض شود که مدفعان از استراتژی $c' \in C$ استفاده می‌کنند که در آن C فضای استراتژی‌های ممکن برای محافظان است، حداکثر آسیب یا آسیب بدبینانه می‌تواند از طریق برنامه‌ریزی ریاضی زیر به‌دست آید:

$$\max_{q \in Q} \sum_{j=1}^{M} q_j U_j(c') \quad (13)$$

که در آن Q فضای استراتژی‌های وارد آوردن صدمه به سیستماست. این برنامه‌ریزی با قیود (۱) تا (۹) اجرا می‌شود. فرض می‌شود که q' پاسخ و L' مقدار تابع هدف یا همان مقدار ماکزیمم است. اگر عوامل خرابکار c' را نشناسند، با اجرای تصادفی استراتژی q' ، این امکان (خطر) وجود دارد که محافظان حداکثر میزان L' را ازدست دهند؛ که تحت استراتژی c' یک موقعیت بدبینانه است و محک مناسبی برای نمایش ریسک ایجاد می‌نماید. به‌علاوه اگر خرابکاران c' را بشناسند، منطق بر آن برای رسیدن به حداکثر دستاورد L' ، استراتژی خرابکارانه q' را اجرا می‌نمایند. می‌توان مشاهده کرد که باوجود این‌که انواع مختلفی از مهاجمان در چارچوب پیشنهادی قابل تصور هستند، اما آن‌ها تنها می‌توانند ریسک یا احتمال موقعیت بدبینانه را افزایش دهند و نمی‌توانند مقدار حداکثر آسیب بدبینانه را افزایش دهند؛ بدین معنا که می‌توان با کاهش آسیب بدبینانه تا حد ممکن، به‌دنبال یک استراتژی قابل‌اطمینان کلی در مقابل تمامی تهدیدات بود.

به‌ازای هر استراتژی $c \in C$ از محافظان، می‌توان مقدار آسیب بدبینانه را با برنامه‌ریزی ماکزیمم‌سازی (۱۳) به‌دست آورد. واضح است که یک آسیب بدبینانه حداقل بر روی فضای استراتژی موجود برای محافظان وجود دارد که می‌توان آن را از طریق برنامه‌ریزی زیر به‌دست آورد:

$$\min_{c\in C}\max_{q\in Q}\sum_{j=1}^{M}q_jU_j(c) \qquad (۱۴)$$

معادله‌ی (۱۴) نیز با قیود (۱) تا (۹) اجرا می‌شود. فرض می‌شود که $\left(c^0,q^0\right)$ پاسخ مسئله بالا و L^0 مقدار تابع‌هدف به‌ازای این پاسخ باشد. از آنجا که L^0 بدبینانه‌ترین آسیب ممکن برای محافظان تحت استراتژی c^0 است، تا زمانی‌که آن‌ها از استراتژی c^0 بهره ببرند، مجزا از استراتژی‌های به‌کار گرفته‌شده برای صدمه به سیستم، آسیب وارده نمی‌تواند از L^0 تجاوز کند. به‌علاوه استراتژی c^0 می‌تواند مقدار تلفات بدبینانه را به یک مقدار مینیمم برساند. در نتیجه می‌توان برای طراحی یک استراتژی قابل‌اطمینان، معیاری به‌شرح زیر را درنظر گرفت:

۲) معیار استراتژی قابل‌اطمینان: در چارچوب پیشنهادی، استراتژی قابل‌اطمینان محافظان c^0 و حداقل‌زیان بدبینانه‌ی محافظان L^0 است که می‌توان آن‌ها را به‌ترتیب به‌صورت زیر به‌دست آورد:

$$c^0=\arg\min_{c\in C}\left(\max_{q\in Q}\sum_{j=1}^{M}q_jU_j(c)\right) \qquad (۱۵)$$

$$L^0=\min_{c\in C}\max_{q\in Q}\sum_{j=1}^{M}q_jU_j(c) \qquad (۱۶)$$

این معیار نشان می‌دهد که تا زمانی که محافظان از استراتژی c^0 استفاده کنند، می‌توانند اطمینان داشته باشند که آسیب‌شان بیش از L^0 نخواهد بود. در واقع L^0 کم‌ترین مقدار در مرز بالایی آسیب محافظان است که آسیب حداقل در بدترین وضعیت ممکن نیز نامیده می‌شود.

۴- الگوریتم تخصیص بودجه

در این بخش یک الگوریتم مبتنی بر تئوری بازی میان افراد خرابکار و محافظان سیستم قدرت برای تهدیدات عمدی نسبت به ادوات شبکه با استفاده از چهارچوب ارائه‌شده در بخش قبل پیشنهاد می‌شود.

۴-۱- آنالیز ابتدائی تخصیص بودجه

با توجه به معیار مشخص‌شده در بخش قبل، می‌توان دریافت که با اتخاذ استراتژی قابل‌اطمینان c^0برای محافظان،حداکثر زیان بدبینانه L^0می‌تواند برای آنها تضمین‌شده باشد. این مقدار می‌تواند با حل رابطه (۱۴) به‌دست آیند. در پژوهش‌های قبلی[21]-[24]، اغلب برای حل برنامه‌ریزی حداقل- حداکثر بر روی به‌دست آوردن نقطه زینی تمرکز داشتند که لزوم آن برقراری رابطه زیر است:

$$\max_{q\in Q}\min_{c\in C}\sum_{j=1}^{M}q_jU_j(c)=\max_{c\in C}\min_{q\in Q}\sum_{j=1}^{M}q_jU_j(c) \qquad (۱۷)$$

با این‌حال معادله (۱۷) نیازمند آن است که تابع هدف حذفی مسئله بتواند تعدادی قید سخت راارضا کند [۲۱]- [۲۴].

تابع حذفی $L(c)=\sum_{j=1}^{M}L_j(c)=\sum_{j=1}^{M}q_jU_j(c)$ است که در آن $\sum_{j=1}^{M}q_j=1$ می‌باشد. درنتیجه، واضح است که می‌توان $L(c)$ را به‌صورت میانگین وزن‌دهی‌شده و سپس نرمال‌شده M ترم از $U_j(c)$ دانست که در آن،درصورتی‌که عنصر j مورد هدف قرار گیرد، هر ترم $U_j(c)$ معادل با زیان مورد انتظار محافظان است.

برای یک مقدار مشخص c، حداکثر مقدار میانگین وزن‌دهی‌شده و نرمال‌شده $\max_{q\in Q}\sum_{j=1}^{M}q_jU_j(c)$ است.می‌توان گفت که اگر در میان تمامی اهداف، تنها یکی از آنها دارای حداکثر میزان آسیب باشد، حداکثر رقابت حذفی می‌تواند با آسیب‌رساندن به این هدف به‌دست آید. اگر به‌تعداد k هدف با میزان حداکثر آسیب قابل‌انتظار یکسان وجود داشته باشد، حداکثر رقابت حذفی می‌تواند با انهدام هر یک از آن‌ها به‌دست می‌آید. به‌هرحال به‌ازای هر استراتژی c که توسط محافظان به‌کار گرفته شود، یک ماکزیمم رقابت حذفی$M(c)$ وجود دارد که می‌توان آن‌را به‌صورت زیر تعریف کرد:

$$M(c)=\max\left\{U_1(c),...U_M(c)\right\} \qquad (۱۸)$$

مشخصاً رابطه (۱۸) معادلی برای $\max_{q\in Q}\sum_{j=1}^{M}q_jU_j(c)$ است. بنابراین برنامه‌ریزی حداقل- حداکثر یا همان $\min_{c\in C}\max_{q\in Q}\sum_{j=1}^{M}q_jU_j(c)$ می‌تواند به معادله‌ی زیر تبدیل شود:

$$\min_{c\in C}M(c) \qquad (۱۹)$$

با تبدیل معادل این رابطه می‌توان بردار q را در برنامه‌ریزی محاسباتی اولیه رابطه (۱۴) حذف نمود. این کار تا حد زیادی پیچیدگی برنامه‌ریزی را کاهش می‌دهد. در واقع برنامه‌ریزی جدید ارائه‌شده در رابطه (۱۹) می‌تواند به‌عنوان مسئله‌ی تخصیص بودجه درنظرگرفته شود؛ که درآن بودجه موردنظر به‌گونه‌ای به $N+1$ متغیر $\left(c_1,...,c_N,c_{\text{recovery}}\right)$ تخصیص داده شود که $M(c)$یعنی حداقل‌زیان بدبینانه محافظان، حداقل گردد.

در این راستا، می‌توان دو نوع مسئله‌ی تخصیص بودجه به‌صورت زیر تشکیل داد:

۱) با فرض آن‌که بودجه‌ی R_0 ثابت است، محافظان باید یک استراتژی قابل‌اعتماد $\left(c_1,...,c_N,c_{\text{recovery}}\right)$ ارائه نمایند که با استفاده از آن $M(c)$ حداقل گردد.

۲) با فرض آن‌که $M(c)$ مشخص است، محافظان باید به یک استراتژی قابل‌اعتماد $\left(c_1,...,c_N,c_{\text{recovery}}\right)$ دست یابند و درنهایت بودجه‌ی نهایی برابر با مجموع عناصر $\left(c_1,...,c_N,c_{\text{recovery}}\right)$ است.

روش‌های حل برای دو نوع مسئله‌ی تخصیص بودجه فرض‌شده بالا به‌ترتیب در چارچوب دو الگوریتم حل A و B شرح داده شده است.

۴-۲- الگوریتم تخصیص بودجه A

مرحله۱) کل بودجه‌ی R_0 را مقداردهی اولیه و C=0 قرار دهید؛ به عبارت دیگر $\left(c_1,...,c_N,c_{\text{recovery}}\right)=0$. حال $r=c_1+c_2+...+c_N+c_{\text{recovery}}$ قرار دهید.

مرحله۲) توابع محافظتی $p_i(c_i)$ و توابع بازیابی $f_i\left(c_{\text{recovery}}\right)$ را برای N عنصر تعریف نمایید.

مرحله۳) تا زمانی‌که $(r<R_0)$ است، با استفاده از یکی ازروش‌های گرادیان معکوس، الگوریتم بهینه‌سازی تک‌هدفه یا چندهدفه سریع‌ترین مسیر کاهش را $c_j^{'}$ را پیدا کرده و $U_j^{'}(c)$ را محاسبه کنید.

مرحله۴) $\left(c_1,...,c_N,c_{\text{recovery}}\right)$ و $U_1(c),...U_M(c)$ را به‌عنوان خروجی درنظر بگیرید.

خروجی $\left(c_1,...,c_N,c_{\text{recovery}}\right)$ طرح نهایی تخصیص بودجه یا همان استراتژی قابل‌اطمینان برای محافظان است. $U_1(c),...U_M(c)$ زیان‌های نهایی تمامی اهداف پس از به‌کارگیری از استراتژی قابل‌اطمینان پیشنهادی می‌باشد. بنابراین حداکثر میزان $\max\{U_1(c),...U_M(c)\}$، زیان بدبینانه مورد انتظار به محافظان است.

۴-۳- الگوریتم تخصیص بودجه B

مرحله۱) فرض کنید $\left(c_1,...,c_N,c_{\text{recovery}}\right)=0$ و هم‌چنین $r=c_1+c_2+...+c_N+c_{\text{recovery}}$. هدف حداقل‌سازی مقدار حداکثر زیان بدبینانه‌ای (U) است که محافظان به‌دنبال آن هستند.

مرحله۲) توابع محافظتی $p_i(c_i)$ و توابع بازیابی $f_i\left(c_{\text{recovery}}\right)$ را برای N عنصر تعریف نمایید. زیان ابتدایی را برای تمامی اهداف M محاسبه نمایید و حداکثر را $U_j^{'}(c)$قرار دهید.

مرحله۳) تا زمانی‌که $\left(U_j^{'}(c)>U\right)$ است، با استفاده از یکی از روش‌های گرادیان معکوس، الگوریتم بهینه‌سازی تک‌هدفه یاچندهدفه سریع‌ترین مسیر کاهش را $c_j^{'}$ را پیدا کرده و $U_j^{'}(c)$ را محاسبه کنید.

مرحله۴) $\left(c_1,...,c_N,c_{\text{recovery}}\right)$و $U_1(c),...U_M(c)$ و r را به‌عنوان خروجی درنظر بگیرید. بردار خروجی $\left(c_1,...,c_N,c_{\text{recovery}}\right)$همان استراتژی قابل‌اطمینان برای محافظان سیستم قدرت است؛درحالی‌که $U_1(c),...U_M(c)$زیان مورد انتظار را برای تمامی M هدف است. ماکزیمم مقدار در میان تمامی درایه‌های این بردار نباید از مقدار U از پیش‌تعیین‌شده بیشتر باشد و r بودجه نهایی است که برای اتخاذ استراتژی مورد اطمینان دلخواه مورد نیاز است.

۵- شبیه‌سازی و مطالعات عددی

به‌منظور ساده‌سازی فرآیند بررسی نتایج، در این مطالعه $y_{\{s\}}$ تنها معادل انرژی ازدست‌رفته در سیستم فرض شده است؛ درحالی‌که خطوط انتقال و پست‌ها مورد هدف قرار گرفته‌اند. به‌علاوه بودجه‌ی R_0 یک کمیت بدون بُعد یعنی یک کمیت بدون‌واحد فیزیکی فرض‌می‌شود. هم‌چنین دو تابع درنظرگرفته‌شده در [۱۸] برای خطوط انتقال، در این پژوهش نیز به‌کار گرفته شده‌اند:

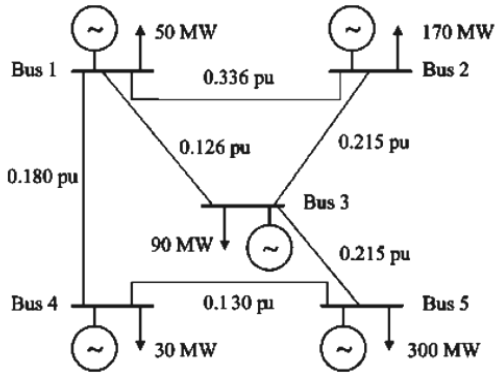
$$p_i(c_i)=1-\frac{c_i}{4+c_i} \qquad (۲۰)$$

$$f_i\left(c_{\text{recovery}}\right)=\frac{10}{10+c_{\text{recovery}}} \qquad (۲۱)$$

زمان ریکاوری پایه t_i^{base} یک ساعت درنظر گرفته شده است [۱۸]. به‌آسانی می‌توان نشان داد که الگوریتم‌های پیشنهادی به‌منظور شناسایی استراتژی‌های معتبر در یک دوره زمانی خاص برای سیستم‌های نمونه‌ی بزرگتر قابل‌تعمیم هستند. علاوه بر آن، می‌توان توابع احتمال و ریکاوری و حتی $y_{\{s\}}$ را برای هر هدف با توجه به وضعیت واقعی آن‌ها و منطبق با نیازهای بهره‌برداران سیستم به مدل‌های دقیق‌تر آن‌ها گسترش داد.

۵-۱- سیستم استاندارد مورد مطالعه

سیستم استاندارد مورد مطالعه در این پژوهش، یک سیستم با پنج باس و شش خط انتقال است [۱۰] که برای ترسیم صحیح روند اجرای الگوریتم‌های پیشنهادی و بیان استراتژی‌های معتبر محافظان و رقابت حذفی نهایی به‌کار گرفته می‌شود. سیستم نمونه پنج‌باس و تقاضاهای توان آن درشکل(۱) نشان داده شده است. راکتانس خط پریونیت به‌ترتیب با توان و ولتاژ مبنی $MVA100$ و $kV138$ بیان شده است.



شکل(۱): سیستم پنج باس

ظرفیت تمامی خطوط انتقال $MW100$ می‌باشند و تمامی ژنراتورها به‌ترتیب دارای حداقل و حداکثر ظرفیت توان 0 تا $MW150$ هستند.

همان‌گونه که در بخش قبل تشریح شد، دو سناریو مختلف درنظر گرفته می‌شود که در سناریو اول با بودجه ثابت، سعی در اتخاذ متدی از بازی هستیم که به‌وسیله آن تحت هرگونه استراتژی از سوی خرابکاران حداکثر صدمات ممکن به سیستم قدرت از حدمشخص-

شده‌ای بیشتر نشود. در سناریو دوم نیز حداکثر بودجه لازم برای دستیابی به یک روش خاص از بازی تعیین می‌شود که در آن حداکثر ریسک وارده به سیستم تحت شرایطی مشابه وضعیت قبل از حد مشخص شده‌ای بیشترنباشد. نکته قابل‌توجه آن‌که به‌کمک روش پیشنهادی علاوه‌بر خطوط انتقال می‌توان پست‌ها و یا نیروگاه‌ها را نیز مورد هدف قرار داد. البته با توجه به حراست شدید فیزیکی نیروگاه‌ها، هزینه صدمه‌زدن به آن‌ها بسیار بالا خواهد بود و چندان مقرون‌به‌صرفه نخواهد بود. درحالی‌که، چنین مسئله‌ای درمورد تجهیزات درون پست‌ها مانند ترانسفورماتورها و یا باسبارها با صرف هزینه کمتر ممکن است. در چنین شرایطی،ساده‌ترین وضعیت برای برنامه‌ریزان عملیات‌های خرابکارانه، تخریب خطوط انتقال است که تقریباً بدون حراست فیزیکی هستند. از این‌رو، در این مطالعه خطوط انتقال و پست‌ها هدف وقایع خرابکارانه عمدی قرار گرفته‌اند و از حمله به نیروگاه‌ها صرف‌نظر شده است، اگرچه روش پیشنهادی قابلیت تعمیم برای حملات خرابکارانه به هریک از ادوات سیستم را داراست.

۵-۲- سناریو ۱: الگوریتم تخصیص A

در این سناریو الگوریتم پیشنهادی تخصیص بودجه A (تشریح‌شده در بخش ۴-۲-) مورد بررسی قرار می‌گیرد.

۵-۲-۱- مطالعه موردی ۱

در این مطالعه موردی$n=1$ قرار داده شده یعنی هدف خرابکاران تنها متشکل از یک خط انتقال است. برای محاسبه انرژی مورد انتظار ازدست‌رفته (EEL) پس از آسیب به یک هدف بدون حفاظت، یک مدل پخش‌بارdc بهینه با برنامه‌ریزی خطی مورد استفاده قرار گرفت [۴]و [۲۵]. با توجه به مدل ارائه‌شده، به‌سادگی می‌توان مقادیر موجود

جدول (۲): انرژی ازدست‌رفته پس از انهدام یک هدف بدون حفاظت (سناریو۱- مطالعه موردی۱)

خط هدف	U_1: 4-5	U_2: 3-5	U_3: 1-2	U_4: 1-3	U_5: 2-3	U_6: 1-4
EEL (MWh)	50	50	0	0	0	0

درجدول (۲) را محاسبه نمود. در این جدول مقادیر EEL بعد از اجرای عملیات خرابکارانه در موردیک خط انتقال بدون حفاظت نشان داده می‌شود.

در این تحقیق دو الگوریتم تخصیص بودجه Aو B پیشنهادی برای مقادیر مختلف بودجه (10،20،30،40و50)، اجرا شده است. با اجرای الگوریتم تخصیص بودجه A و با بهره‌گیری از الگوریتم گرادیان منفی، الگوریتم بهینه‌سازی فاخته(COA) [۲۶] و الگوریتم چندهدفه [۲۵] $NSGAII$، استراتژی بهینه بازی در مقابل خرابکاران به‌منظور کمینه-سازی حداکثر مقدارEELتحت بودجه‌های ثابت به‌دست آمده است. جدول (۳) استراتژی‌های قابل‌اطمینان محافظان را در بودجه‌های مختلف نشان می‌دهد.EEL متناظر با استراتژی‌های تخصیص بودجه پیشنهادی محافظان در جدول (۳)، در جدول (۴) نشان داده شده است. همان‌گونه که از جدول (۴) قابل استنتاج است، میزان انرژی ازدست‌رفته مرتبط با هر یک از اهداف به‌میزان قابل‌توجهی کاهش یافته است. می‌توان مشاهده نمود زمانی که بودجه‌یR_0=10 باشد، استراتژی معتبر ممکن برای محافظانc_1=3.4050، c_2=3.1614، c_2=0.1807، c_{recovery}=3.2498 است و سایرین 0 هستند. بردار بودجه‌بندی را به صورت c=(3.4050, *3.1614, 0 , 0.1807, 0, 0, 3.2498*) نیز می‌توان بیاننمود.جدول (۴نشان می‌دهد که با توجه به این استراتژی، حداکثرEEL در میان تمامی اهداف U_2= 21.07MWh است. تا زمانی‌که $q=(q_1,q_2,0,0,0,0)$ و $q_1+q_2=1$ باشد، مقدار تابع رقابت حذفی $L=\sum_{i=1}^{6} q_i U_i(c) \le 21.07$ ، برقرار خواهد بود.

اگر مهاجمان به‌طور کامل از استراتژی محافظان آگاهی داشته باشند، بدین‌معنی‌که بدانند U_1 و U_2 متناظر با بیش‌ترین میزان EEL

جدول (۳): استراتژی‌های قابل‌اطمینان تحت میزان محدود بودجه (سناریو۱- مطالعه موردی۱)

متد	بودجه	استراتژی قابل اطمینان محافظان						
		c_1: 4-5	c_2: 3-5	c_3: 1-2	c_4: 1-3	c_5: 2-3	c_6: 1-4	C_{recovery}
فاخته	10	3.4050	3.1614	0	0.1807	0	0	3.2498
	20	4.8671	5.1329	0	0	0.0385	0	9.9615
	30	7.4858	7.5374	0	0	0	0	14.9768
	40	10.0162	9.9837	0	0	0	0	20
	50	12.9103	12.9382	0	0	0	0.2609	23.8906
گرادیان منفی	10	5	5	0	0	0	0	0
	20	8.6667	8.6667	0	0	0	0	2.6667
	30	12	12	0	0	0	0	6
	40	15.333	15.333	0	0	0	0	9.333
	50	18.667	18.667	0	0	0	0	12.667

جدول (۴): انرژی مورد انتظار ازدست‌رفته پس از اتخاذ استراتژی تخصیص پیشنهادی (سناریو۱- مطالعه موردی۱)

متد	بودجه	اهداف خرابکاران و انرژی از دست‌رفته مورد انتظار (MWh)					
		U_1: 4-5	U_2: 3-5	U_3: 1-2	U_4: 1-3	U_5: 2-3	U_6: 1-4
فاخته	10	20.3844	21.0777	0	0	0	0
	20	11.2995	10.9705	0	0	0	0
	30	6.9716	6.9544	0	0	0	0
	40	4.7564	4.7675	0	0	0	0
	50	3.4898	3.4840	0	0	0	0
گرادیان منفی	10	22.2000	22.2000	0	0	0	0
	20	12.4600	12.4600	0	0	0	0
	30	7.8100	7.8100	0	0	0	0
	40	5.3500	5.3500	0	0	0	0
	50	3.8900	3.8900	0	0	0	0

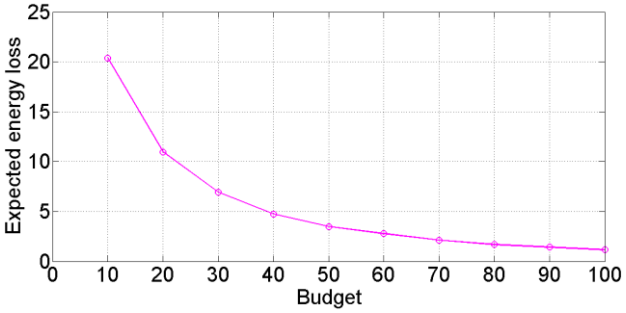
سیستم خواهد بود، آن‌ها باید استراتژی $q=(q_1,q_2,0,0,0,0)$ را

بـــرای واردآوردن حـــداکثر زیـــان بـــه‌مقـــدار $21.07MWh$اجرایـــی نمایند.درغیراین‌صورت، با بکارگیری هر نوع اسـتراتژی دیگـری نتیجـه رقابت حذفی به‌مقدار $21.07MWh$ نخواهد رسید.

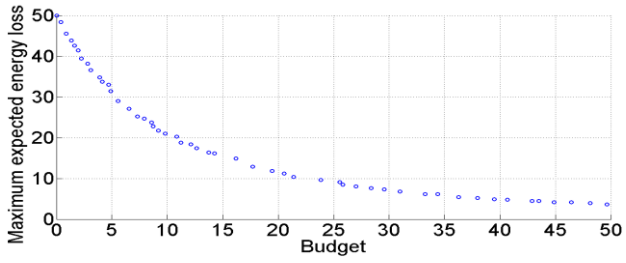
بنابراین تا زمـانی‌کـه محافظـان اسـتراتژی بـازی بـه‌دسـت‌آمـده یعنـی$(3.2498, 3.4050, 3.1614, 0, 0, 0.1807, 0)=c$ را بـه‌کـار گیرند،می‌توانند مطمئن باشند که خسارات وارده به سیسـتم از میـزان بدبینانه‌ی انرژی ازدست‌رفته $21.07MWh$ بیشتر نخواهد شد.

باید توجه داشت که به‌دست‌آوردن پاسخ مسئله تخصیص بودجـه بـه-کمک روش‌های مبتنی بر گرادیان منفی این مزیت را دارند که پـس از اجرا، پاسخ‌های به‌دسـت‌آمـده بـرای Uهـا (در اینجـا U_1 و U_2) برابـر خواهند شد، چراکه در ایـن روش بـه‌انـدازه ΔR_0 بـه U_1 اختصاصـداده می‌شود. در این‌صورت U_2 بیش‌ترین مقدار EEL را دارد و درنتیجه بـه-میزان ΔR_0 به U_2 اختصاص داده می‌شود و این روندادامه پیـدامی‌کنـد. اگرچه باید توجه داشت استفاده از این روش لزومـاً منجـر بـه رسـیدن جواب بهینه کلی نخواهد شد و عموماً وقت‌گیر هستند [[11]۱۱].

شکل(۲) تغییرات ماکزیمم مقـدار انـرژی ازدسـت‌رفتـه بدبینانـه را در مقابل افزایش بودجه تا$100C_{total}$ را نشان می‌دهد. همـان‌گونـه کـه دیده می‌شود، افزایش بودجه تخصیصی به‌منظور کاهش میزان خسارات با افزایش بیش از مقدار حدی$60C_{total}$، نمی‌تواند زیان‌هـای وارده را به‌صورت چشم‌گیری را کاهش دهد. در عمل نیز صـرف چنـین هزینـه بالایی به‌منظورکاهش نـاچیز میـزان انـرژی ازدسـت‌رفتـه در مصـالحه هزینه-سود جایگاهی نخواهد داشت.



شکل(۲): تغییرات EEL در مقابل افزایش بودجه



شکل(۳): پاسخ‌های نامغلوب EEL با بودجه کمتر از ۵۰

واضح است که به‌کارگیری الگوریتم‌های تک‌هدفه برای تخصـیص سطح خاصی از بودجه نمی‌تواند گستره‌ی خوبی از وضعیت سیستم در مقابل تهدیدات را نشان دهد، چراکه در آن تنها یک نقطه بهره‌بـرداری از سیستم مورد بررسی قرار می‌گیرد. در بسـیاری از مسـائل، تغییـرات پارامترهای سیستم نسبت به یکدیگر خطی، نمـایی و یـا بـدون قاعـده است. برای بررسی این مورد در مسئله حاضـر یـک الگـوریتم دوهدفـه به‌خدمت گرفته شده است. در واقع الگوریتم$NSGAII$ برای ایجـاد یـک مصالحه مناسب به‌خدمت گرفتـه شـده اسـت.شـکل(۳) مقـادیر EEL به‌ازای حداکثر بودجـه 50 واحـد را نشـان مـی‌دهنـد. بـه‌بیـان دیگـر پاسخ‌های به‌دست‌آمده از الگوریتم دوهدفه بازه‌هـای مـورد نیـاز بـرای اجرای الگوریتم تک‌هدفه را در اختیار محافظان قرار می‌دهد.

همان‌گونه که نتایج نشان می‌دهد با درنظرگـرفتن روابـط(۲۰) و (۲۱)، می‌توان اذعان نمود که رابطه میان سـرمایه‌گـذاری محافظـان و حداکثر مقدار تابع حذفی وارده توسط عوامل خرابکاردر یـک بـازی بـا حاصل صفر، تقریباً تکه‌ای خطی یا نمایی با شیب نزولـی اسـت. البتـه همان‌گونه که از شکل(۲) نیز قابل‌استنتاج است، افزایش بیشتر بودجـه این رابطه رابه‌سوی وضعیتی تقریباً خطی با شیب تقریباً صفر (قسـمت اشباع منحنی) سوق می‌دهد.

۵-۲-۲- مطالعه موردی ۲

در این مورد$n=2$ قرار داده شده یعنی هدف متشکل از دو خـط انتقـال است. در این وضعیت با توجه به رابطـه (۶) تعـداد 15 حالـت موجـود است. جدول (۵) انرژی ازدست‌رفته مورد انتظـار محافظـان را پـس از حذفهم‌زمان دو خط بدون حفاظت، نشان می‌دهد. با استفاده ازالگوریتم

جدول (۵): مقادیر EEL در مورد هدف قرارگرفتن هم‌زمان دو عنصربدون حفاظت(سناریو۱- مطالعه موردی۲)

خط انتقال هدف	EEL (MWh)	خط انتقال هدف	EEL (MWh)
U1: 3-5, 4-5	300	**U9: 2-3, 3-5**	100
U2: 2-3, 4-5	100	**U10: 1-2, 2-3**	40
U3: 1-4, 4-5	100	**U11: 1-2, 1-3**	20
U4: 1-2, 4-5	100	**U12: 1-3, 2-3**	0
U5: 1-3, 4-5	100	**U13: 1-2, 1-4**	0
U6: 1-2, 3-5	100	**U14: 1-4, 2-3**	0
U7: 1-3, 3-5	100	**U15: 1-3, 1-4**	0
U8: 1-4, 3-5	100		

جدول (۶): استراتژی‌های قابل‌اطمینان تحت میزان محدود بودجه (سناریو۱- مطالعه موردی۲)

بودجه	استراتژی قابل‌اطمینان محافظان						
	C_1: 1-2	C_2: 1-3	C_3: 1-4	C_4: 2-3	C_5: 3-5	C_6: 4-5	$C_{recovery}$
10	0	0	0	0	6.7271	2.0585	1.2175
20	0	0	0	0	6.9006	3.0994	10
30	0.2958	0.7611	0.4496	0.8589	6.6798	5.5690	15.3827
40	1.0169	1.0419	1.0184	1.0175	8.6546	7.3141	19.9375
50	1.3151	1.3099	1.3080	1.3152	10.6375	4.1761	29.9379

پیشنهادی A، استراتژی‌های معتبر محافظان در بودجه‌هـای مختلـف 10، 20، 30، 40 و50 در جـدول (۶) نشـان داده شـده اسـت. مقـادیر EEL پس از اتخاذ این استراتژی تخصیص بودجـه در جـدول (۷)ارائـه شده است. همان‌گونه که دیـده مـی‌شـود بـا درنظرگـرفتن اسـتراتژی حفاظتی مطابق جدول (۶)، حداکثر انرژی ازدست‌رفته بدبینانه متناظر

با میزان بودجه‌بندی‌های درنظرگرفته‌شده به‌ترتیب برابر با 77.283، 39.085، 27.188، 18.031و $14.051MWh$است. این درحالی است‌که بیشینه مقدار EEL قبل از اتخاذ این استراتژی‌ها از سوی محافظان برای انهدام هم‌زمان خطوط5-3و5-4 برابر با $300MWh$ بوده است.

۵-۲-۳- مطالعه موردی ۳

در این مطالعه موردی آسیب به پست‌ها مورد مطالعه قرار گرفته است. بدین‌صورت‌که با انهدام کامل پست، تمامی خطوط انتقال متصل به آن ازدست می‌روند. در این مورد$n=1$ قرار داده شده و هدف عملیات خرابکارانه تنها متشکل از یک پست انتقال است؛ چراکه احتمال آسیب هم‌زمان خرابکاران به دو پست و انهدام آن‌ها کمتر از حدی است که در این پژوهش مدنظر قرار گیرد. اگرچه، مطابق آنچه که پیش‌تر هم اشاره شده بود، در چنین وقایعی استراتژی‌هایی از بازی انتخاب می‌شودکه دارای احتمال بسیار کم هستند و امن‌کردن سیستم در مقابل تهدیدات عمدی هم‌زمان نسبت به دو پست نیازمند هزینه بسیار بالایی است. به‌عنوان مثال هدف قراردادن هم‌زمان دو شین 1 و 5 موجب ازدست‌رفتن 5 خط از 6خط در شبکه نمونه می‌شود. البته همان‌گونه که تکنیک پیشنهادی برای حذف هم‌زمان دو خط انتقال درنظر گرفته شده است، امکان تعمیم برای دو پست نیز وجود دارد.

جدول (۷): EELپس از اتخاذ استراتژی تخصیص پیشنهادی(سناریو۱- مطالعه موردی۲)

بودجه	اهداف مهاجمان و انرژی ازدست‌رفته مورد انتظار (MWh)							
	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8
10	77.283	74.118	74.085	74.118	74.022	61.295	61.216	**61.268**
20	39.022	39.085	39.085	39.085	39.085	34.173	34.173	**34.173**
30	27.188	23.091	25.206	26.106	23.564	25.308	22.844	**24.436**
40	18.031	18.029	18.025	18.031	17.942	17.532	17.445	**17.527**
50	13.538	14.032	14.051	14.032	14.046	11.997	12.009	**12.014**

بودجه	اهداف مهاجمان و انرژی ازدست‌رفته مورد انتظار (MWh)							
	U_9	U_{10}	U_{11}	U_{12}	U_{13}	U_{14}	U_{15}	
10	61.295	35.755	17.903	0	0	0	0	
20	34.173	20	10	0	0	0	0	
30	22.386	12.176	6.260	0	0	0	0	
40	17.530	8.500	4.233	0	0	0	0	
50	11.997	5.673	2.840	0	0	0	0	

جدول (۸): EELدر حمله به یک پست بدون محافظت

شین مورد هدف	خطوط انتقال ازدست‌رفته	EEL(MWh)
Bus 1	U1: 1-2, 1-3, 1-4	60
Bus 2	U2: 1-2, 2-3	170
Bus 3	U3: 1-3, 2-3, 3-5	140
Bus 4	U4: 1-4, 4-5	80
Bus 5	U5: 3-5, 4-5	300

مقادیر EEL در صورت حذف هر یک از پست‌های انتقال به‌شرح جدول (۸) آورده شده است. همان‌گونه که دیده می‌شود، باس ۵ دارای بیش‌ترین حساسیت نسبت به تخریب‌های عمدی است؛ به‌طوری‌که با جداشدن این شین از مدار حدود ۳۵٪ از بار کل شبکه ازدست می‌رود.

با استفاده از الگوریتم پیشنهادی A، استراتژی‌های معتبر محافظان در بودجه‌های مختلف 10، 20، 30، 40 و 50 در جدول (۹) نشان‌داده‌شده است. همان‌گونه که نتایج نشانمی‌دهد با صرف$50C_{\text{total}}$=، انرژی ازدست‌رفته $300MWh$ در باس پنجم به مقدار$9.3503MWh$ تقلیل می‌یابد. علاوه بر آن، این وضعیت تنها حالتی است که در آن به خط 4-1 بودجه تخصیص داده شده است که گویای حساسیت پایین این خط است.

۵-۳- سناریو ۲: الگوریتم تخصیص B

در این سناریو الگوریتم پیشنهادی تخصیص بودجه B (تشریح شده در بخش ۴-۳-) مورد بررسی قرار می‌گیرد. برخلاف سناریو گذشته که در آن میزان بودجه محافظان در تئوری بازی مشخص بوده است و تعیین بهترین استراتژی تخصیص بودجه به خطوط انتقال موردنظر بوده است،

جدول (۹): استراتژی‌های قابل‌اطمینان مدافعان تحت میزان محدود بودجه (سناریو۱- مطالعه موردی۳)

بودجه	استراتژی قابل‌اطمینان محافظان						
	C_1: 4-5	C_2: 3-5	C_3: 1-2	C_4: 1-3	C_5: 2-3	C_6: 1-4	$C_{recovery}$
10	2.7221	2.8337	1.1677	0	1.0372	0	2.2393
20	4.7873	4.7298	2.6335	0	2.5528	0	5.2963
30	6.4795	6.8555	3.9328	0	4.1262	0	8.6059
40	9.5327	6.9083	5.0937	0	5.1989	0	13.2664
50	12.2958	7.6909	6.3432	0	6.4375	0.2867	16.9459

جدول (۱۰): مورد انتظار ازدست‌رفته پس از اتخاذ استراتژی تخصیص پیشنهادی (سناریو۱- مطالعه موردی۳)

بودجه	اهداف خرابکارانو انرژی ازدست‌رفته مورد انتظار (MWh)				
	Bus 1	Bus 2	Bus 3	Bus 4	Bus 5
10	12.6484	85.3738	53.1674	53.4804	85.3738
20	7.8842	40.9080	25.5993	32.7348	40.9066
30	5.4201	22.6777	13.6477	22.5662	22.6777
40	3.7811	13.9754	9.5946	13.9746	13.9756
50	2.6784	9.3503	6.8125	9.3503	9.3503

در این سناریو حداکثر EEL بدبینانه دلخواه خطوط مشخص می‌شود و بر اساس آن، میزان بودجه موردنیاز محاسبه می‌شود.

۵-۳-۱- مطالعه موردی ۱

در این مورد$n=1$ قرار داده شده و هدف خرابکاران تنها متشکل از یک خط انتقال است.جدول (۱۱استراتژی‌های معتبر محافظان را به‌ازای مقادیر مختلف شاخص قابلیت‌اطمینان نشان می‌دهد. حداکثر مقدار بودجه قابل‌تخصیص به هر خط و بودجه ریکاوری 50 درنظر گرفته شده است. EEL به‌ازای مقادیر مختلف بودجه در جدول (۱۲) نشان داده شده است. به عنوان مثال، اگر محافظان بخواهند استراتژی معینی را درنظر بگیرند که توسط آن حداکثر EEL بدبینانه بدون توجه به روش بازی افراد خرابکار به میزان5% میزان قبلی شود، استراتژی $c=(0,\ 0,\ 0,\ 0,\ 32.2864,\ 14.9187,\ 14.9187)$ باید اجرا گردد که طی آن با اعمال هزینه $c_{total}=62.1238$، درصورت تخریب

عمدی یک خط انتقال، حداکثر مقدار انرژی ازدست‌رفته در هیچ صورتی بیش از $2.5MWh$ نخواهد شد.

۵-۳-۲- مطالعه موردی ۲

مطابق سناریو گذشته، در این مورد$n=2$ قرار داده شده است که درآن هدف حملات عمدی متشکل از دو خط انتقال است. با استفاده از متد پیشنهادی B و با به‌کارگیری الگوریتم تک‌هدفه COA، استراتژی‌های معتبر محافظان برای رسیدن به حداکثر EEL بدبینانه با مقادیر $25،15،5،2.5$ و$35MWh$ در جدول (۱۳) نشان داده شده است. EEL پس از اتخاذ استراتژی تخصیص بودجه B در ارائه شده است. حداکثر مقدار بودجه قابل تخصیص به هر خط و بودجه ریکاوری 100 درنظر گرفته شده است.

جدول (۱۱): استراتژی‌های قابل‌اطمینان تحت میزان مشخص انرژی ازدست‌رفته (سناریو۲- مطالعه موردی۱)

حداکثر EEL	استراتژی قابل‌اطمینان محافظان							هزینه کل
	C_1: 4-5	C_2: 3-5	C_3: 1-2	C_4: 1-3	C_5: 2-3	C_6: 1-4	$C_{recovery}$	
2.5	0	0	0	0	14.9187	14.9187	32.2864	62.123
5	0	0	0	0	9.7302	9.7298	19.1343	38.594
15	0	0	0	0	4	4	6.67	14.670
25	0	0	0	0	1.9936	1.9919	3.3520	7.3375
35	0	0	0	0	1.5394	1.5394	0.3160	3.3948

جدول (۱۲): انرژی مورد انتظار ازدست‌رفته پس از اتخاذ استراتژی تخصیص پیشنهادی (سناریو۲- مطالعه موردی۱)

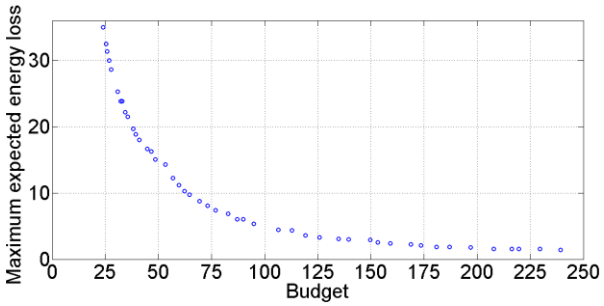
حداکثر EEL	اهداف خرابکاران و انرژی ازدست‌رفته بدبینانه مورد انتظار (MWh)					
	U_1: 4-5	U_2: 3-5	U_3: 1-2	U_4: 1-3	U_5: 2-3	U_6: 1-4
2.5	2.5000	2.5000	0	0	0	0
5	4.9999	4.9998	0	0	0	0
15	14.9970	14.9970	0	0	0	0
25	24.9988	24.9917	0	0	0	0
35	34.9990	34.9990	0	0	0	0

جدول (۱۳): استراتژی‌های قابل‌اطمینان تحت میزان محدود بودجه (سناریو۲- مطالعه موردی۲)

EEL	استراتژی قابل‌اطمینان محافظان							هزینه کل
	C_1: 4-5	C_2: 3-5	C_3: 1-2	C_4: 1-3	C_5: 2-3	C_6: 1-4	$C_{recovery}$	
2.5	10.9083	10.9083	10.9083	10.9083	31.5400	12.8391	56.4081	**144.4204**
5	3.4945	3.4945	3.4945	3.4945	14.6199	8.5131	60.4336	**97.5446**
15	0.8688	0.8688	0.8688	0.8688	8.1484	8.1484	26.4022	**46.1742**
25	0.9062	0.9062	0.9062	0.9062	8.8178	5.0597	13.5053	**31.0076**
35	0	0	0	0	6.6515	4.0683	11.3683	**22.0881**

نکته قابل توجه آن‌که در بسیاری از موارد در انجام بهینه‌سازی، علی رغم درنظرگرفتن یک حد از پیش‌تعیین شده برای حداکثرانرژی ازدست‌رفته، مقدار نهایی حاصل‌شده برای این پارامتر از حد انتظار کمتر شده است. به‌عنوان مثال با هزینه $c_{total}=144.4204$ برای رسیدن به حداکثر انرژی ازدست‌رفته $2.5MWh$، مقادیر U_6-U_{11} از این حد مورد انتظار نیز کمتر شده‌اند. باید اذعان نمود که در این حالت وضعیت سیستم از شاخص قابلیت‌اطمینان موردنظر بهتر شده است؛ اگرچه، این احتمال نیز وجود دارد که با توجه به ویژگی‌های ذاتی الگوریتم‌های تکاملی،پاسخ حاصله نتیجه گیرافتادن الگوریتم درنقاط بهینه محلی باشد و بتوان با صرف هزینه‌های کمتر، به نقاط مرزی قابلیت‌اطمینان که در آن دقیقاًU_6-$U_{11}=2.5$ برسیم.

با اجرای الگوریتم دوهدفه $NSGAII$ برای این مطالعه موردی، با درنظرگرفتن حداکثر انرژی ازدست‌رفته و حداکثر بودجه تخصیصی (مجموع بودجه تخصیصی به خطوط و ریکاوری) به‌عنوان دو تابع هدف مسئله، پاسخ‌های نامغلوب مطابق شکل (۴) به‌دست آمده است. حداکثر بودجه قابل‌تخصیص به خطوط و ریکاوری برابر 50 قرار داده شده است. این منحنی‌به‌ازای شاخص قابلیت اطمینان$35MWh$ محاسبه شده‌اند. همان‌گونه که دیده می‌شود کم‌ترین مقدار ممکن برای انرژی ازدست‌رفته $1.41MWh$ و با $c_{total}=239.2$ممکن است. بی‌شک یافتن سری پاسخ‌های ممکن توسط الگوریتم‌های چندهدفه به محافظان سیستم این امکان را می‌دهد که بودجه‌بندی را مبتنی بر نیازهای شبکه و توانایی‌های افراد تهدیدکننده برنامه‌ریزی کنند. البته باید اشاره نمود که این الگوریتم‌ها لزوماً همیشه بهترین پاسخ در یک بازه را به‌دست نمی‌آورند؛ چراکه برای رسیدن به یک سری از پاسخ‌ها،کل بازه را به چندین زیربازه تقسیم و در هر بازه تعدادی از کل جمعیت را مورد بررسی قرار می‌دهند؛ این درحالی است که الگوریتم‌های تک‌هدفه تمامی جمعیت را در راستای رسیدن به یک نقطه بهره‌برداری از سیستم به‌کار می‌گیرند.



شکل (۴): پاسخ‌های نامغلوب مسئله به‌ازای حداکثر انرژی ازدست‌رفته ۳۵ MWh (سناریو۲، مطالعه موردی ۲)

جدول (۱۴): انرژی مورد انتظار ازدست‌رفته پس از اتخاذ استراتژی تخصیص بودجه پیشنهادی (سناریو۲- مطالعه موردی۲)

حداکثر EEL	اهداف خرابکاران و انرژی ازدست‌رفته مورد انتظار (MWh)							
	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8
2.5	2.500	2.500	2.500	2.500	2.500	2.247	2.247	2.245
5	5.000	5.000	5.000	5.000	5.000	4.602	4.602	4.602
15	15.000	15.000	15.000	15.000	15.000	15.000	15.000	15.000
25	24.999	24.999	24.999	24.999	24.999	22.754	22.754	22.754
35	34.999	34.999	34.999	34.999	34.999	32.186	32.186	32.186
حداکثر EEL	اهداف خرابکاران و انرژی ازدست‌رفته مورد انتظار (MWh)							
	U_9	U_{10}	U_{11}	U_{12}	U_{13}	U_{14}	U_{15}	
2.5	2.247	0.433	0.216	0	0	0	0	
5	4.602	1.617	0.808	0	0	0	0	
15	15.000	7.416	3.708	0	0	0	0	
25	22.754	11.311	5.655	0	0	0	0	
35	32.186	18.719	9.359	0	0	0	0	

۵-۳-۳- مطالعه موردی ۳

در این مورد، از استراتژی B در مقابل حملات خرابکارانه به پست‌های انتقال استفاده می‌شود. در این قسمت حداکثر EEL در اثرازدست‌رفتن یکی از پست‌های انتقال تعیین و مطابق با آن حداقل بودجه مورد نیاز و نحوه تخصیص این بودجه در میان خطوط انتقال متصل به شین را مشخص می‌شود. حداکثر بودجه قابل تخصیص به هر یک از خطوط و ریکاوری برابر با 100 درنظر گرفته شده است. استراتژی‌های معتبر محافظان برای رسیدن به حداکثر EEL بدبینانه در جدول (۱۵) نشان داده شده است. مقادیر EEL پس از اتخاذ استراتژی تخصیص بودجه پیشنهادی در جدول ۱۵ ارائه شده است.

جدول (۱۵): استراتژی‌های قابل‌اطمینان تحت میزان محدود بودجه (سناریو۲- مطالعه موردی۳)

حداکثر EEL	استراتژی قابل‌اطمینان محافظان							هزینه کل
	C_1: 4-5	C_2: 3-5	C_3: 1-2	C_4: 1-3	C_5: 2-3	C_6: 1-4	$C_{recovery}$	
2.5	21.689	15.1839	12.279	0	13.1536	3.0383	28.9624	**94.3067**
5	15.481	10.9776	8.951	0	8.7667	1.4918	22.9009	**68.5697**
15	9.265	6.9082	4.945	0	5.1675	0	12.1142	**38.4020**
25	6.022	6.5376	3.833	0	3.6389	0	8.1822	**28.2159**
35	5.052	5.3364	2.888	0	2.9529	0	6.2262	**22.4566**

به‌منظور دستیابی به مجموعه پاسخ‌های ممکن برای مطالعه موردی حاضر، الگوریتم دوهدفه $NSGAII$ با هدف کمینه‌کردن هم‌زمان حداکثر EEL بدبینانه و همچنین حداقل‌سازی بودجه کل با شاخص $35MWh$ اجرا شده است. شکل (۵) مجموعه‌ای از پاسخ‌ها را برای سطح موردنظر قابلیت‌اطمینان نشان می‌دهد. همان‌گونه که دیده می‌شود، در باس‌های 5 و 2 به‌صورت حدی شاخص تعیین‌شده قابلیت‌اطمینان به‌دست می‌آید؛ اما در سایر باس‌ها مقادیرحاصل‌شده به مراتب پایین‌تر (بهتر) از حد مجاز است.جالب آن‌که نتایج تخصیص بودجه به‌نوعی حساسیت خطوط شبکه را نسبت به قطعی‌های طبیعی و یا خرابکارانه نشان می‌دهد. به‌عنوان مثال در جدول (۱۵): دیده می‌شود که خط 1-2 دارای حداکثر حساسیت است و بیش‌ترین بودجه را به‌خوداختصاص داده است؛ درحالی‌که خط 2-3 کم‌ترین حساسیت را داراست و در هیچ شرایطی بودجه‌ای را به‌خود تخصیص نداده است.

نکته‌ای که در اینجا مورد توجه است آن‌که در خصوص شبکه‌هایی که از لحاظ استراتژیکی در درجه دوم اهمیت‌اند، معقول‌ترین وضعیت برای محافظان آن است که (مطابق سناریو 1) در ابتدا با اجرای یک برنامه دوهدفه سری نقاط بهره‌برداری ممکن را برای محدوده بودجه دردسترس بررسی کنند و نهایتاً با درنظرگرفتن میزان بودجه نهایی، سطح قابلیت‌اطمینان ممکن و جزئیات تخصیص بودجه را به‌وسیله اجرای یک الگوریتم تک هدفه به‌دست آورند.اما در خصوص شبکه‌هایی که از لحاظ استراتژیکی در درجه اول بوده و بسیار حائز اهمیت‌اند، با تغیر خط مشی تخصیص، در ابتدا (مطابق سناریو ۲) یک الگوریتم دوهدفه به‌منظور محدودسازی حداکثر انرژی ازدست‌رفته بدبینانه) اجرامی‌شود و در نهایت با توجه به سری پاسخ‌های ممکن به‌دست‌آمده، تصمیم گرفته می‌شود که آیا برای حصول سطوح بالاتر قابلیت‌اطمینان نیازمند تخصیص بودجه چندین برابر هستیم یا نه؟ به بیان دیگر در مصالحه هزینه-قابلیت اطمینان کدام نقطه موردنظر خواهد بود. سپس با اجرای برنامه تک‌هدفه هزینه بهینه متناسب با قابلیت‌اطمینان موردنظر به‌دست می‌آید.

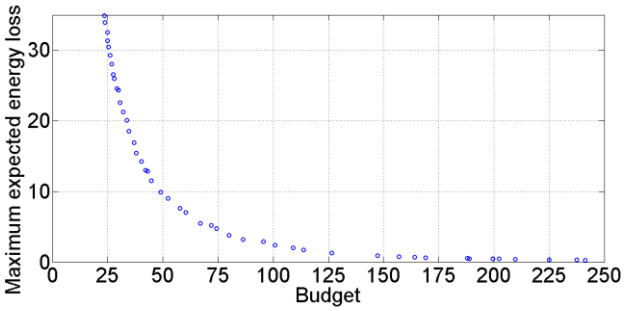
۶- نتایج

در دهه‌های اخیر مفهوم و منشأ تهدیدات و خاموشی‌های سراسری قالبی متفاوت نسبت به گذشته به‌خود گرفته است. تهدیدات عمدی و آسیب‌های خرابکارانه علیه ادوات و زیرساخت‌های سیستم قدرت به‌دلیل صدمات چشم‌گیر به سیستم برق‌رسانی کشورها با روندی صعودی مورد توجه پژوهشگران و گردانندگان این حوزه قرار گرفته‌اند. بدین‌دلیل، در این پژوهش یک طرح جدید به‌شرح زیر به‌منظور مقابله با تهدیدات عمدی انجام شد:

۱. فرمول‌بندی تهدیدات خرابکارانه و آسیب‌های عمدی به سیستم انتقال در قالب تئوری بازی به‌صورت یک رقابت حذفی با حاصل صفر.

جدول (۱۶): انرژی مورد انتظار ازدست‌رفته پس از اتخاذ استراتژی تخصیص بودجه پیشنهادی (سناریو۲- مطالعه موردی۳)

حداکثر EEL	اهداف خرابکاران و انرژی ازدست‌رفته مورد انتظار (MWh)				
	Bus 1	Bus 2	Bus 3	Bus 4	Bus 5
بدون حفاظت	60	170	140	110	300
2.5	0.7168	2.5000	1.7471	2.4983	2.4998
5	1.3675	5.0000	3.5606	5.0000	5.0000
15	4.0432	14.9980	10.1291	14.9960	14.9999
25	5.6155	24.9998	15.3014	24.1445	24.9958
35	7.1574	35.0000	21.2660	29.9542	35.0000



شکل(۵): پاسخ‌های نامغلوب مسئله به‌ازای حداکثر انرژی ازدست‌رفته ۳۵ MWh (سناریو۲، مطالعه موردی ۳)

۲. پیشنهاد دو الگوریتم تخصیص بودجه در مقابل تهدیدات عمدی نسبت به خطوط و پست‌های انتقال بدون درنظرگرفتن نوع استراتژی بازی تهدیدکنندگان سیستم: ۱) محاسبه بهترین شرایط تخصیص میزان ثابتی از بودجه به خطوط انتقال به‌منظور رسیدن به بهترین شرایط قابلیت‌اطمینان ۲) محاسبه بودجه لازم و نحوه تخصیص آن به‌منظور دستیابی به سطح از پیش‌تعیین‌شده‌ای از قابلیت‌اطمینان.

۳. اجرای الگوریتم‌های پیشنهادی برای ازکارانداختن ۱) پست‌های

شبکه انتقال ۲) حذف یک خط انتقال و یا حذف هم‌زمان دو خط انتقال.

۴. به‌کارگیری الگوریتم‌های تکاملی چندهدفه *NSGAII* و تک‌هدفه *COA* به‌عنوان ابزارهای بهینه‌ساز به‌ترتیب به‌منظور ۱) دستیابی به حدود سرمایه مورد نیاز و شاخص‌های اطمینان قابل دسترس سیستم ۲) تعین دقیق نقطه بهره‌برداری متناظر با هریک از سناریوها و متدهای تعریف‌شده.

۷- پیشنهاد کارهای آینده

۱. با توجه به آنکه در این پژوهش تنها حمله‌های تروریستی به خطوط انتقال و پست‌های انتقال شبیه‌سازی شده است، نویسندگان در نظر دارند الگوریتم ارائه‌شده را با حضور نیروگاه‌ها نیز اجرا نمایند. اگرچه مشکل اساسی در مدل‌سازی منابع تولید سنتی مربوط به توابع حفاظت و ریکاوری می‌باشد. علاوه بر آن نیروگاه‌های متفاوت (گازی، بخاری،آبی، هسته‌ای و ....) دارای توابع مختلف هستند، تعیین این توابع به دلیل پیچیدگی ساختار کنترلی نیروگاه‌ها به مراتب سخت‌تر از تعیین این توابع برای خطوط و پست‌های انتقال هستند.

۲. یکی از وضعیت‌های محتمل در صورت وقوع صدمات عمدی هدفمند، امکان رخداد چالش‌های دینامیکی برای کل شبکه است.از این‌رو، پژوهش حاضر را می‌توان با هدف کاهش احتمال فروپاشی دینامیکی شبکه پس از وقوع چند رخداد هم‌زمان اجرا نمود که به مراتب موجب خسارات‌های خواهد شد. اگرچه چالش اساسی در این مورد انجام مطالعات پایداری دینامیکی شبکه و نهایتاً انطباق آن با مدل تئوری بازی پیشنهادی در این مقاله است.

مراجع

[1] M. Kia and H. A. Aalami, "A New Approach for Optimal Location of Power Dispatching Centers Based on Passive Defense Criteria Using EAHP," Advanced Defense Sci. & Tech., 2014 (In Persian).

[2] DHS 2009, the 2009 National Infrastructure Protection Plan. Washington, DC, Department of Homeland Security. [Online]. Available: http://www.dhs.gov.

[3] G. Chen et al., "An improved model for structural vulnerability analysis of power networks," Physica A, vol. 388, pp. 4259–4266, 2009.

[۴] امینی‌فر فرخ، فرهومندی متین. مفاهیم و مبانی ارزیابی تاب‌آوری در شبکه‌های برق. نشریه مهندسی برق و الکترونیک ایران. ۱۳۹۷; ۱۵ (۳) :۸۳-۹۱

[۵] نصرت پور حسین، زنگنه علی. خودترمیمی بهینه شبکه‌های توزیع هوشمند مبتنی بر گراف درخت پوشا و بهبود قابلیت اطمینان شبکه .نشریه مهندسی برق و الکترونیک ایران. ۱۳۹۸; ۱۶ (۱) :۹۱-۱۰۱

[6] Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. Washington, DC: National Academy Press, 2002, Committee on Science and Technology for Countering Terrorism, National Research Council.

[7] R. Ghaffarpour, Y. Hashemi and M. Ehsan, "Applying a Novel Defensive Approach to Commitment Scheduling of Generating Units and Providing a New Probabilistic Technique for Their inaccessibility," Advanced Defense Sci. & Tech., 2015 (In Persian).

[8] R. Ghaffarpour, E. Barzegar and M. Ehsan, "Optimal Displacement of TCSC in Transmission System Buses Utilizing Smart Approaches Aiming at Sensitivity Reduction," Advanced Defense Sci. & Tech., 2014 (In Persian).

[9] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," IEEE Trans. Power Syst., vol. 19, no. 2, pp. 905–912, May 2004.

[10] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," IEEE Trans. Power Syst., vol. 20, no. 2, pp. 789–797, May 2005.

[11] A. Motto, J. M. Arroyo, and F. D. Galiana, "A mixed integer LP procedure for the analysis of electric grid security under disruptive threat,"IEEE Trans. Power Syst., vol. 20, no. 3, pp. 1357–1365, Aug. 2005.

[12] D. Fudenberg and J. Tirole, Game Theory. Cambridge, MA: MIT Press, 1991.

[13] J. Von Neumann and O. Morgenstern, Theory of Games and Economic Behavior. Princeton, NJ: Princeton Univ. Press, 1944.

[14] D. M. Kreps, Game Theory and Economic Modeling. Oxford, U.K.: Oxford Univ. Press, 1990.

[15] R. Powell, "Defending against strategic terrorists over the long run: A basic approach to resource allocation," Institute of Governmental Studies, Sep. 2006.

[16] E. Cornell and S. Guikema, "Probabilistic modeling of terrorist threat: A systems analysis approach to setting priorities among countermeasures," Military Oper. Res., vol. 7, no. 4, pp. 5–20, Dec. 2002.

[17] R. Hohzaki and S. Nagashima, "A Stackelberg equilibrium for a missile procurement problem," Eur. J. Oper. Res., vol. 193, pp. 238–249, Feb. 2009.

[18] A. Holmgren, E. Jenelius, and J.Westin, "Evaluating strategies for defending electric power networks against antagonistic attacks," IEEE Trans. Power Syst., vol. 22, no. 1, pp. 76–84, Feb. 2007.

[19] G. Owen, Game Theory, 3rd ed. New York: Academic, 1995.

[20] B. Rustem and M. Howe, Algorithms for Worst-Case Design and Applications to Risk Management. Princeton, NJ: Princeton Univ. Press, 2002.

[21] M. Willem, Minimax Theorems. Cambridge, MA: Birkhauser, 1996.

[22] B. Ricceri and S. Simons, M inimax Theory and Applications. Nor-well, MA: Kluwer, 1998.

[23] M. Sion, On general minimax theorems,Pacific J. Math. , no. 8, pp. 171–176, 1958.

[24] V. F. Demyanov and A. B. Pevnyi, Numerical methods for finding saddle points, USSR comp, Math. Math. Phys., no. 12, pp. 1099–1127, 1972.

[25] J. Chen, J. S. Thorp, and I. Dobson, Cascading dynamics and mit-igation assessment in power system disturbance via a hidden failure model, Elect. Power Energy Syst., vol. 27, pp. 318–326, 2005.

[26] Rajabioun, R. Cuckoo optimization algorithm. Applied soft computing, 11(8), 5508-5518, 2011.

[27] Srinivas, N., & Deb, K. Muiltiobjective optimization using nondominated sorting in genetic algorithms. Evolutionary computation, 2(3), 221-248, 1994.