یک سامانهٔ مدیریت دسترسی برای کاهش تهدیدهای عملیاتی در سامانهٔ اسکادا

پیام محمودی نصر[1]* و علی یزدیان ورجانی[2]

[1]دانشگاه مازندران، دانشکده فنی و مهندسی، گروه مهندسی کامپیوتر و فناوری اطلاعات، مازندران، ایران

[2]دانشگاه تربیت مدرس، تهران، ایران

چکیده

حمله به سامانه‌های اسکادا در زیرساخت‌های حیاتی خسارت‌های جبران‌ناپذیری به همراه دارد. در سامانهٔ اسکادا اپراتورها نقش کلیدی داشته، و چنانچه وظایف خود را به‌درستی انجام ندهند، درفرآیندهای جاری شبکه اختلال به‌وجود می‌آید. در این مقاله عملکرد نامناسب اپراتورها در کنترل فرآیندها به‌عنوان تهدیدهای عملیاتی شناخته می‌شوند. یک تهدید عملیاتی هنگامی است که اپراتورهای مجاز با انجام‌ندادن وظایف سازمانی و یا سوءاستفاده از مجوزهای قانونی سعی در ایجاد اختلال در پست‌های راه دور می‌کنند. در این مقاله یک سامانهٔ مدیریت دسترسی مبتنی بر اعتماد برای کاهش تهدیدهای عملیاتی ارائه شده است. در این سامانه سطح دسترسی اپراتور به پست‌ها با توجه به مقدار اعتماد اپراتور و سطح بحرانی‌بودن پست تعیین می‌شود. مقدار اعتماد اپراتور در فواصل زمانی معین و یا هنگام مشاهده ناهنجاری در شبکه به‌روزرسانی می‌شود. سامانهٔ پیشنهادی قادر است تا ناهنجاری‌های به‌وجودآمده را شناسایی کند. نتایج شبیه‌سازی با استفاده از داده‌های شبکهٔ برق ایران نشان می‌دهد که سامانهٔ پیشنهادی از کارایی مناسبی برخوردار است.

واژگان کلیدی: کنترل دسترسی، اعتماد، تهدید خودی، تشخیص ناهنجاری، اسکادا

An Access Management System to Mitigate Operational Threats in SCADA System

Payam Mahmoudi-Nasr*[1] & Ali Yazdian-Varjani[2]

[1]Department of Computer Engineering, University of Mazandaran, Mazandaran, Iran

[2]Tarbiat Modares University, Tehran, Iran

Abstract

One of the most dangerous insider threats in a supervisory control and data acquisition (SCADA) system is the operational threat. An operational threat occurs when an authorized operator misuses the permissions, and brings catastrophic damages by sending legitimate control commands. Providing too many permissions may backfire, when an operator wrongly or deliberately abuses the privileges. Therefore, an access management system is required to provide necessary permissions and prevent malicious usage. 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, we propose a new alarm-trust based access management system reducing the potential of operational threats in SCADA system. In the proposed system, the accessibility of a remote substation will be determined based on the operator trust and the criticality level of the substation. The trust value of the operator is calculated using the performance of the operator, periodically or in emergencies, when an anomaly is detected. The criticality level of the substation is computed using its properties. Our system is able to detect anomalies that may result from the operational threats. The simulation results in the SCADA power system of Iran show effectiveness of our system.

Keywords: Access control, trust, insider threat, anomaly detection, SCADA.

* نویسندهٔ عهده‌دار مکاتبات

* Corresponding author

[DOI: 10.29252/jsdp.14.4.3]

۱- مقدمه

سامانه‌های اسکادا[1] سامانه‌های 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 سامانه‌های اسکادا در زیرساخت‌های حیاتی منجر به بروز حوادث زنجیره‌ای[5] در فعالیت‌های اقتصادی و صنعتی خواهد شد. به همین دلیل تأمین امنیت اسکادا نقش به‌سزایی در تأمین امنیت ملی خواهد داشت. این در حالی است که گزارش‌های دریافتی نشان می‌دهند که سامانه‌های اسکادا در معرض انواع تهدیدها هستند[1].

یکی از تهدیدهای خطرناک در سامانه‌های رایانه‌ای، تهدید کاربران خودی[6] است. این تهدید هنگامی اتفاق می‌افتد که کاربر قانونی یا مهاجمی که به مجوزهای قانونی دسترسی پیدا کرده، با سوءاستفاده از مجوزها و انجام دستورهای قانونی، موجب ایجاد نتیجه‌ای غیرقانونی در سامانه می‌شود [2]. بنا بر پژوهش‌های انجام‌شده ۳۳٪ مجموع حوادث سایبری در سال ۲۰۱۰ [3]، ۲۱٪ حملات در سال ۲۰۱۱ و ۶۰٪ کلاه‌برداری‌ها در سال ۲۰۱۲ [4]، ۳۶٪ حملات گزارش‌شده در سال ۲۰۱۳ [5]، ۲۸٪ حملات سایبری در سال ۲۰۱۴ [6] و ۵۰٪ حملات گزارش‌شده در سال ۲۰۱۵ [7] از نوع حمله خودی بوده، و در سامانه‌های اسکادا ۳۰٪ حملات در سال‌های ۲۰۰۱ تا ۲۰۰۳ [8] و۳۳/۳٪ حملات در سال‌های ۲۰۰۰ تا ۲۰۱۱ [9] از نوع خودی و توسط کاربران ناراضی انجام شده است. بنا بر گزارش [10] ۳۴٪ حملات ثبت‌شده در سال ۲۰۱۳ از نوع حمله خودی بوده است.

یکی از انواع تهدیدهای خودی در سامانهٔ 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 سامانه و افزایش ناهنجاری در شبکه است. در سامانهٔ اسکادا پایش وضعیت سامانه، کنترل فرآیندها، انجام واکنش به‌موقع نسبت به رویدادها و هشدارها و درنهایت کنترل بی‌درنگ قابلیت اطمینان[7] شبکه به عهدهٔ 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 برطرف‌کردن هشدارها، و ارسال دستورهای قانونی اشتباه (عمدی یا غیرعمدی) وظایف خود را به‌درستی انجام ندهند، موجب: (۱) جلوگیری و یا تأخیر در انجام یک فرآیند، (۲) اختلال در فرآیندهای جاری، (۳) شکست یک فرآیند، و یا (۴) انجام یک فرآیند نادرست در سامانه می‌شوند. برای مثال به نشتی خطوط لوله شرکت اینبریج[8] در سال ۲۰۱۰ می‌توان اشاره کرد که به‌واسطه مدیریت نامناسب هشدارها در سامانه اسکادا به‌وجود آمد[11].

در این مقاله یک سامانه مدیریت دسترسی بر پایه هشدار و اعتماد به‌منظور کاهش تهدیدهای عملیاتی در سامانه اسکادا ارائه شده است. در این سامانه فرض بر آن است که با تعیین سطح اعتماد اپراتورها در دسترسی به پست‌ها و کنترل تجهیزات آن، از میزان تهدیدهای عملیاتی کاسته خواهد شد. بدین‌ترتیب که هرچه سطح اعتماد اپراتور بیشتر محاسبه شود، اجازهٔ دسترسی به پست‌های بیشتری برای وی فراهم می‌شود. در سامانهٔ پیشنهادی از میزان بحرانی‌بودن[9] پست‌ها در شبکه به‌عنوان حد آستانه برای دسترسی به آن‌ها استفاده می‌شود. اپراتور به شرطی به یک پست دسترسی خواهد داشت که سطح اعتماد وی از سطح بحرانی‌بودن آن پست بیشتر باشد.

برای محاسبه سطح اعتماد اپراتور، از میزان کارایی[10] وی استفاده شده است. ازآنجایی‌که اپراتورها وظیفه برطرف‌کردن هر چه سریع‌تر هشدارها را به عهده دارند، از نرخ برطرف‌شدن هشدارها به‌عنوان شاخصی برای اندازه‌گیری میزان کارایی اپراتور استفاده شده است. سطح اعتماد اپراتور در فواصل زمانی مشخص و یا در مواقع اضطراری (هنگام شناسایی ناهنجاری)، به‌روزرسانی می‌شود. سامانهٔ پیشنهادی روشی را نیز برای تشخیص ناهنجاری با استفاده از روش‌های کنترل کیفیت آماری[11] ارائه می‌دهد. به‌طور خلاصه نوآوری‌های این مقاله عبارت‌اند از:

[1] Supervisory Control and Data Acquisition (SCADA)
[2] Monitoring
[3] Real-Time
[4] Process
[5] Cascade
[6] Insider threat
[7] Reliability
[8] Enbridge Inc.
[9] Criticality
[10] Performance
[11] Statistical Quality Control

[DOI: 10.29252/jsdp.14.4.3]

(۱) ارائه یک سامانه مدیریت دسترسی برای کاهش تهدیدهای عملیاتی سامانهٔ اسکادا بر پایه سطح کارایی اپراتور و بحرانی‌بودن پست‌ها. در این مقاله برای نخستین بار از مقدار اعتماد اپراتور و سطح بحرانی‌بودن پست‌ها برای تعیین مجوزهای دسترسی به پست‌ها استفاده شده است.

(۲) استفاده از روش‌های شناخته‌شدهٔ کنترل کیفیت آماری برای تشخیص ناهنجاری در سامانه اسکادا.

این مقاله بدین‌صورت ادامه داده می‌شود: بخش دوم مقاله به‌مرور پژوهش های پیشین می‌پردازد. در بخش سوم بحث‌های مقدماتی شامل سامانه اسکادا، تفاوت‌های امنیتی، اپراتور اسکادا و تهدیدهای عملیاتی بررسی شده‌اند. سامانهٔ پیشنهادی برای مدیریت دسترسی اپراتور اسکادا و تشخیص ناهنجاری در بخش چهارم ارائه می‌شود. بخش پنجم نحوهٔ ارزیابی و نتایج شبیه‌سازی را نشان می‌دهد. در بخش ششم نتایج حاصل از این مقاله آورده شده است.

۲- پژوهش‌های پیشین

۲-۱- تشخیص ناهنجاری و تهدیدهای خودی

تاکنون سامانه‌های متعددی برای تشخیص ناهنجاری و جلوگیری از تهدیدهای خودی ارائه شده است. تمرکز برخی بر شناسایی الگوهای غیرتکراری [12]، ویژگی‌های رفتاری و روان‌شناختی [13]، آنالیز ترافیک [14] و غیره است. بر اساس مطالعات انجام‌شده در این مقاله تاکنون هیچ‌یک از کارهای انجام‌شده از آنالیز هشدارها به‌منظور شناسایی ناهنجاری و تهدیدهای خودی استفاده نکرده‌اند. منبع [12] با استفاده از داده‌کاوی فایل ثبت وقایع[1] در سامانه‌های کنترل صنعتی روشی برای تشخیص حمله به فرآیندها در سامانه اسکادا ارائه کرده است. این منبع با بررسی معنایی داده‌های سامانه، الگوهای غیرتکراری در فایل ثبت وقایع را شناسایی می‌کند. محدودیت این روش وابستگی به ثبت رویدادهای ناشی از عملکرد اپراتور در فایل ثبت وقایع است. درحالی‌که روش ارائه‌شده در این مقاله قادر است حتی در صورت عدم واکنش اپراتور به هشدارها، ناهنجاری سامانه را شناسایی کند. روشی روان‌شناختی برای شناسایی تهدیدهای خودی در [13] ارائه شده است. در این روش راه‌کاری ارائه می‌شود تا مهاجم خودی، عملی انجام دهد که به‌موجب آن موردتوجه دیگران و درنتیجه شناسایی قرار گیرد (مانند حذف یک فایل). یک چارچوب[2] تشخیص ناهنجاری برای سامانه‌های کنترل صنعتی با استفاده از مدل مارکوف ترافیک شبکه Modbus در [14] ارائه شده است. مروری مناسب بر روش‌های تشخیص ناهنجاری در سامانهٔ اسکادا در منابع [15] آورده شده است. در منبع [16] برای تشخیص حمله به فرآیندها، از آنالیز ویژگی‌های فرآیند مانند محرمانگی داده‌ها، درستی عملکرد فرآیند، و دسترس‌پذیری نتایج آن استفاده شده است. در منبع [17] نیز یک روش مبتنی بر معنا برای تشخیص حمله به فرآیندهای کنترل‌کننده‌های منطقی برنامه‌پذیر[3] ارائه شده است. این منبع ابتدا با استفاده از داده‌های شبکه، فرآیندهای سامانه را شناسایی کرده و سپس با ایجاد سری‌های زمانی برای هر یک از متغیرهای فرآیند، عملکرد مورد نظر آن فرآیند را در سیستم بررسی می‌کند.

۲-۲- اعتماد و سامانه‌های کنترل دسترسی

درحالی‌که استفاده از روش‌های کنترل دسترسی راهکاری بسیار مناسب برای محدودکردن اپراتور مهاجم و جلوگیری از گسترش تهدیدهای خودی است، در سامانه‌های اسکادا به‌دلیل وجود متغیرهای سامانه‌ای فراوان، از مدل‌های کنترل دسترسی یا به‌هیچ‌وجه استفاده‌نشده و یا به شکل محدودی موردتوجه قرارگرفته‌اند.

تاکنون نسخه‌های توسعه‌یافته متعددی از مدل استاندارد کنترل دسترسی RBAC[4] در کاربردهای مختلف ارائه‌شده، که هیچ‌یک از آن‌ها به‌طور کامل مطابق با نیازمندی‌های سامانهٔ اسکادا نیست. منبع [3] یک چارچوب کنترل دسترسی مبتنی بر اعتماد و ریسک برای کاهش تهدیدهای خودی پیشنهاد کرده است. در این چارچوب ابتدا به هر یک از کاربران و مجوزها به‌ترتیب مقداری از اعتماد و ریسک اختصاص داده می‌شود. در ادامه هر کاربر از میان نقش‌هایی که به وی اختصاص داده شده، تنها نقشی را می‌تواند فعال کند که حد آستانه اعتماد موردنیاز آن از اعتماد کاربر کمتر باشد. حد آستانه اعتماد برای فعال‌کردن یک نقش با توجه به مقدار ریسک مجوزهای نقش تعیین می‌شود. چنانچه برای دسترسی به مجوزها از مجموعه نقش‌های متفاوتی بتوان استفاده کرد، مجموعه‌ای که کمترین ریسک را دارد، انتخاب خواهد شد. برای محاسبه ریسک هر مجموعه نقش از شبکه‌های پتری رنگی[5] استفاده

[1] Log file

[2] Framework
[3] Programmable Logic Controllers (PLC)
[4] Role Based Access Control
[5] Colored Petri Net (CPN)

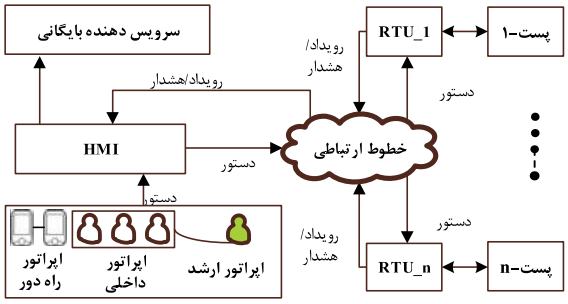
[DOI: 10.29252/jsdp.14.4.3]

شده است. یک روش کنترل دسترسی مبتنی بر اعتماد و وظیفه[1]، برای جلوگیری از تهدیدهای خودی و التزام کاربر به انجام وظایف بعد از دسترسی به مجوزها در [18] ارائه شده است. در این منبع اعتماد کاربر در طول بازه‌های زمانی با توجه به رفتار وی در انجام وظایف بررسی و محاسبه می‌شود. دسترسی کاربر به مجوزها بر اساس مقدار اعتماد اپراتور و سطح بحرانی‌بودن مجموعه وظایف مشخص می‌شود. چنانچه اعتماد کاربر از مقدار بحرانی‌بودن وظایف بیشتر باشد، مجوز دسترسی صادر خواهد شد. در منبع [19] بررسی جامعی در مورد انواع روش‌های محاسبه اعتماد ارائه شده است. یک چارچوب مدیریت کنترل دسترسی بر پایه استاندارد RBAC برای سامانهٔ اسکادا در [20] ارائه شده است. در این منبع از ابزارهای UML[2] و CPN به‌ترتیب برای شناسایی نیازمندی‌ها و قوانین کنترل دسترسی استفاده شده است. تمرکز اصلی این منبع بر استفاده از قابلیت‌های هر یک از ابزارهای بالا بوده و در آن اشاره‌ای به تهدیدهای خودی نشده است. در منبع [21] یک چارچوب مجوزدهی مبتنی بر منطق برای تعریف قوانین امنیتی در سامانه اسکادا پیشنهاد شده است.

۳- پیش‌زمینه

۳-۱- سامانهٔ اسکادا

سامانه‌های اسکادا وظیفه پایش و کنترل بی‌درنگ فرآیندهای شبکه‌های صنعتی را به عهده دارند. در این سامانه‌ها داده‌های اندازه‌گیری‌شده در پست‌ها به‌وسیله RTU[3] جمع‌آوری و از طریق یک شبکهٔ مخابراتی خصوصی و یا عمومی برای مرکز کنترل ارسال می‌شوند. سرویس‌دهنده HMI[4] در مرکز کنترل داده‌های دریافتی را به اپراتورها نمایش داده و برعکس فرمان‌های کنترلی اپراتورها را برای تجهیزات داخل پست‌ها ارسال می‌کند [22]. هرگونه تغییر در شرایط سامانه که نیازمند توجه اپراتورها باشد در قالب یک هشدار اعلام خواهد شد. هنگامی‌که خطا یا خرابی دریکی از تجهیزات شبکه به‌وجود می‌آید، سامانه‌های 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[5] کرده و سپس اقدام مقتضی برای برطرف‌شدن آن(ها) را انجام می‌دهند. تمامی داده‌ها و فرمان‌ها در سرویس‌دهندهٔ بایگانی[6] ذخیره می‌شوند. شکل (۱) ساختار کلی سامانه اسکادا را نشان می‌دهد.



(شکل-۱): ساختار کلی سامانهٔ اسکادا.
(Figure-1): SCADA system architecture.

۳-۲- تفاوت امنیتی با شبکه‌های رایانه‌ای

تفاوت‌های امنیتی مختلفی را بین سامانه‌های رایانه‌ای و کنترل صنعتی ازجمله اسکادا می‌توان بیان کرد. برخی از مهم‌ترین این تفاوت‌ها در جدول (۱) آورده شده که به توضیح تعدادی از آن‌ها می‌پردازیم:

الف) در سامانه‌های کنترل صنعتی ازجمله اسکادا، هرگونه فرمان و اجرای دستور تأثیری مستقیم بر روی دنیای واقعی خواهد گذاشت و این خود عامل مهمی است که موضوع تأمین امنیت را در این‌گونه سامانه‌ها بسیار حساس‌تر نسبت به سامانه‌های رایانه‌ای می‌کند.

ب) سامانه‌های اسکادا بسیار حساس به زمان بوده و به‌صورت بی‌درنگ باید عمل کنند. علت این موضوع آن است که هرگونه تأخیر در برطرف‌کردن هشدارها می‌تواند عاملی برای به‌وجودآمدن هشدارهای زنجیره‌ای[7]، خاموشی شبکه و درنهایت تهدیدی برای زندگی انسان باشد. حساسیت به زمان در سامانه‌های دیگری ازجمله پخش زنده تصاویر و ویدئو نیز مطرح است؛ اما نقض محدودیت‌های زمانی در این‌گونه سامانه‌ها تنها منجر به ازدست‌دادن کیفیت خواهد شد و عامل تخریب کل سامانه و بروز فاجعه در محیط زندگی نخواهد شد. اصطلاحاً این‌گونه سامانه‌ها را سامانه‌های بی‌درنگ نرم و سامانه اسکادا را بی‌درنگ سخت می‌گویند [23].

[1] Obligation
[2] Unified Modeling Language (UML)
[3] Remote Terminal Unit
[4] Human Machine Interface (HMI)
[5] Acknowledge
[6] Historian Server
[7] Cascade

[DOI: 10.29252/jsdp.14.4.3]

ج) تفاوت دیگر وجود حافظه‌های تکه‌تکه‌شده[1] در تجهیزات میدانی است. بسیاری از تجهیزات میدانی اسکادا بدون وقفه و راه‌اندازی مجدد برای مدت‌های طولانی (سال‌ها) به کار خود ادامه می‌دهند. این امر موجب تکه‌تکه‌شدن حافظه آن‌ها می‌شود. به همین دلیل مشکل سرریزی بافر در سامانه‌های اسکادا بسیار مهم‌تر و شایع‌تر نسبت به سامانه‌های رایانه‌ای است.

د) استفاده از سیستم‌عامل‌های بی‌درنگ عامل دیگری برای افزایش آسیب‌پذیری در اسکادا شده است. این امر به علت حساسیت بسیار بالای آن‌ها نسبت به زمان در اختصاص حافظه است.

ه) علاوه‌بر این‌ها موارد دیگری مانند تقاضای دسترسی همیشگی، محدودیت پردازشی و محاسباتی بر روی تجهیزات میدانی، گستره جغرافیایی شبکه و تجهیزات میدانی، تبدیل گسترده سیگنال‌های آنالوگ و دیجیتال به یکدیگر، انواع پارامترهای اجتماعی ازجمله مقاومت اپراتورها در مقابل تغییرات و میل به نگهداری سامانه به‌صورت موروثی و میزان اثربخشی هزینه‌ها عواملی است که موضوع امنیت اسکادا را بسیار پیچیده می‌کند [23].

(جدول-۱) : تفاوت امنیتی سامانه اسکادا با سامانه‌های کامپیوتری.
(Table-1): Security differences between SCADA & computer systems.

عنوان	گروه	شبکه‌های کامپیوتری	سامانه‌های اسکادا
فن‌آوری	طول عمر تجهیزات	۳ تا ۵ سال	۱۵ تا ۲۰ سال
	سیستم‌عامل	سیستم‌عامل‌های معمولی و مرسوم مانند Windows	سیستم عامل‌های بی‌درنگ یا اختصاصی
	پروتکل شبکه	پروتکل‌های معمولی	معمولی یا اختصاصی (Profibus, Modbus, DNP3)
	محدودیت منابع (مانند حافظه)	بدون محدودیت منابع	محدودیت برای اجرای هرگونه سرویس اضافه
عملکرد	تمرکز امنیتی	سرویس‌دهنده‌های مرکزی و داده‌ها	پردازش‌ها در تجهیزات میدانی
	نیازمندی‌های امنیتی (به ترتیب)	محرمانگی، تمامیت داده، دسترس‌پذیری	دسترس‌پذیری، تمامیت داده، محرمانگی
	واکنش بی‌درنگ	اندک	بسیار زیاد
	به‌روزرسانی نرم‌افزارها	به‌صورت دوره‌ای انجام می‌شود.	به‌ندرت اتفاق می‌افتد.

[1] Fragmented

۳-۳- اپراتورهای اسکادا

در سامانه اسکادا اپراتورها نقش کلیدی داشته و بر اساس دستورالعمل‌های ثابت بهره‌برداری وظیفه (۱) کنترل و نظارت بر فرآیندها، (۲) واکنش به‌موقع نسبت به رویدادها و هشدارها، و (۳) صدور فرمان‌های کنترلی به‌منظور حفظ قابلیت اطمینان سامانه را به عهده دارند. 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 برطرف‌کردن آن هشدار می‌کنند. هرگونه تأخیر و اشتباه اپراتور خسارت‌های جبران‌ناپذیری می‌تواند به همراه داشته و قابلیت اطمینان سامانه 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 سامانه (۱) به‌طورمعمول از روش‌های هوشمند پردازش هشدار[2] مانند اولویت‌بندی و فیلترکردن هشدارها، و (۲) تیم اپراتوری در هر نوبت‌کاری استفاده می‌شود. از میان اپراتورها، اپراتوری که از مهارت بیشتری برخوردار است، به‌عنوان اپراتور ارشد مسئولیت نظارت بر عملکرد اپراتورهای دیگر را به عهده دارد.

۴-۳- تهدیدهای عملیاتی

تهدیدهای اسکادا را به دو گروه تهدیدهای خودی (داخلی) و غیرخودی (خارجی) می‌توان تقسیم کرد. تهدیدهای غیرخودی توسط کاربران غیرمجاز و خارج از سامانه مانند هکرها و دولت‌های متخاصم انجام شده، 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 [24]. این امر به‌دلیل آن است که کاربران خودی (۱) دسترسی فیزیکی و قانونی به تجهیزات دارند، (۲) دانش کافی از سامانه‌های رایانه‌ای و نرم‌افزارهای مربوطه دارند، و از همه مهم‌تر (۳) از قوانین و سامانه‌های امنیتی لحاظ‌شده آگاهی دارند.

[2] Intelligent alarm processing

[DOI: 10.29252/jsdp.14.4.3]

تهدیدهای عملیاتی یکی از انواع تهدیدهای خودی در سامانه اسکادا است. این تهدید هنگامی رخ می‌دهد که اپراتور (۱) وظایف خود را بر اساس دستورالعمل‌های ثابت بهره‌برداری به‌درستی انجام نمی‌دهد (عمدی و یا غیرعمدی)، (۲) با سوءاستفاده از مجوزهای قانونی موجب ایجاد اختلال و شکست فرآیندها می‌شود، (۳) به‌طور غیرعمدی مرتکب اشتباه در کنترل فرآیندها سیستم می‌شود. بر این اساس 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.

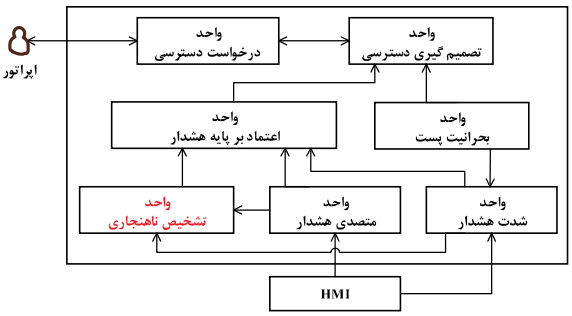
۴- سامانهٔ پیشنهادی مدیریت دسترسی اپراتور

در این بخش یک سامانهٔ مبتنی بر اعتماد و هشدار به‌منظور مدیریت دسترسی اپراتور به پست‌ها ارائه خواهد شد. هدف این سامانه کاهش دسترسی اپراتورهای کم‌تجربه (یا مهاجم) به پست‌های راه دور بر اساس سطح بحرانی‌بودن پست‌ها است. در این سامانه هنگامی اپراتور مجوز دسترسی به یک پست را دارد که مقدار اعتماد وی ($T^{op} \in [0,1]$) از سطح بحرانی‌بودن پست ($CR_{Sub} \in [0,1]$) بیشتر باشد.

قانون دسترسی: اگر $T^{op} > CR_{Sub}$ آنگاه دسترسی ***مجاز*** و در غیر این صورت دسترسی ***غیرمجاز*** است.

در این سامانه به هر اپراتور op یک مقدار اعتمادِ مبتنی بر هشدار در زمان t اختصاص داده می‌شود. چنانچه $(T^{op}, t) = 0$ باشد، اپراتور غیرقابل‌اعتماد است و هنگامی‌که $(T^{op}, t) = 1$ است اپراتور به‌طورکامل قابل‌اعتماد بوده و به‌تمامی پست‌ها در محدوده تحت مسئولیت خود دسترسی خواهد داشت. فرض بر این است که محدوده تحت مسئولیت اپراتور ازقبل توسط اپراتور ارشد تعیین شده است. مقدار اعتماد اولیه اپراتور برابر با یک ($T^{op}_{init} = 1$) فرض می‌شود. بدین ترتیب اپراتور به‌تمامی پست‌های تحت مسئولیت خود در ابتدا دسترسی دارد.

شکل (۲) ساختار سامانهٔ پیشنهادی را نشان می‌دهد.



(شکل-۲): ساختار سامانهٔ پیشنهادی مدیریت دسترسی.
(Figure-2): The structure of the proposed system of access management.

واحد اعتمادبر پایه‌هشدار وظیفه تعیین مقدار اعتماد اپراتورها را به عهده دارد. مقدار اعتماد اپراتور با توجه به مقدار کارایی وی در کنترل پست‌ها محاسبه می‌شود. ازآنجایی‌که اپراتورها درصدد برطرف‌کردن هر چه سریع‌تر هشدارها می‌باشند، مقدار کارایی آن‌ها می‌تواند با توجه به توانایی آن‌ها در برطرف‌کردن هشدارها تعیین شود. به‌عبارت دیگر هرچه اپراتور در برطرف‌کردن هشدار از توانایی بیشتری برخوردار باشد، از اعتماد بیشتری برای کنترل پست‌ها برخوردار خواهد بود. این در حالی است که تهدیدهای عملیاتیِ اپراتور موجب افزایش تعداد هشدارها برطرف‌نشده در سامانه شده و درنتیجه باعث کاهش مقدار اعتماد اپراتور می‌شود. واحد متصدیِ هشدار وظیفه تعیین وضعیت هشدارها را به عهده دارد. در مورد وضعیت هشدارها در بخش‌های بعدی توضیح داده خواهد شد. هرگاه واحد تشخیصِ ناهنجاری یک ناهنجاری را در سامانهٔ شناسایی کند، آن را به واحد اعتمادبر پایه‌هشدار اعلام کرده تا مقدار اعتماد اپراتور به‌روزرسانی شود. مقدار اعتماد اپراتور به‌تناوب در فواصل زمانی معین و یا هنگام تشخیص ناهنجاری به‌روزرسانی می‌شود. واحد درخواستِ دسترسی، مترصد دریافت درخواست اپراتور برای دسترسی به پست‌ها بوده و آن را برای واحد تصمیم‌گیریِ دسترسی ارسال می‌کند. این واحد درخواست موردنظر را با توجه به مقدار اعتماد اپراتور ارزیابی کرده و نتیجه را در غالب اجازه و یا عدم اجازه دسترسی به واحد درخواستِ دسترسی اعلام می‌دارد. واحد بحرانیتِ پست وظیفه محاسبه سطح بحرانی‌بودن پست‌ها را

[1] Ignore

[DOI: 10.29252/jsdp.14.4.3]

به عهده دارد. واحد شدتِ هشدار نیز وظیفه تعیین سطح شدت هشدارها را به عهده دارد.

لازم به ذکر است که در سامانهٔ پیشنهادی تنها مقدار اعتماد اپراتورها به‌روزرسانی می‌شود و فرض بر آن است که اپراتور ارشد همواره دسترسی کامل به‌تمامی پست‌ها را در حوزه تحت مسئولیت خود دارد. در سامانهٔ پیشنهادی هرگاه سطح دسترسی اپراتوری به یک پست تغییر کند، گزارش مربوطه به اطلاع اپراتور ارشد خواهد رسید. این گزارش جهت انجام اقدام مقتضی توسط اپراتور ارشد (مانند تغییر محدوده تحت مسئولیت اپراتور، نظارت بیشتر به عملکرد اپراتور، و از همه مهم‌تر کنترل پست‌هایی که به‌طورموقت از دسترسی اپراتور خارج‌شده‌اند) مورداستفاده قرار خواهد گرفت.

۴-۱- تعیین سطح بحرانی‌بودن پست

اگرچه از روش‌های ارائه‌شده در مقاله‌های دیگر مانند [25] برای رتبه‌بندی سطح بحرانی بودن پست‌ها می‌توان استفاده کرد، در این مقاله روشی جدید بر اساس ویژگی‌های پست (مانند ظرفیت، اهمیت در شبکه، تعداد فیدرهای ورودی/خروجی، موقعیت جغرافیایی و غیره) برای تعیین سطح بحرانی‌بودن پست‌ها ارائه شده 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 n تعداد پست‌ها باشد. چنانچه $g_{p_{ij}} \in [0,1]$ امتیاز کسب‌شده پست iام برای ویژگی p_j باشد، سطح بحرانی‌بودن پست با استفاده از رابطه زیر محاسبه خواهد شد:

$$CR_{sub_i} = \frac{\sum_{j=1}^{k} w_{p_j}.g_{p_{ij}}}{\max\limits_{1\le i\le n} \sum_{j=1}^{k} w_{p_j}.g_{p_{ij}}} \qquad (۱)$$

در این رابطه CR_{sub_i} عبارت است از نسبت امتیاز کسب‌شده پست iام به بیشینهٔ امتیاز کسب‌شده پست‌ها در شبکه.

۴-۲- تعیین سطح شدت هشدار

سطح شدت هر هشدار متناسب با نوع هشدار و سطح بحرانی‌بودن پستی که هشدار در آن اتفاق افتاده تعیین می‌شود. از معیارهای متفاوتی مانند مدت‌زمان پاسخ‌گویی، شدت پیامدها، محل وقوع، تجهیز عامل، و ... برای گروه‌بندی و تعیین نوع هشدارها می‌توان استفاده کرد. فرض کنید هشدارها به m نوع $L = \{l_1, l_2, \dots, l_m\}$ گروه‌بندی‌شده باشند. چنانچه $w_{l_j} \in [0,1]$ با فرض $\sum_{j=1}^{m} w_{l_j} = 1$ وزن نوع هشدار l_j باشد سطح شدت هر یک از هشدارهای نوع l_j از پست iام به‌صورت زیر محاسبه خواهد شد.

$$Sev_{ij} = CR_{sub_i}.W_{l_j} \qquad (۲)$$

۴-۳- محاسبه اعتماد اپراتور

آنچه مطلوب سامانهٔ پیشنهادی است آن است که در محاسبه مقدار اعتماد اپراتور راهکاری ارائه شود تا (۱) چنانچه به‌علت اشتباه غیرعمدی میزان ناهنجاری شبکه افزایش یافته و درنتیجه از اعتماد اپراتور کاسته شد، فرصت جبران (افزایش اعتماد) به وی داده شود، (۲) علاوه‌بر کارایی جاری به سابقهٔ کارایی اپراتور نیز توجه شود.

در این سامانه کارایی اپراتور بر اساس توانایی وی در برطرف‌کردن هشدارها تعیین شده است. می‌دانیم هنگامی‌که هشداری در مرکز کنترل دریافت می‌شود، ابتدا در وضعیت بلاتکلیف[1] است تا توسط اپراتور ابتدا تصدیق و سپس برطرف شود؛ لذا کارایی اپراتور را در هر بازه زمانی با توجه به تعداد هشدارهای برطرف‌شده و برطرف‌نشده (بلاتکلیف و تصدیق‌شده) در محدوده پست‌های تحت کنترل وی می‌توان محاسبه کرد. در هر نوبتِ بازرسی از عملکرد اپراتور، تعدادی هشدار برطرف‌شده و برطرف‌نشده وجود دارد. فرض بر آن است که بازرسی‌ها در فواصل زمانی منظم (که توسط اپراتور ارشد تعیین می‌شود، به‌عنوان مثال هفتگی یا ماهانه) و یا در مواقع اضطراری (هنگام تشخیص ناهنجاری) انجام می‌شوند. فرض کنید در بازرسی o به ترتیب R_{ij} و U_{ij} تعداد هشدارهای برطرف‌شده و برطرف‌نشده از نوع l_j در پست iام باشند. چنانچه m تعداد انواع هشدارها و n تعداد پست‌ها باشد، مقدار کارایی اپراتور op با استفاده از فرمول زیر محاسبه خواهد شد:

$$SP^{op}[o] = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} Sev_{ij}.R_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{m} Sev_{ij}.(R_{ij}+U_{ij})} \qquad (۳)$$

در این فرمول کارایی اپراتور در بازه زمانی مربوط به بازرسی o و با استفاده از نسبت مجموع شدت هشدارهای برطرف‌شده به مجموع شدت تمامی هشدارهای دریافتی در حوزه تحت مسئولیت اپراتور محاسبه شده است. چنانچه اپراتور هیچ‌یک از هشدارهای دریافتی را به‌موقع برطرف نکند مقدار کارایی وی برابر صفر، و برعکس چنانچه تمامی هشدارها به‌موقع برطرف شوند، مقدار کارایی برابر یک خواهد بود.

[1] Pending

[DOI: 10.29252/jsdp.14.4.3]

به‌منظور درنظرگرفتن سابقه کارایی در محاسبه اعتماد اپراتور از رابطه میانگین موزون متحرک نمایی[1] [26] به‌صورت زیر می‌توان استفاده کرد:

$$T_i^{op} = (1-\alpha).T_{i-1}^{op} + \alpha.SP^{op}[o_i] \qquad (۴)$$

در این رابطه T_{i-1}^{op} میانگین وزنی کارایی‌های قبلی و $\alpha \in [0,1]$ ضریب کارایی جاری است. چنانچه از دو مقدار متفاوت α_1 و α_2 در این رابطه استفاده شود، امکان جریمه اپراتور هنگام مشاهده ناهنجاری وجود دارد. بدین ترتیب که اگر $\alpha_1 < \alpha_2$ باشد، چنانچه هنگام مشاهده ناهنجاری از مقدار α_2 ، و در غیر این صورت از مقدار α_1 استفاده شود، سرعت کاهش اعتماد اپراتور بیشتر از افزایش آن خواهد بود.

تفاوت کارایی جاری نسبت به سابقه کارایی اپراتور به‌صورت زیر قابل‌محاسبه است:

$$D_i^{op} = SP^{op}[o_i] - T_{i-1}^{op} \qquad (۵)$$

اگر $D_i^{op} \geq 0$ باشد، اپراتور کارایی خود را نسبت به قبل افزایش داده، و برعکس هنگامی‌که $D_i^{op} < 0$ است مقدار کارایی اپراتور نسبت به قبل کمتر شده است. چنانچه بخواهیم از نوسان‌های زیاد مقدار اعتمادِ اپراتور جلوگیری به عمل‌آوریم، بهتر است از رابطه زیر برای محاسبه اعتماد استفاده کنیم:

$$\begin{cases} T_i^{op} = T_{i-1}^{op}, & \text{in periodically observations} \\ & \text{if } D_i^{op} < 0 \\ T_i^{op} = (1-\alpha).T_{i-1}^{op} + \alpha.SP^{op}[o_i], & \text{otherwise} \end{cases} \qquad (۶)$$

استفاده از رابطه (۶) باعث می‌شود تا مقدار اعتمادِ اپراتور تنها در شرایط تشخیص ناهنجاری کاهش یابد. به‌عبارت دیگر این فرصت به اپراتور داده شده است تا قبل از تشخیص ناهنجاری در سامانه، از دسترسی وی کاسته نشود و امکان برطرف‌کردن هشدارها را داشته باشد. بخش نخست رابطه تنها در بازدیدهای دوره‌ای یعنی زمانی که گزارشی از ناهنجاری در سیستم مشاهده نشده و در شرایطی که سابقه کارایی اپراتور منفی است استفاده می شود.

۵- 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 سامانهٔ اسکادا ثبت می‌شود. چنانچه اپراتور بتواند هشدار(ها) را به‌موقع برطرف نماید به معنای برطرف‌شدن اختلال یا خطای ایجادشده است؛ اما اگر هشدار(ها) برطرف نشود، اختلال یا خطا همچنان در شبکه باقی‌مانده است؛ لذا از هشدارهای برطرف‌نشده به‌عنوان شاخصی برای تعیین شدت خطای موجود در شبکه می‌توان استفاده کرد.

برای تعیین شدت خطایی که وابسته به تهدیدهای عملیاتی اپراتور است، ضروری است تا فرصت کافی برای برطرف‌شدن 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. فرصت زمان موردنیاز برای برطرف‌شدن هر هشدار (که در این مقاله با عنوان *فرصتِ هشدار* شناسایی می‌شود)، مقداری متغیر و متفاوت از دیگر هشدارها می‌تواند باشد. بحث بیشتر در مورد فرصتِ هشدار در بخش بعدی آمده است. هنگامی‌که هشداری در مرکز کنترل نمایش داده می‌شود، ضروری است تا اپراتور قبل از اتمام فرصتِ هشدارِ از پیش تعیین‌شده آن را برطرف کند. چنانچه هشداری در فرصتِ تعیین‌شده برطرف نشود به‌عنوان یک *هشدارِ طولانی* در سامانه شناخته خواهد شد. در این مقاله شدت خطای وابسته به تهدیدهای عملیاتی اپراتور (که با متغیر AoCI نشان داده می‌شود) با استفاده از مجموع شدت هشدارهایِ طولانی اندازه‌گیری می‌شود. در شرایط عادی هنگامی‌که شبکه تحت کنترل است، اپراتور در اسرع وقت اقدام به برطرف‌کردن هشدارها می‌کند، لذا مقدار AoCI به‌طورمعمول صفر و یا نزدیک به صفر است. چنانچه مقدار AoCI از حد آستانه (UCL) خارج شود، به‌عنوان شرایط ناهنجار در سامانه شناسایی و اعلام می‌شود.

توجه به این نکته ضروری است که مقدار AoCI در دو صورت از حد آستانه خارج می‌شود: (۱) تهدیدهای عملیاتی (۲) سیلِ هشدار[2]. سیلِ هشدار هنگامی ایجاد می‌شود که یک یا تعدادی خطا در شبکه منجر به جاری‌شدن سیل‌آسای هشدارهای زنجیره‌ای به ترتیبی می‌شوند که اپراتور فرصت کافی برای برطرف‌کردن آن‌ها را ندارد. هشدارهای سیل‌آسا شرایطی را ایجاد می‌کنند که حتی اپراتورهای باتجربه قادر به برطرف‌کردن آن‌ها و شناسایی عامل خطا نمی‌باشند. بر اساس استاندارد نرخ ایجاد

[1] Exponentially Weighted Moving Average (EWMA)

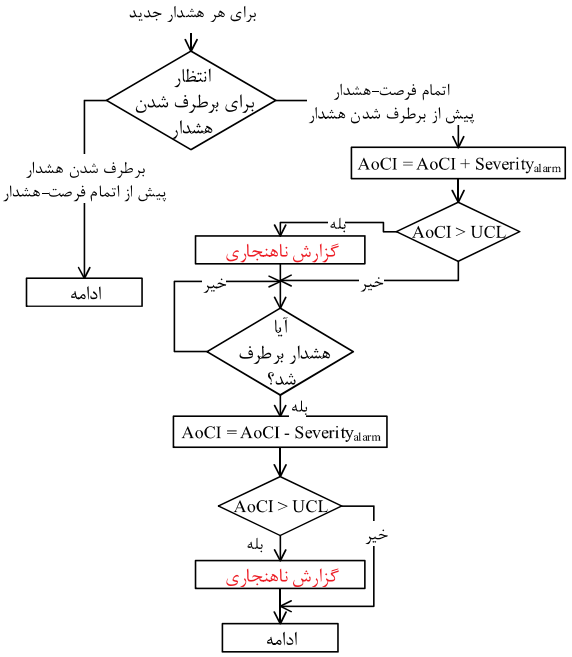
[2] Alarm flooding

[DOI: 10.29252/jsdp.14.4.3]

ده هشدار در ده دقیقه برای هر اپراتور به‌عنوان شرایط سیلِ هشدار شناسایی می‌شود[27].

در سامانهٔ پیشنهادی بایستی راهکاری برای تمایز بین شرایط سیلِ هشدار و تهدیدهای عملیاتی فراهم گردد. زیرا در شرایط سیلِ هشدار اگرچه مقدار AoCI افزایش می‌یابد اما سامانه نباید هیچ‌گونه محدودیتی برای اپراتورها در کنترل پست‌ها ایجاد کند. خوشبختانه امروزه برای جلوگیری از ایجاد شرایط سیل-هشدار در اغلب سامانه‌های اسکادا از روش‌های هوشمند پردازش هشدار استفاده می‌شود[28]. یک پردازنده هوشمند هشدار[1] قادر است تا علاوه‌بر کاهش تعداد هشدارهای نمایش داده‌شده به اپراتور، راه‌کارهای مناسب برطرف‌شدن هشدار را نیز به وی پیشنهاد دهد. بنابراین چنانچه سامانه اسکادا مجهز به یک پردازنده هوشمند هشدار باشد، تهدید عملیاتی تنها عامل افزایش مقدار AoCI و خارج‌شدن آن از حد آستانه خواهد بود.

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



(شکل-۳): شناسایی ناهنجاری به‌صورت بی درنگ.

(Figure-3): Real time anomaly detection.

متغیر AoCI با شروع از مقدار صفر و متناسب با شدت هشدارها تغییر می‌کند. مقدار AoCI هنگامی‌که هشداری در فرصتِ هشدارِ از پیش تعیین‌شده برطرف نشود افزایش، و هنگامی‌که یک هشدارِ طولانی برطرف شود کاهش می‌یابد. به‌عبارت دیگر در هر نوبت بازرسی مقدار AoCI با استفاده از مجموع وزنی تعداد هشدارهایِ طولانی به‌صورت زیر محاسبه می‌شود:

$$AoCI_k = \sum_{i=1}^{n}\sum_{j=1}^{m} Sev_{ij} \cdot C_{ijk} \qquad (۷)$$

در این فرمول Sev_{ij} شدت هشدار، C_{ijk} تعداد هشدارهایِ طولانی از نوع l_j در پست iام، n تعداد پست‌ها، m تعداد انواع هشدارها، و k شماره نوبت بازرسی است. هنگامی‌که مقدار $AoCI_k$ از حد آستانه خارج شود، شرایط ناهنجاری شناسایی‌شده و به سامانهٔ مدیریت کنترل دسترسی به‌منظور تغییر در مقدار اعتماد اپراتور اعلام خواهد شد.

۱-۵- تخمین فرصتِ هشدار

در سامانهٔ پیشنهادی فرصتِ هشدار برای هر هشدارِ از نوع l_j (که با RST_j نمایش داده می‌شود) به‌صورت زیر تخمین زده می‌شود. فرض کنید زمان سپری‌شده از هنگام ظاهرشدن یک هشدار در صفحه HMI تا هنگام برطرف‌شدن آن (به‌عنوان یک مقدار نمونه RST_j) با متغیر $SampleRST_j$ نشان داده شود. پرواضح است که مقدار نمونه $SampleRST_j$ از هر هشدار به هشدار دیگر متناسب با شرایط سامانه و رفتار اپراتور تغییر خواهد کرد. ازآنجاکه آخرین نمونه‌های اندازه‌گیری‌شده گویای شرایط جاری سیستم می‌باشند از رابطه متحرک موزون نمایی به‌منظور تعیین مقدار میانگین RST_j می‌توان استفاده کرد:

$$EstimatedRST_j = (1-\beta)EstimatedRST_j + \beta.SampleRST_j \qquad (۸)$$

در این رابطه $EstimatedRST_j$ مقدار میانگین فرصتِ هشدارِ از نوع l_j و β ضریب آخرین نمونه است. با محاسبه قدرمطلق تفاضل بین $SampleRST_j$ و $EstimatedRST_j$ مقدار تفاوت هر نمونه اندازه‌گیری‌شده از مقدار متوسط فرصتِ هشدار به دست می‌آید. رابطه (۹) نحوه محاسبه میانگین تغییرات RST_j را با استفاده از رابطه متحرک موزون نمایی نشان می‌دهد:

$$DevRST_j = (1-\gamma)DevRST_j + \gamma.\left|SampleRST_j - EstimatedRST_j\right| \qquad (۹)$$

درنهایت برای محاسبه مقدار فرصتِ هشدار از رابطه (۱۰) می‌توان استفاده کرد:

$$RST_j = EstimatedRST_j + \rho.DevRST_j \qquad (۱۰)$$

[1] Intelligent alarm processor

[DOI: 10.29252/jsdp.14.4.3]

در روابط (۹) و (۱۰)، γ ضریب اختلاف بین $EstimatedRST_j$ و $SampleRST_j$، و ρ ضریب متوسط تغییرات RST_j است. بدین ترتیب هنگامی یک هشدارِ از نوع l_j به‌عنوان یک هشدارِ طولانی شناخته خواهد شد که در فرصتِ هشدارِ RST_j برطرف نشود.

۲-۵- تعیین حدود کنترلی

به‌منظور آنالیز متغیر AoCI و تعیین حدود کنترلی از روش‌های کلاسیک کنترل کیفیت آماری برای کنترل عدم انطباق‌ها[1] [26] (مانند انواع نمودارهای C, U, P, D) می‌توان استفاده کرد. در این نمودارها حدود کنترلی در شرایطی تعیین می‌شوند که داده‌های جمع‌آوری‌شده متعلق به شرایط کنترل و پایدار سامانه باشند. در این مقاله هر هشدارِ طولانی به‌مثابه یک خرابی و یا عدم انطباق در یک فرآیند تولیدی و یا پردازشی فرض شده است. با توجه به آنکه مقدار ناهنجاری هر هشدارِ طولانی متناسب با شدت آن متفاوت است، ضروری است تا از نمودار کنترل نقص[2] برای تعیین حدود کنترلی استفاده شود. لازمه استفاده از این نمودار آن است که توزیع آماری نقص‌ها (ترافیک هشدارهایِ طولانی) مطابق با توزیع پوآسون باشد. در فرآیندهای تولیدی و پردازشی به‌طورمعمول فرض بر آن است که توزیع آماری تعداد نقص‌ها مطابق با توزیع پوآسون است. به‌طور مشابه بسیاری از منابع مانند [29] از توزیع پوآسون برای مدل‌سازی ترافیک داده‌های اسکادا استفاده کرده‌اند. در سامانه‌های اسکادا ازآنجایی‌که (۱) احتمال وقوع هشدار در هر یک از منابع کم است و (۲) تعداد منابع بالقوه تولید هشدار به‌دلیل بزرگی و گستردگی شبکه در زیرساخت‌های حیاتی به‌اندازه کافی زیاد است، از توزیع پوآسون برای مدل‌سازی ترافیک هشدارها می‌توان استفاده کرد؛ لذا با فرض آنکه متغیر $AoCI_k$ در رابطه (۷) یک ترکیب خطی از متغیرهای تصادفی مستقل با توزیع پوآسون باشد، مقدار میانگین ناهنجاری با استفاده از رابطه زیر قابل‌محاسبه است:

$$\overline{AoCI} = \ \overline{U} = \sum_{i=1}^{n}\sum_{j=1}^{m} Sev_{ij} \,.\, \bar{u}_{ij} \qquad (۱۱)$$

در این رابطه $\bar{u}_{ij}$ میانگین تعداد هشدارهایِ طولانی برای هر نوع هشدار l_j در پست iام است ($\bar{u}_{ij} = \sum_{k=1}^{N} C_{ijk}/N$ که N مجموع تعداد بازرسی‌ها است).

[1] Nonconformities
[2] Demerit Control Charts (D-chart)

درنهایت حدود کنترلی بالا (UCL) و پایین (LCL) به‌صورت زیر محاسبه خواهند شد:

$$\mathrm{UCL} = \overline{U} + \varphi.\hat{\sigma}_U \,,\ \mathrm{LCL} = \overline{U} - \varphi.\hat{\sigma}_U \qquad (۱۲)$$

$$\hat{\sigma}_U = \sqrt{\sum_{i=1}^{n}\sum_{j=1}^{m} Sev_{ij}^2 \,.\, \bar{u}_{ij}} \qquad (۱۳)$$

در روابط بالا $\hat{\sigma}_U$ انحراف معیار و φ ضریب انحراف معیار است و مقدار آن به‌طورمعمول برابر دو (برای حد اخطار) و یا سه (برای حد نهایی) در نظر گرفته می‌شود [26]. ازآنجاکه هر چه تعداد هشدارها کمتر باشد، شبکه از قابلیت اطمینان بیشتر برخوردار است، مقدار حد آستانه پایین را برابر با صفر می‌توان قرار داد (LCL=0).

۶- راستی‌آزمایی و نتایج شبیه‌سازی

در این بخش به‌منظور آنالیز روش پیشنهادی، دو سناریوی کنترل شبکه و حمله به شبکه موردمطالعه قرارگرفته‌اند. داده‌های موردنیاز سناریوها از سامانه اسکادای شبیه‌سازی‌شده در آزمایشگاه امنیت اسکادای سامانه‌های قدرت دانشگاه تربیت مدرس [30] بر اساس داده‌های بخشی از شبکه برق ایران تهیه شده‌اند. جدول (۲) ویژگی‌های درنظرگرفته‌شده برای هر یک از پست‌ها انتقال و فوق توزیع، و معیار وزن‌دهی آن‌ها را نشان می‌دهد. در جدول (۳) مقدار بحرانی‌بودن پست‌های شبیه‌سازی‌شده با استفاده از ویژگی‌های جدول (۲) و رابطه (۱) نشان داده شده است. به‌منظور تعیین مقدار فرصتِ هشدار برای هر یک از انواع هشدارها و حدود کنترلی، داده‌های اولیه در شرایطی جمع‌آوری شده‌اند که سامانه در حالت پایدار و تحت کنترل کامل اپراتور بوده است. شکل (۴) نمودار تغییر ناهنجاری (متغیر AoCI) را برای داده‌های جمع‌آوری‌شده طی دو سال در شرایط پایدار سامانه 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).

فرض‌های دیگری که در انجام سناریوها در نظر گرفته شده‌اند، عبارت‌اند از: (۱) فاصله زمانی بازرسی‌ها یک‌ماهه در نظر گرفته شده است. (۲) هشدارها به دو گروه اصلی[3] و فرعی[4] تقسیم شده‌اند. (۳) به‌منظور جلوگیری از نوسان زیاد در دسترسی اپراتور به پست‌ها، مقدار اعتماد اپراتور تنها

[3] Major
[4] Minor

[DOI: 10.29252/jsdp.14.4.3]

هنگام مشاهده ناهنجاری کاهش پیداکرده است. (۴) مقادیر پارامترهای درنظرگرفته‌شده عبارت‌اند از: $w_{l_{mi}} = 0.64$ برای هشدارهای فرعی، $w_{l_{mj}} = 0.36$ برای هشدارهای اصلی، $\alpha_1 = 0.125$، $\alpha_2 = 0.33$، $\gamma = \beta = 0.125$، $\varphi =$ $\rho = 2$. (۵) برای جلوگیری از سیلِ هشدارها از سامانه‌های هوشمند پردازش هشدار استفاده می‌شود. (۶) اپراتور ارشد با دیگر اپراتورها در تهدیدهای عملیاتی همدستی نمی‌کند. (۷) هیچ‌گونه تغییری در داده‌های دریافتی به‌منظور فریب سامانه اعمال نمی‌شود.

(جدول-۲): معیار وزن دهی برای تعیین بحرانیت پست ها [21].

(Table-2): Weighting criteria to determine the criticality of substations [21].

P_j	w_{p_j}	توضیحات	معیار وزن دهی	وزن
P_1	۰/۵	ظرفیت ایستگاه (مگاولت آمپر)	ظرفیت ترانس ها ≤۵۰۰ (انتقال) ظرفیت ترانس ها ≤۵۰(فوق توزیع)	۱
			ظرفیت ترانس ها >۵۰۰ (انتقال) ظرفیت ترانس ها >۵۰(فوق توزیع)	/۵
P_2	۰/۵	تعداد ترانسفورماتور	تعداد ترانس ها <۲ عدد	۱
			تعداد ترانس ها ≥۲ عدد	/۵
			کلیدخانه	/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	تعدا فیدرهای ورودی/ خروجی	تعداد< ۱۰ عدد	۱
			۱۰≤ تعداد <۴ (انتقال) ۱۰≤ تعداد <۲ (فوق توزیع)	/۵
			تعداد ≥ ۴ عدد (انتقال) تعداد ≥ ۲عدد (فوق توزیع)	۰
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

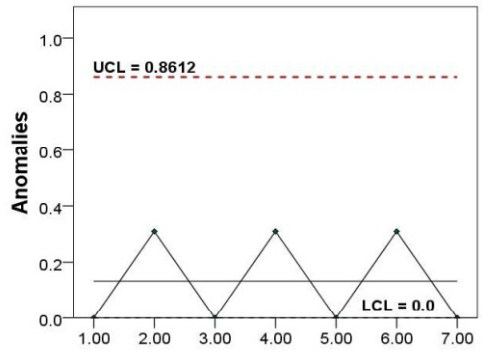
۱-۶- سناریوی حمله

به‌منظور آنکه نشان دهیم در تهدیدهای عملیاتی سامانهٔ پیشنهادی قادر به شناسایی ناهنجاری و کاهش دسترسی اپراتور به پست‌ها است، این سناریو موردمطالعه قرارگرفته است. در این سناریو اپراتور پس‌ازآنکه مقدار اعتماد اولیه‌اش به میزان بیشینه فرض شده است $(T^{op}, t) = 1$، اقدام به یک حمله عملیاتی می‌کند. هر چه تعداد هشدارهایِ طولانی در سامانه اضافه می‌شود، مقدار ناهنجاری نیز افزایش می‌یابد. جدول (۴) و شکل (۵-الف) نشان می‌دهند که نخستین ناهنجاری، هنگامی شناسایی می‌شود که مقدار ناهنجاری به‌میزان ۲/۱۴ افزایش‌یافته و از حد آستانه خارج شده است.

(جدول-۳): سطح بحرانی‌بودن پست‌ها.

(Table-3): The criticality of substations.

عنوان	پست ها					
	A	B	C	D	E	F
P_1	۰/۵	۰/۵	۰/۵	۰/۲۵	۰/۵	۰/۵
P_2	۰/۵	۰/۲۵	۰/۵	۰/۵	۰/۵	۰/۲۵
P_3	۰/۵	۰/۵	۰/۲۵	۰/۵	۰	۰
P_4	۰/۵	۰/۵	۰/۵	۰/۵	۰/۵	۰
P_5	۰/۵	۰/۵	۰/۵	۰/۵	۰/۵	۰/۲۵
P_6	۱	۰/۷۵	۰/۶۲	۱	۰/۷۵	۰/۷۵
جمع امتیاز	۳/۵	۳	۲/۸۷	۳/۲۵	۲/۷۵	۱/۷۵
بحرانیت	۱/۰	۰/۸۶	۰/۸۲	۰/۹۳	۰/۷۹	۰/۵۰



(شکل-۴): حدود کنترلی و تغییر ناهنجاری در شرایط پایدار سامانه.

(Figure-4): Control limits and anomaly changes in reliability state.

در نخستین بازرسی تعداد هشدارهای برطرف شده ۲۷ عدد، تعداد هشدارهایِ طولانی پنج عدد، تعداد هشدارهای بلاتکلیف یا تصدیق‌شده، چهار عدد، و درنهایت مقدار اعتماد اپراتور به ۰/۸۹۳ کاهش پیدا می‌کند. در پایان این بازرسی ازآنجاکه مقدار اعتماد جدید اپراتور از سطح بحرانی‌بودن پست‌های A, D کمتر شده است، از دسترسی وی به این دو پست جلوگیری به‌عمل می‌آید. در ادامه با اتمام فرصتِ هشدار یکی از هشدارهای پست F، مقدار ناهنجاری به ۲/۳۲ افزایش می‌یابد. شکل (۵-ب) مراحل شناسایی دومین ناهنجاری و آغاز بازرسی دوم را نشان می‌دهد. در بازرسی دوم مقدار اعتماد اپراتور به ۰/۵۹۸ کاهش‌یافته و بدین ترتیب در ادامه، اپراتور تنها می‌تواند به پست F دسترسی داشته باشد. هنگامی‌که هشداری دیگر از پست F در فرصت

[DOI: 10.29252/jsdp.14.4.3]

قانونی خود برطرف نمی‌شود، ناهنجاری سوم شناسایی‌شده شکل (۵-ج) و درنتیجه مقدار اعتماد اپراتور در بازرسی سوم به ۰/۴۰۱ کاهش می‌یابد. در این شرایط اپراتور به هیچ‌یک از پست‌ها اجازه دسترسی نخواهد داشت.

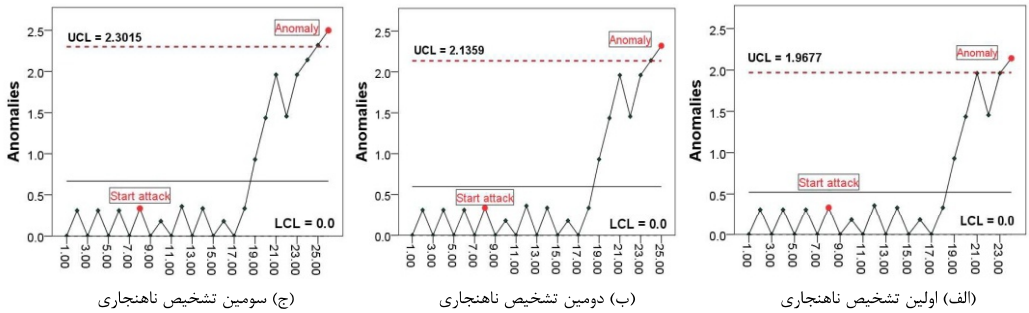
۲-۶- سناریوی کنترل شبکه

این سناریو نشان می‌دهد که چنانچه اپراتور کارایی خود را در کنترل شبکه افزایش دهد، سامانهٔ پیشنهادی قادر است تا مقدار اعتماد و درنتیجه تعداد پست‌های تحت نظارت او را در محدوده تحت مسئولیت وی افزایش دهد. این سناریو هنگامی اتفاق می‌افتد که ناهنجاری شبکه به‌طور غیرعمدی از حد آستانه خارج‌شده و آنگاه اپراتور در اسرع وقت اقدام مقتضی برای کاهش ناهنجاری و برطرف شدن هشدارهای طولانی را انجام می‌دهد. شکل (۶) تغییر ناهنجاری هنگام خروج از حد آستانه و بازگشت آن به شرایط عادی را نشان می‌دهد. جدول (۵) تغییر مقدار اعتماد اپراتور در بازرسی‌های مختلف را نشان می‌دهد. در این سناریو فرض می‌شود که به‌علت یک ناهنجاری غیرعمدی مقدار اعتماد اپراتور به ۰/۸۹۳ کاهش پیدا کرده و درنتیجه پست‌های تحت نظارت وی به B,C,E,F محدود شده است. در ادامه با افزایش کارایی اپراتور و برطرف‌شدن چند هشدارِ طولانی، مقدار ناهنجاری در محدوده مجاز قرار می‌گیرد. جدول (۵) نشان می‌دهد که در پایان بازرسی نخست تعداد هشدارهای برطرف شده ۳۸ عدد، تعداد هشدارهای طولانی یک عدد، و درنتیجه مقدار اعتماد اپراتور به ۰/۹۰۰ افزایش یافته است.

(جدول-۴): سناریوی حمله، مقدار اعتماد اپراتور در بازرسی‌های مختلف.

(Table-4): The attack scenario, the amount of operator trust in various inspections.

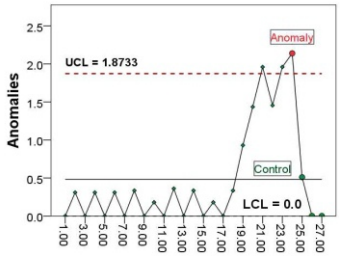
پست	بازرسی (۱) تشخیص ناهنجاری							بازرسی (۲) تشخیص ناهنجاری						
	R_{mj}	R_{mi}	L_{mj}	L_{mi}	N_{mj}	N_{mi}	T^{op}	R_{mj}	R_{mi}	L_{mj}	L_{mi}	N_{mj}	N_{mi}	T^{op}
A	–	–	–	–	–	–	۰/۸۹۳	مسدود						۰/۵۹۸
B	۲	–	–	–	–	–		–	–	–	–	–	–	
C	۵	–	–	۱	–	۱		–	–	–	۱	–	۱	
D	۴	۱	۱	۱	۱	–		مسدود						
E	۳	–	–	۱	–	–	۱/۰۰	–	–	–	۱	–	–	
F	۱۲	–	۱	–	۲	–		–	–	۲	–	۱	–	
	بازرسی (۴)							بازرسی (۳) تشخیص ناهنجاری						
A	مسدود						۰/۴۰۱	مسدود						۰/۴۰۱
B	مسدود							مسدود						
C	مسدود							مسدود						
D	مسدود							مسدود						
E	مسدود							مسدود						
F	مسدود							–	–	۳	–	–	–	



(الف) اولین تشخیص ناهنجاری (ب) دومین تشخیص ناهنجاری (ج) سومین تشخیص ناهنجاری

(شکل-۵): تشخیص ناهنجاری در سناریوی حمله.

(Figure-5): Anomaly detection in attack scenario.



(شکل-۶): کاهش ناهنجاری در سناریوی کنترل شبکه.

(Figure-6): Reducing anomalies in the control scenario.

[DOI: 10.29252/jsdp.14.4.3]

(جدول-۵): سناریوی کنترل شبکه، مقدار اعتماد اپراتور در بازرسی های مختلف

(Table-5): The control scenario, the amount of operator trust in various inspections.

پست	بازرسی (۱) ماهانه							بازرسی (۲) ماهانه						
	R_{mj}	R_{mi}	L_{mj}	L_{mi}	N_{mj}	N_{mi}	T^{op}	R_{mj}	R_{mi}	L_{mj}	L_{mi}	N_{mj}	N_{mi}	T^{op}
A	مسدود						۰/۹۰۰	مسدود						۰/۹۱۳
B	٤	-	-	-	-	-		۹	-	-	-	-	-	
C	۱۱	۱	-	-	-	-		۱٤	-	-	-	-	-	
D	مسدود							مسدود						
E	۹	۱	-	۱	-	-	۰/۸۹۳	۱۵	۱	-	-	-	-	
F	۱۲	-	-	-	-	-		۱۳	-	-	-	-	-	
	بازرسی (۴) ماهانه							بازرسی (۳) ماهانه						
A	مسدود						۰/۹۳۳	مسدود						۰/۹۲٤
B	۸	-	-	-	-	-		۵	۱	-	-	-	-	
C	۱۷	۱	-	-	-	-		۱۸	-	-	-	-	-	
D	مسدود							مسدود						
E	۱۵	۱	-	-	-	-		۲٦	-	-	-	-	-	
F	۱۰	-	-	-	-	-		۱۹	-	-	-	-	-	

در این مرحله با توجه به مقدار بحرانی‌بودن پست‌ها همچنان محدوده دسترسی اپراتور بدون تغییر باقی می‌ماند. در ادامه در بازرسی‌های دوم، سوم و چهارم با افزایش کارایی اپراتور و برطرف‌شدن به‌موقع هشدارها مقدار اعتماد به مقادیر ۰/۹۱۳، ۰/۹۲۴، و ۰/۹۳۳ افزایش می‌یابد. بدین ترتیب در پایان بازرسی چهارم اجازه دسترسی به پست D برای اپراتور فراهم می‌شود. این سناریو نشان می‌دهد که با درنظرگرفتن مقادیر متفاوت برای α_1 و α_2 سرعت افزایش اعتماد به‌مراتب آهسته‌تر نسبت به کاهش آن شده است.

۷- نتیجه‌گیری

در این مقاله یک سامانهٔ مدیریت دسترسی بر پایه اعتماد برای کاهش تهدیدهای عملیاتی سامانه اسکادا ارائه شده است. مقدار اعتماد اپراتور با توجه به کارایی وی در کنترل پست‌ها تعیین می‌شود. در این سامانه دسترسی اپراتور به پست‌ها با توجه به مقدار اعتماد وی و سطح بحرانی‌بودن پست‌ها تعیین می‌شود؛ لذا چنانچه یک تهدید عملیاتی علیه یکی از پست‌ها صورت گیرد، از دسترسی اپراتور به پست‌های دیگر (متناسب با سطح بحرانی بودن پست‌ها) جلوگیری به‌عمل خواهد آمد.

در این مقاله همچنین یک روش آماری برای تشخیص ناهنجاری در سامانهٔ اسکادا ارائه شده است. این روش از شدت هشدارهایِ طولانی در سامانه استفاده می‌کند. بدین ترتیب با استفاده از تشخیص به‌موقع ناهنجاری، از شیوع تهدیدهای عملیاتی نسبت به پست‌های دیگر می‌توان جلوگیری به عمل آورد.

۸- مراجع 8-References

[1] D. Kushner, "The real story of stuxnet," *ieee Spectrum,* vol. 50, pp. 48-53, 2013.

[2] Matthew L. Collins, Michael C. Theis, Randall F. Trzeciak, Jeremy R. Strozer, Jason W. Clark, Daniel L. Costa, *et al.*, "Common sense guide to mitigating insider threats 5th edition," CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2016.

[3] N. Baracaldo and J. Joshi, "An adaptive risk management and access control framework to mitigate insider threats," *Computers & Security,* vol. 39, pp. 237-254, 2013.

[4] P. Legg, N. Moffat, J. R. Nurse, J. Happa, I. Agrafiotis, M. Goldsmith, *et al.*, "Towards a conceptual model and reasoning structure for insider threat detection," *Journal of Wireless Mobile Networks ,Ubiquitous Computing ,and Dependable Applications,* vol. 4, pp. 20-37, 2013.

[5] H. Shey, K. Mak, S. Balaouras, and B. Luu, "Understand the state of data security and privacy: 2015 to 2016," *Forrester Research Inc,* vol. 1, 2013.

[6] N. Baracaldo, B. Palanisamy, and J. Joshi, "G-SIR: An Insider Attack Resilient Geo-Social Access Control Framework," *IEEE Transactions on Dependable and Secure Computing,* 2017.

[7] M. Warkentin, A. C. Johnston, J. Shropshire, and W. D. Barnett, "Continuance of protective security behavior: A longitudinal study," *Decision Support Systems,* vol. 92, pp. 25-35, 2016.

[8] M. Asgarkhani and E. Sitnikova, "A strategic approach to managing security in SCADA systems," in *Proceedings of the 13th European Conference on Cyber warefare and Security*, 2014, pp. 23-32.

[DOI: 10.29252/jsdp.14.4.3]

[9] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of Cyber-Warfare," *Computers & Security,* vol. 31, pp. 418-436, 2012.

[10] H. Bao, R. Lu, B. Li, and R. Deng, "BLITHE: Behavior rule-based insider threat detection for smart grid," *IEEE Internet of Things Journal,* vol. 3, pp. 190-205, 2016.

[11] S. Board, "Pipeline Accident Report," 2010.

[12] D. Hadžiosmanović, D. Bolzoni, and P. H. Hartel, "A log mining approach for process monitoring in SCADA," *International Journal of Information Security,* pp. 1-21, 2012.

[13] T. Sasaki, "A Framework for Detecting Insider Threats using Psychological Triggers," *JoWUA,* vol. 3, pp. 99-119, 2012.

[14] M.-K. Yoon and G. F. Ciocarlie, "Communication pattern monitoring: Improving the utility of anomaly detection for industrial control systems," in *NDSS Workshop on Security of Emerging Networking Technologies*, 2014.

[15] I. Garitano, R. Uribeetxeberria, and U. Zurutuza, "A review of SCADA anomaly detection systems," in *Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011*, 2011, pp. 357-366.

[16] M. Bishop, H. M. Conboy, H. Phan, B. I. Simidchieva, G. S. Avrunin, L. A. Clarke*, et al.*, "Insider threat identification by process analysis," in *Security and Privacy Workshops (SPW), 2014 IEEE*, 2014, pp. 251-264.

[17] D. Hadžiosmanović, R. Sommer, E. Zambon, and P. H. Hartel, "Through the eye of the PLC: semantic security monitoring for industrial processes," in *Proceedings of the 30th Annual Computer Security Applications Conference*, 2014, pp. 126-135.

[18] N. Baracaldo and J. Joshi, "Beyond accountability: using obligations to reduce risk exposure and deter insider attacks," in *Proceedings of the 18th ACM symposium on Access control models and technologies*, 2013, pp. 213-224.

[19] J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials,* vol. 13, pp. 562-583, 2011.

[20] S.-P. Hong, G.-J. Ahn, and W. Xu, "Access control management for SCADA systems," *IEICE TRANSACTIONS on Information and Systems,* vol. 91, pp. 2449-2457, 2008.

[21] O. Rysavy, J. Rab, P. Halfar, and M. Sveda, "A formal authorization framework for networked SCADA systems," in *Engineering of Computer Based Systems (ECBS), 2012 IEEE 19th International Conference and Workshops on*, 2012, pp. 298-302.

[22] پژوهشگاه نیرو"استاندارد سامانه‌های اتوماسیون پست‌های انتقال و فوق توزیع "،وزارت نیرو، ۱۳۸۶.

(NRI, "Substation Automation Systems standard (Transmission and Subtransmission Substations)," Ministry of Energy of Iran, 2008.)

[23] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing*, 2011, pp. 380-388.

[24] J. Lopez, C. Alcaraz, and R. Roman, "Smart control of operational threats in control substations," *Computers & Security,* vol. 38, pp. 14-27, 2013.

[25] A. M. L. da Silva, A. Violin, C. Ferreira, and Z. S. Machado, "Probabilistic evaluation of substation criticality based on static and dynamic system performances," *IEEE Transactions on Power Systems,* vol. 29, pp. 1410-1418, 2014.

[26] D. C. Montgomery, *Introduction to statistical quality control*: John Wiley & Sons (New York), 2009.

[27] I. IEC, "62682 Management of Alarm Systems for the Process Industries," ed: Geneva: IEC, 2014.

[28] N. Mayadevi, S. Ushakumari, and S. Vinodchandra, "SCADA-based operator support system for power plant equipment fault forecasting," *Journal of the Institution of Engineers (India): Series B,* vol. 4, pp. 369-376, 2014.

[29] J. Zhao, Y. Xu, F. Luo, Z. Dong, and Y. Peng, "Power system fault diagnosis based on history driven differential evolution and stochastic time domain simulation," *Information Sciences,* vol. 275, pp. 13-29, 2014.

[30] T. M. U. SPAMLAB. (2017). *SPAMLAB*. Available: https://www.irancert.ir

[DOI: 10.29252/jsdp.14.4.3]

پیام محمودی نصر تحصیلات خـود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی کامپیوتر به‌ترتیب در سال‌های ۱۳۷۳ و ۱۳۷۵ از دانشـگاه صـنعتی امیرکبیر و در مقطع دکترای مهندسـی قدرت در سـال ۱۳۹۵ از دانشـگاه تربیـت‌مـدرس بـه پایـان رسانده و هم‌اکنون استادیار دانشـکده مهندسـی کـامپیوتر و فناوری اطلاعات دانشگاه مازندران است. زمینه‌های پژوهشی مورد علاقهٔ ایشان عبارتنـد از: امنیـت شـبکه‌های صـنعتی، امنیت داده‌ها و شبکه‌های کامپیوتری.

نشانه رایانامه ایشان عبارت است از:

P.mahmoudi@umz.ac.ir

علی یزدیان ورجانی تحصیلات خود را در مقطع کارشناسی مهندسی برق از دانشگاه صنعتی شریف در سال ۱۳۸۶ به اتمام رساند. ایشان مدرک کارشناسی ارشد و دکترای خود را در رشته مهندسی برق از دانشگاه ولنگونگ استرالیا به‌ترتیب در سال‌های ۱۳۷۳ و ۱۳۷۷ دریافت کرد. وی هم‌اکنون عضو هیأت علمی دانشکده مهندسی برق و کامپیوتر دانشگاه تربیت مدرس است. زمینه‌های پژوهشی مورد علاقه ایشان عبارتند از: کاربردهای الکترونیک قدرت، حفاظت و امنیت شبکه ها، و مدیریت امنیت اطلاعات.

نشانه رایانامه ایشان عبارت است از:

Yazdian@modares.ac.ir

[DOI: 10.29252/jsdp.14.4.3]