نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال چهاردهم، شماره ۲، تابستان ۱۴۰۲؛ ص ۱۲۲-۱۱۳

علمی - پژوهشی

ارائه مدلی مبتنی بر نظریه بازی برای مقابله با حملات هم‌زمان سایبری- فیزیکی به شبکه برق

محمدحسین رنجبر[۱*]، علیرضا رضازاده ولوجردی[۲]

۱- استادیار، دانشگاه جامع امام حسین (ع) ۲- دانشیار، دانشگاه شهید بهشتی

(دریافت: ۱۴۰۲/۰۲/۲۹، بازنگری: ۱۴۰۲/۰۴/۲۷، پذیرش: ۱۴۰۲/۰۵/۱۸، انتشار: ۱۴۰۲/۰۶/۱۷)

DOR: https://dorl.net/dor/20.1001.1.26762935.1402.14.2.4.6

چکیده

شبکه برق یکی از مهم‌ترین زیرساخت‌های هر جامعه است که سایر زیرساخت‌ها به آن وابسته هستند. بررسی‌ها نشان می‌دهد که حمله سایبری تزریق داده اشتباه می‌تواند سبب اضافه‌بار شدن خطوط انتقال گردد. معمولاً شبکه برق قابلیت پاسخ‌دادن به اضافه‌بارهای طبیعی خطوط انتقال را دارد؛ اما درصورتی‌که حمله سایبری با یک حمله هدفمند فیزیکی همراه گردد، اضافه‌بار خطوط انتقال می‌تواند از کنترل خارج گشته، و خروج‌های متوالی در خطوط انتقال شبکه رخ دهد. چنین وضعیتی در نهایت به خاموشی محلی و یا سراسری شبکه برق می‌انجامد. برای مقابله با اضافه‌بار خطوط انتقال، بهره‌بردار شبکه با انجام اقدامات اصلاحی به‌کارگیری توان ذخیره بالارونده و پایین‌رونده و همچنین بار زدایی، اضافه‌بار خطوط را رفع می‌نماید. در این مقاله ابتدا نشان می‌دهیم که چگونه حمله هم‌زمان سایبری - فیزیکی می‌تواند میزان بارزدایی شبکه را افزایش دهد. سپس مدلی بر مبنای نظریه بازی برای برنامه‌ریزی تولید شبکه ارائه می‌گردد تا بهره‌بردار بتواند توسط اقدامات اصلاحی فوق، با کمترین هزینه ممکن حمله سایبری - فیزیکی را دفع نماید. مدل ارائه‌شده بر روی شبکه تست ۵ با سه شبیه‌سازی شده و نتایج مورد تحلیل قرار گرفته است.

کلیدواژه‌ها: اضافه‌بار خطوط، تزریق داده اشتباه، حمله سایبری، شبکه برق، کمینه هزینه بدبینانه و نظریه بازی.

Presenting a Game-Based Model for Confronting Cyber-physical attacks to Power Grid

M.H. Ranjbar*, A. Rezazade Valoujerdi
Imam Hossein University

(Received: 2023/05/19, Revised: 2023/07/18, Accepted: 2023/08/09, Published: 2023/09/08)

Abstract

Power grid is one of the most important infrastructure of any society on which other infrastructures depend. Studies show that the false data injection cyberattack can cause transmission lines to overload. Usually, the power grid is capable of responding to the natural overloads of transmission lines, but if a cyberattack is accompanied by a targeted physical attack, the overload of transmission lines can become out of control, and consecutive outages can occur in the power grid's transmission lines. This situation eventually leads to local or nationwide blackouts of the power grid. To confront the overload of transmission lines, the power grid's operator removes the overloads by taking corrective measures such as using the upward and downward reserve power as well as load shedding. In this paper, we first show how a simultaneous cyber-physical attack can increase the amount of load shedding. Then a model based on game theory is presented to plan the load dispatch of the grid so that the operator can repel the cyber-physical attack with the lowest possible cost using corrective measures. The proposed model is simulated on a 5-bus test network and the results are analyzed.

Keywords: Transmission Lines Overload, False Data Injection, Cyber-Attack, Power Grid, Minimum Pessimistic Cost, Game Theory.

*Corresponding Author E-mail: m_ranjbar@sbu.ac.ir

۱. مقدمه

شبکه برق یکی از اساسی‌ترین زیرساخت‌های هر کشور است که بسیاری از زیرساخت‌ها به آن وابسته است [۱]. به جهت همین اهمیت است که زیرساخت شبکه برق برخی از کشورها هدف حملات فیزیکی و سایبری گروه‌ها و کشورهای متخاصم بوده است [۲]. در سالیان اخیر به علت وابستگی شدید کنترل و مانیتورینگ تهاجمات سایبری به شبکه برق افزایش‌یافته است [۳].

بررسی‌ها نشان می‌دهد که حمله سایبری به شبکه برق می‌تواند شبکه را از قیود تعادلی خود خارج سازد. به‌عنوان‌مثال، تزریق داده اشتباه[1] در واحدهای اندازه‌گیر توان سبب می‌شود که برنامه پخش بار شبکه بر اساس اطلاعات اشتباه صورت گیرد و در عمل خط یا خطوطی از شبکه دچار اضافه‌بار گردد [۴ و ۵].

زمانی که حمله سایبری با یک حمله هدفمند فیزیکی همراه گردد، قیود بهره‌برداری شبکه با مشکل جدی مواجه شده و تعادل قیود به شکل قابل‌توجهی می‌خورد. نمونه‌ای از حمله هم‌زمان سایبری - فیزیکی به شبکه برق ونزوئلا در سال ۲۰۱۹ انجام شده است که سبب قطع برق ۱۸ ایالات از جمله پایتخت گردید [۶].

راهکار بهره‌بردار برای مواجه با برهم‌خوردن تعادل شبکه، استفاده از خدمات اصلاحی توان ذخیره و یا در صورت لزوم، بارزدایی است [۷ و ۸]. به‌منظور بهره‌گیری از توان ذخیره واحدهای تولید، قبل از شروع بازه بهره‌برداری باید تخصیص توان تولیدی و توان ذخیره آن‌ها مشخص گردد. درصورتی‌که تخصیص توان ذخیره به واحدها برای مقابله با حوادث پیشرو به‌صورت بهینه انجام نپذیرد، بهره‌برداری از شبکه غیربهینه و متحمل صرف هزینه‌های اضافه است.

بازی دونفره مجموع صفر[2] در نظریه بازی یکی از روش‌های تخصیص بهینه منابع در شرایطی است که عامل حادثه‌ساز نه حوادث طبیعی بلکه مهاجم هوشمندی است که سعی می‌کند به‌گونه‌ای به شبکه حمله کند تا بیشترین خسارت به آن وارد شود [۹]. در سالیان اخیر استفاده از نظریه بازی برای مدل‌سازی تهاجم هوشمندانه به شبکه برق بسیار پرکاربرد بوده است [۱۰ و ۱۲].

در این مقاله ابتدا در بخش دوم به انواع حمله سایبری به شبکه برق پرداخته می‌شود و نشان داده می‌شود که چگونه حمله سایبری می‌تواند سبب اضافه‌بار خطوط گردد و لزوم استفاده از راهکارهای اصلاحی توان ذخیره و بارزدایی تشریح می‌گردد. در بخش سوم بر اساس نظریه بازی، مدلی برای تخصیص و به‌کارگیری تمهیدات اصلاحی توان ذخیره و بارزدایی ارائه می‌گردد تا در صورت وقوع حمله هم‌زمان و هدفمند سایبری و فیزیکی، کمترین خسارت به شبکه وارد گردد. در بخش چهارم مدل پیشنهادی بر روی شبکه تست ۵ با سه، پیاده‌سازی شده و نتایج موردبحث قرار می‌گیرد. در بخش پنجم نیز نتیجه‌گیری بیان می‌گردد. روش پیشنهادی در این مقاله بر تخصیص بهینه توان ذخیره و بارزدایی در سطح انتقال تأکید دارد؛ زیرا تزریق داده اشتباه در سطوح انتقال که میزان مصرف و تولید نسبت به شبکه توزیع مقدار بزرگ‌تری است، بهره‌برداری از سیستم را با چالش مواجه می‌سازد. البته روش پیشنهادی در این مقاله برای شبکه توزیع و همچنین ریزشبکه‌ها نیز درصورتی‌که قیود بهره‌برداری متناسب با آن شبکه‌ها اصلاح گردد، قابل‌پیاده‌سازی است.

۲. حملات سایبری و فیزیکی به شبکه برق

۲-۱. انواع حمله سایبری به شبکه برق

حملات سایبری به شبکه برق یکی از مباحث داغ در حوزه تأمین امنیت شبکه برق است. اساساً حمله سایبری به شبکه برق با دو هدف کلی انجام می‌پذیرد. هدف اول اجرای حمله سایبری به‌منظور انتفاع اقتصادی در بازار انرژی است. به این نوع حملات، حملات سودجویانه گفته می‌شود. هدف دوم اجرای حمله سایبری به‌منظور ایجاد اختلال در عملکرد شبکه برق کشور مورد حمله است. در حقیقت در این نوع حمله، مهاجم می‌کوشد تا به عملکرد شبکه برق در تأمین انرژی پایدار، آسیب وارد نماید. به این نوع حملات، حملات خرابکارانه گفته می‌شود. در این مقاله نوع دوم حملات سایبری مدنظر است.

حملات سایبری از منظر نوع حمله در شبکه‌های هوشمند به سه دسته حملات علیه دسترس‌پذیری داده، حملات علیه یکپارچگی[3] داده و حملات علیه محرمانگی داده تقسیم می‌شوند [۱۳]. در خصوص دسترس‌پذیری داده، باید روند تبادل اطلاعات بین گیرنده‌ها و فرستنده‌های شبکه‌های هوشمند در لحظه و بدون اخلال و توقف صورت پذیرد تا کنترل‌پذیری و بهره‌وری حداکثری محقق شود. در حملات علیه دسترس‌پذیری داده، مهاجم می‌کوشد تا با ارسال اطلاعات اضافی، باعث ترافیک خطوط شود و روند تبادل داده را با مشکل مواجه سازد. در خصوص یکپارچگی داده گفته می‌شود که داده‌ها باید از فرآیند تولید داده تا ارسال به مقصد، بدون هیچ‌گونه تغییریافتگی عمدی یا غیرعمدی منتقل شوند. در حملات علیه یکپارچگی داده، مهاجم می‌کوشد تا داده‌ها را در یکی از حلقه‌های زنجیره انتقال داده، در جهت اهداف خود تغییر دهد. در خصوص محرمانگی داده نیز گفته می‌شود که افراد غیرمجاز نباید داده‌ها را رؤیت نمایند تا از داده‌ها و رانت حاصل از آن‌ها استفاده غیرمجاز نبرند. در بازار انرژی، محرمانگی داده از

[1] False Data Injection
[2] Two Person Zero Sum Game
[3] Integrity

اهمیت ویژه‌ای برخوردار می‌گردد و مهاجم می‌کوشد تا به داده‌ها (قیمت‌های پیشنهادی در بازار انرژی یا وضعیت تولیدکنندگان و مصرف‌کنندگان) دسترسی پیدا کند. حملات خرابکارانه عمدتاً حملات بر علیه یکپارچگی داده هستند که مهاجم می‌کوشد تا با تغییر عمدی اطلاعات، هدف خصمانه خود را اجرا نماید. این نوع حملات به حملات تزریق داده اشتباه معروف است. حملات بر علیه دسترس‌پذیری داده نیز می‌تواند به اخلال در عملکرد شبکه برق منتهی شود.

در شبکه برق، اندازه‌گیری متغیرهایی مانند ولتاژ، توان عبوری و... توسط واحدهای پایانه دوردست[1] و واحدهای اندازه‌گیر فازوری، انجام می‌شود. این داده‌های اندازه‌گیری شده سپس توسط سیستم اکتساب داده و کنترل نظارتی[2] (اسکادا) تجمیع شده و عملیات کنترل شبکه برق باتوجه‌به مقادیر لحظه‌ای اندازه‌گیری شده، صورت می‌پذیرد [۱۳].

برای مهاجمان سایبری این امکان وجود دارد که تعدادی از داده‌های اندازه‌گیری را تغییر دهند. فرض کنید که بردار متغیرهای اندازه‌گیری شده واقعی شبکه که در سیستم اسکادا تجمیع می‌شود برابر X^m باشد. در این صورت اگر مهاجم تعدادی از داده‌های اندازه‌گیری را تغییر داده باشد، متغیرهای اندازه‌گیری جدیدی برای سیستم کنترل تولید می‌شود. به اختلاف بردار اندازه‌گیری غیرواقعی جدید و بردار اندازه‌گیری واقعی، بردار حمله[3] گفته می‌شود [۵]:

$$A = X^{m,a} - X^m \qquad (۱)$$

در رابطه فوق، $X^{m,a}$ بردار متغیرهای اندازه‌گیری شده پس از وقوع حمله سایبری و A بردار حمله است. طول بردار متغیرهای اندازه‌گیری شده و در نتیجه بردار حمله برابر با m است (تعداد m متغیر در شبکه اندازه‌گیری می‌شود). البته این بدین معنی نیست که لزوماً مهاجم سایبری قادر است تمامی m داده اندازه‌گیری شده را مخدوش نماید؛ بلکه حتی با تغییر یکی از داده‌ها نیز حمله پیاده‌سازی شده است.

در یک شبکه، برنامه‌ریزی تولید انرژی توسط نیروگاه‌ها و تخصیص توان ذخیره بین آن‌ها برای بازه‌های بهره‌برداری پیشرو، توسط مسئله پخش بار بهینه اقتصادی تعیین می‌گردد. در بخش بعدی نشان می‌دهیم که درصورتی‌که داده‌های ورودی به مسئله پخش بار بهینه، با مقادیر واقعی هم‌خوان نباشد، چگونه ممکن است خطوطی از شبکه دچار اضافه‌بار گردد و سرویس‌دهی شبکه را با اختلال مواجه سازد. حمله تزریق داده اشتباه به سیستم اسکادا تنها نوع حمله سایبری به شبکه برق نیست. حمله سایبری به فرآیند کنترل خودکار تولید و حمله به ادوات کنترلی FACTS نیز از دیگر انواع حملات سایبری خرابکارانه است.

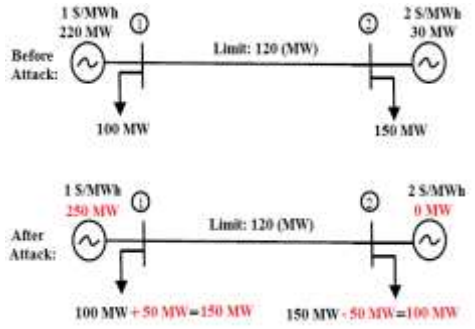
[1] Remote Terminal Units (RTU)
[2] Supervisory Control and Data Acquisition (SCADA)
[3] Attack Vector

۲-۲. اضافه‌بار خطوط ناشی از تزریق داده اشتباه

همان‌گونه که اشاره شد، مهاجم سایبری توانایی دارد تا مقادیر اندازه‌گیری شده را مخدوش سازد. معمولاً مهاجم ترجیح می‌دهد تا مقدار اندازه‌گیری شده برای توان مصرفی بارهای شبکه را تغییر دهد و از تغییر مقادیر اندازه‌گیری شده برای توان تولیدی ژنراتورها خودداری می‌کند. این امر به این دلیل است که معمولاً نیروگاه‌ها در مقادیر نامی خودکار می‌کنند و تغییر توان اندازه‌گیری شده آن‌ها الگوریتم‌های محاسباتی را با تردید همراه می‌سازد.

تزریق داده اشتباه به مقادیر اندازه‌گیری شده بارهای شبکه، می‌تواند سبب اضافه‌بار خطوط شبکه گردد. شکل (۱) یک شبکه ساده دو با سه را نشان می‌دهد که حمله سایبری تزریق داده اشتباه به آن سبب اضافه‌بار خط انتقال وصل‌کننده دو باس می‌شود [۵].

در شکل (۱)، قبل از وقوع حمله واحد تولید ۱ به دلیل ارزان‌تر بودن تولید توان، ۲۲۰ مگاوات توان را تولید کرده که ۱۰۰ مگاوات آن به مصرف باس ۱ و ۱۲۰ مگاوات آن از طریق خط انتقال، به مصرف بار ۲ می‌رسد. واحد تولید ۲ نیز ۳۰ مگاوات توان باقی‌مانده مصرف باس ۲ را تولید می‌کند. در این صورت توان عبوری از خط انتقال ۱۲۰ مگاوات است که برابر با حد بیشینه توان عبوری از آن است.



شکل ۱. اضافه‌بار خط انتقال در شبکه دو با سه [۵]

در حالت دوم، درصورتی‌که بر اثر حمله سایبری، بارهای مصرف باس ۱ و باس ۲ به ترتیب به مقادیر اشتباه ۱۵۰ مگاوات و ۱۰۰ مگاوات تغییر یابد، الگوریتم پخش بار بهینه تصمیم می‌گیرد تا واحد تولید ۱، ۲۵۰ مگاوات را تولید نماید و واحد تولید ۲، خاموش باشد. در این صورت الگوریتم مطابق داده اشتباه فرض می‌کند که ۱۵۰ مگاوات از توان تولیدی واحد ۱ صرف مصرف در باس ۱ و ۱۰۰ مگاوات دیگر نیز از طریق خط انتقال به مصرف باس ۲ می‌رسد. در این صورت، الگوریتم فرض می‌نماید که توان عبوری از خط انتقال از مقدار حد بیشینه عبوری تجاوز نمی‌کند. اما در واقعیت، با تخصیص ۲۵۰ مگاوات به واحد تولید ۱ و خاموش سازی واحد تولید ۲، ۱۰۰ مگاوات توان به مصرف باس ۱ می‌رسد و ۱۵۰ مگاوات توان از طریق خط انتقال عبور می‌کند که ۳۰ مگاوات از حد بیشینه عبوری بیشتر است و خط دچار اضافه‌بار

می‌شود. در مثال فوق، بهره‌بردار برای مقابله با اضافه‌بار خط انتقال، ۳۰ مگاوات از بار باس شماره ۲ را قطع می‌کند.

اضافه‌بار خط انتقال می‌تواند سبب خروج خط انتقال توسط رله‌های خط شود. در مواردی که بارگذاری شبکه سنگین است و ظرفیت خطوط انتقال دیگر نیز اشغال شده است، خروج یک خط انتقال می‌تواند سبب اضافه‌بار متعاقب خطوط مجاور و در نتیجه خروج‌های متوالی خطوط انتقال و در نهایت فروپاشی شبکه گردد. در سال ۲۰۰۳ در ایالات‌متحده خط انتقالی به دلیل حادثه از مدار جدا گردید و پس از آن به دلیل عدم آگاهی وضعیتی مناسب بهره‌بردار و مانورهای اشتباه در بهره‌برداری، خاموشی معروف سال ۲۰۰۳ آمریکا به وقوع پیوست که سبب خاموشی سراسری[1] بزرگی گردید [۱۴].

می‌توان نتیجه گرفت که بهره‌بردار شبکه همواره باید بکوشد تاحدامکان از اضافه‌بار خطوط انتقال جلوگیری نماید. ابزار بهره‌بردار برای مقابله با اضافه‌بار خطوط، استفاده از تمهیداتی چون توان ذخیره بالارونده، پایین‌رونده و بارزدایی است. به‌کارگیری این تمهیدات سبب می‌شود تا بهره‌بردار بتواند در بازه زمانی مناسب نسبت به کاهش بار خطوطی که دچار اضافه‌بار شده‌اند اقدام نماید و از خروج متعاقب آن‌ها جلوگیری نماید.

۲-۳. حمله هم‌زمان سایبری - فیزیکی به شبکه برق

در شرایطی که علاوه بر بارگذاری سنگین، حمله هدفمند فیزیکی با حمله هوشمندانه سایبری، ترکیب شود، می‌توان انتظار داشت که شبکه دچار مشکل جدی شود. به‌عنوان‌مثال، درصورتی‌که در شبکه شکل (۱)، ژنراتور ۱ نیز هم‌زمان مورد حمله قرار گرفته و از شبکه خارج شود، ژنراتور ۲ به علت خاموش بودن و نداشتن آمادگی جهت تولید توان نمی‌تواند در تأمین بار کمک کند و بار کل شبکه قطع می‌گردد.

در این صورت بهره‌بردار باید علاوه بر تأمین توان ذخیره و آمادگی برای بارزدایی به‌منظور جلوگیری از اضافه‌بار شدن خطوط، میزانی از توان ذخیره برای کمبود توان تولیدی در صورت وقوع حمله فیزیکی را تأمین نماید.

حمله فیزیکی می‌تواند علاوه بر ژنراتورها، به خطوط انتقال نیز انجام شود و سبب قطع‌شدن خطوط انتقال گردد [۱۰]. در این صورت با سرریزشدن توان عبوری خط قطع شده بر خطوط مجاور، سایر خطوط نیز ممکن است دچار اضافه‌بار گشته و متعاقباً توسط رله حفاظتی از شبکه جدا گردند.

حمله فیزیکی از منظر شدت حمله به نوع تک‌هدفه و چندهدفه تقسیم‌بندی می‌گردد [۱۰]. در حمله تک‌هدفه مهاجم تنها توانایی و امکان حمله به یک هدف را دارد. در حمله چندهدفه مهاجم می‌تواند هم‌زمان به چندین نقطه حمله فیزیکی نماید. در این مقاله فرض می‌شود که حمله فیزیکی از نوع تک‌هدفه است.

۳. مدل بازی پیشنهادی برای مقابله با حمله هم‌زمان سایبری - فیزیکی

همان‌گونه داده شد، بهره‌بردار شبکه با به‌کارگیری که توضیح اقدامات اصلاحی[2] با اضافه‌بار خطوط مقابله می‌نماید. به‌کارگیری تمهیدات توان ذخیره و بارزدایی هزینه‌ای اضافی بر بهره‌بردار و مصرف‌کنندگان شبکه تحمیل می‌کند. در خصوص به‌کارگیری اقدامات اصلاحی توان ذخیره، بهره‌بردار باید برای تخصیص و به‌کارگیری توان ذخیره بالارونده و پایین‌رونده به نیروگاه‌های شبکه هزینه‌ای پرداخت نماید.

همچنین اقدام اصلاحی بارزدایی که با قطع بار مشترکان همراه است، هزینه‌ای به‌اندازه مجموع ارزش بار ازدست‌رفته[3] در مقدار بار تأمین نشده، به شبکه تحمیل می‌کند.

در مسئله توصیف شده با حالتی مواجه هستیم که مهاجم در تلاش است تا بیشترین هزینه را به شبکه وارد نماید و در مقابل بهره‌بردار شبکه تلاش می‌نماید تا این هزینه را حداقل سازد. این حالت را می‌توان مطابق با چارچوب یک بازی دونفره مجموع صفر، مدل‌سازی کرد [۹]. در چنین چارچوبی مهاجم و مدافع شبکه (بهره‌بردار) به‌صورت هم‌زمان در تلاش‌اند تا راهبُرد بهینه تهاجمی یا تدافعی خود را به صورتی تنظیم نمایند که حداکثر منفعت را احصاء نماید. در نهایت، به‌کارگیری راهبُردهای بهینه توسط مهاجم و مدافع هوشمند به نقطه تعادل نش[4] که جواب نهایی چارچوب بازی است، می‌انجامد. نقطه تعادل نش تضمین می‌کند که در صورت اتخاذ راهبُردهای بهینه توسط مهاجم و مدافع، مینیمم هزینه بدبینانه[5] به شبکه وارد می‌شود که یعنی نه مهاجم می‌تواند هزینه وارد بر شبکه را از این مقدار بیشتر نماید و نه مدافع می‌تواند هزینه وارد را از این مقدار کمتر نماید [۱۵]. در ادامه این بخش، مدل تهاجم، مدل تدافع و چارچوب بازی ارائه می‌گردد.

۳-۱. مدل تهاجم

همان‌گونه که در بخش قبل اشاره شد، حمله تزریق داده اشتباه را می‌توان به‌صورت بردار حمله تعریف شده در رابطه (۱)، در نظر گرفت. بردار حمله عبارت است از هر ترکیب قابل اجرا از تزریق داده اشتباه در مقادیر اندازه‌گیری شده توسط میترهای شبکه که می‌تواند فرآیندهای بهره‌برداری و کنترلی را با مشکل مواجه سازد.

[1] Blackout

[2] Corrective Measures
[3] Value of Lost Load (VOLL)
[4] Nash Equilibrium
[5] Minimum Pessimistic Cost

بنابراین، راهبُرد خالص مهاجم یا بردار حمله A به‌صورت زیر تعریف می‌شود:

$$A=(a_1,a_2,...,a_m) \quad (۲)$$

در بردار فوق برخی از درایه‌ها صفر خواهد بود و برخی دیگر مقدار غیرصفر خواهد داشت. درایه‌هایی که مهاجم به دلیل عدم دسترسی نتوانسته آن‌ها را تغییر دهد و یا به‌صورت عمد آن‌ها را بدون تغییر گذاشته، صفر خواهد بود و مابقی درایه‌ها می‌توانند مقدار غیرصفر داشته باشد.

مهاجم معمولاً مقادیر اندازه‌گیری شده برای توان‌های مصرفی را به‌گونه‌ای تغییر می‌دهد که جمع کل بار مصرفی شبکه نیز تغییر نکند تا الگوریتم‌ها و بهره‌برداران شبکه را با تردید مواجه نسازد؛ لذا می‌توان رابطه زیر را نیز به‌عنوان قیدی برای تهاجم در نظر گرفت:

$$\sum_{i=1}^{m} a_i = 0 \quad (۳)$$

درصورتی‌که همانند فرض مسئله، حمله سایبری با یک حمله فیزیکی همراه باشد، سناریوی حمله ترکیبی از سناریوهای حمله سایبری به همراه سناریوهای حمله فیزیکی خواهد بود. به‌عنوان‌مثال، فرض کنید شبکه دارای N_G ژنراتور و N_L خط انتقال است. با فرض اینکه مهاجم قادر است به یکی از ژنراتورها و یا خطوط انتقال حمله فیزیکی نماید، تعداد N_G+N_L سناریو برای اجرای این حمله فیزیکی وجود خواهد داشت. اگر این تعداد سناریو را با تمام سناریوهای محتمل در حمله سایبری که آن را برابر با (N_S) فرض می‌کنیم، ترکیب کنیم، تعداد کل سناریوها برای حمله ترکیبی سایبری - فیزیکی برابر با مقدار زیر خواهد بود:

$$N_T = N_S \times (N_G + N_L) \quad (۴)$$

در رابطه فوق N_T تعداد کل سناریوها برای حمله ترکیبی سایبری - فیزیکی است.

۳-۲. مدل تدافع

راهکارهای بهره‌بردار شبکه برق به‌عنوان مدافع شبکه برای مقابله با تهاجمات قریب‌الوقوع[1]، استفاده از تمهیدات بهره‌برداری توان ذخیره و بارزدایی است. این اقدامات نه‌تنها برای مقابله با تهدیدات عامدانه که برای مقابله با حوادث طبیعی شبکه برق نیز به‌عنوان اقدامات اصلاحی بهره‌بردار شبکه، شناخته می‌شود؛ بنابراین راهبُرد خالص[2] مدافع قبل از وقوع حمله را می‌توان به‌صورت برداری از توان حقیقی تولیدی و توان‌های ذخیره بالارونده و پایین‌رونده تخصیص‌داده‌شده به واحدهای تولید در نظر گرفت:

$$D=(P_1,R_1^U,R_1^D,...,P_{N_G},R_{N_G}^U,R_{N_G}^D) \quad (۵)$$

در رابطه فوق P_i توان تخصیص‌داده‌شده به ژنراتور i ام، R_i^U توان ذخیره بالارونده تخصیص‌داده‌شده به ژنراتور i ام، R_i^D توان ذخیره پایین‌رونده تخصیص‌داده‌شده به ژنراتور i ام و N_G تعداد کل ژنراتورهای شبکه است.

بعد از وقوع حمله، بهره‌بردار باید با به‌کارگیری توان‌های ذخیره تخصیص‌داده‌شده به ژنراتورها و نهایتاً با بارزدایی، اضافه‌بار ایجاد شده در خطوط را به صفر می‌رساند. درصورتی‌که قبل از وقوع حمله مقادیری مناسبی از توان ذخیره به ژنراتورها اختصاص نیابد و به عبارتی ژنراتورها آمادگی تزریق توان بیشتر یا کاهش توان خود را در بازه زمانی بهره‌برداری پیشرو نداشته باشند، به‌کارگیری این تمهیدات اصلاحی برای بهره‌بردار غیرممکن خواهد بود و بهره‌بردار ناچار است تا صرفاً با بارزدایی پرهزینه، اقدام به مقابله با حمله نماید.

۳-۳. مدل برهم‌کنش[3]

در یک بازی دونفره مجموع صفر، برهم‌کنش مهاجم و مدافع توسط بهینه‌سازی مینیم - ماکزیمم مدل می‌گردد. تخصیص و به‌کارگیری تمهیدات اصلاحی توان ذخیره و نهایتاً بارزدایی برای مقابله با اضافه‌بار خطوط، بر شبکه هزینه اضافی تحمیل می‌نماید. اساساً استفاده از بهینه‌سازی مینیمم - ماکزیمم برای مدل‌سازی چارچوب بازی به این دلیل است تا مطابق قاعده هزینه/منفعت، هزینه استفاده از تمهیدات اصلاحی در برابر منفعت به‌کارگیری این تمهیدات متعادل گردد؛ بنابراین می‌توان مدل برهم‌کنش بازی را به‌صورت زیر تعریف کرد:

$$\min_{d} \max_{a} \sum_{a=1}^{N_T} L_a(d) \quad (۶)$$

در رابطه (۶) d یک راهبُرد دفاعی در فضای تمام راهبُردهای دفاعیِ امکان‌پذیر (D) است، a یک سناریوی تهاجمی در فضای تمام سناریوهای تهاجمی امکان‌پذیر (A) است و $L_a(d)$ هزینه کل وارد بر شبکه بر اثر سناریوی حمله a با وجود به‌کارگیری راهبُرد دفاعی d است.

فضای راهبُردهای دفاعی امکان‌پذیر (D)، یک فضای نامحدود از تمامی ترکیبات ممکن و شدنی تخصیص و به‌کارگیری تمهیدات اصلاحی توان ذخیره و بارزدایی است. برای سناریوهای تهاجمی، فرض می‌کنیم که فضای سناریوهای تهاجمی، محدود و قابل‌شمارش است. این فرض ازآن‌جهت راهگشا است که مطابق مرجع [۱۵]بازی دونفره مجموع صفر شبه محدود (بازی‌ای که در آن راهبردهای حداقل یک بازیگر محدود و قابل‌شمارش است)، قابل‌حل و محاسبه خواهد بود. به‌منظور پیاده‌سازی چنین فرضی، سناریوهای تغییر بارهای شبکه بر اثر حمله سایبری تزریق داده اشتباه، باید به پله‌های ۱۰ درصدی برای هر بار محدود شود. به‌عنوان‌مثال، اگر بار باس مصرف‌کننده‌ای ۱۰۰ مگاوات باشد، فرض می‌کنیم مهاجم سایبری در پله‌های ۱۰ مگاواتی، بار را تغییر

[1] Imminent Attacks
[2] Pure Strategy
[3] Interaction Model

می‌دهد. با چنین فرضی، تعداد سناریوهای حمله سایبری (N_s) محدود گشته و در نتیجه تعداد کل سناریوهای تهاجمی (N_T) نیز محدود می‌گردد.

ازآنجایی‌که اضافه‌بار طولانی‌مدت خطوط انتقال منجر به خرابی فیزیکی آن‌ها و در نتیجه صرف هزینه و وقت هنگفت تعویض می‌شود، بهره‌بردار شبکه به‌گونه‌ای عمل می‌کند تا با به‌کارگیری تمهیدات اصلاحی یا بارزدایی حداکثری از شبکه، اضافه‌بار در خطوط هرگز رخ ندهد. این امر با تعریف قیود بهره‌برداری که در ادامه ذکر خواهد شد، ممکن خواهد بود.

پس از وقوع حمله به شبکه، هزینه کل وارد بر شبکه خود را به‌صورت هزینه اضافی به‌کارگیری تمهیدات توان ذخیره به‌علاوه هزینه ناشی از قطع بارهای شبکه، نشان می‌دهد؛ بنابراین می‌توان هزینه کل وارد بر شبکه در اثر تهاجم ترکیبی a را به‌صورت زیر تعریف کرد:

$$L_a(d)=\sum_{i=1}^{N_G}(C_i^U R_i^U+C_i^D R_i^D)+\sum_{i=1}^{N_G}C_i(r_{i,a}^U-r_{i,a}^D)+\sum_{j=1}^{N_L}LNS_{j,a}(d)\times VOLL_j\times T_{j,a} \quad (۷)$$

در رابطه فوق عبارت اول هزینه ناشی از تخصیص توان ذخیره بالارونده و پایین‌رونده به واحدهای تولید شبکه است. این هزینه چه توان ذخیره‌ای در بازه زمانی پیشرو به‌کارگیری شود و چه نشود، صرفاً جهت آمادگی واحدهای تولید شبکه به آن‌ها پرداخت می‌شود. در این عبارت، R_i^U و R_i^D به ترتیب توان ذخیره بالارونده و پایین‌رونده تخصیص‌داده‌شده به واحد تولید i ام است و C_i^U و C_i^D به ترتیب هزینه تخصیص توان ذخیره بالارونده و پایین‌رونده به واحد تولید i بر حسب دلار بر مگاوات در بازه بهره‌برداری یک‌ساعته است. عبارت دوم هزینه به‌کارگیری توان ذخیره بالارونده و پایین‌رونده است که در صورت استفاده از توان ذخیره بالارونده، به‌صورت هزینه مصرف سوخت خود را نشان می‌دهد و در صورت به‌کارگیری توان ذخیره پایین‌رونده، خود را به‌صورت درآمدی که عدم مصرف سوخت دارد خود را نشان می‌دهد. دراین‌رابطه C_i هزینه تولید توان توسط واحد i و $r_{i,a}^U$ و $r_{i,a}^D$ توان ذخیره بالارونده و پایین‌رونده به کار گرفته شده توسط واحد تولید i در صورت بروز سناریوی حمله a است. عبارت سوم هزینه ناشی از عدم تأمین انرژی توسط شبکه است. $LNS_{j,a}(d)$ انرژی تأمین نشده باس مصرفی j در اثر حمله سایبری - فیزیکی a در صورت به‌کاربردن راهبرد دفاعی d است، $VOLL_j$ ارزش بار ازدست‌رفته باس مصرفی j است و $\mathrm{Tj}_{,a}$ زمان بازیابی بار باس j در اثر حمله a است.

بهینه‌سازی مینیم - ماکزیمم رابطه (۶) باید با توجه قیود بهره‌برداری شبکه که به‌صورت روابط (۸)- (۱۶) است، محاسبه شود:

$$P_{Gk}+\sum_{m=1}^{N_I}B_{k-m}(\delta_m-\delta_k)=P_{Lk} \qquad k=1,\dots,N_I \quad (۸)$$

$$U_{k,a}\left[P_{Gk}+(r_{k,a}^U-r_{k,a}^D)\right]+\sum_{m=1}^{N_I}U_{k-m,a}B_{k-m}(\delta_{m,a}-\delta_{k,a})=P_{Lk}-LNS_{k,a} \qquad k=1,\dots,N_I$$

دسته روابط (۸) و (۹) به ترتیب قیود تعادل تولید و مصرف شبکه در دو حالت قبل از وقوع حادثه (حمله) و بعد از وقوع حمله را تضمین می‌کند. در روابط فوق P_{Gk} و P_{Lk} به ترتیب توان تولیدی تزریقی به باس k ام و توان مصرفی در باس k ام است، $B_{k\text{-}m}$ سوسپتانس خط انتقال بین باس k ام و باس m ام است، δ_k زاویه باس k ام قبل از وقوع حمله است، $\delta_{k,a}$ زاویه باس k ام بعد از وقوع حمله a است، $U_{k,a}$ عددی باینری است که در صورت وقوع حمله فیزیکی به واحد تولید متصل به باس k در سناریوی حمله a، صفر است و در غیر این صورت ۱ است، $U_{k\text{-}m,a}$ عددی باینری است که در صورت وقوع حمله فیزیکی به خط انتقال متصل به باس k و m در سناریوی حمله a، صفر است و در غیر این صورت ۱ است، $LNS_{k,a}$ نیز توان مصرفی زدوده شده از باس k در حین سناریوی حمله a است و N_I نیز تعداد کل باس‌های شبکه است.

$$\left|B_{k-m}(\delta_m-\delta_k)\right|\le P_{k-m}^{\max} \qquad k,m=1,\dots,N_L \quad (۱۰)$$

$$U_{k-m,a}\left|B_{k-m}(\delta_{m,a}-\delta_{k,a})\right|\le P_{k-m}^{\max} \qquad k,m=1,\dots,N_L \quad a=1,\dots,N_T \quad (۱۱)$$

دسته روابط (۱۰) و (۱۱) قیود اضافه‌بار نشدن خطوط انتقال شبکه را به ترتیب قبل از وقوع حمله و بعد از وقوع حمله تضمین می‌کند. در روابط فوق $P_{k-m}^{\max}$ بیشینه توان قابل انتقال از خط بین باس k و m است و N_L تعداد کل خطوط انتقال است.

$$P_{Gk}+R_K^U\le P_{Gk}^{\max} \qquad k=1,\dots,N_I \quad (۱۲)$$

$$P_{Gk}-R_K^D\ge P_{Gk}^{\min} \qquad k=1,\dots,N_I \quad (۱۳)$$

دسته روابط (۱۲) و (۱۳) به ترتیب قیود بیشینه و کمینه توان قابل تولید توسط واحدهای تولید را تضمین می‌کند. در هر بازه زمانی بهره‌برداری، توان تولیدی واحد تولید متصل به باس k به علاوه توان ذخیره بالارونده اختصاص یافته به آن (R_k^U)، نباید از بیشینه توان قابل تولید آن واحد تولید (P_{Gk}^{max})، بیشتر باشد. هم‌زمان توان تولیدی واحد متصل به باس k منهای توان ذخیره پایین‌رونده اختصاص یافته به آن (R_k^D)، نباید از مینیمم توان قابل تولید آن واحد تولید (P_{Gk}^{min})، کمتر شود.

$$0\le r_{K,a}^U\le R_K^U \qquad k=1,\dots,N_I \quad a=1,\dots,N_T \quad (۱۴)$$

$$0\le r_{K,a}^D\le R_k^D \qquad k=1,\dots,N_I \quad a=1,\dots,N_T \quad (۱۵)$$

همچنین مطابق روابط (۱۴) و (۱۵)، توان ذخیره بالارونده و پایین‌رونده به کار گرفته شده پس از وقوع حمله a، باید از مقادیر تخصیص یافته بیشتر نباشد.

$$LNS_{k,a} \le P_{Lk} \qquad k=1,...,N_I \quad a=1,...,N_T \qquad (۱۶)$$

رابطه (۱۶) نیز مقدار باری که از هر باس بعد از وقوع حمله قابل قطع کردن (بارزدایی) است را محدود به میزان بار مصرفی متصل به آن باس می‌کند.

۳-۴. روش حل مدل پیشنهادی

بهینه‌سازی مینیمم - ماکزیمم رابطه (۶) این‌گونه تفسیر می‌شود که به‌ازای یک راهبرد دفاعی مشخص مانند d، راهبرد تهاجمی مشخص مانند a' راهبرد تهاجمی بهینه است که بیشترین هزینه را بر شبکه تحمیل کند.

هم‌زمان بهره‌بردار شبکه به‌عنوان مدافع شبکه می‌کوشد تا راهبرد دفاعی‌اش بهینه گردد. این امر با انتخاب راهبرد بهینه d' که منجر به مینیمم شدن ماکزیمم هزینه وارد شده بر شبکه به‌ازای حمله a' است، انجام می‌شود؛ لذا درصورتی‌که بازی دونفره

مجموع صفر تعریف شده توسط رابطه (۶) شبه محدود باشد، می‌توان حل مسئله بهینه‌سازی مینیمم - ماکزیمم رابطه (۶) را به حل روابط زیر، بازنویسی کرد [۱۴]:

$$\underset{d\in D}{Min}\ M(d) \qquad (۱۷)$$

که $M(d)$ برابر است با:

$$M(d)=\max\left[\mathrm{L}_1(\mathrm{d}),...,\mathrm{L}_{N_T}(\mathrm{d})\right] \qquad (۱۸)$$

در رابطه فوق، منظور از max اپراتور ریاضی ماکزیمم است که در بردار $\left[L_1(d),...,L_{N_a}(d)\right]$ مقدار بیشینه را انتخاب می‌نماید. برای حل مسئله بهینه‌سازی (۱۷)، می‌توان با اضافه‌کردن متغیر کمکی β، اپراتور ریاضی ماکزیمم رابطه (۱۸) را حذف کرد و در عوض مسئله را به یک مسئله مینیمم‌سازی به همراه تعدادی قید نامساوی، تبدیل کرد:

$$\min_{d}\ M(d) \qquad (۱۹)$$

$$\beta \ge L_a(d) \qquad for \quad a=1,...,N_T \qquad (۲۰)$$

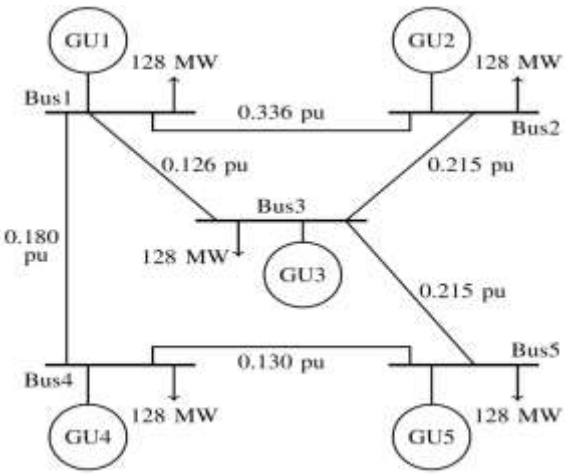
مسئله مینیمم‌سازی رابطه (۱۹)، علاوه بر قیود رابطه (۲۰)، باید دسته قیود روابط (۸)-(۱۶) و قید (۳) را نیز در برگیرد.

۴. تست مدل پیشنهادی و تحلیل نتایج

در این مقاله جهت نشان‌دادن اثرات سوء حمله سایبری - فیزیکی به شبکه برق و نشان‌دادن کارایی مدل ارائه شده، از شبکه تست ۵ با سه استفاده شده است [۱۵]. تصویر این شبکه در شکل (۲) نشان‌داده‌شده است. در این شبکه ظرفیت تمامی خطوط انتقال ۸۰ مگاوات فرض می‌شود. حداکثر توان قابل‌تولید واحدهای تولید شبکه برابر با ۱۵۰ مگاوات است. برای این شبکه، هزینه تولید انرژی و تخصیص توان ذخیره بالارونده و پایین‌رونده برای بازه بهره‌برداری یک‌ساعته و بیشینه توان ذخیره قابل تخصیص به هر واحد تولید، مطابق جداول (۱) و (۲) فرض شده است. همچنین ارزش بارهای ازدست‌رفته این شبکه مطابق جدول (۳) فرض می‌شود.

جدول ۱. هزینه‌های فرضی تولید انرژی و توان ذخیره واحدهای تولید شبکه ۵ با سه

واحد تولید	هزینه تولید انرژی ($/MW)	هزینه تخصیص توان ذخیره بالارونده ($/MW)	هزینه تخصیص توان ذخیره پایین‌رونده ($/MW)
۱	۱۰	۲۰	۱۸
۲	۲۰	۱۵	۱۳
۳	۳۰	۳۰	۲۸
۴	۲۰	۱۵	۱۳
۵	۲۵	۴۰	۳۸



شکل ۲. شبکه ۵ با سه [۱۵]

جدول ۲. بیشینه توان ذخیره قابل تخصیص به واحدهای تولید شبکه

واحد تولید	بیشینه توان ذخیره بالارونده (MW)	بیشینه توان ذخیره پایین‌رونده (MW)
۱	۳۰	۳۰
۲	۲۰	۲۰
۳	۳۰	۳۰
۴	۲۰	۲۰
۵	۲۰	۲۰

جدول ۳. ارزش بار از دست رفته بارهای شبکه بر حسب $/MWh

باس ۱	باس ۲	باس ۳	باس ۴	باس ۵
۳۰۰	۵۰۰	۶۰۰	۳۰۰	۴۰۰

۴-۱. تأثیر حمله هم‌زمان سایبری - فیزیکی

برای نشان‌دادن تأثیر مخرب حمله هم‌زمان سایبری - فیزیکی فرض می‌کنیم که در حالت اول، مهاجم حمله سایبری انجام نمی‌دهد و فقط به واحد تولید شماره ۱ شبکه، حمله فیزیکی انجام می‌دهد و آن را از مدار خارج می‌کند. در این صورت با خارج شدن یکی از واحدهای تولید، شبکه با کمبود ۴۰ مگاوات توان روبرو می‌شود. در نتیجه بهره‌بردار باید این کمبود توان را با قطع کردن ۴۰ مگاوات بار از باسی که کمترین میزان VOLL را دارد، مدیریت نماید. با استفاده از مدل مبتنی بر نظریه بازی ارائه شده و با فرض اینکه تنها یک سناریو برای حمله وجود دارد و آن حمله فیزیکی به واحد تولید ۱ است، بهره‌بردار راهبرد دفاعی خود که همان برنامه بهینه تولید شبکه است را تعیین می کند. جدول (۴) برنامه بهینه تولید شبکه برای مقابله با حمله فیزیکی به واحد تولید ۱ را نشان می‌دهد.

برای حل مسئله بهینه‌سازی ارائه‌شده در این مقاله (رابطه (۱۹) به همراه قیود مربوطه)، از نرم افزار GAMS استفاده شده است. از آنجایی که رابطه بهینه‌سازی (۱۹) و قیود (۲۰)، (۸)-(۱۶) و (۳) همگی خطی هستند، نرم افزار از حل‌گر CPLEX برای تعیین نقطه بهینه استفاده کرده است.

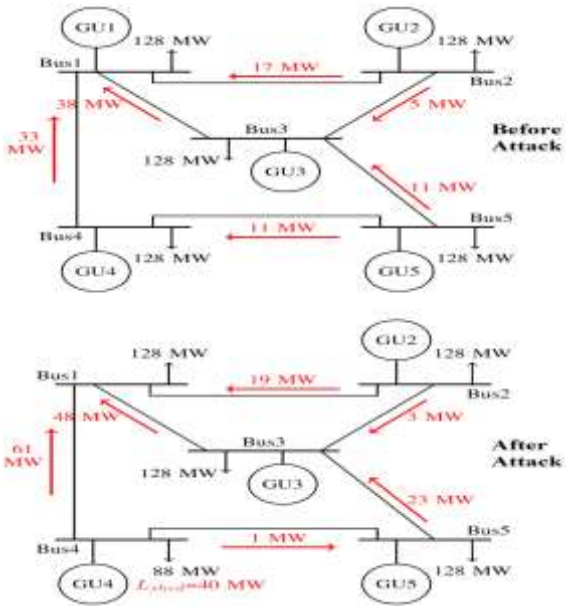
جدول ۴. راهبرد دفاعی بهره‌بردار برای مقابله با حمله به واحد تولید ۱

قبل از وقوع حمله					
	GU1	GU2	GU3	GU4	GU5
P_i	۴۰ MW	۱۵۰MW	۱۵۰MW	۱۵۰MW	۱۵۰MW
R_i^U	۰ MW	۰ MW	۰ MW	۰ MW	۰ MW
R_i^D	۰ MW	۰ MW	۰ MW	۰ MW	۰ MW
بعد از وقوع حمله					
	GU1	GU2	GU3	GU4	GU5
r_i^U	۰ MW	۰ MW	۰ MW	۰ MW	۰ MW
r_i^D	۰ MW	۰ MW	۰ MW	۰ MW	۰ MW

در صورت به‌کارگیری این راهبرد دفاعی، مقادیر توان عبوری از خطوط انتقال قبل و بعد از وقوع حمله بر روی شکل (۳) نشان داده شده است. همان‌گونه که از شکل (۳) مشخص است، بهره‌بردار برای حفظ تعادل تولید و مصرف شبکه باید ۴۰ مگاوات توان از باس ۴ را قطع نماید که ارزان‌ترین VOLL را دارد. هزینه کل وارد بر شبکه در صورت حمله فیزیکی به واحد تولید ۱ با فرض اینکه قطعی بار ناشی از آن یک ساعت به طول بینجامد، برابر با ۲۶۶۵۰ دلار خواهد بود که تفکیک این هزینه در جدول (۵) آورده شده است.

جدول ۵. هزینه کل‌وارد بر شبکه به ازای حمله فیزیکی به واحد تولید ۱

هزینه تولید انرژی	هزینه توان ذخیره	هزینه قطع بار	هزینه کل
۱۴۶۵۰ دلار	-	۱۲۰۰۰ دلار	۲۶۶۵۰ دلار



شکل ۳. توان خطوط قبل و بعد از حمله فیزیکی به واحد تولید ۱

جدول ۶. بار تغییریافته در اثر حمله سایبری تزریق داده اشتباه

بار	L_1	L_2	L_3	L_4	L_5
تغییر یافته	۵۰ MW	۱۷۰ MW	۹۰ MW	۳۰ MW	۳۰۰ MW

جدول ۷. راهبرد دفاعی بهره‌بردار برای مقابله با حمله سایبری - فیزیکی به واحد تولید ۱ و تغییر بارها مطابق جدول (۶)

قبل از وقوع حمله					
	GU1	GU2	GU3	GU4	GU5
P_i	۱۱۸ MW	۱۵۰ MW	۱۵۰ MW	۷۲ MW	۱۵۰ MW
R_i^U	۰ MW	۰ MW	۰ MW	۲۰ MW	۰ MW
R_i^D	۰ MW	۰ MW	۰ MW	۰ MW	۰ MW
بعد از وقوع حمله					
	GU1	GU2	GU3	GU4	GU5
r_i^U	۰ MW	۰ MW	۰ MW	۰ MW	۰ MW
r_i^D	۰ MW	۰ MW	۰ MW	۰ MW	۰ MW

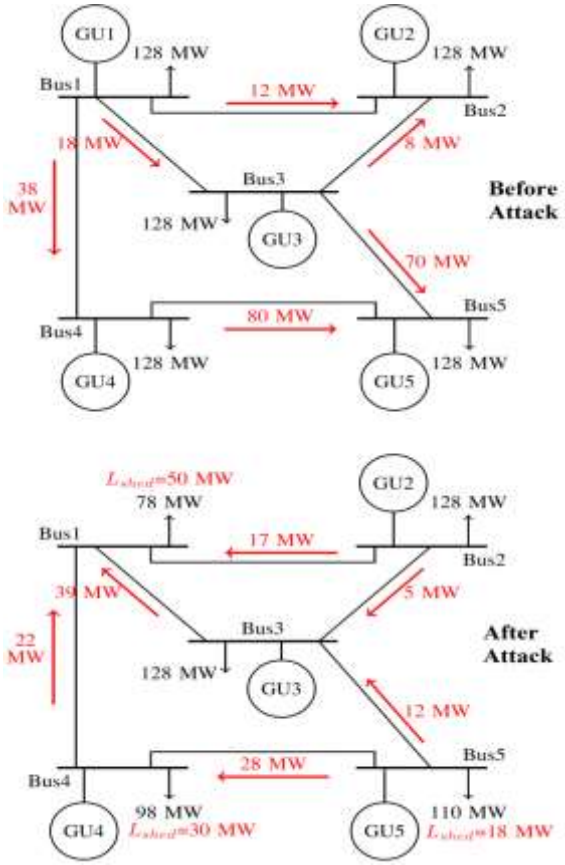
حال فرض کنید که مهاجم علاوه بر حمله فیزیکی به واحد ۱، بردار بارهای اندازه‌گیری شده شبکه را مطابق جدول (۶) تغییر دهد. در این صورت، بهره‌بردار بر اساس اطلاعات اشتباه جدول (۶) اقدام به پخش بار کرده است. در صورت وقوع حمله سایبری - فیزیکی مذکور، راهبرد دفاعی بهینه بهره‌بردار برای برنامه‌ریزی تولید شبکه به‌صورت جدول (۷) در می‌آید. با به‌کارگیری راهبرد دفاعی جدول (۷)، توان عبوری از شبکه قبل و بعد حمله در شکل (۴) نشان داده شده است.

هزینه کل وارد بر شبکه در صورت حمله سایبری - فیزیکی شرح داده شده با فرض اینکه قطعی بار ناشی از آن یک ساعت به

طول بینجامد، برابر با ۴۵۵۵۵ دلار خواهد بود که تفکیک این هزینه در جدول (۸) آورده شده است.

جدول ۸. هزینه کل وارد بر شبکه به ازای حمله فیزیکی به واحد تولید ۱ و تغییر بار مطابق جدول (۶)

هزینه تولید انرژی	هزینه توان ذخیره	هزینه قطع بار	هزینه کل
۱۳۶۵۵ دلار	۷۰۰ دلار	۳۱۲۰۰ دلار	۴۵۵۵۵ دلار



شکل ۴. توان خطوط قبل و بعد از حمله سایبری - فیزیکی به واحد تولید ۱ و تغییر بار مطابق جدول (۶)

۴-۲. راهبرد بهینه دفاعی و تهاجمی

مطابق نظریه بازی، مهاجم هوشمند راهبردی را برای حمله برمی‌گزیند که بیشترین هزینه به شبکه وارد گردد. در سوی مقابل، مدافع هوشمند نیز با شناسایی این راهبرد تهاجمی، راهبرد دفاعی خود را به‌گونه‌ای انتخاب می‌کند که خسارت شبکه در اثر این حمله کمینه گردد. درصورتی‌که تخصیص راهبرد دفاعی باعث شود که خسارت حمله در راهبرد تهاجمی بهینه مهاجم، از یک راهبرد تهاجمی دیگر، کمتر گردد، راهبرد دوم به‌عنوان راهبرد بهینه تهاجمی انتخاب می‌گردد. در این صورت مدافع بخش از منابع دفاعی خود را معطوف به راهبرد دوم می‌کند تا خسارت حمله در راهبرد اول و دوم متعادل گردد. این روند تخصیص منابع و تغییر راهبرد تهاجمی تا جایی ادامه می‌یابد که اصطلاحاً تعادل نش حاصل گردد. در این نقطه، نه مهاجم می‌تواند خسارت حمله را از مقدار مشخص در تعادل نش بیشتر نماید نه مدافع می‌تواند آن را کمتر کند. به خسارت در نقطه تعادل نش، مینیمم خسارت بدبینانه اطلاق می‌گردد.

نقطه تعادل نش برای شبکه فوق به‌ازای تمامی سناریوهای حمله با استفاده از نرم‌افزار GAMS محاسبه شده است. باتوجه‌به محاسبه انجام شده، راهبرد بهینه تهاجمی عبارت است از حمله همزمان فیزیکی به واحد تولید شماره ۳ به همراه حمله سایبری تغییر بار اندازه‌گیری شده مطابق با جدول (۹). برای این راهبرد تهاجمی، راهبرد دفاعی بهینه مطابق جدول (۱۰) محاسبه شده است. در این صورت، مینیمم هزینه بدبینانه یا هزینه شبکه در نقطه تعادل نش برابر خواهد بود با مقدار ۶۳۳۹۵ دلار که تفکیک آن در جدول (۱۱) آورده شده است.

درصورتی‌که بهره‌بردار شبکه توان ذخیره‌ای را برای شبکه لحاظ نکند و یا برنامه‌ریزی تولید خود را به‌گونه‌ای غیر از جدول (۱۰) تعیین نماید، هزینه حمله فیزیکی به واحد تولید ۳ به همراه حمله سایبری همزمان مطابق جدول (۹)، از ۶۳۳۹۵ دلار بیشتر خواهد بود. به عنوان نمونه، اگر بهره‌بردار توان ذخیره را به شبکه اختصاص ندهد هزینه وارد بر شبکه بعد از حمله مذکور برابر با ۷۱۶۲۵ دلار خواهد بود.

جدول ۹. بار تغییریافته بهینه در راهبرد بهینه مهاجم

بار	L_1	L_2	L_3	L_4	L_5
تغییر یافته	۵ MW	۱۴۳ MW	۲۰۸ MW	۱۱ MW	۲۷۳ MW

جدول ۱۰. راهبرد دفاعی بهینه بهره‌بردار برای مقابله با حمله سایبری - فیزیکی به واحد تولید ۳ و تغییر بارها مطابق جدول (۹)

قبل از وقوع حمله

	GU1	GU2	GU3	GU4	GU5
P_i	۱۴۷ MW	۱۵۰ MW	۱۵۰ MW	۴۳ MW	۱۵۰ MW
R_i^U	۰ MW	۰ MW	۰ MW	20 MW	۰ MW
R_i^D	۰ MW	۰ MW	۰ MW	0 MW	۰ MW

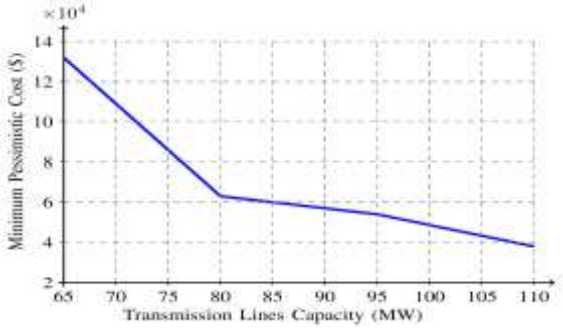
بعد از وقوع حمله

	GU1	GU2	GU3	GU4	GU5
r_i^U	۳ MW	۰ MW	۰ MW	۲۰ MW	۰ MW
r_i^D	۰ MW	۰ MW	۰ MW	۰ MW	۰ MW

جدول ۱۱. هزینه کل وارد بر شبکه به ازای حمله فیزیکی به واحد تولید ۱ و تغییر بار مطابق جدول (۶)

هزینه تولید انرژی	هزینه توان ذخیره	هزینه قطع بار	هزینه کل
۱۳۱۲۵ دلار	۷۹۰ دلار	۴۹۴۸۰ دلار	۶۳۳۹۵ دلار

به‌منظور نشان‌دادن تأثیر ظرفیت خطوط انتقال بر مینیمم هزینه بدبینانه وارد بر شبکه، مطالعه فوق به‌ازای ظرفیت‌های مختلف برای خطوط انتقال انجام شده و نتیجه در شکل (۵) نشان‌داده‌شده است. همان‌گونه که از شکل (۵) مشخص است، در شبکه ۵ با سه موردمطالعه زمانی که ظرفیت خطوط انتقال کمتر از ۸۰ مگاوات است، مینیمم هزینه بدبینانه وارد بر شبکه بر اثر حمله به‌شدت افزایش می‌یابد. دلیل این اتفاق اثرگذاری بیشتر حمله سایبری در حمله هم‌زمان سایبری - فیزیکی بر بارزدایی در شرایطی که خطوط انتقال ظرفیت کمتری دارند، است. با افزایش ظرفیت خطوط انتقال به بیش از ۸۰، مینیمم هزینه بدبینانه شبکه با شیب کمتری کاهش می‌یابد. این امر نشان می‌دهد که با افزایش ظرفیت خطوط انتقال، اثر حمله فیزیکی در حمله هم‌زمان سایبری - فیزیکی که منجر به کمبود ۴۰ مگاوات توان تزریقی به شبکه می‌شود، بیشتر است و حمله سایبری تا حدی کم‌اثر می‌گردد.



شکل ۵. مینیمم هزینه بدبینانه به ازای ظرفیت‌های مختلف خطوط انتقال

۵. نتیجه‌گیری

در این مقاله نشان داده شد که حمله هوشمند سایبری - فیزیکی می‌تواند میزان بارزدایی شبکه را به میزان قابل‌توجهی افزایش دهد و هزینه زیادی بر شبکه تحمیل نماید. هزینه وارد بر شبکه تلفیقی از هزینه بارزدایی (قطع بار) شبکه و هزینه ناشی از تخصیص و به‌کارگیری اقدامات اصلاحی توان ذخیره است. مطابق نظریه بازی، بهره‌بردار می‌تواند برای کاهش هزینه حمله هوشمند سایبری - فیزیکی برنامه‌ریزی تولید شبکه را به‌گونه‌ای بهینه تخصیص دهد تا هزینه حمله هوشمندانه به شبکه تاحدامکان کمینه گردد. نتایج شبیه‌سازی نشان داد که مینیمم هزینه بدبینانه وارد بر شبکه در اثر حمله سایبری - فیزیکی، به‌شدت ظرفیت خطوط انتقال شبکه وابسته است؛ لذا می‌توان انتظار داشت وقوع حمله هم‌زمان سایبری - فیزیکی به شبکه توسط مهاجم هوشمند در مواقع پرباری شبکه که ظرفیت زیادی از خطوط اشغال شده است، انجام شود. در یک برنامه‌ریزی بلندمدت، بهره‌بردار شبکه به‌منظور کاهش هزینه حملات سایبری و حملات هم‌زمان سایبری - فیزیکی، باید ظرفیت خطوط انتقال را افزایش دهد.

۶. مرجع‌ها

[1] Amin, M. “Energy Infrastructure Defense Systems”; Proc. IEEE 2005, 93, 861-876. http://doi.org/10.1109/JPROC.2005.847257

[2] Pablo, H.; Ruiz, M. E. “Against All Odds”; IEEE Power Energy Mag. 2011, 9, 59-66. http://doi.org/10.1109/MPE.2011.940266

[3] Baozhong, T.; Wang, J.; Li, G. “Operational Risk-Averse Routing Optimization for Cyber-Physical Power Systems”; CSEE Journal of Power and Energy Systems, 2022, 8, 801–811. http://doi.org/10.17775/CSEEJPES.2021.00370

[4] Liang, G.; Weller, S. R.; Zhao, J.; Luo, F. “The 2015 Ukraine Blackout: Implications for False Data Injection Attacks”; IEEE Trans. Power Syst. 2017, 32, 3317-3318. http://doi.org/10.1109/TPWRS.2016.2631891

[5] Shayan, H.; Amraee, T. “Network Constrainted Unit Commitment under Cyber Attack Driven Overloads”; IEEE Trans. Smart Grid, 2019, 10, 6449–6460. http://doi.org/10.1109/TPWRS.2016.2631891

[6] Li, F.; Yan, X.; Xie, Y. “A Review of Cyber-Attack Methods in Cyber-Physical Power System”; IEEE 8th International Conference on Advanced Power System Automation and protection, 2019. http://doi.org/10.1109/APAP47170.2019.9225126

[7] Ranjbar, M. H.; Pirayesh, A. “Optimal Reserve Allocation of Power System in Critical Situation for Preparation against Threats”; Advance Defense Sci. & Technol., 2016, 8, 159–167. http://doi.org/20.1001.1.26762935.1395.7.2.7.0

[8] Viafora, N.; Delikaraoglou, S.; Pinson, P.; Hug, G. “Dynamic Reserve and Transmission Capacity Allocation in Wind-Dominated Power Systems”; IEEE Trans. Power Syst., 2021, 36, 3017–3028. http://doi.org/10.1109/TPWRS.2020.3043225

[9] Washburn, A. “Two-Person Zero-Sum Games”; US Springer, http://doi.org/2014.10.1007/978-1-4614-9050-0

[10] Ranjbar, M. H.; Kheradmandi, M.; Pirayesh, A. “Assigning Operating Reserves in Power Systems under Imminent Intelligent Attack Threat”; IEEE Trans. Power Syst. 2019, 34, 2768–2777. http://doi.org/10.1109/TPWRS.2019.2897595

[11] Ganjkhani, M.; Hosseini, M. M.; Parvania, M. “Optimal Defensive Strategy for Power Distribution Systems against Relay Setting Attacks”; IEEE Trans. Power Deliv. 2023, 38, 1499–1509. http://doi.org/10.1109/TPWRD.2022. 3230946

[12] Yan, B.; Yao, P.; Yang, T.; Zhou, B. “Game-Theoretical Model for Dynamic Defense Resource Allocation in Cyber-Physical Power Systems under Distributed Denial of Service Attacks”; J. Mod. Power Syst. Clean Energy, 2023, 38, 1-10. http://doi.org/10.35833/MPCE.2022.000524

[13] Yan, K.; Liu, X.; Lu, Y. “A Cyber-Physical Power System Risk Assessment Model against Cyberattacks”; IEEE Syst. J., 2023, 17, 218–228. http://doi.org/10.1109/JSYST.2022.3215591

[14] “The US Blackout Timeline”; Power Eng., 2003, 17, 11–1.

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, 76–84. http://doi.org/10.1109/TPWRS.2010.2078524