نشریه علمی پدافند غیرعامل

سال دهم، شماره ۲، تابستان ۱۳۹۸، (پیاپی ۳۸): صص ۳۱-۱۵

بررسی روش‌های تخصیص بهینه منابع برای دفاع از شبکه‌های برق در مقابل حملات عامدانه

رضا غفارپور[1*]، سعید صیادی‌پور[2]

تاریخ دریافت: ۱۳۹۵/۰۷/۱۰
تاریخ پذیرش: ۱۳۹۶/۰۴/۱۹

چکیده

گزارش‌ها و آمارهای بین‌المللی نشان می‌دهند که در سال‌های اخیر، شبکه‌های برق یکی از اهداف اصلی گروه‌های تروریستی قرار گرفته‌اند. شبکه برق، در هر کشوری نقشی اساسی را ایفا می‌کند و حیات همه زیرساخت‌های یک کشور وابسته به عملکرد صحیح این شبکه است. بین اقتصاد و صنعت برق هر کشور، ارتباط تنگاتنگی وجود دارد و در صورت مختل‌شدن عملکرد شبکه برق، می‌توان ضررهای اقتصادی عظیمی را برای آن کشور متصور شد. بنابراین، تعداد بسیاری از محققان به دنبال پاسخ به این سؤال که برای کاهش پیامدهای ناشی از حملات عامدانه، چگونه باید منابعِ دفاعی در دسترس را به‌صورت بهینه تخصیص‌دهی کرد، به ارائه مدل‌های متعددی پرداخته‌اند. آگاهی برنامه‌ریز شبکه برق از این روش‌ها، می‌تواند برای انتخاب بهترین راهکار دفاعی برای دفاع از شبکه برق در مقابل حملات عامدانه، مفید باشد. تا به حال هیچ مقاله مروری، برای گردآوری این روش‌ها نوشته نشده است. از این رو، در این مقاله سعی شده است که مروری کامل بر مهم‌ترینِ این مدل‌ها صورت گیرد و یک دسته‌بندی مناسب از این مدل‌ها ارائه شود. در ادامه، مدل‌های مربوط به هر دسته، با تمرکز بر نقاط ضعف و قوت آن‌ها، مورد بررسی و تحلیل قرار گرفته‌اند.

کلیدواژه‌ها: حملات عامدانه، تحلیل آسیب‌پذیری شبکه برق، تخصیص بهینه منابع، انتخاب بهینه راهبرد دفاعی

۱- استادیار، دانشگاه جامع امام حسین (ع)، (rghaffarpour@ihu.ac.ir) - نویسنده مسئول
۲- کارشناس ارشد، دانشگاه صنعتی اصفهان

۱- مقدمه

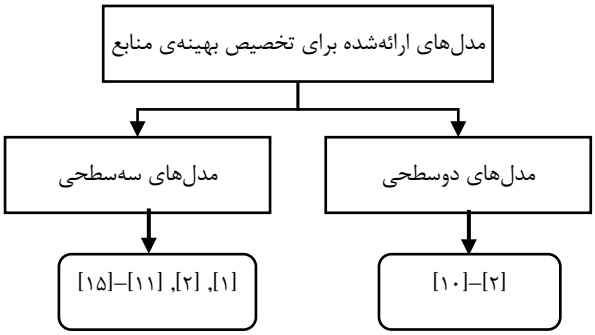
شبکه‌های برق در سراسر دنیا، به شالوده توسعه اقتصادی تبدیل شده‌اند [۱]، که همچون سایر زیرساخت‌های مهم یک کشور، به‌عنوان یکی از اهداف مهم حملات تخریب‌گرانه قرار گرفته‌اند. برای استحکام شبکه برق، برنامه‌ریز شبکه[1] در ابتدا نیاز دارد تا با ابزاری مناسب به شناخت نقاط ضعیف شبکه در مقابل حملات عامدانه بپردازد و پس از آن، با در نظر گرفتن منابع محدودی که در دست دارد، به انتخاب بهترین راهبرد دفاعی بپردازد. به‌منظور فراهم آوردن ابزار نخست، پژوهشگران بسیاری به ارائه مدل‌های ریاضی پیچیده برای ارزیابی آسیب‌پذیری یک شبکه برق در مقابل حملات عامدانه پرداخته‌اند. اگرچه این مدل‌ها در شناسایی نقاط ضعیف شبکه کارآمد هستند، اما برای انتخاب یک راهبرد دفاعی بهینه و تخصیص بهینه منابع (ORA)[2]، نمی‌توان بر نتایج این‌مدل‌ها تکیه کرد [۲]. هدف این مقاله، بررسی مهم‌ترین مدل‌هایی است که در مجلات و نشریات معتبر علمی برای تخصیص بهینه منابع، ارائه شده‌اند.

در ادامه، در بخش دوم این مقاله، دسته‌بندی مناسبی بر روی مدل‌های ارائه‌شده برای تخصیص بهینه منابع صورت می‌گیرد. پس از آن، در بخش‌های سوم و چهارم به بررسی مدل‌های مربوط به هر یک از دسته‌بندی‌ها پرداخته و با تکیه بر نوآوری آن‌ها، جزئیات بیشتری درخصوص مقالات هر دسته ارائه خواهد شد. در ادامه، در بخش پنجم، نتیجه‌گیری بحث و همچنین موضوعات مربوط به تحقیقات آینده بیان خواهد شد. پس از آن، در بخش ششم فهرستی از نمادها و علائم استفاده‌شده در این مقاله ارائه می‌شود و در آخر، در بخش هفتم، مراجع مورد بررسی ارائه خواهند شد.

۲- دسته‌بندی مدل‌های ارائه‌شده برای تخصیص بهینه منابع

تحقیقات انجام‌شده در زمینه تخصیص بهینه منابع را می‌توان به‌طور کلی در دو دسته «مدل‌های دوسطحی» و «مدل‌های سه‌سطحی» جای داد (۰). در مدل‌های دوسطحی، معمولاً کنش و واکنش بین یک مدافع (اپراتور یا برنامه ریزشبکه) و یک مهاجم (گروه تروریست)، به‌صورت یک مدل مدافع-مهاجم (DA)[3] فرمول‌بندی می‌شود. هدف نهایی مدافع در مدل‌های دوسطحی آن است که منابع خود را به‌گونه‌ای تخصیص دهد که دستاورد مهاجم از حمله به شبکه (خسارت)، کمینه‌شده و یا از یک مقدار از پیش‌تعیین‌شده، کمتر شود.

در مدل‌های سه‌سطحی، مدافع به تمام کنش‌های ممکن برای مهاجم، پاسخ بهینه داده و سپس منابع خود را به‌گونه‌ای تخصیص می‌دهد که مهاجم نتواند حتی با اجرای بدترین حمله، میزان خسارت واردشده را از یک حد خاص بیشتر کند. ماهیت چنین کنش و واکنشی به‌صورت یک مسأله سه‌سطحی از نوع مدافع-مهاجم-مدافع (DAD)[4] است که در بخش پنجم به بیان جزئیات بیشتری در این خصوص خواهیم پرداخت.



شکل (۱): دسته‌بندی مدل‌های ارائه‌شده برای تخصیص بهینه منابع

۳- مدل‌های دوسطحی ارائه‌شده برای ORA

فرم کلی مدل‌های دوسطحی، به‌صورت یک مسأله min-max است که در آن، مهاجم سعی در بیشینه کردن خسارت دارد و مدافع به دنبال کمینه کردن تابع هدف مهاجم، از طریق تخصیص بهینه منابع است. در کاربرد شبکه برق، خسارت به میزان بار و یا انرژی قطع‌شده اطلاق می‌شود [۵]. در برخی مراجع، هزینه بهره‌برداری شبکه و هزینه بار قطع‌شده نیز به‌عنوان خسارت در نظر گرفته شده است [۱۱].

اسکاپرا [۶]، در یک مدل دوسطحی، به‌طور کلی به بررسی موضوع تخصیص بهینه منابع برای دفاع از زیرساخت‌های یک کشور پرداخته است. مدل ارائه‌شده در این مقاله سعی در ارائه بهترین راهکار دفاعی به‌گونه‌ای دارد که خسارت ناشی از حمله به تعداد r تجهیز دفاع نشده، کمینه شود. در مسأله سطح بالای این مدل، تصمیم‌گیری درخصوص تجهیزاتی که باید دفاع شوند صورت می‌گیرد. در سطح پایین نیز، بدترین حملاتی که بیشترین خسارت را وارد می‌کنند مدل شده‌اند. تابع هدف این مسأله دوسطحی به‌صورت زیر بیان می‌شود:

[1] Network Planner
[2] Optimal Resource Allocation
[3] Defender-Attacker
[4] Defender-Attacker-Defender

$$\min\left(\max\left(\sum_{n\in H}\sum_{j\in F} D_n U_{nj}\vartheta_{nj}\right)\right) \quad (۱)$$

این تابع هدف، بیان‌گر فاصله وزن‌دهی‌شده برای تأمین تقاضای گره‌های مختلف سیستم (که الزاماً شبکه برق نیست، بلکه مجموعه‌ای از زیرساخت‌ها است)، پس از حمله به تعدادی از تجهیزات سیستم است.

در تحقیقی دیگر، هولمگرِن[1] [۴] به ارزیابی راهبردهای دفاع از شبکه برق در مقابل حملات خصومت آمیز[2] پرداخته است. این مقاله نشان می‌دهد که چگونه می‌توان با استفاده از مفاهیم تئوری بازی، راهبردهایی مناسب برای دفاع از شبکه برق در مقابل حملات خصومت آمیز یافته و این راهبردها را ارزیابی نمود. این مقاله [۴]، به مدل کردن طرف مهاجم و مدافع می‌پردازد و با بیان تعاملات مختلفی که ممکن است بین مهاجم و مدافع وجود داشته باشد، راهکارهای دفاعی مناسبی ارائه می‌کند. مدل‌های ارائه‌شده، جنبه‌های احتمالاتی موجود در حمله و دفاع را در نظر می‌گیرد. در این مقاله، ابتدا مدلی ارائه شده است تا مدافع شبکه بتواند منابع مالـی خود (C_{Total}) را بین دو راهکار حفاظت ($C_{Protection}$) و بازیـابی ($C_{Recovery}$) المان‌های شبکه تقسیم کند. اگر شبکه تحت مطالعه شامل J المان باشد، برای هر المان j، یک تابع حفاظت e_j تعریف می‌شود به این مفهوم که اگر به این المان حمله شود، احتمال تخریب نشدن و سالم ماندن این المان چقدر است. به بیان دیگر، می‌توان گفت که احتمال موفقیت مهاجم در حمله به المان j برابر با e_j و $1-e_j$ است. تابع e_j وابسته به بودجه‌ای است که اپراتور شبکه برای حفاظت از المان j صرف کرده است. مدت زمانی که طول می‌کشد تا یک المان تخریب‌شده بازیابی شود، بستگی به نوع المان و بودجه‌ای که برای بازیابی آن المان اختصاص داده شده، دارد. در ادامه، خواهیم دید که، مهاجم می‌تواند چندین نوع حمله انجام دهد (حمله اتفاقی[3]، حمله مبتنی بر احتمال[4] و بدترین حمله[5]). بنابراین، زمان بازیابی المان تخریب‌شده، می‌تواند وابسته به نوع حمله نیز باشد. اگر t_j^{base} بیان‌گر زمان پایه برای تعمیر المان تخریب‌شده j، بدون بودجه اضافی باشد، آن‌گاه اگر مدافع تصمیم به در نظر گرفتن بودجه بیشتر برای تعمیر و بازیابی آن المان بگیرد، زمان مورد نیاز برای بازیابی کامل آن به‌صورت زیر است:

$$t_j = t_j^{base}.f_j(c_{Recovery}) \quad (۲)$$

در این مقاله (و سایر مقالات) فرض بر این است که مهاجم به قدر کافی توانمند است و از اطلاعات کافی نیز برای حمله به شبکه برق برخوردار است [۲] و [۴]. اگر ترکیب یک یا چند المان شبکه را یک «هدف[6]» بنامیم، آن‌گاه مسأله مهاجم، انتخاب بهترین راهبرد حمله و انتخاب بهترین هدف‌ها است. مجموعه T بیان‌گر مجموعه هدف‌های ممکن و M بیان‌گر تعداد این هدف‌هاست. به‌عنوان مثال، اگر فرض کنیم که در یک زمان، تنها به یک المان حمله می‌شود، آن‌گاه $M=J$، که J تعداد المان‌های شبکه است. اما اگر فرض کنیم که مهاجم می‌تواند به‌طور همزمان به $k>1$ المان حمله کند، آن‌گاه T مجموعه تمام ترکیب‌های شامل k المان $\{i_1, i_2, \ldots, i_k\}$ است:

$$M = \binom{J}{k} \quad (۳)$$

شخص یا گروه مهاجم می‌تواند به‌طور تصادفی از بین هدف‌های فوق، راهبرد خود را انتخاب کند. q_j احتمال انتخاب هدف j توسط مهاجم و حمله به آن به شرط وقوع حمله است:

$$q_j = P(target\ j\ is\ attacked\ |\ attack) \quad (۴)$$

برای مدل‌سازی برهم‌کنش مدافع و مهاجم نیز سه نوع حمله برای مهاجم در نظر گرفته می‌شود [۴]:

۱- بدترین حمله: در این حالت مهاجم سعی بر بیشینه کردن متوسط خسارت دارد و مدافع در پی کمینه کردن این مقدار است. لذا می‌توان این مسأله را به‌صورت زیر مدل کرد:

$$\max_q\left[\min_c \sum_{j=1}^{M}\mu_j(c).q_j\right] \quad (۵)$$

۲- حمله مبتنی بر احتمال: در این راهبرد حمله، مدافع سعی در کمینه کردن احتمال پی‌آمدهای حمله بیش از یک مقدار مشخص ($y_{\min}$) دارد، در همین حال، مهاجم در پی بیشینه کردن این احتمال است. یعنی:

$$\max_q\left[\min_c \sum_{j=1}^{M} P\left(Y_j > y_{\min}\right)q_j\right] \quad (۶)$$

۳- حمله اتفاقی: وقتی که مهاجم هدف خود را به‌صورت اتفاقی انتخاب می‌کند، مسأله پیش روی مدافع، از یک بازی تبدیل

[1] Holmgren
[2] Antagonistic Attacks
[3] Random Attack
[4] Probability-based Attack
[5] Worst-case Attack
[6] Target

به یک مسأله تصمیم‌گیری می‌شود. در این حالت راهبرد مهاجم به‌صورت ساده زیر خواهد بود:

$$q_j = \frac{1}{M}, \quad j = 1,2,\ldots,M \qquad (۷)$$

در مرجع [۴] فرض بر آن است که مدافع، در پی کمینه کردن متوسط کلِ پی‌آمدهای حمله است. این مسأله حالت خاصی از مسأله بدترین حمله است. تابع هدف مدافع به‌صورت زیر تعریف می‌شود:

$$\min_{c} \frac{1}{M} \sum_{j=1}^{M} \mu_j(c) \qquad (۸)$$

در تحقیقی دیگر، چن[1] [۳]، کار هولمگرن [۴] را توسعه داده است. در این مقاله [۳]، برای برهم‌کنش بین مدافع و مهاجم مدل دیگری ارائه شده و در ضمن، برای کمک به مدافع در انتخاب بهترین راهبرد دفاع، دو مدل جدید نیز ارائه شده تا به دو سؤال زیر پاسخ دهد:

۱- وقتی که مدافع شبکه، بودجه محدود دارد، چگونه باید آن را برای داشتن یک راهبرد دفاعی مناسب و بهینه اختصاص دهد؟

۲- اگر مدافع شبکه بخواهد که تلفات ناشی از حمله را به یک مقدار مشخص محدود کند، چقدر بودجه نیاز دارد تا یک راهبرد دفاعی مطمئن به‌کار گیرد؟

هدف اصلی این مقاله [۳]، پاسخ به این سوال است که اگر مدافع مقدار y_S (متوسط تلفات حمله به هدف j، که S زیرمجموعه‌ای از مجموعه j می‌باشد) را بداند، آن‌گاه چگونه باید یک راهبرد دفاعی مؤثر در مقابل تمام حملات ممکن اتخاذ کند. انواع بازی‌هایی که ممکن است بین مدافع و مهاجم وجود داشته باشد به‌صورت زیر است[۴]:

۱- بازی استاتیک: در این نوع بازی، به‌طور همزمان، مدافع یک راهبرد دفاعی c (همان تخصیص بودجه) را اتخاذ و مهاجم یک راهبرد حمله را طراحی می‌کند.

۲- بازی دینامیکی: در بازی دینامیک فرض بر این است که مهاجم از راهبرد مدافع بی‌اطلاع است، در حالی که در واقعیت، گروه مهاجم می‌تواند از راه‌های مختلفی همچون اخاذی و رشوه دادن، از راهبرد دفاعی اتخاذشده توسط مدافع مطلع شود و پس از آن به طراحی راهبرد حمله بپردازد[۱]، [۳] و [۴].

۳- تعدد بازی‌ها[2]: در دو نوع بازی قبل، یا مهاجم از راهبرد مدافع اطلاع نداشت و یا اینکه به‌طور کامل از تصمیم مدافع مطلع بود. حالتی نیز وجود دارد که مهاجم تنها بخشی از تصمیمات مدافع و راهبرد انتخابی او را می‌داند که این موضوع، بازی‌های موجود بین مهاجم و مدافع را متنوع می‌سازد.

در مقاله [۳] سعی بر آن است که، چارچوب جامعی[3] برای در نظر گرفتن انواع بازی‌ها ارائه شود. در فاز اول این چارچوب، مدافع به انتخاب یک راهبرد دفاعی می‌پردازد و در این مرحله هیچ اطلاعی از تصمیمات مهاجم ندارد. در فاز دوم، مهاجم یک راهبرد حمله انتخاب می‌کند و بسته به سه نوع بازی مطرح‌شده، سه نوع مهاجم مختلف تعریف می‌شود. بنا به نظریه مدیریت ریسک، برای هر راهبرد که مدافع در پیش می‌گیرد، یک مقدارِ بیشینه برای تلفاتی که مهاجم می‌تواند موجب شود، وجود دارد. اگر فضای راهبردهای ممکن برای مدافع را C و فضای موجود برای راهبردهای مهاجم را Q بنامیم، آن‌گاه اگر فرض کنیم که مدافع تصمیم به اجرای راهبرد دفاعی $c' \in C$ گرفته، حتماً یک راهبرد حمله بهینه برای مهاجم وجود دارد که از برنامه‌ریزی ریاضی با تابع هدف زیر به‌دست می‌آید و آن را q' می‌نامیم:

$$\max_{q \in Q} \sum_{j=1}^{M} q_j \mu_j(c') \qquad (۹)$$

دو حالت وجود دارد؛ اگر بازی مطرح‌شده بین مدافع و مهاجم از نوع استاتیکی باشد و یا اینکه اطلاعات مهاجم محدود باشد، در این حالت احتمال (ریسک) انتخاب q' توسط مهاجم وجود دارد. در حالت دوم، اگر بازی از نوع دینامیکی باشد، مهاجمِ خبره و کارآزموده قطعاً راهبرد q' را انتخاب می‌کند. q' در واقع متناظر با بدترین حالت ممکن است و به همین خاطر، تلفات ناشی از آن را «بدبینانه‌ترین تلفات» می‌نامیم. نتیجه مهمی که می‌توان گرفت این است که اگرچه راهبردهای حمله مختلفی برای مقابله با راهبرد دفاعی c' وجود دارد، اما مهاجم تنها می‌تواند احتمال و ریسک انتخاب راهبرد q' را بالا ببرد و نه مقدار تلفات متناظر با q' را. پس می‌توان گفت که یک راهبرد دفاعی بهینه سراسری وجود دارد که می‌تواند مقدار این بدبینانه‌ترین تلفات را کمینه کند.

برای هر راهبرد دفاعی $c \in C$، یک راهبرد حمله بهینه وجود دارد که همان‌طور که پیش‌تر گفته شد، از یک برنامه‌ریزی ریاضی

[1] Chen

[2] Manifoldness of Games

[3] Comprehensive Framework

به‌دست می‌آید. حال، مدافع می‌تواند مقدار بدبینانه‌ترین تلفات را که متناظر با q' است، کمینه کند. این راهبرد از برنامه‌ریزی ریاضی با تابع هدف زیر به‌دست می‌آید:

$$\min_{c\in C}\max_{q\in Q}\sum_{j=1}^{M} q_j\mu_j(c') \qquad (۱۰)$$

اگر پاسخ به‌دست‌آمده از این برنامه‌ریزی را (q^0,c^0) بنامیم و مقدار تابع هدف در این حالت y^0 باشد، به این مفهوم است که اگر مدافع، راهبرد دفاعی c^0 را انتخاب کند، راهبرد حمله بهینه برای مهاجم، q^0 است و مستقل از اینکه مهاجم چه نوع راهبردی را انتخاب کند، مقدار تلفات واردشده به سیستم، از مقدار y^0 تجاوز نمی‌کند، که y^0 کمترین مقدار تلفات ممکن به ازای بهترین راهبرد حمله q^0 است. پس c^0 همان راهبرد مطمئن برای مدافع شبکه است و برای انتخاب راهبرد دفاعی مطمئن، یک معیار به این صورت تعریف می‌شود: «راهبرد دفاعی بهینه، c^0 و کمترین مقدار ممکن برای بدبینانه‌ترین تلفات، L^0 است که هر دوی این مقادیر، از روابط زیر به دست می‌آیند»:

$$c^0=\arg\min_{c\in C}\left[\max_{q\in Q}\sum_{j=1}^{M} q_j\mu_j(c')\right] \qquad (۱۱)$$

$$y^0=\min_{c\in C}\left[\max_{q\in Q}\sum_{j=1}^{M} q_j\mu_j(c')\right] \qquad (۱۲)$$

در تحقیقی دیگر، لِویتین[1] [۸] به ارائه مدلی دوسطحی برای انتخاب بهینه راهبرد دفاعی در مقابل حملات عامدانه به یک سیستم که در حالت کلی المان‌های آن دارای ترکیبات سری-موازی هستند، پرداخته است. در ادامه، ابتدا به توضیح مقدمات و تعاریف این مدل پرداخته و سپس مدل نهایی را ارائه خواهیم داد. در این مدل، فرض بر آن است که هر یک از F تجهیز مستقل شبکه، خود از J_j المان تشکیل شده است. برای هر یک از این المان‌ها دو گزینه «جدایی[2]» و «دفاع» وجود دارد که گزینه جدایی، برای جلوگیری از تخریب کارآیی کل تجهیز در نظر گرفته شده است. المان‌هایی که جدا نشده‌اند، یک «گروه حفاظت (PG)[3]» نامیده می‌شوند که باید محافظت شوند. یک حمله موفق به یک PG باعث تخریب کل المان‌های آن می‌شود و از سوی دیگر، یک حمله نمی‌تواند بیش از یک PG را تخریب کند. مسأله جدایی برای المان‌های یک تجهیز را می‌توان به‌صورت تفکیک مجموعه J_j به تعداد M_j زیرمجموعه Φ_{jm} که دو به دو منفصل هستند تعریف کرد:

$$\bigcup_{m=1}^{M_j}\Phi_{jm}=J_j \qquad (۱۳)$$

$$\Phi_{jr}\bigcap\Phi_{js}=\phi;\quad r\neq s \qquad (۱۴)$$

تفکیک مجموعه J_j را می‌توان به‌صورت بردار $\{\varphi_{jn},1\le n\le|J_j|\}$ تعریف کرد که φ_{jn} شماره زیرمجموعه‌ای است که المان n به آن تعلق دارد. ماتریس φ متشکل از بردارهای φ_{jn} به ازای تمام المان‌ها و تجهیزات سیستم، بیان‌گر توزیع المان‌های شبکه در گروه‌های حفاظتی کل سیستم است که آن را «راهبرد جدایی» مدافع می‌نامیم. علاوه بر آن، برای هر PG مربوط به تجهیز j، تعداد A_j+1 نوع حفاظت وجود دارد. هر نوع حفاظت $(0\le\xi_{jm}\le A_j)$، با هزینه و آسیب‌پذیری مربوط به آن، که به‌صورت «احتمال خرابی PG با فرض حمله به آن $(\varepsilon_j(\xi_{jm}))$» تعریف می‌شود، مشخص می‌شود. به‌عنوان مثال $\xi_{jm}=0$ به معنی عدم وجود حفاظت است و قطعاً $\varepsilon_j(0)=1$ خواهد بود. ماتریس ε بیان‌گر «راهبرد حفاظت» مدافع است. با این تعریف، کل هزینه مدافع (جدایی و حفاظت) برابر است با:

$$o(\varepsilon,\varphi)=\sum_{j\in F}\sum_{m=1}^{M_j} o_j\left(\varepsilon_{jm},|\varphi_{jm}|\right) \qquad (۱۵)$$

راهبرد حمله مهاجم نیز به‌صورت $\theta=\{\theta_{jm}\,|\,\forall j\in F,1\le m\le M_j\}$ تعریف می‌شود که در آن، θ_{jm} بیان‌گر احتمال حمله به PG شماره m در تجهیز j است. در این مقاله [۸]، الگوریتمی ارائه شده که با استفاده از آن می‌توان به ازای هر راهبرد حمله و دفاع، بازده سیستم $(\eta_p(\varphi,\varepsilon,\theta))$ را در حالت p محاسبه کرد. پس از آن، اگر $c(q_p,\eta^0)$ تابعی از تلفات مرتبط با کاهش بازده سیستم به مقداری کمتر از η^0 تعریف شود، می‌توان هزینه متوسط این تلفات در هر راهبرد حمله و دفاع را به‌صورت زیر محاسبه کرد:

$$C(\varphi,\varepsilon,\theta,\eta^0)=\sum_{p\in P}\eta_p(\varphi,\varepsilon,\theta)c(q_p,\eta^0) \qquad (۱۶)$$

متوسط کل خسارت واردشده به مدافع، شامل هزینه تلفات ناشی از کاهش بازده سیستم به مقداری کمتر از η^0 و نیز تلفات ذاتی ناشی از تخریب المان‌های سیستم است که به‌صورت زیر محاسبه می‌شود:

$$\varsigma(\varphi,\varepsilon,\theta)=\sum_{j\in F}\sum_{m=1}^{M_j}\theta_{jm}\varepsilon_j(\xi_{jm})\times\left(\varsigma_{jm}^{PG}+\sum_{r\in\Phi_{jm}}\varsigma_{jr}^{e}\right)+C(\varphi,\varepsilon,\theta,\eta^0) \qquad (۱۷)$$

در صورتی که منابع مدافع محدود نباشد، مدافع باید مقدار متوسط خسارت و نیز هزینه سرمایه‌گذاری را کمینه کند. از سوی دیگر اگر منابع مدافع محدود باشد، تنها باید مقدار متوسط

[1] Levitin
[2] Separation
[3] Protection Group

خسارت را کمینه کند. مسأله بهینه‌سازی مدافع در حالت دوم به‌صورت زیر تعریف می‌شود:

$$\varphi^*,\varepsilon^* = \arg\left\{ Min\begin{pmatrix} \varpi.u(o(\varphi,\varepsilon) > C_{Total}) \\ +\varsigma(\varphi,\varepsilon,\theta) \end{pmatrix}\right\} \qquad (۱۸)$$

که در آن $u(\circ)$ بیان‌گر تابع واحد[1] و ϖ یک عدد ثابت بزرگ‌تر از بیشینه خسارت در حالتی است که مدافع محدودیت منابع ندارد. در حالتی که مدافع محدودیت منابع ندارد، این مسأله به‌صورت زیر نوشته می‌شود:

$$\varphi^*,\varepsilon^* = \arg\left\{Min\left(o(\varphi,\varepsilon)+\varsigma(\varphi,\varepsilon,\theta)\right)\right\} \qquad (۱۹)$$

از سوی دیگر، اگر فرض شود که اطلاعات مهاجم از سیستم کامل است، تابع هدف مسأله بهینه‌سازی وی به‌صورت زیر خواهد بود:

$$\theta^* = \arg\left\{Max\left(\varsigma(\varphi,\varepsilon,\theta)\right)\right\} \qquad (۲۰)$$

کاریون[2] [۵] در تخصیص بهینه منابع مدافع، به ارائه مدلی برای توسعه خطوط انتقال شبکه، به‌عنوان راهی برای کاهش خسارت‌های ناشی از حملات احتمالی پرداخته است. در این مدلِ برنامه‌ریزی احتمالاتی[3]، هدف برنامه‌ریز شبکه، انتخاب بهترین گزینه‌های توسعه از بین مجموعه خطوط کاندید است. تابع هدف برنامه‌ریز شبکه به‌صورت زیر تعریف شده است:

$$\begin{aligned} &Minimize \ \sum_{v=1}^{n_V}\pi_v\left[\sum_{n\in N}\Delta P_n^d(v)\right] \\ &+\gamma\sum_{v=1}^{n_V}\pi_v\left[\sum_{n\in N}\alpha_n\Delta P_n^d(v)\right]+\beta\sum_{l\in L^S}C_l^I s_l \end{aligned} \qquad (۲۱)$$

در تابع هدف (۲۱)، ترم اول مربوط به میزان قطع‌بار مورد انتظار[4] بوده که حاصل‌ضرب احتمال هر حمله در مجموع بار قطع‌شده در سناریوهای حمله است. ترم دوم مربوط به هزینه قطع‌بار مورد انتظار است که با ضریب وزنی γ ارزش‌گذاری می‌شود. ترم سوم نیز، هزینه احداث خطوط انتقال جدید است که در ضریب وزنی β ضرب شده است. اعمال ضرایب وزنی γ و β، به برنامه‌ریز سیستم این امکان را می‌دهد تا بین تابع هدف آسیب‌پذیری (ترم‌های اول و دوم) و تابع هدف اقتصادی (ترم سوم) اولویت قائل شود. تابع هدف (۲۱) مشروط به قید بیشینه سرمایه‌گذاری و نیز قیود پخش توان DC شبکه است، که در واقع واکنش اپراتور شبکه را مدل می‌کند. در مدل ارائه‌شده در این مرجع، حملات احتمالی به‌صورت مجموعه‌ای از سناریوها (V) در نظر گرفته شده‌اند. برای تولید تعداد n_V سناریو می‌توان از یک مدل حمله (نظیر آن‌چه که در [۱۸-۱۶] ارائه شده است) استفاده کرد و با طی روند تکراری زیر، مجموعه سناریوهای حملات را تعیین کرد:

مرحله ۱) مقداردهی اولیه بر اساس جدول (۱).

جدول (۱): اولیه برای شروع فرآیند تولید سناریو

پارامتر/متغیر/مجموعه	تعریف	مقدار
n_A	تعداد خطوط تحت حمله	۱
n_S	تعداد سناریوها	۰
Ω_{n_A}	سناریوهای با n_A خط تحت حمله	ϕ
Ω	مجموعه سناریوها	ϕ
ΔP_0^d	مقدار قطع بار بدون حمله	۰
$\Delta P_{n_A}^d$	بیشینه قطع بار با n_A خط تحت حمله	۰

مرحله ۲) حل مدل MTTP[5] و محاسبه نقشه حمله بهینه υ^* و میزان قطع‌بار بهینه $\Delta P_T^{d^*}$ به‌ازای n_A و MTTP Ω_{n_A} مدل حمله مورد استفاده است. این مدل باید به‌گونه‌ای اصلاح شود که نقشه‌های حمله‌ای که قبلاً در Ω_{n_A} مورد بررسی قرار گرفته‌اند، به‌عنوان نقشه حمله بهینه بازگردانده نشوند.

مرحله ۳) به‌روزرسانی مقادیر به‌صورت زیر:

$$\begin{aligned} &If\ \Delta P_T^{d^*} > \Delta P_{n_A-1}^d \\ &\quad \{\Omega_{n_A},\upsilon^*\}\rightarrow\Omega_{n_A} \quad , \quad n_S = n_S+1 \\ &\quad \Delta P_{n_A}^d = \max\{\Delta P_T^{d^*},\Delta P_{n_A}^d\} \\ &Else \\ &\quad \{\Omega,\Omega_{n_A}\}\rightarrow\Omega \quad , \quad \Omega_{n_A}=\phi \\ &\quad n_A = n_A+1 \quad , \quad \Delta P_{n_A}^d = \Delta P_{n_A-1}^d \end{aligned}$$

مرحله ۴) اگر $n_S < n_V$، آنگاه باید به مرحله ۲ برگشت، در غیر این صورت، الگوریتم تولید سناریو پایان می‌یابد.

[1] Unity Function
[2] Carrion
[3] Stochastic Programming
[4] Expected Load Shed
[5] Modified Terrorist Threat Problem

در مرحله ۳، اگر مقدار قطع‌بار بهینه $\Delta P_T^{d^*}$ بیش از مقدار بهینه قطع‌بار حاصل از تخریب n_A-1 خط باشد، آنگاه υ^* به‌عنوان یک سناریو در نظر گرفته می‌شود. در غیر این صورت، غیرممکن است که بتوان با n_A حمله، نقشه‌ای یافت که میزان قطع‌بار آن بیش از $\Delta P^d_{n_A-1}$ باشد. بنابراین، جست‌وجو برای نقشه‌های حمله به ازای n_A پایان می‌یابد و مجموعه سناریوها و n_A به‌روز می‌شوند.

در این مقاله [۵]، احتمال هر سناریو با توجه به دو موضوع تعیین می‌شود؛ احتمال وقوع حمله v متناسب با $\Delta P_T^d(V)$ است و با تعداد خطوطی که در آن حمله تخریب می‌شوند ($I(v)$)، تناسب عکس دارد. این دو موضوع در رابطه زیر لحاظ شده‌اند:

$$\pi_V=\frac{\frac{\Delta P_T^d(v)}{I(v)}}{\sum_{v'=1}^{n_V}\frac{\Delta P_T^d(v')}{I(v')}} \qquad v=1,2,\ldots,n_V \qquad (۲۲)$$

پاول[1] [۷] در تحقیق خود به موضوع دفاع در مقابل حملات تروریستی در بلندمدت و ارائه راهکاری برای تخصیص بهینه منابع پرداخته است. او در تحقیق خود، ابتدا با ارائه مستنداتی نشان داده است که چه در بررسی آسیب‌پذیری یک سیستم و چه در انتخاب یک راهبرد بهینه، الزاماً باید گروه مهاجم را یک گروه کاملاً راهبردی[2] فرض کرد. عدم رعایت این موضوع می‌تواند خسارت‌های زیادی را به دنبال داشته باشد. او در ادامه کار خود به ارائه راهکاری برای تخصیص بهینه منابع پرداخته است. از آن‌جا که تعداد تجهیزات زیاد است، نمی‌توان از تمام تجهیزات دفاع کرد [۷]. این موضوع سبب شده است تا برخی مراجع عنوان کنند که در تخصیص منابع در مقابل حملات عامدانه، تحلیل و مدیریت ریسک[3] الزامی است [۱۹]. مراجع [۷]، [۹]، [۱۰] و [۲۰] نشان داده‌اند که از آن‌جا که در مدل‌های تحلیل ریسک، مهاجم کاملاً راهبردی فرض نمی‌شود، نمی‌توان منابع را به‌طور کاملاً بهینه تخصیص داد. این مراجع به‌جای تحلیل ریسک، از یک چارچوب مبتنی بر نظریه بازی[4] استفاده می‌کنند. در این چارچوب، تصمیمات مدافع و مهاجم، می‌تواند چهار حالت داشته باشد: ۱) حالت با مجموع صفر[5] که در آن اهداف مدافع و مهاجم کاملاً متضاد با یکدیگر است؛ ۲) حالت با مجموع غیرصفر؛ ۳) حالتی که مهاجم می‌تواند تصمیمات مدافع در خصوص تخصیص منابع را ببیند و واکنش مناسب را در هنگام تصمیم‌گیری درخصوص نقشه حمله نشان دهد؛ و ۴) حالتی که تصمیمات مدافع به‌صورت سری انجام می‌گیرد.

در تحلیل ریسک به‌عنوان خسارت مورد انتظار[6] از طرف مهاجم و یا ریسک مرتبط با هر تجهیز، اگر احتمال وقوع یک حمله را «تهدید[7]» بنامیم [۲۱]، احتمال موفقیت یک حمله را «آسیب‌پذیری[8]» [۲۲] و خسارت ناشی از حمله را «پی‌آمد[9]» [۲۱]، در این صورت میزان ریسک به‌صورت زیر محاسبه می‌شود:

$$\zeta_V=\pi_V\times \mathrm{K}_V\times y_V \qquad (۲۳)$$

استفاده از چنین تحلیلی در تخصیص بهینه منابع در یک مطالعه بلندمدت، با دو مشکل اساسی روبرو است؛ اول این‌که تخمین احتمال وقوع یک حمله، احتمال موفقیت آن و همچنین تخمین میزان خسارت ناشی از آن نمی‌تواند در بلندمدت صحیح باشد [۷] و [۲۳]؛ مشکل دوم که اساسی‌تر از مشکل اول است این است که با تقویت یک تجهیز (و یا در حالت کلی، یک پایگاه[10])، مهاجم راهبردی به دنبال هدف‌هایی می‌رود که کمتر دفاع شده‌اند و دسترسی به آن‌ها ساده‌تر است [۲۴]. تقویت یک تجهیز، آسیب‌پذیری و همچنین تهدید آن را کاهش می‌دهد و بنابراین، تهدید سایر تجهیزات را افزایش می‌دهد. به عبارت دیگر، مهاجم در یک حلقه تصمیم‌گیری[11]، بازخوردی بین تهدید و آسیب‌پذیری قرار می‌دهد و این موضوع، تخصیص منابع را در بلندمدت پیچیده می‌کند. با یک مثال می‌توان این مطلب را روشن کرد [۷] و [۹].

فرض می‌کنیم که یک گروه مهاجم قصد حمله به یک پایگاه را دارد و برای این کار، یا از پیشِ رو حمله می‌کند (گزینه ۱) و یا از پشت سر (گزینه ۲). تحلیل تهدید نشان می‌دهد که احتمال این‌که مهاجم از جلو حمله کند، ۶۶٪ است. بنابراین، مدافع اکثر منابع خود را به جلوی پایگاه تخصیص می‌دهد. به دنبال این تصمیم مدافع، مهاجم هدف خود را عوض کرده و از پشت سر حمله می‌کند. زمان اندکی قبل از حمله، یک تحلیل تهدید هشدار می‌دهد که احتمال وقوع حمله از پشت سر تقریباً حتمی

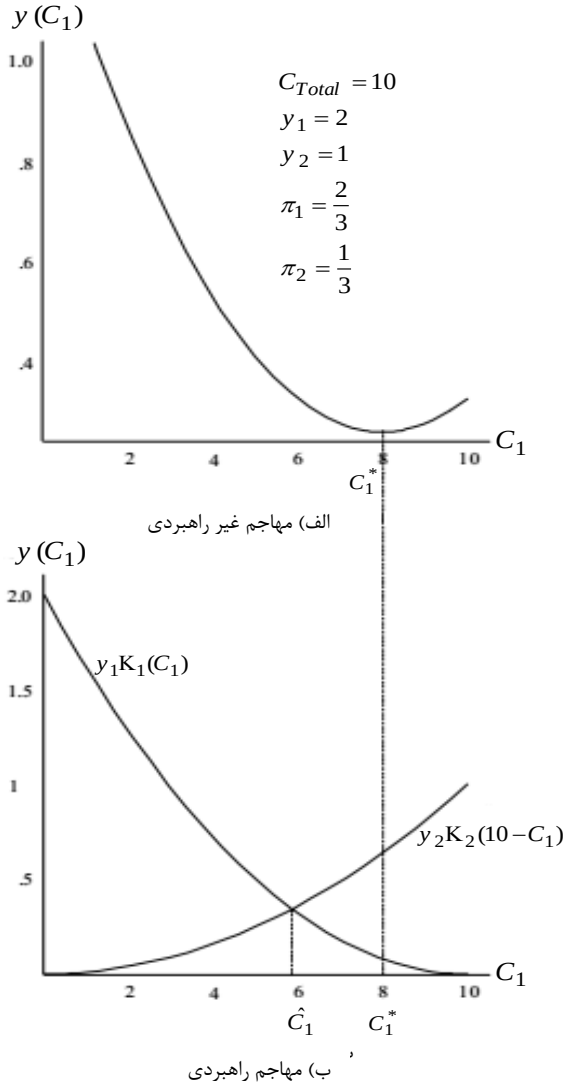
[1] Powell
[2] Fully Strategic
[3] Risk Analysis and Management
[4] Game Theory
[5] Zero-sum Case
[6] Expected Loss
[7] Threat
[8] Vulnerability
[9] Consequence
[10] Site
[11] Decision Making Loop

است. حال این سؤال مطرح می‌شود که آیا مدافع باید منابع خود را بر اساس تحلیل تهدید اولیه تخصیص‌دهی می‌کرد، یا بر اساس تحلیل جدید، یا بر اساس ترکیبی از این دو و یا بر اساس هیچکدام؟ با یک مدل ساده می‌توان به این سؤالات پاسخ داد و اثر نادیده‌گرفتن بازخورد بین تهدید و آسیب‌پذیری را بر تخصیص غیربهینه منابع بررسی کرد. اگر C_1 و C_2، به ترتیب، منابعی باشند که مدافع به دفاع در مقابل گزینه ۱ و ۲ تخصیص می‌دهد، آن‌گاه احتمال موفقیت حمله به گزینه j برابر خواهد بود با $\mathrm{K}_j(C_j)$ که K_j تابعی نزولی از C_j است. و به‌صورت $\mathrm{K}_j(C_j)=(1-C_j/C_{Total})^2$ فرض می‌شود. در این صورت، خسارت مورد انتظار مدافع، تابعی برحسب C_1 است و به‌صورت زیر فرمول‌بندی می‌شود [۷]:

$$y(C_1)=\pi_1\times \mathrm{K}_1(C_1)\times y_1 + (1-\pi_1)\times \mathrm{K}_2(1-C_1)\times y_2 \qquad (۲۴)$$

ترم اول در این رابطه بیان‌گر خسارت مورد انتظار در صورت حمله به گزینه ۱، و ترم دوم بیان‌گر همان مقدار برای حمله به گزینه ۲ است. شکل (۲) مقدار خسارت مورد انتظار را برای دو حالت مهاجم راهبردی و غیرراهبردی نشان می‌دهد. همان‌طور که مشاهده می‌شود، اگر بازخورد بین تهدید و آسیب‌پذیری، با این فرض که تهدید π_1 مستقل از C_1 و اثر آن بر K_1 و K_2 همواره ثابت می‌ماند، نادیده گرفته شود، آن‌گاه تخصیص بهینه منابع به‌صورت $C_1^*=۸$ و $C_2^*=۲$ خواهد بود (۲- الف). در همین حال، (شکل ۲- ب) نشان می‌دهد که با چنین تخصیص منابعی، مهاجم راهبردی با حمله به گزینه ۲ خسارت بیشتری به مدافع تحمیل می‌کند و از این طریق، تحلیل تهدید اولیه صورت‌گرفته توسط مدافع ($\pi_1=٪۶۶$) را باطل می‌کند.

در یک چارچوب مبتنی بر نظریه بازی [۷، ۹ و ۱۰]، نقطه تعادل بازی، اثر بازخوردهای لازم برای بازی بهینه بازیگران را در خود لحاظ می‌کند. در پاسخ بررسی‌شده، C_1^* و π_1 تنها نصف بازی را تشکیل می‌دهند؛ بدین معنی که مدافع در مقابل تصمیم بهینه مهاجم (π_1) بهترین واکنش را نشان می‌دهد، اما مهاجم در مقابل واکنش مدافع هنوز واکنشی نشان نداده است. نقطه تعادل این بازی که بیان‌گر تخصیص بهینه منابع است، در واقع نقطه $\hat{C}_1=۵/۹$ است. اگر مدافع کمتر از این مقدار را به گزینه ۱ اختصاص دهد، آن‌گاه این گزینه مورد حمله قرار می‌گیرد و خسارت آن بیش از خسارت مربوط به نقطه $\hat{C}_1$ است.



الف) مهاجم غیر راهبردی

ب) مهاجم راهبردی

شکل (۲): خسارت مورد انتظار با فرض مهاجم راهبردی و غیرراهبردی [۷]

به‌طور کلی اگر مدافع بخواهد T پایگاه را در مقابل V نوع حمله دفاع کند، مدافع با $|T|\times|V|$ حمله روبه‌رو است. اگر احتمال این‌که پایگاه j تحت حمله نوع v قرار گیرد را با π_{jv} نشان دهیم، آنگاه خسارت مورد انتظار در پایگاه j ناشی از حمله نوع v برابر با $\pi_{jv}\times \mathrm{K}_{jv}(C_{jv})\times y_{jv}$ خواهد بود. با چنین تعریفی، خسارت مورد انتظار مدافع در مقابل یک سناریوی حمله برابر است با:

$$\sum_{j\in T}\sum_{v\in V}\pi_{jv}\times \mathrm{K}_{jv}(C_{jv})\times y_{jv} \qquad (۲۵)$$

در حالی که:

$$\sum_{j\in T}\sum_{v\in V}C_{jv}\le C_{Total} \qquad (۲۶)$$

$$\sum_{j\in T}\sum_{v\in V}\pi_{jv}=1 \qquad (۲۷)$$

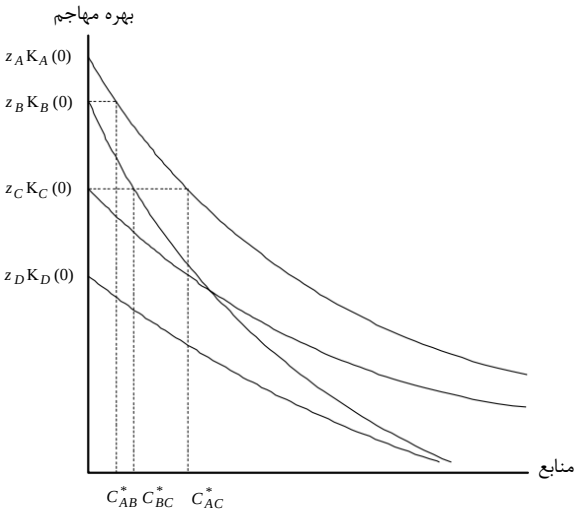
در همین حال، بهره[1] مهاجم از حمله به ازای یک راهبرد دفاعی برابر است با:

$$\sum_{j\in T}\sum_{v\in V}\pi_{jv}\times \mathrm{K}_{jv}(C_{jv})\times z_{jv} \qquad (۲۸)$$

۰ (۳) تخصیص بهینه منابع را در حالت‌های مختلف نشان می‌دهد که در آن، $A=(j_A,v_A)$. پاول [۷] برای به‌دست آوردن راهبرد بهینه فرض می‌کند که ابتدا $C_{jv}=0;\forall j,\forall v$. در این حالت، مطابق۰شکل (۳)، سناریوی A بیان‌گر بهترین انتخاب مهاجم بوده و پس از آن، انتخاب‌های B، C و D قرار دارند. در این حالت، تحت تخصیص بهینه C^*_{AB}، $z_A\mathrm{K}_A(C^*_{AB})=z_B\mathrm{K}_B(0)$ و این یعنی بهره مهاجم تحت سناریوی A برابر با بهره اولیه آن تحت سناریوی B (بدون تخصیص منابع) است. اگر مدافع منابع بیشتری را تنها به دفاع از سناریوی A تخصیص دهد، قطعاً مهاجم با سناریوی B حمله می‌کند و تمام منابع مدافع که پس از C^*_{AB} خرج شده‌اند، هدر می‌رود. بنابراین، مدافع باید به تخصیص منابع در مقابل سناریوهای A و B بپردازد و این کار را تا جایی ادامه دهد که بهره مهاجم از سناریوهای A و B برابر شود و هیچ‌یک بر دیگری ارجحیت نداشته باشد و در عین حال برابر با بهره اولیه مهاجم در سناریوی C باشند. این خواسته با تخصیص (C^*_{AC},C^*_{BC}) رخ می‌دهد که در آن، $z_A\mathrm{K}_A(C^*_{AC})=z_B\mathrm{K}_B(C^*_{BC})=z_C\mathrm{K}_C(0)$. این روند تا جایی ادامه می‌یابد که تمام منابع مدافع تخصیص داده شوند.

سه نکته اساسی در این روش وجود دارد؛ نکته اول این‌که تخصیص نهایی تحت این روش، مستقل از این‌که مهاجم قبل از این تصمیم بگیرد که با چه نوع حمله‌ای به کدام پایگاه حمله کند، بهینه است؛ نکته دوم، نتیجه فرض کردن مهاجم به‌صورت کاملاً راهبردی این است که تخصیص بهینه بلندمدت مستقل از تهدید π_{jv} است؛ و نکته سوم این‌که تخصیص بهینه بلندمدت، وابسته به اهداف و انگیزه‌های مهاجم است (که در z_{jv} مدل شده است) و از خسارت‌های مدافع (که در y_{jv} مدل شده است)، مستقل است.

[1] Gain

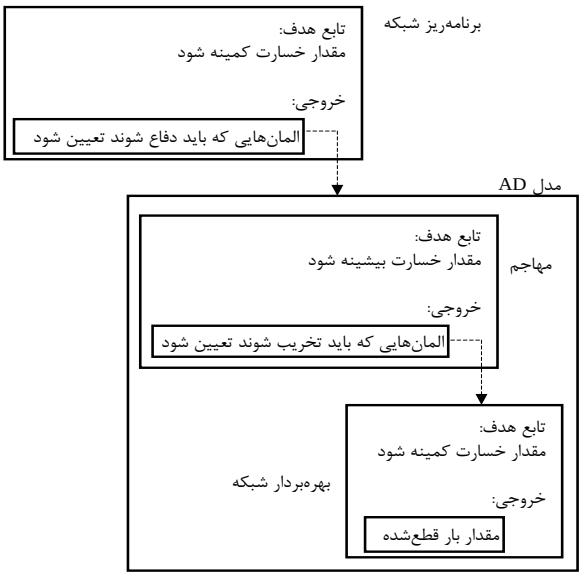


شکل (۳): تخصیص بهینه منابع

۴- مدل‌های سه‌سطحی ارائه‌شده برای ORA

در ارزیابی آسیب‌پذیری شبکه برق، هدف، یافتن نقاط ضعیف شبکه است. توضیح بیشتر این‌که تحقیقاتی که به تحلیل آسیب‌پذیری شبکه برق می‌پردازند، برای یافتن نقاط ضعیف شبکه فرض می‌کنند که یک مهاجم باهوش قصد آسیب‌زدن به سیستم را دارد و از سوی دیگر، مدافع شبکه بهترین واکنش را در مقابل حملات مهاجم نشان می‌دهد. طبیعت این مسأله به‌صورت یک مسأله دوسطحی مهاجم-مدافع (AD)[2] است. اگرچه مدل‌های AD قادرند که المان‌های حیاتی شبکه را شناسایی کنند، اما الزاماً تقویت این المان‌ها نمی‌تواند به‌عنوان بهترین راهبرد دفاعی قلمداد شود. چرا که افزایش یک المان جدید به یک شبکه که دارای J المان است، تعداد المان‌ها را به J+1 افزایش داده است و این به این معنی است که ما با یک شبکه جدید روبرو هستیم که وضعیت بهره‌برداری آن، فلوی عبوری از تجهیزات و نیز وضعیت توزیع نیروگاه‌های آن، با شبکه قبل متفاوت است. این شبکه جدید، باید مجدداً از نظر آسیب‌پذیری مورد ارزیابی قرار گیرد و مطمئناً نتیجه حاصل، با نتیجه ارزیابی شبکه قبل متفاوت است [۲-۱]. چنین موضوعی الزام می‌کند که برای تخصیص بهینه منابع و نیز توسعه و تقویت شبکه می‌بایست از مدل‌های سه سطحی استفاده کرد تا بتوان تمام تأثیرات راهبردهای دفاعی را مورد ارزیابی قرار داد. شمای کلی مدل‌های سه‌سطحی در ۰ (۴) آورده شده است. این مدل، مدل استحکام[3] نیز نامیده می‌شود.

[2] Attacker-Defender
[3] Fortification Model



شکل (۴): شمای کلی مدل‌های DAD

در سطح اول مسأله، مدافع قصد تخصیص بهینه منابع مالی خود را دارد. در سطح دوم، مهاجم، با منابع محدود خود، بهترین نقشه حمله را انتخاب می‌کند و در سطح سوم، مدافع شبکه، شبکه را به‌گونه‌ای بهره‌برداری می‌کند تا خسارت‌های ناشی از حمله مهاجم (در سطح دوم)، با تغییراتی که در ساختار شبکه (در سطح اول) رخ داده است، کمینه شود.

آلگواچیل[1] [۱] در تحقیق خود به ارائه مدلی سه سطحی از نوع DAD پرداخته است. این مقاله و سایر مقالاتی که در این زمینه ارائه شده‌اند، عموماً فرض‌های زیر را در نظر گرفته‌اند:

• شبکه در حالت دائمی خود فرض می‌شود و از اثرات حالت گذرا صرف‌نظر می‌شود؛

• برای ارزیابی اثر حمله، بار قطع‌شده به‌عنوان معیار ارزیابی در نظر گرفته می‌شود؛

• بار سیستم به‌صورت قطعی مدل می‌شود و عموماً برابر با بیشینه بار پیش‌بینی‌شده فرض می‌شود و

• در مدل‌سازی رفتار شبکه، از مدل DC استفاده می‌شود که این مدل در برنامه‌ریزی شبکه نتایج مناسبی به‌دست می‌دهد [۲۵-۲۶].

در این مقاله فرض دیگری نیز در نظر گرفته شده که در آن، تنها خطوط انتقال و ترانسفورماتورهای شبکه می‌توانند مورد حمله واقع شوند و مدافع شبکه نیز، تصمیم‌گیری خود درخصوص استحکام شبکه را تنها به این تجهیزات محدود می‌کند. در سطح اول، مدافع شبکه قصد دارد تا بهترین تجهیزات را برای تقویت و توسعه به‌گونه‌ای انتخاب کند تا میزان بار قطع‌شده کمینه شود. تابع هدف سطح اول به‌صورت زیر بیان می‌شود:

$$\min_{w} \sum_{n\in N} \Delta P_n^{d^*} \qquad (۲۹)$$

اساس مدل سطح دوم و سوم (زیرمسأله AD)، بر پایه مدل حداقل آسیب‌پذیری ارائه‌شده توسط آرویو[2] [۲۷] بنا شده است. در سطح دوم مسأله، مهاجم قصد دارد تابع هدف (۲۹) را با داشتن منابع محدود، بیشینه کند. در فرمول‌بندی AD ارائه‌شده در [۱]، یک قید نسبت به آن‌چه که آرویو [۲۷] ارائه داده است، به مسأله اضافه شده که در آن فرض شده است که اگر المان jام تقویت شده باشد، مهاجم نمی‌تواند به آن حمله کند. در مسأله سطح سوم نیز مدافع شبکه با لحاظ حملات صورت‌گرفته، شبکه را به‌گونه‌ای بهره‌برداری می‌کند که مقدار بار قطع‌شده کمینه شود.

رومِرو[3] [۱۱] در تحقیق خود به برنامه‌ریزی سرمایه‌گذاری در شبکه برق با در نظر گرفتن حملات تروریستی پرداخته است. رویکرد اتخاذشده در این تحقیق نیز یک رویکرد سه‌سطحی با نام مدافع-مهاجم-بهره‌بردار[4] است که در آن، در سطح اول مسأله، مدافع شبکه قصد دارد سرمایه‌گذاری در شبکه برق را به‌گونه‌ای انجام دهد که هزینه‌های پس از حمله کمینه شود. این هزینه‌ها شامل هزینه تولید، هزینه بار قطع‌شده، هزینه تعمیرات برای ترانسفورماتورهای بدون یدک و هزینه جایگزینی ترانسفورماتورهای یدکی می‌شود. این تصمیم‌گیری، قبل از حمله[5] صورت می‌گیرد.

در سطح میانی مسأله، مهاجم به تصمیم‌گیری بهینه درخصوص انتخاب بهترین راهبرد حمله می‌پردازد و می‌داند که بهره‌بردار شبکه (در سطح سوم مسأله)، شبکه را به‌گونه‌ای بهره‌برداری می‌کند که هزینه‌های بهره‌برداری پس از حمله، کمینه شود. در این مقاله نیز مشابه اکثر مقالات ارائه‌شده در این زمینه، فرض بر آن است که تروریست از اطلاعات کامل برخوردار است. در این تحقیق، برای فرآیند تعمیر[6] تجهیزات، چهار مرحله در نظر گرفته شده است؛ در مرحله اول، تمام تجهیزاتی که مورد حمله واقع شده‌اند و نیز آن دسته از المان‌هایی که عملکردشان

[1] Alguacil

[2] Arroyo
[3] Romero
[4] Defender-Attacker-Operator
[5] Pre-attack
[6] Repair

وابسته به این تجهیزات است، هیچ فلویی از آن‌ها عبور نمی‌کند. در مرحله دوم، تنها آن دسته از خطوطی که به پست‌های تخریب‌شده متصل هستند از مدار خارج می‌مانند و بقیه خطوط تعمیر می‌شوند و می‌توانند انرژی حمل کنند. در مرحله سوم، تمام تجهیزات پست‌های تخریب‌شده، به‌جز ترانسفورماتورها، تعمیر می‌شوند. در مرحله چهارم (مرحله نهایی)، فرض می‌شود که ترانسفورماتورهای یدکی نصب می‌شوند. برای تخمین فلوی عبوری از المان‌های شبکه، از پخش‌توان DC در هر یک از چهار مرحله بیان‌شده، استفاده شده است. این پخش توان‌ها با تابع هدف کمینه‌کردن هزینه تولید، هزینه بار قطع‌شده و هزینه جایگزینی ترانسفورماتورهای یدکی اجرا می‌شوند که در رابطه (۳۰) آورده شده است. پخش توان‌های بیان‌شده، در واقع واکنش بهره‌بردار شبکه (سطح سوم) را مدل می‌کنند. تابع هدف مهاجم (سطح میانی)، بیشینه‌کردن مجموع F_Lو هزینه تعمیرات است و تابع هدف مدافع (سطح اول)، کمینه‌کردن تابع هدف مهاجم است.

$$\begin{aligned} &Minimize\ F_L(\delta^G,\delta^L,\delta^S,x^G,x^L,h^D)= \\ &\sum_{k=1,2,3,4}\left(\sum_{n\in N}\alpha_n\Delta P_n^{d^k}+\sum_{g\in G}C_g^E p_g^k\right)(t_k-t_{k-1}) \\ &+\sum_{s\in S}\sum_{i\in O_s}\sum_{(i,j)\in T}\sum_{b\in B}C_i^B(1-r_{ijb})E_{ij}\delta_s^S \end{aligned} \qquad (۳۰)$$

نکته مهمی که در این مقاله به آن توجه شده است این است که ممکن است پس از تعمیر یک خط انتقال، ظرفیت آن تغییر کرده و به دنبال آن، راکتانس آن نیز عوض شود. برای مدل کردن این موضوع، میزان کاهش و یا افزایش راکتانس یک خط انتقال، وابسته به میزان تغییرات ظرفیت آن خط در نظر گرفته شده است.

رُز[۱] در تحقیقی با عنوان «دفاع از شبکه‌های برق» [۱۲] به ارائه مدلی به نام DKI[۲] پرداخته است که این مدل قادر است به ازای منابع محدود دفاعی، مجموعه بهینه تجهیزات شبکه برای حفاظت و دفاع را شناسایی کند. او در یک شبکه نمونه کوچک نشان داده است که با دفاع از کمتر از ۱۰٪ از شین‌های شبکه می‌توان میزان تخریب احتمالی ناشی از حملات را بیش از ۲۰٪ کاهش داد. مدل ارائه‌شده در این مرجع [۱۲]، برای بخش حمله به شبکه، از مدل I-DCOPF[۳] ارائه‌شده توسط سالمرون [۱۶] استفاده کرده است. در این مرجع، نشان داده شده است که در کاربرد شبکه‌های مقیاس بزرگ[۴]، مدل I-DCOPF از کارآمدی خوبی برخوردار نیست و بنابراین برای بخش حمله به شبکه و تعیین بهترین راهبرد حمله، مدل جدیدی با نام NDR[۵] ارائه شده است. این مدل، رفتار شبکه برق را به‌صورت یک مدل «فلوی شبکه با کمترین هزینه[۶]» تقریب می‌زند تا بتواند در زمانی بسیار اندک، یک کران پایین برای میزان تخریبی که مدل دقیق (همان I-DCOPF) به‌دست می‌دهد، به‌دست بیاورد. نتیجه پیاده‌سازی NDR بر روی بخشی از شبکه برق آمریکای شمالی نشان می‌دهد که این مدل قادر است در کمتر از ۶۰۰۰ ثانیه، به ازای دفاع از ۱۰ شین شبکه مورد مطالعه، پاسخ‌هایی به دست آورد که نسبت به مدل دقیق I-DCOPF تا ۴۰٪ میزان خسارت را کاهش دهند.

مدل NDR در واقع کاربرد مدل «بیشینه‌کردن کوتاه‌ترین مسیر» (MXSP)[۷] برای شبکه‌های برق است. مدل MXSP در سال ۲۰۰۲ توسط اسرائیل[۸] و وود[۹][۲۸] ارائه شده است. این مدل، یک گراف جهت‌دار را در نظر می‌گیرد و به کمان‌های[۱۰] این گراف حمله می‌کند. اگر یک کمان مورد حمله واقع شود، یک ضریب جریمه[۱۱] به طول این کمان اضافه می‌شود. این جریمه آنقدر بزرگ می‌شود تا هیچ کمان تخریب‌شده‌ای روی کوتاه‌ترین مسیر وجود نداشته باشد. رُز [۱۲] در تحقیق خود، مراحل تبدیل یک شبکه برق به یک گراف جهت‌دار را توضیح داده و از مدل MXSP برای یافتن مجموعه‌ای از المان‌ها که حمله به آن‌ها می‌تواند هزینه‌های سیستم را بیشینه کند، استفاده کرده است. در ادامه، در مدل دفاعی DKI، که در واقع یک مدل سه‌سطحی DAD است، در هر تکرار از الگوریتم حل، مهاجم مجموعه‌ای از تجهیزاتی که به آن‌ها حمله می‌کند، ارائه می‌دهد. برای «جلوگیری» از یک نقشه حمله، مدافع باید لااقل یکی از المان‌های موجود در آن نقشه حمله را حفاظت کند. DKI از این روند استفاده می‌کند تا مبتنی بر همه نقشه‌های حمله، بهینه‌ترین راهبرد دفاعی را انتخاب کند. اگر تمامی نقشه‌های حمله ممکن، قابل شمارش باشند، در آن صورت، یافتن راهبرد دفاعی بهینه ساده خواهد بود؛ ابتدا، حداقل یک تجهیز از تجهیزات تحت حمله در مخرب‌ترین حمله باید حفاظت شود، سپس یک تجهیز دیگر از تجهیزات تحت حمله در مخرب‌ترین حمله دوم باید انتخاب شود و این روند به همین ترتیب ادامه پیدا

[1] Rose
[2] Defense of Known Interdictions
[3] Interdiction DC Optimal Power Flow
[4] Large-scale Networks
[5] Network Dual Relaxation
[6] Minimum Cost Network Flow
[7] Maximizing the Shortest Path
[8] Israel
[9] Wood
[10] Arcs
[11] Penalty Factor

کند. این روند تا جایی ادامه می‌یابد که منابع مدافع تمام شود. فرمول‌بندی مدل DKI به‌صورت زیر ارائه می‌شود:

$$(DKI)\ \underset{w}{Minimize}\ \ y^0 \qquad (۳۱)$$

مشروط به آن‌که:

$$y^0 \geq d_v^O\left(1-\sum_j \delta_{j,v} w_j\right); \qquad \forall v \in V \qquad (۳۲)$$

$$\sum_j C_j w_j \leq C_{Total} \qquad (۳۳)$$

$$w_j \in \{0,1\}; \qquad \forall j \in J \qquad (۳۴)$$

$$y^0 \geq 0 \qquad (۳۵)$$

در این فرمول‌بندی، DKI(P) یک راهبرد دفاعی بهینه را برای مجموعه حملات معلوم P به‌دست می‌دهد. مقدار تابع هدف، مقدار خسارت را در مقابل بدترین حمله‌ای که با این مقدار منابع دفاعی نمی‌توان از آن دفاع کرد، ارائه می‌دهد.

براون[1] [۲] در پژوهش خود، به‌طور کلی به موضوع دفاع از زیرساخت‌های ملی در مقابل حملات عامدانه می‌پردازد. او در تحقیق خود به تحلیل مدل‌های دوسطحی و سه‌سطحی برای افزایش ارتجاع[2] زیرساخت‌ها می‌پردازد. ارتجاع زیرساخت‌ها در واقع بیان‌گر میزان تاب‌آوری آن‌ها در مقابل حوادث عامدانه و یا غیرعامدانه است. او در تحقیق خود به ارائه سه مثال می‌پردازد، که این مثال‌ها شامل ذخیره راهبردی نفت ایالات متحده آمریکا، گشت مرزی در ایالت آریزونای آمریکا و شبکه برق IEEE Tow-Area Reliability Test System می‌شود. در ادامه، نتایجی مهمی که از این مثال‌ها به‌دست آمده است ارائه خواهد شد.

مدل‌هایی که در [۲] بررسی شده‌اند، شامل مدل‌های کلی دوسطحی AD، DA و مدل سه‌سطحی DAD است. فرم کلی مدل‌های AD به‌صورت زیر است و در آن، یک مهاجم قصد دارد تا هزینه بهینه بهره‌برداری سیستم مدافع را بیشینه کند و این کار را با محدود کردن فعالیت‌های مدافع انجام می‌دهد:

$$(AD)\ \underset{x\in X}{Max} \min_{y\geq 0} cy \qquad (۳۶)$$

$$Ay = b \qquad (۳۷)$$

$$Fy \leq U(1-x) \qquad (۳۸)$$

در یک مدل DA، یک مدافع قصد دارد تا راهبرد دفاعی بهینه w^* را به‌گونه‌ای انتخاب کند که سودی که مهاجم با حل مسأله زیر به‌دست می‌آورد، کمینه شود و یا از یک مقدار خاص تجاوز نکند.

$$(DA)\ \underset{x\in X(w^*)}{Max} \min_{y\in Y(x)} cy \qquad (۳۹)$$

همان‌طور که پیش‌تر نیز گفته شد، اگرچه مدل‌های AD قادرند المان‌های حیاتی شبکه را شناسایی کنند، اما الزاماً تقویت این المان‌ها نمی‌تواند به‌عنوان بهترین راهبرد دفاعی قلمداد شود. انتخاب یک راهبرد دفاعی بهینه مستلزم حل مدل‌های سه‌سطحی DAD است، که فرم کلی تابع هدف آن‌ها به‌صورت زیر است:

$$(DAD)\ \min_{w\in W} Max_{x\in X} \min_{y\geq 0} cy \qquad (۴۰)$$

مشکلی که در حل مدل‌های سه‌سطحی وجود دارد، الگوریتم حل این مدل‌هاست که گاهی دسترسی به نقطه بهینه سراسری را غیرممکن می‌کند. برای حل چنین مدل‌هایی معمولاً از فرض‌های ساده‌کننده‌ای استفاده می‌کنند و از الگوریتم‌ها ابتکاری و فرا ابتکاری بهره می‌برند. نتایج مهمی که این تحقیق به آن‌ها دست یافته است به‌صورت موردی در زیر ارائه شده است:

- یک تحلیل AD می‌تواند میزان حیاتی‌بودن[3] تجهیزات شبکه را تعیین کند. علاوه بر آن، می‌توان با چنین تحلیلی، نقش به‌کار بردن تجهیزات یدکی برای افزایش ارتجاع و تاب‌آوری را مورد ارزیابی قرار داده و ارزش چنین تجهیزاتی را برای شبکه ارزیابی کرد.
- همواره نمی‌توان انتظار داشت که بهینه‌ترین راهبردهای دفاعی یا تهاجمی، به‌صورت مستقیم قابل تحلیل باشند. در سیستم‌های بزرگ، دست‌یابی به چنین راهبردهایی مستلزم بهینه‌سازی و فرمول‌بندی‌های پیچیده است و الزاماً نمی‌توان منطق نتایج را به‌صورت مستقیم و یا حسی مورد تجزیه و تحلیل قرار داد.
- قوانین سرانگشتی و یا درک مهندسی و استفاده از نظر متخصصان مفید است، اما نمی‌توان با تکیه بر آن‌ها، به ارزیابی آسیب‌پذیری یک شبکه و یا انتخاب یک راهبرد دفاعی بهینه برای آن شبکه پرداخت. درصورتی که با چنین مواردی به تحلیل آسیب‌پذیری و انتخاب یک راهبرد دفاعی بپردازیم، این

[1] Brown
[2] Resiliency
[3] Criticality

ریسک وجود دارد که مهاجمی که از ما باهوش‌تر است، نقشه حمله‌ای انتخاب کند که از تحلیل‌های ما بهینه‌تر بوده و در نتیجه خسارت زیادی به سیستم وارد کند.

- معیارهای قابلیت اطمینان[1] کافی نیستند. در معیارهای قابلیت اطمینان، تنها حوادث طبیعی و خطاهای معمول سیستم لحاظ می‌شوند و این در حالی است که خسارت ناشی از حملات عامدانه بسیار بیشتر از موارد بیان‌شده است. بنابراین، برای تقویت سیستم باید به المان‌های حیاتی توجه کرد و نه تنها به المان‌های با کمترین میزان قابلیت اطمینان.
- مهاجم، از دو جنبه نسبت به مدافع دارای برتری است؛ یکی از این جهت که مدافع باید به دفاع از یک شبکه بسیار بزرگ و بررسی مجموعه بسیار زیادی از راهبردهای دفاعی پراکنده بپردازد و این در حالی است که مهاجم می‌تواند تمرکز خود را بر تعداد کمتری از راهبردهای حمله قرار دهد. از سوی دیگر، مهاجم از نقطه‌نظر دسترسی به اطلاعات مربوط به طرف مقابل خود (مدافع)، نسبت به مدافع برتری دارد.
- دسترسی کامل مهاجم به اطلاعات، یک فرض معقول است. یک خودآموز به‌دست‌آمده از گروه‌های القاعده بیان می‌کند که: «تنها با استفاده از منابع اطلاعاتی که در دسترس عموم قرار دارد (نظیر وب‌سایت‌ها) و بدون توسل به هیچ منبع غیرقانونی، می‌توان بیش از ۸۰٪ از اطلاعات مورد نیاز را به‌دست آورد (Federation of American Scientists 2006, p. UK/BM80)». بنابراین، می‌توان تصور کرد که برای یک حمله برنامه‌ریزی‌شده توسط یک گروه هوشمند، دسترسی کامل به اطلاعات وجود دارد.
- راهبردهای دفاعی هزینه‌برند. از آن‌جا که در طراحی شبکه‌ها، تنها اهداف اقتصادی بکار گرفته می‌شوند، و از آن‌جا که انگیزه‌ی کاهش آسیب‌پذیری یک شبکه دارای اهداف غیراقتصادی است، این تناقض باعث می‌شود تا طراحی‌های صورت‌گرفته از نقطه‌نظر آسیب‌پذیری غیربهینه بوده و پس از طراحی، انتخاب یک راهبرد استحکام، هزینه زیادی را به سیستم تحمیل کند.

یوان[2] [۱۴] نیز مشابه بسیاری از مقالاتی که به بررسی و انتخاب بهینه‌ترین راهبرد دفاعی پرداخته‌اند، با ارائه یک مدل سه‌سطحی DAD به تخصیص بهینه منابع مدافع برای حفاظت از شبکه برق پرداخته است. مشابه [۱]، تابع هدف انتخاب‌شده برای مدافع و مهاجم در مدل یوان [۱۴]، کمینه/بیشینه‌کردن میزان قطع‌بار شبکه بوده و مدل حاصل به‌صورت یک مدل min-max-min فرمول‌بندی شده است. این مدل، تفاوت چندانی با مدل ارائه‌شده در [۱] ندارد و تنها در نوع مدل‌سازی و فرمول‌بندی قید عدم حمله به خط انتقالی که حفاظت شده است، با یکدیگر تفاوت دارند. آلگواچیل [۱] برای مدل‌کردن این قید، از رابطه خطی ساده زیر استفاده کرده است:

$$\delta_l \geq w_l; \quad \forall l \in L \qquad (۴۱)$$

در صورتی که خط l دفاع شده باشد ($w_l = 1$)، δ_l به اجبار برابر با یک شده به این معنی که، این خط نمی‌تواند مورد حمله واقع شود ($\delta_l = 0$ به این معنی است که به خط l حمله شده و این خط از مدار خارج است). این در حالی است که، یوان [۱۴] برای مدل کردن قید بیان‌شده، از رابطه غیرخطی زیر استفاده کرده است که البته می‌توان این رابطه را بدون استفاده از متغیرهای باینری جدید، با چند قید خطی جایگزین کرد:

$$w_l = \delta_l w_l; \quad \forall l \in L \qquad (۴۲)$$

در صورتی که خط l دفاع شده باشد ($w_l = 1$)، δ_l به اجبار برابر با یک شده و این به این معنی است که این خط نمی‌تواند مورد حمله واقع شود ($\delta_l = 0$ به این معنی است که به خط l حمله شده و این خط از مدار خارج است). تفاوت دیگری که در قیود مربوط به این دو مدل وجود دارد این است که آلگواچیل [۱]، در مدل‌سازی منابع در دسترس مدافع و مهاجم، این قیود را به‌صورت مساوی در نظر گرفته است و این بدین معنی است که مدافع و مهاجم حتماً از تمامی منابع خود استفاده می‌کنند. این در حالی است که یوان [۱۴] این قیود را منطقی‌تر و به‌صورت نامساوی فرمول‌بندی کرده است. واضح است که در حالت کلی الزامی ندارد که مدافع و مهاجم از تمامی منابع خود استفاده کنند. یکی از چالش‌های اصلی پیشِ روی مدل‌های DAD، حل دقیق[3] این مدل‌ها و کاربرد آن‌ها برای شبکه‌های بزرگ است. نوآوری اصلی تحقیق یوان [۱۴]، ارائه یک راه‌حل جدید برای حل دقیق مسائل سه‌سطحی DAD است.

یائو[4] [۱۵] در تحقیق خود، مشابه [۱] و [۱۴] به ارائه یک مدل سه‌سطحی min-max-min برای تخصیص بهینه منابع مدافع پرداخته است. تفاوت عمده این مدل با موارد مشابه، در روش حل انتخاب‌شده و نیز در نظر گرفتن تمام المان‌های شبکه برای دفاع

[1] Reliability
[2] Yuan
[3] Exact
[4] Yao

است. در مدل ارائه‌شده در این مقاله [۱۵]، اثر تخریب و یا دفاع از یک المان بر روی سایر المان‌های متصل به آن، با استفاده از فرض‌های زیر در نظر گرفته شده است:

- با حمله به یک خط انتقال، تمام خطوط موازی با آن نیز از مدار خارج می‌شوند؛
- با حمله به یک شین، تمام خطوط انتقال، بار و ژنراتورهای متصل به آن نیز از مدار خارج می‌شوند؛
- با حمله به یک پست برق، تمام شین‌های موجود در آن نیز از مدار خارج می‌شوند.
- در صورتی که تجهیز j و یا حداقل یکی از تجهیزاتی که حمله به آن‌ها موجب از کار افتادن آن تجهیز می‌شود ($K(j)$)، دفاع شود، دیگر نمی‌توان به آن تجهیز حمله کرد.

فرض آخر به‌صورت زیر مدل شده است:

$$\delta_j \le \prod_{k \in K(j)} \left(1 - w_j\right), \quad \forall j \in J \qquad (۴۳)$$

این فرض در حالت کلی نمی‌تواند صحیح باشد. به‌عنوان مثال، اگر شین ابتدای یک خط انتقال دفاع شود، طبق این فرض، دیگر مهاجم نمی‌تواند به آن خط حمله کند و این موضوع منطقی نیست.

آلدِرسون[1] [۱۳] نیز مشابه تحقیقات دیگر، به ارائه یک مدل DAD برای تخصیص بهینه منابع پرداخته است. در این مقاله، کامل‌تر از سایر مدل‌های DAD، برای زیرمسأله‌AD، از مدلی استفاده کرده که علاوه بر در نظر گرفتن حملات عامدانه، جنبه‌های تصادفی نیز در نظر گرفته شده‌اند [۲۷، ۲۹ و ۳۰]. در تعریف جنبه‌های تصادفی، به‌عنوان مثال، عمر یک تجهیز یدکی که جایگزین یک تجهیز تخریب‌شده می‌شود، یک ماهیت تصادفی دارد و باید این موضوع در برنامه‌ریزی لحاظ شود.

مرجع [۲۴] به‌طور کلی مسأله دفاع از بخش‌های حیاتی یک کشور را در مقابل حملات فیزیکی مطرح کرده است. این بخش‌ها شامل بخش کشاورزی و غذا، آب، سلامت اجتماعی، خدمات اضطراری، مخابرات، انرژی، صنعت، حمل و نقل، بانک و دارایی، صنعت دارو، پست و کشتیرانی می‌شود. در بین زیرساخت‌های حیاتی کشورها، می‌توان مهم‌ترین آن‌ها را شبکه برق دانست، چرا که تمامی زیرساخت‌های یک کشور وابسته به عملکرد صحیح این شبکه است[۲۴]. در این گزارش نیز مشابه مرجع [۷]، عنوان شده است که گروه‌های مخاصم در بلندمدت به اهداف خود فکر می‌کنند و سه دسته هدف عمده برای حمله این گروه‌ها به زیرساخت‌های یک کشور برشمرده شده است:

۱) اثرات مستقیم زیرساخت‌ها و مختل کردن کارآیی آن‌ها؛
۲) اثرات غیرمستقیم زیرساخت‌ها و تحمیل خسارت‌های مالی برای دولت و جامعه و بخش‌های خصوصی؛ و
۳) تخریب یک زیرساخت برای ضربه زدن به زیرساخت‌های وابسته به آن.

با وجود این‌که در اکثر مقالات ارائه‌شده در زمینه بررسی آسیب‌پذیری و تخصیص بهینه منابع در مقابل حملات عامدانه، تابع هدف مهاجم را هزینه در نظر گرفته‌اند، این گزارش [۲۴]، یکی از چالش‌های اساسی بحث تخصیص بهینه منابع را ارزیابی دقیق خسارت‌های مالی ناشی از حملات عامدانه مطرح می‌کند. حملات عامدانه دارای یک سری خسارت‌ها کوتاه‌مدت و یک سری خسارت‌های بلندمدت هستند و نباید خسارت‌های بلندمدت در سایه خسارت‌های کوتاه‌مدت نادیده گرفته شود. این موضوع لازم می‌دارد که مطالعات آسیب‌پذیری و تخصیص منابع به‌صورت بلندمدت صورت پذیرد [۲۴]. یکی دیگر از چالش‌های پیش رو در بررسی آسیب‌پذیری و تخصیص بهینه منابع این است که عوامل و سازمان‌های مختلفی در این بررسی‌ها مشارکت دارند و گاه مدل‌هایی که سازمان‌های مختلف استفاده می‌کنند یا به نتایج متناقض می‌رسند و یا به نتایجی که قابل قیاس نیستند [۲۴]. چالش دیگر این است که گاهی المان‌های آسیب‌پذیر، جنبه مشترک و بین‌مرزی دارند. به‌عنوان مثال، از آن‌جا که شبکه‌های برق کشورهای مختلف به دلایل متعدد به هم وصل‌اند، آسیب‌پذیری یک شبکه ممکن است جنبه بین‌المللی داشته باشد و باید راهکارهای جدید برای کاهش این‌گونه آسیب‌پذیری‌ها اندیشیده شود [۲۴]. این گزارش [۲۴]، یکی از موضوعات مهمی را که باید به آن توجه کرد، توسعه ابزارهای شبیه‌سازی و بیان استانداردهای مرتبط معرفی می‌کند. در این راستا باید از افراد خبره استفاده کرد و آموزش‌های کافی به کسانی داد که بررسی‌های مرتبط با آسیب‌پذیری و تخصیص منابع را انجام می‌دهند.

۵- نتیجه‌گیری

در این مقاله، مروری جامع بر مهم‌ترین مدل‌های ارائه‌شده برای تخصیص بهینه منابع و انتخاب بهینه راهبرد دفاعی ارائه شد. مدل‌های ارائه‌شده، بر اساس رویکردی که در فرمول‌بندی رفتار مدافع و مهاجم انتخاب کرده‌اند، در دو دسته مدل‌های دوسطحی و مدل‌های سه‌سطحی قرار گرفتند. مدل‌های دوسطحی عموماً

[1] Alderson

به‌صورت مدل‌های مدافع-مهاجم (DA) هستند که در آن، مهاجم سعی در بیشینه‌کردن خسارت دارد و مدافع به دنبال کمینه کردن تابع هدف مهاجم، از طریق تخصیص بهینه منابع است.

یکی از چالش‌های پیش روی این مدل‌ها این است که نمی‌توانند تمام کنش‌ها و واکنش‌های ممکن مدافع و مهاجم را مدل‌سازی کنند. طبیعت چنین کنش و واکنش‌هایی بیشتر مشابه یک مدل سه‌سطحی مدافع-مهاجم-مدافع (DAD) است که در سطح اول آن، مدافع قصد تخصیص بهینه منابع مالی خود را دارد و در سطح دوم، مهاجم با منابع محدود خود، بهترین نقشه حمله را انتخاب می‌کند و در سطح سوم، مدافع شبکه، شبکه را به‌گونه‌ای بهره‌برداری می‌کند تا خسارت‌های ناشی از حمله مهاجم کمینه شود. این نوع مدل‌سازی این امکان را فراهم می‌کند تا بتوان اثر تغییرات ایجادشده در شبکه (در سطح‌های اول و دوم مسأله) را بر روی وضعیت بهره‌برداری سیستم مدل‌سازی کرد و اثر آن را مشاهده کرد.

یکی از چالش‌های اصلی مدل‌های سه‌سطحی، حل دقیق آن‌ها در کاربردهای مقیاس بزرگ است. از آن‌جا که در سطوح پایین این مسائل، متغیرهای گسسته وجود دارد، امکان یکپارچه‌سازی و حل آن‌ها به‌صورت دقیق وجود ندارد. اما با این حال در مدل‌هایی که در این مقاله بررسی شد، روش‌های مؤثری که بیشتر مبتنی بر شمارش حالت‌ها هستند ارائه‌شده است که تا حدی می‌توانند مشکل عنوان‌شده را رفع کنند. بر این اساس، در ادامه این تحقیق می‌توان دسته‌بندی دیگری بر اساس روش حل مقالات مختلف ارائه داد تا برنامه‌ریز شبکه بتواند در کاربردهای مقیاس بزرگ، بهترین روش حل را نیز برای به دست آوردن بهترین جواب ممکن انتخاب کند. روش تجزیه‌ی بندرز[1] نیز در حل مدل‌های پیچیده در مقیاس بزرگ، توانمندی خوبی از خود نشان داده است و می‌توان از این روش برای حل مدل‌های ارائه‌شده استفاده کرد.

در تحقیقات آینده می‌توان مدل‌های DAD را بهبود داد و برای بخش AD آن، از مدل‌های قدرتمندتری که در مراجع برای بررسی آسیب‌پذیری شبکه برق ارائه‌شده است، استفاده کرد. به‌عنوان مثال، می‌توان تخصیص بهینه منابع را با هدف کمینه‌کردن ریسک خاموشی سراسری[2] انجام داد و در این روند، احتمال و ریسک حملات مختلف را نیز لحاظ کرد.

[1] Benders Decomposition
[2] Blackout

۶- فهرست علائم و نمادها

۶-۱- مجموعه‌ها

B	مجموعه ترانسفورماتورهای شبکه.
F	مجموعه شامل تمام تجهیزات در یک سیستم.
G	مجموعه ژنراتورهای شبکه.
H	مجموعه شامل نقاط تقاضا در یک سیستم.
J_j	مجموعه شامل المان‌های تجهیز j.
L	مجموعه خطوط انتقال شبکه.
N	مجموعه شین‌های شبکه.
O_s	مجموعه شین‌های موجود در پست s.
P	مجموعه شامل حالت‌های سیستم.
S	مجموعه پست‌های شبکه.
T	مجموعه هدف‌های ممکن (M بیان‌گر تعداد هدف‌ها).
V	مجموعه سناریوهای حمله.

۶-۲- ثابت‌ها

C_g^E	هزینه تولید مربوط به ژنراتور g.
C_i^B	هزینه جایگزینی ترانسفورماتور i که مورد حمله قرار گرفته است.
C_j	هزینه دفاع از تجهیز j.
C_l^I	هزینه احداث خط انتقال l.
$C_{Protection}$	بخشی از منابع مدافع که برای حفاظت تجهیزات در نظر گرفته شده است.
$C_{Recovery}$	بخشی از منابع مدافع که برای بازیابی تجهیزات در نظر گرفته شده است.
C_{Total}	کل منابع مدافع.

D_n میزان تقاضا در گره n.

E_{ijl} پارامتر خط و ترانسفورماتور (اگر صفر باشد به معنی این است که شاخه ij یک خط انتقال است و اگر یک باشد، ترانسفورماتور).

n_v تعداد سناریوهای حمله.

q_j احتمال انتخاب هدف j و حمله به آن.

q_p احتمال آن‌که سیستم در حالت p باشد.

t_j^{base} زمان پایه برای المان‌هایی که تخریب می‌شوند و بدون بودجه‌ی اضافی تعمیر می‌شوند.

t_k مدت‌زمان لازم برای کامل شدن مرحله kام تعمیرات.

U_{nj} کمترین فاصله برای تأمین بار گره n از تجهیز j در یک سیستم.

$y_{\min}$ کمترین میزان پی‌آمدهای حمله.

α_n هزینه قطع‌بار در شین n.

β ضریب وزنی برای هزینه سرمایه‌گذاری.

γ ضریب وزنی برای هزینه احتمالی قطع بار.

η^0 راندمان مطلوب سیستم.

K_v احتمال موفقیت حمله v (آسیب‌پذیری).

π_v احتمال وقوع سناریوی حمله v (تهدید).

۶-۳- متغیرها

c بردار تخصیص منابع مدافع (راهبرد دفاعی) به‌صورت $c=\{c_1,c_2,\ldots,c_{Recovery}\}$.

d_v^O حداقل هزینه بهره‌برداری با در نظر گرفتن حمله v.

ς^T خسارت کل واردشده به مدافع، شامل هزینه تلفات ناشی از کاهش راندمان سیستم به مقداری کمتر از η^0 و نیز تلفات ذاتی ناشی از تخریب المان‌های سیستم.

ς_{jr}^e ارزش ذاتی المان r در تجهیز j (خسارتی که مدافع در صورت تخریب این المان متحمل می‌شود).

ς_{jm}^{PG} ارزش ذاتی المان گروه حفاظت m در تجهیز j (خسارتی که مدافع در صورت تخریب این گروه حفاظت متحمل می‌شود).

e_j تابع حفاظت تجهیز j.

h^D بردار شامل متغیرهای عدد صحیح خرید ترانسفورماتور (h_i^D اشاره به تعداد ترانسفورماتورهای خریداری‌شده از نوع i می‌کند).

$o(\varepsilon,\varphi)$ کل هزینه مدافع برای راهبرد جدایی (φ) و راهبرد حفاظت ε.

r بردار شامل متغیرهای باینری تعویض ترانسفورماتور (اگر r_{ijb} برابر با یک باشد به معنی این است که در شاخه ij، از ترانسفورماتور یدکی b استفاده شده است، و در غیر این صورت صفر است).

δ^G بردار شامل متغیرهای باینری حمله به ژنراتور (اگر δ_g^G برابر با یک باشد به معنی این است که ژنراتور g مورد حمله قرار گرفته است، و در غیر این صورت صفر است).

ϑ بردار شامل متغیرهای باینری تغذیه گره‌های شبکه (اگر ϑ_{nj} برابر با یک باشد به معنی این است که تقاضای گره n پس از حمله از تجهیز j تأمین می‌شود).

δ^L بردار شامل متغیرهای باینری حمله به خطوط انتقال (اگر δ_{ij}^L برابر با یک باشد به معنی این است که خط ij مورد حمله قرار گرفته است، و در غیر این صورت صفر است).

δ^S بردار شامل متغیرهای باینری حمله به پست (اگر δ_s^S برابر با یک باشد به معنی این است که پست s مورد حمله قرار گرفته است، و در غیر این صورت صفر است).

ς خسارت کل واردشده به مدافع، شامل هزینه تلفات ناشی از کاهش راندمان سیستم به مقداری کمتر از

η^0 و نیز تلفات ذاتی ناشی از تخریب المان‌های سیستم.

$u(\circ)$ تابع واحد: $u(True)=1$ و $u(False)=0$

w_j متغیر باینری دفاع (اگر یک باشد به معنی آن است که تجهیز j ام شبکه به‌عنوان گزینه دفاع انتخاب شده است و در غیر این صورت صفر است).

x^G بردار شامل متغیرهای عدد صحیح توسعه ژنراتور (x_g^G اشاره به افزایش L_g^G واحد ظرفیت به ظرفیت ژنراتور g می‌کند).

x^L بردار شامل متغیرهای عدد صحیح توسعه خط (x_{ij}^l اشاره به افزایش L_{ij} واحد ظرفیت به ظرفیت خط انتقال ij می‌کند).

y^0 بدبینانه‌ترین تلفات ممکن.

y_j خسارت ناشی از حمله به هدف j.

y_S متوسط تلفات حمله به هدف j، که S زیرمجموعه‌ای از مجموعه j می‌باشد.

z_j بهره مهاجم از حمله به هدف j.

$\Delta P_n^{d^*}$ میزان بار قطع‌شده در شین nام.

$\delta_{j,v}$ پارامتر باینری حمله (در صورتی که در نقشه حمله v به تجهیز j حمله شده باشد، یک، و در غیر این صورت صفر خواهد بود).

۷- منابع

1. N. Alguacil, A. Delgadillo, and J. M. Arroyo, “A Trilevel Programming Approach for Electric Grid Defense Planning,” Comput. Oper. Res., vol. 41, pp. 282–290, 2014.
2. G. Brown, M. Carlyle, J. Salmerón, and K. Wood, “Defending Critical Infrastructure,” Interfaces, vol. 36, pp. 530–544, 2006.
3. G. Chen, Z. Y. Dong, D. J. Hill, Y. S. Xue, “Exploring Reliable Strategies for Defending Power Systems Against Targeted Attacks,” IEEE Trans. Power Syst., vol. 26, pp. 1000–1009, 2011.
4. A. J. Holmgren, E. Jenelius, and J. Westin, “Evaluating Strategies for Defending Electric Power Networks Against Antagonistic Attacks,” IEEE Trans. Power Syst., vol. 22, pp. 76–84, 2007.
5. M. Carrión, J. M. Arroyo, and N. Alguacil, “Vulnerability-Constrained Transmission Expansion Planning: A Stochastic Programming Approach,” IEEE Trans. Power Syst., vol. 22, pp. 1436–1445, 2007.
6. M. P. Scaparra and R. L. Church, “A Bilevel Mixed-Integer Program for Critical Infrastructure Protection Planning,” Comput. Oper. Res., vol. 35, pp. 1905–1923, 2008.
7. R. Powell, “Defending Against Strategic Terrorists over the Long Run: a Basic Approach to Resource Allocation,” Working Paper, University of California, Travers Department of Political Science, Berkeley, 2006.
8. G. Levitin, “Optimal Defense Strategy Against Intentional Attacks,” IEEE Trans. Reliab., vol. 56, pp. 148–157, 2007.
9. V. Bier, “Game-Theoretic and Reliability Methods in Counterterrorism and Security,” Statistical Methods in Counterterrorism, pp. 23–40, 2006.
10. E. Kardes and R. Hall, “Survey of Literature on Strategic Decision Making in the Presence of Adversaries,” Nonpublished Research Reports, vol. 115, 2005.
11. N. Romero, N. Xu, L. K. Nozick, I. Dobson, and D. Jones, “Investment Planning for Electric Power Systems under Terrorist Threat,” IEEE Trans. Power Syst., vol. 27, pp. 108–116, 2012.
12. R. W. Rose, “Defending Electrical Power Grids,” M.Sc. Thesis, Naval Postgraduate School, Monterey, CA, 2007.
13. D. L. Alderson, G. G. Brown, W. M. Carlyle, and R. K. Wood, “Solving Defender-Attacker-Defender Models for Infrastructure Defense,” In Informs Computing Society Conference, pp. 28-49, 2011.
14. W. Yuan, L. Zhao, and B. Zeng, “Optimal Power Grid Protection through a Defender–Attacker–Defender Model,” Reliab. Eng. Syst. Saf., vol. 121, pp. 83–89, 2014.
15. Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, “Trilevel Optimization In Power Network Defense,” IEEE Trans. Syst. Man, Cybern, vol. 37, pp. 712–718, 2007.
16. J. Salmeron, K. Wood, and R. Baldick, “Analysis of Electric Grid Security under Terrorist Threat,” IEEE Trans. Power Syst., vol. 19, pp. 905–912, 2004.
17. A. L. 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, pp. 1357–1365, 2005.
18. 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, pp. 789–797, 2005.
19. M. Chertoff, “Remarks for Secretary Michael Chertoff, US Department of Homeland Security, George Washington University Homeland Security Policy Institute,” Georg. Washingt. Univ. Washington, DC, 2005.

20. M. G. F. Bell, "The Use Of Game Theory To Measure The Vulnerability Of Stochastic Networks," IEEE Trans. Reliab, vol. 52, pp. 63–68, 2003.
21. H. H. Willis, A. R. Morral, T. K. Kelly, and J. J. Medby, "Estimating Terrorism Risk," Rand Corporation, 2006.
22. N. J. Rabkin, "Strengthening the Use of Risk Management Principles in Homeland Security Risk Management," U. S. Government Accountability Office, 2008.
23. DHS, "The 2009 National Infrastructure Protection Plan," Department of Homeland Security, 2009.
24. G. W. Bush, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," Nonpublished Research Reports, 2003.
25. R. E. Alvarez, "Interdicting electrical power grids," M. Sc. Thesis, Naval Postgraduate School, Monterey, CA, 2004.
26. A. J. Wood and B. F. Wollenberg, "Power Generation, Operation, and Control," John Wiley & Sons, 2012.
27. J. M. Arroyo, "Bilevel Programming Applied To Power System Vulnerability Analysis under Multiple Contingencies," IET Gener. Transm. Distrib., vol. 4, pp. 178–190, 2010.
28. E. Israeli and R. K. Wood, "Shortest-Path Network Interdiction," Networks, vol. 40, pp. 97–111, 2002.
29. K. J. Cormican, D. P. Morton, and R. K. Wood, "Stochastic Network Interdiction," Oper. Res., 46, pp. 184–197, 1998.
30. D. P. Morton, F. Pan, and K. J. Saeger, "Models for Nuclear Smuggling Interdiction," IIE Trans., vol. 39, pp. 3–14, 2007.

A Review on Optimal Resource Allocation Methodsto Defend the Power Grids against Intentional Attacks

R. Gaffarpour[*], S. Sayyadipour

Abstract

International reports and statistics reveal that power grids have been one of the main targets for terrorist groups in recent years.Power grid has a vital role in all countries and, the functionality of all infrastructures depends on the performance of this network. In acountry, the economy and the electric industry are highly interdependent and, consequently, the malfunction of the power grid results in a huge economic loss for that country. As a result, various models have been proposed by researchers, in an attempt to answer to this question that how the available defensive resources should be optimally allocated to alleviate the negative consequences of the intentional attacks. Power grid planner's knowledge of these models can be helpful in selecting the best defense strategy for defending the power grid against intentional attacks. To the best of our knowledge, no review has been conducted on the proposed methods so far.Hence, in this paper, a comprehensive review of the most important models is conducted and a proper classification is provided. Then, the models belonging to each class are analyzed in detail, focusing on their flaws and merits.

Key Words: *Intentional Attacks, Power Grid Vulnerability Analysis, Optimal Resource Allocation, Optimal Defense Strategy Selection*

[*] Imam Hossein Comprehensive University - (rghaffarpour@ihu.ac.ir) - Writer-in-Charge