*مقاله پژوهشی*

# برنامه‌ریزی مقاوم حمله تزریق داده غلط روی بازارهای انرژی الکتریکی در شبکه‌های هوشمند

حامد بدرسیمایی، رحمت‌الله هوشمند و صغری نوبختیان

**چکیده: حمله تزریق داده غلط (FDIA) یک تهدید سایبری مخرب برای عملکرد اقتصادی بازارهای انرژی الکتریکی در شبکه‌های هوشمند است. یک مهاجم سایبری می‌تواند با پیاده‌سازی یک FDIA و با نفوذ در معاملات مجازیبازارهای انرژی الکتریکی، از طریق دستکاری قیمت برق به سود مالی گزافی دست پیدا کند. در این مقاله، روش جدیدی در مسأله برنامه‌ریزی یک FDIA به صورت کاملاً مخفی و با هدف دستیابی به بیشترین سود مالی از دیدگاه یک مهاجم سایبری مشارکت‌کننده در معاملات مجازی در دو بازار روز پیش (DA) و زمان حقیقی (RT) ارائه شده است. یک فرضیه رایج که در مطالعات موجود روی FDIAs در مقابل بازارهای برق صورت گرفته، این است که مهاجم، اطلاعات کاملی از شبکه هوشمند در اختیار دارد. اما واقعیت این است که مهاجم، منابع محدودی دارد و به سختی می‌تواند به همه اطلاعات شبکه دسترسی پیدا کند. این مقاله روش مقاومی را در طراحی استراتژی حمله با شرایط اطلاعات شبکه ناقص پیشنهاد می‌کند. به طور خاص فرض گردیده که مهاجم نسبت به ماتریس‌های مدل‌کننده شبکه دارای عدم قطعیت است. اعتبار روش پیشنهادی بر اساس سیستم معیار ۱۴- باس IEEE و با استفاده از ابزار Matpower سنجیده شده است. نتایج عددی، موفقیت نسبی حمله پیشنهادی را در حالت‌های از درجه مختلف اطلاعات ناقص تأیید می‌کنند.**

***کلیدواژه:* بازار انرژی الکتریکی، حمله سایبری، حمله تزریق داده غلط، شبکه هوشمند، عدم قطعیت.**

## ۱- مقدمه

وقوع حملات سایبری روی شبکه‌های الکتریکی هوشمند نسبت به قبل محتمل‌تر شده است؛ زیرا بهره‌برداری شبکه هوشمند به شدت وابسته به اطلاعات ناهماهنگ جمع‌آوری شده از دستگاه‌های اندازه‌گیری مختلف مثل دستگاه الکترونیکی هوشمند پست (SIED)[1]، واحد اندازه‌گیری فازور (PMU)[2] و دیگر سنسورهای هوشمند مستقرشده در شبکه است. این در حالی است که سیستم‌های اندازه‌گیری و زیرساخت‌های ارتباطاتی، در معرض حملات سایبری قرار دارند. اخیراً حمله تزریق داده غلط (FDIA)[3] به عنوان یک نوع بسیار مخرب از حملات سایبری ظهور پیدا کرده است. از طریق دستکاری یک تعداد از دستگاه‌های اندازه‌گیری و تزریق اطلاعات نادرست، یک مهاجم سایبری می‌تواند تخمینگر حالت را در سیستم قدرت، مورد هدف قرار دهد تا تخمینی غلط از حالت سیستم زمان حقیقی (RT)[4] حاصل شود [۱] و [۲]. بنابراین با استفاده از FDIA، یک مهاجم می‌تواند به طور قابل توجهی روی همه بخش‌های مختلف شبکه مانند مانیتور، حفاظت، کنترل و بهره‌برداری اقتصادی سیستم تأثیرگذار باشد. بر این اساس، مهاجم مخرب می‌تواند به یک رنج وسیعی از اهداف، از به‌خطرافتادن امنیت شبکه گرفته تا جلوگیری از بهره‌برداری زمان حقیقی سیستم یا ایجاد سودآوری مالی از طریق دستکاری قیمت انرژی در بازارهای برق دست یابد. به منظور اقدام متقابل برای اپراتور سیستم مطلوب است تا اثر چنین حمله‌ای را روی شبکه هوشمند بررسی کند. مقابله با حملات تزریق داده، ذاتاً به دلیل قابلیت مخفی‌بودن آنها بسیار چالش‌برانگیز می‌باشد و عمل تشخیص آنها را دشوار کرده است. در واقع، حملات تزریق داده می‌تواند در پروسه تخمین حالت سیستم مداخله نماید و در عین حال توسط اپراتور شبکه هوشمند غیر قابل تشخیص باشد [۳].

تا کنون چندین شبکه برق در جهان، قربانی حملات سایبری شده‌اند که باعث خرابی غیرمنتظره دستگاه‌ها و قطع برق در مقیاس وسیع گردیده است؛ بنابراین امنیت سایبری، مهم‌ترین موضوع در امر توسعه شبکه‌های برق قلمداد شده است. در زمینه مالی، توسعه و مقررات‌زدایی از بازارهای برق نباید دروازه‌ای برای حملات سایبری سودمحور ایجاد شود. اگرچه بررسی‌های گسترده‌ای در مورد حملات سایبری انجام شده است اما با این حال، بررسی جامع و عمیقی از حملات روی بازارهای برق صورت نگرفته تا آگاهی عمومی را نسبت به اختلاس‌های قابل توجه پولی حتی توسط مهاجمان محدودشده بدهد [۴]. هدف مقاله برای گسترش یک چهارچوب ریاضی جدید برای تحقیق در این زمینه آن است که چگونه یک مهاجم از FDIA از طریق دستکاری اطلاعات شبکه سیستم قدرت بر روی بهره‌برداری‌های بازار برق زمان حقیقی سود می‌برد. مطالعات و کارهای موجود روی حملات تزریق داده روی شبکه‌های هوشمند در [۳] تا [۱۱] آمده است. کار در [۵] یک آنالیز از اثرات اقتصادی تزریق داده را روی بازارهای برق در شبکه قدرت هوشمند معرفی می‌کند. در این مرجع فرض شده که یک مهاجم با اطلاعات کاملی که از شبکه در اختیار دارد در معاملات مجازی بازار برق شرکت می‌کند و استراتژی حمله خود را بر اساس دستکاری قیمت برق در جهت بیشترین سودآوری و با رعایت همه محدودیت‌های حمله طراحی می‌کند. در [۶]، عملیات حمله تزریق داده در محیط بازار برق برای یک میکروشبکه متصل‌شده به سیستم قدرت در

این مقاله در تاریخ ۳۱ خرداد ماه ۱۴۰۰ دریافت و در تاریخ ۱۲ دی ماه ۱۴۰۱ بازنگری شد.

حامد بدرسیمایی، دانشکده فنی مهندسی، گروه مهندسی برق، دانشگاه اصفهان، اصفهان، ایران، (email: badr_hamed@eng.ui.ac.ir).

رحمت‌الله هوشمند (نویسنده مسئول)، دانشکده فنی مهندسی، گروه مهندسی برق، دانشگاه اصفهان، اصفهان، ایران، (email: hooshmand_r@eng.ui.ac.ir).

صغری نوبختیان، دانشکده علوم ریاضی، دانشگاه اصفهان، اصفهان، ایران، (email: nobakht@sci.ui.ac.ir).

1. Substation Intelligent Electronic Device
2. Phasor Measurement Unit
3. False Data Injection Attack
4. Real-Time

نظر گرفته شده است. این حمله می‌تواند خروجی‌های بهینه مدیریت انرژی میکروشبکه مانند هزینه کل تولید را تحت تأثیر قرار دهد. مرجع [۷]، درآمدزایی حمله داده مخرب را روی بازارهای تولید انرژی الکتریکی و استراتژی لازم را برای بیشینه‌سازی درآمد پیشنهاد می‌دهد. مرجع [۸]، حمله توزیع بار (LR)[1] را به عنوان یک نوع از FDIA پیشنهاد می‌دهد که می‌تواند بهره‌برداری شبکه هوشمند را توسط حمله به پخش بار اقتصادی مقید به قیود امنیت (SCED)[2] تحت تأثیر قرار دهد. برای رفع این مشکل، [۹] مسأله پخش بار اقتصادی مقاوم توزیع‌شده را تحت حملات سایبری معرفی کرده است. با هدف کنترل مستقیم قیمت‌های حاشیه محلی (LMPs)[3] در زمان حقیقی از طریق FDIA، [۱۰] یک تئوری کنترل را بر اساس روشی برای آنالیز اثر حمله روی پایداری قیمت‌گذاری پیاده‌سازی می‌کند. در [۱۱] و [۱۲]، یک بازی مجموع صفر بین یک مهاجم و یک مدافع فرمول‌بندی می‌شود که در آن مهاجم، توان عبوری تخمینی از خطوط را برای دستکاری قیمت‌ها تغییر می‌دهد. بر اساس این تئوری بازی، یک مسأله بهینه‌سازی دوسطحی شکل گرفته است. در [۱۳] و [۱۴]، اثر اقتصادی حملات اطلاعات ساختاری به عنوان نوعی تعمیم‌یافته از FDIA در بازارهای برق با استفاده از فعالیت‌های مناقصه مجازی بررسی شده است. اطلاعات ساختاری شبکه‌های هوشمند برای بهره‌برداری سیستم جهت مدیریت شبکه در مسیر ایمن، بسیار حیاتی است اما این اطلاعات می‌تواند توسط یک مهاجم سایبری از طریق تغییر وضعیت روشن/خاموش‌شدن کلیدهای قدرت دستکاری شود. علاوه بر اینها اخیراً در [۱۵]، یک استراتژی حمله پیشنهاد شده که در آن مهاجم سایبری می‌تواند LMPs را به طور مؤثر از طریق دستکاری برخی از پارامترهای حیاتی مدل تغییر دهد و به سود مالی دست یابد.

همچنین یک FDIA می‌تواند به خوبی با یک حمله فیزیکی هماهنگ شود و در واقع حمله فیزیکی- سایبری هماهنگ‌شده (CCPA) را ایجاد کند که تأثیر مخرب‌تری بر عملکرد نرمال شبکه هوشمند دارد. در [۱۶]، حمله هماهنگ‌شده شامل اتصال کوتاه کردن فیزیکی خطوط انتقال، بعد از اعمال نفوذ به شبکه ارتباطی با لایه‌های حفاظت سایبری است. مرجع [۱۷] با هدف به حداکثر رساندن اختلال در بازارهای برق روز پیش (DA)[4] و زمان حقیقی، اقدام به طرح‌ریزی CCPA کرده است. مرجع [۱۸]، یک حمله یک CCPA مبتنی بر تخمین حالت AC را برای مختل‌کردن بهره‌برداری بازار برق از طریق دستکاری قیمت‌های گرهی پیشنهاد می‌کند.

همه مطالعات مربوطه فوق بر اساس این فرضیه است که مهاجم سایبری، دانش کاملی در مورد اطلاعات شبکه هوشمند مورد هدف دارد که شامل توپولوژی شبکه، پارامترهای شاخه‌ها و غیره است. در حقیقت، در هر شبکه هوشمند داده‌شده، اطلاعات شبکه وسیع و بسیار امن و حیاتی است. علاوه بر این، اطلاعات دینامیکی هستند؛ زیرا توپولوژی شبکه می‌تواند در هر دو وضعیت نرمال و وقوع پیشامد مجدداً پیکربندی شود. بنابراین در عمل دسترسی به اطلاعات کامل شبکه برای یک مهاجم محدودشده بسیار مشکل است. در چندین کار اخیر بر اساس [۹] تا [۱۱]، تا حدودی به این چالش مهاجم در طراحی FDIA با توجه به ابزارها، تکنیک‌ها و الزامات مختلف پرداخته شده است. در [۱۹] مهاجم بدون دانش قبلی از توپولوژی شبکه و تنها از طریق مشاهدات فازور با استفاده از آنالیز مؤلفه مستقل خطی، یک حمله مخفی و سودآور را فرمول‌بندی کرده است. در [۲۰]، مهاجم فقط بر اساس اطلاعات زمان حقیقی دریافتی از دستگاه‌های اندازه‌گیری و بدون نیاز به اطلاعات توپولوژی شبکه، یک استراتژی حمله آنلاین را علیه بازار برق زمان حقیقی طراحی می‌کند. حمله تزریق داده سودآور روی بازارهای برق توسط مهاجمین محدودشده با اطلاعات ناقص شبکه در [۲۱] بررسی گردیده است. در این مرجع، عدم قطعیت‌های مرتبط با اطلاعات شبکه به طور تصادفی، مدل و یک چهارچوب احتمالی برای طراحی حمله غیر قابل تشخیص و سودآور ارائه شده است. از ایرادات موجود در این مرجع، نیاز به وجود داده‌های گذشته برای برآورد مناسب توابع توزیع احتمال پارامترها است.

با توجه به کارهای مرتبط فوق از طریق این مقاله، یک استراتژی FDIA به صورت مقاوم در برابر بازار برق زمان حقیقی در شبکه هوشمند پیشنهاد و طراحی می‌گردد؛ به طوری که عدم قطعیت‌های مرتبط با مدل‌سازی مسأله حمله و شبکه مورد مطالعه در نظر گرفته شود. در واقع، ایده ارائه طرح حمله جدید بر اساس رفع یک کاستی در طرح حمله پیشنهادشده در [۲۲] و [۲۳] است که مهاجم در آن، مدل‌سازی مسأله بهینه‌سازی حمله را بر اساس سناریوهای تولیدشده با روش مونت‌کارلو انجام می‌دهد. اما از آنجایی که مشخص‌کردن توابع توزیع‌های احتمالاتی متغیرهای تصادفی، شرط اجرای الگوریتم مونت‌کارلو است، یک مهاجم محدودشده قادر به دستیابی چنین اطلاعات گسترده‌ای که وابسته به سوابق گذشته شبکه است نخواهد بود و در نتیجه طرح حمله نمی‌تواند چندان کارآمد و عملی باشد. لذا در طرح حمله جدید، تمرکز بر روی تنظیماتی است که در آن مهاجم، دانش ناقصی از متغیرهای طراحی را به صورت بازه‌ای و مستقل از سوابق گذشته شبکه مدل‌سازی می‌کند. در واقع این عدم قطعیت در تعریف متغیرها با تعریف ماتریس‌های شبکه در محدوده خطای مشخص مدل‌سازی شده است و بر این اساس مهاجم باید جواب نهایی را با توجه به یک مجموعه سناریوهای ممکن تعیین کند. از آنجایی که هدف حمله، کسب سود در یک سطح اطمینان معین است، یک مهاجم علاقه‌مند به تعیین بدترین حالت مورد اطمینان سودآور روی کل فضای جواب است. در این مقاله نشان داده شده که طراحی چنین استراتژی حمله‌ای منجر به حل یک مسأله بهینه‌سازی غیر محدب تصادفی است. علی‌رغم اینکه چنین مسائل بهینه‌سازی تصادفی برای حل در کلی‌ترین فرم به صورت NP- سخت هستند [۲۴]، در ادامه با استفاده از تکنیک‌های ریاضی نشان داده شده که می‌توان آن را به سادگی یک مسأله بهینه‌سازی معادل مقاوم تبدیل کرد که به طور مؤثر از طریق روش‌های بهینه‌سازی قطعی استاندارد مثل روش نقطه درونی قابل حل است [۲۵].

ادامه مقاله به صورت زیر سازماندهی شده است. در بخش دوم، مدل شبکه و ساختار بازار برق شرح داده می‌شود. در بخش سوم، مدل یک FDIA غیر قابل تشخیص و سودآور در شرایط قطعیت اطلاعات شبکه فرمول‌بندی گردیده است. در بخش چهار، مدل FDIA پیشنهادی با وجود عدم قطعیت‌ها معرفی شده و در بخش پنجم، شبیه‌سازی‌ها در سیستم تست ۱۴- باس IEEE برای بررسی مقاوم‌بودن روش پیشنهادی تحت درجه مختلف از عدم قطعیت‌های مدل مسأله فراهم شده است.

## ۲- بازارهای برق و تئوری تخمین حالت تحت یک FDIA

ابتدا در این بخش، مروری بر بازارهای انرژی الکتریکی و تئوری تسویه بر اساس مدل پخش بار بهینه (OPF) ارائه گردیده و سپس بر

1. Load Redistribution
2. Security-Constrained Economic Dispatch
3. Locational Marginal Prices
4. Day-Ahead

روی تخمین حالت در مدل‌سازی DC شبکه و تأثیرپذیری نتایج تخمین حالت از یک FDIA بحث شده است.

## ۲-۱ بازارهای انرژی الکتریکی

بازارهای برق مقررات‌زدایی‌شده مانند بازار PJM[1] به طور کامل توسط اپراتور مستقل شبکه هوشمند اداره می‌شود. برای تضمین پایداری و بهره‌برداری کارآمد، اپراتور شبکه با تکیه بر اطلاعات دقیق در رابطه با بازارهای برق، مقرون‌به‌صرفه‌ترین واحدهای تولیدی را برای تأمین بارها در سراسر شبکه تعیین می‌کند. ساختارهای بازارهای انرژی رقابتی اغلب بر اساس بازارهای روز پیش (DA) و زمان حقیقی (RT) است [۲۶]. اپراتور شبکه در بازار DA، قیمت‌های حاشیه محلی مبتنی بر ساعت (LMPs) را برای بهره‌برداری روز آینده بر اساس پیشنهادهای انرژی DA مشارکت‌کنندگان تعیین می‌کند [۲۷]. روند تسویه بازار توسط اپراتور شبکه از طریق حل یک مسأله پخش بار بهینه خطی‌شده (DCOPF)[2] انجام می‌گیرد که مقادیر بهینه تولید هر ژنراتور مشارکت‌کننده در بازار و مقادیر DA-LMPs را در هر باس ایجاد می‌کند. رایج‌ترین فرمول‌بندی DCOPF به کار رفته به صورت زیر است [۲۷]

$$\min_{p} \sum_{g\in G} C_g(p_g) \qquad (۱)$$

s.t. :

$$(\lambda^{DA}) : \sum_{g\in G} p_g - \sum_{n\in N} d_n = ۰ \qquad (۲)$$

$$(\tau_g^{DA}) : p_g^{\min} \le p_g \le p_g^{\max} \ , \ \forall g \in G \qquad (۳)$$

$$(\gamma_l^{DA}) : f_l^{\min} \le f_l \le f_l^{\max} \ , \ \forall l \in L \qquad (۴)$$

که مجموعه‌های $\mathrm{N}=\{۱,\dots,N\}$ ، $\mathrm{L}=\{۱,\dots,L\}$ و $\mathrm{G}=\{۱,\dots,G\}$ به ترتیب مربوط به کل $N$ باس، $L$ خط انتقال و $G$ ژنراتور شبکه است. $p_g$ نشان‌دهنده خروج توان اکتیو و $C_g(.)$ تابع هزینه تولید برای ژنراتور $g\in \mathrm{G}$ است. $d_n$ سطح بار پیش‌بینی شده (تقاضا) در باس بار $n\in \mathrm{N}$ است. در (۱)، تابع هدف برای حداقل‌سازی هزینه کل ژنراتورها است. قید (۲) برای ایجاد تعادل توان در کل شبکه است. قید (۳) مربوط به ظرفیت تولید هر ژنراتور است که محدود به مقدار حداقل $p_g^{\min}$ و حداکثر $p_g^{\max}$ است. قید (۴)، محدودیت‌های حداکثر $f_l^{\max}$ و حداقل $f_l^{\min}$ را روی سطح توان خالص عبوری از خط $l$ ایجاد می‌کند؛ به طوری که نقض این قید نشان‌دهنده وجود تراکم برای آن خط است. همچنین $\lambda^{DA}$، $\tau^{DA}$ و $\gamma^{DA}$ مجموعه ضرایب لاگرانژ مرتبط با قیود بهره‌برداری برای حل مسأله DCOPF در بازار DA هستند. در نهایت اپراتور شبکه هوشمند مقادیر $p_g$ را به همه ژنراتورها به عنوان تولید مرجع ارسال می‌کند و پرداخت‌های DA از مصرف‌کنندگان در همه باس‌ها جمع‌آوری می‌شود.

در بازار RT به دلیل ماهیت تصادفی بار و تولید واقعی شبکه (خروج از وضعیت بهره‌برداری بهینه)، LMPs در زمان حقیقی از طریق مسأله DCOPF افزایشی به‌روزرسانی می‌شوند. لذا اپراتور شبکه به نتایج تخمین حالت که منعکس‌کننده حالت زمان حقیقی شبکه است احتیاج دارد. بر این اساس در ابتدا لازم است که اپراتور شبکه، متغیرهای حالت زمان حقیقی شبکه را با داده‌های اندازه‌گیری موجود تخمین بزند. فرض می‌شود که توان‌های خالص تزریقی به باس‌ها به عنوان متغیرهای حالت باشد (مشخص‌شده با بردار $X=[x_۲,\dots,x_N]^T$). ماتریس $H$ نیز به عنوان ماتریس ضرایب انتقال تولید تعریف می‌شود که حساسیت توان‌های عبوری از خطوط را (مشخص‌شده با بردار $F=[f_۱,\dots,f_L]^T$) به تغییرات توان‌های تزریقی به باس‌ها، $x$، به صورت زیر نشان می‌دهد

$$F_{(L\times ۱)} = H_{(L\times N)} \times X_{(N\times ۱)} \qquad (۵)$$

بنابراین حساسیت توان عبوری از خط $l\in \mathrm{L}$ به تغییرات در توان تزریقی به باس $n\in \mathrm{N}$ با $H_{ln}$ نشان داده می‌شود.

یک مدل DCOPF افزایشی برای محاسبه RT-LMPs می‌تواند به صورت زیر فرمول‌بندی شود [۲۶] و [۲۸]

$$\min_{\Delta p} \sum_{g=۱}^{G} C_g^{RT}(\hat{p}_g + \Delta p_g) \qquad (۶)$$

s.t. :

$$(\lambda^{RT}) : \sum_{g\in G} \Delta p_g = ۰ \qquad (۷)$$

$$(\tau_g^{RT}) : \Delta p_g^{\min} \le \Delta p_g \le \Delta p_g^{\max} \ , \ \forall g \in G \qquad (۸)$$

$$(\gamma_l^{RT}) : \begin{cases} \Delta f_l \le ۰ \ , \ \forall l \in L : \hat{f}_l \ge f_l^{\max} \\ \Delta f_l \ge ۰ \ , \ \forall l \in L : \hat{f}_l \le f_l^{\min} \end{cases} \qquad (۹)$$

که در آن $C_g^{RT}$ پیشنهاد ژنراتور $g\in \mathrm{G}$ در بازار RT است و بر اساس توان‌های خروجی و منحنی عرضه مربوطه در بازار RT محاسبه می‌شود [۲۸]. $\hat{p}_g$ و $\Delta p_g$ به ترتیب به عنوان تخمین توان تولیدشده و تغییرات در توان برای ژنراتور $g$ تعریف گردیده است. $\Delta p_g^{\min}$ و $\Delta p_g^{\max}$ یک محدودیت در تغییرات تولید ژنراتور $g$ اعمال می‌کنند و معمولاً در عمل، روی مقادیر $\Delta p_g^{\min}=-۲\mathrm{MW}$ و $\Delta p_g^{\max}=+۰٫۱\mathrm{MW}$ تنظیم می‌شوند [۲۹]. همچنین $\hat{f}_l$ و $\Delta f_l$ به ترتیب به عنوان تخمین توان عبوری و تغییرات در توان برای خط انتقال $l\in \mathrm{L}$ تعریف شده است. قابل توجه این که خطوطی که در شرایط قید (۹) صدق کنند، خطوط با الگوی تراکم نامیده می‌شوند [۳۰] و در این حالت توان‌های عبوری تخمین‌زده خارج از محدودیت‌ها است. علاوه بر اینها مجموعه ضرایب لاگرانژ $\lambda^{RT}$، $\tau^{RT}$ و $\gamma^{RT}$ برای حل مسأله DCOPF افزایشی در بازار RT استفاده می‌شوند.

بدین ترتیب، DA-LMPs و RT-LMPs در هر باس $n\in \mathrm{N}$ به ترتیب توسط مسائل بهینه‌سازی (۱) تا (۴) و (۶) تا (۹) محاسبه می‌شوند. LMPs حاصل‌شده شامل هر دو هزینه افزایش انرژی در هر باس $n$ و هزینه تراکم مرتبط با سهم این باس از تراکم کل شبکه است. مقادیر DA-LMPs و RT-LMPs در هر باس $n\in \mathrm{N}$ به صورت روابط زیر تعیین می‌گردند

$$LMP_n^{DA} = \lambda^{DA} + \sum_{l\in L} H_{l,n}\gamma_l^{DA} \ , \ \forall n \in N, \qquad (۱۰)$$

$$LMP_n^{RT} = \lambda^{RT} + \sum_{l\in L} H_{l,n}\gamma_l^{RT} \ , \ \forall n \in N. \qquad (۱۱)$$

قابل توجه است که برای خطوط انتقال بدون الگوی تراکم، آنگاه $\gamma_l^{DA}=\gamma_l^{RT}=۰$ است. علاوه بر این برای هر $l\in \mathrm{L}$ هنگامی که $\hat{f}_l \ge f_l^{\max}$ (الگوی تراکم مثبت)، آنگاه $\gamma_l^{RT}>۰$ است در حالی که اگر $\hat{f}_l \le f_l^{\min}$ (الگوی تراکم منفی) باشد آنگاه $\gamma_l^{RT}<۰$ است [۵].

نتایج RT-LMPs متکی بر فرمول‌بندی DCOPF افزایشی است که به خروجی تخمینگر حالت وابسته می‌باشد. بنابراین حملات تزریق داده با هدف قرار دادن نتایج تخمین حالت بر مقادیر LMPs در (۱۱) تأثیر

1. Pennsylvania-Jersey-Maryland
2. DC Optimal Power Flow

می‌گذارند. در ادامه مدل FDIA معرفی می‌شود.

## ۲-۲ تخمین حالت و حملات تزریق داده غلط (FDIAs)

یک تخمینگر حالت شبکه هوشمند از اندازه‌گیری‌های توان جمع‌آوری شده از شبکه برای تخمین حالت سیستم استفاده می‌کند [۱] و [۳۱]. ارتباط بین بردار اندازه‌گیری‌ها، $Z$، و بردار حالت سیستم، $X$، در یک مدل تخمین حالت خطی‌شده (DC-SE)[1] به صورت زیر بیان می‌شود

$$Z = SX + E . \quad (۱۲)$$

$S$ ماتریس ژاکوبین اندازه‌گیری‌ها و $E$ بردار خطاهای تصادفی است که فرض شده از یک توزیع $\text{Normal}(۰,\Sigma_E)$ پیروی می‌کند. با استفاده از یک تخمینگر کمترین مربعات وزن‌دار (WLS)[2]، حالت سیستم تخمین زده شده به صورت زیر به دست می‌آید [۳۱]

$$\hat{X} = (S^T \Sigma_E^{-۱} S)^{-۱} S^T \Sigma_E^{-۱} Z = KZ . \quad (۱۳)$$

همچنین با استفاده از حالت‌های تخمین زده شده، یک تخمین از بردار اندازه‌گیری‌ها، $\hat{Z}$، و باقیمانده‌ها، $R$، می‌تواند مطابق روابط زیر محاسبه شود [۳۱]

$$\hat{Z} = S\hat{X} = SKZ = \Re Z \quad (۱۴)$$

$$R = Z - \hat{Z} = (I_M - \Re)Z \quad (۱۵)$$

$I_M$ ماتریس همانی در سایز $M \times M$ و $M$ تعداد کل اندازه‌گیری‌های جمع‌آوری‌شده (سیستم‌های اندازه‌گیری) است.

هنگام وقوع حملات تزریق داده (FDIA)، اندازه‌گیری‌های جمع‌آوری شده از طریق تزریق بردار حمله، $Z_a$، دچار تغییر می‌شوند؛ به عبارتی اندازه‌گیری‌های جدید به فرم $Z_{new} = Z + Z_a$ خواهد بود. بر این اساس حالت‌های تخمین زده شده، $\hat{X}$، و در نتیجه باقیمانده‌ها، $R$، بر اساس اندازه‌گیری‌های جدید به صورت زیر عوض می‌شوند [۳۱]

$$\hat{X}_{new} = KZ_{new} = \hat{X} + KZ_a \text{ و} \quad (۱۶)$$

$$R_{new} = (I_M - \Re)Z_{new} = R + (I_M - \Re)Z_a . \quad (۱۷)$$

قابل توجه است که دلیل اصلی این تغییرات می‌تواند علاوه بر حملات تزریق، در اثر عوامل دیگری مثل خرابی‌های سیستم‌های اندازه‌گیری و یا لینک‌های ارتباطی باشد [۳۱]. بر این اساس، خطاهای اندازه‌گیری نامعلوم در اثر نفوذ داده‌های بد، باعث تغییر نتایج نهایی تخمین حالت سیستم می‌شوند. سیستم‌های قدرت فعلی از تشخیصگر مبتنی بر باقیمانده برای شناسایی داده‌های بد جهت حفاظت از پروسه تخمین حالت استفاده می‌کنند. تست بزرگ‌ترین باقیمانده نرمالیزه‌شده (LNR)[3] از طریق مقایسه نرم $\ell_۲$ بردار باقیمانده‌ها ($\|R\|_۲$) با یک آستانه از پیش تعیین شده $\tau$، شناسایی اندازه‌گیری‌های بد را انجام می‌دهد. به طور دقیق اگر $\|R\|_۲ > \tau$ باشد آنگاه وجود اندازه‌گیری‌های بد احساس می‌شود و در غیر این صورت، $Z$ به عنوان اندازه‌گیری‌های نرمال در نظر گرفته می‌شود [۳۱].

## ۳- اهداف، الزامات و مدل‌سازی یک FDIA

هدف مهاجم سایبری در مدل فرض‌شده، دستکاری RT-LMPs به منظور ایجاد سود مالی از طریق تجارت مجازی است. مهاجم در یک معامله مجازی که در آن لزوماً یک تولیدکننده و یا مصرف‌کننده واقعی نیست می‌تواند از طریق پیشنهادهای عرضه و یا تقاضا در بازارهای انرژی فعالیت داشته باشد. از آنجایی که این پیشنهادهای انرژی باید در راستای یک تجارت سودآور باشد، یک مهاجم با پیشنهاد خرید (فروش) توان مجازی در یک باس مشخص در بازار DA، لازم است تا پیشنهاد فروش (خرید) همان مقدار توان را در همان باس در بازار RT داشته باشد. چنین پیشنهادهای مجازی به هدف اپراتور شبکه هوشمند در رونق و پویایی بازارهای انرژی کمک می‌کند و از طرف دیگر، مشارکت‌کنندگان مجازی نیز از سود مالی به دست آمده از عدم همگرایی احتمالی بین DA-LMPs و RT-LMPs بهره‌مند می‌شوند [۲۶] و [۳۲]. بدین ترتیب با استفاده از یک FDIA، یک پیشنهاددهنده مجازی می‌تواند RT-LMPs را برای ایجاد یک عدم همگرایی سودآور با توجه به نقطه مقابل در بازار DA دستکاری کند. در این رابطه، اپراتور شبکه باید از علت وجود شکاف در قیمت‌گذاری به واسطه وقوع حمله بی‌خبر باشد. این یک شرط لازم برای تدارک یک FDIA موفقیت‌آمیز است که در ادامه مدل شده و مورد بررسی قرار گرفته است.

## ۳-۱ استراتژی حمله غیر قابل تشخیص

همان طور که قبلاً بیان گردید، معیار تشخیص هر داده بد تزریقی به اندازه‌گیری‌ها مبتنی بر تست LNR است. بنابراین مهاجم باید بردار حمله $Z_a$ را به گونه‌ای تزریق کند تا توسط تست LNR شناسایی نشود. با توجه به باقیمانده‌های جدید ($R_{new}$) مطابق (۱۷) و استفاده از نامساوی مثلثاتی می‌توان نوشت

$$\|R_{new}\|_۲ \le \|R\|_۲ + \|(I_M - \Re)Z_a\|_۲ . \quad (۱۸)$$

این نامساوی نشان می‌دهد که اگر $(I_M - \Re)Z_a = ۰$ شود، یعنی بردار حمله $Z_a$ به طور کامل متعلق به فضای پوچی ماتریس $I_M - \Re$ باشد، آنگاه اپراتور شبکه نمی‌تواند تمایزی بین $\|R\|_۲$ و $\|R_{new}\|_۲$ قائل شود و در نتیجه حمله غیر قابل تشخیص باقی می‌ماند. اما چنین امکانی به دلیل محدودیت‌های فنی و بودجه حمله برای مهاجم در عمل وجود ندارد. زیرا تحقیقات نشان می‌دهد که مهاجم، تنها امکان دستکاری برخی از سیستم‌های اندازه‌گیری را دارد و علاوه بر این، بودجه حمله نیز محدود است [۱] و [۲]. به عبارت دیگر، مهاجم فقط می‌تواند به برخی از دستگاه‌های اندازه‌گیری با تعداد مشخص‌شده از قبل دسترسی داشته باشد. بنابراین محدودیت‌های فنی و بودجه‌ای باعث ایجاد محدودیت بر روی برخی از مؤلفه‌های بردار حمله $Z_a$ می‌کنند. این موضوع مشخص می‌کند که مهاجم باید بردار FDIA را به شکل کارآمدتری کشف کند. به عبارت دیگر، مهاجم یک تعداد مشخص از سیستم‌های اندازه‌گیری را به طور هم‌زمان دستکاری می‌کند تا از یک FDIA مخفیانه بهره‌برداری کند. فرض می‌شود که $A$ یک مجموعه از $n_a$ سیستم‌های اندازه‌گیری باشد $(۰ < n_a < M)$ که مهاجم می‌تواند به آنها حمله کند. برای بهره‌برداری یک FDIA موفقیت‌آمیز، مهاجم باید بردار حمله $Z_a$ با مؤلفه‌های $a_m$ را به گونه‌ای طراحی کند تا شرط زیر برقرار شود

$$a_m = ۰ \ , \ \forall m \notin A . \quad (۱۹)$$

این شرط مشخص می‌کند که اگر مهاجم، امکان دستکاری $m$امین داده اندازه‌گیری را نداشته باشد، باید مؤلفه $m$ام در بردار $Z_a$ (یعنی $a_m$) برابر صفر باشد. بنابراین مهاجم باید اندازه عبارت $\|(I_M - \Re)Z_a\|_۲$ را تا حد امکان، کوچک نگه دارد تا در آن صورت، یک طراحی حمله بر اساس

1. DC-State Estimation
2. Weighted Least Squares
3. Largest Normalized Residual

بیشترین احتمال تشخیص‌ناپذیری حاصل کند. قید تشخیص‌ناپذیری حمله از دیدگاه مهاجم در واقع به صورت زیر در نظر گرفته می‌شود

$$\left\|(I_M - \Re)Z_a\right\|_2 \le \varepsilon \,. \qquad (۲۰)$$

در این قید، $\varepsilon$ یک پارامتر طراحی برای مهاجم است. انتخاب مقدار کوچک برای $\varepsilon$، حمله را با احتمال بالاتری غیرقابل تشخیص توسط اپراتور شبکه می‌کند [۵]. اما از طرفی قابلیت مهاجم برای دستکاری تخمین حالت، محدود خواهد گردید. در این مقاله فرض می‌شود که $\varepsilon$ از قبل توسط مهاجم تعیین شده است.

## ۳-۲ استراتژی حمله سودآور

در این قسمت، استراتژی FDIA برای یک مهاجم شرکت‌کننده در بازارهای برق DA و RT فرمول‌بندی می‌شود. در این استراتژی، مهاجم یک تجارت مجازی را در باس‌های انتخابی به منظور دستیابی به سود مالی انجام می‌دهد. به طور خاص در بازار DA، مهاجم توان مجازی $P_v$ را در باس‌های $n_1$ و $n_2$ به ترتیب با قیمت‌های $LMP_{n1}^{DA}$ و $LMP_{n2}^{DA}$ خریداری کرده و به فروش می‌رساند. در بازار RT، بعد از تزریق بردار $Z_a$ برای دستکاری قیمت‌ها، مهاجم توان مجازی $P_v$ را در باس‌های $n_1$ و $n_2$ به ترتیب با قیمت‌های $LMP_{n1}^{RT}$ و $LMP_{n2}^{RT}$ به فروش می‌رساند و خریداری می‌کند. بنابراین از این تجارت مجازی، سودی که مهاجم می‌تواند کسب کند به صورت زیر است

$$\begin{aligned} profit = {} & P_v(LMP_{n1}^{RT} - LMP_{n1}^{DA}) + \\ & P_v(LMP_{n2}^{DA} - LMP_{n2}^{RT}) = \\ & P_v(LMP_{n1}^{RT} - LMP_{n2}^{RT} + LMP_{n2}^{DA} - LMP_{n1}^{DA}) \end{aligned} \,. \qquad (۲۱)$$

با جایگذاری روابط DA-LMPs و RT-LMPs از (۱۰) و (۱۱)، تابع (۲۱) به صورت زیر تبدیل می‌شود

$$profit = P_v \sum_{l \in L} (H_{l,n1} - H_{l,n2})(\gamma_l^{RT} - \gamma_l^{DA}) \,. \qquad (۲۲)$$

به عنوان نتیجه، علامات $H_{l,n1} - H_{l,n2}$ و $\gamma_l^{RT} - \gamma_l^{DA}$ مشخص‌کننده سود مثبت یا منفی مهاجم در تجارت مجازی است. بر این اساس می‌توان یک استراتژی FDIA را به گونه‌ای تعریف کرد که از طریق تغییر وضعیت تراکم خطوط انتقال بین DA و RT، یک سود غیرمنفی حاصل شود. در این رابطه برای یک خط بدون الگوی تراکم، اگر $H_{l,n1} - H_{l,n2} > 0$ باشد آنگاه آن خط نباید دچار تراکم منفی شود و اگر $H_{l,n1} - H_{l,n2} < 0$ باشد آنگاه آن خط دچار تراکم مثبت نشود؛ به عبارتی می‌توان بیان کرد

$$\begin{cases} \hat{f}_l^a \ge f_l^{\min} \;\;, \; \forall l \in L \,\middle|\, H_{l,n1} - H_{l,n2} > 0 \\ \hat{f}_l^a \le f_l^{\max} \;\;, \; \forall l \in L \,\middle|\, H_{l,n1} - H_{l,n2} < 0 \end{cases} \qquad (۲۳)$$

که در آن $\hat{f}_l^a$ نشان‌دهنده تخمین حمله‌شده از $f_l$ است. اما به دلیل نامشخص‌بودن اندازه‌گیری‌ها و خطاهای آنها، یک مهاجم نمی‌تواند تعیین کند که استراتژی حمله به درستی الگوی تراکم را تغییر می‌دهد. در واقع با داشتن حالت‌های تخمین زده شده جدید، $\hat{X}_{new}$، می‌توان $\hat{f}_l^a$ را با استفاده از مؤلفه‌های ردیف $l$ام ماتریس $H$، نشان داده شده با $e_l H$، به صورت $\hat{f}_l^a = e_l H \hat{X}_{new}$ در نظر گرفت. همچنین با استفاده از رابطه $\hat{X}_{new}$ بیان‌شده توسط (۱۶)، آنگاه

$$\hat{f}_l^a = e_l HK(Z + Z_a) = \hat{f}_l + e_l HKZ_a \,. \qquad (۲۴)$$

حال با جایگذاری $Z$ توسط رابطه داده‌شده در (۱۲) و با توجه به اینکه $KS = I_N$ است، $\hat{f}_l^a$ می‌تواند به صورت زیر بیان گردد:

$$\hat{f}_l^a = e_l HX + e_l HKE + e_l HKZ_a \,. \qquad (۲۵)$$

$e_l HX$ با توجه به (۵) معادل با توان عبوری حقیقی، $f_l$، است که از دیدگاه مهاجم یک متغیر تصادفی است. فرض می‌شود که $f_l$ برای هر خط منفرد $l \in L$ دارای توزیع نرمال است به طوری که امید ریاضی آن معادل با توان عبوری بهینه در بازار DA، $f_l^{DA}$، است. علاوه بر این $E \sim \text{Normal}(0, \Sigma_E)$ می‌باشد و بنابراین $\hat{f}_l^a$ نیز یک متغیر تصادفی است که از توزیع نرمال تبعیت می‌کند و امید ریاضی آن به صورت رابطه زیر است

$$\mathrm{E}[\hat{f}_l^a] = f_l^{DA} + e_l HKZ_a \,. \qquad (۲۶)$$

بر این اساس، مهاجم نمی‌تواند تضمین کند که دو شرط بیان‌شده در (۲۳) بتواند همواره برقرار گردد. با این اوصاف، مهاجم می‌تواند بردار حمله $Z_a$ را طوری طراحی کند که با بالاترین احتمال ممکن، شروط (۲۳) صادق باشد. در حقیقت نگرش مهاجم در راستای تغییر امید ریاضی $\hat{f}_l^a$ برای دستیابی به الگوی تراکم مورد نظر به منظور بیشینه‌کردن تابع سود (۲۲) با احتمال حداکثری است. به عبارت دیگر برای جلوگیری از یک تراکم منفی (مثبت) روی یک خط انتقال $l \in L$، مهاجم حمله را طوری طراحی می‌کند که شرط $\mathrm{E}[\hat{f}_l^a] \ge f_l^{\min} + \delta_l$ $(\mathrm{E}[\hat{f}_l^a] \le f_l^{\max} - \delta_l)$ معتبر باشد و هدف آن در بیشینه‌سازی مقدار حاشیه $\delta_l \ge 0$ برای افزایش شانس خود در دستیابی به سود حداکثری است. بدین ترتیب می‌توان نوشت

$$\begin{cases} \mathrm{E}[\hat{f}_l^a] \ge f_l^{\min} + \delta_l \;\;, \; \forall l \in L \,\middle|\, h_l > 0 \\ \mathrm{E}[\hat{f}_l^a] \le f_l^{\max} - \delta_l \;\;, \; \forall l \in L \,\middle|\, h_l < 0 \end{cases} \qquad (۲۷)$$

که در آن تعریف شده:

$$h_l = H_{l,n1} - H_{l,n2} \,. \qquad (۲۸)$$

این نکته قابل توجه است که احتمال غیرمنفی بودن تابع سود (۲۱)، منوط به وجود متغیرهای $\delta_l$ برای همه خطوط شبکه بر اساس (۲۷) است. همچنین یک مقدار بزرگ از حاشیه $\delta_l$ می‌تواند برقراری قیود (۲۷) را با یک احتمال بزرگ‌تر تضمین کند. چنین موضوعی برای مهاجم، ایجاد انگیزه می‌کند تا بردار حمله $Z_a$ را بر اساس بیشینه‌سازی همزمان همه مقادیر $\delta_l$ تعیین کند که این موضوع، راهکاری را مشخص می‌کند تا بتوان تابع هدف حمله را تشکیل داد.

## ۳-۳ بیان هدف حمله

همان طور که استنباط گردید، لازمه راه‌اندازی حمله موفقیت‌آمیز، وجود یک حاشیه $\delta_l$ برای هر $l \in L$ جهت اطمینان از برقراری قیود (۲۷) است اما میزان موفقیت حمله با بیشترین دامنه برای همه مقادیر $\delta_l$ به طور همزمان در ارتباط است. به عبارت دیگر می‌توان داشت:

$$\{\max \delta_1, \max \delta_2, \ldots, \max \delta_L\} \,. \qquad (۲۹)$$

این بدین معنی است که استراتژی حمله باید بر اساس یک مدل بهینه‌سازی $L$ هدفه تعیین گردد. به طور کلی، روش مجموع وزن‌دار (WSM) با ترکیب همه اهداف، مسائل بهینه‌سازی چندهدفه را به تک‌هدفه تقلیل می‌دهند. بر این اساس، ضرایب وزنی $\{w_1, w_2, \ldots, w_L\}$ برای بیان اهداف (۲۸) در قالب یک تابع هدف تکی به صورت رابطه زیر استفاده می‌شود

$$\max \sum_{l \in L} w_l \delta_l \qquad (۳۰)$$

که در آن $\sum_{l \in L} w_l = 1$ است. در واقع هر ضریب $w_l$، سهم خط $l$ را

در قابلیت سودآوری حمله نشان می‌دهد. این واضح است که پاسخ نهایی به شدت وابسته به انتخاب این ضرایب دارد. در اینجا پیشنهاد می‌شود که ضرایب $w_l$ بر اساس تابعی از ضرایب $h_l$ مطابق (۳۱) انتخاب شوند

$$w_l = \frac{|h_l|}{\sum_{l\in L}|h_l|} \ , \ \forall l \in L \ . \qquad (۳۱)$$

بر این اساس، تابع هدف معادل $\varphi(\delta)$ مرتبط با مجموعه اهداف (۲۹) به منظور طراحی استراتژی حمله در طول زمان اجرا به صورت رابطه زیر ارائه می‌شود

$$\max \varphi(\delta) = \sum_{l\in L}|h_l|\,\delta_l \qquad (۳۲)$$

که $\delta = [\delta_1,\ldots,\delta_L]^T$ و بردار متغیرهای بهینه‌سازی وابسته به $Z_a$ است. لازم به ذکر است که به جهت سادگی در محاسبات از عبارت ثابت مخرج (۳۱) صرف نظر شده که تأثیری در پاسخ نهایی $Z_a$ نخواهد داشت.

## ٤- برنامه‌ریزی مقاوم FDIA پیشنهادی با عدم قطعیت‌ها

تمرکز این بخش بر روی یک FDIA پیشنهادی است که مهاجم در طراحی آن با اطلاعات ناقصی از مدل سیستم روبه‌رو است. در بخش اول عدم قطعیت‌های مربوط، معرفی و مدل‌سازی شده و سپس در بخش دوم هدف و قیود حمله تحت این عدم قطعیت‌ها به صورت مقاوم بسط داده شده است. در همین راستا از تکنیک‌های ریاضی پیشنهادی جهت تعیین بدترین سناریو[1] و فرمول‌بندی مسأله برنامه‌ریزی حمله استفاده شده است.

### ٤-١ مدل‌سازی عدم قطعیت‌های اطلاعات شبکه

در واقعیت، اطلاعات شبکه بسیار گسترده و در ضمن موقتی و لحظه‌ای است؛ به طوری که امکان دسترسی جامع به همه اطلاعات توسط مهاجمین سایبری وجود ندارد. از طرفی دستیابی به اهداف و الزامات مطرح‌شده برای یک FDIA به شدت بستگی به دانش کامل و آنی یک مهاجم از اطلاعات شبکه دارد. به طور کلی اطلاعات آفلاین و آنلاین شبکه می‌تواند از طریق تعدادی از کارمندان جاسوس مرکز کنترل، هک‌کردن سیستم‌های مخابراتی و دستیابی به نتایج پخش بار به دست آید [۲]. به هر حال این عدم قطعیت در اطلاعات، یکی از موانع اصلی برای شکل‌گیری حملات مؤثر در بازار برق است و به همین دلیل این مقاله بر روی یک روش FDIA با مدل‌سازی غیرقطعی سیستم دینامیکی انجام شده است. بر این اساس فرض می‌شود که یک عدم تطابق بین مدل دینامیکی سیستم واقعی با آنچه که توسط مهاجم حدس زده می‌شود، وجود دارد. به طور خاص‌تر در مدل‌سازی واقعی ارائه‌شده از سیستم، ماتریس‌های $H$ و $\Re$ به عنوان منشأ عدم قطعیت‌های موجود در طراحی استراتژی حمله در نظر گرفته شده و حدس مهاجم از این ماتریس‌ها به ترتیب با $H^a$ و $\Re^a$ نشان داده شده است. همچنین خطای ماتریسی توصیف‌کننده این عدم قطعیت‌ها به صورت زیر تعریف می‌شود

$$\Delta H \triangleq H - H^a \ , \qquad (۳۳)$$

$$\Delta\Re \triangleq \Re - \Re^a \ . \qquad (۳۴)$$

در واقع $\Delta H$ و $\Delta\Re$ خطاهای مربوط به عدم قطعیت مهاجم درباره درک واقعی از اطلاعات شبکه هوشمند است. همچنین در این مدل عدم قطعیت فرض می‌شود که مؤلفه‌های $\Delta H$ و $\Delta\Re$ متغیرهای تصادفی مستقل هستند و هر مؤلفه در یک بازه (باند) محدود قرار دارد. از این رو به دلیل وجود خطاهای تصادفی مرتبط با ماتریس‌های $H$ و $\Re$، مهاجم با عدم قطعیت در رابطه با تزریق بردار $Z_a$ مواجه است. در حقیقت درک‌های واقعی متفاوت از $H$ و $\Re$ منجر به بردارهای حمله متفاوت می‌شود؛ زیرا در هر صورت بردار $Z_a$ باید در محدودیت‌های مرتبط با اصل غیرقابل تشخیص‌پذیری و سودآوری حمله صدق کند. از این رو استراتژی حمله باید تغییر کند؛ به طوری که مهاجم به جای استفاده از یک مدل سیستمی معلوم تکی، باید طراحی را بر اساس همه سناریوهای مدل ممکن انجام دهد. برای این منظور لازم است که کل فضای عدم قطعیت‌ها تعیین شود. در رابطه با ماتریس $\Re$ با توجه به اینکه خطاهای عدم قطعیت محدود است می‌توان نوشت

$$\left|\Delta\Re_{ij}\right| \le \rho_{ij} \ , \ \forall i,j \in \{1,\ldots,M\} \qquad (۳۵)$$

که $\rho_{ij}$ کران خطا برای مؤلفه $(i,j)$ از ماتریس $\Delta\Re$ است. بنابراین اگرچه مهاجم ماتریس $\Re$ را نمی‌تواند به طور دقیق مشخص کند اما به جای آن می‌داند که متعلق به مجموعه زیر است

$$\Omega_{\Re} = \{\Re \,|\, \Re = \Re^a + \Delta\Re, \|\Delta\Re\|_F \le \rho\} \qquad (۳۶)$$

که $\Omega_{\Re}$ فضای عدم قطعیت ماتریس $\Re$ بوده و شامل یک ناحیه فوق کروی حول مبدأ و به شعاع $\rho = (\sum_i\sum_j \rho_{ij}^2)^{1/2}$ است. علاوه بر این چون کران‌های خطا در مؤلفه‌های ماتریس $\Delta H$ نیز برای مهاجم معلوم است، می‌توان کران معین $\sigma_l$ را برای خطای عدم قطعیت در ضریب $h_l$ از (۲۸) در نظر گرفت. لذا بازه تغییرات $h_l$ به صورت زیر خواهد بود

$$h_l^a - \sigma_l \le h_l \le h_l^a + \sigma_l \ , \ \forall l \in L \qquad (۳۷)$$

که در آن $h_l^a$ حدس مهاجم از ضریب $h_l$ است.

### ٤-٢ برنامه‌ریزی حمله مقاوم

استراتژی مهاجم طبق فرضیات و مدل‌های عدم قطعیت تعریف‌شده، طراحی بردار حمله $Z_a$ است به طوری که به ازای همه سناریوهای عدم قطعیت، بیشترین مقدار تابع هدف (۳۰) حاصل شود و در عین حال قید غیرقابل تشخیص‌پذیری در (۲۰) و قیود سودآوری حمله در (۲۷) همواره محقق شوند. اما به دلیل گستردگی فضای عدم قطعیت‌ها، ایده طراحی با توجه به دستیابی به بدترین سناریوی ممکن دنبال می‌شود. لازم به ذکر است که با درنظرگرفتن همه سناریوها، تابع هدف (۳۰) و قیود (۲۰) و (۲۷) به فرم عبارت‌های غیرمحدب تصادفی هستند. در ادامه ضمن بیان فرم کلی این عبارت‌ها، فرم‌های معادل محدب قطعی آنها استنباط و در روند تشکیل مسأله حمله جایگزین می‌شوند.

#### ٤-٢-١ شرط حمله غیرقابل تشخیص تحت عدم قطعیت‌ها

از دیدگاه مهاجم، حمله با بیشترین احتمال تشخیص‌پذیر خواهد بود، اگر ترکیب بردار $Z_a$ با فضای عدم قطعیت ماتریس $\Re$ $(\Omega_{\Re})$ منجر به بزرگ‌ترین مقدار برای $\|(I_M - \Re)Z_a\|_2$ شود. بنابراین باید داشت:

$$\sup_{\Re\in\Omega_{\Re}} \|(I_M - \Re)Z_a\|_2 \le \varepsilon \ . \qquad (۳۸)$$

واضح است که اگر طراحی حمله بر اساس بدترین سناریو انجام شود، آنگاه می‌توان تضمین کرد که حتماً حمله به ازای هر سناریوی دیگر نیز غیرقابل تشخیص است. به عبارتی می‌توان نوشت:

$$\|(I_M - \Re)Z_a\|_2 \le \varepsilon \ , \ \forall \Re \in \Omega_{\Re} \ . \qquad (۳۹)$$

1. Worst Scenario

این استراتژی حمله بر اساس اصل طراحی مقاوم است. از آنجایی که تعداد بسیاری سناریو در مجموعه $\Omega_{\Re}$ وجود دارند، دسته قیود (۳۹) بسیار بزرگ بوده و یک فضای غیرمحدب از متغیرهای تصمیم را به وجود می‌آورند. بنابراین لازم است این دسته قیود با یک قید معادل تکی جایگزین شوند. بر این اساس با در نظر گرفتن فضای عدم قطعیت $\Omega_{\Re}$ در (۳۶) و استفاده از ویژگی‌های تابع نرم $\ell_2$ می‌توان داشت:

$$\begin{aligned}\left\|(I_M-\Re)Z_a\right\|_2 &= \left\|(I_M-\Re^a)Z_a-\Delta\Re Z_a\right\|_2 \le \\ &\left\|(I_M-\Re^a)Z_a\right\|_2+\left\|\Delta\Re Z_a\right\|_2 \le \\ &\left\|(I_M-\Re^a)Z_a\right\|_2+\left\|\Delta\Re\right\|_2.\left\|Z_a\right\|_2 \le \\ &\left\|(I_M-\Re^a)Z_a\right\|_2+\rho.\left\|Z_a\right\|_2\end{aligned} \quad . \qquad (۴۰)$$

به عنوان نتیجه می‌توان داشت:

$$\sup_{\Re\in\Omega_{\Re}}\left\|(I_M-\Re)Z_a\right\|_2=\left\|(I_M-\Re^a)Z_a\right\|_2+\rho.\left\|Z_a\right\|_2 \qquad (۴۱)$$

که ترکیب آن با (۳۸)، قید تکی مقاوم به صورت (۴۲) برای حمله غیرقابل تشخیص‌پذیر ایجاد می‌شود

$$\left\|(I_M-\Re^a)Z_a\right\|_2+\rho.\left\|Z_a\right\|_2\le\varepsilon \qquad (۴۲)$$

### ٤-۲-۲ شرط حمله سودآور تحت عدم قطعیت‌ها

بر اساس آنچه که در انتهای بخش ۳-۲ استنباط گردید، شرط سودآوری حمله مطابق قید (۲۷) است. در نظر گرفتن این قید به ازای همه سناریوهای عدم قطعیت در راستای اصول طراحی مقاوم‌پذیر است. به عبارت دیگر حمله $Z_a$ مشمول یک حمله مقاوم سودآور است، اگر قیود در (۲۷) به ازای همه سناریوهای عدم قطعیت برقرار شود. از آنجایی که فضای سناریوها غیرمحدب و گسترده است، مبنای طراحی بر اساس انتخاب بدترین سناریوی موجود می‌باشد. چنین طراحی حمله، اولاً مقاوم‌پذیری استراتژی حمله سودآور را در برابر عدم قطعیت‌های دینامیکی شبکه، تضمین و ثانیاً مدل‌سازی مسأله طراحی حمله را با به‌کارگیری تنها یک قید تکی محدب ساده‌تر می‌کند و حل آن را امکان‌پذیر می‌سازد. برای این منظور باید داشت:

$$\begin{cases} a: \inf\limits_{\Re\in\Omega_{\Re}}\{\mathrm{E}[\hat{f}_l^a]\}\ge f_l^{\min}+\delta_l \ , \ \forall l\in L\left|h_l^a\right.>\sigma_l \\ b: \sup\limits_{\Re\in\Omega_{\Re}}\{\mathrm{E}[\hat{f}_l^a]\}\le f_l^{\max}-\delta_l \ , \ \forall l\in L\left|h_l^a\right.<-\sigma_l \\ a\,\&\,b \qquad\qquad , \ \forall l\in L\left|h_l^a\right|\le\sigma_l \end{cases} . \qquad (۴۳)$$

این نکته قابل توجه است که برای هر خط منفرد $l\in\mathrm{L}$ در حالتی که $h_l^a>\sigma_l$ $(h_l^a<-\sigma_l)$ است، علامت $h_l$ به طور قطعی مشخص و مثبت (منفی) خواهد بود؛ لذا استراتژی حمله مقاوم سودآور با درنظرگرفتن بدترین سناریو به صورت نامساوی $a$ $(b)$ در (۳۸) لحاظ می‌گردد. اما در حالتی که $\left|h_l^a\right|\le\sigma_l$ است، نمی‌توان اظهار نظری در مورد علامت $h_l$ داشت. بنابراین در این حالت برای تضمین یک استراتژی همواره سودآور باید درباره خط $l$ تصمیم زیر اتخاذ شود

$$f_l^{\min}+\delta_l\le\mathrm{E}[\hat{f}_l^a]\le f_l^{\max}-\delta_l \ , \ \forall\Re\in\Omega_{\Re} . \qquad (۴۴)$$

به عبارتی مهاجم سعی در نگه‌داشتن خط $l$ در وضعیت بدون تراکم دارد. این قاعده با درنظرگرفتن هر دو نامساوی $a$ و $b$ به طور هم‌زمان در (۴۳) لحاظ شده است.

حال برای تعیین مقادیر inf و sup در (۴۳)، ابتدا وابستگی عبارت $\mathrm{E}[\hat{f}_l^a]$، تعریف‌شده در (۲۶)، به ماتریس $\Re$ مشخص می‌شود. به سادگی می‌توان ماتریس‌های $H$ و $S$ به ترتیب تعریف‌شده در (۵) و (۱۲) را مطابق زیر به یکدیگر مرتبط کرد

$$H=[\cdot_{L\times N}\vdots I_L]S \qquad (۴۵)$$

بر این اساس (۲۶) به صورت زیر بیان می‌گردد

$$\mathrm{E}[\hat{f}_l^a]=f_l^{DA}+\bar{\Re}_l Z_a \qquad (۴۶)$$

که در آن $\bar{\Re}_l$ به صورت رابطه $\bar{\Re}_l=e_l[\cdot_{L\times N}\vdots I_L]\Re$ تعریف گردیده و نشان‌دهنده سطر $N+l$ام از ماتریس $\Re$ است. همچنین با یادآوری $\Re=\Re^a+\Delta\Re$، به طور معادل می‌توان داشت

$$\mathrm{E}[\hat{f}_l^a]=f_l^{DA}+\bar{\Re}_l^a Z_a+\Delta\bar{\Re}_l Z_a \qquad (۴۷)$$

که $\Delta\bar{\Re}_l=e_l[\cdot_{L\times N}\vdots I_L]\Delta\Re$ و $\bar{\Re}_l^a=e_l[\cdot_{L\times N}\vdots I_L]\Re^a$ است. دو عبارت $f_l^{DA}$ و $\bar{\Re}_l^a Z_a$ قطعی است ولی عبارت $\Delta\bar{\Re}_l Z_a$ ماهیت تصادفی دارد. حال با استفاده از نامساوی کوشی‌شوارتز، یک کران بالا و پایین قطعی برای $\Delta\bar{\Re}_l Z_a$ به صورت زیر تعیین می‌گردد

$$\begin{aligned}-\left\|\Delta\bar{\Re}_l\right\|_2.\left\|Z_a\right\|_2 \le -\left|\Delta\bar{\Re}_l Z_a\right| \le \\ \Delta\bar{\Re}_l Z_a\le\left|\Delta\bar{\Re}_l Z_a\right|\le\left\|\Delta\bar{\Re}_l\right\|_2.\left\|Z_a\right\|_2\end{aligned} . \qquad (۴۸)$$

از طرفی با استناد به فضای عدم قطعیت $\Omega_{\Re}$، نامساوی $\left\|\Delta\bar{\Re}_l\right\|_2\le\rho$ برای هر $l\in\mathrm{L}$ صادق است. بنابراین می‌توان نوشت

$$\begin{aligned}\inf_{\Re\in\Omega_{\Re}}\{\Delta\bar{\Re}_l Z_a\}&=-\rho\left\|Z_a\right\|_2 \\ \sup_{\Re\in\Omega_{\Re}}\{\Delta\bar{\Re}_l Z_a\}&=\rho\left\|Z_a\right\|_2\end{aligned} \qquad (۴۹)$$

عبارت (۴۷) در ترکیب آن با (۴۹) مقادیر قطعی را برای $\inf\{\mathrm{E}[\hat{f}_l^a]\}$ و $\sup\{\mathrm{E}[\hat{f}_l^a]\}$ ایجاد می‌کند که بر این اساس، قیود سودآوری حمله در (۴۳) به صورت (۵۰) تبدیل می‌شوند

$$\begin{cases} a: f_l^{DA}+\bar{\Re}_l^a Z_a-\rho\left\|Z_a\right\|_2\ge f_l^{\min}+\delta_l \ , \\ \quad \forall l\in L\left|h_l^a\right.>\sigma_l \\ b: f_l^{DA}+\bar{\Re}_l^a Z_a+\rho\left\|Z_a\right\|_2\le f_l^{\max}-\delta_l \ , \\ \quad \forall l\in L\left|h_l^a\right.<-\sigma_l \\ a\,\&\,b \ , \ \forall l\in L\left\|h_l^a\right|\le\sigma_l \end{cases} . \qquad (۵۰)$$

بر این اساس، قیود سودآوری حمله به گونه‌ای تبدیل به قیود درجه دوم قطعی شده که ۱) مستقل از فضای عدم قطعیت‌های ضرایب $h_l$ و ماتریس $\Re$ است و ۲) هر سناریوی عدم قطعیت را شامل می‌شود. به عبارتی قیود (۵۰) یک انتخاب صحیح از دسته قیود غیرقابل شمارش زیر است

$$\begin{cases} f_l^{DA}+\bar{\Re}_l Z_a\ge f_l^{\min}+\delta_l \ , \ \forall l\in L\left|h_l\right.>0 \ , \ \forall\Re\in\Omega_{\Re} \\ f_l^{DA}+\bar{\Re}_l Z_a\le f_l^{\max}-\delta_l \ , \ \forall l\in L\left|h_l\right.<0 \ , \ \forall\Re\in\Omega_{\Re} \end{cases} . \qquad (۵۱)$$

بر این اساس یک استراتژی حمله سودآور معرفی شده که در آن مهاجم، مقاوم‌پذیری بدترین حالت را در برابر عدم قطعیت‌ها تضمین می‌کند.

### ٤-۲-۳ تابع هدف حمله تحت عدم قطعیت‌ها

همان طور که در بخش ۳-۳ استنباط شد، استراتژی حمله پیشنهادی بر اساس مدل بهینه‌سازی تک‌هدفه مطابق (۳۲) تعیین می‌گردد. تابع هدف $\varphi(\delta)$ به دلیل وابستگی ضرایب $h_l$ به عدم قطعیت‌ها به صورت تصادفی است؛ بنابراین استراتژی مهاجم بیشینه‌سازی یک $\varphi_d(\delta)$ قطعی

می‌باشد به گونه‌ای که به ازای هر سناریوی ممکن به طور مقاوم قید $\varphi_d(\delta) \le \varphi(\delta)$ برقرار باشد؛ لذا می‌توان در نظر گرفت که:

$$\varphi_d(\delta) = \inf \varphi(\delta) = \inf \sum_{l \in L} |h_l| \delta_l \ . \quad (۵۲)$$

فرض می‌شود که بردار خطای عدم قطعیت برای ضرایب $h_l$ به صورت $\Delta h = [\Delta h_1, \ldots, \Delta h_L]$ باشد که $\Delta h_l = h_l - h_l^a \ , \forall l \in L$ است. با استناد به اینکه $\delta_l \ge 0 \ , \ \forall l \in L$ و استفاده از نامساوی مثلثاتی می‌توان نوشت:

$$\sum_{l \in L} \left| h_l^a \delta_l + \Delta h_l \delta_l \right| \ge \left| \sum_{l \in L} h_l^a \delta_l + \sum_{l \in L} \Delta h_l \delta_l \right| . \quad (۵۳)$$

حال با استفاده از نامساوی کوشی‌شوارتز، یک کران پایین قطعی برای عبارت $\sum_{l \in L} \Delta h_l \delta_l$ به صورت زیر مشخص می‌گردد

$$\sum_{l \in L} \Delta h_l \delta_l = \Delta h . \delta \ge - \left| \Delta h . \delta \right| \ge - \left\| \Delta h \right\|_2 . \left\| \delta \right\|_2 . \quad (۵۴)$$

از طرفی با توجه به اینکه $\left| \Delta h_l \right| \le \sigma_l \ , \ \forall l \in L$ است آن گاه حداکثر مقدار ممکن برای $\left\| \Delta h \right\|_2$ را می‌توان به صورت کران بالا مطابق (۵۵) در نظر گرفت

$$\Delta h_{\max} = \max \left\| \Delta h \right\|_2 = \left( \sum_l \sigma_l^2 \right)^{\frac{1}{2}} . \quad (۵۵)$$

بر این اساس اگر نامساوی زیر همواره برقرار باشد:

$$\sum_{l \in L} h_l^a \delta_l - \Delta h_{\max} . \left\| \delta \right\|_2 \ge 0 . \quad (۵۶)$$

آن گاه از ترکیب دو نامساوی (۵۳) و (۵۴) می‌توان تابع هدف معادل $\varphi_d(\delta)$ در (۵۲) را به صورت زیر به دست آورد

$$\varphi_d(\delta) = \inf \sum_{l \in L} |h_l| \delta_l = \sum_{l \in L} h_l^a \delta_l - \Delta h_{\max} . \left\| \delta \right\|_2 . \quad (۵۷)$$

که یک نتیجه مطلوب حاصل شده است زیرا تابع $\varphi_d(\delta)$ برخلاف $\varphi(\delta)$ یک تابع هدف مقاوم در برابر عدم قطعیت‌هاست.

### ٤-۲-٤ فرمول‌بندی مسأله بهینه‌سازی حمله تحت عدم قطعیت‌ها

نهایتاً طراحی بهینه یک FDIA تحت عدم قطعیت‌های مدل سیستم بر اساس الزامات و شرایط به‌دست‌آمده از طریق حل مسأله بهینه‌سازی زیر صورت می‌گیرد

$$\varphi_{\max} = \max_{Z_a} \varphi_d(\delta) \quad (۵۸)$$

s.t. :

$$\sum_{l \in L} h_l^a \delta_l - \Delta h_{\max} . \left\| \delta \right\|_2 \ge 0 \quad (۵۹)$$

$$\left\| (I_M - \Re^a) Z_a \right\|_2 + \rho . \left\| Z_a \right\|_2 \le \varepsilon \quad (۶۰)$$

$$\begin{cases} a : f_l^{DA} + \bar{\Re}_l^a Z_a - \rho \left\| Z_a \right\|_2 \ge f_l^{\min} + \delta_l \ , \\ \quad \forall l \in L \left| h_l^a > \sigma_l \right. \\ b : f_l^{DA} + \bar{\Re}_l^a Z_a + \rho \left\| Z_a \right\|_2 \le f_l^{\max} - \delta_l \ , \\ \quad \forall l \in L \left| h_l^a < -\sigma_l \right. \\ a \,\&\, b \ , \ \forall l \in L \left| \left| h_l^a \right| \le \sigma_l \right. \end{cases} \quad (۶۱)$$

$$\delta_l \ge 0 \ , \ \forall l \in L \quad (۶۲)$$

$$\{ Z_a \left| a_m = 0 \ , \ \forall m \notin A \right. \} . \quad (۶۳)$$

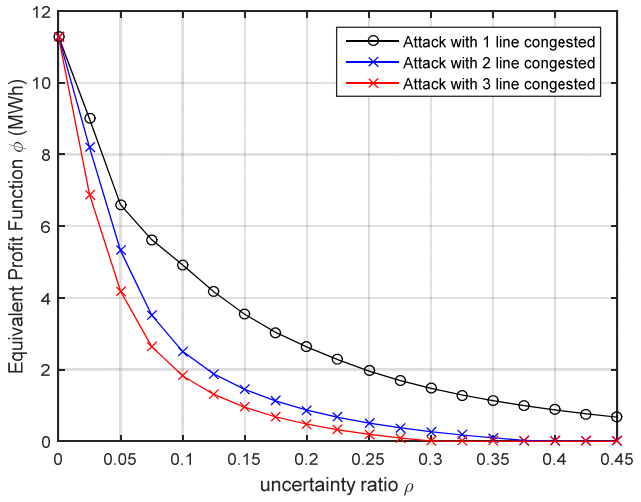
از این رو به طور خلاصه، مسأله برنامه‌ریزی حمله در بازارهای برق برای یک مهاجم سایبری با دانش تصادفی نسبت به ماتریس‌های مدل‌کننده شبکه مطابق (۵۸) تا (۶۳) فرمول‌بندی شده است. ایده اساسی مورد استفاده، تبدیل تابع هدف و قیود تصادفی حمله به معادل‌های قطعی است که در آن صورت بتوان از روش‌های برنامه‌ریزی قطعی مانند روش نقطه درونی برای حل مسأله استفاده کرد.

## ۵- نتایج عددی و بحث

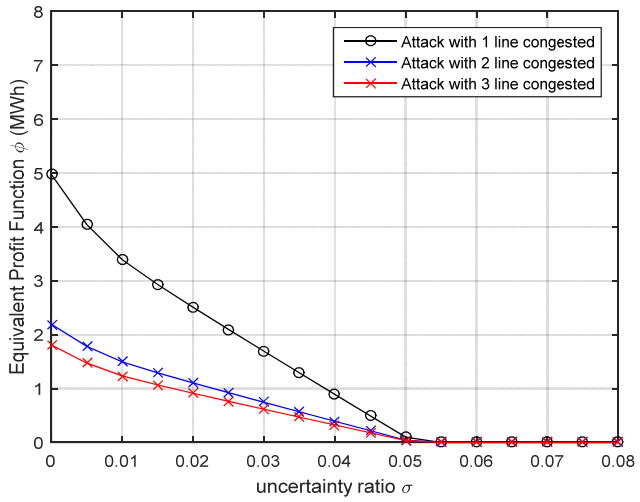
در این بخش، تأثیر FDIA پیشنهادی با وجود عدم قطعیت‌ها در بازارهای RT روی سیستم معیار ۱۴- باس IEEE ارزشیابی می‌شود. بر اساس حمله طراحی‌شده، یک مهاجم سایبری محدودشده از مدل برنامه‌ریزی ارائه‌شده مطابق (۵۸) تا (۶۳) تبعیت می‌کند. برای سادگی در شبیه‌سازی‌ها، فرض گردیده که همه خطاهای عدم قطعیت مربوط به مؤلفه‌های ماتریس $\Delta\Re$ و ضرایب $\Delta h_l$ با همدیگر برابر هستند؛ به عبارتی برای هر $i, j \in \{1, \ldots, M\}$ آنگاه $\rho_{ij} = \rho$ در نظر گرفته شده و همچنین برای هر $l \in L$ آنگاه $\sigma_l = \sigma$ است. دلیل انتخاب این فرضیه، طراحی مسأله حمله مستقل از ابعاد فضای عدم قطعیت‌ها است زیرا ماهیت فضای عدم قطعیت ماتریس $\Delta\Re$ با مدل $\left\| \Delta\Re \right\|_2 \le \rho$ و ضرایب $\Delta h$ با مدل $\left| \Delta h \right| \le \sigma$ به مقادیر $\rho$ و $\sigma$ بستگی ندارند و با تغییر آنها تنها ابعاد فضای عدم قطعیت‌ها تغییر خواهد کرد. همه شبیه‌سازی‌ها با استفاده از بسته‌های نرم‌افزاری مبتنی بر Matlab شامل MATPOWER و حل‌کننده برنامه‌ریزی محدب CVX انجام شده است.

### ۵-۱ تأثیر نرخ خطای عدم قطعیت‌ها

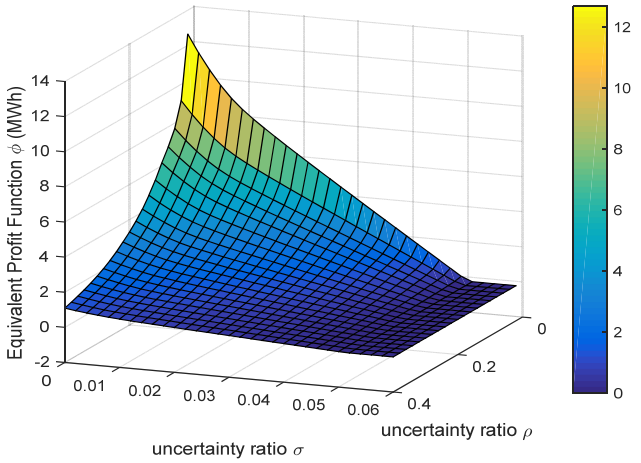
در ابتدای کار، اثر نرخ خطای عدم قطعیت‌های دینامیکی $\rho$ و $\sigma$ بر روی تغییرات تابع سود معادل $\varphi_{\max}$ بررسی می‌شود. برای این منظور تنظیمات مختلف به صورت ۱، ۲ و ۳ خط انتقال تراکم فرض شده است. شکل ۱ تغییرات سود معادل $\varphi_{\max}$ را با تغییرات $\rho$ در ازای ثابت‌بودن $\sigma$ و شکل ۲ تغییرات سود معادل $\varphi_{\max}$ را با تغییرات $\sigma$ در ازای ثابت‌بودن $\rho$ در سیستم ۱۴- باس IEEE نشان می‌دهد. مشاهده می‌شود هنگامی که مهاجم سایبری، دانش کاملی از دینامیک‌های شبکه دارد (یعنی در شکل ۱، $\rho = 0$ و در شکل ۲، $\sigma = 0$ باشد)، آنگاه سودآوری مهاجم در تجارت مجازی بیشترین مقدار را خواهد داشت. مثلاً هنگامی که یک خط متراکم باشد، آنگاه در شکل ۱، $\varphi_{\max} = 11/3 \text{MWh}$ و در شکل ۲، $\varphi_{\max} = 5 \text{MWh}$ است. با افزایش نرخ عدم قطعیت $\rho$ و یا $\sigma$، تابع هدف $\varphi_{\max}$ به طور یکنواخت کاهش می‌یابد و هنگامی که عدم قطعیت به سطح مشخصی می‌رسد، آنگاه $\varphi_{\max} = 0 \text{MWh}$ خواهد شد. دلیل اصلی این مشاهده آن است که بردار حمله $Z_a$ باید برای هر دو شکل در قیود (۵۹) تا (۶۱) صدق کند. به طور خاص برای شکل ۱، هنگامی که نرخ عدم قطعیت $\rho$ افزایش می‌یابد، به منظور برقراری قید (۶۰) باید دامنه بردار حمله $Z_a$ کاهش یابد. بنابراین توانایی مهاجم برای دستکاری نتایج تخمین حالت و در نتیجه دستیابی به سود مالی حداکثری کاهش می‌یابد. همچنین در شکل ۲ علت اصلی روند کاهشی $\varphi_{\max}$ در این است که عدم قطعیت $\sigma$ (یا به طور معادل $\Delta h_{\max}$) مستقیماً روی تابع هدف غیرمنفی تعریف‌شده در (۵۷) تأثیر دارد. علاوه بر این با افزایش $\sigma$، بازه تغییرات ضرایب $h_l$ تعریف‌شده در (۳۷) گسترش می‌یابد. به عنوان نتیجه، از آنجایی که بردار حمله $Z_a$ باید قیود (۶۱) را در ۳ حالت $a$، $b$ و توأماً $a \,\&\, b$ برقرار کند، آنگاه بردار حمله $Z_a$ باید برای تعداد بیشتری از مقادیر $l \in L$ در حالت $a \,\&\, b$ صدق کند که شرایط




شکل ۱: منحنی تغییرات $\varphi_{max}$ با $\rho$ برای تعداد متفاوت خطوط متراکم.




شکل ۲: منحنی تغییرات $\varphi_{max}$ با $\sigma$ برای تعداد متفاوت خطوط متراکم.




شکل ۳: تغییرات $\varphi_{max}$ نسبت به هر دو پارامتر $\rho$ و $\sigma$ در حالت یک خط انتقال متراکم‌شده.

محدودتری را ایجاد می‌کند. از این رو در یک سطح مشخص از عدم قطعیت‌ها دیگر امکان حمله از سمت مهاجم وجود ندارد.

علاوه بر این، شکل‌های ۱ و ۲ تغییرات $\varphi_{max}$ را برای تنظیماتی با تعداد متفاوت از خطوط انتقال متراکم نشان می‌دهند. همان طور که دیده می‌شود، هرچه تعداد خطوط متراکم‌شده افزایش یابد، با اضافه‌شدن به نرخ عدم قطعیت‌های $\rho$ و $\sigma$، دامنه تابع سود $\varphi_{max}$ سریع‌تر کاهش می‌یابد. دلیل اصلی اینجاست که بردار حمله $Z_a$ باید در قید (۶۱) حداقل برای حالت‌های $a$ و یا $b$ صادق باشد. بنابراین هرچه تعداد خطوط بیشتری در وضعیت تراکم باشد، در واقع مهاجم با یک الگوی تراکم سیستمی بزرگ‌تری روبه‌رو است و در نتیجه الزامات سخت‌تری برای طراحی بردار حمله $Z_a$ اعمال می‌کند. در نتیجه، امکان سودآوری مهاجم از طریق تغییر الگوی تراکم توسط یک FDIA کاهش می‌یابد.

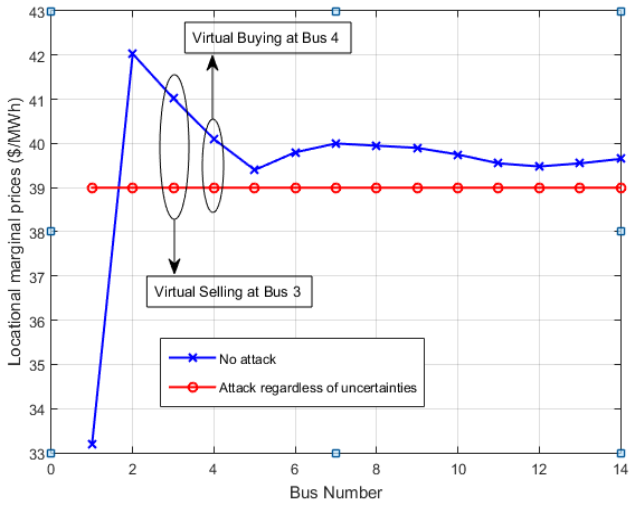
شکل ۳ تأثیر تغییرات هم‌زمان نرخ عدم قطعیت‌های $\rho$ و $\sigma$ را بر روی تابع سود معادل $\varphi_{max}$ برای وضعیت یک خط متراکم‌شده نشان می‌دهد که این تغییرات به صورت یک سطح خمیده با شیب زیاد است. متعاقباً نشان می‌دهد که هرچه مهاجم، اطلاعات کمتری در مورد شبکه داشته باشد، توانایی پایین‌تری در دستکاری نتایج تخمین حالت دارد؛ به طوری که در یک سطح مشخص از اطلاعات ناکافی، مهاجم امکان دستکاری LMPs را در بازار RT نخواهد داشت و احتمال طراحی یک حمله سودآور به صفر می‌رسد.

## ۵-۲ تأثیر حمله بر روی LMPs

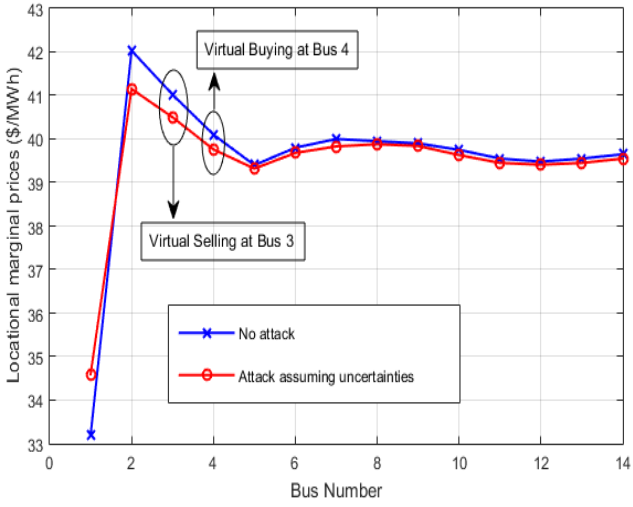
در این بخش، اثر عدم قطعیت‌های مهاجم روی LMPs دستکاری‌شده در بازار برق RT بررسی گردیده است. فرض می‌شود که در بازار DA، خطوط انتقال مشخصی متراکم شده باشد. با اطلاعات دقیق مهاجم از مدل سیستم و تعداد معلوم از سیستم‌های اندازه‌گیری به‌خطرافتاده، خطوط متراکم‌شده در شبکه می‌تواند با بیشترین سطح اطمینان در وضعیت بدون تراکم تشخیص داده شود که منجر به LMPs یکسان در همه باس‌ها در بازار RT می‌شود. در شکل‌های ۴ و ۵ تغییرات LMPs باس‌ها تحت حمله به ترتیب برای دو وضعیت بدون عدم قطعیت‌ها (یعنی برای $\rho=۰$ و $\sigma=۰$) و با درنظرگرفتن عدم قطعیت‌ها (یعنی برای $\rho=۰/۲۵$ و $\sigma=۰/۰۱۵$) است. در این حالت، فقط یک خط (متصل‌شده از باس ۳ به باس ۴) متراکم گردیده است. در بازار DA، مهاجم باس‌های ۳ و ۴ را به ترتیب برای فروش و خرید مقدار یکسان توان مجازی انتخاب می‌کند. بعد از بهره‌برداری از یک FDIA، مهاجم برای خرید و فروش همان مقدار توان مجازی به ترتیب در باس‌های مربوط اقدام می‌کند. در هر دو شکل ۴ و ۵، تنظیمات "No attack" مربوط به بهره‌برداری بدون حمله از شبکه، یعنی $Z_a=۰$ است که در این حالت RT-LMPs با DA-LMPs یکسان بوده و بر اساس (۲۱)، سود تجارت مجازی صفر است. اما هنگامی که یک حمله با اطلاعات کامل اجرا می‌شود، مهاجم می‌تواند کاملاً وضعیت خط متراکم‌شده را در بازار RT عوض کند که سود حاصل از تجارت مجازی در حدود ۶ $/MWh است. این مقدار هنگامی که مدل عدم قطعیت $\rho=۰/۲۵$ و $\sigma=۰/۰۱۵$ در نظر گرفته شود حدوداً به ۱ $/MWh می‌رسد.

## ۵-۳ تأثیر سطح آستانه $\varepsilon$

در این قسمت، نحوه تغییرات تابع سود $\varphi_{max}$ با تغییرات پارامتر آستانه $\varepsilon$ که مرتبط با تست LNR است، ارزیابی می‌شود. در شکل ۶، هنگامی که $\varepsilon$ از صفر شروع به افزایش می‌کند، به همان میزان به موفقیت مهاجم در طراحی FDIA اضافه شده و تابع سود به طور یکنواخت بالا می‌رود ولی در نهایت روند صعودی آن متوقف می‌شود. زیرا برای هر مقدار تنظیم $\rho$ و $\sigma$ داده‌شده، در صورتی مسأله برنامه‌ریزی حمله دارای جواب شدنی است که بردار $Z_a$ قیود به‌هم‌وابسته (۶۰) و (۶۱) را ارضا کند. برای مقادیر کوچک‌تر از $\varepsilon$، قید (۶۰) روی $Z_a$ غلبه می‌کند و در نتیجه با افزایش $\varepsilon$، اجازه برای افزایش دامنه $Z_a$ و در نتیجه ایجاد




شکل ۴: LMPs با و بدون حمله سایبری و بدون حضور عدم قطعیت‌ها.

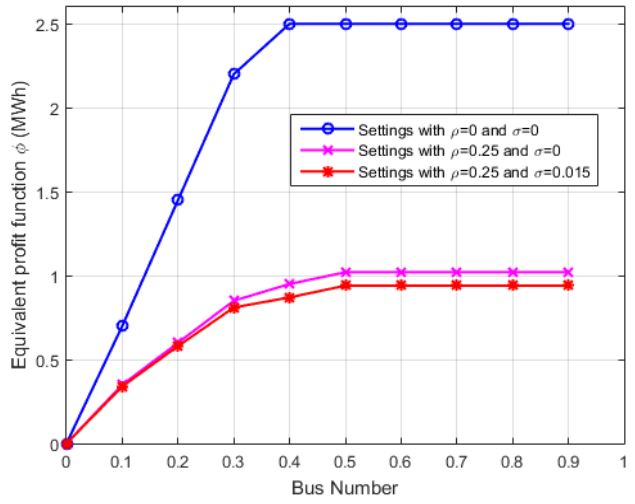



شکل ۵: LMPs با و بدون حمله سایبری و با وجود عدم قطعیت‌ها.

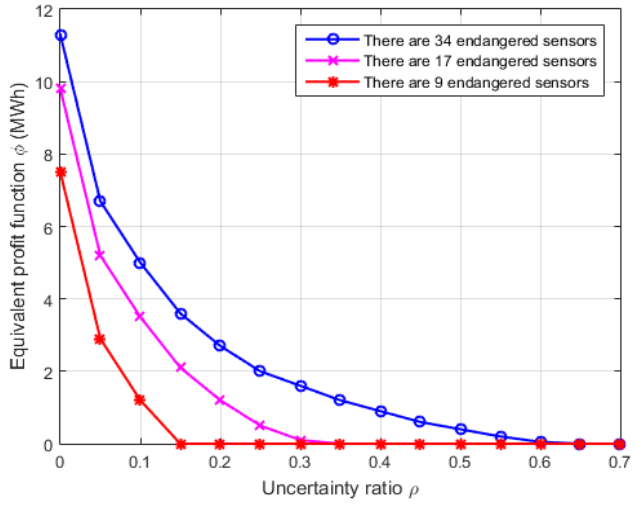
طراحی حمله مؤثرتر فراهم می‌شود. اما هنگامی که $\varepsilon$ به اندازه کافی بزرگ شود، قیود دیگر بر قید (۶۰) غالب می‌شوند و نتیجه اینکه نقطه‌ای فراتر از یک حد سود حداکثری حاصل نمی‌شود که می‌توان گفت $\varphi_{\max}$ به اشباع رسیده است.

## ۵-۴ تأثیر تعداد سیستم‌های اندازه‌گیری به‌خطرافتاده

در این بخش تمرکز روی حالی است که مهاجم فقط می‌تواند اطلاعات تعداد محدودی از سیستم‌های اندازه‌گیری (سنسورها) را دستکاری کند. مطابق (۱۹)، این قضیه حاکی از آن است که مؤلفه‌های بردار $Z_a$ برای سیستم‌های اندازه‌گیری که نمی‌توانند به خطر بیفتند باید برابر صفر باشند. با این فرض، اثر تعداد سنسورهای به‌خطرافتاده بر روی سود معادل $\varphi_{\max}$ ارزیابی می‌شود. برای سیستم IEEE ۱۴- باس تعداد کل سیستم‌های اندازه‌گیری نصب‌شده روی باس‌ها و خطوط شبکه برابر $M = ۳۴$ است. در شکل‌های ۱ تا ۳ مشاهده گردید هنگامی که مهاجم، هر تعداد دلخواه سنسور را به خطر بیندازد، $\varphi_{\max}$ در اثر اعمال محدودیت در اطلاعات مهاجم (افزایش سطح عدم قطعیت‌ها) کاهش می‌یابد. همچنین روند مشابهی زمانی که تعداد سنسورهای مورد حمله واقع شده محدود باشد، ملاحظه خواهد شد؛ زیرا فضای کار برای مهاجم جهت تزریق بردار حمله تقلیل می‌کند. شکل ۷، تغییرات $\varphi_{\max}$ را نسبت به $\rho$ برای مهاجمی که تعداد محدودتری از سنسورها را به خطر می‌اندازد نشان می‌دهد. ملاحظه




شکل ۶: تغییرات $\varphi_{\max}$ نسبت به پارامتر سطح آستانه $\varepsilon$.




شکل ۷: تعداد متفاوت از سیستم‌های اندازه‌گیری به‌خطرافتاده.

می‌شود که برای هر مقدار از $\rho$، به‌خطرافتادن تعداد کمتر از سنسورها باعث سطح سود پایین‌تر می‌شود. این بدین صورت توجیه می‌شود که در کنار قیود غیرقابل تشخیص‌پذیری و سودآوری حمله، مهاجم با یک قید شخصی دیگر مطابق (۶۳) مربوط به دسترسی محدود به همه سیستم‌های اندازه‌گیری مستقرشده مواجه است. برای یک سطح مشخص از عدم قطعیت‌ها، اگر قرار باشد که تعداد کمتری از سنسورها دستکاری شود، آنگاه احتمال ایجاد بردار حمله $Z_a$ که هم غیرقابل تشخیص و هم سودآور باشد به صفر می‌رسد. بنابراین برای هر سطح مشخص از عدم قطعیت‌های داده‌شده، زمانی که تعداد سنسورهای به‌خطرافتاده کمتر از تعداد مشخصی باشد، پیاده‌سازی یک حمله مقاوم مخفی و سودآور در بازار RT امکان‌پذیر نیست.

## ۶- نتیجه‌گیری

در این مقاله، طراحی حمله تزریق داده غلط (FDIA) برای مهاجمین سایبری که اطلاعات ناقصی در مورد دینامیک‌های شبکه هوشمند دارند، ارائه و همچنین اثر این مهاجمین روی بازارهای برق بررسی گردیده است. با ارائه یک مدل جامع برای توصیف خطای عدم قطعیت‌ها، مهاجم می‌تواند در روش طراحی پیشنهادی، بدترین حالت مقاوم را در برابر عدم قطعیت‌ها تضمین کند. به علاوه نتایج شبیه‌سازی در سیستم استاندارد ۱۴- باس IEEE فراهم شده و طراحی حمله پیشنهادی مورد ارزیابی قرار

گرفته است. این نتایج نشان داد که حتی با وجود اطلاعات بسیار ناقص از شبکه (نرخ بزرگ از عدم قطعیت‌ها) برای یک مهاجم هنوز امکان دستکاری قیمت‌های حاشیه محلی (LMPs) در بازارهای زمان حقیقی، بدون اینکه توسط تشخیص‌گر داده بد شناسایی شود، فراهم است. نتیجه نهایی اینکه مهاجمین محدودشده هم قابلیت خلافکاری مالی را در بستر تجارت مجازی بازارهای برق دارند.

## مراجع


[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. on Information and System Security*, vol. 14, no. 1, Article ID: 13, 33 pp., Jun. 2011.

[2] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems-attacks, impacts, and defense: a survey," *IEEE Trans. on Industrial Informatics*, vol. 13, no. 2, pp. 411-423, Apr. 2016.

[3] A. Xu, *et al.*, "Research on false data injection attack in smart grid," in *IOP Conf. Series: Earth and Environmental Science*, *Proc. 8th Annual Int. Conf. on Geo-Spatial Knowledge and Intelligence,* vol. 693, Article ID: 012010, Xi'an, Shaanxi, China, 18-19 Dec. 2020.

[4] Q. Zhang *et al.*, "Profit-oriented false data injection on energy market: reviews, analyses and insights," *IEEE Trans. on Industrial Informatics*, vol. 17, no. 9, pp. 5876-5886, Sept. 2020.

[5] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, pp. 659-666, Dec. 2011.

[6] B. Jin, C. Dou, and D. Wu, "False data injection attacks and detection on electricity markets with partial information in a micro-grid-based smart grid system," *International Trans. on Electrical Energy Systems*, vol. 30, no. 12, Article ID: e12661, Dec. 2020.

[7] L. Jia, R. J. Thomas, and L. Tong, "Malicious data attack on real-time electricity market," in *Proc. IEEE In. Conf. on Acoustics, Speech and Signal Processing, ICASSP'11*, pp. 5952-5955, Prague, Czech Republic, 22-27 May 2011.

[8] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. on Smart Grid*, vol. 2, no. 2, pp. 382-390, Jun. 2011.

[9] B. Huang, Y. Li, F. Zhan, Q. Sun, and H. Zhang, "A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks," *IEEE Trans. on Industrial Informatics*, vol. 18, no. 2, pp. 880-890, Feb. 2021.

[10] R. Tan, V. Badrinath Krishna, D. K. Yau, and Z. Kalbarczyk, "Impact of integrity attacks on real-time pricing in smart grids," in *Proc. of the ACM SIGSAC Conf. on Computer & Communications Security*, pp. 439-450, Berlin, Germany, 4-8 Nov. 2013.

[11] M. Tian, Z. Dong, and X. Wang, "Analysis of false data injection attacks in power systems: a dynamic Bayesian game-theoretic approach," *ISA Trans.*, vol. 115, pp. 108-123, Sept. 2021.

[12] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. on Smart Grid*, vol. 4, no. 1, pp. 160-169, Mar. 2013.

[13] C. Jin, Z. Bao, M. Yu, J. Zheng, and C. Sha, "Optimization of joint cyber topology attack and FDIA in electricity market considering uncertainties," in *Proc. IEEE Power & Energy Society General Meeting, PESGM'21*, 5 pp., Washington, DC, USA, 26-29 Jul. 2021.

[14] D. H. Choi and L. Xie, "Economic impact assessment of topology data attacks with virtual bids," *IEEE Trans. on Smart Grid*, vol. 9, no. 2, pp. 512-520, Mar. 2018.

[15] H. Xu, Y. Lin, X. Zhang, and F. Wang, "Power system parameter attack for financial profits in electricity markets," *IEEE Trans. on Smart Grid*, vol. 11, no. 4, pp. 3438-3446, Jul. 2020.

[16] K. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," *Applied Energy*, vol. 235, pp. 204-218, Feb. 2019.

[17] P. K. Jena, S. Ghosh, and E. Koley, "A binary-optimization-based coordinated cyber-physical attack for disrupting electricity market operation," *IEEE Systems J.*, vol. 15, no. 2, pp. 2619-2629, Jun. 2020.

[18] P. K. Jena, S. Ghosh, E. Koley, D. K. Mohanta, and I. Kamwa, "Design of AC state estimation based cyber-physical attack for disrupting electricity market operation under limited sensor information," *Electric Power Systems Research*, vol. 205, Article ID: 107732, Apr. 2022.

[19] M. Esmalifalak, *et al.*, "A stealthy attack against electricity market using independent component analysis," *IEEE Systems J.*, vol. 12, no. 1, pp. 297-307, Mar. 2018.

[20] S. Tan, W. Z. Song, M. Stewart, J. Yang, and L. Tong, "Online data integrity attacks against real-time electrical market in smart grid," *IEEE Trans. on Smart Grid*, vol. 9, no. 1, pp. 313-322, Jan. 2018.

[21] A. Tajer, "False data injection attacks in electricity markets by limited adversaries: stochastic robustness," *IEEE Trans. on Smart Grid*, vol. 10, no. 1, pp. 128-138, Jan. 2019.

[22] H. Badrsimaei, R. A. Hooshmand, and S. Nobakhtian, "Monte-Carlo-based data injection attack on electricity markets with network parametric and topology uncertainties," *International J. of Electrical Power Energy Systems*, vol. 138, Article ID: 107915, Jun. 2022.

[23] H. Badrsimaei, R. A. Hooshmand, and S. Nobakhtian, "Stealthy and profitable data injection attack on real time electricity market with network model uncertainties," *Electric Power Systems Research*, vol. 205, Article ID: 107742, Apr. 2022.

[24] H. R. Lewis, *Computers and Intractability. A Guide to the Theory of NP-Completeness*, Ed: JSTOR, 1983.

[25] Y. Nesterov and A. Nemirovskii, *Interior-Point Polynomial Algorithms in Convex Programming*, Philadelphia, PA: Society for Industrial and Applied Mathematics, 1994.

[26] A. L. Ott, "Experience with PJM market operation, system design, and implementation," *IEEE Trans. on Power Systems*, vol. 18, no. 2, pp. 528-534, May 2003.

[27] F. Li and R. Bo, "DCOPF-based LMP simulation: algorithm, comparison with ACOPF, and sensitivity," *IEEE Trans. on Power Systems*, vol. 22, no. 4, pp. 1475-1485, Nov. 2007.

[28] T. Zheng and E. Litvinov, "Ex post pricing in the co-optimized energy and reserve market," *IEEE Trans. on Power Systems*, vol. 21, no. 4, pp. 1528-1538, Nov. 2006.

[29] F. Li, Y. Wei, and S. Adhikari, "Improving an unjustified common practice in ex post LMP calculation," *IEEE Trans. on Power Systems*, vol. 25, no. 2, pp. 1195-1197, May 2010.

[30] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Trans. on Power Systems*, vol. 29, no. 2, pp. 627-636, Mar. 2014.

[31] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*, New York, NY, USA: Marcel Dekker, 2004.

[32] W. W. Hogan, "Virtual bidding and electricity market design," *The Electricity J.*, vol. 29, no. 5, pp. 33-47, Jun. 2016.



حامد بدرسیمایی تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی برق گرایش سیستم‌های قدرت به‌ترتیب در سال‌های ۱۳۹۲ و ۱۳۹۴ در دانشگاه آزاد اسلامی نجف آباد و دانشکده مهندسی برق و کامپیوتر دانشگاه بیرجند و مدرک دکتری مهندسی برق گرایش سیستم‌های قدرت را در دانشکده فنی و مهندسی دانشگاه اصفهان در سال ۱۴۰۱ به پایان رسانده است. زمینه‌های تحقیقاتی مورد علاقه ایشان شامل امنیت فیزیکی- سایبری سیستم‌های قدرت، بهره‌برداری بازارهای برق و حفاظت سیستم¬های قدرت می‌باشد.

رحمت الله هوشمند تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی برق– قدرت به‌ترتیب در سال‌های ۱۳۶۸ و ۱۳۷۰ از دانشگاه فردوسی مشهد و دانشگاه تهران و در مقطع دکتری مهندسی برق - قدرت در سال۱۳۸۲ از دانشگاه تربیت مدرس تهران به پایان رسانده است و هم‌اکنون استاد گروه مهندسی برق دانشکده فنی مهندسی دانشگاه اصفهان می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: شبکه‌های هوشمند، منابع انرژی تجدیدپذیر و سیستم‌های قدرت تجدید ساختار یافته.

صغری نوبختیان تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد ریاضی از دانشگاه شیراز و اصفهان به‌ترتیب در سال‌های ۱۳۶۵ و ۱۳۷۰ و در مقطع دکتری در سال ۱۳۷۷ از دانشگاه مگ گیل کانادا به پایان رسانده است. او هم‌اکنون استاد گروه ریاضی کاربردی و علوم کامپیوتر دانشکده ریاضی و آمار دانشگاه اصفهان می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان شامل بهینه سازی غیر خطی و کنترل بهینه می‌باشد.