فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

Winter, 2021, 2 (4), 45-50
DOR: 20.1001.1.27832570.1400.2.4.9.6

Received: 23 Aug 2021
Accepted: 12 Oct 2021

Providing a Solution Based on Fuzzy Logic to Reduce False Positive Alarms in the Intrusion Detection System

Mohammad Akhlaghpour

1.MSc, Member of Young Researchers and Elites Club, Faculty of Computer, Khorasghan Branch, Islamic Azad University, Isfahan, Iran. M.Akhlaghpour@khuisf.ac.ir

Abstract

Introduction: The intrusion detection system is responsible for identifying and detecting unauthorized external use of the system that is misused or damaged by internal users. Therefore, the intrusion detection system is created in the form of software and hardware, each of which has its own advantages and disadvantages. The speed and accuracy of the hardware system and the failure of their security by intruders are other features of such systems. If the software related to intrusion detection, acceptability, and the difference between different operating systems are used, they give more generality to the software systems. More suitable software systems are chosen.

Method: The behavior of the intrusion detection system is discussed in opposition to various intrusion methods, and in order to deal with intrusion into the system and computer networks, several methods have been created under the name of intrusion detection, which monitors the events that have occurred in a system and into computer networks.

Results: the performance of the intrusion detection system is presented in order to influence the behavior of the abuse detection system as well as anomaly detection using fuzzy logic based on an alpha device. The obtained results showed the accuracy rate up to 91.26% and the detection of false alarms up to 90.96%.

Discussion: An Intrusion detection system is essential as the first line of defense for the network. Many algorithms depend on the quality of the data set provided for intrusion detection. Of course, in recent developments in knowledge data collection access systems, there has been an increase in interest in data-driven approaches to curb the increase in control system cyber-attacks related to false alarms. Most machine learning-based intrusion detection systems rely on web applications/operating systems or network layers to detect targeted attacks by host or network. Nevertheless, there is still a lack of sufficient research in the evaluation and collection of intrusion detection system datasets for false alarm behaviors, which requires further studies in this field.

Keywords: Intrusion Detection System, False Alarms, Computer Networks, Fuzzy Logic.

فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

ارائه راه‌کاری مبتنی‌بر منطق فازی جهت کاهش هشدارهای مثبت کاذب در سیستم تشخیص نفوذ

تاریخ دریافت: ۱۴۰۰/۰۶/۰۱
تاریخ پذیرش: ۱۴۰۰/۰۷/۲۰

سال دوم، زمستان ۱۴۰۰
شمارهٔ چهارم، صص: ۴۵ – ۵۰

محمد اخلاق‌پور

کارشناسی ارشد، عضو باشگاه پژوهشگران جوان، دانشکدهٔ کامپیوتر، واحد خوراسگان، دانشگاه آزاد اسلامی، اصفهان، ایران.
M.Akhlaghpour@khuisf.ac.ir

چکیده: سیستم تشخیص نفوذ به‌عنوان اولین خط دفاعی برای شبکه ضروری است. الگوریتم‌های زیادی در کیفیت مجموعه داده‌های ارائه‌شده برای شناسایی نفوذ تأثیردارد. البته تحولات اخیر در سیستم‌های دستیابی به مجموعه داده‌های دانش، باعث افزایش علاقه در رویکردهای داده‌محور برای مهار افزایش حملات سایبری سیستم کنترلی مرتبط با هشدارهای کاذب شده‌است. بیشتر سیستم‌های تشخیص نفوذ مبتنی‌بر یادگیری ماشین به‌منظور شناسایی حملات هدفمند توسط میزبان یا شبکه به برنامه‌های وب / سیستم عامل یا سطح شبکه متکی هستند. بااین‌وجود، متأسفانه کمبود تحقیقات کافی در ارزیابی و جمع‌آوری مجموعه داده‌های مربوط به سیستم تشخیص نفوذ برای رفتارهای هشدارهای کاذب هم‌چنان وجوددارد، که مطالعات بیشتر در این حوزه را می‌طلبد. در این مقاله عملکرد سیستم تشخیص نفوذ، به‌منظور بررسی تأثیر رفتار سیستم تشخیص سوءاستفاده و هم‌چنین تشخیص ناهنجاری با استفاده از منطق فازی مبتنی‌بر دستگاه آلفا ارائه‌شده است. نتایج به‌دست‌آمده میزان دقت را تا ۹۱/۲۶٪ و تشخیص هشدارهای کاذب را تا میزان ۹۰/۹۶٪ نشان‌داده‌است.

واژه‌های کلیدی: سیستم تشخیص نفوذ، هشدارهای کاذب، شبکه‌های کامپیوتری، منطق فازی.

1. مقدمه

سیستم تشخیص نفوذ[1]، وظیفه شناسایی و تشخیص هرگونه استفادهٔ غیرمجاز از سیستم و سوءاستفاده یا آسیب تو سط کاربران داخلی و خارجی را برعهده دارد. از همین‌رو، سیستم تشخیص نفوذ، به صورت نرم‌افزار و سخت‌افزار ایجادشده‌است که هرکدام مزایا و معایب خاص خود را دارند.

سرعت و دقت از مزایای سیستم سخت‌افزاری بوده و عدم شکست امنیتی آن‌ها توسط نفوذگران، قابلیت دیگر این‌گونه سیستم‌ها است. در صورتی‌که استفاده آسان از نرم‌افزارهای مرتبط به تشخیص نفوذ، قابلیت انعطاف‌پذیری و تفاوت سیستم عامل مختلف، عمومیت بیشتری به سیستم‌های نرم‌افزاری می‌دهند؛ بنابراین سیستم‌های نرم‌افزاری، انتخاب مناسب‌تری هستند. در همین راستا رفتار این سیستم در تقابل با انواع روش‌های نفوذ مطرح است. به‌منظور مقابله با نفوذ به سیستم و شبکه‌های کامپیوتری، روش‌های متعددی تحت‌عنوان تشخیص نفوذ ایجادشده‌است، که عمل نظارت بر وقایع اتفاق‌افتاده در یک سیستم به شبکه کامپیوتری را برعهده‌دارند و به دو دسته رفتار غیرعادی[2] و مبتنی‌بر امضاء[3] تقسیم‌می‌شوند.

در روش تشخیص رفتار غیرعادی، یک نما از رفتار عادی ایجاد می‌شود و برای تشخیص چنین رفتاری باید رفتار عادی را شناسایی‌کرده و الگوها و قواعد خاصی برای آن‌ها پیداکرد. بنابراین نفوذهای غیرعادی برای تشخیص سخت هستند؛ زیرا هیچ‌گونه الگوی ثابتی برای نظارت وجود ندارد. از همین رو، تکنیک و معیارهایی در تشخیص رفتار غیرعادی تحت‌عنوان تشخیص سطح آستانه[4]، معیارهای آماری[5] و معیارهای فانون‌گرا[6] به‌کارمی‌روند.

در این مقاله به‌کمک مجموعه داده ،کشف دانش و داده‌کاوی[7] ۱۹۹۸، سیستمی برای افزایش میزان دقت و تشخیص هشدار کاذب با استفاده از منطق فازی مبتنی‌بر دستگاه آلفا ارائه‌شده‌است. نتایج به‌دست آمده میزان دقت را تا ۹۱/۲۶٪ و تشخیص هشدارهای کاذب را تا میزان ۹۰/۹۶٪ نشان‌داده‌است.

انواع معماری سیستم تشخیص نفوذ

سیستم‌های تشخیص نفوذ، دارای معماری‌های متفاوتی مانند معماریمبتنی‌بر میزبان[8]، مبتنی‌بر شبکه[9] و مبتنی‌بر توزیع‌شده[10] شناخته‌می‌شوند. که هرکدام دارای حالت‌های منحصر به خود و مزایا و معایب هستند.

در سیستم تشخیص نفوذ مبتنی‌بر میزبان، می‌توانند حملات و تهدیداتی را روی سیستم‌های بحرانی را تشخیص‌دهند، که شامل دسترسی به فایل‌ها، اسب تروا و ... می‌شوند و توسط سیستم تشخیص نفوذ مبتنی‌بر شبکه قابل‌تشخیص نیستند.

یکی از مزایای سیستم تشخص نفوذ مبتنی‌بر میزبان، توانایی سازماندهی بسیار خوب تصمیمات برای هر میزبان منحصربه‌فرد می‌باشد. در مقابل نیز، سازگاری کم‌بین سیستم عامل و در نتیجه نرم‌افزارهای چندگانه، از معایب سیستم تشخیص نفوذ مبتنی‌بر میزبان هستند، که تنها برای یک سیستم عامل نوشته‌می‌شوند.

در سیستم تشخیص نفوذ مبتنی‌بر شبکه، وظیفه شناسایی و تشخیص نفوذهای غیرمجاز را قبل از رسیدن به سیستم‌های بحرانی برعهده‌دارند. این نوع سیستم، معمولاً دو بخش ناظر[11] و عامل[12]را شامل می‌شود. این دو بخش معمولاً در پشت دیواره آتش و بقیه نقاط دسترسی برای تشخیص هرنوع فعالیت غیرمجاز نصب‌می‌گردند.

سیستم‌های تشخیص نفود مبتنی‌بر شبکه، می‌توانند طوری برنامه‌ریزی‌شوند که مزاحمتی در طول کار ایجادنشود و حضور هر حمله‌ای که تشخیص‌می‌دهند را درون فایل رویدادها ثبت‌کنند و بدون این‌که مهاجم متوجه‌شود، به مدیر شبکه اطلاع‌دهند. هم‌چنین از معایب سیستم تشخیص نفوذ مبتنی‌بر شبکه، می‌توان به واحد گزارش‌گیری اشاره‌کرد که می‌توانند تعداد زیادی از رویدادها را گزارش‌دهند. به‌همین دلیل به یک فرد متخصص نیاز است تا گزارش‌ها را تجزیه و تحلیل کرده و موارد نادرست را شناسایی‌نماید.

در سیستم تشخیص نفوذ توزیع‌شده، از چندین سیستم تشخیص نفوذ، مبتنی‌بر میزبان یا میتنی‌بر شبکه یا ترکیبی از این دو نوع همراه یک ایستگاه مدیریت مرکزی تشکیل شده‌است. از همین رو، ایستگاه مرکزی، وظیفه بررسی گزارش‌های رسیده یا آگاه‌سازی مسئول امنیتی سیستم و هم‌چنین وظیفه به‌روزرسانی پایگاه قوانین تشخیص هریک از سیستم‌های تشخیص نفوذ موجود در شبکه را برعهده‌دارد. هم‌چنین در سیستم تشخیص نفوذ توزیع‌شده، پیچیدگی زیاد است و بر این اساس، مشخصات این نوع سیستم‌ها، کامل مشخص‌نیست. بنابراین با وجود معماری و پویایی در شناسایی هشدارهای کاذب، می‌توان در حوزه‌های متفاوت ،راه‌کارهایی مؤثر در شناسایی نفوذ ارائه‌نمود.

2. پیشینهٔ پژوهش

در تحقیق لی یو و همکارانش در سال ۲۰۲۰ آمده که بیشتر ابزارهای تشخیص نفوذ مبتنی‌بر یادگیری ماشینی که برای سیستم‌های کنترل صنعتی تهیه‌شده‌اند، روی بسته‌های شبکه آموزش به‌صورت ضبط‌شده، قراردادهمی‌شوند و برای تشخیص نفوذ، تنها به نظارت بر ترافیک لایه شبکه متکی‌اند. این امر باعث ایجاد سیستم‌های ضعف نفوذ می شود، زیرا حملات سایبری سیستم‌های کنترل صنعتی تأثیر واقعی و معناداری بر متغیر فرآیند دارند که در این مطالعه نیز آمده‌است، تعداد محدودی از محققان اندازه‌گیری فرآیند را درنظرمی‌گیرند. بااین‌حال، در سیستم‌های پیچیده، تغییر متغیر فرآیند می‌تواند ناشی از ترکیب‌های مختلف از وقایع غیرطبیعی باشد. در این مقاله پیشرفت‌های اخیر در الگوریتم‌های تشخیص نفوذ، محدودیت‌ها، چالش‌ها و وضعیت کاربرد آن‌ها در زیرساخت‌های مهم بررسی‌شده‌است [۱].

در تحقیق مارکس و همکارش در سال ۲۰۲۰ آمده است که حملات سایبری به اینترنت اشیاء با سرعت نگران‌کننده‌ای در حال رشدند، زیرا فناوری‌های اینترنت اشیاء، به‌معنای واقعی کلمه همه چیز را به شبکه‌ها وصل می‌کنند. در سال ۲۰۲۰، بیش از ۲۵٪ از حملات شناسایی‌شده در شرکت‌ها، اینترنت اشیاء را درگیرخواهدکرد. ازاین‌رو، درمان امنیت اینترنت اشیاء به‌عنوان یک فاکتور طراحی اجباری بسیار مهم است. علاوه بر این، سیستم مستقر اینترنت اشیاء باید پیوسته بررسی‌شود تا رفتارهای مخرب مانند ریزش بسته، انتشار کرم یا حملات را ردیابی‌کند. در این مقاله سیستم تشخیص نفوذ مبتنی‌بر ناهنجاری به‌منظور شبکه‌های بلوتوث مش[۱۳] ارائه‌شده‌است. قراردادن بهینه ساعت‌های نگهبان براساس شبیه‌سازی‌های انجام‌شده توسط نرم‌افزار BMW watch Sim پیشنهادشده که نتایج آزمایشی حاصل از آزمایشگاه نشان‌داده‌است که قرارگرفتن ساعت نگهبان پیشنهادشده توسط شبیه‌ساز امکان شناسایی مؤثر نفوذهای دنیای واقعی را فراهم‌می‌آورد [۲].

در تحقیق ا سیری و همکارش در سال ۲۰۲۰ ا شاره شده ا ست که نفوذ در سیستم‌های نظارت کنترل و اکتساب داده‌ها، موردتوجه محققان قرارگرفته‌است، زیرا اتصال به شبکه‌های عمومی در بسیاری از صنایع ضروری است. ماهیت و ویژگی‌های سیستم‌های نظارت کنترل و انتساب داده‌ها، ملاحظات و تکنیک‌های خاصی را برای تشخیص تزریق لازم‌می‌داند و کارهای بسیاری نیز در این زمینه انجام‌شده‌است و از تکنیک‌های تشخیص نفوذ عمومی گرفته تا تغییرات خاص که مخصوص سیستم‌های نظارت کنترل و اکتساب داده‌ها طراحی‌شده‌اند. از همین‌رو، این مقاله به یک طبقه‌بندی پرداخته‌است که ویژگی های ویژه سیستم‌های تشخیص نفوذ سایبر فیزیکی را با نمونه‌هایی از ادبیات ارائه‌می‌دهد. علاوه بر این، یک مطالعه موردی برای مقایسه داده‌های خط لوله گاز شبیه‌سازی‌شده برای مقایسه اثربخشی طبقه‌بندی درخت تصمیم‌گیری به‌منظور طبقه‌بندی‌های مختلف در سیستم‌های نظارت کنترل و اکتساب داده‌ها، ارائه شده‌ا ست. در نتایج آمده‌ا ست، سیستم تشخیص نفوذ که ترکیبی از معیارهای فیزیکی و شبکه استفاده‌می‌کند، می‌تواند به‌طور قابل توجهی فقط از معیارهای شبکه یا معیارهای فیزیکی استفاده‌کند [۳].

تحقیق کونال و همکارش در سال ۲۰۲۰ نیز به گسترش سریع شبکه‌های رایانه‌ای که باعث بروز آسیب‌پذیری می‌شود، اشاره‌دارد که به‌نوبه‌خود امنیت را به‌خطرمی‌اندازد. بنابراین، به نظارت بر ترافیک شبکه منتقل‌شده از طریق این شبکه‌ها نیاز است. از همین‌رو، آسیب‌پذیری شبکه می‌تواند خسارات بزرگی را به سازمان‌ها واردکند و یک سیستم مؤثر و قدرتمند تشخیص نفوذ می‌تواند ناهنجاری‌ها را شناسایی‌کرده و درصورت نیاز، زنگ خطر ایجادکند. در این مطالعه هم‌چنین آمده است که اخیراً تکنیک‌های یادگیری ماشین برای ساختن سیستم‌های هوشمند شناسایی ناهنجاری، برای شناسایی حملات جدید محبوبیت زیادی کسب‌کرده‌اند و دقت زیادی نیز دارند. در همین راستا، طبقه‌بندی یادگیری ماشین ابتدا با استفاده از داده‌های آموزشی برای یادگیری الگوی حمله به تهاجم‌ها آموزش داده‌می‌شوند و سپس در برابر داده‌های آزمون برای تمایز داده‌های عادی و داده‌های غیرعادی آزمایش‌می‌شوند. در این مقاله با استفاده از تکنیک ارزیابی ویژگی‌های مبتنی‌بر رتبه‌بندی برای کاهش تعداد صفات و ارزیابی مدل اجراشده با استفاده از گروه IBK (K-NN)، درخت تصادفی، REP Tree، j48graft و طبقه‌بندی‌کننده جنگل تصادفی به نتایج تجربی دقت طبقه‌بندی دودویی ۹۹/۷۲٪ و طبقه‌بندی چند طبقه با ۹۹/۶۹٪ دست‌یافته‌اند، که این مدل از داده‌های NSL-KDD برای ارزیابی عملکردها استفاده شده است. بنابراین با نتایج تجربی در این مقاله مطرح‌شده‌است، پیچیدگی زمان و هزینه محاسباتی به‌دلیل کاهش ابعادی داده‌ها و رویکرد ترکیبی که برای طبقه‌بندی استفاده‌می‌شود، به حداقل رسیده‌است [۴].

در تحقیق سان و همکارش در سال ۲۰۲۰ آمده که با پیشرفت و رشد فن‌آوری‌های مختلف بی‌سیم، پیاده‌سازی سیستم‌های قدرتمند تشخیص نفوذ ضروری است. در این مقاله برروی اجرای طبقه‌بندی مبتنی‌بر Deep Gated Recurrent Unit (DGRU) و هم‌چنین یک الگوریتم استخراج ویژگی مبتنی‌بر بسته‌بندی برای بی‌سیم سیستم تشخیص نفوذ، ارائه‌شده‌است. در عملکرد DGRU IDS، با استفاده از مجموعه داده‌های معیار NSL-KDD ارزیابی‌شده‌است. علاوه بر این، از چندین الگوریتم محبوب از جمله شبکه‌های عصبی مصنوعی، حافظه کوتاه‌مدت عمیق، کوتاه‌مدت، جنگل تصادفی، بی‌هوای بیبی و شبکه‌های عصبی عمیق پیش‌بینی به‌منظور مقایسه، استفاده‌شده‌است. نتایج تجربی این تحقیق نشان‌داده‌است که DGRU IDS افزایش عملکرد قابل‌توجهی نسبت به روش‌های موجودداشته‌است [۵].

در تحقیق انجام شده لی و همکاران‌اش در سال ۲۰۲۰ ا شاره شده که چندین سال است روش‌های یادگیری ماشین به‌طور گسترده در تشخیص نفوذ استفاده‌می‌شود. بااین‌حال، این تکنیک‌ها همچنان از نبود مجموعه داده‌های دارای برچسب، سربار سنگین و دقت کم رنج‌می‌برند. از همین‌رو، برای بهبود دقت طبقه‌بندی و کاهش زمان آموزش در این مقاله به یک روش یادگیری عمیق مؤثر، یعنی سیستم تشخیص نفوذ نفوذ خودکار-رمزگذار براساس الگوریتم جنگل تصادفی ارائه شده‌ا ست. این روش مجموعه آموزشی را با انتخاب ویژگی‌ها و گروه‌بندی ویژگی‌ها ایجادمی‌کند. براساس این تحقیق، پس از آموزش، این مدل می‌تواند نتایج را با رمزگذار خودکار پیش‌بینی‌نماید و زمان تشخیص را تا حد زیادی کاهش‌دهد و به‌طور مؤثر دقت پیش‌بینی را بهبودبخشد. نتایج تجربی این تحقیق نشان‌داده ا ست، که روش پیشنهادی از نظر آموزش آ سان، با سازگاری قوی و دقت بالا در تشخیص به ما شین‌های سنتی مبتنی‌بر روش‌های تشخیص نفوذ متکی بر ماشین برتری دارد[۶].

3. روش پیشنهادی

در این تحقیق به کمک برنامه شبیه‌ساز، با استفاده از روش مرکب و پروفایل آلفا، در میزان دقت و کاهش هشدارهای کاذب افزایش و بهبود قابل‌توجهی داشته‌است.

در این شبیه‌سازی ابتدا داده‌های آموزشی و آزمایشی به‌عنوان نمونه از مجموعه داده کشف دانش و داده‌کاوی ۱۹۹۸ گرفته می‌شود. هم‌چنین فیلترکردن برای ویژگی‌های کم‌اهمیت و نویزپرداز، برای کاهش ابعاد داده استفاده‌می‌شوند.

آزمایش اعتبارسنجی انجام‌شده، توسط شبکه پخش زمینه در ماژول تشخیص سوءاستفاده ارزیابی‌می‌شوند. به‌علاوه، اگر شبکه پخش پس‌زمینه در شبیه‌سازی نتواند نوع حمله را تشخیص‌دهد، مکانیزم یادگیری توسط تشدید انطباقی شبکه برای دسته‌بندی حملات ناشناخته پیاده‌سازی‌می‌شود.

تمام ویژگی‌ها، تأثیر قاطع روی خروجی حاصل از دسته‌بندی‌ها ندارند؛ بعضی از این ویژگی‌ها، حتی دسته‌بندی‌های اشتباهی را تولیدمی‌کنند. از این رو، انتخاب ویژگی مناسب، فاکتور بسیار مهمی می‌باشد که می‌تواند روی کارآیی در سیستم‌های تشخیص نفوذ، تأثیرگذار باشد. قبل از آموزش مدل شبکه پخش پس‌زمینه، باید برای داده‌های آموزشی، نرمال‌شود و این داده‌های آموزشی باید به داده‌هایی که توسط شبکه پخش پس‌زمینه قابل‌تشخیص باشند، تبدیل‌شوند.

این شبیه‌سازی با استفاده از nntool، در نرم‌افزار متلب پیاده‌سازی شده‌است و کارایی آزمایش‌های انجام‌شده با استفاده از فرمول‌های Detection rate، False Positive rate و Accuracy ارزیابی‌شده‌است:

۱) نرخ تشخیص: $\frac{\text{تعداد تشخیص حملات}}{\text{تعداد حملات}} \times ۱۰۰$

۲) نرخ مثبت کاذب: $\frac{\text{تعداد ارتباطات طبقه‌بندی}}{\text{تعداد ارتباطات غیرعادی}} \times ۱۰۰$

۳) دقت: $\frac{\text{ارتباطات صحیح طبقه‌بندی‌شده}}{\text{تعداد ارتباطات}} \times ۱۰۰$

نتایج شبیه‌سازی در جدول (۱) نشان‌داده‌شده است.

جدول ۱: کارآیی ارزیابی‌شده تشخیص نفوذ ترکیبی

نرخ تشخیص (٪)	دقت (٪)
۹۰/۹۶	۹۱/۲۶

از kdd.data_10_percent.gz به‌عنوان نمونه آموزشی و آزمایشی مجموعه داده آزمایشی استفاده‌شده‌است.

4. ارزیابی

همان‌گونه که در تعاریف سیستم تشخیص نفوذ و معرفی معماری‌های پایه‌ای سیستم تشخیص نفوذ، اشاره‌شده‌است، باتوجه به توسعه شبکه‌های رایانه‌ای برای توسعه و بهبود اثربخش سیستم‌ها، مدل‌های مختلفی برای تشخیص و هم‌چنین کاهش هشدارهای کاذب به‌وجودآمده‌اند.

با اشاره به تحقیقات انجام‌شده و استفاده از منطق فازی مبتنی‌بر دستگاه آلفا به‌کمک مجموعه داده کشف دانش و داده‌کاوی نتایج به‌دست‌آمده میزان دقت ۹۱/۲۶٪ و تشخیص هشدارهای کاذب تا میزان ۹۰/۹۶٪ بهبودیافته‌است.

مدل‌هایی هم‌چون یادگیری ماشین، ناهنجاری و ... نیز در وضعیت شناسایی حملات نسبت به شرایط مشابه ادوار گذشته، بهبودیافته‌است. بنابراین سیستم تشخیص نفوذ، نقش تأثیرگذاری برای شناسایی و ارتقاء سیستم‌های شبکه‌ای در حوزه‌های متفاوت دارد. به‌عنوان نمونه، از آن جا که الگوریتم یادگیری ماشین برای طبقه‌بندی ترافیک و تشخیص رفتار مخرب در شبکه‌های اینترنت اشیاء استفاده‌می شود، تصمیم‌گیری مشارکتی که توسط چندین نگهبان توزیع‌شده در مناطق مختلف شبکه درنظرگرفته‌شده، وظیفه پردازش ترافیک عمدتاً محلی را برعهده‌دارند.

۶. نتیجه‌گیری و کارهای آینده

سیستم تشخیص نفوذ، به لحاظ توسعه روزافزون استفاده از سیستم‌های شبکه‌ای از اهمیت بالایی برخوردارند. ازهمین‌رو، در این مقاله رفتار سیستم تشخیص نفوذ را بنا به تعدادی از آخرین تحقیقات ارائه‌شده در سال ۲۰۲۰، باتوجه به معماری‌های مختلف ارائه‌شده، بررسی‌کرده‌ایم. مقایسه تحقیقات ارائه‌شده با مطالعات مشابه پیشین نشان‌دهنده آن بود که عملکرد سیستم تشخیص نفوذ بنابه استفاده از الگوریتم‌های تعریف‌شده، نتایج قابل‌قبولی نسبت‌به وضعیت‌های پیشین داشته‌است.

در همین راستا با استفاده از منطق فازی مبتنی‌بر دستگاه آلفا، به‌منظور افزایش تشخیص هشدارهای کاذب و افزایش دقت اقدام‌شد که نتایج به‌دست‌آمده میزان دقت ۹۱/۲۶٪ و نرخ تشخیص ۹۰/۹۶٪ را نشان‌داد. لذا، با ادامه روند مطالعات می‌توان در زمینه سیستم تشخیص نفوذ در کاهش هشدارهای کاذب و هم‌چنین ارتقاء بهره‌وری در حوزه‌های مرتبط با پیشگیری و شناسایی نفوذ ارائه‌نمود.

به‌عنوان پیشنهاد به‌منظور مطالعات آینده، استفاده از الگوریتم زنبورعسل پیشنهادمی‌شود و هم‌چنین در مورد قابلیت اطمینان داده‌ها و منابع موجود مخازن داده منبع باز در توسعه سیستم‌های شناسایی نفوذ، می‌تواند تحقیق جامع‌تری صورت‌پذیرد.

پی‌نوشت

1. Intrusion Detection System (IDS)
2. Anomaly Detection
3. Signature-based
4. Threshold Detection
5. Statistical Measure
6. Rule-based Measure
7. Knowledge Discovery Data Mining (KDD)\
8. Host-based Detection
9. Network-based Detection
10. Distributed Detection
11. Monitor
12. Agent
13. Mesh

مراجع

[1] A. Ayodeji, Y.-k. Liu, N. Chao, L.-q. Yang, A new perspective towards the development of robust data-driven intrusion detection for industrial control systems, Nuclear Engineering and Technology (2020).

[2] M. Krzysztoń, M. Marks, Simulation of watchdog placement for cooperative anomaly detection in Bluetooth Mesh Intrusion Detection System, Simulation Modelling Practice and Theory, (2020).

[3] M. Al-Asiri, El-S. M. El-Alfy, On Using Physical Based Intrusion Detection in SCADA Systems, Procedia Computer Science 170, (2020).

[4] Kunala, M. Dua, Attribute Selection and Ensemble Classifier based Novel Approach to Intrusion Detection System, Procedia Computer Science 167, (2020).

[5] S. M. Kasongo, Y. Sun, A Deep Gated Recurrent Unit based model for wireless intrusion detection system, ICT Express, (2020).

[6] X. K. Li, W. Chen, Q. Zhang, L. Wu, Building Auto-Encoder Intrusion Detection System based on random forest feature selection, Computers & Security, (2020).