مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال هفتم، شماره ۳، پاییز ۱۳۹۵؛ ص ۲۱۸-۲۰۹

سیستم تشخیص ناهنجاری مبتنی بر هشدار برای مقابله با تهدیدهای عملیاتی در سیستم اسکادا

پیام محمودی نصر[۱]، علی یزدیان ورجانی[۲*]
۱-دانشجوی دکتری، ۲- استادیار، دانشگاه تربیت مدرس
(دریافت: ۹۴/۰۸/۱۸، پذیرش: ۹۴/۱۰/۲۲)

چکیده

حمله به سیستم‌های اسکادا در زیرساخت‌های حیاتی خسارت‌های جبران‌ناپذیری به همراه دارد. چنانچه اپراتورهای اسکادا وظایف خود را به‌درستی انجام ندهند، در فرآیندهای جاری سیستم اختلال به‌وجود می‌آید. عملکرد نامناسب اپراتورها در کنترل فرآیندها به‌عنوان تهدید عملیاتی شناخته می‌شود. ازآنجایی‌که هشدارها یکی از مهم‌ترین پارامترها در سیستم‌های اسکادا می‌باشند، در این مقاله یک سیستم تشخیص ناهنجاری مبتنی بر هشدار برای مقابله با تهدیدهای عملیاتی در سیستم اسکادا ارائه شده است. در این سیستم از روش‌های کنترل کیفیت آماری برای تعیین حدود کنترلی و تشخیص ناهنجاری استفاده‌شده است. مقدار ناهنجاری متناسب با شدت هشدارهای برطرف نشده- طولانی به‌روزرسانی می‌شود. این سیستم قادر است تا ناهنجاری‌های به‌وجود آمده در شبکه و پست‌ها را به تفکیک و به‌صورت بی‌درنگ شناسایی کند. نتایج شبیه‌سازی در شبکه‌های پتری رنگی و با استفاده از داده‌های سیستم اسکادای شبکه برق ایران نشان می‌دهد که روش پیشنهادی از کارایی لازم برخوردار است.

کلید واژه‌ها: تشخیص ناهنجاری، تهدید خودی، هشدار، اسکادا.

An Anomaly Detection System for Operational Threats in SCADA System

P. Mahmoudi Nasr, A. Yazdian Varjani*
Tarbiat Modares University
(Received: 09/11/2015; Accepted: 12/01/2016)

Abstract

One of the most dangerous insider threats in a supervisory control and data acquisition (SCADA) system is operational threat. An operational threat occurs when an SCADA operator does not perform his duties, or decides to abuse the privileges in order to perform malicious operations in remote substations. An operational threat on a critical infrastructure has the potential to cause large financial losses and irreparable damages at the national level. In this paper a new alarm-based anomaly detection system has been proposed to detect operational threats in SCADA system. The proposed system uses statistical quality control techniques for detecting anomalies and estimating control limits. The value of anomaly is calculated according to the severity of longed-unresolved alarms. The simulation results in power system SCADA as a case study show effectiveness of proposed system.

Keywords: Anomaly Detection, Alarm, Insider Threat, SCADA.

*Corresponding Author E-mail: Yazdian@modares.ac.ir

۱. مقدمه

سیستم‌های اسکادا[1] سیستم‌های پیچیده و توزیع‌شده‌ای هستند که به‌منظور پایش[2] و کنترل بی‌درنگ[3] فرآیند[4]های صنعتی در زیرساخت‌های حیاتی مانند شبکه‌های توزیع برق، آب، نفت و گاز استفاده می‌شوند. حمله به سیستم‌های اسکادا در زیرساخت‌های حیاتی منجر به بروز حوادث زنجیره‌ای[5] در فعالیت‌های اقتصادی و صنعتی خواهد شد. به همین دلیل تأمین امنیت اسکادا نقش به سزایی در تأمین امنیت ملی خواهد داشت. این در حالی است که گزارش‌های دریافتی نشان می‌دهند که سیستم‌های اسکادا در معرض انواع تهدیدها می‌باشند [۱].

یکی از تهدیدهای خطرناک در انواع سیستم های کامپیوتری، تهدید کاربران خودی[6] است. این تهدید هنگامی اتفاق می‌افتد که کاربر قانونی، یا مهاجمی که به مجوزهای قانونی دسترسی پیداکرده، با سوءاستفاده از مجوزها و انجام دستورهای قانونی موجب ایجاد نتیجه‌ای غیرقانونی در سیستم می‌شود. بنا بر تحقیقات انجام‌شده ۳۳٪ مجموع حوادث سایبری در سال ۲۰۱۰[۲]، ۲۱٪ حملات در سال ۲۰۱۱ و ۶۰٪ کلاه‌برداری‌ها در سال ۲۰۱۲ [۳] از نوع حمله خودی بوده و در سیستم‌های اسکادا ۳۰٪ حملات در سال‌های ۲۰۰۱ تا ۲۰۰۳ [۴] و ٪۳۳/۳ حملات در سال‌های ۲۰۰۰ تا ۲۰۱۱ [۵] از نوع خودی و توسط کاربران ناراضی انجام‌شده است. ۳۴٪ حملات ثبت‌شده در سال ۲۰۱۳ از نوع حمله خودی بوده است[۶].

یکی از انواع تهدیدهای خودی در سیستم اسکادا تهدید عملیاتی است. تهدیدهای عملیاتی توسط اپراتور اسکادا، یا مهاجمی که به مجوزهای اپراتور دسترسی پیداکرده انجام می‌شود و هدف آن ایجاد اختلال در فرآیندهای سیستم و افزایش ناهنجاری در شبکه است. در سیستم اسکادا پایش وضعیت[7] سیستم، کنترل فرآیندها، انجام واکنش به‌موقع نسبت به رویدادها و هشدارها و درنهایت کنترل بی‌درنگ قابلیت اطمینان[8] شبکه به عهده اپراتورها است. به همین دلیل اپراتورهای اسکادا دارای نقش کلیدی بوده و تصمیم‌های آن‌ها تأثیر فراوانی در حفظ قابلیت اطمینان شبکه دارد. چنانچه اپراتورها با بی‌توجهی به هشدارها، تأخیر در برطرف کردن هشدارها و ارسال دستورهای قانونی اشتباه (عمدی یا غیرعمدی) وظایف خود را به‌درستی انجام ندهند موجب جلوگیری و یا تأخیر در انجام یک فرآیند، اختلال در فرآیندهای جاری، شکست یک فرآیند و یا انجام یک فرآیند نادرست در سیستم می‌شوند. به عنوان نمونه می‌توان به نشتی خطوط لوله شرکت اینبریج[9] در سال ۲۰۱۰ اشاره کرد که به‌واسطه مدیریت نامناسب هشدارها در سیستم اسکادا به وجود آمد [۷]. هدف این مقاله ارائه یک سیستم تشخیص ناهنجاری[10] برای شناسایی تهدیدهای عملیاتی در سیستم اسکادا است.

باوجود آن‌که تحقیقات فراوانی به‌منظور شناسایی ناهنجاری در سیستم اسکادا تاکنون انجام‌شده [۱۴-۸] اما منابع محدودی [۱۸-۱۵] به شناسایی عملکرد نامناسب اپراتورها پرداخته‌اند. بسیاری از منابع [۸ و ۱۴-۱۰] با استفاده از آنالیز ترافیک داده‌های اسکادا به شناسایی الگوهای نامتعارف ترافیکی پرداخته‌اند. اگرچه این‌گونه روش‌ها دارای کاربرد فراوان هستند اما به دلیل آن‌که درتهدیدهای عملیاتی از مجوزهای قانونی برای کنترل فرآیندهای سیستم استفاده می‌شود، آنالیز ترافیک داده‌ها قادر به شناسایی ناهنجاری نمی‌باشند. برخی منابع به‌مرور روش‌های تشخیص ناهنجاری در سیستم اسکادا پرداخته‌اند [۸ و ۹]. یک چارچوب[11] تشخیص ناهنجاری برای سیستم‌های کنترل صنعتی با استفاده از مدل مارکوف ترافیک شبکه Modbus توسط یون و همکاران [۱۰] ارائه‌شده است. به‌منظور شناسایی دسترسی‌های غیرمجاز، ژو و همکاران [۱۱] با استفاده از سیستم تشخیص نفوذ Snort ابزاری نظارتی بر رویدادهای سیستم اسکادا ارائه کرده‌اند. کارکانو و همکاران [۱۴-۱۲] راه‌کاری برای شناسایی مجموعه‌ای از وضعیت‌های بحرانی از پیش تعریف‌شده در سیستم اسکادا ارائه کرده‌اند. در این منابع وضعیت بحرانی به‌نوعی از پیکربندی سیستم اطلاق می‌شود که موجب توقف و یا ایجاد خرابی در سیستم گردد. این منابع با استفاده از دستورات کنترلی اپراتور بر روی سیستم شبیه‌ساز، فاصله وضعیت جاری سیستم را از مجموعه وضعیت‌های بحرانی از پیش تعیین‌شده محاسبه می‌کنند. چنانچه این فاصله از مقدار آستانه کمتر شود به‌عنوان یک ناهنجاری شناسایی و اعلام خواهد شد. در این منابع به ترتیب اثبات روش [۱۲]، نحوه دست‌یابی به دستورهای کنترلی اپراتور در شبکه‌های Modbus و DNP3 [۱۳] و نتایج شبیه‌سازی [۱۴] آورده شده است. بالدوسلی و همکاران [۱۵] با استفاده از اطلاعات مربوط به ترافیک متعارف و شناخته‌شده در سیستم اسکادا، روشی برای شناسایی الگوهای ترافیکی نامتعارف ارائه کرده‌اند. هادزیومانویچ [۱۶] با استفاده از داده‌کاوی فایل ثبت وقایع[12] در سیستم‌های کنترل صنعتی روشی برای تشخیص حمله به فرآیندها در سیستم اسکادا ارائه کرده است. این منبع با

[1] Supervisory Control and Data Acquisition (SCADA)
[2] Monitoring
[3] Real-Time
[4] Process
[5] Cascade
[6] Insider threat
[7] Status
[8] Reliability
[9] Enbridge Inc.
[10] Anomaly Detection System (ADS)
[11] Framework
[12] Log file

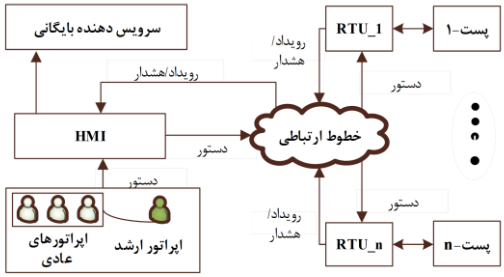
بررسی معنایی داده‌های سیستم، الگوهای غیرتکراری را در فایل ثبت وقایع شناسایی می‌کند. محدودیت این روش وابستگی به ثبت رویدادهای ناشی از عملکرد اپراتور در فایل ثبت وقایع است. این در حالی است که ممکن است اپراتور نسبت به یک هشدار واکنشی نشان ندهد و درنتیجه رویدادی در فایل ثبت وقایع ذخیره نگردد. نویسنده در مقاله دیگری [۱۷] نیز یک روش مبتنی بر معنا برای تشخیص حمله به فرآیندهای کنترل‌کننده‌های منطقی برنامه‌پذیر[1] ارائه کرده است. این منبع ابتدا با استفاده از داده‌های شبکه، فرآیندهای سیستم را شناسایی کرده و سپس با ایجاد سری‌های زمانی برای هر یک از متغیرهای فرآیند، عملکرد موردنظر آن فرآیند را در سیستم بررسی می‌کند. بای شاپ [۱۸] برای تشخیص حمله به فرآیندها، از آنالیز ویژگی‌های فرآیند مانند محرمانگی داده‌ها، درستی عملکرد فرآیند و دسترس‌پذیری نتایج آن استفاده کرده است. بر این اساس نوآوری‌های این مقاله عبارت‌اند از:

- تعیین هشدارهای برطرف نشده- طولانی در سیستم اسکادا با استفاده از تخمین زمان موردنیاز برای برطرف شدن انواع هشدارها.
- پیشنهاد یک سیستم تشخیص ناهنجاری مبتنی بر هشدار با استفاده از تکنیک‌های کنترل کیفیت آماری[2] به‌منظور شناسایی تهدیدهای عملیاتی.

در سیستم اسکادا فرض بر آن است که اپراتورها وظیفه برطرف کردن هر چه سریع‌تر هشدارها را به عهده‌دارند، لذا هرگونه تهدید عملیاتی اپراتورها ممکن است موجب افزایش تعداد هشدارهای برطرف نشده گردد. در سیستم پیشنهادی با تعیین سطح بحرانی بودن[3] پست‌ها و سطح شدت انواع هشدارها، از مجموع شدت هشدارهای برطرف نشده- طولانی به‌عنوان شاخصی برای اندازه‌گیری میزان ناهنجاری هر یک از پست‌ها و شبکه استفاده می‌شود. چنانچه میزان ناهنجاری از سطح آستانه بیشتر شود به‌عنوان ناهنجاری شناسایی می‌گردد. برای تعیین سطح آستانه ناهنجاری از روش‌های کنترل کیفیت آماری استفاده شده است.

۲. سیستم اسکادا: فرصت‌ها و چالش‌ها

سیستم‌های اسکادا وظیفه پایش و کنترل بی‌درنگ فرآیندهای شبکه‌های صنعتی را به عهده‌دارند. در این سیستم‌ها داده‌های اندازه‌گیری شده در پست‌ها به‌وسیله RTU[4] جمع‌آوری و از طریق یک شبکه مخابراتی خصوصی و یا عمومی برای مرکز کنترل ارسال می‌شوند. سرویس‌دهنده HMI[5] در مرکز کنترل داده‌های دریافتی را به اپراتورها نمایش داده و برعکس فرمان‌های کنترلی اپراتورها را برای تجهیزات داخل پست‌ها ارسال می‌کند[۱۹ و ۲۰]. هرگونه تغییر در شرایط سیستم که نیازمند توجه اپراتورها باشد در قالب یک هشدار اعلام خواهد شد. هنگامی‌که خطا یا خرابی دریکی از تجهیزات شبکه به وجود می‌آید، سیستم‌های حفاظتی در پست هشدار(های) مربوطه را ایجاد و توسط RTU به مرکز کنترل ارسال می‌کنند. اپراتورهای اسکادا با مشاهده هشدار (ها) ابتدا آن (ها) را تصدیق[6] کرده و سپس اقدام مقتضی برای برطرف شدن آن (ها) را انجام می‌دهند. تمامی داده‌ها و فرمان‌ها در سرویس‌دهنده بایگانی[7] ذخیره می‌گردند. شکل (۱) ساختار کلی سیستم اسکادا را نشان می‌دهد.



شکل ۱. ساختار کلی سیستم اسکادا

۲-۱. اپراتورهای اسکادا

در سیستم اسکادا اپراتورها نقش کلیدی داشته و بر اساس دستورالعمل‌های ثابت بهره‌برداری وظیفه کنترل و نظارت بر فرآیندها، واکنش به‌موقع نسبت به رویدادها و هشدارها و صدور فرمان‌های کنترلی به‌منظور حفظ قابلیت اطمینان سیستم را به عهده‌دارند. هنگامی‌که هشداری از طرف یکی از پست‌های تحت نظارت اپراتور در صفحه‌نمایش سرویس‌دهنده HMI ظاهر می‌شود، اپراتور با بررسی دقیق و تصمیم‌گیری به‌موقع سعی در برطرف کردن آن هشدار می‌نماید. هرگونه تأخیر و اشتباه اپراتور می‌تواند خسارت‌های جبران‌ناپذیری به همراه داشته و قابلیت اطمینان سیستم را با مشکل روبرو کند.

پردازش به‌موقع هشدارها و تصمیم‌گیری در مورد نحوه برطرف کردن آن‌ها امری دشوار و پراسترس حتی برای اپراتورهای باتجربه است. به‌منظور کاهش استرس کاری اپراتور و افزایش امنیت سیستم، معمولاً از تکنیک‌های هوشمند پردازش هشدار[8]

[1] Programmable Logic Controllers (PLC)
[2] Statistical Quality Control
[3] Criticality
[4] Remote Terminal Unit
[5] Human Machine Interface (HMI)
[6] Acknowledge
[7] Historian Server
[8] Intelligent Alarm Processing

[۲۱] مانند اولویت‌بندی و فیلتر کردن هشدارها استفاده می‌شود.

۲-۲. تهدیدهای عملیاتی

تهدیدهای اسکادا را می‌توان به دو گروه تهدیدهای خودی (داخلی) و غیرخودی (خارجی) تقسیم کرد. تهدیدهای غیرخودی توسط کاربران غیرمجاز و خارج از سیستم مانند هکرها و دولت‌های متخاصم انجام‌شده، درحالی‌که تهدیدهای خودی توسط کاربران مجاز (و یا مهاجمی که به مجوزها دسترسی پیداکرده) و با سوءاستفاده از مجوزهای قانونی انجام می‌شود. اگرچه تعداد تهدیدهای خودی ممکن است کمتر از تعداد تهدیدهای غیرخودی باشد اما میزان موفقیت و آسیب آن‌ها به‌مراتب بیشتر وجدی‌تر از تهدیدهای غیرخودی است [۲۲]. این امر به دلیل آن است که کاربران خودی دسترسی فیزیکی و قانونی به تجهیزات داشته، دانش کافی از سیستم‌های کامپیوتری و نرم‌افزارهای مربوطه دارند، و از همه مهم‌تر از قوانین و سیستم‌های امنیتی لحاظ شده آگاهی دارند.

تهدیدهای عملیاتی یکی از انواع تهدیدهای خودی در سیستم اسکادا است. این تهدید هنگامی رخ می‌دهد که اپراتور:

- وظایف خود را بر اساس دستورالعمل‌های ثابت بهره‌برداری به‌درستی انجام نمی‌دهد (عمدی و یا غیرعمدی).
- با سوءاستفاده از مجوزهای قانونی موجب ایجاد اختلال و شکست فرآیندها می‌شود.
- به‌طور غیرعمدی مرتکب اشتباه در کنترل فرآیندها سیستم می‌شود.

بنابراین تهدیدهای عملیاتی را می‌توان به‌صورت زیر دسته‌بندی کرد:

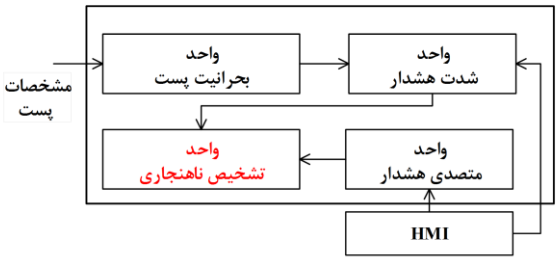
(۱) *تهدید وابسته به هشدارها:* این تهدید هنگامی به وقوع می‌پیوندد که اپراتور هشدارها را به‌موقع برطرف نمی‌کند. تصدیق گروهی و نادیده[1] گرفتن هشدارها، تأخیر در برطرف کردن هشدارها و پاسخ اشتباه به هشدارها (ناقص و یا نامناسب) از انواع این تهدید است.

(۲) *تهدید پیکربندی:* این تهدید هنگامی به وقوع می‌پیوندد که تنظیم نامناسبی دریکی از تجهیزات پست توسط اپراتور (عمدی و یا غیرعمدی) ایجاد می‌شود؛ مانند تغییر نامناسب تپ‌چنجر ترانسفورماتور و باز/بسته کردن نامناسب فیدرهای خروجی در شبکه قدرت.

۳. سیستم پیشنهادی تشخیص ناهنجاری

در این بخش یک سیستم مبتنی بر هشدار به‌منظور تشخیص ناهنجاری درتهدیدهای عملیاتی ارائه خواهد شد. در سیستم اسکادا هرچه اپراتور از مهارت بیشتری در کنترل شبکه برخوردار باشد از میزان شدت هشدارهای برطرف نشده کاسته می‌شود. درحالی‌که تهدیدهای عملیاتیِ اپراتور موجب افزایش تعداد هشدارهای برطرف نشده در سیستم می‌گردد؛ بنابراین از آنجا که اپراتورها درصدد برطرف کردن هر چه سریع‌تر هشدارها می‌باشند، از میزان شدت هشدارهای برطرف نشده می‌توان به‌عنوان شاخصی برای تعیین شدت ناهنجاری استفاده کرد.

شکل (۲) ساختار سیستم پیشنهادی را نشان می‌دهد. واحد بحرانیت-پست وظیفه محاسبه سطح بحرانی بودن پست‌ها را به عهده دارد. واحد شدت- هشدار نیز سطح شدت هشدارها را محاسبه می‌کند. واحد متصدی- هشدار وظیفه تعیین وضعیت هشدارهای دریافتی از سرویس‌دهنده HMI را به عهده دارد (در مورد وضعیت هشدارها در بخش‌های بعدی توضیح داده خواهد شد). واحد تشخیص- ناهنجاری با بررسی وضعیت هشدارها، میزان ناهنجاری سیستم را محاسبه کرده و در صورت تشخیص ناهنجاری آن را اعلام می‌کند.



شکل ۲. ساختار سیستم پیشنهادی تشخیص ناهنجاری

۳-۱. تعیین سطح بحرانی بودن پست

یک روش مبتنی بر قابلیت اطمینان برای تعیین سطح بحرانی بودن پست‌ها و تأثیر آن‌ها در میزان کارایی شبکه قدرت در [۲۳] ارائه‌شده است. اگرچه از قابلیت اطمینان می‌توان برای رتبه‌بندی و تعیین سطح بحرانی بودن پست‌ها استفاده کرد، اما از معیارهای متفاوت دیگری نیز می‌توان بهره جست مانند، میزان درآمد پست، افزونگی تجهیزات، و غیره. در این مقاله از یک روش کمّی مبتنی بر ویژگی‌های پست (مانند ظرفیت، سطح ولتاژ، اهمیت در شبکه، تعداد فیدرهای ورودی/خروجی، موقعیت جغرافیایی و اهمیت ناحیه تحت پوشش، و غیره) برای تعیین سطح بحرانی بودن پست‌ها استفاده‌شده است. فرض کنید مجموعه $\{p_1, p_2, \dots, p_k\}$ شامل ویژگی‌های پست و $w_{p_j} \in [0,1]$ مقدار وزن ویژگی p_j و nتعداد پست‌ها باشد. چنانچه $g_{p_{ij}} \in [0,1]$ امتیاز کسب‌شده پست iام برای ویژگی p_j باشد، سطح نسبی بحرانی بودن پست با استفاده از رابطه زیر محاسبه خواهد شد:

[1] Ignore

$$CR_{sub_i} = \frac{\sum_{j=1}^{k} w_{p_j} . g_{p_{ij}}}{\max_{1 \le i \le n} \sum_{j=1}^{k} w_{p_j} . g_{p_{ij}}} \quad (1)$$

در این رابطه $CR_{sub_i} \in [0,1]$ که با عنوان *بحرانیت نسبی* شناخته می‌شود عبارت از نسبت امتیاز کسب‌شده پست iام به حداکثر امتیاز کسب‌شده پست‌ها در شبکه است.

۳-۲. تعیین سطح شدت هشدار

از معیارهای متفاوتی مانند شدت پیامدها، مدت‌زمان پاسخگویی، محل وقوع، تجهیز عامل و ... می‌توان برای گروه‌بندی و تعیین نوع هشدارها استفاده کرد. در شبکه برق ایران هشدارها با توجه به‌شدت پیامدها، به دو گروه اصلی[1] و فرعی[2] تقسیم می‌شوند. هشدارهای اصلی مانند (Circuit breaker failure و DC/AC supply failure) هشدارهای اولیه‌ای هستند که اپراتور با برطرف کردن به‌موقع آن‌ها، از ایجاد هشدارهای فرعی مانند (Differential relay trip و Over-current/voltage relay trip) جلوگیری به عمل می‌آورد. به‌عبارت‌دیگر هشدارهای فرعی شرایط وخیم‌تری را در سیستم اعلام می‌کنند. فهرستی از انواع هشدارهای اصلی و فرعی در منبع [۲۴] آمده است. در این مقاله سطح شدت هر هشدار متناسب با نوع هشدار و سطح بحرانی بودن پستی که هشدار در آن اتفاق افتاده تعیین می‌گردد. فرض کنید هشدارها به m نوع گروه‌بندی‌شده باشند. چنانچه $w_j \in [0,1]$ با فرض $\sum_{j=1}^{m} w_j = 1$ وزن نوع هشدار j باشد سطح شدت هر یک از هشدارهای نوع j از پست iام به‌صورت زیر محاسبه می‌شود.

$$Sev_{ij} = CR_{sub_i} . W_j \quad (2)$$

چنانچه $Sev_{ij} = 1$ باشد نشان‌دهنده حداکثر شدت هشدار و برعکس چنانچه $Sev_{ij} = 0$ یعنی هشدار بدون شدت است.

۳-۳. روش تشخیص ناهنجاری

روش پیشنهادی برای تشخیص ناهنجاری بر پایه هشدار و با استفاده از روش‌های کنترل کیفیت آماری است. می‌دانیم که هرگونه اختلال و خطای ایجادشده در شبکه به‌صورت یک یا چند هشدار در سیستم اسکادا ثبت می‌شود. چنانچه اپراتور بتواند هشدار (ها) را به‌موقع برطرف نماید به معنای برطرف شدن اختلال یا خطای ایجادشده است؛ اما اگر هشدار (ها) برطرف نشود، اختلال یا خطا همچنان در شبکه باقی‌مانده است. لذا می‌توان از هشدارهای برطرف نشده به‌عنوان شاخصی برای تعیین شدت خطای موجود در شبکه استفاده کرد.

برای تعیین شدت خطایی که وابسته به تهدیدهای عملیاتی اپراتور است، ضروری است تا فرصت کافی برای برطرف شدن هر هشدار به اپراتور داده شود. چنانچه هشداری در فرصتِ زمانی از پیش تعیین‌شده برطرف نشود، آن‌گاه به‌عنوان شاخصی برای تعیین شدت خطای وابسته به تهدیدهای عملیاتی در نظر گرفته خواهد شد. پرواضح است که فرصت زمان موردنیاز برای برطرف شدن هر هشدار (که در این مقاله با عنوان *فرصت-هشدار* شناسایی می‌شود)، مقداری متغیر و متفاوت از هر هشدار دیگر می‌تواند باشد. بحث بیشتر در مورد نحوه تعیین مقدار فرصت- هشدار در بخش بعدی آمده است. هنگامی‌که هشداری در مرکز کنترل نمایش داده می‌شود، ضروری است تا اپراتور قبل از اتمام فرصت- هشدارِ از پیش تعیین‌شده آن را برطرف نماید. چنانچه هشداری در فرصتِ تعیین‌شده برطرف نشود به‌عنوان یک *هشدار- برطرف نشده- طولانی* در سیستم شناخته می‌شود. در این مقاله شدت خطای وابسته به تهدیدهای عملیاتی اپراتور (که با متغیر U نشان داده می‌شود) با استفاده از مجموع شدت هشدارهای-برطرف نشده-طولانی اندازه‌گیری می‌شود. در شرایط عادی هنگامی‌که شبکه تحت کنترل است، اپراتور در اسرع وقت اقدام به برطرف کردن هشدارها می‌نماید، لذا مقدار U معمولاً صفر و یا نزدیک به صفر است. چنانچه مقدار U از حداکثر مقدار آستانه[3] خارج شود به‌عنوان شرایط ناهنجار در سیستم شناسایی و اعلام می‌گردد.

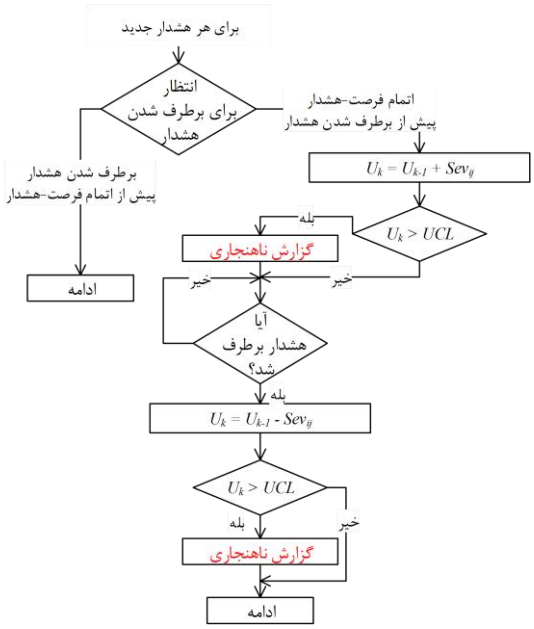
توجه به این نکته ضروری است که مقدار U در دو صورت از حد آستانه خارج می‌شود: (۱) تهدیدهای عملیاتی (۲) سیل-هشدار[4]. سیل-هشدار هنگامی ایجاد می‌شود که یک یا تعدادی خطا در شبکه منجر به جاری شدن سیل‌آسای هشدارهای تکراری و زنجیره‌ای به ترتیبی می‌شوند که اپراتور فرصت کافی برای برطرف کردن آن‌ها را ندارد. هشدارهای سیل‌آسا شرایطی را ایجاد می‌کنند که حتی اپراتورهای باتجربه قادر به برطرف کردن آن‌ها و شناسایی عامل خطا نمی‌باشند. بر اساس استاندارد نرخ ایجاد ۱۰ هشدار در ۱۰ دقیقه برای هر اپراتور به‌عنوان شرایط سیل-هشدار شناسایی می‌شود [۲۶-۲۵].

خوشبختانه امروزه برای جلوگیری از ایجاد شرایط سیل- هشدار در سیستم‌های اسکادا از تکنیک‌های هوشمند پردازش هشدار استفاده می‌شود [۲۱ و ۲۷]. یک پردازنده هوشمند هشدار[5] قادر است تا علاوه بر کاهش تعداد هشدارهای نمایش داده‌شده، راه‌کارهای مناسب برطرف شدن هشدار را نیز به اپراتور پیشنهاد دهد [۲۱]؛ لذا چنانچه سیستم اسکادا مجهز به یک پردازنده

[1] Major
[2] Minor
[3] Upper Control Limit (UCL)
[4] Alarm Flooding
[5] Intelligent Alarm Processor

هوشمند هشدار باشد، تهدید عملیاتی تنها عامل افزایش مقدار U و خارج شدن آن از حد آستانه خواهد بود.

با فرض استفاده از یک پردازنده هوشمند هشدار، شکل (۳) نحوه محاسبه U را به‌صورت بی‌درنگ نشان می‌دهد.



شکل ۳. مراحل شناسایی ناهنجاری به‌صورت بی‌درنگ

متغیر U با شروع از مقدار صفر و متناسب با شدت هشدارها تغییر می‌کند. مقدار U هنگامی‌که هشداری در فرصت- هشدارِ از پیش تعیین‌شده برطرف نشود افزایش، و هنگامی‌که یک هشدار-برطرف نشده- طولانی برطرف شود کاهش می‌یابد. به‌عبارت‌دیگر مقدار U با استفاده از مجموع وزنی تعداد هشدارهای-برطرف نشده-طولانی به‌صورت زیر محاسبه می‌شود:

$$U_k = \sum_{i=1}^{n} \sum_{j=1}^{m} Sev_{ij} \cdot C_{ijk} \qquad (۳)$$

در این فرمول C_{ijk} تعداد هشدارهای-برطرف نشده-طولانی از نوع j در پست iام و k شماره نمونه‌گیری (مرحله بازرسی) است. هنگامی‌که مقدار U_k از حد آستانه خارج شود یک وضعیت ناهنجار در سیستم شناسایی و اعلام خواهد شد.

تخمین فرصت-هشدار: در سیستم پیشنهادی فرصت- هشدار برای هر هشدارِ از نوع j (که با RST_j نمایش داده می‌شود) به این صورت تخمین زده می‌شود. فرض کنید زمان سپری‌شده از هنگام ظاهر شدن یک هشدار در صفحه HMI تا هنگام برطرف شدن آن (به‌عنوان یک مقدار نمونه RST_j) با متغیر RST_j^{sample} نشان داده شود. پرواضح است که مقدار نمونه RST_j^{sample} از هر هشدار به هشدار دیگر متناسب با شرایط سیستم و رفتار اپراتور تغییر خواهد کرد. ازآنجاکه آخرین نمونه‌های اندازه‌گیری شده گویای شرایط جاری سیستم می‌باشند، می‌توان از رابطه متحرک موزون نمایی[1] به‌منظور تعیین مقدار میانگین RST_j استفاده کرد.

$$RST_j^{estimate} = (1-\alpha) RST_j^{estimate} + \alpha . RST_j^{sample} \qquad (۴)$$

در این رابطه $RST_j^{estimate}$ مقدار میانگین فرصت- هشدارِ از نوع j و α ضریب آخرین نمونه است. با محاسبه قدر مطلق تفاضل بین RST_j^{sample} و $RST_j^{estimate}$ مقدار تفاوت هر نمونه اندازه‌گیری شده از مقدار متوسط فرصت- هشدار به دست می‌آید. رابطه (۵) نحوه محاسبه میانگین تغییرات RST_j با استفاده از رابطه متحرک موزون نمایی را نشان می‌دهد.

$$RST_j^{deviation} = (1-\beta) RST_j^{deviation} + \beta . \left| RST_j^{sample} - RST_j^{estimate} \right| \qquad (۵)$$

و به‌این‌ترتیب مقدار فرصت- هشدار از رابطه (۶) محاسبه می‌شود.

$$RST_j^{timeout} = RST_j^{estimate} + \rho . RST_j^{deviation} \qquad (۶)$$

در روابط (۵) و (۶)، β ضریب اختلاف بین $RST_j^{estimate}$ و RST_j^{sample} و ρ ضریب متوسط تغییرات RST_j است. بنابراین هنگامی یک هشدارِ از نوع j به‌عنوان یک هشدار- برطرف نشده- طولانی شناخته خواهد شد که در فرصت- هشدار $RST_j^{timeout}$ برطرف نشود.

تعیین حدود کنترلی: به‌منظور آنالیز متغیر U و تعیین حدود کنترلی از روش‌های کلاسیک کنترل کیفیت آماری برای کنترل عدم انطباق‌ها[2] [۲۸] (مانند انواع نمودارهای c, u, p, D) می‌توان استفاده کرد. در این نمودارها حدود کنترلی در شرایطی تعیین می‌گردند که داده‌های جمع‌آوری‌شده متعلق به شرایط کنترل و پایدار سیستم باشند. در این مقاله هر هشدار-برطرف نشده-طولانی به‌مثابه یک خرابی و یا عدم انطباق در یک فرآیند تولیدی و یا پردازشی در مدل‌های آماری فرض شده است. با توجه به آنکه مقدار ناهنجاری هر هشدار-برطرف نشده-طولانی متناسب با شدت آن متفاوت است، ضروری است تا از نمودار کنترل نقص[3] برای تعیین حدود کنترلی استفاده شود. لازمه استفاده از این نمودار آن است که توزیع آماری نقص‌ها (ترافیک هشدارهای-برطرف نشده- طولانی) مطابق با توزیع پوآسون باشد [۲۸ و ۲۹]. در بحث کنترل کیفیت آماری برای فرآیندهای تولیدی و پردازشی معمولاً فرض می‌کنند که توزیع آماری تعداد نقص‌ها مطابق با توزیع پوآسون است. به‌طور مشابه بسیاری از منابع مانند [۳۰ و ۳۱] از توزیع پوآسون برای مدل‌سازی ترافیک داده‌های اسکادا استفاده کرده‌اند. در سیستم‌های اسکادا ازآنجایی‌که

[1] Exponentially Weighted Moving Average (EWMA)
[2] Nonconformities
[3] Demerit Control Charts (D-chart)

احتمال وقوع هشدار در هر یک از منابع کم است و تعداد منابع بالقوه تولید هشدار به دلیل بزرگی و گستردگی شبکه در زیرساخت‌های حیاتی به‌اندازه کافی زیاد است، می‌توان از توزیع پوآسون برای مدل‌سازی ترافیک هشدارها استفاده کرد. لذا با فرض آنکه متغیر U_k در رابطه (۳) یک ترکیب خطی از متغیرهای تصادفی مستقل با توزیع پوآسون باشد، مقدار میانگین ناهنجاری با استفاده از رابطه زیر قابل‌محاسبه است.

$$\bar{U} = \sum_{i=1}^{n} \sum_{j=1}^{m} Sev_{ij} . \bar{u}_{ij} \qquad (۷)$$

در این رابطه $\bar{u}_{ij}$ میانگین تعداد هشدارهای- برطرف نشده- طولانی برای هر نوع هشدار j در پست iام است ($\bar{u}_{ij} = \sum_{k=1}^{N} C_{ijk}/N$ که N مجموع تعداد بازرسی‌ها است). درنهایت حدود کنترلی بالا و پایین[1] به‌صورت زیر محاسبه خواهند شد.

$$\mathrm{UCL} = \bar{U} + \varphi . \hat{\sigma}_U \ , \ \mathrm{LCL} = \bar{U} - \varphi . \hat{\sigma}_U \qquad (۸)$$

$$\hat{\sigma}_U = \sqrt{\sum_{i=1}^{n} \sum_{j=1}^{m} Sev_{ij}^{2} . \bar{u}_{ij}} \qquad (۹)$$

در روابط بالا $\hat{\sigma}_U$ انحراف معیار و φ ضریب انحراف معیار است و مقدار آن معمولاً برابر ۲ (برای حد اخطار) و یا ۳ (برای حد نهایی) در نظر گرفته می‌شود [۲۸]. ازآنجاکه هر چه تعداد هشدارها کمتر باشد شبکه از قابلیت اطمینان بیشتر برخوردار است، مقدار حد آستانه پایین را می‌توان برابر با صفر قرار داد (LCL=0)

۴. نتایج شبیه‌سازی

در این بخش به‌منظور آنکه نشان دهیم روش پیشنهادی قادر به شناسایی ناهنجاری در شرایط مختلف است از دو سناریو با شدت حمله متفاوت استفاده‌شده است. در سناریوی اول تنها یکی از پست‌ها تحت حمله عملیاتی شدید قرارگرفته درحالی‌که در سناریوی دوم فرض بر آن است که اپراتور با زیرکی فراوان به‌منظور مخفی ماندن حملات، از حملات عملیاتی ضعیف اما گسترده بر روی همه پست‌ها استفاده می‌کند. داده‌های موردنیاز سناریوها با استفاده از شبکه‌های پتری رنگی[2] در آزمایشگاه امنیت اسکادای سیستم‌های قدرت در دانشگاه تربیت مدرس [۳۲] و متناسب با داده‌های واقعی در سیستم اسکادای شبکه برق ایران شبیه‌سازی‌شده‌اند. سیستم اسکادای شبیه‌سازی‌شده دارای پنج پست انتقال و فوق توزیع است. جدول (۱) ویژگی‌های در نظر گرفته‌شده برای هر یک از پست‌ها انتقال و فوق توزیع و معیار وزن دهی آن‌ها را منطبق با داده‌های گزارش شده [۲۴] نشان می‌دهد. در جدول (۲) مقدار بحرانی بودن پست‌های شبیه‌سازی‌شده با استفاده از ویژگی‌های جدول (۱) و رابطه (۱) نشان داده‌شده است. به‌منظور تعیین مقدار فرصت- هشدار برای هر یک از انواع هشدارها و حدود کنترلی، داده‌های اولیه در شرایطی جمع‌آوری‌شده‌اند که سیستم در حالت پایدار و تحت کنترل کامل اپراتور بوده است.

جدول ۱. معیار وزن دهی برای تعیین بحرانیت پست‌ها

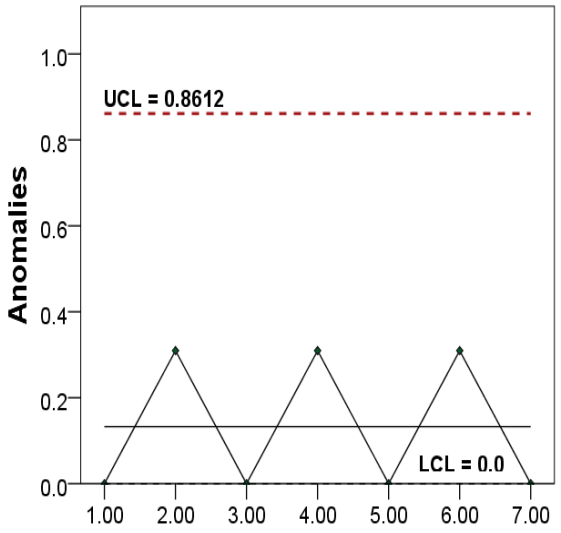
P_j	w_{p_j}	توضیحات	معیار وزن دهی	وزن
P_1	۰/۵	ظرفیت ایستگاه (مگاولت آمپر)	ظرفیت ترانس‌ها ≤۵۰۰ (انتقال)	۱
			ظرفیت ترانس‌ها ≤۵۰(فوق توزیع)	
			ظرفیت ترانس‌ها >۵۰۰ (انتقال)	/۵
			ظرفیت ترانس‌ها >۵۰(فوق توزیع)	
P_2	۰/۵	تعداد ترانسفورماتور	تعداد ترانس‌ها >۲ عدد	۱
			تعداد ترانس‌ها ≤۲ عدد	/۵
			کلید خانه	/۷۵
			بدون ترانس (فوق توزیع)	۰
P_3	۰/۵	نوع شینه بندی ایستگاه	چند کلیدی (یک و نیم کلیدی)	۱
			دوبل/باس اصلی و فرعی/ مش	/۵
			باسبار ساده / حلقوی باز، H و π	۰
P_4	۰/۵	تعداد فیدرهای ورودی/ خروجی	تعداد< ۱۰ عدد	۱
			۱۰≤ تعداد <۴ (انتقال)	/۵
			۱۰≤ تعداد <۲ (فوق توزیع)	
			تعداد ≤ ۴ عدد (انتقال)	۰
			تعداد ≤ ۲عدد (فوق توزیع)	
P_5	۰/۵	رینگ یا شعاعی	رینگ	۱
			شعاعی	/۵
P_6	۱	اهمیت ایستگاه در شبکه	بسیار مهم (> 1000mV)	۱
			مهم	/۷۵
			معمولی (< 100mV)	/۵

جدول ۲. سطح بحرانی بودن پست‌ها

عنوان	امتیاز پست‌ها				
	A	B	C	D	E
P_1	۰/۵	۰/۵	۰/۵	۰/۲۵	۰/۵
P_2	۰/۵	۰/۲۵	۰/۵	۰/۵	۰/۵
P_3	۰/۵	۰/۵	۰/۲۵	۰/۵	۰
P_4	۰/۵	۰/۵	۰/۵	۰/۵	۰/۵
P_5	۰/۵	۰/۵	۰/۵	۰/۵	۰/۵
P_6	۱	۰/۷۵	۰/۶۲	۱	۰/۷۵
جمع امتیاز	۳/۵	۳	۲/۸۷	۳/۲۵	۲/۷۵
بحرانیت نسبی	۱/۰	۰/۸۶	۰/۸۲	۰/۹۳	۰/۷۹

[1] Lower Control Limit (LCL)
[2] Color Petri Net

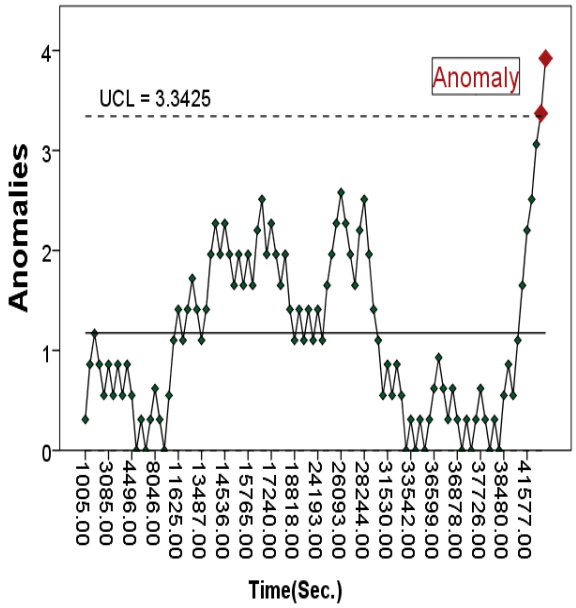
شکل (۴) نمودار تغییر ناهنجاری شبکه (متغیر U) برای داده‌های جمع‌آوری‌شده طی دو سال در شرایط پایدار سیستم را نشان می‌دهد. همان‌طور که مشاهده می‌شود مقدار ناهنجاری همواره برابر صفر بوده و تنها در سه مورد مقدار آن کمی از صفر بالاتر رفته است (مقادیر صفر تکراری در تهیه نمودار در نظر گرفته نشده‌اند).



شکل ۴. تغییر ناهنجاری شبکه در شرایط پایدار

موارد دیگری که در انجام سناریوها در نظر گرفته شده‌اند عبارت‌اند از: (۱) مقدار ناهنجاری برای هر یک از پست‌ها و شبکه به‌طور جداگانه اندازه‌گیری شده‌اند. (۲) هشدارها به دو گروه اصلی[1] و فرعی[2] تقسیم شده‌اند. (۳) برای مطابقت هر چه بیشتر با شرایط واقعی، نرخ ایجاد هشدارهای اصلی چندین برابر نرخ هشدارهای فرعی در نظر گرفته شده است. (۴) مقادیر پارامترهای در نظر گرفته‌شده عبارت‌اند از: $w_{l_{mi}} = 0.64$ برای هشدارهای فرعی، $w_{l_{mj}} = 0.36$ برای هشدارهای اصلی، $\alpha = 0.125$، $\beta = 0.25$، $\varphi = \rho = 2$. (۵) برای جلوگیری از سیل- هشدارها از سیستم‌های هوشمند پردازش هشدار استفاده می‌شود. (۵) هیچ‌گونه تغییری در داده‌های دریافتی به‌منظور فریب سیستم اعمال نمی‌گردد.

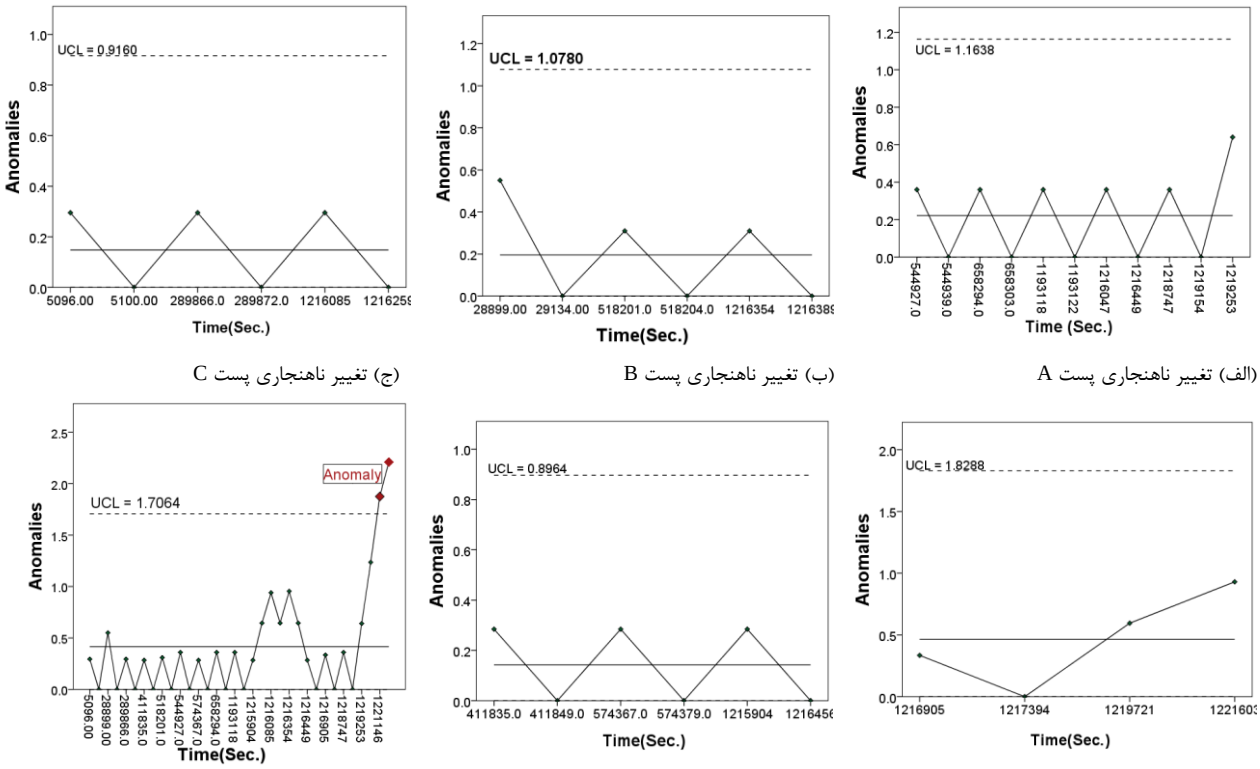
سناریوی اول، حمله عملیاتی شدید به یک پست: در این سناریو، تنها پست B موردحمله عملیاتی شدید اپراتور قرارگرفته و رفتار اپراتور نسبت به پست‌های دیگر به‌طور عادی فرض شده است؛ به‌عبارت‌دیگر سیستم شبیه‌سازی‌شده به نحوی پیکربندی‌شده است که ۷۰٪ هشدارهای پست B مورد بی‌توجهی اپراتور قرارگرفته و با تأخیر برطرف شوند. هر چه تعداد هشدارهای- برطرف نشده- طولانی در پست B اضافه می‌شود مقدار ناهنجاری آن نیز افزایش می‌یابد. شکل (۵) تغییر ناهنجاری پست B را تا خروج از مقدار آستانه و تشخیص ناهنجاری نشان می‌دهد. مشاهده می‌شود که متناسب با رفتار اپراتور در برطرف کردن هشدارها، میزان ناهنجاری تغییر کرده است. در این سناریو از آغاز حمله اپراتور تا تشخیص ناهنجاری حدود ۱۱ ساعت گذشته است. در طی این مدت از میان ۵۰ هشداری که به‌موقع برطرف نشده و موجب افزایش ناهنجاری شده، ۴۳ هشدار قبل از خروج ناهنجاری از حد آستانه برطرف شده است.



شکل ۵. تغییر ناهنجاری در سناریوی حمله عملیاتی شدید به یک پست

سناریوی دوم، حمله عملیاتی ضعیف به همه پست‌ها: در این سناریو تمامی پست‌های شبکه مورد حمله ضعیف اپراتور قرارگرفته است. این سناریو ممکن است توسط اپراتور مهاجم به‌قصد مخفی نگه‌داشتن حمله و یا اشتباه‌های غیرعمدی اپراتور کم‌تجربه اتفاق بیافتد. در این سناریو سیستم شبیه‌سازی‌شده به نحوی پیکربندی شده است که اپراتور به ۳۰٪ از هشدارها با تأخیر پاسخ می‌دهد. شکل (۶) تغییر ناهنجاری هر یک از پست‌ها و شبکه را به تفکیک نشان می‌دهد. مشاهده می‌شود که تغییر ناهنجاری تمامی پست‌ها در محدوده مجاز است، اما ناهنجاری کلی شبکه از حد آستانه خارج شده است. در این سناریو حدود ۱۴ روز از آغاز حمله مخفیانه اپراتور تا شناسایی آن سپری شده است.

[1] Major
[2] Minor



(الف) تغییر ناهنجاری پست A (ب) تغییر ناهنجاری پست B (ج) تغییر ناهنجاری پست C

(د) تغییر ناهنجاری پست D (ه) تغییر ناهنجاری پست E (و) تغییر ناهنجاری شبکه

شکل ۶. تغییر ناهنجاری به تفکیک در پست‌ها و شبکه در سناریوی حمله عملیاتی ضعیف به همه پست‌ها

۵. نتیجه‌گیری

در این مقاله به‌منظور شناسایی تهدیدهای عملیاتی در سیستم اسکادا یک سیستم تشخیص ناهنجاری مبتنی بر *هشدار*، که به‌عنوان یکی از مهم‌ترین پارامترها در سیستم اسکادا محسوب می‌شود، ارائه‌شده است. در این سیستم برای هر یک از پست‌ها یک سطح بحرانی بودن در نظر گرفته‌شده و میزان ناهنجاری متناسب با شدت هشدارهای- برطرف نشده- طولانی محاسبه می‌شود. روش پیشنهادی در مقایسه با روش‌های ارائه‌شده قبلی قادر است تا مقدار ناهنجاری را به‌صورت بی‌درنگ و به تفکیک برای هر یک از پست‌ها و شبکه محاسبه، و در صورت تشخیص ناهنجاری آن را شناسایی کند. علاوه بر آن، این روش می‌تواند ناهنجاری ناشی از تهدیدهای عملیاتی را حتی در صورت عدم واکنش اپراتور به هشدارها و عدم ثبت داده در فایل ثبت وقایع تشخیص دهد. این مقاله نشان داد که با استفاده از روش‌های شناخته‌شده کنترل کیفیت آماری، می‌توان ناهنجاری را در سیستم اسکادا شناسایی کرد.

۶. مراجع

[1] Miller, B.; Rowe, D. “A Survey SCADA of and Critical Infrastructure Incidents”; Proc. of the 1st ACM Annual Conference on Research in Information Technology 2012, 51-56.

[2] Baracaldo, N.; Joshi, J. “An Adaptive Risk Management and Access Control Framework to Mitigate Insider Threats”; Computers & Security 2013, 39, 237-254.

[3] Legg, P. A.; Moffat, N.; Nurse, J. R.; Happa, J.; Agrafiotis, I.; Goldsmith, M.; Creese, S. “Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection”; Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 2013, 4, 20-37.

[4] Asgarkhani, M.; Sitnikova, E. “A Strategic Approach to Managing Security in SCADA Systems”; Proc. of 13th European Conference on Cyber Warfare and Security 2014, 23-31.

[5] Nicholson, A.; Webber, S.; Dyer, S.; Patel, T.; Janicke, H. “SCADA Security in the Light of Cyber-Warfare”; Computers & Security 2012, 31, 418-436.

[6] Bao, H.; Lu, R.; Li, B.; Deng, R. “BLITHE: Behavior Rule Based Insider Threat Detection for Smart Grid”; IEEE Internet of Things Journal 2016, 3, 190-205.

[7] National Transportation Safety Board “Pipeline Accident Report (No. NTSB/PAR-12/01 PB2012-916501)”; Washington, D.C., National Technical Information Service, 2010.

Igure, V. M.; Laughter, S. A.; Williams, R. D. “Security Issues in SCADA Networks”; Computers & Security 2006, 25, 498-506.

[19] Stouffer, K.; Falco, J.; Scarfone, K. “Guide to Industrial Control Systems (ICS) Security”; NIST Special Publication 2008, 800-882.

[20] Wu, Y.; Kezunovic, M.; Kostic, T. “An Advanced Alarm Processor Using Two-level Processing Structure”; Power Tech. 2007, 125-130.

[21] Lopez, J.; Alcaraz, C.; Roman, R. “Smart Control of Operational Threats in Control Substations”; Computers & Security 2013, 38, 14-27.

[22] Da Silva, A. M. L.; Violin, A.; Ferreira, C.; Machado, Z. S. “Probabilistic Evaluation of Substation Criticality Based on Static and Dynamic System Performances”; IEEE Trans. Power Systems 2014, 29, 1410-1418.

[23] Niroo Research Institute (NRI) “Substation Automation Systems Standard (Transmission & Subtransmission S/S)”; Ministry of Energy of Iran, Tavanir, 2008, (In Persian).

[24] Kondaveeti, S. R.; Izadi, I.; Shah, S. L.; Black, T.; Chen, T. “Graphical Tools for Routine Assessment of Industrial Alarm Systems”; Computers & Chemical Engineering 2012, 46, 39-47.

[25] ANSI/ISA-18.2 “Management of Alarm Systems for the Process Industries”; International Society of Automation, Research Triangle Park, 2009.

[26] Mayadevi, N.; Ushakumari, S. S.; Vinodchandra, S. S. “SCADA-based Operator Support System for Power Plant Equipment Fault Forecasting”; Journal of the Institution of Engineers (India): Series B, 2014, 95, 369-376.

[27] Montgomery, D. C. “Introduction to Statistical Quality Control”; John Wiley & Sons, 2009, 288-344.

[28] Nembhard, D. A.; Nembhard, H. B. “A Demerits Control Chart for Autocorrelated Data”; Quality Engineering 2000, 13, 179-190.

[29] Xin, J.; Shi, D.; Duan, X. “Implementation of Integrative Information Transmission in Substation with DiffServ Network”; Proc. of International Conference on Power System Technology IEEE 2004, 763-767.

[30] Zhao, J.; Xu, Y.; Luo, F.; Dong, Z.; Peng, Y. “Power System Fault Diagnosis Based on History Driven Differential Evolution and Stochastic Time Domain Simulation”; Information Sciences 2014, 275, 13-29.

[31] TMU SPAMLAB, http://www.irancert.ir, 2015.

[8] Barbosa, R. R. R. “Anomaly Detection in SCADA Systems: A Network Based Approach”; University of Twente, 2014.

[9] Garitano, I.; Uribeetxeberria, R.; Zurutuza, U. “A Review of SCADA Anomaly Detection Systems”; Proc. of the 6th International Conference SOCO in Soft Computing Models in Industrial and Environmental Applications 2011, 357-366.

[10] Yoon, M. K.; Ciocarlie, G. F. “Communication Pattern Monitoring: Improving the Utility of Anomaly Detection for Industrial Control Systems”; Proc. of the NDSS Workshop on Security of Emerging Networking Technologies (SENT), 2014.

[11] Zhu, B.; Sastry, S. “SCADA-specific Intrusion Detection/Prevention Systems: a Survey and Taxonomy”; Proc. of the 1st Workshop on Secure Control Systems (SCS), 2010.

[12] Carcano, A.; Fovino, I. “State-Based Network Intrusion Detection Systems for SCADA Protocols: A Proof of Concept”; Proc. of the 4th International Workshop on Critical Information Infrastructures Security (CRITIS'09), 2009, 138-150.

[13] Fovino, I. N.; Carcano, A.; Murel, T. D. L.; Trombetta, A.; Masera, M. “Modbus/DNP3 State-Based Intrusion Detection System”; Proc. of 24th IEEE International Conference on Advanced Information Networking and Applications 2010, 729-736.

[14] Carcano, A.; Coletta, A.; Guglielmi, M.; Masera, M.; Trombetta, A. “A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems”; IEEE Trans. Industrial Informatics 2011, 7, 179-186.

[15] Balducelli, C.; Lavalle, L.; Vicoli, G. “Novelty Detection and Management to Safeguard Information-intensive Critical Infrastructures”; International Journal of Emergency Management 2007, 4, 88-103.

[16] Hadžiosmanović, D.; Bolzoni, D.; Hartel, P. H. “A Log Mining Approach for Process Monitoring in SCADA”; International Journal of Information Security 2012, 11, 231-251.

[17] Hadžiosmanović, D.; Sommer, R.; Zambon, E.; Hartel, P. H. “Through the Eye of the PLC: Semantic Security Monitoring for Industrial Processes”; Proc. of the 30th ACM Annual Computer Security Applications Conference 2014, 126-135.

[18] Bishop, M.; Conboy, H. M.; Phan, H.; Simidchieva, B. I.; Avrunin, G. S.; Clarke, L. A.; Peisert, S. “Insider Threat Identification by Process Analysis”; Proc. of the Security and Privacy Workshops (SPW) 2014, 251-264.