نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۴۰۱-۳۹۱

«علمی- پژوهش»

ارائه الگوریتمی جهت شناسایی آسیب‌پذیرترین شین در شبکه هوشمند برق در حمله سایبری مبتنی بر تخمین حالت

امیرحسین طیبی[۱]، رضا شریفی[۲*]، امیرحسین سالمی[۳]، فرامرز فقیهی[۴]

۱- دانشجوی دکتری تخصصی، گروه مهندسی برق، واحد اراک، دانشگاه آزاد اسلامی، اراک، ایران ۲- استادیار، گروه مهندسی برق، واحد تهران غرب، دانشگاه آزاد اسلامی، تهران، ایران ۳- استادیار، گروه مهندسی برق، واحد اراک، دانشگاه آزاد اسلامی، اراک، ایران ۴- استادیار، گروه مهندسی برق، واحد علوم تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران

(دریافت: ۹۸/۱۱/۰۶، پذیرش: ۹۹/۰۲/۲۲)

چکیده

با توجه به خودکارسازی شبکه‌های قدرت و مبادله داده‌ها در یک زیرساخت مخابراتی، احتمال طرح‌ریزی حمله سایبری بسیار بالا است. در این راستا بهینه‌سازی بودجه‌های حمله و دفاع در حمله سایبری در شبکه قدرت از اهمیت خاصی برخوردار است. در این مقاله در راستای فاز تهاجم سایبری به شبکه قدرت، انتخاب آسیب‌پذیرترین شین عملیاتی با استفاده از فن تخمین حالت طی الگوریتم جدیدی تحلیل و شبیه‌سازی‌شده است. برای این منظور تزریق داده غلط به اطلاعات ارسالی از PMU به‌گونه‌ای که قابل‌تشخیص برای بهره‌بردار شبکه تحت تهاجم نباشد صورت می‌پذیرد. به‌عنوان یک مطالعه موردی پیاده‌سازی الگوریتم پیشنهادی برای یک شبکه ۱۴ شینِ IEEE انجام‌شده است و بهترین شین ازنظر قرارگیری تحت تهاجم شناسایی‌شده است. عملکرد این الگوریتم مبنی بر نتایج حاصل از تخمین حالت شبکه پس از رخداد حمله سایبری بر روی شین‌های مختلف است. درنهایت قسمتی از شبکه که تخریب اطلاعات در آن بخش بیشترین آسیب را به شبکه وارد می‌کند مشخص می‌شود.

کلیدواژه‌ها: تزریق داده غلط، حمله غیرقابل تشخیص، سامانه قدرت، تخمین حالت، بردار اندازه‌گیری

Presentation of an Algorithm for Identification of the Most Vulnerable Bus in Electric Smart Grid Through Cyber-Attack Based on State Estimation

A. H. Tayebi, R. Sharifi*, A. H. Salemi, F. Faghihi
Faculty of Electrical Engineering, West Tehran Branch, Islamic Azad University, Tehran, Iran
(Received: 26/01/2020; Accepted: 11/05/2020)

Abstract

Considering the power grids automation and network data transferring in telecommunication infrastructure, the possibility of planning a cyber-attack grows up intensively. In this regard, the optimization of the budget for attack (BA) and budget for defense (BD) in a power network through cyber-attack is so crucial. In this paper, regarding the cyber invasion phase, the choice of the most vulnerable operating bus using the state estimation technique through a new algorithm is analyzed and simulated. For this purpose, false data injection is performed on the data sent from the PMU in such a way that it is not detectable to the network dispatching operator under the invasion. As a case study implementation of the suggested algorithm for a 14 IEEE bus network is carried out and the best bus in terms of exposure under attack is identified. The performance of this algorithm is based on the results obtained from state estimating of the grid after occurring a cyber-attack on different buses. Finally, the part of the grid, which the destruction of information in that part leads to the most damage to the grid, is determined.

Keywords: False Data Injection, Undetectable Attack, Power System, State Estimation, Measurement Vector.

*Corresponding Author E-mail: Sharifi.r@wtiau.ac.ir

۱. مقدمه

شبکه‌های هوشمند یکی از مهم‌ترین ساختارهای مبتنی بر دستگاه‌های سایبر-فیزیکی می‌باشند. به همین خاطر این شبکه‌ها دارای قابلیت اطمینان بالا و کارایی بیشتر در زمان افزایش مصرف می‌باشند. ادوات ارتباط داخلی از قبیل واحدهای اندازه‌گیری فازور PMU (Phasor measurement units) و اندازه‌گیرهای هوشمند ازجمله زیرساخت‌های مهم این شبکه‌ها برای رسیدن به اهدافشان به‌حساب می‌آیند. این زیرساخت‌های سایبری با بالا بردن دسترسی و انتقال اطلاعات در سامانه، از طریق ادغام ارتباطات، محاسبات و فناوری‌های پیشرفته کنترل، وضعیت سامانه را کنترل می‌کنند. درواقع سامانه‌های سایبر- فیزیکی نسل جدیدی از سامانه‌ها هستند که منابع محاسباتی، وسایل ارتباطی عملیات فیزیکی را شامل می‌شوند. ازجمله کاربردهایی که این سامانه‌ها دارند تخمین حالت سامانه با استفاده از اطلاعات به‌دست‌آمده از این سامانه‌ها است. تخمین حالت درواقع پروسه تخمین متغیرهای حالت نامعلوم با استفاده از مقادیر اندازه‌گیری شده توسط اندازه‌گیرها در شبکه است. تخمین حالت یکی از مهم‌ترین ابزارهای مدیریت انرژی سامانه است. تخمین حالت سامانه وضعیت فیزیکی سامانه را مشخص می‌کند (البته باوجود نویز) که می‌توان با استفاده از این اطلاعات دستورات لازم را به سامانه‌های فیزیکی ارسال کرد. پس تخمین حالت سامانه از لوازم مهم کنترل سامانه است.

امنیت شبکه‌های برق یکی از عواملی است که در کنترل این سامانه‌ها نقش اساسی دارد. یکی از راه‌کارهای مقابله با هر مجموعه‌ای از بین بردن این امنیت و درنتیجه ایجاد اخلال در سامانه برق‌رسانی آن مجموعه است. مهاجمین برای از کار انداختن شبکه‌های قدرت دست به حمله به این شبکه‌ها برای از کار انداختن عملکرد صحیح آن‌ها می‌زنند. پس یکی از راه‌کارهای آسیب رساندن به دشمن ایجاد اختلال در شبکه‌های برق‌رسانی و درنتیجه ایجاد خاموشی در شبکه‌های برق است. این اختلال را می‌توان به طرق مختلف ایجاد کرد. یکی از راه‌های اختلال در شبکه‌های قدرت حمله فیزیکی به این شبکه‌ها و از بین بردن زیرساخت‌های انتقال برق از قبیل خطوط انتقال یا ترانسفورماتورها است؛ اما روش دیگری که برای ایجاد اختلال در شبکه‌های قدرت وجود دارد حملات سایبری به زیرساخت‌های سایبری- فیزیکی این شبکه‌ها است.

حملات سایبری می‌توانند سامانه‌های کنترل‌کننده شبکه‌های الکتریکی را تضعیف کنند یا حتی به‌طورکلی از بین ببرند. درگذشته تصور می‌شد که حملات سایبری نمی‌توانند امنیت سامانه‌های برق صنعتی را تهدید کنند؛ اما در سال‌های گذشته حملات سایبری تأثیر بسیار مهمی در مسائل امنیتی چه در بحث صنعتی و چه از دیدگاه تأمین‌کنندگان انرژی داشته‌اند. مثلاً در سال ۲۰۰۰ سامانه SCADA (Supervisory Control and Data Acquisition) فاضلاب شهری یکی از ایالت‌های استرالیا موردحمله قرار گرفت. در سال ۲۰۰۳ به سامانه‌های کامپیوتری یکی از نیروگاه‌های اتمی یکی از ایالت‌های امریکا توسط حملات سایبری نفوذ کردند. همچنین در سال ۲۰۱۰ نیز یک حمله سایبری به تأسیسات اتمی نطنز صورت گرفت.

در سال‌های اخیر حملات سایبری به تهدیدی مهم برای یکپارچگی سامانه‌های تخمین حالت سامانه تبدیل‌شده است. حملات سایبری که به‌خوبی برنامه‌ریزی‌شده باشند می‌توانند اثرات فاجعه باری بر روی سامانه بگذارند تا حدی که ممکن است منجر به خاموشی سراسری در شبکه گردند. یکی از انواع متداول این حملات، حمله از طریق تزریق اطلاعات غلط به سامانه است. در این نوع حمله دشمن با تزریق اطلاعات غلط تخمین حالت سامانه را با خطا مواجه می‌کند که این عمل منجر به تصمیم‌گیری غلط از طریق سامانه‌های کنترلی می‌گردد.

در این سال‌ها مقالات زیادی به بررسی حملات سایبری بر روی شبکه‌های برق پرداخته‌اند. این حملات از جهت‌های مختلفی موردبررسی و تحلیل قرارگرفته‌اند. در [۲-۱] به بررسی و تحلیل حملات از نوع تزریق اطلاعات غلط بر روی شبکه‌های هوشمند پرداخته شده است. در این مقالات روش‌ها و تحلیل‌هایی برای شناسایی و تشخیص این حملات ارائه شده است. همچنین روش‌هایی ارائه‌شده که میزان خسارات ناشی از این حملات کاهش یابد.

یکی از مواردی که بر روی میزان اثرگذاری حملات و همچنین نوع راهبرد حمله تأثیرگذار است، مکان قرار گرفتن واحدهای اندازه‌گیری (PMUها) است. این اندازه‌گیرها انواع متفاوتی دارند. یکی از راهبردهای دفاع در برابر حملات سایبری ارتقا امنیت این اندازه‌گیرها به نحوی است که دشمن قابلیت نفوذ به آن‌ها را نداشته باشد؛ اما همان‌طور که اشاره شد نحوه قرارگیری این اندازه‌گیرها در شبکه بر روی تأثیرگذاری حمله دشمن مؤثر است.

در [۴-۳] به بررسی مسئله جایابی بهینه PMUها پرداخته شده است. این جایابی بهینه با در نظر گرفتن شرایط اضطراری در شبکه انجام‌شده و درنهایت بهترین حالت قرارگیری PMU ها با توجه به انواع مختلف خطاهایی که ممکن است در شبکه وجود داشته باشد، مشخص می‌شود. در [۵] با توجه به این‌که شبکه مورد یک حمله سایبری از نوع تزریق اطلاعات غلط قرارگرفته، راه‌کاری ارائه‌شده که در این شرایط وضعیت ادوات سایبری- فیزیکی سامانه به‌درستی تخمین زده شود.

یکی دیگر از مباحث مرتبط با حملات سایبری بحث دفاع در برابر این حملات است؛ یعنی پس از تشخیص اتفاق افتادن حمله سایبری، باید راه‌کارهایی ارائه شود که بتوان از این شبکه‌ها در برابر این حملات دفاع کرد. در [۶] به بررسی دفاع در برابر حملات از نوع تزریق داده غلط بر روی تخمین متغیرهای حالت سامانه پرداخته‌شده است. ازجمله مسائل مهمی که در این مقاله موردبررسی قرارگرفته این است که کدام‌یک از اندازه‌گیرها محافظت شوند تا سامانه آسیب کمتری ببیند. همچنین مسئله تأثیر انتخاب PMU محافظت‌شده بر روی بودجه دفاعی سامانه موردبررسی قرارگرفته. به این معنی که کدام‌یک از PMU ها محافظت شود تا بودجه دفاعی افزایش کمتری داشته باشد.

در این مقاله بر روی ساختار حملات سایبری غیرقابل تشخیص بحث شده است. درنتیجه حمله‌ای که در اینجا موردبررسی قرارگرفته یک حمله از نوع تزریق داده غلط به شکلی است که مدافع قابلیت تشخیص این حمله را نداشته باشد. پس ابتدا در مورد نحوه انجام یک حمله سایبری غیرقابل تشخیص بحث شده است. بحث حمله سایبری در اینجا از دیدگاه مهاجم مطرح‌شده است؛ یعنی سعی بر این است که حمله سایبری ترتیب داده شود که بدون اینکه مدافع متوجه آن بشود (بدون اینکه تغییر یا تناقضی در مقادیر متغیرهای حالت یا پارامترهای اندازه‌گیری شده وجود داشته باشد) مقادیر اندازه‌گیری شده PMU ها و درنتیجه حالت‌های تخمین زده‌شده تخریب شوند. یکی از اطلاعاتی که مهاجم برای انجام چنین حمله‌ای به آن نیاز دارد، اطلاعات کامل نسبت به ساختار شبکه مدافع است. پس باید به این نکته توجه کرد که برای انجام حمله غیرقابل تشخیص به یک شبکه نیاز به داشتن اطلاعات از آن شبکه است.

یکی از مواردی که در تعیین میزان اثرپذیری حمله مؤثر است منطقه حمله است. این بدان معنی است که کدام‌یک از اندازه‌گیرهای سامانه تخریب شود تا بیشترین تأثیر مخرب را بر روی شبکه مدافع بگذارد. در این مقاله الگوریتمی ارائه‌شده که با استفاده از آن می‌توان بهترین ناحیه برای دستیابی به بیشترین آسیب را مشخص نمود. شبیه‌سازی‌هایی انجام‌شده تا تأثیر این حملات در شرایط مختلف حمله موردبررسی قرار گیرد.

۲. روش تحقیق

تخمین حالت سامانه یکی از موارد مهم در مدیریت انرژی یک سامانه است. برای دست‌یابی به این مهم مرکز کنترل سامانه قدرت اطلاعات اندازه‌گیری شده را از RTUها (Terminal Unit Remote) دریافت می‌کنند. اطلاعاتی که RTUها به ما می‌دهند شامل توان اکتیو و راکتیو تزریقی به شین‌ها، توان اکتیو و راکتیو جاری بین خطوط و ولتاژ و زاویه ولتاژ شین اصلی می‌شود. اطلاعات این اندازه‌گیرها در تخمین حالت سامانه مورداستفاده قرار می‌گیرند. اطلاعات اندازه‌گیری که از این RTUها به‌دست می‌آیند، ممکن است حاوی خطاهای ناشی از اندازه‌گیری باشند. این خطاهای اندازه‌گیری اغلب به شکل تصادفی هستند که منشأ به وجود آمدن آن‌ها می‌تواند نویزهای موجود یا عملکرد غلط ادوات اندازه‌گیری باشد. همان‌طور که مشخص است اگر چنین خطاهایی وجود داشته باشد، این خطاها به یکدیگر وابسته نبوده و روش‌های تخمین حالت می‌توانند حالت سامانه را به‌درستی تخمین بزنند. گذشته از این خطاهای کوچک، ممکن است در مواقعی که اشکالات ارتباطی در سامانه به وجود می‌آید خطاهای بزرگ‌تری نیز وجود داشته باشد. این خطاها نیز به یکدیگر وابسته نبوده و توسط روش‌های تشخیص خطای موجود قابل شناسایی هستند.

در این مقاله بر روی حملات سایبری از نوع تزریق اطلاعات غلط بحث شده که سامانه‌های تشخیص خطا قابلیت شناسایی آن‌ها را ندارند. درواقع این نوع اطلاعات به شکلی هماهنگ شده به سامانه تزریق می‌شوند که سامانه تشخیص خطا را دور می‌زنند. در مقابله با این حملات کارهای متفاوتی انجام می‌شود. در [۷] به بررسی اثرات ناشی از حملات تزریق اطلاعات غلط بر روی سامانه‌ها و نحوه نجات سامانه در برابر این حملات پرداخته‌شده است.

۲-۱. تخمین حالت DC

تخمین حالت DC بر اساس معادله خطی (۱) انجام می‌شود.

$$z = Hx + e \qquad (۱)$$

در این رابطه، $z = (z_1, z_2, \dots, z_m)^T$ بردار اندازه‌گیری است که شامل m اندازه‌گیر است. این اندازه‌گیری‌ها شامل تزریق توان اکتیو به شین‌ها و توان اکتیو جاری بین خطوط انتقال می‌شود. $x = (x_1, x_2, \dots, x_n)^T$ بردار حالت صحیح سامانه است که باید تخمین زده شود. درنتیجه تعداد متغیرهای حالت n متغیر در نظر گرفته‌شده است. H یک ماتریس ژاکوبی $m \times n$ است که تابع خطی اندازه‌گیری نام دارد. H بر اساس ساختار شبکه به‌دست می‌آید. $e = (e_1, e_2, \dots, e_m)^T$ بردار خطای اندازه‌گیری است و R ماتریس قطری است که کوواریانس خطای اندازه‌گیری را نشان می‌دهد.

اگر تعداد اندازه‌گیرها برای تخمین حالت کافی باشد، شبکه قدرت یک شبکه رؤیت پذیر است. الگوریتم‌های متفاوتی برای جایابی اندازه‌گیرها وجود دارد که شبکه را رؤیت‌پذیر کند [۸]. اصولاً تعداد اندازه‌گیرهایی که در شبکه وجود دارد بیش از آن

تعدادی است که برای رؤیت پذیر شدن شبکه موردنیاز است (اغلب $m > n$). در تخمین حالت DC فرض می‌شود که دامنه ولتاژ شین‌ها برابر ۱ است. همچنین ادمیتانس‌های موازی و مقاومت خطوط قابل صرف‌نظر هستند. توان اکتیو جاری بین دو شین از رابطه $P_{ij} = \frac{\theta_i - \theta_j}{X_{ij}}$ قابل‌محاسبه است که در آن X_{ij} راکتانس شاخه بین i و j و همچنین θ_i و θ_j زاویه فاز شین‌های i و j هستند.

$\hat{x}$ که همان حالت تخمین زده‌شده سامانه است به روش DC از کمینه کردن تابع معادله (۲) به‌دست می‌آید.

$$F(x) = (z - Hx)^T R^{-1} (z - Hx) \quad (۲)$$

بردار $\hat{x}$ که تابع بالا را حداقل می‌کند از رابطه (۳) به‌دست می‌آید [۹].

$$\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z \quad (۳)$$

۲-۲. تشخیص داده بد و حملات از نوع تزریق داده غلط

ازجمله روش‌هایی که می‌توان برای تشخیص حمله استفاده کرد این است که مقدار باقیمانده $r = z - H\hat{x}$ را به‌دست آورد. برای تشخیص اینکه حمله‌ای اتفاق افتاده یا خیر می‌توان این مقدار باقیمانده را با یک مقدار مشخصی که از قبل با توجه به شرایط مختلف مشخص‌شده مقایسه کرد. این روش به روش تشخیص داده بد مرسوم است. اگر از دید حمله‌کننده نگاه شود، باید حمله به شکلی اتفاق بیفتد که توسط این روش قابل‌تشخیص نباشد. برای انجام چنین حمله‌ای باید اولاً ساختار شبکه مدافع برای حمله‌کننده شناخته‌شده و دقیقاً مشخص باشد (حمله‌کننده از H اطلاعات داشته باشد) و ثانیاً مهاجم قابلیت این را داشته باشد که به‌طور هم‌زمان چند اندازه‌گیر را تخریب کند [۱۰]. اگر مهاجم بتواند بردار اندازه‌گیری را به شکل $z_b = z + a$ تغییر دهد، در صورتی می‌شود سامانه تشخیص مدافع را از کار انداخت که $a = Hc$ باشد. در این رابطه a داده مخربی است که به اندازه‌گیرها اضافه‌شده و c خطای تزریق‌شده به حالت سامانه است. همان‌طور که مشاهده می‌شود مقدار بردار اندازه‌گیری در این حالت تغییر کرده است اما بعد از اعمال شدن این داده مخرب، حالت سامانه‌ای که توسط روش تخمین DC تخمین زده می‌شود به شکل $\hat{x}_{bad} = \hat{x} + c$ تغییر می‌کند. با استفاده از این بردار تخمین حالت مقدار باقیمانده که روش تشخیص حمله از آن استفاده می‌کند به شکل رابطه (۴) به‌دست می‌آید [۱۱].

$$r_{bad} = z_{bad} - H\hat{x}_{bad} = z + a - H(\hat{x} + c) = z - H\hat{x} = r \quad (۴)$$

همان‌طور که مشاهده می‌شود رابطه به‌دست‌آمده برای مقدار باقیمانده با توجه به بردار تخمین حالت پس از حمله با مقدار آن قبل از انجام حمله یکسان است. پس با این روش حمله‌ای اتفاق افتاده که سامانه تشخیص حمله مدافع قابلیت تشخیص آن را ندارد.

۲-۳. تخمین حالت AC و تزریق داده غلط در این حالت

در این حالت برخلاف تخمین حالت DC یک تابع غیرخطی بین اندازه‌گیری‌ها و حالت سامانه وجود دارد. این تابع به شکل (۵) است.

$$z = h(x) + e \quad (۵)$$

در این رابطه، h یک تابع غیرخطی بین بردار اندازه‌گیری (z) و بردار حالت سامانه (x) است. در این حالت بردار x شامل اندازه ولتاژ شین‌ها و زاویه فاز آن‌ها است. در این حالت مهاجم برای اینکه سامانه تشخیص حمله مدافع را بی‌اثر کند باید برداری به شکل $a = h(\hat{x} + c) - h(\hat{x})$ را به بردار اندازه‌گیری اضافه کند. در حالت AC هریک از متغیرهای حالت می‌توانند بر روی مقادیر چهار اندازه‌گیری که ممکن است در اطراف آن‌ها وجود داشته باشد، تأثیر بگذارد. این چهار اندازه‌گیر شامل حس‌گرهای اندازه‌گیری توان اکتیو و راکتیو شین مربوط به آن متغیر حالت و حس‌گرهای اندازه‌گیری توان اکتیو و راکتیو جاری بین آن شین و شین‌های مجاور است. پس نکته مهم در این حالت این است که برای هدف قرار دادن یک متغیر حالتی که مربوط به شین i می‌باشد، اندازه‌گیری‌هایی که باید تخریب شوند P_i، Q_i، P_{ij} و Q_{ij} است که j مجموعه شین‌های متصل به شین i است.

اگر حمله‌کننده بخواهد هم‌زمان چند متغیر حالت را تغیر دهد، نیاز به تخریب تعداد بیشتری کنتور هست. مثلاً اگر حمله‌کننده بخواهد مجموعه K متغیر حالت را تغییر دهد، توان اکتیو و راکتیو تزریقی به این شین‌ها و توان اکتیو و راکتیو بین این شین‌ها و شین‌های اطرافشان باید تخریب شود. به همین خاطر حمله به بیش از یک متغیر حالت ازنظر اقتصادی به‌صرفه نیست، خصوصاً اگر این متغیرها مربوط به دو شینی باشد که فاصله آن‌ها از هم زیاد است. درنتیجه اگر تصمیم بر حمله به بیش از یک متغیر باشد تا حد امکان شین‌هایی انتخاب می‌شود که به هم نزدیک باشند [۱۲].

در انجام یک حمله غیرقابل تشخیص دو چیز باید مشخص شود. در مرحله اول باید مشخص شود که کدام‌یک از اندازه‌گیرها باید تخریب شود و در مرحله دوم مقادیر این تغییرات مشخص می‌شوند. در تخمین حالت AC همه اندازه‌گیرهایی که با شین تخریب‌شده در ارتباط هستند، باید تخریب شوند. در حالت DC ماتریس H ماتریسی بود که نشان می‌داد کدام اندازه‌گیری با کدام متغیر حالت در ارتباط است. در تخمین حالت AC همان‌طور که

اشاره شد رابطه بین متغیرهای حالت و مقادیر اندازه‌گیری شده یک رابطه غیرخطی است. در اینجا ماتریس ژاکوبی $h(x)$ که به شکل (۶) تعریف می‌شود مشخص می‌کند که کدام‌یک از اندازه‌گیرها به کدام‌یک از متغیرهای حالت وابسته است. به این شکل که اگر اندازه‌گیری به متغیر حالتی وابسته باشد، سطر مربوط به آن اندازه‌گیر در ستون آن متغیر حالت غیر صفر است؛ یعنی اگر اندازه‌گیری به متغیر حالتی وابسته نباشد، درایه مربوط به آن در ماتریس برابر صفر است [۱۳].

$$J_h = \begin{bmatrix} {dh_1}/{dx_1} & {dh_1}/{dx_2} & \cdots & {dh_1}/{dx_n} \\ \vdots & \vdots & \ddots & \vdots \\ {dh_m}/{dx_1} & {dh_m}/{dx_2} & \cdots & {dh_m}/{dx_n} \end{bmatrix} \quad (۶)$$

با بررسی این ماتریس می‌توان با توجه به مقادیر غیر صفر هر ستون متوجه شد که برای تغییر در یک متغیر حالت حداقل چه تعداد اندازه‌گیر باید تخریب شود (درواقع به تعداد عناصر غیر صفر موجود در هر ستون). بعدازاینکه مشخص شد که کدام اندازه‌گیرها باید تغییر کنند سؤال مهم دیگری که وجود دارد این است که مقادیر جدید آن‌ها چه مقداری باید باشد.

مقادیر توان اکتیو (P_{ij}) و راکتیو (Q_{ij}) جاری در خطوط از معادلات (۷) و (۸) قابل‌دستیابی است.

$$P_{ij} = V_i^2.g_{ij} - V_iV_jg_{ij}\cos(\theta_i-\theta_j) - V_iV_jb_{ij}\sin(\theta_i-\theta_j) \quad (۷)$$

$$Q_{ij} = -V_i^2.(b_{ij}+b_{ij}^{sh}) + V_iV_jb_{ij}\cos(\theta_i-\theta_j) - V_iV_jg_{ij}\sin(\theta_i-\theta_j) \quad (۸)$$

در این روابط V_i ولتاژ شین iام که به‌عنوان شین مبدأ در نظر گرفته‌شده و V_j ولتاژ شین jام که شین مقصد خط انتقال است در نظر گرفته‌شده است. همچنین g_{ij} و b_{ij} پارامترهای مربوط به ادمیتانس سری خطوط انتقال و b_{ij}^{sh} پارامتر مربوط به ادمیتانس موازی خط انتقال می‌باشد. θ_i و θ_j نیز به ترتیب مقادیر اندازه فاز شین‌های مبدأ و مقصد هستند. همچنین مقادیر توان اکتیو و راکتیو تزریقی به شین‌ها از روابط (۹) و (۱۰) محاسبه می‌شوند.

$$P_i = \sum_{j\in\vartheta_i} P_{ij} \quad (۹)$$

$$Q_i = \sum_{j\in\vartheta_i} Q_{ij} \quad (۱۰)$$

در این روابط ϑ_i مجموعه شین‌های متصل به شین i می‌باشد. مشابه حالت DC انتخاب ستون و اندازه‌گیری که باید تنظیم شود، متغیر حالتی که باید تخریب شود را تعیین می‌کند. فرض شود که مهاجم برای تخریب V_i به‌عنوان متغیر حالت سعی می‌کند که توان انتقالی بین شین‌های i و j را تغییر دهد، در این صورت معادله (۱۱) باید حل شود تا مشخص شود که دامنه ولتاژی که به توان جاری مدنظر منجر می‌شود چقدر است.

$$P_{ij} = V_{i,a}^2.g_{ij} - V_{i,a}V_j.g_{ij}\cos(\theta_i-\theta_j) - V_{i,a}V_j.b_{ij}\sin(\theta_i-\theta_j) \quad (۱۱)$$

در این رابطه زیر وند a متغیر حالتی را نشان می‌دهد که توسط حمله‌کننده تحت تأثیر قرار می‌گیرد. معادله (۱۱) یک معادله درجه دوم است که دو جواب دارد. در اغلب موارد فقط یکی از پاسخ‌ها با توجه به شرایط قابل‌پذیرش هستند. در آنالیز DC مهاجم نیازی به دانستن مقادیر متغیرهای حالت ندارد اما در حالت AC این‌گونه نیست؛ یعنی علاوه بر اینکه باید معادله (۱۱) را حل کند باید مقادیر V_j و $\theta_i-\theta_j$ را نیز تخمین بزند.

با مشخص شدن مقدار $V_{i,a}$ مقادیر دیگر اندازه‌گیرها نیز توسط روابط (۷) و (۸) قابل‌دستیابی هستند. در آنالیز AC یک گزینه دیگری که وجود دارد این است که θ_i به‌عنوان متغیر حالتی در نظر گرفته شود که باید تخریب شود. با توجه به این حقیقت که حساسیت توان‌های جاری در خطوط و توان‌های تزریقی به شین‌ها نسبت به زاویه ولتاژ بیشتر از اندازه ولتاژ است، با ایجاد تغییرات کمتر در زاویه ولتاژ، تأثیر بیشتری روی توان جاری در خطوط گذاشته می‌شود. طبیعتاً اگر هر دو آن‌ها (هم‌اندازه و هم زاویه ولتاژ) به‌عنوان متغیر حالت تخریب‌شده در نظر گرفته شوند، مجموعه جواب‌های ممکن بزرگ‌تر می‌شود. در این حالت برای اینکه تغییرات اندازه‌گیرهایی که در مرحله اول گفته شد منجر به یک حمله مخفی (غیرقابل تشخیص) شود باید شرایط معادله (۱۲) را داشته باشد. در این شرایط سامانه تشخیص اطلاعات غلط نمی‌تواند انجام حمله را تشخیص دهد [۱۴].

$$\|z_{bad}-h(\hat{x}_{bad})\| = \|z+a-h(\hat{x}+c)\| = \left\|\begin{pmatrix} z_1 \\ z_2+a_2 \end{pmatrix} - \begin{pmatrix} h_1(\hat{x}) \\ h_2(\hat{x}_1,\hat{x}_2+c) \end{pmatrix}\right\| = \left\|\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} - \begin{pmatrix} h_1(\hat{x}) \\ h_2(\hat{x}_1,\hat{x}_2) \end{pmatrix}\right\| = \|z-h(\hat{x})\| < \tau \quad (۱۲)$$

در این رابطه متغیرهایی که زیر وند ۱ دارند مربوط به اندازه‌گیری‌ها و متغیرهای حالتی هستند که توسط مهاجم تغییر داده نشده‌اند. متغیرهایی که زیر وند ۲ دارند آن‌هایی هستند که تخریب‌شده‌اند. بردار a مربوط به تغییرات موردنیاز در اندازه‌گیرهای موردحمله قرارگرفته و بردار c مربوط به تغییرات در متغیرهای حالت تخمین زده‌شده می‌باشند.

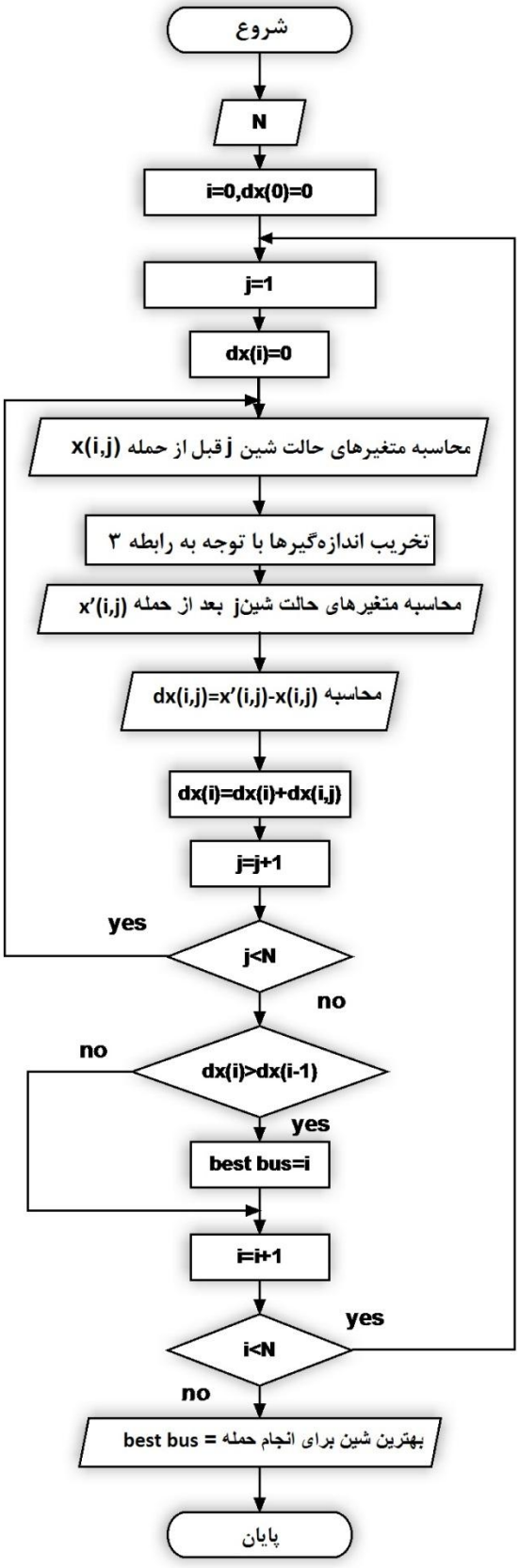
از معادله (۱۲) نتیجه می‌شود که بردار تغییر در اندازه‌گیری که نتیجه آن حمله غیرقابل تشخیص است به شکل (۱۳) می‌باشد.

$$a_2 = h_2(\hat{x}_1,\hat{x}_2+c) - h_2(\hat{x}_1,\hat{x}_2) \quad (۱۳)$$

درنتیجه در حالت AC مهاجم باید مقادیر تخمین زده‌شده برای مجموعه متغیرهای حالتی که در h_2 وجود دارد را بداند.

۲-۴. ارائه الگوریتم شناسایی آسیب‌پذیرترین شین

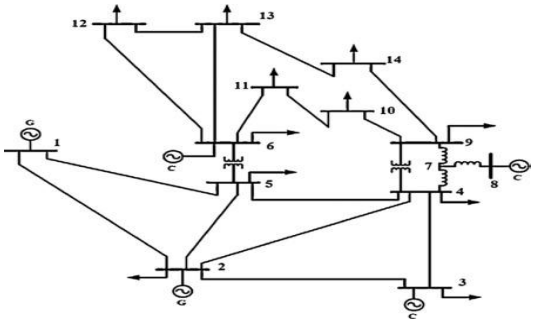
شکل حمله به یک شبکه قدرت می‌تواند اثرات مختلفی بر روی شبکه بگذارد. یکی از مواردی که در میزان اثرگذاری یک حمله سایبری مؤثر است قسمتی از شبکه است که تحت حمله قرار می‌گیرد. در این بررسی فرض بر این است که هیچ‌یک از شین‌های شبکه تحت مطالعه (به‌جز شین شماره ۱) شین‌های حفاظت‌شده نیستند (منظور شین‌هایی هستند که کنترل‌گر شبکه مدافع از صحت اطلاعات ارسالی توسط آن‌ها اطمینان دارد). درنتیجه تزریق داده غلط به‌منظور تخریب بردار اندازه‌گیری می‌تواند بر روی هر یک از شین‌ها اتفاق افتد. سؤالی که مطرح می‌شود این است که حمله سایبری بر روی کدام شین اتفاق افتد که بیشترین مقدار آسیب را به شبکه مدافع وارد کند. البته نکته مهم دیگری که وجود دارد این است که منظور از بیشترین آسیب چیست. بیشترین آسیب می‌تواند از دو دیدگاه در نظر گرفته شود که به هدف مهاجم برمی‌گردد. در برخی انواع حمله‌ها هدف مهاجم تعداد متغیر حالت تخریب‌شده بیشتر نیست و فقط دامنه تغییر یک متغیر حالت مدنظر است؛ یعنی در این حالت مهاجم از بین گزینه‌های مختلف حمله به شین‌ها به دنبال آن شینی می‌گردد که بیشترین تغییر را در یک متغیر حالت ایجاد می‌کند؛ اما در حالت کلی و ازنظر کنترل شبکه بیشترین تخریب زمانی در شبکه مدافع ایجاد می‌شود که بیشترین تعداد متغیر حالت دچار بیشترین تغییر شود. پس در این مقاله بدین منظور الگوریتمی ارائه‌شده که از بین شین‌های مختلف یک شبکه، شینی که حمله به آن باعث بیشترین تغییر کلی در مقادیر متغیرهای حالت شبکه می‌شود را مشخص می‌کند. ذکر این نکته نیز مهم است که در این محاسبه نوع حمله به‌تمامی شین‌ها یکسان در نظر گرفته می‌شود. همچنین فرض شده که ازنظر محدودیت یا هزینه انجام حمله هیچ تفاوتی بین شین‌های مختلف شبکه وجود ندارد. اگر میزان هزینه حمله به شین‌های مختلف شبکه برای ایجاد تغییر یکسان در متغیرهای حالت آن‌ها متفاوت باشد باید هزینه حمله نیز در الگوریتم در نظر گرفته شود. الگوریتم انتخاب بهترین شین در جهت ایجاد بیشترین آسیب در شبکه مدافع در شکل (۱) نشان داده‌شده است. تصمیم‌گیری این الگوریتم بر اساس اطلاعات به‌دست‌آمده پس از انجام تخمین حالت در سامانه به‌دست‌آمده است. منظور از تخمین حالت در اینجا همان تخمین حالت AC است.



شکل ۱. الگوریتم شناسایی آسیب‌پذیرترین شین شبکه مدافع در جهت تخریب مقادیر متغیرهای حالت

۳. نتایج و بحث

در این مقاله یک شبکه ۱۴ شینِ IEEE برای انجام شبیه‌سازی مورداستفاده قرار می‌گیرد. ساختار چنین ریز شبکه‌ای در شکل (۲) نشان داده‌شده است. اطلاعات فنی مربوط به این ریزشبکه در [۱۵] ارائه شده است. شین‌های ۱ تا ۵ به ژنراتورها متصل هستند که می‌توانند یکی از انواع منابع تولید پراکنده در نظر گرفته شوند. در ابتدا با توجه به مقادیر توان اکتیو و راکتیو ارسالی از اندازه‌گیرها مقادیر متغیرهای حالت سامانه تخمین زده می‌شود. توان‌های اکتیو و راکتیو تزریقی به شین‌های ۳، ۴، ۸، ۱۰، ۱۱، ۱۲ و ۱۴ توسط اندازه‌گیرهای این شین‌ها در دسترس هستند. شماره اندازه‌گیرهای توان اکتیو در بردار اندازه‌گیری از ۳ تا ۹ و شماره اندازه‌گیرهای توان راکتیو از ۱۰ تا ۱۶ است. همچنین اندازه‌گیرهایی در این شبیه‌سازی بر روی خطوط (۱ و ۲)، (۲ و ۳)، (۴ و ۲)، (۴ و ۷)، (۵ و ۲)، (۶ و ۱۳)، (۱۱ و ۶) و (۱۲ و ۱۳) قرارگرفته و توان‌های اکتیو و راکتیو جاری بین خطوط را اندازه‌گیری می‌کنند. شماره اندازه‌گیرهای توان اکتیو این خطوط از ۱۷ تا ۲۴ و اندازه‌گیرهای توان راکتیو از ۲۵ تا ۳۲ در بردار اندازه‌گیری می‌باشد. اندازه‌گیرهای شماره ۱ و ۲ نیز بر روی شین یک برای اندازه‌گیری اندازه و زاویه ولتاژ قرار دارد.



شکل ۲. ساختار ریز شبکه استاندار ۱۴ شین IEEE [۱۵]

یکی از مسائلی که در بحث حملات سایبری می‌تواند موردتوجه قرار گیرد مکان‌های قرارگیری این اندازه‌گیرها است. درواقع از دید مدافع با تغییر جایگاه این اندازه‌گیرها می‌توان در برابر حملات سایبری احتمالی به تخریب‌های کمتر دست‌یافت. پس یکی از مباحثی که می‌تواند موردتوجه قرار گیرد کمینه کردن اثر یک حمله خاص بر روی شبکه با تغییر آرایش قرارگیری PMU ها است. چون در این مقاله منافع مهاجم مدنظر قرارگرفته شده و انجام یک حمله با حداکثر میزان تخریب در شبکه مدافع مدنظر است، با در نظر گرفتن مکان‌های متفاوت برای تخریب داده اثرات حمله‌بر روی شین‌های مختلف بررسی‌شده و بهترین حالت حمله از دید مهاجم به‌دست می‌آید.

در حالت عادی و بدون اتفاق افتادن حمله مقادیری که برای متغیرهای حالت این شبکه با استفاده از اطلاعات PMU ها تخمین زده می‌شود در جدول (۱) نشان داده‌شده است. مقادیر جداول و نتایج همه شبیه‌سازی‌های این مقاله در فضای نرم‌افزار MATLAB انجام‌شده است.

جدول ۱. متغیرهای حالت شبکه بدون اتفاق افتادن حمله

شماره شین	دامنه ولتاژ	اندازه فاز
۱	۱,۰۶۰۰	۰,۰۰۰۰
۲	۱,۰۴۵۰	-۴,۹۸۰۰
۳	۱,۰۱۰۰	-۱۲,۷۲۰۰
۴	۱,۰۱۸۶	-۱۰,۳۲۰۰
۵	۱,۰۲۰۳	-۸,۷۸۰۰
۶	۱,۰۶۹۸	-۱۴,۲۲۰۰
۷	۱,۰۶۱۹	-۱۳,۳۷۰۰
۸	۱,۰۹۰۰	-۱۳,۳۷۰۰
۹	۱,۰۵۶۱	-۱۴,۹۵۰۰
۱۰	۱,۰۵۱۱	-۱۵,۱۰۰۰
۱۱	۱,۰۵۶۹	-۱۴,۸۰۰۰
۱۲	۱,۰۵۵۰	-۱۵,۰۸۰۰
۱۳	۱,۰۵۰۲	-۱۵,۱۶۰۰
۱۴	۱,۰۳۵۶	-۱۶,۰۴۰۰

همچنین در این حالت مقادیر اندازه‌گیری شده PMU ها در جدول (۲) نشان داده شده است.

جدول ۲. مقادیر اندازه‌گیری شده PMUها بدون وجود حمله

شماره PMU	مقدار	شماره PMU	مقدار
۱	۱,۰۶۰۰	۱۷	۱,۵۶۸۳
۲	۰	۱۸	۰,۷۳۱۹
۳	-۰,۹۴۲۰	۱۹	-۰,۵۴۴۶
۴	-۰,۴۷۸۰	۲۰	۰,۲۸۰۹
۵	۰	۲۱	-۰,۴۰۶۱
۶	-۰,۰۹۰۰	۲۲	۰,۱۷۷۴
۷	-۰,۰۳۵۰	۲۳	-۰,۷۲۸
۸	-۰,۰۶۱۰	۲۴	۰,۰۱۶۱
۹	-۰,۱۴۹۰	۲۵	-۰,۲۰۳۹
۱۰	۰,۰۴۳۹	۲۶	۰,۰۳۵۷
۱۱	۰,۰۳۹۰	۲۷	۰,۰۳۳۹
۱۲	۰,۱۷۳۶	۲۸	-۰,۰۹۴۲
۱۳	-۰,۰۵۸۰	۲۹	-۰,۰۱۶۳
۱۴	-۰,۰۱۸۰	۳۰	۰,۰۷۱۶
۱۵	-۰,۰۱۶۰	۳۱	-۰,۰۳۳۵
۱۶	-۰,۰۵۰۰	۳۲	۰,۰۰۷۴

همان‌طور که اشاره شد مهاجم باید نسبت به پارامترها و ساختار شبکه مدافع اطلاعات کامل داشته باشد. همچنین ایجاد

تغییر در این پارامترها با توجه به سامانه‌های امنیتی و حفاظتی مدافع پروسه‌ای هزینه‌بر است. پس مهاجم برای ایجاد تغییر در این پارامترها نیاز به‌صرف هزینه دارد. طبیعتاً هرچه میزان هزینه مدافع در جهت به کار بردن لایه‌های دفاعی بیشتر، مقادیر بالاتری باشد، مهاجم برای انجام حمله و نفوذ در شبکه اطلاعاتی مدافع باید هزینه بیشتری مصرف کند. همچنین میزان تغییر در این پارامترها و تعداد پارامترهای تغییریافته با میزان هزینه لازم جهت حمله نسبت مستقیم دارد. در این مقاله فرض بر این است که مهاجم تنها می‌تواند یکی از متغیرهای حالت را تخریب کند. این بدان معنی است که بردار c که در حالت حمله به بردار $\hat{x}$ افزوده می‌شود فقط دارای یک درایه غیر صفر است.

حمله سایبری در نظر گرفته می‌شود که مقدار مربوط به سطر شماره ۱۰ بردار تخمین حالت را به میزان ده درصد افزایش دهد؛ یعنی بردار c در این حمله به شکل $c = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0.1\hat{x}(10)\ 0\ 0\ 0\ 0]$ می‌باشد. مقادیر متغیرهای حالت تخمین زده‌شده پس از انجام این حمله سایبری در جدول (۳) نشان داده شده است. درواقع مقادیر این جدول عناصر بردار $\hat{x}_{bad}$ می‌باشد.

جدول ۳. مقادیر متغیرهای حالت تخمین زده‌شده بعد از حمله سایبری بر روی شین شماره ۱۰

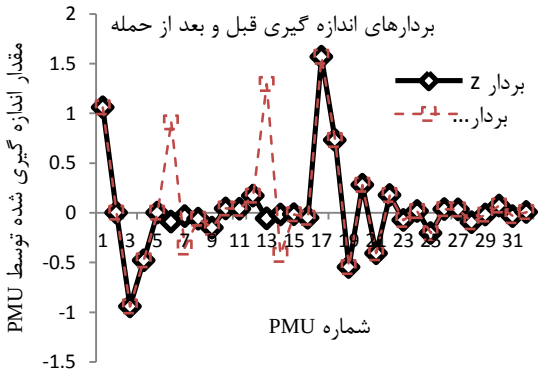
شماره شین	دامنه ولتاژ	اندازه فاز
۱	۱,۰۶۰۰	۰,۰۰۰۰
۲	۱,۰۴۵۰	-۴,۹۸۰۰
۳	۱,۰۱۰۰	-۱۲,۷۲۰۰
۴	۱,۰۱۸۶	-۱۰,۳۲۰۰
۵	۱,۰۲۰۳	-۸,۷۸۰۰
۶	۱,۰۵۶۷	-۱۴,۲۳۰۰
۷	۱,۰۶۱۹	-۱۳,۳۷۰۰
۸	۱,۰۹۰۰	-۱۳,۳۷۰۰
۹	۱,۰۵۶۱	-۱۴,۹۵۰۰
۱۰	۱,۱۳۷۳	-۱۳,۷۸۰۰
۱۱	۱,۰۴۳۶	-۱۴,۸۲۰۰
۱۲	۱,۰۴۱۷	-۱۵,۱۱۰۰
۱۳	۱,۰۳۶۹	-۱۵,۱۹۰۰
۱۴	۱,۰۲۹۷	-۱۶,۰۷۰۰

همچنین بردار اندازه‌گیری که در این حالت به‌دست می‌آید به شکل جدول (۴) است. مقادیر جدول (۴) همان z_{bad} هستند که از روی c و درنتیجه مقدار a به‌دست‌آمده از آن به‌دست‌آمده است. بردار z_{bad} درواقع برداری است که مهاجم باید برای عدم‌تشخیص تغییر متغیر حالت دهم توسط مدافع مقادیر این بردار را تنظیم کند. یعنی بردار اندازه‌گیری z باید توسط مهاجم به z_{bad} تبدیل شود.

جدول ۴. مقادیر اندازه‌گیری شده توسط PMUها بعد از انجام حمله سایبری (این مقادیری است که مهاجم باید برای PMUها تنظیم کند)

شماره PMU	مقدار	شماره PMU	مقدار
۱	۱,۰۶۰۰	۱۷	۱,۵۶۸۳
۲	۰	۱۸	۰,۷۳۱۹
۳	-۰,۹۴۲۰	۱۹	-۰,۵۴۴۶
۴	-۰,۴۷۸۰	۲۰	۰,۲۸۰۹
۵	۰	۲۱	-۰,۴۰۶۱
۶	۰,۹۰۹۱	۲۲	۰,۱۷۷۴
۷	-۰,۳۵۰۶	۲۳	-۰,۷۲۸
۸	-۰,۰۶۱۰	۲۴	۰,۰۱۶۱
۹	-۰,۱۴۹۰	۲۵	-۰,۲۰۳۹
۱۰	۰,۰۴۳۹	۲۶	۰,۰۳۵۷
۱۱	۰,۰۳۹۰	۲۷	۰,۰۳۳۹
۱۲	۰,۱۷۳۶	۲۸	-۰,۰۹۴۲
۱۳	۱,۲۹۴۵	۲۹	-۰,۰۱۶۳
۱۴	-۰,۴۲۳۰	۳۰	۰,۰۷۱۶
۱۵	-۰,۰۱۶۰	۳۱	-۰,۰۳۳۵
۱۶	-۰,۰۵۰۰	۳۲	۰,۰۰۷۴

برای درک بهتر اندازه‌گیرهایی که باید مقادیر آن‌ها تغییر کند این دو بردار در شکل (۳) باهم مقایسه شده‌اند.

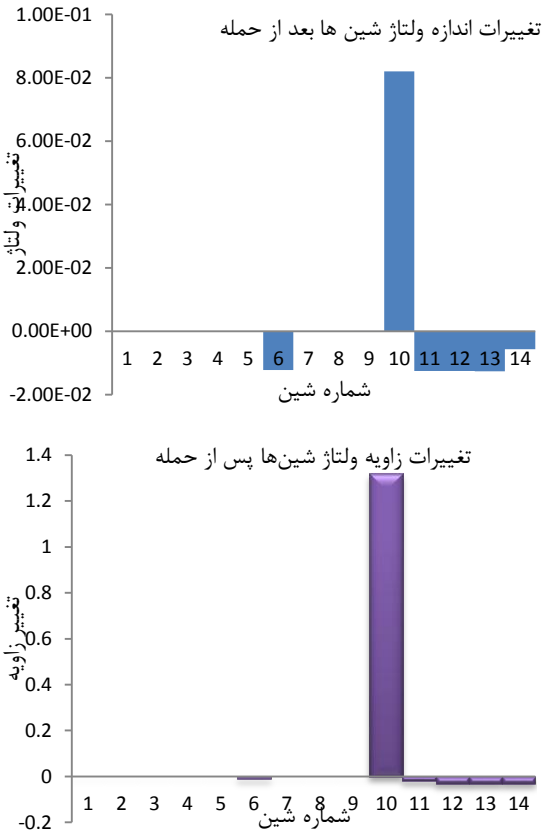


شکل ۳. مقایسه بردار z و z_{bad}

چنانچه مشخص است مهاجم برای انجام حمله اشاره‌شده باید مقدار اندازه‌گیری‌شده توسط ۴ اندازه‌گیر را تخریب کند. درصورتی‌که مهاجم چنین حمله‌ای انجام دهد، در مقادیر متغیرهای حالت تخمین زده‌شده سامانه تغییراتی ایجاد می‌شود. میزان تأثیرگذاری حمله با توجه به میزان انحراف مقادیر متغیرهای حالت تخمین زده‌شده بعد از انجام این تغییرات با مقدار تخمین زده‌شده قبل از حمله آن‌ها مشخص می‌شود.

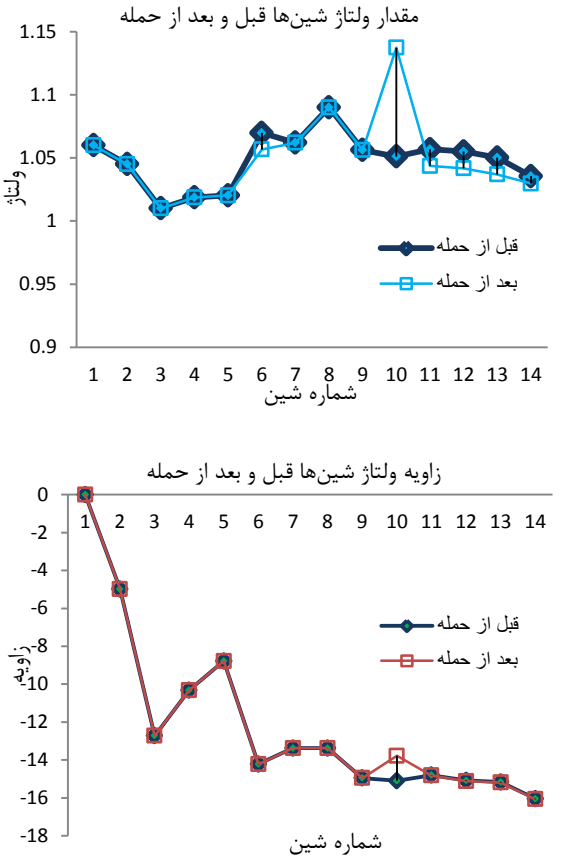
حمله سایبری به شکلی اتفاق می‌افتد که سامانه تشخیص حمله مدافع متوجه اتفاق افتادن این حمله نمی‌شود. میزان تغییرات ولتاژ و زاویه ولتاژ شین‌ها در شکل (۴) نشان داده شده

است. همچنین دیاگرام تغییرات متغیرهای حالت در شکل (۵) نشان داده‌شده است.



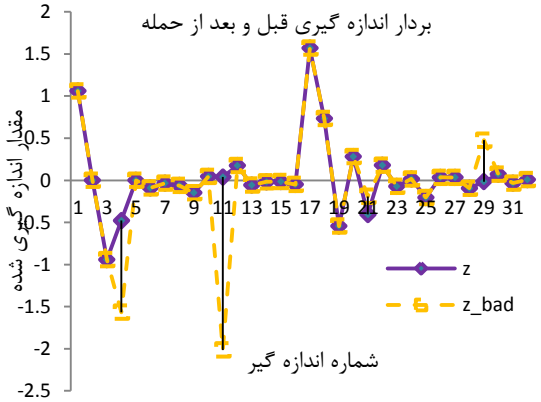
شکل ۴. تغییرات اندازه و زاویه ولتاژ پس از انجام حمله سایبری بر روی شین شماره ۱۰

همان‌گونه که مشخص است علاوه بر شین شماره ۱۰ مقادیر تخمین زده‌شده مربوط به ۵ شین دیگر نیز تخریب‌شده و سامانه مدافع بر اساس این مقادیر برای شبکه تصمیم‌گیری خواهد کرد. با انجام شبیه‌سازی حمله سایبری بر روی همه شین‌های شبکه می‌توان در هر حالت به اطلاعات مشابهی دست‌یافت. با مقایسه این حالت‌ها و استفاده از الگوریتم‌های بهینه‌سازی می‌توان به بهترین شین از دید مهاجم که باید موردحمله قرار گیرد دست‌یافت. قطعاً بهترین حمله از دید مهاجم حمله‌ای است که در آن با تخریب کمترین اندازه‌گیر، بیشترین میزان تغییر در متغیرهای حالت سامانه را ایجاد کند. الگوریتم ارائه‌شده در این مقاله در این زمینه کمک می‌کند که بهترین شین برای حمله را شناسایی کنیم. برای شبکه‌ای با چنین ساختاری حمله به شین شماره ۵ بهترین گزینه برای مهاجم است. اگرچه ازنظر تعداد شین‌هایی که متغیرهای حالتشان تغییر می‌کند و همچنین دامنه تغییرات متغیرهای حالت گزینه‌های بهتری (مثلاً شین شماره ۳) نیز برای حمله وجود دارد اما باید به این نکته توجه شود که با حمله به شین ۵ با تخریب کمترین اندازه‌گیر، بیشترین تغییر قابل‌دست‌یابی خواهد بود.



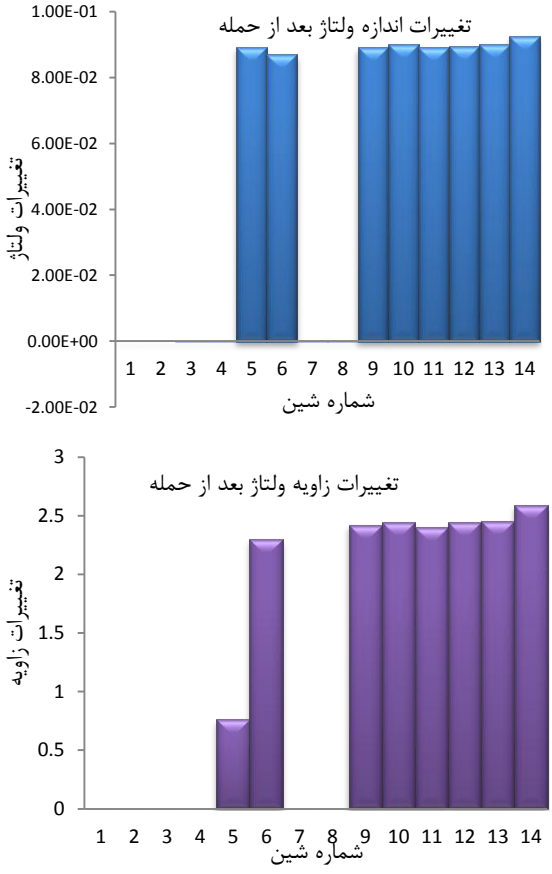
شکل ۵. مقادیر متغیرهای حالت تخمین زده‌شده پیش و پس از انجام حمله سایبری

پس در شرایط یکسان ازنظر میزان تغییر در بردار $\hat{x}$، میزان تخریب شبکه با حمله به شین ۵ چشمگیرتر از حمله به شین شماره ۱۰ می‌باشد.



شکل ۶. اندازه‌گیرهایی که باید توسط مهاجم جهت حمله به شین ۵ تخریب شوند و میزان تغییر آن‌ها

نتایج حمله بر روی شین شماره ۵ در شکل‌های (۶) و (۷) نشان داده‌شده است. شکل (۶) اندازه‌گیرهایی که باید تخریب شوند را نشان می‌دهد. همان‌طور که مشخص است در این حالت نیز مقادیر اندازه‌گیری شده توسط ۴ اندازه‌گیر باید تخریب شوند؛ اما با این تغییر مقادیر متغیرهای حالت تخمین زده‌شده ۸ شین دچار تغییر چشمگیر می‌گردد. این تغییر می‌تواند سامانه‌های کنترلی و حفاظتی شبکه مدافع را به‌طورکلی دچار اختلال و اشتباه کند به‌نحوی‌که پایداری و ثبات شبکه به‌طورکلی از بین برود. در [۱۶] حمله سایبری در دو سناریو مورد بررسی قرار گرفته است. در سناریو اول حمله سایبری مد نظر قرار گرفته که با انجام آن بیشترین هزینه اقتصادی به شبکه مدافع وارد می‌شود. در سناریو دوم، هدف انجام حمله سایبری با بیشترین آسیب به امنیت شبکه و بزرگ‌ترین انحرافات در پخش بار است. در نهایت خطوط انتقالی که انجام حمله بر روی آنها بیشترین آسیب را از این دو منظر به شبکه وارد می‌کنند شناسایی می‌شوند. مشابه مقاله حاضر، نتایج به‌دست‌آمده نشان می‌دهد که بیشترین آسیب زمانی به شبکه مدافع وارد می‌شود که حمله سایبری بیشترین تخریب را در تخمین حالت بیشترین متغیرهای حالت شبکه ایجاد کند.



شکل ۷. تفاوت مقادیر متغیرهای حالت تخمین زده‌شده قبل و بعد از حمله بر روی شین شماره ۵

همان‌طور که مشخص است با توجه به الگوریتم ارائه‌شده بهترین شین جهت انجام حمله شین شماره ۵ بود که بیشترین تغییر را در متغیرهای حالت با کمترین تخریب اندازه‌گیر ایجاد می‌کند.

۴. نتیجه‌گیری

برای ایجاد اختلال در یک شبکه قدرت به‌جای انجام حمله فیزیکی می‌توان از حملات سایبری استفاده کرد. بدین منظور می‌توان از حملات از نوع تزریق داده غلط به شبکه مدنظر استفاده کرد. حمله از نوع تزریق اطلاعات غلط می‌تواند موجب تخمین حالت نادرست و درنتیجه تصمیم‌گیری‌های غلط در شبکه گردد. در این مقاله بر روی حمله سایبری بر روی شبکه قدرت بدون قابلیت تشخیص مدافع بحث شد؛ یعنی حمله از نوع تزریق داده غلطی که سامانه تشخیص حمله مدافع متوجه آن نمی‌شود. درنتیجه در این مقاله منافع مهاجم مدنظر قرارگرفته است. پس از بررسی روش تزریق داده غلط و تغییر متغیرهای حالت سامانه، شبیه‌سازی‌هایی بر روی یک شبکه نمونه صورت گرفت و نتایج این شبیه‌سازی‌ها با تغییر نقطه حمله موردبررسی قرار گرفت. به شکلی که بهترین نقطه برای انجام حمله سایبری بر روی شبکه مدافع مشخص شد. برای تشخیص بهترین نقطه حمله الگوریتمی ارائه شد که این الگوریتم با واردکردن اطلاعات شبکه موردحمله، بهترین شین را جهت حمله معرفی می‌کند. یکی از مواردی که در راستای این مقاله می‌تواند موردبررسی قرار گیرد بحث روش‌های تشخیص حمله و دفاع در برابر حملات سایبری است. درواقع به‌جای در نظر گرفتن منافع حمله‌کننده می‌توان منافع مدافع را در جهت آسیب کمتر در برابر حملات سایبری در نظر گرفت. به‌عنوان‌مثال ازنظر مدافع می‌توان با تغییر مکان قرارگیری اندازه‌گیرهایی که مقادیر اندازه گرفته‌شده توسط آن‌ها مطمئن هستند، می‌توان به بهترین مکان برای قرارگیری آن‌ها در جهت کاهش اثرات حملات سایبری دست‌یافت. با توجه به الگوریتم ارائه‌شده، برای شبکه ۱۴ شین موردبررسی در این مقاله بهترین شین برای انجام حمله شین شماره ۵ است. اگرچه که به‌عنوان‌مثال با تخریب متغیرهای حالت شین شماره ۳ میزان کلی تغییر در متغیرهای حالت تخمین زده‌شده بیشتر است، اما در این حالت تعداد اندازه‌گیرهایی که مقدار آن‌ها باید تغییر کند بیشتر است و درنتیجه انجام حمله هزینه بیشتری خواهد داشت. درنتیجه با استفاده از الگوریتم ارائه‌شده با انجام یک حمله از نوع تزریق داده غلط به‌صورتی که قابلیت تشخیص برای مدافع ندارد می‌توان تأثیرگذارترین حمله به شبکه مدافع را ایجاد کرد.

۵. مرجع‌ها

[1] Wang, Y.; Amin, M. M.; Fu, J.; Moussa, H. B. “A Novel Data Analytical Approach for False Data Injection Cyber-Physical Attack Mitigation in Smart Grids”; IEEE Access 2017, 5, 26022-26033.

[2] He, Y.; Mendis, G. J.; Wei, J. “Real-Time Detection of False Data Injection Attacks in Smart Grid: a Deep Learning-Based Intelligent Mechanism”; IEEE Trans. Smart Grid 2017, 8, 2505-2516.

[3] Asgari, A.; Firouzjah, K. G. “Optimal PMU Placement for Power System Observability Considering Network Expansion and$N-1$ Contingencies”; IET Gener. Transm. Distrib. 2018, 12, 4216-4224.

[4] Lu, C.; Wang, Z.; Ma, M.; Shen, R.; Yu, Y. “An Optimal PMU Placement with Reliable Zero Injection Observation”; IEEE Access 2018, 6, 54417-54426.

[5] Guan, Y.; Ge, X. “Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks”; IEEE Trans. Signal Inf. Process. Networks 2018, 4, 48-59.

[6] Deng, R.; Xiao, G.; Lu, R. “Defending Against False Data Injection Attacks on Power System State Estimation,” IEEE Trans. Ind. Inf. 2017, 13, 198-207.

[7] Deng, R.; Xiao, G.; Lu, R.; Liang, H.; Vasilakos, A. V. “False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: a Survey”; IEEE Trans. Ind. Inf. 2017, 13, 411-423.

[8] Monticelli, A. “State Estimation in Electric Power Systems a Generalized Approach”; Kluwer Academic Publishers, 1999.

[9] Huang, Y.; Tang, J.; Cheng, Y.; Li, H.; Campbell, K. A. “Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis”; IEEE Syst. J. 2016, 10, 532-543.

[10] Gaffarpour, R.; Jam, A.; Ranjbar, A. M. “Optimal Mix of Distributed Generation Allocation to Improve the Security of Energy Supply in Defensive Sites Using Principles of Passive Defence”; Advanced Defence Sci. & Tech. 2015, 7, 19-32. (In Persian).

[11] Bi, S.; Zhang, Y. J. “Graphical Methods for Defense against False-Data Injection Attacks on Power System State Estimation”; IEEE Trans. Smart Grid 2014, 5, 1216-1227.

[12] Zamani Gargari, M.; Ghaffarpour, R. “Increasing Energy Security by Using the Concept of Resiliency in Multi-Energy Infrastructures”; Advanced Defence Sci. & Tech. 2019, 10, 419-432.

[13] He, Y.; Mendis, G. J.; Wei, J. “Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism”; IEEE Trans. Smart Grid 2017, 8, 2505-2516.

[14] Mohammadpourfard, M.; Sami, A.; Weng, Y. “Identification of False Data Injection Attacks With Considering the Impact of Wind Generation and Topology Reconfigurations”; IEEE Trans. Sustainable Energy 2018, 9, 1349-1364.

[15] Taher, S. A.; Mahmoodi, H.; Aghaamouei, H. “Optimal PMU Location in Power Systems Using MICA”; Alex. Eng. J. 2016, 55, 399-406.

[16] Liang, G.; Weller, S. R.; Zhao, J.; Luo, F.; Dong, Z. Y. “A Framework for Cyber-Topology Attacks: Line-Switching and New Attack Scenarios”; IEEE Trans. Smart Grid 2017, 10, 1704-1712.