دانشکده مهندسی برق و رباتیک

پایان‌نامه کارشناسی ارشد مهندسی سیستمهای قدرت

# تشخیص حملات تزریق اطلاعات غلط در تخمین حالت شبکه‌های قدرت

نگارنده : محمدامین یزدان‌پرست

استاد راهنما

دکتر محسن اصیلی

تیر ۱۳۹۷

شماره: ۲/۱۵۷٤/ت/ب
تاریخ: ۹۷/٤/۲۰

**باسمه‌تعالی**

مدیریت تحصیلات تکمیلی

## فرم شماره (۳) صورتجلسه نهایی دفاع از پایان نامه دوره کارشناسی ارشد

با نام و یاد خداوند متعال، ارزیابی جلسه دفاع از پایان نامه کارشناسی ارشد خانم / آقای **محمد امین یزدان پرست** با شماره دانشجویی ۹۳۱۸۴۵۴ رشته **مهندسی قدرت** گرایش **سیستم** تحت عنوان: **تشخیص حملات تزریق اطلاعات غلط در تخمین حالت شبکه های قدرت** که در تاریخ **۱۳۹۷/۰۴/۲۰** با حضور هیأت محترم داوران در دانشگاه صنعتی شاهرود برگزار گردید به شرح ذیل اعلام می گردد:

قبول ( با امتیاز ۱۸/۰۸ درجه خیلی خوب ) ☑ مردود ☐

نوع تحقیق: نظری ☑ عملی ☐

| عضو هیأت داوران | نام ونام خانوادگی | مرتبهٔ علمی | امضاء |
|---|---|---|---|
| ۱ـ استادراهنمای اول | محسن اصلی | استادیار | |
| ۲- استادراهنمای دوم | — | — | — |
| ۳- استاد مشاور | — | — | — |
| ۴-نماینده تحصیلات تکمیلی | امیرحسن نیا | استادیار | |
| ۵- استاد ممتحن اول | رحمت اله هوشمند | استاد | |
| ۶ـ استاد ممتحن دوم | یوسف عامری | استادیار | |

نام و نام خانوادگی رئیس دانشکده:

تاریخ و امضاء و مهر دانشکده:

**تبصره:** در صورتی که کسی مردود شود حداکثر یکبار دیگر (در مدت مجاز تحصیل) می تواند از پایان نامه خود دفاع نماید (دفاع مجدد نباید زودتر از ۴ ماه برگزار شود).

**تقدیم اثر**

تقدیم به پدر و مادر مهربانم که در طی تمام مراحل سهل و دشوار زندگی پشتیبان من بوده‌اند و دلسوزانه مرا راهنمایی و هدایت نموده‌اند. تقدیم به همسر عزیز، یار و یاور من که مرا در تمامی مرحله زندگی یاری نمود و همچون دوستی دلسوز برایم بود. تقدیم به همراهانم در پیشرفت‌ها، خوشی‌ها و ناخوشی‌ها...

## تشکر و قدردانی

الهی؛

الهی: یکتای بی‌همتایی، قیوم توانایی، بر همه چیز دانایی، بر همه حال بینایی، از عیب مصفایی، از شریک مبرایی؛

الهی: اصل هر دوایی، جان داوری دل هایی، بر تخت عرش معلایی، مسند نشین استغنایی، خطبه الوهیت را سزایی، به توزیبد ملک خدایی ؛

الهی: به عجز و بیچارگی خود گواهم و از لطف و عنایت تو آگاهم، خواست خواست توست من چه خواهم ؛

الهی: تو بساز که دیگران ندانند و تو نواز که دیگران نتوانند؛

الهی: دلی ده که طاعت افزون کند و توفیق طاعتی که به بهشت رهنمون کند؛

.....

ای عزیز بدان که بهترین کارها شناختن خدای تعالی است (جل جلاله)

اول خدای را باید شناخت که اول هر چیزی است اگر همه نه هند او بدهد و چون چیزی داد هیچ کس نتواند بستاند و چون او نهد کسی نتواند که بدهد او را نگاه دارو عمر را در پرستش او خرج کن که حساب خرج هر کس را او خواهد خواست و دلیل راه علم و نمایند صراط مستقیم حق سبحان را دان، عقل را بیناشمار؛

**در پایان از استاد ارجمند و عزیزم، جناب آقای دکتر اصیلی که ما را در جهت آموختن علم و تحصیل یاری کرده‌اند، نهایت تشکر رادارم و از زحمات بی‌دریغ و دلسوزانه ایشان و دیگر اساتید گرامی و دوستانی که مرا در این مهم یاری رساندند، سپاسگزاری می‌نمایم و از قادر بی‌همتا برای ایشان آرزوی سلامتی و موفقیت روزافزون را خواستارم.**

# تعهد نامه

اینجانب **محمدامین یزدان‌پرست** دانشجوی دوره کارشناسی ارشد رشته **سیستم‌های قدرت** دانشکده **برق و رباتیک** دانشگاه صنعتی شاهرود نویسنده پایان‌نامه **تشخیص حملات تزریق اطلاعات غلط در تخمین حالت شبکه‌های قدرت** تحت راهنمایی **دکتر محسن اصیلی** متعهد می‌شوم:

- تحقیقات در این پایان‌نامه توسط اینجانب انجام‌شده است و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهش‌های محققان دیگر به مرجع مورداستفاده استناد شده است.
- مطالب مندرج در پایان‌نامه تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است.
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می‌باشد و مقالات مستخرج با نام «دانشگاه صنعتی شاهرود» و یا «Shahrood University of Technology» به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان‌نامه تأثیرگذار بوده‌اند، در مقالات مستخرج از پایان‌نامه رعایت می‌گردد.
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده(یا بافت‌های آن‌ها) استفاده شده است، ضوابط و اصول اخلاقی رعایت شده است.
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است، اصل رازداری، ضوابط و اصول اخلاق انسانی رعایت شده است.

**تاریخ**

**امضای دانشجو**

**مالکیت نتایج و حق نشر**

- کلیه حقوق معنوی این اثر و محصولات آن(مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده) متعلق به دانشگاه صنعتی شاهرود می‌باشد. این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در پایان‌نامه بدون ذکر مرجع مجاز نمی‌باشد.

## چکیده

در سیستم‌های قدرت، متغیرهای حالت شامل مقادیر ولتاژوزوایای نسبی فاز در گره‌های سیستم می‌باشند. اندازه‌گیری‌هایی موردنیاز است تا بتوان عملکرد سیستم را در وضعیت بلادرنگ هم برای کنترل قابلیت اطمینان و هم برای قیود موجود در توزیع اقتصادی بار، تخمین زد. تخمین حالت مهم‌ترین قسمت در پایش شبکه قدرت است که طی آن حالت سیستم تعیین‌شده و بهره‌بردار به کمک آن قادر به تصمیم‌گیری مناسب در مورد اعمال احتمالی لازم جهت حفظ عملکرد سیستم در حالت عادی و مطمئن می‌باشد. برای انجام تخمین حالت، داده‌های اندازه‌گیری از واحدهای ترمینال از راه دور(RTUs) به مرکز کنترل سیستم قدرت ارسال می‌شود. دراین‌بین حال اگر مهاجم به طریقی اطلاعات ارسالی به مرکز کنترل را موردحمله قرار دهد، می‌تواند باعث تخمینی اشتباه شده در تخمین گر شود.

در این پایان‌نامه روشی برای تشخیص حملات تزریق داده بد به سیستم قدرت هوشمند پیشنهاد داده خواهد شد. در مرحله اول روشی پیشنهادی با استفاده از اطلاعات فعلی و گذشته سیستم قدرت و محاسبه تغییرات اندازه‌گیرهای سیستم، تابع هیستوگرام تغییرات را محاسبه می‌کند. سپس در مرحله بعد با استفاده از تابع تشخیص پیشنهادی از روی تابع هیستوگرام محاسبه‌شده در مرحله قبل به تشخیص حملات تزریق داده بد می‌پردازد. روش پیشنهادی برای هراندازه گیری به‌صورت جداگانه تشخیص را انجام داده و ازاین‌رو با توجه به ساختار شبکه قادر به شناسایی هدف مهاجم در تخریب متغیر حالت موردنظر می‌باشد.



**کلمات کلیدی:** تشخیص داده بد، تخمین حالت، حملات سایبری، شبکه هوشمند، سیستم قدرت.

# فهرست مطالب

# فهرست اشکال

# فهرست جداول

# فصل اول:

# مقدمه ای بر مساله

## ۱-۱- مقدمه

مفهوم شبکه‌های هوشمند[1] باهدف بروز کردن شبکه‌های برق کنونی و معرفی مجموعه‌ای از فناوری‌ها و خدمات جدید که شبکه‌های برق را قابل‌اطمینان‌تر و بهینه می‌سازد، معرفی شد. در دهه اخیر، واژه شبکه هوشمند به واژه آشنایی برای شبکه‌های برق تبدیل‌شده است. بر اساس تعریف سازمان انرژی ایالات‌متحده آمریکا، شبکه هوشمند یک شبکه گسترده انرژی خودکار است که در آن انتقال توان الکتریکی و تبادل اطلاعات به‌صورت دوطرفه صورت می‌گیرد. این شبکه قابلیت پایش و پاسخگویی به هر نوع تغییرات در شبکه از منابع تولید تا مصرف‌کنندگان و حتی تک‌تک تجهیزات را دارد[۱].

یک شبکه هوشمند نشان‌دهنده چشم‌اندازی از سیستم‌های قدرت آینده است که فناوری‌های سنجش پیشرفته، روش‌های کنترلی و فناوری‌های ارتباطی در سطوح انتقال و توزیع را به‌منظور تأمین برق به‌صورت هوشمند و کاربرپسند تلفیق می‌کند[۲][۳]. با توجه به گزارش اولیه از شبکه مدرن وزارت انرژی ایالات‌متحده، ویژگی‌های اصلی یک شبکه هوشمند، مشتری‌پسندی، خودترمیم بودن، مقاوم در برابر حمله، توانایی تطبیق با همه نوع تولید و ذخیره، بازار برق مبتنی بر عملکرد کارآمد و کیفیت توان بالا است[۳]. این شبکه مدرن توسط چند عامل اقتصادی، سیاسی، زیست‌محیطی، اجتماعی و فنی ایجاد می‌شود.

در سال‌های گذشته تغییرات سریعی از شبکه‌های سنتی به شبکه‌های هوشمند جدید صورت گرفت تا با افزایش مصرف و نیاز بیشتر تطابق پیدا کند. در این زمینه برخی روش‌های خاص جهت این حرکت تکاملی ارائه‌شده است که شامل بازآرایی سریع[۴]، هوشمند شدن سیستم[۵]، عدم تمرکزگرایی سیستم قدرت و پراکنده بودن[۶] و ادوات مانیتورینگ سریع می‌باشد. در مراحل اولیه تشکیل شبکه‌های هوشمند، نمایش وضعیت سیستم وظیفه اصلی می‌باشد که بدون آن ایده مطرح‌شده بی‌فایده است. یکی از استراتژی‌های مهم و مفید جهت مانیتورینگ سیستم، تخمین حالت

[1] Smart Grids

می‌باشد[۷]. تخمین حالت سیستم قدرت به فرآیندی اطلاق می‌گردد که در آن حالت سیستم الکتریکی توسط دستگاه‌های اندازه‌گیری بسیاری که در مکان‌های مختلف شبکه قرارگرفته‌اند ارزیابی می‌گردد[۸]. ازلحاظ فنی تخمین حالت به‌عنوان راه‌حلی جهت یافتن فازورهای ولتاژ باس‌ها درزمانی خاص می‌باشد. درمجموع، یک راه‌حل سریع و آسان نصب ادوات اندازه‌گیری دقیق در تمام باس‌های سیستم جهت محاسبه اندازه و زاویه ولتاژ تمامی باس‌هاست. اگرچه این راه ممکن است با خرابی‌ها و یا خطاهای اندازه‌گیری همراه باشد. جهت حل این مشکل می‌توان از اندازه‌گیری‌های پی‌درپی استفاده نمود تا خطاهای اندازه‌گیری کاهش یابد و حالتی بهینه که در مسئله تخمین حالت مطرح‌شده است، به دست آید.

در سیستم مدیریت انرژی مدرن[1]، برنامه تخمین حالت یکسری از مقادیر خام اندازه‌گیری شده را پردازش و یک حل پخش بار سریع را به دست می‌آورد که پایداری توابع پیشرفته، برای مشاهده و کنترل سیستم است. تخمین حالت بر اساس روابط ریاضی بین متغیرهای حالت سیستم و اندازه‌گیری‌ها است، متغیرهای حالت می‌تواند مقادیر ولتاژ و زاویه ولتاژ در تمام شین‌های سیستم باشند.

عمل محاسبه متغیرهای حالت مجهول بر اساس روش‌های آماری با حداکثر یا حداقل کردن معیار خاصی، صورت می‌گیرد. معیار مرسوم این است که تفاوت بین مقادیر محاسبه‌شده(تخمین زده‌شده) و مقادیر واقعی پارامترهای اندازه‌گیری شده حداقل شود. در یک سیستم توزیع تخمینگر حالت به این صورت طراحی می‌گردد که با توجه به اینکه در مقادیر اندازه‌گیری شده خطا وجود دارد و ممکن است برخی از اندازه‌گیری‌ها اضافی باشند، بهترین تخمین را از مقادیر دامنه و زاویه ولتاژ شین‌ها در اختیار قرار دهد. سپس اطلاعات خروجی از تخمین حالت در مرکز کنترل سیستم در پخش بار سریع و کنترل قابلیت اطمینان سیستم‌ها مورداستفاده قرار می‌گیرد. معمولاً تعداد اندازه‌گیری‌ها از مقدار

[1] Energy Management System

موردنیاز جهت تخمین حالت بیشتر است، بنابراین تخمینگر حالت مجموعه‌ای از اندازه‌گیری‌های اضافی را به‌منظور تخمین حالت سیستم‌ها پردازش می‌نماید. سه نوع اندازه‌گیری سریع وجود دارد:

الف) اندازه‌گیری‌های آنالوگ شامل مقدار ولتاژ شین‌ها، توان‌های اکتیو و راکتیو جاری و تزریقی در خطوط

ب) اندازه‌گیری‌های منطقی شامل حالت کلیدها و بریکرها(دژنکتورها)

پ) اندازه‌گیری‌های مجازی که ممکن است شامل تخمین بار مصرفی(اطلاعات قبلی) و تزریق‌های صفر در شین‌های پسیو باشد.

تخمینگر با استفاده از مجموعه اندازه‌گیری‌های آنالوگ و بر اساس مشخصات توپولوژیکی سیستم از قبیل امپدانس خطوط(اندازه‌گیری منطقی) و مجموعه‌ای از اندازه‌گیری‌های مجازی (به‌عنوان ورودی) اقدام به تخمین حالت‌های سیستم قدرت می‌نماید. حال اگر مجموعه اندازه‌گیری‌ها به تعداد کافی باشند و نحوه توزیع آن‌ها در سیستم مناسب باشد، تخمینگر حالت قادر خواهد بود حالت سیستم را محاسبه نماید. روش‌های متعددی برای به دست آوردن راه‌حل تخمین حالت پیشنهادشده است که این روش‌ها به‌صورت خلاصه در فصل بعد مرور می‌گردند.

درگذشته بیشتر سیستم‌های قدرت، قابل‌مشاهده و کنترل نبود. بنابراین اجرای تخمین حالت وجود نداشت. تحت این شرایط برنامه پخش بار سیستم توزیع اغلب برای مقاصد برنامه‌ریزی همچون تلفات سیستم و محاسبه ساختارهای مختلف فیدرها برای کاهش تلفات سیستم بکار می‌رفت. کار اصلی تخمین حالت به حداقل رساندن خطاها و نقص‌های موجود در اطلاعات می‌باشد. معمولاً این خطاها کوچک هستند، اما در برخی موارد ممکن است زیاد باشد. یک تخمینگر حالت می‌تواند خطاهای کوچک موجود در مقادیر اندازه‌گیری شده را برطرف کند و خطاهای بزرگ اندازه‌گیری شده را آشکار و مشخص نماید.

برای انجام شبیه‌سازی سیستم قدرت با روش تخمین حالت به دو نوع اطلاعات نیاز می‌باشد، اطلاعات شبکه و اطلاعات اندازه‌گیری شده. همچنین دو نوع تخمینگر حالت وجود دارد: استاتیکی و دینامیکی.

پارامترهایی که برای تخمین حالت دقیق قابل‌استفاده‌اند شامل توان اکتیو و راکتیو، اندازه ولتاژ یا جریان می‌باشد. در این رابطه الگوریتم تکرار حداقل مربعات وزندار[1] روشی مناسب و مفید است که اصولاً مورداستفاده قرار می‌گیرد و از نمونه‌های اندازه‌گیری متفاوتی استفاده می‌نماید تا سیستم را ارزیابی کرده و اطلاعات حالت استاتیکی و یا شبه استاتیکی آن را ارائه نماید[۹]. تابع تخمینگر حالت سنتی به مرکزیت یک مرکز کنترل عمل می‌نماید و داده‌های مطلوب، زمان حقیقی و استاتیکی، را جهت حل پردازشگر توپولوژی[2]، تخمین حالت[3] و داده بد[4] به‌صورت تناوبی تشخیص و حل می‌نماید[۱۰-۱۲]. بنابراین یکی از نتایج مهم تخمین حالت بهینه، بهره‌برداری مؤثر و امن سیستم قدرت در شرایط نرمال و گذرا می‌باشد[۱۳-۱۵].

اما یکی از اصلی‌ترین و مهم‌ترین مراحل پردازش‌های تخمین حالت، مرحله پردازش داده بد شامل شناسایی و حذف اطلاعات بد از مجموعه اندازه‌گیری در دسترس می‌باشد که بسته به عامل این داده بد،روش‌های مختلفی جهت حل آن ارائه‌شده است. در بین سه نوع مختلف داده‌های بد، حملات مخرب که به حملات سایبری نیز مشهور است و در شبکه هوشمند اتفاق می‌افتد، یکی از انواع جدید داده‌های بد است که با بروز شبکه‌های هوشمند پدیدار شده و با گذر زمان احتمال وقوع آن چندین برابر شده است. این حالت از داده بد تنها در شبکه هوشمند رخ می‌دهد.

به‌عنوان مثالی از این نوع داده بد می‌توان این‌گونه ذکر کرد که در شبکه‌های هوشمند تمام دستگاه‌ها IP مخصوص خود را دارا می‌باشند، لذا ممکن است مصرف‌کنندگان به اطلاعات مصرف توان خود و همچنین کنترل آن از طریق وب دسترسی داشته باشند. این مسیر دوطرفه احتمال آسیب-

[1] WLS
[2] Topology Processor
[3] State Estimation
[4] Bad Data

پذیری را فراهم می‌کند. و یا مهاجم ممکن است از طرق غیرقابل‌پیش‌بینی به شبکه نفوذ کند و از طریق دستیابی به نرم‌افزار شبکه، بار را تغییر دهد تا شبکه را به حالت ناپایداری سوق دهد.

برای تشخیص داده بد ناشی از عامل سوم(حملات سایبری)، روش‌های زیادی در مقالات متفاوت ارائه‌شده است و روش‌های مرسوم قادر به تشخیص این نوع از داده‌ها نیستند. چراکه این داده‌ها کاملاً هوشمند بوده و با داشتن اطلاعات پیکربندی سیستم، به‌گونه‌ای داده‌ها را تغییر می‌دهد که روش‌های مرسوم قادر به تشخیص نیستند.

نوع داده بدی که در این پژوهش مدنظر قرار دارد از نوع سومی بوده و باید روشی برای تشخیص این نوع از داده‌های بد ارائه گردد. به‌طورکلی راه‌های مقابله با تزریق داده‌های بد به دودسته تقسیم می‌شوند:

۱. روش مبتنی بر حفاظت

۲. روش مبتنی بر تشخیص

روش اول، این‌گونه است که دستگاه‌های نصب‌شده در سطح سیستم قدرت، هرکدام به‌صورت جداگانه حفاظت‌شده می‌باشند و کار به مرحله تشخیص نیز کشیده نمی‌شود. روش دوم بر مبنای تشخیص خطا عمل می‌کند و شامل الگوریتم‌های متفاوتی است که بنا به تخصص و سلیقه متخصصین این امر طراحی‌شده است و روش‌های زیادی در مقالات ارائه‌شده است که در این پژوهش نیز از این روش بهره می‌بریم.

در این پژوهش روش جدید مبتنی بر تشخیص برای برطرف شدن محدودیت‌های روش‌های موجود جهت تشخیص داده‌های بد نوع سوم ارائه می‌شود. ایده اصلی روش پیشنهادی ردیابی تغییرات اندازه‌گیری‌ها بین مراحل متوالی می‌باشد. سپس شاخص‌های فاصله از اندازه‌گیری‌های گذشته با استفاده از روش فاصله نسبی لگاریتمی محاسبه می‌شوند. مقدار آستانه که از داده‌های پیشین محاسبه می‌شود، برای تشخیص حملات پنهانی تزریق داده‌های بد مورداستفاده قرار می‌گیرد. به این صورت که هنگامی‌که داده اشتباه به سیستم قدرت تزریق می‌شود، هیستوگرام تغییرات اندازه‌گیری از

اندازه‌گیری‌های گذشته منحرف‌شده و درنتیجه به یک شاخص فاصله بزرگ‌تر منجر می‌شود. اگر شاخص فاصله بزرگ‌تر از آستانه باشد، این نتیجه دریافت می‌گردد که اندازه‌گیری‌ها و داده‌های جدید دریافتی دستکاری‌شده و تقلبی می‌باشند.

در ادامه با توجه به موضوع تحقیق بیان کامل‌تری از تخمین حالت و داده‌های بد در توابع تخمین حالت ارائه‌شده و در پایان ضرورت و اهداف و فرضیات تحقیق موردبررسی قرار می‌گیرند.

### ۱-۲- اهداف و ضرورت انجام تحقیق

امروزه برق و کیفیت آن به یک امر حیاتی و جدایی‌ناپذیر از زندگی انسان تبدیل‌شده است و قطع آن حتی برای زمان کوتاه ممکن است خسارت‌های قابل‌توجهی را موجب شود، لذا قابلیت اطمینان سیستم‌های قدرت از اهمیت بالایی برخوردار بوده و همواره پژوهشگران مقالات و مطالعات بسیاری در این زمینه منتشر می‌کنند. از طرفی مفهوم شبکه‌های هوشمند باهدف بروز کردن شبکه‌های برق کنونی و معرفی مجموعه‌ای از فناوری‌ها و خدمات جدید که شبکه‌های برق را قابل‌اطمینان‌تر، بهینه و دوستدار محیط‌زیست می‌سازد، معرفی شد. در مراحل اولیه تشکیل شبکه‌های هوشمند، نمایش وضعیت سیستم وظیفه اصلی می‌باشد که بدون آن ایده مطرح‌شده بی‌فایده است.

همچنین کنترل قابلیت اطمینان، نیازمند نظارت و داشتن اطلاعاتی از سیستم قدرت می‌باشد که این اطلاعات توسط دستگاه‌های اندازه‌گیری نصب‌شده در نقاط مختلف سیستم به دست می‌آید. ولی سؤالی که مطرح می‌شود این است که اطلاعات ارائه‌شده توسط دستگاه‌های اندازه‌گیری به چه میزانی قابل‌اعتماد است، علاوه بر این، حتی اگر این اطلاعات نیز قابل‌اعتماد باشد، ازلحاظ اقتصادی آیا امکان‌پذیر است که برای به دست آوردن هر پارامتر، یک دستگاه اندازه‌گیری نصب شود. لذا برای حل چالش فوق، باید راه‌حلی ارائه شود که هم قابلیت اطمینان سیستم را افزایش داده و از طرفی توجیه اقتصادی نیز داشته باشد. تخمین حالت در سیستم‌های قدرت به‌منظور برآورده کردن هر دو نیاز فوق بکار گرفته می‌شود. همچنین یکی از استراتژی‌های مهم و مفید جهت مانیتورینگ سیستم، تخمین حالت می‌باشد،بطوریکه با تعداد محدودی از داده‌های به‌دست‌آمده از دستگاه‌های اندازه‌گیری، تخمین

حالت قادر است خطاهای کوچک را فیلتر و خطاهای فاحش و بزرگ را تشخیص داده و سرانجام اطلاعاتی را که به علت قطع خطوط ارتباطی دریافت نشده است با مقادیر مناسب پر کند. پس حل تخمین حالت و نتایج به‌دست‌آمده از آن در افزایش قابلیت اطمینان سیستم‌های قدرت از اهمیت ویژه‌ای برخوردار بوده، ضمن اینکه نیم‌نگاهی به مسائل اقتصادی نیز دارد.

اما یکی از مشکلاتی که محاسبات تخمین حالت را تهدید می‌نماید وجود داده‌های بد در توابع تخمین حالت است که برای حل آن، تابع پردازش داده بد شامل شناسایی و حذف اطلاعات بد از مجموعه اندازه‌گیری در دسترس مورداستفاده قرار می‌گیرد. اما همان‌گونه که در بخش پیش نیز بیان گردید نوع جدید داده‌های بد که با بروز شبکه‌های هوشمند به وجود آمد، نوع سوم بوده که شامل حملات سایبری می‌باشد.

برای تشخیص داده بد ناشی از عامل سوم، روش‌های زیادی در مقالات متفاوت ارائه‌شده است و روش‌های مرسوم قادر به تشخیص این نوع از داده‌ها نیستند چراکه این داده‌ها کاملاً هوشمند بوده و با داشتن اطلاعات پیکربندی سیستم، به‌گونه‌ای داده‌ها را تغییر می‌دهد که روش‌های مرسوم قادر به تشخیص نیستند.

بدین ترتیب این ضرورت حس می‌گردد که مسئله تخمین حالت با حملات تزریق داده‌های بد مسئله‌ای مناسب جهت فعالیت بوده که هنوز باوجود مطالعات جای کار بسیاری دارد تا روش‌هایی مناسب جهت حل مشکل ارائه گردد.

بنابراین در این پژوهش روش جدید مبتنی بر تشخیص برای برطرف شدن محدودیت‌های روش-های موجود جهت تشخیص داده‌های بد نوع سوم ارائه می‌شود. ایده اصلی روش پیشنهادی ردیابی دینامیک‌های اندازه‌گیری‌ها با محاسبه شاخص‌های فاصله بین مراحل متوالی الگوریتم می‌باشد. روش پیشنهادی بر روی شبکه ۱۴ باسه مورد تست قرارگرفته و نتایج آن ارائه می‌گردد.

## ۱-۳- ساختار پایان‌نامه

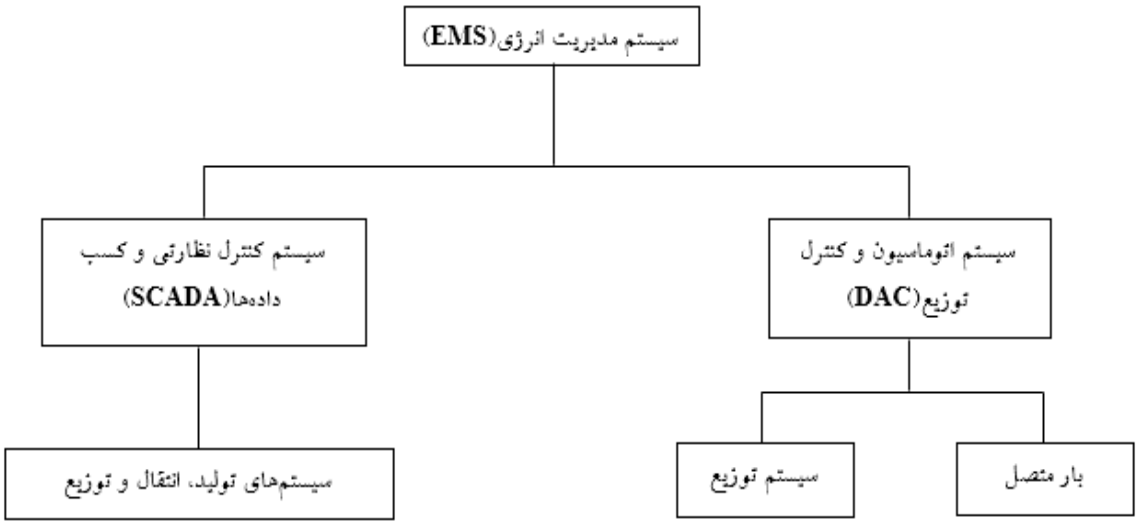
در این فصل در ابتدا مقدمه‌ای پیرامون موضوع تحقیق بیان گردید و سپس در ادامه به اهداف و ضرورت تحقیق و فرضیات در نظر گرفته‌شده پرداخته شد. در فصل دوم پس از بیان مقدمه، مختصری پیرامون انواع داده‌های بد و روش‌های مختلف تخمین حالت و مقابله با تزریق داده بد بحث می‌گردد. پس‌ازآن سوابق تحقیق و برخی روش‌های دیگر از تشخیص داده بد و اشتباه موردبررسی قرار می‌گیرند. در فصل سوم سیستم و روش پیشنهادی جهت تشخیص تزریق حملات داده اشتباه در شبکه ارائه می‌گردد. در این فصل روابط مورداستفاده بیان‌شده و نحوه مدل‌سازی مسئله تشریح می‌گردد. در فصل چهارم، به‌منظور تست روش پیشنهادی، این روش بر روی شبکه ۱۴ باسه تست‌شده و نتایج آن ارائه می‌شود. شبیه‌سازی سیستم پیشنهادی در محیط نرم‌افزار متلب صورت می‌گیرد و نتایج به‌دست‌آمده مورد تحلیل قرار خواهد گرفت. در ادامه در فصل پنجم، نتیجه‌گیری نهایی از تحقیق و دستاوردها، راهکارها و پیشنهادات لازم برای تحقیق و مطالعات آینده ارائه خواهد شد.

# فصل دوم:

# تخمین حالت و تشخیص داده بد در سیستم های قدرت

## ۲-۱-مقدمه

هدف اصلی سیستم قدرت، تولید، انتقال و توزیع انرژی الکتریکی با بازده خوب است. بهره‌برداری از سیستم، به سیستم‌های کنترل و نظارت پیچیده‌ای که ازنظر جغرافیایی پراکنده و ازنظر کارکرد مثل شکل ۲-۱ می‌باشند، نیازمند است. مطابق این شکل، کنترل کل سیستم بر عهده سیستم مدیریت انرژی[۱] است. سیستم کنترل نظارتی و کسب داده‌ها[۲] بر سیستم‌های تولید و انتقال احاطه دارد. سیستم اتوماسیون و کنترل توزیع(DAC[۳]) بر سیستم‌های توزیع و بارهای متصل احاطه دارد[۱۸].




شکل ۲-۱- نظارت و کنترل سیستم قدرت الکتریکی[۱۸]

به‌منظور درک بهتر لزوم استفاده از تخمین حالت در سیستم‌های قدرت، در این فصل در ابتدا مروری بر اتوماسیون سیستم‌های قدرت انجام می‌شود و سپس پیرامون تخمین حالت بحث می‌شود. در انتها مروری بر سوابق تحقیق صورت می‌گیرد.

## ۲-۲- اتوماسیون سیستم‌های قدرت

تا مدت‌ها وسایل اتوماتیک نظارت و کنترل، بخشی از سیستم کنترل نظارتی و کسب داده‌ها بود. اخیراً اتوماسیون، بخشی از کل سیستم مدیریت انرژی شده است که سیستم توزیع و انتقال را نیز در برمی‌گیرد. دلایل وجودی سیستم اتوماسیون و کنترل چنین است:

[1] EMS
[2] SCADA
[3] Distribution Automation & Control

- بهبود بازده کل سیستم در بهره‌گیری از سرمایه و انرژی
- کاهش الزامات ذخیره‌سازی در انتقال و تولید
- افزایش اطمینان بخشی در سرویس‌دهی به بارهای اصلی
- مدیریت مصرف‌کنندگان و درجه‌بندی دیماندها ازنظر زیان ناشی از خاموشی

پیشرفت در تکنولوژی، اتوماسیون واقعی را عملی کرد. اخیراً مهندسان سیستم‌های قدرت به ابزارهای نوینی مانند مینی کامپیوترهای ارزان و میکروپروسسورهای نیرومندی مجهز شده‌اند که بسیاری از مفاهیم اتوماسیون را دست‌یافتنی کرده‌اند.

عبارت اتوماسیون، معنای گسترده‌ای دارد و هرروزه کاربردهای جدیدی بدان افزوده می‌شود. ازنظر عده‌ای، این عبارت به معنای سیستمی ارتباطی در سطح توزیع و انتقال است که بار مشترک را کنترل می‌کند و بار حداکثر را با مدیریت بار کاهش می‌دهد[۱۸]. از دید عده‌ای دیگر، اتوماسیون به معنای پست توزیعی است که انسانی برای نظارت بر آن حضور ندارد و یک پردازشگر می‌تواند بر آن نظارت کند. پردازشگری که در پست توزیع قرار دارد همواره از وضعیت سیستم خبر می‌دهد، می‌تواند تصمیمات کاربردی بگیرد، فرمان بفرستد و هرگونه تغییری در وضعیت سیستم را به مرکز دیسپاچینگ توزیع[1] گزارش کند و بسته به نیاز شرکت برق‌رسانی ،آن تغییرات را در حافظه نگه دارد و یا از ذخیره‌سازی آن صرف‌نظر کند[۱۸].

## ۲-۳- نقش سیستم‌های کنترل و نظارت مدرن در پست‌ها

همان‌گونه که واضح است سیستم‌های کنترل و نظارت و جمع‌آوری اطلاعات از سطح دستگاه شروع‌شده و اطلاعات موردنیاز از چندین دستگاه به سطح پست انتقال می‌یابد. با توجه به اینکه پست-ها در هر سطحی از ولتاژ که باشند جزئی از اجزای اصلی تشکیل‌دهنده شبکه سراسر می‌باشند، پس کنترل و نظارت دقیق و مستمر به معنی جلوگیری از اتلاف انرژی و ارتقاء بازدهی در بهره‌برداری از شبکه است و این جزء ارکان اساسی طراحی، توسعه و بهینه‌سازی پست‌ها می‌باشد. با توجه به اینکه

[1] Distribution Dispatching Center

تصمیم‌گیرنده نهایی در پستـها اپـراتـور می‌باشد، لذا داشتن اطلاعات لازم و کافی و به‌صورت لحظه‌ای و همچنین داشتن ابزارهای دقیق جهت تجزیه‌وتحلیل وقایع می‌تواند منجر به تصمیم‌گیری صحیح و عملاً برآورد نیازهای فوق باشد. تکنولوژی پست‌ها بخصوص در قسمت تجهیزات فشارقوی در سال‌های گذشته چندان تغییری نکرده است و علیرغم یکسان ماندن، روش‌های حفاظت، کنترل و نظارت با توجه به پیشرفت‌های حاصله در این زمینه کاملاً دگرگون‌شده است و این امر جز با اتوماسیون پست‌ها تحقق‌نیافته که در آن ریزپردازنده‌ها و کامپیوترها نقش بااهمیت و اساسی ایفا می‌کنند[۱۸].

## ۲-۴- تخمین حالت در سیستم‌های قدرت

تخمین حالت، عمل تخصیص مقدار به یک متغیر نامعلوم سیستم بر طبق معیاری بخصوص است که با استفاده از اندازه‌گیری از آن سیستم انجام می‌شود. معمولاً اندازه‌گیری، حالات ناقص و اضافی دارد و عمل تخمین حالات سیستم، بر اساس روش‌های آماری صورت می‌پذیرد که با حداکثر و یا حداقل معیاری بخصوص، مقادیر واقعی متغیرهای حالت تخمین‌زده می‌شوند. معیار رایج و آشنا این است که مجموع مربعات تفاوت بین مقادیر تخمینی و حقیقی حداقل شود.

ایده تخمین حالت بر اساس حداقل مربعات از اوایل قرن نوزدهم وجود داشته است. پیشرفت عمده در این زمینه در کاربرد آن در مسائل هوا–فضا در قرن بیستم اتفاق افتاده است. در این‌گونه کاربردها، مسئله عمده، شامل موقعیت‌یابی یک جسم فضایی(مانند موشک، هواپیما و غیره) و تخمین مسیر حرکت آن با توجه به اندازه‌گیری‌های ناقص و اضافی از بردار موقعـیـت و سرعت آن است. در بسیاری از کاربردها، این‌گونه اندازه‌گیری‌ها بر اساس مشاهدات و یا سیگنال‌های راداری است که ممکن است به اغتشاش آلوده و دارای خطاهای اندازه‌گیری باشد، تخمینگر حالات سیستم، ممکن است هم استاتیکی و هم‌دینامیکی باشد. هر دو نوع از این تخمین گرها برای سیستم‌های قدرت ایجادشده‌اند.

در سیستم‌های قدرت، متغیرهای حـالـت شامل مقادیر ولتاژ و زوایای نسبی فـاز در گره‌های سیستم می‌باشند. اندازه‌گیری‌هایی موردنیاز است تا بتوان عملکرد سیستم را در وضعیت بدون وقفه هم برای کنترل قابلیت اطمینان و هم برای قیود موجود در توزیع اقتصادی بار، تخمین زد. ورودی به

یک تخمینگر شامل اندازه‌گیری‌های ناقص از مقادیر ولتاژ و توان است. تخمین‌گر بدین‌صورت طراحی می‌شود که بهترین تخمین را از مقادیر ولتاژ و زوایای فاز در اختیار قرار دهد، با توجه به اینکه خطا در مقادیر اندازه‌گیری شده وجود دارد و این‌که ممکن است بعضی از اندازه‌گیری‌ها اضافی باشند. سپس اطلاعات خروجی از تخمین‌گر را در مراکز کنترل سیستم در مطالعه توزیع اقتصادی بار با در نظر گرفتن قابلیت اطمینان سیستم و نیز کنترل سیستم، بکار می‌برند.

همانطوریکه مسئله نظارت بر توان‌های انتقالی و ولتاژهای یک سیستم اهمیت ویژه‌ای دارد. تنها با مقایسه هر مقدار اندازه‌گیری شده با مقدار حد آن می‌توان به اپراتورهای سیستم اطلاع داد که آیا مشکلی در سیستم انتقال وجود دارد یا خیر به آن امید که آن‌ها بتوانند با انجام اعمال اصلاحی اضافه‌بار خطوط و یا ولتاژهای خارج از محدوده مجاز را برطرف نمایند.

در نظارت بر یک سیستم انتقال با مسائل بسیاری مواجه است. این مسائل عمدتاً از طبیعت مبدل-های اندازه‌گیری و از مشکلات مخابراتی و ارسال مقادیر اندازه‌گیری شده به مرکز کنترل ناشی می-شود. مبدل‌ها مانند هر وسیله اندازه‌گیری، دارای خطا هستند. اگر خطاها کم باشند ممکن است کشف نشوند و تنها باعث تفسیر نادرست مقادیر شوند. به‌علاوه مبدل‌ها ممکن است دارای خطای فاحش اندازه‌گیری باشند به‌گونه‌ای که خروجی آن‌ها غیرقابل استفاده باشد. به‌عنوان‌مثال زمانی که مبدل به‌صورت معکوس متصل شود که مقادیر را با علامت منفی نشان دهد. به این دلیل است که روش‌های تخمین حالت در سیستم‌های قدرت ایجادشده است. همچنان که مشخص می‌شود، یک تخمین گر حالت قادر است خطاهای کوچک تصادفی را صاف کند، خطاهای فاحش را تشخیص داده و آشکار نماید و سرانجام اطلاعاتی را که به علت قطع خطوط ارتباطی دریافت نشده است با مقادیر مناسب پر کند. آنچه لازم است انجام شود آن است که اطلاعات دریافتی از هر اندازه‌گیری به‌منظور بهترین تخمین از مقادیر واقعی زوایا، توان‌های انتقالی خطوط، بار و تولید شین‌ها مورداستفاده واقع شود.

به‌طورکلی متغیرهای حالت در یک سیستم قدرت شامل مقادیر ولتاژ و زوایای فاز تمام شین‌ها به‌جز یک شین است. زاویه فاز شین مبنا را معمولاً مساوی صفر گرفته می‌شود. البته در صورت تمایل

می‌توان از مؤلفه‌های حقیقی و موهومی ولتاژ شین استفاده کرد. می‌توان با استفاده از اندازه‌گیری‌ها، یکی از حالت‌های سیستم را تخمین زد، در این صورت سایر مقادیر لازم را می‌توان محاسبه کرد. پیش‌فرض این است که پیکربندی شبکه را نیز بدانیم. اتوترانسفورماتورهای دارای کنترل اتوماتیک اتصالات سر سیم‌پیچی و یا تنظیم‌کننده‌های زوایای فاز در اغلب شبکه‌ها یافت می‌شوند و وضعیت اتصالات سر آن‌ها را نیز می‌توان به‌عنوان مقادیر اندازه‌گیری شده از طریق کانال‌های دورسنجی به مرکز کنترل ارسال کرد. به‌عبارت‌دیگر باید وضعیت آن‌ها را نیز به‌عنوان حالت‌های سیستم در نظر گرفت چراکه جهت محاسبه توان‌های انتقالی ترانسفورماتورها و تنظیم‌کننده‌ها، دانستن آن‌ها ضروری است[۱۷-۱۸].

به‌طورکلی تخمین حالت شامل توابعی به شرح زیر است[17]:

- ✓ **پردازنده‌ی توپولوژی:** اطلاعات موقعیت بریکرها و سوئیچ‌ها را جمع‌آوری کرده و دیاگرام تک‌خطی(توپولوژی) سیستم را تنظیم می‌کند.
- ✓ **تجزیه‌وتحلیل رؤیت پذیری:** امکان حل شدن تخمین حالت را برای مجموعه اندازه‌گیری-های در دسترس مشخص می‌کند و شاخه مشاهده ناپذیر و جزایر مشاهده‌پذیر را در صورت وجود در سیستم، شناسایی می‌کند.
- ✓ **حل تخمین حالت:** بهترین تخمین از دامنه ولتاژ و فاز باس‌ها را با استفاده از مدل شبکه و مجموعه اندازه‌گیری‌های در دسترس ارائه داده و همچنین بهترین تخمین را برای همه جریانات خط، بارها، تپ‌های ترانسفورماتور و خروجی‌های ژنراتور فراهم می‌کند.
- ✓ **پردازش داده بد:** شناسایی و حذف اطلاعات بد از مجموعه اندازه‌گیری در دسترس.
- ✓ **پردازش خطای ساختاری و پارامتر(خطای توپولوژی):** پارامترهای مختلف شبکه، ازجمله پارامترهای مدل خط انتقال، پارامترهای ترانسفورماتور با تپ متغیر، خازن موازی و یا پارامترهای سلف را تخمین می‌زند و خطاهای ساختاری در پیکربندی شبکه را تشخیص داده و موقعیت بریکرهای نادرست را شناسایی می‌کند

## ۲-۴-۱- راه‌های حل تخمین حالت

با توجه به تابع اندازه‌گیری که حالت سیستم و اندازه‌گیری را مدل می‌نماید، دو راه برای اجرای تخمین حالت وجود دارد: ۱) تخمین حالت DC و ۲) تخمین حالت ACالبته تزریق داده‌های اشتباه در هر دو تخمین حالت DC و AC ممکن است رخ دهد.

### ۲-۴-۱-۱- تخمین حالت DC

تخمین حالت DC بر اساس تابع اندازه‌گیری خطی به‌صورت زیر می‌باشد:

$$z = Hx + e \qquad (۱-۲)$$

$z \in \mathbb{R}^{m\times 1}$ بردار اندازه‌گیری است که شامل m اندازه‌گیری می‌باشد. این m اندازه‌گیری شامل توان اکتیو تزریقی در باس‌ها و توان اکتیو عبوری در خطوط انتقال می‌باشد. $x \in \mathbb{R}^{n\times 1}$ بردار حالت سیستم می‌باشد.

در تخمین حالت dc، $x$ شامل زوایای فاز در تمام باس‌ها به‌جز باس اسلک می‌باشد که در این زاویه فاز برابر صفر تنظیم‌شده است. ماتریس $H \in \mathbb{R}^{m\times n}$ تابع اندازه‌گیری خطی می‌باشد. H با توجه به ساختار فیزیکی شبکه قدرت تعیین می‌گردد. $e \in \mathbb{R}^{m\times 1}$ بردار خطاهای اندازه‌گیری می‌باشد[۳۵-۳۶].

در تخمین حالت DC فرض می‌شود که تمامی اندازه‌های ولتاژ باس برابر یک است.همچنین تمامی المان‌های موازی و مقاومت شاخه‌ها قابل صرف‌نظر است(ناچیز است).

توان اکتیو انتقالی بین باس‌های i و j توسط رابطه‌ی $P_{ij} = (\theta_i - \theta_j)/x_{ij}$ محاسبه می‌گردد که در آن $x_{ij}$ راکتانس شاخه‌ی بین باس i و j، $\theta_i$ و $\theta_j$ به ترتیب زاویه‌ی فاز باس i و j می‌باشد و توان تزریقی به باس i توسط رابطه $P_i = \sum_j P_{ij}$ محاسبه می‌گردد.[۳۵,۳۰].

### ۲-۴-۱-۲- تخمین حالت AC

برخلاف تخمین حالت DC، تخمین حالت AC از یک تابع غیرخطی بین اندازه‌گیری‌ها و حالت سیستم استفاده می‌نماید. در تخمین حالت AC تابع اندازه‌گیری غیرخطی به‌صورت زیر نشان داده می‌شود:

$$z = H(x) + e \qquad (۲-۲)$$

که در آن $H()$ یک تابع غیرخطی بین بردار اندازه‌گیری $z$ و بردار حالت سیستم $x$ می‌باشد.

در تخمین حالت AC، متغیرهای حالت سیستم شامل زاویه فاز و دامنه‌های ولتاژ باس‌ها هستند. در تخمین حالت AC، اندازه‌گیری‌ها شامل توان‌های حقیقی و موهومی تزریقی و توان‌های حقیقی و موهومی انتقالی می‌باشد. که توسط روابط زیر محاسبه می‌گردد [۳۵,۳۰].

**۱) توان اکتیو و راکتیو تزریقی در باس iام**

$$P_i = V_i \sum_{j \in \Omega_i} V_j \left( G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij} \right) \qquad (۲-۲)$$

$$Q_i = V_i \sum_{j \in \Omega_i} V_j \left( G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij} \right) \qquad (۲-۳)$$

**۲) توان اکتیو و راکتیو انتقالی از باس iام به باس jام**

$$P_{ij} = V_i^2 \left( g_{si} + g_{ij} \right) - V_i V_j \left( g_{ij} \cos\theta_{ij} + b_{ij} \sin\theta_{ij} \right) \qquad (۲-۴)$$

$$Q_{ij} = -V_i^2 \left( b_{si} + b_{ij} \right) - V_i V_j \left( g_{ij} \sin\theta_{ij} - b_{ij} \cos\theta_{ij} \right) \qquad (۲-۵)$$

که این روابط داریم:

$V_i$ ولتاژ در باس i

$\theta_i$ زاویه فاز در باس i

$\theta_{ij}$ $\theta_i - \theta_j$

$G_{ij} + jB_{ij}$ ادمیتانس خط بین باس i و باس j

$g_{si} + jb_{si}$ ادمیتانس شاخه شنت در باس i

$\Omega_i$ مجموعه باس‌های متصل به باس i

## ۲-۵- داده های بد

هر نوع اطلاعات نادرستی که به تخمینگر تزریق می‌شود، داده بد می‌گویند. یکی از توابع اصلی تخمینگر حالت، تشخیص داده‌های بد، شناسایی و حذف آن‌ها در صورت ممکن می‌باشد. اندازه‌گیری‌ها ممکن است شامل خطاهایی به دلایل مختلف باشند. خطاهای تصادفی معمولاً به علت دقت محدود وسایل اندازه‌گیری و ادوات ارتباطی در اندازه‌گیری‌ها به وجود می‌آیند. اگر به‌اندازه کافی اندازه‌گیری وجود داشته باشد، چنین خطاهایی توسط تخمینگر حالت فیلتر می‌شود. نحوه این فیلتر کردن به روش مورداستفاده برای تخمین حالت بستگی خواهد داشت.

همچنین خطاهای اندازه‌گیری بزرگ می‌توانند در دستگاه‌های اندازه‌گیری که تحت تأثیر دیگر عوامل قرار دارند یا خراب‌شده‌اند و یا اتصالات در آن‌ها اشتباه بوده است، رخ بدهند. همچنین خرابی-های سیستم‌های ارتباطاتی و نویز ایجادشده به دلیل تداخلات غیرمنتظره نیز می‌توانند منجر به انحرافات بزرگ و خطاها در ثبت اندازه‌گیری‌ها شوند[۱۷].

علاوه بر موارد فوق، یک تخمینگر حالت ممکن است توسط اطلاعات توپولوژی غلط که به‌عنوان داده بد در تخمینگر حالت شناخته می‌شود، فریب بخورد و دچار اشتباه شود. مدیریت چنین حالت‌هایی پیچیده بوده و اصلاح خطاهای توپولوژی به‌طور مجزا در مبحث جداگانه‌ای قابل‌بحث بوده که از حوصله این پژوهش خارج می‌باشد.

برخی از داده‌های بد، قابل‌شناسایی و تشخیص بوده و می‌توان قبل از تخمین حالت آن‌ها را توسط برخی تست‌های معمول شناسایی و حذف نمود. اندازه‌های ولتاژ منفی، اندازه‌گیری‌ها با چندین مرتبه بزرگ‌تر یا کوچک‌تر از مقادیر قابل‌انتظار، یا تفاوت زیاد بین جریان ورودی و خروجی یک گره در داخل پست نمونه‌هایی از چنین داده‌های بد هستند. متأسفانه، تمام انواع داده بد به‌راحتی توسط چنین روش‌هایی قابل آشکارسازی نیستند؛ بنابراین، تخمینگرهای حالت باید مجهز به ویژگی‌های

پیشرفته‌تری باشند تا بتوانند هر نوع داده بدی را تشخیص داده و شناسایی نمایند[۱۷]. نحوه تشخیص و اصلاح داده بد، به روش تخمین حالت مورداستفاده بستگی دارد که مروری مختصر بر برخی از روش‌ها صورت می‌گیرد.

وقتی‌که از روش تخمین WLS استفاده می‌شود، عملیات تشخیص و شناسایی داده بد تنها بعد از فرآیند تخمین حالت توسط پردازش باقی‌مانده مقادیر اندازه‌گیری صورت می‌گیرد. به‌طورکلی تجزیه‌وتحلیل موردنظر مبتنی بر ویژگی‌های باقی‌مانده‌های مذکور شامل توزیع‌های احتمالی امید ریاضی آن‌ها می‌باشد.

داده بد ممکن است در روش‌های متفاوت بسته به نوع، مکان و تعداد اندازه‌گیری‌هایی که دارای خطا می‌باشند، ظاهر شود. این داده‌ها می‌توانند به‌طورکلی به‌صورت ذیل دسته‌بندی شوند:

۱-داده بد منفرد: فقط یک اندازه‌گیری در کل سیستم دارای خطای بزرگ می‌باشد.

۲-داده بد چندگانه: بیش از یک اندازه‌گیری در سیستم خطا خواهد داشت.

داده بد چندگانه ممکن است در اندازه‌گیری‌هایی رخ دهد که باقیمانده آن‌ها همبستگی قوی و یا ضعیفی دارند. اندازه‌گیری‌هایی که دارای همبستگی قوی هستند، خطاهای آن‌ها دیگر مقادیر تخمینی اندازه‌گیری‌ها را به‌شدت تحت تأثیر قرار می‌دهد و موجب می‌شود که داده‌های خوب دارای خطا بوده درحالی‌که داده‌های بد دارای خطاهای بزرگ می‌باشند. اندازه‌گیری‌هایی با همبستگی ضعیف، اثرات خطای آن‌ها بر روی یکدیگر ناچیز می‌باشد. زمانی که باقی‌مانده اندازه‌گیری‌ها دارای همبستگی قوی هستند، خطاهای آن‌ها ممکن است دارای تطابق باشند و یا نباشند. خطاهای هماهنگ، خطاهایی هستند نسبت به یکدیگر سازگاری و تطابق دارند. بنابراین داده بد چندگانه به سه گروه دسته‌بندی می‌شوند:

۱-داده بد چندگانه غیرمتعامل(روی‌هم اثری ندارند): داده بد در اندازه‌گیری‌هایی که باقی‌مانده آن‌ها همبستگی ضعیفی دارند.

۲-داده بد چندگانه متعامل ناهماهنگ: داده بد ناهماهنگ در اندازه‌گیری‌هایی که همبستگی قوی دارند.

۳-داده بد متعامل هماهنگ: داده بد سازگار در اندازه‌گیری‌هایی که همبستگی قوی دارند.

ارزیابی درجه تعامل بین اندازه‌گیری‌ها و تجزیه‌وتحلیل خطاها بر اساس حساسیت باقیمانده‌های اندازه‌گیری نسبت به خطاهای اندازه‌گیری قابل انجام است[۱۷].

## ۲-۵-۱- طبقه‌بندی اندازه‌گیری‌ها

سیستم‌های قدرت ممکن است دارای انواع مختلف دستگاه‌های اندازه‌گیری باشند که به‌طور گسترده در سیستم پخش‌شده و هیچ الگوی توپولوژی واضحی ندارند. این اندازه‌گیری‌ها خصوصیات متفاوتی دارند و خروجی‌های آن‌ها بسته به مقدار و موقعیت آن‌ها تخمین حالت سیستم را تحت تأثیر قرار می‌دهد. بنابراین، تخمین حالت نه‌تنها به مقدار اندازه‌گیری شده، بلکه به مکان اندازه‌گیری هم وابسته می‌باشد. همچنین، این مقادیر اندازه‌گیری شده ممکن است به یک یا چند دسته زیر تعلق داشته باشند:

- **اندازه‌گیری بحرانی:** اندازه‌گیری بحرانی، اندازه‌گیری است که با حذف آن از مجموعه مقادیر اندازه‌گیری، سیستم مشاهده ناپذیر می‌شود. ستون ماتریس کوواریانس باقی‌مانده $\Omega$ متناظر با یک اندازه‌گیری بحرانی برابر با صفر خواهد بود. بعلاوه، باقی‌مانده یک اندازه‌گیری بحرانی همیشه صفر است.

- **اندازه‌گیری اضافی(غیر بحرانی):** اندازه‌گیری اضافی، اندازه‌گیری هست که بحرانی نباشد. فقط اندازه‌گیری‌های اضافی دارای باقی‌مانده غیر صفر می‌باشند.

- **زوج بحرانی:** دو اندازه‌گیری اضافی که حذف هم‌زمان آن‌ها از مجموعه مقادیر اندازه‌گیری شده، سیستم را رؤیت ناپذیر می‌کند.

- **مجموعه Kتایی بحرانی:** یک مجموعه Kتایی بحرانی شامل Kتا اندازه‌گیری اضافی می‌باشد که حذف هم‌زمان تمام آن‌ها سیستم را مشاهده ناپذیر خواهد کرد. هیچ مجموعه Kتایی بحرانی اندازه‌گیری شامل یک زوج و یا مجموعه بحرانی مرتبه پایین‌تر از خود نمی‌باشد. این K تا ستون از ستون ماتریس کوواریانس باقی‌مانده $\Omega$، با توجه به با Kتای بحرانی به‌صورت خطی‌وابسته می‌باشند[۱۷].

## ۲-۵-۲- انواع داده‌های بد در سیستم قدرت

داده‌های بد در یک سیستم می‌تواند ناشی از عوامل زیر باشد[۳۰]:

**- داده بد ناشی از خطاهای توپولوژی:**

SE با مدل الکتریکی که توسط پردازشگر توپولوژی(TP[1]) به دست می‌آید، عملیات خود را انجام می‌دهد. به‌عبارت‌دیگر، TP مدل تفصیلی بخش/سویچ باس را به مدل فشرده‌تر و مفیدتر باس/شاخه تبدیل می‌نماید. لازم به ذکر است که در این فرآیند، برخی اندازه‌گیری‌ها باید نادیده گرفته شوند(همانند پخش بار توسط CBها) درحالی‌که موارد دیگر در یک نقطه اندازه‌گیری واحد(همانند سنجش تزریق چندین مقطع باس و گردآوری آن‌ها در یک باس واحد الکتریکی) ادغام می‌شوند. یک CB باوجود چندین سوئیچ ایزوله، شامل یک یا چند وضعیت منطقی می‌باشد.

اغلب وضعیت صحیح تمامی CBها در سیستم شناخته‌شده می‌باشد. اما در بعضی مواقع، وضعیت یک CB مشخص ممکن است اشتباه باشد. این امر هنگامی رخ می‌دهد که بعضی از سوییچ‌های ایزوله، اندازه‌گیری نشده یا از راه دور عمل نکردند و نقص پیداکرده‌اند. دلایل دیگر مانند بریکری که توسط تیم تعمیرکاری در حال تعمیر بوده و گزارش نشده- قطع یک خط یا ترانسفورماتور- جدا شدن باس و یا خطای مکانیکی دستگاه‌های سیگنال دهنده و ... می‌باشد. در چنین مواقعی TP با CBی روبرو می‌شود که وضعیت آن نامشخص می‌باشد. در چنین مواقعی، TP باید مشابه‌ترین وضعیت نزدیک به وضعیت

[1] Topology Processor

CB را که درگذشته برای همان بریکر ثبت‌شده است و یا با استفاده از مقادیر مرتبط با اندازه‌گیری‌ها تصمیم بگیرد. بنابراین امکان انتخاب وضعیت اشتباه برای CB، اجتناب‌ناپذیر است.

هنگامی‌که این اتفاق روی می‌دهد، مدل باس/شاخه تولیدی توسط TP اشتباه بوده و منجر به خطای توپولوژی می‌گردد. بنابراین همان‌گونه که از عنوان آن مشخص است، این خطا مربوط به شرایط فیزیکی سیستم است.

برخلاف خطاهای پارامتری، اغلب این خطاها تا زمانی که از مقدار آستانه تجاوز صورت نکند، ناشناخته باقی می‌مانند. خطاهای توپولوژی معمولاً موجب می‌شوند که SE به‌طور قابل‌ملاحظه‌ای دچار مشکل گردد. درنتیجه این خطاهای توپولوژی باعث می‌شود که فرآیند تشخیص داده بد مختل شده و بعضی از داده‌های صحیح و آنالوگ را نیز به‌عنوان داده بد تشخیص دهد. لذا با توجه به فرآیند تشخیص داده بد، این داده از مجموعه داده‌ها حذف‌شده(درحالی‌که نباید حذف شود) و دوباره الگوریتم تخمین حالت اجراشده و درنتیجه تخمینگر، تخمین اشتباهی ارائه می‌دهد و یا واگرا خواهد شد. قابل‌ذکر است که برای تشخیص این نوع از داده‌ها نیز می‌توان روش خاصی ارائه داد. ولی در وهله اول باید خطای توپولوژی کنترل شود. بنابراین لازم است که یک مکانیزم پیشرفته‌ای برای تشخیص و شناسایی این خطاهای بد بکار گرفته شود[۱۷].

**- داده بد ناشی از خطای اندازه‌گیری:**

خطاهای ناشی از دقت محدود دستگاه‌های اندازه‌گیری، خرابی دستگاه‌ها، قطع خطوط ارتباطی ارسال اطلاعات و نویز در سیستم مخابراتی، ازجمله خطاهای اندازه‌گیری هستند.

**- داده‌های بد ناشی از حملات مخرب که به حملات سایبری مشهور است که در شبکه هوشمند اتفاق می‌افتد:**

این حالت تنها در شبکه هوشمند رخ می‌دهد، ولی دو حالت قبلی چه شبکه هوشمند باشد و یا شبکه سنتی، امکان رخ دادن آن‌ها وجود دارد. همچنین قابل‌ذکر است که عامل اول مقوله‌ای جدا بوده و در تابع مربوط به پردازش داده بد بررسی نمی‌گردد، بلکه در تابع پنجم

موردبررسی قرار می‌گیرد، لذا از بحث در مورد این نوع از داده‌های بد و روش‌های تشخیص آن، خودداری می‌شود. واضح است که در شبکه‌های هوشمند تمام دستگاه‌ها، IP مخصوص خود را دارا می‌باشند، لذا ممکن است مصرف‌کنندگان به اطلاعات مصرف توان خود و همچنین کنترل آن از طریق وب دسترسی داشته باشند. این مسیر دوطرفه احتمال آسیب-پذیری را فراهم می‌کند. و یا مهاجم ممکن است از طرق غیرقابل‌پیش‌بینی به شبکه نفوذ کند و از طریق دستیابی به نرم‌افزار شبکه، بار را تغییر دهد تا شبکه را به حالت ناپایداری سوق دهد. بنابراین با توجه به گسترش شبکه‌های هوشمند و رویکرد شرکت‌های برق بر این امر، لازم است که مطالعات بسیاری در این زمینه نیز صورت گیرد تا راهکارهایی جهت تشخیص و شناسایی این داده‌ها ارائه گردد. این مورد موضوع موردبحث در این پژوهش بوده که در فصل آتی بیشتر بر روی آن بحث می‌شود. در بخش بعدی برخی از روش‌های رایج تشخیص و شناسایی داده بد به‌طور مختصر بیان می‌گردند.

### ۲-۵-۳- روش‌های رایج تشخیص و شناسایی داده بد

تشخیص، اشاره به این دارد که مجموعه اندازه‌گیری شده شامل داده بد می‌باشد یا خیر. شناسایی، فرآیند یافتن دستگاه اندازه‌گیری خاص حاوی داده بد می‌باشد. تشخیص و شناسایی داده بد به ساختار تمام اندازه‌گیری‌ها در یک سیستم قدرت معین وابسته می‌باشد.

داده بد در صورتی تشخیص داده می‌شود که حذف اندازه‌گیر متناظر آن، سیستم را رؤیت ناپذیر نکند. به‌عبارت‌دیگر، داده بدی که در اندازه‌گیری‌های بحرانی ظاهر شود، قابل‌تشخیص نیست.

یک اندازه‌گیری منفرد شامل داده بد تنها در صورتی قابل‌تشخیص است که:

- اندازه‌گیری بحرانی نباشد.
- متعلق به جفت بحرانی نباشد.

منطق پردازش داده بد باید توانایی تشخیص محدودیت ذاتی مذکور در تشخیص و شناسایی داده بد منفرد را داشته باشد. درصورتی‌که شرایط مذکور در نظر گرفته شود، داده بد منفرد می‌تواند توسط

روش‌هایی که تاکنون ارائه‌شده و در ادامه به‌صورت خلاصه ارائه خواهد شد، تشخیص داده‌شده و شناسایی شوند. تشخیص حالت داده بد چندگانه خیلی مشکل‌تر می‌باشد و روش‌های تشخیص آن‌ها نیز متفاوت است[۱۷].

برای یافتن داده بد ناشی از عامل اول، روش‌های خاصی وجود دارد که خارج از بحث این مقاله است.. اما برای تشخیص داده بد ناشی از عامل دوم، روش‌های مختلفی ازجمله WLS ،LAV، Mوجود دارد که به روش‌های مرسوم مشهور می‌باشد. برای تشخیص داده بد ناشی از عامل سوم، روش‌های زیادی در مقالات متفاوت ارائه‌شده است و روش‌های مرسوم قادر به تشخیص این نوع از داده‌ها نیستند، چراکه این داده‌ها کاملاً هوشمند بوده و با داشتن اطلاعات پیکربندی سیستم، به‌گونه‌ای داده‌ها را تغییر می‌دهند که روش‌های مرسوم قادر به تشخیص نیستند. بااین‌وجود برخی از روش‌های مرسوم تشخیص و شناسایی داده بد به شرح ذیل می‌باشد:

### ۲-۵-۳-۱- روش حداقل مربعات وزندار

### ۲-۵-۳-۱-۱- روش‌های تشخیص داده بد در WLS

- **آزمون توزیع مربع کای($x^2$):** آزمون مربعات کای برای داده بد، بر مبنای مشخصات توزیع $X^2$ ساخته می‌شود. در این روش ،مجموعه N متغیر تصادفی مستقل بر اساس توزیع نرمال استاندارد تعریف‌شده و تابع $f(x)$ دارای توزیع $x^2$ با $m-n$ درجه آزادی می‌باشد.

در یک سیستم قدرت حداقل $n$ اندازه‌گیری باید وجود داشته باشند تا تعادل روابط توان برقرارشده و اغلب $m-n$ خطاهای اندازه‌گیری به‌صورت مستقل خطی می‌باشند. بنابراین بیشترین درجه آزادی $m-n$ است که این امر، نشان‌دهنده اختلاف بین تعداد کلی اندازه‌گیری‌ها و حالات سیستم می‌باشد.

تابع هدف تخمین حالت WLS، ($J(x)$)، برای تقریب تابع $f(x)$ و تست تشخیص داده بد مورداستفاده قرار می‌گیرد. بنابراین تست توزیع $x^2$ برای تشخیص داده بد شامل مراحل: ۱) حل مسئله تخمین WLS و محاسبه تابع هدف، ۲) یافتن مقادیر جدول توزیع مربع کای

مربوطه برای تشخیص میزان احتمال و درجه آزادی، ۳) اگر $J(x) \geq x^2_{(m-n),p}$، وجود داده بد مشکوک می‌باشد[۱۷].

- **آزمون باقی‌مانده نرمالایز شده:** تست $X^2$ به دلیل استفاده از تقریب خطاهای اندازه‌گیری دارای دقت کمی می‌باشد. بنابراین ممکن است در پیدا کردن دادهٔ بد در موارد خاص، درست عمل نکند. روش باقی‌مانده‌های نرمالایز شده آزمون دقیق‌تری برای تشخیص دادهٔ بد می‌باشد. مقادیر نرمالایزه شدهٔ باقی‌مانده برای اندازه‌گیری i را می‌توان با استفاده از تقسیم قدر مطلق آن بر عنصر متناظر قطری آن در ماتریس کوواریانس باقیمانده، به دست آورد. بردار باقیمانده نرمالایزشده ($r^N$) دارای توزیع نرمال می‌باشد. بنابراین بزرگ‌ترین عنصر $r^N$ را می‌توان با یک مقدار آستانه پیش‌فرض مقایسه نمود تا از وجود داده بد اطلاع حاصل کرد. این مقدار آستانه با توجه به سطح موردنظر و حساسیت مرحله تشخیص تعیین می‌گردد[۱۷].

### ۲-۵-۳-۱-۲- روش‌های شناسایی داده بد در WLS

پس از تشخیص دادهٔ بد در مجموعهٔ اندازه‌گیری‌ها، با پردازش بیشتر بر روی باقیمانده‌ها می‌توان آن‌ها را شناسایی نمود. شناسایی داده بد نیز همانند روش‌های تشخیص، از باقیمانده‌ها استفاده می‌کند، اما باکمی پردازش بیشتر بر روی آن‌ها. از بین روش‌های موجود، دو مورد مشهورتر بوده که در مرجع [۱۷] نیز ارائه‌شده است.

- **آزمون بزرگ‌ترین باقیمانده نرمالایز شده($r^N_{max}$):** ویژگی‌های باقیمانده‌های نرمالایز شده برای یک دادهٔ بد موجود در مجموعهٔ اندازه‌گیری‌ها را می‌توان برای ایجاد یک آزمون برای شناسایی و متعاقباً از بین بردن دادهٔ بد، استفاده نمود. این آزمون به بزرگ‌ترین باقی‌ماندهٔ نرمالایز شده(آزمون $r^N_{max}$ ) اشاره دارد و شامل مراحل زیر است: ۱) حل مسئله تخمین WLS و به دست آوردن عناصر بردار باقیمانده مقادیر اندازه‌گیری شده، ۲) محاسبهٔ باقیمانده‌های نرمالایز شده، ۳) یافتن k بدین‌صورت که $r^N_k$ بزرگ‌ترین مقدار در میان تمام $r^N_i, i =$ 1, … , $m$ها باشد، ۴) اگر $r^N_k > c$، آنگاه kامین اندازه‌گیری به‌عنوان دادهٔ بد مشکوک می‌باشد.

در غیراینصورت، فرآیند متوقف‌شده و هیچ داده بدی وجود ندارد، ۵) حذف کردن kامین اندازه‌گیری از مجموعهٔ مقادیر و برگشت به مرحلهٔ اول می‌باشد.

- **آزمون فرضیه شناسایی:** ضعف عمده روش $r_{max}{}^{N}$ این است که بر اساس باقیمانده‌هایی می‌باشد که به‌شدت به یکدیگر وابسته‌اند. ازاین‌رو در موارد داده بد چندگانه، این وابستگی ممکن است منجر به تولید مقادیر باقیمانده نسبتاً بزرگی برای داده‌های خوب و همچنین داده-های بد شود. یک‌راه تشخیص بین اندازه‌گیری خوب و بد، تخمین خطای اندازه‌گیری به‌صورت مستقیم به‌جای استفاده از آزمایش باقیمانده است. یکی از چنین روش‌هایی آزمون فرضیه شناسایی است. این روش با روش بزرگ‌ترین باقیمانده نرمالیزه شده که داده‌های بد را بر اساس تخمین محاسباتی خطای اندازه‌گیری شناسایی می‌کند، متفاوت است. تخمین تمامی خطاهای اندازه‌گیری با استفاده از محاسبه باقیمانده ممکن نمی‌باشد چراکه رتبه ماتریس $S$ کمتر از تعداد اندازه‌گیری‌های $m$ می‌باشد. درواقع برای یک سیستم با $n$ حالت، رتبه نمی‌تواند از $(m-n)$ بزرگ‌تر باشد. بنابراین حداکثر $(m-n)$ خطای اندازه‌گیری می‌تواند با استفاده از ماتریس کاهش‌یافته $S$ تخمین زده شود. ازاین‌رو کارایی این روش به این کاهش اولیه بستگی دارد، یعنی انتخاب یک مجموعه اندازه‌گیری مشکوک اولیه که شامل همه داده‌های بد باشد. روش آزمون فرضیه شناسایی از باقی‌مانده‌های نرمالیزه شده برای این انتخاب استفاده می‌کند و ازاین‌رو ممکن است یک یا چند مورد از داده‌های بد که باقیمانده نرمالیزه شده آن‌ها کوچک می‌باشد، نادیده گرفته شوند[۱۷].

اما روش‌های فوق مبتنی بر روش WLS می‌باشند. روش‌های دیگری نیز وجود دارند که مستحکم-تر از روش WLS بوده، اما دامنه آن‌ها بسیار فراگیر است و در مقالات متعدد ارائه‌شده‌اند. روش WLS بر اساس یک سری مفروضات در مورد خطاهای اندازه‌گیری فرمول‌بندی می‌شود. این خطاها به‌عنوان متغیرهای تصادفی مستقل توزیع‌شده بر اساس توزیع گاوسی با میانگین صفر و واریانس مشخص در نظر گرفته می‌شوند. اما خطاهایی که به علت عوامل دوم و سوم ایجاد می‌شوند نیاز به روش‌های

مستحکم‌تری برای تشخیص و شناسایی دارند که در ادامه به چند مورد به‌صورت خلاصه اشاره می-گردد:

### ۲-۵-۳-۲- تخمینگر M

این تخمینگر اولین بار توسط Huber برای تخمین حالت مستحکم مرکز توزیع ارائه شد و مبتنی بر رگرسیون می‌باشد. در کل تخمینگر M، یک تخمینگر مبتنی بر حداکثر درستنمایی می‌باشد. این روش یک تابع هدف را حداقل می‌کند که این تابع هدف به‌صورت تابعی از باقیمانده‌های اندازه‌گیری با توجه به محدودیت‌های روابط اندازه‌گیری تعریف می‌شود. در برخی منابع در ابتدا بیان‌شده است که تشخیص داده بد با تغییر الگوریتم تخمین که اندازه‌گیری‌های بد در طی فرآیند تخمین شناسایی و مشخص می‌شوند، باید صورت گیرد. این روش از تعداد زیادی تخمینگر M استفاده می‌کند. در [۱۷] تنها دو روش نیوتن و حداقل مربعات وزندار مجدد موردبررسی قرارگرفته است که اولی به محاسبه مشتقات اول و دوم $\rho$ نیاز دارد و دومی از محاسبه مشتق دوم خودداری نموده و بر اساس روش مبتنی بر تکرار حداقل مربعات وزندار مجدد می‌باشد.

### ۲-۵-۲-۳- تخمینگر LAV

در این روش مسئله تخمین حالت به‌عنوان یک مسئله برنامه‌ریزی خطی مدل شده که می‌تواند توسط یکی از روش‌های توسعه‌یافته حل LP حل شود. این روش خود شامل دو روش ساده و نقطه داخلی است. در این روش مسئله تخمین LAV در چهارچوب استاندارد LP مدل‌سازی شده و توسط یکی از دو روش فوق حل می‌گردد[۱۷].

روش‌های ۲-۵-۲-۲ و ۲-۵-۲-۳، نسبت به روش ۲-۵-۲-۱ در مقابل داده‌های بد مقاوم‌تر می-باشند. پس از شناسایی داده بد، داده بد باید قبل از تکرار(یا شروع سیکل) تخمین حالت، حذف شود. البته روش‌های بسیار دیگری نیز برای تشخیص و شناسایی داده بد در مقالات متعدد پیشنهادشده است که در بخش بعدی مروری بر برخی از آن‌ها صورت می‌گیرد.

## ۲-۶-مروری بر پیشینه تحقیق

در ابتدا مروری بر مطالعات انجام‌شده درزمینهٔ تخمین حالت صورت می‌گیرد:

- در مرجع [۱۹] نویسندگان برای تخمین حالت شبکه توزیع از الگوریتم کلونی مورچگان استفاده نموده‌اند.

- در [۲۰-۲۱] روشی ترکیبی بر اساس الگوریتم [۱]جهت تخمین حالت شبکه توزیع در حضور تولید پراکنده استفاده‌شده است.

- در [۲۲] روش تخمین حالت جدیدی ارائه‌شده است تا اندازه و زاویه فاز جریان در سیستم توزیع سه فاز را ارزیابی نماید. به عبارتی از سیستم فازی Takagi-Sugeno جهت تخمین حالت‌های سیستم در شرایط نامتعادلی فیدرها استفاده‌شده است.

- در [۲۳] روش دومرحله‌ای بر اساس تکنیک WLS[۲] جهت تخمین حالت فیدرهای جریان ارائه‌شده است که در آن زیرسیستم WLS معرفی‌شده و هر زیرسیستم به‌صورت انفرادی حل می‌گردد.

- در [۲۴] تخمین حالت سیستم قدرت با استفاده از روش پخش بار احتمالی صورت گرفته است.

- در [۲۵] روشی سنکرون شده برای تخمین حالت سیستم‌های سه فاز ارائه گردیده است که روش آن مبتنی بر الگوریتمHBMO[۳](بهینه‌سازی جفت‌گیری زنبورعسل) می‌باشد که هدف آن،افزایش دقت تخمین حالت در حضور DG در شبکه است. از الگوریتم HBMOبرای جستجوی پاسخ در فضای مسئله در سیستم سه فاز استفاده‌شده است.

- در [۲۶] برای حل مسئله تخمین حالت در سیستم‌های توزیع در حضور منابع تولید پراکنده و ادوات DFACTS از الگوریتم بهینه‌سازی تکامل دیفرانسیلی استفاده‌شده و با روش بهینه‌سازی ازدحام ذرات مقایسه شده است. برای شبیه‌سازی‌ها شبکه ۳۴ باسه IEEE مورداستفاده قرارگرفته

[1] Particle swarm optimization
[2] weighted least square
[3] Honey-bee mating optimization

است. نتایج بیانگر کارایی روش تکامل دیفرانسیلی در تخمین حالت سیستم‌های توزیع مجهز به ادوات گوناگون غیرخطی می‌باشد.

- در [۲۷] هدف از پژوهش انجام تخمین حالت در شبکه توزیع الکتریکی در حضور تجهیزات عملی مانند مولدهای پراکنده و جبران‌کننده‌های استاتیک می‌باشد. ویژگی‌های غیرخطی تجهیزات عملی مانند تولید پراکنده(DG) و جبران‌کننده‌های استاتیک(SVCs) در سیستم‌های توزیع باعث ناپیوسته و مشتق‌ناپذیرشدن تابع هدف برای تخمین حالت سیستم توزیع می‌شوند. روش‌های عمده تخمین حالت سیستم توزیع به دودسته تقسیم می‌شوند، روش‌های آماری و فرمول‌بندی تخمین حالت بار. معمولاً روش‌های سابق از روش‌های همگرایی تکراری مانند روش شبه نیوتنی استفاده می‌کردند و روش‌های جدیدتر از آنالیز حساسیت استفاده می‌کنند. ازآنجاکه روش‌های مرسوم تخمین حالت سیستم توزیع مربوط به هر دو دسته‌بندی می‌شوند، فرض می‌شود معادلات تابع هدف و معادلات مربوط به تخمین حالت سیستم توزیع پیوسته و مشتق‌پذیر باشند. بااین‌حال، با توجه به ویژگی‌های غیرخطی تجهیزات عملی در سیستم‌های توزیع، تابع هدف نمی‌تواند پیوسته و مشتق‌پذیر باشد و از روش‌های مرسوم نمی‌توان استفاده کرد. روش‌های هوشمند به‌عنوان ابزاری عملی برای بهینه‌سازی غیرخطی در نظر گرفته‌شده‌اند و مسئله‌ی تخمین حالت، حداقل کردن یک تابع هدف غیرخطی با در نظر گرفتن مجموعه‌ای از قیود نامساوی غیرخطی است و برای رسیدن به این هدف از روش بهینه‌سازی اجتماع ذرات(PSO) استفاده‌شده است. برای اثبات کارایی الگوریتم پیشنهادی، یک سیستم توزیع ۱۳ شینه عملی و سیستم آزمون توزیع ۳۴ شینه IEEE در نظر گرفته‌شده است.

- در [۲۸] ابتدا یک روش کارا، دقیق و سریع برای تخمین حالت سیستم‌های توزیع ارائه می‌شود. در این روش از الگوریتم تکاملی آموزش و یادگیری بهبودیافته استفاده‌شده است. عملکرد الگوریتم آموزش و یادگیری با اضافه نمودن جهشی بر مبنای تئوری موج کوچک و الگوریتم تکامل تفاضلی، بهبودیافته است. الگوریتم بهینه‌سازی پیشنهادی روی پنج تابع کلاسیک ارزیابی و نتایج با دو الگوریتم دیگر مقایسه شده است. پس‌ازآن، چگونگی به‌کارگیری این الگوریتم برای تخمین حالت سیستم‌های

توزیع توضیح داده می‌شود. این روش توانایی حل توابع غیرخطی، غیر محدب و متغیرهای گسسته را دارد. روش پیشنهادی برای تخمین حالت در سیستم‌های توزیع روی دو سیستم ۳۲ و ۸۳ باسه پیاده‌سازی و نتایج به‌دست‌آمده با الگوریتم‌های دیگر مقایسه شده است. از طرف دیگر افزایش استفاده از انرژی‌های نو باعث ایجاد عدم قطعیت در توان تولیدی آن‌ها می‌شود. لذا برای اعمال عدم قطعیت در مسئله تخمین حالت، ابتدا نحوه‌ی مدل‌سازی عدم قطعیت موجود در توان مصرفی بارها و توان تولیدی منابع انرژی‌های نو برای استفاده در تخمین حالت سیستم‌های توزیع ارائه و سپس چگونگی در نظر گرفتن این متغیرهای تصادفی در مسئله، مدل‌سازی و تخمین حالت احتمالاتی پیشنهادشده است. در انتها روش ارائه‌شده بر روی سیستم توزیع ۶۹ باسه پیاده‌سازی و نتایج به‌دست‌آمده مقایسه و تحلیل می‌شود.

در ادامه برخی از کارهای صورت گرفته درزمینه تشخیص تزریق داده بد موردبررسی قرار می‌گیرد:

- در [۲۹] تشخیص حملات تزریق داده بد با استفاده از روش مبتنی بر حفاظت انتخاب استراتژیک مجموعه سنسورهای اندازه‌گیری و روش اندازه‌گیری و انتخاب استراتژیک مستقل مقادیر متغیرهای حالت صورت گرفته است. این روش‌ها در تخمین حالت DC پیاده‌سازی شده است. نتایج نشان می‌دهند که حفاظت از مجموعه اندازه‌گیری‌های اساسی برای تشخیص چنین حملاتی لازم و کافی می‌باشد.

- در [۳۰] مسئله تشخیص داده بد به‌صورت مسئله‌ای با ماتریس جداگانه در نظر گرفته‌شده است. در این پژوهش با توجه به اندازه‌گیری‌های موقت و اساسی با تعداد بعد کم در حالات سیستم قدرت و طبیعت پراکنده حملات تزریق داده بد، روشی جدید مبتنی بر جداسازی متغیرهای حالت نامی و غیرمتعارف سیستم قدرت ارائه‌شده است. برای حل مسئله از دو روش قانون بهینه‌سازی اتمی و فاکتورگیری از ماتریس با مرتبه کم استفاده‌شده است. نتایج شبیه‌سازی نشان می‌دهند که روش‌های

ارائه‌شده به‌خوبی می‌توانند حالات بهره‌برداری سیستم قدرت و همچنین حملات مشکوک را مشخص نمایند حتی اگر داده‌های اندازه‌گیری شده کامل نباشد.

- در [۳۱] نوع جدیدی از حملات تزریق داده بد ارائه‌شده است که در آن مخربان می‌توانند ساختار سیستم را استخراج نموده تا چنین حملاتی را صورت داده و با دور زدن روش‌های موجود تشخیص داده بد خطاهای ساختگی را ایجاد نمایند. همچنین دو سناریو از حملات واقعی ترتیب داده‌شده است که در آن‌ها مخرب می‌خواهد برخی ادوات مشخص(بسته به نوع حفاظت آن‌ها) را تخریب نماید و یا منابع موجود را جهت عملکرد نامناسب محدود نماید. همچنین مشاهده‌شده است که مخرب می‌تواند بردارهای حمله را ایجاد نموده تا هم نتایج تخمین حالت و هم روش‌های قراردادی را تغییر دهد. نتایج نشان می‌دهد که باوجوداین حملات باید ساختار حفاظتی و امنیتی سیستم قدرت در برابر حملات مورد بازبینی قرار گیرد.

- در [۳۲] بررسی کلی پیرامون استراتژی حفاظتی و نحوه یافتن حملات پراکنده و دستگاه‌های اندازه‌گیری امن صورت گرفته است. سپس با توجه به تأثیر تزریق داده بد، دو روش تشخیص حملات تزریق داده بد بر اساس توزیع‌های متغیرهای حالت ارائه‌شده است. به عبارتی مسئله به‌صورت یک تست فرضی از توزیع نرمال استاندارد با داده فرضی فرمول‌بندی می‌شود. نتایج از عملکرد مناسب روش ارائه‌شده حکایت دارد.

- در [۳۳] با توجه به متمرکز بودن روش‌های فعلی برای دفع حملات تزریق داده بد و گران بودن اجرای آن‌ها و همچنین عدم ایجاد امنیت کامل در برابر حملات سایبری در شبکه‌های هوشمند، روشی تشخیصی مبتنی بر مشارکت hostهای توزیع‌شده ارائه‌شده است. در این پژوهش از الگوریتم انتخاب اکثریت بر اساس قانون برای تشخیص داده‌های بد ارسالی توسط PMUها استفاده‌شده است. همچنین سیستمی جدید با الگوریتم به‌روزرسانی متفاوت طراحی‌شده است تا وضعیت کلی PMUها ارزیابی‌شده و حملات داده بد به‌طور واضح مشخص گردد. نتایج از عملکرد مناسب روش پیشنهادی حکایت دارد.

- در [۳۴] روشی مبتنی بر ماشین آموزش بزرگ بهبودیافته(Improved ELM) برای تشخیص حملات داده بد ارائه‌شده است. برای افزایش دقت و بهبود عملکرد تشخیص از الگوریتم‌های کلونی زنبورعسل و تکامل تفاضلی تواما جهت بهینه‌سازی استفاده‌شده است. همچنین از Autoencoder برای کاهش بعد داده اندازه‌گیری شده که داده‌ها را به‌خوبی با بعد کامل نمایش می‌دهد استفاده‌شده است. روش پیشنهادی به‌خوبی و با دقت کامل توانسته است حملات تزریق داده بد را تشخیص دهد.

- در [۴۱] آسیب‌پذیری بازار انرژی محلی از حملات تزریق داده اشتباه در یک ریز شبکه هوشمند مسکونی موردبررسی قرارگرفته و تأثیر این حملات بر سود و درآمدهای مالی مشترکین مطرح گردید. در یک بازار انرژی محلی، مهاجم می‌تواند به الگوهای تولید و مصرف انرژی صحیح مشترکین دست‌یافته و براین اساس سیگنال حمله خود را به‌منظور به دست آوردن ماکزیمم سود از خرید/فروش انرژی بهینه نماید که بدین ترتیب تعادل تولید-تقاضا نیز پابرجا مانده و حمله نامشخص می‌باشد. بدین منظور یک مسئله بهینه‌سازی از مهاجم فرمول‌بندی شده تا ماکزیمم سود ممکن از مشترکین واقعی به دست آید. نتایج نشان می‌دهد که تزریق داده اشتباه موجب کاهش تا حدود ۹۰ درصدی سود مشترکین در برخی ساعات مشخص می‌شود.

- در [۴۲] مروری جامع بر حملات تزریق داده اشتباه که نوعی حمله سایبری می‌باشد در سیستم‌های قدرت مدرن از سه دیدگاه صورت گرفته است: مدل‌های حملات، تأثیر آن‌ها بر بهره‌برداری سیستم و استراتژی‌های دفاعی در برابر آن‌ها. همچنین پیشنهادهایی جهت ادامه مطالعات آینده در این مسیر و چالش‌های پیش روی روش‌های موجود نیز بیان گردید.

- در [۴۳] هدف یافتن شرایط غیر ایمن در یک تخمین حالت غیر ایمن در سیستم قدرت می‌باشد که در آن حملات مشکوکی وجود داشته که توسط بخش تشخصی قابل‌شناسایی نمی‌باشد و موجب خطا در تخمین می‌شود. بخصوص شرایط لازم و کافی برای وجود ناامنی معرفی می‌گردد که در آن تمامی کانال‌های ارتباطاتی تحت کنترل مهاجم می‌باشند. بعلاوه الگوریتمی ویژه نیز ارائه می‌شود که حملات را در تخمین سیستم ناامن ایجاد می‌نماید. همچنین در یک سیستم ناامن، یک شمای حفاظتی ارائه

می‌شود که در آن ،تنها تعداد کمی از کانال‌های ارتباطی نیاز به حفاظت در برابر حملات تزریق داده بد دارند. نتایج از کارایی روش پیشنهادی حکایت دارند.

- در [۴۴] بیان می‌گردد که چگونه حملات تزریق داده بد به‌صورت کورکورانه ایجادشده بدون اینکه هیچ اطلاعی از ساختار سیستم شامل اطلاعات توپولوژی و راکتانس خطوط موجود باشد. در این مقاله مشخص می‌شود که حملات داده بد درصورتی‌که تخمینگر حالت حاوی اندازه‌گیری‌های غلط فاحشی باشد مانند خرابی دستگاه‌ها و خطاهای ارتباطی، قابل‌تشخیص می‌باشند. استراتژی پیشنهادی حملات مبتنی بر سرقت پراکنده بهینه‌شده با جداسازی خطاهای فاحش از ماتریس اندازه‌گیری بر این مشکل غلبه می‌نماید. نتایج نشان می‌دهند که روش پیشنهادی کمترین خطا را داشته و بازده آن بسیار بالا می‌باشد.

- در [۴۵] مطرح‌شده است که PMUهای مورداستفاده در سیستم قدرت به دلایل مختلف در برابر حملات داده بد آسیب‌پذیر می‌باشند. در این مقاله یک روش هوشمند مبتنی بر شبکه محاسباتی سلولار(CNN) برای مدل پیش‌بین غیرمتمرکز و تخمین حالت دینامیکی سیستم قدرت به همراه داده‌های PMU ارائه‌شده است. روش CNN مبتنی بر DSE داده‌های بد ارائه‌شده توسط بخش‌های مختلف PMUها مقابله می‌نماید.

- در [۴۶] یک روش سیستماتیک مبتنی بر آنالیز موجک برای پیش فیلتر تخمین حالت به‌منظور تشخیص و حذف داده بد ارائه‌شده است. داده‌های بد ناخواسته مانند خرابی اندازه‌گیرهای گذرا و اندازه‌گیری‌های به‌دست‌آمده در گذراهای سیستم در تغییرات ناگهانی کوتاه‌مدت فرآیند اندازه‌گیری به‌صورت ذاتی وجود دارند. این موارد باید در مرحله پیش فیلتر تشخیص داده شوند چراکه حضور آن-ها در مرحله آنالیز داده بد مشکلات بیشتری را تحمیل می‌نماید. نتایج سرعت عمل پیش فیلتر نمودن این داده‌ها را نشان می‌دهد.

- در [۴۷] روشی جهت پردازش داده بد برای داده آنالوگ در یک پست ارائه‌شده است. با توجه به اینکه هر پست، یک استانداردی دارد و شارش توان الکتریکی در آن در جهت مشخصی می‌باشد،

قوانین تشخیص و تصحیح داده بد از پردازش منطقی روابط بین نشانه‌ها و خطاها به دست می‌آید. در این مقاله دلایل محافظه‌کارانه به همراه روش ماژولار استفاده‌شده است تا بازده و قابلیت تصحیح داده افزایش یابد. روش پیشنهادی بر اساس آنالیز منطقی خطاهای ممکن و نشانه‌های آن‌ها در هنگام وقوع تدوین‌شده است. روش پیشنهادی هم ساده بوده و دقت بالایی را در نتایج ارائه نموده است.

## ۲-۷- جمع‌بندی فصل

در این فصل در ابتدا مقدمه‌ای پیرامون موضوع موردبررسی بیان گردید. سپس در بخش اول به معرفی و بیان مقدمه‌ای در مورد سیستم‌های اتوماسیون قدرت پرداخته شد. پس‌ازآن تخمین حالت در اتوماسیون بیان گردید و مشخص شد که یکی از بخش‌های اساسی اتوماسیون سیستم‌های قدرت، تخمین حالت می‌باشد. بدین ترتیب در بخش دوم در مورد تخمین حالت در سیستم‌های قدرت نیز بحث شد و به برخی از روش‌های آن اشاره شد. پس‌ازآن درباره تشخیص داده‌های بد و تعیین اینکه در چه مواردی از روش WLS برای تخمین حالت استفاده می‌شود، بحث شد. همچنین بیان گردید که تشخیص یک داده بد با استفاده از روش باقیمانده نرمالیزه شده حداکثر، $r_{max}^{N}$ ممکن است. از طرف دیگر، تشخیص چندین داده بد مشکل‌تر است و دو روش جایگزین برای این هدف ذکر شد. توانایی تشخیص و تعیین داده‌های بد به نوع و پیکربندی اندازه‌گیری‌ها نیز بستگی دارد. در انتها نیز مروری بر روش‌های تخمین حالت و تشخیص داده‌های بد و اشتباه در سیستم‌های قدرت پرداخته شد و به برخی روش‌های جدید که در مقالات مختلف ارائه‌شده است، اشاره گردید. در فصل آینده مدل‌سازی مسئله و روش پیشنهادی جهت تشخیص حملات تزریق داده اشتباه ارائه می‌شود.

# فصل سوم:

# تشخیص حملات تزریق داده اشتباه در تخمین حالت در شبکه هوشمند

## ۳-۱- مقدمه

در سال‌های گذشته تغییرات سریعی از شبکه‌های سنتی به شبکه‌های هوشمند جدید صورت گرفت تا با افزایش مصرف و نیاز بیشتر تطابق پیدا کند. در این زمینه برخی روش‌های خاص جهت این حرکت تکاملی ارائه‌شده است که شامل بازآرایی سریع، متفکر شدن سیستم، عدم تمرکزگرایی سیستم قدرت و ادوات مانیتورینگ سریع می‌باشد. در مراحل اولیه تشکیل شبکه‌های هوشمند، نمایش وضعیت سیستم، وظیفه اصلی می‌باشد که بدون آن ، ایده مطرح‌شده بی‌فایده است. یکی از استراتژی‌های مهم و مفید جهت مانیتورینگ سیستم، تخمین حالت می‌باشد. تخمین حالت سیستم قدرت به فرآیندی اطلاق می‌گردد که در آن حالت سیستم الکتریکی توسط دستگاه‌های اندازه‌گیری بسیاری که در مکان‌های مختلف شبکه قرارگرفته‌اند ارزیابی می‌گردد. ازلحاظ فنی تخمین حالت به‌عنوان راه‌حلی جهت یافتن فازورهای ولتاژ باس‌ها درزمانی خاص می‌باشد. درمجموع، یک راه‌حل سریع و آسان نصب ادوات اندازه‌گیری دقیق در تمام باس‌های سیستم جهت محاسبه فازور سنکرون ولتاژ تمامی باسها می‌باشد[۳۷].

تخمین حالت ،عملیاتی مهم در شبکه سیستم مدیریت انرژی قدرت(EMS[1]) می‌باشد. در اجرای تخمین حالت، مرکز کنترل سیستم قدرت، داده‌های اندازه‌گیری شده را از واحدهای ترمینال از راه دور(RTUs) جمع‌آوری می‌کند. این داده‌ها به‌طورکلی شامل توان اکتیو و راکتیو تزریقی، توان اکتیو و راکتیو جاری‌شده در خطوط انتقال، و اندازه ولتاژ در باس‌های تولید می‌باشند. داده‌های اندازه‌گیری شده با استفاده از تخمین حالت DC و یا AC به حالت سیستم(زاویه فاز و دامنه ولتاژ باس) تبدیل می‌شوند[۳۵].

اما در این مسئله ممکن است خرابی‌ها و یا خطاهای اندازه‌گیری نیز رخ دهد. جهت حل این مشکل می‌توان از اندازه‌گیری‌های پی‌درپی استفاده نمود تا خطاهای اندازه‌گیری کاهش یابد و حالتی بهینه که در مسئله تخمین حالت مطرح‌شده است، به دست آید. پارامترهایی که برای تخمین حالت

[1] Energy Management System

دقیق قابل‌استفاده هستند شامل توان تزریقی اکتیو و راکتیو، اندازه ولتاژ یا جریان می‌باشد. در این رابطه الگوریتم تکرار WLS (حداقل مربعات وزندار) روشی مناسب و مفید است که اصولاً مورداستفاده قرار می‌گیرد و از نمونه‌های اندازه‌گیری متفاوتی استفاده می‌نماید تا سیستم را ارزیابی کرده و اطلاعات حالت استاتیکی و یا شبه استاتیکی آن را ارائه نماید. تابع تخمینگر کلاسیک به مرکزیت یک مرکز کنترل عمل می‌نماید و داده‌های مطلوب، زمان حقیقی و استاتیکی را جهت حل پردازشگر توپولوژی(TP)، تخمین حالت (SE)و تشخیص داده بد(BD)به‌صورت تناوبی تشخیص و حل می‌نماید. بنابراین یکی از نتایج مهم تخمین حالت بهینه بهره‌برداری مؤثر و امن سیستم قدرت هم در شرایط نرمال و هم در شرایط بروز پیش‌آمد و اضطراری می‌باشد[۳۷].

بنابراین تخمین حالت دقیق سیستم بسیار مهم می‌باشد، زیرا اطلاعات حالت به‌دست‌آمده از تخمین حالت سیستم در توابع و امور دیگر EMS، مانند آنالیز پایداری، حذف بار زدایی و ... استفاده می‌شوند. داده‌های اندازه‌گیری شده و جمع‌آوری‌شده از RTUها ممکن است شامل خطاهای اندازه‌گیری تصادفی کوچک باشند، که این مسئله می‌تواند توسط نویز و یا عدم دقت تجهیزات اندازه‌گیری ایجاد شود. این خطاهای کوچک اندازه‌گیری به‌طورکلی از هم مستقل می‌باشند. در صورت وجود این اختلافات جزئی خطاهای اندازه‌گیری، تخمین حالت به روش حداقل مربعات وزندار می‌تواند حالت سیستم را به‌طور دقیق ارزیابی کند.

جدای از خطاهای اندازه‌گیری جزئی که توسط نویز و عدم دقت در اندازه‌گیری به وجود می‌آیند، ممکن است داده‌های اندازه‌گیری شامل خطاهای بزرگ‌تری به دلیل اتصال اشتباه دستگاه‌های اندازه‌گیری و یا عیب و نقص در ارتباطات باشند. این خطاهای اندازه‌گیری بزرگ به‌صورت مستقل در نظر گرفته‌شده و با استفاده از پردازش باقیمانده روش تشخیص داده بد سنتی شناسایی می‌گردد.

در سال‌های اخیر، با ظهور شبکه‌های هوشمند و به دنبال آن هوشمند شدن و تحت وب کار کردن دستگاه‌های اندازه‌گیری، این دستگاه‌ها در معرض حملات سایبری قرارگرفته است لذا حملات سایبری به‌صورت تهدیدی برای امنیت بهره‌برداری سیستم‌های قدرت پدیدار شده‌اند. در [۳۱] مشخص گردید

که نوع جدید حملات سایبری به نام حملات تزریق داده اشتباه می‌تواند از مرحله تشخیص داده بد به روش سنتی در مسئله تخمین حالت سیستم قدرت عبور نماید. چراکه باقیمانده‌های اندازه‌گیری با حملات تزریق داده اشتباه مشابه با باقیمانده‌های اندازه‌گیری بدون حملات تزریق داده اشتباه می-باشند.

روش‌های مختلفی برای دفاع حملات تزریق داده اشتباه ارائه‌شده است. این روش‌ها به دودسته ۱) مبتنی بر حفاظت و ۲) مبتنی بر تشخیص تقسیم‌بندی می‌شوند. روش‌های مبتنی بر حفاظت که با استفاده از سنسورهای مشخص حفاظتی در برابر حملات تزریق داده اشتباه مقابله می‌نمایند، دارای دو اشکال می‌باشند. مشکل اول کاهش فراوانی داده‌ها بوده چراکه تنها اندازه‌گیری‌های حفاظت‌شده قابل‌اعتماد بوده و مورداستفاده قرار می‌گیرد. مشکل دوم نیز عدم امنیت کامل خود سیستم حفاظتی در تمامی زمان‌ها می‌باشد و اگر هکرها بتوانند در این زمان در سیستم‌های حفاظتی نفوذ کرده و اندازه‌گیری‌ها را تغییر دهند، تخمین حالت درخطر قرار دارد. روش‌های مبتنی بر تشخیص با آنالیز اندازه‌گیری‌های خام و اولیه می‌توانند موارد غیرمعمول را از مواردی که با توزیع اندازه‌گیری‌های گذشته تناسب ندارد تشخیص دهند. اما مشکل این روش‌ها نیز این است که توانایی تشخیص داده اشتباه که کاملاً با اندازه‌گیری‌های گذشته متناسب باشد یا مانند داده اندازه‌گیری گذشته باشد را ندارد[۴۹,۴۸].

در این فصل روش جدید مبتنی بر تشخیص برای برطرف شدن محدودیت‌های روش‌های موجود جهت تشخیص داده‌های بد نوع سوم ارائه می‌شود. ایده اصلی روش پیشنهادی ردیابی تغییرات اندازه‌گیری‌ها بین مراحل متوالی می‌باشد. سپس شاخص‌های فاصله از اندازه‌گیری‌های گذشته با استفاده از روش فاصله نسبی لگاریتمی محاسبه می‌شوند. مقدار آستانه که از داده‌های پیشین محاسبه می‌شود، برای تشخیص حملات پنهانی تزریق داده‌های بد مورداستفاده قرار می‌گیرد. به این صورت که هنگامی‌که داده اشتباه به سیستم قدرت تزریق می‌شود، هیستوگرام تغییرات اندازه‌گیری از اندازه‌گیری‌های گذشته منحرف‌شده و درنتیجه به یک شاخص فاصله بزرگ‌تر منجر می‌شود. اگر

شاخص فاصله بزرگ‌تر از آستانه باشد، این نتیجه دریافت می‌گردد که اندازه‌گیری‌ها و داده‌های جدید دریافتی دستکاری‌شده و تقلبی می‌باشند.

در این فصل در ادامه موارد ذیل موردبررسی قرار می‌گیرند: در ادامه ابتدا تخمین حالت ac در شبکه‌های هوشمند تشریح می‌گردد. سپس پیشینه تخمین حالت، تشخیص داده بد و حملات تزریق داده اشتباه ارائه می‌شود. در بخش چهارم روش‌های موجود و روش پیشنهادی برای تشخیص حملات تزریق داده اشتباه موردبررسی قرار می‌گیرند.

**متغیرها و اصطلاحات**

| | | | |
|---|---|---|---|
| $\tilde{z}$ | بردارهای اندازه‌گیری | $P_{ij}^{Be,line}$ | توان کامل جاری‌شده بین باس‌های i-j |
| $\tilde{r}$ | بردار خطا | $P_{ij,max}^{Be,line}$ | ماکزیمم مقدار توان انتقالی بین باس‌های i-j |
| $\widetilde{W}$ | ماتریس ضریب وزن | $P_{Load,max}^{j}$ | ماکزیمم مقدار jامین بار |
| $\widetilde{H}$ | ماتریس اندازه‌گیری عملیاتی | $Q_c^j$ | مقدار توان راکتیو jامین باس |
| $f(\tilde{X})$ | تابع هدف | $n_{gen}$ | تعداد واحدهای تولید |
| $\delta$ | ضریب وزنی | $N_{equality}$ | تعداد مساوی‌ها |
| $h$ | معادله حالت | $J_j(\tilde{X})$ | قید برابر |
| $n_{load}$ | تعداد بارها | $\alpha_1$ | ضرایب هدف ثابت |
| $V_{Pg_j}$ | ولتاژ jامین DG | $X_{estimated\ value}$ | مقدار تخمین زده‌شده |
| $P_{Gen,min}^{j}$ | حداقل مقدار توان اکتیو تولیدی توسط jامین واحد | $V_{Load_j}$ | ولتاژ jامین بار |

## ۳-۲- تخمین حالت در شبکه‌های هوشمند

معمولاً صنعت برق سعی می‌کند تا توان الکتریکی را با بیشترین قابلیت اطمینان و کیفیت و کمترین هزینه و انتشار آلودگی و تلفات به مصرف‌کننده تحویل نماید. شبکه‌های هوشمند پاسخی

جدید برای رسیدن به این اهداف می‌باشند. در یک شبکه هوشمند هنگامی‌که مصرف‌کنندگان از الگوی بار هوشمند با هزینه و الگوی مصرف هوشمندانه پیروی می‌کنند، نیروگاه‌ها و واحدهای تولیدی نیز باید تولید خود را به همان میزان مدیریت نمایند. جهت نیل به چنین اهدافی، لزوم مانیتور نمودن کل سیستم و کسب اطلاعات موردنیاز از تمامی باس‌ها امری واضح و آشکار است. ازنقطه‌نظر فنی، طراحی شبکه هوشمند، از دید سه ناحیه مصرف‌کنندگان، تجهیزات و ارتباطات موردبررسی قرار می‌گیرد. نتیجتاً، استفاده از تکنولوژی شبکه هوشمند در سه بخش تولید، انتقال و توزیع انعکاس می‌یابد که از دید سرویس الکتریکی و شبکه، ویژگی‌های مفیدی را ارائه می‌نماید. مسئله مهم و حیاتی در ایده شبکه‌های هوشمند، دستیابی مناسب به داده‌های موردنیاز در شبکه می‌باشد که به این امر مختصراً تخمین حالت اطلاق می‌گردد. استفاده از تخمین حالت مناسب مزایای زیر را به دنبال دارد[۳۷]:

**الف) اصلاح پیک‌بار:** استفاده از شبکه هوشمند در هر دو سمت تولید و تقاضا تأثیر می‌گذارد که نتیجه مستقیم آن اصلاح پیک‌بار می‌باشد.

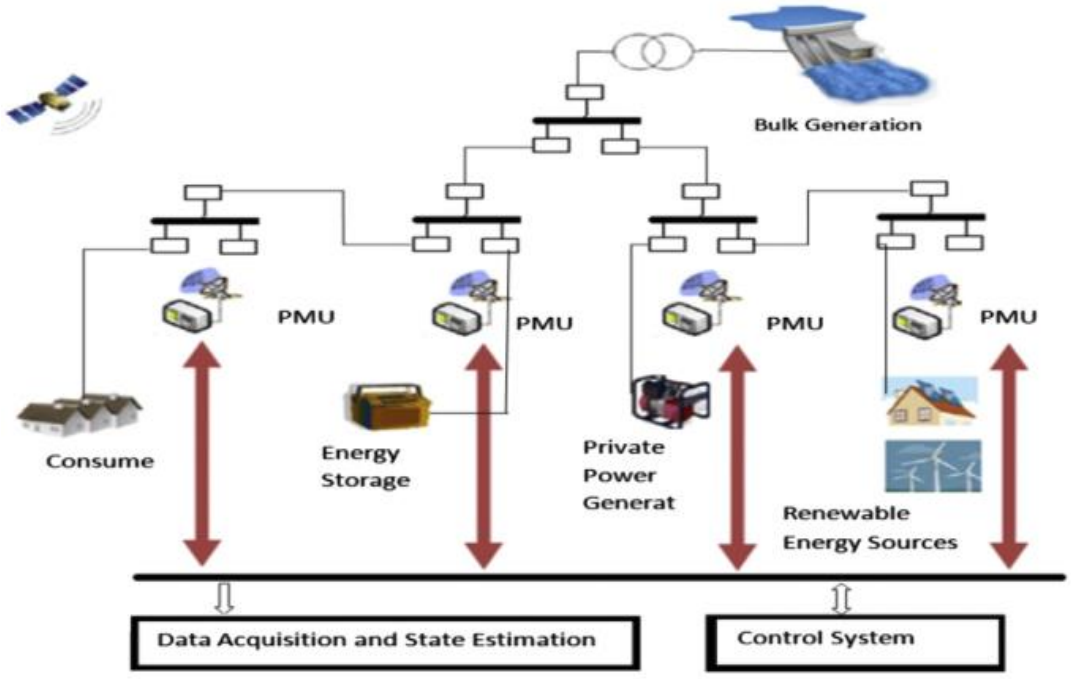
**ب) کاهش مصرف سوخت‌های فسیلی:** کاهش تلفات انرژی در فیدرها و همچنین امکان تغییر توپولوژی شبکه توسط برخی روش‌های مفید مانند بازآرایی منجر به کاهش مصرف سوخت‌های فسیلی می‌گردد.

**ج) کاهش قطعی بار:** شبکه هوشمند منجر به کاهش زمان خروج، تعداد دفعات خروج و خاموشی‌های ناخواسته می‌گردد.

**د) کاهش هزینه‌های سرمایه‌گذاری:** دلیل اصلی سرمایه‌گذاری جدید در شبکه‌های الکتریکی فعلی رشد بار می‌باشد که در اصل در ساعات پیک‌بار رخ می‌دهد. با استفاده از ایده شبکه‌های هوشمند و روش‌های مدیریت هوشمند، می‌توان رشد بار را کنترل نمود که این امر هزینه سرمایه‌گذاری را کاهش می‌دهد.

ه) **کاهش هزینه‌های سوئیچینگ:** کاهش هزینه‌های سوئیچنیگ مشترکین قابل‌کنترل نیز از مزایای شبکه‌های هوشمند می‌باشد[۳۷].

شکل ۳-۱ یک شبکه هوشمند نمونه را نشان می‌دهد. در این شکل واحد اندازه‌گیری فازورداده‌های شبکه را اندازه‌گیری و سنکرون می‌نماید. لازم به ذکر است که اختلاف در جمع‌آوری داده‌های زاویه-های ولتاژ باس‌ها کمتر از یک میلی‌ثانیه می‌باشد. در طی فرآیند تخمین حالت، داده‌های بد و اندازه‌گیری‌های ناسالم از مجموعه داده‌ها حذف می‌گردند. واضح است که قبل و بعد از فرآیند پاک‌سازی داده‌ها رؤیت پذیری سیستم نیز باید بررسی گردد. مسئله مهم این می‌باشد که شبکه هوشمند به تعداد مناسبی از ادوات پردازش داده شامل وسایل اندازه‌گیری و کنترل نیاز دارد. این امر می‌تواند پیچیدگی و هزینه کلی شبکه‌های هوشمند جدید را به‌طورجدی افزایش دهد، مگر اینکه با استفاده از روش تخمین حالت مناسب از ادوات سخت‌افزاری کمتری در سیستم استفاده گردد که در این بخش این مسئله با استفاده از روش WLS ارائه می‌شود[۳۷].




شکل ۳-۱- سیستم هوشمند نمونه [۳۷]

**۳-۲-۱- تخمینگر حداقل مربعات وزندار(WLS)**

در مقالات ذکرشده است که اگر ادوات آنالوگ برای جمع‌آوری جریان و ولتاژ سنکرون شوند، آنگاه روابط تخمین حالت به حالت خطی تبدیل می‌شوند(شرط اول). در این حالت، با استفاده از ادوات PMU مناسب، تابع اندازه‌گیری جدیدی برای تخمین حالت به وجود می‌آید که در فضای مختلط به‌صورت خطی می‌باشد. در این فضا هم حالات و هم اندازه‌گیری‌ها خطی بوده و در حالت پیچیده منجر به تخمین حالت خطی می‌شود. روابط خطی تخمین حالت به‌صورت زیر نمایش داده می-شوند[۳۷]:

$$Min\ \tilde{r}^T\widetilde{W}\tilde{r}\ ,\quad s.t.\quad \tilde{z}=\widetilde{H}\tilde{x}+\tilde{r} \tag{۱-۳}$$

که $\tilde{z}$ بردار اندازه‌گیری، $\tilde{r}$ بردار خطا، $\widetilde{W}$ ماتریس ضرایب وزنی، $\tilde{x}$ بردار حالات سیستم، و $\widetilde{H}$ ماتریس تابعی اندازه‌گیری سیستم است که به بردار اندازه‌گیری و حالات سیستم وابسته است.

در مسئله تخمین حالت، هر اندازه‌گیری به‌صورت $\tilde{z}_i = z_{i,real} + jz_{i,imag}$، هر حالت به فرم $\tilde{x}_i = x_{i,real} + jx_{i,imag}$ و هر خطا بصورت $\tilde{r}_i = \tilde{r}_{i,real} + j\tilde{r}_{i,imag}$ نمایش داده می‌شود. جهت فرمول‌بندی ماتریسی، بردار اندازه‌گیری حالت و خطا به ترتیب بصورت $\tilde{z}_i = \begin{bmatrix} z_{i,real} \\ jz_{i,imag} \end{bmatrix}$، $\tilde{z}_i = \begin{bmatrix} x_{i,real} \\ jx_{i,imag} \end{bmatrix}$ و $\tilde{z}_i = \begin{bmatrix} r_{i,real} \\ jr_{i,imag} \end{bmatrix}$ در فضای حقیقی نمایش داده می‌شوند. ورودی $\tilde{h}_{i,j} = h_{i,j,real} + jh_{i,j,imag}$ توسط یک ماتریس $2 \times 2$ در فضای حقیقی بصورت $\tilde{H} = \begin{bmatrix} h_{i,j,real} & -jh_{i,j,imag} \\ jh_{i,j,imag} & h_{i,j,real} \end{bmatrix}$ نمایش داده می‌شود. با در نظر گرفتن m سنجش و اندازه‌گیری و n حالت، رابطه (۳-۱) بصورت زیر بازنویسی می‌گردد[۳۷]:

$$Min\ J = \tilde{r}^T\widetilde{W}\tilde{r}, \tag{۲-۳}$$

$$s.t.\quad \tilde{z} = \begin{pmatrix} \tilde{z}_{,1} \\ \vdots \\ \tilde{z}_{,m} \end{pmatrix} = \widetilde{H}\tilde{x} + \tilde{r} = \begin{pmatrix} \widetilde{H}_{1,1} & \dots & \widetilde{H}_{1,n} \\ \vdots & \ddots & \vdots \\ \widetilde{H}_{m,1} & \dots & \widetilde{H}_{m,n} \end{pmatrix} \begin{pmatrix} \tilde{x}_1 \\ \vdots \\ \tilde{x}_n \end{pmatrix} + \begin{pmatrix} \tilde{r}_1 \\ \vdots \\ \tilde{r}_m \end{pmatrix}$$

که $\widetilde{W}$ ماتریس وزنی قطری می‌باشد که تمامی ورودی‌های آن اعداد حقیقی بوده و $\widetilde{W}_i$ برای هر اندازه‌گیری بلوک وزنی $2 \times 2$ به‌صورت زیر می‌باشد:

$$W_i = \begin{pmatrix} \sigma^2_{z1,real} & 0 \\ 0 & \sigma^2_{z1,real} \end{pmatrix} \quad (۳-۳)$$

بنابراین با کاهش $J$ نسبت به $\tilde{X}$، مشتق جزئی آن محاسبه‌شده و به‌صورت $\frac{\partial J}{\partial X} = 0$ تنظیم می‌گردد. خروجی رابطه فوق، بردار $\tilde{X}$ می‌باشد که شامل حالات مسئله است. با در نظر گرفتن تابع توزیع نرمال واحدهای اندازه‌گیری خطا، $\tilde{X}$ به‌صورت زیر محاسبه می‌گردد:

$$\tilde{X} = (H^T W H)^{-1} H^T W z \quad (۴-۳)$$

که $H^T$ شبه ماتریس معکوس $H$ است که به ازای $m > n$ ایجاد می‌گردد. لازم به ذکر است که درجه $H$ کامل است، یعنی همواره تعداد اندازه‌گیری‌های m بیشتر از تعداد متغیرهای n می‌باشد. همچنین اندازه‌گیری‌ها نیز به‌طور خطی‌مستقل‌اند. شرط لازم برای یافتن حداقل نقطه ساکن $J$ این است که مشتق دوم $J$ مقداری مثبت معلوم باشد. فرمول‌بندی تخمینگر حالت در بخش بعدی توضیح داده می‌شود[۳۷].

**۳-۲-۲- تابع برازندگی**

درروش WLS، برای تخمین حالت تابع برازندگی به‌صورت زیر در نظر گرفته می‌شود که باید حداقل گردد:

$$\text{if } \frac{\partial J}{\partial \tilde{X}} = 0, then\ Min\ f(\tilde{X}) = \sum_{j=1}^{m} \delta_j \left(z_j - h_j(\tilde{X})\right)^2$$

$$\begin{cases} \tilde{X} = \left[\tilde{X}_{1,VG}, \tilde{X}_{2,Vload}\right]^T \ 1 \times n \\ \tilde{X}_{1_{VG}} = \left[\tilde{X}^1_{V,Pg}, \tilde{X}^2_{V,Pg}, \dots, \tilde{X}^{n_{gen}}_{V,Pg}\right]^T \ ; \ n = n_{gen} + n_{load} \\ \tilde{X}_{1_{Vload}} = \left[\tilde{X}^1_{V,load}, \tilde{X}^2_{V,load}, \dots, \tilde{X}^{n_{load}}_{V,load}\right]^T \end{cases} \quad (۵-۳)$$

که $z$ داده اندازه‌گیری شده، $f(\tilde{X})$ تابع برازندگی، $\tilde{X}$ بردار متغیرهای حالت، $\delta$ ضریب وزنی، $h$ معادله حالت، $m$ تعداد اندازه‌گیری‌ها، $n_{gen}$ تعداد باس‌های تولید، $n_{load}$ تعداد بارها، $V_{Pg_j}$ ولتاژ jامین باس تولید و $V_{load_j}$ ولتاژ jامین باس بار می‌باشد[۳۷].

### ۳-۲-۳- محدودیت‌های مسئله

در طی فرآیند حل مسئله محدودیت‌های زیر باید در نظر گرفته شوند[۳۷]:

- **حداکثر ظرفیت تولید واحدها**

$$P^{j}_{Gen,min} \le P^{j}_{Gen} \le P^{j}_{Gen,max} \quad , \ j = 1,2,3,\dots,n_{Gen}$$
$$Q^{j}_{Gen,min} \le Q^{j}_{Gen} \le Q^{j}_{Gen,max} \quad , \ j = 1,2,3,\dots,n_{Gen} \qquad (۶-۳)$$

که $P^{j}_{Gen,min}$، $Q^{j}_{Gen,min}$، $Q^{j}_{Gen,max}$ و $P^{j}_{Gen,max}$ به ترتیب مقادیر حداقل و حداکثر توان‌های اکتیو و راکتیو تولیدی توسط واحد تولیدی jام می‌باشد.

- **حداکثر شارش توان در فیدرها**

$$\left|P^{Be,line}_{ij}\right| < P^{Be,line}_{ij,max} \qquad (۷-۳)$$

که $P^{Be,line}_{ij}$ توان کامل عبوری بین باس i-j می‌باشد و $P^{Be,line}_{ij,max}$ مقدار ماکزیمم توان انتقالی بین باس‌های i-j می‌باشد.

- **محدوده ولتاژ باس‌ها**

$$V_{Bus,max} \le V_{Bus,j} \le V_{Bus,max} \quad , \ j = 1,2,3,\dots,n_b \qquad (۸-۳)$$

که $V_{Bus,j}$ مقدار ولتاژ باس jام، $V_{Bus,max}$ و $V_{Bus,max}$ به ترتیب ماکزیمم و مینیمم مقدار ولتاژ باس jام می‌باشد و $n_b$ تعداد کل باس‌ها است.

- **محدودیت بارها**

$$P^{j}_{Load,min} \le P^{j}_{Load} \le P^{j}_{Load,max} \quad , \ j = 1,2,3,\dots,N_{Load} \qquad (۹-۳)$$

که $P^{j}_{Load,min}$ و $P^{j}_{Load,max}$ به ترتیب مقادیر مینیمم و ماکزیمم jامین بار و $N_{Load}$ تعداد بارها می‌باشد. واحد کنترل بر عملکرد واحدهای تنظیم‌کننده ولتاژ(VRها[1]) و کنترلرهای راکتیو به‌صورت محلی نظارت نموده و آن‌ها را مدیریت می‌نماید[۳۷].

[1] Voltage Regulators

## ۳-۳- تشخیص حملات تزریق اطلاعات غلط

تشخیص داده‌های بد به روش مرسوم بر اساس آنالیز باقیمانده $r = z - \hat{z} = z - H\hat{x}$ می‌باشد که در فصل دوم توضیحات مربوط به باقیمانده اندازه‌گیری داده شد. اگر خطاهای اندازه‌گیری مستقل باشند و از توزیع نرمال تبعیت کنند، آنگاه باقیمانده $\|r\|$ از توزیع مربع کای تبعیت می‌کند. به‌منظور تشخیص وجود داده‌های بد، باقیمانده با یک مقدار آستانه که با یک‌فاصله اطمینان خاصی محاسبه‌شده است، مقایسه می‌گردد.

با توجه به مرجع [۳۱]، اگر مهاجم از ساختار سیستم(H) اطلاع داشته باشد، می‌تواند هم‌زمان چندین داده اندازه‌گیری را دستکاری کند و از بخش تست تشخیص داده‌های بد به روش مرسوم عبور کند.

اگر اندازه‌گیری دستکاری‌شده $z_{bad} = z + a$، به تخمین حالت DC تزریق شود، تخمینگر یک متغیر حالت اشتباه $\hat{x}_{bad} = \hat{x} + c$ را ارائه خواهد داد. درصورتی‌که $a = Hc$ باشد( که H همان تابع اندازه‌گیری یا به‌عبارت‌دیگر رابطه پخش بار است که در بخش بعدی توضیح داده می‌شود)، می‌تواند از آزمون تشخیص داده‌های بد به روش مرسوم عبور کند که در آن $a$ داده‌های مخرب اضافه‌شده به اندازه‌گیری اصلی و $c$ خطای تزریقی در حالت سیستم می‌باشد.. حملات تزریق داده اشتباه می‌توانند از آزمون مرسوم تشخیص داده‌های بد عبور کند چراکه باقیمانده اندازه‌گیری پس از حملات تزریق داده اشتباه به‌صورت زیر خواهد بود:

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

این امر به این معنی است که باقیمانده اندازه‌گیری پس از تزریق داده‌های اشتباه به سیستم، افزایش نخواهد یافت. بنابراین روش‌های مرسوم تشخیص داده‌های بد نمی‌توانند حملات تزریق داده-های اشتباه را تشخیص دهند[۴۷-۴۹].

در مرجع [۳۶] تزریق داده‌های اشتباه DC به تزریق داده اشتباه AC توسعه داده‌شده است. همچنین در [۳۶]، مشخص‌شده است که به‌منظور عبور از تشخیص داده بد در تخمین حالت AC،

مهاجم نیاز دارد که هم از مقدار حالت سیستم و هم پیکربندی سیستم اطلاع داشته باشد. در تخمین حالت AC، داده‌های اشتباه که به اندازه‌گیری واقعی اضافه‌شده‌اند، اگر به‌صورت $a = h(\hat{x} + c)$ باشد، آنگاه حملات تزریق داده اشتباه می‌تواند از مرحله تشخیص داده بد به روش مرسوم عبور $h(\hat{x})$ کند.

به‌طورکلی مهاجم تنها می‌تواند از طریق دستگاه‌های اندازه‌گیری داده‌های اشتباه را به تخمین حالت تزریق نماید، اما می‌تواند از طریق این دستگاه‌ها، دو هدف متفاوت را ردیابی کند. یکی دستکاری بعضی از متغیرهای حالت سیستم و دیگری دستکاری برخی از اندازه‌گیری‌های سیستم است[۴۴].

در این پژوهش، تخمین حالت AC موردبررسی و آنالیز قرار می‌گیرد و روش ارائه‌شده برای تخمین حالت DC نیز قابل‌استفاده می‌باشد.

### ۳-۳-۱- هدف قرار دادن متغیرهای حالت سیستم

در تخمین حالت‌های AC، دو نوع از متغیرهای حالت وجود دارد: ۱)زاویه‌ی فاز باس($\theta$)، ۲)دامنه ولتاژ باس($V$). اگر مهاجم متغیر حالت خاصی را مورد هدف قرار دهد، تمام اندازه‌گیرهای وابسته به این متغیر حالت را باید دستکاری کند تا باقیمانده اندازه‌گیری صفر و یا مقدار ناچیزی شود. مقادیر اندازه‌گیری شده وابسته به حالت سیستم با معادلات زیر نمایش داده می‌شود:

**۱) توان اکتیو و راکتیو تزریقی در باس iام**

$$P_i = V_i \sum_{j \in \Omega_i} V_j \left( G_{ij} \cos \theta_{ij} + B_{ij} \sin \theta_{ij} \right) \qquad (۱۰-۳)$$

$$Q_i = V_i \sum_{j \in \Omega_i} V_j \left( G_{ij} \sin \theta_{ij} - B_{ij} \cos \theta_{ij} \right) \qquad (۱۱-۳)$$

**۲) توان اکتیو و راکتیو انتقالی از باس iام به باس jام**

$$P_{ij} = V_i^2 \left( g_{si} + g_{ij} \right) - V_i V_j \left( g_{ij} \cos \theta_{ij} + b_{ij} \sin \theta_{ij} \right) \qquad (۱۲-۳)$$

$$Q_{ij} = -V_i^2\left(b_{si} + b_{ij}\right) - V_i V_j\left(g_{ij}\sin\theta_{ij} - b_{ij}\cos\theta_{ij}\right) \qquad (۱۳-۳)$$

که در روابط بالا داریم:

$V_i$ ولتاژ در باس i

$\theta_i$ زاویه فاز در باس i

$\theta_{ij}$ $\theta_i - \theta_j$

$G_{ij} + jB_{ij}$ ادمیتانس خط بین باس i و باس j

$g_{si} + jb_{si}$ ادمیتانس شاخه شنت در باس i

$\Omega_i$ مجموعه باس‌های متصل به باس i

با توجه به روابط (۳-۱۳) تا (۳-۱۶)، مشخص است که برای هدف قرار دادن یک متغیر حالت، به‌عنوان‌مثال $V_i$، داده‌های اندازه‌گیری مربوط $P_i$، $Q_i$، $P_{ij}$ و $Q_{ij}$ که $j \in \Omega_i$ نیاز است تا دستکاری شوند. اگر مهاجم قصد داشته باشد حالت‌های مختلف را هم‌زمان تغییر دهد، به دستکاری اندازه‌گیرهای مختلف بیشتر نیاز دارد. برای مثال، اگر مهاجم بخواهد $V_k$ که $k \in \mathbf{U}_a$ و یک مجموعه از شماره باس‌ها است را تغییر دهد، اندازه‌گیری‌هایی که نیاز است تا دستکاری شوند، $P_k$، $Q_k$، $P_{kj}$ و $Q_{kj}$ خواهند بود[۳۵-۳۶].

### ۳-۳-۲- هدف قرار دادن اندازه‌گیری‌های خاص

راه دیگری که مهاجم می‌تواند به سیستم نفوذ کند، و باقیمانده اندازه‌گیری، مقدار کوچکی باشد، این است که مقدار یک اندازه‌گیر خاص را مورد هدف قرار دهد. طبق روابط پخش بار، هراندازه گیر خاص، حداقل توسط دو متغیر حالت سیستم تعیین می‌شود. هنگامی‌که مهاجم، مقدار یک اندازه‌گیر خاص را به مقدار موردنظر خود درمی‌آورد، حداقل یک متغیر حالت تغییر می‌یابد، در این حالت، برای عبور از تشخیص داده بد مرسوم(ناچیز نگه‌داشتن مقدار باقیمانده اندازه‌گیری)، باید تمام اندازه‌گیرهای وابسته به متغیرهای حالت تغییریافته را طوری تغییر نماید که تخمینگر دقیقاً همان مقدار تغییریافته

را برای متغیر حالت برآورد کند تا مقدار اندازه‌گیری به دست آمده برای آن اندازه‌گیر خاص، دقیقاً همان مقدار موردنظر مهاجم شود[۳۵].

## ۳-۴- روش مقابله با حملات تزریق داده اشتباه در تخمین حالت AC

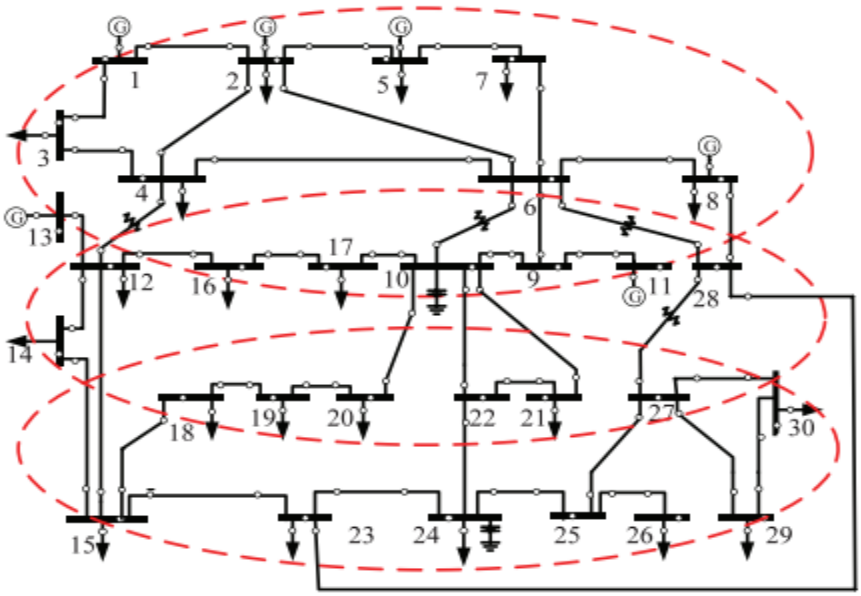
### ۳-۴-۱- روش‌های دفاعی موجود

اقدامات متقابل موجود را می‌توان به دو گروه دسته‌بندی کرد: روش‌های مبتنی بر حفاظت و روش-های مبتنی بر تشخیص.

#### ۳-۴-۱-۱-روش‌های مبتنی بر حفاظت

یک سیستم قدرت ازآنجایی‌که معمولاً ناحیه جغرافیایی وسیعی-بعنوان مثال بیشتر از ۱میلیون کیلومترمربع را در برمی‌گیرد، بنابراین بهره‌بردار شبکه می‌تواند برخی از دستگاه‌های اندازه‌گیری مهم را از بین تمامی دستگاه‌ها جهت حفاظت انتخاب نماید که به‌عنوان‌مثال آن‌ها را با روش‌های مخفی و کدگذاری کردن، مانیتورینگ دائم و یا قطع ارتباط با اینترنت محافظت کند[۴۸]. دستگاه‌های اندازه‌گیری در تخمین حالت DC سیستم‌های قدرت به دو نوع توان اکتیو تزریقی در باس‌ها و توان اکتیو جاری‌شده در خطوط تقسیم‌بندی می‌شوند. همان‌گونه که پیشتر نیز بیان گردید برای محاسبه توان اکتیو تزریقی در هر باس یک دستگاه اندازه‌گیری و برای محاسبه توان اکتیو جاری‌شده در هر خط به دو دستگاه اندازه‌گیری نیاز می‌باشد[۴۹].

به‌عنوان‌مثال اگه یک شبکه ۳۰ باسه مطابق شکل ۳-۲ در نظر بگیریدکه در آن باس ۹ به باس‌های ۶، ۱۰ و ۱۱ متصل شده است. اگر یک مهاجم بخواهد متغیر حالت باس ۹ را تغییر دهد، لازم است که دستگاه‌های اندازه‌گیری جهت توان تزریقی $P_9$، $P_6$، $P_{10}$ و $P_{11}$ و دستگاه اندازه‌گیری جهت شارش توان $P_{6,9}$، $P_{9,10}$، $P_{10,9}$، $P_{9,11}$ و $P_{11,9}$ را متناسب با نوع دستکاری تنظیم نماید[۴۹].




شکل ۳-۲- شبکه ۳۰ باسه نمونه به همراه دستگاه‌های اندازه‌گیری [۴۹]

از سوی دیگر اگر بهره‌بردار سیستم از دستگاه محاسباتی توان تزریقی $P_9$ محافظت نماید، مهاجم هیچ شانسی جهت دستکاری و حمله به متغیرهای حالت باس‌های ۹، ۶، ۱۰ و ۱۱ ندارد. اما اگر دستگاه اندازه‌گیری واقع در خط انتقال $P_{9,6}$ محافظت شود، تنها متغیرهای حالت باس‌های ۹ و ۶ غیرقابل دستکاری می‌باشند.

با توجه به مثال فوق می‌توان پی برد که دستگاه‌های اندازه‌گیری توان تزریقی در باس‌ها از دستگاه‌های اندازه‌گیری توان جاری‌شده در خطوط مهم‌تر می‌باشند. از دیدگاه تخمین حالت، اندازه‌گیری‌های توان تزریقی نقشی مهم در تعیین یک متغیر حالت خاص ایفا می‌کنند درحالی‌که اندازه‌گیری‌های توان جاری‌شده در خطوط اندازه‌گیری اضافی بوده که دقت تخمین حالت را بهبود می‌بخشند[۴۹].

اگر توان تزریقی باس i محافظت شود، فضای جستجو برای مهاجم از $\binom{n}{k}$ به $\binom{n-|\mathcal{N}_i|-1}{k}$ کاهش می‌یابد. بنابراین دستگاه‌های تحت حفاظتی که توان تزریقی باس‌های متصل به تعداد زیادی از باس‌ها را اندازه‌گیری می‌کنند، پیچیدگی هدایت حملات تزریق داده اشتباه را افزایش می‌دهند درحالی‌که محافظت از تمامی باس‌ها در شبکه قدرت امکان‌پذیر نمی‌باشد[۴۹].

بااین‌وجود در فصل دوم پیرامون مراجعی که از این روش استفاده می‌کردند بحث گردید. در این منابع برای جلوگیری از حملات تزریق داده‌های اشتباه، روشی با استفاده از حفاظت از اندازه‌گیری‌های سنسورهای خاص ارائه گردیده است. این روش با محاسبه‌ی مجموعه‌ای حداقل از اندازه‌گیری‌ها در تخمین حالت DC و AC که نیاز به محافظت دارند، قابل‌استفاده است بااین‌حال، دو اشکال درروش مبتنی بر حفاظت وجود دارد. ازآنجایی‌که تنها به اندازه‌گیری‌های حافظت شده می‌توان اعتماد نمود، اولین اشکال کاهش فروانی اندازه‌گیری‌ها می‌باشد. اشکال دوم این است که حفاظت از اندازه‌گیری‌ها ممکن است در ٪۱۰۰ از کل زمان‌ها کار نکند. اگر مهاجم قادر به نفوذ در سیستم حفاظت باشد، پس تخمین حالت هنوز هم در معرض خطر بزرگ قرار دارد.

### ۳-۴-۱-۲-روش‌های مبتنی بر تشخیص

در حملات سرقت داده‌ها، مهاجم ممکن است اندازه‌گیری‌های چندین سنسور را تا حالت مرزی تغییر دهد تا حدی که اندازه‌گیری‌های انفرادی دستکاری شده توسط روش‌های آماری ارائه‌شده در مراجع قابل‌تشخیص نباشد. برای تشخیص چنین حملات سرقت داده، در [۴۹] یک روش تشخیص مبتنی بر فاصله بر اساس آزمون فرضیه ارائه‌شده است.

هنگامی‌که بردار اندازه‌گیری در مرکز کنترل جمع‌بندی شود، باید مشخص گردد که این بردار اندازه‌گیری دچار حمله شده است یا نه. با توجه به آزمون فرضیه، از توزیع اندازه‌گیری‌ها به‌عنوان ویژگی تشخیص استفاده‌شده است. برای تشخیص حملات داده اشتباه دو فرضیه $H_0$ و $H_1$ در نظر گرفته‌شده است: $H_0$ فرضیه بی‌اثری می‌باشد که هنگامی‌که اندازه‌گیری معتبر است استفاده می‌گردد و $H_1$ فرضیه جایگزین است که برای اندازه‌گیر موردحمله قرارگرفته استفاده می‌شود. با در نظر گرفتن عناصر غیر صفر در بردار حمله، دو فرضیه زیر را می‌توان در نظر داشت:

$$H_0: \|a\|_0 = 0$$
$$H_1: \|a\|_0 > 0 \qquad (۱۴-۳)$$

با توجه به بخش ۳-۲ و ۳-۳، باقیمانده اندازه‌گیری در تخمین حالت می‌تواند به دو بخش تقسیم گردد: $(z - H\hat{x})$ و $(a - Hc)$ که با استفاده از بزرگ‌ترین باقی‌مانده نرمالیز شده [1](که در بخش ۲-۵-۳ توضیح داده شد)قابل‌تشخیص نمی‌باشد واز بردار اندازه‌گیری و بردار حمله به دست می‌آید. لازم به یادآوری است که حملات تزریق داده اشتباه با استفاده از تست (بخش ۲-۵-۳)قابل‌تشخیص نمی‌باشد چراکه درصورتی‌که مهاجم توپولوژی سیستم و الگوریتم تشخیص داده بد را بداند، در اندازه‌گیری اشتباه، $a - Hc$ برابر صفر خواهد بود[۴۹].

اما در [۴۹] مدل بایسین [2]فرض شده است که در آن اندازه‌گیری‌ها با استفاده از توزیع گاوسی چندمتغیره به‌صورت تصادفی بوده و بر اساس داده پیشین تخمین زده می‌شود. اما لازم به ذکر است که توزیع گاوسی اغلب برای توصیف پدیده‌های کیفی در علوم طبیعی و رفتاری مورداستفاده قرار می‌گیرد. توزیع گاوسی ازنظر تئوری می‌تواند بدین‌صورت تعبیر گردد که با فرض تعداد زیادی اثرات مستقل کوچک به‌صورت افزایشی در هر مشاهده شرکت نماید. اما در صورت وجود حملات تزریق داده اشتباه، برخی از اندازه‌گیری‌های خاص باید به‌صورت مرزی تغییر نموده و ترکیب آن اندازه‌گیری‌ها منجر به دور شدن متغیرهای حالت از مقادیر درست خود می‌شود. اما باید این را دانست که الگوریتم تشخیصی اثربخش‌تر است که نرخ تشخیص بالاتر و نرخ مثبت اشتباه کمتری داشته باشد[۴۹].

همچنین در [۴۹] برای تشخیص حملات که در داده‌ها به‌صورت مرزی در طی بازه زمانی دستکاری می‌شوند، از روش تشخیص مبتنی بر زمان، روش آنلاین غیر پارامتری کاسوم [3]که مکانیزم تشخیص را تغییر می‌دهد استفاده‌شده است. بدین ترتیب با توجه به دو فرض رابطه (۳-۱۴)، الگوریتم کاسوم فرض می‌کند که مشاهده $y(i)$ تحت فرض $H_0$(با تابع توزیع احتمال $p_0$) شروع‌شده و در زمان $k_s$ به فرض $H_1$ تغییر می‌یابد. هدف این روش تشخیص شناسایی این تغییر در کمترین زمان ممکن می‌باشد. برای ارزیابی تأثیر این روش نیز دو کمیت نرخ مثبت اشتباه و زمان تشخیص در نظر

[1] Largest Normalized Residue
[2] Bayesian
[3] cusum

گرفته‌شده است. در این روش نیز الگوریتمی اثربخش‌تر است که مقادیر هر دو کمیت در آن کمتر باشد[۴۹].

به‌طور خلاصه در فصل دوم پیرامون مراجعی که از روش‌های مبتنی بر تشخیص استفاده می‌کردند نیز بحث گردید. با توجه به توضیحات فوق مشاهده می‌گردد که نوع دیگری از اقدام متقابل ارائه‌شده برای شناسایی حملات احتمالی تزریق داده‌های اشتباه با استفاده از روش بایسین[1] می‌باشد. درروش بایسین فرض می‌شود که بردار حالت‌های سیستم یک بردار تصادفی با توزیع گاوسی $\mathcal{N}(\mu_x, \Sigma_x)$ است. توزیع از داده‌های پیشین تخمین زده می‌شود. توزیع تخمین‌زده شده به‌عنوان یک مرجع در آزمون فرضیه برای حالت جدید استفاده می‌گردد. این روش از حملاتی که منجر به حالات غیرطبیعی شدید سیستم می‌شود، جلوگیری می‌کند.

اما ضعف روش بایسین این است که نمی‌تواند حملاتی که داده‌های اندازه‌گیری متناسب با توزیع داده‌های پیشین را تزریق می‌کند، تشخیص دهد. برای مثال، اگر یک مهاجم داده‌های اندازه‌گیری فعلی را با داده‌های اندازه‌گیری قبلی که در توزیع قرار می‌گیرند، جایگزین کند، روش مبتنی بر بایسین نمی‌تواند حمله را تشخیص دهد. در این پژوهش، روش جدیدی ارائه می‌شود که می‌تواند بر مشکلات فوق غلبه کند.

### ۳-۴-۲- روش پیشنهادی

سیستم‌های قدرت به‌عنوان سیستم‌های شبه استاتیک در نظر گرفته می‌شوند. در سیستم‌های شبه استاتیک، حالت سیستم دائماً ولی به‌آرامی در حال تغییر می‌باشد به‌طوری‌که وضعیت سیستم در هرلحظهٔ تنها مقدار کمی از وضعیت قبلی سیستم فاصله دارد. در سیستم‌های قدرت ،این امر به این معنی است که اندازه‌گیری‌های به‌دست‌آمده از RTUها باید به‌آرامی تغییر نماید.

روش پیشنهادی ،حملات تزریق اطلاعات غلط را با ردیابی تغییرات اندازه‌گیری بین مراحل متوالی تشخیص می‌دهد. بطوریکه وجود تغییرات اندازه‌گیری بزرگ‌تر می‌تواند نشان از وجود حملات تزریق

[1] Bayesian

اطلاعات غلط باشد. برای تعیین میزان تغییرات اندازه‌گیری، از شاخصی بنام فاصله نسبی لگاریتمی استفاده می‌گردد.

زمانی که هیچ تزریق داده اشتباهی وجود ندارد، شاخص فاصلهٔ نسبتاً کوچک خواهد بود. با تزریق داده‌های اشتباه به سیستم‌های قدرت، شاخص فاصله افزایش خواهد یافت.لذا برای تشخیص حملات تزریق اطلاعات غلط، برای شاخص موردنظر، یک مقدار حد تعیین می‌شود.

### ۳-۴-۲-۱- فاصله نسبی لگاریتمی

این شاخص فاصله در حقیقت اختلاف لگاریتمی بین تغییرات اندازه‌گیری گام زمانی فعلی با گام زمانی قبلی و تغییرات اندازه‌گیری اطلاعات تاریخی می‌باشد. شاخص فاصله پیشنهادی از شاخص KLD[1] [۱۶] الهام گرفته است و شکل تغییریافته آن می‌باشد.

شاخص KLD که به آن افت نیز اطلاق می‌گردد در حقیقت اختلاف بین دو توزیع احتمال را اندازه‌گیری می‌کند. از دیدگاه تئوری اطلاعات، KLD داده‌های اضافی می‌باشد که برای انتقال یک فرآیند تصادفی($\{p_i\}$) به همراه فرآیند رمزگذاری شده نامناسب $\{q_i\}$ که جایگزین آن است، لازم می-باشد[۴۰].

شاخص KLD در سال ۱۹۵۱ توسط Richard Leibler و Solomon Kullback معرفی‌شده است. این شاخص کاربرد بسیاری دارد. در مرجع [۳۸] از KLD برای اصلاح بافت استفاده‌شده است. در [۳۹]، شاخص KLD برای کمک به بهبود جستجوی صوتی مورداستفاده قرارگرفته است. در [۴۰] بیان‌شده است که شاخص KLD حتی می‌تواند تغییرات غیر ایستای سیگنال‌های عصبی را نیز نشان دهد. بااین‌وجود شاخص فاصله پیشنهادی به‌صورت زیر تعریف می‌شود:

$$D_i = 0.01 \times \sum_{k=0}^{m} \left| ln\, DZ_i^c - ln\, DZ_i^h(k) \right| \qquad (۱۵-۳)$$

[1] Kullback-Leibler

که $DZ_i^c$ تغییرات اندازه‌گیری بین گام زمانی فعلی و گام زمانی قبلی(که در این پروژه اختلاف گام‌ها ۵ دقیقه می‌باشد) و $DZ_i^h(k)$ تغییرات اندازه‌گیری اطلاعات گذشته در کل زمان می‌باشد. $m$ تعداد کل گام‌های اطلاعات گذشته است و $k$ گام زمانی می‌باشد. در تعریف بالا، قرارداد می‌شود که $|\ln DZ_i^c - \ln 0| = \infty$ و $|\ln 0 - \ln DZ_i^h| = -\infty$ . شاخص فاصله پیشنهادی، فاصله متریک واقعی نمی‌باشد. مقدار آن همواره غیر منفی بوده و همچنین تنها در حالتی که $DZ_i^c = DZ_i^h$ باشد صفر می‌شود. در مسئله موردبررسی در این پژوهش، از شاخص فاصله تعریف‌شده در رابطه (۳-15) برای تشخیص حملات سایبری پنهان در سیستم قدرت استفاده می‌شود.

برای درک بهتر عملکرد شاخص فوق، در ذیل شاخص دیگری تعریف می‌کنیم، و با مقایسه نتایج به‌دست‌آمده برای این دو شاخص، می‌توان اثبات کرد که فاصله نسبی لگاریتمی، شاخص مناسبی برای تشخیص تزریق داده‌های اشتباه می‌باشد.

### ۳-۴-۲-۲- فاصله مطلق

این شاخص یک روش ساده و بدون هیچ پیچیدگی با مقایسه اختلاف بین تغییرات اندازه‌گیری فعلی و گذشته می‌باشد. در این پژوهش این شاخص، فاصله مطلق نامیده می‌شود. این فاصله به‌صورت زیر تعریف می‌شود:

$$AD_i = 0.01 \times \sum_{k=0}^{m} \left| DZ_i^c - DZ_i^h(k) \right| \qquad (۱۶-۳)$$

## ۳-۵- خلاصه فصل

در این فصل در ابتدا پس از بیان مقدمه و مسئله تحقیق، پیرامون هدف تحقیق بحث گردید و سپس در بخش بعد تخمین حالت در شبکه‌های هوشمند به‌طور خلاصه تشریح شد و ساختار و نحوه مدل‌سازی سیستم جهت تخمین حالت AC و همچنین قیود و محدودیت‌های مسئله بحث شد. در ادامه تشخیص داده بد و حملات تزریق داده اشتباه در تخمین حالت DC موردبررسی قرار گرفت و انواع روش‌های مقابله با حملات تزریق داده اشتباه بیان گردید. کلیه روش‌های مقابله با تزریق داده

اشتباه در دودسته روش‌های مبتنی بر حفاظت و مبتنی بر تشخیص قرار می‌گیرند. هرکدام از روش‌ها موردبحث قرارگرفته و مشکلات هریک معرفی گردید. سپس روش پیشنهادی جهت مقابله در برابر حملات تزریق داده اشتباه بررسی شد و مدل و نحوه اجرای آن مطرح گردید. همان‌گونه که اشاره شد روش مورداستفاده، روش فاصله نسبی لگاریتمی می‌باشد که از شاخص KLD الهام گرفته‌شده است. در فصل بعد مدل سیستم پیشنهادی در این فصل بر روی شبکه ۱۴ باسه موردبررسی قرار می‌گیرد و نتایج آن ارائه می‌گردد.

# فصل چهارم:

# شبیه‌سازی و ارزیابی روش پیشنهادی

## ۴-۱- مقدمه

در شبکه الکتریکی هرروز شاهد ارتباط بیشتر بین دارایی‌های سایبری و زیرساخت‌های فیزیکی کنترل تولید، انتقال و توزیع می‌باشیم. با توجه به تقاضای رو به افزایش جهت سرویس‌های الکتریکی قابل‌اطمینان، با ظرفیت بالا و اقتصادی لازم است که کنترل و مانیتورینگ زمان حقیقی در بهره-برداری از سیستم‌های قدرت بیشتر در نظر گرفته شود. اما امنیت و قابلیت اطمینان شبکه قدرت در تمامی زمان‌ها تضمین شدنی نمی‌باشد و برخی رویدادها می‌تواند مسائل و مشکلاتی جدی برای تولیدکنندگان و مصرف‌کنندگان الکتریسیته به وجود آورد. به‌عنوان‌مثال خاموشی سراسر سال ۲۰۰۳ در Northeast نشان داد که حتی یک خطای کوچک در بخشی از شبکه قدرت(در این حالت خروج یک خط انتقال در اوهایو شمالی) تأثیرات متوالی دارد که منجر به بیلیون‌ها دلار خسارات اقتصادی می‌شود. امروزه بااتصال ادوات سایبری و فیزیکی حملات سایبری در شبکه قدرت افزایش‌یافته که می‌تواند منجر به خروج توان و حتی خاموشی سیستم، و یا خسارات مالی سنگین به دلیل بهره‌برداری غیر بهینه از شبکه قدرت شود[۳۰].

اما تخمین حالت که حالت بهره‌برداری از سیستم قدرت را با توجه به مدل زمان حقیقی شبکه الکتریکی تخمین می‌زند، تابعی کلیدی از سیستم مدیریت انرژی(EMS) می‌باشد[۳۰]. در سیستم-های قدرت، متغیرهای حالت شامل مقادیر ولتاژ و زوایای نسبی فاز در گره‌های سیستم می‌باشند. شرکت‌های برق معمولاً از اطلاعات قبلی بار مصرفی برای پیش‌بینی بار در فیدرهای توزیع جهت کنترل و تحلیل فیدر به‌صورت بدون وقفه استفاده می‌نمایند. اندازه‌گیری‌هایی موردنیاز است تا بتوان عملکرد سیستم را در وضعیت بلادرنگ هم برای کنترل قابلیت اطمینان و هم برای قیود موجود در توزیع اقتصادی بار، تخمین زد. تخمین حالت مهم‌ترین قسمت در پایش شبکه قدرت است که طی آن حالت سیستم تعیین‌شده و بهره‌بردار به کمک آن قادر به تصمیم‌گیری مناسب در مورد اعمال احتمالی لازم جهت حفظ عملکرد سیستم در حالت عادی و مطمئن می‌باشد. بهبود در دقت تخمین حالت یکی از مزایای مهم PMU می‌باشد[۵۰].

روش‌های تخمین حالت مدرن در دهه ۱۹۷۰ ابداع شدند. در این روش‌ها، فلوی توان اکتیو و راکتیو خطوط و اندازه‌های ولتاژ از باس‌بار پست‌ها با استفاده از اندازه‌گیری به‌دست‌آمده و با سیستم اسکادا به یک واحد مرکزی برای انجام محاسبات ارسال می‌شدند. هنوز در بسیاری از کشورهای جهان، از همین روش برای تخمین حالت شبکه استفاده می‌شود. با توجه به کند بودن شبکه مخابراتی، محدودیت باند فرکانسی و عدم وجود هم‌زمانی در جمع‌آوری داده‌ها، داده‌های اندازه‌گیری شده از بخش‌های مختلف شبکه تقدم و تاخر زمانی به‌اندازه چندین ثانیه تا چند دقیقه نسبت به یکدیگر داشتند. لذا حالت تخمین زده‌شده تنها در شرایط ماندگار از دقت مناسب برخوردار بود. با در نظر گرفتن امکان بروز تغییرات و فعال شدن دینامیک شبکه در این محدوده زمانی، نتایج، تنها تقریبی از حالت واقعی سیستم را به دست می‌داد که در خوش‌بینانه‌ترین نگاه، مقدار متوسطی از حالت واقعی سیستم بود و لذا به نام «تخمین حالت استاتیکی» خوانده می‌شد. به همین دلیل سرعت و هم‌زمانی ایجادشده درروش اندازه‌گیری فازوری هم‌زمان مؤلفه‌های ولتاژ باس‌بارها(و همچنین جریان‌ها) باعث شد که این روش به‌طور مستقیم، ابزار طبیعی انجام تخمین حالت یا به عبارت بهتر «اندازه‌گیری حالت» در شبکه محسوب شود. حتی اگر در مرکز کنترل هیچ نرم‌افزار تخمین حالتی هم وجود نداشته باشد، درصورتی‌که PMUها در تمامی نقاط موردنظر نصب‌شده باشند، اطلاعات فراهم آمده، نماینده حالت سیستم در هرلحظه است. اما این نکته را باید در نظر گرفت که در صورت حذف کامل تخمین حالت و استفاده از PMU ها در کل شبکه به‌عنوان نماینده تخمین حالت قطعاً نسبت به خطاهای اندازه‌گیری و یا شکست در اندازه‌گیری‌های از راه دور بسیار آسیب‌پذیر خواهد بود [۵۱].

نکته مهم استفاده از اندازه‌گیری فازوری جهت تخمین حالت سیستم آن است که به‌منظور تخمین حالت سیستم لزومی ندارد که اندازه‌گیری در تمامی نقاط موردنظر انجام شود. داشتن تعداد محدودی PMU در نقاط کلیدی شبکه به کمک نرم‌افزارهای موجود، کل سیستم را رؤیت پذیر می‌کند و لذا دغدغه مستمری برای نصب PMUهای جدید در اثر اجرای طرح‌های توسعه شبکه وجود ندارد[۵۰].

اغلب در سیستم قدرت برای تخمین حالت‌های سیستم از مدل اندازه‌گیری خطی سازی شده استفاده می‌شود که مبتنی بر اندازه‌گیری‌ها در باس‌ها یا خطوط انتقال می‌باشند. بخصوص مرکز کنترل انرژی(ECC) هر چند ثانیه و یا دقیقه توان‌های اکتیو و راکتیو عبوری از خطوط و تزریقی از باس‌ها را به‌عنوان داده اندازه‌گیری شده از سیستم دریافت داده و کنترل نظارتی(SCADA) دریافت می‌نماید[۳۰].

ورودی به یک تخمینگر شامل اندازه‌گیری‌های ناقص از مقادیر ولتاژ و توان، توان موهومی یا توان ظاهری است. تخمینگر بدین‌صورت طراحی می‌شود که بهترین تخمین را از مقادیر ولتاژ و زوایای فاز در اختیار قرار دهد. با توجه به اینکه خطا در مقادیر اندازه‌گیری شده وجود دارد و این‌که ممکن است بعضی از اندازه‌گیری‌ها اضافی باشند. سپس، اطلاعات خروجی از تخمینگر را در مراکز کنترل سیستم در مطالعه توزیع اقتصادی بار با در نظر گرفتن قابلیت اطمینان سیستم و نیز کنترل سیستم، بکار می‌برند.

در سیستم مدیریت انرژی مدرن، برنامه تخمین حالت یک سری از مقادیر خام اندازه‌گیری شده را پردازش می‌کند و یک راه‌حل پخش بار بلادرنگ را معرفی می‌کند که پایـداری را برای توسعه، مشاهده، کنترل و امنیت سیستم فراهم می‌کند. SE بر اساس روابط ریاضی بین متغیرهای حالت سیستم(مثلاً: دامنه ولتاژ و زوایای شین‌ها) و اندازه‌گیری‌ها است. روش‌های متعددی برای به دست آوردن راه‌حل SE بکار رفته است[۳۷].

تخمین حالت، حالت بهره‌برداری زمان حقیقی شبکه قدرت را ارائه نموده و به‌منظور تصمیم‌گیری برای افزایش امنیت و پایداری سیستم توسط بهره‌بردار بسیار حیاتی می‌باشد[۳۰]. پارامترهایی که برای تخمین حالت دقیق قابل‌استفاده‌اند شامل توان تزریقی اکتیو و راکتیو، اندازه ولتاژ یا جریان می‌باشد. تابع تخمینگر حالت سنتی به مرکزیت یک مرکز کنترل عمل می‌نماید و داده‌های مطلوب، زمان حقیقی و استاتیکی را جهت حل پردازشگر توپولوژی(TP)، تخمین حالت(SE) و داده بد(BD)

به‌صورت تناوبی تشخیص و حل می‌نماید. بنابراین یکی از نتایج مهم تخمین حالت بهینه بهره‌برداری مؤثر و امن سیستم قدرت در شرایط نرمال و پیش‌آمدی می‌باشد[۳۷].

بااین‌وجود دقت تخمین حالت توسط اندازه‌گیری‌های بد در سیستم قدرت تحت تأثیر قرار می‌گیرد. همچنین داده بد می‌تواند به علت وجود خطاهای توپولوژی در شبکه، اندازه‌گیری غیر نرمال ایجاد به دلیل مشکلات در دستگاه‌ها و حملات مشکوک و سایبری به وجود آید. برای تشخیص و شناسایی اندازه‌گیری‌های بد در حالت سیستم قدرت، روش‌های مبتنی بر آزمون آماری باقیمانده‌های اندازه‌گیری ارائه‌شده و مورداستفاده قرار می‌گیرد که در فصل دوم به برخی از آن‌ها اشاره گردید. اما مشخص است که حملات تزریق داده اشتباه می‌توانند روش‌های تشخیص کلاسیک مبتنی بر آزمون‌های باقیمانده را نیز تغییر دهند و دستکاری نمایند. حملات تزریق داده سنکرون به دستگاه‌های اندازه‌گیری با دانستن توپولوژی سیستم، قابلیت اعمال به دستگاه‌ها به همراه اندازه‌گیری‌های خود را دارد. بعلاوه بردارهای حمله می‌توانند به صورتی مؤثر و سیستماتیک ساخته شوند که حتی در صورت محدودیت مهاجم در منابع که شامل دستگاه‌ها نیز می‌شود، فرآیند تخمین حالت بدین ترتیب گمراه شده و الگوریتم‌های کنترلی سیستم قدرت تحت تأثیر قرار بگیرد. بنابراین لازم است که درزمینهٔ آسیب‌پذیری تخمین حالت در برابر حملات تزریق داده اشتباه که عواقب بسیار بدی را در شبکه ایجاد می‌نماید، توجهی بیش‌ازپیش صورت گیرد[۳۰].

آشکار ساختن حملات تزریق داده اشتباه برای امنیت و قابلیت اطمینان سیستم قدرت امری بسیار تعیین‌کننده است. بنابراین این امر چالشی مهم در سیستم قدرت می‌باشد چراکه مهاجمین ممکن است بتوانند بردارهای حملات داده اشتباه در برابر شمای حفاظتی را تشکیل داده و بردارهای حملات را به سیستم قدرت تزریق نمایند که این حملات می‌تواند روش‌های کلاسیک جهت تشخیص داده بد را دور بزند. بعلاوه داده اندازه‌گیری معیوب به دلیل حملات بی‌وقفه و یا خرابی دستگاه‌ها، تشخیص حملات مشکوک را پیچیده نموده و مسئله تخمین حالت را سخت می‌نماید[۳۰].

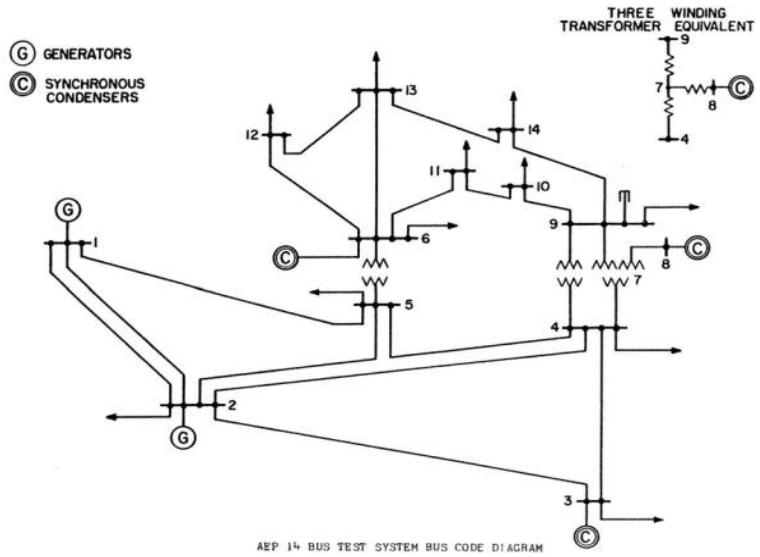
اما همان‌گونه که پیش‌تر نیز بیان گردید در فصل پیشین مسئله تشخیص حملات تزریق داده اشتباه در تخمین حالت AC در شبکه قدرت موردبررسی قرار گرفت. همچنین روش جدید مبتنی بر تشخیص برای برطرف شدن محدودیت‌های روش‌های موجود جهت تشخیص داده‌های بد نوع سوم ارائه شد. مشخص شد که ایده اصلی روش پیشنهادی ردیابی تغییرات اندازه‌گیری‌ها بین مراحل متوالی می‌باشد. سپس شاخص‌های فاصله از اندازه‌گیری‌های گذشته با استفاده از روش فاصله نسبی لگاریتمی محاسبه می‌شوند. مقدار آستانه که از داده‌های پیشین محاسبه می‌شود، برای تشخیص حملات پنهانی تزریق داده‌های اشتباه مورداستفاده قرار می‌گیرد. به این صورت که هنگامی‌که داده اشتباه به سیستم قدرت تزریق می‌شود، هیستوگرام تغییرات اندازه‌گیری از اندازه‌گیری‌های گذشته منحرف‌شده و درنتیجه به یک شاخص فاصله بزرگ‌تر منجر می‌شود. اگر شاخص فاصله بزرگ‌تر از آستانه باشد، این نتیجه دریافت می‌گردد که اندازه‌گیری‌ها و داده‌های جدید دریافتی دستکاری‌شده و تقلبی می‌باشند. بنابراین نحوه حل مسئله در فصل گذشته به‌تفصیل بیان گردید.

روش پیشنهادی در فصل گذشته جهت تست و بررسی صحت، در این فصل بر روی شبکه‌ی تست ۱۴ باسه تست می‌گردد. برای ارزیابی روش پیشنهادی جهت حل مسئله، روش مطروحه در فصل سوم جهت حل مسئله تشخیص تزریق داده اشتباه در شبکه تست پیاده‌سازی شده است. شبکه تست موردبررسی در این فصل شبکه ۱۴ باسه می‌باشد که در شکل ۴-۱ دیاگرام آن نشان داده‌شده است و در ادامه موردبررسی قرار می‌گیرد. اطلاعات باس‌بارها و خطوط شبکه نیز در بخش ۴-۲ آمده است. کد اصلی برنامه در نرم‌افزار متلب R2017b نوشته‌شده و اجرا گردیده است.

در این فصل ابتدا شبکه‌ی نمونه‌ای که برای بررسی روش پیشنهادی مورداستفاده قرارگرفته است، معرفی می‌گردد. سپس، شبیه‌سازی روش پیشنهادی برای این شبکه ارائه‌شده و نتایج حاصل از تشخیص حملات تزریق داده اشتباه در تخمین حالت AC در شبکه توسط روش پیشنهادی در سناریو موردنظر بررسی می‌گردد. در بخش ارائه نتایج هیستوگرام متغیرهای حالت مختلف و تغییرات اندازه‌گیری‌ها و ... در زمان‌های مختلف شامل حملات داده اشتباه و بدون حمله و ... ارائه خواهد شد.

## ۴-۲- معرفی شبکه ۱۴ باسه موردمطالعه

در این بخش، پیرامون آماده‌سازی سیستم تست به‌منظور آزمایش کردن عملکرد روش پیشنهادی بحث می‌گردد. شبکه موردبررسی در این مطالعه، شبکه ۱۴ باسه IEEE [۵۲] می‌باشد که به‌منظور تحقق اهداف مسئله، مطابق باکار انجام‌شده کمی دچار تغییرات می‌شود. این شبکه شامل ۱۴ باس بوده که ۵ باس آن شامل شین‌های ۱ و ۲ و ۳ و ۶ و ۸ آن دارای ژنراتور می‌باشد که در تمامی این باس‌ها تولید به شیوه کلاسیک صورت می‌گیرد. همچنین در این شبکه ۱۱ باس‌بار و ۲۰ خط انتقال وجود دارد که در شکل ۴-۱ نشان داده‌شده است و اطلاعات خطوط و باس‌های شبکه در جداول ۴-۱ ارائه‌شده است.




شکل ۴-۱- دیاگرام شماتیک شبکه ۱۴ باسه [۵۲]

جدول ۴-۱- اطلاعات شبکه تست

(الف) اطلاعات خطوط شبکه تست [۵۲]

| Line No | Between Buses | Line impedance | | Half Line Charging Susceptance per unit |
|---|---|---|---|---|
| | | R per unit | X per unit | |
| 1 | 1 – 2 | 0.01938 | 0.05917 | 0.02640 |
| 2 | 2 – 3 | 0.04699 | 0.19797 | 0.02190 |
| 3 | 2 – 4 | 0.05811 | 0.17632 | 0.01870 |
| 4 | 1 – 5 | 0.05403 | 0.22304 | 0.02460 |
| 5 | 2 – 5 | 0.05695 | 0.17388 | 0.01700 |
| 6 | 3 – 4 | 0.06701 | 0.17103 | 0.01730 |
| 7 | 4 – 5 | 0.01335 | 0.04211 | 0.0064 |
| 8 | 5 – 6 | 0.0 | 0.25202 | 0.0 |
| 9 | 4 – 7 | 0.0 | 0.20912 | 0.0 |
| 10 | 7 – 8 | 0.0 | 0.17615 | 0.0 |
| 11 | 4 – 9 | 0.0 | 0.55618 | 0.0 |
| 12 | 7 – 9 | 0.0 | 0.11001 | 0.0 |
| 13 | 9 – 10 | 0.03181 | 0.08450 | 0.0 |
| 14 | 6 – 11 | 0.09498 | 0.19890 | 0.0 |
| 15 | 6 – 12 | 0.12291 | 0.25581 | 0.0 |
| 16 | 6 – 13 | 0.06615 | 0.13027 | 0.0 |
| 17 | 9 – 14 | 0.12711 | 0.27038 | 0.0 |
| 18 | 10 – 11 | 0.8205 | 0.19207 | 0.0 |
| 19 | 12 – 13 | 0.22092 | 0.19988 | 0.0 |
| 20 | 13 – 14 | 0.17093 | 0.34802 | 0.0 |

(ب) اطلاعات باس‌های شبکه تست [۵۲]

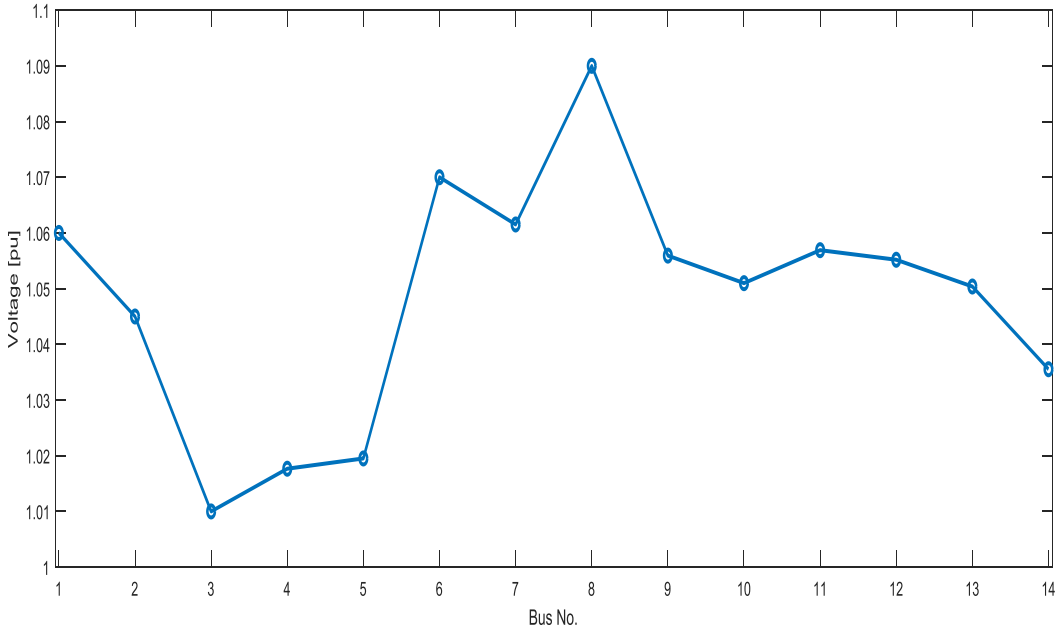
| Bus number | Starting bus voltage | | Generation | | Load | |
|---|---|---|---|---|---|---|
| | Magnitude p.u. | Phase angle deg | MW | MVAr | MW | MVAr |
| 1* | 1·06 | 0 | 0 | 0 | 0 | 0 |
| 2 | 1·0 | 0 | 40 | 0 | 21·7 | 12·7 |
| 3 | 1·0 | 0 | 0 | 0 | 94·2 | 19·0 |
| 4 | 1·0 | 0 | 0 | 0 | 47·8 | −3·9 |
| 5 | 1·0 | 0 | 0 | 0 | 7·6 | 1·6 |
| 6 | 1·0 | 0 | 0 | 0 | 11·2 | 7·5 |
| 7 | 1·0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 1·0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 1·0 | 0 | 0 | 0 | 29·5 | 16·6 |
| 10 | 1·0 | 0 | 0 | 0 | 9·0 | 5·8 |
| 11 | 1·0 | 0 | 0 | 0 | 3·5 | 1·8 |
| 12 | 1·0 | 0 | 0 | 0 | 6·1 | 1·6 |
| 13 | 1·0 | 0 | 0 | 0 | 13·5 | 5·8 |
| 14 | 1·0 | 0 | 0 | 0 | 14·9 | 5·0 |

همچنین توان مبنای این شبکه ۱۰۰MVA است و بار نامی آن ۲۵۹MW و ۷۳.۵MVar می‌باشد. دیگر اطلاعات مربوط به این شبکه در مرجع [۵۲] آمده است. میزان تلفات توان اکتیو و راکتیو در حالت پایه و بدون هیچ‌گونه واحد جبران سازی در این شبکه به ترتیب برابر با 13/3933KW و 30/1224KVAR می‌باشد.

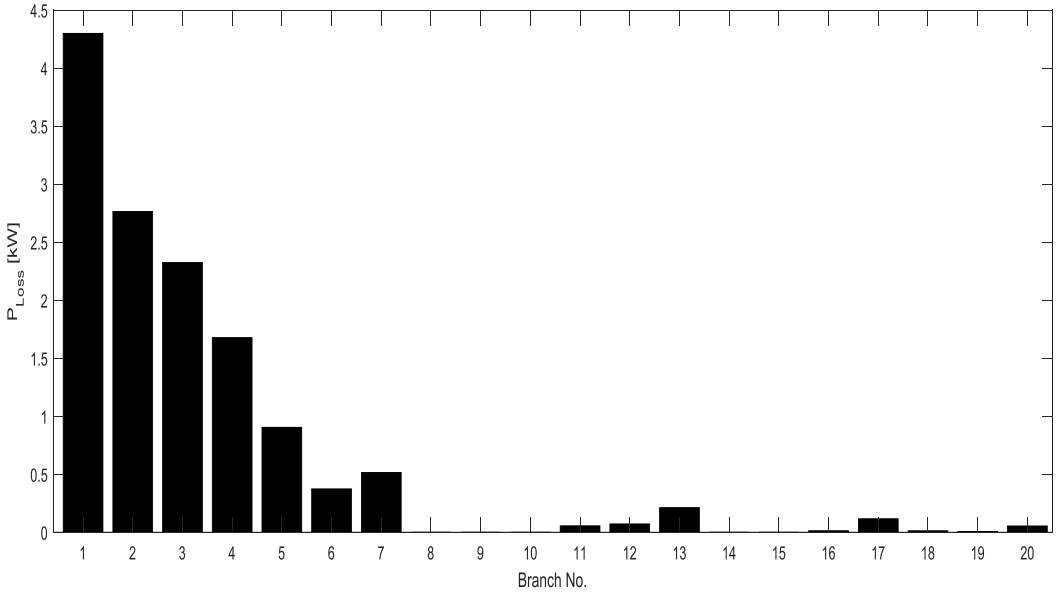
در مسئله پخش بار، باس شماره ۱ باس اسلک بوده و مابقی باس‌ها به‌عنوان باس PQ در نظر گرفته می‌شوند به‌جز باس‌هایی که در آن‌ها تولید نیز وجود دارد که به‌عنوان باس PV فرض می‌گردند. مقادیر مثبت توان راکتیو نشان‌دهنده حالت القایی و مقادیر منفی توان راکتیو نشان‌دهنده حالت خازنی می‌باشد. محدوده‌های بالایی و پایینی ولتاژ برای تمامی باس‌های این شبکه انتقال به ترتیب 0/9pu و 1/1pu در نظر گرفته‌شده است.

شکل ۴-۲ منحنی پروفیل ولتاژ این شبکه و شکل ۴-۳ منحنی تلفات خطوط و شکل ۴-۴ منحنی توان عبوری از خطوط شبکه ۱۴ باسه را نشان می‌دهد. با مشاهده نمودارهای این شبکه مشاهده می‌شود که میزان تلفات در حالت پایه در این شبکه برابر با 3933KW و 30/1224KVAR می‌باشد که حدوداً برابر با 0/05% بار کل شبکه است و همچنین کمترین باس شبکه ازلحاظ سطح ولتاژ، باس ابتدایی شماره ۳ با مقدار ۱/۱pu می‌باشد. همچنین مشخص است که ولتاژ شبکه کاملاً بین محدوده

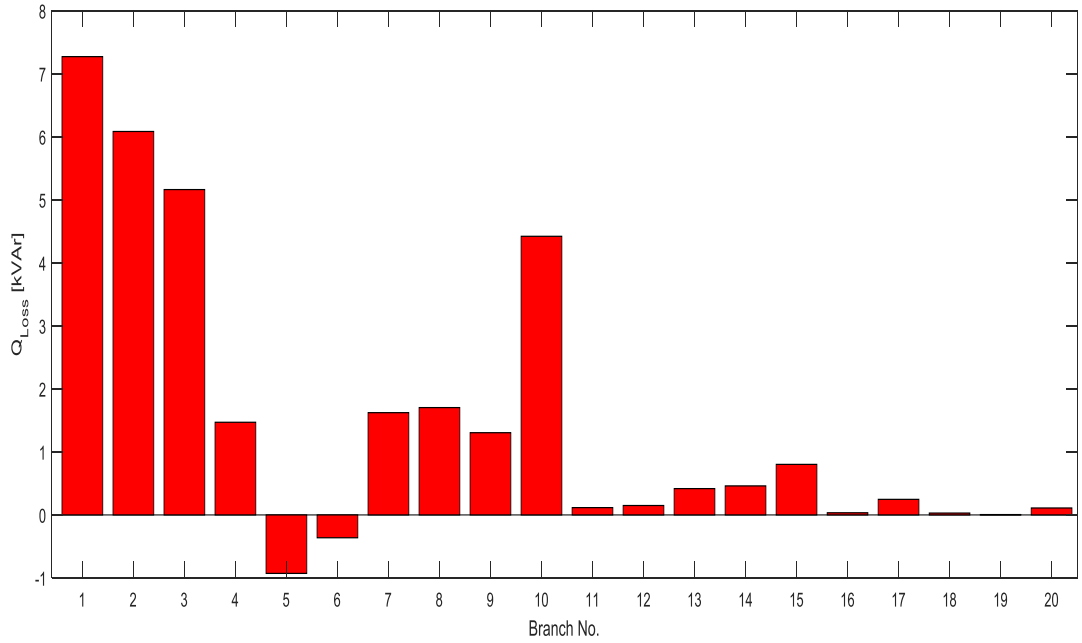
تعریف‌شده می‌باشد که با توجه به نوع انتقال این شبکه این امر بدیهی بوده چراکه تلفات آن بسیار کم و قابل صرف‌نظر است و درنتیجه افت ولتاژ آن نیز بدون وقوع هیچ رویدادی ناچیز است. زیرا در شبکه انتقال خاصیت اهمی خطوط بسیار کم و ناچیز می‌باشد.




شکل ۴-۲- منحنی پروفیل ولتاژ شبکه ۱۴ باسه

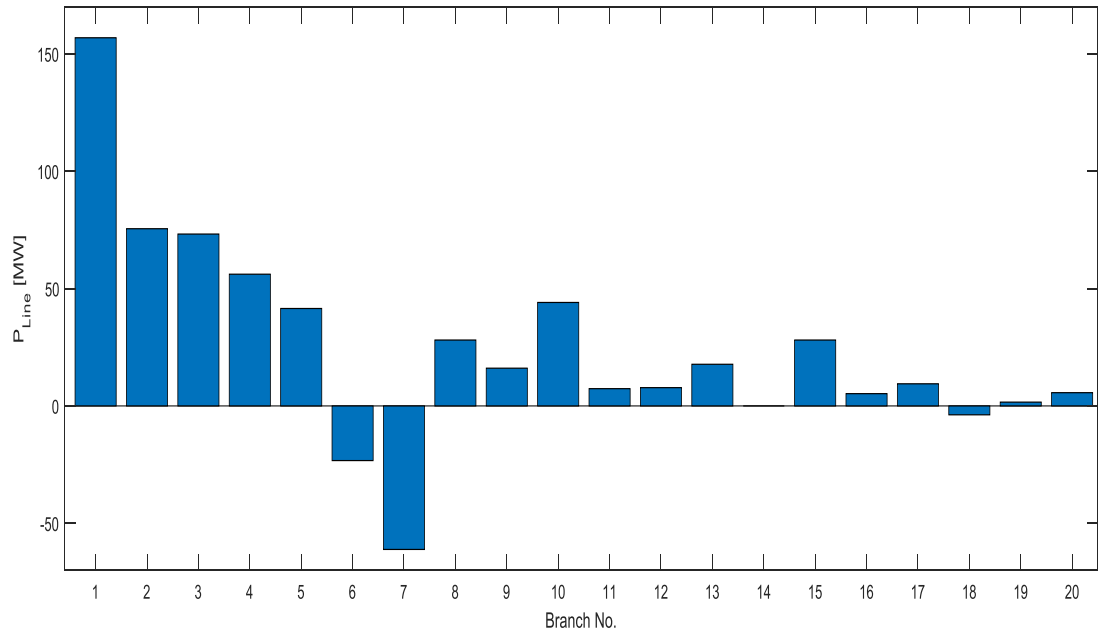



(الف) تلفات توان اکتیو

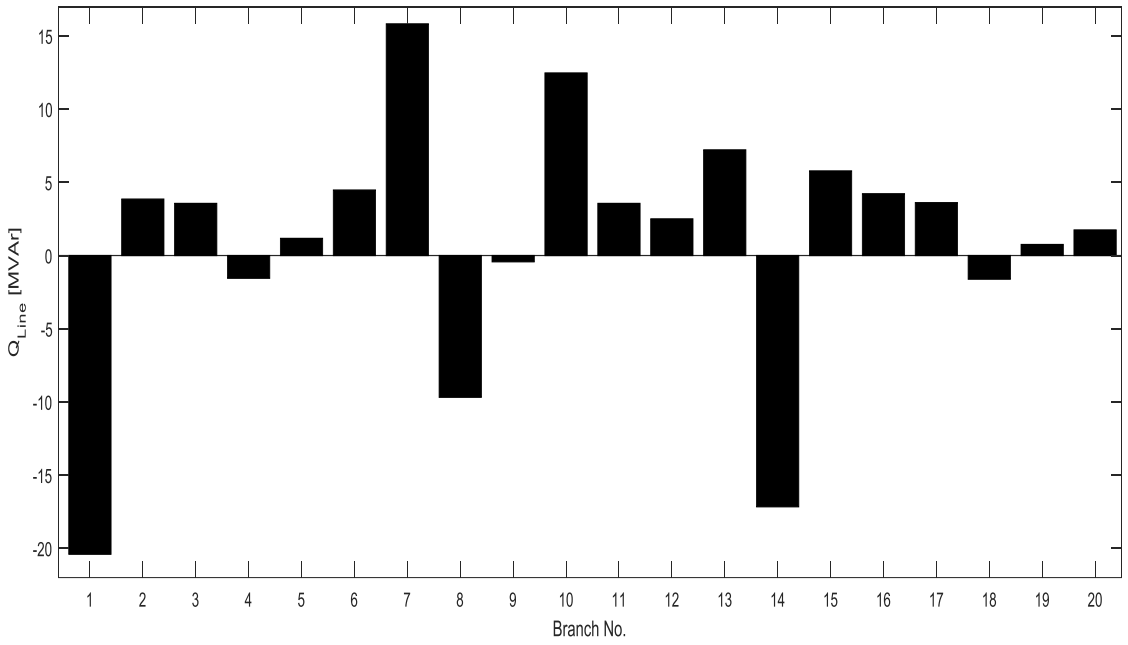



(ب) تلفات توان راکتیو

شکل ۴-۳- منحنی تلفات توان در هر خط شبکه ۱۴ باسه




(الف) توان اکتیو




(ب) توان راکتیو

شکل ۴-۴- منحنی توان عبوری از هر خط شبکه ۱۴ باسه

با توجه به محدودیت ذکرشده برای ولتاژ بین $0.9 \leq |V_j| \leq 1.1$ ولتاژ تمامی باس‌ها در محدوده مجاز تعریف‌شده می‌باشد و تلفات خطوط شبکه هم‌مقدار متعادل و کمی برای یک شبکه ۱۴ باسه می‌باشد.

تلفات اکتیو خطوط مربوط به خطوطی می‌باشد که دارای بخش اهمی هستند و همچنین تلفات توان منفی نشان‌دهنده خاصیت خازنی آن خط می‌باشد که توان راکتیو جذب نمی‌کند و تولید می‌نماید. زیرا شبکه ۱۴ باسه یک شبکه انتقال است.

همچنین توان عبوری خطوطی که منفی می‌باشد بدین معنی است که این جهت شارش توان عکس جهت در نظر گرفته‌شده می‌باشد. با توجه به شکل‌های فوق همان‌گونه که مشاهده می‌شود به علت ساختار حلقوی شبکه جریان عبوری از خطوط متفاوت بوده به مقدار بار موجود در باس‌های نزدیکی آن خط بستگی دارد و بنابراین لازم است تا مانیتورینگ شبکه توسط روش تخمین حالت دائم صورت گیرد تا در صورت وجود تغییرات ناگهانی و وقوع پیشامد و ... بتوان از فروپاشی آن جلوگیری

به عمل آورد. اما در کنار تخمین حالت، با توجه به هوشمند بودن شبکه لازم است که روشی برای تشخیص حملات تزریق داده اشتباه نیز بکار گرفته شود.


شکل ۴-۵- تصویر NYISO از ۱۱ نواحی سیستم قدرت الکتریکی در ایالت نیویورک کشور USA[۵۴]

اما با توجه به موضوع پژوهش و تست روش پیشنهادی در تشخیص حملات تزریق داده اشتباه، داده بار مورداستفاده در این شبکه تست، بر اساس اپراتور مستقل سیستم در نیویورک(NYISO[1]) از سال ۲۰۱۲ تنظیم‌شده است. با توجه به شکل ۴-۵، درداده NYISO، ۱۱ ناحیه دارای بار وجود دارد. فاصله زمانی داده بارها، پنج دقیقه می‌باشد.

[1] New York independent system operator

### ۴-۲-۱- روند تولید داده‌های شبکه تست و حل مسئله به روش پیشنهادی

با توجه به فقدان داده حالت سیستم در هر پنج دقیقه، برای تولید داده‌های حالت سیستم از الگوی بار NYISO و همچنین نحوه شبیه‌سازی روش پیشنهادی، از روند زیر استفاده‌شده است که فلوچارت آن نیز در شکل ۴-۶ ارائه‌شده است:


شکل ۴-۶- فلوچارت تولید داده‌های حالت سیستم از الگوی بار NYISO و همچنین نحوه شبیه‌سازی روش پیشنهادی

**مرحله ۱:** اطلاعات ثبت‌شده مربوط به شبکه‌ی نیویورک برای مدل‌سازی اطلاعات شبکه موردمطالعه در نظر گرفته‌شده است. این اطلاعات مربوط به سال ۲۰۱۲ که به‌صورت ۵ دقیقه‌ای ذخیره‌شده و برای هر ۱۱ منطقه این شبکه به‌صورت جداگانه در نظر گرفته‌شده است. بدین ترتیب نمونه‌های موردنظر برای شبکه موردمطالعه به‌صورت ۵ دقیقه‌ای و در بازه یک‌ساله در نظر گرفته‌شده‌اند. اسامی مناطق شبکه نیویورک عبارت‌اند از:

Capital, Central, Dunwod, Genese, Hud VL, Longil, MHK VL, Millwd, N.Y.C., North, West

**مرحله ۲:** در مرحله دوم اطلاعات شبکه نیویورک بر روی شبکه ۱۴ باسه IEEE قرار داده می‌شود. مراحل انجام این کار به این صورت است که مقدار بیشینه سطح توان شبکه نیویورک مساوی با مقدار بیشینه سطح توان شبکه ۱۴ باسه در نظر گرفته می‌شود. سپس با همان نسبت تبدیل مقدار توان اکتیو تمامی نواحی دیگر تصحیح خواهد شد. حال هر یک از نواحی از طریق یک ماتریس لینک بر روی شبکه ۱۴ باسه نگاشت می‌گردد. ارتباط هر باس‌بار سیستم ۱۴ باسه IEEE با یک ناحیه از NYISO با استفاده از ماتریس زیر صورت می‌گیرد:

$$\begin{bmatrix} 2 & 3 & 4 & 5 & 6 & 9 & 10 & 11 & 12 & 13 & 14 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \end{bmatrix} \quad (۱-۴)$$

سطر اول ماتریس فوق، شماره باس سیستم ۱۴ باس IEEE می‌باشد و سطر دوم آن مربوط به شماره ناحیه NYISO است. برای محاسبه توان راکتیو شبکه موردمطالعه نیز بدین گونه عمل می‌شود که با توجه به ضریب توان هر باس شبکه ۱۴ باسه استاندارد IEEE، از روی توان اکتیو نگاشت شده بر روی شبکه ۱۴ باسه، مقدار توان راکتیوی که باید نگاشت شود، محاسبه خواهد شد. به عبارتی بار NYISO با بار اکتیو و راکتیو اولیه شبکه ۱۴ باس IEEE نرمالیزه می‌شود، به‌گونه‌ای که شبکه تست نزدیک به حالت اولیه‌ی سیستم ۱۴ باسه IEEE بهره‌برداری گردد. پس‌ازاین مرحله، داده بار اکیتو و راکتیو برای سیستم ۱۴ باسه IEEE به دست خواهد آمد. با توجه به فقدان اطلاعات بار راکتیو، فرض می‌گردد که بار سیستم دارای یک ضریب توان ثابت می‌باشد و بنابراین نیاز است که تنها توان

حقیقی(اکتیو) پیش‌بینی گردد. اگر داده‌های قبلی از توان راکتیو در دسترس باشد، می‌توان این فرض را اصلاح نمود.

**مرحله ۳:** افزودن بار اکتیو جدید. یافتن نسبت کل بار جدید به‌کل بار اولیه شبکه ۱۴ باسه IEEE. ضرب کردن این نسبت در تولید تمامی ژنراتورها. در اینجا، فرض می‌گردد که تولیدات ژنراتورها با همان نسبت مانند بار کل، افزایش می‌یابد. این فرض می‌تواند بسته به نظر اپراتورهای سیستم قابل تنظیم باشد چراکه بهره‌برداران سیستم، از برنامه‌ریزی زمان‌های پیش‌رو اطلاع دارند.

**مرحله ۴:** تکرار مرحله قبل برای توان راکتیو.

**مرحله ۵:** محاسبه حالت سیستم($X$) با استفاده از آنالیز پخش بار. در این مرحله پس از تشکیل شبکه اصلاح‌شده، برای هر نمونه موردمطالعه، با اعمال پخش بار مقدار متغیرهای حالت و اندازه‌گیرهای شبکه محاسبه خواهد شد. ترتیب متغیرها در بردار متغیرهای شبکه به‌صورت زیر می‌باشد:

$$X = [X_1, X_2, \dots, X_{14}, X_{15}, X_{16}, \dots, X_{27}] = [V_1, V_2, \dots, V_{14}, \theta_2, \theta_3, \dots, \theta_{14}] \quad (۲-۴)$$

**مرحله ۶:** محاسبه مقدار اندازه‌گیری‌های سیستم $z = h(x)$، که در آن $h()$ معادله پخش بار به‌دست‌آمده از ساختار سیستم می‌باشد. ترتیب متغیرها در بردار اندازه‌گیری‌های شبکه به‌صورت زیر می‌باشد:

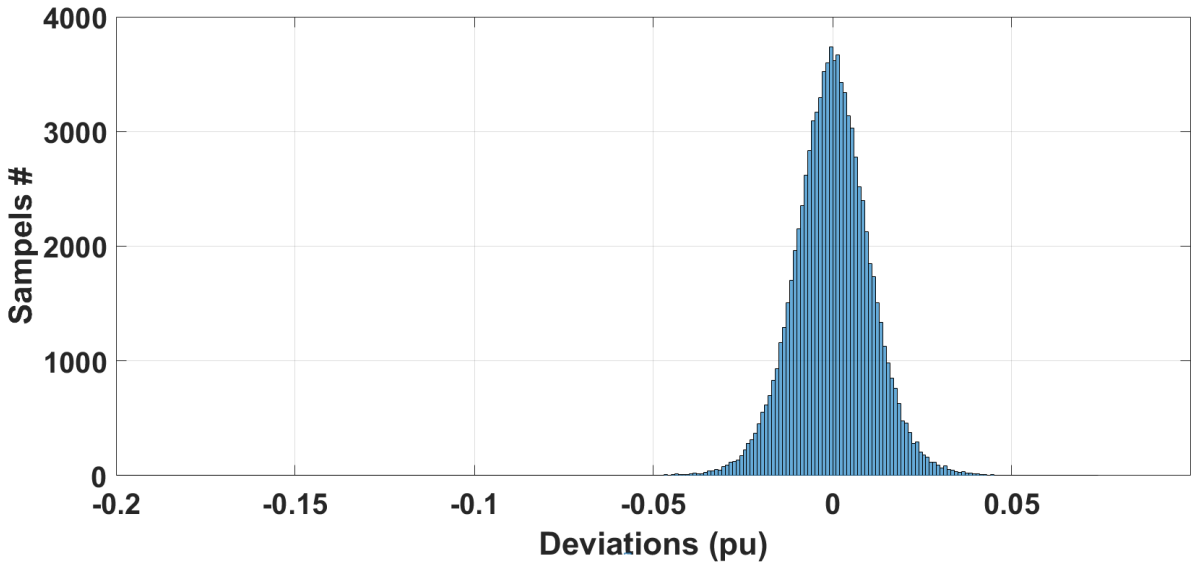
$$\begin{aligned} Z = & \\ & [Z_1, Z_2, \dots, Z_{14}, Z_{15}, Z_{16}, \dots, Z_{28}, Z_{29}, Z_{30}, \dots, Z_{48}, Z_{49}, Z_{50}, \dots, Z_{68}] \\ = & \left[P_1, P_2, \dots, P_{14}, Q_1, Q_2, \dots, Q_{14}, P_{L_1}, P_{L_2}, \dots, P_{L_{20}}, Q_{L_1}, Q_{L_2}, \dots, Q_{L_{20}}\right] \end{aligned} \quad (۳-۴)$$

**مرحله ۷:** برای محاسبه تغییرات اندازه‌گیری اطلاعات گذشته $DZ_i^h(k)$ از اطلاعات ثبت‌شده درگذشته، استفاده‌شده است. اطلاعات ۱۰ ماه اول سال شبکه موردمطالعه به‌عنوان اطلاعات تاریخی ثبت‌شده در نظر گرفته‌شده است. در این مرحله مقدار انحرافات اندازه‌گیری برای هر اندازه‌گیر

به‌صورت جداگانه از طریق رابطه (۴-۴) محاسبه می‌شود. این انحرافات برای اطلاعات تاریخی ثبت‌شده در نظر گرفته‌شده است.

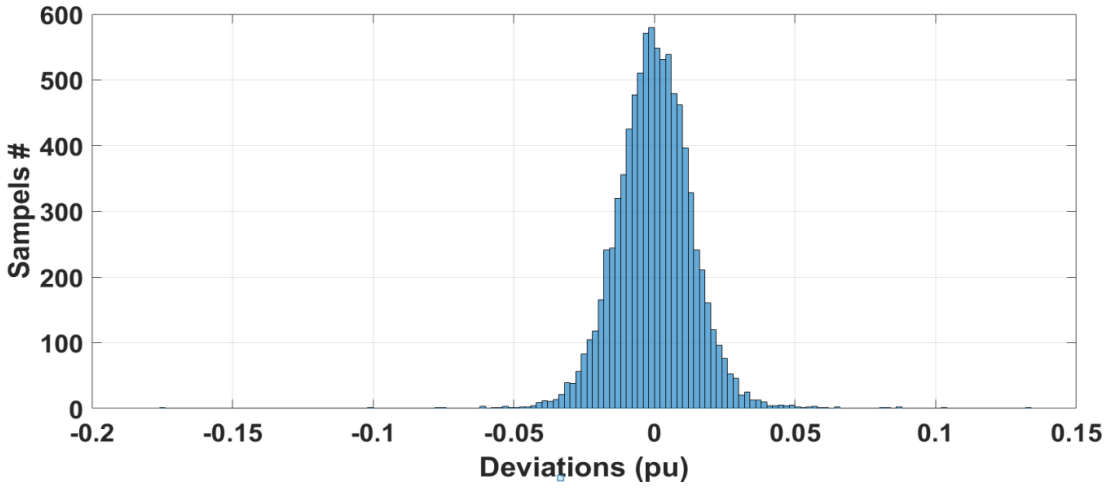
$$DZ_i^h(k) = \{z(k) - z(k-1) \quad | \in 1^{st} - 10^{th}\, month\} \tag{۴-۴}$$

پس از ایجاد مجموعه بالا برای هر اندازه‌گیری، می‌توان هیستوگرام این مجموعه را رسم نمود. شکل ۴-۷ منحنی هیستوگرام $DZ_i^h(k)$ برای اولین اندازه‌گیر شبکه موردمطالعه را نشان می‌دهد.




شکل ۴-۷- منحنی هیستوگرام ماه اول تا آخر ماه دهم اولین اندازه‌گیر شبکه به‌عبارت‌دیگر توان حقیقی باس اول(منحنی هیستوگرام $DZ_i^h(k)$)

**مرحله ۸:** در این مرحله تغییرات اندازه‌گیری فعلی $DZ_i^c$ محاسبه می‌شود. هیستوگرام $DZ_i^c$ با توجه به تغییرات اطلاعات جاری شبکه به دست می‌آید. شکل ۴-7 منحنی هیستوگرام $DZ_i^c$ را برای اولین اندازه‌گیر شبکه موردمطالعه نشان می‌دهد.




شکل ۴-۸- منحنی هیستوگرام ماه جاری اولین اندازه‌گیر شبکه(منحنی هیستوگرام $\boldsymbol{DZ_i^c}$)

**مرحله ۹:** در این مرحله پس از تشکیل هیستوگرام $DZ_i^c$ و $DZ_i^h(k)$ برای هر اندازه‌گیر، مقدار دو شاخص یعنی فاصله نسبی لگاریتمی پیشنهادی و فاصله مطلق با توجه به روابط (۳-۱۵) و (۳-۱۶) محاسبه می‌گردند.

## ۴-۳- شبیه‌سازی روش پیشنهادی در تشخیص حملات تزریق داده اشتباه

در بخش گذشته شبکه مورد تست معرفی‌شده و نحوه اعمال تغییرات در شبکه و همچنین روند حل مسئله جهت بررسی روش پیشنهادی تشخیص حملات تزریق داده اشتباه نیز بیان گردید. در این بخش در ابتدا نحوه شبیه‌سازی حملات تزریق داده اشتباه،توضیح داده می‌شود و سپس تغییرات اندازه‌گیری و شاخص فاصله که در فصل و بخش گذشته توضیحاتی پیرامون آن‌ها بیان گردید، به‌تفصیل تشریح می‌شوند. پس‌ازآن،در بخش بعدی سناریو بندی مسئله معرفی‌شده و نتایج شبیه-سازی روش پیشنهادی برای سناریو موردنظر ارائه می‌گردد.

### ۴-۳-۱- شبیه‌سازی حملات تزریق داده اشتباه

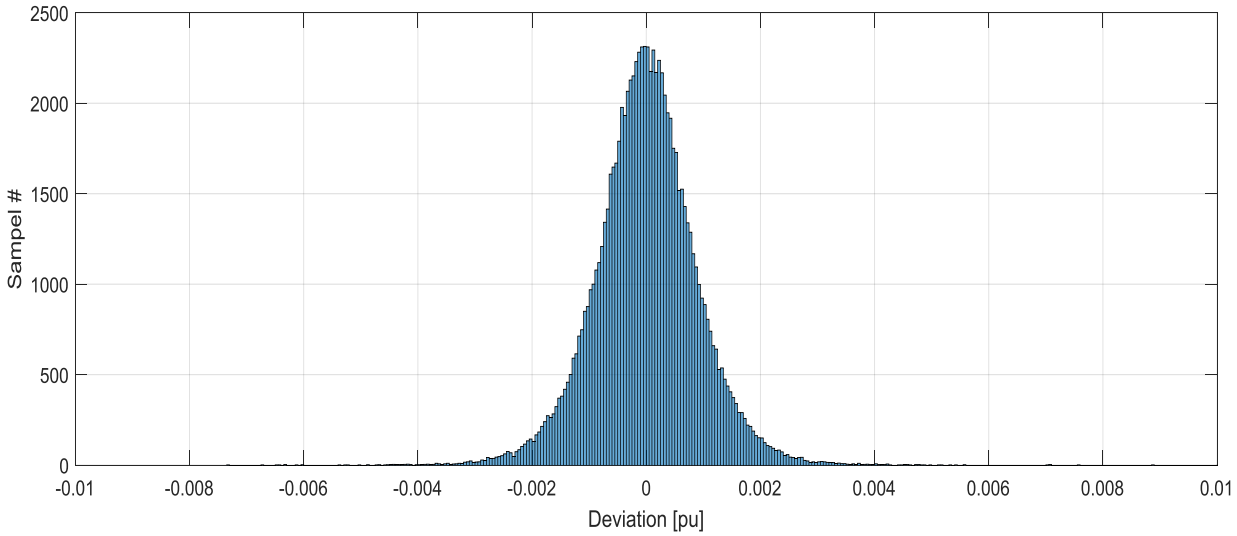
به‌منظور آزمایش روش پیشنهادی، حملات تزریق داده‌های اشتباه توسط هدف قرار دادن متغیرهای مختلف حالت سیستم شبیه‌سازی‌شده است. حالت دستکاری‌شده سیستم پس از حمله

توسط رابطه $x_{bad} = x + c$ مشخص می‌شود. اندازه‌گیری مربوطه برای حالت سیستم دستکاری‌شده $z_{bad} = h(x_{bad})$ می‌باشد.

برای تخمین حالت AC در سیستم ۱۴ باسه IEEE، ۲۷ متغیرهای حالت(شامل ۱۴ اندازه ولتاژ باس و ۱۳ زاویه فاز باس) در نظر گرفته‌شده است که در بخش گذشته تشریح داده شد. حملات تزریق داده اشتباه بر روی هر یک از این ۲۷ متغیر حالت شبیه‌سازی‌شده است.

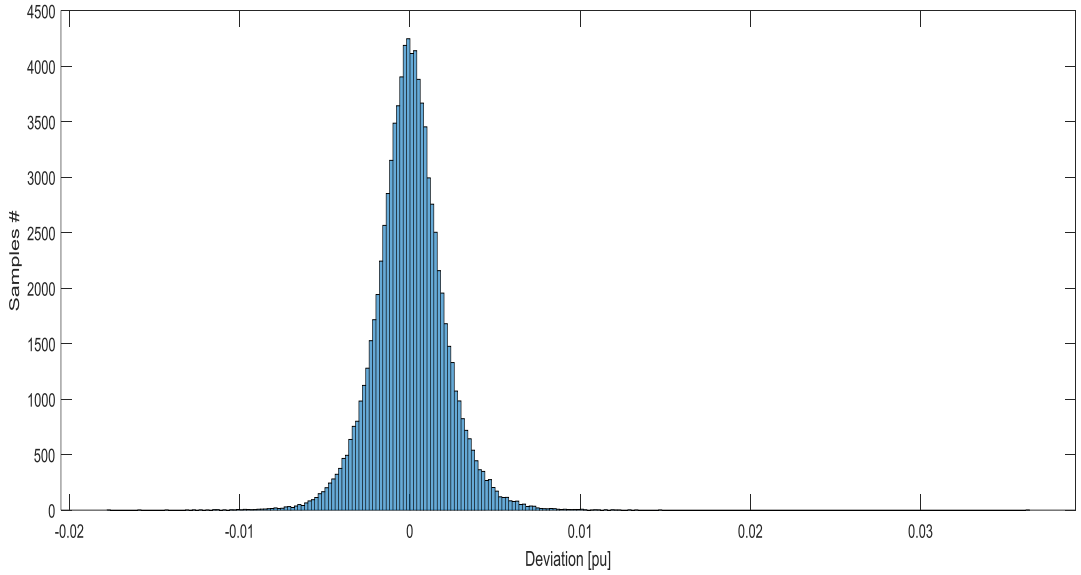
## ۴-۳-۲- تغییرات اندازه‌گیری

سیستم‌های قدرت به‌عنوان سیستم‌های شبه استاتیک در نظر گرفته می‌شوند. حالت سیستم قدرت دائماً ولی به‌آرامی در حال تغییر می‌باشد. این امر به این معنی است که اندازه‌گیری‌های به‌دست‌آمده از RTUها باید به‌آرامی تغییر نماید. داده‌های اندازه‌گیری به‌دست‌آمده از RTUها در گام زمانی $i$ توسط $z(i)$ نشان داده می‌شود. همان‌گونه که در مرحله ۷ از روند بخش قبلی نیز بیان گردید، تغییرات اندازه‌گیری به‌صورت $z(k) - z(k-1)$ تعریف می‌شود. در شکل ۴-۹ هیستوگرام $DZ_i^h(k)$ تغییرات اندازه‌گیری از ژانویه ۲۰۱۲ تا ماه اکتبر ۲۰۱۲ بدون هیچ‌گونه حملات تزریق داده-های اشتباه نشان داده‌شده است.




شکل ۴-۹- منحنی هیستوگرام تغییرات اندازه‌گیری از ژانویه تا اکتبر ۲۰۱۲ ($DZ_i^h(k)$)

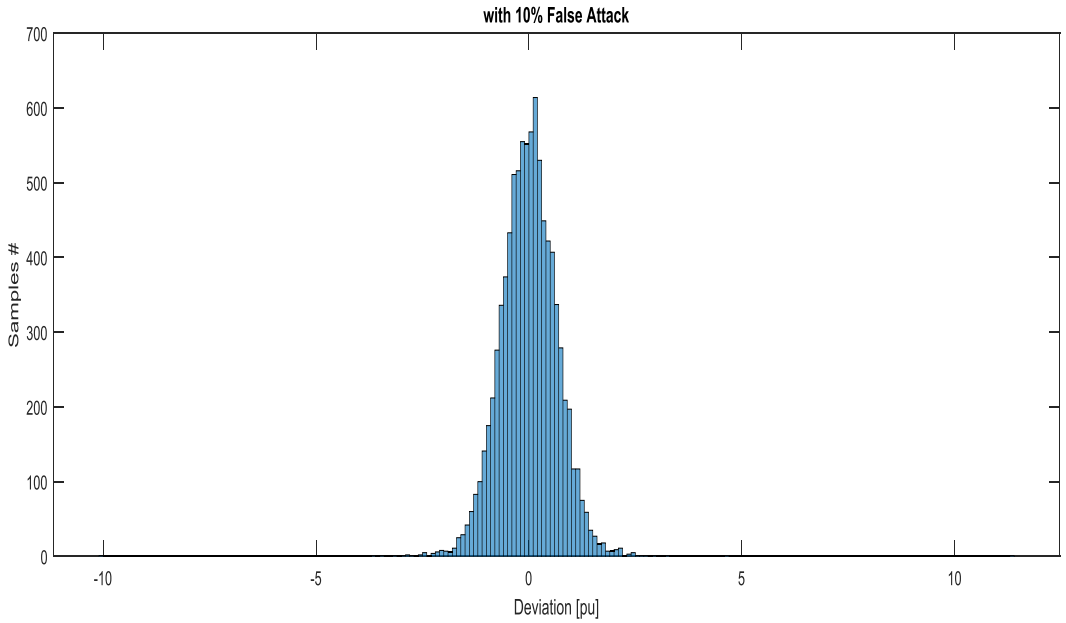
با توجه به شکل ۴-۹ می‌توان مشاهده نمود که اغلب تغییرات اندازه‌گیری کوچک و نزدیک به صفر می‌باشند چراکه همانطورکه در ابتدای بخش توضیح داده شد، سیستم‌های قدرت به‌عنوان سیستم‌های شبه استاتیک در نظر گرفته می‌شود و اندازه‌گیری‌ها تغییرات مداوم و آرامی خواهند داشت. این هیستوگرام به تابع $DZ_i^h(k)$ در رابطه (۳-۱۵) تبدیل‌شده است. وقتی‌که هیچ حملات تزریق داده اشتباهی وجود ندارد، هیستوگرام تغییرات اندازه‌گیری بین ماه‌های مختلف مشابه می‌باشد. شکل ۴-۱۰ هیستوگرام $DZ_i^c$ تغییرات اندازه‌گیری در نوامبر ۲۰۱۲ بدون هیچ حملات تزریق داده اشتباه را نشان می‌دهد.




شکل ۴-۱۰- منحنی هیستوگرام تغییرات اندازه‌گیری در نوامبر ۲۰۱۲($DZ_i^c$)

با مقایسه شکل ۴-۹ و ۴-۱۰، مشاهده می‌شود که دو نمودار هیستوگرام تقریباً مشابه می‌باشند و همچنین با توجه به دو منحنی ۴-۹ و ۴-۱۰ مشخص می‌شود که در صورت عدم وجود حملات داده بد، تغییرات اندازه‌گیری در اکثر نمونه‌ها برابر و یا نزدیک به صفر می‌باشد و مقدار اختلاف ناچیز می‌تواند ناشی از خطای دستگاه‌ها و ... باشد. بااین‌حال، زمانی که داده‌های اشتباه به سیستم قدرت تزریق می‌شوند، هیستوگرام تغییرات اندازه‌گیری فعلی متفاوت خواهد بود. برای نشان دادن تأثیر تزریق داده اشتباه روی تغییرات اندازه‌گیری، حمله‌ای با ۱۰٪ افزایش در متغیر اول حالت سیستم یعنی $V_1$ و

$c = (0.1 \times V_1, 0, \dots, 0)$ شبیه‌سازی می‌شود. این حمله در هر گام زمانی از ماه دسامبر شبیه‌سازی‌شده است. شکل ۴-11 هیستوگرام $DZ_i^c$ تغییرات اندازه‌گیری($z_{bad}(k) - z(k-1)$) در هنگامی‌که داده اشتباه به سیستم تزریق می‌شود را نشان می‌دهد.




شکل ۴-۱۱- منحنی هیستوگرام تغییرات اندازه‌گیری در ماه دسامبر به همراه حملات تزریق داده اشتباه($DZ_i^c$)

با توجه به شکل‌های ۴-۱۰ و ۴-۱۱، می‌توان دریافت که تزریق داده‌های اشتباه، تغییرات اندازه‌گیری را تحت تأثیر قرار می‌دهد و مقدار آن در صفر متمرکز نبوده و دارای مقادیر بزرگ‌تری می‌باشد. باکمی توجه به شکل‌های ۴-۹ تا ۴-۱۱ متوجه خواهیم شد که با تعریف یک مقدار آستانه می‌توان با توجه به میزان انحراف نمونه‌ها از تزریق داده اشتباه آگاه شد.

### ۴-۳-۳- شاخص فاصله

همان‌طور که پیش‌تر نیز بیان گردید برای تعیین اختلاف بین دو هیستوگرام، دو شاخص متفاوت معرفی‌شده و مورد آزمایش قرار می‌گیرد. برای هر دو شاخص، دو هیستوگرام $DZ_i^c$ و $DZ_i^h(k)$ وجود دارد. در این پژوهش، هیستوگرام $DZ_i^h(k)$ از داده‌های قبلی تغییرات اندازه‌گیری(مطابق شکل ۴-۱۱) به دست می‌آید، اما هیستوگرام $DZ_i^c$ تنها برای هر گام زمانی(در هرماه محاسباتی) محاسبه می‌شود. برای سیستم ۱۴ باسه IEEE موردمطالعه، در هر مرحله ۶۸ اندازه‌گیری وجود دارد که در بخش قبلی

توضیح داده شد و بیان شد که بردار اندازه‌گیری‌ها مطابق با رابطه (۴-۳) می‌باشد که این بردار شامل توان اکتیو و راکتیو تزریقی، توان اکتیو و راکتیو جاری‌شده در خط انتقال می‌باشد. برای تغییرات هر اندازه‌گیری در هر مرحله زمانی(شامل ۶۸ اندازه‌گیری) تابع توزیع $p$ محاسبه می‌گردد.

## ۴-۴- ارائه نتایج شبیه‌سازی روش پیشنهادی در تشخیص حملات تزریق داده اشتباه

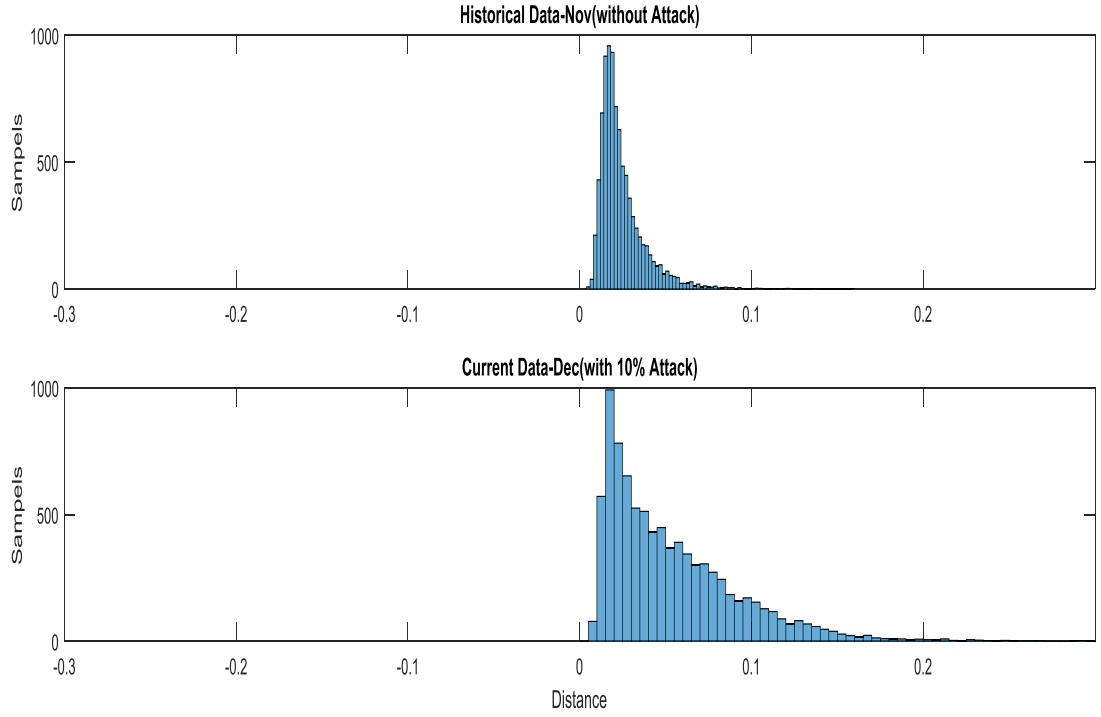
در این بخش نتایج شبیه‌سازی روش پیشنهادی برای تشخیص حملات تزریق اطلاعات غلط، موردبررسی قرار می‌گیرد:

بدین منظور شبیه‌سازی در نرم‌افزار MATLAB صورت گرفته است و نتایج سناریو به‌صورت جدول و شکل ارائه می‌گردد. در ادامه نتایج سناریو ارائه می‌شود.

### ۴-۴-۱- سناریوی حملات تزریق داده اشتباه به متغیرهای حالت

در این سناریو یک متغیر حالت به‌عنوان هدف حمله قرار داده می‌شود و تمامی اندازه‌گیری‌های مرتبط با آن حالت با داده اشتباه جایگزین می‌شود. در این بخش در ابتدا شاخص‌های معرفی‌شده در شرایط وجود حمله و عدم وجود حمله مورد تست و بررسی قرار می‌گیرند تا رفتار و کارایی هریک مشخص شود.

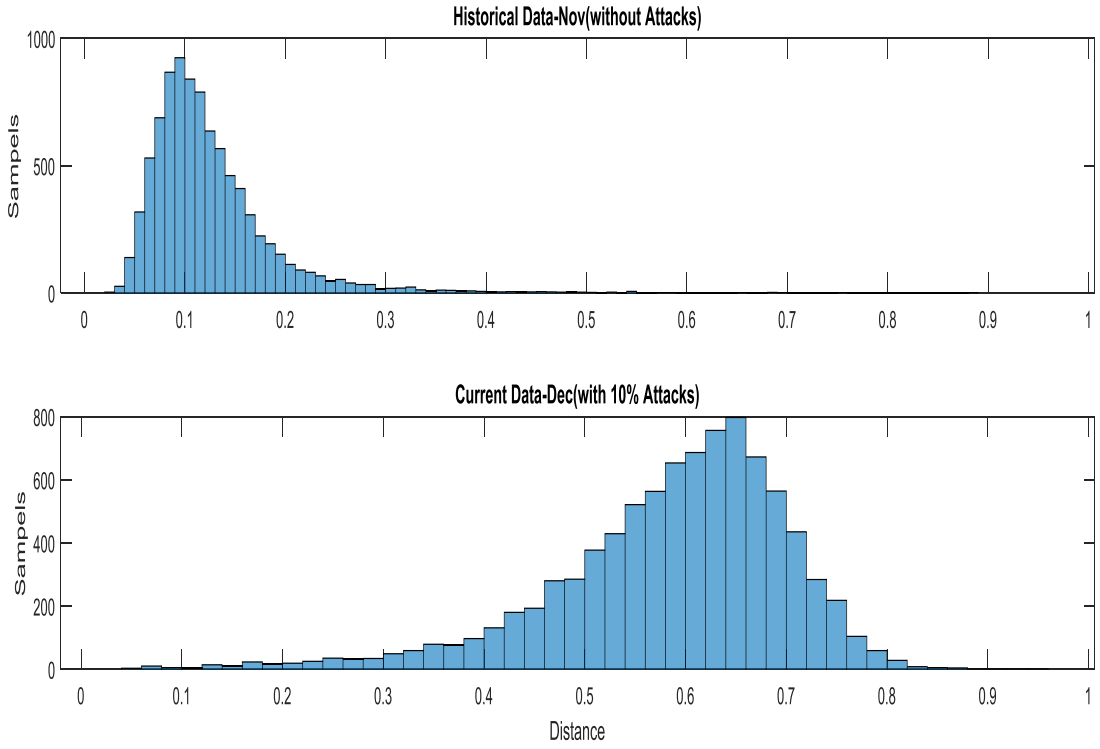
- **شاخص فاصله مطلق:** در مرحله اول فاصله مطلق بین $DZ_i^c$ و $DZ_i^h(k)$ که با استفاده از رابطه‌ی (۳-۱۶) به دست می‌آید، مورد آزمایش قرار می‌گیرد. شکل ۴-۱۲ منحنی هیستوگرام فاصله مطلق برای ماه نوامبر بدون وجود حملات تزریق داده اشتباه و ماه دسامبر در حضور حملات داده اشتباه ۱۰٪ را نشان می‌دهد.




شکل ۴-۱۲- منحنی هیستوگرام شاخص فاصله مطلق تغییرات اندازه‌گیری در ماه نوامبر و دسامبر.

با توجه به شکل‌های فوق مشخص است که در ماه نوامبر محدوده فاصله مطلق بین ۰ تا ۰.۱ می‌باشد درحالی‌که در ماه دسامبر باوجود حملات محدوده فاصله مطلق بین ۰ تا ۰.۳ بوده که این از همپوشانی دو شکل حکایت دارد. همچنین در مقایسه بافاصله مطلق بدون وجود حمله(ماه نوامبر)، فاصله مطلق با حملات تزریق داده‌های اشتباه عمدتاً بزرگ‌تر می‌باشد. بااین‌حال، مقداری همپوشانی در محدوده ۰ تا 0/1 بین دو شکل فوق وجود دارد. این امر به این معنی است که زمانی که ما یک نمونه اندازه‌گیری بافاصله مطلق بین ۰ و 0/1 داشته باشیم، این نمونه می‌تواند هم شامل و هم فاقد حمله باشد. بنابراین تشخیص نمونه‌ای در این بازه که شامل حمله می‌باشد یا خیر امری مشکل است. پس شاخص فاصله مطلق کاندید مناسبی برای تست حملات تزریق داده اشتباه نمی‌باشد.

- **شاخص فاصله نسبی لگاریتمی:** همان‌گونه که بیان گردید این شاخص بر اساس رابطه (۳-۱۵) محاسبه می‌شود. شکل ۴-۱۳ منحنی هیستوگرام شاخص فاصله نسبی لگاریتمی برای ماه نوامبر بدون حضور حملات تزریق داده اشتباه و برای ماه دسامبر در حضور حملات تزریق داده اشتباه را نشان می‌دهد.




شکل ۴-۱۳- منحنی هیستوگرام شاخص فاصله نسبی لگاریتمی تغییرات اندازه‌گیری در ماه نوامبر و دسامبر.

منحنی هیستوگرام شکل ۴-۱۳ نشان می‌دهد که شاخص فاصله نسبی اکثر نمونه‌ها در ماه نوامبر و بدون وجود حملات تزریق داده اشتباه کمتر از 0/4 می‌باشد. اما فاصله نسبی لگاریتمی اغلب نمونه‌ها در ماه دسامبر بزرگ‌تر از 0/4 می‌باشد. با مقایسه دو شکل فوق، می‌توان دریافت که با تزریق حملات داده‌های اشتباه، شاخص فاصله نسبی لگاریتمی افزایش خواهد یافت.

برخلاف شاخص فاصله مطلق، در دو منحنی هیستوگرام شاخص فاصله نسبی لگاریتمی همپوشانی بسیار کمتری وجود دارد. برای تشخیص حملات تزریق داده اشتباه، مقدار آستانه‌ای برای شاخص فاصله نسبی لگاریتمی با توجه به داده‌های قبلی تعریف می‌گردد. سپس در طول زمان اجرا این مقدار آستانه با هر نمونه مقایسه می‌شود. اگر در طول زمان اجرا، شاخص فاصله نسبی لگاریتمی بزرگ‌تر از حد آستانه باشد، آنگاه این احتمال وجود دارد که داده‌های اشتباه به سیستم تزریق‌شده‌اند.

اما باید توجه نمود که انتخاب یک مقدار آستانه دقیق موجب می‌شود که دقت مرحله تشخیص نیز افزایش یابد. در حقیقت مقدار آستانه، تلورانس تغییرات اندازه‌گیری برای الگوریتم تشخیص را معین

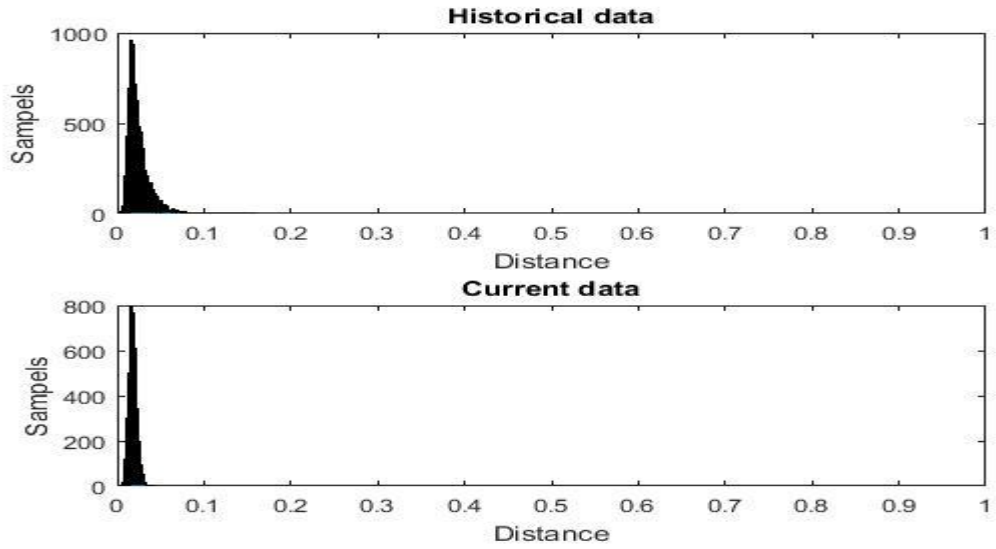
می‌نماید. اگر مقدار آستانه در مقدار بسیار زیادی تنظیم شود، روش پیشنهادی توانایی تشخیص حملات را نخواهد داشت چراکه تقریباً مقدار شاخص تمامی نمونه‌ها کمتر از مقدار آستانه می‌باشد. اما اگر مقدار آستانه در مقدار بسیار کمی هم تنظیم شود، برخی از داده‌های اندازه‌گیری صحیح ممکن است به‌عنوان داده اشتباه در نظر گرفته شوند و در فرآیند تشخیص دچار اشتباه شویم.

می‌توان بیشترین فاصله و انحراف داده‌های قبلی را به‌عنوان مقدار آستانه در نظر گرفت. اما ممکن است بیشترین مقدار انحراف، مقداری بسیار بزرگ باشد و مشکلاتی را ایجاد نماید. در شکل ۴-۱۲ بیشترین مقدار شاخص فاصله نسبی0/9بوده که از اغلب نمونه‌های ماه دسامبر بسیار بزرگ‌تر می‌باشد. اگر از مقدار 0/9 به‌عنوان مقدار آستانه استفاده گردد، نمی‌توان حملات تزریق داده اشتباه را تشخیص داد. همچنین لازم به ذکر است که مقدار انحراف بسیار زیاد در داده‌های قبلی ممکن است به دلیل خطای اندازه‌گیری درداده سیستم نیز به وجود آید.

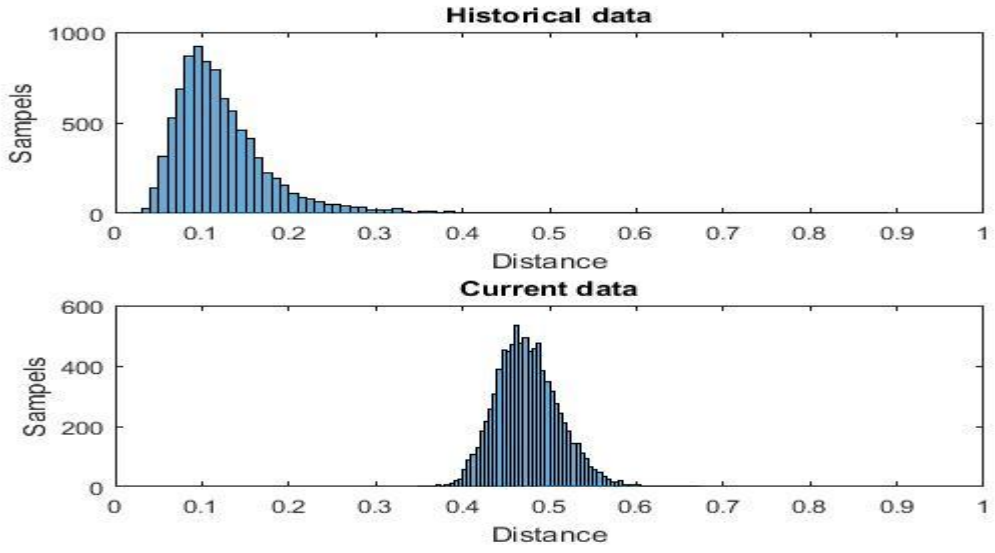
برای حل این مشکل در این پژوهش، بیشترین مقدار شاخص فاصله نسبی از داده‌های قبلی با میزان اطمینان بالایی انتخاب می‌گردد. به‌عنوان‌مثال ۹۹٪ از سطح اطمینان بدین معنی می‌باشد که مقدار آستانه بزرگ‌تر از ۹۹٪ داده قبلی است. در شکل ۴-۱۳ ۹۹٪ بیشترین شاخص فاصله نسبی قابل‌اطمینان، 0/3 می‌باشد که از اغلب نمونه‌های ماه دسامبر کوچک‌تر است. این ۹۹٪ سطح اطمینان به‌عنوان مقدار آستانه در نظر گرفته‌شده و برای تشخیص حملات تزریق داده اشتباه در ادامه شبیه-سازی مورداستفاده قرار می‌گیرد.

تا اینجا مقایسه‌ای بین دو شاخص فاصله مطلق و فاصله نسبی لگاریتمی پیشنهادی انجام شد و علت انتخاب شاخص پیشنهادی جهت تشخیص حملات تزریق داده اشتباه مشخص گردید. در ادامه جهت تست روش پیشنهادی حملات تزریق داده اشتباه بر روی تمامی متغیرهای حالت سیستم شبیه‌سازی می‌شود، اما به دلیل وسعت نتایج، تنها بخشی از آن‌ها ارائه می‌شود. در هر حمله یک متغیر حالت به‌اندازه ٪۲ مقدار نامی خود افزایش داده می‌شود. پس از اجرای شبیه‌سازی نتایج شامل هیستوگرام‌های شاخص‌های فاصله مطلق و فاصله نسبی محاسبه‌شده و درصد تشخیص تزریق داده

اشتباه برای هر اندازه‌گیری ارائه می‌گردد. در شکل‌های ۴-۱۴ تا ۴-۱۷ هیستوگرام شاخص‌های فاصله مطلق و نسبی لگاریتمی و درصد تشخیص برای اندازه‌گیری‌های مختلف در حمله تزریق داده اشتباه در متغیر اول(ولتاژ باس ۱) در شبکه موردمطالعه ارائه‌شده است.

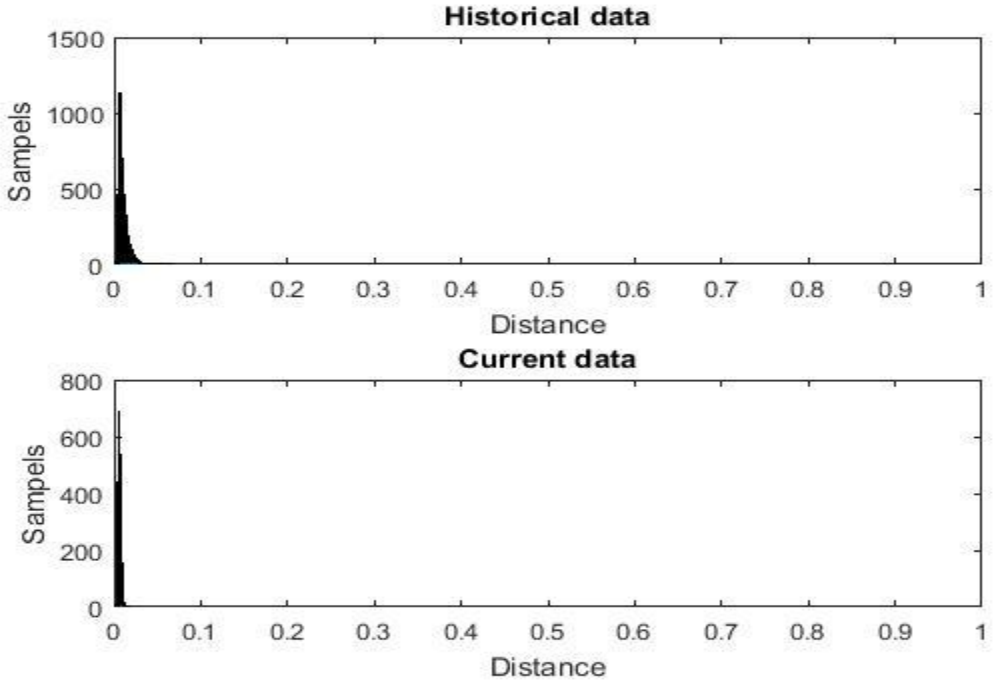



(الف) شاخص فاصله مطلق

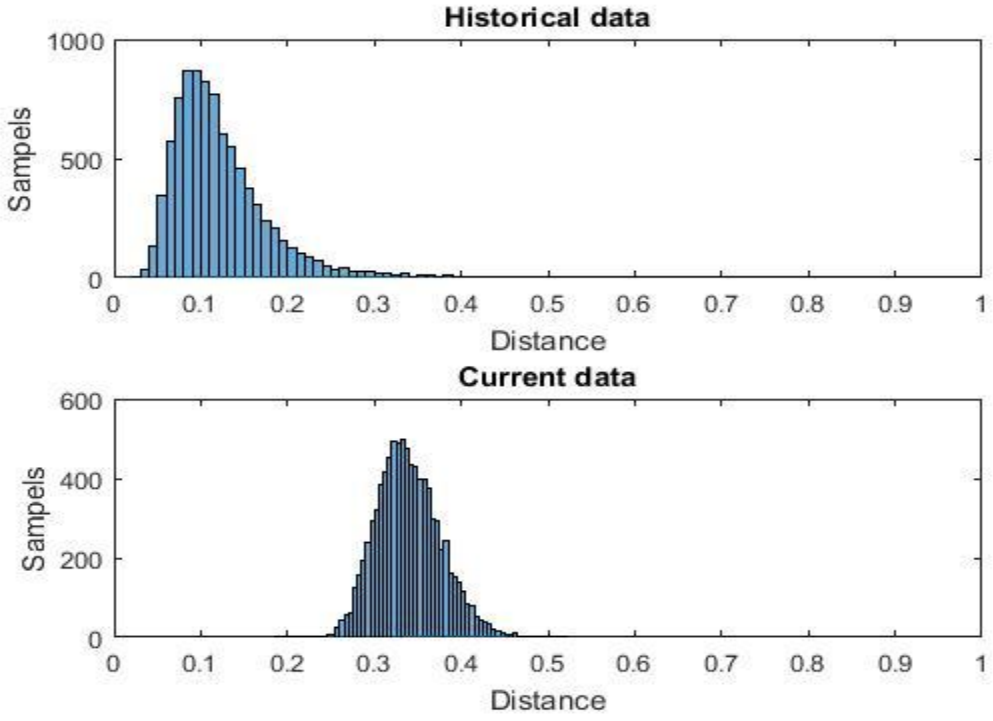



(ب) شاخص فاصله نسبی لگاریتمی

شکل ۴-۱۴- شاخص فاصله مطلق و نسبی لگاریتمی برای اندازه‌گیر ۲ در حمله تزریق داده اشتباه در متغیر ۱(ولتاژ باس ۱)

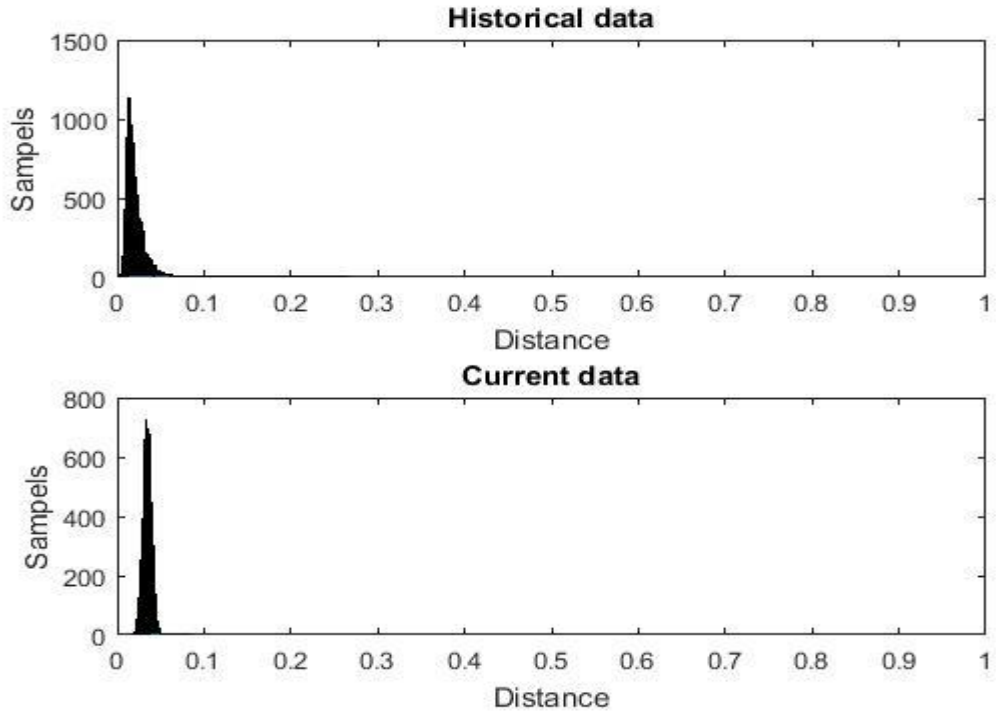



(الف) شاخص فاصله مطلق

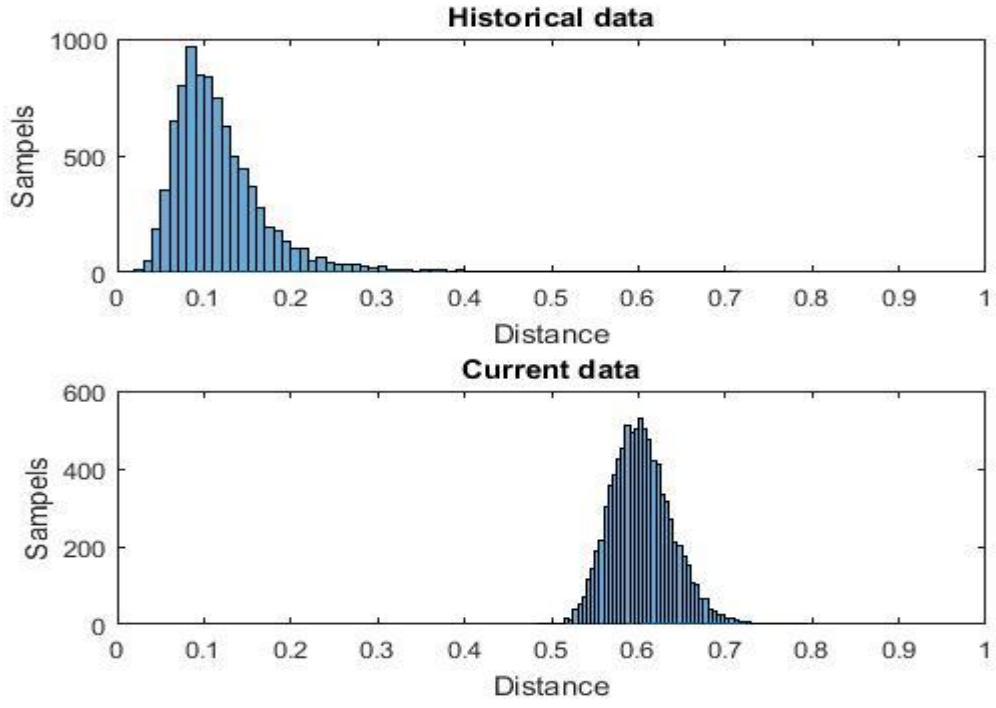



(ب) شاخص فاصله نسبی لگاریتمی

شکل ۴-۱۵- شاخص فاصله مطلق و نسبی لگاریتمی برای اندازه‌گیری ۱۶ در حمله تزریق داده اشتباه در متغیر ۱(ولتاژ باس ۱)




(الف) شاخص فاصله مطلق



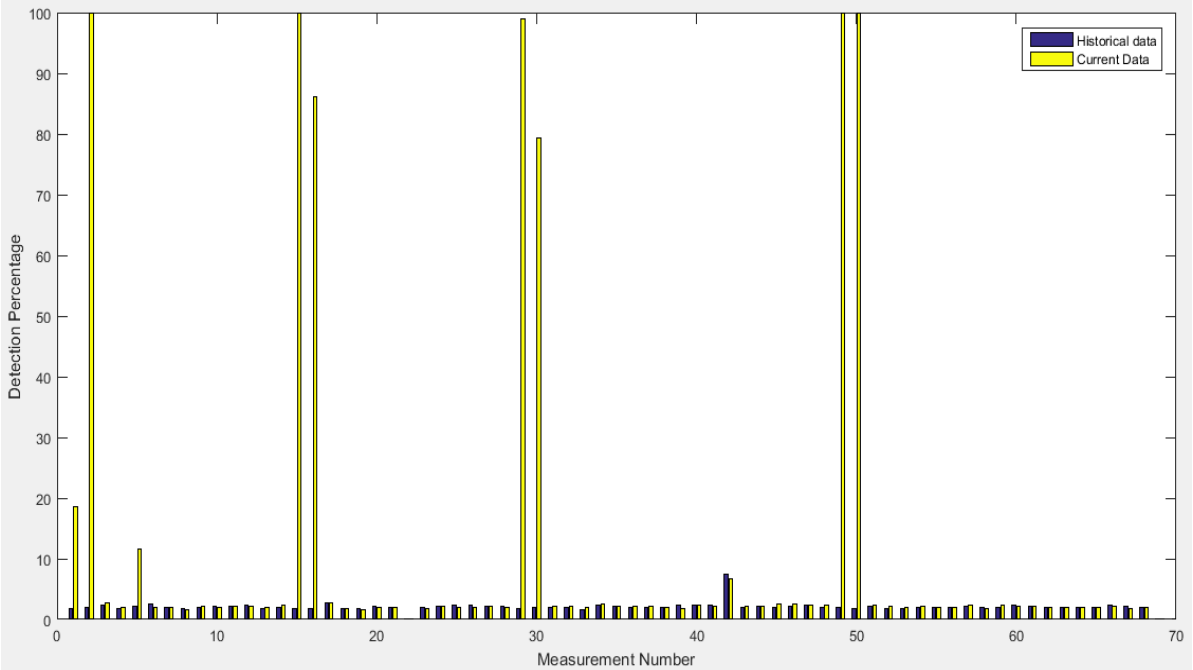

(ب) شاخص فاصله نسبی لگاریتمی

شکل ۴-۱۶- شاخص فاصله مطلق و نسبی لگاریتمی برای اندازه‌گیری ۴۹ در حمله تزریق داده اشتباه در متغیر ۱(ولتاژ باس ۱)

همان‌گونه که مطرح گردید در این بخش حمله تزریق داده اشتباه در متغیر اول شبکه یعنی ولتاژ باس اول شبکه صورت گرفته است. با توجه به اینکه شکل ۴-۱۴ برای اندازه‌گیری دوم که توان اکتیو تزریقی در باس ۲ می‌باشد، رسم شده است، کاملاً مشخص است که در اثر حمله تزریق داده اشتباه به متغیر اول، اندازه‌گیری مربوط به آن کاملاً تحت تأثیر قرارگرفته است به‌نحوی‌که با انتخاب مقدار آستانه 0/3 ، شاخص فاصله نسبی در مقایسه با داده‌های قبلی، دارای مقادیر بسیار زیادی بیشتر از 0/3 بوده که این امر نشان‌دهنده وجود حمله می‌باشد ضمن اینکه شاخص مطلق دارای همپوشانی کامل با داده‌های قبلی بوده که نمی‌تواند وجود حمله را تشخیص دهد. پس حمله به ولتاژ باس ۱، بر روی اندازه‌گیری دوم آن‌که توان اکتیو تزریقی باس ۲ می‌باشد، تأثیر گذاشته است.

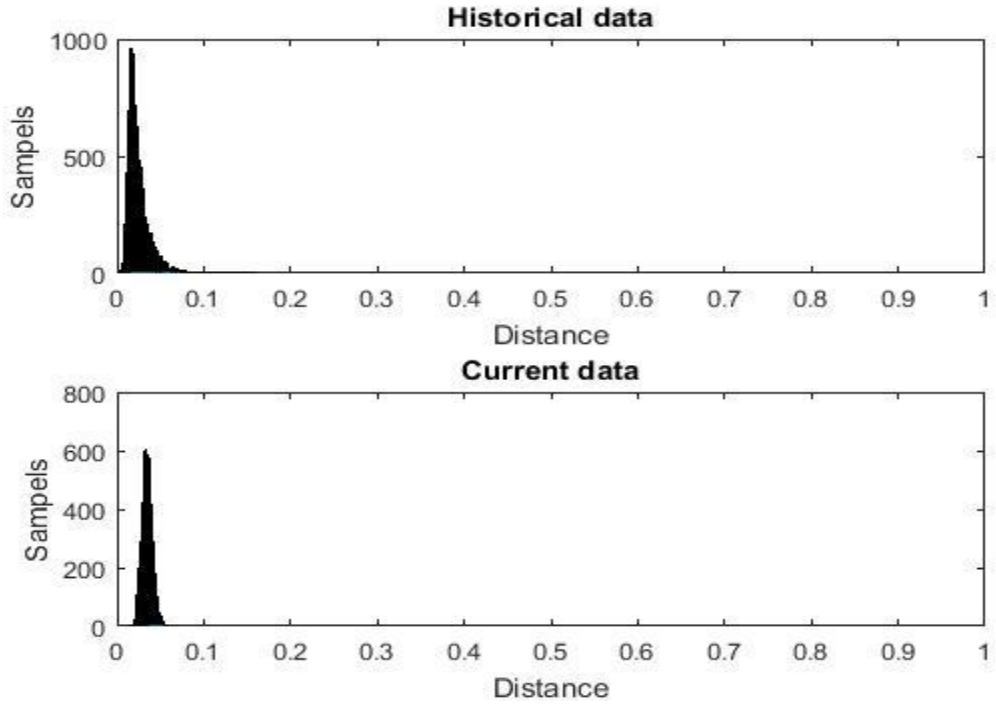
در شکل ۴-۱۵ نیز شاخص‌های فاصله مطلق و نسبی برای اندازه‌گیری شانزدهم که توان راکتیو تزریقی باس دوم می‌باشد، رسم شده است. با توجه به آن مشخص می‌گردد که با مقایسه داده قبلی و فعلی شاخص مطلق حمله‌ای مشخص نبوده درحالی‌که در شاخص فاصله نسبی واضح است که نمونه-های بسیاری بیشتر از مقدار آستانه قرارگرفته است. پس کارایی شاخص نسبی پیشنهادی بیشتر نمود پیداکرده است ضمن اینکه لازم به ذکر است که با توجه به شکل ۴-۱ که دیاگرام شبکه را نشان می-دهد، می‌توان دریافت که حمله به متغیر اول باید بر روی اندازه‌گیری‌های مربوط به باس اول، دوم و پنجم تأثیر گذارد که شامل درایه‌های ۱، ۲، ۵، ۱۵، ۱۶، ۱۹، ۲۹، ۳۰، ۴۹ و ۵۰ ماتریس اندازه‌گیری می‌باشد که این درایه‌ها توان اکتیو و راکتیو تزریقی این باس‌ها و توان عبوری در خطوط ۱ و ۵ هستند.

با توجه به توضیح فوق و شکل ۴-۱۶ تأثیر حمله در هیستوگرام شاخص نسبی اندازه‌گیری ۴۹ نیز واضح است که نمونه‌های زیادی از مقدار آستانه بیشتر می‌باشند و مشابه موارد قبلی هیستوگرام شاخص مطلق نیز اطلاعات مناسبی از حمله در اختیار قرار نمی‌دهد. شکل ۴-۱۷ درصد تشخیص دو روش شاخص مطلق و نسبی پیشنهادی در اندازه‌گیری‌های مختلف را نشان می‌دهد.

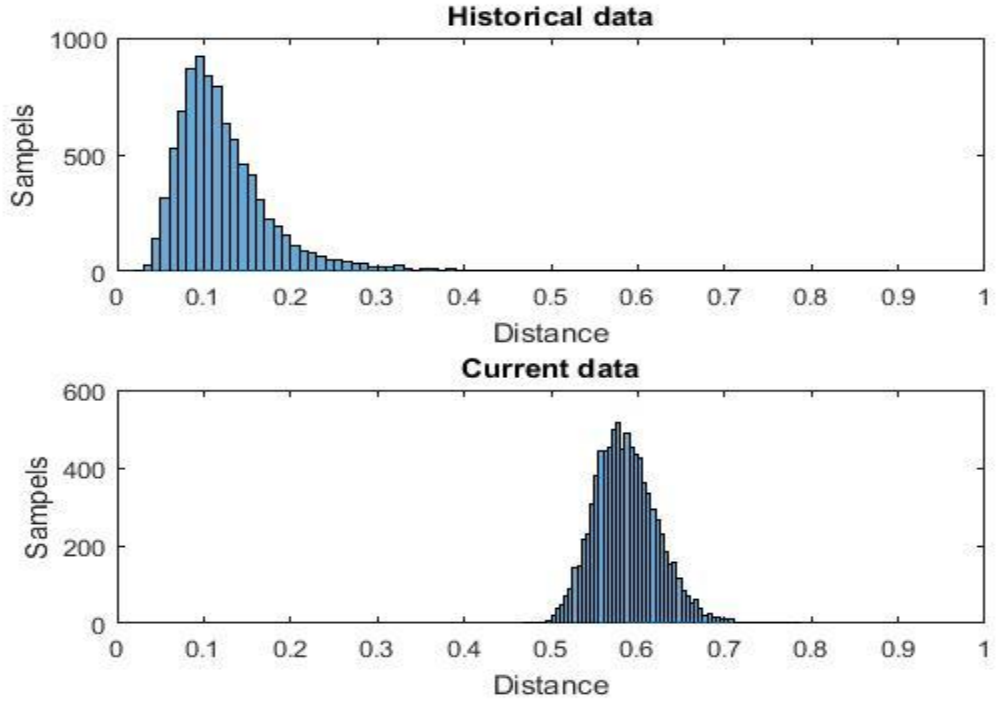



شکل ۴-۱۷- درصد تشخیص شاخص فاصله مطلق و نسبی لگاریتمی برای اندازه‌گیری‌های مختلف در حمله تزریق داده اشتباه در متغیر ۱(ولتاژ باس ۱)

طبق اینکه حمله به متغیر اول باید بر روی اندازه‌گیری‌های مربوط به باس اول، دوم و پنجم تأثیر بگذارد که شامل درایه‌های ۱، ۲، ۵، ۱۵، ۱۶، ۱۹، ۲۹، ۳۰، ۴۹ و ۵۰ ماتریس اندازه‌گیری می‌باشد که این درایه‌ها توان اکتیو و راکتیو تزریقی این باس‌ها و توان عبوری در خطوط ۱ و ۵ هستند و با توجه به شکل فوق مشخص است که بیشترین تشخیص در تمامی اندازه‌گیری‌های تحت تأثیر حمله مربوط به شاخص فاصله نسبی پیشنهادی بوده ضمن اینکه شاخص پیشنهادی توانسته در تمامی اندازه‌گیری‌های دستکاری‌شده به‌طور موفقیت‌آمیزی حمله را تشخیص دهد. همچنین با توجه به شکل ۴-۱۷ درصورتی‌که متغیر موردحمله ناشناخته باشد، می‌توان طبق اندازه‌گیری‌هایی که دچار دستکاری شده‌اند و ساختار شبکه به متغیر موردحمله نیز پی برد و این امر کارایی روش پیشنهادی را بیشتر نشان می‌دهد. در ادامه فرض می‌شود که متغیر شانزدهم که زاویه ولتاژ باس ۳ شبکه مورد مطالعه است، دچار حمله شده و نتایج مربوط به آن در شکل‌های ۴-۱۸ تا ۴-۲۱ رسم شده است.

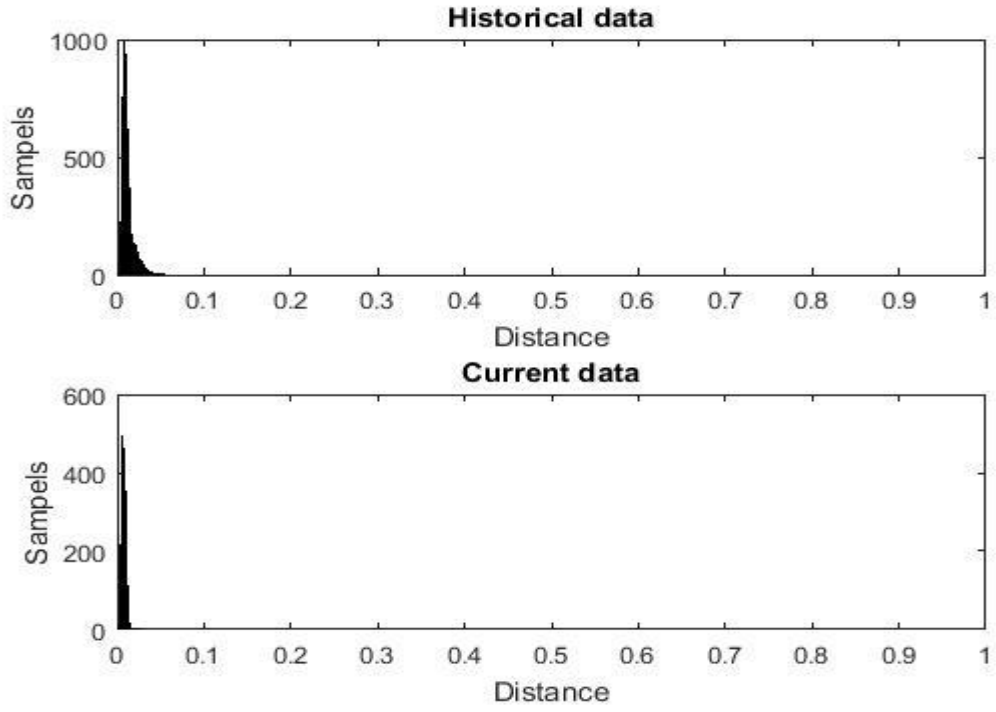



(الف) شاخص فاصله مطلق

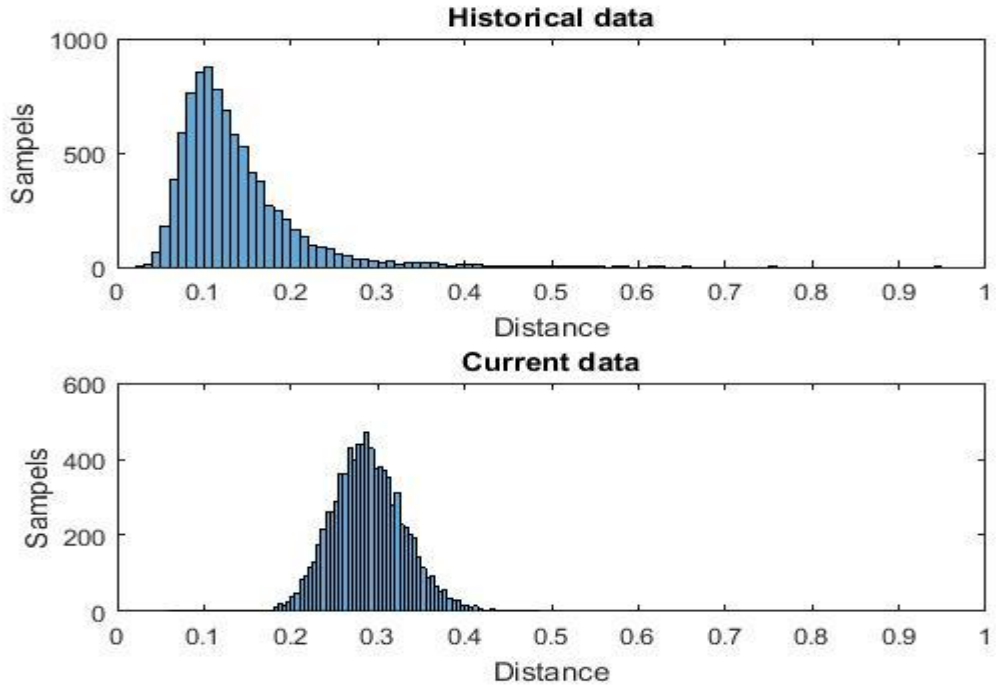



(ب) شاخص فاصله نسبی لگاریتمی

شکل ۴-۱۸- شاخص فاصله مطلق و نسبی لگاریتمی برای اندازه‌گیری ۲ در حمله تزریق داده اشتباه در متغیر ۱۶(زاویه فاز ولتاژ باس ۳)

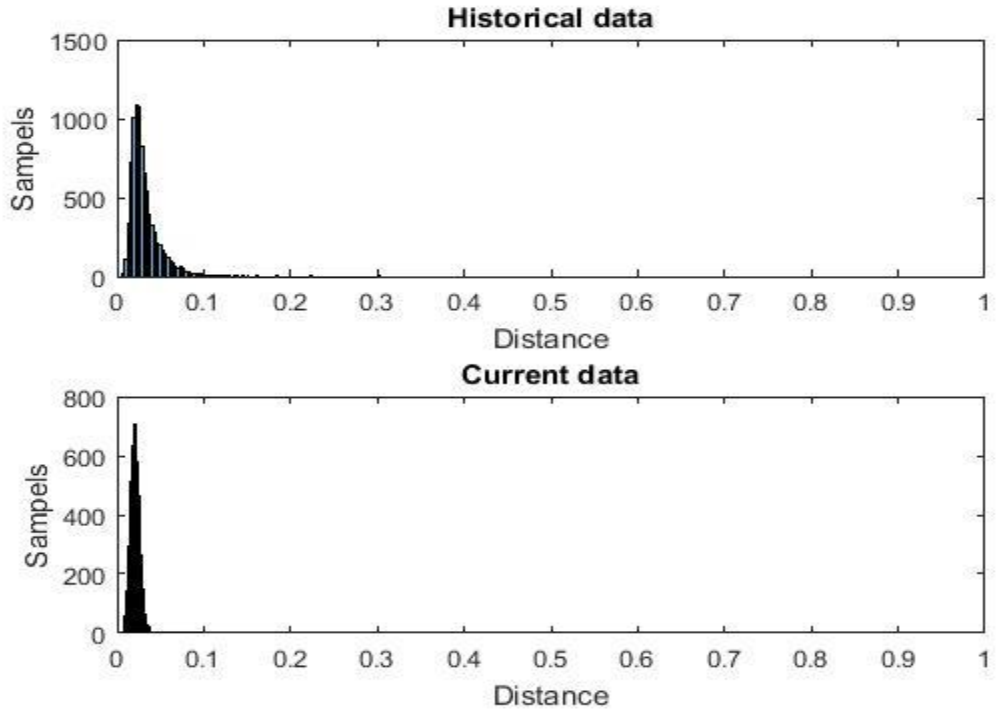



(الف) شاخص فاصله مطلق

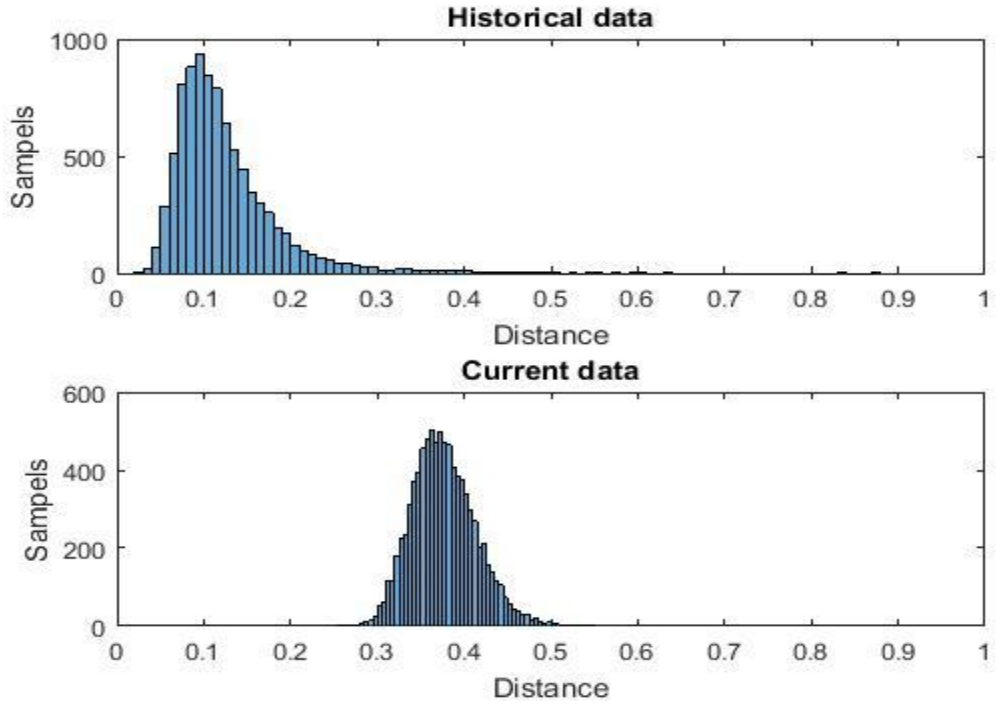



(ب) شاخص فاصله نسبی لگاریتمی

شکل ۴-۱۹- شاخص فاصله مطلق و نسبی لگاریتمی برای اندازه‌گیری ۱۷ در حمله تزریق داده اشتباه در متغیر ۱۶(زاویه فاز ولتاژ باس ۳)




(الف) شاخص فاصله مطلق




(ب) شاخص فاصله نسبی لگاریتمی

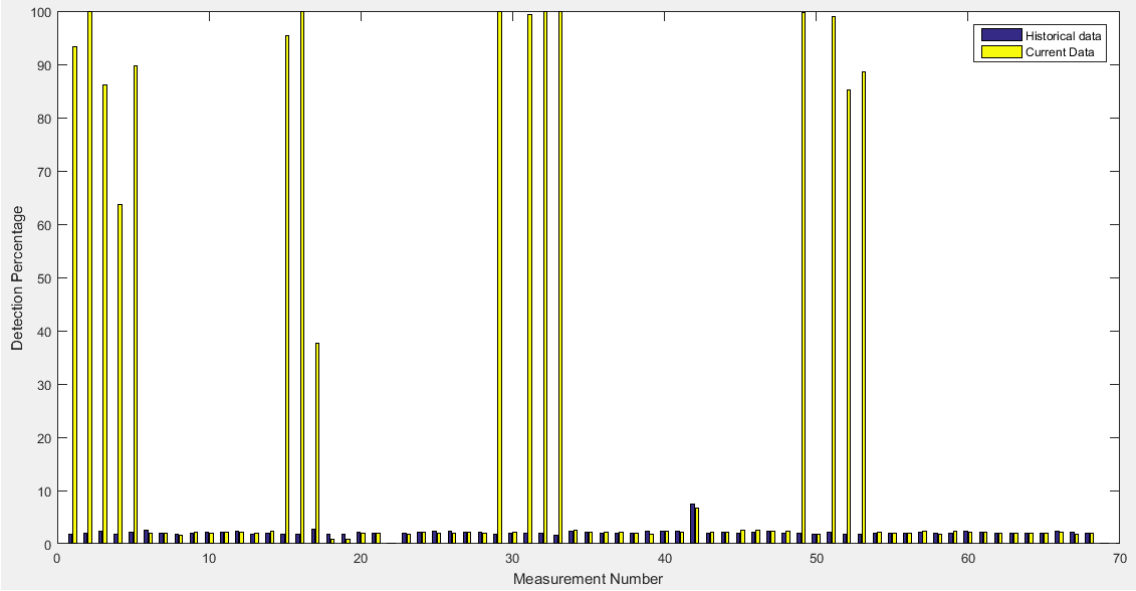
شکل ۴-۲۰- شاخص فاصله مطلق و نسبی لگاریتمی برای اندازه‌گیری ۳۱ در حمله تزریق داده اشتباه در متغیر ۱۶(زاویه فاز ولتاژ باس ۳)

همان‌گونه که مطرح گردید این بخش مشابه با بخش قبل بوده، اما در این بخش حمله تزریق داده اشتباه در متغیر شانزدهم شبکه یعنی زاویه فاز ولتاژ باس سوم شبکه صورت گرفته است. با توجه به اینکه شکل ۴-۱۸ برای اندازه‌گیری دوم که توان اکتیو تزریقی در باس ۲ می‌باشد، رسم شده است، کاملاً مشخص است که در اثر حمله تزریق داده اشتباه به متغیر شانزدهم، اندازه‌گیری مربوط به آن کاملاً تحت تأثیر قرارگرفته است به‌نحوی‌که با انتخاب مقدار آستانه 0/3، شاخص فاصله نسبی در مقایسه با داده‌های قبلی، دارای نمونه‌های بسیار زیادی دارای انحراف بیشتر از 0/3بوده که این امر نشان‌دهنده وجود حمله می‌باشد ضمن اینکه شاخص مطلق دارای همپوشانی کامل با داده‌های قبلی بین صفر و 0/1بوده که نمی‌تواند وجود حمله را تشخیص دهد. پس حمله به زاویه ولتاژ باس ۳، بر روی اندازه‌گیری دوم که توان اکتیو تزریقی باس ۲ می‌باشد، تأثیر گذاشته است.

در شکل ۴-۱۹ نیز شاخص‌های فاصله مطلق و نسبی برای اندازه‌گیری هفدهم که توان راکتیو تزریقی باس سوم می‌باشد، رسم شده است. با توجه به آن مشخص می‌گردد که با مقایسه داده قبلی و فعلی شاخص مطلق حمله‌ای مشخص نبوده و شاخص مطلق بین مقدار انحراف ۰ تا ۰.۲ دارای همپوشانی بوده درحالی‌که در شاخص فاصله نسبی واضح است که نمونه‌های بسیاری دارای انحراف بیشتر از مقدار آستانه می‌باشند. پس کارایی شاخص نسبی پیشنهادی بیشتر نمود پیداکرده است ضمن اینکه لازم به ذکر است که با توجه به شکل ۴-۱ که دیاگرام شبکه را نشان می‌دهد، می‌توان دریافت که حمله به متغیر شانزدهم باید بر روی اندازه‌گیری‌های مربوط به باس دوم، سوم، چهارم تأثیر بگذارد که شامل درایه‌های ۲، ۳، ۴، ۱۶، ۱۷، ۱۸، ۳۱، ۳۲، ۳۳، ۵۱، ۵۲، ۵۳ ماتریس اندازه‌گیری می‌باشد که این درایه‌ها توان اکتیو و راکتیو تزریقی این باس‌ها و توان عبوری در خطوط مرتبط هستند.

با توجه به توضیح فوق و شکل ۴-۲۰ تأثیر حمله در هیستوگرام شاخص نسبی اندازه‌گیری ۳۱ نیز واضح است که مقدار انحراف نمونه‌های زیادی از مقدار آستانه بیشتر می‌باشند و مشابه موارد قبلی هیستوگرام شاخص مطلق نیز اطلاعات مناسبی از حمله در اختیار قرار نمی‌دهد و بین مقادیر انحراف

۰ تا 0/05دارای همپوشانی می‌باشد. شکل ۴-۲۱ درصد تشخیص دو روش شاخص مطلق و نسبی پیشنهادی در اندازه‌گیری‌های مختلف را نشان می‌دهد.




شکل ۴-۲۱- درصد تشخیص شاخص فاصله مطلق و نسبی لگاریتمی در ماه یازدهم و دوازدهم برای اندازه‌گیری‌های مختلف در حمله تزریق داده اشتباه در متغیر ۱۶(زاویه فاز ولتاژ باس ۳)

طبق اینکه حمله به متغیر چهارم باید بر روی اندازه‌گیری‌های مربوط به باس دوم، سوم، چهارم تأثیر بگذارد که شامل درایه‌های ۲، ۳، ۴، ۱۶، ۱۷، ۱۸، ۳۱، ۳۲، ۳۳، ۵۱، ۵۲، ۵۳ ماتریس اندازه‌گیری می‌باشد که این درایه‌ها توان اکتیو و راکتیو تزریقی این باس‌ها و توان عبوری در خطوط مرتبط هستند و با توجه به شکل فوق مشخص است که بیشترین تشخیص در تمامی اندازه‌گیری‌های تحت تأثیر حمله مربوط به شاخص فاصله نسبی پیشنهادی بوده ضمن اینکه شاخص پیشنهادی توانسته در تمامی اندازه‌گیری‌های دستکاری‌شده به‌طور موفقیت‌آمیزی حمله را تشخیص دهد. همچنین با توجه به شکل ۴-۲۱ درصورتی‌که متغیر موردحمله ناشناخته باشد، می‌توان طبق اندازه‌گیری‌هایی که دچار دستکاری شده‌اند و ساختار شبکه به متغیر موردحمله نیز پی برد و این امر کارایی روش پیشنهادی را بیشتر نشان می‌دهد. به عبارتی با بررسی اندازه‌گیری‌های دچار حمله و همچنین متغیر موردحمله، مکان موردحمله در شبکه مشخص می‌گردد.

با توجه به کثرت داده‌ها و نتایج شبیه‌سازی و عدم امکان ارائه تمامی موارد، مابقی نتایج به‌صورت خلاصه در جدول ۴-۲ ارائه‌شده است.

جدول ۴-۲- خلاصه نتایج تست حملات تزریق داده اشتباه در متغیرهای حالت سیستم

| متغیر هدف مورد | $Orginal\ Data \times 100\%$ | | $Orginal\ Data \times 110\%$ | |
|---|---|---|---|---|
| تزریق | D | % | D | % |
| $V_1$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $V_2$ | ۷۹ | ۱ | ۸۹۱۸ | ۹۹.۹ |
| $V_3$ | ۷۹ | ۱ | ۷۷۶۶ | ۸۷ |
| $V_4$ | ۷۹ | ۱ | ۸۸۸۲ | ۹۹.۵ |
| $V_5$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $V_6$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $V_7$ | ۷۹ | ۱ | ۷۰۵۲ | ۷۹ |
| $V_8$ | ۷۹ | ۱ | ۸۹۲ | ۱۰ |
| $V_9$ | ۷۹ | ۱ | ۸۸۷۳ | ۹۹.۴ |
| $V_{10}$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $V_{11}$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $V_{12}$ | ۷۹ | ۱ | ۷۹۴۵ | ۸۹ |
| $V_{13}$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $V_{14}$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $\theta_2$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $\theta_3$ | ۷۹ | ۱ | ۶۶۹۵ | ۷۵ |
| $\theta_4$ | ۷۹ | ۱ | ۸۹۰۰ | ۹۹.۷ |
| $\theta_5$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $\theta_6$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $\theta_7$ | ۷۹ | ۱ | ۳۵۷۰ | ۴۰ |

| | | | | |
|---|---|---|---|---|
| $\theta_8$ | ۷۹ | ۱ | ۱۳۳۹ | ۱۵ |
| $\theta_9$ | ۷۹ | ۱ | ۸۸۸۲ | ۹۹.۵ |
| $\theta_{10}$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $\theta_{11}$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $\theta_{12}$ | ۷۹ | ۱ | ۷۴۰۹ | ۸۳ |
| $\theta_{13}$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |
| $\theta_{14}$ | ۷۹ | ۱ | ۸۹۲۷ | ۱۰۰ |

هر ردیف جدول ۴-۲ یک متغیر حالت که هدف حمله قرارگرفته است را نشان می‌دهد. برای هر متغیر حالت تزریقی به‌اندازه ۱۰٪ مقدار اصلی آن در نظر گرفته‌شده است که به‌صورت ۱۱۰٪ نشان داده‌شده است. ۱۱۰٪ بدین معنی می‌باشد که متغیر دستکاری‌شده سیستم ۱۰٪ بیشتر از مقدار واقعی می‌باشد. ۱۰۰٪ نیز بدین معنی است که هیچ حمله‌ای رخ نداده است.

نتایج هر متغیر حالت هدف و مقدار تزریقی به دو صورت ٪ و D نشان داده‌شده است. D نشان-دهنده نمونه‌های تشخیص داده‌شده و تحت حمله قرارگرفته می‌باشد. ٪ مقدار درصد نمونه‌هایی که تشخیص داده‌شده‌اند را نشان می‌دهد که از تقسیم D بر کل نمونه‌ها به دست می‌آید. در این مطالعه برای هر سناریو حمله، ۸۹۲۷ نمونه وجود دارد.

ستون سوم جدول نشان می‌دهد که وقتی متغیر حالت تحت حمله ۱۱۰٪ مقدار نامی است، روش پیشنهادی می‌تواند در برابر اغلب حملات بدون هیچ نمونه تشخیص نداده‌ای محافظت نماید و یا تعداد نمونه‌های غیرقابل تشخیص بسیار کم و قابل‌چشم‌پوشی می‌باشد. اما هنگامی‌که متغیر حالت تحت حمله ۱۰۵٪ متغیر اصلی است، نمونه‌های بیشتری وجود دارد که تشخیص داده نشده‌اند. این امر بدین دلیل است که ۱۰۵٪ در برابر ۱۰۰٪ به مقدار اصلی نزدیک‌تر بوده و حملات تأثیر کمتری بر اندازه‌گیرها می‌گذارند. به عبارتی میزان دستکاری متغیرها و اندازه‌گیری‌ها در درصد تشخیص بسیار

تأثیرگذار است چراکه هر چه میزان انحراف داده بیشتر شود، در منحنی هیستوگرام از مقدار آستانه تجاوز نموده و راحت‌تر قابل‌مقایسه و تشخیص می‌باشد.

با توجه به جدول ۴-۲ مشخص می‌شود که تشخیص اینکه کدام متغیر حالت تحت حمله قرارگرفته مشکل می‌باشد. اما این امر توسط نمودارهای ارائه‌شده در شکل‌های ۴-۲۳ و ۴-۱۹ راحت‌تر است چراکه به‌صورت ریز و جزئی میزان تشخیص هر اندازه‌گیری را مشخص نموده است که بر اساس آن و با توجه به ساختار شبکه می‌توان به‌راحتی متغیر تحت حمله مشخص نمود. در این پژوهش، تشخیص حمله به متغیرهای حالت در باس‌های ۳، ۷، ۸ و ۱۲ مشکل‌تر است. این امر بدین دلیل است که این باس‌ها ارتباط کمتری با دیگر باس‌های شبکه‌دارند و حمله به این متغیرهای حالت بر اندازه‌گیری‌های کمتری تأثیر می‌گذارد. به عبارتی میزان ارتباط هر متغیر با دیگر اندازه‌گیری‌های شبکه در درصد تشخیص داده اشتباه بسیار تأثیرگذار است.

ستون دوم جدول ۴-۲ نیز نتایج تست‌هایی است که هیچ حمله تزریق داده اشتباهی رخ نداده است. با توجه به جدول مشخص است که روش پیشنهادی ۹۹٪ از نمونه‌های تست را بدون حمله تشخیص داده است. عدد ۱ نشان داده‌شده در این ستون نشان‌دهنده این است که تنها ۱٪ داده اشتباه تشخیص داده‌شده است که آن‌هم می‌تواند ناشی از خطا در اندازه‌گیری و یا محاسبات و ... باشد. این امر نشان می‌دهد که روش پیشنهادی به‌درستی عمل نموده و هیچ اندازه‌گیری سالمی را به‌عنوان حمله اشتباه تشخیص نمی‌دهد.

بنابراین طبق نتایج این سناریو مشخص می‌شود که روش پیشنهادی در تمامی موارد توانسته داده‌های اشتباه را تشخیص داده و هیچ اندازه‌گیری سالمی را به‌عنوان حمله اشتباه تشخیص نداده‌اند ضمن اینکه با رسم هیستوگرام‌ها و نمودارهای درصد تشخیص می‌توان مکان وقوع حمله را نیز تشخیص داد.

## ۴-۵- جمع‌بندی و خلاصه فصل

در این فصل روش پیشنهادی در فصل سوم در مورد تشخیص تزریق داده اشتباه در شبکه هوشمند، بر روی یک شبکه تست پیاده‌سازی و اجرا گردید و نتایج آن در سناریو حمله متغیرهای حالت سیستم ارائه گردید. نتایج به‌صورت عدد، جدول، هیستوگرام و منحنی و ... ارائه شد و مورد تحلیل قرار گرفت. طبق نتایج ارائه‌شده مشخص گردید که شاخص فاصله مطلق به دلیل وجود همپوشانی در داده‌های قبلی و موجود قادر به تشخیص حملات تزریقی نمی‌باشد، اما شاخص فاصله نسبی پیشنهادی با تعریف یک مقدار آستانه مناسب می‌تواند به‌خوبی حملات را تشخیص داده و حتی با تحلیلی هر اندازه‌گیری در شبکه می‌توان مکان وقوع حمله را نیز مشخص نمود.

# فصل پنجم:

# نتیجه گیری و پیشنهادات

## ۵-۱- نتیجه‌گیری

ورودی به یک تخمینگر شامل اندازه‌گیری‌های ناقص از مقادیر ولتاژ و توان، توان موهومی یا توان ظاهری است. تخمینگر بدین‌صورت طراحی می‌شود که بهترین تخمین را از مقادیر ولتاژ و زوایای فاز در اختیار قرار دهد. پارامترهایی که برای تخمین حالت دقیق قابل‌استفاده‌اند شامل توان تزریقی اکتیو و راکتیو، اندازه ولتاژ یا جریان می‌باشد.

اما همواره حملات داده بد در انواع مختلف مسائل تخمین حالت را با تهدید مواجه می‌نماید. با توجه به هوشمند شدن شبکه‌های امروزی، حملات داده بد ممکن است در قالب حملات تزریق داده اشتباه که به‌عنوان حملات سایبری شناخته می‌شوند، صورت گیرند. حملات تزریق داده اشتباه بهره-برداری امن از شبکه قدرت را با تهدید مواجه می‌نماید. در این پژوهش،روشی جدید برای تشخیص حملات تزریق داده اشتباه ارائه گردید. روش پیشنهادی مبتنی بر شاخص فاصله نسبی لگاریتمی می-باشد که فاصله بین دو تابع $DZ_i^c$ و $DZ_i^h(k)$ را محاسبه می‌نماید. همچنین در این پژوهش از انحراف اندازه‌گیری داده‌های قبلی برای تشکیل $DZ_i^h(k)$ استفاده‌شده است و تابع $DZ_i^c$ در هر بازه زمانی، از اختلاف اندازه‌گیری بین گام زمانی فعلی و گام قبلی محاسبه‌شده است.

در شرایط معمول و عدم وجود حملات تزریق داده اشتباه، شاخص فاصله نسبی لگاریتمی عددی کوچک می‌باشد. اما در صورت وقوع حمله در سیستم، شاخص فاصله نسبی افزایش‌یافته تا به‌راحتی حمله تشخیص داده شود.

در فصل چهارم روش پیشنهادی بر روی شبکه تست پیاده‌سازی و اجرا شد و نتایج آن در سناریو حمله به متغیرهای حالت سیستم ارائه گردید. طبق نتایج ارائه‌شده مشخص گردید که شاخص فاصله مطلق به دلیل وجود همپوشانی در داده‌های قبلی و موجود قادر به تشخیص حملات تزریقی نمی-باشد، اما شاخص فاصله نسبی پیشنهادی با تعریف یک مقدار آستانه مناسب می‌تواند به‌خوبی حملات را تشخیص داده و حتی با تحلیل هر اندازه‌گیری در شبکه می‌توان مکان وقوع حمله را نیز مشخص نمود.

بنابراین نتایج مشخص نموده‌اند که روش پیشنهادی می‌تواند با دقت بالایی بسیاری از حملات تزریق داده اشتباه را تشخیص دهد. اما این امر نیز مشخص شد که تشخیص حملات تزریق داده اشتباه در متغیرهای خاصی از سیستم مشکل می‌باشد که دلیل آن کوچک بودن بازه زمانی و یا ارتباط کم آن متغیرها با دیگر اندازه‌گیری‌ها بیان گردید.

## ۵-۲- پیشنهادات

اما با توجه به نتایج مطرح‌شده می‌توان پیشنهاد نمود که در آینده کارهای زیر بر روی مسئله صورت گیرد:

۱) با توجه به نیاز روزافزون شبکه‌های مدرن به هوشمند سازی و مواجه شبکه‌های هوشمند با حملات تزریق اطلاعات بد، موضوع موردبررسی این پایان‌نامه می‌تواند بسیار کاربردی باشد. هرچند در این پایان‌نامه سعی بر آن بود که اطلاعات ثبت‌شده شبکه واقعی استفاده شود ولی به خاطر در دسترس نبودن تمامی اطلاعات مجبور به اصلاح شبکه موردمطالعه شده بودیم. ازاین‌رو بررسی روش پیشنهادی روی یک شبکه واقعی با در نظر گرفتن تمامی اطلاعات شبکه می‌تواند به‌عنوان یک پیشنهادی مطلوب در جهت کاربردی کردن آن ارائه شود.

۲) استفاده از تابع معیار دیگری برای شناسایی خطا به‌عنوان پیشنهاد دیگر می‌تواند برای ادامه کار طرح پیشنهادی ارائه شود.

۳) روش پیشنهادی بر اساس اطلاعات آماری گذشته و فرض صحت آن استوار است، ارائه روش دیگر که بتواند بدون در نظر گرفتن این فرض تشخیص حمله را انجام دهد، موضوع جالب و قابل‌توجه می‌باشد.

۴) با توجه به اینکه در شبکه‌های هوشمند، مهاجم از راه‌های مختلفی می‌تواند به شبکه حمله کند و ما در این پژوهش تنها یک نوع حملات سایبری به نام حملات تزریق اطلاعات غلط بررسی قرار گرفت، لذا پیش‌بینی راه‌های مختلف نفوذ مهاجم به شبکه و ارائه روشی برای دفاع در

مقابل آن حملات، می‌تواند موضوعی جالب و درعین‌حال برای امنیت شبکه بسیار پراهمیت می‌باشد.

# فهرست منابع


[1] The U.S. Department of Energy's Report (2008), The smart grid: An introduction.

[2] Q. Li and M. Zhou, "The future-oriented grid-smart grid," J. Comput. vol. 6, no. 1, pp. 98–105, 2011.

[3] P. Agrawal, "Overview of DOE microgrid activities," in Proc. Symp. Microgrid,Montreal,QC, Canada, 2006 [Online]. Available: http://der.lbl.gov/2006microgrids_files/USA/Presentation_7_Part1_Poonumgrawal.pdf.

[4] Niknam T, Kavousifard A, Baziar Aliasghar. Multi-objective stochastic distribution feeder reconfiguration problem considering hydrogen and thermal energy production by fuel cell power plants. Energy 2012;42(1):563e73.

[5] Bahmani-Firouzi B, Farjah E, Azizipanah-Abarghooee R. An efficient scenariobased and fuzzy self-adaptive learning particle swarm optimization approach for dynamic economic emission dispatch considering load and wind power uncertainties. Energy 2013;50(1):232e44.

[6] Kavousi-Fard A, Abunasri A, Zare A, Hoseinzadeh R. Impact of plug-in hybrid electric vehicles charging demand on the optimal energy management of renewable micro-grids. Energy 2014;78:904e15.

[7] Niknam T, Bahmani Firouzi B. A practical algorithm for distribution state estimation including renewable energy sources. Renew Energy 2009;34(11): 2309e16.

[8] Guo Y, Wu W, Zhang B, Sun H. A distributed state estimation method for power systems incorporating linear and nonlinear models. Int J Electr Power Energy Syst 2015;64:608e16.

[9] Niknam T, Narimani MR, Aghaei J, Azizipanah-Abarghooee R. Improved particle swarm optimization for multiobjective optimal powerflow considering cost, loss, emission, and voltage stability index. IET Generation, Trans Dis 2012;6(6):515e27.

[10] Yang T, Sun H, Bose A. Transition to a two-level linear state estimatordpart I: architecture. IEEE Trans Power Sys 2011;26(1):46e53.

[11] Menegak A. Valuation for renewable energy: a comparative review. Renew Sustain Energy Rev 2008;12:2422e37.

[12] Meliopoulos APS, Cokkinides G, Huang R, Farantatos E, Choi Y. Smart grid technologies for autonomous operation and control. IEEE Trans Smart Grid 2011;2(1):1e10.

[13] Georgilakis PS, Katsigiannis YA. Reliability and economic evaluation of small autonomous power systems containing only renewable energy sources. Renew Energy 2009;34(1):65e70.

[14] Xie L, Choi D, Vincent PH. Fully distributed state estimation for wide-area monitoring systems. IEEE Trans Smart Grid 2012;3(3):1154e69.

[15] Niknam T, Doagou Mojarrad H, Bahmani Firouzi B. A new optimization algorithm for multi-objective economic/emission dispatch. Int J Electr Power Energy Syst 2013;46:283e93.

[16] T. M. Cover and J. A. Thomas, Elements of Information Theory. Hoboken, NJ, USA: Wiley, 1991.

[17] Ali Abur, Antonio Gomez Exposito," Power System State Estimation ", Marcel Dekker Pob.

[۱۸] علی کلوانی اعظم، "تخمین حالت در سیستم‌های توزیع"، پایان‌نامه کارشناسی ارشد.

[19] Niknam T, Ranjbar AM, R.Shirani A. A new approach for distribution state estimation based on ant colony algorithm with regard to distributed generation. J Intell Fuzzy Syst 2005;16(2):119e31.

[20] Naka S, Genji T, Yura T, Fukuyama Y. A hybrid particle swarm optimization for distribution state estimation. IEEE Trans. Power Syst 2003;18(1):60e8.

[21] Lu Z, Ji T, Tang WH, Wu QH. Optimal harmonic estimation using a particle swarm optimizer. IEEE Trans Power Deliv 2008;23(2):1166e74.

[22] Wangand H, Schulz NN. A revised branch current-based distribution system state estimation algorithm and meter placement impact. IEEE Trans Power Syst 2004;19:207e13.

[23] Konjic T, Miranda V, Kapetanovic I. Fuzzy inference systems applied to LV substation load estimation. IEEE Tran. Power Syst 2005;20(2):742e9.

[24] Wan J, Miu KN. A zonal load estimation studies in radial power distribution networks. IEEE Trans Power Deliv 2002;17(4):1106e12.

[25] Ghosh A, Lubkeman DL, Downey MJ, Jones RH. Distribution circuit state estimation using a probabilistic approach. IEEE Trans Power Syst 1997;12: 45e51.

[۲۶] کمال بهلکه، سیدجلال سیدشنوا، مهدی نوشیار، تخمین حالت سیستم های توزیع درحضور منابع تولید پراکنده و ادوات DFACTS با استفاده ازالگوریتم تکامل دیفرانسیلی، مقاله‌های همایش‌های ایران. پنجمین کنفرانس ملی مهندسی برق و الکترونیک ایران. دانشگاه آزاد اسلامی واحد گناباد، ۱۳۹۲.

[۲۷] کمال بهلکه، تخمین حالت شبکه توزیع الکتریکی با حضور منابع تولید پراکنده با استفاده از الگوریتم بهینه سازی اجتماع ذرات، پایان‌نامه کارشناسی ارشد- وزارت علوم، تحقیقات و فناوری- دانشگاه محقق اردبیلی - دانشکده ۱۳۹۲.

[۲۸] بهاره باقری، تخمین حالت در شبکه‌های توزیع با در نظر گرفتن عدم قطعیت‌های ناشی از بار و منابع انرژی‌های نو، پایان‌نامه کارشناسی ارشد، وزارت علوم، تحقیقات و فناوری - دانشگاه صنعتی شیراز - دانشکده مهندسی برق و الکترونیک، ۱۳۹۳.

[29] Rakesh B. Bobba, Katherine M. Rogers, Qiyan Wang, Himanshu Khurana, Klara Nahrstedt and Thomas J. Overbye, Detecting False Data Injection Attacks on DC State Estimation.

[30] Lanchao Liu, Mohammad Esmalifalak, Qifeng Ding, Valentine A. Emesih, and Zhu Han, Detecting False Data Injection Attacks on Power Grid by Sparse Optimization, IEEE TRANSACTIONS ON SMART GRID, VOL. 5, NO. 2, MARCH 2014.

[31] Yao Liu, Peng Ning, Michael K. Reiter, False Data Injection Attacks against State Estimation in Electric Power Grids, CCS'09, November 9–13, 2009, Chicago, Illinois, USA.

[32] Yuancheng Li, Yiliang Wang, State summation for detecting false data attack on smart grid, Electrical Power and Energy Systems 57 (2014) 156–163.

[33] Beibei Li, Rongxing Lu, Wei Wang, Kim-Kwang Raymond Choo, Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system, J. Parallel Distrib. Comput. (2016).

[34] Liqun Yang, Yuancheng Li, Zhoujun Li, Improved-ELM method for detecting false data attack in smart grid, Electrical Power and Energy Systems 91 (2017) 183–191.

[35] Gu Chaojun, Panida Jirutitijaroen and Mehul Motani, Detecting False Data Injection Attacks in AC State Estimation, IEEE TRANSACTIONS ON SMART GRID, 2015.

[36] G. Hug and J. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," IEEE Trans. Smart Grid, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[37] Reza Khorshidi, Faridon Shabaninia, Taher Niknam, A new smart approach for state estimation of distribution grids considering renewable energy sources, Energy 94 (2016) 29-37.

[38] M. Do and M. Vetterli, "Wavelet-based texture retrieval using generalized Gaussian density and Kullback–Leibler distance," IEEE Trans. Image Process., vol. 11, no. 2, pp. 146–158, Feb. 2002.

[39] H. Lin, Z. Ou, and X. Xiao, "Generalized time-series active search with Kullback–Leibler distance for audio fingerprinting," IEEE Signal Process. Lett., vol. 13, no. 8, pp. 465-468, Aug. 2006.

[40] S. Tong, Z. Li, Y. Zhu, and N. Thakor, "Describing the nonstationarity level of neurological signals based on quantifications of timefrequency representation," IEEE Trans. Biomed. Eng., vol. 54, no. 10, pp. 1780–1785, Oct. 2007.

[41] Shama N, Islam M. A, Mahmud A, M.T. Oo, Impact of optimal false data injection attacks on local energy trading in a residential microgrid, ICT Express Volume 4, Issue 1, March 2018, Pages 30-34.

[42] Xuan Liu, Zuyi Li, False data attack models, impact analyses and defense strategies in the electricity grid, The Electricity Journal, Volume 30, Issue 4, May 2017, Pages 35-42.

[43] Liang Hu, Zidong Wang, Qing-Long Han, Xiaohui Liu, State estimation under false data injection attacks: Security analysis and system protection, Automatica, Volume 87, January 2018, Pages 176-183.

[44] Adnan Anwar, Abdun Naser Mahmood, Mark Pickering, Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements, Journal of Computer and System Sciences, Volume 83, Issue 1, February 2017, Pages 58-72.

[45] Ganesh K, Venayagamoorthy, Computational Approaches for Bad Data Handling in Power System Synchrophasor Networks, IFAC Proceedings Volumes, Volume 47, Issue 3, 2014, Pages 11269-11274.

[46] D. Singh, R.K. Misra, V.K. Singh, R.K. Pandey, Bad data pre-filter for state estimation, International Journal of Electrical Power & Energy Systems, Volume 32, Issue 10, December 2010, Pages 1165-1174.

[47] Seung Ho Hyun, Bogun Jin, Seung Jae Lee, A novel Bad Data Processing algorithm for analog data in substation automation systems, Applied Mathematics and Computation, Volume 205, Issue 2, 15 November 2008, Pages 824-831.

[48] T. Kim and H. Poor, "Strategic Protection against Data Injection Attacks on Power Grids," IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 326-333, June 2011.

[49] Qingyu Yang, Jie Yang, Wei Yu, Dou An, Nan Zhang, and Wei Zhao, On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures,IEEE Transactions on Parallel and distributed systems,vol 25,No.3,March2014.

[۵۰] نیما امین، "جایابی بهینه دستگاه‌های اندازه‌گیری فازور در شبکه‌های قدرت"، دانشگاه صنعتی شاهرود- دانشکده برق و رباتیک- پایان‌نامه کارشناسی ارشد، تیر ۱۳۹۰.

[۵۱] ماهنامه صنعت برق، صفحات ۱۶-۲۵، شماره ۱۵۶، چهارشنبه ۱۳۸۸/۱۰/۳۰، قابل دسترسی بصورت آنلاین در: وب سایت خبری روابط عمومی شرکت توانیرhttp://news.tavanir.org.ir.

[52] Freris LL, Sasson AM. Investigation of the load flow problem. Proc IEE 1968; 115(10):1459–69.

[53] M. Nejati, N. Amjady, and H. Zareipour, "A new stochastic search technique combined with scenario approach for dynamic state estimation of power systems," IEEE Trans. Power Syst., vol. 27, no. 4, pp. 2093–2105, Nov. 2012.

[54] POWER TRENDS, New York's Evolving Electric Grid, 2017. Available Online at: https://www.eenews.net/assets/2017/05/19/document_ew_01.pdf

**Abstract**

In power systems, state variables include voltage values and phase angles in the system nodes. Measurements are required to estimate system performance in real-time operation for both reliability control and economic load dispatch. The state estimation is the most important part of the monitoring of the power grid, in which the state of the system is determined and the operator is able to make the appropriate decision about the possible actions necessary to maintain the system's performance in a normal and reliable manner. To perform a state estimation, measurement data from Remote Terminal Units is sent to the power control system. Meanwhile, if the attacker attacks the information sent to the control center in some way, it can cause an estimation error in the estimator.

In this thesis, we propose a method for identifying bad data injections to the smart grid in a power system. In the first step, the proposed method uses the historical data of the power system and it calculates the deviation of the system's measurements and their histogram function. In the next step, using the proposed detection function through the histogram function calculated in the previous step, bad data injection attacks are detected. The proposed method performs a separate detection for each measurement. Therefore, according to the network structure, it is able to identify the target of an attacker.

**Keywords:** Bad Data detection, state estimation, cyber attacks, smart grid, power system.

**Shahrood University of Technology**

**Faculty of Electrical and Robotics Engineering**

**M.Sc. Thesis in Electrical Power Systems Engineering**

# Detection of False Data Injection Attacks in State Estimation of Power Networks

By: **Mohammad Amin Yazdanparast**

Thesis Supervisor:

**Dr. Mohsen Assili**

**July 2018**