مجله نخبگان علوم و مهندسی
Journal of Science and Engineering Elites
جلد ۸- شماره ۵ - سال ۱۴۰۲
www.ElitesJournal.ir

تاثیر هوش مصنوعی در ارتقا توانمندی‌های زیر سامانه‌های الکترونیکی، مخابراتی و سایبری در بستر جنگ الکترونیک

عرفانه نوروزی*[۱]، آریا بیرانوند[۲]

۱- استادیار گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه آزاد اسلامی واحد بین الملل قشم، ایران
۲- استادیار گروه جنگ الکترونیک، دانشکده جنگال، جنگ الکترونیک آجا تهران، ایران

*noroozierfaneh@gmail.com

ارسال: آبان ماه ۱۴۰۲ پذیرش: آذر ماه ۱۴۰۲

چکیده

جنگ الکترونیک (EW)[۱] یکی از مهمترین ویژگی‌های نبردهای مدرن و امروزی است. این حوزه می‌تواند بر نحوه استفاده نیروهای نظامی از طیف الکترومغناطیسی جهت شناسایی اهداف یا در اختیار گذاشتن اطلاعات به‌طرز چشم‌گیری تأثیرگذار باشد. تحولات اخیر در زمینه هوش مصنوعی (AI)[۲] نشان می‌دهد که این فناوری در حال ظهور یک تأثیر قطعی و بالقوهِ دگرگون‌ساز بر قدرت نظامی در هر کشوری خواهد داشت. الگوریتم‌های مبتنی بر هوش مصنوعی می‌توانند نقش بسیار موثری در حوزه‌های مختلف EW مانند: پردازش سیگنال‌های راداری در راستای شناسایی و طبقه‌بندی انواع فرستنده‌ها، تشخیص نوع عملیات جمینگ و مشخصه‌های آن و هم‌چنین توسعه الگوریتم‌های موثر ضد اخلال داشته باشند. تکنیک‌های هوش مصنوعی همچنین می‌توانند انواع سیستم‌های EW را به‌گونه‌ای توانمند سازند که به‌طور مستقل و خودکافی کار کنند. تمرکز ما در این مقاله بر روی توصیف جنبه‌های اساسی EW و اجزاء مرتبط با آن، عناصر مختلف و تکنولوژی‌های مربوط به نسل فعلی سیستم‌های EW، کاربرد هوش مصنوعی در سامانه‌ها و تجهیزات جنگ الکترونیک به‌خصوص در حوزه (EA) به‌عنوان یک عنصر کمکی جهت تصمیم‌گیری و انجام واکنش صحیح و موثر در برابر سامانه‌ها و تجهیزات راداری در صحنه نبرد و سناریوهای در حال تکامل EW برای نیروهای نظامی (در حال حاضر و یا برنامه‌های آتی) است. دو تکنیک اصلی ECM شامل ECM عامل و ECM غیرعامل است.

واژگان کلیدی: هوش مصنوعی، امنیت سایبری، یادگیری ماشین، سامانه‌های الکترونیکی، جنگ الکترونیک.

۱- مقدمه

فناوری‌های نوین به‌عنوان یک عامل مهم و تعیین‌کننده در معادلات و مناسبات اقتصادی، سیاسی، نظامی و حتی فرهنگی و اجتماعی محسوب شده و در واقع معیاری برای سنجش قدرت بکار می‌رود، در حوزه سازمانی و بنگاه‌ها نیز بر تمامی فعالیت‌های زنجیرهِ ارزش تاثیرگذار است. نیروهای نظامیِ مدرن به طرز چشم‌گیری به انواع مختلفی از فناوری‌های پیچیده و پیوسته در حال تحول برای به‌دست آوردن دست برتر با بهره‌گیری از تجهیزات الکترونیکی وابسته هستند[۳]. جنگ الکترونیک مجموعه‌ای تخصصی از ابزارها

[1] Electronic Warefare
[2] Artificial Intelligence

و تجهیزات و هنر بکارگیری آنهاست که نیروهای چهارگانه نظامیِ دریایی، هوایی، فضایی و زمینی را در چگونگی و میزان بهره-برداری از طیف الکترومغناطیسی در سطوح مختلف حمایت می‌کند. امروزه در هر سرزمینی توجه ویژه‌ای به گسترش و توسعه دانش طراحی و تولید سیستم‌ها و مجموعه‌های وابسته به جنگ الکترونیک شده، چرا که این حوزه دانشی به‌عنوان لبه فناوری در نظر گرفته می‌شود[۴]. با وجود ارتقا توانمندی و افزایش بهره‌وری تجهیزات در اختیار با استفاده از EW، بهینه‌سازی منابع مورد استفاده و تصمیم‌گیری کارآمد به‌عنوان یک مسئله چالش برانگیز و مهم در یک عملیات نظامی مدرن برشمرده می‌شود. کاربردهای هوش مصنوعی (AI) به‌صورت تواماً با EW می‌تواند به‌عنوان یک گزینه راه‌گشا و موثر مورد استفاده قرار گیرد؛ چراکه پتانسیل بالقوه‌ای جهت پر کردن شکاف بین توانایی رزم الکترونیک و مهارت‌های به دست آمده در این بستر وجود دارد. در مجموع، EW و AI می‌تواند نقش مهمی در راستای ایجاد ترکیبی توانمند و کارآمد در رشد و پیشرفت کشورهای در حال توسعه در حوزه‌های وابسته به علوم الکترونیک، مخابرات،فضای سایبری، ریزپردازنده‌ها، کامپیوترها و ... ایفا کند[۵].

اما چرا بکارگیری هوش مصنوعی در کنار EW ضروری و الزام‌آور است؛ از دلایل اصلی ارجحیت استفاده از سیستم‌های EW مبتنی بر هوش مصنوعی شامل قابلیت‌های تاثیرگذار در تصمیم‌گیری، مدیریت حجم زیادی از داده‌هایِ گردآوری شده، تجزیه و تحلیل آنی و ارائه اطلاعات با در نظر گرفتن جزییات، آگاهی موقعیتی، تجسم صحنه در حال تحول و ایجاد پاسخ‌ها و واکنش‌های مناسب در کم‌ترین زمان ممکن می‌باشد. علاوه بر این، سیستم‌ها و تجهیزات الکترونیکی، مخابراتی، کامپیوتری و ... که از قابلیت‌های هوش مصنوعی استفاده می‌کنند، به‌دلیل محاسبات ذاتی‌شان، قابلیت تصمیم‌گیری و تصمیم‌سازی، خودکنترلی، خودتنظیمی و خودعامل‌سازیِ به‌مراتب بهتری از خود نشان می‌دهند[۶]. اقدامات متقابل الکترونیکیِ (EA)[1] فعال شامل تخریب اثربخشی پشتیبانی جنگ الکترونیک دشمن از طریق انتشار و انتقال انرژی الکترومغناطیسی است. در این حوزه با دو فاکتور اصلی و اساسی سروکار داریم؛ جمینگِ نویزی و جمینگِ فریب[۱].

جمینگ مانع از انجام عملیات متداول رادار در اندازه‌گیری موقعیت و سرعت هدف می‌شود، در حالی‌که تکنیک‌های فریب سبب ایجاد موقعیت و سرعت نادرست و ساخت یک هدف جعلی می‌شوند. با عنایت به اینکه اهمیت و پیچیدگی حوزه بکارگیری و فناوری در زمینه فریب از اهمیت ویژه‌ای برخوردار است به‌طور کلی عملیات فریب در حوزه الکترونیکی را می‌توان در چهار دسته کلی زیر تعریف نمود:

(۱) تولید اهداف جعلی؛ (۲) فریب برد؛ (۳) فریب سرعت؛ (۴) فریب زاویه[۳ و ۷].

تولید اهداف جعلی: این نوع فریب نوعی از پارازیت موثر است که در برابر رادارهای هشدار اولیه، رهگیر و رادارهای رهگیری کنترل زمینی می‌تواند مورد استفاده قرار گیرد. در این نوع فریب با تولید تعداد زیادی اکوی جعلی هدف مشابه با اکوی اصلی هدف به دنبال گیج کردن رادار دشمن و اپراتور می‌باشیم[۱]. زمانی که این تکنیک با موفقیت انجام شود اپراتور رادار نمی‌تواند بین هدف اصلی و اهداف جعلی تمایز قائل شود[۲].

فریب در برد (RGPO)[2]: در این تکنیک، به دنبال ایجاد فریب در تشخیص برد توسط سامانه راداری و یا سامانه هدایت خودکار موشک می‌باشیم. روش کار به این صورت است که در ابتدا گیت برد سامانه راداری دریافت و بر اساس الگوهای از پیش مشخص شده به آن یک تاخیر زمانیِ منطقی اضافه شده و سپس باز انتشار داده می‌شود، نتیجه به این صورت خواهد بود که به علت وجود اختلاف بین مدارهای زمانی، فاصله واقعی تا هدف اشتباه برآورد شده و نهایتاً اطلاعات غلط نمایش داده خواهد شد.

فریب در سرعت (VGPO)[3]: رادارِ موج پیوسته و پالس داپلر اهداف را بر اساس سرعت یا فرکانس جابجایی داپلر ردگیری می‌کند. در این تکنیک فریب، اطلاعاتِ ردگیری سرعت با تولید اهدافی با سرعت مشابه هدف اصلی جایگزین می‌شوند، این کار از طریق ربایش گیت سرعت، نویز داپلر و نویز داپلر باند باریک صورت می‌پذیرد.

---

[1] Electronic Attack
[2] Range gate pull-off
[3] Velocity gate pull-off

فریب در زاویه: در این تکنیک، تمرکز ما بر روی توانایی رادار ردیاب برای استخراج زاویه صحیح و اطلاعات ارتفاع یک هدف است. بنابراین، رادار اطلاعات نادرست در مورد موقعیت زاویه‌ای هدف را در نهایت به دست خواهد آورد. بر اساس الگوریتم‌های اندازه‌گیری زاویه، چندین تکنیک فریب زاویه‌ای مختلف داریم. مدولاسیون سرعت اسکن و اخلال بهره معکوس از جمله تکنیک-هایی است که می‌توان در برابر رادارهای اسکن مخروطی به‌کار برد؛ از طرفی برای رادارهای ردگیر حین اسکن (LORO)[1] اخلال موج مربعی جاروبی می‌تواند موثر واقع گردد و برای رادارهای تک پالسی از جمینگ چشم متقاطع (چشم لوچ) استفاده نمود[۲].

۲- تاریخچه و مروری بر کارهای انجام شده

این یک واقعیت ثابت شده است که سیستم‌های EW دارای تاثیر مستقیم و عامل برتری‌ساز بر روی فضای اطلاعاتی نبردها و تقابل‌های نظامی می‌باشد. در حال حاضر، به‌منظور تعیین ارزش ذاتی تکنیک‌های هوش مصنوعی به‌عنوان یک جزء از یک سیستم نوین و بهبود یافته EW به‌طور گسترده‌ای در حال بررسی هستند؛ به‌گونه‌ای که استفاده بهینه و کارآمد از منابع به‌طور کامل ارتقا یافته و یا تقویت شود. در همین راستا، تعدادی از تکنیک‌های مبتنی بر هوش مصنوعی جهت بهبود عملکرد یک سیستم EW ارائه شده است[۹ و ۱۳]. EW هر اقدام نظامی که شامل استفاده از کل طیف الکترومغناطیسی به‌منظور رهگیری، تجزیه و تحلیل و دستکاری جهت استفاده دیرهنگام دشمن از طیف و تواماً حفاظت از طیف الکترومغناطیس جهت استفاده موثر نیروهای خودی می‌باشد. هدف از EW تشخیص دشمن به‌صورت الکترونیکی است که به‌عنوان بخشی از قابلیت‌های مورد استفاده در صحنه تعارض می‌باشد، از بین بردن موثر پشتیبانی جنگ الکترونیک دشمن و جلوگیری و ممانعت از اثربخشی اقدامات جنگ الکترونیکِ خصمانه بر علیه نیروهای خودی از دیگر قابلیت‌های EW است که می‌توان بدان اشاره نمود.

EW مجموعه‌ای از تاکتیک‌ها و تکنیک‌هایی است که برای جلوگیری از دسترسی آزاد به طیف الکترومغناطیسی و ممانعت از سرویس‌دهی و خدمات ارائه شده توسط سیستم‌های ارتباطی و یا راه‌کنش‌های مبتنی بر رادار به عنوان بخشی از طرح‌ریزی یک عملیات نظامی مورد بهره‌برداری قرار می‌گیرد. EW از سه زیرشاخه اصلی به‌شرح زیر تشکیل شده است. در میان تکنیک‌های ML/DL موارد زیر مطلوب و کارآمد ارزیابی گردیده‌اند:

۱) ANN : یک شبکه عصبی انسان آنالوگ ساده‌شده ریاضی است که به سبک لایه هوشمند و به شیوه بازگشتی و طبقه‌بندی وظایف، اطلاعات ورودی را پردازش می‌کند. ANN می‌تواند به تنهایی آموزش دیده و یک خروجی قابل قبول تولید کنید که محدود به ورودیِ مشروط نیست. با توجه به نوع معماری موازی، ظرفیت تحمل خطا، توانایی مدیریت و توصیف داده‌های نویزی و ناقص انواع رادار، از ANN جهت شناسایی یک انتشاردهنده راداری و انجام فرآیند تشخیص، انتخاب نوع جمینگ و ... استفاده می‌شود [۷ و ۱۴و ۱۶-۱۷]. علاوه بر این، ANN را می‌توان با المان‌های دیگری مانند تکنیک‌های هوش مصنوعی از جمله: GA، DNN و ... ترکیب نمود. برای شکل‌دهی به یک الگوریتم ترکیبی به‌منظور توسعه سیستم تشخیص جمینگ، شناسایی پارامتر اسکن آنتن رادار و ... در [۱۶ و ۱۸] بحث شده است. عملکرد الگوریتم‌های مبتنی بر ANN در حوزه‌های مختلف EW از نظر دقت در جدول شماره (۱) نشان داده شده است.

۲) CNN: روش‌های مبتنی بر DL به موفقیت بزرگی در پردازش گفتار، متن و تصویر دست یافته‌اند[۱۹]. CNN نوعی از DL است که مزایای زیادی در استخراج ویژگی‌های متمایز و ثابت ورودی‌ها دارد. توانایی بالقوه استخراج ویژگی CNN توسط علوم اعصاب الهام گرفته شده است[۲۰]. علاوه بر این، CNN به‌طور پیوسته‌ای در حوزه پردازش و طبقه‌بندی سیگنال‌های جمینگ رادار بسیار موفق بوده است [۸ و ۲۱-۲۲]. با این حال، روش‌های مبتنی بر CNN معمولاً به تعداد زیادی نمونه‌های آزمایشی نیاز دارند. بنابراین در شرایط آزمایشگاهی که نمونه‌ها محدود هستند، از سیامی CNN -(S-CNN) می‌توان استفاده نمود[۲۰]. اثربخشی الگوریتم‌های مبتنی بر CNN از نظر دقت در حوزه‌های مختلف EW در جدول شماره (۱) نشان داده شده است.

[1] Lobe-On-Receive-Only

۳) حافظه کوتاه مدت ماندگار (LSTM) : RNNهای قدیمی یک مانع بزرگ به نام محوشدگی گرادیان (یادگیری ژرف) داشتند که منجر به بروز مشکلاتی در هنگام پردازش طولانی مدت داده‌ها می‌شد [۸]. برای حل این مشکل، یک معماری اصلاح شده از ساختار RNN تحت عنوان LSTM توسعه داده شد. LSTM قادر به یادگیری در فرآیندهای طولانی مدت است [۳۵]. این ویژگی برای طبقه‌بندی، پردازش و پیش‌بینی سری‌های زمانی با توجه به وجود تاخیرهای زمانی با مدت نامعلوم مناسب است. LSTM عمدتاً برای حل مسئله پیش‌بینی زمان استفاده می‌شود؛ چراکه می‌تواند وضعیت لحظه بعدی را بر اساس وضعیت داده‌ها در لحظه قبل پیش‌بینی کند. از این رو، می‌توان از آن در پردازش سیگنال رادار و گزینش تکنیک جمینگ مناسب استفاده نمود [۲۳].

۴) یادگیری تقویتی عمیق (DRL)[1]: تقویت یادگیری حوزه‌ای از یادگیری ماشینی است که برای انجام اقدامات مناسب و کارآمد برای به حداکثر رساندن نتیجه موثر در یک موقعیت خاص استفاده می‌شود. از این نوع یادگیری برای یافتن و گزینش رفتار مناسب یا مسیر صحیحی که باید در یک موقعیت خاص طی شود بهره گرفته می‌شود[۲۴]. DRL ترکیبی از یادگیری تقویتی و یادگیری عمیق است. یادگیری Q، الگوریتم یادگیری تقویتی ساده شده‌ایست که به‌دنبال این است که ساختار یادگیری را به‌گونه‌ای پیاده-سازی کند تا نتیجه کلی را به مقدار بیشینه ممکن برساند [۱۹]. یک الگوریتم یادگیری تقویتی که ترکیبی از یادگیری Q با شبکه‌های عصبی عمیق است، تحت عنوان شبکه Q عمیق (DQN)[2] نامیده می‌شود. تکنیک‌های DRL می‌تواند برای توسعه الگوریتم های ضدجمینگ در یک رادار معمولی استفاده شود. روش‌های مبتنی بر یادگیری تقویتی می‌تواند به رادار در یادگیری استراتژی انتخاب شده توسط اخلال‌گرها با توجه به تجربه و دانشِ خود و سپس انتخاب استراتژی توانمند جهت مقابله با جمینگ، کمک کند[۲۵].

۳- تکنیک‌های هوش مصنوعی

هوش مصنوعی در واقع یک هوش غیرانسانی است که به کمک آن می‌توان یک سیستم مبتنی بر کامپیوتر را به‌گونه‌ای توسعه داد که بتواند از مهارت‌های ذهنی انسان الگوبرداری کرده و آن‌ها را شبیه‌سازی کند. به‌طور متداول تکنیک‌های رایج هوش مصنوعی یادگیری به‌صورت ماشینی (ML)[3]می‌باشند، که مشتمل بر شبکه‌های عصبی مصنوعی (ANN)[4] و یادگیری عمیق (DL)[5] یا شبکه عصبی عمیق (DNN)[6]، منطق ابهام[7]، الگوریتم ژنتیک و ... است. این تکنیک‌ها در ادامه به‌طور خلاصه مورد بحث قرار خواهد گرفت.

۳-۱- یادگیری ماشین

شبکه عصبی مصنوعی (ANN): یک ANN در واقع یک ابزار محاسباتی غیرپارامتریک است که می‌توان آن را به‌گونه‌ای آموزش داد تا وظایفِ محاسباتی مختلفی مانند تشخیص الگو، طبقه‌بندی، خوشه‌بندی داده‌ها[8]، و ... را انجام دهد. واحد محاسباتی در ANN یک نورون مصنوعی است، که می‌تواند پس از دریافت پاسخ ورودی از همتای بیولوژیکی خروجی را ایجاد کند. این نورون‌ها با پیوندهای سیناپسی با وزن‌ها در ارتباط هستند و در لایه‌هایی گروه‌بندی شده تا شبکه‌ای را جهت پردازش یک سیگنال ورودی پیاده‌سازی کنند. شبکه شامل یک لایه ورودی، تعدادی لایه پنهان و یک لایه خروجی است. ANNها ممکن است دو نوع پیکربندی شبکه متفاوت داشته باشند، یعنی شبکه با بازخورد و شبکه بدون بازخورد. شبکه دارای بازخورد، یک شبکه غیر تکراری یا غیر بازگشت‌شونده است و اطلاعات به‌صورت یک‌طرفه جریان دارد. شبکه با بازخورد، یک شبکه تکرارشونده یا بازگشت‌شونده می-باشد و اطلاعات در آن می‌تواند در هر دو طرف از طریق حلقه به‌وجود آمده جریان داشته باشد. مکانیسم یادگیری مورد استفاده در

[1] Deep reinforcement learning
[2] Deep Q- Network
[3] Machine Learning
[4] Artifcial Neural Network
[5] Deep Learning
[6] Deep Neural Network
[7] Fuzzy Logic
[8] data clustering

شبکه‌های عصبی مصنوعی ممکن است به‌صورت یادگیری تحت نظارت یا بدون نظارت باشد. پرسپترون چند لایه (MLP)[1] ساده-ترین ANN پیش‌خوردی آموزش‌دیده با یک الگوریتم پس انتشاری است، بهترین روش مبتنی بر یادگیری غیر پارامتریک بوده و برای پیش‌بینی، طبقه‌بندی و آمارگیری مناسب است. نمونه دیگری از ANN پیشخوردی، شبکه عصبی تاخیر زمانی (TDNN)[2] است. شبکه عصبی بازگشتی (RNN)[3] و شبکه آمارگیرِ خودکارِ غیرخطی با ورودی‌های برون‌زا (NARX) نمونه‌هایی از ANN دارای بازخورد هستند. MLP ظرفیت پردازش زمان را نداشته، در حالی‌که TDNN، RNN و NARX نشان می‌دهند که توانایی پردازش سیگنال‌های وابسته به زمان را دارند.

۳-۲- سیستم‌های فازی[4]

منطق فازی[5]، مجموعه ثابتِ متداول را با طبقه‌بندی آماری که از طریق توابع همووندی با قابلیت ردگیریِ تغییرات محدود در ورودی‌ها شکل گرفته است، ترکیب می‌کند. سیستم‌های فازی تلاش می‌کنند تا با استفاده از ANN و اطلاعات مجهول، سیال و نامتقن در قالب یک روش مشابه با تصمیم‌گیری انسانی عمل کنند [۳۱]. سیستم‌های فازی قابلیت یادگیری یا حافظه ندارند. از این‌رو، مدل‌سازی فازی اغلب با تکنیک‌های دیگری ترکیب شده و یک سیستم هیبریدی (ترکیبی) را ایجاد می‌کنند. به‌عنوان مثال، سیستم‌های عصبی-فازی، که ترکیبی از یک شبکه عصبی و سیستم فازی است از جمله این سیستم‌های هیبریدی محسوب می‌شود. این نوع سیستم‌ها کاربرد گسترده‌ای در مجموعه‌های راداری و مباحث مرتبط با پردازش سیگنال دارند[۲۷].

۳-۳- الگوریتم ژنتیک (GAs)[6]

GA تلاش می‌کند تا فرآیندهای ارزیابیِ رویدادهای طبیعی را تکرار و با برقراری یک پشتیبانیِ نظارتی، از حصول نتیجه مطلوب با اتخاذ یک راه حل بهینه مطمعن شود. این یک تکنیک تکرارپذیر بر اساس احتمال است. الگوریتم تا زمانی فرآیند پیشرفت خود را دنبال می‌کند که رضایت بخش بوده و مشکل را حل کند. راه‌حل‌های مطلوب در یک جامعه هدف اتخاذ و ویژگی‌های آن به زیرشاخه‌ها منتقل می‌شوند، که جایگزین راه‌حل‌هایی خواهند بود که بازدهی و تاثیرگذاری کم‌تری ایجاد کرده‌اند. بر خلاف برخی از تکنیک‌های جستجوی تصادفی، که یک راه حلِ واحد را در اختیار قرار می‌دهد، GA مجموعه‌ای از راه‌حل‌ها را با خود دارد، بنابراین احتمال ایجاد یک خطای کاذب، کاهش یافته و راه‌حل موجود بهینه‌سازی می‌شود [۲۶]. GA برای حل طیف وسیعی از چالش‌ها ترجیح داده می‌شود. برای محیط‌های پویا، چندین ANN و DNN باهم ترکیب می‌شوند [۲۷]. به‌طور مشابه، سیستم های فازی نیز با GA ترکیب شده و در طیف وسیعی از کاربردها مانند: پردازش سیگنال‌های راداری مورد استفاده قرار می‌گیرند[۲۶]. در بخش‌های بعدی، به مواردی اشاره می‌شود که اهمیت هوش مصنوعی در EW و ویژگی‌های برجسته کاربردی آن مشخص می‌گردد.

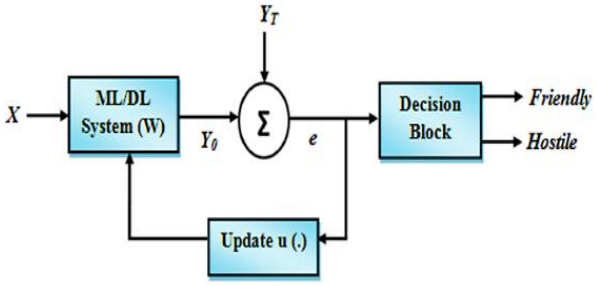
۴- سامانه جنگ الکترونیکِ مبتنی بر هوش مصنوعی

هوش مصنوعی در EW می‌تواند به نیروهای خودی کمک شایانی جهت مقابله با اقدامات دشمن و اختلال در خطوط و شبکه‌های ارتباطی آن‌ها از جمله GPS، سیگنال‌های ماهواره ای و ... کند. AI می‌تواند ظرفیت دانشی و اثربخشی EW برای اجرای هدفمند یک عملیات چند دامنه‌ای را بهبود بخشد. داده‌های دریافتی به ترتیب اولویت سریع و دقیق رتبه‌بندی شده و بنابراین سیگنال‌هایی با درجه اهمیت کمتر حذف می‌شوند. همچنین در پردازش حجم زیادی از داده‌ها نیز کاربرد داشته و در نتیجه تشخیص الگو و استخراج اطلاعات معنی‌دار با درجه اعتبار بالاتری صورت خواهد پذیرفت.

---

[1] Multi layer perceptron
[2] Time Delay Neural Network
[3] Recurrent neural network
[4] Fussy Systems
[۲] منطق فازی منطقی است که در آن برخلاف منطق‌های کلاسیک، عوامل متغیر از قبیل زمان و احتمال را در قالب اعداد بیان می‌کند.
[6] Genetic Algorithm

شکل شماره (۱)، جستجو و ردگیری سیستم به‌منظور نظارت مداوم بر امواج طیف الکترومغناطیسی برای مکان‌یابی آثار اقدامات خصمانه یا دوستانه را نشان می‌دهد. بلوک دیاگرام یک سیستم EW مبتنی بر هوش مصنوعی در شکل شماره (۲) نشان داده شده است. آنتن، انرژی الکترومغناطیسی دریافتی را تبدیل به یک سیگنال الکتریکی کرده به‌طوری که سایر فعالیت‌ها توسط بلوک‌های بعدی به‌راحتی انجام پذیرد. برای کاربردهای ECM انرژی الکتریکی به بخش‌های خاصی از طیف الکترومغناطیسی به‌منظور افزایش قابلیت‌های رزمی برده می‌شود. یک گیرنده برای شناسایی فرکانس سیگنال ارسالی و AOA سیگنال به‌منظور محاسبه محل فرستنده به‌کار رفته است. واحد آنالیز مقادیر پارامترهای سیگنال مانند PRF، عرض پالس، قدرت سیگنال، قطبش، TOA و AOA و ... موجود را اندازه‌گیری می‌کند. این اطلاعات برای تهیه یک بانک اطلاعاتی از تهدیدات و به منظور تهیه و ترسیم یک EOB صحیح و دقیق برای افزایش اشراف اطلاعاتی و آگاهی محیطی از توانمندی نیروی مقابل در صحنه رزم واقعی مورد استفاده قرار می‌گیرد.

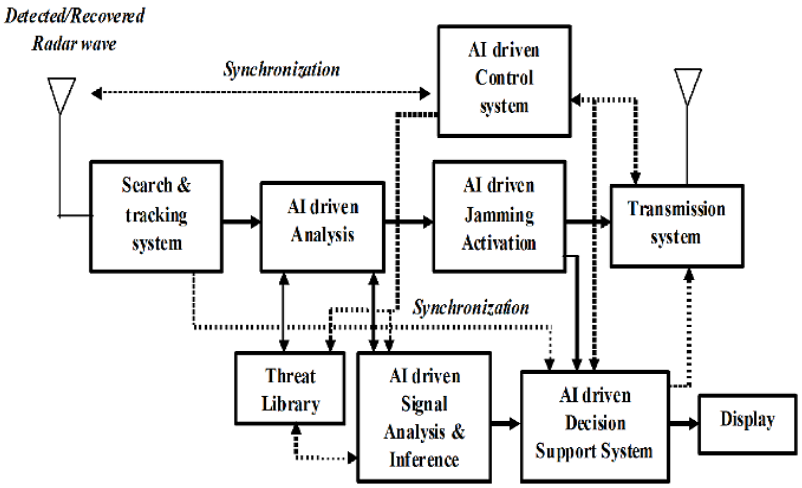


شکل ۱- پیاده‌سازی سیستم مبتنی بر هوش مصنوعی

اضافه بر این، طراحی و پیاده‌سازی اقدامات متقابل نوین به صورت هدفمند و جدی نیز به‌کار برده می‌شود. واحد تجزیه و تحلیل سیگنال و واحد استنتاج ممکن است از هوش مصنوعی بهره ببرد. عملکرد ماژول تجزیه و تحلیل سیگنال به این صورت است که پارامترهای سیگنال دریافتی از منبع متخاصم و یا از یک منبع دوستانه را به‌منظور شناسایی سیگنال مذکور اندازه‌گیری می‌کند. اطلاعات مورد نیاز در مورد پارامترهای سیگنال هدف از کتابخانه و بانک تهدیدات بارگذاری‌شده دریافت می‌شود. بسته به تصمیم اتخاذ شده توسط ماژول تجزیه و تحلیل، واحد فعال‌سازِ عملیات جمینگ یک سیگنال پارازیت مناسب اتخاذ می‌کند. پس از آن، آنتن اخلال‌گر سیگنال پارازیت را در راستای هدف هدایت می‌کند. سیستم کنترل نیز می‌تواند به‌گونه‌ای از طریق هوش مصنوعی هدایت شود که با سیستم ارسال سیگنال پارازیت، واحد تجزیه و تحلیل کننده سیگنال، کتابخانه تهدید و رادار آنتن دریافت سیگنال هماهنگی داشته باشد. ممکن است از الگوریتم هوش مصنوعی در این بخش استفاده شود تا تنها اجازه دریافت سیگنال رادار متخاصم داده شده تا به موجب آن سیگنال ارتباطی خودی از تخریب مصون بماند.

بنابراین سیگنال دشمن را می‌توان جهت استخراج پارامترهای مهم آن با کمک کتابخانه تهدید و ماژول تجزیه و تحلیل مورد بررسی و ارزیابی قرار داد. سپس این امکان فرآهم می‌شود تا یک سیگنال جمینگ مناسب بر اساس خروجی‌های واحد تجزیه و تحلیل و تصمیم‌گیرنده به‌منظور مقابله با رادار تهدید و ایجاد اختلال در عملکرد رادار مذکور در اندازه‌گیری موقعیت و سرعت اهداف، ساخته و ارسال گردد. به‌طور کلی، اگر از یک ML/DL مبتنی بر سیستم هوش مصنوعی در بلوک EW استفاده شود، نقش آن ارائه یک پیش‌بینی از وضعیت در حال تغییر خواهد بود. این وضعیت را می‌توان به‌صورت ریاضی و با استفاده از یک بلوک دیاگرام تعمیم‌یافته همانطور که در شکل شماره (۲) نیز نمایش داده شده، نشان داد. حال اگر پارامتر "X" را یک سیگنال ورودی داده شده به یک سیستم ML/DL (W) در نظر بگیریم، آن‌گاه خروجی 'Y0' در قالب رابطه (۱) بیان می‌شود:

$$Y0 = [X][W] \quad (۱)$$



شکل۲- بلوک دیاگرام پایه یک سامانه جنگ الکترونیک مبتنی بر هوش مصنوعی

برای یک سیستم ML/DL تحت نظارت، استقرا خروجی هدف با YT سنجیده می‌شود و سیگنال خطا نیز به‌صورت رابطه (۲) بیان می شود:

$$e = Y0 - YT \qquad (۲)$$

به‌روز رسانی وزن یا تطبیق [W] تا زمان به حداقل رساندن خطا ادامه دارد. این بخشی از یادگیری تحت نظارت انجام می‌پذیرد. برای حالتی که Y0 فاقد نظارت است با یک توزیع گاوسی مدل شده و اگر الزامات انحراف/واریانس استاندارد را برآورده سازد، سیستم آن‌را در قالب یک فرآیند آموزش کامل در نظر می‌گیرد. پس از پایان مرحله آموزش/یادگیری، خروجی از طریق یک آستانه بر اساس بلوک تصمیم‌گیری که سیگنال ورودی را به عنوان سیگنال خودی و یا خصمانه تفکیک می‌کند، ارسال می‌شود. یک ترکیب از الگوریتم‌های مبتنی بر هوش مصنوعی در خصوص پردازش سیگنال پیشرفته و هوشمند می‌توانند به نیروهای نظامیِ متخصص در شناسایی تغییرات روزافزون و گسترده تهدیدات به‌طور مثال تهدیدات ناشی از رادارهای تطبیقی کشورهای هدف و روش‌های مقابله با آن‌ها کمک شایانی داشته باشد. علاوه بر این، این الگوریتم‌ها قابلیت این را دارند که سیستم‌های EW را به‌گونه‌ای توانمند سازند تا به‌طور مستقل تهدیدات را شناسایی و بهترین و موثرترین اقدامات مقابله‌ای را بر علیه آن‌ها اتخاذ نمایند.

البته از طرفی این امکان وجود دارد که بر اثربخشی اقدامات مقابله‌ای نظارت داشته باشند تا در صورت نیاز و یا ناکارآمد بودن اقدامات اتخاذ شده (به‌طور مثال در برابر یک رادار متخاصم) سایر تکنیک‌های موثر و قابل تطبیق را به‌کار ببرند. الگوریتم‌های هوشمند مبتنی بر هوش مصنوعی با استفاده از ANN، DNN ترکیبی از فن‌آوری ANN-GA یا تکنیک ANN-DNN را می‌توان برای تجزیه و تحلیل مشخصه‌های منحصر به فرد رادارِ هدف استفاده تا از این طریق گسیل‌گرهای مختلف موجود در محیط پیرامون را به طرز صحیح و دقیقی شناسایی و طبقه‌بندی نمود. این الگوریتم‌ها می‌توانند همچنین جهت تشخیص اخلال‌گرها و ویژگی‌های آن‌ها استفاده شده و برای توسعه روش‌های موثر ضدجمینگ به‌کار گرفته شوند. جدول زیر نشان می دهد که چگونه تکنیک های هوش مصنوعی در طرح¬های کاربردی مختلف در تمام زیرمجموعه های EW نتایج امیدوارکننده ای در اختیار قرار می دهد.

جدول ۱- صحت و دقت عملکرد تکنیک‌های هوش مصنوعی در جنگ الکترونیک

کاربرد تکنیک‌های هوش مصنوعی	حوزه‌های جنگ الکترونیک	دقت صحت اثربخشی
CNN بر اساس نوع تشخیص مدولاسیون PRI	ES	٪ ۹۶.۱
CNN، SAE بر اساس سامانه تشخیص سیگنال رادار	ES	٪ ۹۹.۸
شبکه عصبی بر اساس طبقه‌بندی و تشخیص انتشاردهنده سیگنال راداری	ES	٪ ۸۴
تفکیک‌کننده ترکیبی شامل CNN و ENN جهت تشخیص شکل موج راداری	ES	٪ ۹۴.۵
GA-ANN بر اساس سیستم آشکارساز جمینگ فریب	EA	٪ ۹۵.۲

SVM بر اساس مدل انتخاب نوع جمینگ	EA	٪ ۹۸.۳۴
DNN بر اساس سامانه تشخیص پیش‌یابی اخلالگر و مشخصه‌های آن	EA	٪ ۸۵
الگوریتم یادگیری ماشین مشتمل بر تفکیک‌کننده ساده بیزی و ANN آشکارسازی، طبقه‌بندی و انتخاب نوع اقدام مقابله‌ای موثر در برابر تهدیدات [۷]	EA/ES	٪ ۹۶
ANN مبتنی بر تشخیص مدولاسیون PRI	ES	٪ ۹۹
DCNN و CDAE مبتنی بر تشخیص مدولاسیون درون‌پالسی سیگنال رادار	ES/EA	٪ ۹۵
الگوریتم هوش مصنوعی (ANN، SVM و DNN) برای تشخیص پارامتر اسکن آنتن رادار	ES	٪ ۹۰
خوشه‌بندی WARDS و PNN بر اساس آشکارسازی و طبقه‌بندی سیگنال ارسالی رادار	ES	٪ ۱۰۰
ANN، میزان احتمال و آنتروپی تقریبی برای طبقه‌بندی سیگنال رادار	ES	٪ ۹۹
الگوریتم هوش مصنوعی (NB، DT، ANN و SVM) برای تخمین و تشخیص پریود و نوع اسکن آنتن رادار	ES	٪ ۹۷

سیستم‌های EW موجود می‌بایست ماهیتی پویا به‌همراه یک سیستم بازخوردی حلقه بسته داشته باشند. این ویژگی شرایطی به‌وجود می‌آورد که یک پاسخ هوشمندانه به‌منظور سرکوب رادار تهدید ارسال شود. از این‌رو تکنیک‌های هوش مصنوعی می‌توانند یک ابزار قدرتمند برای سیستم‌های EW جهت بهره‌برداری از سیگنال‌های راداری ناشناخته محسوب شوند. علاوه بر این، مکانیسم بازخورد می‌تواند بین سیستم ارسال و دریافت یک هماهنگی مناسب ایجاد کرده تا عملکرد عملیات جمینگ بهینه‌سازی گردد. با کمک یادگیری ماشین و تشخیص ساختار الگوریتم‌ها، سیستم‌های هوشمند EW ممکن است قادر باشیم تا فرآیندهای ذهنی انسان از قبیل ادراک، حافظه، قضاوت و استدلال را به گونه‌ای مشابه تقلید کنیم.

۵- جنگ الکترونیک و کاربردهای ویژه تکنیک‌های هوش مصنوعی

چندین تکنیک خاص مربوط به ECM عامل و غیرعامل و ECCM در زمینه‌های کاربردی و مهم که در بیشتر اسناد و مدارک معتبر بدان اشاره شده در این بخش مد نظر است. علاوه بر این، چند تکنیک هوش مصنوعی نیز که برای کاربردهای خاص EW مناسب هستند، مقایسه خواهند شد.

ECM: بیشتر اقدامات ECM وابسته به المان‌های بسیار مهمی به نام زمان و مکان بوده که گاهاً با سرعت بالا و یا به‌صورت آرام به‌کارگیری می‌شوند؛ بنابراین برای طیف وسیعی از این کاربردهای متنوع، ممکن است ابزارهای ML/DL گزینه مناسبی باشند. در اینجا چند مورد از حوزه‌های ECM با توجه به کاربرد تکنیک‌های ML/DL مورد بحث قرار می‌گیرند. اخلال، یک تهدید برای یک سیستم راداری نظارتی محسوب شده و انجام اقدامات ضد جمینگ یکی از راه‌حل‌ها برشمرده می‌شود. بنابراین، طبقه‌بندی جمینگ راداری اولین قدم به سوی دستیابی به وضعیت ضدجمینگ است. در این راستا، یک روش مبتنی بر CNN برای طبقه‌بندی انواع سیگنال جمینگ راداری در[۲۷] مورد بحث قرار گرفته است. در این روش در ابتدا، یک D-CNN برای طبقه‌بندی سیگنال جمینگ راداری تحت شرایط آزمایشگاهی طراحی شده است. از آنجا که گردآوری نمونه‌های آزمایشی جهت دریافت خروجی‌های قابل قبول وقت‌گیر و پرهزینه است، بنابراین برای حل این چالش، یک شبکه سیامی مبتنی بر CNN برای طبقه‌بندی سیگنال جمینگ راداری، توسعه داده شده است.

در هر دو روش دقت طبقه‌بندی خوبی گزارش شده است. در [۲۸] یک روش جدید برای تشخیص جمینگ نوع "سدی" و طبقه‌بندی رادار روزنه مصنوعی (SAR)[1] بر اساس CNN مورد بحث قرار گرفته است. در این روش می‌توان به‌طور موثری نسبت به

[1] Synthetic Aperture Radar

آشکارسازی و طبقه‌بندی جمینگ در سیگنال‌های فرکانس پایین SAR اقدام نمود. دو روش مطلوب برای پیش‌بینی تکنیک جمینگ در برابر سیگنال تهدید دریافتی با استفاده از روش یادگیری عمیق در [28] ارائه شده است. در مرحله اول، یک DNN جهت استخراج مقادیر ویژگی‌ها به‌صورت دستی از لیست کلمه توصیف پالس (PDW)[1] سیگنال رادار استفاده می‌شود؛ سپس حافظه کوتاه مدت ماندگار (LSTM)[2] استفاده می‌شود که لیست PDW را به‌عنوان ورودی دریافت می‌کند. این مدل‌های یادگیری عمیق، تکنیک‌های مناسب اختلال را در برابر سیگنال‌های تهدید دریافتی بدون استفاده از کتابخانه را پیش‌بینی و برآورد می‌کنند. عملکرد پیش‌بینی و پیچیدگیِ زمانی دو روش باهم مقایسه می‌شود. بر اساس گزارش‌های به‌دست آمده، دقت پیش‌بینی مدل LSTM بیشتر از مدل DNN بوده اما مدل اول نیاز به زمان آموزش طولانی‌تری دارد.

"چف" نقش مهمی در محیط جنگ الکترونیک ایفا می‌کند[۲۹]. ابرهای چف به‌طور موثری قادر به انجام ماموریت خودحفاظتی از انواع سکوهای شناوری و پروازی در بستر جنگ الکترونیک هستند. انجام ماموریت عادی و عملکرد متداول یک رادار در زمان حضور چف چالش مهم و جدی است که رادار با آن مواجه است. بنابراین، مطالعه بر روی ویژگی‌های راداریِ ابر چف و اقدامات متقابل در برابر جمینگ چف بسیار حائز اهمیت است. از این جهت، تکنیکی برای تشخیص جمینگ چف بر اساس روش طبقه‌بندی SVM ارائه شده در است [۲۹]. در [۳۰] روشی برای تشخیص مشخصه‌های سیگنال جمینگ راداری شامل جمع‌پذیری، ضرب‌پذیری و کانولوشن جمینگ پوششی و جمینگ فریب متداول بر اساس شبکه‌های عصبی BP مورد بحث قرار گرفته است. در ابتدا، سیگنال-های جمینگ مرکب با تمام سیگنال‌های دریافتی (اِکو، جمینگ و نویز) در یک PRI مدل می‌شوند؛ سپس ویژگی‌ها در حوزه زمان، فرکانس و ابعاد هندسی استخراج می‌شوند. بعد از آن، طبقه‌بندی بر اساس شبکه عصبی BP جهت تشخیص انواع سیگنال‌های جمینگ مرکب ایجاد می‌شود.

۶- نتیجه‌گیری

جنگ الکترونیک یک قابلیت و دست برتر در نیروهای نظامی محسوب می‌شود که هم در زمان صلح و هم در زمان جنگ قابل به‌کارگیری و بهره‌برداریست. پیشرفت در فن‌آوری و علوم دیجیتال این امکان را برای نیروهای نظامی مدرن فرآهم کرده تا نسبت به توسعه اقدامات جنگ الکترونیک به‌گونه‌ای بسیار انعطاف‌پذیر و سازگار مبادرت نمایند تا سیستم‌ها و سامانه‌هایی طراحی و پیاده‌سازی نمایند که امکان انطباق سریع با محیط الکترومغناطیسی را داشته و از طرفی نیز با بهره‌گیری از الگوریتم‌های هوش مصنوعی به ایفای نقش خود بپردازند. استفاده از هوش مصنوعی، اجرای عملیات جنگ الکترونیک را به صورت مستقل و خودکافی تسهیل می‌کند، آگاهی موقعیتی را افزایش داده و به تصمیم‌گیری قابلیت اطمینان و اعتماد می‌بخشد. در این راستا یک سیستم جنگ الکترونیک مبتنی بر هوش مصنوعی می‌تواند در شناسایی یک رادار متخاصم ساطع‌کننده موثر به‌گونه‌ای موثر عمل کند تا میزان کشنده بودن آن تهدید را مشخص کند سپس بسته به درک و دانشی که از تهدید حاصل می‌شود می‌توان یک استراتژی مقابله‌ای مناسب بر اساس هوش مصنوعی و به‌منظور خنثی کردن تهدید خصمانه ترسیم و اجرا نمود. علاوه بر این، EW اطلاعات جمع‌آوری شده را می‌تواند به‌منظور درک صحیحی از نظم الکترونیکی از میدان نبرد، ایجاد آگاهی از موقعیت و توسعه اقدامات مقابله‌ای بر اساس سناریویی مشخص، پس از انجام فرآیند تجزیه و تحلیل در قالب یک بانک تهدید آماده‌سازی کرده و در اختیار نیروهای بهره‌بردار قرار دهد. EW در این روش مبتنی بر هوش مصنوعی می‌تواند به طراحان و فرماندهان میدان نبرد با بهره‌گیری از ابزارهای قابل اعتماد جهت اجرای اقدامات جنگی کمک کند.

۷- مراجع

1. F. Neri, Introduction to Electronic Defense Systems, 2nd ed. Rijeka, Croatia: SciTech, 2006.

[1] pulse description width
[2] Long short-term memory

۲. بی ون براونت، لِروی، "اقدامات متقابل الکترونیکیِ کاربردی (Applied ECM)"، ترجمه آریا بیرانوند، انتشارت پژوهش‌های نظری و مطالعات راهبردی نداجا، تهران، ۱۴۰۰، چاپ اول.

3. N. Waghray, ``Electronic warfare: The next step in national security,'' in Proc. Annu. IEEE India Conf., Dec. 2011, pp. 1_5.

4. L. Lazarov, ``Perspectives and trends for the development of electronic warfare systems,'' in Proc. Int. Conf. Creative Bus. Smart Sustain. Growth (CREBUS), Mar. 2019, pp. 1_3.

5. S. D. Spiegeleire, M. Mass, and T. Sweijs, Arti_cial Intelligence and the Future of Defense: Strategic Implications for Small-and Medium-Sized Force Providers. Hague, The Netherland: HCSS, 2017.

6. T. Singh and A. Gulhane. 8 Key Military Applications for Arti_cial Intelligence in 2018. Accessed: Jan. 6, 2020. [Online]. Available: https://blog.marketresearch.com/8-key-military-applications-for artificial-intelligence-in-2018

7. A. D. Martino, Introduction to Modern EW Systems. Norwood, MA, USA: Artech House, 2012.

8. H. Rahman, Introduction to Electronic Defense Systems. Boca Raton, FL, USA: CRC Press, 2019. [11] M. S. K. Shankar and B. V. Mohan, ``Recent advances in electronic warfare-esm systems,'' in Proc. AECE-IRAJ Int. Conf., 2013, pp. 125_130.

9. M. Erenet, Y. B. Salman, and J. S. Park, ``Clustering for electronic warfare information,'' in Proc. 18th Int. Conf. Control, Autom. Syst. (ICCAS), 2018, pp. 1195_1197.

10. S. Amuru, C. Tekin, M. van der Schaar, and R. M. Buehrer, ``A systematic learning method for optimal jamming,'' in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2015, pp. 2822_2827.

11. S. Noh and U. Jeong, ``Intelligent command and control agent in electronic warfare settings,'' Int. J. Intell. Syst., vol. 25, no. 6, pp. 514_528, Jun. 2010.

12. X. Li, Z. Huang, F. Wang, X. Wang, and T. Liu, ``Toward convolutional neural networks on pulse repetition interval modulation recognition,'' IEEE Commun. Lett., vol. 22, no. 11, pp. 2286_2289, Nov. 2018.

13. A. M. Elbir, K. V. Mishra, and Y. C. Eldar, ``Cognitive radar antenna selection via deep learning,'' 2018.

14. Y. Liu and Q. Zhang, ``An improved algorithm for PRI modulation recog- nition,'' in Proc. IEEE Int. Conf. Signal Process., Commun. Comput. (ICSPCC), Oct. 2017, pp. 1_5.

15. N. Petrov, I. Jordanov, and J. Roe, ``Radar emitter signals recognition and classi_cation with feedforward networks,'' Procedia Comput. Sci., vol. 22, pp. 1192_1200, Jan. 2013.

16. T. Wan, X. Fu, K. Jiang, Y. Zhao, and B. Tang, ``Radar antenna scan pattern intelligent recognition using visibility graph,'' IEEE Access, vol. 7, pp. 175628_175641, 2019.

17. B. Barshan and B. Eravci, ``Automatic radar antenna scan type recognition in electronic warfare,'' IEEE Trans. Aerosp. Electron. Syst., vol. 48, no. 4, pp. 2908_2931, Oct. 2012.

18. D. Wei, S. Zhang, S. Chen, H. Zhao, and L. Zhu, ``Research on deception jamming of chaotic composite short-range detection system based on bispectral analysis and genetic algorithm_back propagation,'' Int. J. Distrib. Sensor Netw., vol. 15, no. 5, pp. 1_11, 2019.

19. Y. LeCun, Y. Bengio, and G. Hinton, ``Deep learning,'' Nature, vol. 521, no. 7553, pp. 436_444, May 2015, doi: 10.1038/nature14539.

20. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning: Adap- tive Computation and Machine Learning Series. Cambridge, MA, USA: MIT Press, 2016.

21. J. Gao, Y. Lu, J. Qi, and L. Shen, ``A radar signal recognition system based on non-negative matrix factorization network and improved artificial bee colony algorithm,'' IEEE Access, vol. 7, pp. 117612_117626, 2019.

22. G. Shao, Y. Chen, and Y. Wei, ``Convolutional neural network based radar jamming signal classification with suficient and limited samples,'' IEEE Access, vol. 8, pp. 80588_80598, 2020.

23. G.-H. Lee, J. Jo, and C. H. Park, ``Jamming prediction for radar signals using machine learning methods,'' Secur. Commun. Netw., vol. 2020.

24. Y. Li, X. Wang, D. Liu, Q. Guo, X. Liu, J. Zhang, and Y. Xu, ``On the performance of deep reinforcement learning-based anti-jamming method confronting intelligent jammer,'' Appl. Sci., vol. 9, no. 7, pp. 3161_3176, 2019.

25. L. Kang, J. Bo, L. Hongwei, and L. Siyuan, ``Reinforcement learning based anti jamming frequency hopping strategies design for cognitive radar,'' in Proc. IEEE Int. Conf. Signal Process., Commun. Comput. (ICSPCC), Qingdao, China, Sep. 2018.

26. S. H. Chen, A. J. Jakeman, and J. P. Norton, ``Artificial intelligence techniques: An introduction to their use for modelling environmental systems," Math. Comput. Simul., vol. 78, nos. 2_3, pp. 379_400, Jul. 2008.

27. N.Waghray and P. M. Menghal, ``Simulation of radar topology networks to evolve the electronic warfare survivability metrics," in Proc. 3rd Int. Conf. Electron. Comput. Technol., Apr. 2011, pp. 355_359.

28. Y. Liu, S. Xing,Y. Li, D. Hou, and X.Wang, ``Jamming recognition method based on the polarisation scattering characteristics of chaff clouds," IET Radar, Sonar Navigat., vol. 11, no. 11, pp. 1689_1699, Nov. 2017.

29. F. Ruo-Ran, ``Compound jamming signal recognition based on neural networks," in Proc. 6th Int. Conf. Instrum. Meas., Comput., Commun. Control (IMCCC), Harbin, China, Jul. 2016.

30. Q. Tan andY. Song, ``Sidelobe suppression algorithm for chaoticFMsignal based on neural network," in Proc. 9th Int. Conf. Signal Process., Beijing, China, Oct. 2008, pp. 2429_2433.

31. S. H. Chen, A. J. Jakeman, and J. P. Norton, ``Artifcial intelligence techniques: An introduction to their use for modelling environmental systems," Math. Comput. Simul., vol. 78, nos. 2_3, pp. 379_400, Jul. 2008.

The Effect of Artificial Intelligence in Improving the Capabilities of Subsystems Electronic, Telecommunication and Cyber in the Electronic Platform

Erfaneh Norouzi *[1], Arya Beyranvand[2]

1- Assistant Professor, Department of Computer Engineering, Technical and Engineering Faculty, Islamic Azad University Qeshm International Branch, Iran

2-Assistant Professor of Electronic Warfare Department, Faculty of Forestry, AJA Electronic Warfare, Tehran, Iran

*noroozierfaneh@gmail.com

Abstract

Electronic warfare (EW) is one of the most important features of modern battles. This area can significantly affect the way military forces use the electromagnetic spectrum to identify targets or provide information. Recent developments in the field of artificial intelligence (AI) show that this emerging technology will have a definite and potentially transformative impact on the military power of any country. Algorithms based on artificial intelligence can play a very effective role in various fields of EW, such as: processing radar signals in order to identify and classify types of transmitters, detecting the type of jamming operation and its characteristics, and such development of effective anti-disruption algorithms. Artificial intelligence techniques can also enable various types of EW systems to work independently and self-sufficiently. Our focus in this article is on describing the basic aspects of EW and its related components, various elements and technologies related to the current generation of EW systems, the application of artificial intelligence in electronic warfare systems and equipment, especially in the field (EA) as an auxiliary element to make decisions and perform a correct and effective reaction against radar systems and equipment in the battle scene and evolving EW scenarios for military forces (currently or future plans) Is. The two main ECM techniques include active ECM and passive ECM.

keywords: Artificial Intelligence, Cyber security, Machine Learning, Eelectronic systems, Electronic Warfare.