مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال هفتم، شماره ۴، زمستان ۱۳۹۵؛ ص ۳۳۷-۳۲۷

ارائه روشی برای ارزیابی و کاهش ریسک سامانه قدرت در برابر تهدیدات تروریستی

محمدحسین رنجبر[۱]، ابوالفضل پیرایش[۲*]

۱- دانشجوی دکتری، ۲- استادیار، دانشگاه شهید بهشتی

(دریافت: ۹۴/۱۲/۲۲، پذیرش: ۹۵/۰۶/۲۰)

چکیده

ارزیابی ریسک زیرساخت‌ها در برابر تهدیدات یکی از مهم‌ترین ملاحظات پدافند غیرعامل است. سامانه قدرت به عنوان یکی از مهم‌ترین زیرساخت‌های هر کشور که دیگر زیرساخت‌ها بدان وابسته است، همواره هدفی جذاب برای گروه‌های تروریستی بوده است. هدف از این مقاله ارائه روشی برای ارزیابی ریسک سامانه قدرت در برابر تهدیدات تروریستی و همچنین ارائه روشی برای کاهش ریسک سامانه با تخصیص بهینه بودجه پدافند غیرعامل برای مستحکم‌سازی تجهیزات آن است. بدین منظور ابتدا مدل احتمالی حمله موفقیت‌آمیز تروریستی به تجهیزات سامانه مشخص می‌شود و در گام بعد با مشخص کردن خسارت ناشی از حمله، ریسک سامانه برای سناریوهای مختلف تعیین می‌شود. در ادامه، بودجه پدافند غیرعامل برای مستحکم‌سازی تجهیزات به صورت بهینه اختصاص می‌یابد. به منظور نشان دادن کارایی روش ارائه‌شده برای ارزیابی و کاهش ریسک سامانه قدرت، سامانه آزمایش ۲۴ باسه IEEE مورد آزمون قرار گرفته است. نتایج شبیه‌سازی نشان می‌دهد که چگونه با اختصاص بودجه پدافند غیرعامل، ریسک سامانه کاهش می‌یابد.

کلیدواژه‌ها: ارزیابی ریسک، آسیب‌پذیری، احتمال حمله موفقیت‌آمیز، خسارت ناشی از حمله، مسئله بهینه‌سازی کوله‌پشتی

Providing a Method to Assess and Reduce the Risk of Power System against Terrorist Threats

M. H. Ranjbar, A. Pirayesh[*]

Shahid Beheshti University

(Received: 13/03/2016; Accepted: 13/03/2016)

Abstract

Risk assessment of infrastructures against threats, is one of the most important consideration in passive defence. Power system is an infrastructures on which other infrastructures are depended. This infrastructure is always regarded by terrorists as an attractive target. This paper presents a method for risk assessment of power system. It also presents a method for risk reduction of power system based on optimal allocation of defence budget for hardening facilities of power system. First, probability model of successful terrorist attack to power system's facilities is presented and by combining of this probability and consequences of attack, risk of each scenario is achieved. Then, power system's defence budget is optimally allocated for hardening its facilities. In order to indicate the effectiveness of these methods, IEEE 24-bus reliability test system is tested. Results show how system's risk is reduced by the allocation of defence budget for system protection.

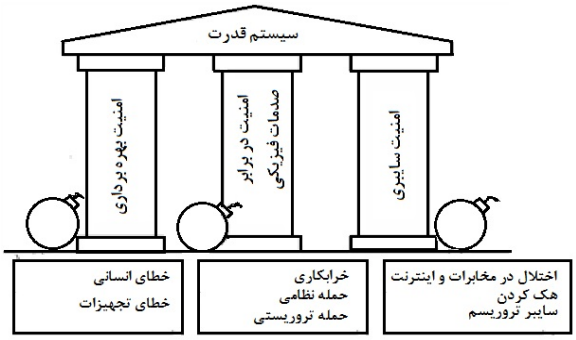
Keywords: Risk Assessment, Vulnerability, Probability of Successful Attack, Consequences, Knapsack Problem

[*] Corresponding Author E-mail: A_pirayesh@sbu.ac.ir

۱. مقدمه

بحث آسیب‌پذیری و ریسک سامانه‌ها و زیرساخت‌های اساسی برای اولین بار در دهه ۱۹۷۰ میلادی برای امنیت تأسیسات هسته‌ای در برابر تهدیدات تروریستی و خراب‌کارانه به صورت جدی مطرح شد. در طول سالیان گذشته، مفاهیمی نظیر آسیب‌پذیری، ریسک، مدیریت بحران و اخیراً نظریه بازی بحث مقابله با تهدیدات امنیتی زیرساخت‌های اساسی را شکل داده‌اند [۸-۱]. در سال‌های اخیر، تجربیات جنگ‌ها و حملات تروریستی بر اهمیت مطالعه آسیب‌پذیری و ریسک زیرساخت‌های اساسی افزوده است. یکی از مهم‌ترین زیرساخت‌های اساسی هر کشور، زیرساخت شبکه برق آن است زیرا زیرساخت‌های دیگر به آن وابسته‌اند. جنگ‌های بالکان و عراق نمونه‌هایی از حملات مستقیم به زیرساخت سامانه قدرت است [۹].

شکل (۱) ابعاد مسئله امنیت سامانه قدرت را نشان می‌دهد. مقابله با تهدیدات بهره‌برداری، تهدیدات فیزیکی و همچنین تهدیدات سایبری ستون‌های امنیت سامانه قدرت را تشکیل می‌دهند.



شکل ۱. ابعاد مسئله امنیت سامانه قدرت [۱۰]

تهدیدات بهره‌برداری به حوادث درون شبکه‌ای نظیر خطا و خرابی تجهیزات و برون شبکه‌ای مانند برخورد صاعقه، طوفان و اشتباه عوامل انسانی اطلاق می‌شود. در سالیان متمادی مسئله امنیت و قابلیت اطمینان سامانه قدرت در برابر این تهدیدات در نظر گرفته شده و راهکارهای مقابله با آن شناخته شده است.

تهدیدات فیزیکی یا تهدیدات امنیتی به اقداماتی اطلاق می‌شود که عامدانه و از روی عناد برای ایجاد اختلال در زیرساخت سامانه قدرت انجام می‌شود. عملیات تروریستی، خراب‌کارانه و نظامی از نمونه‌های تهدیدات فیزیکی سامانه قدرت هستند. خسارات و اختلالات چنین تهدیداتی می‌تواند بسیار زیاد و تأثیرگذار باشد. مطالعه تحقیقات گذشته در خصوص مقابله با تهدیدات امنیتی و فیزیکی سامانه‌ها، ابهامات و سردرگمی‌هایی را ایجاد می‌کند که علت آن عدم وحدت نظر متخصصان و دانشمندان این حوزه در خصوص برخی مفاهیم نظیر آسیب‌پذیری، ریسک و تهدید است [۱۱]. در این تحقیق سعی شده است تا این مفاهیم به صورت روشن تعریف و دسته‌بندی گردد. با جمع‌بندی تحقیقات گذشته می‌توان نتیجه گرفت که مسئله مقابله با تهدیدات سامانه قدرت از مفاهیم و موضوعاتی تشکیل شده است که به صورت پلکانی، پشت سرهم قرار می‌گیرند و همدیگر را تکمیل می‌کنند. این مفاهیم در شکل (۲) توسط نگارنده نشان داده شده است.

شکل ۲. مفاهیم موضوعی مسئله مقابله با تهدیدات امنیتی سامانه‌ها

در تمامی برنامه‌های دفاع از سامانه قدرت در برابر تهدیدات امنیتی، اولین گام شناسایی نقاط گلوگاهی یا ارزیابی آسیب‌پذیری سامانه قدرت است [۱۲]. احتمال وقوع حمله به این نقاط گلوگاهی با توجه به ویژگی‌های جغرافیایی و پدافندی آن‌ها و همچنین احتمال موفقیت‌آمیز بودن حمله در صورت وقوع با توجه به ویژگی‌های پدافندی و مستحکم‌سازی آن نقاط، بحث بعدی در برنامه دفاع از سامانه قدرت را شکل می‌دهد. فرض کنید نقطه‌ای در شبکه قدرت به عنوان نقطه گلوگاهی مطرح شود که از دست رفتن آن موجب خسارت بسیار بزرگی به شبکه شود ولی درعین‌حال با توجه به دور بودن آن از منطقه تهدید، احتمال از دست رفتن آن بر اثر حمله موفقیت‌آمیز بسیار اندک است. در این صورت آن نقطه در برنامه دفاع و مستحکم‌سازی چندان مورد توجه قرار نمی‌گیرد. در نظر گرفتن هم‌زمان میزان خسارت ناشی از دست رفتن تأسیسات در اثر حمله و احتمال وقوع حمله موفقیت‌آمیز به آن‌ها مفهوم ریسک را شکل می‌دهد.

هدف از این تحقیق، بررسی ریسک سامانه قدرت در برابر تهدیدات تروریستی است. در بخش دوم مفهوم ریسک ارائه و تفاوت آن با آسیب‌پذیری بررسی شده است. در بخش سوم روش محاسباتی برای ارزیابی ریسک سامانه قدرت و کاهش بهینه آن بررسی شده است. در بخش چهارم اعمال شبیه‌سازی و نتایج و در بخش آخر نیز نتیجه‌گیری بیان شده است.

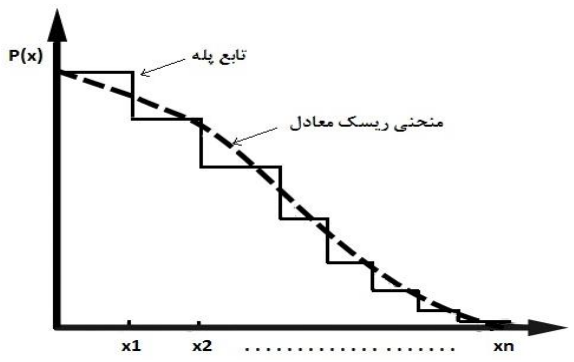
۲. مفهوم ریسک

در دهه‌های اخیر مفهوم ریسک مورد توجه دولت‌مردان و متخصصان قرار گرفته است. ارائه یک مفهوم کامل و قابل‌لمس از ریسک که در همه جا قابل استفاده باشد، ضروری است. این امر توسط کاپلان و همکاران [۱۳] انجام شده است. در سال ۱۹۷۶ لارنس ریسک را "احتمال و شدت اتفاقات نامطلوب" تعریف کرد. یک سال بعد کاپلان تعریف ریسک را در غالب سه سؤال روبه‌رو که به سؤالات سه‌گانه معروف است، اصلاح کرد. چه اتفاقات نامطلوبی می‌تواند بیفتد؟ احتمال هر کدام چقدر است؟ خسارت و نتیجه هر کدام چیست؟ در این تعریف اتفاقات (سناریوها) به تعریف قبلی اضافه شده است.

کمی‌سازی ریسک در دو گام انجام می‌شود. در گام اول برای تبیین ریسک و کمی‌سازی آن باید به سه سؤال بالا پاسخ داد. پاسخ به سؤالات بالا به مجموعه‌ای از اتفاقات (سناریوها) ممکن می‌انجامد که هر کدام احتمالی برای وقوع و خسارتی دارند. این مجموعه در جدول (۱) نشان داده شده است. اگر سناریوهای این جدول به این صورت مرتب شود که خسارت‌ها (xiها) از کوچک به بزرگ قرار بگیرند، در واقع می‌توان احتمالات تجمعی (P_i) را به صورت تجمعی با جمع کردن احتمالات منفرد (p_i) از پایین جدول به بالای جدول به دست آورد. حال اگر این جدول تجمعی در دو بعد رسم شود به صورتی که محور افقی xi ها و محور عمودی احتمالات تجمعی باشد منحنی ریسک ترسیم شده است. شکل (۳) این منحنی را به صورت پله‌ای نشان می‌دهد.

جدول ۱. لیست سناریوها، احتمالات وقوع و نتایج حاصله

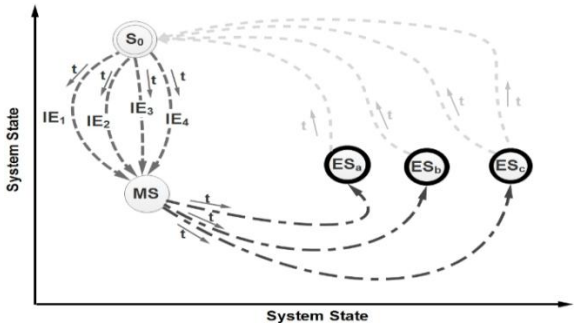
سناریو	احتمال	نتیجه	احتمال تجمعی
s_1	p_1	x_1	$P_1= p_1+ P_2=1$
s_2	p_2	x_2	$P_2= p_2+ P_3$
s_3	p_3	x_3	$P_3= p_3+ P_N$
s_N	p_N	x_N	$P_N= p_N$



شکل ۳. منحنی ریسک

برخی متخصصان ریسک را احتمال وقوع ضربدر خسارت تعریف کرده‌اند. در این صورت ریسک یک نقطه می‌شود که برای مجموع سناریوها برابر با مقدار میانگین منحنی ریسک است.

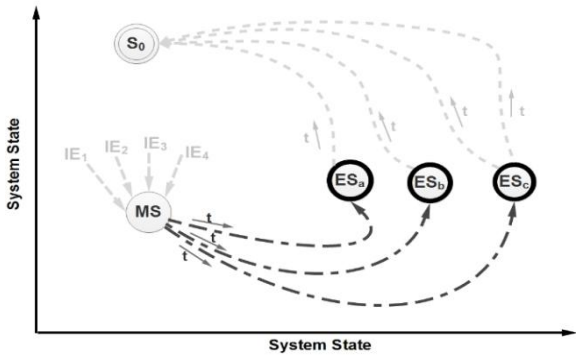
در گام دوم برای کمی‌سازی مفهوم ریسک، عدم قطعیت[1] در مقادیر منحنی نیز مطرح می‌شود و نشان داده می‌شود مفهوم ریسک فراتر از آن است که بتوان آن را با یک منحنی نشان داد [۱۳]. گاهی اوقات مفهوم ریسک و آسیب‌پذیری در مقالات و مراجع سبب سردرگمی می‌شود [۱۱]. آسیب‌پذیری پاسخ سامانه به حادثه و مقابله سامانه با آن حادثه مشخص است و به زبان ساده نتایج و عواقب حاصل از حادثه (حمله) با فرض وقوع آن است [۳]. در واقع در تحلیل آسیب‌پذیری احتمال وقوع حادثه در نظر گرفته نمی‌شود و فرض می‌شود که حادثه رخ داده است و با فرض رخ دادن آن، عواقب و خسارت حادثه محاسبه و بررسی می‌شود. ریسک بر احتمال وقوع حملات و نتایج و خسارت ناشی از آن‌ها تأکید دارد یعنی هم‌زمان هم به احتمال وقوع حملات توجه می‌کند و هم به نتایج و عواقب آن‌ها. در واقع ارزیابی آسیب‌پذیری گامی از ارزیابی ریسک است [۳ و ۱۲]. اگر تنها احتمال و استعداد وقوع سناریوها و حملات مورد مطالعه قرار گیرد، ارزیابی تهدید صورت گرفته است. برای روشن شدن بحث از شکل‌های زیر کمک گرفته می‌شود. در شکل‌های زیر سه حالت سامانه به نام‌های حالت اولیه (S_0)، حالت میانی (MS) و حالت نهایی (ES) نشان داده شده است. در حالت اولیه سامانه در شرایط کار عادی خود قرار دارد. حالت میانی زمانی اتفاق می‌افتد که سامانه در اثر یک اتفاق شروع‌کننده[2] (IE) از حالت کار عادی خارج شده و حادثه‌ای رخ می‌دهد. مثلاً یکی از اجزای سامانه از دست رود. حالت نهایی نیز زمانی اتفاق می‌افتد که حالات میانی تأثیراتی بر عملکرد سامانه بگذارد و پس از آن حالت سامانه به حالت نهایی پایدار در آید. با توجه به شکل (۴)، ارزیابی ریسک تحلیل کل مسیر طی شده از نقطه حالت اولیه به نقطه حالت نهایی است.



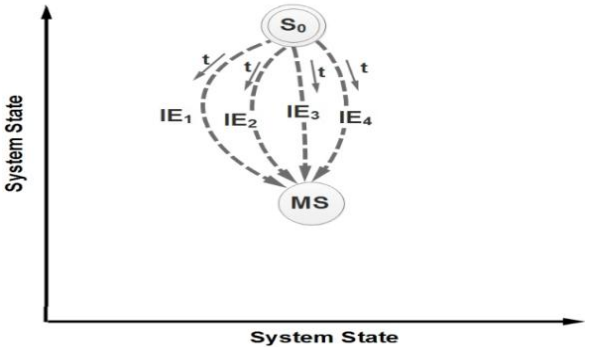
شکل ۴. ارزیابی ریسک [۳]

[1] Uncertainty
[2] Initiating Event

ارزیابی آسیب‌پذیری تحلیل مسیر طی شده از نقطه حالت میانی تا نقطه حالت پایانی است (شکل (۵)). یعنی بررسی و تحلیل عواقب و نتایجی که با فرض رخ دادن یک حادثه نهایتاً حاصل می‌شود. ارزیابی تهدید تحلیل مسیر طی‌شده از نقطه حالت اولیه تا نقطه حالت میانی است (شکل (۶)). یعنی بررسی و تحلیل احتمالات و سناریوهایی که ممکن است از حالت اولیه به نقطه رخداد حادثه رسید.



شکل ۵. ارزیابی آسیب‌پذیری [۳]



شکل ۶. ارزیابی تهدید

به عنوان مثال برای یک سامانه قدرت فرض کنید که سامانه در حال کار کردن در شرایط عادی است. در اثر وقوع حمله و یا حملاتی به پست‌های الکتریکی این شبکه، عملکرد سامانه دچار اختلال شده و خسارتی به سامانه تحمیل می‌شود. در این صورت تحلیل و بررسی احتمال وقوع حمله به پست الکتریکی مشخص و موفقیت‌آمیز بودن حمله به آن با توجه به ویژگی‌های جغرافیایی، پدافندی و تجربی آن، ارزیابی تهدید برای پست الکتریکی است.

حال اگر فرض شود که پست الکتریکی در صورت وقوع حمله موفقیت‌آمیز از دست رفته، ارزیابی و تحلیل نتایج و خسارت حاصله بر سامانه، ارزیابی آسیب‌پذیری است. در نهایت تحلیل و ارزیابی کل مسئله در مورد احتمال وقوع و خسارت ناشی از وقوع حمله موفقیت‌آمیز، ارزیابی ریسک سامانه است.

۳. روش پیشنهادی ارزیابی ریسک

۳-۱. مدل احتمال حمله موفقیت‌آمیز به اجزای سامانه

هدف این مقاله ارزیابی ریسک سامانه قدرت در برابر تهدیدات امنیتی و تروریستی است. با توجه به تعریف ریسک، ابتدا مدلی برای تعیین احتمال حمله موفقیت‌آمیز تروریستی به اجزای سامانه قدرت ارائه می‌شود. در ادامه عواقب و نتایج حاصل از حمله تروریستی بررسی می‌شود. ریسک سامانه قدرت به صورت ترکیب احتمال حمله موفقیت‌آمیز و خسارت حمله تعیین می‌شود.

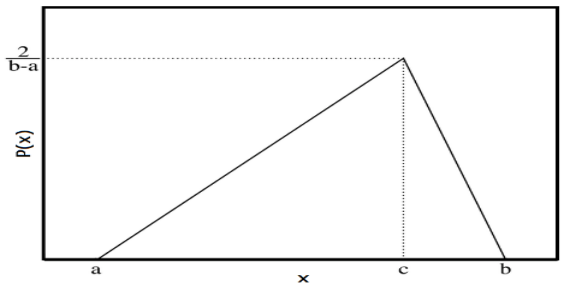
غفارپور و همکاران [۱۴]، روشی برای ارزیابی ریسک سامانه قدرت ارائه کرده‌اند. در این روش احتمال وقوع حمله موفقیت‌آمیز به همراه خسارت ناشی از حمله، ریسک سامانه قدرت را تشکیل می‌دهند. در روش مذکور نویسندگان برای تعیین احتمال حمله به تجهیزات سامانه قدرت مجموعه‌ای از مشخصات حمله‌کنندهحمله‌کننده مانند انگیزه حمله، میزان فعالیت، منابع، ساختار سازمانی حمله‌کننده، روش حمله و غیره توجه کرده‌اند. تعیین احتمال حمله موفقیت‌آمیز بر اساس پارامترهای متعدد حمله‌کننده، منجر به عدم قطعیت بسیار زیاد خواهد شد. مدافع از اطلاعات، انگیزه‌ها، تاکتیک‌ها و روش‌های مهاجم، اطلاعات روشنی در دست ندارد و یا ممکن است فریب بخورد. بنابراین غالباً در این نوع مسائل، بهتر است مدافع بر روی داشته‌ها و دانسته‌های خود تمرکز کند.

بر خلاف روش ارائه‌شده توسط غفارپور و همکاران [۱۴]، در این مقاله، روش ارائه‌شده برای تعیین مدل احتمال حمله موفقیت‌آمیز تروریستی، بر وضعیت موجود پدافندی اجزای سامانه تمرکز می‌کند. در این روش، سامانه قدرت به زیرسامانه‌ها و زیرسامانه‌ها خود به اجزائی تقسیم می‌شوند برای هر جز از سامانه سه تابع جلوگیری، شناسایی و واکنش تعریف می‌شود [۱۱].

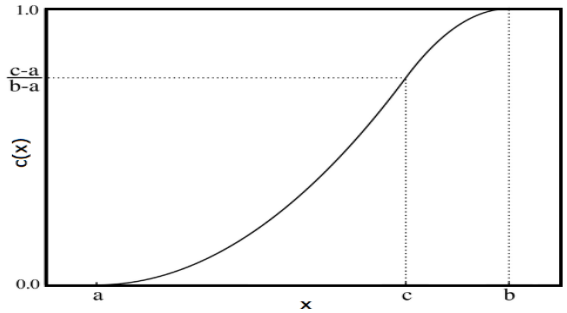
جلوگیری[1] به معنای اقداماتی است که طرف خراب‌کار را از نفوذ و دسترسی به اجزای سامانه بازمی‌دارد مانند پست نگهبانی، کشیدن حصار، وضعیت جغرافیایی منطقه و غیره. شناسایی به معنی فهمیدن و آگاه کردن دیگران از وقوع اعمال خراب‌کارانه است. دوربین‌های مداربسته و آژیر خطر نمونه‌هایی از اقدامات شناسایی است. واکنش به معنی اقداماتی است که از زمان به صدا درآمدن آژیر تا حضور سریع نیروهای امنیتی برای واکنش و ممانعت از انجام خراب‌کاری انجام می‌پذیرد. پارامترهایی مانند نزدیکی تأسیسات به ایستگاه‌های پلیس، آمادگی نیروهای پلیس منطقه، وضعیت جغرافیایی منطقه و غیره در تابع واکنش

[1] deterrence

تأثیرگذارند. هر یک از این توابع با توجه به وضعیت موجود و اقدامات پدافندی انجام‌شده، توسط متخصصان و کارشناسان امنیتی مشخص می‌شوند. برای تعیین توابع جلوگیری، شناسایی و واکنش متخصصان از توابع توزیع احتمال استفاده می‌کنند. به طور مثال برای تابع شناسایی، متخصصان امنیتی با توجه به تعداد دوربین‌های مداربسته، مکان آن‌ها، آژیرهای امنیتی و همچنین پارامترهای دیگر، یک توزیع احتمال به کار می‌برند. دلیل استفاده از توزیع احتمال لحاظ کردن عدم قطعیت در مقداردهی به این توابع است. یک توزیع احتمال مناسب برای توابعی که توسط متخصصان برآورد می‌شود، توزیع احتمال مثلثی است [۱۵]. تابع چگالی احتمال این توزیع احتمالی و تابع توزیع تجمعی آن به ترتیب در شکل‌های (۷ و ۸) نشان داده شده است. پارامتر a کمترین، پارامتر b بیش‌ترین و c محتمل‌ترین حالت است.

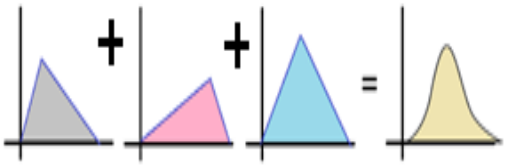


شکل ۷. تابع چگالی احتمال تابع توزیع مثلثی



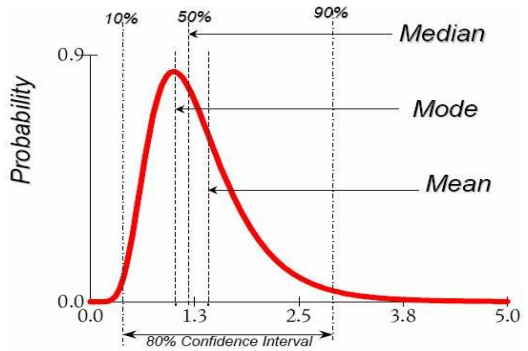
شکل ۸. تابع توزیع تجمعی تابع توزیع مثلثی

پارامترهای این توابع توزیع احتمال به وسیله متخصصان امنیتی و توسط نظریه بایز[1] مشخص می‌شود [۱۵]. اگر مجموع سه تابع جلوگیری، شناسایی و واکنش را به عنوان تابع ممانعت[2] تعریف می‌شود که به معنای ممانعت از انجام حمله موفقیت‌آمیز باشد، بعد از مشخص شدن توابع جلوگیری، شناسایی و واکنش، می‌توان احتمال وقوع حمله موفقیت‌آمیز به آن جزء از زیرسامانه را محاسبه کرد. برای این منظور ابتدا باید وزن توابع جلوگیری، شناسایی و واکنش در تابع ممانعت توسط متخصصان برآورد شود. سپس با توجه به وزن هر کدام از توابع توسط روش مونت‌کارلو این توابع توزیع احتمال را تجمیع[3] کرد و تابع توزیع احتمال ممانعت آن جزء از زیرسامانه را به دست آورد [۱۵]. شکل (۹) نمونه‌ای از تجمیع توابع توزیع احتمال را نشان می‌دهد.



شکل ۹. تجمیع توابع توزیع مثلثی

ممکن است در روش ارائه‌شده همچنان بحث عدم قطعیت نگران کننده باشد. بدین منظور می‌توان برای اطمینان بیشتر، این توابع را توسط چند گروه از متخصصان تعیین کرد و توابع را تجمیع کرد تا عدم قطعیت به کلی در مسئله لحاظ شود [۱۱]. نکته‌ای که باید مورد توجه واقع شود این است که احتمال ممانعت از وقوع حمله یک عدد مشخص نیست و دارای پراکندگی است. طبیعتاً در مسائلی که با انواع عدم قطعیت‌ها مواجه است، احتمالات به صورت توابع توزیع احتمال بیان می‌شوند (شکل (۱۰)). در صورتی که پراکندگی تابع توزیع احتمال کم باشد، با تقریب می‌توان احتمال ممانعت از وقوع حمله را یک عدد مشخص که همان پر تکرارترین حالت (مود) است، در نظر گرفت [۱۱].



شکل ۱۰. مود، میانه و میانگین یک تابع توزیع احتمال

در نهایت با تعیین احتمال ممانعت از وقوع حمله A، می‌توان احتمال وقوع حمله موفقیت‌آمیز را به صورت زیر محاسبه کرد:

$$p = 1 - A \qquad (۱)$$

برای زیرسامانه‌های یک سامانه نیز می‌توان روند قبل را تکرار کرد. بدین منظور ابتدا باید توابع ممانعت A(x) تمامی اجزا زیرسامانه تعیین شود. سپس وزن هر کدام از این اجزاء در عملکرد زیرسامانه توسط مطالعات قابلیت اطمینان سامانه‌ها [۱۶]

[1] Bayes Theorem
[2] Avoidance
[3] Aggregation

تعیین شود. سپس با تجمیع این توابع توسط روش مونت‌کارلو تابع توزیع ممانعت کل زیرسامانه تعیین می‌شود.

۳-۲. خسارت سامانه در اثر وقوع حمله موفقیت‌آمیز

همان طور که در بخش قبل بیان شد، ارزیابی آسیب‌پذیری سامانه به معنای تحلیل و تعیین عواقب و خسارت ناشی از وقوع یک اتفاق (در اینجا حمله تروریستی به سامانه) است. از آنجایی که برای حفظ پایداری سامانه و پاسخ هم‌زمان به حمله تروریستی به سامانه قدرت، یکی از مؤثرترین و مهم‌ترین راهکارها قطع بار است و همچنین، هدف حملات نظامی و تروریستی نیز قطع هر چه بیشتر بار است، می‌توان میزان بار تأمین نشده در صورت وقوع حمله موفقیت‌آمیز را به عنوان خسارت سامانه در اثر وقوع حمله در نظر گرفت. اکثر مراجعی که در زمینه دفاع از سامانه قدرت در برابر تهدیدات تحقیق کرده‌اند از همین شاخص برای تعیین خسارت سامانه قدرت و ارزیابی آسیب‌پذیری آن استفاده کرده‌اند [۱۹-۱۷]. در این مراجع میزان بار تأمین نشده با استفاده از پخش بار DC و با فرض از دست رفتن اجزایی از سامانه قدرت در صورت وقوع حمله موفقیت‌آمیز محاسبه شده است. در این تحقیق همانند مراجع ذکرشده، توان تأمین نشده سامانه به عنوان میزان خسارت ناشی از حمله در نظر گرفته شده است.

۳-۳. ریسک سامانه قدرت در برابر حملات

در بخش قبل بیان شد که ریسک یک سامانه از سه عنصر سناریوها، احتمال وقوع آن‌ها و میزان خسارت ناشی از وقوع آن‌ها شکل می‌گیرد. برای یک سامانه قدرت چندین سناریوی حمله که شامل حمله به نقاط مختلف سامانه و اجزای مختلف آن است و همچنین حملات هم‌زمان به سامانه وجود دارد. یکی از سؤالاتی که همواره در زمینه ریسک سامانه‌ها مطرح بوده این است که آیا می‌توان تمامی سناریوها را در نظر گرفت. طبیعتاً برای یک سامانه قدرت که از المان‌های متعددی تشکیل شده است این امر غیرممکن است اما می‌توان این سناریوها را با روش‌های کاهش سناریو[1] به اندازه قابل قبولی کاهش داد. فرض کنید برای یک سامانه قدرت سناریوها مشخص شود و احتمال وقوع موفقیت‌آمیز هر یک به علاوه میزان خسارت ناشی از وقوع آن‌ها تعیین شود. در این صورت جدول سناریوها همانند جدول (۱) تهیه می‌شود. در یک سامانه قدرت سناریوها شامل حمله به اجزای مختلف سامانه (خطوط انتقال، پست‌ها و نیروگاه‌ها) و یا حمله هم‌زمان به چندین جزء سامانه است.

برای یک تک سناریو ریسک به صورت حاصل‌ضرب احتمال وقوع موفقیت‌آمیز آن سناریو در میزان خسارت ناشی از وقوع آن تعریف می‌شود. ریسک سامانه برای کل سناریوها (حملات) به صورت مجموع حاصل‌ضرب احتمالات در خسارت‌ها تعریف می‌شود که همان میانگین منحنی ریسک است.

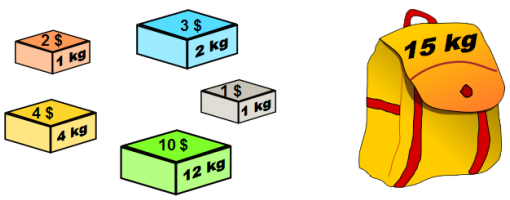
$$R = \sum_{s=1}^{SN} p_s \times x_s \qquad (۲)$$

در این رابطه، R ریسک کل سامانه، P_s احتمال وقوع موفقیت‌آمیز سناریوی s و x_s خسارت ناشی از سناریوی s است.

هرگونه تلاش در جهت بهبود مسائل پدافند غیرعامل سامانه قدرت و همچنین مدیریت بحران سامانه قدرت در برابر تهدیدات سبب کاهش ریسک سامانه قدرت در برابر تهدیدات می‌شود. این کاهش ریسک سامانه باید تا رسیدن به نقطه قابل‌قبول (ایده‌آل) ادامه داشته باشد. در ادامه روشی بهینه برای دفاع از سامانه قدرت در جهت کاهش ریسک سامانه ارائه می‌شود.

۳-۴. کاهش ریسک سامانه قدرت

راهبردهای متنوع و راهکارهای گوناگونی برای پدافند غیرعامل سامانه قدرت و مدیریت بحران سامانه قدرت در زمان وقوع حمله وجود دارد که بسته به نظر سیاست‌گذاران این حوزه مورد استفاده قرار می‌گیرد. در این تحقیق رویکردی برای کاهش ریسک سامانه قدرت در برابر تهدیدات امنیتی و تروریستی ارائه می‌شود. در این رویکرد فرض می‌شود که بودجه پدافند و دفاع از سامانه قدرت محدود باشد. این بودجه صرف مستحکم‌سازی و پدافند غیرعامل تأسیسات سامانه قدرت می‌شود. با فرض محدودیت این بودجه ریسک سامانه باید تا حد امکان کاهش یابد. مشخص است که این رویکرد یک مسئله بهینه‌سازی است. این مسئله بهینه‌سازی به مسئله کوله‌پشتی[2] شباهت دارد (شکل (۱۱)). در مسئله بهینه‌سازی کوله‌پشتی هدف این است که برای رفتن به یک سفر تعدادی از وسایل که هر کدام وزن مشخص و ارزش مشخصی دارد را طوری در یک کوله‌پشتی که قابلیت حمل وزن محدودی دارد جاسازی کنید، که بیش‌ترین ارزش در کوله‌پشتی قرار گیرد.



شکل ۱۱. مسئله بهینه‌سازی کوله‌پشتی

[1] Scenario Reduction

[2] Knapsack Problem

در اینجا مسئله کوله‌پشتی این‌گونه تغییر می‌یابد که قابلیت حمل وزن محدود کوله‌پشتی همان بودجه دفاعی محدود است، وسایل کوله‌پشتی همان المان‌ها و اجزای سامانه قدرت هستند که باید از آن‌ها دفاع شود، ارزش وسایل کوله‌پشتی همان ریسک حمله به هر کدام از اجزای سامانه است و وزن وسایل کوله‌پشتی برابر با بودجه مورد نیاز برای تقویت پدافند هر یک از المان‌های سامانه است. مسئله بهینه‌سازی کوله‌پشتی به صورت زیر قابل‌بیان است:

$$Maximize \sum_{j=1}^{m} v_j \times x_j$$
$$subject\ to: \quad \sum_{j=1}^{m} w_j \times x_j \le W \qquad (۳)$$

در این رابطه، j وسایل موجود برای گذاشتن در کوله‌پشتی، v_j ارزش هر کدام از وسایل، w_j وزن هر کدام از وسایل، W محدودیت حمل وزن توسط کوله‌پشتی است.

x_j یک مقدار باینری است که اگر وسیله برای کوله‌پشتی انتخاب شود مقدار آن ۱ و اگر انتخاب نشود مقدار آن صفر خواهد بود.

این مسئله بهینه‌سازی باینری-خطی توسط روش‌های بهینه‌سازی حل می‌شود. پس از حل این مسئله بهینه‌سازی، المان‌ها و اجزای سامانه قدرت که باید تقویت شوند مشخص می‌شود و ریسک کاهش‌یافته سامانه پس از حل این مسئله مشخص می‌شود.

نکته‌ای که در حل مسئله بهینه‌سازی کاهش ریسک باقی می‌ماند، مشخص‌کردن بودجه مورد نیاز برای تقویت پدافند هر المان سامانه (w_j) است.

اطلاعات بودجه مورد نیاز برای تقویت پدافند هر جزء از اجزای سامانه توسط کارشناسان پدافند غیرعامل تعیین می‌شود. به عنوان مثال برای یک پست انتقال با مساحت مشخص، جغرافیای مشخص، ظرفیت مشخص و پارامترهای دیگر مشخص می‌شود که چه مقدار بودجه برای پدافند آن در برابر حمله تروریستی نیاز است تا احتمال وقوع حمله موفقیت‌آمیز به صفر نزدیک شود و ریسک سامانه برای این سناریو مشخص به اندازه $p_s \times x_s$ کاهش یابد (در اینجا p_s احتمال وقوع حمله موفقیت‌آمیز قبل از اعمال تمهیدات پدافند غیرعامل است).

هولمگرن و همکاران [۱۹] رابطه‌ای کلی به صورت تابعی نزولی برای کاهش احتمال حمله موفقیت‌آمیز به اجزای سامانه بر حسب بودجه دفاعی به‌کاررفته برای تقویت آن اجزاء ارائه کرده‌اند.

$$p_i = 1 - \frac{c_i}{k_i^p + c_i} \qquad (۴)$$

در این رابطه، i اجزای سامانه قدرت، c_i بودجه به‌کاررفته برای تقویت پدافند هر یک از اجزاء است ($). K^p_i درجه آزادی تعریف‌شده برای تابع است. این درجه آزادی برای پست‌ها ۲، برای ژنراتورها ۳ و برای خطوط ۴ تعریف شده است. P_i احتمال حمله موفقیت‌آمیز به جزء i است.

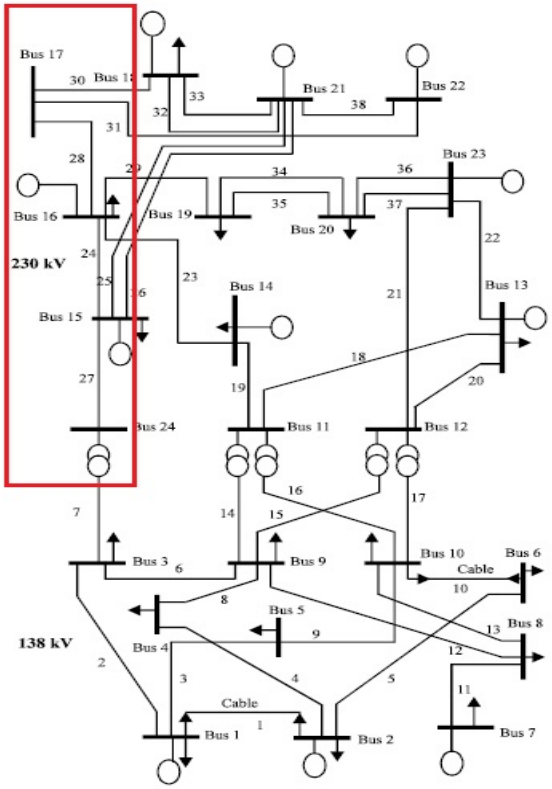
از رابطه (۴) مشخص است که اگر بودجه به‌کاررفته برای پدافند اجزاء به مقادیر بسیار زیاد میل کند، احتمال حمله موفقیت‌آمیز به آن‌ها به سمت صفر میل می‌کند. بنابراین با استفاده از اطلاعات تجربی که توسط کارشناسان پدافند غیرعامل برای تعیین بودجه مورد نیاز برای پدافند اجزای سامانه قدرت مشخص می‌شود و یا با استفاده از روابطی مانند رابطه ارائه‌شده توسط هولمگرن، می‌توان مسئله بهینه‌سازی کاهش ریسک سامانه قدرت را حل کرد.

۴. اعمال شبیه‌سازی و نتایج

کاربرد روش ارائه‌شده بر روی شبکه آزمایش ۲۴ باسه IEEE انجام‌شده است [۲۰]. این شبکه در شکل (۱۲) نشان داده شده است. بار شبکه برابر ۳۴۲۰ مگاوات (بار پیک) در نظر گرفته شده است. همچنین فرض می‌شود خط انتقال ۲۸ برای تعمیرات برنامه‌ای خارج از مدار است و تروریست‌ها با داشتن اطلاعات از این برنامه اقدام به حمله می‌کنند. فرض می‌شود در اثر حمله به خطوط دومداره (موازی) مانند خطوط ۲۵ و ۲۶، هر دو از مدار خارج می‌شوند.

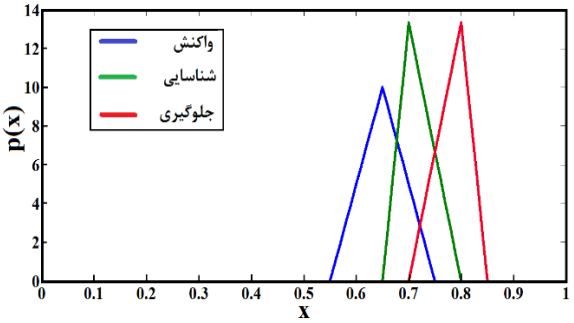
در ابتدا ریسک برای یک سناریوی مشخص محاسبه می‌شود. این سناریو، حمله تروریستی به پست الکتریکی متصل به باس ۲۴ است. این سامانه شامل ۲ زیرسامانه شبکه ۱۳۸ و ۲۳۰ کیلوولت است. اجزای این زیرسامانه‌ها شامل خطوط انتقال، پست‌های الکتریکی و واحدهای تولیدی نشان داده‌شده در شکل (۱۲) هستند. ابتدا احتمال وقوع حمله موفقیت‌آمیز به جزء مشخص که در اینجا پست الکتریکی متصل به بأس ۲۴ است، محاسبه می‌شود. فرض می‌شود پست الکتریکی ۲۴ دارای نگهبان، روشنایی، سیم‌خاردار و دوربین‌های مداربسته است. همچنین فرض می‌شود که این پست در منطقه شهری واقع است و در فاصله قابل‌توجهی از ایستگاه‌های پلیس قرار دارد.

متخصصان امنیتی، برای توابع جلوگیری، شناسایی و واکنش از توابع توزیع احتمال مثلثی استفاده می‌کنند. محور x این توابع از صفر تا ۱۰۰ با توجه به اقدامات پدافندی صورت گرفته برای جلوگیری، شناسایی و واکنش متغیر است. بیش‌ترین اقدام پدافندی ممکن با عدد ۱۰۰ و کمترین اقدام پدافندی با عدد صفر برآورد می‌شود. محور y نیز احتمال را نشان می‌دهد.



شکل ۱۲. شبکه آزمایش ۲۴ باسه IEEE

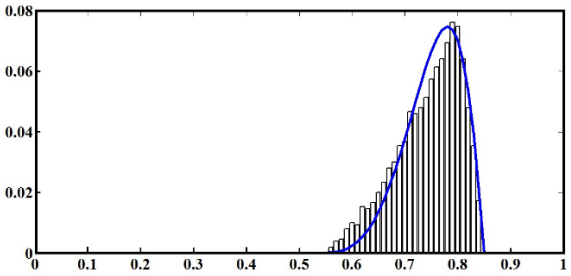
کارشناسان با بررسی دقیق کیفیت و مکان قرارگیری پست نگهبانی، روشنایی و سیم‌خاردار و همچنین با استفاده از نظریه بایز، برای تابع توزیع احتمال مثلثی جلوگیری میزان محتمل‌ترین حالت را ۸۰، کمترین مقدار را ۷۰ و بیش‌ترین مقدار را ۸۵ تعیین می‌کنند. برای تابع توزیع شناسایی با توجه به تعداد و مکان قرارگیری دوربین‌های مداربسته، محتمل‌ترین حالت ۷۰، کمترین مقدار ۶۵ و بیش‌ترین مقدار ۸۰ تعیین می‌شود. برای تابع توزیع واکنش با توجه به مکان نزدیک‌ترین پایگاه پلیس و مسیر و عوامل دیگر، محتمل‌ترین حالت ۶۵، کمترین مقدار ۵۵ و بیش‌ترین مقدار ۷۵ تعیین می‌شود. این توابع توزیع با نرمالیزه کردن محور X بین صفر و یک در شکل (۱۳) نشان داده شده‌اند.



شکل ۱۳. توابع توزیع مثلثی شناسایی، جلوگیری و واکنش پست ۲۴

تجمیع این توابع توزیع برای به دست آوردن تابع توزیع احتمال ممانعت، با استفاده از روش مونت‌کارلو و با توجه به وزن هر یک از این توابع در تابع ممانعت حاصل می‌شود. نتیجه تجمیع توابع توزیع احتمال فوق معمولاً به صورت تابع توزیع احتمال بتا ارائه می‌شود. متخصصان به عنوان نمونه برای ممانعت از حمله به پست الکتریکی وزن توابع جلوگیری، شناسایی و واکنش را بر حسب تجربه به ترتیب ۶۰، ۲۰ و ۲۰ درصد برآورد می‌کنند.

در اثر تجمیع توابع توزیع فوق با استفاده از روش مونت‌کارلو در ۷۵۰۰۰ تکرار، تابع توزیع احتمال ممانعت به صورت تابع توزیع بتا با دو پارامتر α=۵/۲ و β=۲/۱ استخراج شد. این تابع توزیع در شکل (۱۴) ترسیم شده است.



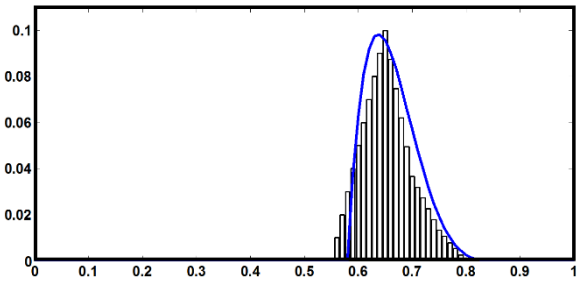
شکل ۱۴. تابع توزیع احتمال ممانعت پست ۲۴ در داخل شهر

این تابع توزیع احتمال دارای مود ۰/۷۸ و واریانس ۰/۰۲۴ است. همان طور که قبلاً توضیح داده شد می‌توان با تقریب، احتمال ممانعت از حمله به پست ۲۴ را برابر مود تابع توزیع در نظر گرفت. با استفاده از رابطه (۱)، احتمال حمله موفقیت‌آمیز به پست الکتریکی مذکور به صورت زیر تعیین می‌شود:

$$p_{24} = 1 - 0.78 = 0.22$$

حالتی را در نظر بگیرید که پست الکتریکی ۲۴ دارای نگهبان، حصار، سیم‌خاردار و روشنایی مناسب است ولی در حومه شهر واقع است. در این حالت کارشناسان امنیتی، تابع جلوگیری را به این صورت برآورد می‌کنند که دارای کمترین مقدار ۵۵، بیش‌ترین مقدار ۷۰ و محتمل‌ترین حالت ۶۵ است. در نتیجه، تابع توزیع احتمال ممانعت پست الکتریکی ۲۴ به صورت زیر تغییر می‌کند. در اینجا احتمال حمله موفقیت‌آمیز تروریستی به پست، برابر با ۰/۳۷ می‌شود که نسبت به حالت قبل ۱۵ درصد افزایش یافته است.

در گام بعد میزان خسارت ناشی از حمله موفقیت‌آمیز به پست الکتریکی متصل به باس ۲۴ محاسبه می‌شود [۲۱]. با استفاده از پخش بار، میزان توان تأمین نشده در صورت از دست رفتن پست مذکور برابر با ۸۲ مگاوات خواهد شد.



شکل ۱۵. تابع توزیع احتمال ممانعت پست ۲۴ در حالتی که پست در حومه شهر قرار گرفته باشد.

در نتیجه ریسک برای این تک سناریو (حمله موفقیت‌آمیز به پست الکتریکی متصل به باس ۲۴) برابر خواهد بود با:

$$R_{24} = 82 \times 0.22 = 18.04$$

برای به دست آوردن ریسک سامانه، همین روند برای تک‌تک سناریوها که شامل حملات جداگانه به هر یک از المان‌های شبکه و یا حمله هم‌زمان به دو یا چند المان است باید تکرار شود.

با استفاده از تجربیات گذشته و همچنین اطلاعات به‌روز از مهاجم می‌توان توانایی مهاجم برای حمله به سامانه را برآورد کرد. فرض کنید که با توجه به حضور گروه‌های مهاجم در شمال غربی منطقه، وقوع حمله به ناحیه‌ای که در شکل (۱۲) نشان داده شده است محدود می‌شود. همچنین، فرض کنید می‌توان برآورد کرد که مهاجمین توانایی حمله هم‌زمان به سه هدف را ندارند و در مورد حمله هم‌زمان به دو هدف، تنها قادر به حمله به دو خط مجاور هستند. بنابراین می‌توان سناریوها را به جدول (۲) کاهش داد. روند قبل برای تمامی سناریوهای جدول بالا انجام می‌گیرد و جدول (۳) حاصل می‌شود.

جدول ۲. جدول سناریوهای کاهش‌یافته

عنوان سناریو	شرح سناریو
سناریوی ۱	حمله به پست الکتریکی ۲۴
سناریوی ۲	حمله به واحد تولیدی بأس ۱۵
سناریوی ۳	حمله به واحد تولیدی بأس ۱۶
سناریوی ۴	حمله به خط انتقال ۲۳
سناریوی ۵	حمله به خط انتقال ۲۴
سناریوی ۶	حمله به خطوط موازی ۲۵ و ۲۶
سناریوی ۷	حمله به خط انتقال ۲۷
سناریوی ۸	حمله به خط انتقال ۲۹
سناریوی ۹	حمله به خط انتقال ۳۰
سناریوی ۱۰	حمله به خط انتقال ۳۱
سناریوی ۱۱	حمله همزمان به خطوط انتقال ۳۰ و ۳۱
سناریوی ۱۲	حمله همزمان به خطوط انتقال ۲۴ و ۲۵ و ۲۶

جدول ۳. جدول سناریوها به همراه احتمال وقوع و خسارت منتج

سناریو	احتمال موفقیت	خسارت (MW)	ریسک سناریو	رتبه اهمیت
سناریوی ۱	۰/۲۲	۸۲	۱۸/۰۴	۱۰
سناریوی ۲	۰/۰۵	۲۵۶	۱۲/۸	۱۱
سناریوی ۳	۰/۰۳	۲۰۰	۶	۱۲
سناریوی ۴	۰/۷۰	۶۹	۴۸/۳	۵
سناریوی ۵	۰/۷۵	۱۷۵	۱۳۱/۲۵	۳
سناریوی ۶	۰/۶۰	۷۱۸	۴۳۰/۸	۱
سناریوی ۷	۰/۷۰	۸۲	۵۷/۴	۴
سناریوی ۸	۰/۵۰	۵۱	۲۵/۵	۹
سناریوی ۹	۰/۸۰	۵۴	۴۳/۲	۶
سناریوی ۱۰	۰/۷۵	۵۴	۴۰/۵	۷
سناریوی ۱۱	۰/۶	۶۰	۳۶	۸
سناریوی ۱۲	۰/۴۵	۷۲۰	۳۲۴	۲
ریسک کل سامانه			۱۱۷۳/۷۹	

حال با مشخص شدن ریسک سناریوها، بودجه محدود پدافند به گونه‌ای بهینه تخصیص می‌یابد که ریسک کل سامانه کمتر شود. این امر توسط حل مسئله بهینه‌سازی کوله‌پشتی انجام می‌پذیرد. برای حل مسئله کوله‌پشتی، بودجه پدافند مورد نیاز برای کاهش احتمال حمله موفقیت‌آمیز به هر کدام از تجهیزات سامانه تا حد صفر باید محاسبه شود. در اینجا حد صفر برای احتمال حمله موفقیت‌آمیز به تجهیزات سامانه عدد ۰/۰۱ در نظر گرفته شده است. محاسبه بودجه پدافندی برای کاهش احتمال حمله موفقیت‌آمیز به هر کدام از تجهیزات سامانه تا حد صفر، با توجه به میزان پدافند کنونی و همچنین ویژگی‌های منحصربه‌فرد جغرافیایی، محلی، فنی و دیگر عوامل پیچیده است و نیازمند اطلاعات و تحلیل‌های گسترده است که در این مقاله نمی‌گنجد. در این مقاله از رابطه ساده و اولیه ارائه‌شده توسط هولمگرن (رابطه (۴))، برای محاسبه بودجه پدافندی جهت کاهش احتمال حمله موفقیت‌آمیز از تا حد صفر استفاده شده است. با استفاده از رابطه (۴) بودجه پدافندی برای کاهش احتمال حمله موفقیت‌آمیز به تجهیزات تا حد صفر، به صورت جدول‌های (۴ و ۵) به دست آمده است.

جدول ۴. بودجه واحد پدافند مورد نیاز برای تجهیزات سامانه جهت کاهش احتمال حمله موفقیت‌آمیز به آن‌ها تا حد صفر (۰/۰۱)

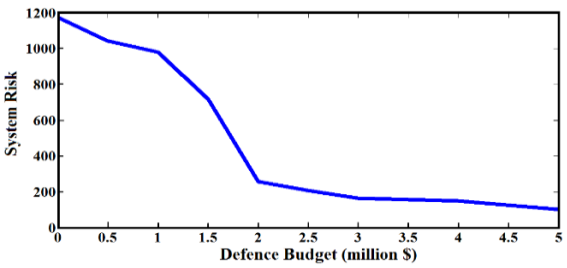
نوع تجهیزات (واحد)	بودجه واحد پدافند مورد نیاز
خط انتقال (۱ مایل)	۳۹۶۰۰۰ دلار
واحد تولید (۱۰۰ مگاوات)	۲۹۷۰۰۰ دلار
پست الکتریکی (۱۰۰ مگاوات)	۱۹۸۰۰۰ دلار

جدول ۵. بودجه پدافند مورد نیاز برای تجهیزات سامانه جهت کاهش احتمال حمله موفقیت‌آمیز به آن‌ها تا حد صفر (۰/۰۱)

تجهیزات	ظرفیت یا طول	بودجه پدافند مورد نیاز
پست الکتریکی ۲۴	۴۰۰ مگاوات	۷۳۶۶۳۷ دلار
واحد تولید ۱۵	۲۱۵ مگاوات	۵۱۶۰۰۰ دلار
واحد تولید ۱۶	۱۵۵ مگاوات	۳۱۰۰۰۰ دلار
خط انتقال ۲۳	۲۷ مایل	۱۰۶۴۵۷۲ دلار
خط انتقال ۲۴	۱۲ مایل	۴۷۳۶۰۰ دلار
خطوط ۲۵ و ۲۶	۳۴ مایل	۱۳۳۷۳۳۴ دلار
خط انتقال ۲۷	۳۶ مایل	۱۴۱۹۴۲۹ دلار
خط انتقال ۲۹	۱۶ مایل	۶۲۷۲۰۰ دلار
خط انتقال ۳۰	۱۰ مایل	۳۹۵۰۰۰ دلار
خط انتقال ۳۱	۷۳ مایل	۲۸۸۱۰۶۷ دلار

با حل مسئله بهینه‌سازی کوله‌پشتی توسط الگوریتم تکاملی تفاضلی[1]، بودجه پدافندی کل به صورت بهینه بین تجهیزات سامانه قدرت تخصیص می‌یابد و ریسک کل سامانه به صورت بهینه کاهش می‌یابد. به ازای مقادیر مختلف بودجه پدافندی کل، تخصیص بودجه پدافندی بین تجهیزات سامانه قدرت در جدول (۶) نشان داده شده است. کاهش ریسک سامانه قدرت به ازای افزایش بودجه پدافندی کل در شکل (۱۶) نشان داده شده است.

این نمودار نشان می‌دهد که برای رسیدن به سطوح مختلف ریسک قابل‌قبول سامانه، چه مقدار بودجه پدافندی کل باید برای مستحکم‌سازی تجهیزات واقع در منطقه شمال غرب سامانه اختصاص یابد. به طور مثال اگر سیاست‌گذاران دفاعی ریسک قابل‌قبول سامانه قدرت را در برابر تهدیدات تروریستی، ۲۰۰ واحد تعیین کنند، باید بودجه‌ای حدود ۲/۵ میلیون دلار برای مستحکم‌سازی سامانه اختصاص دهند. نمودار به ازای بودجه بین ۱ تا ۲ میلیون دلار، با کاهش سریع ریسک همراه است. به ازای مقادیر بیشتر از ۲ میلیون دلار، روند کاهش ریسک کند می‌شود. اگرچه حالت ایده‌آل حالتی است که ریسک سامانه برابر با صفر باشد ولی در عمل این امر محقق نمی‌شود، زیرا نیازمند صرف هزینه‌های بسیار بالا است.



شکل ۱۶. منحنی کاهش ریسک سامانه به ازای افزایش بودجه پدافندی

جدول ۶. تخصیص بهینه بودجه پدافندی کل برای مستحکم‌سازی تجهیزات سامانه (و: واحد تولید، پ: پست الکتریکی، خ: خط انتقال)

بودجه پدافندی کل	تجهیزات انتخابی برای مستحکم‌سازی	ریسک جدید سامانه
۰/۵ میلیون دلار	خ ۲۴	۱۰۴۲/۵۴
۱ میلیون دلار	خ ۲۴، خ ۳۰	۹۹۹/۳۵
۱/۵میلیون دلار	خ ۲۵و۲۶	۷۴۳
۲ میلیون دلار	خ۲۴، خ ۲۵و۲۶	۲۸۷
۲/۵ میلیون دلار	خ۲۴، خ ۲۵و۲۶، خ ۳۰	۲۴۳/۸
۳ میلیون دلار	خ۲۴، خ ۲۹، خ ۳۰، خ۲۵و۲۶	۲۱۸/۳
۴ میلیون دلار	خ۲۳، خ۲۴، خ۲۹، خ ۳۰، خ۲۵و۲۶	۱۷۰
۵ میلیون دلار	و۱۶، خ۲۴، خ ۲۷، خ ۳۰، خ۲۵و۲۶ ، خ ۲۳	۱۳۲/۸

۵. نتیجه‌گیری

در این مقاله ابتدا به تعریف ریسک سامانه‌ها در برابر تهدیدات پرداخته شد و تفاوت ریسک با آسیب‌پذیری به طور کامل شرح داده شد. با توجه به تعریف ریسک، ابتدا مدل احتمالی حمله موفقیت‌آمیز تروریستی به اجزای سامانه مورد بررسی قرار گرفت و با ترکیب آن با خسارات ناشی از حمله موفقیت‌آمیز، ریسک سامانه قدرت به صورت یک رابطه ریاضی ارائه شد. سپس با قرینه‌سازی مسئله بهینه‌سازی کوله‌پشتی، مدلی برای کاهش ریسک سامانه قدرت بر مبنای اختصاص بودجه پدافندی برای مستحکم‌سازی تجهیزاتی که ریسک بالاتری دارند، ارائه شد. در تخصیص بهینه بودجه توسط مسئله کوله‌پشتی، هم‌زمان هم به رتبه و اهمیت هر کدام از تجهیزات در ریسک کل سامانه و هم به بودجه مورد نیاز برای مستحکم‌سازی آن‌ها توجه می‌شود. ممکن است یکی از تجهیزات سامانه دارای رتبه بالاتری از اهمیت در ریسک کل سامانه قرار داشته باشد ولی با توجه به هزینه بسیار بالا برای مستحکم‌سازی، بودجه‌ای برای پدافند آن اختصاص نیابد. روش‌های ارائه‌شده بر روی شبکه آزمایش ۲۴ باسه IEEE مورد آزمون قرار گرفت و کارایی نتایج نشان داده شد. بحث تعیین دقیق میزان بودجه مورد نیاز برای مستحکم‌سازی تجهیزات سامانه قدرت می‌تواند در مطالعات بعدی مورد بررسی قرار گیرد.

[1] Differential Evolution

۶. مراجع

[1] Yusta, J. M.; Correa, G. J.; Lacal-Arantegui, R. "Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art"; Energy Policy 2001, 39, 6100–6119.

[2] Zimmerman, R. "Decision-Making and the Vulnerability of Interdependent Critical Infrastructure"; IEEE Int. Conf. Systems, Man and Cybernetics, 2004, 5, 4059-4063.

[3] Johansson, J. "Risk and Vulnerability Analysis of Inter Dependent Technical Infrastructures"; Ph.D. Dissertation, Lund University, 2010.

[4] Shahidehpour, M.; Fu, Y.; Wiedman, T. "Impact of Natural Gas Infrastructure on Electric Power Systems"; Proc. IEEE, 2005, 93, 1042 -1056.

[5] Oren, S. S. "Risk Management *vs.* Risk Avoidance in Power Systems"; IEEE Power Eng. Society General Meeting, 2006, 1-3.

[6] Leffler, L. "The NERC Program for the Electricity Sector Critical Infrastructure Protection"; IEEE Power Eng. Society Winter Meeting, 2001, 95-97.

[7] Skolicki, Z.; Wadda, M. M.; Houck, M. H.; Arciszewski, T. "Reduction of Physical Threats to Water Distribution Systems"; J. Water Resour. Plann. Manage. 2006, 132, 211-217.

[8] Li, H.; Rosenwald, G. W.; Jung, L.; Liu, C. C. "Strategic Power Infrastructure Defense"; Proc. IEEE, 2005, 93, 918-933.

[9] Firouzi, H. "Introduction of Strategic Aspects of Electricity Network's Reliable Management from the Perspective of Crisis Management"; Passive Defense Quarterly 2013, 14, 11-18 (In Persian).

[10] Adelpour, M.; Ghasemi, H. "Essentials of Passive Defense in Electric Power Systems"; Iranian Conference on Electrical Engineering (ICEE), 2012, 370-375.

[11] Ezell, B. C. "Infrastructure Vulnerability Assessment Model (I-VAM)"; Risk Anal. 2007, 27, 571-583.

[12] Garrick, B. L.; Hall, L. E.; Kilger, M.; McDonald, L. C.; O'Toole, T.; Probst, P. S.; Parker, E. R.; Rosenthal, R. "Confronting the Risks of Terrorism: Making the Right Decisions"; Reliab. Eng. Syst. Safe. 2004, 86, 129-176.

[13] Kaplan, S.; Garrick, B. L. "On the Quantitative Definition of Risk"; Risk Anal. 1989, 1, 11-27.

[14] Ghaffarpour, R.; Pourmoosa, A. A. "Risk Assessment, Modeling, and Ranking for Power Network Facilities Regarding to Sabotage"; Advance Defence Sci. Tech. 2015, 2, 127-144 (In Persian).

[15] Chytka, T. M. "Development of an Aggregation Methodology for Risk Analysis in Aerospace Conceptual Vehicle Design"; Ph.D. Dissertation, Old Dominion University, 2003.

[16] Billinton, R.; Allan, R. N. "Reliability Evaluation of Engineering Systems: Concepts and Techniques"; Springer, 1992.

[17] Chen, G.; Dong, Z. Y.; Hil, D. L. "Exploring Reliable Strategies for Defending Power Systems Against Targeted Attacks"; IEEE Trans. Power Syst. 2011, 26, 1000-1009.

[18] Wood, K.; Baldick, R.; Salmeron, J. "Analysis of Electric Grid Security Under Terrorist Threat"; IEEE Trans. Power Syst. 2004, 19, 905-912.

[19] Holmgren, A. L.; Jenelius, E.; Westin, j. "Evaluating Strategies for Defending Electric Power Networks Against Antagonistic Attacks"; IEEE Trans. Power Syst. 2007, 22, 76- 84.

[20] "The IEEE Reliability Test System-1996"; IEEE Trans. Power Syst. 1999, 14, 1010–1020.

[21] Ranjbar, M. H. "Optimal Allocation of Reserve Power in Electricity Market"; M.S. Thesis, Shahid Beheshti University, 2012 (In Persian).