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

Spring 2023, 4 (1), 1-10
DOI: 10.71856/impcs.2023.903591

Received: 19 Feb 2023
Accepted: 16 Apr 2023

مقاله پژوهشی

Using the Modified Colonial Competition Algorithm to Increase the Speed and Accuracy of the Intelligent Intrusion Detection System

Mohammad Nazarpour[1], Navid Nezafati[۲*], Sajjad Shokouhyar[3]

1. Ph.D. Student, Department of Information Technology Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran.
2. Assistant Professor, Department of Management, Shahid Beheshti University, Tehran, Iran. (*Corresponding Author*), n_nezafati@sbu.ac.ir
3. Associate professor, Department of Management, Shahid Beheshti University,Tehran, Iran.

Abstract

Introduction: In recent decades, rapid development in the world of technology and networks has achieved, also there is a spread of Internet of thing services in all fields over the world. Piracy numbers have increased, also a lot of modern systems were penetrated. Thus the developing information security technologies to detect the new attack become an important requirement.

Method: One of the most important information security technologies is an Intrusion Detection System (IDS) that uses machine learning and deep learning techniques to detect anomalies in the network. In all of the information processing systems, detecting cyber-attacks is one of the main challenges and its effects can be blocked or limited by timely detection of attacks. The IoT system is no exception to this phenomenon, and with the high development of this technology and the expansion of its infrastructure, the need for an intelligent intrusion detection system with high accuracy and speed is essential. Neural networks are modern systems and computational methods for machine learning, knowledge representation, and the application of acquired knowledge to maximize the output accuracy of complex systems. Neural networks have already been used to solve many problems related to pattern recognition, data mining, data compression and research is still underway with regards to intrusion detection systems. One of the disadvantages of using training with classical methods in neural networks is getting stuck in local optimal points. In this paper, we use the meta-heuristic algorithm of Imperial competition algorithm (ICA) to train neural networks and show that in the field of intrusion detection in the IoT system, it can show much better accuracy and speed to classical training methods.

Results: Results show that our proposed method has 90% accuracy. This method has a better performance in comparison to classical neural network that has 75% accuracy.

Discussion: In this article, we will show that the use of imperial competition evolutionary optimization algorithms instead of traditional methods can increase the accuracy of the IDS system. In addition, evolutionary optimization algorithms are zero order and less complicated than gradient methods. Therefore, using this method, in addition to reducing the cost of system implementation, can increase the speed and accuracy of intrusion detection. In addition, from reliability point of view, we will show that the ICA-based systems are more stable in different implementations.

Keywords: Attack detection, neural network, fuzzy rule, adaptive formulation, ICA algorithm.

فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران
واحد زنجان

استفاده از الگوریتم رقابت استعماری اصلاح‌شده برای افزایش سرعت و دقت سیستم تشخیص نفوذ هوشمند

تاریخ دریافت:۱۴۰۱/۱۱/۳۰
تاریخ پذیرش: ۱۴۰۲/۰۱/۲۷

دورهٔ چهارم، بهار ۱۴۰۲
شمارهٔ اول، صص: ۱-۱۰

محمد نظرپور[۱]، نوید نظافتی[۲*]، سجاد شکوهیار[۳]

۱. دانشجوی دکتری، مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران.
۲. استادیار، گروه مدیریت، دانشگاه شهید بهشتی، تهران، ایران. (نویسندهٔ مسئول) n_nezafati@sbu.ac.ir
3. دانشیار، گروه، مدیریت، دانشگاه شهید بهشتی، تهران، ایران.

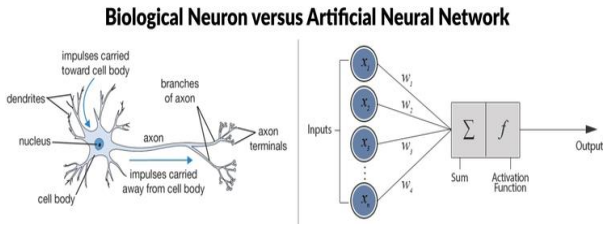
چکیده: در تمام سیستم‌های پردازش اطلاعات، شناسایی حملات سایبری یک چالش اصلی محسوب‌می‌شود و با شناسایی به‌موقع حملات می‌توان اثرات آن را مسدود یا کم کرد. سیستم اینترنت اشیا نیز از این پدیده مستثنی نبوده و با پیشرفت رو به رشد این فناوری و گسترش زیرساخت‌های آن، نیاز به سیستم تشخیص نفوذ هوشمند با دقت و سرعت بالا یک امر ضروری است. شبکه‌های عصبی سیستم‌های مدرنی هستند که از روش‌های محاسباتی نوین برای یادگیری ماشین، نمایش دانش و در نهایت استفاده از دانش کسب‌شده برای به حداکثر رساندن پاسخ‌های خروجی سیستم‌های پیچیده استفاده‌می‌کنند. یکی از معایب استفاده از آموزش با روش‌های کلاسیک در شبکه‌های عصبی، گیرافتادن در نقاط بهینه محلی است. در این مقاله از الگوریتم فراابتکاری رقابت امپریال (ICA) برای آموزش شبکه های عصبی استفاده‌کرده، نشان‌دادیم که این الگوریتم در زمینه تشخیص نفوذ در سیستم اینترنت اشیا، می‌تواند عملکرد بسیار بهتری از منظر سرعت و دقت نسبت به روش‌های آموزشی کلاسیک داشته‌باشد. نتایج نشان‌می‌دهد روش پیشنهادی دارای دقت ۹۰٪ می‌باشد که در مقایسه با روش شبکه عصبی کلاسیک که دارای دقت ۷۵ درصد بوده عملکرد بهتری دارد.

واژه‌های کلیدی: تشخیص حمله، شبکه عصبی، قانون فازی، فرمولاسیون انطباقی، الگوریتمICA .

مقدمه

امروزه فناوری جدیدی به نام اینترنت اشیا در حال گسترش روزافزون است. تحلیل‌ها نشان‌می‌دهند که این فناوری جدید که گامی بزرگ در تحول فضای مجازی محسوب‌می‌شود، علاوه بر تاثیرگذاری بر تمامی عرصه‌های زندگی بشر در آینده ، در بسیاری از حوزه‌ها کاربردهای فراوان خواهدداشت. اینترنت اشیا شامل شبکه‌ای از اشیا است که می‌توانند از طریق کامپیوتر و اینترنت با اشیاء دیگر ارتباط برقرارکنند. هر یک از این اشیاء هوشمند دارای آدرس پروتکل اینترنتی مخصوص به خود هستند تا از این طریق دستگاه ارسال‌کننده یا دریافت‌کننده اطلاعات قابل شناسایی باشد. این اشیاء هوشمند قادر به تشکیل سیستم‌هایی هستند که توانایی برقراری ارتباط با یکدیگر را دارند. چنین سیستم‌هایی پتانسیل زیادی برای تغییرات اساسی در خانه‌ها، مکان‌های اجتماعی، شرکت‌ها و حتی شهرها و بخش‌های مختلف اقتصادی در سطوح داخلی و بین‌المللی کشورها دارند. تحلیلگران اقتصادی پیش‌بینی‌می‌کنند که این فناوری در دهه آینده سهم چشمگیری در رشد اقتصادی خواهدداشت. حوزه‌هایی که در آینده به‌طور اجتناب‌ناپذیری تحت‌تأثیر این فناوری قرارخواهندگرفت عبارتند از: کشاورزی، انرژی، مدیریت دولتی، مراقبت‌های بهداشتی، تولید، صنعت و حمل و نقل. در عین حال، بزرگترین چالشی که در این زمینه وجوددارد تامین امنیت این دستگاه-هاست. این موضوع باعث‌شده‌است که شرکت‌های اینترنتی برنامه‌ریزی-کنند تا روزبه‌روز خدمات جدید خود را در این زمینه افزایش‌دهند.

چالش‌هایی در تجاری‌سازی فناوری اینترنت اشیا وجوددارد که باید مورد توجه قرارگیرد. یکی از مهم‌ترین چالش‌ها حفظ حریم خصوصی و امنیت اطلاعات است [۳-۱]. باید اذعان داشت که رضایت مصرف-کنندگان از این فناوری به این چالش‌ها بستگی دارد. امروزه فناوری اینترنت اشیا از فناوری‌های پیشرفته‌ای مانند انتقال داده از طریق مسیرهای فیبر نوری، استفاده از رایانش ابری و سایر فناوری‌های به‌روز برای ارسال و دریافت سیگنال، پردازش و ذخیره‌سازی استفاده‌می‌کند که تهدید حملات به زیرساخت‌های این حوزه را افزایش‌می‌دهد. تهدیدها و حملاتی که در حوزه اینترنت اشیاء رخ‌می‌دهد را می‌توان به چهار دسته کلی طبقه‌بندی‌کرد: ۱- حملات سرویس انکار (DOS) ۲ - حملات خطرات شناسایی رمز عبور از راه دور (R2L) ۳ - حملات خطرات کشف رمز عبور کاربر از اساس (U2R) ۴-جستجو و تحقیق در مورد حملات (PROBING). یکی از راه‌های مقابله با حملات و تهدیدها در اینترنت اشیا، استفاده از مدل‌ها و مکانیسم‌های یادگیری ماشینی است [۹-۴]. یادگیری ماشینی زیرمجموعه‌ای از فناوری هوش مصنوعی است که عمدتاً مبتنی بر یادگیری ماشینی مبتنی بر تجربیات خودِ ماشین و پیش‌بینی‌های ناشی از آن تجربیات است. الگوریتم‌های یادگیری ماشین، از مجموعه‌ای از داده‌ها به نام مجموعه داده‌های آموزشی استفاده‌می‌کنند و مدل‌های مورد نیاز را به‌وجودمی‌آورند. هنگامی که داده‌های جدید به الگوریتم یادگیری ماشین واردمی‌شود، سیستم می‌تواند فرآیند پیش‌بینی را بر اساس مدل ایجادشده اجراکند. یکی از معروف‌ترین، پرکاربردترین و قوی‌ترین الگوریتم‌ها و مدل‌ها برای ماشین‌های یادگیری، شبکه عصبی مصنوعی است [۱۴-۱۰]. هدف این مقاله شناسایی تهدیدات و حملات یک سیستم اینترنت اشیا از طریق شبکه عصبی مصنوعی اصلاح‌شده است. هدفِ این مقاله شناسایی تهدیدها و حملات سیستم اینترنت اشیا توسط یک شبکه عصبی مصنوعی اصلاح‌شده است. شبکه‌های عصبی ساختارهای شبکه‌ای بسیار سازمان‌یافته اند که بر اساس مدل عملکرد سیستم عصبی انسان طراحی‌شده‌اند. شبکه‌های عصبی سه لایه ورودی، میانی و خروجی توسط نورون‌ها تشکیل‌شده و به هم متصل‌می‌شوند. در شبکه‌های عصبی، اطلاعات از طریق نورون‌های ورودی دریافت‌می‌شود. لایه‌های میانی و نورون‌ها که ممکن است به صورت چندلایه باشند، این اطلاعات را دریافت، سپس آن را پردازش و تجزیه و تحلیل می‌کنند. انتقال اطلاعات تا رسیدن به لایه خروجی ادامه‌می‌یابد. شبکه عصبی همچنین از یک مدل ریاضی یا محاسباتی برای پردازش اطلاعات استفاده‌می‌کند که بر اساس رویکرد اتصالی- محاسباتی عمل‌می‌کند. یکی از انواع کلاسیک شبکه‌های عصبی مصنوعی، شبکه پرسپترون است. شکل۱ شماتیک یک شبکه عصبی مصنوعی و یک شبکه عصبی بیولوژیکی را نشان‌می‌دهد.



شکل۱: شماتیک نورون بیولوژیکی (سمت چپ) در مقابل شبکه عصبی مصنوعی (سمت راست)

در شبکه عصبی مصنوعی، داده‌های X1 تا Xn وارد نورون‌های ورودی می‌شوند. سپس هریک از این داده‌ها در ضرایب W ضرب‌می‌شوند. باید توجه‌داشت که فرآیند آموزش بر اساس داده‌های ورودی است و ضرایب W در پایان فرآیند تشخیص داده‌می‌شوند. حاصل‌ضرب داده‌های ثابت (w) در داده‌های X به مقادیر ثابتی به نام بایاس (b) اضافه‌می‌شود که باید در فرآیند آموزش نیز تشخیص داده‌شود. در نهایت، تمام این مقادیر در لایه خروجی واردمی‌شوند. آخرین لایه شامل یک تابع فعال است که یک تابع غیرخطی محسوب‌می‌شود. تاکنون روش‌های مختلفی برای آموزش شبکه‌های عصبی یا به‌عبارتی تعیین ضرایب w برای مجموعه داده‌های یک سیستم ارائه‌شده‌است. متداول‌ترین روش آموزش روش بازگشت BP است زیرا این سیستم سرعت عملکرد مطلوبی در یافتن پاسخ بهینه ضرایب W دارد [۱۶-۱۵]. در این روش در هر تکرار دو مرحله وجوددارد. در مرحله اول ضرایب W اولیه در داده ضرب‌می‌شود و عملیات تا رسیدن به خروجی ادامه‌می‌یابد و این خروجی احتمالاً با خروجی واقعی بسیار فاصله دارد. سپس خطای بین خروجی واقعی و خروجی محاسبه‌شده توسط شبکه عصبی محاسبه‌می‌شود. اکنون که

متوجه‌شدیم الگوریتم از نظر وزن و انحراف چه مقدار خطا دارد، در یک الگوی تکرار به مرحله دوم می‌رویم. در این مرحله، می‌توانیم به عقب برگردیم و وزن‌ها و انحراف‌ها را همگام کنیم. یعنی وزن‌ها و انحراف‌ها را طوری تغییردهیم که در تکرار بعدی نتیجه‌ای نزدیکتر به خروجی واقعی با خطای کمتر تولیدکنند. متأسفانه، همه این الگوریتم‌ها که بر روی یک شیب خطا عمل‌می‌کنند، در گیرافتادن در نقطه بهینه محلی دچار مشکل‌می‌شوند و قادر به دریافت پاسخ سراسری نیستند [۱۸-۱۷]. این گیرافتادن در نقطه پاسخ محلی منجر به توقف جریان آموزش شبکه عصبی قبل از رسیدن به پاسخ بهینه اولیه می‌شود.

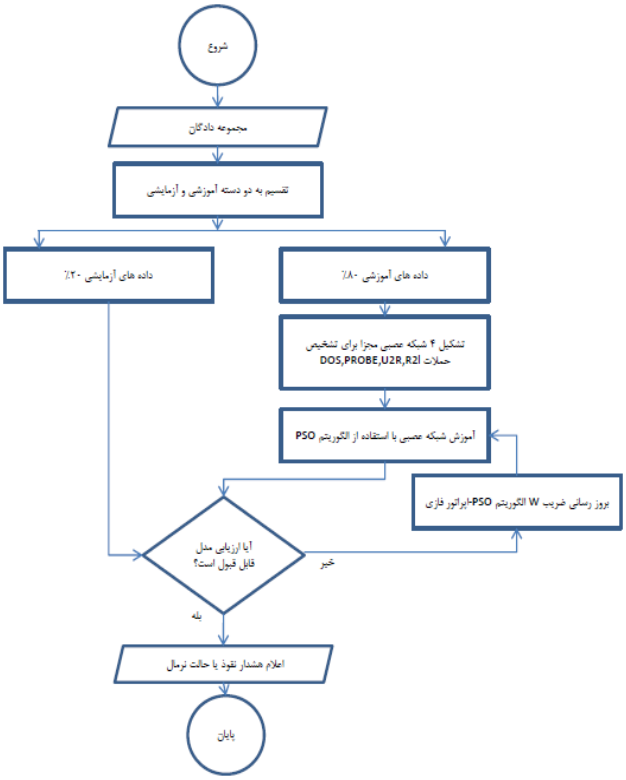
با این فرآیند آموزشی، شبکه عصبی قادر به ارائه مدل دقیقی از سیستم نیست و باید به روش‌های آموزشی دقیق‌تری نگاه‌کنیم. یکی از راه‌های احتمالی به‌دست‌آوردن یک مدل دقیق از سیستم مبتنی بر شبکه عصبی، استفاده از الگوریتم‌های بهینه‌سازی تکاملی است. الگوریتم‌های بهینه‌سازی تکاملی قادر به بهینه‌سازی و حل مسائل بسیار پیچیده و همچنین مسائل چندمنظوره هستند. یکی از الگوریتم‌های بهینه‌سازی تکاملی که سرعت عملکرد خوبی دارد، الگوریتم PSO است. علاوه بر این، این الگوریتم مانند سایر الگوریتم‌های تکاملی (ژنتیک و رقابت استعماری و غیره) محاسبات ساده‌تری دارد. در این مقاله، ما از الگوریتم PSO برای آموزش شبکه عصبی استفاده‌کردیم. در ادامه نشان‌خواهیم‌داد که اگرچه آموزش با الگوریتم PSO پاسخ بسیار دقیق‌تری نسبت به روش آموزش BPمی‌دهد، اما باز هم می‌توان با تغییر الگوریتم PSO به پاسخ‌های بسیار دقیق‌تری رسید. برای این منظور از ترکیب سیستم فازی با PSO و الگوریتم ICA استفاده‌کردیم و نشان‌دادیم که با آموزش شبکه عصبی توسط الگوریتم تغییریافته ICA می‌توان به نتایج بسیار قابل‌قبولی دست‌یافت.

بیان مسئله

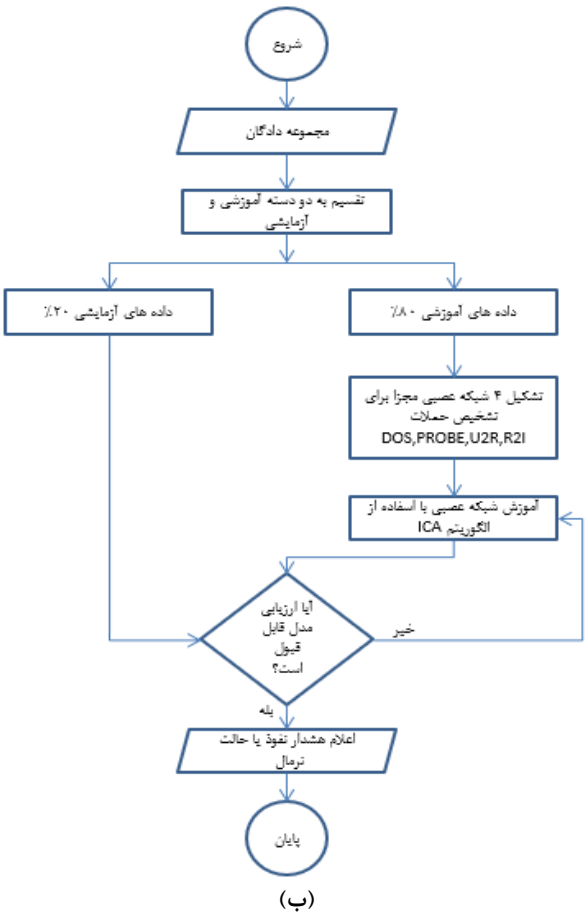
امروزه استفاده از اینترنت اشیا در صنایع مختلف امری ضروری است چنانکه صنایع پیشرو در دنیا و حتی ایران در حال پیاده‌سازی آن می‌باشند. با گسترش زیرساخت‌های این تکنولوژی چالش‌های آن هم زیاد می‌شود. حملات سایبری یکی از چالش‌های بسیار مهم در این حوزه می‌باشد طوری که حتی اگر قوی‌ترین زیرساخت‌ها در این صنایع پیاده‌شود ولی به ایجاد سیستم‌های مقابله با این حملات توجه نشود نه‌تنها کارایی سیستم بالا نمی‌رود بلکه ممکن است باعث اختلال در فرآیند شود. به همین منظور در این مقاله می‌خواهیم یکی از روش‌های مقابله و تشخیص نفوذ هوشمند در حوزه امنیت سایبری را پیاده‌سازی کنیم. برای رسیدن به این سیستم روش‌های متفاوتی وجوددارد ولی استفاده از روش‌های آموزش ماشین و به‌ویژه شبکه عصبی امروزه یکی از روش‌های سریع و دقیق در این حوزه است. به همین منظور در این مقاله برای پیاده‌سازی سیستم IDS از شبکه عصبی استفاده‌کردیم. علاوه بر این ضعف‌های شبکه عصبی را در حوزه آموزش با ترکیب الگوریتم‌های بهینه‌سازی رقابت امپریال (ICA) برطرف نموده و نشان‌داده‌ایم که می تواند کارایی سیستم IDS را بسیار بالا ببرد.

محتوا و روش‌ها

ساختار کلی و نمودار طرح پیشنهادی در شکل ۲ آمده‌است. مطابق شکل، در مرحله اول باید داده‌های سیستم پیشنهادی جمع‌آوری‌شود. این مقاله از داده‌های مجموعه KDD-CUP استفاده‌می‌کند. مرحله دوم، مربوط به پیش‌پردازش داده‌ها است، ازجمله پاک‌کردن داده‌های مشابه، نرمال‌سازی داده‌ها، مهندسی ویژگی داده‌ها و حذف آن‌ها. سپس داده‌هایی که فشرده‌شده‌اند به دو دسته آموزشی (۸۰٪ داده) و آزمایشی (۲۰٪ داده) تقسیم‌می‌شوند. در این مقاله برای تشخیص نفوذ هوشمند چهار نوع حمله DOS,PROBE,R2L,U2R، چهار شبکه عصبی تشکیل‌می‌دهیم. هرکدام از این شبکه‌های عصبی دارای ۴۱ ورودی و یک خروجی است. تعداد ورودی‌های شبکه عصبی نیز معادل با تعداد ۴۱ ویژگی مربوط به مجموعه دادگان KDD-CUP می‌باشد. خروجی هر شبکه دارای دو حالت یک و صفر می‌باشد، که یک در این حالت بیانگر تشخیص حمله و صفر تشخیص حالت نرمال است. برای آموزش شبکه عصبی و تشکیل مدل می‌توان از روش سنتی پس انتشار (Back Propagation) استفاده‌کرد ولی این روش در نقاط بهینه محلی گرفتار شده و دارای دقت کافی نیست. در ادامه از دو روش PSO و ICA برای آموزش شبکه عصبی استفاده‌می‌کنیم. همان‌طورکه در فلوچارت شکل ۲ (الف)، آمده‌است شبکه عصبی می‌تواند با استفاده از الگوریتم PSO آموزش داده‌شود. در ادامه برای افزایش دقت PSO استفاده از عملگر فازی پیشنهادمی‌شود. علاوه‌بر PSO ، ICA نیز یک الگوریتم با دقت بالایی در حل مسائل بهینه‌سازی می‌باشد. به همین منظور برای افزایش سرعت و دقت IDS از الگوریتم ICA (شکل ۲ (ب)) در مقایسه الگوریتم PSOاستفاده‌می‌نمائیم و نشان‌می‌دهیم که عملکرد بهتری نسبت به آن دارد.



(الف)



(ب)

شکل ۲: چارچوب کلی تشخیص حمله (الف) با استفاده از الگوریتم PSO مبتنی‌بر شبکه عصبی، (ب) با استفاده از الگوریتم ICA مبتنی‌بر شبکه عصبی

الگوریتم ازدحام ذرات کلاسیک (CLASSICAl PSO)

در سال ۱۹۹۵ ابرهارت و کندی برای اولین بار PSO را به‌عنوان یک روش جستجوی نامشخص برای بهینه‌سازی عملکردی معرفی‌کردند. این الگوریتم از حرکت انبوه پرندگان جویای غذا الهام گرفته‌شده‌است. گروهی از پرندگان به‌طور تصادفی در فضا دنبال غذا می‌گردند. تنها یک تکه غذا در فضای جستجو وجوددارد. هر راه‌حل یک ذره نامیده‌می شود و دارای یک مقدار شایستگی است که توسط تابع شایستگی محاسبه-می‌شود. هرچه ذره در فضای جستجو به هدف (غذا در مدل حرکت پرنده) نزدیکتر باشد، ارزش بیشتری دارد. همچنین هر ذره سرعتی دارد که حرکت ذره را هدایت‌می‌کند. هر ذره با پیروی از ذرات بهینه در وضعیت فعلی در فضای مسئله حرکت‌می‌کند. الگوریتم‌های بهینه‌سازی ازدحام ذرات از جمله الگوریتم‌های بهینه‌سازی تکاملی هستند. مهمترین مزیت این الگوریتم‌ها نسبت به سایر الگوریتم‌های بهینه‌سازی این است که به عملیات پیچیده و روابط ریاضی مانند مشتق و انتگرال نیاز ندارند [۲۱-۲۰]. این الگوریتم‌ها یا بر اساس فرآیندهای بیولوژیکی و مبادلات موجودات زنده (مانند مورچه‌ها، پرندگان، ژنتیک و غیره) یا ارتباطات و رفتارهای سیاسی-اجتماعی انسان (مانند الگوریتم‌های رقابت استعماری یا بهینه‌سازی مبتنی‌بر معلم- شاگرد) مدل‌سازی‌می‌شوند. [۲۳-۲۲]. الگوریتم PSO نیز براساس جستجوی زیستگاه‌های مناسب توسط پرندگان مدل‌سازی شده‌است. این الگوریتم سال ۱۹۹۵ با مطالعه مشترک ابرهارت و کندی براساس حرکت پرندگان و ماهی‌ها و دو اصل حیات مصنوعی و تکامل ارائه و ابداع شد. مانند سایر الگوریتم‌های تکاملی، این الگوریتم نیز با مجموعه‌ای از ذرات یک ماتریس با موقعیت کاملاً تصادفی شروع‌می‌شود. هر ذره در این ماتریس یک پرنده نامیده-می‌شود و این پرندگان می‌توانند در فضای n ام پرواز کنند (n تعداد متغیرهای مسئله بهینه‌سازی است). در هر مرحله شرایط جدید آن‌ها براساس تجربیات شخصی گذشته و موقعیت همسایگانشان به‌روزرسانی می‌شود. قدرت هر ذره از این مجموعه از پرندگان با بردار زیر تعریف‌می-شود [۲۵-۲۴]:

$$Xi= [X_{i1}, X_{i2} ,\ldots\ldots X_{in}]^T \in S \qquad (1)$$

در اینجا S فضای جستجو و Xi موقعیت هر پرنده در تکرار الگوریتم i است. هر ذره در هر مرحله یک سرعت دارد. بنابراین، بردار سرعت همه ذرات با رابطه ۲ تعریف‌می‌شود [۲۷-۲۶]:

$$Vi= [V_{i1}, V_{i2},\ldots\ldots V_{in}]^T \in S \qquad (2)$$

بهترین موقعیت شخصی که هر پرنده از ابتدا تا مرحله i دارد بهترین موقعیت شخصی نامیده‌می‌شود و برای همه ذرات با بردار زیر در هر مرحله تعریف‌می‌شود [۲۵-۲۳]:

$$Pi= [P_{i1}, P_{i2},\ldots\ldots P_{in}]^T \in S \qquad (3)$$

بر اساس روابط و تعاریفی که در بالا توضیح‌داده‌شد، سرعت هر پرنده در هر مرحله از تکرار با رابطه زیر محاسبه و به‌روز می‌شود [۲۵-۲۳]:

$$\vec{v}_i^{k+1} = w\vec{v}_i^k + c_1 r_1 \times (\vec{p}_i - \vec{x}_i^k) + c_2 r_2 \times (\vec{p}_g - \vec{x}_i^k) \quad (4)$$

$$\vec{X}_i^{k+1} = \vec{V}_i^{k+1} + \vec{X}_i^k \quad (5)$$

در اینجا سرعت به‌روزشده ذره به‌ترتیب در تکرار k + 1 و سرعت و موقعیت قبلی ذره است. علاوه‌بر این، بهترین موقعیت ذره I ام و موقعیت ذره‌ای که بهترین موقعیت شخصی را در بین پرندگان دارد نشان‌می‌دهد. در اینجا c1 و c2 ضرایب ثابت هستند و معمولاً ۲ است. ضریب w به‌عنوان ضریب وزن اینرسی شناخته‌می‌شود. r1 و r2 دو عدد تصادفی بین صفر و یک هستند که به الگوی جستجو ماهیت تصادفی می‌دهند.

قوانین فازی تشخیص ضریب اینرسی W

ضریب وزن W در مرحله فعلی تاثیر زیادی بر سرعت هر پرنده دارد، بنابراین افزایش این ضریب باعث افزایش سرعت می‌شود. چون فرض بر این است که در رابطه شماره ۵، مقدار هر جابجایی یک است، بنابراین هرچه سرعت بیشتر باشد، جابجایی ذرات در یک مرحله بیشتر می‌شود و در نتیجه فضای جستجو زیاد و از دقت آن کاسته‌می‌شود. برعکس این قضیه نیز صادق است. ازاین‌رو در انتخاب این ذره باید مقدار تعادل مناسبی درنظرگرفته‌شود. در این مقاله این تعادل با استفاده از قواعد و *اگرهای* فازی انجام‌شده‌است. بهترین انتخاب این است که ضریب w را با استفاده از منطق فازی با نزدیک یا دور بودن Gbest از هر مرحله از Gbest مورد نظر مطابقت‌دهیم. بنابراین مقادیر w و NFV که در زیر تعریف‌شده‌اند، ورودی‌های موتور استنتاج فازی هستند و خروجی آن Δw است [۲۷-۲۶].

$$\omega^{k+1} = \omega^k + \Delta\omega \quad (۶)$$

در اینجا FV سطح Gbest در مرحله فعلی و FVmin سطح Gbest در اولین تکرار است و FVmax یک عدد بسیار بزرگ است. معمولاً ضریب W باید بین ۰,۹ تا ۰,۴ باشد. ازآنجاکه تصحیح ضریب W در حین اجرای برنامه ممکن است در حال افزایش یا کاهش باشد، هر دو تصحیح مثبت و منفی برای این ضریب ضروری هستند. در این تحقیق عدد کوچکی با مقدار ۰,۱ درنظرگرفته‌شده‌است که با ضریب W جمع و کم می‌شود.

$$\omega^{k+1} = \omega^k + \Delta\omega \quad (۷)$$

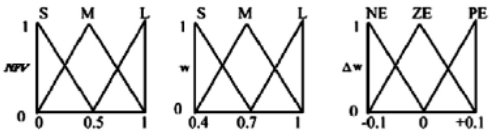
در اینجا wΔ مقدار تصحیح مشابهی است و برابر با ±۱ است. البته گاهی اوقات مقدار صفر است که در چنین شرایطی وضعیت آن مطابق جدول ۱ پیشنهادمی‌شود. توجه‌داشته‌باشید که مقادیر Gbest باید به‌صورت توابع عضویت بیان‌شوند تا مقدار بهینه وزن ضریب W به‌دست‌آید.

در این مقاله توصیه‌می‌شود که توابع عضویت مثلثی طوری انتخاب‌شوند که دارای سه حالت باشند:

بزرگ یا L، کوچک یا S، متوسط یا M. همچنین خروجی‌های مدل فازی، همان‌طورکه در جدول ۱ آمده‌است، دارای سه مقدار (+0.1) PE، (NE (-0.1 یا (0) ZE هستند. طبق جدول ۱، ممکن است براساس مقادیر مختلف NFV وW نُه حالت رخ‌دهد. اگر هم NFV و هم W کوچک باشند، نیازی به تغییر w نیست زیرا از یک طرف Gbest به سطح بهینه رسیده‌است و از طرف دیگر نمی‌توان W را آنقدر کاهش‌داد که از حد قابل‌تغییر فراتر رفت، اگر NFV کم و W متوسط باشد، باز هم می‌توانیم W را ۰,۱ کاهش‌دهیم تا دقت جستجو افزایش‌یابد. اگر NFV کم باشد و W بالا باشد، می‌توانیم w را به اندازه قبل ۰,۱ کاهش‌دهیم. رابطه بین ورودی‌ها و خروجی‌ها در جدول ۱ نشان‌داده شده‌است. توابع عضویت مثلثی نیز در شکل ۳ آورده‌شده‌است. از این توابع برای دریافت متغیرهای ورودی و خروجی استفاده‌می‌شود.

جدول ۱: قوانین فازی متغیرهای ورودی و خروجی [۲۷-۲۶]

ΔW		W		
		S	M	L
NFV	S	ZE	NE	NE
	M	PE	ZE	NE
	L	PE	ZE	NE

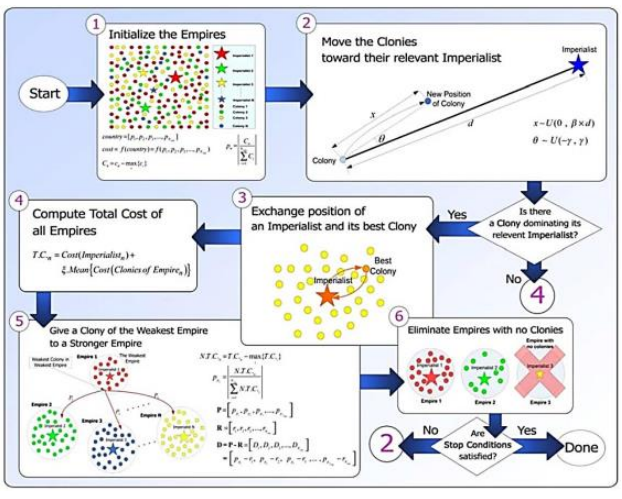


شکل ۳: توابع عضویت. [۲۷-۲۶]

الگوریتم رقابت امپریال (ICA)

در سال‌های اخیر، الگوریتم‌های فراابتکاری برای بهینه‌سازی مسائل مهندسی مورداستفاده قرارگرفته‌اند. این الگوریتم‌ها یا براساس پدیده‌های طبیعی (از قبیل کلونی مورچه‌ها و الگوریتم‌های پرندگان) یا نمونه‌ای از ارتباطات اجتماعی- انسانی (مانند الگوریتم‌های رقابت امپراتوری و الگوریتم‌های معلم- شاگرد) مدل‌سازی‌می‌شوند. مهمترین مزیت این الگوریتم‌ها سادگی و بی‌نیازبودن آن‌ها به مسائل پیچیده ریاضی مانند مشتق و انتگرال است. الگوریتم رقابت امپریال (ICA) یک مدل‌سازی ریاضی مبتنی‌بر فرآیند تکامل اجتماعی-سیاسی است و برای بهینه‌سازی مسائل مهندسی استفاده‌می‌شود. این الگوریتم بر اساس ۳ اصل انقلاب، سیاست جذب و رقابت استعماری پایه‌گذاری شده‌است [۳۱-۲۸]. الگوریتم ICA، مانند سایر الگوریتم‌های تکاملی، از تعدادی افراد که جمعیت نامیده‌می‌شوند، شروع‌می‌شود که به هریک از این افراد "کشور" می‌گویند. تعدادی از بهترین عناصر جمعیت (معادل نخبگان در الگوریتم ژنتیک و ذره در تراکم ذرات) به‌عنوان امپریالیست انتخاب‌می‌شوند. بقیه جمعیت نیز مستعمره آن‌ها محسوب‌می‌شوند. استعمارگران بسته به

قدرت خود، این مستعمرات را در یک فرآیند خاص ترسیم‌می‌کنند. قدرت کل هر جمهوری به اجزای تشکیل‌دهنده آن، دولت امپریالیستی (به‌عنوان هسته مرکزی) و مستعمرات آن بستگی‌دارد. از دیدگاه محاسبات ریاضی، کل قدرت دولت امپریالیستی، به‌علاوه درصدی از میانگین قدرت مستعمرات آن قدرت امپراتوری را شکل‌می‌دهد [۳۱-۲۸]. در مرحله دوم کشور شاهنشاهی تلاش‌می‌کند کشور استعماری را وابسته به فرهنگ و آداب و رسوم آن کشور کند که به این امر تابع جذب می‌گویند. کشور استعمارگر از رویه خاصی برای استعمار دیگر کشورها استفاده‌می‌کند. در مرحله سوم، طبق روال طبیعی، ممکن است برخی از کشورهای استعمارشده انقلاب‌کنند و بتوانند قدرت امپراتوری را به‌دست‌گیرند. پس از اعمال توابع جذب و انقلاب برای هر کشور، مجددا تابع هزینه برای هر یک از مستعمرات محاسبه‌می‌شود. در این مرحله اگر برای هر یک از امپراتوری عملکرد هدف استعماری بهتر از امپراتوری‌ها باشد، تغییرات در هر دو کشور انجام‌می‌شود. پس از این عملیات، بهترین پاسخ برای همه امپراتوری‌ها و مقدار همه کشورهای استعماری به‌عنوان بهترین پاسخ و مقدار فعلی در این تکرار الگوریتم ذخیره‌می‌شود [۳۱-۲۸]. حال اگر مقدار تابع هدف پاسخ فعلی کیفیت بهتری نسبت به بهترین مقدار عدد به‌دست‌آمده قبلی داشته‌باشد، پاسخ جدید و مقدار جدید جایگزین پاسخ قبلی می‌شود. از طرف دیگر، باید توجه‌داشت که پس از پایان الگوریتم، این پاسخ و مقدار به‌عنوان پاسخ مسئله ارائه‌می شود. در مرحله چهارم، مجموع عملکرد امپریالیست به اضافه ضریب میانگین توابع هدف مستعمرات آن به‌عنوان کل قدرت یک امپراتوری تعریف‌می‌شود. توجه به این نکته ضروری است که این ضریب به کاربر اجازه‌می‌دهد تا تأثیر امپریالیستی یا میانگین دولت‌های استعماری را بر قدرت نهایی هر امپراتوری تعیین‌کند. همچنین در جریان رقابت استعماری که مبتنی‌بر مقایسه قدرت امپراتوری‌هاست، ضعیف‌ترین عضو از ضعیف‌ترین امپراتوری انتخاب و به یکی از امپراتوری‌های دیگر منتقل-می‌شود. لازم به ذکر است که اگر یک امپراتوری هیچ کشور استعماری نداشته‌باشد، دولت امپراتوری آن به یک دولت استعماری تبدیل‌شده و به یکی از امپراتوری‌ها منتقل‌می‌شود [۲۸-۳۱]. شکل زیر مراحل و روابط پیاده‌سازی این الگوریتم را نمایش‌می‌دهد:



شکل ۴: مراحل کلی و روابط الگوریتم ICA [۲۸-۳۱]

در الگوریتم کلاسیک ICA، β یک پارامتر ثابت است. در این مقاله، ما برتی بهبود کارایی ICA، مقدار ثابت β را در مرحله دوم با معادله خطی به‌صورت زیر انتخاب‌می‌کنیم:

$$\beta = \beta_0 * \text{ITER max/ITER} \quad \text{where } \beta_0=2 \qquad (8)$$

در ابتدای اجرای الگوریتم، β بزرگ است و فضای جستجو افزایش‌می‌یابد. در ادامه اجرای الگوریتم این ضریب کوچکتر شده و دقت جستجو افزایش‌می‌یابد.

تابع هدف

در این تحقیق، برای مدل‌سازی سیستم تشخیص حمله و ناهنجاری‌ها، از ساختار شبکه عصبی پرسپترون تک‌لایه استفاده‌کردیم. علاوه بر این، ما شبکه عصبی را با استفاده از الگوریتم‌های BP، الگوریتم‌های کلاسیک PSO، FPSO (PSO فازی)، و الگوریتم ICA آموزش‌دادیم. همچنین طبق فرمول زیر از تابع سیگموئید به‌عنوان آخرین لایه شبکه عصبی استفاده‌کردیم.

$$a(z)=\frac{1}{1+\exp(-z)} \qquad (9)$$

دقت مدل پیشنهادی بر اساس تشخیص صحیح مدل به‌دست‌آمده توسط شبکه عصبی و با رابطه زیر محاسبه می شود:

$$\omega^{k+1} = \omega^{k} + \Delta\omega \qquad (10)$$

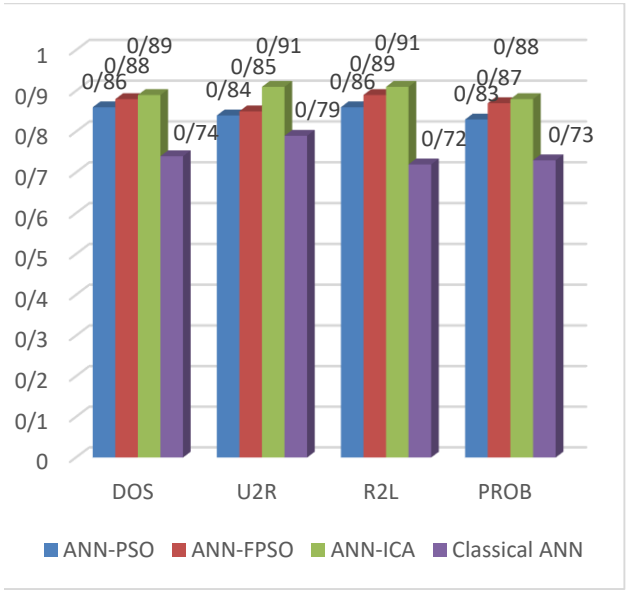
چون الگوریتم پرنده ذاتاً تابع هدف را به حداقل می‌رساند، تابع زیر باید برای افزایش دقت تابع هدف تعریف‌شود:

$$\text{تابع هدف} = -\left(\frac{TP+TN}{TP+TN+FP+FN}\right) \qquad (11)$$

نتیجه‌گیری و بحث

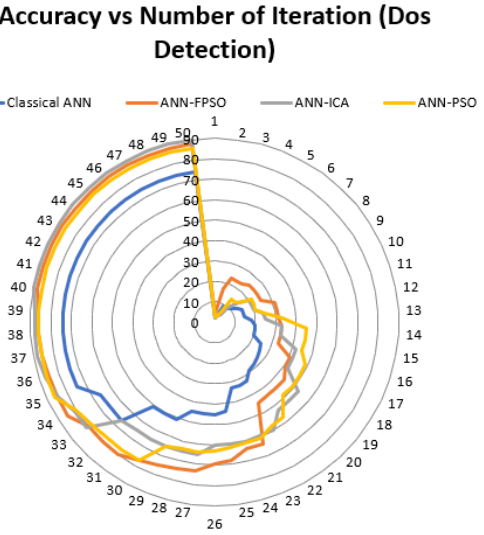
همان‌طور که در بخش قبل ذکرشد شبکه عصبی کلاسیک در نقاط بهینه محلی گرفتارشده و برای مدل‌سازی سیستم تشخیص هوشمند از دقت کافی برخوردار نمی‌باشد. به همین منظور ما در اینجا از الگوریتم ICA برای آموزش شبکه عصبی استفاده‌نمودیم تا علاوه‌بر افزایش دقت، سرعت تشخیص نفوذ را نیز بهبوددهیم. در ادامه برای ارزیابی مدل پیشنهادی خروجی به‌دست‌امده را با شبکه عصبی کلاسیک و شبکه عصبی مبتنی بر اموزش با استفاده از PSO مقایسه‌نمودیم. شکل۵ سطح دقت را برای روش‌های مختلف آموزش شبکه عصبی نشان‌می‌دهد. در اینجا فرض‌می‌کنیم که حداکثر تکرار برابر با ۵۰ و همچنین تعداد ذرات

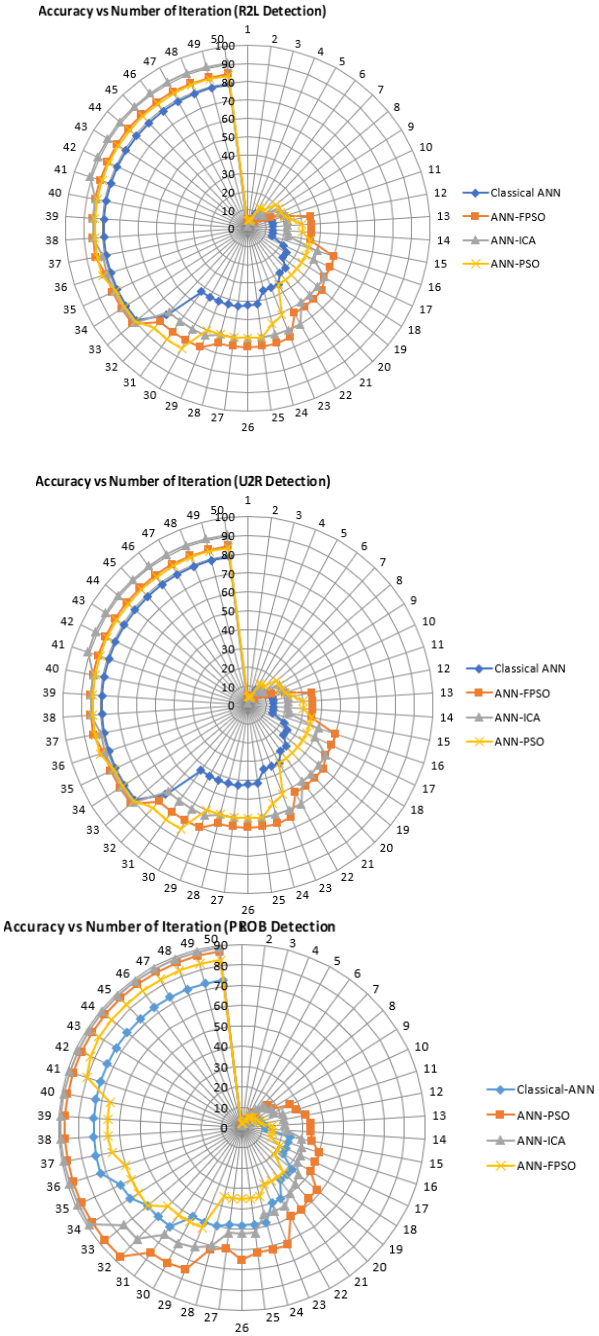
برای PSO و ICA به‌ترتیب برابر با ۴۰ و ۲۰۰ است. مطابق شکل، آموزش شبکه عصبی با الگوریتم کلاسیک PSO بسیار بهینه‌تر از آموزش با الگوریتم BP است. علاوه‌بر این، همان‌طور که انتظار می‌رفت، الگوریتم کلاسیک PSO در نقطه بهینه محلی درگیرشد و ترکیب FPSO پاسخ دقیق‌تری را ارائه‌داد. همانگونه که در شکل دیده‌می‌شود الگوریتم ICA نیز می‌تواند عملکرد بهتری نسبت به PSO و شبکه عصبی کلاسیک از منظر گرفتارشدن در نقاط بهینه محلی داشته‌باشد.



شکل ۵: دقت الگوریتم های مختلف یادگیری ماشین

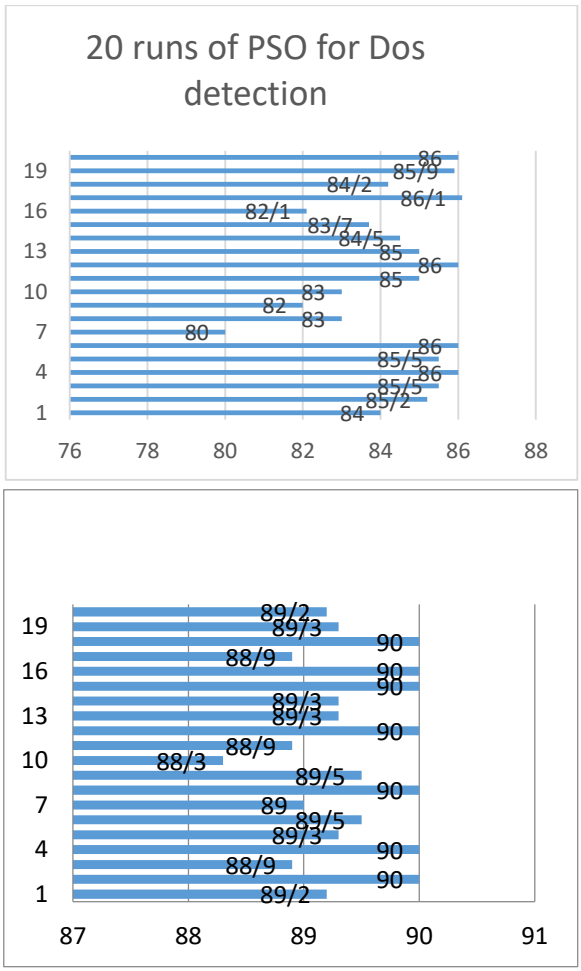
شکل ۶، سرعت همگرایی الگوریتم‌های مختلف در تکرار الگوریتم برای تشخیص حملات مختلف را نشان‌می‌دهد. همان‌طور که در شکل قابل‌مشاهده است، الگوریتم ICA علاوه‌بر دقت بسیار بالا، سرعت همگرایی بهتری نیز دارد. بنابراین، این الگوریتم الگوریتمی بسیار بهینه برای افزایش دقت و سرعت تشخیص حمله است.





شکل ۶: مشخصه همگرایی روش پیشنهادی در تشخیص حملات مختلف

سرانجام، در شکل ۷، دقت الگوریتم‌های PSO و ICA را پس از اجرای ۲۰ برنامه برای شناسایی حملات DOS نشان‌می‌دهیم. طبق شکل، الگوریتم ICA نسبت به الگوریتم PSO قابل‌اعتمادتر است به این دلیل که در اجراهای مختلف، پاسخ‌های نسبتاً یکسانی را ارائه‌می‌دهد.



شکل۷: دقت اجرای الگوریتم بالا ANN-PSO و پایین ANN- ICA

نتیجه

در این مقاله ما از الگوریتم بهینه‌سازی رقابت استعماری اصلاح‌شده برای آموزش شبکه عصبی استفاده کردیم تا یک سیستم تشخیص نفوذ هوشمند با دقت و سرعت بالا برای شبکه اینترنت اشیا طراحی و پیاده-کنیم. در راستای ارزیابی مدل پیشنهادی آن را با شبکه عصبی کلاسیک و شبکه عصبی با آموزش توسط ICA و Fuzzy PSO مقایسه کرده، نشان‌دادیم در مقایسه با آن‌ها سرعت بیشتری داشته و کمتر گرفتار نقطه بهینه محلی می‌گردد. در نهایت نشان‌دادیم این الگوریتم قدرتمند برای تشخیص حملات و ناهنجاری‌ها درساختار اینترنت اشیا دارای دقت عملکرد ۹۰٪ می باشد درحالی‌که دقت ANN-PSO معادل ۸۶ درصد و دقت ANN- CLASSIC حدود ۷۵ ٪ می‌باشد.

References

1- Hasan, Mahmudul, et al. "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches." *Internet of Things* 7 (2019): 100059.
2- Kotenko, Igor, et al. "Attack detection in IoT critical infrastructures: a machine learning and big data processing approach." *2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*. IEEE, 2019.
3- Foley, John, Naghmeh Moradpoor, and Henry Ochen. "Employing a Machine Learning Approach to Detect Combined Internet of Things Attacks against Two Objective Functions Using a Novel Dataset." *Security and Communication Networks* 2020 (2020).
4- Doshi, Rohan, Noah Apthorpe, and Nick Feamster. "Machine learning ddos detection for consumer internet of things devices." *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018.
5- Syed, Naeem Firdous, et al. "Denial of service attack detection through machine learning for the IoT." *Journal of Information and Telecommunication* (2020): 1-22.
6- Radi, Sanaz Amirmokhtar, and Sajjad Shokouhyar. "Toward consumer perception of cellphones sustainability: A social media banalytics." *Sustainable Production and Consumption* 25 (2021): 217-233.
7- Shokohyar, Sajjad, Ehsan Taati, and Sara Zolfaghari. "The Effect of Drivers' Demographic Characteristics on Road Accidents in Different Seasons Using Data Mining." *Promet-Traffic&Transportation* 29.6 (2017): 555-567.
8- Arabi, Mahsa, Saeed Mansour, and Sajjad Shokouhyar. "Optimizing a warranty–based sustainable product service system using game theory." *International Journal of Sustainable Engineering* 11.5 (2018): 330-341.
9- Shokouhyar, Sajjad, Mohammad Reza Seddigh, and Farhad Panahifar. "Impact of big data analytics capabilities on supply chain sustainability: A case study of Iran." *World Journal of Science, Technology and Sustainable Development* (2020).
10- Manimurugan, S., et al. "Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network." *IEEE Access* 8 (2020): 77396-77404.
11- Latif, Shahid, et al. "A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random N`eural Network." *IEEE Access* 8 (2020): 89337-89350.
12- Nia, Masoud Ramezani, and Sajjad Shokouhyar. "Analyzing the effects of visual aesthetic of Web pages on users' responses in online retailing using the VisAWI method." *Journal of Research in Interactive Marketing* (2020).
13- Shokohyar, Sajjad, Seed Mansour, and Behrooz Karimi. "Simulation-based optimization of ecological leasing: a step toward extended producer responsibility (EPR)." *The International Journal of Advanced Manufacturing Technology* 66.1 (2013): 159-169.
14- Sharifi, Zahra, and Sajjad Shokouhyar. "Promoting consumer's attitude toward refurbished mobile phones: A social media analytics approach." *Resources, Conservation and Recycling* 167 (2021): 105398.

15- Alkronz, Eyad Sameh, et al. "Prediction of Whether Mushroom is Edible or Poisonous Using Back-propagation Neural Network." (2019).
16- Wang, Weilin, et al. "Estimation of PM2. 5 concentrations in China using a spatial back propagation neural network." *Scientific reports* 9.1 (2019): 1-10.
17- Mohammadi, Farzaneh, et al. "Modelling and optimizing pyrene removal from the soil by phytoremediation using response surface methodology, artificial neural networks, and genetic algorithm." *Chemosphere* 237 (2019): 124486.
18- Azimi, Yousef, Seyed Hasan Khoshrou, and Morteza Osanloo. "Prediction of blast induced ground vibration (BIGV) of quarry mining using hybrid genetic algorithm optimized artificial neural network." *Measurement* 147 (2019): 106874.
19- Cai, Jianghui, et al. "A Novel Clustering Algorithm Based on DPC and PSO." *IEEE Access* 8 (2020): 88200-88214.
20- Singh, Shakti, Prachi Chauhan, and NirbhowJap Singh. "Capacity optimization of grid connected solar/fuel cell energy system using hybrid ABC-PSO algorithm." *International Journal of Hydrogen Energy* (2020).
21- Devarasiddappa, D., M. Chandrasekaran, and R. Arunachalam. "Experimental investigation and parametric optimization for minimizing surface roughness during WEDM of Ti6Al4V alloy using modified TLBO algorithm." *Journal of the Brazilian Society of Mechanical Sciences and Engineering* 42.3 (2020): 1-18.
22- Qiao, Weibiao, Hossein Moayedi, and Loke Kok Foong. "Nature-inspired hybrid techniques of IWO, DA, ES, GA, and ICA, validated through a k-fold validation process predicting monthly natural gas consumption." *Energy and Buildings* (2020): 110023.
23- Prithi, S., and S. Sumathi. "LD2FA-PSO: A novel Learning Dynamic Deterministic Finite Automata with PSO algorithm for secured energy efficient routing in Wireless Sensor Network." *Ad Hoc Networks* 97 (2020): 102024.
24- Kacimi, Mohand Akli, et al. "New mixed-coding PSO algorithm for a self-adaptive and automatic learning of Mamdani fuzzy rules." *Engineering Applications of Artificial Intelligence* 89 (2020): 103417.
25- Jallal, Mohammed Ali, Samira Chabaa, and Abdelouhab Zeroual. "A novel deep neural network based on randomly occurring distributed delayed PSO algorithm for monitoring the energy produced by four dual-axis solar trackers." *Renewable Energy* 149 (2020): 1182-1196.
26- Niknam, Taher, Ehsan Azadfarsani, and Masoud Jabbari. "A new hybrid evolutionary algorithm based on new fuzzy adaptive PSO and NM algorithms for distribution feeder reconfiguration." *Energy Conversion and Management* 54.1 (2012): 7-16.
27- Niknam, Taher, Hassan Doagou Mojarrad, and Majid Nayeripour. "A new fuzzy adaptive particle swarm optimization for non-smooth economic dispatch." *Energy* 35.4 (2010): 1764-1778.
28- Gao, Liuyang, et al. "Target Signal Extraction Method Based on Enhanced ICA with Reference." *Mathematical Problems in Engineering* 2019 (2019).
29- Gao, Wei, et al. "A predictive model based on an optimized ANN combined with ICA for predicting the stability of slopes." *Engineering with Computers* 36.1 (2020): 325-344.
30- Qiao, Weibiao, Hossein Moayedi, and Loke Kok Foong. "Nature-inspired hybrid techniques of IWO, DA, ES, GA, and ICA, validated through a k-fold validation process predicting monthly natural gas consumption." *Energy and Buildings* (2020): 110023.
31- Kaewwit, Chesada. "High accuracy EEG biometrics identification using ICA and AR model." *Journal of Information and Communication Technology* 16.2 (2020): 354-373.