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

بهنام همائی[۱]، دانشجو کارشناسی ارشد؛ سعید اباذری[۲]، دانشیار؛ مجتبی برخورداری 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 درنظرگرفتن اندازه‌گیری‌های انجام‌شده توسط واحد اندازه‌گیری فازور (PMU) و تخمین دینامیکی متغیرهای حالت سیستم توسط تخمین‌گر کالمن مورد بحث قرارگرفته است. حمله‌ی موردنظر به کانال‌های ارتباطی بین PMU و تخمین‌گر حالت صورت می‌گیرد. نشان داده شده است به‌دلیل ماهیت هوشمند حمله‌ی FDI طراحی‌شده، 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 به‌گونه‌ای طراحی کند که در چند PMU به‌طور جزئی تزریق داده غلط انجام شود، آشکارساز طراحی‌شده قادر خواهدبود این حمله را به‌سرعت تشخیص دهد. احتمال تشخیص نادرست به‌دلیل اثر نویز کمتر از ۱ درصد است. تأثیر حمله‌ی FDI بر تخمین حالت سیستم و کارایی روش موردمطالعه 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 Student [1]; Saeed Abazari, Associate Professor [2]; Mojtaba Barkhordari Yazdi, Assistant Professor [3]

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: ۱۳۹۷/۲/۱۵و ۱۳۹۷/۴/۲۳
تاریخ پذیرش مقاله: ۱۳۹۷/۴/۳۱
نام نویسنده مسئول: سعید اباذری
نشانی نویسنده مسئول: ایران - شهرکرد - بلوار رهبر - دانشگاه شهرکرد - دانشکده فنی و مهندسی.

۱- مقدمه

با پیشرفت سریع حس‌گرها، 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 منجربه 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 موردبحث 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 قابل‌انجام است. بااین‌حال دلیل تمرکز این مقاله بر حمله‌ی FDI این است که در این نوع حمله دست‌کاری حساب‌شده داده‌های سیستم اندازه‌گیری، منجربه 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 موردبحث قرارگرفته‌است. در [۸] به حفاظت از مجموعه اندازه‌گیری‌های اصلی و در [۹] حفاظت از سیستم قدرت براساس PMU[۷] پرداخته شده‌است. بااین‌حال نویسنده در [۱۰] بیان می‌کند که باوجود حفاظت مبتنی‌بر PMU، مهاجم قادر است به مجموعه اندازه‌گیری‌ها حمله کند و منجربه 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 وزن‌دار، به‌دلیل هم گرایی سریع و پیاده‌سازی آسان استفاده‌شده‌است. مراجع مختلفی مانند [۱۱، ۱۲] به بررسی امنیت سایبری سیستم تحت حمله‌ی FDI با روش‌های تخمین حالت استاتیکی می‌پردازد؛ درحالی‌که به‌دلیل 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 به‌کمک 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 این‌گونه داده‌ها، بردار اندازه‌گیری به‌طور قابل‌توجهی تغییر خواهدکرد [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) ارائه‌شده و سپس به مدل‌سازی حمله‌ی FDI بر روی سیستم قدرت پرداخته‌شده‌است. در بخش سوم نشان داده‌شده که حمله‌ی FDI در سیستم قدرت با ترکیب تخمین گر کالمن و آشکارساز χ^2 قابل‌تشخیص نیست. سپس روش ارائه‌شده 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 مشاهده‌شده از داده‌های تخمین زده‌شده در هرلحظه 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- باتوجه به مزایای استفاده از PMU و استفاده فزاینده از آن در شبکه های قدرت، از داده‌های حاصل از PMU برای تخمین حالت استفاده‌شده است. به‌این‌ترتیب تشخیص حمله FDI در این مقاله مبتنی‌بر مدل فرایند با درنظرگرفتن PMU است.

۲- الگوریتمی که برای تولید حمله FDI مطرح شده‌است مبتنی‌بر الگوریتم بهبودیافته‌ای‌است که در مرجع [۲۴] معرفی‌شده است. با این الگوریتم شرط ناامن‌شدن سیستم ساده‌تر می‌شود و به‌عبارتی تشخیص حمله دشوارتر خواهدشد. در این مقاله نشان‌داده شده‌است که آشکارساز فاصله اقلیدسی قادر به تشخیص این حمله است. براساس بررسی‌های انجام‌شده، این الگوریتم حمله تاکنون در شبکه‌های قدرت مورداستفاده قرار نگرفته‌است.

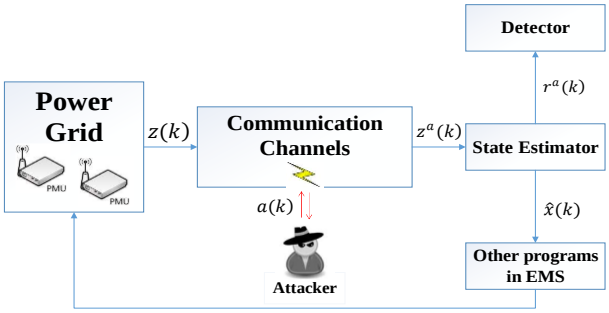
۳- در روش ارائه‌شده فقط نیمی از اطلاعات دریافتی از PMU برای تشخیص حمله مورداستفاده قرارمی‌گیرد و به‌این‌ترتیب بار محاسباتی کاهش‌یافته و سرعت تشخیص حمله افزایش می‌یابد.

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 استفاده‌شده‌است. حالت‌های تخمین‌زده‌شده به سیستم مدیریت انرژی[۱۰] (EMS) ارسال می‌شود تا برای اهدافی مانند مانیتورینگ و کنترل شبکه مورداستفاده قرار گیرد.

ساختار کلی تخمین حالت شبکه‌ی برق مبتنی‌بر PMU تحت حملات سایبری در شکل ۱ نشان داده‌شده‌است. در مسئله‌ی موردنظر، مهاجم با حمله‌ی سایبری از نوع FDI ازطریق خطوط ارتباطی بین شبکه برق و تخمین گر حالت به اندازه‌گیری‌های انجام‌شده توسط PMU داده‌ی غلط تزریق می‌کند. به‌این‌ترتیب با ایجاد مشکل در تخمین حالت عمل‌کرد طبیعی شبکه‌ی برق مختل می‌شود. هدف اصلی مسئله تشخیص دقیق و سریع حمله‌ی طراحی‌شده با بهره‌گیری از داده‌های دریافتی از فیلتر کالمن و واحدهای اندازه‌گیری فازوری است.

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



شکل ۱: تخمین حالت شبکه‌ی برق مبتنی‌بر PMU تحت حملات سایبری

۲-۱- شبکه‌ی برق بدون حضور حملات سایبری

در ادامه مدل شبکه‌ی برق در حالت کارکرد نرمال و بدون حضور حملات سایبری به‌همراه مدل اندازه‌گیری PMU توضیح داده‌خواهد شد. معادله دینامیکی

$$x(k+1) = Ax(k) + Bu + \omega(k) \qquad (۱)$$

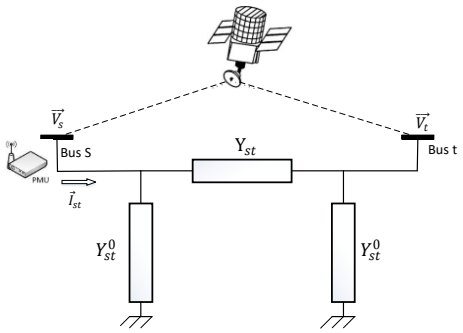
به عنوان مدل سیستم قدرت N باسه استفاده می‌شود که $x(k) \in \mathbb{R}^n$ حالت سیستم و بردار فازور ولتاژ تمامی باس‌ها، $u \in \mathbb{R}^n$ ولتاژ نامی، $\omega(k) \in \mathbb{R}^n$ نویز گوسی فرآیند با میانگین صفر و ماتریس کوواریانس $W(k)$، $n = 2N$، A ماتریس حالت و برای سادگی $B \triangleq I - A$ تعریف می‌شود.

در سیستم قدرت N باسه، حالت سیستم به‌صورت

$$x(k) = [x_{r,1}(k)\ x_{r,2}(k)\ \cdots\ x_{r,N}(k)\ x_{i,1}(k)\ x_{i,2}(k)\ \cdots\ x_{i,N}(k)]^T$$

نمایش داده می‌شود که $x_{r,\ell}(k)$ و $x_{i,\ell}(k)$ به‌ترتیب نشان‌دهنده بخش حقیقی و موهومی ولتاژ باس ℓام هستند.

PMU نه‌تنها فازور ولتاژ باس‌ها، بلکه جریان عبوری از خطوط متصل به این باس‌ها را نیز اندازه‌گیری می‌کند. با فرض استفاده از مدل π برای شاخه‌های شبکه، $Y_{st} \triangleq g_{st} + ib_{st}$ ادمیتانس شاخه سری و $Y_{st}{}^0 \triangleq g_{st}^0 + ib_{st}^0$ نصف ادمیتانس شاخه متصل به باس s و t در شکل۲ نشان داده‌شده‌است. m اندازه‌گیری و n حالت وجود دارند به‌طوری‌که، $m > n$ است.



شکل ۲: ولتاژ باس و جریان فازور در مدل π

باس‌های متصل‌شده به PMU ها با $s_1, s_2, \cdots, s_M$ مشخص می‌شوند. اندازه‌گیری‌های $z_{s_l} \in \mathbb{R}^{2(1+N_l)}$ از PMU ℓام مستقرشده در باس s_l به‌دست‌آمده که به‌صورت بردار

$$z_{sl} = \left[x_{r,s_l}\ x_{i,s_l}\ z_{r,t_1^{s_l}}\ z_{i,t_1^{s_l}}\ \cdots\ z_{r,t_{N_l}^{s_l}}\ z_{i,t_{N_l}^{s_l}}\right]^T \qquad (۲)$$

قابل‌نمایش است که x_{r,s_l} و $x_{,s_l}$ به‌ترتیب، قسمت‌های حقیقی و موهومی ولتاژ اندازه‌گیری‌شده باس s_l هستند. اندازه‌گیری‌های جریان خط متصل‌شده به دو باس s_l و $t_\eta^{s_l}$ به‌صورت

$$\begin{aligned} z_{r,t_\eta^{s_l}} &= x_{r,s_l}\, g^0_{s_l,t_\eta^{s_l}} - x_{i,s_l} b^0_{s_l,t_\eta^{s_l}} + \left(x_{r,s_l} - x_{r,t_\eta^{s_l}}\right) g_{s_l,t_\eta^{s_l}} \\ &\quad - \left(x_{i,s_l} - x_{i,t_\eta^{s_l}}\right) b_{s_l,t_\eta^{s_l}} \\ z_{i,t_\eta^{s_l}} &= x_{i,s_l}\, g^0_{s_l,t_\eta^{s_l}} + x_{r,s_l} b^0_{s_l,t_\eta^{s_l}} + \left(x_{i,s_l} - x_{i,t_\eta^{s_l}}\right) g_{s_l,t_\eta^{s_l}} \\ &\quad + \left(x_{r,s_l} - x_{r,t_\eta^{s_l}}\right) b_{s_l,t_\eta^{s_l}} \end{aligned} \qquad (۳)$$

به‌دست 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 گرفته‌شده، اندازه‌گیری‌های PMU به شکل

$$z(k) = Hx(k) + v(k) \qquad (۴)$$

نمایش داده‌می‌شود که $z(k) \in \mathbb{R}^m$ خروجی اندازه‌گیری‌شده، $v(k) \in \mathbb{R}^m$ نویز اندازه‌گیری گوسی با میانگین صفر و ماتریس کوواریانس $R(k)$ و $m = 2(\mathrm{M} + \mathrm{N}_1 + \mathrm{N}_2 + \cdots + \mathrm{N}_l)$ است.

به‌طورمعمول زاویه و اندازه فازور ولتاژها به‌طور جداگانه‌ای به‌عنوان متغیرهای حالت در نظر گرفته می‌شود. در این مقاله بخش حقیقی و موهومی ولتاژ باس‌ها را به‌عنوان متغیرهای حالت معرفی کرده‌ایم که منجربه خطی‌شدن مدل اندازه‌گیری PMU می‌شود [۱۸، ۱۹]. همچنین فرض شده‌است که جفت ماتریس‌های (A,B) (H) به‌ترتیب کنترل‌پذیر و مشاهده‌پذیر هستند.

۲-۲- تخمین گر حالت فیلتر کالمن

فیلتر کالمن برای تخمین متغیرهای حالت سیستم و مقایسه آن با مقادیر اندازه‌گیری‌شده توسط PMU به‌کاربرده می‌شود. باتوجه به مدل اندازه‌گیری (۴)، از فیلتر کالمن گسسته به‌دلیل سرعت همگرایی خوب و سهولت پیاده‌سازی استفاده‌می‌شود [۲۰، ۲۱].

در الگوریتم فیلتر کالمن، فرض می‌شود که در (۱) ماتریس‌های $A = I$ و $B = 0$ ورودی کنترلی سیستم، ک در فرمول‌بندی تأثیری ندارد، صرف‌نظر می‌شود. نویز در الگوریتم فیلتر کالمن گسسته به‌صورت

$$\begin{matrix} P(v) \sim N\big(0, R(k)\big) \\ P(\omega) \sim N\big(0, W(k)\big) \end{matrix} \qquad (۵)$$

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

$$\tilde{e}(k+1) \triangleq x(k+1) - \tilde{x}(k+1) \qquad (۶)$$

$$e(k+1) \triangleq x(k+1) - \hat{x}(k+1) \qquad (۷)$$

تعریف می‌شوند و ماتریس کوواریانس خطای پیش‌بینی به‌صورت

$$\tilde{P}(k+1) = \mathbb{E}\big(\tilde{e}(k+1)\tilde{e}^T(k+1)\big) \qquad (۸)$$

و نیز ماتریس کوواریانس خطای تخمین به‌صورت

$$P(k+1) = \mathbb{E}\big(e(k+1)e^T(k+1)\big) \qquad (۹)$$

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

در الگوریتم فیلتر کالمن حالت تخمین‌زده‌شده با اجرای پی‌درپی مراحل زیر به دست می‌آید:

۱- به‌روزرسانی زمان/ پیش‌بینی:

$$\tilde{x}(k+1) = \hat{x}(k) \qquad (۱۰)$$

$$\tilde{P}(k+1) = P(k) + W(k) \qquad (۱۱)$$

۲- به‌روزرسانی اندازه‌گیری/ تخمین:

$$K(k+1) = \tilde{P}(k+1)H^T\left(H\tilde{P}(k+1)H^T + R(k+1)\right)^{-1} \qquad (۱۲)$$

$$\hat{x}(k+1) = \tilde{x}(k+1) + K(k+1)\big(z(k+1) - H\tilde{x}(k+1)\big) \qquad (۱۳)$$

$$P(k+1) = (I - K(k+1)H)\tilde{P}(k+1) \qquad (۱۴)$$

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

$$\begin{matrix} P \triangleq \lim_{k\to\infty} \tilde{P}(k+1) \\ K = PH^T(HPH^T + R)^{-1} \end{matrix} \qquad (۱۵)$$

به دست می‌آید؛ بنابراین روابط ساده تخمین گر به‌صورت

$$\begin{cases} x(k+1) = Ax(k) + \omega(k) \\ \hat{x}(k+1) = A\hat{x}(k) + Kr(k+1) \\ r(k+1) = z(k+1) - HA\hat{x}(k) \end{cases} \qquad (۱۶)$$

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

از خطای تخمین e(k)، خطای تخمین دینامیکی

$$\begin{matrix} e(k+1) = Ae(k) - Kr(k+1) + \omega(k) \\ = (I - KH)\big(Ae(k) + \omega(k)\big) - Kv(k+1) \end{matrix} \qquad (۱۷)$$

به‌دست 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.

همان‌طورکه 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 ایجادشده توسط مهاجمان هستند. در قسمت بعد، حمله‌ی سایبری FDI معرفی شده‌است که می‌تواند امنیت سیستم قدرت را تحت‌تأثیر قرار دهد.

۲-۳- حمله‌ی تزریق داده‌ی غلط

در این بخش، مدل حمله‌یFDI معرفی شده‌است و پس‌ازآن 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 شده‌است [۱۶، ۲۴]. همچنین مهاجم توانایی تزریق داده‌ی غلط را به کانال‌های ارتباطی بین PMU و تخمین‌گر دارد. تحت حملات FDI، اندازه‌گیری‌های دریافت‌شده توسط تخمین‌گر به‌صورت

$$z^a(k) = Hx^a(k) + a(k) + v(k) \qquad (۱۸)$$

است که $x^a(k)$ حالت سیستم تحت حمله‌ی FDI و $a(k) \in \mathbb{R}^m$ نشان‌دهنده داده‌ی غلط تزریق‌شده توسط مهاجم در لحظه k است. بردار حمله به‌صورت $a(k) = B_a a^0(k)$ تعریف می‌شود که ماتریس تزریق داده $B_a = diag\{\gamma_1, \cdots, \gamma_m\}$ نشان می‌دهد کدام کانال ارتباطی توسط مهاجم به خطر افتاده‌است. اگر $\gamma_\tau = 1$ مهاجم توانایی تزریق داده‌ی غلط به کانال ارتباطی τام را دارد و در غیراین‌صورت $\gamma_\tau = 0$ است.

همچنین $B_a = 0$ به معنای این است که حمله‌ی FDI بر هیچ کانال ارتباطی صورت نگرفته‌است و در غیراین‌صورت مهاجم توانایی تزریق داده‌ی غلط به‌تمامی ($B_a = I_m$) 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 به‌صورت

$$\begin{cases} x^a(k+1) = Ax^a(k) + \omega(k) \\ \hat{x}^a(k+1) = A\hat{x}^a(k) + Kr^a(k+1) \\ r^a(k+1) = z^a(k+1) - HA\hat{x}^a(k) \end{cases} \quad (۱۹)$$

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

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

$$e^a(k+1) = Ae^a(k) - Kr^a(k+1) + \omega(k) \quad (۲۰)$$

به دست می‌آید. با درنظرگرفتن اثر حملات FDI بر شبکه‌ی برق، اختلاف‌های سیستم (۱۹) و (۱۶) به‌صورت

$$\Delta x(k) \triangleq x^a(k) - x(k),\ \Delta\hat{x}(k) \triangleq \hat{x}^a(k) - \hat{x}(k)$$
$$\Delta r(k) \triangleq r^a(k) - r(k),\ \Delta e(k) \triangleq e^a(k) - e(k)$$

تعریف می‌شوند؛ که $\Delta x(\mathrm{k})$ $\Delta\hat{x}(\mathrm{k})$ $\Delta r(\mathrm{k})$ و $\Delta e(\mathrm{k})$ به‌ترتیب اختلاف حالت، اختلاف تخمین، اختلاف باقی‌مانده و اختلاف خطا است. دینامیک‌های $\Delta\hat{x}(\mathrm{k}+1)$ ، $\Delta(\mathrm{k}+1)$ و $\Delta r(\mathrm{k}+1)$ به‌صورت

$$\begin{aligned} \Delta\hat{x}(k+1) &= A\Delta\hat{x}(k) + K\Delta r(k+1) \\ &= (I - KH)A\Delta\hat{x}(k) + Ka(k+1) \end{aligned} \quad (۲۱)$$

$$\Delta e(k+1) = A\Delta e(k) - K\Delta r(k+1) \quad (۲۲)$$

$$\begin{aligned} \Delta r(k+1) &= HA\Delta e(k) + a(k+1) \\ &= -HA\Delta\hat{x}(k) + a(k+1) \end{aligned} \quad (۲۳)$$

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

حملات تولیدشده $a(k)$ از الگوریتم جدید ارائه‌شده در [۲۴] و معادله

$$a(k+1) = HA\Delta\hat{x}(k) + \sigma(k+1)\mathcal{M}I_m^{\xi} \quad (۲۴)$$

به‌دست 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 ξام از I_m که $\xi \in \{1, \cdots, m\}$ 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، به‌طوری‌که

$$\lim_{k\to\infty} \|\Delta\hat{x}(k)\| = \infty \quad (۲۵)$$

و

$$\|\Delta r(k)\| \leq \mathcal{M} \quad (۲۶)$$

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

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

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

۳- تشخیص حملات FDI

آشکارسازها به‌منظور تشخیص خطا[۱۱] یا تشخیص حمله‌ی سایبری مورداستفاده 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 محاسبه‌شده‌ای مقایسه می‌شود. به‌این‌ترتیب آشکارساز قدرتمند χ^2 در بسیاری از موارد موفق عمل می‌کند و حتی نتیجه بهتری ازنظر عدم اعلام آلارم اشتباه نسبت به سایر آشکارسازها دارد [۱۴].

بااین‌حال 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 به‌گونه‌ای طراحی و اجرا می‌کند که آشکارسازهای آماری ازجمله آشکارساز χ^2 توانایی تشخیص این حمله را ندارند. به‌همین‌دلیل استفاده از آشکارساز فاصله اقلیدسی پیشنهادشده‌است [۱۶].

به‌این‌ترتیب، 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 به‌منظور شناسایی کارکرد غیرطبیعی سیستم قدرت است [۱۴]. در این مطالعه نیز ابتدا عمل‌کرد این آشکارساز را در سیستم موردمطالعه قرار می‌دهیم. آشکارساز χ^2 مقدار تابع

$$g(k) = r^T(k)(HPH^T + R)^{-1}r(k) \quad (۲۷)$$

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

شبکه‌ی برق تحت حملات FDI در نظر گرفته‌شده‌است. همان‌گونه که گفته‌شده برای‌آنکه سیستم نسبت به این حملات ناامن باشد

باید $\|\Delta r(k)\| \le \mathcal{M}$ باشد. دراین‌صورت وقتی $\|\Delta r(k)\|$ در عبارت $\|r^a(k)\| \le \|\Delta r(k)\| + \|r(k)\|$، در تمام لحظات به‌اندازه کافی کوچک باشد، آن‌گاه آشکارساز نمی‌تواند به‌احتمال‌زیاد بین $r(k)$ $r^a(k)$ تفاوتی قائل شود. به‌این‌ترتیب، برای ایجاد حمله، مهاجم با روانه‌کردن 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 مشخص‌شده‌است. از طرفی مهاجم باید توالی حمله را به‌گونه‌ای طراحی کند که $\lim_{k\to\infty} \Delta\hat{x}(k) = \infty$ 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 x^2 غیرقابل‌کشف 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 به‌خوبی 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 دونقطه در فضای اقلیدسی به‌صورت

$$d(p,q) = \sqrt{(p_1-q_1)^2 + (p_2-q_2)^2 + \cdots + (p_n-q_n)^2} \qquad (۲۸)$$

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 $p_\ell(k) = \hat{x}_\ell(k)$ 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 به‌معنی حمله‌ی صورت‌گرفته به داده‌های اندازه‌گیری است.

مقدار آستانه τ براساس داده‌های پیشین تنظیم شده و برای به حداقل‌رساندن نویز، آستانه را در 3σ (σ انحراف معیار) تنظیم شده‌است. تنظیم آستانه در 3σ می‌تواند نویز را تا ۹۹/۷۳٪ 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 خواهدداد. اگر $d(p,q)$ ناگهان تغییر کند به معنای وجود بردار تزریق‌شده‌است.

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

$$\mathrm{d}(\mathrm{p}_\ell(k),\mathrm{q}_\ell(k)) \triangleq \mathrm{d}\left(\hat{x}^a{}_\ell(k), x^a{}_\ell(k)\right) = \sqrt{\sum_{\ell=1}^{N}\left(\left(\hat{x}^a{}_{r,\ell}(k) - x^a{}_{r,\ell}(k)\right)^2 + \left(\hat{x}^a{}_{i,\ell}(k) - x^a{}_{i,\ell}(k)\right)^2\right)} \qquad (۲۹)$$

در لحظه k تعریف شده‌است. ازآنجایی‌که متغیرهای حالت به دو بخش حقیقی و موهومی ولتاژ باس‌ها تقسیم می‌شوند و ازطرفی تأثیر حملات 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

$$\mathrm{d}(\mathrm{p}_\ell(k),\mathrm{q}_\ell(k)) = \sqrt{\sum_{\ell=1}^{N}\left(\hat{x}^a{}_{r,\ell}(k) - x^a{}_{r,\ell}(k)\right)^2} \qquad (۳۰)$$

در لحظه k محاسبه می‌شود که $\hat{x}^a{}_{r,\ell}(k)$ بخش حقیقی ولتاژ تخمین‌زده‌شده و $x^a{}_{r,\ell}(k)$ بخش حقیقی ولتاژ اندازه‌گیری‌شده تحت حمله‌ی سایبری است.

باتوجه به تعریف ۱ بخش ۲-۳، درصورتی‌که سیستم تحت حملات ناامن شود، با برقرارساختن شرایط

$$\lim_{k\to\infty} \|\Delta\hat{x}(k)\| = \infty \qquad (۳۱)$$

$$\lim_{k\to\infty} \left\|\mathrm{d}\left(\mathrm{p}_\ell(k),\mathrm{q}_\ell(k)\right)\right\| = \infty \qquad (۳۲)$$

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.

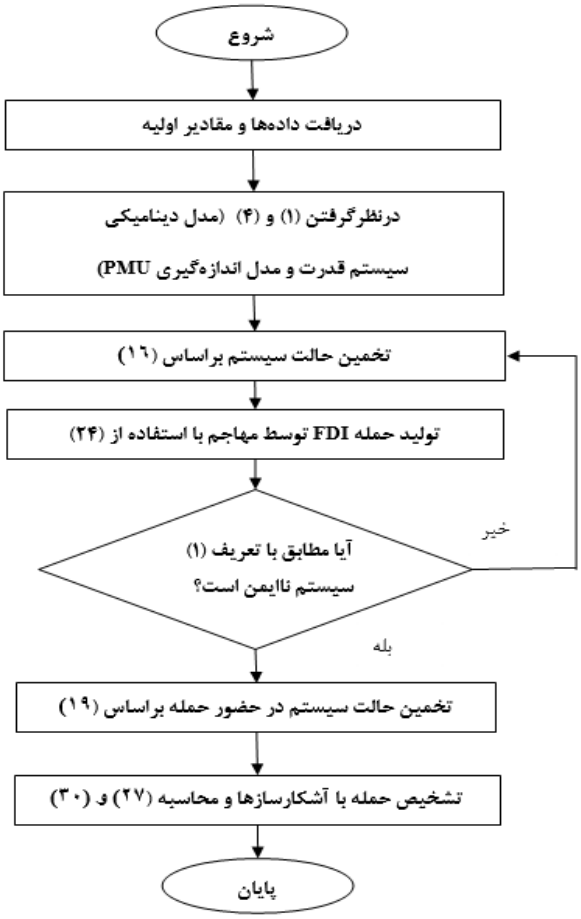
شکل ۳ ساختار روش پیشنهادی تشخیص حمله‌ی FDI را نشان می‌دهد. در این پژوهش مدل سیستم قدرت و مدل اندازه‌گیر با روابط (۱) و (۴) بیان می‌شود. بخش حقیقی و موهومی ولتاژ باس‌ها به‌عنوان متغیرهای حالت توسط اندازه‌گیر PMU اندازه‌گیری شده و این مقادیر برای تخمین حالت دینامیکی توسط خطوط ارتباطی به تخمین گر کالمن ارسال می‌شوند. اگر مهاجم توانایی طراحی حمله‌ی سایبری FDI موفق و تزریق داده‌ی غلط طبق رابطه‌ی (۲۴) را به کانال‌های ارتباطی بین PMU و تخمین‌گر 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

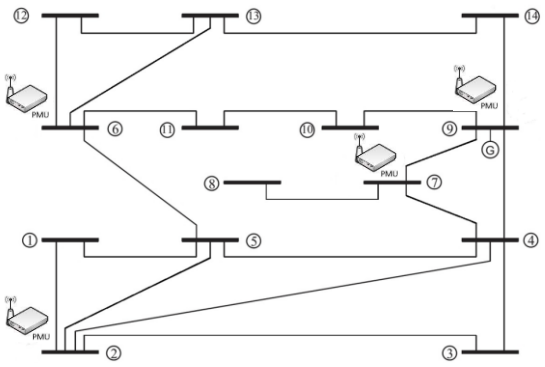
در این بخش روش ارائه‌شده، بر سیستم استاندارد IEEE مورد ارزیابی قرارگرفته است. شبیه‌سازی‌ها با نرم‌افزار MATLAB و بسته نرم‌افزاری MATPOWER انجام شده‌است [۲۶]. سیستم ۱۴ باسه IEEE با مدل (۱) و پارامترهای $A = diag_{28}\{0.98\}$، $B = diag_{28}\{0.02\}$ و $W(k) = diag_{28}\{0.1^2\}$ است. u ، ولتاژ نامی در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

جدول ۱ پیوست آورده شده‌است. 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 $\mathrm{P}(0) = 10^{-4} I_{28}$ است.

پیکربندی PMU ها در شکل ۴ نشان داده‌شده 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



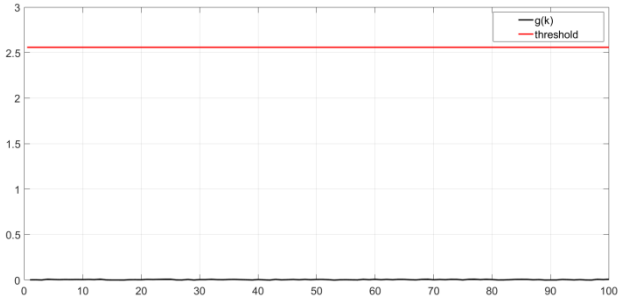
شکل ۴: سیستم ۱۴ باسه IEEE و پیکربندی PMU ها [۲۷]

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

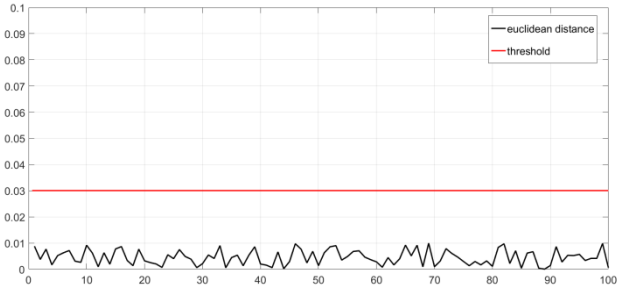
به‌طورکلی احتمال تشخیص حمله، در هر دو آشکارساز، وابسته به مقدار آستانه است. در آشکارساز χ^2 آستانه از جدول χ^2 و در آشکارساز فاصله اقلیدسی از انحراف معیار توزیع گوسی به‌دست می‌آید.

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 حالتی‌که حمله‌ای صورت‌نگرفته نشان می‌دهد. همان‌طورکه قبلاً گفته شد هم‌گرایی فیلتر کالمن با انتخاب مناسب بهره‌ی کالمن تضمین‌شده‌است؛ بنابراین باتوجه‌به عدم وجود حمله مقدار $g(k)$ از (۲۷) فقط ناشی از نویز تصادفی اندازه‌گیری است. این مقدار هرچند به‌دلیل تصادفی‌بودن 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 درحالتی‌که حمله صورت نگرفته‌است نشان می‌دهد. همان‌گونه‌که 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 آلارم نادرست ناشی از نویز رخ نداده‌است.



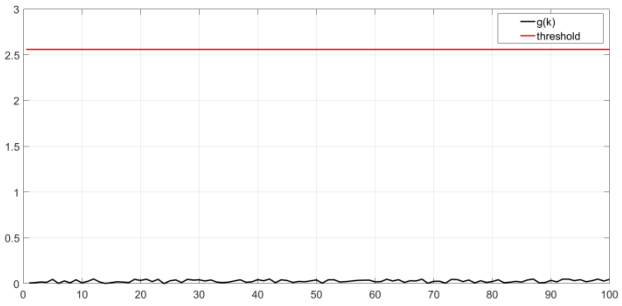
شکل ۵: عمل‌کرد آشکارساز χ^2 بدون حضور حمله‌ی FDI



شکل ۶: عمل‌کرد 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. به‌عبارت‌دیگر اختلاف تخمین حالت بسیار بزرگ خواهدبود. این در حالی است که مطابق شکل ۷ $g(k)$ که از اختلاف

باقی‌مانده به دست می‌آید هرگز از مقدار آستانه تجاوز نکرده‌است. بنابراین می‌توان نتیجه گرفت که آشکارساز χ^2 نتوانسته حمله‌ی موردنظر را تشخیص دهد.

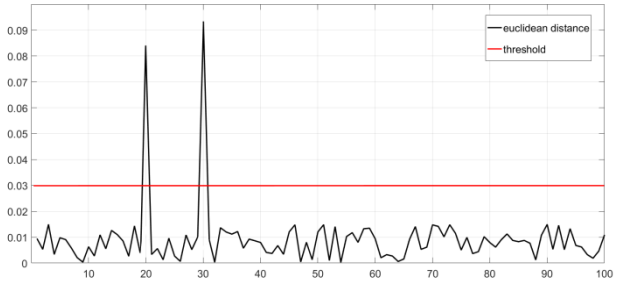


شکل ۷: عمل‌کرد آشکارساز χ^2 تحت حمله‌ی FDI

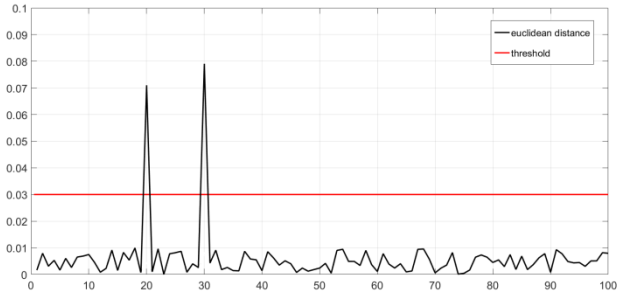
در شکل ۸ نشان‌داده شده‌است که آشکارساز فاصله اقلیدسی اختلاف فاصله بین مقادیر اندازه‌گیری و تخمین‌زده‌شده را در گام‌های ۲۰ و ۳۰ تشخیص می‌دهد. به‌عبارت‌دیگر، حمله‌ی FDI در گام ۲۰ توسط آشکارساز فاصله اقلیدسی قابل‌تشخیص است.

همان‌طور که در توضیحات روش پیشنهادی بیان شد می‌توان با استفاده از رابطه (۳۰)، فقط از بخش حقیقی داده‌های اندازه‌گیری‌شده و تخمین‌زده‌شده استفاده نمود و حمله‌ی FDI را تشخیص داد. دراین‌صورت حجم محاسبات به نصف کاهش پیدا می‌کند. شکل ۹ عمل‌کرد آشکارساز اقلیدسی در حضور حمله، تنها با استفاده از بخش حقیقی داده‌های اندازه‌گیری و تخمینی را نشان می‌دهد.

درمجموع می‌توان مشاهده کرد که آشکارساز فاصله اقلیدسی طراحی‌شده با استفاده از نیمی از داده‌ها می‌تواند بدون کاسته‌شدن از کیفیت عمل‌کرد به تشخیص دقیق و سریع حمله‌ی FDI بپردازد.



شکل ۸: عمل‌کرد آشکارساز فاصله اقلیدسی تحت حمله‌ی FDI



شکل ۹: عمل‌کرد آشکارساز فاصله اقلیدسی تحت حمله‌ی FDI با استفاده از بخش حقیقی داده‌ها

۵- نتیجه‌گیری

در این مقاله، روشی برای تشخیص حمله‌ی FDI در شبکه‌ی برق مبتنی‌بر PMU با استفاده از تخمین گر کالمن همراه با آشکارساز ارائه شده‌است. پس از حمله‌ی صورت‌گرفته آسیب‌پذیری سیستم قدرت مبتنی‌بر PMU موردبررسی قرار گرفت. انتخاب حمله‌ی FDI همان‌طورکه ملاحظه شد، به این دلیل است که اکثر آشکارسازهای متداول تشخیص خطا، مانند آشکارساز χ^2 در تشخیص این نوع حمله ناتوان هستند. نشان داده‌شد که روش به‌کاررفته مبتنی‌بر 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. همان‌طورکه از نتایج شبیه‌سازی مشاهده شد، روش ارائه‌شده در این پژوهش به‌نحوی است که آشکارساز فاصله اقلیدسی و فیلتر کالمن با محاسبه اختلاف داده‌های مشاهده‌شده از داده‌های تخمین زده‌شده در هرلحظه به تشخیص حملات می‌پردازند. می‌توان حملاتی که داده‌های اندازه‌گیری PMU را دست‌کاری‌کرده یا به تزریق داده غلط در سیستم قدرت مبتنی‌بر PMU می‌پردازد با روش مذکور تشخیص داد. همچنین بدون ازدست‌رفتن کلیت مسئله برای پایین‌آوردن حجم محاسبات و کاهش زمان عمل‌کرد می‌توان تنها از بخش حقیقی اندازه‌گیری‌های انجام‌شده و حالات تخمین‌زده‌شده استفاده کرد.

پیوست

جدول ۱: ولتاژ نامی در حالت نرمال

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

مراجع

[۱] سعید اباذری، مجتبی برخورداری یزدی و عباس عرب دردری، «*طراحی کنترل‌کننده مقاوم SVC مبتنی بر WAMS با در نظر گرفتن نامعینی*

تأخیر زمانی سیگنال‌های راه دور»، مجله مهندسی برق، دوره ۴۵، دانشگاه تبریز، ۱۳۹۴.

[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.

[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.

زیرنویس‌ها

[1] Cyber-Physical System
[2] Stuxnet
[3] False Data Injection
[4] Integrity Attack
[5] Denial Of Service
[6] Replay Attack
[7] Phasor Measurement Unit
[8] Random Attack
[9] Euclidean Distance
[10] Energy Management System
[11] Fault detection
[12] Residual
[13] Bad Data Detection