

## ارائه الگوریتمی جهت شناسایی آسیب پذیرترین شین در شبکه هوشمند برق در حمله سایبری مبتنی بر تخمین حالت

امیرحسین طیبی<sup>۱</sup>، رضا شریفی<sup>۲\*</sup>، امیرحسین سالمی<sup>۳</sup>، فرامرز فقیهی<sup>۴</sup>

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 آسیب پذیرترین شین عملیاتی با استفاده از فن تخمین حالت طی الگوریتم جدیدی تحلیل و شبیه‌سازی شده است. برای این منظور تزریق داده غلط به اطلاعات ارسالی از PMU به گونه‌ای که قابل تشخیص برای بهره‌بردار شبکه تحت تهاجم نباشد صورت می‌پذیرد. به‌عنوان یک مطالعه موردی پیاده‌سازی الگوریتم پیشنهادی برای یک شبکه ۱۴ شین IEEE انجام شده است و بهترین شین از نظر قرارگیری تحت تهاجم شناسایی شده است. عملکرد این الگوریتم مبنی بر نتایج حاصل از تخمین حالت شبکه پس از رخداد حمله سایبری بر روی شین‌های مختلف است. در نهایت 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.

## ۱. مقدمه

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 مورد حمله 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 تبدیل شده است. حملات سایبری که به‌خوبی برنامه‌ریزی شده 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 مورد بررسی و تحلیل قرار گرفته‌اند. در [۱-۲] 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 ارائه شده 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 [۳-۴] به بررسی مسئله جایابی بهینه PMUها پرداخته شده است. این جایابی بهینه با در نظر گرفتن شرایط اضطراری در شبکه انجام شده و در نهایت بهترین حالت قرارگیری PMUها 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 قرار گرفته، راه‌کاری ارائه شده که در این شرایط وضعیت ادوات سایبری- فیزیکی سامانه به‌درستی تخمین زده شود.

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 (Phasor measurement units) PMU و اندازه‌گیرهای هوشمند از جمله زیرساخت‌های مهم این شبکه‌ها برای رسیدن به اهدافشان به حساب 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. در واقع سامانه‌های سایبر- فیزیکی نسل جدیدی از سامانه‌ها هستند که منابع محاسباتی، وسایل ارتباطی عملیات فیزیکی را شامل می‌شوند. از جمله کاربردهایی که این سامانه‌ها دارند تخمین حالت سامانه با استفاده از اطلاعات به‌دست‌آمده از این سامانه‌ها است. تخمین حالت در واقع 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 با وجود 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 در نتیجه ایجاد اختلال 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 در نتیجه 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 به‌طور کلی از بین ببرند. در گذشته 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

شین‌ها، توان اکتیو و راکتیو جاری بین خطوط و ولتاژ و زاویه ولتاژ شین اصلی می‌شود. اطلاعات این اندازه‌گیری‌ها در تخمین حالت سامانه مورد استفاده قرار می‌گیرند. اطلاعات اندازه‌گیری که از این RTUها به دست 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 به درستی 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. در واقع این نوع اطلاعات به شکلی هماهنگ شده به سامانه تزریق می‌شوند که سامانه تشخیص خطا را دور می‌زند. 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 پرداخته شده است.

## ۲-۱. تخمین حالت DC

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

$$z = Hx + e \quad (1)$$

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. در نتیجه تعداد متغیرهای حالت  $n$  متغیر در نظر گرفته شده است.  $H$  یک ماتریس ژاکوبی  $m \times n$  است که تابع خطی اندازه‌گیری نام دارد.  $H$  بر اساس ساختار شبکه به دست 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 اندازه‌گیری‌ها برای تخمین حالت کافی باشد، شبکه قدرت یک شبکه رؤیت پذیر است. الگوریتم‌های متفاوتی برای جابجایی اندازه‌گیری‌ها وجود دارد که شبکه را رؤیت‌پذیر کند [۸]. اصولاً تعداد اندازه‌گیری‌هایی که در شبکه وجود دارد بیش از آن

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 پرداخته شده است. از جمله مسائل مهمی که در این مقاله مورد بررسی قرار گرفته این است که کدام‌یک از اندازه‌گیری‌ها محافظت شوند تا سامانه آسیب کمتری ببیند. همچنین مسئله تأثیر انتخاب PMU محافظت‌شده بر روی بودجه دفاعی سامانه مورد بررسی قرار گرفته. به این معنی که کدام‌یک از PMUها محافظت شود تا بودجه دفاعی افزایش کمتری داشته باشد.

در این مقاله بر روی ساختار حملات سایبری غیرقابل تشخیص بحث شده است. در نتیجه حمله‌ای که در اینجا مورد بررسی قرار گرفته 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 مطرح شده 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 PMUها و در نتیجه حالت‌های تخمین زده شده 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 اندازه‌گیری‌های سامانه تخریب شود تا بیشترین تأثیر مخرب را بر روی شبکه مدافع بگذارد. در این مقاله الگوریتمی ارائه شده که با استفاده از آن می‌توان بهترین ناحیه برای دستیابی به بیشترین آسیب را مشخص نمود. شبیه‌سازی‌هایی انجام شده تا تأثیر این حملات در شرایط مختلف حمله مورد بررسی 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

قبل از انجام حمله یکسان است. پس با این روش حمله ای 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 اندازه گیری ها و حالت سامانه وجود دارد. این تابع به شکل (۵) است.

$$z = h(x) + e \quad (5)$$

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

اگر حمله کننده بخواهد هم زمان چند متغیر حالت را تغییر دهد، نیاز به تخریب تعداد بیشتری کنتور هست. مثلاً اگر حمله کننده بخواهد مجموعه  $K$  متغیر حالت را تغییر دهد، توان اکتیو و راکتیو تزریقی به این شین ها و توان اکتیو و راکتیو بین این شین ها و شین های اطرافشان باید تخریب شود. به همین خاطر حمله به بیش از یک متغیر حالت از نظر اقتصادی به صرفه نیست، خصوصاً اگر این متغیرها مربوط به دو شینی باشد که فاصله آن ها از هم زیاد است. در نتیجه اگر تصمیم بر حمله به بیش از یک متغیر باشد تا حد امکان شین هایی انتخاب می شود که به هم نزدیک باشند [۱۲].

در انجام یک حمله غیرقابل تشخیص دو چیز باید مشخص شود. در مرحله اول باید مشخص شود که کدام یک از اندازه گیری ها باید تخریب شود و در مرحله دوم مقادیر این تغییرات مشخص می شوند. در تخمین حالت AC همه اندازه گیری هایی که با شین تخریب شده در ارتباط هستند، باید تخریب شوند. در حالت DC ماتریس  $H$  ماتریسی بود که نشان می داد کدام اندازه گیری با کدام متغیر حالت در ارتباط است. در تخمین حالت AC همان طور که

تعدادی است که برای رؤیت پذیر شدن شبکه مورد نیاز است (اغلب  $m > n$ ). در تخمین حالت DC فرض می شود که دامنه ولتاژ شین ها برابر ۱ است. همچنین ادمیتانس های موازی و مقاومت خطوط قابل صرف نظر هستند. توان اکتیو جاری بین دو شین از رابطه  $P_{ij} = \frac{\theta_i - \theta_j}{X_{ij}}$  قابل محاسبه است که در آن  $X_{ij}$  راکتانس شاخه بین  $i$  و  $j$  و همچنین  $\theta_i$  و  $\theta_j$  زاویه فاز شین های  $i$  و  $j$  هستند.

$\hat{x}$  که همان حالت تخمین زده شده سامانه است به روش DC از کمینه کردن تابع معادله (۲) به دست می آید.

$$F(x) = (z - Hx)^T R^{-1} (z - Hx) \quad (2)$$

بردار  $\hat{x}$  که تابع بالا را حداقل می کند از رابطه (۳) به دست می آید [۹].

$$\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z \quad (3)$$

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

از جمله روش هایی که می توان برای تشخیص حمله استفاده کرد این است که مقدار باقیمانده  $r = z - H\hat{x}$  را به دست آورد. برای تشخیص اینکه حمله ای اتفاق افتاده یا خیر می توان این مقدار باقیمانده را با یک مقدار مشخصی که از قبل با توجه به شرایط مختلف مشخص شده مقایسه کرد. این روش به روش تشخیص داده بد مرسوم است. اگر از دید حمله کننده نگاه شود، باید حمله به شکلی اتفاق بیفتد که توسط این روش قابل تشخیص نباشد. برای انجام چنین حمله ای باید اولاً ساختار شبکه مدافع برای حمله کننده شناخته شده و دقیقاً مشخص باشد (حمله کننده از  $H$  اطلاعات داشته باشد) و ثانیاً مهاجم قابلیت این را داشته باشد که به طور هم زمان چند اندازه گیر را تخریب کند [۱۰]. اگر مهاجم بتواند بردار اندازه گیری را به شکل  $z_b = z + a$  تغییر دهد، در صورتی می شود سامانه تشخیص مدافع را از کار انداخت که  $a = Hc$  باشد. در این رابطه  $a$  داده مخربی است که به اندازه گیری ها اضافه شده و  $c$  خطای تزریق شده به حالت سامانه است. همان طور که مشاهده می شود مقدار بردار اندازه گیری در این حالت تغییر کرده است اما بعد از اعمال شدن این داده مخرب، حالت سامانه ای که توسط روش تخمین DC تخمین زده می شود به شکل  $\hat{x}_{bad} = \hat{x} + c$  تغییر می کند. با استفاده از این بردار تخمین حالت مقدار باقیمانده که روش تشخیص حمله از آن استفاده می کند به شکل رابطه (۴) به دست می آید [۱۱].

$$r_{bad} = z_{bad} - H\hat{x}_{bad} = z + a - H(\hat{x} + c) = z - H\hat{x} = r \quad (4)$$

همان طور که مشاهده می شود رابطه به دست آمده برای مقدار باقیمانده با توجه به بردار تخمین حالت پس از حمله با مقدار آن

ولتاژی که به توان جاری مدنظر منجر می‌شود چقدر است.

$$P_{ij} = V_{i,a}^2 \cdot g_{ij} - V_{i,a} V_j \cdot g_{ij} \cos(\theta_i - \theta_j) - V_{i,a} V_j \cdot b_{ij} \sin(\theta_i - \theta_j) \quad (11)$$

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  $\theta_j - \theta_i$  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  $\theta_i$  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 هم‌زاویه 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].

$$\|z_{bad} - h(\hat{x}_{bad})\| = \|z + a - h(\hat{x} + c)\| = \left\| \begin{pmatrix} z_1 \\ z_2 + a_2 \end{pmatrix} - \begin{pmatrix} h_1(\hat{x}) \\ h_2(\hat{x}_1, \hat{x}_2 + c) \end{pmatrix} \right\| = \left\| \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} - \begin{pmatrix} h_1(\hat{x}) \\ h_2(\hat{x}_1, \hat{x}_2) \end{pmatrix} \right\| = \|z - h(\hat{x})\| < \tau \quad (12)$$

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 قرار گرفته 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.

$$a_2 = h_2(\hat{x}_1, \hat{x}_2 + c) - h_2(\hat{x}_1, \hat{x}_2) \quad (13)$$

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].

$$J_h = \begin{bmatrix} dh_1/dx_1 & dh_1/dx_2 & \dots & dh_1/dx_n \\ \vdots & \vdots & \ddots & \vdots \\ dh_m/dx_1 & dh_m/dx_2 & \dots & dh_m/dx_n \end{bmatrix} \quad (6)$$

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.

$$P_{ij} = V_i^2 \cdot g_{ij} - V_i V_j g_{ij} \cos(\theta_i - \theta_j) - V_i V_j b_{ij} \sin(\theta_i - \theta_j) \quad (7)$$

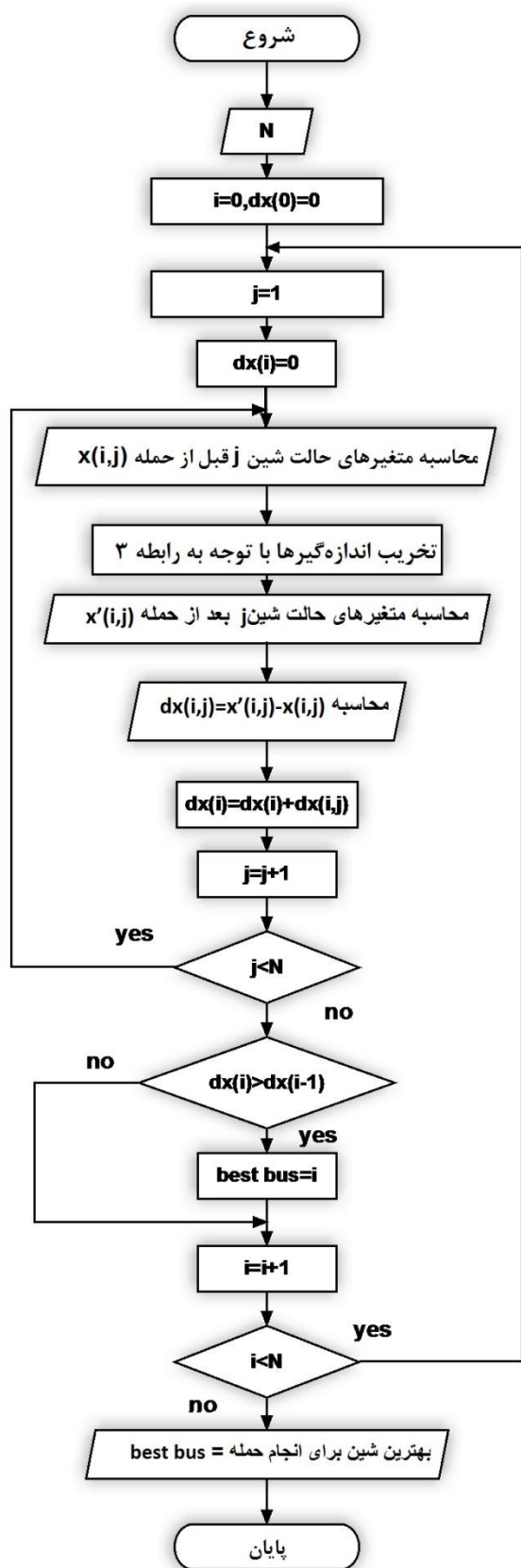
$$Q_{ij} = -V_i^2 \cdot (b_{ij} + b_{ij}^s) + V_i V_j b_{ij} \cos(\theta_i - \theta_j) - V_i V_j g_{ij} \sin(\theta_i - \theta_j) \quad (8)$$

در این روابط  $V_i$  ولتاژ شین  $i$ ام که به‌عنوان شین مبدأ در نظر گرفته‌شده و  $V_j$  ولتاژ شین  $j$ ام که شین مقصد خط انتقال است در نظر گرفته‌شده است. همچنین  $g_{ij}$  و  $b_{ij}$  پارامترهای مربوط به ادمیتانس سری خطوط انتقال و  $b_{ij}^s$  پارامتر مربوط به ادمیتانس موازی خط انتقال می‌باشد.  $\theta_i$  و  $\theta_j$  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.

$$P_i = \sum_{j \in \theta_i} P_{ij} \quad (9)$$

$$Q_i = \sum_{j \in \theta_i} Q_{ij} \quad (10)$$

در این روابط  $\theta_i$  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



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

در نتیجه در حالت AC مهاجم باید مقادیر تخمین زده شده برای مجموعه متغیرهای حالتی که در  $h_2$  وجود دارد را بداند.

#### ۲-۴. ارائه الگوریتم شناسایی آسیب پذیرترین شین

شکل حمله به یک شبکه قدرت می تواند 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 می گیرد. در این بررسی فرض بر این است که هیچ یک از شین های شبکه تحت مطالعه (به جز شین شماره ۱) شین های حفاظت شده نیستند (منظور شین هایی هستند که کنترل گر شبکه مدافع از صحت اطلاعات ارسالی توسط آن ها اطمینان دارد). در نتیجه تزریق داده غلط به منظور تخریب بردار اندازه گیری می تواند بر روی هر یک از شین ها اتفاق افتد. سؤالی که مطرح می شود 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 می تواند از دو دیدگاه در نظر گرفته شود که به هدف مهاجم برمی گردد. در برخی انواع حمله ها هدف مهاجم تعداد متغیر حالت تخریب شده بیشتر نیست و فقط دامنه تغییر یک متغیر حالت مدنظر است؛ یعنی در این حالت مهاجم از بین گزینه های مختلف حمله به شین ها به دنبال آن شینی می گردد که بیشترین تغییر را در یک متغیر حالت ایجاد می کند؛ اما در حالت کلی و از نظر کنترل شبکه بیشترین تخریب زمانی در شبکه مدافع ایجاد می شود که بیشترین تعداد متغیر حالت دچار بیشترین تغییر شود. پس در این مقاله بدین منظور الگوریتمی ارائه شده که از بین شین های مختلف یک شبکه، شینی که حمله به آن باعث بیشترین تغییر کلی در مقادیر متغیرهای حالت شبکه می شود را مشخص می کند. ذکر این نکته نیز مهم است که در این محاسبه نوع حمله به تمامی شین ها یکسان در نظر گرفته می شود. همچنین فرض شده که از نظر محدودیت یا هزینه انجام حمله هیچ تفاوتی بین شین های مختلف شبکه وجود ندارد. اگر میزان هزینه حمله به شین های مختلف شبکه برای ایجاد تغییر یکسان در متغیرهای حالت آن ها 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 داده شده است. تصمیم گیری این الگوریتم بر اساس اطلاعات به دست آمده پس از انجام تخمین حالت در سامانه به دست آمده است. منظور از تخمین حالت در اینجا همان تخمین حالت AC است.

## ۳. نتایج و بحث

متغیرهای حالت این شبکه با استفاده از اطلاعات PMU ها تخمین زده می‌شود در جدول (۱) نشان داده شده است. مقادیر جداول و نتایج همه شبیه‌سازی‌های این مقاله در فضای نرم‌افزار MATLAB انجام شده 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

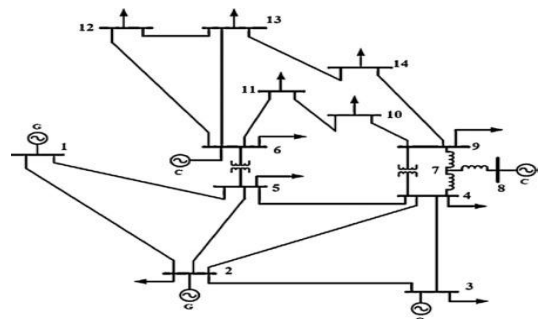
همچنین در این حالت مقادیر اندازه‌گیری شده PMU ها در جدول (۲) نشان داده شده است.

جدول ۲. مقادیر اندازه‌گیری شده PMU ها 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

در این مقاله یک شبکه ۱۴ شین IEEE برای انجام شبیه‌سازی مورد استفاده قرار می‌گیرد. ساختار چنین ریز شبکه‌ای در شکل (۲) نشان داده شده است. اطلاعات فنی مربوط به این ریز شبکه 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)، (۳ و ۴)، (۴ و ۷)، (۵ و ۲)، (۶ و ۱۳)، (۱۱ و ۶) و (۱۲ و ۱۳) قرار گرفته 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.



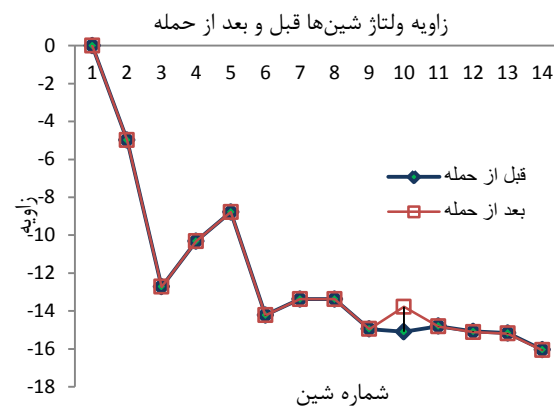
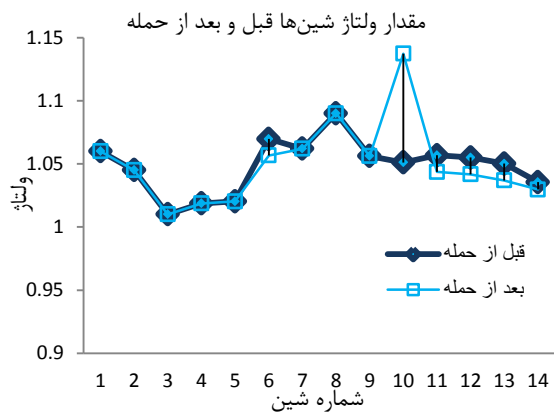
شکل ۲. ساختار ریز شبکه استاندارد ۱۴ شین IEEE [۱۵]

یکی از مسائلی که در بحث حملات سایبری می‌تواند مورد توجه قرار گیرد مکان‌های قرارگیری این اندازه‌گیرها است. در واقع از دید مدافع با تغییر جایگاه این اندازه‌گیرها می‌توان در برابر حملات سایبری احتمالی به تخریب‌های کمتر دست یافت. پس یکی از مباحثی که می‌تواند مورد توجه 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 قرار گرفته شده و انجام یک حمله با حداکثر میزان تخریب در شبکه مدافع مدنظر است، با در نظر گرفتن مکان‌های متفاوت برای تخریب داده اثرات حمله بر روی شین‌های مختلف بررسی شده و بهترین حالت حمله از دید مهاجم به دست می‌آید. در حالت عادی و بدون اتفاق افتادن حمله مقادیری که برای

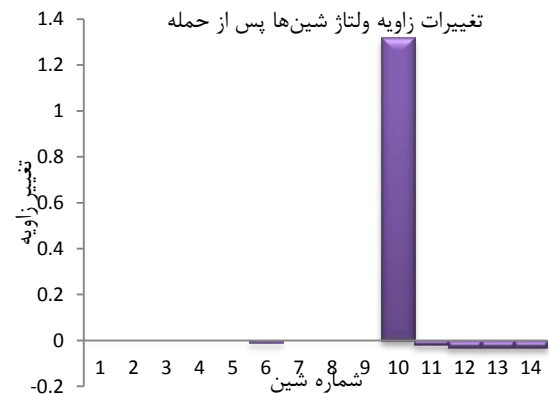
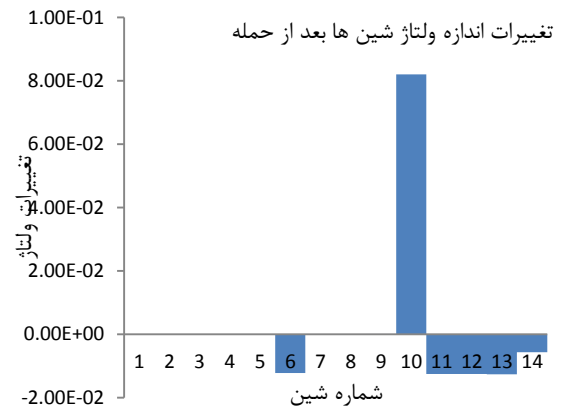




حمله به شین ۵ با تخریب کمترین اندازه‌گیر، بیشترین تغییر قابل‌دستیابی خواهد بود.



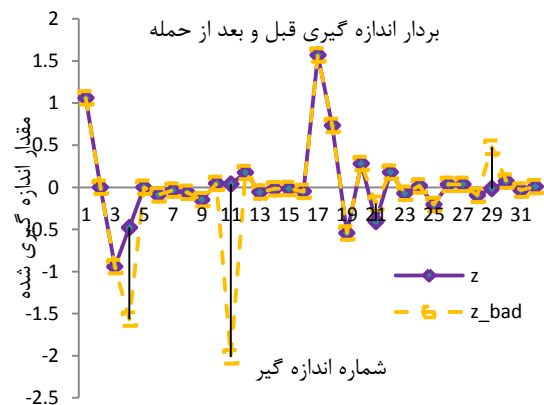
است. همچنین دیاگرام تغییرات متغیرهای حالت در شکل (۵) نشان داده شده است.



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

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

پس در شرایط یکسان از نظر 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

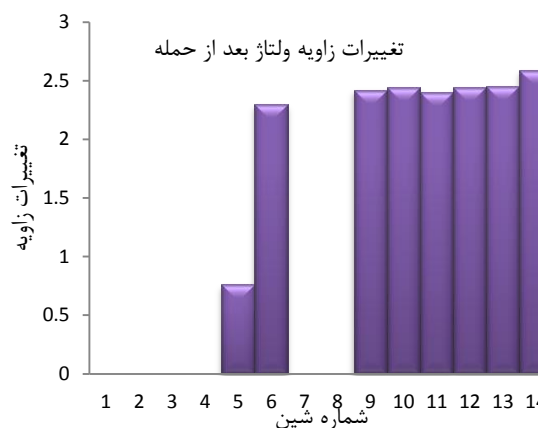
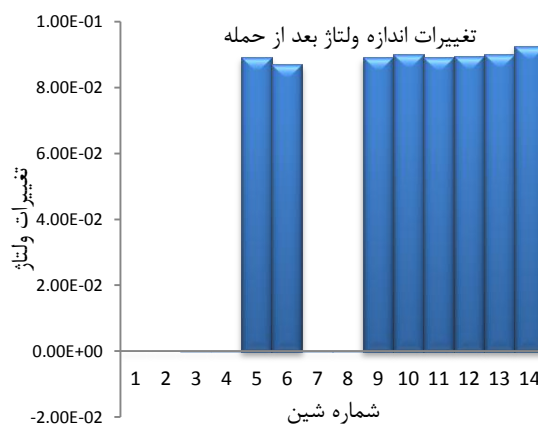
همان‌گونه که مشخص است علاوه بر شین شماره ۱۰ مقادیر تخمین زده شده مربوط به ۵ شین دیگر نیز تخریب شده و سامانه مدافع بر اساس این مقادیر برای شبکه تصمیم‌گیری خواهد کرد. با انجام شبیه‌سازی حمله سایبری بر روی همه شین‌های شبکه می‌توان در هر حالت به اطلاعات مشابهی دست‌یافت. با مقایسه این حالت‌ها و استفاده از الگوریتم‌های بهینه‌سازی می‌توان به بهترین شین از دید مهاجم که باید مورد حمله 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 ارائه شده 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 از نظر 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

همان طور که مشخص است با توجه به الگوریتم ارائه شده بهترین شین جهت انجام حمله شین شماره ۵ بود که بیشترین تغییر را در متغیرهای حالت با کمترین تخریب اندازه گیر ایجاد می کند.

#### ۴. نتیجه گیری

برای ایجاد اختلال در یک شبکه قدرت به جای انجام حمله فیزیکی می توان از حملات سایبری استفاده کرد. بدین منظور می توان از حملات از نوع تزریق داده غلط به شبکه مدنظر استفاده کرد. حمله از نوع تزریق اطلاعات غلط می تواند موجب تخمین حالت نادرست و در نتیجه تصمیم گیری های 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 نمی شود. در نتیجه در این مقاله منافع مهاجم مدنظر قرار گرفته است. پس از بررسی روش تزریق داده غلط و تغییر متغیرهای حالت سامانه، شبیه سازی هایی بر روی یک شبکه نمونه صورت گرفت و نتایج این شبیه سازی ها با تغییر نقطه حمله مورد بررسی 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 وارد کردن اطلاعات شبکه مورد حمله، بهترین شین را جهت حمله معرفی می کند. یکی از مواردی که در راستای این مقاله می تواند مورد بررسی قرار گیرد بحث روش های تشخیص حمله و دفاع در برابر حملات سایبری است. در واقع به جای در نظر گرفتن منافع حمله کننده می توان منافع مدافع را در جهت آسیب کمتر در برابر حملات سایبری در نظر گرفت. به عنوان مثال از نظر مدافع می توان با تغییر مکان قرارگیری اندازه گیری هایی که مقادیر اندازه گرفته شده توسط آن ها مطمئن هستند، می توان به بهترین مکان برای قرارگیری آن ها در جهت کاهش اثرات حملات سایبری دست یافت. با توجه به الگوریتم ارائه شده، برای شبکه ۱۴ شین مورد بررسی در این مقاله بهترین شین برای انجام حمله شین شماره ۵ است. اگرچه که به عنوان مثال با تخریب متغیرهای حالت شین شماره ۳ میزان کلی تغییر در متغیرهای حالت تخمین زده شده بیشتر است، اما در این حالت تعداد اندازه گیری هایی که مقدار آن ها باید تغییر کند بیشتر است و در نتیجه انجام حمله هزینه بیشتری خواهد داشت. در نتیجه با استفاده از الگوریتم ارائه شده با انجام یک حمله از نوع تزریق داده غلط به صورتی که قابلیت تشخیص برای مدافع ندارد می توان تأثیر گذارترین حمله به شبکه مدافع را ایجاد کرد.

نتایج حمله بر روی شین شماره ۵ در شکل های (۶) و (۷) نشان داده شده است. شکل (۶) اندازه گیری هایی که باید تخریب شوند را نشان می دهد. همان طور که مشخص است در این حالت نیز مقادیر اندازه گیری شده توسط ۴ اندازه گیر باید تخریب شوند؛ اما با این تغییر مقادیر متغیرهای حالت تخمین زده شده ۸ شین دچار تغییر چشمگیر می گردد. این تغییر می تواند سامانه های کنترلی و حفاظتی شبکه مدافع را به طور کلی دچار اختلال و اشتباه کند به نحوی که پایداری و ثبات شبکه به طور کلی 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 می شود. در سناریو دوم، هدف انجام حمله سایبری با بیشترین آسیب به امنیت شبکه و بزرگ ترین 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 می کنند شناسایی می شوند. مشابه مقاله حاضر، نتایج به دست آمده نشان می دهد که بیشترین آسیب زمانی به شبکه مدافع وارد می شود که حمله سایبری بیشترین تخریب را در تخمین حالت بیشترین متغیرهای حالت شبکه ایجاد کند.



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

## ۵. مراجع‌ها

- [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.
- [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.