Defensive Researches and Management

Layered Defense Against Drone Threats: Integration of Intelligent Detection-to-Response Systems

Farhad Kiani Falavarjani *[1]

1. Corresponding Author: PhD Student in Aerospace Engineering, Faculty of Mechanical Engineering, Malek Ashtar University of Technology, Shahin Shahr, Isfahan, Iran.
Email: Aerospace1362@gmail.com

Volume info

Vol. 25
Series: 111
Spring 2026
P.P: 109-140

Article Type

Research Paper

Article History

Received:
2025-07-02
Revised:
2025-09-07
Accepted:
2026-06-01
Published:
2026-06-01

ISSN – E-ISSN

ISSN: 2008-6121
E-ISSN: 2645-5218

Abstract

With the escalating threats posed by drones in military and security domains, the design of efficient and intelligent defense systems to counter these threats has become an undeniable necessity. This article aims to elucidate a conceptual model of intelligent layered defense against drone threats by examining the structures, technologies, and algorithms employed in this field. The research approach involves a systematic review of scientific and technical literature, with data gathered from credible domestic and international sources. The findings indicate that effective layered defense systems consist of four primary layers: initial detection and monitoring, intelligent assessment and decision-making, counteraction and neutralization, and command and control (C4I). In this framework, the integration of multi-source data and the application of artificial intelligence play a pivotal role in enhancing the accuracy, speed, and effectiveness of defensive responses. The article concludes that the design of intelligent, adaptive, and multi-layered architectures represents the primary pathway to bolstering defensive resilience against the complex and evolving threats posed by drones.

Keywords: Layered Defense, Countering Drones, Anti-Drone Systems, Multi-Source Data Integration, Artificial Intelligence in Defense, Threat Detection Systems.

Cite this Article: Kiani Falavarjani, F. (2026). Layered Defense Against Drone Threats: Integration of Intelligent Detection-to-Response Systems. Scientific Journal of Defensive Researches and Management, 25(111), 109-140.

doi : 10.47176/mdr.2025.1413

Publisher: Imam Hossein University.

پدافند لایه‌ای در برابر تهدیدات پهپادی: ادغام سامانه‌های هوشمند شناسایی تا واکنش

فرهاد کیانی فلاورجانی [1]*

۱. نویسنده مسئول: دانشجوی دکتری مهندسی هوافضا، دانشکده مکانیک دانشگاه صنعتی مالک اشتر شاهین شهر، اصفهان، ایران. Email: Aerospace1362@gmail.com

چکیده

با رشد فزاینده تهدیدات ناشی از پهپادها در حوزه‌های نظامی، امنیتی، طراحی سامانه‌های دفاعی کارآمد و هوشمند برای مقابله با این تهدیدات ضرورتی انکارناپذیر یافته است. مقاله حاضر با هدف تبیین مدل مفهومی پدافند لایه‌ای هوشمند در برابر تهدیدات پهپادی، به بررسی ساختارها، فناوری‌ها و الگوریتم‌های به‌کاررفته در این حوزه پرداخته است. رویکرد پژوهش، مرور نظام‌مند ادبیات علمی و فنی بوده و اطلاعات از منابع معتبر داخلی و بین‌المللی گردآوری شده است. یافته‌ها نشان می‌دهد که سامانه‌های پدافند لایه‌ای مؤثر، از چهار لایه اصلی شامل: شناسایی و پایش اولیه، ارزیابی و تصمیم‌گیری هوشمند، مقابله و خنثی‌سازی، و لایه فرماندهی و کنترل (C4I) تشکیل می‌شوند. در این ساختار، ادغام داده‌های چندمنبعی و بهره‌گیری از هوش مصنوعی، نقش کلیدی در افزایش دقت، سرعت و اثربخشی واکنش دفاعی ایفا می‌کنند. نتیجه‌گیری مقاله حاکی از آن است که طراحی معماری‌های هوشمند، تطبیق‌پذیر و چندلایه، مسیر اصلی ارتقاء تاب‌آوری دفاعی در برابر تهدیدات پیچیده و متحول پهپادی به شمار می‌رود.

کلیدواژه‌ها: پدافند لایه‌ای، مقابله با پهپاد،سامانه ضدپهپادی، ادغام داده‌های چندمنبعی،هوش مصنوعی در دفاع سامانه‌های شناسایی تهدید.

استناد: کیانی فلاورجانی، فرهاد. (۱۴۰۵). پدافند لایه‌ای در برابر تهدیدات پهپادی: ادغام سامانه‌های هوشمند شناسایی تا واکنش. فصلنامه مدیریت و پژوهش های دفاعی، ۲۵(۱۱۱)، ۱۴۰-۱۰۹.

doi : 10.47176/mdr.2025.1413

ناشر: دانشگاه جام امام حسین(ع).

مقدمه

با گسترش کاربرد پهپادها در حوزه‌های نظامی، اطلاعاتی و تروریستی، این وسایل پرنده بدون سرنشین به یکی از اصلی‌ترین تهدیدات نوین علیه زیرساخت‌ها، تأسیسات حساس و نیروهای نظامی بدل شده‌اند. پهپادها به دلیل قابلیت پرواز در ارتفاع پایین، سطح مقطع راداری بسیار کوچک، مانورپذیری بالا، هزینه ساخت و به‌کارگیری پایین، و همچنین قابلیت اجرای عملیات مستقل یا گروهی[1]، چالش‌های جدی برای سامانه‌های دفاعی سنتی ایجاد کرده‌اند. تجربه کشورها در درگیری‌های اخیر نیز نشان می‌دهد که حتی پهپادهای ساده‌ی تجاری، در صورت تجهیز به بارهای انفجاری یا دوربین‌های شناسایی، می‌توانند به ابزارهای مؤثر تهاجمی و جاسوسی تبدیل شوند(محمدی و همکاران،۱۴۰۲). در پاسخ به این نوع تهدیدات، مفهوم پدافند لایه‌ای[2] مطرح شده است؛ رویکردی ساخت‌یافته و چندسطحی برای مقابله با تهدیدات هوایی نوین. پدافند لایه‌ای برخلاف سامانه‌های واکنشی سنتی که عمدتاً بر اساس یک حسگر یا یک سطح واکنش عمل می‌کنند، از ترکیب چندین لایه‌ی شناسایی، تحلیل، ارزیابی و مقابله استفاده می‌کند.(پدرام و همکاران،۱۳۹۷). این ساختار چندلایه، انعطاف‌پذیری بیشتری در برابر طیف متنوعی از تهدیدات پهپادی فراهم می‌سازد، به‌طوری‌که حتی در صورت شکست یا اخلال در یک لایه، لایه‌های دیگر بتوانند تهدید را شناسایی یا خنثی کنند.هر لایه از این ساختار می‌تواند شامل فناوری‌های متفاوتی باشد؛ از حسگرهای اولیه نظیر رادارهای بردکوتاه، حسگرهای آکوستیک، سامانه‌های تصویری اپتیکی/مادون‌قرمز، تا سامانه‌های تحلیل داده و در نهایت تجهیزات واکنشی مانند اخلالگرهای امواج، پهپادهای رهگیر یا حتی سامانه‌های تسلیحاتی دقیق.

در این میان، نقش سامانه‌های هوشمند و الگوریتم‌های تحلیل بلادرنگ به‌عنوان مغز متفکر این ساختار برجسته است. در محیط‌های پیچیده امروزی که داده‌ها از منابع مختلف و به‌صورت پیوسته تولید می‌شوند، صرفاً داشتن تجهیزات شناسایی و واکنش کافی نیست. بلکه نیاز به سیستم‌هایی است که بتوانند داده‌ها را از منابع متعدد (چند سنسور، چند نقطه جغرافیایی، چند نوع سیگنال) به‌صورت هماهنگ تحلیل کنند و با دقت بالا تهدیدات واقعی را از موارد غیرتهدید تشخیص

1 Swarm Drones
2 Layered Defense

دهند(شریفی تهرانی و همکاران،۱۳۹۹). برای پیاده‌سازی این رویکرد، بهره‌گیری از فناوری‌های پیشرفته هوش مصنوعی مانند شبکه‌های عصبی کانولوشنی ، شبکه‌های بازگشتی، سیستم‌های خبره فازی، الگوریتم‌های یادگیری تقویتی و همچنین روش‌های شناسایی الگو[1] ضروری است. این سامانه‌ها می‌توانند بر اساس یادگیری مستمر از تهدیدات گذشته، دقت شناسایی تهدیدات آینده را ارتقاء دهند و واکنش سامانه را بهینه‌سازی کنند. در مجموع، بهره‌گیری از پدافند لایه‌ای هوشمند نه‌تنها به کاهش بار کاری اپراتورها کمک می‌کند، بلکه باعث کاهش چشمگیر خطای انسانی، افزایش سرعت واکنش و ارتقاء تاب‌آوری دفاعی در برابر تهدیدات پیچیده و ترکیبی پهپادی خواهد شد(Chen, and Pan 2022)

بیان مسئله

با توجه به تحولات سریع در فناوری پهپادها و افزایش دسترسی به آن‌ها، این سامانه‌ها به یکی از مهم‌ترین تهدیدات نوظهور در محیط‌های نظامی و امنیتی تبدیل شده‌اند. توانایی پهپادها در انجام عملیات شناسایی، جاسوسی، و حتی حملات دقیق، ضرورت طراحی و توسعه سامانه‌های دفاعی کارآمد را بیش از پیش نمایان کرده است.

با این حال، سامانه‌های پدافند هوایی سنتی که عمدتاً برای مقابله با هواپیماهای بزرگ طراحی شده‌اند، در برابر پهپادهای کوچک، سریع و با سطح مقطع راداری پایین، کارایی لازم را ندارند. این سامانه‌ها اغلب فاقد قابلیت‌های چندلایه برای شناسایی زودهنگام، ردیابی مداوم و مقابله مؤثر هستند. علاوه بر این، حجم بالای داده‌های دریافتی از منابع مختلف، نیاز به یکپارچه‌سازی و پردازش سریع را برای تصمیم‌گیری به‌هنگام، به یک چالش جدی تبدیل کرده است.

با وجود پژوهش‌های متعدد در زمینه سامانه‌های ضدپهپادی، مطالعات کمتری بر ارائه یک چارچوب مفهومی جامع که تمامی لایه‌های دفاعی را از شناسایی تا واکنش، با تمرکز بر ادغام داده‌های چندمنبعی و بهره‌گیری از هوش مصنوعی، به صورت یکپارچه مدل‌سازی کند، تمرکز داشته‌اند. بسیاری از رویکردهای موجود، بر یک لایه یا یک فناوری خاص متمرکز بوده‌اند و از ارائه یک دیدگاه سیستمی و یکپارچه در برابر تهدیدات پیچیده غافل مانده‌اند.

1 Pattern Recognition

بنابراین، با توجه به مشکلات و خلاءهای ذکر شده، هدف اصلی این پژوهش، تبیین یک مدل مفهومی برای پدافند لایه‌ای هوشمند در برابر تهدیدات پهپادی با تمرکز بر ادغام داده‌های چندمنبعی و کاربرد هوش مصنوعی است. این مدل، به دنبال ارائه یک معماری جامع برای افزایش دقت، سرعت و تاب‌آوری سامانه‌های دفاعی در برابر تهدیدات پیچیده و متحول پهپادی است.

مبانی نظری

۱. پدافند لایه‌ای:پدافند لایه‌ای یک رویکرد ساختاریافته در امنیت نظامی و سایبری است که با هدف افزایش تاب‌آوری دفاعی، از چندین سطح حفاظتی با عملکرد مکمل بهره می‌برد. این مفهوم در ابتدا در دفاع موشکی و سایبری توسعه یافت و بعدها به حوزه امنیت فیزیکی و هوایی از جمله مقابله با پهپادها نیز تعمیم داده شد. در ساختار پدافند لایه‌ای، هر لایه از سیستم نقش خاصی در شناسایی، تحلیل و پاسخ به تهدید ایفا می‌کند. این ساختار اجازه می‌دهد که حتی در صورت شکست یکی از لایه‌ها، دیگر لایه‌ها فعال شوند و از نفوذ تهدید جلوگیری کنند(B. Liu and Sun 2021).

چارچوب نظری پدافند لایه‌ای در برابر تهدیدات پهپادی، فراتر از یک مفهوم عملیاتی صرف است و ریشه در تلفیق پیچیده‌ای از دانش‌های متقاطع دارد(شریفی تهرانی و همکاران،۱۳۹۹). چهار حوزه دانشی اصلی که این چارچوب را تشکیل می‌دهند، عبارتند از: دفاع هوایی، مهندسی داده، هوش مصنوعی، و طراحی سامانه‌های سایبری-فیزیکی.

۲. دفاع هوایی :نخستین و بنیادی‌ترین حوزه، دفاع هوایی است. پدافند لایه‌ای در برابر پهپادها، بر اصول و تجربیات دیرینه دفاع هوایی تکیه دارد.این اصول شامل(, Xiaojing, and Chi 2023):

- شناسایی و ردیابی هدف: در دفاع هوایی سنتی، این امر توسط رادارها و سامانه‌های اپتیکی انجام می‌شد. در برابر پهپادها، با توجه به ابعاد کوچک، سرعت پایین و قابلیت پرواز در ارتفاع پایین، نیاز به حسگرهای متنوع‌تر و حساس‌تر (مانند حسگرهای صوتی، لرزه‌ای و رادارهای کوچک با قابلیت تشخیص اهداف ریز) است.
- ارزیابی تهدید: درک ماهیت تهدید (دوست یا دشمن بودن، نوع، ابعاد، سرعت، و مسیر حرکت) برای انتخاب بهترین روش مقابله حیاتی است.

- تصمیم‌گیری و تخصیص منابع: انتخاب مؤثرترین و به صرفه‌ترین مکانیزم مقابله (مانند اخلالگر، پهپاد رهگیر، یا سلاح فیزیکی) بر اساس نوع تهدید و وضعیت عملیاتی.
- مقابله و انهدام/خنثی‌سازی: به کارگیری ابزارهای مناسب برای از بین بردن یا بی‌اثر کردن تهدید.

۳. مهندسی داده: تهدیدات پهپادی در عصر حاضر، منبعی عظیم از داده‌های متنوع هستند؛ از تصاویر، ویدئوها، سیگنال‌های رادیویی، و داده‌های راداری و صوتی گرفته تا اطلاعات ناوبری و موقعیت (GPS، ارتفاع، سرعت، جهت) و حتی داده‌های محیطی مانند شرایط آب و هوایی و جغرافیایی. مهندسی داده در اینجا نقشی حیاتی ایفا می‌کند، چرا که مسئولیت جمع‌آوری، ذخیره‌سازی، پردازش، و مدیریت کارآمد این حجم عظیم و ناهمگن از اطلاعات را بر عهده دارد (Renu and Sarveshwaran2025).

۴. هوش مصنوعی: هوش مصنوعی، قلب تپنده چارچوب نظری پدافند لایه‌ای در برابر پهپادها به شمار می‌رود؛ چراکه سرعت فزاینده تهدیدات و ضرورت واکنش‌های آنی، اتکا صرف به تصمیم‌گیری انسانی را ناکافی ساخته است(Brust et al. 2021). هوش مصنوعی در چندین سطح کلیدی وارد عمل می‌شود: ابتدا، پردازش و تلفیق داده‌های حسگرها را با بهره‌گیری از الگوریتم‌های پیشرفته، به‌ویژه شبکه‌های عصبی عمیق، انجام می‌دهد تا با ترکیب داده‌های خام و ناهمگن، تصویری جامع و دقیق از وضعیت ایجاد کند که به طور چشمگیری دقت شناسایی را بالا برده و هشدارهای غلط را کاهش می‌دهد. در گام بعدی، هوش مصنوعی با استفاده از بینایی ماشین و الگوریتم‌های یادگیری عمیق، قادر به تشخیص و طبقه‌بندی خودکار پهپادها در تصاویر و ویدئوهاست و حتی می‌تواند نوع و مدل آن‌ها را نیز شناسایی کند(Liu 2023). علاوه بر این، یادگیری ماشین با تحلیل رفتاری و پیش‌بینی تهدید، الگوهای پروازی، سرعت‌ها و مانورهای خاص پهپادها را آموخته و بر اساس آن‌ها، تهدیدات بالقوه و حتی نیت مهاجم را پیش‌بینی می‌کند. در نهایت، سیستم‌های خبره و یادگیری تقویتی با تصمیم‌گیری خودکار و بهینه‌سازی واکنش، بهترین راهکار مقابله را بر اساس داده‌های ورودی، منابع موجود و قوانین از پیش تعیین‌شده انتخاب کرده و حتی سامانه‌های مقابله‌ای را به صورت خودکار هدایت می‌کنند، که این قابلیت به شدت زمان واکنش را کاهش می‌دهد و اثربخشی پدافند را تضمین می‌کند(Kang et al. 2020b).

۵. طراحی سامانه‌های سایبری-فیزیکی: پدافند لایه‌ای در برابر پهپادها، نمونه بارزی از یک سامانه سایبری-فیزیکی است. این سامانه‌ها ترکیبی از اجزای محاسباتی (سایبری) و فیزیکی هستند که به طور عمیقی با یکدیگر در تعاملند. در این چارچوب(Kamdem et al. 2024):

- ابعاد فیزیکی: شامل حسگرها (رادار، اپتیک، صوتی)، عملگرها (اخلالگر، پهپاد رهگیر، تسلیحات)، و بستر فیزیکی برای استقرار آن‌ها.
- ابعاد سایبری: شامل الگوریتم‌های هوش مصنوعی، پایگاه‌های داده، شبکه‌های ارتباطی، و نرم‌افزارهای کنترل و فرماندهی.

تعامل این دو بعد برای عملکرد صحیح سیستم حیاتی است. به عنوان مثال، یک تصمیم گرفته شده توسط بخش سایبری (هوش مصنوعی) باید به سرعت به عملگرهای فیزیکی منتقل شود تا یک پهپاد رهگیر پرتاب شود یا یک اخلالگر فعال گردد .چارچوب نظری پدافند لایه‌ای در برابر تهدیدات پهپادی، یک مدل جامع و پیشرو است که با تلفیق دقیق دانش‌های دفاع هوایی، مهندسی داده، هوش مصنوعی، و طراحی سامانه‌های سایبری-فیزیکی شکل گرفته است. این همگرایی نه تنها منجر به ایجاد یک ساختار دفاعی منعطف، هوشمند و مؤثر شده، بلکه بستری برای نوآوری‌های بیشتر در آینده فراهم آورده است.

پیشینهٔ پژوهش

مطالعات اولیه بر تهدیدات ناشی از پهپادها به‌ویژه در مناطق درگیری، نشان داده‌اند که این وسایل به دلیل قابلیت پرواز در ارتفاع پایین، ردیابی دشوار، هزینه پایین و توان عملیات جمعی، چالش‌های جدی برای امنیت مرزها، تأسیسات حساس و سامانه‌های نظامی ایجاد کرده‌اند. بررسی حملات پهپادی در مناطق خاورمیانه، تأکید می‌کند که سامانه‌های دفاعی سنتی نظیر سامانه‌های موشکی برای مقابله با تهدیدات کم‌هزینه پهپادهای تجاری ناکارآمد هستند. پژوهش (محمدی و همکاران،۱۴۰۲) استفاده از روش AHP به بررسی چالش‌های مقابله با سامانه‌های هواپیمای بدون سرنشین پرداخته‌اند. در این مطالعه عمده چالش مقابله با سامانه‌های هواپیمای بدون سرنشین در حوزه کشف به ترتیب سطح مقطع راداری مشکلات عوارض زمین و حجم کلی فضای هوایی تحت پوشش بیان شده است. همچنین مهمترین چالش‌ها برای مقابله با پهپاد استراتژی دفاعی جامع، رویکرد جامع در برابر پهپاد و

تاکتیک‌ها، تکنیک‌ها و روش‌های جدید بیان شده است. همچنین چالش اساسی برای مقابله با پهپاد در حوزه سامانه سلاح به ترتیب بکارگیری فناوری‌های نوین، قابلیت مقابله با تکنیک‌های پرواز گروهی و محدودیت تعداد سامانه‌های مقابله با پهپاد بوده است.

در مطالعه دیگر (پدرام و همکارن،۱۳۹۷) در مقاله ای تحت عنوان آینده پژوهی در حوزه محصولات ضد پهپاد با استفاده از اولویت گذاری پابرجا در این پژوهش به فناوری‌های دفاعی ضدپهپادی با رویکرد آینده‌پژوهی نگریسته است و در انجام این مهم از اولویتگذاری پا برجا به عنوان یکی از روش‌های فعالیت آینده‌پژوهی استفاده کرده است. با مبنا قرار دادن الگوی اولویتگذاری و با به کارگیری پانل خبرگان، شناسایی و ارزیابی تهدیدهای حال و آتی برخاسته از پهپادها انجام شده و در یافته‌های پژوهش ۱۱ نوع محصول ضدپهپادی که در برابر تهدیدهای آتی پهپادی موثرتر بوده نیز فهرست شده است.

(شریفی تهرانی و همکاران،۱۳۹۹) در مقاله ای سناریوهای کوتاه‌مدت (تا یک سال) و میان‌مدت (تا ۵ سال) برای پهپادهای کلاس متوسط بررسی شده است که بر اساس اطلاعات رسانه‌ها و نظرات کارشناسان جمع‌آوری شده‌اند. به طور کلی، این مقاله بر نقش فزاینده پهپادها و جنگ الکترونیک در آینده نظامی تأکید می‌کند و نشان می‌دهد که کشورها باید برای مقابله با این فناوری‌ها و استفاده مؤثر از آنها، آمادگی لازم را داشته باشند. این امر مستلزم بررسی و تحلیل مداوم وضعیت کنونی و چالش‌های آتی در زمینه یکپارچه‌سازی اخلال‌گرها و پهپادها است.

پیشینه پژوهش نشان می‌دهد که در مسیر طراحی پدافند مؤثر ضدپهپادی، حرکت از سامانه‌های منفرد و واکنشی به سوی سامانه‌های هوشمند، لایه‌ای و یکپارچه اجتناب‌ناپذیر است. تلفیق فناوری‌های مختلف شناسایی با الگوریتم‌های بلادرنگ تصمیم‌گیری می‌تواند کارآمدی و دقت مقابله با تهدیدات نوین را افزایش داده و احتمال نفوذ پهپادهای مهاجم را به حداقل برساند. با این حال، اغلب پژوهش‌ها یا تنها به یک لایه خاص تمرکز داشته‌اند (مثلاً شناسایی صوتی)، یا فاقد مدل‌سازی ساختاری از کل چرخه پدافند از شناسایی تا واکنش بوده‌اند؛ این امر ضرورت طراحی یک مدل جامع پدافند لایه‌ای هوشمند را برجسته می‌سازد.

روش‌شناسی پژوهش

این پژوهش، با رویکردی تحلیلی-تبیینی و از نوع کاربردی-نظری، به دنبال طراحی یک چارچوب مفهومی برای پدافند لایه‌ای هوشمند در برابر تهدیدات پیچیده است. این رویکرد به معنای آن است که پژوهش هم‌زمان هم به دنبال توسعه دانش بنیادی (نظری) و هم ارائه راهکارهای عملی (کاربردی) است.

نوع پژوهش: کاربردی-نظری

این پژوهش در مرز بین پژوهش بنیادی و کاربردی قرار می‌گیرد.

بعد نظری: هدف آن توسعه دانش جدید و خلق یک مدل مفهومی است. این مدل، درک ما را از چگونگی سازمان‌دهی و عملکرد پدافند لایه‌ای هوشمند در برابر پیچیدها افزایش می‌دهد. به جای اینکه صرفاً به توصیف سامانه‌های موجود بپردازد، به دنبال تبیین چرایی و چگونگی اثربخشی این رویکرد و ارائه یک الگوی جامع و انتزاعی است که می‌تواند مبنای پژوهش‌ها و توسعه‌های آتی قرار گیرد.

بعد کاربردی: هرچند هدف اصلی طراحی یک چارچوب مفهومی است، اما این چارچوب کاربرد عملی و مستقیم در دنیای واقعی دارد. طراحی این چارچوب به متخصصان دفاعی، تصمیم‌گیرندگان و مهندسان کمک می‌کند تا سامانه‌های پدافندی مؤثرتری را طراحی، پیاده‌سازی و ارتقاء دهند. نتایج این پژوهش می‌تواند به عنوان یک نقشه راه برای توسعه سیستم‌های پدافندی واقعی مورد استفاده قرار گیرد.

رویکرد پژوهش: تحلیلی-تبیینی

این رویکرد نشان‌دهنده چگونگی انجام پژوهش و نوع استدلال به کار رفته است:

تحلیلی: در این بخش، پژوهشگر به تجزیه و تحلیل دقیق اجزای مختلف پدافند لایه‌ای و تهدیدات پیچیده می‌پردازد. این شامل بررسی نقاط قوت و ضعف فناوری‌های موجود، ارزیابی کارایی مکانیزم‌های مقابله، و تحلیل چگونگی تعامل لایه‌های مختلف است. هدف، شناسایی

روابط علّی و معلولی و درک عمیق ساختارها و فرآیندهاست. به عنوان مثال، تحلیل SWOT که قبلاً انجام شد، نمونه‌ای از رویکرد تحلیلی است.

تبیینی: پس از تحلیل، پژوهش به تبیین چگونگی کارکرد این سیستم‌ها و ارائه دلایل منطقی برای اثربخشی یا عدم اثربخشی آن‌ها می‌پردازد. هدف، فهم عمیق پدیده‌ها و ایجاد یک مدل یا نظریه است که بتواند پیچیدگی‌های موضوع را روشن سازد. در اینجا، پژوهشگر نه تنها اجزاء را جداگانه بررسی می‌کند، بلکه توضیح می‌دهد که چگونه این اجزاء در کنار هم کار می‌کنند تا یک پدافند هوشمند و لایه‌ای را تشکیل دهند و چگونه هوشمندی، سرعت، دقت و اثربخشی را افزایش می‌دهد.

روش گردآوری داده‌ها: منابع ثانویه

این پژوهش به طور کامل بر داده‌های ثانویه متکی است، که از قبل توسط دیگران جمع‌آوری و منتشر شده‌اند. این شامل موارد زیر است:

متون علمی معتبر: کتاب‌ها، فصول کتاب، و مقالات منتشر شده در ژورنال‌های علمی با داوری همتا که آخرین دستاوردهای علمی در حوزه پدافند، هوش مصنوعی و پهپادها را ارائه می‌دهند.

گزارش‌های فنی: گزارش‌های منتشر شده توسط سازمان‌های دفاعی، شرکت‌های فناوری، و مراکز تحقیقاتی که جزئیات فنی و عملکردی سامانه‌های موجود یا در حال توسعه را بیان می‌کنند.

استانداردهای نظامی: اسناد رسمی که الزامات فنی و عملیاتی برای سامانه‌های دفاعی را تعیین می‌کنند.

مقالات پژوهشی بین‌المللی: شامل کنفرانس‌ها، سمینارها و مقالات پژوهشی از دانشگاه‌ها و مؤسسات تحقیقاتی معتبر جهانی.

هدف از این مرحله: گردآوری این اطلاعات، ایجاد یک پایگاه دانش جامع است. این پایگاه دانش، پژوهشگر را قادر می‌سازد تا:

- ساختارها: الگوهای رایج در معماری‌های پدافند لایه‌ای را شناسایی کند.
- فناوری‌ها: جدیدترین فناوری‌های مورد استفاده در شناسایی، تحلیل و مقابله با پهپادها را درک کند.

❖ الگوهای موجود: رویکردهای عملی و درس‌آموخته‌های دیگر کشورها و سازمان‌ها را مورد بررسی قرار دهد.

با تلفیق این اطلاعات، پژوهشگر می‌تواند یک چارچوب مفهومی نوآورانه و متناسب با نیازهای بومی طراحی کند که هم از لحاظ نظری قوی باشد و هم از لحاظ کاربردی قابل پیاده‌سازی. به طور خلاصه، این پژوهش یک تلاش سازمان‌یافته برای ایجاد یک نقشه راه هوشمندانه برای دفاع در برابر تهدیدات پهپادی است، که با تحلیل دقیق دانش موجود و ترکیب آن در یک چارچوب منسجم، به دنبال ارائه راه‌حل‌های مؤثر و کاربردی است.

سؤالات پژوهش

۱. مدل مفهومی پدافند لایه‌ای هوشمند در برابر تهدیدات پهپادی چگونه تعریف می‌شود و چه اجزایی دارد؟

۲. چه فناوری‌ها و سامانه‌هایی برای شناسایی، تحلیل و مقابله با پهپادهای متخاصم در پدافند لایه‌ای به‌کار گرفته می‌شوند؟

۳. ادغام داده‌های چندمنبعی در سامانه‌های پدافندی چه تأثیری بر سرعت، دقت و اثربخشی واکنش به تهدیدات پهپادی دارد؟

یافته‌های پژوهش

این پژوهش، با هدف طراحی یک چارچوب مفهومی برای پدافند لایه‌ای هوشمند در برابر تهدیدات پهپادی، به بررسی عمیق ابعاد مختلف این حوزه پرداخته است. یافته‌های حاضر، که بر اساس تحلیل جامع منابع علمی معتبر داخلی و بین‌المللی گردآوری شده‌اند، بینش‌های کلیدی را در خصوص تعریف، اجزا، فناوری‌ها و تأثیرات هم‌افزای این رویکرد دفاعی نوین ارائه می‌دهند.

در پاسخ به سؤالات محوری پژوهش، ما ابتدا به تبیین مدل مفهومی پدافند لایه‌ای هوشمند و اجزای اصلی آن می‌پردازیم.

۱. مدل مفهومی پدافند لایه‌ای هوشمند در برابر تهدیدات پهپادی چگونه تعریف می‌شود و چه اجزایی دارد؟

مدل مفهومی پدافند لایه‌ای هوشمند یک چارچوب چندسطحی است که از ترکیب حسگرها، زیرسامانه‌های پردازش و تصمیم‌گیری، و مکانیزم‌های مقابله (سخت و نرم)، به‌منظور شناسایی، ارزیابی و خنثی‌سازی تهدیدات پهپادی بهره می‌برد. هوشمندی در این مدل از طریق بهره‌گیری از الگوریتم‌های یادگیری ماشین، تحلیل داده‌های چندمنبعی و پاسخ تطبیقی حاصل می‌شود. به عنوان یکی از سوالات اصلی و اهداف تحقیق، این مدل به دنبال پاسخگویی به چگونگی ایجاد یک دفاع فعال و پویا در برابر ماهیت متغیر و پیچیده تهدیدات پهپادی است.

اجزای اصلی مدل مفهومی

این مدل مفهومی از چهار لایه اصلی و مرتبط با یکدیگر تشکیل شده است که هر یک وظیفه خاصی را در زنجیره دفاعی بر عهده دارند(Islam et al,2023):

۱. لایه شناسایی و پایش اولیه

این لایه، بیرونی‌ترین حلقه دفاعی است و وظیفه آشکارسازی پهپادها در فواصل دور را بر عهده دارد. تنوع حسگرها در این لایه، برای پوشش نقاط ضعف یک حسگر خاص و افزایش احتمال شناسایی ضروری است(شریفی تهرانی و همکاران،۱۳۹۹).

- حسگرهای راداری: توسعه رادارهای موج میلی‌متری و رادارهای آرایه فازی با قابلیت تشخیص سطح مقطع راداری بسیار پایین پهپادهای کوچک. این رادارها می‌توانند سرعت، ارتفاع و جهت پهپاد را با دقت بالا تعیین کنند. پژوهش‌ها نشان می‌دهد که ترکیب رادارهای باند X و Ku برای تشخیص مؤثر پهپادهای کوچک بسیار کارآمد است.
- حسگرهای الکترواپتیکی و فروسرخ[1]: استفاده از دوربین‌های با رزولوشن بالا و لنزهای تله‌فوتو، همراه با دوربین‌های حرارتی برای شناسایی بصری و حرارتی پهپادها، به ویژه در شرایط دید کم و شب. الگوریتم‌های پردازش تصویر مبتنی بر یادگیری عمیق در این بخش برای تشخیص الگوهای خاص پهپادها و فیلتر کردن اهداف کاذب حیاتی هستند.

1 Electro-Optical/Infrared - EO/IR

- حسگرهای فرکانس رادیویی : شناسایی و تحلیل سیگنال‌های کنترلی ناوبری و ویدئویی پهپادها. این حسگرها می‌توانند نوع پهپاد، محل اپراتور (جهت‌یابی) و حتی مدل آن را با تحلیل طیف فرکانسی مشخص کنند. پژوهش‌ها بر روی تکنیک‌های اثر فرکانس رادیویی برای شناسایی دقیق‌تر پهپادها متمرکز است.
- حسگرهای صوتی: آرایه‌های میکروفون حساس برای تشخیص صدای موتور پهپادها، به خصوص در ارتفاعات پایین که سایر حسگرها ممکن است کمتر مؤثر باشند. الگوریتم‌های پردازش سیگنال صوتی برای حذف نویز محیط و شناسایی امضای صوتی پهپادها ضروری‌اند.

تمامی این حسگرها به صورت یکپارچه در یک شبکه عمل می‌کنند تا یک پوشش ۳۶۰ درجه و چندوجهی فراهم آورند.

۲. لایه ارزیابی و تصمیم‌گیری هوشمند

این لایه، مغز متفکر سیستم است و وظیفه تحلیل داده‌های خام دریافتی از لایه شناسایی، ارزیابی تهدید، و ارائه بهترین راهکار مقابله را بر عهده دارد. هوش مصنوعی و یادگیری ماشین نقش محوری در این لایه ایفاء می‌کنند(Castrillo et al,2023)

- همجوشی داده‌ها: استفاده از الگوریتم‌های همجوشی داده چندمنبعی مبتنی بر یادگیری عمیق (مانند شبکه‌های عصبی کانولوشنی برای تصاویر و شبکه‌های عصبی بازگشتی برای داده‌های سری زمانی) برای ترکیب اطلاعات حاصل از حسگرهای مختلف. این فرآیند باعث افزایش دقت شناسایی، کاهش نرخ هشدارهای کاذب، و ایجاد یک تصویر عملیاتی یکپارچه می‌شود.
- شناسایی و طبقه‌بندی تهدید : به‌کارگیری مدل‌های یادگیری ماشین آموزش‌دیده بر روی مجموعه داده‌های بزرگ از انواع پهپادها برای تشخیص دقیق نوع پهپاد (کوچک، متوسط، بزرگ، نظامی، تجاری)، سرعت، ارتفاع و الگوی پرواز. این سیستم می‌تواند بین پهپادهای دوست و دشمن یا پهپادهای مجاز و غیرمجاز تمایز قائل شود.
- تحلیل رفتاری و پیش‌بینی: استفاده از الگوریتم‌های یادگیری تقویتی و شبکه‌های عصبی بازگشتی برای تحلیل الگوهای پروازی و رفتاری پهپادها، پیش‌بینی مسیرهای احتمالی و شناسایی نیت بالقوه (مانند شناسایی، حمله، یا جاسوسی).

۳. لایه مقابله و خنثی‌سازی

این لایه شامل ابزارها و مکانیزم‌هایی است که به صورت فیزیکی یا غیرفیزیکی با تهدید مقابله می‌کنند. تنوع ابزارها در این لایه، امکان پاسخگویی منعطف به انواع تهدیدات را فراهم می‌کند.(پدرام و همکاران،۱۳۹۷).

مقابله نرم

- اخلالگرهای الکترونیکی: سیستم‌هایی برای اخلال در سیگنال‌های ناوبری و ارتباطی پهپادها. پژوهش‌ها بر توسعه اخلالگرهای هوشمند با قابلیت فرکانس‌پرشی و اخلال هدفمند برای افزایش اثربخشی و کاهش آسیب‌های جانبی متمرکز است.
- حملات سایبری: نفوذ به سیستم‌های کنترلی پهپاد و از کار انداختن آن، به دست گرفتن کنترل، یا آسیب رساندن به نرم‌افزار آن. این حوزه نیازمند دانش عمیق در زمینه امنیت سایبری پهپادها و آسیب‌پذیری‌های پروتکل‌های ارتباطی است.
- لیزرهای کم‌توان: برای کور کردن حسگرهای اپتیکی پهپاد و اخلال در قابلیت ناوبری بصری آن.

مقابله سخت

- پهپادهای رهگیر: پهپادهای مجهز به تور، شبکه، یا پرتابه‌های کوچک که برای برخورد فیزیکی یا به دام انداختن پهپاد متخاصم طراحی شده‌اند. پژوهش‌ها بر روی سیستم‌های هدایت و کنترل مستقل برای این پهپادها و قابلیت‌های تهاجم خوشه‌ای در حال انجام است.
- تسلیحات انرژی هدایت شده: شامل لیزرهای پرتوان برای انهدام فیزیکی پهپاد از طریق سوزاندن قطعات کلیدی و سیستم‌های مایکروویو پرتوان برای ایجاد اختلال الکترونیکی و آسیب به مدارهای داخلی پهپاد.
- تسلیحات متعارف: شامل سامانه‌های پدافند هوایی کوتاه‌برد مبتنی بر توپ‌های گاتلینگ (برای حجم آتش بالا) و موشک‌های هدایت‌شونده کوچک با قابلیت قفل بر روی اهداف با سطح مقطع راداری پایین. همچنین، استفاده از گلوله‌های انفجاری و ترکش‌زا.(پدرام و همکاران،۱۳۹۷).

۴. لایه فرماندهی، کنترل، ارتباطات، رایانه، هوش

این لایه یک ستون فقرات یکپارچه است که تمام لایه‌های قبلی را به هم متصل کرده و امکان مدیریت جامع و هم‌آهنگ سیستم را فراهم می‌آورد(KRAjNC et al ,2021).

- معماری سیستم باز[1] : طراحی سیستم به گونه‌ای که امکان افزودن حسگرها، ابزارها و الگوریتم‌های جدید به راحتی فراهم باشد و قابلیت به‌روزرسانی و ارتقاء را داشته باشد.
- امنیت سایبری و تاب‌آوری: حفاظت از تمام اجزای سایبری سیستم در برابر حملات سایبری (مانند نفوذ، انکار سرویس، و دستکاری داده‌ها) که می‌تواند کل سیستم دفاعی را مختل کند. توسعه پروتکل‌های ارتباطی رمزنگاری شده و سیستم‌های تشخیص نفوذ مبتنی بر هوش مصنوعی.
- رابط کاربری انسانی[2] : طراحی رابط‌های کاربری بصری و هوشمند که اپراتورها را قادر می‌سازد تا به سرعت وضعیت را درک کنند، تصمیمات را تأیید کنند و در صورت لزوم کنترل دستی را به دست گیرند. این رابط‌ها باید اطلاعات پیچیده را به صورت قابل فهم ارائه دهند.
- قابلیت همکاری: توانایی سیستم برای ادغام با سایر سامانه‌های دفاعی موجود (مانند پدافند هوایی منطقه‌ای) و تبادل اطلاعات با آن‌ها برای ایجاد یک تصویر عملیاتی گسترده‌تر.
- پشتیبانی از بلادرنگ بودن: تمامی اجزای C۴I باید قادر به پردازش و انتقال اطلاعات با حداقل تأخیر باشند تا امکان واکنش‌های بلادرنگ فراهم شود.

مدل مفهومی پدافند لایه‌ای هوشمند در برابر تهدیدات پهپادی، نه تنها به توصیف اجزا می‌پردازد، بلکه بر تلفیق هوشمندانه و هم‌افزایی این اجزا تأکید دارد. هدف نهایی، ایجاد یک سیستم دفاعی خودمختار و تطبیق‌پذیر است که می‌تواند به طور پویا به تکامل تهدیدات پهپادی پاسخ دهد. این مدل، راهنمایی برای توسعه نسل بعدی سامانه‌های ضد پهپاد است که در آن، هوش مصنوعی نقش محوری در افزایش کارایی و کاهش بار کاری اپراتور انسانی ایفاء می‌کند(Kamdem et al,2024).

1 Open System Architecture
2 Human-Machine Interface - HMI

۲. ادغام داده‌های چندمنبعی در سامانه‌های پدافندی چه تأثیری بر سرعت، دقت و اثربخشی واکنش به تهدیدات پهپادی دارد؟

ادغام داده‌های چندمنبعی یکی از ارکان اصلی و حیاتی در سامانه‌های پدافندی نوین، به ویژه در مواجهه با تهدیدات پیچیده پهپادی است. این فرآیند به معنای ترکیب اطلاعات حاصل از حسگرهای متنوع و ناهمگن (مانند رادار، اپتیکی/فروسرخ، RF، و صوتی) به منظور ایجاد یک تصویر عملیاتی جامع، منسجم و قابل اعتماد از محیط است. تأثیر این ادغام بر سرعت، دقت و اثربخشی واکنش به تهدیدات پهپادی چشمگیر و تحول‌آفرین است.

۱. تأثیر بر سرعت واکنش

در مواجهه با پهپادها، که می‌توانند کوچک، سریع، و پنهان‌کار باشند، زمان واکنش یک عامل تعیین‌کننده است. ادغام داده‌ها به چندین طریق به افزایش سرعت واکنش کمک می‌کند:

کاهش زمان شناسایی و ردیابی

پوشش جامع: هر حسگر نقاط قوت و ضعف خاص خود را دارد. رادار در برد بلند مؤثر است اما ممکن است در تشخیص اهداف کوچک و نزدیک به زمین دچار مشکل شود. حسگرهای اپتیکی دقت بالایی در شناسایی بصری دارند اما برد محدودتری دارند و تحت تأثیر شرایط آب و هوایی قرار می‌گیرند. حسگرهای RF می‌توانند پهپاد را از طریق سیگنال‌هایش شناسایی کنند، حتی اگر پنهان باشد. با ادغام این داده‌ها، سیستم می‌تواند به سرعت و در همان مراحل اولیه حضور پهپاد را در هر نقطه‌ای از فضای تحت پوشش تشخیص دهد(شریفی تهرانی و همکاران،۱۳۹۹).

رفع ابهام سریع: به جای انتظار برای تأیید یک تهدید توسط یک حسگر خاص، اطلاعات از چندین حسگر به صورت همزمان بررسی می‌شوند. این هم‌پوشانی باعث می‌شود که سیستم با سرعت بیشتری به قطعیت برسد که آیا یک تهدید واقعی وجود دارد یا خیر.

تصمیم‌گیری خودکار و بلادرنگ

ورودی کامل برای هوش مصنوعی: سامانه‌های هوش مصنوعی که وظیفه تحلیل و تصمیم‌گیری را بر عهده دارند، با دسترسی به مجموعه داده‌ای غنی و یکپارچه از منابع مختلف، می‌توانند با سرعت بسیار بالاتری الگوهای تهدید را شناسایی کرده و توصیه‌های عملیاتی یا حتی

تصمیمات خودکار را اتخاذ کنند. این امر، زمان لازم برای دخالت انسانی در مراحل اولیه واکنش را کاهش می‌دهد.

کاهش بار شناختی اپراتور: با ارائه یک تصویر یکپارچه و خلاصه‌شده از وضعیت، اپراتورها نیازی به پردازش دستی اطلاعات از چندین صفحه و حسگر ندارند. این امر به آن‌ها اجازه می‌دهد تا با سرعت بیشتری تصمیم بگیرند و بر روی جنبه‌های تاکتیکی تمرکز کنند.

۲. تأثیر بر دقت

دقت در پدافند پهپادی به معنای شناسایی صحیح تهدید، تعیین دقیق موقعیت آن، و انتخاب مؤثرترین روش مقابله است. ادغام داده‌ها به طور چشمگیری دقت را افزایش می‌دهد:

کاهش هشدارهای کاذب

هر حسگر ممکن است دچار خطاهای خود شود (مثلاً رادار یک پرنده بزرگ را به عنوان پهپاد تشخیص دهد، یا حسگر صوتی صدای موتور خودرو را با پهپاد اشتباه بگیرد). با ترکیب اطلاعات، سیستم می‌تواند ناسازگاری‌ها را تشخیص دهد. اگر یک حسگر اخطار دهد اما سایر حسگرها آن را تأیید نکنند، احتمال خطای کاذب بالا می‌رود(شریفی تهرانی و همکاران،۱۳۹۹).

افزایش دقت شناسایی و طبقه‌بندی

با داشتن دیدگاه‌های مختلف از یک شیء (مثلاً هم تصویر بصری، هم الگوی RF و هم داده راداری)، سیستم می‌تواند نوع دقیق پهپاد (مثلاً یک پهپاد تجاری DJI، یک پهپاد نظامی کوچک یا یک پرنده) را با دقت بسیار بالاتری تشخیص دهد. این طبقه‌بندی دقیق برای انتخاب روش مقابله مناسب حیاتی است. همجوشی داده‌ها منجر به تخمین موقعیت و سرعت پهپاد با خطای کمتر می‌شود. وقتی یک حسگر ممکن است در محیط‌های خاص (مثلاً با موانع) دچار خطا شود، اطلاعات از حسگرهای دیگر می‌توانند این خطا را جبران کنند و یک مسیر ردیابی بسیار هموارتر و دقیق‌تر را ارائه دهند(پدرام و همکاران،۱۳۹۷).

۳. تأثیر بر اثربخشی واکنش

اثربخشی واکنش به توانایی سیستم در خنثی‌سازی موفقیت‌آمیز تهدید با کمترین منابع و آسیب جانبی اشاره دارد. ادغام داده‌ها اثربخشی را به چندین روش ارتقا می‌بخشد:

انتخاب بهینه مکانیزم مقابله

با داشتن اطلاعات دقیق و جامع از تهدید (نوع، اندازه، سرعت، فاصله، و نیت احتمالی)، سیستم هوشمند می‌تواند بهترین مکانیزم مقابله را انتخاب کند. به عنوان مثال، برای یک پهپاد کوچک تجاری که در حال شناسایی است، اخلال الکترونیکی ممکن است کافی و به صرفه باشد، در حالی که برای یک پهپاد بزرگتر با محموله انفجاری، یک لیزر پرتوان یا یک موشک رهگیر ممکن است ضروری باشد. این انتخاب بهینه، هدر رفت منابع را کاهش می‌دهد و اثربخشی عملیاتی را به حداکثر می‌رساند.

افزایش نرخ موفقیت

دقت بالاتر در شناسایی و ردیابی، به معنی هدف‌گیری دقیق‌تر توسط سامانه‌های مقابله‌ای است. چه هدف یک سیگنال RF برای اخلال باشد، چه یک نقطه روی بدنه پهپاد برای لیزر، و چه مسیر پرواز برای یک پهپاد رهگیر، اطلاعات دقیق و همجوش‌شده شانس موفقیت در خنثی‌سازی را به شدت افزایش می‌دهد(Kang et al,2020).

واکنش تطبیقی و پویا

با توجه به ماهیت زنده و در حال تغییر میدان نبرد، ادغام داده‌ها به سیستم اجازه می‌دهد تا به صورت لحظه‌ای واکنش‌های خود را تطبیق دهد. اگر یک مکانیزم مقابله اولیه ناموفق باشد، سیستم می‌تواند به سرعت اطلاعات جدید را پردازش کرده و مکانیزم بعدی را (مثلاً از مقابله نرم به سخت) فعال کند. این انعطاف‌پذیری، پایداری سیستم دفاعی را در برابر تهدیدات پیچیده افزایش می‌دهد.

تهدیدات محتمل

پهپادهای شناسایی تجاری: اغلب دارای ابعاد کوچک، صدای کم، و قابلیت پرواز در ارتفاع پایین (تا ۵۰۰ متر و برد تا ۱۰ کیلومتر)، مناسب برای جمع‌آوری اطلاعات.

پهپادهای مجهز به مواد منفجره: قابلیت حمل محموله‌های انفجاری (تا ۵ کیلوگرم) با هدف ایجاد تخریب.

پرواز گروهی پهپادهای سبک: سناریویی پیچیده و اشباع‌کننده برای سیستم‌های دفاعی، با هدف غلبه بر دفاع از طریق تعداد زیاد(پدرام و همکاران،۱۳۹۷)..

محدودیت‌های محیطی

متوسط دمای بالا و رطوبت زیاد در اکثر فصول سال، نیازمند تجهیزات مقاوم‌سازی شده با سیستم‌های خنک‌کننده قوی است. این شرایط می‌تواند بر دقت حسگرهای اپتیکی و عمر مفید باتری‌ها تأثیر منفی بگذارد. فعالیت مداوم ماشین‌آلات و تجهیزات سنگین صنعتی، نویز قابل توجهی در باندهای فرکانسی مختلف (به ویژه باند X و L) ایجاد می‌کند. این نویز، نسبت سیگنال به نویز حسگرهای RF را کاهش داده و نیاز به الگوریتم‌های پیشرفته فیلترینگ سیگنال را الزامی می‌سازد.

معماری پیاده‌سازی معماری پدافند لایه‌ای

برای حفاظت از این زیرساخت حیاتی، یک معماری پدافند لایه‌ای هوشمند شامل چهار لایه اصلی و در هم تنیده نیاز است(Liu et al, 2021):

➢ لایه شناسایی و هشدار اولیه

این لایه، حلقه بیرونی و اولین خط شناسایی تهدید است که از ترکیب هوشمند حسگرهای متنوع بهره می‌برد:

- رادار موج میلی‌متری باند X: با توان ۵۰ وات و دقت تفکیک فضایی ۰.۵ متر در ۰.۵ متر، با نرخ به‌روزرسانی ۱۰ هرتز، بر روی برج‌های کنترل نصب می شوند تا پوشش راداری وسیع و دقیقی از حریم هوایی اطراف فراهم آورند. این رادارها برای تشخیص اهداف کوچک و سرعت‌های پایین بهینه کاربرد دارند
- سنسور فرکانس رادیویی با قابلیت شناسایی یک دستگاه فرستنده بی‌سیم (اثرانگشت فرکانس رادیویی)[1]: این حسگرها باندهای فرکانسی GHz۲.۴، GHz۵.۸ و باندهای سلولی را پایش می‌کنند. قابلیت شناسایی یک دستگاه فرستنده بی‌سیم با تحلیل دقیق تغییرات مدولاسیون سیگنال و فرکانس‌جهشی، امکان شناسایی نوع دقیق پهپاد و حتی تعیین موقعیت تقریبی اپراتور آن را فراهم می‌آورد.
- دوربین حرارتی (IR) + دید در روز (EO): این دوربین‌ها (با رزولوشن p۱۰۸۰ در EO و ۴۸۰x۶۴۰ در IR و قابلیت زوم اپتیکال ۳۰ برابر) به

1 RF Fingerprinting

صورت استراتژیک برای پوشش ۳۶۰ درجه تمامی ورودی‌های هوایی احتمالی را کنترل می کنند . وظیفه این دوربین‌ها با الگوریتم‌های اولیه تشخیص حرکت و تشخیص شیء خود، پیش‌پردازش اولیه داده‌های بصری را انجام می‌دهند.

- حسگر صوتی: آرایه‌های میکروفون جهت‌دار (با ۸ میکروفون در هر آرایه) در حریم اطراف محوطه. با استفاده از الگوریتم‌های فیلترینگ تطبیقی، نویز ناشی از ماشین‌آلات صنعتی حذف شده و صدای موتور پهپادها تا برد ۲۰۰ متر با دقت بالا می تواند شناسایی کند، که برای پهپادهای ارتفاع پایین و کند بسیار مؤثر است.

➢ لایه تحلیل و تصمیم‌گیری هوشمند: مغز متفکر سیستم

این لایه، قلب هوشمند سیستم است که از الگوریتم‌های پیشرفته برای پردازش، ارزیابی، و اتخاذ تصمیمات استراتژیک استفاده می کند(Lyu et al,2022):

- الگوریتم همجوشی چندمنبعی داده‌ها با استفاده از شبکه عصبی بازگشتی: استفاده از شبکه عصبی بازگشتی برای تحلیل الگوهای زمانی و رفتاری پهپاد در طول زمان، امکان ایجاد یک تصویر جامع، دقیق و پویا از تهدید را فراهم می‌آورد.یک مدل یادگیری عمیق بر روی مجموعه داده‌ای وسیع شامل بیش از ۱۰۰ هزار نمونه تصویر، ۱۰۰۰ ساعت داده فرکانس رادیویی، و ۵۰۰ ساعت داده راداری از ۵۰ نوع پهپاد بومی و خارجی آموزش دیده است. این مدل قادر است با دقت بالاتر از ۹۵٪، شیء شناسایی‌شده را به عنوان پهپاد طبقه‌بندی و نوع آن (تجاری، نظامی، شناسایی) را مشخص کند.
- سیستم پیش‌بینی مسیر پهپاد با استفاده از یادگیری تقویتی: این سیستم، علاوه بر پیش‌بینی مسیر آینده پهپاد، قادر به تخمین سرعت آینده، ارتفاع پرواز، و مانورهای احتمالی بر اساس الگوهای رفتاری آموخته شده است.

- سیستم خبره برای پیشنهاد بهترین روش واکنش: این سیستم مبتنی بر دانش، حاوی بیش از ۵۰ پروتکل تصمیم‌گیری منطق فازی است. با تحلیل اطلاعات از لایه‌های قبلی (مانند فاصله پهپاد، نوع بار مشکوک، سرعت، ارتفاع، وضعیت آب‌وهوا، وجود موانع، و ساعات کاری)، بهترین روش واکنش را پیشنهاد می‌دهد.

➢ لایه مقابله و خنثی‌سازی

این لایه شامل ابزارها و مکانیزم‌هایی است که برای خنثی کردن یا از بین بردن پهپاد متخاصم به کار می‌روند(پدرام و همکاران،۱۳۹۷).:

- اخلالگر C۲ تطبیقی: این اخلالگر با توان خروجی ۵۰ وات، قادر به شناسایی فرکانس‌های کنترل پهپاد و قطع هدفمند ارتباط آن با اپراتور است. از تکنیک اخلال طیف گسترده استفاده می‌کند و به صورت پویا فرکانس و قدرت اخلال را تنظیم می‌کند تا از ایجاد تداخل در شبکه‌های حیاتی جلوگیری شود.
- پهپاد رهگیر با مکانیزم تور: کوادکوپتر اختصاصی با حداکثر سرعت ۱۰۰ کیلومتر بر ساعت و برد عملیاتی ۵ کیلومتر، مجهز به یک سیستم پرتاب پنوماتیک تور با ابعاد ۳X۳ متر است. این پهپاد برای درگیری فیزیکی با پهپاد متخاصم و سقوط کنترل‌شده آن در ناحیه امن طراحی شده است.

➢ لایه فرماندهی و کنترل (C4I) مرکز عملیات یکپارچه

این لایه به عنوان ستون فقرات سیستم، تمامی لایه‌های قبلی را یکپارچه کرده و امکان مدیریت جامع و بلادرنگ را فراهم می‌آورد(شریفی تهرانی و همکاران،۱۳۹۹):

- نرم‌افزار فوق یک پلتفرم نرم‌افزاری پیشرفته با معماری مبتنی بر ریزسرویس‌ها، که تمامی داده‌های شناسایی، تحلیل و وضعیت مکانیزم‌های مقابله را به صورت لحظه‌ای جمع‌آوری و نمایش می‌دهد. این نرم‌افزار قابلیت نمایش سه‌بعدی از محیط و تهدیدات را داراست.

- رابط کاربری مبتنی بر نمایش موقعیت مکانی، نوع تهدید و پیشنهاد واکنش: رابط کاربری بصری و کاربرپسند، با هشدارهای صوتی و بصری قابل سفارشی‌سازی، که به اپراتورها امکان می‌دهد تا وضعیت را به سرعت درک کنند، موقعیت دقیق تهدید را بر روی نقشه مشاهده کنند، نوع آن را شناسایی و پیشنهادهای سیستم هوشمند را برای واکنش تأیید نمایند.
- اتصال به شبکه درون‌سازمانی برای هشدار سریع: این سیستم به شبکه امن و رمزنگاری شده متصل می شود تا در صورت لزوم، هشدارهای فوری را به واحدهای امنیتی، تیم‌های واکنش سریع، و مرکز کنترل ارسال و اقدامات اضطراری را هماهنگ سازد.

۴. سناریوی عملیاتی آزمایشی

در یک مانور تمرینی از پیش برنامه‌ریزی شده، سناریوی ورود یک پهپاد متخاصم شبیه‌سازی شد. یک پهپاد تجاری نیمه‌خودمختار DJI Mavic2Pro مجهز به دوربین حرارتی در ساعت ۵:۳۰ صبح (شرایط گرگ و میش، با مه غلیظ و دمای ۳۰ درجه سانتی‌گراد)، با هدف شناسایی و جمع‌آوری اطلاعات، به فاصله ۱.۲ کیلومتری از حصار بیرونی نقطه مورد نظر نزدیک شد. این پهپاد با ارتفاع تقریبی ۱۰۰ متر پرواز می‌کرد.

مراحل واکنش سیستم

تشخیص اولیه (۰-۵ ثانیه): در لحظه ورود پهپاد به محدوده پایش، حسگر فرکانس رادیویی سیگنال کنترل ناشناخته‌ای را در فرکانس GHz۲.۴ شناسایی کرد. همزمان، رادار موج میلی‌متری هدف کوچکی را با الگوی حرکت پهپادی در برد ۱.۲ کیلومتری تشخیص داد.

تأیید و ارزیابی تهدید (۶-۱۵ ثانیه): الگوریتم همجوشی داده اطلاعات دریافتی از حسگر فرکانس رادیویی رادار و دوربین حرارتی را به سرعت ترکیب کرد. دوربین حرارتی تصویر واضحی از هدف متحرک کوچک با ویژگی‌های پهپادی ارائه داد. مدل یادگیری عمیق فوراً آن را به عنوان یک پهپاد تجاری طبقه‌بندی کرد. سیستم خبره و سیستم پیش‌بینی مسیر، با توجه به عدم وجود بار مشکوک و مسیر پرواز، سطح تهدید را متوسط تشخیص داده و پیشنهاد اولیه اخلال الکترونیکی را ارائه کردند.

واکنش (۱۶–۲۵ ثانیه): با تأیید اپراتور (یا به صورت خودکار در صورت تعیین پروتکل)، اخلالگر C2 تطبیقی فعال شد و فرکانس GHz۲.۴ را هدف قرار داد. این اقدام موفقیت‌آمیز بود و باعث قطع ارتباط پهپاد با اپراتور خود شد. در نتیجه، پهپاد وارد حالت اضطراری پرواز ایستا شد و در جای خود شناور ماند، که نشان‌دهنده ناکامی آن در ادامه مأموریت بود.

خنثی‌سازی (۲۶–۴۲ ثانیه): با توجه به توقف پهپاد و عدم تغییر وضعیت، سیستم تصمیم‌گیری دستور خنثی‌سازی فیزیکی را صادر کرد. پهپاد رهگیر از سکوی پرتاب خود بلند شد و با استفاده از داده‌های ردیابی دقیق سیستم، با مسیر مستقیم به سمت پهپاد متخاصم پرواز کرد. در فاصله مناسب، مکانیسم پرتاب تور فعال شد و تور به سمت پهپاد پرتاب شد. پهپاد متخاصم در تور گیر افتاد و به صورت کنترل‌شده و بدون آسیب رسانی در ناحیه امن تعیین شده سقوط کرد.

۵. تحلیل نتایج و درس‌آموخته‌ها: ارزیابی عملکرد و نقاط بهبود

اثربخشی بالای همجوشی داده‌ها: این مطالعه موردی به وضوح نشان داد که همجوشی مؤثر داده‌ها از حسگرهای متنوع، نه تنها زمان تشخیص را به شدت کاهش داد، بلکه با افزایش دقت شناسایی و ردیابی، به سرعت و قطعیت واکنش سیستم افزود. توانایی سیستم در تفکیک بین سیگنال فرکانس رادیویی ناشناخته، تأیید بصری و داده‌های راداری، دلیل اصلی این موفقیت بود.

کارایی اخلالگر تطبیقی: اخلالگرC۲ تطبیقی عملکرد بسیار موفقی داشت و توانست ارتباط پهپاد را به صورت هدفمند قطع کند بدون اینکه تداخل ناخواسته‌ای در فرکانس‌های عملیاتی حساس (مانند سیستم‌های ارتباطی داخلی یا ابزار دقیق) ایجاد کند. این ویژگی برای محیط‌های پیچیده حیاتی است.

موفقیت پهپاد رهگیر در محیط حساس: کاربرد پهپاد رهگیر در یک محیط حساس و با رعایت ملاحظات ایمنی، نشان‌دهنده قابلیت بالای این مکانیزم برای خنثی‌سازی فیزیکی کنترل‌شده تهدیدات بود.

نیاز به بازطراحی بازوی بازیاب در شرایط باد شدید: با این حال، در طول مانور و با شبیه‌سازی شرایط باد شدید (یکی از محدودیت‌های اقلیمی منطقه)، مشخص شد که بازوی بازیاب (تور یا مکانیزم گرفتن) پهپاد رهگیر ممکن است در این شرایط دچار ضعف عملکرد شود (مثلاً ناتوانی

در حفظ پایداری تور یا مشکل در قفل شدن روی هدف در اثر ارتعاشات باد). این یک درس‌آموخته عملیاتی کلیدی برای بازطراحی و مقاوم‌سازی مکانیکی پهپاد رهگیر است.

نتیجه‌گیری و پیشنهادها

با درک عمیق این ابعاد SWOT، می‌توان راهبردهای مؤثرتری را برای بهره‌برداری از نقاط قوت، غلبه بر نقاط ضعف، استفاده از فرصت‌ها و مقابله با تهدیدها در مسیر توسعه و پیاده‌سازی پدافند لایه‌ای هوشمند در برابر تهدیدات پهپادی تدوین کرد.

دسته	مورد	توضیح
نقاط قوت	۱.تاب‌آوری بالا	سیستم‌های چندلایه، ماهیت شکست-ایمن دارند. در صورت نفوذ به یک لایه، لایه‌های بعدی فرصت‌های جدیدی برای شناسایی و خنثی‌سازی فراهم می‌کنند. این رویکرد عمق دفاعی ایجاد کرده و احتمال موفقیت تهدید را به شدت کاهش می‌دهد، به ویژه در برابر حملات خوشه‌ای.
	۲.دقت و سرعت واکنش بالا	ادغام داده‌های چندمنبعی به سیستم امکان می‌دهد تا به آگاهی موقعیتی کامل دست یابد، هشدارهای کاذب را به حداقل رسانده و دقت شناسایی و ردیابی را افزایش دهد. هوش مصنوعی داده‌ها را بلادرنگ پردازش کرده، الگوهای تهدید را شناسایی و تصمیمات خودکار یا پیشنهادی را با سرعت بالا ارائه می‌دهد که زمان واکنش را از دقیقه به ثانیه کاهش می‌دهد.
	۳. انعطاف‌پذیری و تطبیق‌پذیری	قابلیت استفاده از طیف وسیعی از مکانیزم‌های مقابله (نرم و سخت) امکان پاسخ متناسب با هر نوع تهدید را فراهم می‌کند. قابلیت یادگیری و بهبود مستمر هوش مصنوعی (از طریق یادگیری تطبیقی) به سیستم اجازه می‌دهد تا تاکتیک‌های جدید مهاجمان را آموخته و استراتژی‌های دفاعی خود را بهینه کند.
	۴. کاهش آسیب‌پذیری	با ایجاد حلقه‌های دفاعی متعدد و مقابله با تهدید در فواصل دورتر، خطر آسیب به زیرساخت‌ها، تأسیسات حیاتی و نیروهای نظامی به حداقل می‌رسد و زمان بیشتری برای واکنش‌های اضطراری فراهم می‌شود.
	۵. بهینه‌سازی منابع	انتخاب هوشمندانه و هدفمند مکانیزم مقابله (مثلاً استفاده از اخلالگر نرم برای پهپادهای کم‌خطر به جای شلیک موشک گران‌قیمت) از هدر رفت منابع جلوگیری کرده و بهره‌وری عملیاتی را افزایش می‌دهد.
نقاط	۱. پیچیدگی بالا	طراحی، پیاده‌سازی و یکپارچه‌سازی سیستم‌های چندلایه با حسگرهای متنوع، سرورهای

دسته	مورد	توضیح
	و هزینه اولیه زیاد	قدرتمند و مکانیزم‌های مقابله، نیازمند سرمایه‌گذاری هنگفت در تحقیق، توسعه و اجرا است که می‌تواند مانعی برای کشورهای با بودجه محدود باشد.
	۲. نیاز به زیرساخت‌های قوی و تخصصی	عملیاتی کردن این سیستم‌ها نیازمند مراکز داده قدرتمند، قابلیت‌های پردازشی لبه‌ای، و نیروی انسانی بسیار متخصص در حوزه‌های هوش مصنوعی، امنیت سایبری و مهندسی سیستم است که تربیت و حفظ آن‌ها دشوار است.
	۳.چالش‌های امنیت سایبری	سطح حمله وسیع ناشی از ماهیت شبکه‌ای و وابسته به نرم‌افزار، سیستم را در برابر حملات سایبری (نفوذ، انکار سرویس، دستکاری داده‌ها یا فریب) آسیب‌پذیر می‌سازد که می‌تواند کل دفاع را مختل یا به تصمیم‌گیری‌های خطرناک منجر شود.
	۴.مشکلات یکپارچه‌سازی	تضمین سازگاری و تعامل بی‌نقص بین فناوری‌ها و سامانه‌های مختلف از تولیدکنندگان گوناگون (پروتکل‌های ارتباطی، فرمت‌های داده، سازگاری نرم‌افزاری) می‌تواند پیچیده و زمان‌بر باشد.
فرصت‌ها	۱.توسعه فناوری‌های نوین	پیشرفت‌های مداوم در هوش مصنوعی (یادگیری عمیق، یادگیری تقویتی)، حسگرهای نسل جدید (کوچکتر، دقیق‌تر)، فناوری‌های مقابله پیشرفته (لیزر،) و شبکه‌های ارتباطی G5، می‌تواند قابلیت‌ها را به طور چشمگیری ارتقاء دهد.
	۲. همکاری‌های بین‌المللی و اشتراک دانش	تهدید پهپادها یک معضل جهانی است. همکاری‌های تحقیقاتی و عملیاتی میان کشورها می‌تواند به تسریع توسعه، کاهش هزینه‌ها، استانداردسازی سیستم‌ها و به اشتراک‌گذاری اطلاعات تهدید کمک کند.
	۳. بازار رو به رشد امنیت و دفاع	با افزایش آگاهی از تهدیدات پهپادی، تقاضا برای سامانه‌های پدافندی مؤثر افزایش می‌یابد که فرصت‌های تجاری و سرمایه‌گذاری جدیدی را در این حوزه ایجاد می‌کند.
	۴. کاربردهای غیرنظامی	فناوری‌های توسعه یافته برای پدافند نظامی می‌توانند در زمینه‌های غیرنظامی مانند مدیریت ترافیک هوایی پهپادها ، حفاظت از زیرساخت‌های حیاتی غیرنظامی و امنیت رویدادهای عمومی نیز به کار گرفته شوند.
	۵. توسعه دکترین‌های دفاعی نوین	این فرصت برای بازتعریف و گسترش دکترین‌های دفاع هوایی و امنیتی ملی متناسب با ماهیت نوین تهدیدات پهپادی (از جمله حملات خوشه‌ای و پهپادهای خودمختار) فراهم می‌شود.
تهدید	۱.تکامل سریع	این بزرگترین تهدید است. مهاجمان به سرعت در حال توسعه پهپادهای جدید با

دسته	مورد	توضیح
	تهدیدات پهپادی	قابلیت‌های پیشرفته‌تر مانند پنهان‌کاری بیشتر، مقاومت در برابر اخلال، هوشمندی داخلی (خودمختاری) و تاکتیک‌های نوین حمله (مانند حملات خوشه‌ای) هستند که مقابله با آن‌ها را به شدت دشوار می‌کند.
	۲. دسترسی آسان به فناوری پهپادی	هزینه پایین و در دسترس بودن پهپادهای تجاری با قابلیت‌های قابل تبدیل به ابزارهای تهدیدآمیز امکان می‌دهد تا با هزینه‌ای ناچیز، تهدیدات قابل توجهی را ایجاد کنند.
	۳. محیط‌های عملیاتی پیچیده	استفاده از پهپادها در محیط‌های شهری متراکم، مناطق با تداخلات الکترومغناطیسی بالا یا شرایط آب و هوایی نامساعد می‌تواند عملکرد حسگرها و مکانیزم‌های مقابله را مختل کند و به هشدارهای کاذب منجر شود.
	۴. جنگ الکترونیک و سایبری متقابل	دشمنان نه تنها در حال توسعه پهپادهای بهتر هستند، بلکه توانایی‌های خود را در زمینه جنگ الکترونیک (مانند اخلالگرهای پیشرفته) و حملات سایبری (برای نفوذ و کنترل سیستم‌های پدافندی) بهبود می‌بخشند که می‌تواند کارایی سیستم‌های هوشمند را تضعیف کند.

تحلیل راهبردی SWOT: پدافند لایه‌ای هوشمند در برابر پهپادها

تحلیل SWOT مدل مفهومی پدافند لایه‌ای هوشمند در برابر تهدیدات پهپادی، ابزاری حیاتی برای درک موقعیت استراتژیک این رویکرد است. با توجه به ماتریس ارائه شده، می‌توان راهبردهای چهارگانه را برای بهینه‌سازی مدل و افزایش کارایی آن استخراج کرد.

۱. راهبردهای تهاجمی[1]:این راهبردها بر استفاده از نقاط قوت داخلی برای بهره‌برداری حداکثری از فرصت‌های بیرونی تمرکز دارند.

- استراتژی توسعه و نوسازی: با بهره‌گیری از تاب‌آوری بالا و انعطاف‌پذیری سیستم (نقاط قوت)، می‌توان از توسعه فناوری‌های نوین در هوش مصنوعی و حسگرهای نسل جدید (فرصت‌ها) برای ایجاد یک مزیت رقابتی پایدار در بازار رو به رشد امنیت و دفاع بهره برد.

1 SO - Strengths-Opportunities

- استراتژی همکاری‌های بین‌المللی: با تکیه بر دقت و سرعت بالای سیستم (نقطه قوت)، می‌توان در همکاری‌های بین‌المللی و پروژه‌های مشترک شرکت کرد (فرصت) و به استانداردهای جهانی و اشتراک دانش دست یافت. این امر به کاهش هزینه‌های تحقیق و توسعه کمک می‌کند.

۲. راهبردهای ترمیمی[1]:این راهبردها به دنبال استفاده از فرصت‌ها برای غلبه بر نقاط ضعف هستند.

- استراتژی سرمایه‌گذاری هدفمند: با توجه به پیچیدگی بالا و هزینه اولیه زیاد (نقطه ضعف)، باید از افزایش تقاضا در بازار (فرصت) و فرصت‌های سرمایه‌گذاری برای جذب بودجه و منابع مالی لازم برای تحقیق و توسعه زیرساخت‌های قوی استفاده کرد.
- استراتژی توسعه استانداردها: با وجود مشکلات یکپارچه‌سازی (نقطه ضعف)، می‌توان با شرکت در همکاری‌های بین‌المللی و تلاش برای توسعه دکترین‌های دفاعی نوین (فرصت)، به ایجاد استانداردهای مشترک و پروتکل‌های ارتباطی یکپارچه دست یافت.
- ۳. راهبردهای دفاعی[2]:این راهبردها بر استفاده از نقاط قوت برای مقابله با تهدیدات بیرونی متمرکز هستند.
- استراتژی مقابله پویا: با استفاده از قابلیت تطبیق‌پذیری و یادگیری مستمر هوش مصنوعی (نقطه قوت)، می‌توان با تکامل سریع تهدیدات پهپادی و جنگ الکترونیک متقابل (تهدیدات) مقابله کرد. سیستم باید به طور مداوم تاکتیک‌های جدید را بیاموزد و استراتژی‌های دفاعی خود را به‌روزرسانی کند.
- استراتژی کاهش ریسک: تاب‌آوری بالا و بهینه‌سازی منابع (نقاط قوت) به سیستم اجازه می‌دهد تا در برابر دسترسی آسان به فناوری پهپادی (تهدید) که منجر به افزایش حملات خوشه‌ای می‌شود، مقاومت کند و با هدف قرار دادن پهپادهای کلیدی، از هدر رفت منابع جلوگیری کند.

1 WO - Weaknesses-Opportunities
2 ST - Strengths-Threats

۴. راهبردهای تدافعی[1]:این راهبردها بر به حداقل رساندن نقاط ضعف و جلوگیری از تأثیر تهدیدات تمرکز دارند و به عنوان آخرین خط دفاعی عمل می‌کنند.

- استراتژی توسعه نیروی انسانی: با توجه به نیاز به نیروی انسانی متخصص (نقطه ضعف) و تکامل سریع تهدیدات (تهدید)، باید در آموزش و تربیت نیروی انسانی متخصص در حوزه‌های هوش مصنوعی و امنیت سایبری سرمایه‌گذاری کرد تا بتوان به چالش‌های پیچیده‌ای مانند جنگ سایبری متقابل پاسخ داد.
- استراتژی مدیریت ریسک سایبری: با توجه به آسیب‌پذیری در برابر حملات سایبری (نقطه ضعف)، باید تمرکز را بر توسعه مکانیزم‌های دفاعی پیشرفته و چندلایه در برابر نفوذ، انکار سرویس و دستکاری داده‌ها قرار داد تا بتوان از تخریب سیستم توسط دشمنان جلوگیری کرد.

این تحلیل راهبردی نشان می‌دهد که مدل پدافند لایه‌ای هوشمند، با وجود چالش‌های داخلی، پتانسیل بالایی برای ایجاد یک برتری استراتژیک در برابر تهدیدات نوین دارد، به شرطی که راهبردهای مناسب برای تبدیل فرصت‌ها به مزیت و مقابله با تهدیدات اتخاذ شوند.

تحلیل کمی عملکرد و هزینه-فایده پدافند لایه‌ای در برابر پهپاد نمونه (مثال عددی)

در این تحلیل، پهپاد DJI Mavic3 به عنوان یک مثال واقعی از تهدیدات تجاری پرکاربرد در نظر گرفته شده است. این پهپاد با ابعاد کوچک (۳۰×۲۰×۱۵ سانتی‌متر)، سرعت متوسط (تا 100 کیلومتر بر ساعت) و سطح مقطع راداری پایین، یک هدف چالش‌برانگیز محسوب می‌شود.در این تحلیل، یک پهپاد فرضی با مشخصات زیر را در نظر می‌گیریم:

- نوع پهپاد: پهپاد انتحاری کوچک
- سرعت: ۱۰۰ کیلومتر بر ساعت (۲۷.۸ متر بر ثانیه)
- برد عملیاتی: ۱۰ کیلومتر
- ارزش هدف: یک تأسیسات با ارزش تخمینی ۲۰۰ میلیون دلار.

1 WT - Weaknesses-Threats

در هر لایه از مدل پدافندی، می‌توان از مفاهیم آماری و احتمالی استفاده نمود تا عملکرد آن را به صورت عددی بیان شود. احتمال شناسایی[1] و احتمال هشدار کاذب[2] این دو معیار اساسی برای ارزیابی عملکرد یک سنسور یا یک سیستم شناسایی هستند. برای مثال، اگر سه لایه شناسایی داشته باشیم:

- لایه ۱ (رادار) Pd۱: و Pfa۱
- لایه ۲ (اپتیکال) Pd۲: و Pfa۲
- لایه ۳ (صوتی) Pd۳: و Pfa۳

احتمال شناسایی کل با استفاده از همجوشی داده‌ها، احتمال شناسایی کل افزایش می‌یابد. به عنوان مثال، می‌توان از یک فرمول ساده زیر با این فرض که سنسورها مستقل عمل می‌کنند استفاده نمود.

$$P_d(Total) = 1 - (1 - P_{d1})(1 - P_{d2})(1 - P_{d3})$$

در ادامه، عملکرد هر لایه دفاعی بر اساس این مثال، به صورت کمی مدل‌سازی و در جدول زیر جمع‌بندی شده است.

جدول ۱. تحلیل کمی عملکرد پدافند لایه‌ای بر اساس SWOT

توضیح و مثال عددی	مورد	دسته
لایه ۱ (شناسایی دوربرد – رادار): احتمال شناسایی یک پهپاد کوچک به دلیل سطح مقطع راداری پایین، نسبتاً کم است، حدود۰.۴ لایه ۲ (شناسایی میانی – دوربین های اپتیکال مادون سرخ): با ورود پهپاد به برد دید دوربین‌ها، احتمال شناسایی افزایش می‌یابد، حدود ۰.۷ لایه ۳ (شناسایی نزدیک – صوتی) در نزدیکی هدف، احتمال شناسایی بسیار بالا می‌رود، حدود ۰.۹۵	احتمال شناسایی در هر لایه	تحلیل عملکردی
لایه ۱ (رادار): در محیط‌های پرنویز، احتمال هشدار کاذب بالاست حدود۰.۱۵ لایه ۲ (دوربین های اپتیکال مادون سرخ) به دلیل وضوح تصویر، احتمال هشدار کاذب کمتر است، حدود ۰.۰۵	احتمال هشدار کاذب در هر لایه	

1 :Pdاحتمال اینکه سیستم، یک پهپاد واقعی را به درستی شناسایی کند

2 :Pfaاحتمال اینکه سیستم، یک شیء غیرپهپادی (مانند پرنده) را به اشتباه به عنوان پهپاد شناسایی کند.

توضیح و مثال عددی	مورد	دسته
لایه ۳ (صوتی) به دلیل تأیید نوع تهدید، احتمال هشدار کاذب بسیار پایین است حدود۰.۰۱		
زمان کل واکنش ≈ ۲۴.۵ ثانیه زمان شناسایی (همجوشی داده‌ها): ۷ ثانیه زمان تصمیم‌گیری هوش مصنوعی: ۰.۵ ثانیه زمان فعال‌سازی مقابله: ۱۷ ثانیه (با فرض استفاده از یک پرتابه ضدپهپادی)	زمان واکنش	

جدول ۲. تحلیل کمی هزینه فایده پدافند لایه‌ای بر اساس SWOT

توضیح و مثال عددی	مورد	دسته
هزینه کل تقریبی: ۳۰ میلیون دلار هزینه حسگرها (رادار، اپتیکال، صوتی): ۱۰ میلیون دلار هزینه زیرساخت و:توسعه هوش مصنوعی ۵ میلیون دلار هزینه مکانیزم‌های مقابله: ۱۵ میلیون دلار	هزینه پیاده‌سازی(هزینه تحقیق و توسعه، خرید و پیاده‌سازی زیرساخت‌های چندلایه.)	۲ .تحلیل هزینه–فایده
هزینه خسارت احتمالی از یک حمله موفق: ۲۰۰ میلیون دلار (ارزش تخمینی هدف)	هزینه جبران خسارت	
هزینه مورد انتظار حمله موفق بدون پدافند: ۲۰۰ میلیون دلار هزینه سرمایه‌گذاری اولیه ۳۰ میلیون دلاری، با کاهش چشمگیر هزینه مورد انتظار خسارت در طول زمان، توجیه‌پذیر می‌شود. این سیستم با انتخاب هوشمندانه، از شلیک گران‌قیمت موشک (مثلاً در برابر یک پهپاد شناسایی) جلوگیری کرده و با استفاده از اخلالگر کم‌هزینه، بهره‌وری عملیاتی را به شدت افزایش می‌دهد.	توجیه اقتصادی	
هزینه مقابله با موشک: ۱۰۰,۰۰۰ دلار به ازای هر موشک با اخلالگر: ۱,۰۰۰ دلار به ازای هر بار فعال‌سازی سیستم هوشمند با انتخاب اخلالگر برای پهپادهای کم‌خطر (در ٪۸۰ موارد)، هزینه‌های عملیاتی را به شدت کاهش می‌دهد.	بهینه‌سازی منابع	

پیشنهادات برای توسعه و پیاده‌سازی پدافند لایه‌ای هوشمند در برابر تهدیدات پهپادی

با توجه به تحلیل SWOT و درک عمیق از ماهیت و چالش‌های پدافند لایه‌ای هوشمند در برابر تهدیدات پهپادی، در ادامه پیشنهاداتی راهبردی و عملیاتی برای توسعه و پیاده‌سازی مؤثرتر این سیستم‌ها ارائه می‌شود:

۱. سرمایه‌گذاری متوازن در تحقیق و توسعه

اولویت‌بندی پژوهش‌های کاربردی: تمرکز بر توسعه نسل جدید حسگرهای با قابلیت تشخیص بالا برای اهداف کوچک و پنهان‌کار (مانند رادارهای میکرو-دوپلر، حسگرهای کوانتومی). همچنین، سرمایه‌گذاری در فناوری‌های لیزر پرتوان و سیستم‌های مایکروویو پرتوان به دلیل سرعت بالا و هزینه عملیاتی پایین.

پیشرفت در هوش مصنوعی و یادگیری ماشین: تخصیص منابع به تحقیقات در زمینه یادگیری تقویتی برای بهبود تصمیم‌گیری خودکار و پاسخ تطبیقی، و همچنین یادگیری عمیق در پردازش داده‌های چندوجهی برای افزایش دقت همجوشی داده‌ها و کاهش هشدارهای کاذب.

۲. تقویت امنیت سایبری و تاب‌آوری سیستم‌ها

طراحی امن از ابتدا: امنیت سایبری باید از همان مراحل اولیه طراحی سیستم پدافندی لحاظ شود، نه به عنوان یک بخش اضافی در پایان پروژه.

سیستم‌های تشخیص نفوذ مبتنی بر هوش مصنوعی: پیاده‌سازی سامانه‌های پیشرفته‌ای که قادر به شناسایی الگوهای غیرعادی و حملات سایبری به صورت بلادرنگ باشند.

معماری‌های مقاوم در برابر شکست: طراحی سیستم‌هایی که حتی در صورت نفوذ به بخشی از آن‌ها، قادر به ادامه عملیات و ایزوله کردن بخش آسیب‌دیده باشند. استفاده از زیرساخت‌های لبه‌ای امن برای کاهش وابستگی به شبکه‌های متمرکز.

۳. توسعه منابع انسانی متخصص و ایجاد همکاری‌های چندجانبه

آموزش و تربیت نیروی متخصص: سرمایه‌گذاری در برنامه‌های آموزشی دانشگاهی و فنی برای تربیت مهندسان، محققان و اپراتورهای متخصص در حوزه‌های هوش مصنوعی، جنگ الکترونیک، امنیت سایبری و مهندسی سیستم‌های ضد پهپاد.

۴. رویکرد ماژولار و مقیاس‌پذیر در طراحی سیستم‌ها

معماری سیستم باز : طراحی سیستم‌های پدافندی به گونه‌ای که بتوان حسگرها، زیرسیستم‌ها و مکانیزم‌های مقابله را از تولیدکنندگان مختلف به راحتی یکپارچه کرد. این امر از وابستگی به یک شرکت خاص جلوگیری کرده و امکان ارتقاء و به‌روزرسانی مداوم را فراهم می‌آورد.

مقیاس‌پذیری: قابلیت تطبیق سیستم با نیازهای عملیاتی مختلف، از حفاظت نقطه‌ای (مانند یک تأسیسات خاص) تا پوشش منطقه‌ای گسترده. این انعطاف‌پذیری به بهینه‌سازی هزینه‌ها نیز کمک می‌کند.

۵. تمرین و ارزیابی مستمر سیستم‌ها در محیط‌های واقعی

سناریوهای شبیه‌سازی شده و واقعی: انجام آزمایش‌ها و مانورهای منظم با استفاده از پهپادهای واقعی و شبیه‌سازی سناریوهای حملات پیچیده (مانند حملات خوشه‌ای) برای ارزیابی عملکرد سیستم در شرایط نزدیک به واقعیت.

این پیشنهادات، با تمرکز بر پیشرفت فناوری، تقویت امنیت، تدوین چارچوب‌های قانونی و اخلاقی، توسعه منابع انسانی و اتخاذ رویکردهای طراحی مدرن، می‌تواند مسیر را برای توسعه و پیاده‌سازی موفقیت‌آمیز پدافند لایه‌ای هوشمند در برابر تهدیدات پهپادی هموار سازد.

فهرست منابع

محمدی, اردشیر, حسین نواده توپچی, ایرج فروزان, حسین شکوهی, ابراهیم ایجابی. ۱۴۰۲. ٬بررسی چالش‌های مقابله با سامانه‌های هواپیمای بدون سرنشین، علوم و فنون نظامی، سال نوزدهم، شماره ۶۳،

پدرام، عبدالرحیم ، احمدیان، مهدی ، امیرمزلقانی، یوسف،۱۳۹۷، آینده پژوهی درحوزه محصولات ضد پهپاد با استفاده از اولویت گذاری پابرجا، فصلنامه آینده پژوهی دفاعی شماره ۱۱، دوره ۳

شریفی تهرانی، امید، صادقی ، علیرضا، علوی، سید محمد،۱۳۹۹،چالش های آینده یکپارچه سازی پهپاد و اخلالگر، فصلنامه مطالعات جنگ، سال دوم،شماره ششم

Brust, Matthias R., Grégoire Danoy, Daniel H. Stolfi, and Pascal Bouvry. 2021. ‘Swarm-Based Counter UAV Defense System’. Discover Internet of Things 1 (1): 2. https://doi.org/10.1007/s43926-021-00002-x.

Castrillo, Vittorio Ugo, Angelo Manco, Domenico Pascarella, and Gabriella Gigante. 2022. ‘A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones’. Drones 6 (3): 65.

Chen, Yu-Jia, Xiao-Chun Chen, and Miao Pan. 2022. ‘Defense Against Machine Learning Based Attacks in Multi-UAV Networks: A Network Coding Based Approach’. IEEE Transactions on Network Science and Engineering 9 (4): 2562–78. https://doi.org/10.1109/TNSE.2022.3165971.

Islam, Shafkat, Shahriar Badsha, Ibrahim Khalil, Mohammed Atiquzzaman, and Charalambos Konstantinou. 2023. ‘A Triggerless Backdoor Attack and Defense Mechanism for Intelligent Task Offloading in Multi-UAV Systems’. IEEE Internet of Things Journal 10 (7): 5719–32. https://doi.org/10.1109/JIOT.2022.3172936.

Kamdem, Priva Chassem, Alain B. Zemkoho, Laurent Njilla, Marcellin Nkenlifack, and Charles A. Kamhoua. 2024. ‘Two-Layer Deception Model Based on Signaling Games Against Cyber Attacks on Cyber-Physical Systems’. IEEE Access 12:171559–70. https://doi.org/10.1109/ACCESS.2024.3478808.

Kang, Honggu, Jingon Joung, Jinyoung Kim, Joonhyuk Kang, and Yong Soo Cho. 2020a. ‘Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems’. IEEE Access 8:168671–710. https://doi.org/10.1109/ACCESS.2020.3023473.

KRAjNC, Zoltán, and Erika Vallus. 2021. ‘Contemporary Low Slow and Small (LSS) Threat from the Air Defence View’. Security & Future 5 (2): 46–48.

Liu, Baohong, and Juntao Sun. 2021. ‘Stackelberg Game under Asymmetric Information in Unmanned Aerial Vehicle Swarm Active Deception Defense: From a Multi-Layer Network Perspective’. In 2021 International Conference on Big Data and Intelligent Decision Making (BDIDM), 75–79. https://doi.org/10.1109/BDIDM53834.2021.00022.

Lyu, Chenyang, and Renjun Zhan. 2022. ‘Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicle’. IEEE Aerospace and Electronic Systems Magazine 37 (1): 6–31.

Tianfeng, Fan, Meng Xiaojing, and Zhang Chi. 2023. ‘Development Status of Anti UAV Swarm and Analysis of New Defense System’. In Journal of Physics: Conference Series, 2478:092011. IOP Publishing.

Tripathi, Nikhil, and Neminath Hubballi. 2022. ‘Application Layer Denial-of-Service Attacks and Defense Mechanisms: A Survey’. ACM Computing Surveys 54 (4): 1–33. https://doi.org/10.1145/3448291.