A survey on detecting false data injection in power systems with auto-encoder based deep learning methods

M. Bakhshipour, F. Namdari*, M. B. Dolatshahi

*Assistant Professor, Amol Specialized University of New Technologies, Amol, Iran

(Received: 28/01/2021, Accepted: 19/06/2021)

ABSTRACT

The number of cyber-attacks affecting power systems and leading to physical and economic damages has grown rapidly over the last decade. Among the most significant types of cyber-attacks, are the class of false data injection attacks (FDIAs) which affect the power network monitoring systems. FDIAs endanger the power grid with manipulating the power system state estimation (SE). Also, the electricity theft has recently become another purpose of the FDAIs. Machine learning based methods are known as one of the FDIAs detection approaches. In this paper, first, using the deep auto-encoder method, the dimensions of the problem and the number of data entry for problem classification and detection are reduced. Then, by employing the support vector machine (SVM) approach and the data learning method, the procedure of cyber-attack detection is formed. Also, the precision of the proposed approach is improved by changing the number of data being trained. The presented method is evaluated on the IEEE 14 and 118 bus systems. The obtained simulation results demonstrate that the new method can successfully be applied for an accurate and effective detection of FDIAs.

Keywords: False data, cyber-attacks, deep learning, problem dimension reduction.

*Corresponding Author Email: Namdari.f@lu.ac.ir

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Publisher: Imam Hussein University © Authors

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۲، تابستان ۱۴۰۱، ص ۱۷-۱۱

علمی - پژوهشی

شناسایی تزریق داده کاذب در سامانه قدرت با استفاده از روش‌های یادگیری عمیق مبتنی بر خودرمزگذار

محمد بخشی‌پور[۱]، فرهاد نامداری[۲*]، محمدباقر دولتشاهی[۳]

۱- دانشجوی دکترا، ۲- دانشیار، گروه برق، ۳- استادیار، گروه آموزشی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه لرستان، خرم آباد، لرستان، ایران

(دریافت:۱۳۹۹/۱۱/۰۹، پذیرش:۱۴۰۰/۰۳/۲۹)

چکیده

در دهه گذشته، تعداد حملات سایبری به‌منظور هدف قرار دادن سامانه‌های قدرت که سبب خسارات فیزیکی و اقتصادی می‌گردد، افزایش یافته است. حملات تزریق داده کاذب، از جمله حملات سایبری می‌باشند که بر سامانه نظارت شبکه‌های برق اثر می‌گذارد. حملات با تزریق داده کاذب، با دستکاری در تخمین حالت سامانه قدرت، سبب به خطر انداختن شبکه قدرت می‌شود، همچنین به تازگی برقدزدی یکی از اهداف تزریق داده کاذب قرار گرفته است. روش‌های یادگیری ماشینی، یکی از راهکارهای تشخیص داده‌های کاذب است. در این مقاله، ابتدا با استفاده از روش خودرمزگذار عمیق، ابعاد مسئله، تعداد ورودی برای طبقه‌بندی مسئله و شناسایی، کاهش یافته و سپس با استفاده از روش بردار ماشین پشتیبانی و آموزش داده‌ها، عمل شناسایی انجام شده است. روش تشخیص، برای سامانه‌های ۱۴ و ۱۱۸ شینه IEEE مورد بررسی و مقایسه قرار گرفته و دقت هر روش بر اساس نتایج شبیه‌سازی طبقه‌بندی شده و همچنین به‌منظور اثربخشی روش پیشنهادی، با تغییر در تعداد داده‌های تحت آموزش، تأثیر تغییر در دقت شناسایی ارزیابی شده است که نتایج حاکی از اثر بخشی روش پیشنهادی می‌باشد.

کلیدواژه‌ها: داده کاذب، حملات سایبری، یادگیری عمیق، کاهش ابعاد مسئله

۱- مقدمه

امروزه سامانه‌های قدرت به‌منظور مدیریت تقاضا و تقسیم انرژی به‌صورت مؤثر، دارای حسگرها و ژنراتورهایی هستند که قابلیت ارتباط دو سویه را دارند [۱]. با وجود اینکه سامانه‌های ارتباطی دارای مزایای زیاد و مناسبی هستند که سبب راحتی فعالیت‌ها می‌گردد، اما این سامانه‌های ارتباطی، مستعد دستکاری برای حملات سایبری می‌باشند. حفظ پایداری در برابر حملات سایبری دشمن، همواره مورد توجه بوده است [۲]. حملات سایبری انواع گوناگونی را شامل می‌شود. حملات سایبری می‌تواند یکپارچه، مبتنی بر زمان، حملات متوالی وابسته، حملات هماهنگ و حملاتی که سبب تأخیر یا توقف فعالیت شوند، باشد [۳].

با توجه به توسعه بازار برق، حملات سایبری با هدف اختلال در برق‌رسانی و برق‌دزدی نیز انجام می‌پذیرد. از متداول‌ترین حملات در شبکه هوشمند که سبب اشتباه در اندازه‌گیری می‌شود، تزریق داده کاذب است [۱]. در ۲۳ دسامبر ۲۰۱۵، شبکه برق اوکراین هک شد و برق‌رسانی به صدها خانه بر اثر این حادثه مختل شد و سبب خاموشی گردید، این اولین حمله سایبری بود که منجر به قطع برق شد [۴]. لیو و همکاران نشان دادند که با استفاده از تزریق داده کاذب می‌توان تشخیص داده‌های بد را دور زد و خطای دلخواه را بدون شناسایی به حالت‌گر سامانه تزریق نمود [۵]. با توجه به عدم توانایی در شناسایی حملات با تزریق داده کاذب به روش تخمین حالت استاندارد، لزوم طبقه‌بندی این حملات احساس می‌شود.

مقالات زیادی به‌منظور شناسایی حملات تزریق داده کاذب ارائه شده است. ژانگ و همکاران در مرجع [۶] الگوریتمی مبتنی بر داده به‌منظور تشخیص داده‌های کاذب غیر قابل مشاهده را ارائه کرده‌اند. این الگوریتم به‌منظور کاهش ابعاد داده‌ها از رمزگذاری خودکار استفاده می‌کند. در مرجع [۷]، راوات و همکاران ارزیابی فیلتر کالمن را برای محاسبه تغییر اندازه‌گیری‌ها استفاده کردند، و حملات را با استفاده از روش‌های تطبیق شباهت آشکارساز مربع کای و آشکارساز کسینوسی مشخص کرد. رویکردهای تطبیق شباهت کسینوس هنگامی که به‌عنوان آشکارساز حملات تزریق داده کاذب و سایر حملات در شبکه هوشمند عمل می‌کند، از برتری برخوردار است. در مرجع [۸] حملات تزریق داده‌های کاذب با درنظر گرفتن خرابی حسگرها در شبکه‌های قدرت با تخمین حالت و سامانه تشخیص داده‌های بد (BDD) بررسی کرده‌اند. در مرجع [۹]، تانگ و همکاران نسبت احتمال کلی را برای تشخیص حملات مستقیم خارجی و تخمین حالت سامانه قدرت با استفاده از مدل خودهمبستگی مبتنی بر

* رایانامه نویسنده مسئول: Namdari.f@lu.ac.ir

* این مقاله یک مقاله با دسترسی آزاد است که تحت شرایط و ضوابط مجوز Creative Commons Attribution (CC BY) توزیع شده است.

© نویسندگان

ناشر: دانشگاه جامع امام حسین (ع)

نویز ارائه داده‌اند.

لی و یانگ [۱۰] از فناوری تشخیص گرافیکی به‌منظور تشخیص اندازه‌های دستکاری شده استفاده کرده‌اند. برای حل مسئله شناسایی موقعیت‌های حملات مستقیم خارجی از بعد متفاوت در سامانه‌های قدرت، شبکه‌هایی همراه با مدل گرافیکی شبکه را ایجاد کرده‌اند که می‌تواند خواص جزئی اطراف را از قبیل مکان، جهت، اتصال و غیره حفظ نماید. در مرجع [۱۱]، از روش یادگیری ماشین برای شناسایی حمله تزریق داده کاذب استفاده شده است. در مقایسه با روش مدل ماشین بردار پشتیبان[1] روش ارائه شده نیازی به مدل‌های حمله ندارد. چندین روش مبتنی بر یادگیری ماشین برای تشخیص حملات تزریق داده کاذب در مراجع [۱ و ۱۲] ارائه شده است. مرجع [۱۳] الگوریتم‌های بیشتری را برای شناسایی حملات تزریق داده کاذب آزمایش و مقایسه کرده است. الگوریتم‌های مانند SVM خطی و گاوسی، K نزدیک‌ترین همسایه[2] و یک شبکه عصبی یک لایه را مورد بررسی قرار داده است. مرجع [۱۳] ادعا کردند knn از حساسیت بیشتری برخورد است در حالی که SVM برای مسائل با مقیاس بزرگ بهتر است.

در مرجع [۱۴]، از آمار به‌منظور شناسایی حملات پنهان در سامانه قدرت استفاده کرده‌اند. نویسندگان دو الگوریتم مبتنی بر یادگیری ماشین برای تشخیص حمله ارائه داده‌اند. یکی از الگوریتم‌ها از یادگیری نظارت شده برای آموزش SVM بهره می‌گیرد. الگوریتم دیگر بدون آموزش داده‌ها، انحراف را اندازه‌گیری می‌کند. هر دو الگوریتم به‌منظور کاهش ابعاد بالای پردازش داده‌ها و پیچیدگی محاسبات، تحلیل اجزای اصلی را در پیش گرفتند. مرجع [۱۵] با اشاره به نیاز افزایش آگاهی به‌منظور مقابله بهتر و مناسب در برابر حملات سایبری با توجه به علاقه این حملات به استفاده از روش‌های مشابه طبقه‌بندی اقدامات متقابل در برابر تزریق داده‌های کاذب را امری ضروری دانسته و به این امر پرداخته است. در مرجع [۱۶]، یک آشکارساز حملات تزریق داده کاذب دو مرحله‌ای را نشان می‌دهد که شامل روش‌های SVM و تحلیل اجزای اصلی است. در مرحله اول، ابعاد زیاد اندازه‌گیری‌ها توسط تحلیل ابعاد اصلی به بعد پایین‌تر کاهش می‌یابد. بنابراین، حملات تزریق داده کاذب در داده‌های بعدی پایین توسط SVM در مرحله دوم شناسایی می‌شوند. مرجع [۱۷] به مطالعه و بررسی تشخیص حملات تزریق داده کاذب بر اساس همبستگی در زمان واقعی می‌پردازد. همچنین در مرجع [۱۸] با تکیه بر روش‌های یادگیری ماشین و با انتخاب ویژگی و پارامتر مناسب کارایی محاسباتی الگوریتم یادگیری ماشین را تا حد زیادی بهبود می‌بخشد. در مرجع [۱۹]، آشکارسازی حملات مستقیم و پنهان تزریق داده کاذب با طبقه‌بندی یادگیری نظارت شده مقایسه شده است. مرجع [۲۵] به بررسی روش‌های یادگیری ماشینی برای تشخیص حملات تزریق داده کاذب پرداخته است. این مرجع با اشاره به احتمال خرابی حسگر و دور زدن روش‌های تشخیص دیتای نادرست و تزریق داده کاذب، روش‌های تزریق را بررسی کرده است. در این مرجع روش‌های SVM و خودرمزنگار به‌صورت جداگانه تشریح شده است.

در این مقاله به بررسی تزریق داده کاذب در سامانه‌های قدرت پرداخته می‌شود. اولویت‌ها و مشارکت‌های مقاله ارائه راهکاری جهت کاهش در ابعاد داده‌ها و سپس شناسایی دقیق حملات می‌باشد. یکی از مشکلات برای شناسایی در سامانه قدرت، تعداد بالای اندازه‌گیری‌هاست. این امر زمانی بروز می‌کند که سامانه بزرگ شود. زیرا زمانی که الگوریتم‌های شناسایی با تعداد کمتری برچسب روبه‌رو باشند، توانایی بالاتری جهت شناسایی حملات دارند. در ادامه ابتدا روش تخمین حالت شرح داده شد، سپس در بخش بعدی حملات تزریق داده کاذب شرح داده شد. در بخش روش‌های انجام، روش خودرمزنگار عمیق شرح داده شد و سپس ماشین بردار پشتیبان به‌عنوان روش طبقه‌بندی ارائه شد. در انتها روش پیشنهادی در دو سامانه ۱۴ و ۱۱۸ شینه IEEE اجرا شد. از نوآوری‌های مقاله می‌توان به ارائه ترکیب روش خودرمزنگار و SVM جهت تشخیص حملات سایبری اشاره کرد. همچنین در این مقاله تأثیر نویز بر تشخیص حملات سایبری بررسی شده است.

۲- مدل‌سازی مسئله

SCADA در سامانه قدرت، با جمع‌آوری ولتاژ و جریان بار به تخمین وضعیت واقعی سامانه می‌پردازد. اشتباه در میزان اندازه‌گیری و یا دستکاری در آن سبب عدم تخمین درست از وضعیت شبکه می‌شود. از آنجایی که بر اساس مقادیر جریان و ولتاژ، وضعیت سامانه تخمین زده شده و این تخمین، دستوراتی را جهت اجرا در سامانه قدرت صادر می‌کند، تغییرات در اندازه‌گیری می‌توان سبب دستور اشتباه و در نتیجه مختل شدن برق‌رسانی شود، از این رو تخمین حالت شبکه برای امنیت و عملکرد پایدار شبکه هوشمند امری مهم و لازم است. به‌طور خلاصه در این بخش، تخمین حالت و حمله تزریق داده کاذب معرفی شده است.

۲-۱- تخمین حالت

تخمین حالت، تعیین و تخصیص مقدار به متغیر نامعلوم می‌باشد. ایده تخمین حالت در اوایل قرن نوزدهم، بر اساس حداقل مربعات

[1] Support Vector Machine (SVM)
[2] K-Nearest Neighbors (knn)

به وجود آمد. در سامانه‌های شبکه هوشمند، به‌منظور پیش‌بینی وضعیت سامانه، از تخمین حالت استفاده می‌شود. تخمین حالت رابطه‌ای بین متغیر حالت سامانه و اندازه‌گیری واقعی آن در سامانه قدرت نشان می‌دهد.

$$Z=H(x)+e; \quad (۱)$$

که در این رابطه، Z نشان دهنده بردار اندازه‌گیری شده، x نشانگر بردار متغیرهای حالت و H ماتریس ژاکوبی هست. مقدار e بردار خطای اندازه‌گیری است که به‌صورت تصادفی با پیروی از توزیع گاوسی ایجاد می‌شود. متغیر حالت در سامانه شامل زاویه فاز و دامنه‌های ولتاژ شینه‌هاست. در تخمین حالت اندازه‌گیری‌ها شامل توان حقیقی و موهومی تزریقی و انتقالی است. میلی و همکارانیک روش سریع جهت تخمین حالت را ارائه داده‌اند که در دو سامانه ۱۴ و ۱۱۸ شینه IEEE بررسی کرده‌اند [۲۰]. همچنین مرجع [جدید] به‌طور کامل تخمین حالت در سامانه را اشاره دارد.

تخمین حالت بر اساس روابط ریاضی بین متغیرهای حالت سامانه و اندازه‌گیری‌ها است. عمل محاسبه متغیرهای حالت مجهول بر اساس روش مجموع حداقل کردن مربعات وزن‌دار انجام می‌پذیرد. تابع هدف روش مجموع کمترین مربعات وزن‌دار بر اساس رابطه (۲) است.

$$J(x)=\sum_{i=1}^{m}\frac{(z_i-h_i(x))^2}{\sigma_i^2} \quad (۲)$$

بر اساس رابطه (۲)، x بردار حالت تخمین زده، z_i مقدار iامین اندازه‌گیری $h_i(x)$ مقدار تخمینی این اندازه‌گیری، σ_i^2 واریانس iامین اندازه‌گیری و m تعداد اندازه‌گیری مشخص است.

معیار خاصی، صورت می‌گیرد. معیار مرسوم اینست که تفاوت بین مقادیر محاسبه شده (تخمین زده شده) و مقادیر اندازه‌گیری شده (مقادیر حقیقی) حداقل شود. در یک سامانه 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 شینه‌ها در اختیار قرار دهد. سپس اطلاعات خروجی از تخمین حالت در مرکز کنترل سامانه در پخش بلادرنگ و کنترل قابلیت اطمینان سامانه‌های توزیع مورد استفاده قرار می‌گیرد. معمولاً تعداد اندازه‌گیری‌ها از مقدار مورد نیاز جهت تخمین حالت بیشتر است بنابراین تخمینگر حالت مجموعه‌ای از اندازه‌گیری‌های اضافی را به‌منظور تخمین حالت سامانه‌های توزیع پردازش می‌نماید.

۲-۲- حملات تزریق داده کاذب

حمله با تزریق داده کاذب از رایج‌ترین حملات سایبری است که آشکارسازی دشواری دارد. زیرا در مقایسه با حملات دیگر سایبری، دشمن می‌تواند با ارائه روش‌ها و توالی در حملات، راهکارهای آشکارسازی را فریب داده و سبب اشتباه روش‌ها شود [۲۱ و ۲۲]. از این رو، این عامل، انگیزه‌ای برای پژوهش در زمینه ارائه آشکارسازی برای حملات تزریق داده کاذب شده است. حملات تزریق داده کاذب، با تزریق داده غلط به مقادیر اندازه‌گیری شده، خروجی‌های تخمین حالت سامانه قدرت را خراب می‌کنند. به‌منظور موفقیت در حمله تزریق داده کاذب و همچنین عدم شناسایی در این حمله، مناسب است که باقیمانده تخمین حالت از آزمون آستانه کمتر شود. به‌طور رایج، در حملات با تزریق داده کاذب در صورت وجود سه عنصر آگاهی از عملکرد سامانه قدرت، توانایی در دستکاری اندازه‌گیری‌های اندازه‌گیر و آگاهی از اطلاعات عملیاتی و کلیدی شبکه قدرت در مهاجم، حمله موفقیت‌آمیز خواهد بود. در حملات تزریق داده کاذب، با تزریق بردار غیر صفر $a=(a1,a2,\ldots,am)T$ سبب تغییر در مقدار اندازه‌گیری شده (بر اساس رابطه ۳) و این امر سبب تغییر در مقادیر تخمین حالت می‌گردد (رابطه ۴).

$$Zbad=Z+a \quad (۳)$$

$$Xbad=x+c \quad (۴)$$

بر این اساس خطا به‌صورت رابطه (۵) تبدیل خواهد شد. زمانی که a=HC باشد، یک تزریق داده کاذب کامل است که روش‌های سنتی، داده‌های کاذب را شناسایی نمی‌کنند. در صورتی که a≠HC باشد، اما $\Delta a < \tau - r = \tau_a$ باشد، نیز روش‌های سنتی قابلیت تشخیص داده کاذب را نخواهد داشت که این حمله از نوع تزریق داده کاذب ناقص است.

$$\begin{aligned} r = z - \hat{z} &= h(x) + e + a - h(x) - H\tilde{x} \\ &\quad - Hc \\ &= (e - H\tilde{x}) + (a - HC) \end{aligned} \quad (۵)$$

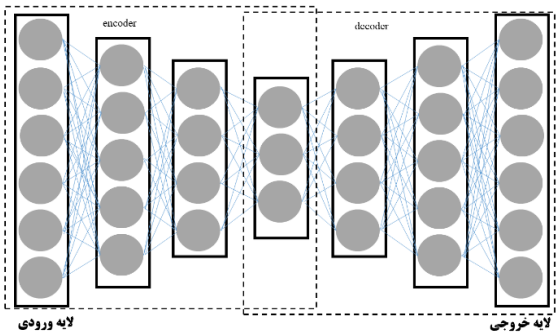
تخمین حالت، تعیین و تخصیص مقدار به متغیر نامعلوم می‌باشد. ایده تخمین حالت در اوایل قرن نوزدهم، بر اساس حداقل مربعات به وجود آمد. در سامانه‌های شبکه هوشمند، به‌منظور پیش‌بینی وضعیت سامانه، از تخمین حالت استفاده می‌شود. تخمین حالت رابطه‌ای بین متغیر حالت سامانه و اندازه‌گیری واقعی آن در سامانه قدرت نشان می‌دهد.

۲-۳- روش خودرمزگذار[1] عمیق

خودرمزگذار یک روش یادگیری بدون نظارت است. روش خودرمزگذار یک الگوریتم یادگیری عمیق است که از دو شبکه

[1] Autoencoder

متقارن با چند لایه کم عمق تشکیل شده است [۲۳] . شکل (۱) نشان دهنده یک خودرمزگذار است. رمزگذار از دو بخش تشکیل شده است، نیمی از شبکه کار رمزگذاری را انجام می‌دهند در حالی که نیمه دوم رمزگشایی می‌کند. روش تحلیل اجزای اصلی انعطاف پذیری کمتری نسبت به روش خودرمزگذار دارد زیرا روش خودرمزگذار حاصل رابط خطی و غیر خطی است در حالی که روش تحلیل اجزای اصلی، فقط خطی است. خروجی خودرمزگذار نمایش کمتری از ورودی است.



شکل (۱): نمایی از خودرمزگذار

فرض کنید مجموعه‌ای از نمونه‌های آموزشی بدون برچسب وجود دارد، فرآیند رمزگذاری و رمزگشایی توسط خودرمزنگار بر اساس روابط (۶) و (۷) می‌باشد.

$$d=S(W_1x+b_1) \quad (۶)$$

$$h_{w,t}(x)=S(W_2d+b_2) \quad (۷)$$

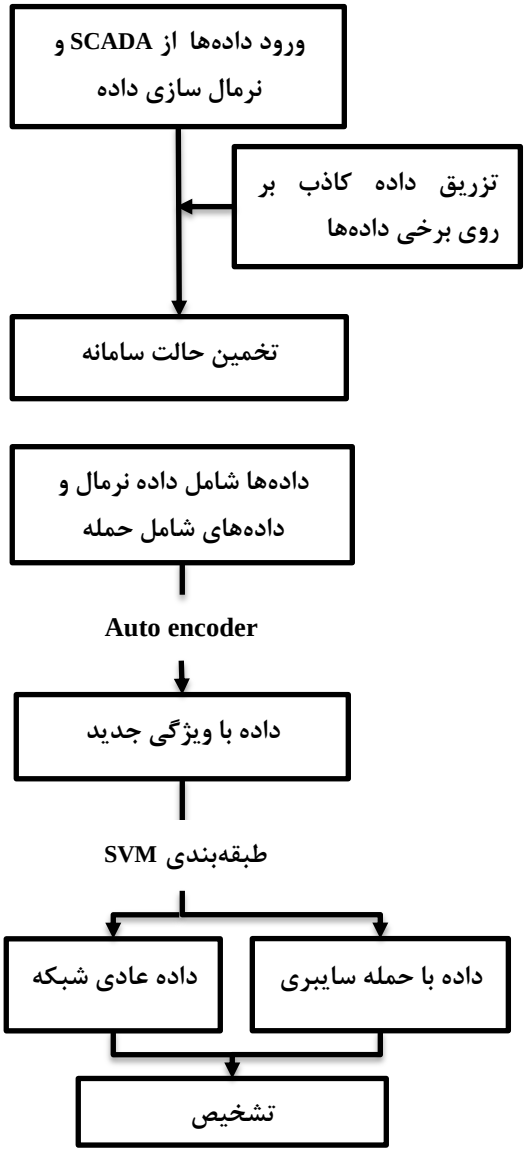
در این روابط، S یک تابع سیگموئید، W_1 ماتریس وزن بین لایه ورودی و لایه پنهان، W_2 ماتریس وزن بین لایه پنهان و لایه خروجی، bi بایاس است و $h_{w,b}(x)$ مقدار فعال‌سازی لایه خروجی در شبکه وزن w، بایاس b و ورودی x است. شبکه عصبی توسط الگوریتم پس انتشار که برای آموزش خودرمزنگار مناسب است، استفاده می‌گردد.

۲-۴- ماشین بردار پشتیبان

برای طبقه‌بندی به‌صورت "امن" یا "زیرحمله"، از ماشین بردار پشتیبان استفاده شده است. طبقه‌بندی SVM به تئوری یادگیری آماری متکی است و با استفاده از قوانین به حداقل رساندن ریسک ساختاری، گروهی از موضع گیری‌های مثبت را از یک کلاس از موارد منفی جدا کند. SVM حاشیه بین بردارهای پشتیبان را به حداکثر می‌رساند زیرا جداسازی تمام کلاس‌ها ضروری است [۲۴]. SVM به دلیل دقت طبقه‌بندی بالا و عملکرد در حل وظایف رگرسیون و طبقه‌بندی، یک روش یادگیری عامیانه است. SVM در ابتدا برای طبقه‌بندی باینری طراحی شده است. بعداً، آن را به سناریوهای چند طبقه تعمیم داد. شکل (۲) فلوچارت روش پیشنهادی ارائه شده است.

۳- نتایج و بحث

در مرحله شبیه‌سازی، از سامانه آزمون ۱۴ و ۱۱۸ شینه IEEE جهت ارزیابی استفاده شده است. اندازه‌گیری توان تزریقی در هر شینه با استفاده از تولباکس Matpower در محیط نرم‌افزار متلب ایجاد شده است. به جهت مقایسه دقت شناسایی روش پیشنهادی و صحت‌سنجی آن، روش پیشنهادی با روش ترکیبی شبکه عصبی و SVM در مرجع [۲۶] مقایسه شد.



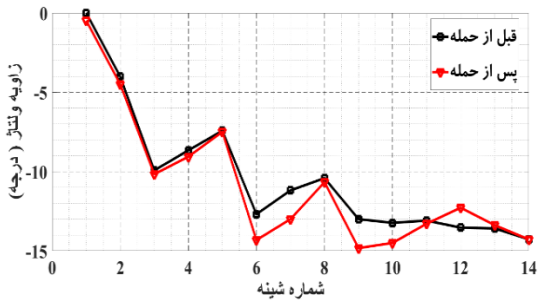
شکل (۲): فلوچارت تشخیص تزریق داده کاذب

خطای اندازه‌گیری بر اساس توزیع گاوسی می‌باشند. داده‌های ورودی برای سامانه ۱۴ شینه شامل ۴۱ پارامتر و برای سامانه ۱۱۸ شینه برابر ۴۸۹ پارامتر می‌باشد که توسط روش

خودرمزگذار کاهش یافته است. مجموعه کل داده‌های ۵۰۰ مورد است که از این موارد ۷۰ داده شامل تزریق داده کاذب است. ۱۰ درصد از داده‌ها نیز برای مرحله آزمون برگزیده شده‌اند. دقت روش ارائه شده بر اساس رابطه (۸) محاسبه می‌شود.

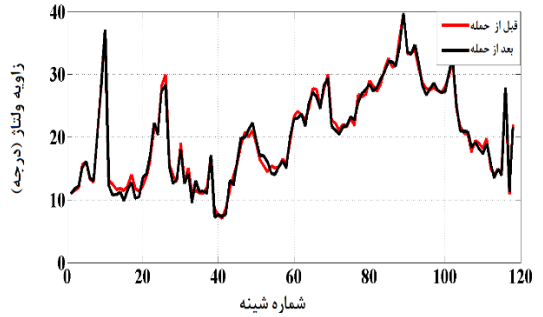
$$\text{Accuracy}=\frac{t_p+t_n}{Total\ Samples} \quad (۸)$$

در رابطه (۸)، t_p تعداد عملکرد درست روش ارائه شده در شناسایی حملات می‌باشد و t_n تعداد عملکرد درست روش ارائه شده در شناسایی داده‌ها بدون حملات می‌باشد. به‌منظور بررسی اثرگذاری روش ارائه شده جهت شناسایی حملات با تزریق داده کاذب، تعداد داده جهت آموزش را متفاوت درنظر گرفته شد. تعداد کل نمونه‌ها به ترتیب ۱۰۰، ۲۰۰، ۳۰۰، ۴۰۰ و ۵۰۰ نمونه انتخاب شد. تعداد نمونه‌های تزریق داده کاذب به ترتیب برای هر کدام ۱۴، ۲۸، ۴۲، ۵۶ و ۷۰ انتخاب شد. در هر مرحله ۱۰ درصد از کل تعداد نمونه به‌عنوان آزمون انتخاب می‌شود و از دیگر نمونه‌ها برای آموزش استفاده می‌شود. یک نمونه از تغییرات در اندازه‌گیری زاویه ولتاژ برای سامانه ۱۴ شینه در شکل (۳) نشان داده شده است. مشخص است که برآورد فاز بدون اینکه شناسایی شود، اصلاح شده است.



شکل (۳): تغییرات در اندازه فاز ولتاژ در سامانه ۱۴ شینه

شکل (۴)، برآورد فاز بدون شناسایی را در سامانه ۱۱۸ شینه نشان می‌دهد. شکل (۵) نمودار تغییرات تعداد کل داده بر دقت شناسایی را در سامانه ۱۴ شینه با روش پیشنهادی و روش مرجع [۲۶] ارائه می‌دهد.



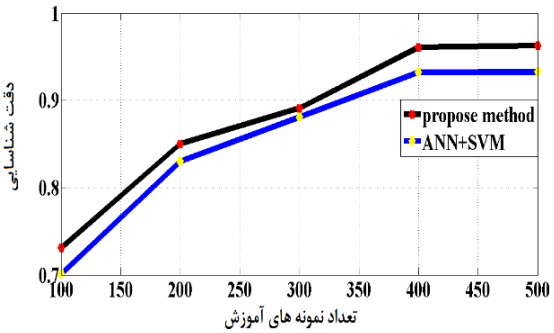
شکل (۴): تغییرات در اندازه فاز ولتاژ در سامانه ۱۱۸ شینه

در صورتی که داده‌های کمی برای آموزش انتخاب گردد، شناسایی در سامانه ۱۴ شینه با ۳۰ درصد خطا همراه است. در صورتی که حداقل ۴۰۰ نمونه کل انتخاب شود، شناسایی بالای ۹۰ درصد خواهد بود و قابل قبول است. به‌طوری که دقت شناسایی در سامانه ۱۴ شینه با ۵۰۰ نمونه کل، ۹۶ درصد خواهد بود، همچنین روش پیشنهادی اثربخشی بهتری از خود نشان می‌دهد.

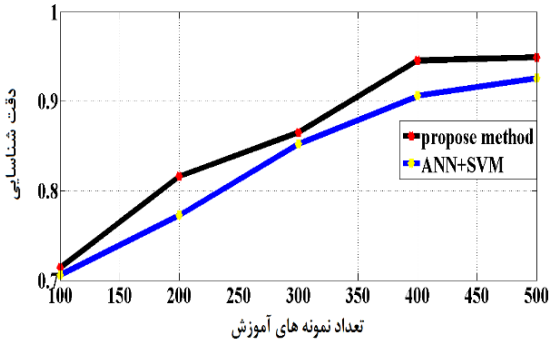
جدول (۱): دقت شناسایی روش پیشنهادی در سامانه ۱۴ و ۱۱۸ شینه IEEE

شاخص‌ها	شبکه ۱۴ شینه	شبکه ۱۱۸ شینه
دقت شناسایی روش پیشنهادی	۰,۹۶۲۸	۰,۹۴۹۲
ANN+SVM	۰/۹۳۲۵	۰/۹۰۱۸

شکل (۶) نمودار تغییرات تعداد کل داده‌ها بر روی دقت شناسایی روش پیشنهادی و روش ANN+SVM را نشان می‌دهد که علاوه بر اثربخشی روش پیشنهادی، نشان می‌دهد با اضافه شدن تعداد داده‌ها دقت شناسایی کمتر شده است. اما با توجه به اینکه در روش پیشنهادی ابتدا ویژگی‌ها استخراج می‌شود، اثربخشی مطلوبی دارد.

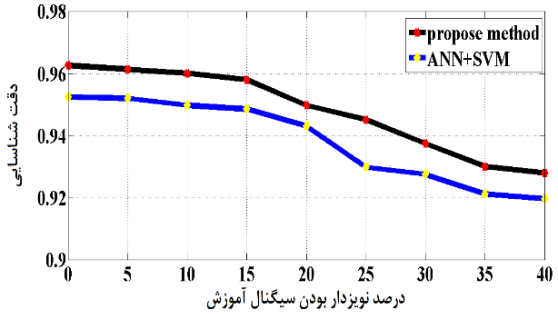


شکل (۵): منحنی تغییرات کل داده‌ها بر روی دقت شناسایی در سامانه ۱۴ شینه

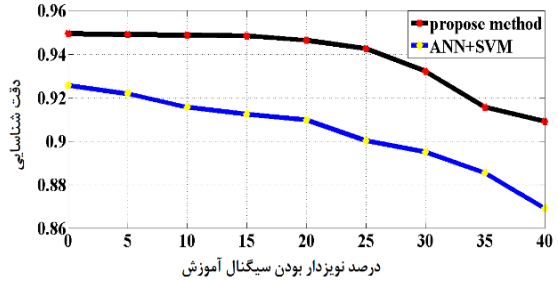


شکل (۶): منحنی تغییرات کل داده‌ها بر روی دقت شناسایی در سامانه ۱۱۸ شینه

به‌منظور تأثیر نویز در شناسایی حملات از حالت عادی سامانه، اثرات نویز در سیگنال را با نرخ‌های متفاوت در سیگنال آموزش مورد بررسی قرار گرفت. در این حالت ۵۰۰ نمونه برای هر سامانه انتخاب شد. شکل‌های (۷ و ۸) دقت شناسایی را در برابر درصد نویز نشان می‌دهد. با افزایش درصد نویز به کل سامانه، دقت در روش پیشنهادی کاهش می‌یابد اما شناسایی از ۹۰ درصد کمتر نخواهد شد. همچنین با افزایش نویز تا ۲۰ درصد، روش پیشنهادی قابلیت شناسایی با دقت بالا، بدون تأثیر در نتیجه کلی را نشان می‌دهد.



شکل (۷): تأثیر نویزدار بودن سیگنال آموزش بر دقت شناسایی در سامانه ۱۴ شینه



شکل (۸): تأثیر نویزدار بودن سیگنال آموزش بر دقت شناسایی در سامانه ۱۱۸ شینه

همچنین به‌منظور بررسی روش پیشنهادی، تأثیر نویز را در روش ترکیبی ANN و SVM بررسی شده است. در سامانه ۱۱۸ شینه که مسئله دارای داده‌های بیشتری است، روش پیشنهادی عملکرد بسیار مناسب‌تری در برابر نویز داشته است.

۴- نتیجه‌گیری

در این مقاله، یک طرح مبتنی بر خودرمزگذار عمیق با روش طبقه‌بندی SVM برای شناسایی و تشخیص حملات تزریق داده کاذب در سامانه‌های قدرت ارائه شد. از روش خودرمزگذار عمیق، به‌منظور کاهش در ابعاد مسئله و کاهش پیچیدگی استفاده می‌شود، زیرا پارامترها اندازه‌گیری شده برای سامانه‌های بزرگ، سبب پیچیدگی مسئله شده که برای این امر با کاهش ابعاد مسئله پرداخته شد. از این رو ابتدا داده‌ها آماده شده و به روش خودرمزگذار عمیق وارد شده است و سپس خروجی آن به SVM وارد شده است و آموزش شناسایی حملات با روش SVM انجام شد، که یک روش نظارت شده است. همچنین در این مقاله، تأثیر افزایش نویز در داده‌های آموزش مورد ارزیابی قرار گرفت و نشان داده شد که روش ارائه شده در مقابل نویز، عملکرد خوبی دارد. به‌منظور مقایسه روش پیشنهادی و اثربخشی آن، روش ارائه شده با روش ANN+SVM مقایسه شد. از آن‌هایی که با استفاده از روش خودرمزگذار ویژگی‌های داده‌ها استخراج شده و SVM با داده کمتری روبه‌روست، سبب بهبود جواب مسئله شده است.

۵- مراجع

[1] S. Jacob, H. Karimipour, and A. Dehghantanha, "Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection," In 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), 2019.

[2] M. Rahimi, F. Faghihi, B. Mozafari, "Control Strategy to Maintain Stability of Micro-grids, During Occurring Cyber Attacks on the Power Grid," Scientific Journal of Electronic and Cyber Defense, vol. 5, no. 2, pp. 47-58, 2017.

[3] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical Attack-resilient Wide-area Monitoring, Protection, and Control for the Power Grid," Proceedings of the IEEE, vol. 105, no. 7. pp. 1389-1407, 2017.

[4] A. Qiu, Zh. Ding, and Sh. Wang, "A Descriptor System Design Framework for False Data Injection Attack Toward Power Systems," Electric Power Systems Research, vol. 192, pp. 106932, 2020.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids," ACM Transactions on Information and System Security (TISSEC), vol. 14, no. 1, pp. 1-33, 2011.

[6] Y. Zhang, J. Wang, and B. Chen, "Detecting False Data Injection Attacks in Smart Grids: A Semi-supervised Deep Learning Approach," IEEE Transactions on Smart Grid, vol. 12, no. 1, pp. 623-634, 2020.

[7] D. B. Rawat and Ch. Bajracharya, "Detection of False Data Injection Attacks in Smart Grid Communication Systems," IEEE Signal Processing Letters, vol. 22, no. 10, pp. 1652-1656, 2015.

[8] A.-Y. Lu and G.-H. Yang, "False Data Injection Attacks against State Estimation in the Presence of Sensor Failures," Information Sciences, vol. 508, pp. 92-104, 2020.

[9] B. Tang, J. Yan, S. Kay, and H. He, "Detection of False Data Injection Attacks in Smart Grid under Colored Gaussian Noise," In 2016 IEEE Conference on Communications and Network Security (CNS), 2016.

[10] Y. Li and Y. Wang, "Developing Graphical Detection Techniques for Maintaining State Estimation Integrity against False Data Injection Attack in Integrated Electric Cyber-physical System," Journal of Systems Architecture, vol. 105, pp. 101705, 2020.

[11] Y. Chakhchoukh, S. Liu, M. Sugiyama, and H. Ishii, "Statistical Outlier Detection for Diagnosis of Cyber Attacks in Power State Estimation," In 2016 IEEE Power and Energy Society General Meeting (PESGM), 2016.

[12] S. Mohammadi, V. Desai, and H. Karimipour, "Multivariate Mutual Information-based Feature Selection for Cyber Intrusion Detection," In 2018 IEEE Electrical Power and Energy Conference (EPEC), 2018.

[13] M. Ozay, I. Esnaola, F. Tunay Yarman Vural, S. R. Kulkarni, and H. Vincent Poor, "Machine Learning Methods for Attack Detection in the Smart Grid," IEEE Transactions on Neural Networks and Learning Systems, vol. 27, no. 8, pp. 1773-1786, 2015.

[14] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Zh. Han, "Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid," IEEE Systems Journal, vol. 11, no. 3, pp. 1644-1652, 2014.

[15] M. Ahmed and A.-S. Kh. Pathan, "False Data Injection Attack (FDIA): An Overview and New Metrics for Fair Evaluation of Its Countermeasure," Complex Adaptive Systems Modeling, vol. 8, pp. 1-14, 2020.

[16] S. Waghmare, F. Kazi, and N. Singh, "Data Driven Approach to Attack Detection in a Ccyber-physical Smart Grid System," In 2017 Indian Control Conference (ICC), 2017.

[17] H. Karimipour and V. Dinavahi, "On False Data Injection Attack against Dynamic State Estimation on Smart Power Grids," In 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE), 2017.

[18] D. B. Rawat, and Ch. Bajracharya, "Detection of False Data Injection Attacks in Smart Grid Communication Systems," IEEE Signal Processing Letters, vol. 22, no. 10, pp. 1652-1656, 2015.

[19] J. Yan, B. Tang, and H. He, "Detection of False Data Attacks in Smart Grid with Supervised Learning," In 2016 International Joint Conference on Neural Networks (IJCNN), 2016.

[20] L. Mili, M. G. Cheniae, N. S. Vichare, and P. J. Rousseeuw, "Robust State Estimation Based on Projection Statistics [of Power Systems]." IEEE Transactions on Power Systems, vol. 11, no. 2, pp. 1118-1127, 1996.

[21] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Zh. Yang Dong, "AR of False Data Injection Attacks against Modern Power Systems," IEEE Transactions on Smart Grid, vol. 8, no. 4, pp.1630-1638, 2016.

[22] G. Liang, S. R. Weller, J. Zhao, F.Luo, and Zh. Yang Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317-3318, 2016.

[23] Y. Wang, H. Yao, and S. Zhao, "Auto-encoder Based Dimensionality Reduction," Neurocomputing, vol. 184, pp. 232-242, 2016.

[24] S. M. Erfani, S. Rajasegarar, Sh. Karunasekera, and Ch. Leckie, "High-dimensional and Large-scale Anomaly Detection Using a Linear One-class SVM with Deep Learning," Pattern Recognition, vol. 58, pp. 121-134, 2016.

[25] A. Sayghe, Y. Hu, I. Zografopoulos, X. R. Liu, R. G. Dutta, Y. Jin, and Ch. Konstantinou, "Survey of Machine Learning Methods for Detecting False Data Injection Attacks in Power Systems," IET Smart Grid, 2020.

[26] A. Kajal, and S. K. Nandal, "A Hybrid Approach for Cyber Security: Improved Intrusion Detection System Ising Ann-svm," Indian Journal of Computer Science and Engineering, vol. 11, no. 4,pp. 325-412, 2020.