Computational Intelligence in Electrical Engineering
Vol. 14, No. 2, 2023
Research Paper

Bad Data Detection in Electrical Grid's State Estimation due to Cyber Attack on Measurements Using DRGP and GSR algorithms

Samira Amini [1], Rahmat-Allah Hooshmand [2], Mohammad Ataei [3]
[1] Dept. of Electrical Engineering, University of Isfahan, Isfahan, Iran
[2] Dept. of Electrical Engineering, University of Isfahan, Isfahan, Iran
[3] Dept. of Electrical Engineering, University of Isfahan, Isfahan, Iran

Abstract:
Nowadays, using telecommunication systems and advanced measuring devices underlies cyberattacks on electrical grids. Bad data injection and failure to detect it on time, cause drastic damage to the network. This paper presents a new method for bad data detection (BDD) in state estimating when a cyber attacker manipulates the important measurements. Therefore, the new attack index is defined by simultaneously manipulating the network parameters and injecting incorrect data into the measured values. For this purpose, considering the masking and swamping effect, the diagnostic robust generalized potential (DRGP) algorithm detected and isolated high-leverage measurements installed in important locations from low-leverage measurements. Then, the state estimation process performs using low-leverage measurements. The Generalized Studentized Residual (GSR) algorithm detects bad data. With simultaneous manipulation of network parameters and measurement values, conventional BDD methods are unable to detect an attack. To evaluate the performance of the proposed method, they were implemented on the IEEE standard 14-bus network using MATLAB and Rstudio software. The simulation results show the ability of the proposed algorithm to detect a bad data attack.

Keywords: State Estimation, Bad Data Detection, Cyberattack, Bad Data Injection Attack, Smart Grid.

https://doi.org/10.22108/ISEE.2022.132857.1548

مقاله پژوهشی

تشخیص داده بد در تخمین حالت شبکه‌های قدرت در اثر حمله سایبری به اندازه‌گیری‌ها با استفاده از الگوریتم‌های پتانسیل و باقیماندهٔ تعمیم‌یافته

سمیرا امینی[۱]، رحمت الله هوشمند[۲*]، محمد عطایی[۳]

۱- کارشناسی ارشد، گروه برق، دانشکده فنی و مهندسی - دانشگاه اصفهان- اصفهان- ایران
samira.amini@eng.ui.ac.ir

۲- استاد گروه برق، دانشکده فنی و مهندسی - دانشگاه اصفهان- اصفهان- ایران
hooshmand_r@eng.ui.ac.ir

۳- استاد گروه برق، دانشکده فنی و مهندسی - دانشگاه اصفهان- اصفهان- ایران
ataei@eng.ui.ac.ir

چکیده: گسترش استفاده از سیستم‌های مخابراتی و دستگاههای اندازه‌گیری پیشرفته در شبکه‌های قدرت، زمینه‌ساز برقراری حملات سایبری در این شبکه‌ها است. وقوع حمله تزریق داده بد و تشخیص‌ندادن به‌موقع آن، آسیب‌های جبران‌ناپذیری را به شبکه تحمیل می‌کند. در این مقاله، روش جدیدی به‌منظور تشخیص داده بد (BDD) در تخمین حالت، هنگامی که مهاجم سایبری اندازه‌گیری‌های حساس و مهم را اندازه‌گیری می‌کند، ارائه می‌شود. بدین منظور، شاخص جدید حمله با دستکاری‌کردن هم‌زمان پارامترهای شبکه و تزریق داده‌های اشتباه به مقادیر اندازه‌گیری‌شده تعریف می‌شود. در این صورت، ابتدا دستگاههای اندازه‌گیری با اهمیت و نفوذ بالا که در مکان‌های حساس نصب شده‌اند، از دستگاههای اندازه‌گیری با اهمیت و نفوذ پایین با وجود اثر masking و swaming با استفاده از الگوریتم پتانسیل تعمیم‌یافته و مطمئن (DRGP) تشخیص و جداسازی می‌شوند. بعد از این دسته‌بندی، مجدد[۵] فرآیند تخمین حالت با استفاده از اندازه‌گیری‌های با نفوذ پایین انجام می‌شود. اندازه‌گیری‌های حاوی داده بد با استفاده از الگوریتم باقیمانده تعمیم‌یافته (GSR) تشخیص داده می‌شوند. با دستکاری‌کردن هم‌زمان پارامترهای شبکه و مقادیر اندازه‌گیری‌ها، روش‌های معمول BDD قادر به تشخیص حمله نیستند. به‌منظور بررسی کارایی الگوریتم‌های تشخیص داده بد بیان‌شده، پیاده‌سازی آنها روی شبکه استاندارد ۱۴ و ۱۲۳ باسه IEEE با استفاده از نرم‌افزارهای MATLAB و Rstudio انجام شده است. نتایج، شبیه‌سازی توانایی الگوریتم پیشنهادی را در تشخیص حمله داده بد به‌خوبی نشان می‌دهند.

واژه‌های کلیدی: تخمین حالت، تشخیص داده بد، حمله سایبری، حمله تزریق داده بد، شبکه هوشمند.

۱- مقدمه

با گسترش و توسعه فناوری اطلاعات و ارتباطات در شبکه‌های برق، به بحث امنیتی و سایبری شبکه‌های هوشمند بسیار توجه شده است. شبکه‌های قدرت هوشمند با سیستم‌های سایبری پشتیبانی می‌شوند. در این راستا، استفاده از تکنولوژی ارتباطات و اطلاعات که به‌منظور افزایش کارایی، کیفیت و قابلیت اطمینان در پروسه‌های صنعتی، شبکه‌های قدرت و شبکه‌های واحد اندازه‌گیری فازور (PMU[۱]) به کار می‌رود، تهدیدات ناخواسته‌ای را متوجه این شبکه‌ها کرده است. این خطرات شامل حملات سایبری به‌منظور ایجاد وقفه در تولید، انتقال و توزیع برق یا

[۱] تاریخ ارسال مقاله: ۱۴۰۰/۱۲/۰۵
تاریخ پذیرش مقاله: ۱۴۰۱/۰۴/۱۲
نام نویسندهٔ مسئول: رحمت الله هوشمند
نشانی نویسندهٔ مسئول: ایران، اصفهان - دانشگاه اصفهان- دانشکده فنی و مهندسی - گروه برق

همچنین، دستکاری داده‌های ارسالی در شبکه است. در بدترین حالت، وقوع این حملات به فروپاشی و خاموشی سراسری منجر خواهد شد [۱].

یکی از انواع حملات سایبری، حمله تزریق داده بد[۲](BDI) است. در این نوع حمله با دستکاری‌کردن اندازه‌گیری‌ها و تزریق داده‌های غلط به پارامترهای شبکه در حین ارسال به مرکز کنترل، مسائل تخمین حالت[۳] و بهره‌برداری ایمن از شبکه با مشکل مواجه می‌شود. در جریان حمله، تلاش مهاجم مبنی بر حداکثرسازی خسارت با کمترین هزینه است. بنابراین، لایه‌های مختلف امنیت سایبری باید به نحوی طراحی شود که تهدیدهای این حملات را به حداقل برساند. همچنین لازم است از رویکردهای مبتنی بر تشخیص حمله، به‌منظور تشخیص داده بد[٤](BDD) در اندازه‌گیری‌ها استفاده شود.

گام نخست در راستای تحلیل امنیت، مشاهده و نظارت بر حالت فعلی شبکه است که شامل دستیابی به اندازه‌گیری‌ها از تمامی قسمت‌ها و تحلیل آنها به‌منظور تخمین حالت‌های شبکه است [۲]. به‌منظور اطلاع از وضعیت شبکه، لازم است کمیت‌های اندازه‌گیری‌شده با سنسورها یا واحد اندازه‌گیری فازور ازطریق بسترهای مخابراتی و اینترنتی به مرکز کنترل ارسال شود. سپس با استفاده از اندازه‌گیری‌های دریافت‌شده و بررسی رؤیت‌پذیری شبکه، حالت‌های شبکه تخمین زده می‌شود. داده‌ها و اندازه‌گیری‌ها ممکن است با مهاجم دستکاری شوند و اطلاعات جعلی به دست بهره‌بردار شبکه برسد. در صورت عدم تشخیص داده‌های اشتباه، برنامه‌های تخمین حالت، پخش بار، برنامه‌ریزی تولید، پیش‌بینی بار و اقدامات کنترلی شبکه به‌شدت تحت تأثیر قرار خواهند گرفت [۳]. در مقالات مختلف، برای حفاظت شبکه در مقابل حملات سایبری به دو اقدام عملیاتی مختلف اشاره شده است. نخستین روش بر مبنای اقدامات حفاظتی است که تمامی ادوات اندازه‌گیری موجود هر کدام به‌صورت مجزا حفاظت شوند. دومین روش بر مبنای تشخیص حملات با استفاده از الگوریتم‌های مختلف است. در این اقدام با تجزیه‌وتحلیل اندازه‌گیری‌های، موارد غیر معمول شناسایی می‌شوند. در مرجع [٤] به بیان BDD به‌صورت بلادرنگ براساس دینامیک تغییرات اندازه‌گیری با تحت تأثیر قرار گرفتن یک متغیر حالت، پرداخته شده است. در مرجع [٥] از آشکارساز متوالی براساس نسبت احتمال کلی به‌منظور تشخیص سریع BDD استفاده شده است. در مرجع [٦] به بیان استراتژی‌های حمله BDI در ناحیه‌های محلی با فرض دسترسی مهاجم سایبری به اطلاعات و توپولوژی بخش‌های محلی شبکه پرداخته شده است. از میان روش‌های BDD که بر مبنای مقایسهٔ مقدار باقیمانده اندازه‌گیری (تفاضل بین اندازه‌گیری مشاهده‌شده و تخمین زده شده) با مقدار آستانه از پیش تعریف شده است، می‌توان به آزمون کای – مربع [۷]، آزمون باقیمانده نرمالیزه‌شده [۸، ۹]، شاخص فاصله مطلق(AD[٥]) [۱۰] و شاخص KLD[٦] [٤] اشاره کرد.

ضعف عمدهٔ روش‌های سنتی تشخیص مبتنی بر تحلیل باقیمانده این است که براساس اندازه‌گیری‌های وابسته به هم است. در صورتی که چندین اندازه‌گیری با مهاجم دستکاری شوند، ممکن است به تولید مقدار باقیمانده نسبتاً بزرگ برای اندازه‌گیری‌هایی منجر شود که حتی آلوده به خطا نیستند [۱۱]. در مرجع [۱۲]، برای رفع این مشکل از تخمین مستقیم خطای اندازه‌گیری‌ها با بهره‌گیری از آزمون فرضیه استفاده شده است. عملکرد درست این روش در گروی محاسبات آماری پیچیده است [۷]. در مرجع [۱۱] از مدل پخش توان AC در روش تشخیص BDI با بهره‌گیری از ساختار گراف شبکه استفاده شده است. روش بیان‌شده در این مرجع قادر به تشخیص حملات BDI است که با استفاده از مدل‌های خطی‌سازی شده DC قابل تشخیص نبوده‌اند. در مرجع [۱۳] به بیان حملات سایبری به یکپارچگی و دسترس‌پذیری داده‌ها در تخمین حالت شبکه پرداخته شده است. همچنین، حملات یکپارچگی با حملات BDI مقایسه شده‌اند. در مرجع [۱٤] به بیان نحوه بهینه‌سازی تعداد اندازه‌گیری‌هایی پرداخته‌اند که باید برای تأثیر بر تعداد متغیرهای حالت داده شده دستکاری شوند.

در این مقاله، به‌منظور بررسی صحت و درستی داده‌های دریافتی در مرکز کنترل و تشخیص نفوذ داده بد به کمیت‌های اندازه‌گیری‌شده، از روش DRGP[۷] -GSR استفاده شده است. به این منظور، استراتژی‌های جدید حمله، تعریف و از راههای متنوعی داده‌های جعلی به

کمیت‌های اندازه‌گیری تزریق شده‌اند. همچنین، به سبب حفظ امنیت کامل شبکه و تأثیر حمله در متغیرهای اندازه ولتاژ و زاویه بأس، در روش ارائه‌شده از تخمین حالت AC با دقت بالا استفاده شده است. با توجه به اینکه اساس روش‌های تشخیص بر مبنای مقایسه مقدار باقیمانده با مقدار آستانه از پیش تعریف شده است، تلاش مهاجم بر دستکاری‌کردن اندازه‌گیری‌های متناظر با نقاط با نفوذ بالا (HLP[۸]) است؛ زیرا مقدار باقیمانده متناظر با این اندازه‌گیری‌ها کوچک است؛ بنابراین، با استفاده هم‌زمان از دو الگوریتم DRGP-GSR، همه انواع اندازه‌گیری‌های آلوده به خطا شناسایی می‌شوند. نتایج شبیه‌سازی، کارایی و توانایی الگوریتم‌های ارائه‌شده در مقابله سایر روش‌های تشخیص و انواع شاخص‌های حمله را نشان می‌دهند.

بخش‌های دیگر مقاله به شرح زیر سازماندهی شده‌اند. در بخش دوم، به بیان مدلسازی حمله و تأثیر آن در تخمین حالت شبکه پرداخته می‌شود. در بخش سوم، نقاط آسیب‌پذیر شبکه و مهم از دید مهاجم بیان می‌شود. در بخش چهارم، روش پیشنهادی برای تشخیص داده بد توضیح داده می‌شود. در بخش پنجم، نتایج شبیه‌سازی الگوریتم‌های ارائه‌شده روی شبکه نمونه بررسی می‌شوند.

۲- مدل‌سازی حمله BDI در تخمین حالت

برای بررسی شرایط بهره‌برداری سیستم، برآورد حالت‌های شبکه با استفاده از فرآیند تخمین حالت در مرکز کنترل انجام می‌شود. در حملات سایبری، مهاجم سعی دارد به نقاطی حمله کند که بیشترین آسیب را به شبکه وارد کند؛ به گونه‌ای که از سیستم‌های تشخیص داده بد عبور کند؛ بنابراین، مهاجم با دستکاری‌کردن پارامترهای متناظر با اندازه‌گیری‌ها سعی در ایجاد نقاطی با نفوذ بالا دارد که احتمال تشخیص خطا در آنها پایین است. برای حفظ امنیت شبکه و شناسایی اینگونه حملات، وجود سیستم‌های تشخیص دادهٔ بد قوی الزامی است. در صورتی که خطاها متعلق به اندازه‌گیری‌های حساس و نقاط نفوذ (LP[۹]) نباشند، حذف آنها به‌منظور تخمین دقیق مشکلی ایجاد نمی‌کند؛ با این حال، اگر داده بد به اندازه‌گیری‌های موجود در مجموعه نفوذ متعلق باشد، به مدیریت دقیقی نیاز خواهد داشت.

اطلاعات ورودی به تخمین‌گر حالت شامل سه دسته است [۳]:

۱- اطلاعات دستگاههای اندازه‌گیری که شامل توان‌های تزریقی به باس‌ها و توان انتقالی در خطوط است؛ این اطلاعات با z نمایش داده می‌شوند.

۲- اطلاعات مربوط به توپولوژی شبکه که شامل وضعیت سوئیچ‌ها و بریکرها است و با t نمایش داده می‌شود.

۳- اطلاعات مربوط به پارامترها که شامل امپدانس خطوط و واریانس خطا مربوط به اندازه‌گیری‌ها است و با p نشان داده می‌شود.

به‌منظور مدلسازی جامع و بررسی دقیق شبکه با هدف دستکاری‌کردن مقادیر اندازه‌گیری‌های توسط مهاجم، از مدل تخمین حالت AC استفاده می‌شود [۱۰]. ارتباط غیرخطی بین بردار اندازه‌گیری و بردار حالت به‌صورت رابطه زیر بیان می‌شود [۱۵]:

$$z = h(x) + e \qquad (۱)$$

که h یک تابع غیر خطی بین بردار اندازه‌گیری z و بردار حالت x است و e بردار نویز اندازه‌گیری‌ها با توزیع نرمال و میانگین صفر است. بردار حالت x شامل اندازه و فاز ولتاژ باس‌ها است. ماتریس ژاکوبین با ابعاد نشان داده می‌شود (m و n به‌ترتیب بیان‌کنندهٔ تعداد اندازه‌گیری‌ها و تعداد متغیرهای حالت است). برای تخمین حالت‌های شبکه، باید تعداد اندازه‌گیری‌ها از تعداد متغیرهای حالت بیشتر باشد. مهاجم با تزریق بردار حمله a به بردار اندازه‌گیری‌های z، باعث تغییر در مقادیر اندازه‌گیری‌شده می‌شود.

$$z_{bad} = z + a \qquad (۲)$$

که بردار اندازه‌گیری دستکاری شده است. مقدار خطای c به بردار متغیرهای حالت بر اثر دستکاری‌کردن کمیت‌های اندازه‌گیری‌شده اضافه می‌شود. در صورت عدم تشخیص دادهٔ غلط تزریق‌شده به اندازه‌گیری‌ها، اقدامات اپراتور

براساس بردار حالت اشتباه است. در مراجع [۱۶] و [۱۷] به بیان استراتژی‌های مختلف حمله پرداخته شده است.

رایج‌ترین روش تخمین حالت‌های شبکه، استفاده از الگوریتم تکراری حداقل مربعات وزندار (WLS[۱۰]) است و تابع هدف آن به‌صورت رابطه زیر بیان می‌شود:

$$\min J(x) = [z - h(x)]^T R^{-1} [z - h(x)] \qquad (۳)$$

که R و به‌ترتیب بیان‌کنندهٔ ماتریس کوواریانس خطای اندازه‌گیری (I ماتریس یکه است) و ماتریس قطری ضرایب وزنی هستند. روابط مربوط به محاسبه توان‌های اکتیو و راکتیو در [۱۸] آمده‌اند. متغیرهای حالت تخمین زده شده با شامل نشان داده و به‌صورت رابطه زیر محاسبه می‌شود:

$$\hat{x} = (H^T R^{-1} H)^T H^T R^{-1} z \qquad (٤)$$

با استفاده از حالت‌های تخمینی، بردار اندازه‌گیری‌های تخمین زده شده با نمایش داده و به‌صورت زیر تعریف می‌شود:

$$\hat{z} = H (H^T R^{-1} H)^{-1} H^T R^{-1} z = Kz \qquad (۵)$$

که K ماتریس نفوذ بالا نامیده می‌شود. مقادیر قطری بزرگ این ماتریس، متناظر با اندازه‌گیری‌هایی است که نفوذ و اهمیت زیادی دارند و تأثیر بیشتری روی حالت‌های تخمین زده شده دارند [۱۹].

اساس روش‌های BDD بر مبنای تحلیل مقدار باقیمانده است و به‌صورت زیر بیان می‌شود:

$$r_{bad} = z_{bad} - \hat{z}_{bad} = z + a - h(\hat{x} + c) \qquad (٦)$$

به‌منظور تشخیص وجود داده بد، مقدار باقیمانده با مقدار آستانه از پیش تعیین شده مطابق با تجربیات مقایسه می‌شود. در صورتی که مقدار باقیمانده از مقدار آستانه تجاوز کند، بیان‌کنندهٔ وجود داده بد تزریق‌شده به پارامترهای شبکه است [۱۲].

۳- نقاط نفوذ مؤثر برای حمله

مطابق با مدل حمله بیان‌شده در بخش قبلی، مهاجم تلاش می‌کند نقاطی از سیستم را دستکاری و به آن حمله کند که احتمال تشخیص آن برای اپراتور سیستم، ضعیف باشد؛ بنابراین، حمله کننده باید در هر سیستمی، نقاط با قابلیت نفوذ بالا را مشخص کند تا حمله موثری صورت دهد.

بر اساس این، در فرآیند تخمین حالت در ماتریس ژاکوبین H، هر سطر از این ماتریس با نشان داده می‌شود که در فضای n بُعدی قرار دارد و به آن، فضای ضرایب گفته می‌شود. درواقع هر نقطه ، یک نقطه (n+1) بُعدی در فضای ضرایب تعریف می‌کند که با سطرهای ماتریس H رسم شده‌اند. اگر ای، فاصله زیادی از سایر سطرهای ماتریس H داشته باشد، به آن نقطه، نقطه نفوذ (LP) گفته می‌شود و اندازه‌گیری متناظر با آن سطر، اندازه‌گیری نفوذ نامیده می‌شود. در صورتی که مقدار فاصله از سایر سطرهای ماتریس H خیلی بیشتر باشد، نقطه مذکور، نقطه‌ای با نفوذ بالا(HLP[۱۱]) و در صورتی که این میزان فاصله خیلی کمتر باشد، نقطه مذکور، نقطه‌ای با نفوذ پایین (LLP[۱۲]) نامیده می‌شود. اندازه‌گیری‌های متناظر با این نقاط به ترتیب اندازه‌گیری با نفوذ بالا (HLM[۱۳]) و اندازه‌گیری با نفوذ پایین[۱٤](LLM) گفته می‌شوند [۱۹]، [۳]. مقدار نفوذ، میزان فاصله هر سطر از ماتریس H را نسبت به سایر سطرهای ماتریس H می‌سنجد. ویژگی خاص این اندازه‌گیری‌ها، این است که باقیمانده متناظر با آنها حتی در صورتی که به مقدار خطای زیادی آلوده باشند، بسیار کوچک است [۲۰]؛ بنابراین، مهاجم تلاش می‌کند نقاطی را دستکاری کند که احتمال تشخیص آن ضعیف باشد. به عبارت دیگر، مطلوب است تا به نقاط HLMها حمله کند.

با توجه به اینکه مقدار باقیمانده متناظر با این اندازه‌گیری‌ها کوچک است و اساس تشخیص داده‌های بد نیز بر مبنای باقیمانده‌ها است، باعث گمراه‌شدن اپراتور در مرکز کنترل می‌شود. بر این مبنا، روش‌های تشخیص مبتنی بر باقیمانده به‌تنهایی قادر به تشخیص و شناسایی LPهای آلوده به خطا نیستند و باید از روش‌های قوی برای تشخیص داده بد در این اندازه‌گیری‌ها استفاده کرد [۲۰]. عوامل زیر به شکل‌گیری LP منجر می‌شوند [۳]:

۱- اندازه‌گیری‌های توان تزریقی روی باس‌هایی قرار گرفته باشند که شاخه‌های بیشتری در مقایسه با سایر باس‌ها به آن وصل باشند. به عبارت دیگر، مؤلفه‌های غیر صفر بیشتری در سطرهای ماتریس ژاکوبین H وجود داشته باشد.

۲- اندازه‌گیری‌های توان تزریقی روی باس‌هایی قرار گرفته باشند که شاخه‌های متصل به آن، دارای امپدانس بسیار متفاوت نسبت به سایر شاخه‌ها باشند.

۳- اندازه‌گیری‌های توان انتقالی روی شاخه‌ای قرار گرفته باشند که امپدانس آن نسبت به سایر شاخه‌ها خیلی متفاوت باشد.

٤- وزن اختصاص داده شده به یک اندازه‌گیری نسبتاً بزرگ باشد.

در تجزیه‌وتحلیل ماتریس H، همیشه یک یا چند اندازه‌گیری وجود دارند که بر حل نهایی، بیشتر از اندازه‌گیری‌های دیگر تأثیر می‌گذارند. نقاطی که مقدار متغیر پاسخ آنها (یعنی مقدار اندازه‌گیری تخمین زده شده) دور از بقیه نقاط قرار گرفته باشد، نقاط خارج از خط[۱۵] (یعنی اندازه‌گیری که حاوی داده بد است) نامیده می‌شوند [۲۰]. نقطه LPای که اندازه‌گیری یا سطر متناظر با آن در ماتریس H، آلوده به خطا باشد، نقطه نفوذ بد و نقطه LPای که عاری از خطا باشد، نقطه نفوذ خوب نامیده می‌شود [۱۹]. در مراجع [۲۱, ۲۲] به بیان روش‌هایی ازجمله مؤلفه‌های قطری ماتریس نفوذ بالا (K)، فاصله مهلانوبیس اندازه‌گیری‌ها و پردازش تصویری به‌منظور شناسایی LP پرداخته شده است. اگرچه در مقالات متعدد به بیان روش‌هایی برای شناسایی نقاط نفوذ پرداخته‌اند، به تأثیر وجود دو پدیده masking و swamping اشاره‌ای نشده است.

۳-۱- پدیده masking و swamping

زمانی که مجموعه اندازه‌گیری‌ها شامل بیش از یک نقطه HLP باشند، حذف یک یا چند اندازه‌گیری از مجموعه باعث می‌شود اندازه‌گیری‌های دیگری با نفوذ بالا ظاهر شوند؛ در حالی که این اندازه‌گیری‌ها از همان ابتدا مشخص نبود نفوذ بالایی دارند. درواقع، HLPها LLP در نظر گرفته شده‌اند. به این اثر پوشش یا masking گفته می‌شود. در اندازه‌گیری‌هایی که بیش از یک اندازه‌گیری HLM وجود داشته باشد، ممکن است بعضی از LLMها به‌صورت اشتباه، HLM در نظر گرفته شوند؛ به این اثر swamping گفته می‌شود [۲۳].

٤- روش تشخیص نقاط با نفوذ بالا در حمله

در تجزیه‌وتحلیل مدل تخمین حالت، لازم است مجموعه مقادیر ماتریس H تعیین شوند که تأثیر زیادی بر برازش مدل دارند. در مجموعه اندازه‌گیری‌ها با وجود HLP به دلیل وجود دو پدیده masking و swamping، در صورتی که نقاط به‌درستی تشخیص داده نشوند، به نتایج اشتباه در برازش مدل تخمین حالت منجر خواهند شد؛ بنابراین، می‌باید قبل از اجرای هر گونه اقدامی، مکان HLMها تشخیص داده شود و تأثیر آن بر مدل ارزیابی شود. مؤلفه‌های قطری ماتریس K و مقدار باقیمانده متناظر با اندازه‌گیری‌ها، شواهد موردنیاز برای ردیابی اندازه‌گیری‌های مهم را فراهم می‌کنند؛ اما استفاده از هر کدام از آنها به‌تنهایی مؤثر نخواهد بود. بدین سبب، بهتر است از ترکیب آنها استفاده شود. با توجه به اینکه تا کنون تأثیر این دو پدیده در مدل‌سازی تخمین حالت در نظر گرفته نشده است، سبب ایجاد انگیزه به‌منظور بررسی آن در این مقاله آمده است.

٤-۱- الگوریتم پتانسیل تعمیم‌یافته و مطمئن (DRGP)

زمانی که مجموعه اندازه‌گیری‌ها شامل بیش از یک نقطه HLP باشند، حذف یک یا چند اندازه‌گیری از مجموعه باعث می‌شود اندازه‌گیری‌های دیگری به اشتباه با نفوذ بالا ظاهر شوند. عکس این قضیه نیز برقرار است. در این مقاله به‌منظور جلوگیری از تشخیص اشتباه اندازه‌گیری‌ها از یک رویکرد قوی و تشخیصی استفاده می‌شود. ابتدا با استفاده از رویکرد قوی، نقاط با نفوذ بالا شناسایی و حدس زده می‌شوند و رویکرد تشخیصی حدس فوق را تأیید می‌کند. شناسایی LP براساس فاصله هر نقطه از مرکز نقاطی است که توده ابر مانند تشکیل داده‌اند. محاسبهٔ مقدار فاصله براساس مطالعات آماری است که بتوان مرکز و ماتریس کوواریانس توده ابرمانند را محاسبه کرد. به این منظور از

شاخص فاصله قوی مهلانوبیس[۱۶] (RMD) (به‌منظور شناسایی HLPها استفاده می‌شود. شاخص RMD با رابطه زیر تعریف می‌شود [۲۴]:

$$RMD_i = \sqrt{[H_i - \bar{H}][C(H)]^{-1}[H_i - \bar{H}]^T} \qquad (۷)$$

که H_i بیان‌کنندهٔ iامین سطر از ماتریس H، $\bar{H}$ بیان‌کنندهٔ مرکز بیضی با حداقل حجم (MVE[۱۷]) است که L نقطه از تعداد m نقطه را می‌پوشاند و $C(H)$ ماتریس کوواریانس است. محاسبه $\bar{H}$ و $C(H)$ با روش‌های معمول میانگین حسابی و ماتریس کوواریانس دقیق نیست و قادر به تشخیص HLPهای واقعی نیستند؛ بنابراین، می‌باید از روش MVE استفاده کرد. به‌منظور مطالعه دقیق روش MVE به مقاله [۲۵] مراجعه شود. پس از محاسبه مقدار بردار مرکز و ماتریس کوواریانس بیضی با حداقل حجم، مقدار RMD برای تمام اندازه‌گیری‌های موجود محاسبه می‌شود. مقدار *cut-off* برای مقایسه مقادیر RMD اندازه‌گیری‌ها طبق رابطه زیر تعریف می‌شود:

$$cut-off = Median(RMD_i) + cMAD(RMD_i) \qquad (۸)$$

که *Median* مقدار میانه است و مقدار ثابت c برابر با ۲ یا ۳ در نظر گرفته می‌شود. مقدار انحراف مطلق میانه (MAD[۱۸]) مطابقه با رابطه زیر محاسبه می‌شود.

$$MAD(x) = Median\left|\frac{x - Median(x)}{0.6745}\right| \qquad (۹)$$

با محاسبه مقدار RMD، آن دسته از اندازه‌گیری‌هایی که مقدار RMD متناظر با آنها از مقدار *cut-off* بیشتر باشد، در دسته‌ای به اسم D قرار خواهند گرفت و از مجموعه اصلی حذف خواهند شد. اندازه‌گیری‌های باقیمانده در دسته R قرار می‌گیرند. در مرحلهٔ بعد لازم است مقدار پتانسیل تعمیم‌یافته (*pot*) برای هر دو دسته اندازه‌گیری‌ها محاسبه شود. در صورتی که اندازه‌گیری که به اشتباه به‌عنوان اندازه‌گیری HLP شناخته‌شده از دسته D حذف می‌شود و به دسته R اضافه می‌شود، مجدد، فرآیند تخمین حالت با اندازه‌گیری‌های موجود در دسته R اجرا می‌شود. این روند تا زمانی ادامه دارد که همه اندازه‌گیری‌های دسته D، اندازه‌گیری‌هایی با اهمیت بالا باشند. مقدار پتانسیل تعمیم‌یافته برای مجموعه اندازه‌گیری‌های قرارگرفته در هر دو دسته D و R طبق رابطه زیر محاسبه می‌شود [۱۹]:

$$pot^*_{ii} = \begin{cases} \dfrac{K_{ii}^{-(D)}}{1 - K_{ii}^{-(D)}} & \forall i \in R \\ K_{ii}^{-(D)} & \forall i \in D \end{cases} \qquad (۱۰)$$

که pot^*_{ii} بیان‌کنندهٔ مقدار پتانسیل تعمیم‌یافته و مطمئن است. مقدار *cut-off* برای مقایسهٔ مقدار پتانسیل تعمیم‌یافته از رابطه زیر محاسبه می‌شود:

$$cut-off = Median(pot^*_{ii}) + cMAD(pot^*_{ii}) \qquad (۱۱)$$

مقدار ثابت c در این معادله برابر با ۳ در نظر گرفته شده است. با محاسبه مقدار *pot* برای هر دو دسته از اندازه‌گیری‌ها، لازم است مقدار پتانسیل متناظر با اندازه‌گیری‌های دسته D با مقدار *cut-off* رابطه (۱۱) مقایسه شود. در صورتی که همه اندازه‌گیری‌های موجود در دسته D مقدار *pot* متناظرشان از مقدار *cut-off* بزرگ‌تر باشد، HLPها تعیین می‌شوند؛ در غیر این صورت، باید آن اندازه‌گیری که کمترین مقدار پتانسیل را دارد، به دسته R منتقل شود و مجدداً مقدار *pot* برای هر دو دسته جدید D و R محاسبه شود. این فرآیند تا زمانی ادامه می‌یابد که همه اندازه‌گیری‌های دسته D، مقدار *pot* بزرگ‌تری از مقدار *cut-off* داشته باشند. مراحل اجرای الگوریتم DRGP به شرح زیر است:

۱- مقدار RMD براساس تخمین‌گر MVE محاسبه می‌شود.

۲- با مقایسه مقادیر RMD اندازه‌گیری‌ها با مقدار *cut-off* رابطه (۸)، اندازه‌گیری‌ها در دو گروه D و R دسته‌بندی می‌شوند.

۳- مقدار *pot* برای اندازه‌گیری‌های هر دو دسته D و R محاسبه و با مقدار *cut-off* رابطه (۱۱) مقایسه می‌شود. عمل مقایسه و انتقال اندازه‌گیری دسته D که به‌اشتباه به‌عنوان HLP شناسایی شده باشد، به دسته R تا زمانی که

همهٔ اندازه‌گیری‌های موجود در دسته D مقدار *pot* بزرگ‌تری از مقدار *cut-off* داشته باشند، ادامه خواهد داشت.

٤-۲- شناسایی داده بد

اندازه‌گیری‌های موجود در شبکه می‌تواند به‌آسانی با اهداف مختلف توسط مهاجم سایبری دستکاری شوند. همان‌طور که بیان شد مقدار باقیمانده در HLMها تقریباً نزدیک به صفر است و بسیاری از تخمین‌گرها ازجمله تخمین‌گر LAV قادر به تشخیص داده بد در HLMها نیستند. سایر تخمین‌گرها ازجمله LMS، LTS و RLS محاسبات بسیار پیچیده‌ای دارند؛ بنابراین، پس از شناسایی و دسته‌بندی HLM و LLMها لازم است وجود دادهٔ بد در اندازه‌گیری‌ها بررسی و تشخیص داده شود. با توجه به اینکه باقیمانده‌ها تابعی از مقدار نفوذ هستند، باید شناسایی HLPها و تشخیص داده بد در LPها با هم ترکیب شود و به‌صورت هم‌زمان اتفاق بیفتد؛ در غیر این صورت، به نتایج اشتباه منجر خواهد شد. برای تشخیص داده بد در کمیت‌های اندازه‌گیری‌شده از روش باقیمانده تعمیم‌یافته (GSR[19]) استفاده می‌شود. در این صورت وجود داده‌های غلط تزریق‌شده در دو دسته D و R به‌طور مجزا تشخیص داده و به‌صورت زیر محاسبه می‌شود:

$$r^{*}_{st,i}=\begin{cases}\dfrac{r_i^{-(D)}}{\hat{\sigma}_{R-i}\sqrt{1-K_{ii}^{-(D)}}} & \forall i\in R\\[2ex] \dfrac{r_i^{-(D)}}{\hat{\sigma}_{R}\sqrt{1+K_{ii}^{-(D)}}} & \forall i\in D\end{cases} \qquad (۱۲)$$

که $r_i^{-(D)}$ مقدار باقیمانده اندازه‌گیری iام با استفاده از مجموعه اندازه‌گیری‌های دسته D است. همچنین، $K_{ii}^{-(D)}$ مقدار مؤلفه قطری ماتریس $K^{-(D)}$ و $\hat{\sigma}^2$ تخمین حداقل مربعات واریانس است.

باقیمانده تعمیم‌یافته با مقدار آستانه برابر با ۳ مقایسه می‌شود. پس از آنکه مقدار DRGP و GSR محاسبه شوند، منحنی پتانسیل تعمیم‌یافته و مطمئن _ باقیمانده تعمیم‌یافته (DRGP-GSR) رسم می‌شود. در منحنی DRGP-GSR، اندازه‌گیری‌های HLM در ناحیه بالای منحنی، اندازه‌گیری‌های LLM در ناحیه پایین منحنی، اندازه‌گیری‌های HLM حاوی داده غلط، بسته به علامتشان در ناحیه بالا و در سمت راست یا چپ منحنی و اندازه‌گیری‌های LLM حاوی داده غلط، بسته به علامتشان در ناحیه پایین و در سمت راست یا چپ منحنی قرار می‌گیرند؛ بنابراین، با این روش، نقاط HLP و همچنین، نقاط آلوده به خطا شناسایی می‌شوند.

۵- الگوریتم روش پیشنهادی

براساس مطالب ارائه‌شده در بخش‌های ۲ تا ٤، فلوچارت مدل‌سازی حمله و روش پیشنهادی تشخیص BDI در شکل (۱) نشان داده شده است و مراحل اجرای الگوریتم به شرح زیرند:

گام ۱: در این مرحله برای مدل‌سازی حمله BDI، به تعدادی از اندازه‌گیری‌های موجود در شبکه داده‌هایی تزریق می‌شود.

گام ۲: به‌منظور تخمین متغیرهای حالت شبکه شامل اندازه و فاز ولتاژ باس‌ها از روش تخمین حداقل مربعات وزندار استفاده می‌شود.

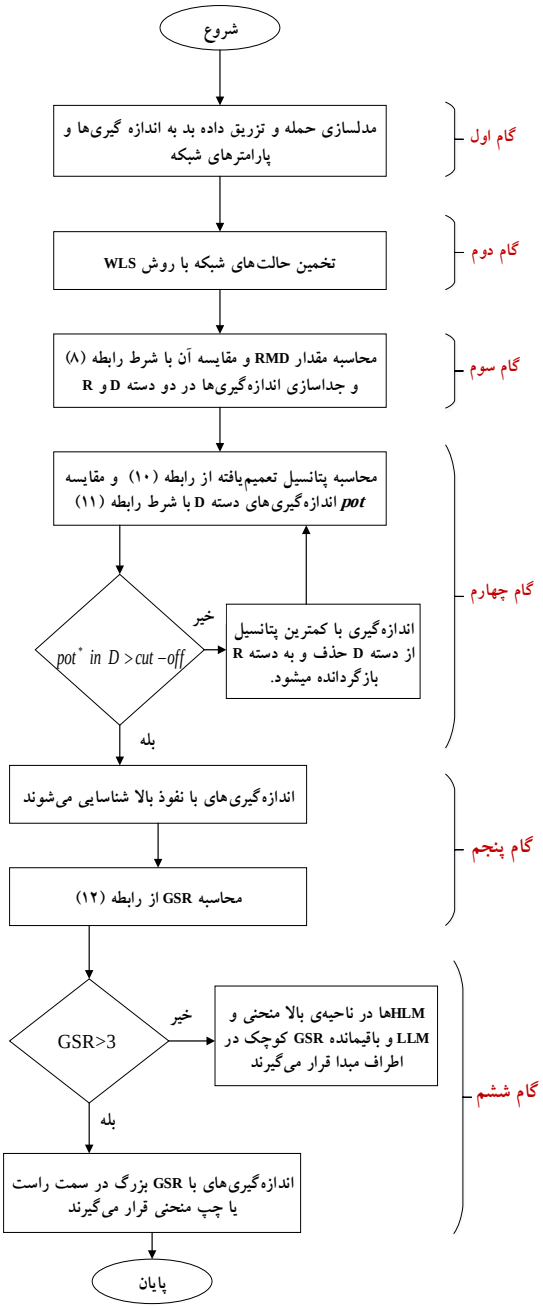
گام ۳: در این مرحله مقدار RMD محاسبه و با مقدار *cut-off* رابطه (۸) مقایسه می‌شود. اندازه‌گیری‌هایی که مقدار RMD آنها از مقدار *cut-off* بزرگ‌تر باشد، در دسته D و سایر اندازه‌گیری‌ها در دسته R قرار می‌گیرند.

گام٤: در این مرحله مقدار *pot* مطابق با رابطه (۱۰) محاسبه می‌شود. سپس مقدار *pot* اندازه‌گیری‌های دسته D با مقدار *cut-off* رابطه (۱۱) مقایسه می‌شود. در صورتی که همهٔ اندازه‌گیری‌های دسته D مقدار *pot* بزرگ‌تری از مقدار *cut-off* داشته باشند، HLMها شناسایی می‌شوند. در غیر این صورت باید اندازه‌گیری با کمترین مقدار پتانسیل از دسته D حذف و به دسته R بازگردانده شود. این فرآیند تا زمانی ادامه می‌یابد که همهٔ اندازه‌گیری‌های دسته D، مقدار *pot* بزرگ‌تر از مقدار *cut-off* داشته باشند.

گام ۵: پس از شناسایی HLPها، مقدار GSR اندازه‌گیری‌ها مطابق با رابطه (۱۲) محاسبه و با عدد ۳ مقایسه می‌شود. اندازه‌گیری‌هایی که مقدار GSR آنها از عدد

۳ بزرگ‌تر باشد، حاوی داده جعلی‌اند و اندازه‌گیری داده بد شناخته می‌شوند.

گام ٦: در مرحله آخر، منحنی DRGP-GSR ترسیم می‌شود. اندازه‌گیری‌های LLM و دارای GSR کوچک در اطراف مبدأ قرار خواهند گرفت. همچنین، HLM در ناحیهٔ بالای منحنی قرار می‌گیرند.



شکل (۱): فلوچارت الگوریتم پیشنهادی

٦- نتایج شبیه‌سازی

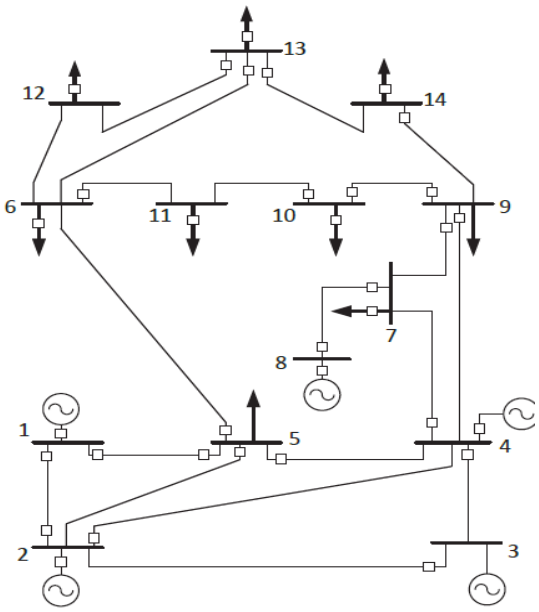
٦-۱- شبکه‌های نمونه

روش تشخیص داده بد پیشنهادشده بر شبکه‌های استاندارد ١٤ و ١٢٣ باسه IEEE پیاده‌سازی شده است. شبیه‌سازی الگوریتم‌های موجود با نرم‌افزارهای MATLAB و RStudio انجام شده است. اطلاعات بار و پارامترهای شبکه ١٤ و ١٢٣ باسه به‌ترتیب در [٢٦]، [٢٧] و [٢٨] موجودند. شماتیک شبکه ١٤ باسه در شکل (٢) نشان داده شده است. مقادیر اندازه‌گیری‌ها با اضافه‌کردن نویز تصادفی نرمال با میانگین صفر و انحراف استاندارد ۰/۰۱ به نتایج پخش بار AC تولید شده‌اند. فرض شده است اطلاعات از ادوات اندازه‌گیری معمولی حاصل شده است. سناریوهای مختلفی برای دستکاری‌کردن اندازه‌گیری‌ها و پارامترهای شبکه برای بررسی کارایی روش پیشنهاد شده تعریف شده‌اند.

٦-۲- سناریو اول: دستکاری همزمان اندازه‌گیری‌ها و پارامترهای شبکه ١٤ باسه IEEE توسط مهاجم

در سناریو اول فرض می‌شود مهاجم به اندازه‌گیری‌های توان اکتیو و راکتیو و همچنین، پارامترهای شبکه دسترسی پیدا می‌کند و داده‌های جعلی به آنها تزریق می‌کند. نفوذ به پارامترهای شبکه (راکتانس خطوط) به طراحی حملهٔ دقیقی نیاز دارد که به صرف هزینه و زمان زیادی منجر می‌شود. پارامترهای اندازه‌گیری‌شده شبکه ١٤ باسه در جدول (١) آورده شده‌اند. درخور ذکر است لازمهٔ پیاده‌سازی روش پیشنهادی بر روی شبکه‌های واقعی، وجود تعداد کافی ادوات اندازه‌گیری برای رؤیت‌پذیری شبکه است. با توجه به آنکه دسترسی مهاجم به داده‌های مرکز کنترل بسیار سخت و شاید بتوان گفت در عمل امکان‌پذیر نیست، برای بررسی توانایی روش پیشنهادی فرض شده است امکان

دسترسی مهاجم به مرکز کنترل فراهم است.



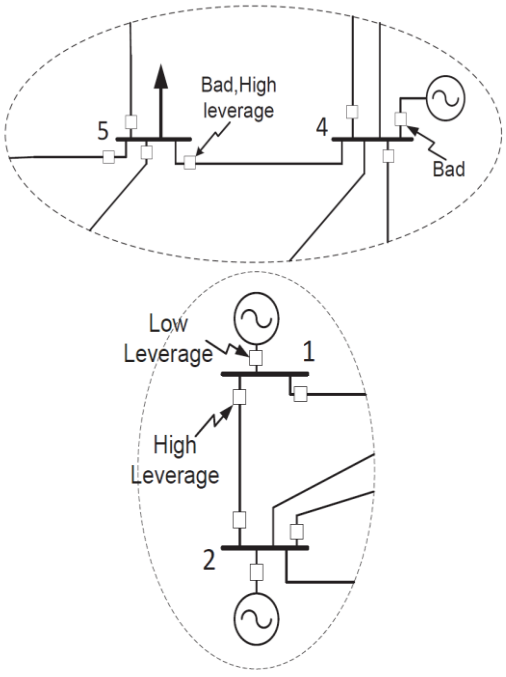
شکل (۲): شماتیک شبکه ۱۴ باسه IEEE

جدول (۱): مقدار اندازه‌گیری‌ها و پارامترهای دستکاری‌شده در شبکه ۱۴ باسه IEEE

مقدار اندازه‌گیری / پارامتر پس از حمله(pu)	مقدار اولیه اندازه‌گیری / پارامترها (pu)	اندازه‌گیری / پارامترهای مورد حمله
۰/۶۶۵۷	۰/۶۱۵۷	P_{5-4}
۳/۱۶۵۳	۲/۳۱۵۳	P_1
-۰/۵۲۲۷	-۰/۴۷۷۲	P_4
۰/۰۴۹۱۷	۰/۰۵۰۱	x_{1-2}
۰/۲۲۲۹۴	۰/۲۲۲۸	x_{1-5}
۰/۲۰۸۱۲	۰/۲۰۷۱	x_{4-7}

تلاش مهاجم برای دستکاری‌کردن اندازه‌گیری‌ها، ایجاد نقاطی با نفوذ بالا و تزریق داده‌های اشتباه به این دسته از اندازگیری‌ها است. به باس چهارم این شبکه، پنج شاخه متصل است که نسبت به سایر باس‌ها تعداد شاخه‌های بیشتری به این باس متصل است. مقدار راکتانس شاخه‌های متصل به باس یک نسبت به راکتانس سایر باس‌ها کمتر است و راکتانس شاخه متصل بین باس چهار و پنج نیز مقدار کوچکی دارد. همچنین، کاهش مقدار راکتانس شاخه‌های مرتبط با این باس‌ها باعث می‌شود اندازه‌گیری‌های مربوط به این باس‌ها و شاخه‌ها به‌عنوان اندازه‌گیری‌های با نفوذ بالا شناسایی شوند؛ بنابراین، با تزریق خطا به چنین اندازه‌گیری‌هایی، تشخیص داده بد در آنها دشوار خواهد بود. شماتیک این نقاط در شکل (۳) نشان داده شده است. در جدول (۱) پارامترها و اندازه‌گیری‌های مورد حمله و میزان خطای تزریقی به آنها آورده شده‌اند.

پس از تزریق خطا به پارامترها و مقادیر اندازه‌گیری‌ها و اجرای فرآیند تخمین حالت‌های شبکه، باید اندازه‌گیری‌های آلوده به خطا شناسایی شوند. در این راستا تلاش بر جداسازی و دسته‌بندی اندازه‌گیری‌های HLM و LLM است. به‌منظور شناسایی HLMها، ابتدا باید مقدار RMD متناظر با هر یک از اندازه‌گیری‌ها محاسبه شود که این نتایج در جدول (۲) آمده‌اند. اندازه‌گیری‌هایی که مقدار RMD بزرگ‌تری از مقدار *cut-off* دارند، به‌عنوان HLM حدس زده می‌شوند و در دسته D قرار خواهند گرفت. با توجه به مقدار RMD فاصله نسبتاً زیاد اندازه‌گیری‌های P_{4-5}، P_4، P_1 و Q_{1-2} نسبت به بقیهٔ اندازه‌گیری‌ها مشهود و نمایان است. چون در روش RMD ممکن است برخی از اندازه‌گیری‌ها که اهمیت چندانی ندارند، به اشتباه به‌عنوان اندازه‌گیری دارای اهمیت بالا شناخته شوند و بالعکس، لازم است با اجرای الگوریتم DRGP از شناسایی نوع اندازه‌گیری‌ها مطمئن شد.



شکل(۳): شماتیک نقاط HLP و LLP شبکه ۱۴ باسه IEEE

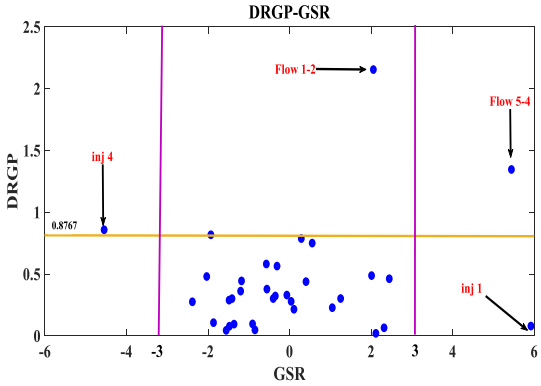
جدول (۲): نتایج شبیه‌سازی در سناریو اول برای شبکه ۱۴ باسه IEEE

ردیف	اندازه‌گیری	مقدار RMD (cut_off=۵/۴۲۴۸	$K_{ii}^{-(D)}$	DRGP (*cut-off*= ۰/۸۷۶۷)	GSR (*cut-off*= ۳/۰)
۱	$P_{۲-۱}$	٤/۲۷٤٥	۰/۰٤٥۸	۰/۰٤۷۹	−۰/۸٤۹٥
۲	$P_{۳-۲}$	٥/۰۱۷٦	۰/۰٦۱۱	۰/۰٦٥۰	۱/۹۸۷۰
۳	$P_{۲-٤}$	۳/۹۱۰۷	۰/۲٤۳۹	۰/۳۲۲٥	−۰,۳٥۰
٤	$P_{۱-٥}$	٥/۷۱۷۱	۰/۰۷۲۰	۰/۰۷۷۷	−۱/٤۷٦۰
٥	$P_{٥-۲}$	٤/۱۰۸۰	۰,۳۲۷٦	۰/٤۸۷۳	۲/٥۸۲
٦	$P_{٥-٤}$	۱٦/۲۰۰	۱/۳٤٥۸	۱/۳٤٥۸	٥/۲۱۲
۷	$P_{٥-٦}$	٥/۲٤۲٦	۰/۳٦۰٦	۰/٥٦٤۲	−۰/٦٥۱
۸	$P_{٤-۷}$	٤/۹٤۰۷	۰/۰۹٦۳	۰/۱۰٦٥	−۱/٤٥۷
۹	$P_{۸-۷}$	۳/٦٤٤۸	۰/۲٦٥۷	۰/۳٦۱۷	−۱/٤۹۱
۱۰	$P_{۹-۷}$	٥/۲۳٦۸	۰/۲۷٤٤	۰/۳۷۸۰	−۰/٦٤٥٥
۱۱	$P_{۹-۱۰}$	٥/۱۳٥۹	۰/۳٦۷۷	۰/٥۸۱۳	−۰/۷٥٦۰
۱۲	$P_{٦-۱۱}$	٥/۲٤۱۲	۰/۳۰۷۷	۰/٤٤٤۳	−۱/٥۰۱۷
۱۳	$P_{۱۳-٦}$	٥/۲٤۲۱	۰/٤۲۸۷	۰/۷٥۰۲	۰/٤۲٥٥
۱٤	$P_{۱۰-۱۱}$	٥/۱٦۷٥	۰/۱۸٥٥	۰/۲۲۷۷	۰/۹٦۷۸
۱٥	$P_{۱۳-۱٤}$	٥/۲۳۰۹	۰/۲۳۱٥	۰/۳۰۱۱	−۱/٥۲٦۳
۱٦	$P_{۱}$	٤/٦۷٦٦	۰/۷۳۹	۰/۰۷۹۲	٥/۷۸٦۱
۱۷	$P_{٤}$	۲۸/۱۰	۰/۸۷۷٦	۰/۸۷۷٦	−۳/۹۳٦۷
۱۸	$P_{۸}$	۳/٦٤٤۸	۰/۰۸۸۰	۰/۰۹٦٦	−۰/٦۸۹۰
۱۹	$P_{۱۰}$	٥/۱٤٥٦	۰,۲۳۱۸	۰/۳۰۱٦	−۰/۱۸٦٤
۲۰	$P_{۱۲}$	٥/۲۰۲۷	۰/۲۱۸۱	۰/۲۷۸۸	۰/۸۲٦٤
۲۱	$P_{۱٤}$	٥/۲٤۰۳	۰/۳۲٤۸	۰/٤۸۱۰	−۲/٥۲۳
۲۲	$Q_{۱-۲}$	۲٥/٥۰۰	۲/۱٥٤۰	۲/۱٥٤۰	۲/۰۰۸
۲۳	$Q_{٥-۱}$	٥/۱۷۱۰	۰/۰٤۲٦	۰/۰٤٤٤	−۱/۸۷۸
۲٤	$Q_{٤-۳}$	٥/۲۳٤۸	۰/۲۱٦۰	۰/۲۷٥٥	−۲/۱۸٥
۲٥	$Q_{۷-۸}$	٥/۲٤۲٦	۰/۳۱٦	۰/٤٦۲۰	۲/٥٥٤۸
۲٦	$Q_{۹-٤}$	٤/٤۸۲۷	۰/۲۳۱۸	۰/۳۰۱۸	۰/۸٥۹۷
۲۷	$Q_{۱۰-۹}$	٤/٦۸٤٥	۰/۲٤۸۰	۰/۳۲۹۸	−۰/۱٦٤۳
۲۸	$Q_{۱٤-۹}$	٥/۲٤۲۷	۰/۳۰٤۸	۰/٤۳۸٥	۰/٦٤۲۰
۲۹	$Q_{۱۳-۱۲}$	٥/۲٤۲۰	۰/۲۲٤۰	۰/۲۸۸۷	−۱,٤۸۳٦
۳۰	$Q_{۲}$	٥/۲٤۰۸	۰/٤٤۹۷	۰/۸۱۷٥	−۱/۳٥٦٤
۳۱	$Q_{٦}$	٥/۲٤۲٦	۰/۰۱۹۸	۰/۰۲۰۱	۲/۱۱٥۳
۳۲	$Q_{۷}$	٥/۲۳۷۸	۰/٤٤۰۳	۰/۷۸٦۸	۰/۱٤٦۲
۳۳	$Q_{۱۱}$	٥/۲٤۲۷	۰/۱۷٦۹	۰/۲۱٥۰	۰/۱۰٤٦
۳٤	$Q_{۱۳}$	٥/۲۳۲٦	۰/۰۸٦٥	۰/۰۹٤۸	−۱/۸٥٤

مقدار مؤلفه‌های قطری ماتریس K و نتایج DRGP مربوط به اندازه‌گیری‌ها در جدول (۲) آورده شده است. مشاهده می‌شود مقدار DRGP مربوط به اندازه‌گیری‌های P_{4-5}، P_4 و Q_{2-1} از مقدار ۰/۸۷۶۶ بزرگ‌تر است و اندازه‌گیری HLM شناخته می‌شوند.

مطابق با نتایج نشان داده شده در جدول (۲)، اندازه‌گیری P_{5-1} دچار اثر swamping و به‌اشتباه، HLM شناخته شده است. همان‌گونه که گفته شد روش RMD ممکن است در تشخص نوع اندازه‌گیری‌ها دچار اشتباه شود؛ بنابراین، با روش RMD نوع اندازه‌گیری‌ها حدس زده می‌شود و با الگوریتم DRGP از حدس زده شده اطمینان حاصل می‌شود. نتایج مقدار GSR محاسبه‌شده در جدول (۲) آورده شده‌اند. نتایج ذکرشده نشان می‌دهند مقدار باقیمانده تعمیم‌یافته سه اندازه‌گیری P_{4-5}، P_1 و P_4 از مقدار ۳ بزرگ‌تر است. نتایج ذکرشده بیان‌کنندهٔ کارایی الگوریتم DRGP در شناسایی LPها است؛ در حالی که مقدار نفوذ (مؤلفه‌های قطری ماتریس K) قادر به شناسایی صحیح LPها نیست. همچنین، الگوریتم GSR به‌خوبی اندازه‌گیری‌های دستکاری‌شده را تشخیص می‌دهد.

با رسم نمودار نقطه‌ای DRGP-GSR در شکل (٤) مشاهده می‌شود اندازه‌گیری‌های با نفوذ بالا (HLM) شامل P_{4-5}، P_4 و Q_{2-1} در ناحیهٔ بالای منحنی و اندازه‌گیری‌های با نفوذ پایین (LLM) در ناحیهٔ پایین منحنی قرار گرفته‌اند. اندازه‌گیری‌ها با نفوذ بالا و حاوی داده غلط (HLM,BD) شامل P_{4-5}، P_4 در سمت بالا و با توجه به علامت مقدار GSR در سمت چپ یا راست منحنی واقع شده‌اند. همچنین، اندازه‌گیری‌های با نفوذ پایین و حاوی داده بد (LLM,BD) شامل P_1، با توجه به علامت GSR در سمت چپ یا راست منحنی قرار می‌گیرند. بیشتر نقاط در ناحیهٔ مربوط به LLPها و نزدیک به مبدأ قرار دارند؛ زیرا مقدار باقیمانده کوچکی دارند. نقاطی که مورد حمله قرار گرفته‌اند، از این نقاط دورند و در نواحی پرتی قرار می‌گیرند.



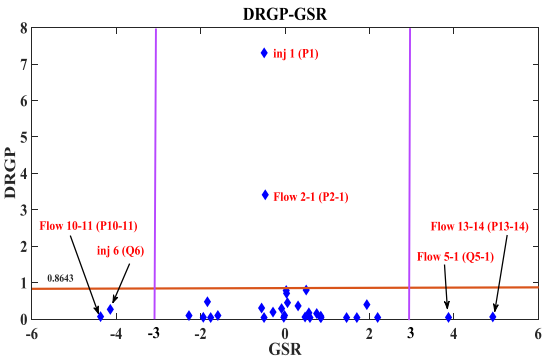
شکل (٤): منحنی DRGP-GSR شبکه ١٤ باسه IEEE در سناریو اول

٦-٣- سناریو دوم: حمله به کمیت‌های اندازه‌گیری‌شده در شبکه ١٤ باسه IEEE

در این سناریو، بردار حمله با توزیع نرمال تصادفی ایجاد شده است و به مقدار اندازه‌گیری‌ها اضافه می‌شود. نتایج حاصل از مقدار RMD، DRGP و GSR در جدول (۳) آورده شده‌اند. نتایج حاصل از مقدار DRGP نشان می‌دهند اندازه‌گیری‌های P_{2-1} و P_1 اندازه‌گیری‌های با نفوذ بالا (HLM) شناخته شده‌اند؛ زیرا مقدار DRGP متناظر با آنها از مقدار ۰/۸٦٤۳ بزرگ‌تر است. نتایج حاصل از مقدار GSR نشان می‌دهند میزان خطای تزریق‌شده به اندازه‌گیری‌های P_{10-11}، P_{13-14}، Q_{5-1} و Q_6 درخور توجه است. مقدار GSR متناظر با این اندازه‌گیری‌ها از عدد ۳ بزرگ‌تر است؛ بنابراین، این اندازه‌گیری‌ها حاوی داده بد هستند. نمودار نقطه‌ای DRGP-GSR مربوط به سناریو دوم در شکل (۵) نشان داده شده است.

مشاهده می‌شود اندازه‌گیری‌های P_{2-1} و P_1 در ناحیهٔ

بالای منحنی قرار گرفته‌اند. اندازه‌گیری‌های آلوده به خطا شامل اندازه‌گیری‌های P_{10-11}، P_{13-14}، Q_{5-1} و Q_6 است و چون اندازه‌گیری‌های با نفوذ پایین (LLM.BD) هستند، در ناحیهٔ پایین منحنی قرار می‌گیرند. اندازه‌گیری‌های Q_{5-1} و P_{13-14} با توجه به مقدار مثبت GSR در سمت راست و اندازه‌گیری‌های P_{10-11} و Q_6 با توجه به مقدار منفی GSR متناظرشان در سمت چپ منحنی قرار خواهند گرفت.



شکل (۵): منحنی DRGP-GSR شبکه ۱٤ باسه IEEE در سناریو دوم

٦-٤- دستکاری هم‌زمان اندازه‌گیری‌ها و پارامترهای شبکه ۱۲۳ باسه IEEE توسط مهاجم

در این شبکه، مقادیر اندازه‌گیری‌ها با اضافه‌کردن نویز تصادفی نرمال با میانگین صفر و انحراف استاندارد ۰/۰۱ به نتایج پخش بار AC تولید شده‌اند. استراتژی حمله در این شبکه با افزودن خطاهای تصادفی به مقادیر اندازه‌گیری‌های توان تزریقی در باس‌های ۱٤، ۳٦، ۵۵ و ٦۷ (P_{14}، P_{36}، P_{55} و P_{67}) و اندازه‌گیری توان انتقالی از خط ۵٤ به ۵۵ (P_{55-54}) در نظر گرفته شده است.

با توجه به تعداد زیاد اندازه‌گیری‌ها از آوردن مقادیر RMD، DRGP و GSR همهٔ اندازه‌گیری‌ها صرف‌نظر می‌شود و فقط مقادیر مربوط به اندازه‌گیری‌های مورد حمله در جدول (٤) آورده می‌شوند. منحنی نقطه‌ای DRGP-GSR شبکه ۱۲۳ باسه IEEE در شکل (٦) نشان داده شده است. مطابق با نتایج شبیه‌سازی اندازه‌گیری‌های P_{55}، P_{14}، P_{14-9} و P_{54-55} مقدار DRGP بزرگ‌تری از مقدار ۰/۸۷٦۷ دارند و اندازه‌گیری‌های HLM شناخته می‌شوند. نتایج حاصل از مقدار GSR نشان می‌دهند اندازه‌گیری‌های P_{55}، P_{14}، P_{55-54} و P_{67}، مقدار GSR بزرگ‌تری از مقدار ۳ دارند؛ بنابراین، این اندازه‌گیری‌ها حاوی داده بد هستند؛ زیرا میزان خطای تزریق‌شده به آنها شایان توجه بوده است. باوجود تزریق خطا به اندازه‌گیری P_{36} مقدار GSR متناظر با آن از مقدار ۳ کمتر است و علت عدم شناسایی آن به‌منزلهٔ اندازه‌گیری حاوی داده بد، تزریق خطا بسیار ناچیز است. همچنین، با توجه به مقدار DRGP متناظر با آن، اندازه‌گیری LLM است که اهمیت زیادی بر تخمین حالت شبکه ندارد.

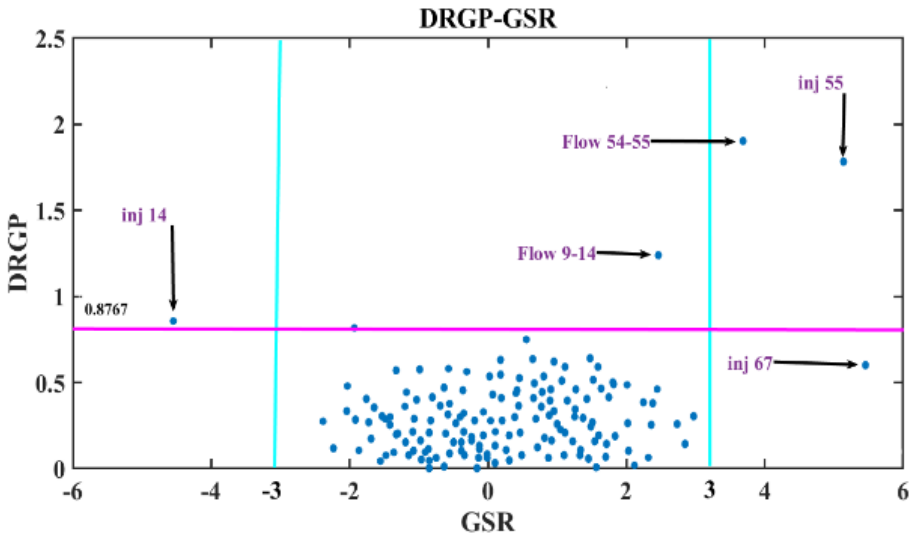
همچنین، اندازه‌گیری‌های آلوده به خطا شامل P_{55} و P_{55-54} چون اندازه‌گیری‌های با نفوذ بالا (HLM.BD) هستند، در ناحیهٔ بالا و با توجه به علامت مقدار GSR در سمت راست منحنی قرار گرفته‌اند. اندازه‌گیری P_{14} از نوع اندازه‌گیری HLM است و با توجه به علامت منفی GSR متناظر با آن، در سمت بالا و چپ منحنی قرار گرفته است. اندازه‌گیری (P_{67}) چون اندازه‌گیری LLM و حاوی داده بد است، در ناحیه پایین و سمت راست منحنی قرار گرفته است.

جدول (۳): نتایج شبیه‌سازی در سناریو دوم

ردیف	اندازه‌گیری	DRGP (cut_off=0.8643)	GSR (cut_off=3/0)
۱	$P_{۲-۱}$	۳/٤۱۳۳	-۰/٤۷۱۳۷
۲	$P_{۳-۲}$	۰/۷۸۵۸	۰/۰۲۵۲۵
۳	$P_{۲-٤}$	۰/٤۵۲۲	۰/۰۵۵٤٦
٤	$P_{۱-۵}$	۰/۷۹۹۳	۰/٤۹۹۰
۵	$P_{۵-۲}$	۰/۲۸۹۷	-۰/۰۸٤٤
٦	$P_{۵-٤}$	۰/۵۰٦۰	۱/۳٦۸۲
۷	$P_{۵-٦}$	۰/۳۰۵۱	-/۵۵۸۰
۸	$P_{٤-۷}$	۰/۱۵۵۱	۰/۷٤۸٤
۹	$P_{۸-۷}$	۰/۰٤۳٦۱	۱/٦۹۹٦
۱۰	$P_{۹-۷}$	۰/۱۷۳۸	۰/۵٦۲۰
۱۱	$P_{۹-۱۰}$	۰/۰٤٦۱۹	۲/۱۹۲۵
۱۲	$P_{٦-۱۱}$	۰/۰۵۱۰	۰/۸۳۷۷
۱۳	$P_{۱۳-٦}$	۰/۰۹۹۸	-۱/۵۹٤۷
۱٤	$P_{۱۰-۱۱}$	۰/۰٦۹۳٦	-٤/۳۷٤۸
۱۵	$P_{۱۳-۱٤}$	۰/۰٦۱۷۳	٤/۹۲۱۷
۱٦	$P_{۱}$	۷/۳۰۷۹	-۰/٤۹٦۸
۱۷	$P_{٤}$	۰/۳٦۳۸	۰/۳۰٦٤
۱۸	$P_{۸}$	۰/۰٤۳٦۱	۱/٤۵٦۳
۱۹	$P_{۱۰}$	۰/۰۵۸۳۰	۰/٤۷۲۵
۲۰	$P_{۱۲}$	۰/۰۵۰۸٦	-۱/۹۳۹۹
۲۱	$P_{۱٤}$	۰/۰۸۲۰	-۰/۸٤۵۰
۲۲	$Q_{۱-۲}$	۰/۱۰۱۵	-۰/۰۱٤۷۷
۲۳	$Q_{۵-۱}$	۰/۰٤۷۹۲	۳/۸۷۱۹
۲٤	$Q_{٤-۳}$	۰/٤۷۷۵	-۱/۸٤۲۰
۲۵	$Q_{۷-۸}$	۰/۳۹۹۱	۱/۹۳٦٦
۲٦	$Q_{۹-٤}$	۰/۰٤۳٤۸	۰/۸٤۹۵
۲۷	$Q_{۱۰-۹}$	۰/۷۰۷٦	۰/۰۳۳۸۲
۲۸	$Q_{۱٤-۹}$	۰/۰۹۷٦۹	-۲/۲۷۹۵
۲۹	$Q_{۱۳-۱۲}$	۰/۰٤٤۲۵	-۰/٤۹۹۸
۳۰	$Q_{۲}$	۰/۱۹٤۰	-۰/۲۸۷٤
۳۱	$Q_{٦}$	۰/۲٦۸۲	-٤/۱٤۳۸
۳۲	$Q_{۷}$	۰/۰٤۳٦	۰/۵۸۷۸
۳۳	$Q_{۱۱}$	۰/۰٤٤۵	-۱/۷٦٤۹
۳٤	$Q_{۱۳}$	۰/۰۵۰۲٤	-۰/۰۳۱۳۸

جدول (٤): نتایج شبیه‌سازی بر شبکه ۱۲۳ باسه IEEE

اندازه‌گیری	DRGP (cut_off=۰/۸۷۶۷	GSR (cut_off=۳/۰
$P_{۱٤}$	۰/۸۹۷۵	-٤,۸٦۵
$P_{٦۷}$	۵/٤۷٦	۵/۳۳٦
$P_{۵۵}$	۱/۸۹۸	٤/۵۷٦
$P_{۳٦}$	۰/۷٦۵	۲/۰۵٦
$P_{۵۵-۵٤}$	۱/۸۵۷	۳/٦۸۸



شکل (٦): منحنی DRGP-GSR شبکه ۱۲۳ باسه IEEE

۷- مقایسهٔ نتایج روش پیشنهادی با سایر روش‌ها

به‌منظور بیان کارایی دقیق و بالای روش پیشنهادی، شناسایی اندازه‌گیری‌های HLM و LLM با استفاده از الگوریتم‌های DRGP و RMD بر شبکه ١٤ باسه انجام شده است. همچنین، شناسایی اندازه‌گیری‌های حاوی داده بد با استفاده از الگوریتم GSR و روش باقیمانده استیودنت‌شده داخلی انجام شده است که در ادامه، نتایج تحلیل شده‌اند.

۷-۱- مقایسهٔ الگوریتم DRGP با RMD در شبکه ١٤ باسه IEEE

در مقایسهٔ نتایج روش ارائه‌شده با سایر روش‌ها، از نتایج شبیه‌سازی جدول (۲) بر شبکه ١٤ باسه مشاهده شد که الگوریتم DRGP به‌خوبی قابلیت تشخیص درست اندازه‌گیری‌های HLM را از اندازه‌گیری‌های LLM دارد؛ در حالی که روش‌های نفوذ (مقدار مؤلفه‌های قطری ماتریس K) و RMD به اثر masking و swamping آسیب‌پذیرند و قادر به تشخیص و جداسازی درست اندازه‌گیری‌های HLM و LLM نیستند.

در روش مقدار نفوذ و RMD، ممکن است نوع اندازه‌گیری‌ها به اشتباه تشخیص داده شوند؛ یعنی اندازه‌گیری HLM، به‌اشتباه اندازه‌گیری LLM شناخته شود و بالعکس. این در حالی است که الگوریتم DRGP با محاسبه مقدار پتانسیل متناظر با اندازه‌گیری‌های موجود در دو دسته D و R، شناسایی اشتباه اندازه‌گیری‌ها را با روش RMD اصلاح می‌کند؛ بنابراین، روش DRGP قابلیت تشخیص دقیق HLM ها را از LLMها دارد.

۷-۲- مقایسهٔ الگوریتم GSR با باقیمانده استیودنت‌شده داخلی در شبکه ١٤ باسه IEEE

در رابطه با بررسی صحت و دقت الگوریتم BDD ارائه‌شده، نتایج حاصل از مقادیر GSR با روش باقیمانده استیودنت داخلی[۲۰] مقایسه شده‌اند. نتایج مقادیر GSR و باقیمانده استیودنت‌شده داخلی در سناریو اول شبکه ١٤ باسه در جدول (۵) آورده شده‌اند. با مشاهده نتایج ملاحظه می‌شود اندازه‌گیری $P_{۲-۵}$ مقدار باقیمانده استیودنت‌شده داخلی آن از مقدار ۳ بزرگ‌تر است و به‌عنوان اندازه‌گیری حاوی داده بد شناسایی شده است؛ در حالی که مقدار GSR متناظر با این اندازه‌گیری از مقدار ۳ کوچک‌تر است. همچنین، روش باقیمانده استیودنت‌شده داخلی قادر به تشخیص اندازه‌گیری $P_{٤}$ به‌عنوان اندازه‌گیری حاوی داده بد نبوده است؛ بنابراین، روش باقیمانده استیودنت‌شده داخلی

نه‌تنها قادر به تشخیص درست اندازه‌گیری‌های آلوده به خطا نیست، ممکن است اندازه‌گیری مورد حملهِ قرار نگرفته را به‌منزلهٔ اندازه‌گیری آلوده به خطا شناسایی کند؛ اما روش GSR قادر به تشخیص صحیح اندازه‌گیری‌های آلوده به خطا است.

۸- نتیجه‌گیری

در این مقاله، روش جدیدی در شناسایی داده بد تزریق‌شده به اندازه‌گیری‌ها و پارامترهای شبکه ارائه شده است. در این روش، علاوه‌بر شناسایی اندازه‌گیری‌های با نفوذ بالا و پایین، اندازه‌گیری‌های آلوده به خطا و دستکاری‌شدهٔ مهاجم، به تفکیک هر نوع اندازه‌گیری تشخیص داده می‌شوند. نتایج شبیه‌سازی نشان می‌دهند احتمال تشخیص اشتباه اندازه‌گیری‌های دستکاری‌شده با جداسازی نوع اندازه‌گیری‌های HLM و LLM بسیار کاهش یافته است. در این صورت، حتی اگر مهاجم قادر به نفوذ به مرکز کنترل و دستکاری پارامترهای شبکه باشد، به گونه‌ای که سیستم تشخیص داده بد را دور بزند، الگوریتم‌های ارائه‌شده با قدرت بالا، اندازه‌گیری‌های دستکاری‌شده و آلوده به خطا را شخیص می‌دهند. جداسازی اندازه‌گیری‌های با نفوذ بالا و تخمین حالت‌های شبکه با استفاده از اندازه‌گیری‌های با نفوذ پایین، امکان موفق‌شدن مهاجم را هرچند نقشه‌های بسیار دقیق را پیاده‌سازی کند، محدود خواهد کرد.

جدول (۵): مقایسهٔ نتایج روش پیشنهادی با سایر روش‌ها

اندازه‌گیری	Internally studentized residual (*cut-off*= ۳/۰)	GSR (*cut-off*= ۳/۰)
$P_{۲-۱}$	۰/۷۹۸	-۰/۸۴۹۵
$P_{۳-۲}$	۱/۳۴۳	۱/۹۸۷۰
$P_{۲-٤}$	۰/۸۹۱	-۰,۳۵۰
$P_{۱-٥}$	۰/۵۳۲	-۱/٤۷٦۰
$P_{٥-۲}$	۳/۷۳۱	۲/۵۸۲
$P_{٥-٤}$	۳/۲۳۸	٥/۲۱۲
$P_{٥-٦}$	۱/٥٤٦	-۰/٦٥۱
$P_{٤-۷}$	۱/۲۸۷	-۱/٤٥۷
$P_{۸-۷}$	۰/۹۰۸	-۱/٤۹۱
$P_{۹-۷}$	۱/۸۸۱	-۰/٦٤٥٥
$P_{۹-۱۰}$	۰/۹٤۳	-۰/۷٥٦۰
$P_{٦-۱۱}$	۰/۷۸٦	-۱/٥۰۱۷
$P_{۱۳-٦}$	۰/۱۸۷	۰/٤۲٥٥
$P_{۱۰-۱۱}$	۰/٦۷۸	۰/۹٦۷۸
$P_{۱۳-۱٤}$	۱/۳٤۲	-۱/٥۲٦۳
$P_{۱}$	۳/٤٤۲	٥/۷۸٦۱
$P_{٤}$	۰/٥٥۲	-۳/۹۳٦۷
$P_{۸}$	۰/٦۷٤	-۰/٦۸۹۰
$P_{۱۰}$	۰/٤٥۲	-۰/۱۸٦٤
$P_{۱۲}$	۰/۱۲۳	۰/۸۲٦٤
$P_{۱٤}$	۱/۲٦٥	-۲/٥۲۳
$Q_{۱-۲}$	۲/٥۷٦	۲/۰۰۸
$Q_{٥-۱}$	۲/٥۳٦	-۱/۸۷۸
$Q_{٤-۳}$	۱/۹۳۲	-۲/۱۸٥
$Q_{۷-۸}$	۱/٥٤٦	۲/٥٥٤۸
$Q_{۹-٤}$	۰/۳۸۷	۰/۸٥۹۷
$Q_{۱۰-۹}$	۰/٥٥۷	-۰/۱٦٤۳
$Q_{۱٤-۹}$	۰/٤٥٦	۰/٦٤۲۰
$Q_{۱۳-۱۲}$	۰/۱۱٥	-۱,٤۸۳٦
$Q_{۲}$	۰/٥٦۷	-۱/۳٥٦٤
$Q_{٦}$	۰/۲٥۷	۲/۱۱٥۳
$Q_{۷}$	۲/٤۳٦	۰/۱٤٦۲
$Q_{۱۱}$	۰/٦۷٥	۰/۱۰٤٦
$Q_{۱۳}$	۰/۸۳۲	-۱/۸٥٤

۹-مراجع

1. Liang, G., et al., *A review of false data injection attacks against modern power systems.* IEEE Transactions on Smart Grid, 2016. 8(4): p. 1630-1638.
2. KP, V.P. and J. Bapat. *Bad data detection in smart grid for AC model*. in *2014 Annual IEEE India Conference (INDICON)*. 2014. IEEE.
3. Tan, S., et al. *LPAttack: Leverage point attacks against state estimation in smart grid*. in *2014 IEEE Global Communications Conference*. 2014. IEEE.
4. Singh, S.K., et al., *Joint-transformation-based detection of false data injection attacks in smart grid.* IEEE Transactions on Industrial Informatics, 2017. 14(1): p. 89-97.
5. Li, S., Y. Yılmaz, and X. Wang, *Quickest detection of false data injection attack in wide-area smart grids.* IEEE Transactions on Smart Grid, 2014. 6(6): p. 2725-2735.
6. Liu, X., et al., *Modeling of local false data injection*

reconfiguration method for enhancing resilience of distribution systems considering the whole process of resiliency. International Transactions on Electrical Energy Systems, 2020. 30(2): p. e12199.
18. Tran, N.N., et al., *Designing Constraint-Based False Data-Injection Attacks Against the Unbalanced Distribution Smart Grids.* IEEE Internet of Things Journal, 2021. 8(11): p. 9422-9435.
19. Majumdar, A. and B.C. Pal, *Bad data detection in the context of leverage point attacks in modern power networks.* IEEE Transactions on Smart Grid, 2016. 9(3): p. 2042-2054.
20. Habshah, M., M. Norazan, and A. Rahmatullah Imon, *The performance of diagnostic-robust generalized potentials for the identification of multiple high leverage points in linear regression.* Journal of Applied Statistics, 2009. 36(5): p. 507-520.
21. Lim, H.A. and H. Midi, *Diagnostic Robust Generalized Potential based on Index Set Equality (DRGP (ISE)) for the identification of high leverage points in linear model.* Computational statistics, 2016. 31(3): p. 859-877.
22. Chen, J. and A. Abur, *Placement of PMUs to enable bad data detection in state estimation.* IEEE Transactions on Power Systems, 2006. 21(4): p. 1608-1615.
23. Rahmatullah Imon, A., *Identifying multiple influential observations in linear regression.* Journal of Applied statistics, 2005. 32(9): p. 929-946.
24. Deka, D., R. Baldick, and S. Vishwanath, *Hidden attacks on power grid: optimal attack strategies and mitigation.* arXiv preprint arXiv:1401.3274, 2014.
25. *A. T. Koru, "Finding Minimum Volume Ellipsoid Enclosing N Points via Semi-Definite Programming," 2016.*.
26. *Power systems test case archive."http://www.ee.washington.edu/research/pstca/.*
27. Group, D.T.F.W., *Distribution test feeders.* Available from: ewh. ieee. org/soc/pes/dsacom/testfeeders/index. htmi, 2010.
28. Kersting, W.H., *Radial distribution test feeders.* IEEE Transactions on Power Systems, 1991. 6(3): p. 975-985.

attacks with reduced network information. IEEE Transactions on Smart Grid, 2015. 6(4): p. 1686-1696.
7. Bretas, A.S., N.G. Bretas, and B.E. Carvalho, *Further contributions to smart grids cyber-physical security as a malicious data attack: Proof and properties of the parameter error spreading out to the measurements and a relaxed correction model.* International Journal of Electrical Power & Energy Systems, 2019. 104: p. 43-51.
8. Zhao, J. and L. Mili, *Vulnerability of the largest normalized residual statistical test to leverage points.* IEEE Transactions on Power Systems, 2018. 33(4): p. 4643-4646.
9. Arvani, A. and V.S. Rao, *Detection and protection against intrusions on smart grid systems.* International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2014. 3(1): p. 38-48.
10. Li, B., et al., *Detecting false data injection attacks against power system state estimation with fast go-decomposition approach.* IEEE Transactions on Industrial Informatics, 2018. 15(5): p. 2892-2904.
11. Drayer, E. and T. Routtenberg, *Detection of false data injection attacks in smart grids based on graph signal processing.* IEEE Systems Journal, 2019. 14(2): p. 1886-1896.
12. Liu, Y., P. Ning, and M.K. Reiter, *False data injection attacks against state estimation in electric power grids.* ACM Transactions on Information and System Security (TISSEC), 2011. 14(1): p. 1-33.
13. Pan, K., et al., *Cyber risk analysis of combined data attacks against power system state estimation.* IEEE Transactions on Smart Grid, 2018. 10(3): p. 3044-3056.
14. Yang, Q., et al. *On a hierarchical false data injection attack on power system state estimation*. in *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*. 2011. IEEE.
15. Deng, R., P. Zhuang, and H. Liang, *False data injection attacks against state estimation in power distribution systems.* IEEE Transactions on Smart Grid, 2018. 10(3): p. 2871-2881.
16. Lakshminarayana, S., et al., *Data-driven false data injection attacks against power grids: A random matrix approach.* IEEE Transactions on Smart Grid, 2020. 12(1): p. 635-646.
17. Wang, H., et al., *A novel planning attack*

[1] Phasor Measurement Unit
[2] Bad Data Injection
[3] State Estimation
[4] Bad Data Detection
[5] Absolut Distance
[6] Kullback-Leibler Distance
[7] Diagnostic Robust Generalized Potential
[8] High Leverage Point
[9] Leverage Point

[10] Weighted Least Square
[11] High Leverage Point
[12] Low Leverage Point
[13] High Leverage Measurement
[14] Low Leverage Measurement
[15] Outlier
[16] Robust Mahalanobis Distance (RMD)
[17] Minimum Volume Ellipsoid
[18] Median Absolut Deviation
[19] Generalized Studentized Residual (GSR)
[20] Internally Studentized Residual