

تشخیص حمله‌ی سایبری تزریق داده‌ی غلط در شبکه‌ی برق مبتنی بر PMU با استفاده از فیلتر کالمن

بهنام همایی^۱، دانشجو کارشناسی ارشد؛ سعید ابازری^۲، دانشیار؛ مجتبی برخوردار یزدی^۳، استادیار

۱- دانشکده فنی و مهندسی - دانشگاه شهرکرد - شهرکرد - ایران - homaei@stu.sku.ac.ir

۲- دانشکده فنی و مهندسی - دانشگاه شهرکرد - شهرکرد - ایران - abazari-s@eng.sku.ac.ir

۳- بخش مهندسی برق - دانشگاه شهید باهنر کرمان - کرمان - ایران - barkhordari@uk.ac.ir

چکیده: با گسترش استفاده از شبکه‌های ارتباطی و ساختار سایبر- فیزیکی در سیستم‌های قدرت، حملات سایبری به تهدیدی جدی در شبکه‌ی برق تبدیل شده‌است. برهم‌کنش شبکه‌های ارتباطی (لایه سایبری) و شبکه‌های برق (لایه فیزیکی)، فرایند تخمین حالت سیستم‌های قدرت را نسبت به حملات سایبری آسیب‌پذیر کرده‌است. در این مقاله، مسئله‌ی تشخیص حمله‌ی تزریق داده‌ی غلط (FDI) در شبکه‌ی برق با در نظر گرفتن اندازه‌گیری‌های انجام‌شده توسط واحد اندازه‌گیری فازور (PMU) و تخمین دینامیکی متغیرهای حالت سیستم توسط تخمین‌گر کالمن مورد بحث قرار گرفته است. حمله‌ی مورد نظر به کانال‌های ارتباطی بین PMU و تخمین‌گر حالت صورت می‌گیرد. نشان داده شده است به دلیل ماهیت هوشمند حمله‌ی FDI طراحی شده، آشکارساز χ^2 که کارایی خوبی برای تشخیص سایر انواع حملات سایبری دارد، قادر به تشخیص این نوع حمله نیست. در مقابل روش ارائه‌شده که از آشکارساز فاصله اقلیدسی و فیلتر کالمن استفاده می‌کند، کارایی خوبی در تشخیص حمله‌ی FDI از خود نشان می‌دهد. اگر مهاجم با الگوریتمی پیشرفته و بر اساس اطلاعاتی که از شبکه و پارامترهای آن دارد، حمله را به گونه‌ای طراحی کند که در چند PMU به طور جزئی تزریق داده غلط انجام شود، آشکارساز طراحی شده قادر خواهد بود این حمله را به سرعت تشخیص دهد. احتمال تشخیص نادرست به دلیل اثر نویز کمتر از ۱ درصد است. تأثیر حمله‌ی FDI بر تخمین حالت سیستم و کارایی روش مورد مطالعه در تشخیص حمله در سیستم استاندارد ۱۴ باسه IEEE نشان داده شده‌است.

واژه‌های کلیدی: حملات سایبری، حمله‌ی تزریق داده‌ی غلط (FDI)، واحد اندازه‌گیری فازور (PMU)، فیلتر کالمن.

Detection of False Data Injection Attack in PMU-based Power Grid Using Kalman Filter

Behnam Homaei, MSc Student¹; Saeed Abazari, Associate Professor²; Mojtaba Barkhordari Yazdi, Assistant Professor³

1- Faculty of Technical and Engineering, University of shahrekord, shahrekord, Iran, Email: homaei@stu.sku.ac.ir

2- Faculty of Technical and Engineering, University of shahrekord, shahrekord, Iran, Email: abazari-s@eng.sku.ac.ir

3- Electrical Engineering Department, Shahid Bahonar University of Kerman, Kerman, Iran, Email: barkhordari@uk.ac.ir

Abstract: Cyber-attacks have become a serious threat to the power grid by expanding the use of communication networks and cyber-physical systems in power systems. due to the connection between communication networks (cyber layer) and Power Grids (physical layer), state estimation of power systems is vulnerable to cyber- attacks. In this paper, state estimation in the power system without any cyber-attacks has occurred, then the detection of false data injection attack power grid when the measurements made by phasor measurement unit (PMU), and the dynamic estimation of the system state variables are estimated by Estimator Kalman. The attack is applied to the communication channels between the PMU and the state estimator. The proposed method which is based on the Kalman filter and the Euclidean distance detector has a good performance in detection of complex attacks such as a false data injection attack. The effectiveness of the proposed method is shown by simulating false data injection attacks on the IEEE 14-bus system. The impact of the FDI attack on the state estimation system and the effectiveness of the proposed method is shown detection of attacks in an IEEE 14-bus system is shown.

Keywords: Cyber-attacks, false data injection (FDI) attack, phasor measurement unit (PMU), kalman filter.

تاریخ ارسال مقاله: ۱۳۹۶/۷/۷

تاریخ اصلاح مقاله: ۱۳۹۷/۲/۱۵ و ۱۳۹۷/۴/۲۳

تاریخ پذیرش مقاله: ۱۳۹۷/۴/۳۱

نام نویسنده مسئول: سعید ابازری

نشانی نویسنده مسئول: ایران - شهرکرد - بلوار رهبر - دانشگاه شهرکرد - دانشکده فنی و مهندسی.

۱- مقدمه

با پیشرفت سریع حس گر‌ها، کامپیوترها و شبکه‌های ارتباطی سیستم‌های قدرت به سیستم‌های سایبر-فیزیکی^۱ پیچیده‌ای تبدیل شده‌است. امروزه شبکه برق اساساً توسط سیستم‌های سایبری پشتیبانی می‌شود که از یک‌سو منجر به بهبود نظارت و کنترل شبکه شده و از سوی دیگر تأمین امنیت آن به‌عنوان مسئله‌ای مهم در سیستم قدرت خودنمایی می‌کند [۱]. در دهه‌ی اخیر با پیشرفت سیستم سایبر-فیزیکی و کاربرد آن در سیستم قدرت، آسیب‌پذیری جدیدی تحت عنوان حملات سایبری پدید آمده‌است [۲].

یکی از مهم‌ترین حملات سایبری در سیستم کنترل بنام استاکس‌نت^۲ در سال ۲۰۱۰ گزارش شد که یکی از اهداف آن آسیب رساندن به تجهیزات تأسیسات هسته‌ای ایران بود [۳]. چنین حملاتی باعث شد مسئله امنیت سایبری و آسیب‌پذیری سیستم‌ها به مسئله‌ای جدی در تحقیقات تبدیل شود.

حمله‌ی تزریق داده‌ی غلط (FDI^۳) به سیستم قدرت برای اولین بار در [۴]، با فرض آگاهی کامل مهاجم از سیستم مطرح شد. در سناریوی مطرح‌شده، فرض می‌شود که مهاجم از ماتریس متغیرهای حالت سیستم قدرت هدف آگاهی دارد و داده‌های خرابکارانه را با علم به این ماتریس می‌سازد. سپس داده‌های غلط را به سیستم نظارت و کنترل تزریق کرده تا فرآیند کنترل را دچار اشتباه کند [۵].

مرجع [۶] حملات FDI به شبکه‌ی برق اوکراین در اواخر سال ۲۰۱۵ و وقوع حملات FDI در شرایط عملی سیستم قدرت را مورد بحث قرار داده‌است. نتیجه این حملات، خسارت‌ها و خاموشی‌های گسترده برای ۲۲۵ هزار مشترک بود [۷].

به‌جز حمله‌ی FDI حملات دیگری مانند حمله به تمامیت اطلاعات^۴، حمله‌ی منع خدمت^۵ و حمله‌ی بازسازی اطلاعات^۶ نسبت به سیستم کنترلی و خطوط ارتباطی قابل انجام است. باین‌حال دلیل تمرکز این مقاله بر حمله‌ی FDI این است که در این نوع حمله دست‌کاری حساب‌شده داده‌های سیستم اندازه‌گیری، منجر به ایجاد داده‌های غلط می‌شود و روش‌های مرسوم قادر به تشخیص این نوع حمله نیستند [۵].

استراتژی‌های گوناگونی برای مقابله با حمله‌ی FDI در مراجع مختلف مورد بحث قرار گرفته‌است. در [۸] به حفاظت از مجموعه اندازه‌گیری‌های اصلی و در [۹] حفاظت از سیستم قدرت براساس PMU^۷ پرداخته شده‌است. باین‌حال نویسنده در [۱۰] بیان می‌کند که باوجود حفاظت مبتنی بر PMU، مهاجم قادر است به مجموعه اندازه‌گیری‌ها حمله کند و منجر به قطع برق شبکه انتقال شود.

یکی از راه‌های مقابله با حملات سایبری تشخیص به‌موقع آن‌ها است. یک استراتژی کلی برای تشخیص یا شناسایی حملات FDI، استفاده از تخمین گر و آشکارساز مناسب است. آشکارسازها با پردازش داده‌های حاصل از تخمین حالت و مقادیر قرائت‌شده به تشخیص حملات می‌پردازند [۱۴]. در همین راستا روش‌های استاتیکی تخمین

حالت سیستم قدرت مانند روش حداقل مربعات وزن دار، به دلیل هم گرایی سریع و پیاده‌سازی آسان استفاده شده‌است. مراجع مختلفی مانند [۱۱، ۱۲] به بررسی امنیت سایبری سیستم تحت حمله‌ی FDI با روش‌های تخمین حالت استاتیکی می‌پردازد؛ درحالی‌که به دلیل ماهیت دینامیکی شبکه‌ی برق، روش‌های استاتیکی در پیش‌بینی وضعیت آینده سیستم قدرت و تشخیص حملات دینامیکی FDI، ناتوان هستند [۱۳].

مطالعات نشان می‌دهد که آشکارساز χ^2 یک انتخاب معمول برای تشخیص حملات به کمک تخمین گر کالمن است [۱۵]. آشکارساز χ^2 می‌تواند خطاها و حملات مختلفی مانند حمله تصادفی^۸ و حمله منع خدمت را تشخیص دهد، زیرا با تزریق این گونه داده‌ها، بردار اندازه‌گیری به‌طور قابل توجهی تغییر خواهد کرد [۱۶]. این در حالی است که حمله‌ی FDI را نمی‌توان توسط آشکارسازهای آماری متداول شناسایی کرد [۱۷].

در این مقاله، ابتدا مدل شبکه‌ی برق در حالت کارکرد عادی (بدون حملات سایبری) ارائه شده و سپس به مدل‌سازی حمله‌ی FDI بر روی سیستم قدرت پرداخته شده‌است. در بخش سوم نشان داده شده که حمله‌ی FDI در سیستم قدرت با ترکیب تخمین گر کالمن و آشکارساز χ^2 قابل تشخیص نیست. سپس روش ارائه شده فیلتر کالمن و آشکارساز فاصله اقلیدسی^۹ در تشخیص این نوع حمله معرفی می‌شود. در این روش آشکارساز فاصله اقلیدسی و فیلتر کالمن با محاسبه اختلاف داده‌های مشاهده شده از داده‌های تخمین زده شده در هر لحظه به تشخیص حملات می‌پردازند. در بخش چهارم نتایج شبیه‌سازی به‌منظور ارزیابی کارایی آشکارساز فاصله اقلیدسی بر سیستم ۱۴ باسه IEEE ارائه شده‌است. در پایان، جمع‌بندی و نتیجه‌گیری ارائه می‌شود. نوآوری‌های اصلی این مقاله عبارت‌اند از:

۱- با توجه به مزایای استفاده از PMU و استفاده فزاینده از آن در شبکه‌های قدرت، از داده‌های حاصل از PMU برای تخمین حالت استفاده شده است. به این ترتیب تشخیص حمله FDI در این مقاله مبتنی بر مدل فرایند با در نظر گرفتن PMU است.

۲- الگوریتمی که برای تولید حمله FDI مطرح شده‌است مبتنی بر الگوریتم بهبود یافته‌ای است که در مرجع [۲۴] معرفی شده است. با این الگوریتم شرط ناامن شدن سیستم ساده‌تر می‌شود و به عبارتی تشخیص حمله دشوارتر خواهد شد. در این مقاله نشان داده شده‌است که آشکارساز فاصله اقلیدسی قادر به تشخیص این حمله است. براساس بررسی‌های انجام شده، این الگوریتم حمله تاکنون در شبکه‌های قدرت مورد استفاده قرار نگرفته‌است.

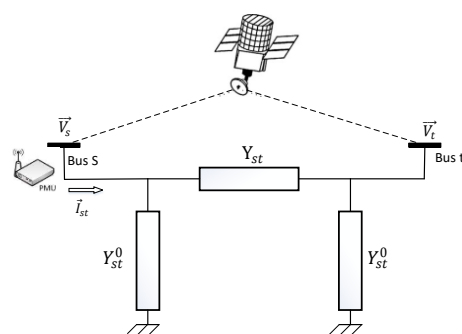
۳- در روش ارائه شده فقط نیمی از اطلاعات دریافتی از PMU برای تشخیص حمله مورد استفاده قرار می‌گیرد و به این ترتیب بار محاسباتی کاهش یافته و سرعت تشخیص حمله افزایش می‌یابد.

۲- بیان مسئله

شبکه‌ی قدرت موردبررسی N باس دارد که در M باس PMU نصب شده‌است. فرض می‌شود که با این اندازه‌گیری‌ها رؤیت پذیری کامل در شبکه برقرار است. در این شبکه برای تخمین حالت سیستم از تخمین گر کالمن استفاده شده‌است. حالت‌های تخمین زده شده به سیستم مدیریت انرژی^۱ (EMS) ارسال می‌شود تا برای اهدافی مانند مانیتورینگ و کنترل شبکه مورد استفاده قرار گیرد.

ساختار کلی تخمین حالت شبکه‌ی برق مبتنی بر PMU تحت حملات سایبری در شکل ۱ نشان داده شده‌است. در مسئله‌ی موردنظر، مهاجم با حمله‌ی سایبری از نوع FDI از طریق خطوط ارتباطی بین شبکه برق و تخمین گر حالت به اندازه‌گیری‌های انجام شده توسط PMU داده‌ی غلط تزریق می‌کند. به این ترتیب با ایجاد مشکل در تخمین حالت عمل کرد طبیعی شبکه‌ی برق مختل می‌شود. هدف اصلی مسئله تشخیص دقیق و سریع حمله‌ی طراحی شده با بهره‌گیری از داده‌های دریافتی از فیلتر کالمن و واحدهای اندازه‌گیری فازوری است.

در ادامه‌ی این بخش پس از معرفی مدل شبکه به همراه PMU روند تخمین حالت توسط فیلتر کالمن بیان می‌شود. سپس به مدل سازی حمله‌ی FDI بر سیستم قدرت و الگوریتم ایجاد این حمله پرداخته شده‌است. به عبارتی در این بخش سیستم قدرت با تخمین گر حالت در شرایط ناامن و در معرض حمله مدل شده‌است. در بخش بعد تخمین حالت در حضور حمله FDI و چگونگی آشکارسازی حمله موردبررسی قرار گرفته‌است.



شکل ۲: ولتاژ باس و جریان فازور در مدل π

باس‌های متصل شده به PMU با $s_1, s_2, \dots, s_M$ مشخص می‌شوند. اندازه‌گیری‌های $z_{s_l} \in \mathbb{R}^{2(1+N_l)}$ از PMU s_l مستقر شده در باس s_l به دست آمده که به صورت بردار

$$z_{s_l} = [x_{r,s_l} \ x_{i,s_l} \ z_{r,t_1^{s_l}} \ z_{i,t_1^{s_l}} \ \dots \ z_{r,t_{N_l}^{s_l}} \ z_{i,t_{N_l}^{s_l}}]^T \quad (2)$$

قابل نمایش است که x_{r,s_l} و x_{i,s_l} به ترتیب، قسمت‌های حقیقی و موهومی ولتاژ اندازه‌گیری شده باس s_l هستند. اندازه‌گیری‌های جریان خط متصل شده به دو باس s_l و $t_\eta^{s_l}$ به صورت

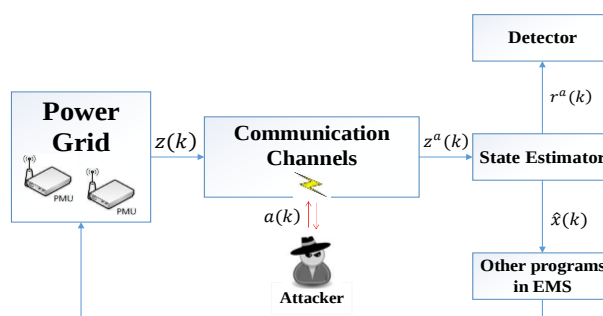
$$z_{r,t_\eta^{s_l}} = x_{r,s_l} g_{s_l,t_\eta^{s_l}}^0 - x_{i,s_l} b_{s_l,t_\eta^{s_l}}^0 + (x_{r,s_l} - x_{r,t_\eta^{s_l}}) g_{s_l,t_\eta^{s_l}} - (x_{i,s_l} - x_{i,t_\eta^{s_l}}) b_{s_l,t_\eta^{s_l}} \quad (3)$$

$$z_{i,t_\eta^{s_l}} = x_{i,s_l} g_{s_l,t_\eta^{s_l}}^0 + x_{r,s_l} b_{s_l,t_\eta^{s_l}}^0 + (x_{i,s_l} - x_{i,t_\eta^{s_l}}) g_{s_l,t_\eta^{s_l}} + (x_{r,s_l} - x_{r,t_\eta^{s_l}}) b_{s_l,t_\eta^{s_l}}$$

به دست می‌آید که $z_{r,t_\eta^{s_l}}$ و $z_{i,t_\eta^{s_l}}$ به ترتیب، اندازه‌گیری‌های جریان حقیقی و موهومی هستند.

باتوجه به نویز اندازه‌گیری در نظر گرفته شده، اندازه‌گیری‌های PMU به شکل

$$z(k) = Hx(k) + v(k) \quad (4)$$



شکل ۱: تخمین حالت شبکه‌ی برق مبتنی بر PMU تحت حملات سایبری

۱-۲- شبکه‌ی برق بدون حضور حملات سایبری

در ادامه مدل شبکه‌ی برق در حالت کارکرد نرمال و بدون حضور حملات سایبری به همراه مدل اندازه‌گیری PMU توضیح داده خواهد شد. معادله دینامیکی

$$x(k+1) = Ax(k) + Bu + \omega(k) \quad (1)$$

به عنوان مدل سیستم قدرت N باسه استفاده می‌شود که $x(k) \in \mathbb{R}^n$ حالت سیستم و بردار فازور ولتاژ تمامی باس‌ها، $u \in \mathbb{R}^n$ ولتاژ نامی، $\omega(k) \in \mathbb{R}^n$ نویز گوسی فرآیند با میانگین صفر و ماتریس

$$K(k+1) = \bar{P}(k+1)H^T(H\bar{P}(k+1)H^T + R(k+1))^{-1} \quad (12)$$

$$\hat{x}(k+1) = \tilde{x}(k+1) + K(k+1)(z(k+1) - H\tilde{x}(k+1)) \quad (13)$$

$$P(k+1) = (I - K(k+1)H)\bar{P}(k+1) \quad (14)$$

K بهره کالمن نامیده می‌شود. در [۲۲، ۱۵] نشان داده شده که بهره کالمن پس از چند تکرار هم‌گرا شده و می‌توان به سادگی مقدار حالت ماندگار K را در تخمین گر کالمن استفاده کرد. مقدار بهره کالمن را می‌توان از روابط

$$P \triangleq \lim_{k \rightarrow \infty} \bar{P}(k+1) \quad (15)$$

$$K = PH^T(HPH^T + R)^{-1}$$

به دست می‌آید؛ بنابراین روابط ساده تخمین گر به صورت

$$\begin{cases} x(k+1) = Ax(k) + \omega(k) \\ \hat{x}(k+1) = A\hat{x}(k) + Kr(k+1) \\ r(k+1) = z(k+1) - HA\hat{x}(k) \end{cases} \quad (16)$$

به دست می‌آید؛ که در آن $\hat{x}(k+1)$ و $r(k+1)$ به ترتیب تخمین حالت و باقی‌مانده تخمین در لحظه $k+1$ هستند.

از خطای تخمین $e(k)$ ، خطای تخمین دینامیکی

$$e(k+1) = Ae(k) - Kr(k+1) + \omega(k) \quad (17)$$

$$= (I - KH)(Ae(k) + \omega(k)) - Kv(k+1)$$

به دست می‌آید. تخمین گر کالمن پایدار است اگر و تنها اگر ماتریس $(I - KH)A$ پایدار شود [۲۳]. طبیعی است که در ادامه فرض شده، تخمین گر با انتخاب بهره K مناسب پایدار است.

همان‌طور که در شکل ۱ مشاهده شد، PMU ها و تخمین گر توسط شبکه‌های باسیم یا بی‌سیم به یکدیگر متصل شده‌اند و مستعد ابتلا به حملات سایبری ایجاد شده توسط مهاجمان هستند. در قسمت بعد، حمله‌ی سایبری FDI معرفی شده است که می‌تواند امنیت سیستم قدرت را تحت تأثیر قرار دهد.

۳-۲- حمله‌ی تزریق داده‌ی غلط

در این بخش، مدل حمله‌ی FDI معرفی شده است و پس از آن چگونگی تأثیر آن بر دینامیک‌های سیستم بررسی می‌شود. فرض می‌شود دشمن در مورد مدل سیستم دانش کامل دارد و مقادیر ماتریس‌های A ، H ، W ، R و بهره K برای مهاجم شناخته شده است [۲۴، ۱۶]. همچنین مهاجم توانایی تزریق داده‌ی غلط را به کانال‌های ارتباطی بین PMU و تخمین گر دارد. تحت حملات FDI، اندازه‌گیری‌های دریافت شده توسط تخمین گر به صورت

$$z^a(k) = Hx^a(k) + a(k) + v(k) \quad (18)$$

است که $x^a(k)$ حالت سیستم تحت حمله‌ی FDI و $a(k) \in \mathbb{R}^m$ نشان‌دهنده داده‌ی غلط تزریق شده توسط مهاجم در لحظه k است. بردار حمله به صورت $a(k) = B_a a^0(k)$ تعریف می‌شود که ماتریس تزریق داده $B_a = \text{diag}\{\gamma_1, \dots, \gamma_m\}$ نشان می‌دهد کدام کانال ارتباطی توسط مهاجم به خطر افتاده است. اگر $\gamma_\tau = 1$ مهاجم توانایی تزریق داده‌ی غلط به کانال ارتباطی τ ام را دارد و در غیر این صورت $\gamma_\tau = 0$ است.

نمایش داده می‌شود که $z(k) \in \mathbb{R}^m$ خروجی اندازه‌گیری شده، $v(k) \in \mathbb{R}^m$ نویز اندازه‌گیری گوسی با میانگین صفر و ماتریس کوواریانس $R(k)$ و $m = 2(M + N_1 + N_2 + \dots + N_l)$ است.

به طور معمول زاویه و اندازه فازور ولتاژها به طور جداگانه‌ای به عنوان متغیرهای حالت در نظر گرفته می‌شود. در این مقاله بخش حقیقی و موهومی ولتاژ باس‌ها را به عنوان متغیرهای حالت معرفی کرده ایم که منجر به خطی شدن مدل اندازه‌گیری PMU می‌شود [۱۹، ۱۸]. همچنین فرض شده است که جفت ماتریس‌های (A, B) و (H) به ترتیب کنترل پذیر و مشاهده پذیر هستند.

۲-۲- تخمین گر حالت فیلتر کالمن

فیلتر کالمن برای تخمین متغیرهای حالت سیستم و مقایسه آن با مقادیر اندازه‌گیری شده توسط PMU به کار برده می‌شود. با توجه به مدل اندازه‌گیری (۴)، از فیلتر کالمن گسسته به دلیل سرعت همگرایی خوب و سهولت پیاده‌سازی استفاده می‌شود [۲۰، ۲۱].

در الگوریتم فیلتر کالمن، فرض می‌شود که در (۱) ماتریس‌های $A = I$ و $B = 0$ ورودی کنترلی سیستم، k در فرمول بندی تأثیری ندارد، صرف نظر می‌شود. نویز در الگوریتم فیلتر کالمن گسسته به صورت

$$P(v) \sim N(0, R(k)) \quad (5)$$

$$P(\omega) \sim N(0, W(k))$$

توصیف می‌شود؛ به عبارتی نویز گوسی با میانگین صفر است که $R(k)$ و $W(k)$ به ترتیب ماتریس‌های کوواریانس نویز اندازه‌گیری و نویز فرآیند هستند [۲۱]. فیلتر کالمن شامل دو بخش به روزرسانی زمان یا پیش‌بینی و به روزرسانی اندازه‌گیری یا تخمین است. اگر حالت واقعی، حالت پیش‌بینی شده و حالت تخمین زده شده در لحظه $k+1$ به ترتیب به صورت $x(k+1)$ ، $\tilde{x}(k+1)$ و $\hat{x}(k+1)$ تعریف شود، خطاها به صورت

$$\tilde{e}(k+1) \triangleq x(k+1) - \tilde{x}(k+1) \quad (6)$$

$$e(k+1) \triangleq x(k+1) - \hat{x}(k+1) \quad (7)$$

تعریف می‌شوند و ماتریس کوواریانس خطای پیش‌بینی به صورت

$$\bar{P}(k+1) = \mathbb{E}(\tilde{e}(k+1)\tilde{e}^T(k+1)) \quad (8)$$

و نیز ماتریس کوواریانس خطای تخمین به صورت

$$P(k+1) = \mathbb{E}(e(k+1)e^T(k+1)) \quad (9)$$

به دست می‌آیند که $\mathbb{E}(\cdot)$ امید ریاضی خطاها است.

در الگوریتم فیلتر کالمن حالت تخمین زده شده با اجرای پی‌درپی مراحل زیر به دست می‌آید:

۱- به روزرسانی زمان/پیش‌بینی:

$$\tilde{x}(k+1) = \hat{x}(k) \quad (10)$$

$$\bar{P}(k+1) = P(k) + W(k) \quad (11)$$

۲- به روزرسانی اندازه‌گیری/تخمین:

اگر دو شرط (۲۵) و (۲۶) هم‌زمان برقرار نباشد، در این صورت شبکه‌ی برق تحت حمله "امن" نامیده می‌شود.

مدل حمله‌ی FDI در سیستم قدرت مبتنی بر PMU ارائه شد. هدف مهاجم از ارسال توالی حمله به کانال‌های ارتباطی افزایش اختلاف تخمین حالت $\Delta \hat{x}(k)$ به سمت بی‌نهایت است، بدون آنکه هشدار توسط آشکارساز χ^2 صادر شود. به عبارت دیگر شبکه‌ی برق بدون آنکه توسط آشکارسازهای متداول تشخیص داده شود، ناپایدار می‌شود. در ادامه به روش حل مسئله پرداخته شده است.

۳- تشخیص حملات FDI

آشکارسازها به منظور تشخیص خطا^{۱۱} یا تشخیص حمله‌ی سایبری مورد استفاده قرار می‌گیرند. حملات سایبری نیز انواع گوناگونی دارند. تشخیص خطا در اندازه‌گیری، خرابی اندازه‌گیرها، خطا در خطوط مخابراتی و همچنین بسیاری از حملات سایبری را می‌توان با تحلیل باقی‌مانده^{۱۲} انجام داد. اگر خطاهای اندازه‌گیری مستقل از یکدیگر و با توزیع نرمال باشند، باقی‌مانده تخمین از توزیع χ^2 پیروی می‌کند. برای تشخیص خطا یا حمله از طریق برنامه تشخیص داده‌های نادرست^{۱۳}، باقی‌مانده با مقدار آستانه محاسبه شده‌ای مقایسه می‌شود. به این ترتیب آشکارساز قدرتمند χ^2 در بسیاری از موارد موفق عمل می‌کند و حتی نتیجه بهتری از نظر عدم اعلام آلام اشتباه نسبت به سایر آشکارسازها دارد [۱۴].

با این حال حمله‌ی FDI یک حمله‌ی سایبری پیشرفته و هوشمند است که در آن باتوجه به اطلاعاتی که مهاجم از توپولوژی شبکه، پارامترهای الکتریکی و پارامترهای کنترلی در اختیار دارد حمله‌ی تزریق داده غلط را به گونه‌ای طراحی و اجرا می‌کند که آشکارسازهای آماری از جمله آشکارساز χ^2 توانایی تشخیص این حمله را ندارند. به همین دلیل استفاده از آشکارساز فاصله اقلیدسی پیشنهاد شده است [۱۶].

به این ترتیب، هنوز هم شناسایی آسیب‌پذیری سیستم در مسائل تخمین حالت موجود، توسعه روش‌های تشخیص حمله و همچنین بررسی امنیت سایبری سیستم‌ها مهم و چالش‌برانگیز است.

۳-۱- آشکارساز χ^2

آشکارساز χ^2 یک انتخاب معمول به منظور شناسایی کارکرد غیرطبیعی سیستم قدرت است [۱۴]. در این مطالعه نیز ابتدا عمل‌کرد این آشکارساز را در سیستم مورد مطالعه قرار می‌دهیم. آشکارساز χ^2 مقدار تابع

$$g(k) = r^T(k)(HPH^T + R)^{-1}r(k) \quad (27)$$

را در لحظه k محاسبه می‌کند که P کوواریانس خطای ماندگار است. سپس $g(k)$ با آستانه تعیین شده α مقایسه می‌شود، اگر $g(k) > \alpha$ آنگاه هشدار صادر خواهد شد.

شبکه‌ی برق تحت حملات FDI در نظر گرفته شده است. همان‌گونه که گفته شده برای آنکه سیستم نسبت به این حملات ناامن باشد

همچنین $B_a = 0$ به معنای این است که حمله‌ی FDI بر هیچ کانال ارتباطی صورت نگرفته است و در غیر این صورت مهاجم توانایی تزریق داده‌ی غلط به تمامی $(B_a = I_m)$ یا بخشی $(B_a \neq I_m)$ از کانال‌های ارتباطی را دارد.

باتوجه به اندازه‌گیری‌های در معرض خطر $z^a(k)$ ، براساس تخمین گر (۱۶)، تخمین حالت دینامیکی به صورت

$$\begin{cases} x^a(k+1) = Ax^a(k) + \omega(k) \\ \hat{x}^a(k+1) = A\hat{x}^a(k) + Kr^a(k+1) \\ r^a(k+1) = z^a(k+1) - HA\hat{x}^a(k) \end{cases} \quad (19)$$

خواهد بود که $\hat{x}^a(k+1)$ و $r^a(k+1)$ به ترتیب حالت سیستم، تخمین حالت و باقی‌مانده تخمین در لحظه $k+1$ با استفاده از اندازه‌گیری‌های به خطر افتاده (۱۸) هستند.

خطای تخمین به صورت $e^a(k) \triangleq x^a(k) - \hat{x}^a(k)$ تعریف می‌شود و سپس دینامیک $e^a(k)$ به صورت

$$e^a(k+1) = Ae^a(k) - Kr^a(k+1) + \omega(k) \quad (20)$$

به دست می‌آید. با در نظر گرفتن اثر حملات FDI بر شبکه‌ی برق، اختلاف‌های سیستم (۱۹) و (۱۶) به صورت

$$\begin{aligned} \Delta x(k) &\triangleq x^a(k) - x(k), \quad \Delta \hat{x}(k) \triangleq \hat{x}^a(k) - \hat{x}(k) \\ \Delta r(k) &\triangleq r^a(k) - r(k), \quad \Delta e(k) \triangleq e^a(k) - e(k) \end{aligned}$$

تعریف می‌شوند؛ که $\Delta x(k)$ ، $\Delta \hat{x}(k)$ و $\Delta r(k)$ به ترتیب اختلاف حالت، اختلاف تخمین، اختلاف باقی‌مانده و اختلاف خطا است. دینامیک‌های $\Delta \hat{x}(k+1)$ ، $\Delta x(k+1)$ و $\Delta r(k+1)$ به صورت

$$\begin{aligned} \Delta \hat{x}(k+1) &= A\Delta \hat{x}(k) + K\Delta r(k+1) \\ &= (I - KH)A\Delta \hat{x}(k) + Ka(k+1) \end{aligned} \quad (21)$$

$$\Delta e(k+1) = A\Delta e(k) - K\Delta r(k+1) \quad (22)$$

$$\begin{aligned} \Delta r(k+1) &= HA\Delta e(k) + a(k+1) \\ &= -HA\Delta \hat{x}(k) + a(k+1) \end{aligned} \quad (23)$$

به دست می‌آیند. همچنین $\Delta \hat{x}(0) = \hat{x}^a(0) - \hat{x}(0) = 0$ است.

حملات تولید شده $a(k)$ از الگوریتم جدید ارائه شده در [۲۴] و معادله

$$a(k+1) = HA\Delta \hat{x}(k) + \sigma(k+1)\mathcal{M}I_m^\xi \quad (24)$$

به دست می‌آید؛ که $\sigma(k+1) = \pm \sigma$ و $\mathcal{M} \in (0,1)$ ، یک عدد مثبت، I_m ماتریس همانی با ابعاد $m \times m$ و I_m^ξ نشان‌دهنده ستون ξ ام از I_m که $\xi \in \{1, \dots, m\}$ است.

برای توصیف مخفی‌ماندن چنین حملاتی تعریف زیر را در نظر می‌گیریم:

تعریف ۱: [۲۴] سیستم (۱) با تخمین گر (۱۶) "ناامن" نامیده می‌شود اگر توالی حمله $a(k)$ وجود داشته، به طوری که

$$\lim_{k \rightarrow \infty} \|\Delta \hat{x}(k)\| = \infty \quad (25)$$

و

$$\|\Delta r(k)\| \leq \mathcal{M} \quad (26)$$

$\mathcal{M}$ عددی مثبت و به اندازه کافی کوچک در نظر گرفته می‌شود. شرایط (۲۵) و (۲۶) باید هر دو برقرار باشد.

بر اندازه ولتاژ بیشتر از زاویه فاز ولتاژ است [۱۷]، حملات سایبری بر بخش حقیقی ولتاژ تأثیرگذاری بیش‌تری دارند. پس بدون ازدست‌رفتن کلیت مسئله برای کاهش حجم محاسبات می‌توان تنها از بخش حقیقی اندازه‌گیری‌های انجام‌شده و حالات تخمین‌زده‌شده استفاده کرد؛ بنابراین تابع آشکارساز فاصله اقلیدسی به‌صورت

$$d(p_\ell(k), q_\ell(k)) = \sqrt{\sum_{t=1}^N (\hat{x}_{r,\ell}^a(k) - x_{r,\ell}^a(k))^2} \quad (30)$$

در لحظه k محاسبه می‌شود که $\hat{x}_{r,\ell}^a(k)$ بخش حقیقی ولتاژ تخمین‌زده‌شده و $x_{r,\ell}^a(k)$ بخش حقیقی ولتاژ اندازه‌گیری‌شده تحت حمله‌ی سایبری است. با توجه به تعریف ۱ بخش ۲-۳، در صورتی که سیستم تحت حملات ناامن شود، با برقرارساختن شرایط

$$\lim_{k \rightarrow \infty} \|\Delta \hat{x}(k)\| = \infty \quad (31)$$

$$\lim_{k \rightarrow \infty} \|d(p_\ell(k), q_\ell(k))\| = \infty \quad (32)$$

و به‌طور هم‌زمان می‌توان به تشخیص حمله‌ی FDI در شبکه پرداخت. آشکارساز فاصله اقلیدسی با محاسبه اختلاف داده‌های مشاهده‌شده و داده‌های تخمین‌زده‌شده به تشخیص حملات می‌پردازد؛ بنابراین، می‌توانیم حملاتی را که داده‌های اندازه‌گیری PMU دست‌کاری‌شده یا تزریق داده غلط صورت می‌گیرد، با روش مذکور تشخیص داد.

شکل ۳ ساختار روش پیشنهادی تشخیص حمله‌ی FDI را نشان می‌دهد. در این پژوهش مدل سیستم قدرت و مدل اندازه‌گیر با روابط (۱) و (۴) بیان می‌شود. بخش حقیقی و موهومی ولتاژ باس‌ها به‌عنوان متغیرهای حالت توسط اندازه‌گیر PMU اندازه‌گیری شده و این مقادیر برای تخمین حالت دینامیکی توسط خطوط ارتباطی به تخمین گر کالمن ارسال می‌شوند. اگر مهاجم توانایی طراحی حمله‌ی سایبری FDI موفق و تزریق داده‌ی غلط طبق رابطه‌ی (۲۴) را به کانال‌های ارتباطی بین PMU و تخمین گر داشته‌باشد، امنیت سیستم قدرت طبق تعریف ۱ به خطر می‌افتد. در این صورت تخمین حالت دینامیکی با استفاده فیلتر کالمن و مطابق (۱۹) انجام می‌گیرد. تشخیص حمله‌ی FDI طبق تعریف ۱ و رابطه‌ی (۲۷) توسط آشکارساز χ^2 امکان‌پذیر نیست؛ بنابراین تشخیص حمله موردنظر با آشکارساز فاصله اقلیدسی و با استفاده از بخش حقیقی اندازه‌گیری‌های انجام‌شده و حالات تخمین‌زده‌شده مطابق رابطه (۳۰) انجام می‌شود.

۴- نتایج شبیه‌سازی

در این بخش روش ارائه‌شده، بر سیستم استاندارد IEEE مورد ارزیابی قرار گرفته است. شبیه‌سازی‌ها با نرم‌افزار MATLAB و بسته نرم‌افزاری MATPOWER انجام شده‌است [۲۶]. سیستم ۱۴ باس IEEE با مدل (۱) و پارامترهای $A = \text{diag}_{28}\{0.98\}$ ، $B = \text{diag}_{28}\{0.02\}$ و $W(k) = \text{diag}_{28}\{0.1^2\}$ است. u ، ولتاژ نامی در حالت نرمال u ، در

باید $\|\Delta r(k)\| \leq \mathcal{M}$ باشد. در این صورت وقتی $\|\Delta r(k)\|$ در عبارت $\|r^a(k)\| \leq \|\Delta r(k)\| + \|r(k)\|$ در تمام لحظات به‌اندازه کافی کوچک باشد، آن‌گاه آشکارساز نمی‌تواند به‌احتمال زیاد بین $r(k)$ و $r^a(k)$ تفاوتی قائل شود. به این ترتیب، برای ایجاد حمله، مهاجم با روانه کردن چند حمله‌ی FDI باید از ایجاد یک تغییر بزرگ در اختلاف باقی‌مانده تخمین $\Delta r(k)$ جلوگیری کند [۲۴]. فرض کرده‌شده که $\mathcal{M}$ از قبل توسط مهاجم مشخص شده‌است. از طرفی مهاجم باید توالی حمله را به گونه‌ای طراحی کند که $\lim_{k \rightarrow \infty} \Delta \hat{x}(k) = \infty$ شود.

با توجه به رابطه (۲۷) و وابستگی آشکارساز χ^2 به بردار باقی‌مانده تخمین، شرایطی محتمل است که تحت آن توالی حمله‌ی FDI در سیستم وجود دارد ولی توسط آشکارساز χ^2 غیرقابل کشف باقی می‌ماند. برای رفع این نقص و حل این مسئله آشکارساز فاصله اقلیدسی را معرفی شده‌است.

۳-۲- آشکارساز فاصله اقلیدسی

اگرچه آشکارساز χ^2 به خوبی تحمل نویز را دارد و در بسیاری از موارد کارساز است [۱۴] ولی ممکن است قادر به تشخیص حمله‌ی تزریق داده‌ی غلط نباشد؛ بنابراین، آشکارساز فاصله اقلیدسی را معرفی می‌کنیم.

فاصله بین دوتقطه در فضای اقلیدسی به‌صورت

$$d(p, q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \dots + (p_n - q_n)^2} \quad (28)$$

محاسبه می‌شود که p_ℓ مقادیر تخمین‌زده‌شده، q_ℓ مقادیر اندازه‌گیری‌شده حالات سیستم و $\ell = (1, 2, \dots, N)$ است. در هر مرحله تخمین گر در مرکز کنترل، بردار تخمین حالت $\hat{x}_\ell(k) = p_\ell(k)$ و بردار اندازه‌گیری حالات سیستم $q_\ell(k) = x_\ell(k)$ را پردازش می‌کند. سپس آشکارساز فاصله اقلیدسی این مقادیر را دریافت کرده و در صورت اختلاف داده‌ها بیشتر از مقدار آستانه τ ، آشکارساز هشدار را صادر می‌کند که به معنی حمله‌ی صورت گرفته به داده‌های اندازه‌گیری است.

مقدار آستانه τ براساس داده‌های پیشین تنظیم شده و برای به حداقل رساندن نویز، آستانه را در 3σ (انحراف معیار) تنظیم شده‌است. تنظیم آستانه در 3σ می‌تواند نویز را تا 99.7% فیلتر کند [۱۷، ۲۵].

چون اندازه‌گیری‌ها از سراسر سیستم و با چندین PMU انجام می‌شود، حتی اگر مهاجم به‌طور جزئی اندازه‌گیری‌های هر PMU را تغییر دهد، مجموع این اندازه‌گیری‌ها اختلاف بزرگی را نشان خواهد داد. اگر $d(p, q)$ ناگهان تغییر کند به معنای وجود بردار تزریق شده‌است.

با توجه به (۲۸) تابع آشکارساز فاصله اقلیدسی را به‌صورت

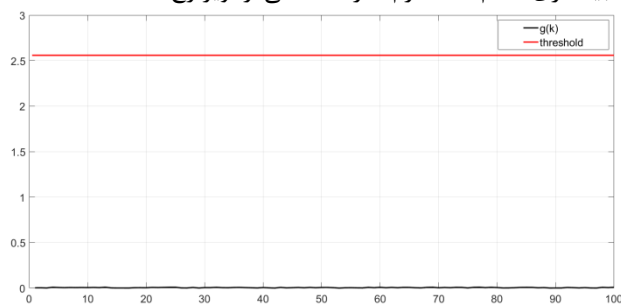
$$d(p_\ell(k), q_\ell(k)) \triangleq d(\hat{x}_{r,\ell}^a(k), x_{r,\ell}^a(k)) = \sqrt{\sum_{t=1}^N ((\hat{x}_{r,\ell}^a(k) - x_{r,\ell}^a(k))^2 + (\hat{x}_{i,\ell}^a(k) - x_{i,\ell}^a(k))^2)} \quad (29)$$

در لحظه k تعریف شده‌است. از آنجایی که متغیرهای حالت به دو بخش حقیقی و موهومی ولتاژ باس‌ها تقسیم می‌شوند و از طرفی تأثیر حملات

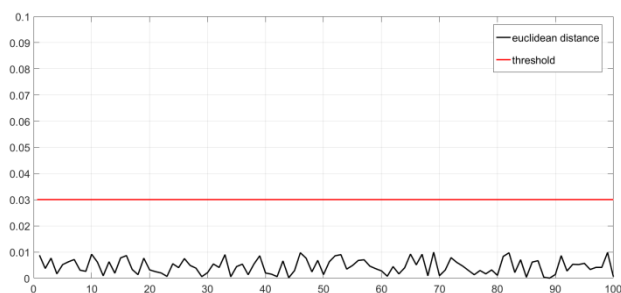
فرض می‌شود مهاجم توانایی تزریق داده‌ی غلط به تمامی کانال ارتباطی $(B_a = I_m)$ را دارد و توالی حمله $a(k)$ تولیدشده، منجر به $(A) \geq 1$ می‌شود [۲۴].

به‌طور کلی احتمال تشخیص حمله، در هر دو آشکارساز، وابسته به مقدار آستانه است. در آشکارساز χ^2 آستانه از جدول χ^2 و در آشکارساز فاصله اقلیدسی از انحراف معیار توزیع گوسی به‌دست می‌آید. در این بررسی مقدار آستانه هر دو آشکارساز به‌گونه‌ای تنظیم می‌شود که ۹۹٪ از نویز را فیلتر کند. پس احتمال هشدار آشکارسازها به‌دلیل نویز، کمتر از ۱٪ است.

شکل ۵ نتایج شبیه‌سازی با استفاده از آشکارساز χ^2 را در حالتی که حمله‌ای صورت‌نگرفته نشان می‌دهد. همان‌طور که قبلاً گفته شد هم‌گرایی فیلتر کالمن با انتخاب مناسب بهره‌ی کالمن تضمین‌شده است؛ بنابراین باتوجه به عدم وجود حمله مقدار $g(k)$ از (۲۷) فقط ناشی از نویز تصادفی اندازه‌گیری است. این مقدار هرچند به‌دلیل تصادفی بودن نویز تغییر می‌کند ولی همواره نزدیک صفر و کمتر از مقدار آستانه است. همچنین شکل ۷ نتایج شبیه‌سازی با استفاده از آشکارساز فاصله اقلیدسی را در حالتی که حمله صورت‌نگرفته است نشان می‌دهد. همان‌گونه که در این شکل نیز مشاهده می‌شود مقدار $d(k)$ که از رابطه (۲۹) محاسبه می‌شود بسیار کمتر از مقدار آستانه است. درواقع می‌توان از شکل‌های ۶ و ۷ نتیجه گرفت که با مقادیر آستانه انتخاب‌شده، در شبیه‌سازی انجام‌شده آلام نادرست ناشی از نویز رخ نداده است.



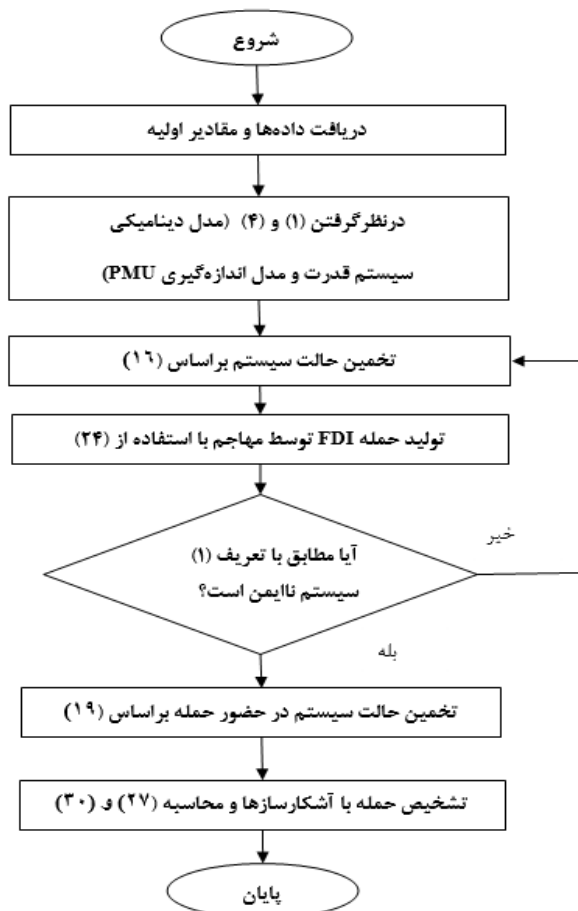
شکل ۵: عمل کرد آشکارساز χ^2 بدون حضور حمله‌ی FDI



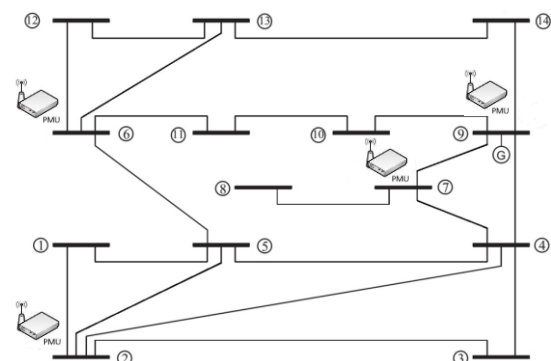
شکل ۶: عمل کرد آشکارساز فاصله اقلیدسی بدون حضور حمله‌ی FDI

شکل ۷ رفتار آشکارساز χ^2 تحت حمله‌ی FDI را نشان می‌دهد. در شبیه‌سازی انجام‌شده، حمله‌ی FDI از گام ۲۰ اعمال‌شده و در گام ۳۰ خاتمه می‌یابد. طبق تعریف ۱ تخمین‌ها با مقادیر اندازه‌گیری‌شده تطابق ندارند. به عبارت دیگر اختلاف تخمین حالت بسیار بزرگ خواهد بود. این در حالی است که مطابق شکل ۷ $g(k)$ که از اختلاف

جدول ۱ پیوست آورده شده است. طبق فرض، ولتاژ اولیه تمامی باس‌های $\ell = 1, 2, \dots, 14$ برابر $x_{r,\ell}(0) = 1 pu$ و $x_{i,\ell}(0) = 0 pu$ و ماتریس کوواریانس خطای تخمین حالت اولیه $P(0) = 10^{-4} I_{28}$ است. پیکربندی PMU ها در شکل ۴ نشان داده شده که بر اساس [۲۷، ۲۸]، سیستم اندازه‌گیری فقط از اندازه‌گیر PMU در باس‌های ۲، ۶، ۷ و ۹ استفاده کرده است. ماتریس کوواریانس نویز اندازه‌گیری PMU، $R(k) = diag_{38}(0.01^2)$ است. با توجه به ساختار انتخاب‌شده، سیستم قدرت کنترل‌پذیر و مشاهده‌پذیر است.



شکل ۳: روش تشخیص حمله‌ی FDI در سیستم قدرت



شکل ۴: سیستم ۱۴ باس IEEE و پیکربندی PMU ها [۲۷]

۵- نتیجه‌گیری

در این مقاله، روشی برای تشخیص حمله‌ی FDI در شبکه‌ی برق مبتنی بر PMU با استفاده از تخمین گر کالمن همراه با آشکارساز ارائه شده است. پس از حمله‌ی صورت گرفته آسیب پذیری سیستم قدرت مبتنی بر PMU مورد بررسی قرار گرفت. انتخاب حمله‌ی FDI همان طور که ملاحظه شد، به این دلیل است که اکثر آشکارسازهای متداول تشخیص خطا، مانند آشکارساز χ^2 در تشخیص این نوع حمله ناتوان هستند. نشان داده شد که روش به کاررفته مبتنی بر آشکارساز فاصله اقلیدسی در تشخیص حمله‌ی FDI کارساز است. در همین راستا آشکارساز فاصله اقلیدسی، برای تشخیص حمله‌ی FDI در سیستم استاندارد ۱۴ باسه IEEE مورد ارزیابی قرار گرفت. همان طور که از نتایج شبیه سازی مشاهده شد، روش ارائه شده در این پژوهش به نحوی است که آشکارساز فاصله اقلیدسی و فیلتر کالمن با محاسبه اختلاف داده‌های مشاهده شده از داده‌های تخمین زده شده در هر لحظه به تشخیص حملات می پردازند. می توان حملاتی که داده‌های اندازه گیری PMU را دست کاری کرده یا به تزریق داده غلط در سیستم قدرت مبتنی بر PMU می پردازد با روش مذکور تشخیص داد. همچنین بدون ازدست رفتن کلیت مسئله برای پایین آوردن حجم محاسبات و کاهش زمان عمل کرد می توان تنها از بخش حقیقی اندازه گیری های انجام شده و حالات تخمین زده شده استفاده کرد.

پیوست

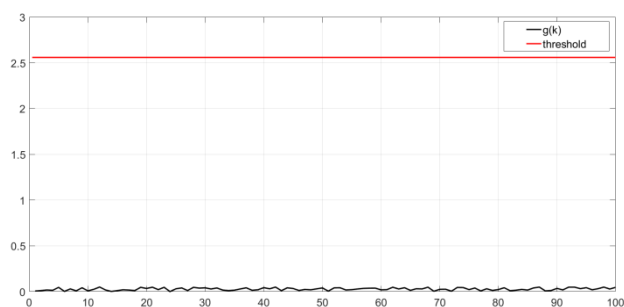
جدول ۱: ولتاژ نامی در حالت نرمال

بخش موهومی ولتاژ	بخش حقیقی ولتاژ	باس
۰	۱/۰۶۰۰	۱
۰/۰۹۴۳	۱/۰۳۶۸	۲
۰/۲۱۷۳	۰/۹۶۰۹	۳
۰/۱۸۲۱	۰/۹۸۵۸	۴
۰/۱۵۶۳	۰/۹۹۵۸	۵
۰/۲۶۹۴	۱/۰۰۱۶	۶
۰/۲۵۱۲	۱/۰۰۲۲	۷
۰/۲۶۴۳	۱/۰۲۷۰	۸
۰/۲۷۴۳	۰/۹۸۲۷	۹
۰/۲۷۴۴	۰/۹۷۶۹	۱۰
۰/۲۷۵۹	۰/۹۸۵۰	۱۱
۰/۲۷۵۹	۰/۹۸۰۶	۱۲
۰/۲۷۴۸	۰/۹۷۵۵	۱۳
۰/۲۸۱۲	۰/۹۵۵۲	۱۴

مراجع

- [۱] سعید ابازری، مجتبی برخوردار یزدی و عباس عرب دردری، «طراحی کنترل کننده مقاوم SVC مبتنی بر WAMS با در نظر گرفتن نامعینی

باقی مانده به دست می آید هرگز از مقدار آستانه تجاوز نکرده است. بنابراین می توان نتیجه گرفت که آشکارساز χ^2 نتوانسته حمله‌ی موردنظر را تشخیص دهد.

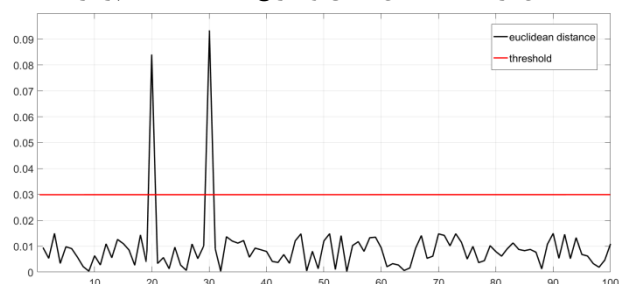


شکل ۷: عمل کرد آشکارساز χ^2 تحت حمله‌ی FDI

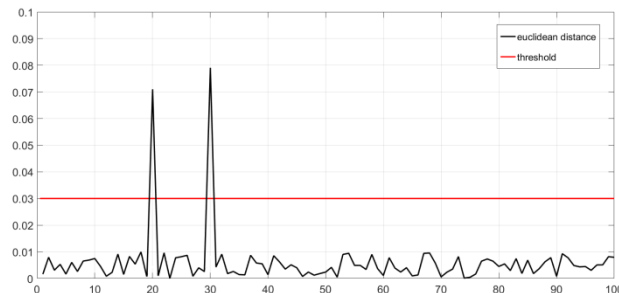
در شکل ۸ نشان داده شده است که آشکارساز فاصله اقلیدسی اختلاف فاصله بین مقادیر اندازه گیری و تخمین زده شده را در گام های ۲۰ و ۳۰ تشخیص می دهد. به عبارت دیگر، حمله‌ی FDI در گام ۲۰ توسط آشکارساز فاصله اقلیدسی قابل تشخیص است.

همان طور که در توضیحات روش پیشنهادی بیان شد می توان با استفاده از رابطه (۳۰)، فقط از بخش حقیقی داده های اندازه گیری شده و تخمین زده شده استفاده نمود و حمله‌ی FDI را تشخیص داد. در این صورت حجم محاسبات به نصف کاهش پیدا می کند. شکل ۹ عمل کرد آشکارساز اقلیدسی در حضور حمله، تنها با استفاده از بخش حقیقی داده های اندازه گیری و تخمینی را نشان می دهد.

در مجموع می توان مشاهده کرد که آشکارساز فاصله اقلیدسی طراحی شده با استفاده از نیمی از داده ها می تواند بدون کاسته شدن از کیفیت عمل کرد به تشخیص دقیق و سریع حمله‌ی FDI بپردازد.



شکل ۸: عمل کرد آشکارساز فاصله اقلیدسی تحت حمله‌ی FDI



شکل ۹: عمل کرد آشکارساز فاصله اقلیدسی تحت حمله‌ی FDI با

استفاده از بخش حقیقی داده ها

- [16] Y. Mo and B. Sinopoli, *False data injection attacks in cyber physical systems*. In First Workshop on Secure Control Systems, 2010.
- [17] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370-379, 2014.
- [18] X. Bian, X. R. Li, H. Chen, D. Gan, and J. Qiu, "Joint estimation of state and parameter with synchrophasors—Part I: State tracking," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1196-1208, 2011.
- [19] G. N. Korres and N. M. Manousakis, "State estimation and observability analysis for phasor measurement unit measured systems," *IET Generat., Transmiss. Distrib.*, vol. 6, no. 9, pp. 902-913, Sep. 2012.
- [20] J. Zhang, G. Welch, G. Bishop, and Z. Huang, "A two-stage Kalman filter approach for robust and real-time power system state estimation," *IEEE Trans. Sustainable Energy*, vol. 5, no. 2, pp. 629-636, Apr. 2014.
- [21] S. Sarri, L. Zanni, M. Popovic, J.-Y. Le Boudec, and M. Paolone, "Performance assessment of linear state estimators using synchrophasor measurements," *IEEE Trans. Sustain. Energy*, 2016.
- [22] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Journal of Basic Engineering*, vol. 82, pp. 35-45, 1960.
- [23] J. P. Hespanha, *Linear Systems Theory*. Princeton university press, 2009.
- [24] L. Hu, W. Zidong and N. Wasif, "Security analysis of stochastic networked control systems under false data injection attacks," *UKACC 1th International Conference on. IEEE*, 2016.
- [25] W. J. Dixon and F. J. Massey, "Introduction to statistical analysis," *McGraw-Hill New York*, 1969, vol. 344.
- [26] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12-19, Feb. 2011.
- [27] G. N. Korres and N. M. Manousakis, "State estimation and bad data processing for systems including PMU and SCADA measurements," *Electr. Power Syst. Res.*, vol. 81, no. 7, pp. 1514-1524, 2011.
- [۲۸] سهیل مرادی، رضا محمدی چبنلو و نوید تقی‌زادگان کلانتری، «مکان‌یابی بهینه واحدهای اندازه‌گیر فازوری برای مکان‌یابی خطا در شبکه قدرت با در نظر گرفتن باس‌های تزریق صفر و خروج تکی خطوط»، *مجله مهندسی برق*، دوره ۴۶، دانشگاه تبریز، ۱۳۹۵.
- [2] G. Liang, J. Zhao, F. Luo, S. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630-1638, 2017.
- [3] T. Chen, "Stuxnet, the real start of cyber warfare? [editor's note]," *IEEE Network*, vol. 24, no. 6, pp. 2-3, 2010.
- [4] 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. 13, 2011.
- [5] Z. Li, M. Shahidehpour and F. Aminifar, "Cybersecurity in Distributed Power Systems," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1367-1388, 2017.
- [6] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout implications for false data injection attacks," *IEEE Trans. Power Systems*, vol. 32, no. 4, pp. 3317-3318, 2017.
- [7] NCCIC/ICS-CERT, *Cyber-attack against Ukrainian critical infrastructure*, released 20 June 2016, <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>.
- [8] A. Anwar, A.N. Mahmood, and Z. Tari, "Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid," *Information Systems*, vol. 53, pp. 201-212, 2015.
- [9] T.T. Kim and H.V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326-333, 2011.
- [10] X. Liu, Z. Li and Z. Li, *Impacts of bad data on the PMU based line outage detection*. arXiv preprint arXiv:1502.04236, 2015, <http://arxiv.org/abs/1502.04236>.
- [11] Y. Guo, W. Wu, B. Zhang, and H. Sun, "An efficient state estimation algorithm considering zero injection constraints," *IEEE Transactions on Power Systems*, vol. 28, no.3, pp. 2651-2659, 2013.
- [12] M. Risso, A. J. Rubiales, and P. A. Lotito, "Hybrid method for power system state estimation," *IET Generation, Transmission & Distribution*, vol. 9, no.7, pp. 636-643, 2015.
- [13] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, 2012.
- [14] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in 2010 49th IEEE Conference on Decision and Control (CDC), pp. 5967-5972, 2010.
- [15] B. Brumback and M. Srinath, "A chi-square test for fault-detection in kalman filters," *IEEE Transactions on Automatic Control*, vol. 32, no. 6, pp. 552-554, 1987.

زیر نویس‌ها

⁸ Random Attack⁹ Euclidean Distance¹⁰ Energy Management System¹¹ Fault detection¹² Residual¹³ Bad Data Detection¹ Cyber-Physical System² Stuxnet³ False Data Injection⁴ Integrity Attack⁵ Denial Of Service⁶ Replay Attack⁷ Phasor Measurement Unit