مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال نهم، شماره ۱، بهار ۱۳۹۷؛ ص ۲۸-۱۱

مروری بر تحلیل آسیب‌پذیری شبکه برق: رویکردها، مدل‌ها و روش‌های حل

سعید صیادی‌پور[۱]، رضا غفارپور[۲*]، علی‌محمد رنجبر[۳]
۱- کارشناس ارشد دانشگاه صنعتی اصفهان، ۲- مربی، دانشگاه امام حسین (ع)، ۳- استاد، دانشگاه صنعتی شریف
(دریافت: ۹۵/۰۸/۱۱، پذیرش: ۹۵/۱۱/۲۰)

چکیده

در سال‌های اخیر، شبکه‌های برق در سراسر دنیا یکی از اهداف اصلی حملات تروریستی بوده‌اند. این حملات در طراحی شبکه‌های برق در نظر گرفته نشده‌اند. به دنبال خاموشی‌های سراسری متعدد در سال‌های اخیر، پژوهشگران بسیاری به مطالعه آسیب‌پذیری شبکه‌های برق، در حوزه‌های بهره‌برداری و برنامه‌ریزی، در مقابل حملات عامدانه پرداخته‌اند. تاکنون، مطالعه‌ای کامل و دسته‌بندی مناسبی از این مطالعات انجام نشده است. در این مقاله، رویکردهای مختلف در بررسی آسیب‌پذیری شبکه‌های برق، ارائه و دسته‌بندی شده است. بر این اساس، اهداف مختلف گروه‌های متخاصم از حمله به شبکه‌های برق، مدل‌های ریاضی و روش‌های حل آن‌ها، چالش‌های پیشِ رو و راهکارهای برخورد با این چالش‌ها به تفصیل بیان شده است. دسته‌بندی‌های مناسبی که در این مقاله ارائه شده است، به برنامه‌ریزان شبکه کمک می‌کند تا در توسعه و بهره‌برداری شبکه، جنبه‌های مختلف تحلیل آسیب‌پذیری را در تصمیم‌گیری خود لحاظ کنند.

کلیدواژه‌ها: حملات عامدانه، تحلیل آسیب‌پذیری شبکه برق، امنیت شبکه برق، توسعه شبکه برق

A Review on Vulnerability Analysis of Electric Grid: Approaches, Models, and Solution Methods

S. Sayydipour, R. Ghaffarpour*, A. M. Ranjbar
Imam Hossein University
(Received: 01/11/2016; Accepted: 08/02/2017)

Abstract

In recent years, electric grids have been one of the main targets of terrorist attacks all over the world. These attacks are not considered in the design of electric grids. Subsequent to several blackouts in recent years, many researchers have studied the vulnerability of electric grids against intentional attacks, in both the operation and planning contexts. No review and classification of these studies is provided so far. In this paper, different approaches to vulnerability analysis of electric grids are presented and classified. Then, different objectives of antagonistic groups in attacking the electric grids, mathematical models and solution methodologies, challenges and solutions to deal with these challenges are represented in detail. Proper classifications that are presented in this paper help the network planners to incorporate several aspects of vulnerability analysis in their decisions about network planning and operation.

Keywords: Intentional Attacks, Electric Grid Vulnerability Analysis, Electric Grid Security, Electric Grid Expansion.

* Corresponding Author E-mail: rghaffarpour@ihu.ac.ir

۱. مقدمه

شبکه برق، یکی از زیرساخت‌های حیاتی هر کشور است و ادامه حیات سایر زیرساخت‌ها، وابسته به عملکرد صحیح این شبکه است [۱]. معیارهایی که به طور عمده در مطالعات امنیت شبکه برق مورد استفاده قرار می‌گیرد، معیارهای قابلیت اطمینان *N-1* و *N-2* است [۲ و ۳]. استفاده از چنین معیارهایی در بهره‌برداری شبکه‌های برق، تضمین می‌کند که با خروج تصادفی یک و یا دو المان شبکه، عملکرد شبکه مختل نشده و بهره‌برداری شبکه بدون مشکل ادامه می‌یابد [۲]. در دنیای امروز، روش‌های سنتی مطالعه امنیت شبکه برق، با دو چالش روبه‌رو هستند. چالش اول، افزایش گزارش‌های مبنی بر وقوع حملات عامدانه[1] به شبکه‌های برق و خاموشی‌های سراسری در دو دهه اخیر است [۱۰-۴] که خروج‌های ناشی از این حملات، در مطالعات سنتی N-1 و N-2 دیده نشده است. چالش دوم برخاسته از این موضوع است که مطالعات سنتی قابلیت اطمینان، تنها خروج‌های تصادفی را مدنظر قرار می‌دهند و این در حالی است که حملات عامدانه به صورت هدفمند و برنامه‌ریزی شده صورت می‌گیرند [۱۱].

با این توصیف، معیارهای قابلیت اطمینان، دیگر برای تضمین امنیت شبکه‌های برق کفایت نمی‌کنند و در کنار مطالعات امنیت شبکه، لازم است که مطالعات آسیب‌پذیری شبکه نیز به دقت انجام پذیرد [۱۱ و ۱۲]. در سال‌های اخیر، پس از حادثه ۱۱ سپتامبر ۲۰۰۱، بحث مطالعات مقید به آسیب‌پذیری[2] اهمیت ویژه‌ای یافته است و سرمایه‌گذاری در شبکه‌های برق برای طراحی و توسعه آن‌ها، و همچنین بهره‌برداری شبکه‌های برق با در نظر گرفتن آسیب‌پذیری شبکه در مقابل حملات عامدانه صورت می‌گیرد [۱۸-۱۳]. در مطالعات آسیب‌پذیری، اگر چه 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. در صورتی که با چنین مواردی به تحلیل آسیب‌پذیری و انتخاب یک راهبرد دفاعی بپردازیم، این 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 سامانه وارد کند [۱۹]. بنابراین، آگاهی برنامه‌ریزان شبکه‌های برق از مدل‌ها و تحلیل‌های ریاضی که در مراجع مختلف برای بررسی آسیب‌پذیری شبکه برق ارائه شده است، امری ضروری است.

در این مقاله، مروری خواهیم داشت بر مهم‌ترین مدل‌هایی که برای بررسی آسیب‌پذیری شبکه‌های برق ارائه شده‌اند. ارائه یک مطالعه جامع از مدل‌های ارائه شده، ابزاری مفید در اختیار طراحان، برنامه‌ریزان و بهره‌برداران شبکه‌های برق قرار می‌دهد تا بتوانند در طراحی، برنامه‌ریزی و بهره‌برداری شبکه، جنبه‌های مختلف آسیب‌پذیری را در نظر بگیرند.

در ادامه، ابتدا در بخش دوم به بیان رویکردهای مختلفی که در زمینه تحلیل آسیب‌پذیری شبکه‌های برق وجود دارد پرداخته خواهد شد. پس از آن، در بخش سوم مروری بر مهم‌ترین مدل‌های ارائه شده برای بررسی آسیب‌پذیری شبکه‌های برق خواهد شد. سپس، در بخش چهارم به بیان چالش‌های پیش روی این مدل‌ها پرداخته خواهد شد و مهم‌ترین روش‌هایی که برای حل آن‌ها ارائه شده است، مورد بررسی قرار می‌گیرد. در آخر، در بخش پنجم نتیجه‌گیری تحقیق ارائه می‌شود.

۲. رویکردهای تحلیل آسیب‌پذیری شبکه‌های برق

پس از حادثه ۱۱ سپتامبر ۲۰۰۱، موضوع بررسی آسیب‌پذیری زیرساخت‌های ملی، در اولویت‌های اصلی برنامه‌ریزی بسیاری از کشورها قرار گرفت [۱۷ و ۳۰-۲۰]. به طور کلی، مطالعات آسیب‌پذیری، مهم‌ترین زیرساخت‌های ملی شامل بخش‌های کشاورزی، بانکداری، نفت و صنایع شیمیایی، پست، کشتی‌رانی، دستگاه‌های مخابراتی و تبادل اطلاعات، آب، غذا، دارو و سلامت، حمل و نقل و شبکه برق را دربر می‌گیرد [۱۹ و ۳۱]. گزارش‌های منتشر شده از وقوع حملات مختلف به زیرساخت‌های بیان شده در نقاط مختلف دنیا باعث شده است تا دولت‌ها، سالانه هزینه‌های بسیار زیادی را برای شناسایی و تقویت نقاط ضعف زیرساخت‌های خود صرف کنند [۲۰].

یکی از این زیرساخت‌ها، زیرساخت شبکه الکتریکی است که نمونه‌های بسیاری، آسیب‌پذیری این زیرساخت مهم را نشان می‌دهد. طبق آمار ارائه شده توسط MIPT[3]، طی یک دوره ۱۰ ساله، از سال ۱۹۹۴ تا سال ۲۰۰۴، بیش از ۳۰۰ حمله متخاصمانه در سراسر جهان به شبکه‌های برق صورت گرفته است [۳۲]. در یک دسته‌بندی، می‌توان منشأ تهدیدهای شبکه برق را در چهار گروه جای داد [۳۳]:

- تهدید طبیعی[4]: شامل حوادث طبیعی نظیر سیل، زلزله و طوفان که وقوع آن‌ها توسط انسان کنترل نمی‌شود؛

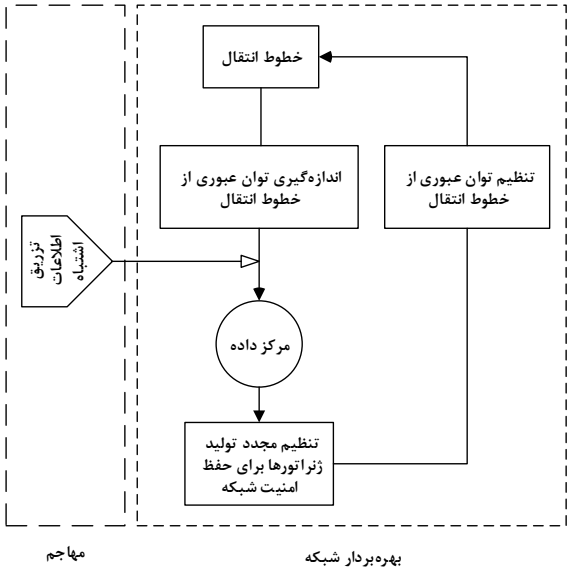
[1] Intentional Attacks
[2] Vulnerability-Constrained Studies
[3] Memorial Institute for the Prevention of Terrorism
[4] Natural Threat

• تهدید تصادفی[1]: خطاهای معمول شبکه برق که منجر به خروج تجهیزات شده و امنیت شبکه را به خطر می‌اندازند؛

• تهدید معاند[2]: اعمالی که به طور عمد توسط یک شخص و یا گروه معاند صورت می‌گیرد تا عملکرد شبکه برق را مختل کند؛

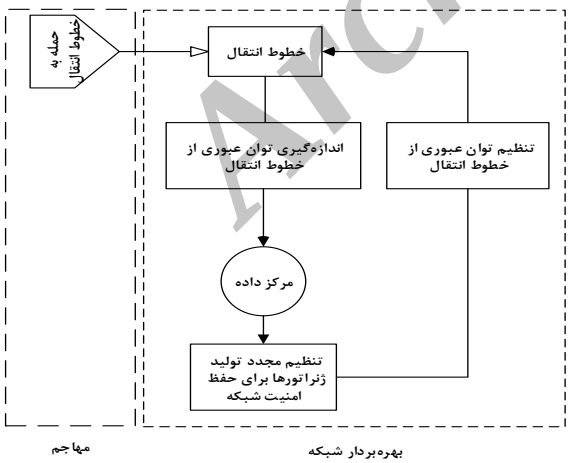
• تهدید ظهوری[3]: تهدیدهایی که هم‌زمان با توسعه شبکه برق، نظیر پیوستن انرژی‌های تجدیدپذیر و همچنین وابستگی شبکه برق به سایر زیرساخت‌ها پدید آمده‌اند [۲۹ و ۳۴].

در خصوص تهدیدهای معاند، سه دسته تهدید مختلف از طرف شبکه برق برای جامعه وجود دارد [۳۵]: ۱) حمله به شبکه برق: که در این تهدید، خود شبکه برق هدف است (به عنوان مثال، حمله از طریق بمب‌های گرافیتی و خروج چند خط انتقال به صورت هم‌زمان [۲۸ و ۳۸-۳۶])، ۲) حمله با شبکه برق: به عنوان مثال، می‌توان با انتشار مواد شیمیایی و یا بیولوژیکی خطرناک از طریق برج‌های خنک‌کن یک نیروگاه، به اجتماع آسیب وارد کرد و ۳) حمله از طریق شبکه برق: به عنوان نمونه، می‌توان با وصل کردن مولد پالس الکترومغناطیسی به شبکه برق، به تجهیزات مخابراتی و رایانه‌های متصل به شبکه آسیب جدی وارد کرد [۲۳، ۲۸ و ۳۸-۳۶]. در خصوص دسته اول (که تمرکز اصلی این مقاله نیز بر این دسته حملات است)، شبکه برق هم از نظر ساختار فیزیکی و هم از نظر مباحث مخابراتی و امنیت اطلاعات می‌تواند مورد تهاجم قرار گیرد. نمونه‌هایی از ضعف‌های مخابراتی شبکه برق و نیز نمونه‌هایی واقعی از سوءاستفاده‌های صورت گرفته از ضعف‌های مخابراتی و امنیتی موجود در شبکه های برق ارائه شده است [۱۷ و ۲۲]. این دسته از حملات را حملات سایبری[4] می‌نامند که در آن‌ها، تنها با استفاده از سامانه‌های مخابراتی، عملکرد صحیح شبکه برق مختل می‌شود [۲۲ و ۴۳-۳۹]. روند نمای ارائه شده در شکل (۱)، عملکرد بهره‌بردار شبکه و مهاجم را به خوبی نشان می‌دهد. همان‌طور که در این شکل مشاهده می‌شود، در حالت بهره‌برداری معمولی شبکه، تجهیزات اندازه‌گیری، اطلاعات وضعیت شبکه را به یک مرکز داده ارسال می‌کنند. این داده‌ها پس از پردازش، به بهره‌بردار شبکه ارسال می‌شوند و بهره‌بردار شبکه بر اساس این اطلاعات و در صورت نیاز، توان تولیدی ژنراتورها را دوباره تنظیم می‌کند تا توان عبوری از خطوط شبکه در محدوده امن باقی بماند. در این حالت، مهاجم تنها از طریق تزریق اطلاعات اشتباه می‌تواند بهره‌بردار شبکه را به خطا انداخته و عملکرد صحیح شبکه را مختل کند.



شکل ۱. روند نمای حملات سایبری به شبکه برق

دسته دیگری از حملات، حملاتی هستند که به طور مستقیم ساختار فیزیکی شبکه برق را هدف قرار می‌دهند [۱۱، ۱۵، ۱۹ و ۵۶-۴۴]. روند نمای این دسته از حملات در شکل (۲) نمایش داده شده است. این دسته از حملات، حملات فیزیکی[5] نامیده می‌شوند. خسارت ناشی از این حملات بسیار شدیدتر از دسته حملات سایبری بوده و عمده حملات صورت گرفته در سال‌های اخیر، در این دسته جای می‌گیرند [۳۲]. به خاطر صدمات شدید این دسته از حملات، بیشتر پژوهشگران نیز تمرکز خود را بر این دسته از حملات قرار داده‌اند که در بخش سوم به بیان جزئیات این تحقیقات پرداخته خواهد شد.

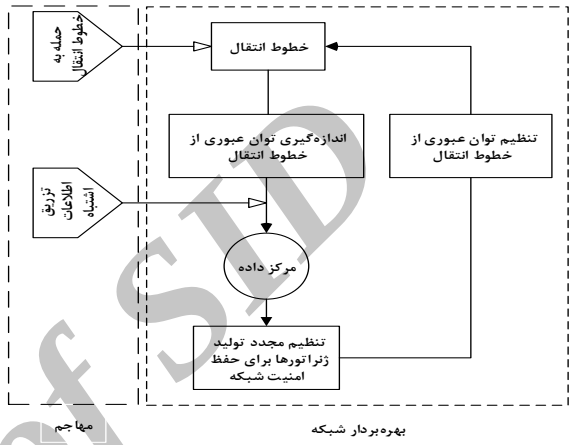


شکل ۲. روند نمای حملات فیزیکی به شبکه برق

دسته دیگری از حملات که ترکیبی از دو دسته قبل است، حملات سایبری-فیزیکی[6] است که به صورت هم‌زمان، ساختار فیزیکی شبکه برق را هدف قرار می‌دهند و از طریق سامانه‌های

[1] Accidental Threat
[2] Malicious Threat
[3] Emerging Threat
[4] Cyber Attacks
[5] Physical Attacks
[6] Cyber-Physical Attacks

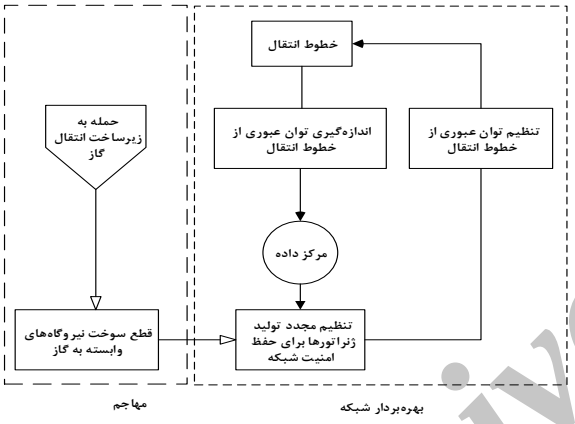
مخابراتی، تخریب‌هایی انجام می‌دهند که ارتباط مخابراتی بخش‌های مختلف سامانه قطع شده و مدیریت وضعیت تحت حمله دشوارتر شود [۶۱-۵۷]. شکل (۳) روند نمای این دسته از حملات را نشان می‌دهد. همان‌طور که مشاهده می‌شود، مهاجم می‌تواند به طور هم‌زمان هم به زیرساخت فیزیکی و هم به زیرساخت مخابراتی شبکه برق حمله کند و آگاهی بهره‌بردار را از وضعیت نقاط تحت حمله کاهش دهد.



شکل ۳. روند نمای حملات سایبری-فیزیکی به شبکه برق

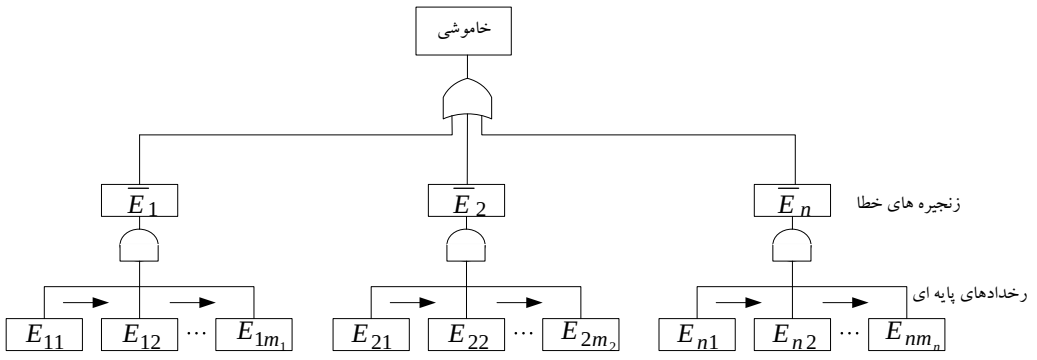
در رویکردی دیگر، برخی از محققان به بررسی امنیت و آسیب‌پذیری شبکه برق از ناحیه وابستگی به سایر زیرساخت‌ها از جمله زیرساخت نفت و گاز پرداخته‌اند. این دسته از مطالعات را تحلیل آسیب‌پذیری وابستگی[1] می‌نامند [۶۹-۶۲]. در واقع می‌توان گفت که مطالعات مربوط به حملات سایبری-فیزیکی، زیرمجموعه مطالعات آسیب‌پذیری وابستگی هستند که به بررسی آسیب‌پذیری شبکه برق از ناحیه وابستگی به سامانه‌های مخابراتی می‌پردازند. در خصوص سایر زیرساخت‌ها، به عنوان مثال، سوخت بسیاری از نیروگاه‌ها در سراسر جهان، از نوع گازی بوده و توسط شبکه گاز تأمین می‌شود. در مواقعی که شبکه گاز با اختلال مواجه می‌شود، اگر این اختلال برای مدتی به قوت خود باقی بماند، سوخت و ذخیره نیروگاه‌هایی که از سوخت گاز استفاده می‌کنند و عمده آن‌ها در ساعت‌های پیک شبکه به مدار وصل می‌شوند، با مشکل مواجه می‌شود و این موضوع می‌تواند موجب قطع بخشی از بار سامانه شود. روند نمای این دسته از حملات نیز در شکل (۴) نمایش داده شده است.

رویکرد دیگری که در بررسی آسیب‌پذیری شبکه برق وجود دارد، تشخیص خروج‌هایی است که صرف‌نظر از عمد و یا غیر عمد بودن منشأ آن‌ها، منجر به خاموشی سراسری[2] شبکه می‌شوند [۷۹-۷۰]. اساس مدل‌هایی که با این رویکرد به بررسی آسیب‌پذیری شبکه برق می‌پردازند، مبتنی بر اثر دومینو[3] است که بیان می‌کند که خطاهای متوالی[4] همواره وابسته به رخدادهای دیگر هستند [۷۰ و ۷۹].



شکل ۴. روند نمای حملات مورد نظر در تحلیل آسیب‌پذیری وابستگی

در خصوص شبکه برق، این اثر در نظریه زنجیره خطا[5] استفاده می‌شود که ساختار کلی آن در شکل (۵) نشان داده شده است. در این شکل، E_{ij} رخداد پایه j ام مربوط به زنجیره خطای i ام است. به عنوان مثال، زنجیره خطای شماره ۱ ($\overline{E_1}$)، ترکیبی از وقوع هم‌زمان رخدادهای پایه‌ای E_{11} تا E_{1m_1} است که منجر به خاموشی سامانه می‌شود.

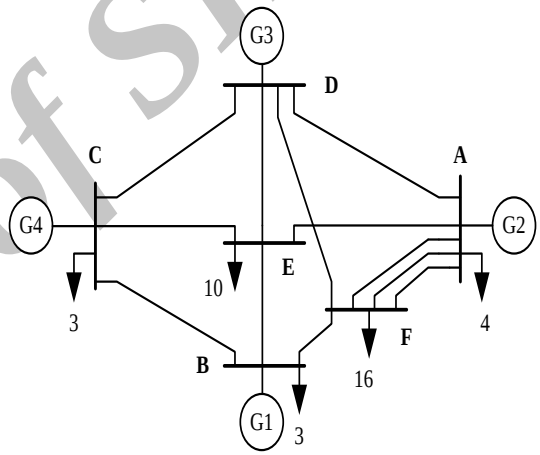


شکل ۵. منطق زنجیره خطا [۷۰]

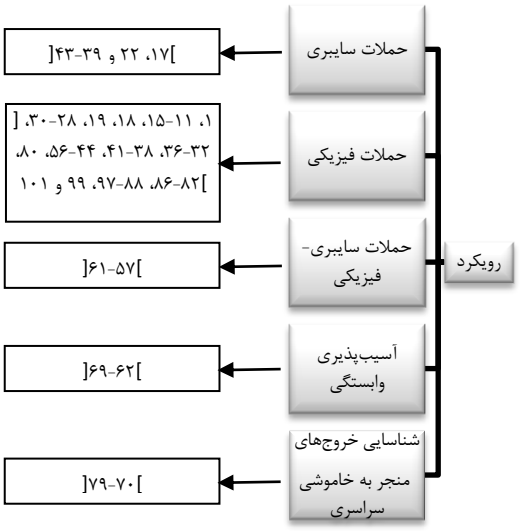
[1] Interdependency Vulnerability Analysis

[2] Blackout
[3] Domino Effect
[4] Cascading Failures
[5] Fault Chain Theory

اثر دومینو در شبکه برق را می‌توان با یک مثال ساده شرح داد [۷۰]. با توجه به شکل (۶)، اگر یکی از خطوط انتقال کانال A-F تحت تعمیر باشد و در همین زمان، یکی دیگر از خطوط این کانال به دلیل وقوع یک خطای تک‌فاز از مدار خارج شود، خط سوم دچار اضافه‌بار[1] شده و سامانه حفاظت شبکه، این خط را نیز از مدار خارج می‌کند. در چنین شرایطی، کل بار شین F بر روی خطوط B-F و D-F افتاده و این خطوط نیز یکی پس از دیگری، به دلیل اضافه‌بار از مدار خارج می‌شوند. شکل (۷) دسته‌بندی مناسبی از رویکردهای مختلفی که برای بررسی آسیب‌پذیری شبکه برق در مراجع مختلف انتخاب شده است، ارائه می‌دهد. به طور کلی، موضوع آسیب‌پذیری شبکه برق موضوع بسیار گسترده‌ای است که بررسی تمام ابعاد آن از محدوده این مقاله خارج است.



شکل ۶. شبکه شش شینه نمونه [۷۰]

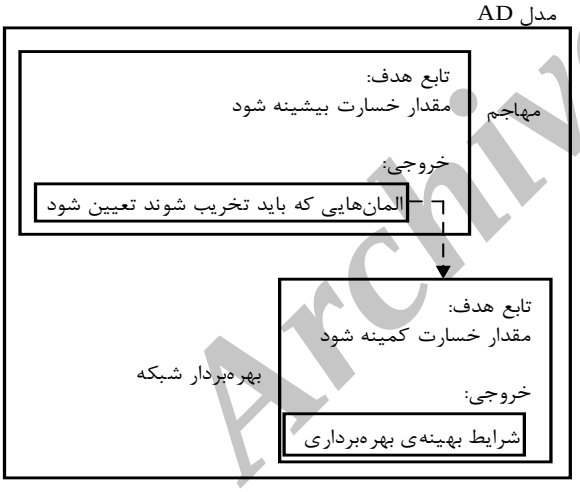


شکل ۷. دسته‌بندی مراجع، از منظر رویکرد آسیب‌پذیری

در ادامه، با محوریت مطالعاتی که آسیب‌پذیری ساختار فیزیکی شبکه برق را مورد بررسی قرار داده‌اند، جزئیات و روابط ریاضی مربوط به مهم‌ترین مدل‌های ارائه شده را بیان خواهد شد.

۳. مدل‌های ارائه شده برای تحلیل آسیب‌پذیری شبکه‌های برق

سالمرون [۴۵] نخستین کسی است که مسئله امنیت شبکه برق تحت حملات عامدانه را فرمول‌بندی کرده است. سالمرون مسئله پیشِ رو را به صورت یک مسئله Max-min فرمول‌بندی کرده است که قادر است المان‌های حیاتی شبکه برق را شناسایی کند. ساختار مدل ارائه شده توسط سالمرون (و اکثر مقالات ارائه شده در این زمینه) به صورت یک مسئله دو سطحی مهاجم-مدافع (AD)[2] است (شکل ۸). مسئله سطح بالا، مسئله حمله و مسئله سطح پایین بیانگر واکنش مدافع (بهره‌بردار یا برنامه‌ریز شبکه) در مقابل حملات است. در زیر بخش‌های بعد به بررسی بیشتر مسئله‌های مهاجم و مدافع پرداخته و تابع هدف‌ها و قیودی که در مراجع مختلف برای این مسائل در نظر گرفته شده است را با بیان روابط ریاضی نمونه، تشریح خواهد شد.



شکل ۸. شمای کلی مدل‌های دو سطحی AD

۳-۱. مسئله مهاجم (حمله)

در مسئله حمله، مهاجم تجهیزاتی از شبکه را مورد حمله قرار می‌دهد که خروج آن‌ها بیشترین خسارت را به سامانه وارد می‌کند. در تعیین میزان «خسارت»، شاخص‌های مختلفی در مراجع مختلف در نظر گرفته شده است:

- هزینه بار قطع شده [۴۴-۴۷]
- هزینه انرژی قطع شده [۴۵ و ۵۲]

[1] Overload

[2] Attacker-Defender

- هزینه تولید [۱۴، ۴۴، ۴۵ و ۵۲]
- میزان بار (یا انرژی) قطع شده [۱، ۱۱، ۴۸، ۵۴، ۷۴ و ۸۰]
- مدت زمان بازیابی سامانه [۱۲]
- بار توزیع شده بر روی خطوط انتقال شبکه [۵۳، ۵۷-۵۵، ۸۱ و ۸۲]
- خاموشی سراسری شبکه [۷۸-۷۰]
- حد پایداری شبکه [۴۹]
- هزینه‌های پس از حمله شامل هزینه تولید، هزینه بار قطع شده، هزینه تعمیرات برای ترانسفورمرهای بدون یدک و هزینه جایگزینی ترانسفورمرهای یدکی [۱۴] است.

در دنیای واقعی، هدف اصلی یک گروه مهاجم، افزایش وحشت در جامعه است که شاخص‌های گفته شده تا حد خوبی می‌توانند سیگنال‌هایی هم‌سو با میزان وحشت در جامعه ارسال کنند [۵۲]. نکته‌ای که باید به آن اشاره کرد، ارتباط بین شاخص‌های مطرح شده در بحث آسیب‌پذیری شبکه برق و شاخص‌های قابلیت اطمینان شبکه است. شاخص‌های بار قطع شده، انرژی قطع شده و میزان بار توزیع شده بر روی خطوط انتقال شبکه، در بحث قابلیت اطمینان شبکه نیز به عنوان معیارهایی برای سنجش میزان مطمئن بودن شبکه مطرح می‌شوند. تفاوت این شاخص‌ها در بحث آسیب‌پذیری و قابلیت اطمینان، منشأ قطع بار، قطع انرژی و یا میزان بار توزیع شده بر روی خطوط انتقال شبکه است. زمانی که بررسی قابلیت اطمینان شبکه مد نظر است، در سناریوهای مختلف خروج *اتفاقی* خط و یا نیروگاه، شاخص‌های مورد نظر محاسبه می‌شوند و قابلیت اطمینان شبکه مورد ارزیابی قرار می‌گیرد. این در حالی است که در بررسی آسیب‌پذیری شبکه، خروج المان‌های شبکه، منشأ اتفاقی ندارند و توسط گروهی متخاصم، برنامه‌ریزی شده‌اند.

دقت شود که هر کدام از شاخص‌های گفته شده برای تعریف خسارت، می‌تواند به عنوان تابع هدف مهاجم در مدل AD ارائه شده در شکل (۸) قرار گیرد. در ادامه، شاخص‌های مطرح شده، با جزئیات بیشتر مورد بررسی قرار خواهند گرفت.

در حالتی که تابع هدف مهاجم، بیشینه کردن هزینه‌های قطع بار و هزینه‌های تولید است، این تابع هدف به صورت زیر تعریف می‌شود [۱۵، ۴۷-۴۴ و ۸۳]:

$$Max\left\{\sum_{i\in\Omega^G}\sum_{b\in\Lambda_i^G}C_{ib}^G g_{ib}+\sum_{j\in\Omega^D}\sum_{a\in\Lambda_j^D}C_{ja}^C s_{ib}\right\} \qquad (۱)$$

عبارت اول در این رابطه بیانگر هزینه‌های تولید و عبارت دوم بیانگر هزینه قطع بار در شبکه است. از آنجا که هزینه قطع بار بسیار بزرگ‌تر از هزینه تولید است، اگر چه تابع هدف مهاجم به صورت رابطه (۱) فرمول‌بندی می‌شود اما در تمام مراجع، در مطالعات عددی از هزینه‌های تولید صرف‌نظر می‌کنند. مرجع [۵۲] در نتایج عددی تحقیق خود، مقادیر مربوط به هزینه‌های تولید و قطع بار را به تفکیک ارائه داده است و نشان داده است که هزینه‌های تولید در مقایسه با هزینه‌های قطع بار بسیار ناچیز و قابل صرف نظر هستند. در صورتی که در رابطه (۱)، عبارت اول و ضریب C_{ja}^C حذف شوند، رابطه حاصل بیانگر میزان بار قطع شده در شبکه خواهد بود [۱، ۱۱، ۴۸، ۵۴، ۷۴ و ۸۰]. ضریب C_{ja}^C در واقع به صورت یک ضریب وزنی عمل کرده و این امکان را فراهم می‌کند تا بتوان بین بارهای مختلف شبکه از جمله بارهای خانگی، تجاری و صنعتی تمایز قائل شد [۵۲].

در برخی گزارش‌ها، تابع هدف مسئله حمله به صورت بیشینه کردن بار توزیع شده بر روی خطوطی که در مدار هستند (و به آن‌ها حمله نشده است) در نظر گرفته شده است [۵۷].

$$Max\left[\sum_{l\in\Omega^L}|\Delta p_l|.\left(1-\delta_l^{Line}\right)\right] \qquad (۲)$$

در این رابطه، Δp_l میزان تغییر فلوی واقعی ایجاد شده در خط l، پس از وقوع تمام حملات است. اساس مسئله حمله به این صورت است که مهاجم ابتدا به برخی از خطوط شبکه حمله می‌کند و پس از آن سعی می‌کند تا از طریق حملات سایبری، به گونه‌ای تشخیص خروج خطوطی که به آن‌ها حمله شده است را غیر ممکن کند [۵۷]. این کار از طریق تزریق اطلاعات اشتباه در خصوص وضعیت کلیدهای خط انتقال صورت می‌گیرد. در یک شبکه برق که مجهز به سامانه‌های تخمین حالت[1] است، تنها تغییر وضعیت کلیدهای شبکه برای گمراهی بهره‌بردار شبکه و عدم آگاهی او از خروج یک خط انتقال کافی نیست. بنابراین، مهاجم علاوه بر تغییر اطلاعات مربوط به حالت[2] کلیدهای خط انتقال تحت حمله، با تزریق اطلاعات اشتباه در خصوص میزان بار متصل به دو سر خط انتقال و نیز فلوی اندازه‌گیری شده عبوری از آن خط، می‌تواند بهره‌بردار شبکه را به گونه‌ای به خطا بیاندازد که تصور کند خط انتقال تحت حمله همچنان در مدار است. این موضوع سبب قطعی بخشی از بار شبکه می‌شود.

مهم‌ترین قیدی که مهاجم با آن روبه‌رو است، قید محدودیت منابع[3] است که معمولاً به صورت محدودیت تعداد افراد[4] مدل‌سازی می‌شود [۱۲، ۱۵، ۴۴، ۴۵، ۴۷ و ۵۲].

[1] State Estimation Systems
[2] State
[3] Resource Limitation Constraint
[4] Individuals

$$\sum_{i\in\Omega^G} R_i^{Gen}\delta_i^{Gen} + \sum_{l\in\Omega^L} R_l^{Line}\delta_l^{Line} + \sum_{n\in\Omega^N} R_n^{Bus}\delta_n^{Bus} + \sum_{s\in\Omega^S} R_s^{Sub}\delta_s^{Sub} \le R_T \quad (۳)$$

به عنوان مثال، در برخی مراجع فرض شده است که برای حمله به یک پست برق، سه نفر از افراد مهاجم باید به‌کار گرفته شوند (R_s^S = ۳) [۴۵]. فرضی که در بسیاری از مقالات در نظر گرفته می‌شود این است که مهاجم تنها می‌تواند به خطوط انتقال حمله کند. این فرض از دو جنبه می‌تواند منطقی باشد؛ یکی اینکه ژنراتورها و پست‌های برق معمولاً به خوبی محافظت می‌شوند و احتمال موفقیت مهاجم در حمله به آن‌ها کم است و به علاوه، حمله به این المان‌ها هزینه زیادی می‌طلبد [۱۵، ۴۸ و ۸۳]. علاوه بر آن، حمله به خطوط انتقال که معمولاً از بیابان‌ها و نقاط دور از دسترس رد می‌شوند بسیار ساده‌تر بوده و مهاجم می‌تواند با صرف هزینه کمتر، احتمال موفقیت خود را در حمله زیاد کند [۴۴ و ۵۲]. آمار گزارش شده از حملات صورت گرفته بر روی شبکه‌های برق در سراسر دنیا نیز این موضوع را تأیید می‌کند. در ایالات متحده آمریکا، بیش از ٪۹۰، و در بقیه کشورها حدود ٪۶۰ از حملات صورت گرفته، خطوط انتقال را هدف خود قرار داده‌اند [۳۲ و ۸۴].

فرض اساسی دیگری که در مطالعات آسیب‌پذیری در نظر گرفته می‌شود این است که مهاجم از اطلاعات کافی در خصوص مدافع برخوردار است [۱۱، ۱۵، ۱۶، ۱۹، ۴۷-۴۵، ۵۲ و ۵۷] (در برخی مراجع، حالت‌هایی که مهاجم به اطلاعات کامل مدافع دسترسی ندارد، در حد بیان روابط بررسی شده است [۸۵ و ۸۶]). دسترسی کامل مهاجم به اطلاعات، یک فرض معقول است. یک خودآموز به‌دست آمده 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 غیر قانونی، می‌توان بیش از ٪۸۰ از اطلاعات مورد نیاز را به‌دست آورد» [۱۹]. بنابراین می‌توان تصور کرد که برای یک حمله برنامه‌ریزی شده توسط یک گروه هوشمند، دسترسی کامل به اطلاعات وجود دارد. به علاوه، همان‌طور که پیش‌تر نیز گفته شد، هدف از مطالعات آسیب‌پذیری، شناسایی نقاط ضعیف شبکه است و برای این کار لازم است که بدترین حالت ممکن در نظر گرفته شود. فرض دسترسی کامل مهاجم به اطلاعات مدافع، یک فرض کمک کننده برای مدل‌سازی بدترین حالت ممکن است.

مسئله مهاجم از دیدگاه دیگری نیز مورد بررسی قرار گرفته است [۱۱، ۴۸، ۵۴، ۸۰ و ۸۵] و به گونه‌ای به این سؤال پاسخ داده شده که اگر مهاجم بخواهد میزان قطع بار شبکه از یک مقدار از پیش تعیین شده (S^*) بیشتر شود، چقدر باید هزینه کند. در این حالت، تابع هدف مسئله مهاجم به صورت زیر تعریف می‌شود:

$$Min \sum_{l\in\Omega^L} \delta_l^{Line} \quad (۴)$$

تابع هدف (۴) بیانگر حداقل تعداد حملات است که مقید به قید زیر است:

$$\sum_{j\in\Omega^D}\sum_{a\in\Lambda_j^D} s_{ib} \ge S^* \quad (۵)$$

نکته‌ای که باید به آن دقت کرد این است که اگر چه در مدل‌های AD، مسئله حمله از دید مهاجم بررسی می‌شود، اما کاربر[1] نهایی مدل‌های AD، برنامه‌ریز (یا اپراتور) شبکه است. به این معنی که با استفاده از یک مدل AD، برنامه‌ریز شبکه می‌تواند از دید مهاجم به شبکه نگاه کند و مخرب‌ترین حملات را پیش‌بینی کرده و نقاط ضعیف شبکه را شناسایی کند. با چنین توصیفی، استفاده از مدل‌هایی که از تابع هدف‌های مشابه با رابطه (۴) استفاده می‌کنند، به گونه‌ای مشابه مطالعات *N-k* است که به این سؤال پاسخ می‌دهند که آیا مجموعه‌ای متشکل از *k* المان (و یا کمتر) وجود دارد که خروج آن‌ها باعث از کارافتادگی سامانه شود [۸۷]؟

برای بررسی مسئله آسیب‌پذیری شبکه برق، می‌توان از یک شاخص ناپایداری استفاده کرد [۴۹]. برای خط انتقال *l*، حاشیه امن[2] به صورت فاصله بین وضعیت بهره‌برداری کنونی آن و حد امنیت[3] (p_l^*) آن تعریف می‌شود. حد امنیت یک خط (که کمتر از ظرفیت آن خط است)، مقداری است که اگر فلوی خط از آن حد بیشتر شود (در یک شرایط بهره‌برداری معلوم)، با تغییری اندک در یکی از بارهای سامانه، لااقل یکی از خطوط شبکه از مدار خارج می‌شود و ناپایداری سامانه افزایش می‌یابد. حد امنیت یک خط، وابسته به ساختار و نیز وضعیت بهره‌برداری شبکه است و عموماً با توجه به ظرفیت خطوط پایین‌دست آن (با توجه به جهت عبور جریان) تعیین می‌شود. شاخص ناپایداری به صورت زیر تعریف می‌شود [۴۹]:

$$\kappa^{inst} = \sum_{l\in\Omega^L} \max\left\{p_l - p_l^*, 0\right\} \quad (۶)$$

در این رابطه، اگر مقدار فلوی عبوری یک خط از حد امنیت آن فراتر رود، شاخص ناپایداری شبکه افزایش می‌یابد. بنابراین، مهاجم حملات خود را به گونه‌ای برنامه‌ریزی می‌کند که شاخص ناپایداری شبکه حداکثر شود.

[1] User
[2] Safety Margin
[3] Security Limit

برخی مراجع، تابع هدف مهاجم را هزینه انرژی (و نه بار) قطع شده در نظر گرفته‌اند [۴۴ و ۴۵]. در این مراجع، فرض شده است که زمانی که یک خط مورد حمله واقع می‌شود، این خط برای یک دوره مشخص از شبکه خارج می‌شود. ممکن است در این دوره بخشی از تقاضای بارهای شبکه تأمین نشود. بنابراین، مهاجم آن دسته از خطوطی را مورد حمله قرار می‌دهد که خروج آن‌ها برای یک دوره مشخص، بیشترین مقدار انرژی قطع شده را به همراه داشته باشد. در یکی از گزارش‌ها [۵۲]، برای نخستین بار بحث مطالعه آسیب‌پذیری شبکه‌های برق را در یک دوره میان‌مدت (T) مطرح کرده است و نشان داده است که لحاظ عبارت «زمان» در بررسی آسیب‌پذیری شبکه‌های برق الزامی است. در این تحقیق عنوان شده است که یک مهاجم باهوش برای انتخاب مخرب‌ترین حمله، علاوه بر تصمیم‌گیری در خصوص «مکان» حملات (چیزی که سایر مراجع نیز به آن پرداخته‌اند)، در خصوص «زمان» حملات نیز تصمیم‌گیری می‌کند. این مدل، در واقع، به برنامه‌ریز شبکه کمک می‌کند تا به این سؤال پاسخ دهد که شبکه برق او، «کی و کجا» آسیب‌پذیرتر است؟ [۵۲]. در این مدل، علاوه بر قید محدودیت منابع مهاجم، قیود دیگری که در مسئله مهاجم در نظر گرفته شده است شامل موارد زیر می‌شود [۵۲]:

$$\sum_{l\in\Omega^L}\left[R_l^{Line}.\delta_l^{Line}(t)\right]\le R(t);\quad \forall t\le T \tag{۷}$$

$$z_l=\sum_{t=1}^{T}\delta_l^{Line}(t);\quad \forall l\in\Omega^L \tag{۸}$$

$$z_l\le Z_l^{\max};\quad \forall l\in\Omega^L \tag{۹}$$

$$x_l(t)-\delta_l^{Line}(t)\ge 0;\quad \forall l\in\Omega^L,\forall t\le T \tag{۱۰}$$

$$\sum_{t=1}^{T}x_l(t)=W_l.z_l;\quad \forall l\in\Omega^L \tag{۱۱}$$

$$x_l(\mathrm{t})-x_l(\mathrm{t}-1)\le x_l(t+W_l-1) -\sum_{r=t+1}^{t+W_l-1}\delta_l^{Line}(\mathrm{r});\forall l\in\Omega^L,\forall t\le T \tag{۱۲}$$

$$x_l(t+W_l-1)-\delta_l^{Line}(t)\ge 0;\quad \forall l\in\Omega^L,\forall t\le T \tag{۱۳}$$

$$\sum_{r=t}^{t+W_l-1}\delta_l^{Line}(r)\le 1;\quad \forall l\in\Omega^L,\forall t\le T \tag{۱۴}$$

قید (۷) بیان می‌کند که مهاجم الزاماً تمام نیروهای خود را در یک بازه زمانی t به‌کار نمی‌گیرد (برخلاف سایر مراجع که با بررسی آسیب‌پذیری شبکه برق در یک تصویر از وضعیت بهره‌برداری شبکه، که معمولاً وضعیت پیک بار شبکه است، فرض می‌کنند که مهاجم همه منابع خود را در همان زمان استفاده می‌کند). قید (۸) تعداد حملاتی را که در زمان‌های مختلف بر روی یک خط انتقال صورت گرفته است (حملات چندگانه[1]) شمارش می‌کند و قید (۹)، یک کران بالا برای تعداد این حملات در نظر می‌گیرد. نکته مهمی که باید به آن دقت کرد این است که در نظر گرفتن زمان در بررسی آسیب‌پذیری شبکه برق [۵۲]، این امکان را فراهم می‌کند تا بتوان حملات چندگانه را نیز مدل‌سازی کرد. بدون در نظر گرفتن زمان، امکان مدل‌سازی این عمل مهم مهاجم امکان‌پذیر نیست. قید (۱۰) بیان می‌کند که اگر خطی مورد حمله قرار گیرد، بلافاصله برای تعمیرات از مدار خارج می‌شود. مدت زمان لازم برای تعمیرات هر خط (W_l)، با در نظر گرفتن تعداد حملات صورت گرفته بر روی هر خط، در رابطه (۱۱) شمارش می‌شود. قید (۱۲) تضمین کننده پیوستگی تعمیرات یک خط است. قید (۱۳) نشان می‌دهد که برای هر حمله، یک تعمیرات جداگانه انجام می‌شود. درنهایت، قید (۱۴) بیان می‌کند که زمانی که یک خط تحت تعمیر است، مهاجم به آن حمله نمی‌کند، چرا که چنین کاری باعث هدر رفتن منابع مهاجم می‌شود.

دسته‌ای از پژوهش‌ها برای بررسی آسیب‌پذیری شبکه برق، به تعریف شاخص‌هایی برای رتبه‌بندی میزان حیاتی بودن[2] تجهیزات شبکه پرداخته‌اند [۵۵، ۵۶ و ۸۸-۹۴]. در این مطالعات که معمولاً مبتنی بر نظریه شبکه‌های پیچیده[3] هستند، شبکه برق به صورت یک گراف جهت‌دار وزن‌دار مدل می‌شود که در آن، توان از مراکز تولید (گره منبع[4]) به نقاط مصرف (گره چاهک[5]) شارش می‌یابد. شاخص‌هایی که در این مطالعات مطرح شده‌اند شامل موارد زیر است:

- شاخص مرکزیت (CI)[6] [۵۵، ۵۶ و ۸۸]
- شاخص ریسک (RI)[7] [۸۹-۹۱]
- شاخص میانگی (BI)[8] [۹۲ و ۹۵]
- شاخص کوتاه‌ترین مسیر (SPI)[9] [۹۳ و ۹۴]

شاخص مرکزیت برای شاخه ارتباط دهنده گره‌های n_1 و n_2 در شبکه‌ای شامل u منبع و v چاهک به صورت زیر تعریف می‌شود [۵۵]:

$$\kappa^{cent}=\frac{\sum_{i=1}^{u}\sum_{j=1}^{v}p_{n_1n_2}^{ij}}{\sum_{i=1}^{u}\sum_{j=1}^{v}P_{\max}^{ij}} \tag{۱۵}$$

در این رابطه، $P_{\max}^{ij}$ حداکثر فلویی است که می‌تواند از منبع i به چاهک j شارش کند. با محاسبه CI برای تمام خطوط شبکه و

[1] Multiple Attacks

[2] Criticality
[3] Complex Networks Theory
[4] Source Node
[5] Sink
[6] Centrality Index
[7] Risk Index
[8] Betweenness Index
[9] Shortest Path Index

سپس مرتب کردن آن‌ها به ترتیب صعودی، می‌توان خطوط شبکه را بر اساس میزان حیاتی بودن آن‌ها برای شبکه رتبه‌بندی کرد.

برای محاسبه ریسک تجهیزات شبکه برق می‌توان از شبکه بیزین[1] استفاده کرد [۸۹]. در واقع تشکیل شبکه بیزین که منتج از نظریه احتمالات است، کمک می‌کند تا بتوان احتمال وقوع حمله به هر یک از تجهیزات شبکه برق و همچنین نتایج احتمالی این حمله را با در نظر گرفتن پارامترهایی نظیر عوامل سیاسی، اقتصادی، اجتماعی، فنی و جغرافیایی تعیین کرد. برای این منظور، می‌توان مقدار شاخص ریسک را که از رابطه (۱۶) محاسبه می‌شود، برای همه المان‌های شبکه محاسبه کرد و سپس آن‌ها را به صورت نزولی مرتب کرد. تجهیزاتی که ریسک بالاتری برای شبکه برق در مقابل حملات عامدانه به همراه دارند، نقش حیاتی‌تری برای شبکه ایفا می‌کنند.

$$\kappa^{risk} = P(A)\sum_{k=1}^{4} P_k(C).D_{r_k} \qquad (۱۶)$$

$$D_r = f\left(C_F, C(P_L)\right) \qquad (۱۷)$$

در این روابط، $P(A)$ احتمال حمله به هر یک از تجهیزات شبکه است، $P(C)$ احتمال موفقیت حمله و D_r بیانگر میزان آسیب است. رابطه (۱۷) نشان می‌دهد که میزان آسیب، تابعی است از هزینه تعمیر و یا تعویض تجهیزات (C_F) و هزینه تحمیلی به بارهای شبکه به خاطر قطع بخشی از بار آن‌ها ($C(P_L)$). نکته‌ای که باید به آن دقت کرد این است که مقدار D_r وابسته به «نتیجه حمله» است که چهار حالت «شدت کم»، «نسبتاً شدید»، «شدید» و «فاجعه‌آمیز» برای آن تعریف می‌شود [۸۹]. در واقع، نتیجه حمله بیان می‌کند که اگر به یکی از تجهیزات شبکه حمله شود، نتیجه آن حمله و شدت تأثیر آن بر روی شبکه به چه میزان است. این مقدار وابسته به احتمال حمله به آن تجهیز، ارزش تجهیز و نیز وضعیت شبکه برق در زمان حمله به آن تجهیز است [۸۹].

شاخص دیگری که برای رتبه‌بندی تجهیزات شبکه برق از نظر میزان حیاتی بودن برای شبکه مطرح می‌شود، شاخص میانگی است (BI). BI نیز مشابه CI، مبتنی بر نظریه شبکه‌های پیچیده است، با این تفاوت که ایرادهای وارد به CI را ندارد. CI، اگر چه در شبکه‌هایی نظیر شبکه گسترده جهانی (www)[2] کارکرد خوبی از خود نشان داده است، اما در خصوص شبکه‌های برق، فاصله الکتریکی شین‌ها، ظرفیت خطوط انتقال و اثری که توان تزریقی/ برداشتی هر شین بر فلوی عبوری از هر خط می‌گذارد در این شاخص دیده نشده است و این موضوع از اعتبار نتایج حاصل در دنیای واقعی می‌کاهد [۹۲]. در شبکه برق، حساسیت فلوی عبوری از یک خط نسبت به تزریق/ برداشت توان در یک شین، با فاکتور توزیع انتقال توان (PTDF)[3] محاسبه می‌شود [۲]. این فاکتور نشان می‌دهد که اگر تزریق/برداشت در یک شین به اندازه یک واحد افزایش یابد و در شین کمکی[4] جبران شود، فلوی عبوری از آن خط چقدر تغییر می‌کند (h_{ln}). حال اگر توان تزریقی در یک شین تولید i به اندازه یک واحد افزایش یابد و این توان در شین مصرف j برداشت شود، با استفاده از مدل خطی شبکه برق خواهید داشت:

$$h_l^{ij} = h_{li} - h_{lj} \qquad (۱۸)$$

این فاکتور نشان دهنده میزان تغییر فلوی خط l در اثر تزریق و برداشت در شین‌های، به ترتیب، i و j است. اگر $P_l^{\max}$ بیانگر ظرفیت خط انتقال l باشد، اثر این ظرفیت بر روی حداکثر توان قابل انتقال از شین تولید i به شین مصرف j، با شاخص ظرفیت انتقال C_i^j محاسبه می‌شود [۹۲]:

$$C_i^j = \min_{l\in\Omega^L}\left(\frac{P_l^{\max}}{\left|h_l^{ij}\right|}\right) \qquad (۱۹)$$

به عبارتی، C_i^j بیانگر توانی است که از شین تولید i به شین مصرف j منتقل می‌شود، زمانی که اولین خط انتقال در شبکه به حد ظرفیت خود برسد. با این توضیحات، BI برای شین n به صورت زیر تعریف می‌شود:

$$\kappa_n = \frac{1}{2}\sum_{i\Psi^G}\sum_{j\in\Psi^D} C_i^j \sum_{l\in\Omega^L}\left|h_l^{ij}\right| \qquad (۲۰)$$

و این شاخص برای خط انتقال l به صورت:

$$\kappa_l = \max\left\{\kappa_l^+, \left|\kappa_l^-\right|\right\} \qquad (۲۱)$$

که در آن:

$$\kappa_l^+ = \sum_{i\Psi^G}\sum_{j\in\Psi^D} C_i^j h_l^{ij}, \text{if } h_l^{ij} > 0 \qquad (۲۲)$$

$$\kappa_l^- = \sum_{i\Psi^G}\sum_{j\in\Psi^D} C_i^j h_l^{ij}, \text{if } h_l^{ij} < 0 \qquad (۲۳)$$

BI بیانگر میزان اهمیت یک تجهیز برای شبکه است [۹۲].

آخرین شاخصی که بر اساس نظریه شبکه‌های پیچیده برای رتبه‌بندی تجهیزات شبکه (در این مورد، خطوط انتقال شبکه) تعریف می‌شود، شاخص کوتاه‌ترین مسیر است (SPI) [۹۳ و ۹۴]. در شبکه‌های پیچیده، کوتاه‌ترین مسیر بیانگر کمترین تعداد کمانی است که گره‌های n_1 و n_2 را به هم وصل می‌کند. برای

[1] Bayesian Network
[2] World Wide Web
[3] Power Transfer Distribution Factor
[4] Slack Bus

محاسبه این شاخص در خصوص شبکه‌های برق، ابتدا شبکه برق به صورت یک گراف جهت‌دار مدل می‌شود [۹۴] و سپس به کمان‌های[1] این گراف حمله می‌شود [۹۳]. اگر یک کمان مورد حمله واقع شود، یک ضریب جریمه[2] به طول این کمان اضافه می‌شود. این جریمه آن قدر بزرگ می‌شود تا هیچ کمان تخریب شده‌ای روی کوتاه‌ترین مسیر وجود نداشته باشد.

۳-۲. مسئله مدافع (دفاع)

همان‌طور که پیش‌تر نیز گفته شد، اکثر مدل‌های ارائه شده برای بررسی آسیب‌پذیری شبکه‌های برق، به صورت مدل‌های AD هستند. ماهیت مسئله آسیب‌پذیری (به عنوان یک بازی بین مدافع و مهاجم، از منظر نظریه بازی[3]) به اینگونه است که ابتدا مهاجم حمله می‌کند و پس از آن، مدافع به حملات مهاجم پاسخ می‌دهد. پاسخ مدافع در واقع بهره‌برداری بهینه سامانه است، به گونه‌ای که خسارت ناشی از حملات (که در بخش قبل به تفصیل بیان شد) کمینه شود. بنابراین، تابع هدف مدافع عکس تابع مهاجم است و مسئله دو سطحی حاصل، یک مسئله max-min است. به عنوان مثال، اگر مهاجم بخواهد مطابق (۱) هزینه‌های قطع بار و هزینه‌های تولید را بیشینه کند، اپراتور شبکه باید به گونه‌ای سامانه را بهره‌برداری کند این تابع هدف کمینه شود. مسئله مدافع در این حالت به صورت زیر تعریف می‌شود:

$$Minimize\ (1) \tag{۲۴}$$

مشروط به آنکه:

$$p_l=(1-\delta_l^{Line})\sum_{n\in N}\left[B_l.A_{nl}.\theta_n\right];\quad \forall l\in\Omega^L \tag{۲۵}$$

$$\sum_{i\in\Psi_n^G}\sum_{b\in\Lambda_i^G}g_{ib}+\sum_{j\in\Psi_n^D}\sum_{a\in\Lambda_j^D}s_{ja} -\sum_{l\in\Omega^L}\left[A_{nl}.p_l\right]=\sum_{j\in\Psi_n^D}\sum_{a\in\Lambda_j^D}D_{ja}^{\max};\forall n\in N \tag{۲۶}$$

$$-P_l^{\max}(1-\delta_l^{Line})\le p_l\le P_l^{\max}(1-\delta_l^{Line});\quad \forall l\in\Omega^L \tag{۲۷}$$

$$-\pi\le\theta_n\le\pi;\forall n\in N\setminus n:\hat{n} \tag{۲۸}$$

$$\theta_n=0;\quad n:\hat{n} \tag{۲۹}$$

$$G_{ib}^{\min}\le g_{ib}\le G_{ib}^{\max};\forall i\in\Omega^G,\forall b\in\Lambda_i^G \tag{۳۰}$$

$$0\le s_{ja}\le D_{ja}^{\max};\quad \forall j\in\Omega^D,\forall a\in\Lambda_j^D \tag{۳۱}$$

رابطه‌های (۳۱-۲۴) در واقع بیانگر یک نسخه اصلاح شده از پخش توان اقتصادی جریان مستقیم (DCOPF)[4] است که در آن:

- هزینه قطع بار نیز به تابع هدف اضافه شده است (قید(۲۴)،
- فلوی عبوری از خط انتقالی که به آن حمله شده است، صفر است (قیود (۲۵) و (۲۷)) و
- برای محاسبه مقدار قطع بار در هر شین (قید (۳۱))، یک ژنراتور مجازی در آن شین در نظر گرفته شده است که تنها مسئولیت تولید بار قطع شده را دارد [۴۵].

اگر خط انتقال l مورد حمله قرار بگیرد ($\delta_l^{Line}=1$)، آنگاه عبارت $(1-\delta_l^{Line})$ در (۲۵) به اجبار مقدار فلوی عبوری از آن را صفر می‌کند. در مرجع [۵۲]، عبارت زمان به همه رابطه‌های (۳۱-۲۴) اضافه شده است. در مراجعی که حمله به شین‌ها، پست‌ها، خطوط موازی و ژنراتورها نیز در نظر گرفته شده است [۱۴، ۱۵، ۴۷-۴۴، ۸۳ و ۹۶]، قیود مرتبط با فلوی عبوری از خطوط انتقال و ظرفیت آن‌ها، و نیز قید مربوط به ظرفیت ژنراتورها به صورت زیر فرمول‌بندی شده است:

$$p_l=\left(1-\delta_l^{Line}\right)\left(1-\delta_{o(l)}^{Bus}\right)\left(1-\delta_{d(l)}^{Bus}\right)\prod_{s|l\in\Psi_s^L}\left(1-\delta_s^{Sub}\right) \prod_{l'|l'\in\Lambda_l^{Par}}\left(1-\delta_{l'}^{Line}\right)\sum_{n\in\Omega^N}\left[B_l.A_{nl}.\theta_n\right];\quad \forall l\in\Omega^L \tag{۳۲}$$

$$-P_l^{\max}\left(1-\delta_l^{Line}\right)\left(1-\delta_{o(l)}^{Bus}\right)\left(1-\delta_{d(l)}^{Bus}\right)\prod_{s|l\in\Psi_s^L}\left(1-\delta_s^{Sub}\right) \prod_{l'|l'\in\Lambda_l^{Par}}\left(1-\delta_{l'}^{Line}\right)\le p_l\le P_l^{\max}\left(1-\delta_l^{Line}\right)\left(1-\delta_{o(l)}^{Bus}\right) \left(1-\delta_{d(l)}^{Bus}\right)\prod_{s|l\in\Psi_s^L}\left(1-\delta_s^{Sub}\right)\prod_{l'|l'\in\Lambda_l^{Par}}\left(1-\delta_{l'}^{Line}\right);\ \forall l\in\Omega^L \tag{۳۳}$$

$$G_{ib}^{\min}\left(1-\delta_i^{Gen}\right)\left(1-\delta_{n(i)}^{Bus}\right)\le g_{ib}\le \left(1-\delta_i^{Gen}\right)\left(1-\delta_{n(i)}^{Bus}\right)G_{ib}^{\max};\forall i\in\Omega^G,\forall b\in\Lambda_i^G \tag{۳۴}$$

به عنوان مثال، قید (۳۲) بیان می‌کند که فلوی عبوری از خط انتقال l در سه حالت به اجبار صفر می‌شود:

۱- به خود خط، یا یکی از شین‌های ابتدایی و انتهایی آن حمله شود (به ترتیب، $\delta_l^{Line}=1$، $\delta_{o(l)}^{Bus}=1$ و $\delta_{d(l)}^{Bus}=1$)،

۲- یکی از پست‌هایی که این خط به آن وصل می‌شود مورد حمله قرار گیرد ($\prod_{s|l\in\Psi_s^L}\left(1-\delta_s^{Sub}\right)=1$) و یا

۳- به یک خط موازی آن حمله شود ($\prod_{l'|l'\in\Lambda_l^{Par}}\left(1-\delta_{l'}^{Line}\right)=1$).

ممکن است مدافع شبکه سرمایه‌گذاری در شبکه برق را به گونه‌ای انجام دهد که هزینه‌های پس از حمله کمینه شود [۱۴]. این هزینه‌ها شامل هزینه تولید، هزینه بار قطع شده، هزینه تعمیرات برای ترانسفورمرهای بدون یدک و هزینه جایگزینی ترانسفورمرهای یدکی می‌شود [۱۴]. این تصمیم‌گیری، قبل از

[1] Arcs
[2] Penalty Factor
[3] Game Theory
[4] Direct Current Optimal Power Flow

حمله[1] صورت می‌گیرد. در مسئله مهاجم، مهاجم به تصمیم‌گیری بهینه در خصوص انتخاب بهترین راهبُرد حمله می‌پردازد و می‌داند که بهره‌بردار شبکه، شبکه را به گونه‌ای بهره‌برداری می‌کند تا هزینه‌های بهره‌برداری پس از حمله کمینه شود. در این مدل، برای فرآیند تعمیر[2] تجهیزات، چهار مرحله در نظر گرفته شده است [۱۴]؛ در مرحله اول، تمام تجهیزاتی که مورد حمله واقع شده‌اند و نیز آن دسته از المان‌هایی که عملکردشان وابسته به این تجهیزات است، هیچ فلویی از آن‌ها عبور نمی‌کند. در مرحله دوم، تنها آن دسته از خطوطی که به پست‌های تخریب شده متصل هستند از مدار خارج می‌مانند و بقیه خطوط تعمیر می‌شوند و می‌توانند انرژی حمل کنند. در مرحله سوم، تمام تجهیزات پست‌های تخریب شده، به جز ترانسفورمرها، تعمیر می‌شوند. در مرحله چهارم (مرحله نهایی)، فرض می‌شود که ترانسفورمرهای یدکی نصب می‌شوند. برای تخمین فلوی عبوری از المان‌های شبکه، از DCOPT در هر یک از چهار مرحله بیان شده استفاده شده است. این پخش توان‌ها با تابع هدف کمینه کردن هزینه تولید، هزینه بار قطع شده و هزینه جایگزینی ترانسفورمرهای یدکی اجرا می‌شوند که در رابطه ۰ آورده شده است [۱۴].

$$\begin{aligned} &Minimize\ \ F_L(\delta^{Gen},\delta^{Line},\delta^{Sub},y^{Gen},y^{Line},\gamma^D)= \\ &\sum_{k=1,2,3,4}\left(\sum_{n\in\Omega^N}\alpha_n\Delta P_n^{d^k}+\sum_{i\in\Omega^G}C_i^G g_i^k\right)(\omega_k-\omega_{k-1}) \\ &+\sum_{s\in S}\sum_{n_1\in\Psi_s^N}\sum_{(n_1,n_2)\in(\Omega^L\cup\Omega^E)}\sum_{e\in\Omega^E}C_{n_1}^E\left(1-r_{n_1n_2e}\right)Q_{n_1n_2e}\delta_s^S \end{aligned} \qquad (۳۵)$$

نکته مهمی که در این مرجع 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 [۱۴]. 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.

۴. چالش‌ها و روش‌های حل

همواره بحث آسیب‌پذیری شبکه برق با چند چالش روبه‌رو بوده است. یکی از این چالش‌ها شامل مدل‌سازی دقیق مهاجم است [۱۹، ۹۷ و ۹۸]. همان‌طور که پیش‌تر نیز گفته شد، کاربر نهایی مدل‌های AD، برنامه‌ریز شبکه است و در واقع، در استفاده از یک مدل AD، برنامه‌ریز شبکه به مدل‌سازی مهاجم پرداخته و از منظر مهاجم به شبکه نگاه می‌کند. بنابراین، مدلی که برای مهاجم استفاده می‌شود، تخمینی است از رفتار مهاجم در دنیای واقعی که الزاماً نمی‌تواند دقیق باشد [۱۹، ۴۵ و ۵۲]. ترکیبی از تابع هدف‌های مختلف که در این مقاله بررسی شد، می‌تواند ابزار بسیار مفیدی برای برنامه‌ریز شبکه فراهم کند تا مدل‌سازی مسئله را هر چه بیشتر به دنیای واقعی نزدیک کند. چالش دیگری که در ادامه چالش اول است، تخمین منابع مهاجم است. همان‌طور که دیده شد، مهم‌ترین قیدی که برای مهاجم در نظر گرفته می‌شود، قید محدودیت منابع است که به صورت محدودیت تعداد افراد در دسترس مدل می‌شود (رابطه‌های (۳ و ۷)). حداکثر مقداری که برای منابع مهاجم در نظر گرفته می‌شود چقدر است؟ در پاسخ به این سؤال، دو راهکار در نظر گرفته شده است؛ در راهکار اول، می‌توان یک مدل AD را برای تعداد دفعات زیاد، به ازای مقادیر مختلف برای منابع مهاجم اجرا کرد و آن دسته از المان‌هایی که در اکثر اجراها به عنوان المان‌های حیاتی شناخته می‌شوند را المان‌های آسیب‌پذیر نامید [۱۱، ۴۷، ۴۸، ۵۲ و ۵۴]. در راهکار دوم، برخی محققین به مدل‌سازی احتمالاتی مهاجم پرداخته‌اند و عدم قطعیت‌های مختلفی که در خصوص مهاجم وجود دارد را به صورت احتمالاتی و مبتنی بر سناریو[3]، و یا بررسی اطلاعات پیشین در خصوص عملکرد مهاجمان در یک منطقه تحت مطالعه، مدل‌سازی کرده‌اند [۱۳، ۱۸، ۳۱، ۸۲، ۸۹، ۹۰، ۹۳، ۹۴، ۹۹ و ۱۰۰]. به عنوان مثال، می‌توان حملات احتمالی را به صورت مجموعه‌ای از سناریوها (V) در نظر گرفت [۱۳]. برای تولید تعداد υ_V سناریو می‌توان از یک مدل حمله استفاده کرد [۴۵، ۴۷ و ۴۸] و با طی روند تکراری زیر، مجموعه سناریوهای حملات را تعیین کرد [۱۳]:

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

مرحله ۲) حل مدل مهاجم و محاسبه نقشه حمله بهینه ν^* و میزان قطع بار بهینه S_T^* به ازای υ_A و Ω_{υ_A} مدل حمله مورد استفاده است. این مدل باید به گونه‌ای اصلاح شود که نقشه‌های حمله‌ای که قبلاً در Ω_{υ_A} مورد بررسی قرار گرفته‌اند، به عنوان نقشه حمله بهینه بازگردانده نشوند.

مرحله ۳) حل مدل مهاجم و محاسبه نقشه حمله بهینه ν^* و میزان قطع بار بهینه S_T^* به ازای υ_A و Ω_{υ_A} مدل حمله مورد استفاده است. این مدل باید به گونه‌ای اصلاح شود که نقشه‌های حمله‌ای که قبلاً در Ω_{υ_A} مورد بررسی قرار گرفته‌اند، به عنوان نقشه حمله بهینه بازگردانده نشوند.

مرحله ۴) به‌روزرسانی مقادیر به صورت زیر:

[1] Pre-Attack
[2] Repair
[3] Scenario-Based

$$If\ s_T^* > s_{\upsilon_A - 1}$$
$$\{\Omega_{\upsilon_A}, v^*\} \to \Omega_{\upsilon_A} \quad , \quad \upsilon_S = \upsilon_S + 1$$
$$s_{\upsilon_A} = \max\{s_T^*, s_{\upsilon_A}\}$$
$$Else$$
$$\{\Omega, \Omega_{\upsilon_A}\} \to \Omega \quad , \quad \Omega_{\upsilon_A} = \phi$$
$$\upsilon_A = \upsilon_A + 1 \quad , \quad s_{\upsilon_A} = s_{\upsilon_A - 1}$$

مرحله ۵) اگر $\upsilon_S < \upsilon_V$، آنگاه باید به مرحله (۲) برگشت، در غیر این صورت، الگوریتم تولید سناریو پایان می‌یابد.

جدول ۱. مقادیر اولیه برای شروع فرآیند تولید سناریو [۱۳]

پارامتر/متغیر/مجموعه	تعریف	مقدار
υ_A	تعداد خطوط تحت حمله	۱
υ_S	تعداد سناریوها	۰
Ω_{υ_A}	سناریوهای با υ_A خط تحت حمله	ϕ
Ω	مجموعه سناریوها	ϕ
s_0	مقدار قطع بار بدون حمله	۰
s_{υ_A}	حداکثر قطع بار با υ_A خط تحت حمله	۰

در مرحله (۳)، اگر مقدار قطع بار بهینه s_T^* بیش از مقدار بهینه قطع بار حاصل از تخریب $\upsilon_A - 1$ خط باشد، آنگاه v^* به عنوان یک سناریو در نظر گرفته می‌شود. در غیر این صورت، غیر ممکن است که بتوان با υ_A حمله، نقشه‌ای یافت که میزان قطع بار آن بیش از $s_{\upsilon_A - 1}$ باشد. بنابراین، جست‌وجو برای نقشه‌های حمله به ازای υ_A پایان می‌یابد و مجموعه سناریوها و υ_A به‌روز می‌شوند. در این مدل، احتمال هر سناریو با توجه به دو موضوع تعیین می‌شود؛ احتمال وقوع حمله v متناسب با $s_T(V)$ است و با تعداد خطوطی که در آن حمله تخریب می‌شوند ($I(v)$)، تناسب عکس دارد. این دو موضوع در رابطه زیر لحاظ شده‌اند [۱۳]:

$$\pi(v) = \frac{\frac{s_T(v)}{I(v)}}{\sum_{v'=1}^{\upsilon_V} \frac{s_T(v')}{I(v')}} \qquad v = 1,2,\ldots,\upsilon_V \qquad (۳۶)$$

چالش سومی که پیش روی مدل‌های ارائه شده برای آسیب‌پذیری شبکه برق وجود دارد، حل ریاضی آن‌ها است. طبیعت تصمیم‌گیری در بازی بین مهاجم و مدافع، به صورت «آری یا خیر» است که اینگونه تصمیم‌گیری با استفاده از متغیرهای باینری[1] مدل‌سازی می‌شود. حل یک مدل برنامه‌ریزی مختلط با عدد صحیح[2] برای شبکه‌های مقیاس بزرگ[3] در دنیای واقعی مشکل است. در یک مدل AD، برای هر المان شبکه یک متغیر باینری حمله در نظر گرفته می‌شود. به علاوه، اگر عبارت زمان نیز در نظر گرفته شود، علاوه بر اینکه تعداد متغیرهای باینری حمله در تعداد دوره‌های زمانی[4] افق مطالعه ضرب می‌شوند، برای هر المان شبکه باید متغیر باینری تعمیرات نیز در نظر گرفته شود. این مشکل زمانی برجسته‌تر می‌شود که مدل ارائه شده غیر خطی باشد. تاکنون الگوریتمی ارائه نشده است که تضمین کند جواب بهینه سراسری[5] مربوط به یک مدل غیر خطی مختلط با عدد صحیح (MINLP)[6] را به‌دست آورد. از سوی دیگر، به خاطر حساسیت بسیار زیاد مسئله آسیب‌پذیری شبکه برق و هزینه‌های بسیار سنگینی که برای افزایش تاب‌آوری شبکه، به یک کشور تحمیل می‌شود، نمی‌توان تصمیم‌گیری را مبتنی بر جواب‌های بهینه محلی[7] انجام داد، مگر اینکه الگوریتم حل قادر باشد تا شاخصی از فاصله بین جواب بهینه محلی به‌دست آمده و جواب بهینه سراسری ارائه دهد.

الگوریتم‌هایی نظیر الگوریتم شاخه و برش (BAC)[8]، شاخه و کران (BAB)[9] و نسخه‌هایی از روش تجزیه بندرز (BD)[10] می‌توانند چنین شاخصی را به‌دست دهند. نکته‌ای که باید به آن دقت کرد این است که اگر چه مدل‌هایی که به صورت برنامه‌ریزی خطی مختلط با عدد صحیح (MILP)[11] ارائه می‌شوند، می‌توانند جواب بهینه سراسری را به‌دست آورند، اما در کاربرد واقعی برای شبکه‌های بزرگ، به ناچار باید از روش‌های حل تقریبی نظیر تجزیه بندرز و یا الگوریتم‌های فرا ابتکاری نظیر الگوریتم ژنتیک (GA)[12]، بهینه‌سازی تجمع ذرات (PSO)[13] و یا روش‌های ترکیبی[14] استفاده کرد. جدول (۲) دسته‌بندی مناسبی از نوع مدل‌سازی و الگوریتم حل استفاده شده در گزارش‌های مختلف ارائه می‌دهد.

[1] Binary Variables
[2] Mixed-Integer Programming
[3] Large-Scale Networks
[4] Time Periods
[5] Global Optimal Solution
[6] Mixed-Integer Non-Linear Programming
[7] Local Optimal Solutions
[8] Branch and Cut
[9] Branch and Bound
[10] Benders Decomposition
[11] Mixed-Integer Linear Programming
[12] Genetic Algorithm
[13] Particle-Swarm Optimization
[14] Hybrid

جدول ۲. دسته‌بندی مدل‌ها بر اساس مدل‌سازی و روش حل

مدل‌سازی / روش حل	MILP	MINLP	NLP[1]	LP
BAB یا BAC	[۱، ۱۱، ۱۳، ۱۹، ۴۷، ۴۸، ۵۲ و ۹۴]			
BD	[۱۵، ۱۶ و ۹۳]	[۴۴-۴۶، ۸۳ و ۹۹]		
GA		[۵۴]		
PSO		[۱۸]		
GSA[2]		[۳۴]		
MCS[3]			[۷۴ و ۷۸]	
Hybrid		[۱۴ و ۵۳]	[۲۹ و ۹۰]	
Simplex				[۴۹]
تکراری	[۵۷، ۸۰، ۸۲، ۹۶ و ۱۰۱]	[۱۲ و ۷۷]	[۳۱، ۵۰، ۵۵، ۵۶، ۶۴، ۶۹-۷۳، ۷۵، ۸۵، ۸۶، ۸۸، ۸۹، ۹۲ و ۹۵]	

۵. نتیجه‌گیری

در این مقاله مرور کاملی بر مدل‌های ارائه شده برای بررسی آسیب‌پذیری شبکه‌های برق انجام شد. در ابتدا، رویکردهایی که در خصوص بررسی آسیب‌پذیری شبکه برق وجود دارد به تفصیل بیان شد. این رویکردها شامل بررسی آسیب‌پذیری شبکه برق در مقابل حملات سایبری، حملات فیزیکی، حملات سایبری-فیزیکی، وابستگی به سایر زیرساخت‌ها (به ویژه شبکه گاز) و خروج‌های متوالی که منجر به خاموشی سراسری شبکه می‌شود، می‌گردد. پس از بیان رویکردها، با ارائه یک دسته‌بندی مناسب، مراجع مختلف از منظر رویکردی که برای بررسی آسیب‌پذیری شبکه برق انتخاب کرده‌اند، در دسته‌های مختلف قرار گرفتند.

در ادامه مقاله، با تمرکز بر مقالاتی که به بررسی آسیب‌پذیری فیزیکی و یا سایبری-فیزیکی شبکه‌های برق پرداخته‌اند، مسئله مهاجم و مدافع شبکه برق به طور کامل و با بیان روابط ریاضی نمونه، تشریح شدند. در توضیح مسئله مهاجم، شاخص‌های مختلفی که در مراجع مورد مطالعه به عنوان «خسارت» در نظر شده‌اند، به تفکیک بیان شدند و روابط ریاضی آن‌ها ارائه شد. این شاخص‌ها شامل هزینه (یا میزان) بار یا انرژی قطع شده، هزینه تولید، مدت زمان بازیابی سامانه، بار توزیع شده بر روی خطوط انتقال شبکه، خاموشی سراسری شبکه، حد پایداری شبکه، هزینه‌های مرتبط با تعمیرات ترانسفورمرهای بدون یدک و هزینه جایگزینی ترانسفورمرهای یدکی می‌شود. پس از بیان مسئله مهاجم، مسئله مدافع (برنامه‌ریز شبکه برق) به تفصیل مورد بررسی قرار گرفت و روابط ریاضی نمونه برای تابع هدف و قیودی که مدافع شبکه با آن‌ها روبه‌رو است ارائه شد.

پس از بیان مسئله مهاجم و مدافع، به چالش‌های موجود در بحث بررسی آسیب‌پذیری شبکه برق پرداخته شد. در مراجع مختلف، چالش‌های متفاوت همراه با راهکارهای گوناگون برای رفع این چالش‌ها ارائه شده است. مهم‌ترین چالش‌هایی که یک برنامه‌ریز شبکه برق در بررسی آسیب‌پذیری شبکه با آن‌ها روبه‌رو است، شامل پیش‌بینی و مدل‌سازی دقیق رفتار مهاجمان در دنیای واقعی، تخمین صحیح مقدار منابع مهاجم، حل دقیق ریاضی و به‌دست آوردن جواب‌های قابل اتکا در کاربرد واقعی یک مدل ارائه شده برای بررسی آسیب‌پذیری شبکه برق، می‌شود. راهکارهای گوناگونی که مراجع مختلف برای برخورد با این چالش‌ها ارائه داده‌اند، در این مقاله تشریح شد.

در آخر، مدل‌های ارائه شده، از منظر مدل‌سازی و روش حل مسئله مورد بررسی قرار گرفتند. در یک دسته‌بندی مناسب، مدل‌های ارائه شده در گزارش‌های مختلف، از نظر نوع مدل‌سازی و روش حل مسئله در دسته‌های متفاوتی قرار گرفتند. پوشش کامل این مقاله می‌تواند ابزاری بسیار قدرتمند در اختیار برنامه‌ریزان و مدافعان شبکه‌های برق قرار دهد تا بتوانند با رویکردهای مختلف در بررسی آسیب‌پذیری شبکه برق، چالش‌ها، قیود مختلف پیش رو، تابع هدف‌های مختلفی که مهاجمان ممکن است انتخاب کنند و نیز روش‌های حل مسئله در مقیاس بزرگ، آشنا شوند و بهترین، کامل‌ترین و مطمئن‌ترین شیوه را در بررسی آسیب‌پذیری شبکه برق انتخاب کنند.

۶. فهرست علائم و نمادها

فهرست مجموعه‌ها، ثابت‌ها و متغیرهای استفاده شده در این مقاله در این بخش ارائه شده است. در این فهرست، از تکرار مواردی که در متن تعریف شده‌اند خودداری شده است.

۶-۱. مجموعه‌ها

T	دوره مطالعه.
V	مجموعه سناریوهای حمله.
Φ^D	مجموعه شین‌های بار شبکه.
Φ^G	مجموعه شین‌های ژنراتوری شبکه.
Λ_j^D	مجموعه بلوک‌های بار j.
Λ_i^G	مجموعه بلوک‌های ژنراتور i.
Λ_l^{Par}	مجموعه خطوط موازی با خط l.

[1] Non-Linear Programming
[2] Gravitational Search Algorithm
[3] Monte-Carlo Simulation

Ω^D مجموعه بارهای شبکه.

Ω^E مجموعه ترانسفورمرهای شبکه.

Ω^G مجموعه ژنراتورهای شبکه.

Ω^L مجموعه خطوط انتقال شبکه.

Ω^N مجموعه شین‌های شبکه.

O_s مجموعه شین‌های موجود در پست s.

Ω^S مجموعه پست‌های شبکه.

Ψ_n^G مجموعه ژنراتورهای متصل به شین n.

Ψ_n^D مجموعه بارهای متصل به شین n.

Ψ_s^L مجموعه خطوط متصل به پست s.

Ψ_s^N مجموعه شین‌های موجود در پست s.

۶-۲. ثابت‌ها

A_{nl} درایه (n,l) مربوط به ماتریس تلاقی شبکه (در صورتی که شین n سمت ارسال خط l باشد، ۱، در صورتی که سمت دریافت آن باشد، ۱- و در غیر این صورت صفر است). $d(l)$ و $o(l)$، به ترتیب، بیانگر شین‌های انتها و ابتدای خط l هستند.

B_l عکس راکتانس خط l.

C_e^E هزینه جایگزینی ترانسفورمر e که مورد حمله قرار گرفته است.

$C_{ib}^G(t)$ هزینه تولید مربوط به بلوک bام مربوط به ژنراتور iام در زمان t (t در صورت نیاز حذف می‌شود).

$C_{ja}^C(t)$ هزینه قطع بار مربوط به بلوک aام مربوط به بار jام در زمان t (t در صورت نیاز حذف می‌شود).

$D_{ja}^{\max}(t)$ توان بلوک a مربوط به بار j در زمان t (t در صورت نیاز حذف می‌شود).

E_{ij} رخداد پایه j ام مربوط به زنجیره خطای i ام.

$\overline{E_i}$ زنجیره خطای i ام.

$G_{ib}^{\max}$ حداکثر توان تولیدی بلوک b ژنراتور i.

$G_{ib}^{\min}$ حداقل توان تولیدی بلوک b ژنراتور i.

$\hat{n}$ شین مرجع.

p_l^* حد امنیت خط انتقال l.

$Q_{n_1n_2e}$ تعداد سناریوهای حمله.

$Q_{n_1n_2e}$ پارامتر خط و ترانسفورمر (اگر صفر باشد به معنی این است که شاخه n_1n_2 یک خط انتقال است و اگر یک باشد، ترانسفورمر).

R_i^{Gen} تعداد افراد لازم برای حمله به ژنراتور i.

R_l^{Line} تعداد افراد لازم برای حمله به خط انتقال l.

R_n^{Bus} تعداد افراد لازم برای حمله به شین n.

R_s^{Sub} تعداد افراد لازم برای حمله به پست s.

R_T کل افراد مهاجم در افق زمانی T.

$R(t)$ کل افراد در دسترس مهاجم در بازه زمانی t.

S^* مقدار از پیش تعیین شده برای میزان قطع بار شبکه

W_l تعداد بازه‌های زمانی لازم برای انجام تعمیرات اجباری خط l.

$Z_l^{\max}$ حداکثر تعداد حملاتی که می‌تواند بر روی خط l در افق زمانی T صورت گیرد.

υ_v تعداد سناریوهای حمله.

ω_k مدت زمان لازم برای کامل شدن مرحله kام تعمیرات.

α_n هزینه قطع بار در شین n.

π_v احتمال وقوع سناریوی حمله v.

۶-۳. متغیرها

$g_{ib}(t)$ توان تولیدی مربوط به بلوک b مربوط به ژنراتور i در زمان t (t در صورت نیاز حذف می‌شود).

$p_l(t)$ فلوی عبوری از خط انتقال l در زمان t (t در صورت نیاز حذف می‌شود).

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

$s_{ib}(t)$ میزان قطع بار مربوط به بلوک a مربوط به بار j در زمان t (t در صورت نیاز حذف می‌شود).

$x_l(t)$ متغیر باینری تعمیرات خط l (اگر برابر با یک باشد به معنی این است که خط تحت تعمیر است).

y^{Gen} بردار شامل متغیرهای عدد صحیح توسعه ژنراتور (y_i^{Gen} اشاره به افزایش P_i^{Gen} واحد ظرفیت به ظرفیت ژنراتور i می‌کند).

y^{Line} بردار شامل متغیرهای عدد صحیح توسعه خط (y^l اشاره به افزایش P_l^{Line} واحد ظرفیت به ظرفیت خط انتقال l می‌کند).

z_l تعداد حملات صورت گرفته بر روی خط l در افق مطالعه T.

Δp_l میزان تغییر واقعی ایجاد شده در فلوی اندازه‌گیری شده مربوط به خط l پس از وقوع تمام حملات.

$\delta_n^{Bus}(t)$ متغیر باینری حمله به شین n در زمان t (اگر برابر با یک باشد به معنی این است که شین n در زمان t مورد حمله قرار گرفته است). اندیس t در صورت نیاز

حذف می‌شود. δ^{Bus} بیانگر بردار شامل متغیر حمله همه شین‌ها است.

$\delta_i^{Gen}(t)$ متغیر باینری حمله به ژنراتور i در زمان t (اگر برابر با یک باشد به معنی این است که ژنراتور i در زمان t مورد حمله قرار گرفته است). اندیس t در صورت نیاز حذف می‌شود. δ^{Gen} بیانگر بردار شامل متغیر حمله همه ژنراتور است.

$\delta_l^{Line}(t)$ متغیر باینری حمله به خط l در زمان t (اگر برابر با یک باشد به معنی این است که خط l در زمان t مورد حمله قرار گرفته است). اندیس t در صورت نیاز حذف می‌شود. δ^{Line} بیانگر بردار شامل متغیر حمله همه خط‌ها است.

$\delta_s^{Sub}(t)$ متغیر باینری حمله به پست s در زمان t (اگر برابر با یک باشد به معنی این است که پست s در زمان t مورد حمله قرار گرفته است). اندیس t در صورت نیاز حذف می‌شود. δ^{Sub} بیانگر بردار شامل متغیر حمله همه پست‌ها است.

κ_n^{bet} شاخص میانگی برای شین n.

κ^{cent} شاخص مرکزیت (CI).

κ^{inst} شاخص ناپایداری شبکه.

κ^{risk} شاخص ریسک (RI).

$\theta_n(t)$ زاویه ولتاژ شین n در زمان t (t در صورت نیاز حذف می‌شود).

γ^D بردار شامل متغیرهای عدد صحیح خرید ترانسفورمر (γ_e^D اشاره به تعداد ترانسفورمرهای خریداری شده از نوع e می‌کند).

۷. مراجع

[1] Alguacil, N.; Delgadillo, A.; Arroyo, J. M. "A Trilevel Programming Approach for Electric Grid Defense Planning"; Comput. Oper. Res. 2014, 41, 282–290.

[1] Wood, A. J.; Wollenberg, B. F. "Power Generation, Operation, and Control"; 3rd ed. John Wiley & Sons; 2012.

[2] Ren, H. ; Dobson, I.; Carreras, B. A. "Long-Term Effect of the N-1 Criterion on Cascading Line Outages in an Evolving Power Transmission Grid"; IEEE Trans. Power Syst. 2008, 23, 1217–1225.

[3] Smith, J. F. "Critical Infrastructures at Risk: Securing the European Electric Power System"; Berkeley Electronic Press, USA, 2008.

[4] Andersson, G.; Donalek, P.; Farmer, R.; Hatziargyriou, N.; Kamwa, I.; Kundur, P.; Martins, N.; Paserba, J.; Pourbeik, P.; Sanchez-Gasca, J. "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance"; IEEE Trans. Power Syst. 2005, 20, 1922–1928.

[5] Larsson, S.; Ek, E. "The Black-Out in Southern Sweden and Eastern Denmark, September 23, 2003"; IEEE PES Power Syst. Conf. and Exposition 2004, 309-313.

[6] Berizzi, A. "The Italian 2003 Blackout"; Power Eng. Society General Meeting, 2004, 2, 1673–1679.

[7] Makarov, Y. V.; Reshetov, V. I.; Stroev, V. A.; Voropai, N. I. "Blackouts in North America and Europe: Analysis and Generalization"; IEEE Power Tech. 2005, 1–7.

[8] Van der Vleuten, E.; Lagendijk, V. "Transnational Infrastructure Vulnerability: the Historical Shaping of the 2006 European Blackout"; Energy Policy 2010, 38, 2042–2052.

[9] Anagnostatos, S. D.; Halevidis, C. D.; Polykrati, A. D.; Bourkas, P. D.; Karagiannopoulos, C. G. "Examination of the 2006 Blackout in Kefallonia Island, Greece"; Int. J. Electr. Power Energy Syst. 2013, 49, 122–127.

[10] Arroyo, J. M. "Bilevel Programming Applied to Power System Vulnerability Analysis under Multiple Contingencies"; IET Gener. Transm. Distrib. 2010, 4, 178–190.

[11] Rocco, C. M.; Ramirez-Marquez, J. E.; Salazar, D. E.; Yajure, C. "Assessing the Vulnerability of a Power System through a Multiple Objective Contingency Screening Approach"; IEEE Trans. Reliab. 2011, 60, 394–403.

[12] Carrión, M.; Arroyo, J. M.; Alguacil, N. "Vulnerability-Constrained Transmission Expansion Planning: A Stochastic Programming Approach"; IEEE Trans. Power Syst. 2007, 22, 1436–1445.

[13] Romero, N.; Xu, N.; Nozick, L. K.; Dobson, I.; Jones, D.; Parameters, A. M. "Investment Planning for Electric Power Systems under Terrorist Threat"; IEEE Trans. Power Syst. 2012, 27, 108–116.

[14] Salmeron, J.; Wood, K.; Baldick, R. "Optimizing Electric Grid Design under Asymmetric Threat (II)"; Naval Postgraduate School, California, 2004.

[15] Salmeron, J.; Wood, K. "Homeland Security Research and Technology Proposal (Optimizing Electric Grid Design under Asymmetric Threat)"; Naval Postgraduate School, California, 2002.

[16] Murray, A. T.; Grubesic, T. H. "Critical Infrastructure Protection: the Vulnerability Conundrum"; Telemat. Informatics 2012, 29, 56–65.

[17] Gaffarpour, R.; Hashemi, Y.; Ehsan, M. "Involving Defensive Approach in Unit Commitment Scheduling and Presenting Probability Model of Plants Inaccessibility"; Advanced Defence Sci. & Tech. 2015, 5, 231–246 (In Persian).

[18] Brown, G.; Carlyle, M.; Salmerón, J.; Wood, K. "Defending Critical Infrastructure"; Interfaces 2006, 36, 530–544.

[19] Chertoff, M. "National Infrastructure Protection Plan"; Department of Homeland Security (DHS), Washington DC, 2009.

[20] Bush, G. W. "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets"; Department of Homeland Security, USA, 2003.

[21] Watts, D. "Security and Vulnerability in Electric Power Systems"; 35th North American Power Symposium 2003, 559–566.

[22] Foster Jr, J. S.; Gjelde, E.; Graham, W. R.; Hermann, R. J.; Kluepfel, H. M.; Lawson, R. L.; Soper, G. K.; Wood Jr, L. L.; Woodard, J. B. "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume 1: Executive Report"; Department of Homeland Security, USA, 2004.

[41] Xie, L.; Mo, Y.; Sinopoli, B. "Integrity Data Attacks in Power Market Operations"; IEEE Trans. Smart Grid, 2011, 2, 659–666.

[42] Kosut, O.; Jia, L.; Thomas, R. J.; Tong, L. "On Malicious Data Attacks on Power System State Estimation"; 45th Int. Universities Power Eng. Conf. 2010, 1–6.

[43] Salmeron, J.; Wood, K.; Baldick, R. "Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids"; IEEE Trans. Power Syst. 2009, 24, 96–104.

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

[45] Salmeron J.; Wood, R. K. "The Value of Recovery Transformers in Protecting an Electric Transmission Grid against Attack"; IEEE Trans. Power Syst. 2015, 30, 2396–2403.

[46] Motto, A. L.; Arroyo, J. M.; Galiana, F. D. "A Mixed-Integer LP Procedure for the Analysis of Electric Grid Security under Disruptive Threat"; IEEE Trans. Power Syst. 2005, 20, 1357–1365.

[47] Arroyo, J. M.; Galiana, F. D. "On the Solution of the Bilevel Programming Formulation of the Terrorist Threat Problem"; IEEE Trans. Power Syst. 2005, 20, 789–797.

[48] Cheng, M. X.; Crow, M.; Ye, Q. "A Game Theory Approach to Vulnerability Analysis: Integrating Power Flows with Topological Analysis"; Int. J. Electr. Power & Energy Syst. 2016, 82, 29–36.

[49] Chen, G.; Dong, Z. Y.; Hill, D. J.; Zhang, G. H. "An Improved Model for Structural Vulnerability Analysis of Power Networks"; Phys. A Stat. Mech. its Appl. 2009, 388, 4259–4266.

[50] Chen, G.; Dong, Z. Y.; Hill, D. J.; Zhang, G. H.; Hua, K. Q. "Attack Structural Vulnerability of Power Grids: A Hybrid Approach Based on Complex Networks"; Phys. A: Stat. Mech. its Appl. 2010, 389, 595–603.

[51] Sayyadipour, S.; Yousefi, G. R.; Latify, M. A. "Mid-Term Vulnerability Analysis of Power Systems under Intentional Attacks"; IET Gener. Transm. Distrib. 2016, 10, 3745-3755.

[52] Bier, V. M.; Gratz, E. R.; Haphuriwat, N. J.; Magua, W.; Wierzbicki, K. R. "Methodology for Identifying Near-Optimal Interdiction Strategies for a Power Transmission System"; Reliab. Eng. Syst. Saf. 2007, 92, 1155–1161.

[53] Arroyo, J. M.; Fernández, F. J. "A Genetic Algorithm Approach for the Analysis of Electric Grid Interdiction with Line Switching"; 15th Int. Conf. Intelligent Syst. Applications to Power Syst. 2009, 1–6.

[54] Dwivedi, A.; Yu, X. "A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis"; IEEE Trans. Ind. Informatics 2013, 9, 81–88.

[55] Dwivedi, A.; Yu, X.; Sokolowski, P. "Identifying Vulnerable Lines in a Power Network Using Complex Network Theory"; IEEE Int. Symposium on Industrial Electronics, 2009, 18–23.

[56] Li, Z.; Shahidehpour, M.; Alabdulwahab, A.; Abusorrah, A. "Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems"; IEEE Trans. Smart Grid 2016, 7, 2260 - 2272.

[57] Pasqualetti, F.; Dörfler, F.; Bullo, F. "Cyber-Physical Attacks in Power Networks: Models, Fundamental Limitations and Monitor Design"; 50th IEEE Conf. Decision and Control and European Control Conf. 2011, 2195–2201.

[58] Chen, T. M.; Sanchez-Aarnoutse, J. C.; Buford, J. "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid"; IEEE Trans. Smart Grid 2011, 2, 741–749.

[23] O'Kelly, M. E.; Kim, H. "Survivability of Commercial Backbones with Peering: A Case Study of Korean Networks"; Critical Infrastructure 2007, 107–128.

[24] Buenneke, R. "Protection of Commercial Satellite Communications Infrastructure"; Astropolitics 2004, 2, 237–259.

[25] Coaffee, J. "Protecting Vulnerable Cities: the UK's Resilience Response to Defending Everyday Urban Infrastructure"; Int. Aff. 2010, 86, 939–954.

[26] Center for the Protection of National Infrastructure (CPNI), Protecting against Terrorism, 3rd ed. 2010.

[27] Ghaffarpour, R.; Barzegar, E. "Enhancing the Resiliency of Azarbayjan's Electric Grid against Graphite Bomb"; Passive Defense Quarterly 2015, 6, 31-46 (In Persian).

[28] Ghaffarpour, R.; Jam, A. R.; Ranjbar, A. M. "Optimal Arrangement of Dispersed Generation Resources to Enhance the Energy Security in Defense Sites from a Passive Defense Perspective"; Passive Defense Quarterly 2016, 7, 19-32 (In Persian).

[29] Gaffarpour, R.; Velayati, M. H. "Enhancing Passive Defence of Power System Networks Using Prediction Damping, Type and Location of Power System's Oscillations"; Advanced Defence Sci. & Tech. 2015, 2, 19–32 (In Persian).

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

[31] Zimmerman, R.; Dooskin, N.; Miller, J.; Hartwell, R.; Remington, W.; Simonoff, J. S.; Lave, L. B.; Schuler, R. E.; Restrepo, C. E.; Lave, B.; Schuler, R. E.; Restrepo, C. E. "Electricity Case: Main Report-Risk, Consequences, and Economic Accounting"; Institute for Civil Infrastructure Systems, New York, 2005.

[32] Bompard, E.; Huang, T.; Wu, Y.; Cremenescu, M. "Classification and Trend Analysis of Threats Origins to the Security of Power Systems"; Int. J. Electr. Power Energy Syst. 2013, 50, 50–64.

[33] Sadeghi, H.; Abdollahi, A.; Mohammadian, M.; Rashidinejad, M. "Evaluating the Effects of Renewable Energy Resources from Passive Defence and Social Welfare Perspectives in the Context of Expansion Planning"; Advanced Defence Sci. & Tech. 2015, 2, 71-86 (In Persian).

[34] Amin, M. "Security Challenges for the Electricity Infrastructure" Computer 2002, 35, 8–10.

[35] Ghaffarpour, R.; Mir Motahhari, R. "A Method for Alleviating the Disruptions Caused by Graphite Bombs, Considering the Stability of Power System"; Passive Defense Quarterly 2013, 1, 69-71 (In Persian).

[36] Ghaffarpour, R.; Mir Motahhari, R. "Groupin the Electric Grid Substations Based on the System Response to Graphite Attacks"; Passive Defense Quarterly 2016, 2, 7-18 (In Persian).

[37] Ghaffarpour, R.; Ahmadi, A. "Setting the Outage Priority of Power Lines Connecting to a Substation, to Reduce the Losses Caused by Graphite Bombs"; Passive Defense Quarterly 2016, 2, 7-18 (In Persian).

[38] Matisziw, T. C.; Murray, A. T.; Grubesic, T. H. "Exploring the Vulnerability of Network Infrastructure to Disruption"; Ann. Reg. Sci. 2009, 43, 307–321.

[39] Murray, A. T.; Grubesic, T. H. "Reliability and Vulnerability in Critical Infrastructure: A Quantitative Geographic Perspective"; Heidelberg, Springer, 2007.

[40] Murray, A. T.; Matisziw, T. C.; Grubesic, T. H. "Critical Network Infrastructure Analysis: Interdiction and System Flow"; J. Geogr. Syst. 2007, 9, 103–117.

Electric Power Networks"; Proc. of the 37th Annual North American Power Symposium, 2005, 59–66.

[77] Chen, Q.; Mili, L. "Composite Power System Vulnerability Evaluation to Cascading Failures Using Importance Sampling and Antithetic Variates"; IEEE Trans. Power Syst. 2013, 28, 2321–2330.

[78] Pinar, A.; Meza, J.; Donde, V.; Lesieutre, B. "Optimization Strategies for the Vulnerability Analysis of the Electric Power Grid"; SIAM J. Optim. 2010, 20, 1786–1810.

[79] Zhao, L. ; Zeng, B. "Vulnerability Analysis of Power Grids with Line Switching"; IEEE Trans. Power Syst. 2013, 28, 2727–2736.

[80] Bier, V. "Game-Theoretic and Reliability Methods in Counterterrorism and Security"; Statistical Methods in Counterterrorism 2006, 23–40.

[81] Cormican, K. J.; Morton, D. P.; Wood, R. K. "Stochastic Network Interdiction" Oper. Res. 1998, 46, 184–197.

[82] Alvarez, R. E. "Interdicting Electrical Power Grids"; M.Sc. Thesis, Monterey, California, Naval Postgraduate School, 2004.

[83] Simonoff, J. S.; Restrepo, C. E.; Zimmerman, R. "Risk-Management and Risk-Analysis-Based Decision Tools for Attacks on Electric Power"; Risk Anal. 2007, 27, 547–570.

[84] Holmgren, A. J.; Jenelius, E.; Westin, J.; Holmgren, A. J. "Evaluating Strategies for Defending Electric Power Networks against Antagonistic Attacks"; IEEE Trans. Power Syst. 2007, 22, 76–84.

[85] Chen, G.; Dong, Z. Y.; Hill, D. J.; Xue, Y. S. "Exploring Reliable Strategies for Defending Power Systems against Targeted Attacks"; IEEE Trans. Power Syst. 2011, 26, 1000–1009.

[86] Bienstock, D.; Verma, A. "The Nk Problem in Power Grids: New Models, Formulations, and Numerical Experiments"; SIAM J. Optim. 2010, 20, 2352–2380.

[87] Ernster, T. A.; Srivastava, A. K. "Power System Vulnerability Analysis-Towards Validation of Centrality Measures"; IEEE Transmission and Distribution Conf. and Exposition 2012, 1–6.

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

[89] Bompard, E.; Gao, C.; Napoli, R.; Russo, A.; Masera, M.; Stefanini, A. "Risk Assessment of Malicious Attacks Against Power Systems"; IEEE Trans. Syst., Man, Cybern. Part A: Syst. Humans 2009, 39, 1074–1085.

[90] Holmgren, A. J. "Electricity Case: Risk Analysis of Infrastructure Systems-Different Approaches for Risk Analysis of Electric Power Systems"; Department of Homeland Security, USA, 2005.

[91] Bompard, E.; Wu, D.; Xue, F. "The Concept of Betweenness in the Analysis of Power Grid Vulnerability"; Complexity in Eng. 2010, 52–54.

[92] Israeli, E.; Wood, R. K. "Shortest-Path Network Interdiction"; Networks 2002, 40, 97–111.

[93] Rose, R. W. "Defending Electrical Power Grids"; Thesis, Monterey California, Naval Postgraduate School, 2007.

[94] Dong, X.; Nyberg, T. R.; Hämäläinen, P.; Xiong, G.; Liu, Y.; Hou, J. "Vulnerability Analysis of Smart Grid Based on Complex Network Theory"; 5th Int. Conf. on Information Sci. and Tech. 2015, 525–529.

[59] Sridhar, S.; Hahn, A.; Govindarasu, M. "Cyber–Physical System Security for the Electric Power Grid"; Proc. of the IEEE 2012, 100, 210–224.

[60] Mo, Y.; Kim, T. H. J.; Brancik, K.; Dickinson, D.; Lee, H.; Perrig, A.; Sinopoli, B. "Cyber–Physical Security of a Smart Grid Infrastructure"; Proc. IEEE 2012, 100, 195–209.

[61] Poljanšek, K.; Bono F.; Gutiérrez, E. "Seismic Risk Assessment of Interdependent Critical Infrastructure Systems: the Case of European Gas and Electricity Networks"; Earthq. Eng. Struct. Dyn. 2012, 41, 61–79.

[62] Nakawiro, T.; Bhattacharyya, S. C. "High Gas Dependence for Power Generation in Thailand: the Vulnerability Analysis"; Energy Policy 2007, 35, 3335–3346.

[63] Wang, S.; Hong, L.; Ouyang, M.; Zhang, J.; Chen, X. "Vulnerability Analysis of Interdependent Infrastructure Systems under Edge Attack Strategies"; Saf. Sci. 2013, 51, 328–337.

[64] Urbina, M.; Li, Z. "Modeling and Analyzing the Impact of Interdependency Between Natural Gas and Electricity Infrastructures"; IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008, 1–6.

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

[66] Rinaldi, S. M.; Peerenboom, J. P.; Kelly, T. K. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", IEEE Control Syst. 2001, 21, 11–25.

[67] NERC Planning Committee "Gas/Electricity Interdependencies and Recommendations"; North American Electric Reliability Council, 2004.

[68] Wang, S.; Hong, L.; Chen, X. "Vulnerability Analysis of Interdependent Infrastructure Systems: A Methodological Framework"; Phys. A: Stat. Mech. its Appl. 2012, 391, 3323–3335.

[69] Wang, A.; Luo, Y.; Tu, G.; Liu, P. "Vulnerability Assessment Scheme for Power System Transmission Networks Based on the Fault Chain Theory"; IEEE Trans. Power Syst. 2011, 26, 442–450.

[70] Bernstein, A.; Bienstock, D.; Hay, D.; Uzunoglu, M.; Zussman, G. "Sensitivity Analysis of the Power Grid Vulnerability to Large-Scale Cascading Failures"; ACM Sigmetrics Perform. Eval. Rev. 2012, 40, 33–37.

[71] Jinling, L.; Yuan, C.; Yongli, Z. "Identification of Cascading Failures Based on Overload Character of Transmission Lines"; Third Int. Conf. on Electric Utility Deregulation and Restructuring and Power Technologies 2008, 1030–1033.

[72] Baldick, R.; Chowdhury, B.; Dobson, I.; Dong, Z.; Gou, B.; Hawkins, D.; Huang, Z.; Joung, M.; Kim, J.; Kirschen, D. "Vulnerability Assessment for Cascading Failures in Electric Power Systems"; Power Syst. Conf. Exposition 2009, 1–9.

[73] Yu, X.; Singh, C. "A Practical Approach for Integrated Power System Vulnerability Analysis with Protection Failures"; IEEE Trans. Power Syst. 2004, 19, 1811–1820.

[74] De La Ree, J.; Liu, Y.; Mili, L.; Phadke, A. G.; Dasilva, L. "Catastrophic Failures in Power Systems: Causes, Analyses, and Countermeasures"; Proc. IEEE 2005, 93, 956–964.

[75] Chassin, D. P.; Posse, C. "Evaluating North American Electric Grid Reliability using the Barabasi–Albert Network Model"; Phys. A: Stat. Mech. its Appl. 2005, 355, 667–677.

[76] Donde, V.; Lopez, V.; Lesieutre, B.; Pinar, A.; Yang, C.; Meza, J. "Identification of Severe Multiple Contingencies in

[95] Yao, Y.; Edmunds, T.; Papageorgiou D.; Alvarez, R. "Trilevel Optimization in Power Network Defense"; IEEE Trans. Syst. Man, Cybern. 2007, 37, 712–718.

[96] Paté-Cornell, E.; Guikema, S. "Probabilistic Modeling of Terrorist Threats: a Systems Analysis Approach to Setting Priorities among Countermeasures"; Mil. Oper. Res. 2002, 7, 5–23.

[97] Powell, R. "Defending Against Strategic Terrorists over the Long Run: a Basic Approach to Resource Allocation"; Institute of Governmental Studies: UC Berkeley, 2006.

[98] Alderson, D. L.; Brown G. G. ; Carlyle, W. M.; Wood, R. K. "Solving Defender-Attacker-Defender Models for Infrastructure Defense"; Operations Research, Computing, and Homeland Defense: Hanover, 2011, 28-49.

[99] Willis, H. H. "Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection"; Department of Homeland Security, USA, 2007.

[100] Bell, M. G. F. "The Use of Game Theory to Measure the Vulnerability of Stochastic Networks"; IEEE Trans. Reliab. 2003, 52, 63–68.