JIPET

Journal of Intelligent Procedures in Electrical Technology
Vol. 13/ No. 51/ Autumn 2022
P-ISSN: 2322-3871, E-ISSN: 2345-5594, http://jipet.iaun.ac.ir/

20.1001.1.23223871.1401.13.51.3.6
Research Article

Combined Intrusion Detection System to Deal with Cyber Attacks in Industrial Control Systems with a Dedicated Network

Mohammad Safari[1], *PhD Student*, Elham Parvinnia[1], *Assistant Professor*, Alireza Keshavarz Haddad[2], *Associate Professor*

[1]Department of Computer Engineering, Shiraz Branch, Islamic Azad University, Shiraz, Iran
[2]School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran
safari.md@gmail.com, parvinnia@iaushiraz.ac.ir, keshavarz@shirazu.ac.ir

Abstract
Most control systems use a dedicated communication network with specific protocols. Intrusion detection systems developed based on network traffic with standard protocols, or existing datasets cannot detect significant threats on these control systems. New sophisticated malicious codes usually attacked these systems by sending known and understandable commands to the control systems and ultimately sabotaging the physical process. These attacks do not alter network traffic, so they are not detectable with standard network-based intrusion detection systems. In this paper, we proposed an innovative combined method for identifying different types of attacks on control systems with a dedicated network. We have provided a combination of methods for detecting semantic or stealth attacks and identifying attacks that affect the traffic of the control system network. For the first time in practice, the effect of common types of attacks on a control system with a specific network has been investigated, and the rules for detecting these attacks have been obtained. Experimental results in this study show that the extracted rules identify 100% of the already known attacks. The proposed new approach, based on identifying the control system commands from the extracted network records, also thoroughly detects semantic attacks. The process data behavioral method used in this study can detect about 99% of semantic attacks using classification algorithms based on Data set which is created in this study.

Keywords: behavioral intrusion detection system, industrial control system, industrial intrusion detection system, semantic and stealthy attacks

Received: 28 June 2021
Revised: 30 July 2021
Accepted: 1 September 2021

Corresponding Author: Dr. Elham Parvinnia

Citation: M. Safari, E. Parvinnia, A. Keshavarz Haddad, "Combined intrusion detection system to deal with cyberattacks in industrial control systems with a dedicated network", Journal of Intelligent Procedures in Electrical Technology, vol. 13, no. 51, pp. 31-51, December 2022 (in Persian).

20.1001.1.23223871.1401.13.51.3.6
مقاله پژوهشی

سیستم تشخیص نفوذ ترکیبی برای مقابله با حملات سایبری در سیستم‌های کنترل صنعتی با شبکه اختصاصی

محمد صفری[۱]، دانشجوی دکتری، الهام پروین‌نیا[۱]، استادیار، علیرضا کشاورزحداد[۲]، دانشیار

۱- دانشکده مهندسی کامپیوتر- واحد شیراز، دانشگاه آزاد اسلامی، شیراز، فارس، ایران
۲- دانشکده مهندسی برق و کامپیوتر- دانشگاه شیراز، شیراز، فارس، ایران
safari.md@gmail.com, parvinnia@iaushiraz.ac.ir, keshavarz@shirazu.ac.ir

چکیده: اغلب سیستم‌های کنترل، دارای شبکه ارتباطی با پروتکل‌های خاص هستند. سیستم‌های تشخیص نفوذی که بر پایه روش‌های کنترل ترافیک شبکه با پروتکل‌های معمول توسعه داده شده‌اند و یا از مجموعه داده‌های موجود استفاده کرده‌اند، برای سیستم‌های کنترل کارایی لازم را ندارند. همچنین کدهای مخرب جدید و پیچیده برای حمله به سیستم‌های کنترل و در نهایت خراب‌کاری در فرایند فیزیکی از دستورات شناخته شده و قابل درک سیستم‌های کنترل استفاده می‌کنند. این حملات تغییری در ترافیک شبکه ایجاد نمی‌کنند، بنابراین به‌وسیله سیستم‌های تشخیص نفوذ مبتنی بر شبکه قابل تشخیص نیستند. در این مقاله روشی ابتکاری و ترکیبی برای شناسایی انواع حملات به سیستم‌های کنترل با شبکه اختصاصی پیشنهاد شده است. به‌منظور شناسایی کامل حملات به سیستم‌های کنترل ترکیبی از روش‌های شناسایی حملات معنایی یا دزدکی و شناسایی حملات با تاثیر بر ترافیک شبکه سیستم کنترل ارائه شده است. برای اولین بار به‌صورت عملی تاثیر انواع حملات معمول بر روی یک سیستم کنترل با شبکه خاص بررسی و قوانین تشخیص این حملات به‌دست آمده است. نتایج تجربی در این مطالعه نشان داده است که قوانین استخراج شده به‌صورت صددرصد حملات مرتبط از قبل شناخته شده را شناسایی می‌کند. روش جدید ارائه شده مبتنی بر شناسایی دستورات سیستم کنترل از روی رکوردهای استخراج شده شبکه نیز به‌صورت کامل حملات معنایی را تشخیص می‌دهد. روش مبتنی بر داده‌های فرایندی نیز قادر به تشخیص حدود ۹۹ درصد از حملات معنایی با استفاده از الگوریتم‌های طبقه‌بندی و مجموعه داده استفاده شده است.

کلمات کلیدی: حملات معنایی و دزدکی، سیستم تشخیص نفوذ فرایندی، سیستم‌های کنترل صنعتی، سیستم تشخیص نفوذ صنعتی

تاریخ ارسال مقاله: ۱۴۰۰/۴/۷
تاریخ بازنگری مقاله: ۱۴۰۰/۵/۸
تاریخ پذیرش مقاله: ۱۴۰۰/۶/۱۷

نام نویسنده‌ی مسئول: دکتر الهام پروین نیا
نشانی نویسنده‌ی مسئول: شیراز- جاده شهرک صدرا- دانشگاه آزاد اسلامی واحد شیراز- دانشکده مهندسی- بخش کامپیوتر

۱- مقدمه

از آنجا که سیستم‌های کنترل صنعتی یکی از قسمت‌های مهم زیرساخت‌های حیاتی صنایع محسوب می‌شوند و وظیفه آنها کنترل کارکرد بهینه و حفظ ایمنی صنایع مختلف است، امروزه مورد توجه مهاجمین به‌منظور خراب‌کاری قرار گرفته است. سیستم‌های کنترل صنعتی در کلیه فرایندهای صنعتی نظیر پالایشگاه‌ها، نیروگاه‌ها و کارخانه‌های تولیدی و همچنین در فرایندهای خدماتی مانند متروها، فرودگاه‌ها و غیره وجود دارند. در دهه‌های اخیر به‌دلیل اهمیت سیستم‌های کنترل صنعتی و درهم آمیختگی این سیستم‌ها با دانش فن‌آوری اطلاعات، مورد توجه هکرها برای حمله و در نهایت از کار انداختن صنایع قرار گرفته است [۱]. برای مقابله با خطرات ناشی از حملات سایبری تکیه بر دانش و تحقیقات راه‌های مقابله با بدافزارها در فن-آوری اطلاعات کفایت نمی‌کند [۲]. بنابراین تحقیقات گسترده‌ای برای امنیت سیستم‌های کنترل صنعتی انجام گرفته است [۳-۶]. یکی از راه‌های افزایش امنیت سیستم‌های کنترل صنعتی بهره‌گیری از سیستم‌های تشخیص نفوذ[۱](IDS) با طراحی خاص سیستم‌های کنترل صنعتی است. به‌طور کلی سیستم‌های تشخیص نفوذ بر مبنای منبع داده مورد استفاده و تکنیک‌های تشخیص، دسته‌بندی می‌شوند. اگر منابع داده سیستم‌های تشخیص نفوذ بسته‌های شبکه باشد، سیستم تشخیص نفوذ مبتنی بر شبکه[۲](NIDS) است و اگر منابع داده اطلاعات کامپیوتر میزبان و فعل و انفعالات این کامپیوترها باشد، سیستم تشخیص نفوذ مبتنی بر میزبان[۳](HIDS) است. بر مبنای روش‌های تشخیص سنتی سیستم‌های تشخیص نفوذ به دو دسته کلی تشخیص ناهنجاری[۴]و تشخیص سوء استفاده[۵]دسته‌بندی می‌شوند. در روش تشخیص سوء استفاده مبنای کار مقایسه اثر امضاء[۶] حملات شناخته شده با اطلاعات جمع‌آوری شده است. این روش دارای قدرت تشخیص بسیار بالا در مورد حملات شناخته شده هستند. ضعف بزرگ این روش عدم توانایی در تشخیص حملات روز صفر[۷] و ناشناخته است. در روش تشخیص ناهنجاری به‌دلیل مقایسه اطلاعات جمع‌آوری شده با یک الگوی نرمال از قبل آموزش دیده امکان تشخیص حملات از قبل ناشناخته نیز وجود دارد ولی دقت تشخیص در این روش کمتر از روش تشخیص اثر امضاء یا همان تشخیص سوء استفاده است و تعداد تشخیص خطای بالا در این روش قابل پیش‌بینی است [۷-۹].

در دسته‌بندی‌های جدید سیستم‌های تشخیص نفوذ صنعتی علاوه بر تکنیک‌های تشخیص به مشخصات سیستم‌های کنترل نیز توجه شده است. در این دسته‌بندی‌ها سیستم‌های تشخیص نفوذ بر پایه تجزیه و تحلیل پروتکل، کاوش در ترافیک شبکه و تجزیه و تحلیل داده‌های فرایندهای کنترل، تقسیم‌بندی شده‌اند [۱۰،۱۱]. در تکنیک‌های تجزیه و تحلیل پروتکل از روش‌های مبتنی بر تشخیص سوء استفاده بهره گرفته می‌شود. در این رویکرد بسته‌های انتقالی از شبکه‌های سیستم کنترل به‌وسیله قوانین تعریف شده مورد بازرسی عمیق[۸] قرار می‌گیرد و تشخیص داده می‌شود که این بسته‌ها مشخصات پروتکل‌های شبکه سیستم‌های کنترل را رعایت کرده باشند. دقت این رویکرد وابسته به قوانین تعریف شده است و معمولا زمان بر است. رویکردهای کاوش در ترافیک شبکه با فرض اینکه فعالیت‌های سیستم‌های کنترل محدود و تکراری است و دارای یک شبکه با توپولوژی ساده و ثابت با تعداد کاربر مشخص شده و محدود هستند، شکل گرفته است. از فرضیات ذکر شده نتیجه‌گیری شده است که شبکه سیستم‌های کنترل در حالت نرمال دارای ترافیک پایدار است. بنابراین امکان ایجاد یک رابطه غیرخطی پیچیده میان ترافیک حالت نرمال و رفتار حالت نرمال و غیر نرمال سیستم کنترل وجود دارد. همچنین امکان جمع آوری ترافیک حالت نرمال و اعمال الگوریتم‌های داده‌کاوی برای تشخیص ناهنجاری وجود دارد. با توجه به اینکه در دو روش قبلی ارتباط میان سیستم کنترل و دنیای فیزیکی به‌عنوان یک اصل مهم در نظر گرفته نشده است بنابراین حمله کننده‌ها می‌توانند بدون دست‌کاری مشخصات پروتکل و ایجاد ترافیک غیر نرمال، داده‌ها را دست‌کاری نمایند و در نهایت خراب‌کاری صورت گیرد. برای شناسایی این حملات که به آنها حملات معنایی[۹] یا یواشکی[۱۰] نیز اطلاق می‌شود از سیستم‌های تشخیص نفوذ مبتنی بر فرایند کنترل فیزیکی استفاده می‌شود. تغییرات غیر قابل انتظار در این داده‌ها نشان دهنده یک نفوذ است [۱۲]. تجزیه و تحلیل دستورات سیستم‌های کنترل و توالی و زمان‌بندی میان دستورات دارای اهمیت فوق العاده‌ای است. بنابراین هرگونه تغییر در توالی و یا زمان‌بندی بدون تغییر در ترافیک شبکه می‌تواند نشان‌گر یک نفوذ و یا حمله سایبری باشد. در روش آخر یک مدل که قادر باشد به‌صورت دقیقی تکامل یک سیستم کنترل صنعتی را توصیف و خروجی‌های مورد انتظار در آینده را پیش‌بینی کند، طراحی می‌شود و سپس با مقایسه این خروجی‌ها با خروجی‌های مشاهده شده احتمال نفوذ تشخیص داده می-

شود [۱۱]. اغلب بدافزارهای جدید و پیچیده برای حمله به سیستم‌های کنترل و در نهایت خراب‌کاری در فرایند فیزیکی از دستورات شناخته شده و قابل درک سیستم‌های کنترل سوء استفاده می‌کنند. اگر از این دستورات به ظاهر مشروع و قانونی در جهت خراب‌کاری استفاده شوند با روش‌های کنترل ترافیک شبکه، بخصوص سیستم‌های کنترلی که دارای شبکه‌هایی با پروتکل‌های خاص هستند، قابل شناسایی نیستند. در این مطالعه به‌منظور شناسایی کامل حملات به سیستم‌های کنترل ترکیبی از روش‌های شناسایی حملات دزدکی و شناسایی حملات به ترافیک شبکه سیستم کنترل را ارائه داده‌ایم. این روش-های ترکیبی برای اولین بار به‌صورت اختصاصی روی یک سیستم کنترل دارای شبکه اختصاصی مورد بررسی قرار گرفته است. بنابراین نوآوری اول این مقاله توجه به تمامی انواع حملات به سیستم‌های کنترل در یک مطالعه است. در این مقاله به هر دو نوع حملات تاثیرگذار بر ترافیک شبکه و حملات دزدکی و معنایی به سیستم کنترل در یک مطالعه توجه شده است. بنابراین بر خلاف سایر مطالعات که تمرکزشان به یکی از انواع حملات بوده است و سایر حملات مغفول مانده است، در این جا سعی شده است یک راه حل جامع با ترکیب روش‌های تشخیص نفوذ برای تشخیص حملات به سیستم‌های کنترل، بدون توجه به نوع حمله ارائه گردد. برای تشخیص حملاتی که باعث تغییر در ترافیک نرمال شبکه و یا روند رکوردهای ارسالی در شبکه می-شوند از روش‌های بر پایه قوانین تعریف شده استفاده شده است. برای بالا بردن دقت تشخیص، دو رویکرد موازی در پیش گرفته شده است. در رویکرد اول قوانین حاکم بر ترافیک نرمال شبکه اختصاصی سیستم کنترل را در حالت‌های مختلف استخراج نموده‌ایم و تخطی از این قوانین را بعدا برای تشخیص حالت غیر نرمال و حمله در نظر گرفته‌ایم. علاوه بر بررسی ترافیک عادی به‌منظور تکمیل قوانین تشخیص حملات معمول تاثیرگذار بر ترافیک شبکه رویکرد دومی نیز برای اولین بار در این مطالعه مورد بررسی و استفاده قرار گرفته است. در این رویکرد حملات شناخته شده‌ای به کنترل‌کننده صورت گرفته و شبیه‌سازی شده است. با استفاده از ابزارهای نرم‌افزاری تست نفوذ و ارزیابی شبکه حملاتی را به شبکه سیستم‌های کنترل و کنترل‌کننده اعمال نموده‌ایم و بسته‌های شبکه را در این حالت‌ها دریافت و ذخیره نموده‌ایم. از روی داده‌های به‌دست آمده قوانین تشخیص این حملات نیز تولید شده است. بنابراین نوآوری دوم این مقاله استفاده از روش‌های بر پایه قوانین تعریف شده در تشخیص حملات تاثیرگذار بر ترافیک شبکه است. در این مطالعه به‌جای استفاده از مجموعه داده‌های مانند مجموعه داده آزمایشگاه امنیت شبکه (NSL-KDD) که اصولا برای شبکه‌های سیستم‌های کنترل تولید نشده‌اند و تاثیر گذاری آنها برای تشخیص حملات به شبکه‌های سیستم‌های کنترل مورد بررسی قرار نگرفته است از یک روش ابتکاری اثر امضاء حملات استفاده شده است.

برای تشخیص حملات معنایی و دزدکی نیز دو رویکرد به‌صورت موازی مورد استفاده قرار گرفته است. در رویکرد اول روشی ابتکاری مبتنی بر شبکه برای تشخیص دستوراتی که توسط یک حمله‌کننده بدون مجوز به سیستم کنترل اعمال می‌شوند، پیشنهاد شده است. این روش پیشنهادی برخلاف سایر روش‌های مبتنی بر شبکه که در مطالعات قبلی انجام شده است قادر به تشخیص حملات معنایی و یواشکی به سیستم‌های کنترل است. در این مطالعه از روش تشخیص سوء استفاده و مبتنی بر بسته‌های ارسالی شبکه برای تشخیص دستورات به‌ظاهر مشروع استفاده می‌کنیم. در این مطالعه اثر امضاء دستوراتی که از ایستگاه اپراتوری به سمت سیستم کنترل ارسال می‌شود با ضبط ترافیک شبکه به‌دست آمده است. برای تشخیص دستورات غیر نجیب، دستوراتی که از روی شبکه سیستم کنترل قبل از رسیدن به خود سیستم کنترل تشخیص داده می‌شود را با دستورات واقعی اجرا شده توسط اپراتور مقایسه می‌شود. با توجه به اینکه ممکن است سیستم‌های کنترل پروتکل شبکه‌های خاص خود را داشته باشند که اغلب در دسترس قرار ندارد و جزء اطلاعات اختصاصی سازندگان است. بنابراین در این مطالعه فرض نموده‌ایم در مورد جزئیات پروتکل اختصاصی شبکه سیستم کنترل اطلاعاتی موجود نیست و بر این مبنی راه‌حل پیشنهادی را ارائه نموده‌ایم. بنابراین نوآوری دیگر این مطالعه، استفاده از اطلاعات و بسته‌های شبکه برای تشخیص حملات معنایی بدون فرض تغییر در مشخصات پروتکل و ترافیک شبکه و همچنین بدون وابستگی به دانش جزئیات پروتکل اختصاصی سازندگان سیستم‌های کنترل است. در رویکرد دوم برای تشخیص حملات معنایی و دزدکی از رفتار فرایند تحت کنترل استفاده می‌شود. با توجه به ماهیت فرایند تحت کنترل رفتار حالت عادی و نرمال فرایند، با استفاده از متغیرهای اندازه‌گیری شده فرایند، شبیه‌سازی می‌شود. در این روش داده‌های حالت‌های عادی که از سیستم‌های کنترل جمع‌آوری شده است برای

آموزش الگوریتم‌های یادگیری ماشین و داده‌کاوی استفاده می‌شوند. نوآوری دیگر این مطالعه اختصاصی سازی روش‌های تشخیص نفوذ جهت استفاده در یک سیستم کنترل با پروتکل شبکه اختصاصی است. علاوه بر آن ترکیب روش‌های مختلف تشخیص نفوذ مناسب سیستم‌های کنترل به‌منظور پوشش حداکثری تشخیص حملات مختلف به سیستم کنترل نیز جزء نوآوری‌های این مطالعه است.

برای اینکه بتوانیم نتایج مدل پیشنهادی را در عمل و تجربه مورد بررسی قراردهیم و یک نمونه واقعی از این مدل پیشنهادی را ارائه کنیم از یک بستر واقعی سیستم کنترل یوکوگاوا[۳] شبکه اختصاصی[۴] که تمامی مشخصه‌های ذکر شده قبلی را دارا است، بهره گرفته‌ایم. نتایج نشان می‌دهد که این روش ترکیبی، به‌خوبی قادر به تشخیص هردو نوع حمله منجر به تغییر ترافیک شبکه و همچنین حملات با استفاده از دستورات بظاهر مشروع که تغییری در ترافیک شبکه یا مشخصات پروتکل نمی-دهند، است. نتایج تجربی در این مطالعه نشان داده است که قوانین استخراج شده بصورت صددرصد حملات مرتبط از قبل شناخته شده را شناسایی می‌کند. بدیهی است در این روش انتظار شناسایی حملات ناشناخته وجود ندارد. روش جدید ارائه شده مبتنی بر شناسایی دستورات سیستم کنترل از روی رکوردهای استخراج شده شبکه نیز بصورت کامل حملات معنایی را تشخیص می‌دهد. روش مبتنی بر داده‌های فرایندی مورد استفاده در این مطالعه نیز قادر به تشخیص حدو ۹۹ درصد از حملات معنایی با استفاده از الگوریتم‌های طبقه‌بندی و مجموعه داده تهیه شده در این مطالعه، است. البته کارایی این روش وابستگی شدید به نوع فرایند و داده‌های کلیدی انتخاب شده دارد. به دلیل اینکه در اغلب موارد امکان استفاده از مجموعه داده‌های تولیدی استاندارد برای تولید سیستم‌های تشخیص نفوذ مبتنی بر شبکه، خاص سیستم‌های کنترل وجود ندارد با توسعه روش پیشنهادی در این مقاله امکان تشخیص حملات دیگر نیز وجود دارد. این مطالعه قابل توسعه به سایر سیستم‌های کنترل با مشخصات متفاوت و با دستورات مشروع متنوع تر نیز است.

۲- پیشینه تحقیق

پایه و اساس سیستم‌های تشخیص نفوذ مبتنی بر شبکه مجموعه داده مورد استفاده برای آموزش و تست مدل‌ها است. به این منظور مجموعه داده‌های متنوعی در طول سالیان گذشته معرفی و مورد استفاده قرار گرفته است. در مقاله [۱۳] یک مرور کاملی بر انواع مجموعه داده‌های معرفی شده و مزایا و معایب آنها انجام شده است. از اولین مجموعه داده‌های مبتنی بر شبکه که برای سیستم‌های تشخیص نفوذ مورد استفاده قرار گرفته‌اند، مجموعه داده بین‌المللی کشف دانش و داده‌کاوی[۵] KDD CUP99 است که از ترافیک شبکه به‌وسیله پروژه برنامه ارزیابی سیستم‌های تشخیص نفوذ موسوم به[۶] DARPA 1998 جمع-آوری و تولید شده است. هر چند که این مجموعه داده به‌صورت وسیعی به‌عنوان معیار برای ارزیابی سیستم‌های تشخیص نفوذ مورد استفاده قرار گرفته است اما وجود رکوردهای تکراری که باعث سوءگیری الگوریتم‌ها به سمت حملات پرتکرار می‌شوند، بزرگترین عیب آن است. برای رفع ایراد این مجموعه داده یک مجموعه داده دیگر با نام مجموعه داده آزمایشگاه امنیت شبکه NSL-KDD از آن اقتباس شده است. در مقاله [۱۴] تکنیکی معرفی شده است که با سرعت بیشتر به‌توان از روی اثر امضاء حملات شناخته شده، اثر حملات را روی داده‌های شبکه پیدا نمود. در این روش نسبت به روش اثر امضاء اپریوری[۷] از نظر سرعت، پیشرفت حاصل شده است. با توجه به‌اینکه در این روش‌ها زمان زیادی از کشف امضاء صرف جستجوی بانک اطلاعاتی می‌شود، بنابراین در این مقاله روش جدیدی برای کوتاه‌کردن زمان جستجوی بانک اطلاعاتی پیشنهاد شده است. پیشنهاد استفاده از رویکرد یادگیری عمیق برای اجرا و توسعه سیستم‌های تشخیص نفوذ مبتنی بر شبکه توسط مقاله [۱۵] ارائه شده است. در این پیشنهاد و مطالعه از مجموعه داده آزمایشگاه امنیت شبکه NSL-KDD برای ارزیابی استفاده شده است. در ادامه همین مسیر مقاله [۱۶] یک تکنیک جدید یادگیری عمیق برای سیستم تشخیص نفوذ ارائه کرده است. در این پژوهش از رمز خودکار عمیق غیر متقارن[۸] (NDAE) برای یادگیری نظارت نشده ویژگی[۹] استفاده شده است. با این روش پیشرفت قابل توجه در پارامترهای ارزیابی نسبت به سایر روش‌های پیشنهادی حاصل شده است. در مقاله [۱۷] به یکی از حملات معروف شبکه تحت عنوان SYN-Flood پرداخته شده است. این حمله با مصرف منابع شبکه باعث اخلال در وظائف نرمال شبکه می-شود. در این مقاله سیستم تحت حمله با استفاده ازتئوری صف‌بندی مدل‌سازی می‌شود و مسأله دفاع در برابر حملات SYN-

Flood را به یک مسأله بهینه‌سازی نگاشت می‌دهد. از الگوریتم بهینه‌سازی اجتماع ذرات و فیلتر موثر انطباقی برای بروزکردن دو پارامتر مهم و تاثیرگذار در حملات SYN-Flood استفاده شده است. در مقاله [۱۸] یک مدل ماشین‌بردار پشتیبان که هسته‌های آن وزن‌دار شده به همراه پارامترهای هسته‌های ماشین بردار پشتیبان برای سیستم تشخیص نفوذ ارائه شده است. با توجه به پیچیدگی بالای مسئله، از یک الگوریتم ژنتیک جزیره‌ای پویای خود تطبیق استفاده شده است. باتوجه به حجم بالای داده‌ها، از اتوانکودر نیز برای کاهش حجم داده‌ها استفاده شده است. نتایج ارزیابی نشانگر بهبود کارایی و دقت است. پژوهش-های زیادی در حوزه سیستم‌های تشخیص نفوذ مبتنی بر شبکه صورت گرفته است که در بررسی جامع صورت گرفته توسط [۱۹] به آنها پرداخته شده است و همچنین انواع حملات به شبکه و موتورهای تصمیم‌گیری در این پژوهش مورد بررسی قرار گرفته است. با توجه به اینکه این مقاله متمرکز بر روی سیستم‌های کنترل و شبکه‌های سیستم‌های کنترل است، بیشتر به تحقیقات و بررسی‌های صورت گرفته در این حوزه می‌پردازیم. در مقاله [۲۰] بر پایه این استدلال که شبکه‌های سیستم‌های کنترل در مقایسه با شبکه‌های کسب و کار دارای نظم و ثبات بیشتری در توپولوژی ارتباطات و ساختار هستند یک سیستم تشخیص نفوذ مبتنی بر مدل پیشنهاد شده است. در این مطالعه مدل‌ها در سه سطح مدل‌سازی پروتکل برای مشخص‌کردن مودباس/ تی سی پی؛[۲] مدل‌سازی نظم الگوی ارتباط و در نهایت یک ماژول برای بازرسی سرویس‌های شبکه طراحی شده است. توسط مقاله [۲۱] یک سیستم تشخیص نفوذ که قادر است حملات پیچیده سایبری به اسکادا را شناسایی کند، پیشنهاد شده است. در این مطالعه مودباس[۱] به‌عنوان شبکه سیستم کنترل یا اسکادا[۲] فرض شده است. در مقاله [۲۲] یک سیستم تشخیص نفوذ برای شبکه‌های اسکادا مبتنی بر پروتکل IEC60870-5-104 ارائه شده است. در روش ارائه شده از تجزیه و تحلیل عمیق پروتکل و بازرسی عمیق بسته‌ها[۳] بهره‌گیری شده است. این سیستم تشخیص نفوذ شامل تشخیص اثر امضاء و مدل‌سازی بوسیله یک ترافیک نمونه ارزیابی و تست شده است. به‌منظور افزایش امنیت سایبری شبکه سیستم کنترل و اسکادا یک سیستم تشخیص نفوذ مبتنی بر قوانین[۴] با استفاده از بازرسی عمیق بسته‌ها توسط مقاله [۲۳] پیشنهاد شده است. این سیستم تشخیص نفوذ به‌منظور استفاده در سیستم‌های کنترل سفارش‌سازی شده است. قوانین اثر امضاء پیشنهاد شده قادر است بصورت دقیق حملات شناخته شده را شناسایی کند ضمنا سیستم تشخیص نفوذ بر پایه مدل‌سازی سیستم که در کنار آن قرار داده شده است قادر به تشخیص حملات ناشناخته است. در مطالعه [۲۴] آسیب‌پذیری سیستم‌های کنترل در مقابل دست‌کاری سیستم عامل به‌منظور دست‌یابی به درک بهتر تهدیدات ناشی از حملات دستکاری سیستم عامل بررسی شده است. همچنین یک روش تجزیه و تحلیل سیستم‌عامل ارائه شده است. یک آزمایش اثباتی برای نشان دادن چگونگی دست-کاری سیستم‌عامل و جای‌گذاری آن با سیستم عامل قانونی در یک سیستم کنترل آلن بردلی[۵] انجام شده است. در مقاله [۲۵] امکان‌پذیر بودن دستکاری سیستم عامل یک سیستم کنترل به‌منظور اجرای یک حمله که از راه دور فعال می‌شود، مورد بررسی قرار گرفته است. برای بدست آوردن ساختار سیستم عامل از روش مهندسی معکوس استفاده شده است و بعد از درک سیستم عامل یک ویژگی قابل بهره‌برداری که بتوان با آن سیستم کنترل را از راه دور غیر فعال کرد اضافه و سیستم عامل دست‌کاری می‌شود. در این مقاله توصیه‌های طراحی برای کمک به کاهش نقاط ضعف احتمالی در سیستم عامل پیشنهاد شده است. یکی از مشکلات روش‌های تشخیص نفوذ اثر امضاء تعداد زیاد هشدارهای کاذب است. به همین دلیل تعداد زیادی پژوهش در جهت کاهش هشدارهای کاذب پیشنهاد شده است که تعدادی از آنها در ابزارهای مدیریت اطلاعات حوادث امنیتی[۶] استفاده شده است. در مقاله [۲۶] این روش‌ها مرور شده و یک طبقه‌بندی از آنها ارائه شده است. در مقاله [۲۷] به ۲۸ حمله سایبری ممکن به سیستم‌های کنترلی که از پروتکل مودباس استفاده می‌کنند پرداخته شده است. در مقاله [۲۸] یک روش تشخیص رفتار غیر نرمال را با استفاده از یادگیری الگوی ترافیک نرمال بر روی پروتکل مودباس/ تی سی پی پیشنهاد شده است. رویکرد این مقاله نیز با در نظر گرفتن فرض الگوی ترافیک منظم شبکه سیستم کنترل در حالت نرمال سیستم کنترل است. در مقاله [۲۹] یک روش ابتکاری برای تولید یک مدل ترافیک بر اساس ساختار سری زمانی در یک سیستم صنعتی شیمیایی پیشنهاد شده است. یک مدل ساختاری ساده که سری زمانی را به چهار مولفه تجزیه می‌کند. در مقاله [۳۰] روش فوز تست[۷] را برای تشخیص بدافزار در سیستم‌های کنترل صنعتی ارائه شده است. در روش پیشنهاد شده فایل پیکربندی نرم افزار کنترل صنعتی بعنوان فایل منبع رنگ شده و بعنوان فایل نمونه فوزینگ در نظر گرفته شده است. ابتدا

داده‌های کلیدی را که احتمالا خطر ایمنی بالقوه دارند در فایل پیکربندی از طریق تجزیه و تحلیل رنگ پویا پیدا می‌شود. سپس داده‌ها را جهش داده[۲۸] و یک فایل غیر نرمال تولید می‌شود و در نهایت تست فاز صورت می‌گیرد. یک نوع جدید حمله سایبری به سیستم‌های کنترل که باعث تغییر بازه زمانی میان دستورات سیستم‌های کنترل می‌شود در مقاله [۳۱] مورد بررسی قرار گرفته است. در این مطالعه این نوع حمله در نرم‌افزار متلب شبیه‌سازی و اثرات آن تجزیه و تحلیل شده است. در این مطالعه فرض شده است یک حمله‌کننده بسیار حرفه‌ای با تاثیرگذاری بر روی ترتیب کنترل بتواند به فرایند فیزیکی صدمه بزند. در این مطالعه بعنوان نمونه مورد مطالعه یک مجموعه خنثی‌سازی شیمیایی مورد استفاده قرار گرفته ولی امکان اجرای آن در فرایندهای دیگر نیز وجود دارد. در مطالعه [۳۲] حملات مفهومی به شبکه‌های سیستم‌های کنترل که به‌وسیله تشخیص ناهنجاری معمول قابل تشخیص نیستند را ارائه کرده است. در این نوع حملات بعد از در اختیار قرار گرفتن کانال ارتباطی میان ایستگاه‌های اپراتوری و سیستم کنترل، حمله باعث می‌شود که ایستگاه اپراتوری مقادیر غلط فرایندی را به اپراتور نمایش دهد و سبب فریب اپراتور و انجام تصمیم دستی شود. با فرض ثابت و قابل پیش‌بینی بودن ترافیک شبکه سیستم‌های کنترل، در مطالعه [۳۳] الگوی تشخیص ناهنجاری بر پایه زمان[۲۹]استفاده از مشخصات آماری ثابت الگوی ترافیکی پیشنهاد شده است. این روش پیشنهادی بوسیله سه مجموعه داده ارزیابی و راستی آزمایی شده است. یکی از مجموعه داده‌ها از ترافیک واقعی تولید و دو مجموعه دیگر از شبکه‌های شبیه‌سازی شده به‌دست آمده‌اند. ارزیابی سیستم تشخیص نفوذ پیشنهادی بر روی الگوی ترافیک مودباس، S7 و IEC104 صورت گرفته است. در مطالعه [۳۴] استدلال شده است که در شبکه سیستم‌های کنترل کارهای مشخص به‌صورت تکراری انجام می‌شود. بنابراین برای یک کار مشخص الگوی ترافیکی شبکه سیستم کنترل الگوی که از فعالیت نرمال حاصل می‌شود، استفاده شده است. در این روش رفتار نرمال را در تمام الگوهای ترافیکی براساس تعداد بسته‌های ترافیکی شبکه در یک بازه زمانی مشخص که بین دو دستگاه تبادل می‌شود، یادگیری می‌شود. نتایج این روش به‌وسیله یک محیط تست واقعی ارزیابی شده است. مکانیزمی برای تشخیص حمله و کاهش آن با تمرکز بر حافظه ورودی سیستم کنترل توسط مقاله [۳۵] ارائه شده است. در این مطالعه مکانیسم تشخیص حمله و پاسخ به حمله در حافظه اجرایی سیستم کنترل تعبیه می‌شود. برای کمک به بررسی این مفهوم یک محیط تست که یک فرایند تصفیه آب را مدل می‌کند، توسعه داده شده است. بر خلاف بیشتر تحقیقات که برای تشخیص حمله در سیستم‌های کنترل بر تشخیص ناهنجاری در شبکه‌های سیستم‌های کنترل تمرکز دارند، در این مطالعه در خود سیستم کنترل انجام می‌شود. برای پیشرفت و توسعه امنیت سایبری سیستم‌های کنترل صنعتی در مطالعه [۳۶] یک سیستم تشخیص نفوذ بر پایه استراتژی دفاع در عمق[۳۰]پیشنهاد شده است. در این مطالعه برای ایجاد لایه‌های دفاعی از هرسه مجموعه داده ترافیک شبکه، داده‌های کامپیوتر میزبان و داده‌های فرایند فیزیکی بهره‌گیری شده است. حملات سایبری مانند تغییر دستورات و تزریق داده غلط[۳۱]که به‌وسیله بازدید از داده‌های ترافیک شبکه و داده‌های کامپیوتر میزبان امکان پذیر نیست، به‌وسیله بازدید از داده‌های فرایند فیزیکی شناسایی می‌شوند. در مقاله [۳۷] یک روش شناسایی حملات سایبری در سیستم‌های کنترل بر اساس تشخیص الگوی زمانی[۳۲]پیشنهاد شده است. این روش نه تنها قادر به تشخیص ناهنجاری در داده‌های مبادله شده فیمابین اجزاء سیستم‌های کنترل که از طریق شبکه اسکادا تبادل می‌شوند هستند، بلکه قادر به تشخیص ناهنجاری‌های هستند که از طریق سوء استفاده از دستورات قانونی و مشروع صورت می‌گیرد.

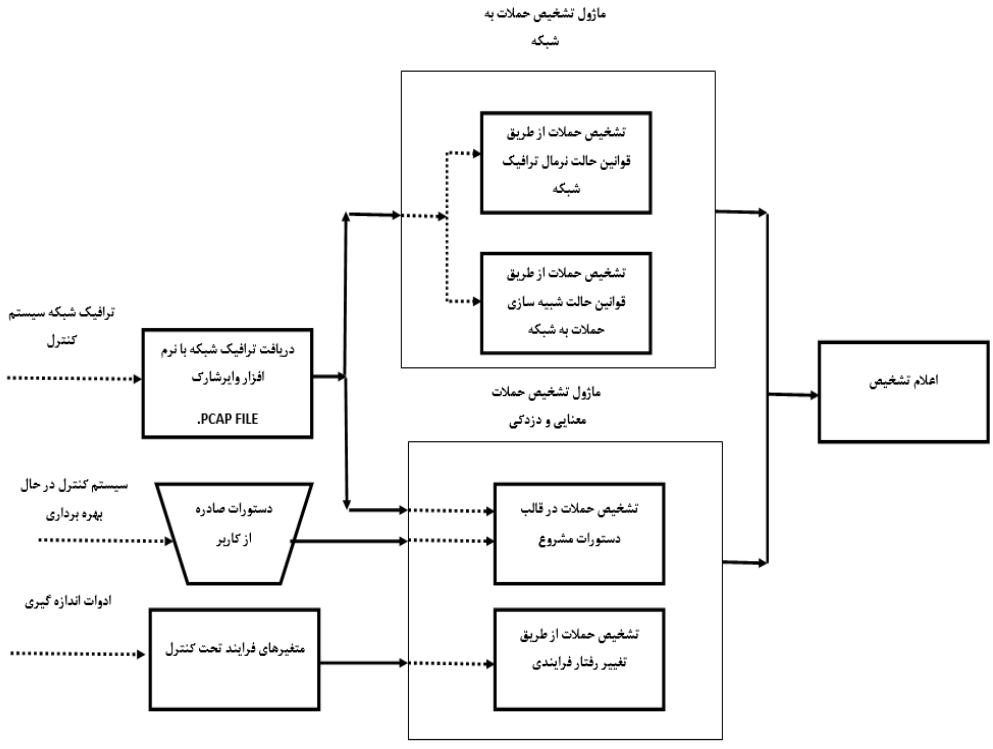
فرض‌های که در مورد شبکه مودباس/ تی سی پی وجود دارد قابل تعمیم به سایر شبکه‌های سیستم کنترل نیست. الگوی زمانی دستورات سیستم‌های کنترل وابسته به فرایندهای مورد کنترل است یعنی الگوی زمانی یک واحد تولیدی با الگوی زمانی واحد تولیدی دیگر متفاوت است. در موارد خاص نیز ممکن است الگوی زمانی یک واحد تولیدی در شرایط مختلف یکسان نباشد و بستگی به پارامترهای فرایند کنترل دارد. در روش پیشنهادی این مقاله این ایرادها وجود ندارد و نسبت به روش ذکر شده دارای مزیت نسبی است. مطالعات ذکر شده اغلب با فرض ثابت و تکراری بودن ترافیک شبکه سیستم‌های کنترل صورت گرفته است ولی در این مطالعه استدلال می‌کنیم که فرض ثابت بودن و قابل پیش‌بینی بودن الگوی ترافیک شبکه سیستم‌های کنترل بجز در ارتباطات و پروتکل‌های خاص مثل مودباس که تبادل اطلاعات از قبل تعریف شده دارند، صحیح نیست. بعنوان مثال در سیستم‌های کنترل گسترده‌ای مثل یوکوگاوا یا امرسون[۳۳]که از شبکه‌های غیر از شبکه مودباس

استفاده می‌کنند و تبادل اطلاعات مهندسی و اپراتوری همزمان روی یک شبکه صورت می‌گیرد، فرض تکراری بودن الگوی ترافیک شبکه بدلیل وابستگی بسته‌های ارسالی به تعداد اجزاء شبکه و نوع عملیاتی که در این اجزاء انجام می‌شود، متناسب با واقعیت نیست. همچنین اطلاعات کافی از پروتکل شبکه‌های سیستم‌های کنترل نیز به دلیل محرمانه بودن اغلب آنها از سوی سازندگان سیستم‌های کنترل وجود ندارد ولی در مطالعات ذکر شده این موضوع مورد توجه نبوده است. در اغلب مطالعات نیز فرض شده است که در زمان حمله ترافیک شبکه سیستم‌های کنترل دست‌کاری می‌شود و از الگوی نرمال خود پیروی نمی-کند. ولی بدافزارهای جدید و پیچیده برای حمله به سیستم‌های کنترل و در نهایت خرابکاری در فرایند فیزیکی از دستورات شناخته شده و قابل درک سیستم‌های کنترل سوء استفاده می‌کنند. اگر از این دستورات به ظاهر مشروع و قانونی در جهت خراب‌کاری استفاده شوند با رکوردهای ارسالی در شبکه ارسال می‌شوند. برای بالا بردن دقت تشخیص، دو رویکرد موازی را در پیش گرفته‌ایم. در رویکرد اول قوانین حاکم بر ترافیک نرمال شبکه را در حالت‌های مختلف استخراج نموده‌ایم و تخطی از این قوانین را بعدا برای تشخیص حالت غیر نرمال و حمله در نظر گرفته‌ایم. علاوه بر بررسی ترافیک عادی به‌منظور تکمیل قوانین تشخیص حملات معمول تاثیرگذار بر ترافیک شبکه رویکرد دومی نیز در این مطالعه مورد بررسی و استفاده قرار گرفته است. در این رویکرد حملات شناخته شده‌ای به کنترل‌کننده صورت گرفته و شبیه‌سازی شده است. در این مطالعه با استفاده از ابزارهای نرم افزاری تست نفوذ و ارزیابی شبکه حملاتی را به شبکه سیستم‌های کنترل و کنترل‌کننده اعمال نموده‌ایم و بسته-های شبکه را در این حالت‌ها دریافت و ذخیره نموده‌ایم. از روی داده‌های به‌دست آمده قوانین تشخیص این حملات نیز تولید شده است. برای تشخیص حملات معنایی و دزدکی نیز دو رویکرد به‌صورت موازی مورد استفاده قرار گرفته است. در رویکرد اول روشی ابتکاری مبتنی بر شبکه برای تشخیص دستوراتی که توسط یک حمله‌کننده بدون مجوز به سیستم کنترل اعمال می‌شوند، پیشنهاد شده است. این روش پیشنهادی برخلاف سایر روش‌های مبتنی بر شبکه قادر به تشخیص حملات معنایی و یواشکی به سیستم‌های کنترل است. در این مطالعه از روش تشخیص سوء استفاده و مبتنی بر بسته‌های ارسالی شبکه برای تشخیص دستورات به‌ظاهر مشروع استفاده می‌کنیم. در این مطالعه اثر امضاء دستوراتی که از ایستگاه اپراتوری به سمت سیستم کنترل ارسال می‌شود با ضبط ترافیک شبکه به‌دست آمده است. در این مطالعه برای تشخیص دستورات غیر نجیب، دستوراتی که از روی شبکه سیستم کنترل قبل از رسیدن به خود سیستم کنترل تشخیص داده می‌شود را با دستورات واقعی اجرا شده توسط اپراتور مقایسه می‌کنیم. با توجه به اینکه ممکن است سیستم‌های کنترل پروتکل شبکه‌های خاص خود را داشته باشند که اغلب در دسترس قرار ندارد و جزء اطلاعات اختصاصی سازندگان است بنابراین در این مطالعه فرض نموده‌ایم در مورد جزئیات پروتکل اختصاصی شبکه سیستم کنترل اطلاعاتی موجود نیست و بر این مبنی راه حل پیشنهادی را ارائه نموده‌ایم. بنابراین نوآوری این روش، استفاده از اطلاعات و بسته‌های شبکه برای تشخیص حملات معنایی بدون فرض تغییر در مشخصات پروتکل و ترافیک شبکه و همچنین بدون وابستگی به دانش جزئیات پروتکل اختصاصی سازندگان سیستم‌های کنترل است. در رویکرد دوم برای تشخیص حملات معنایی و دزدکی از رفتار فرایند تحت کنترل استفاده می‌شود. با توجه به ماهیت فرایند تحت کنترل رفتار حالت عادی و نرمال فرایند، با استفاده از متغیرهای اندازه‌گیری شده فرایند، شبیه‌سازی می-شود. در این روش داده‌های حالت‌های عادی که از سیستم‌های کنترل جمع‌آوری شده است برای آموزش الگوریتم‌های یادگیری ماشین و داده‌کاوی استفاده می‌شوند. نو آوری دیگر این مطالعه اختصاص‌سازی روش‌های تشخیص نفوذ جهت استفاده در یک سیستم کنترل با پروتکل شبکه اختصاصی است. علاوه بر آن ترکیب روش‌های مختلف تشخیص نفوذ مناسب سیستم‌های کنترل به‌منظور پوشش حداکثری تشخیص حملات مختلف به سیستم کنترل نیز جزء نوآوری‌های این مطالعه است. برای اینکه بتوانیم نتایج مدل پیشنهادی را در عمل و تجربه مورد بررسی قراردهیم و یک نمونه واقعی از این مدل پیشنهادی را ارائه کنیم ما از یک بستر واقعی سیستم کنترل یوکوگاوا با شبکه Vnet/IP که تمامی مشخصه‌های ذکر شده قبلی را دارا است، بهره گرفته‌ایم. نتایج نشان می‌دهد که این روش ترکیبی، بخوبی قادر به تشخیص هر دو نوع حمله منجر به تغییر ترافیک شبکه و همچنین حملات با استفاده از دستورات بظاهر مشروع که تغییری در ترافیک شبکه یا مشخصات پروتکل نمی-دهند، است. به دلیل اینکه در اغلب موارد امکان استفاده از مجموعه داده‌های تولیدی استاندارد برای تولید سیستم‌های تشخیص نفوذ مبتنی بر شبکه، خاص سیستم‌های کنترل وجود ندارد با توسعه روش پیشنهادی در این مقاله امکان تشخیص

حملات دیگر نیز وجود دارد. این مطالعه قابل توسعه به سایر سیستم‌های کنترل با مشخصات متفاوت و با دستورات مشروع متنوع‌تر نیز است. در ادامه و در بخش دوم این مقاله روش تحقیق ارائه شده است و در بخش سوم پیاده‌سازی روش تحقیق و نتایج حاصل از پیاده‌سازی ارائه شده است و در بخش نهائی نتایج و مطالعات پیشنهادی آتی بیان شده است.

۳- روش تحقیق

هدف از این مطالعه تشخیص کلیه حملاتی است که به سیستم‌های کنترل دارای شبکه ارتباطی با پروتکل‌های خاص صورت می‌گیرد، است. در این مطالعه حملات را به دو دسته حملات دزدکی یا یواشکی و حملات معمول تاثیرگذار بر ترافیک شبکه تقسیم‌بندی می‌کنیم. در این تقسیم‌بندی حملات معمول تاثیرگذار بر ترافیک شبکه به حملاتی اطلاق می‌شود که باعث تغییر در ترافیک شبکه سیستم‌های کنترل و یا تغییر در روند معمول رکوردهای ارسالی در شبکه می‌شوند. به‌عنوان مثال اگر یک حمله‌کننده قصد حمله انکار سرویس (DoS[۳۴]) به یک کنترل‌کننده را داشته است اجبارا ترافیک شبکه سیستم کنترل مطابق روال معمول نخواهد بود و تغییر می‌کند. در حملات دزدکی از دستورات به ظاهر مشروع برای خراب‌کاری در سیستم‌های کنترل سوء استفاده می‌کنند. در این نوع حملات پیچیده تغییری در ترافیک شبکه و یا روند معمول رکوردهای ارسالی در شبکه ایجاد نمی‌شود. بدین منظور حمله کننده باید از دستورات شناخته شده و قابل درک سیستم‌های کنترل سوء استفاده کند. شناسایی حملات دزدکی نیز با روش‌های شناسایی سایر حملات متفاوت است و روش‌های معمول در این گونه موارد کارایی ندارند. به‌منظور شناسایی کامل حملات به سیستم‌های کنترل ترکیبی از روش‌های شناسایی حملات دزدکی و شناسایی حملات به ترافیک شبکه سیستم کنترل را ارائه می‌دهیم. شکل (۱) دیاگرام ترکیبی روش‌های تشخیص حملات که در این مطالعه پیشنهاد شده است را نشان می‌دهد.



شکل (۱): ترکیب پیشنهادی روش‌های تشخیص حملات
Figure (1): Attack detection methods proposed combination

۳-۱- تشخیص حملات تاثیرگذار بر ترافیک شبکه

در این مطالعه برای تشخیص حملاتی که باعث تغییر در ترافیک نرمال شبکه و یا روند رکوردهای ارسالی در شبکه می‌شوند از روش‌های بر پایه قوانین تعریف شده استفاده نموده‌ایم. در این مطالعه برای بالا بردن دقت تشخیص، دو رویکرد موازی را در

پیش گرفته‌ایم. در رویکرد اول قوانین حاکم بر ترافیک نرمال شبکه را در حالت‌های مختلف استخراج نموده‌ایم و تخطی از این قوانین را بعدا برای تشخیص حالت غیر نرمال و حمله در نظر گرفته‌ایم. ترافیک نرمال شبکه را در حالت‌های مختلف دریافت و ذخیره نموده‌ایم. در ایستگاه‌های کاربری/مهندسی دو امکان مانیتورینگ و تغییرات مهندسی کنترل‌کننده وجود دارد با فرض اینکه یک ایستگاه می تواند بعنوان کاربری یا مهندسی و یا هر دو حالت مورد استفاده قرار گیرد ترکیبی از وضعیت‌های این دو حالت را تعریف و ترافیک شبکه را در تمامی وضعیت‌ها دریافت و ذخیره نموده‌ایم. جدول (۱) این حالت‌ها را نمایش می‌دهد.

Table (1): Different modes of a operation/engineering station

جدول(۱): حالت‌های مختلف یک ایستگاه کاربری/ مهندسی

نرم افزار مانیتورینگ	نرم افزار مهندسی
مانیتورینگ غیرفعال	نرم افزار مهندسی غیرفعال
مانیتورینگ فعال با یک صفحه گرافیک سبک	نرم افزار مهندسی فعال
مانیتورینگ فعال با یک صفحه گرافیک متوسط	نرم افزار مهندسی در حالت تغییرات آنلاین
مانیتورینگ فعال با یک صفحه گرافیک سنگین	نرم افزار مهندسی در حالت تغییرات آفلاین
مانیتورینگ فعال با چندین صفحه گرافیک سنگین	

با توجه به اینکه موارد ذکر شده در جدول بالا وضعیت نرمال یک ارتباط معمول میان یک ایستگاه کاربری/ مهندسی را نمایش می‌دهد، بررسی ترافیک شبکه و روند توالی رکوردهای ارتباطی در این حالت‌ها در جهت به‌دست آوردن قوانینی که بتواند حالت‌های غیر نرمال ترافیک شبکه و روند توالی را تشخیص دهد، مورد استفاده قرار گرفته است. بدیهی است که در این روش فرض تکراری بودن و ثابت بودن ترافیک شبکه که در سایر مطالعات مورد استفاده قرار گرفته است را در نظر نمی‌گیریم. حالت-های معمولی که ممکن است در یک ارتباط دو طرفه کنترل کننده و ایستگاه کاربری/ مهندسی وجود داشته باشد و اثرات این حالت‌ها بر ترافیک شبکه و روند رکوردهای تبادلی این حالت‌ها را برای تشخیص حالت‌های غیر بررسی کرده‌ایم. مثلا اگر کاربری صفحات زیادی از ایستگاه کاربری/ مهندسی را مورد استفاده قرار دهد، ترافیک شبکه سنگین و در غیر اینصورت سبک خواهد بود. این حالت‌ها به اراده و احتیاج‌های کاربر بستگی دارد لذا فرض تکراری بودن ترافیک شبکه در این حالت‌ها صحیح نیست و در این مطالعه نیز از آن پرهیز نموده‌ایم.

۳-۲- تشخیص حملات دزدکی یا یواشکی[۳۵]

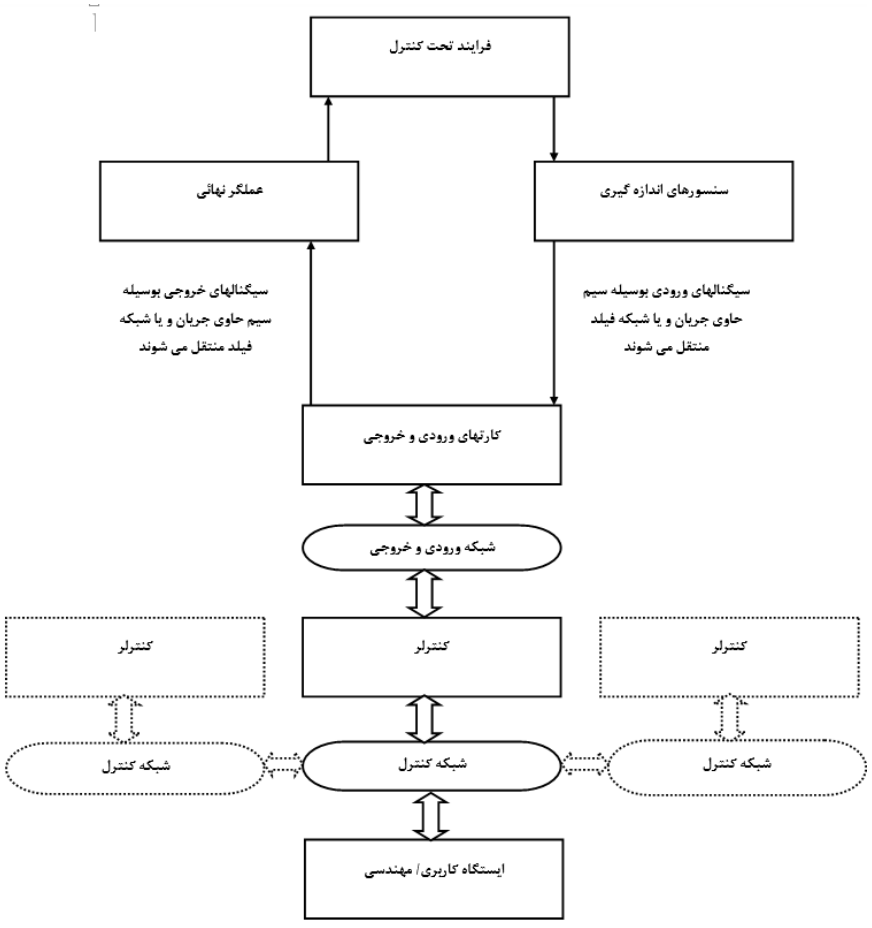
حملات دزدکی یا یواشکی حملات پیچیده‌ای هستند که از دستورات قانونی موجود در سیستم‌های کنترل سوء استفاده می-کنند. با توجه به اینکه این حملات ظاهر قانونی دارند و بر ترافیک شبکه سیستم‌های کنترل تاثیرگذار نیستند با استفاده از روش‌های ذکر شده در بخش قبلی قابل تشخیص نیستند. برای تشخیص این حملات از ترکیب دو رویکرد زیر استفاده نموده-ایم.

- تشخیص حملات دزدکی با استفاده از شناسایی دستورات قانونی از روی اثر امضاء دستورات با ضبط رکوردهای انتقالی شبکه
- تشخیص حملات دزدکی با استفاده از تغییر رفتار داده‌های فرایندی یا تغییر رفتار فرایند تحت کنترل

۳-۲-۱-تشخیص حملات دزدکی با استفاده از شناسایی دستورات قانونی از روی اثر امضاء دستورات با ضبط رکوردهای انتقالی شبکه

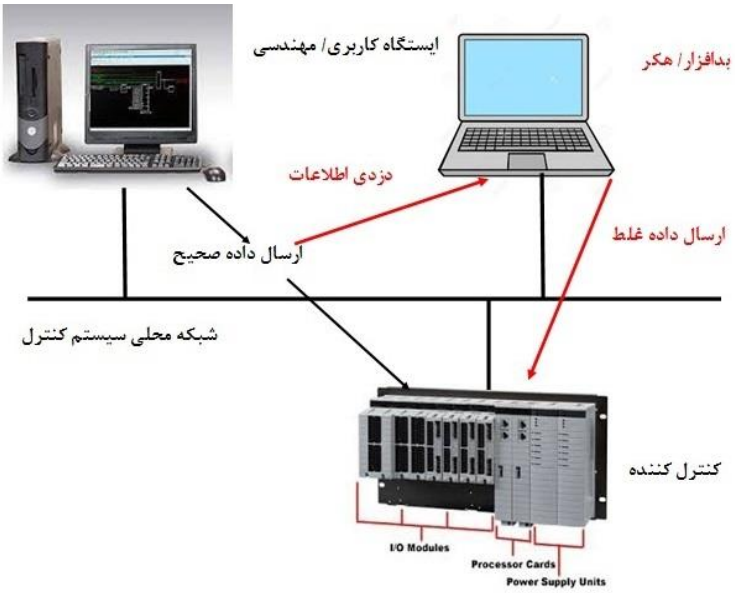
در حالت نرمال و عادی کاربر و یا مهندسین سیستم‌های کنترل که دارای مجوز لازم هستند از ایستگاه‌های کاربری و یا ایستگاه‌های مهندسی دستورات لازم کاربری و یا مهندسی را از طریق شبکه سیستم‌های کنترل به سیستم کنترل ارسال می-کنند. در این حالت فعالیت‌های انجام شده توسط نرم افزار ثبت وقایع در ایستگاه‌های کاربری و یا مهندسی ثبت می‌شود. شکل (۲) ساختار عملکرد یک سیستم کنترل را نمایش می‌دهد. دستوراتی که از ایستگاه‌های کاربری به سیستم کنترل می‌رسد توسط سیستم کنترل پردازش و سپس خروجی سیستم کنترل از طریق کارت‌های خروجی به عملگر نهائی[۳۶]ستور لازم را

صادر می‌کند. تغییراتی که عملگر نهائی ایجاد می‌کند باعث ایجاد اثر فیزیکی در فرایند تحت کنترل می‌شود. اگر یک هکر یا بدافزار بتواند بجای یک کاربر یا مهندس سیستم دستوراتی به ظاهر مشروع از ایستگاه‌های کاربری و یا هر عنصر متصل به شبکه به سیستم کنترل ارسال کند باعث اثرگذاری مخرب در فرایند تحت کنترل شده است. برای اجرای این نوع حمله در ابتدا نیاز هست که حمله‌کننده خود را بجای یک عنصر مشروع جا بزند که اصطلاحا به آن حمله مرد وسطی[۳۷](MIM) گفته می‌شود. در مرحله بعد حمله‌کننده دستورات مشروع در قالبی که برای سیستم کنترل قابل شناسایی باشد، ارسال می‌نماید. در قسمت دوم حمله عملیات تزریق داده غلط[۳۸]صورت گرفته است. محتمل‌ترین امکان برای یک حمله‌کننده در جهت اجرای این حمله استفاده از یکی از ایستگاه‌های کاربری و یا مهندسی موجود در شبکه است. شکل (۳) نمایی از یک حمله تزریق داده غلط به سیستم کنترل را نمایش می‌دهد. روش پیشنهادی این مطالعه تشخیص دستورات مشروع ارسالی به سیستم کنترل از روی بسته‌های ارسالی به کنترلرها از طریق شبکه انتقالی است. بدین منظور دستورات تشخیص داده شده از روی بسته‌های شبکه سیستم کنترل با دستورات ذخیره شده در ثبت وقایع نرم افزار مانیتورینگ و یا مهندسی مقایسه می‌گردد. در صورت اختلاف میان این دستورات نشانگر یک حالت غیر عادی در دستورات ارسالی به کنترلرها است. شکل (۴) فلوچارت نحوه تشخیص دستورات غیر عادی به کنترل‌کننده‌ها را نشان می‌دهد. در واقع این فلوچارت بیانگر سیستم تشخیص نفوذ دستورات مشروع است. اگر هکری حمله‌ای را در قالب دستورات مشروع تدارک ببیند آن دستور به دلیل اینکه خارج از روال نرم افزار مورد استفاده کاربر انجام شده است در فایل ثبت وقایع ذخیره نمی‌شود. بخش اصلی این سیستم تشخیص نفوذ، نحوه تشخیص دستورات مشروع از روی بسته‌های ارسالی شبکه است. به این منظور نیاز است که اثر امضاء کلیه دستورات ارسالی به کنترل-کننده‌ها تهیه و سپس رکوردهای ضبط شده شبکه سیستم کنترل برای تشخیص اثر امضاء مشابه مورد بازرسی قرار گیرد. در صورت مشابهت رکوردهای ارسالی با اثر امضاء یکی از دستورات، دستور مورد نظر شناسایی شده است.



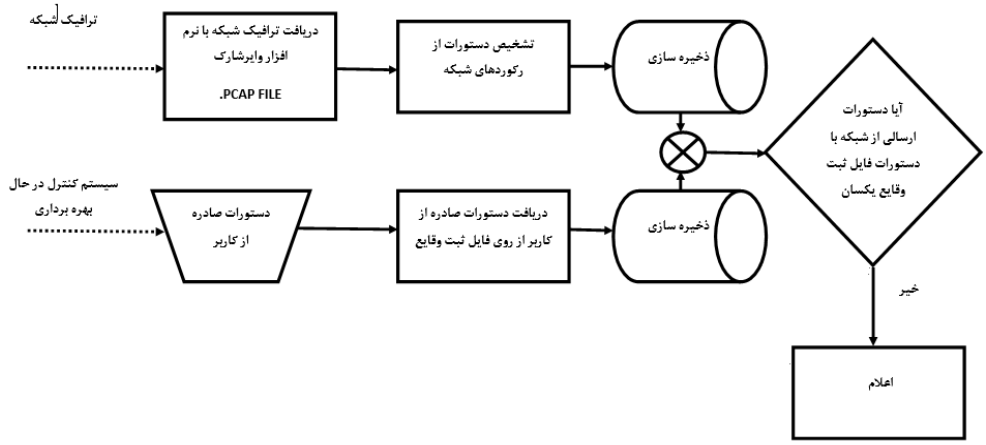
شکل (۲): ساختار عملکردی سیستم کنترل

Figure (2): Control system functional structure



شکل(۳): تزریق داده غلط به سیستم کنترل

Figure (3): Incorrect data injection to control system



شکل(۴): سیستم پیشنهادی تشخیص نفوذ دستورات به ظاهر مشروع

Figure (4): Proposed intrusion detection system for seemingly legitimate commands

برای به‌دست آوردن اثر امضاء دستورات از روی رکوردهای ارسالی نیاز است که این دستورات به‌صورت مکرر اجرا شوند و رکوردهای مربوطه در اجراهای مکرر مورد مقایسه قرار گیرند. از مقایسه رکوردهای حاصل از اجراهای مکرر تعداد رکورد موثر در اجرای این دستور، توالی این رکوردها و ویژگی‌های مورد نیاز در هر رکورد به‌دست می‌اید.

سه مورد ذکر شده شاخص‌های اصلی اثر امضاء دستورات هستند. منظور از ویژگی‌ها در این طرح پیشنهادی، فیلدهای موجود در پروتکل‌های شناخته شده شبکه مورد استفاده است. به‌عنوان مثال طول بسته ارسالی می‌تواند یکی از ویژگی‌های کلیدی مورد استفاده در رکوردها باشد. علاوه بر تعداد رکوردهای موثر توالی این رکوردها لازمه تشخیص اثر امضاء دستورات است.

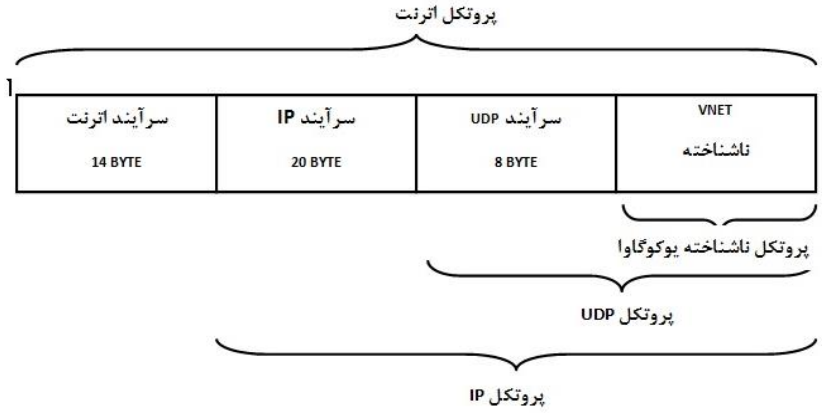
۳-۲-۲- تشخیص حملات دزدکی با استفاده از تغییر رفتار داده‌های فرایندی یا تغییر رفتار فرایند تحت کنترل

هدف از حملات معنایی و دزدکی تغییرات غیر عادی در فرایند تحت کنترل با استفاده از دستورات به ظاهر نجیب است. به این منظور حمله‌کننده پارامترها و یا متغیرهای مهم فرایند را دست‌کاری می‌کند. این تغییرات موجب اخلال در واحد تولیدی یا صدمه به دستگاه‌ها خواهد شد. در این روش با توجه به ماهیت فرایند تحت کنترل رفتار حالت عادی و نرمال فرایند، با استفاده از متغیرهای اندازه‌گیری شده فرایند، شبیه‌سازی می‌شود. در این روش داده‌های حالت‌های عادی که از سیستم‌های کنترل

جمع‌آوری شده است برای آموزش الگوریتم‌های یادگیری ماشین و داده‌کاوی استفاده می‌شوند. برای پیاده‌سازی و استفاده از این روش در کنار سایر روش‌های بیان شده نیاز به شناخت کامل فرایند تحت کنترل است. اصلی‌ترین مرحله این روش ساخت مجموعه داده اختصاصی برای آن فرایند تحت کنترل است.

۴- پیاده‌سازی و نتایج تجربی

برای دریافت داده‌های شبکه و ارزیابی روش‌های پیشنهادی و بررسی نتایج تجربی در این مطالعه از سیستم کنترل یوکوگاوا با شبکه پروتکل اختصاصی Vnet/IP بهره گرفته‌ایم. اطلاعات شبکه سیستم کنترل یوکوگاوا با نام Vnet بدلیل اختصاصی بودن نامشخص است. بنابراین با فرض نامشخص بودن اطلاعات فیلدهای این شبکه و فقط با مشخصات پروتکل‌های دیگری که این پروتکل بر آنها سوار شده است مطالعات این روش تکمیل شده است. در شکل (۵) ساختار و قالب کلی پروتکل Vnet/IP نمایش داده شده است [۳۸]. ساختار کلی سیستم‌های کنترل شبکه‌های متنوعی برای برقراری ارتباطات درونی و بیرونی وجود دارد. در این مطالعه هدف محافظت از خود کنترل‌کننده‌ها و توسعه سیستم تشخیص نفوذی است که انواع حملات به خود کنترل‌کننده را تشخیص دهد. بنابراین تمرکز این مطالعه بر روی شبکه Vnet/IP است که ارتباط فیمابین ایستگاه‌های کاربری/مهندسی و کنترل‌کننده‌ها را برقرار می‌کند. ارتباطات سایر اجزا داخلی و ارتباطات بیرونی خارج از بحث این پژوهش است. در این مطالعه فرض کرده‌ایم که در شبکه یک کنترل‌کننده و یک ایستگاه مهندسی/کاربری وجود دارد. بنابراین کلیه دستوراتی که توسط کاربر مجوزدار یا هکر و بدافزار اجرا می‌شود با مبدا این ایستگاه کاربری و به مقصد این کنترل‌کننده ارسال می‌گردد. در این مطالعه بسته و داده‌های شبکه را قبل از هر کنترل‌کننده به‌وسیله نرم‌افزار وایرشارک[۹]در فایل‌های pcap. جمع‌آوری کرده‌ایم. سپس با استفاده از امکان تی شارک فیلدهای مورد نیاز به فایل‌های CSV صادر نموده‌ایم. در این مطالعه برای آماده‌سازی داده‌ها و پیاده‌سازی روش‌های پیشنهادی از سخت افزار و نرم افزارهای موجود در جدول (۲) بهره گرفته‌ایم.



شکل(۵): قالب کلی پروتکل Vnet/IP

Figure (5): Vnet/IP protocol general format

Table (2): Hardware and software used for implementation

جدول (۲): سخت افزار و نرم افزار مورد استفاده جهت پیاده‌سازی

Computer Characteristics	DELL OPTIPLEX 9020 Intel Core i5-4570, CPU 3.2 GHZ, Memory 4 GB
Operating System	Windows 7 Ultimate 64 bit
Python Version	Anaconda ,Inc3.6.5
Keras Version	2.2.4
Tensorflow Version	1.15.0
Scikit-Learn Version	0.22.1
Numpy Version	1.17.4
Spyder Version	4.0.0
Pandas Version	0.25.3
Matplotlib Version	3.1.1
Pyod Version	0.7.7.1

۴-۱- پیاده‌سازی روش تشخیص حملات تاثیرگذار بر ترافیک شبکه

برای دریافت ترافیک شبکه در حالت نرمال یک مجموعه سیستم کامل یوکوگاوا با حداقل اجزاء مورد نیاز برپا داشته‌ایم. در این مجموعه تست از یک کنترل‌کننده یوکوگاوا به همراه نمونه‌های از کارت‌های ورودی و خروجی سیگنال یوکوگاوا، یک ایستگاه کاربری/ مهندسی، رایانه با نرم‌افزار وایرشارک برای جمع‌آوری داده‌های شبکه و یک سوییچ که برای اتصال این اجزاء، استفاده نموده‌ایم. سوئیچ به نحوی پیکربندی شده است که خروجی پورت ارسال و دریافت داده‌ها به سمت کنترل‌کننده را در پورتی که به کامپیوتر حاوی وایرشارک است، کپی می‌کند. بنابراین تمامی داده‌ها به سمت کنترل‌کننده دریافت می‌شود. شکل‌های (۶) و (۷) مجموعه تست و آزمایشگاه نمونه‌برداری سیستم کنترل یوکوگاوا را که برای دریافت ترافیک نرمال شبکه مورد استفاده قرار گرفته است نمایش می‌دهد. پس از دریافت ترافیک شبکه در حالت‌های مختلف نرمال و بررسی این ترافیک، قوانین تشخیص حالت غیر نرمال از روی داده‌های این ترافیک به‌دست آمده است. علاوه بر بررسی ترافیک عادی به‌منظور تکمیل قوانین تشخیص حملات معمول تاثیرگذار بر ترافیک شبکه رویکرد دومی نیز در این مطالعه مورد بررسی و استفاده قرار گرفته است. در این رویکرد حملات شناخته شده‌ای به کنترل‌کننده صورت گرفته و شبیه‌سازی شده است. با استفاده از ابزارهای نرم‌افزاری تست نفوذ و ارزیابی شبکه مطابق جدول (۳) حملاتی را به شبکه سیستم‌های کنترل و کنترل‌کننده اعمال نموده‌ایم و بسته‌های شبکه را در این حالت‌ها دریافت و ذخیره نموده‌ایم. از روی داده‌های به‌دست آمده قوانین تشخیص این حملات تولید شده است. در نتیجه اعمال این تست‌ها مشخص شد که کنترل‌کننده در قسمت ارتباطات با شبکه به شدت آسیب‌پذیر است و به‌راحتی ارتباط آن با شبکه تحت تاثیر حملات قطع می‌گردد. نتیجه قطع این ارتباط عدم کنترل کاربر بر مانیتورینگ سایت صنعتی تحت کنترل است که وضعیتی به شدت خطرناک است که می‌تواند بعنوان هدف اصلی حمله کننده-ها باشد. پس از دریافت ترافیک شبکه در حالت‌های مختلف کارکرد نرمال و تست با ابزارهای ذکر شده و بررسی این ترافیک، قوانین تشخیص حالت غیر نرمال از روی داده‌های این ترافیک ها به‌دست آمده است. تعدادی از این قوانین به‌صورت توصیفی در جدول (۴) مشخص شده است. این قوانین برای تولید تشخیص حملاتی که تاثیرگذار بر این ترافیک بوده است در این مطالعه مورد استفاده قرار گرفته است. در این مطالعه با ترکیب قوانین موجود در جدول (۴) به تشخیص حملات معمول تاثیرگذار بر ترافیک شبکه دست یافته‌ایم.

در این مطالعه جهت استخراج قوانین از روی رکوردهای جمع‌آوری شده، بیشتر قوانین واضح که به‌صورت چشمی قابل درک است، استخراج شده است. بدیهی است در مطالعات تکمیلی امکان استخراج قوانین بیشتری با شیوه‌های نوین وجود دارد ولی در این جا جهت جلوگیری از تطویل بحث به آن پرداخته نشده است. بدیهی است همانند تمامی روش‌های مبتنی بر قوانین تعریف شده این روش جهت شناسایی حملات شناخته شده بسیار کارا و تشخیص آن قطعی است ولی برای تشخیص حملات از قبل ناشناخته بستگی به تطابق اثرات حمله مورد نظر نسبت به حملات قبلی دارد و در صورت عدم تطابق نمی‌توان انتظار داشت که قابل تشخیص باشد.

شکل(۶): مجموعه تست سیستم کنترل یوکوگاوا

Figure (6): Yokogawa control system testbed

شکل(۷): آزمایشگاه نمونه‌برداری داده‌های سیستم کنترل یوکوگاوا
Figure (7): Yokogawa control system data sampling laboratory

Table (3): List of network penetration and testing tools used in this study
جدول (۳): لیست ابزار نفوذ و تست شبکه مورد استفاده در این مطالعه

Test Tools
UDP STRESS TESTER
UDP UNICORN
STAR TRINITY NETWORK TESTER
PORT SCANNER
UDP FLOODER
FBENCH
LOIC
ANGRY IP SCANNER
NS AUDITOR
NETWORK SCANNER

Table (4): Derived rules from normal traffic and attacks
جدول(۴): قوانین بدست آمده از ترافیک نرمال و حملات

ردیف	نمونه‌های از قوانین دریافتی ناشی از ترافیک نرمال و غیر نرمال شبکه حاصل از ابزارهای تست برای تشخیص حالت‌های غیر نرمال
۱	از ایستگاه‌های مهندسی و یا کاربری دو رکورد متوالی با طول ماکزیمم (۱۵۱۴بیات) به سمت کنترلر ارسال نمی‌شود.
۲	از ایستگاه‌های مهندسی و یا کاربری بیشتر از سه رکورد متوالی به سمت کنترلر ارسال نمی‌شود و حتما یک رکورد بازخورد باید از کنترلر به ایستگاه اپراتوری و یا کاربری فیمابین موجود باشد.
۳	بیشتر از ۵ رکورد متوالی نباید از یک مبدا ایستگاه اپراتوری و یا کاربری بصورت Broadcasting ارسال شود.
۴	پورت مقصد وقتی رکوردی از ایستگاه مهندسی یا اپراتوری به سمت کنترلر ارسال می شود برابر با ۵۳۱۳ یا ۹۹۴۰ است.
۵	پورتهای مبداء همواره ۳۳۴۴۰ و یا ۳۳۴۴۲ است.
۶	فاصله زمانی بین دو رکورد ارسالی به سمت کنترلر نباید کمتر از ۰/۰۰۰۰۰۳ ثانیه باشد
۷	بیشتر از دو رکورد متوالی با پروتکل ICMP نباید به سمت کنترلر ارسال شود.
۸	از یک مبداء مشخص در یک بازه زمانی محدود نباید بیشتر از دو رکورد با پروتکل ICMP به کنترلر ارسال شود.

۴-۲-پیاده‌سازی روش تشخیص حملات دزدکی با استفاده از شناسایی دستورات قانونی از روی اثر امضاء

برای پیاده‌سازی این روش، لیست دستورات کاربری و مهندسی که امکان اجرای آن از ایستگاه کاربری/ مهندسی وجود دارد، بر اساس مدارک سیستم کنترل یوکوگاوا و تجارب خبرگان این حوزه تهیه شده است. سپس با اجرای این دستورات تعداد رکوردهای ارسالی به شبکه، توالی رکوردها و فیلدهای لازم جهت تشخیص آنها به‌دست آمده است. برای هر کدام از این دستورات یک ماتریس که شامل موارد ذکر شده است در فایل CSV. به‌عنوان اثر امضاء آن دستور ذخیره شده است. در جدول (۵) لیست این دستورات که برای این سیستم کنترل خاص تهیه شده است نمایش داده شده است. لازم به ذکر است این

لیست با اندکی تغییر برای سایر برندهای سیستم‌های کنترل نیز می‌توان تهیه نمود. با توجه بـه فـرض ناشـناخته بـودن قالـب بسته پروتکل Vnet در این مطالعه از فیلدهای موجود در قالب بسته سایر پروتکل‌ها برای به‌دست آوردن ویژگی‌های لازم در اثر امضاء دستورات بهره‌گیری شده است. ویژگی‌های مورد استفاده در این مطالعه مطابق جدول (۶) است.

Table (5): Commands list

جدول(۵): لیست دستورات

Row	Name	Description
1	Start CPU	Start controller
2	Stop CPU	Stop controller
3	PID change	PID parameter change (for example setpoint change(
4	Controller configuration	Controller online configuration change
5	FB change	Function block or logic drawing change
6	Online download	Online download
7	Offline download	Whole programm configuration and offline download
8	IO node creation	Input / output node hardware creation
9	IOM configuration	IO module online configuration change
10	Module add	Add module in IO node
11	Module delete	Delete module from IO node

Table (6): Attribute used in signature

جدول(۶): ویژگی‌های مورد استفاده در اثر امضاء

Row	Feature name	Description
1	Frame.len	Total frame length
2	Eth.src	Ethernet source address
3	Eth.dst	Ethernet destination address
4	Eth.type	Ethernet type
5	IP.src	IP source address
6	IP.dst	IP destination address
7	IP.version	IP version
8	IP.len	IP frame length
9	IP.len-hdr	IP header length
10	IP.ttl	IP time to live
11	IP.proto	IP protocol
12	IP.fragment	IP fragment
13	IP.offset.frag	IP fragment offset
14	IP.count.fragment	IP fragment count
15	UDP.srcport	UDP source port
16	UDP.dstport	UDP destination port
17	UDP.length	UDP total length
18	Data.len	Vnet length

لازم به‌ذکر است این ویژگی‌ها با توجه به فرضیه‌ها برای این مطالعه به‌دست آمده است. مثلا به دلیـل ایـن‌کـه در ایـن مطالعـه فرض شده است یک کنترل‌کننده و یک ایستگاه کاربری/ مهندسی در شبکه وجود دارد آدرس‌های این دو در ویژگی‌ها گنجانده شده است. اگر تعداد ایستگاه‌ها افزایش یابد بدیهی است اثر امضاء دستورات صادر شده از هر ایستگاه متفاوت خواهد بود. دلیـل دیگر گنجاندن آدرس IP و فیزیکی کنترل‌کننده و ایستگاه کاربری در ویژگی‌های مورد استفاده در اثـر امضـاء اهمیـت تـوالی و ترتیب ارسال بسته‌ها از سوی طرفین برای یک دستور خاص است. به‌طور خلاصه این جدول شـامل ویژگـی‌هـای اسـت کـه در رکوردهای ارسالی بر روی شبکه می‌توانند جهت تشخیص اثر امضاء دستورات مورد استفاده قرار گیرند. سایر ویژگی‌ها در اینجـا تاثیر معناداری برای تشخیص دستورات نداشته‌اند. مرحله بعد از استخراج اثر امضاء دستورات، جستجو در رکوردهای دریافتی از شبکه برای یافتن اثر امضاء مشابه دستورات است. در رکوردهای دریافتی از شبکه تعداد زیادی رکورد غیر قابـل اسـتفاده مثـل رکوردهای که از ایستگاه‌های موجود در شبکه به‌صورت اشاعه عمومی[۱] ارسال شده است، موجـود اسـت. رکوردهـای نظـایر ایـن قبل از جستجو اثر امضاء دستورات حذف می‌شود. نتایج تجربی بر روی محیط تست توسعه داده شده نشان مـی‌دهـد کـه روش پیشنهادی قادر است کلیه دستورات ذکر شده که اثر امضاء آنها به‌دست آمده است، شناسایی کند. بدیهی است ایـن شـیوه بـه-

عنوان یک نمونه اولیه ارائه شده است و فرضیه‌های به‌کار گرفته شده ممکن است در یک محیط صنعتی واقعی صحیح نباشد ولی با توسعه این شیوه امکان شناسایی دستورات مشروع از روی رکوردهای شبکه بدون دانستن اطلاعات درون بسته‌های پروتکل خاص سیستم کنترل وجود دارد.

۴-۳- پیاده‌سازی روش تشخیص حملات دزدکی با استفاده از تغییر رفتار داده‌های فرایندی یا تغییر رفتار فرایند تحت کنترل

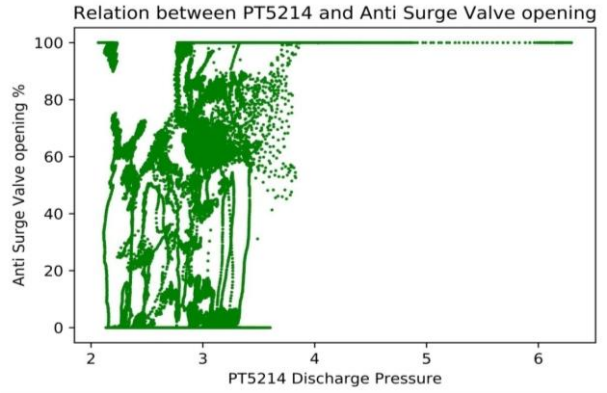
در این مطالعه برای بررسی کارایی این روش در کنار سایر روش‌های بیان شده از مجموعه داده‌ای که بیانگر حالت‌های عادی یک کمپرسور دورانی است، بهره‌گرفته ایم. این مجموعه داده به‌وسیله اطلاعات ثبت شده سنسورهای ابزاردقیق یک کمپرسور در حالت‌های مختلف کارکرد جمع‌آوری شده است. در مرحله پیش پردازش با استفاده از نمودارهای جفتی و مدارک سازنده کمپرسور و خبرگان این موضوع پارامترهای که وابستگی معناداری با خروجی‌های حیاتی سیستم کنترل داشته است را به‌عنوان ویژگی‌های این مجموعه داده انتخاب شده است. شکل (۸) یک نمودار جفتی است که ارتباط معنا دار بین فشار خروجی و میزان باز بودن شیر ایمنی جلوگیری از سرج بعنوان یکی از خروجی‌های حیاتی سیستم کنترل را نمایش می‌دهد. با استفاده از این نمودارها ویژگی‌های این مجموعه داده که تاثیرگذار بر خروجی‌های حیاتی سیستم کنترل هستند، به‌دست آمده است.

الگوریتم‌های مختلف رگرسیون غیر خطی، تشخیص داده‌های دیده نشده[۴۲]تشخیص ناهنجاری و طبقه‌بندی در این مجموعه داده اعمال و بهترین نتایج حاصل از الگوریتم‌های اعمال شده به این مجموعه داده در جدول (۷) نشان داده شده است. در این مطالعه الگوریتم‌های ذکر شده در ستون اول جدول بر روی مجموعه داده به‌دست آمده با ۲۰۰ هزار رکورد اعمال و این نتایج به‌دست آمده است. برای جلوگیری از سوءگیری الگوریتم‌ها و صحت سنجی نتایج از روش اعتبار سنجی 5-Fold بهره‌گیری شده است. همان‌طور که بیان شد برای استفاده از این روش با ترکیب سایر روش‌های ذکر شده نیاز است که فرایندی که توسط سیستم کنترل در حال کنترل است کاملا شناخته شود. این روش می‌تواند حملات دزدکی که تاثیر بر ترافیک شبکه نگذاشته‌اند ولی از دستورات مشروع به‌منظور خراب‌کاری در فرایند استفاده کرده‌اند را شناسایی کند. بدیهی است مجموعه داده و فرایندی که در این مطالعه مورد استفاده قرار گرفت، به‌عنوان نمونه‌ای برای معرفی این روش بوده است و برای سایر فرایندها باید شرایط خاص آن فرایند در نظر گرفته شود.

۵- نتیجه‌گیری و مطالعات آینده

به‌طور کلی حملات به سیستم‌های کنترل را می‌توان به دو گروه تقسیم‌بندی نمود. حملات منجر به تغییر ترافیک شبکه سیستم کنترل و حملات معنایی یا دزدکی. هدف از این مطالعه تشخیص کلیه حملاتی است که به سیستم‌های کنترل دارای شبکه ارتباطی با پروتکل‌های خاص صورت می گیرد، است. با توجه به این‌که اغلب بدافزارهای جدید و پیچیده برای حمله به سیستم‌های کنترل و در نهایت خراب‌کاری در فرایند فیزیکی از دستورات شناخته شده و قابل درک سیستم‌های کنترل سوء استفاده می‌کنند. اگر از این دستورات به ظاهر مشروع و قانونی در جهت خراب‌کاری استفاده شوند با روش‌های کنترل ترافیک شبکه بخصوص سیستم‌های کنترلی که دارای شبکه‌هایی با پروتکل‌های خاص هستند، قابل شناسایی نیستند. حملاتی که از دستورات مشروع سیستم‌های کنترل سوء استفاده می‌کنند تغییری در الگوی ترافیک و مشخصات پروتکل ایجاد نمی‌کنند. به‌منظور شناسایی کامل حملات به سیستم‌های کنترل ترکیبی از روش‌های شناسایی حملات دزدکی و شناسایی حملات به ترافیک شبکه سیستم کنترل را برای اولین بار به‌صورت عملی روی یک سیستم کنترل با شبکه خاص ارائه داده‌ایم. در این مطالعه برای تشخیص حملاتی که باعث تغییر در ترافیک نرمال شبکه و یا روند رکوردهای ارسالی در شبکه می‌شوند از روش‌های بر پایه قوانین تعریف شده استفاده نموده‌ایم. برای بالا بردن دقت تشخیص، دو رویکرد موازی را در پیش گرفته‌ایم. در رویکرد اول قوانین حاکم بر ترافیک نرمال شبکه را در حالت‌های مختلف استخراج نموده‌ایم و تخطی از این قوانین را بعدا برای تشخیص حالت غیر نرمال و حمله در نظر گرفته‌ایم. علاوه بر بررسی ترافیک عادی به‌منظور تکمیل قوانین تشخیص حملات معمول تاثیرگذار بر ترافیک شبکه رویکرد دومی نیز در این مطالعه مورد بررسی و استفاده قرار گرفته است. در این رویکرد برای

اولین بار حملات شناخته شده‌ای به کنترل‌کننده صورت گرفته و شبیه‌سازی شده است. با استفاده از ابزارهای نرم‌افزاری تست نفوذ و ارزیابی شبکه حملاتی را به شبکه سیستم‌های کنترل و کنترل‌کننده دارای شبکه اختصاصی اعمال نموده‌ایم و بسته‌های شبکه را در این حالت‌ها دریافت و ذخیره نموده‌ایم. از روی داده‌های به‌دست آمده قوانین تشخیص این حملات نیز تولید شده است. برای تشخیص حملات معنایی و دزدکی نیز دو رویکرد را به‌صورت موازی مورد استفاده قرار داده‌ایم. در رویکرد اول روشی ابتکاری مبتنی بر شبکه برای تشخیص دستوراتی که توسط یک حمله‌کننده بدون مجوز به سیستم کنترل اعمال می‌شوند، پیشنهاد شده است.



شکل(۸): نمودار جفتی رابطه بین فشار خروجی و میزان باز بودن شیر ضد سرج
Figure (8): Relation between anti surge valve opening and output pressure pair chart

Table (7): Result from different algorithm implementation

جدول(۷): نتایج حاصل از اعمال الگوریتم‌های مختلف

Algorithm	Accuracy	Precision	Recall	F1 Score	Cohens kappa	ROC AUC
Novelty Detection one class SVM	۰/۹۸۵۷۶۴	۱	۰/۹۷۹۶۴۰۸	۰/۹۸۹۷۱	۰/۹۶۶۶۰	۰/۹۸۹۸۲۰۴
Anomaly Detection KNN	۰/۹۹۴۵	۰/۹۶۱۱۵۵	۰/۹۹۹۲۷	۰/۹۷۹۸۳	۰/۹۷۶۶۴	۰/۹۹۶۵۱۷۶
Anomaly Detection ABOD	۰/۹۹۰۱	۰/۹۳۱۰۵۱	۰/۹۹۹۳۷	۰/۹۶۳۸۶	۰/۹۵۸۱۳	۰/۹۹۴۰۴۱۲
Classification K Neighbor Classifier	۰/۹۹۹۹۱۰	۰/۹۹۹۷۱۸	۱	۰/۹۹۹۸۵	۰/۹۹۹۷۹	۰/۹۹۹۹۳۴۸
Clasification SVC	۰/۹۹۹۹۱۰	۱	۰/۹۹۹۷۳	۰/۹۹۹۸۶	۰/۹۹۹۷۹	۰/۹۹۹۸۶۶۴
Classification Decision Tree Classifier	۰/۹۹۹۹۱۰	۱	۰/۹۹۹۷۳	۰/۹۹۹۸۶	۰/۹۹۹۸۰	۰/۹۹۹۸۶۹
Classification Random Forrest Classifier	۰/۹۹۹۹۱۰	۱	۰/۹۹۹۷۳	۰/۹۹۹۸۶	۰/۹۹۹۸۰	۰/۹۹۹۸۶۸۸
Classification AdaBoost Classifier	۰/۹۹۹۹۱۰	۰/۹۹۹۷۳۴	۱	۰/۹۹۹۸۶	۰/۹۹۹۸	۰/۹۹۹۹۳۳

این روش پیشنهادی برخلاف سایر روش‌های مبتنی بر شبکه قادر به تشخیص حملات معنایی و یواشکی به سیستم‌های کنترل است. در این مطالعه از روش تشخیص سوء استفاده و مبتنی بر بسته‌های ارسالی شبکه برای تشخیص دستورات به ظاهر مشروع استفاده می‌کنیم. در این مطالعه اثر امضاء دستوراتی که از ایستگاه اپراتوری به سمت سیستم کنترل ارسال می‌شود با ضبط ترافیک شبکه به‌دست آمده است. در این مطالعه برای تشخیص دستورات غیر نجیب، دستوراتی که از روی شبکه سیستم کنترل قبل از رسیدن به خود سیستم کنترل تشخیص داده می‌شود را با دستورات واقعی اجرا شده توسط اپراتور مقایسه می‌کنیم. با توجه به اینکه ممکن است سیستم‌های کنترل پروتکل شبکه‌های خاص خود را داشته باشند که اغلب در دسترس قرار ندارد و جزء اطلاعات اختصاصی سازندگان است بنابراین در این مطالعه فرض نموده‌ایم در مورد جزئیات پروتکل اختصاصی شبکه سیستم کنترل اطلاعاتی موجود نیست و بر این مبنی راه حل پیشنهادی را ارائه نموده‌ایم. بنابراین نوآوری این روش، ابتدا ترکیب روش‌های مختلف تشخیص حملات و بومی‌سازی آنها برای یک سیستم کنترل دارای شبکه اختصاصی است. دومین نوآوری استفاده از اطلاعات و بسته‌های شبکه برای تشخیص حملات معنایی بدون فرض تغییر در مشخصات پروتکل و ترافیک شبکه و همچنین بدون وابستگی به دانش جزئیات پروتکل اختصاصی سازندگان سیستم‌های کنترل است. در رویکرد

دوم برای تشخیص حملات معنایی و دزدکی از رفتار فرایند تحت کنترل استفاده می‌شود. با توجه به ماهیت فرایند تحت کنترل رفتار حالت عادی و نرمال فرایند، با استفاده از متغیرهای اندازه‌گیری شده فرایند، شبیه‌سازی می‌شود. در این روش داده‌های حالت‌های عادی که از سیستم‌های کنترل جمع‌آوری شده است برای آموزش الگوریتم‌های یادگیری ماشین و داده-کاوی استفاده می‌شوند. برای اینکه بتوانیم نتایج مدل پیشنهادی را در عمل و تجربه مورد بررسی قرار دهیم و یک نمونه واقعی از این مدل پیشنهادی را ارائه کنیم از یک بستر واقعی سیستم کنترل یوکوگاوا با شبکه Vnet/IP که تمامی مشخصه‌های ذکر شده قبلی را دارا است، بهره گرفته‌ایم. نتایج نشان می‌دهد که این روش ترکیبی، بخوبی قادر به تشخیص هردو نوع حمله منجر به تغییر ترافیک شبکه و همچنین حملات با استفاده از دستورات بظاهر مشروع که تغییری در ترافیک شبکه یا مشخصات پروتکل نمی‌دهند، است. نتایج تجربی در این مطالعه نشان داده است که قوانین استخراج شده به‌صورت صددرصد حملات مرتبط از قبل شناخته شده را شناسایی می‌کند. بدیهی است در این روش انتظار شناسایی حملات ناشناخته وجود ندارد. روش جدید ارائه شده مبتنی بر شناسایی دستورات سیستم کنترل از روی رکوردهای استخراج شده شبکه نیز به‌صورت کامل حملات معنایی را تشخیص می‌دهد. روش مبتنی بر داده‌های فرایندی مورد استفاده در این مطالعه نیز قادر به تشخیص حدود ۹۹ درصد از حملات معنایی با استفاده از الگوریتم‌های طبقه‌بندی و مجموعه داده استفاده شده است. البته کارایی این روش وابستگی شدید به نوع فرایند و داده‌های کلیدی انتخاب شده دارد. به دلیل اینکه در اغلب موارد امکان استفاده از مجموعه‌داده-های تولیدی استاندارد برای تولید سیستم‌های تشخیص نفوذ مبتنی بر شبکه، خاص سیستم‌های کنترل وجود ندارد با توسعه روش پیشنهادی در این مقاله امکان تشخیص حملات دیگر نیز وجود دارد. این مطالعه قابل توسعه به سایر سیستم‌های کنترل با مشخصات متفاوت و با دستورات مشروع متنوع تر نیز است. در این مطالعه که با فرض یک ایستگاه اپراتوری و یک کنترل کننده انجام شده است قابل توسعه به یک شبکه کامل سیستم‌های کنترل در مطالعات آینده است. همچنین در مطالعات آینده برای کشف قوانین در زمان نرمال و حمله از روی رکوردهای دریافتی از شبکه بجای کشف و جستجوی دستی شیوه‌های نوین نیز به کار گرفت. بدیهی است این شیوه بعنوان یک نمونه اولیه ارائه شده است و فرضیه‌های به کار گرفته شده ممکن است در یک محیط صنعتی واقعی صحیح نباشد ولی با توسعه این شیوه امکان شناسایی دستورات مشروع از روی رکوردهای شبکه بدون دانستن اطلاعات درون بسته‌های پروتکل خاص سیستم کنترل وجود دارد.

References

مراجع

[1] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, S. Sezer, "STPA-safeSec: Safety and security analysis for cyber-physical systems", Journal of Information Security and Applications, vol. 34, pp. 183-196, June 2017 (doi: 10.1016/j.jisa.2016.05.008).

[2] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, "Guide to industrial control system (ics) security", NIST Special Publication 800-82, 2015 (doi:10.6028/NIST.SP.800-82r2).

[3] D. Zhang, Q. Wang, G. Feng, Y. Shi, A. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber–physical systems", ISA Transactions, vol. 116, pp. 1-16, Jan.2021 (doi: 10.1016/j.isatra.2-021.01.036).

[4] M. Kravchik, A. Shabtai, "Efficient cyber attack detection in industrial control systems using lightweight neural networks and pca", IEEE Trans. on Dependable and Secure Computing, Jan. 2021 (doi: 10.1109/T-DSC.2021.3050101).

[5] S. Mokhtari, A. Abbaspour, KK. Yen, A. Sargolzaei, "A machine learning approach for anomaly detection in industrial control systems based on measurement data", Electronics, vol. 10, no. 4, Article Number: 407, Jan. 2021 (doi: 10.3390/electronics10040407).

[6] F. Zhang, JW. Hines, J. Coble, "Industrial control system testbed for cybersecurity research with industrial process data", Proceeding of the ICAPP, pp. 279-284, April 2018.

[7] C. Edward J.M, A. Kott, "Cyber-security of SCADA and other industrial control systems", Springer, 2016 (ISBN: 978-3-319-32125-7).

[8] E. Knapp, J. Langill, "Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems", Syngress; Dec. 2014.

[9] K. Stouffer, J. Falco, K. Scarfone, "Guide to industrial control systems (ICS) security", NIST special publication, 800(82), 16-16, 2011.

[10] R. Mitchell, I. Chen, "A survey of intrusion detection techniques for cyber-physical systems", Computer Science, ACM Computing Surveys, vol. 46, Article Number: 55, April 2014 (doi: 10.1145/2542049).
[11] Y. Hu, A. Yang, H. Li, Y. Sun, L. Sun, "A survey of intrusion detection on industrial controlsystems", International Journal of Distributed Sensor Networks, vol. 14, no. 8, pp. 1-14, Aug. 2018 (doi: 10.1177/155-0147718794615).
[12] C. Xavier, J. Moyano, G. Leon, " A real-time anomaly-based IDS for cyber-attack detection at the industrial process level of critical infrastructures", International Journal of Critical Infrastructure Protection, vol. 23, pp. 11-20, Dec. 2018 (doi: 10.1016/j.ijcip.2018.08.002).
[13] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, A. Hotho, "A survey of network-based intrusion detection data sets", Computers and Security, vol. 86, pp. 147-167, Sept. 2019 (doi: 10.1016/j.cose.2019.0-6.005).
[14] H. Zhengbing, L. Zhitang, W. Junqi, "A novel network intrusion detection system (NIDS) based on signatures search of data mining", Proceeding of the IEEE/WKDD, pp. 10-16, Adelaide, SA, Australia, Jan. 2008 (doi: 10.1109/WKDD.2008.48).
[15] A. Javaid, Q. Niyaz, W. Sun, M. Alam, "A deep learning approach for network intrusion detection system", Proceedings of the BIONETICS, vol. 24, pp. 21-26, 2016 (doi: 10.4108/eai.3-12-2015.2262516).
[16] N. Shone, T.N. Ngoc, V.D. Phai, Q. Shi, "A deep learning approach to network intrusion detection", IEEE Trans. on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, Feb. 2018 (doi: 10.1109/-TETCI.2017.2772792).
[17] M. Momeni, S. Gharravi, F. Hourali, "Reducing the impact of SYN flood attacks by improving the accuracy of the PSO algorithm by adaptive effective filters", Journal of Intelligent Procedures in Electrical Technology, vol. 10, np. 37, pp. 51-57, Spring 2019 (in Persian).
[18] E. Faghihnia, S.R.K. Tabakh Farizani, M. Kheirabadi, "Improved intrusion detection system based on distributed self-adaptive genetic algorithm to solve support vector machine in form of multi kernel learning with auto encoder", Journal of Intelligent Procedures in Electrical Technology, vol. 12, no. 45, pp. 77-93, Spring 2021 (dor: 20.1001.1.23223871.1400.12.1.6.2) (in Persian).
[19] N. Moustafa, J. Hu, J. Slay, "A holistic review of network anomaly detection systems: Acomprehensive survey", Journal of Network and Computer Application, vol. 128, pp. 33-55, 2019 (doi: 10.1016/j.jnca.201-8.12.006).
[20] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, A. Valdes, "Using model-based intrusion detection for SCADA networks", Proceedings of the SCADA security scientific symposium, vol. 46, pp. 1-12, Jan. 2007.
[21] A. Carcano, I. Fovino, M. Masera, A. Trombetta, "State-based network intrusion detection systems for SCADA protocols: a proof of concept", InInternational Workshop on Critical Information Infrastructures Security, pp. 138-150, Berlin, Heidelberg, Sept. 2009 (doi: 10.1007/978-3-642-14379-3_12).
[22] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, H. Wang, "Rule-based intrusion detection system for SCADA networks", Proceeding of the IEEE/RPG, pp. 1-4, Beijing, Sept. 2013 (doi: 10.1049/cp.2013.1729).
[23] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, H.F. Wang, "Intrusion detection system for IEC 60870-5-104 based SCADA networks", Proceeding of the IEEE/PESMG, pp. 1-5, Vancouver, BC, Canada, July 2013 (doi: 10.1109/PESMG.2013.6672100).
[24] B. Zachry, J. Butts, J. Lopez Jr, T. Dube, "Firmware modification attacks on programmable logic controllers", International Journal of Critical Infrastructure Protection, vol. 6, pp. 76-84, 2013 (doi: 10.101-6/j.ijcip.2013.04.004).
[25] S. Carl, J. Butts, S. Dunlap, "An evaluation of modification attacks on programmable logic controllers", International Journal of Critical Infrastructure Protection, vol. 7, pp. 61-68, 2014 (doi: 10.1016/j.ijcip.201-4.01.004).
[26] N. Hubballi, V. Suryanarayanan, "False alarm minimization techniques in signature-based intrusion detection systems: A survey", Computer Communications, vol. 49, pp. 1-17, 2014 (doi: 10.1016/j.comcom.20-14.04.012).
[27] G. Wei, M. Thomas, "On cyber attacks and signature based intrusion detection for modbus based industrial control systems", Journal of Digital Forensics, Security and Law, vol. 9, Article Number: 3, 2014 (doi: 10.15394/jdfsl.2014.1162).
[28] B.K. Kim, D.H. Kang, T.M. Chung, "Detecting abnormal behavior in SCADA networks using normal traffic pattern learning", Computer Science and its Applications, Springer, Berlin, Heidelberg, pp. 121-126, 2015 (doi: 10.1007/978-3-662-45402-2_18).
[29] L. Yingxu, Z. Liu, Z. Song, Y. Wang, Y. Gao, "Anomaly detection in industrial autonomous decentralized system based on time series", Simulation Modelling Practice and Theory, vol. 65, pp. 57-71, June 2016 (doi: 10.1016/j.simpat.2016.01.013).

[30] Y. Peng, J. Liang, G. Xu, "Malware detection method for the industrial control systems", Proceeding of the IEEE/CCIS, pp. 255-259, Beijing, China, Aug. 2016 (doi: 10.23919/JCC.2021.01.012).
[31] W. Li, L. Xie, Z. Deng, Z. Wang, "False sequential logic attack on SCADA system and its physical impact analysis", Computers and Security, vol. 58, pp. 149-159, June 2016 (doi: 10.1016/j.cose.2016.01.001).
[32] A. Kleinmann, O. Amichay, A. Wool, D. Tenenbaum, O. Bar, L. Lev, "Stealthy deception attacks against SCADA systems", Computer and Security, vol. 14, pp. 93-109, Sept. 2017 (doi: 10.1007/978-3-319-72817-9_7).
[33] L. Chih-Yuan, S. Nadjm-Tehrani, M. Asplund, "Timing-based anomaly detection in SCADA networks", International Conference on Critical Information Infrastructures Security, pp. 48-59, Cham, 2017 (doi: 10.1-007/978-3-319-99843-5_5).
[34] J. Yun, Y. Hwang, W. Lee, H. Ahn, S. Kim, "Statistical similarity of critical infrastructure network traffic based on nearest neighbor distances", InInternational Symposium on Research in Attacks, Intrusions, and Defenses, vol. 10, pp. 577-599, Cham, Sept. 2018 (doi: 10.1007/978-3-030-00470-5_27).
[35] A. Robles-Durazno, N. Moradpoor, J. McWhinnie, G. Russell, I. Maneru-Marin, "PLC memory attack detection and response in a clean water supply system", International Journal of Critical Infrastructure Protection, vol. 26, Article Number: 100300, Sept. 2019 (doi: 10.1016/j.ijcip.2019.05.003).
[36] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, J. Coble, "Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data", IEEETrans. on Industrial Informatics, vol. 15, no. 7, pp. 4362-4369, July 2019 (doi: 10.1109/TII.2019.2891261).
[37] M. Kalech, "Cyber-attack detection in SCADA systems using temporal pattern recognition techniques", Computers & Security, vol. 84, pp. 225-238, 2019 (doi: 10.1016/j.cose.2019.03.007).
[38] Vnet/IP Built In Security, Technical Information, Doc No:TI30A10A20-01E, 2011, Yokogawa Corporation.

زیرنویس‌ها

1. Intrusion detection system
2. Network based IDS
3. Host based IDS
4. Anomaly detection
5. Misuse detection
6. Signature
7. Zero day
8. Deep inspection
9. Semantic
10. Stealthy
11. Rule based IDS
12. Network security laboratory-international knowledge discovery and data mining
13. Yokogawa CS300
14. Vnet/IP
15. International knowledge discovery and data mining
16. The defense advanced research projects agency
17. Signature aperiori
18. Non-symmetric deep auto encoder
19. Unsupervised feature learning
20. Modbus/TCP
21. Modbus
22. Supervisory control and data acquisition
23. Deep packet inspection
24. Rule based IDS
25. Allen bradley control logix l61
26. Security information and event management
27. Fuzz test
28. Mutate
29. Timing based anomaly detection
30. Defense in depth
31. False Data Injection
32. Temporal pattern recognition
33. Emerson delta V

34. Denial of service
35. Stealthy
36. Actuator
37. Man in the middle
38. Data false injection
39. Wireshark
40. Tshark
41. Broadcasting
42. Novelty detection