Journal of Safe City

Online ISSN: 2676-556X

Journal Homepage: www.ispdrc.ir

Research Paper

Prioritized Solutions of Electronic and Cyber Defense in Drone Detection and Defense using Analytical Hierarchy Process (AHP)

Mojtaba Araghizadeh[a], Gholam Reza Jalali Farahani[b], Foruzan, Hamid[c]

[a]*Passive Defense Faculty of Malek Ashtar University of Technology, Tehran, Iran*
[b]*Supreme National Defense University, Tehran, Iran*
[c]*Department of Passive Defense Strategic Management, Supreme National Defense University, Tehran, Iran*

ARTICLE INFO

Keywords:
Analytic Hierarchy Process, Drone Threats, Detection, Defense, Electronic Defense, Cyber Defense

Received:
10 May 2024
Received in revised form:
05 July 2024
Accepted:
24 July 2024
pp. 153-169

ABSTRACT

Drones now have many useful functions, ranging from monitoring pipelines, photography, filming, and as a hobby for teenagers. Despite diversity of civil and military uses of drones for countries, they have threats for critical infrastructures and key assets. Nowadays, they are used beside war fighter planes. Drone attacks can be done by commercial drones dropping bombs, firing a missile, or crashing into a target. One of the main concerns is the unauthorized use of drones near critical infrastructure, public events, and sensitive locations. For instance, drones flying near airports or nuclear power plants pose a serious threat to security. Unauthorized drone activities can interfere with operations, compromise safety, and even facilitate criminal acts. Furthermore, because of their high efficiency and low cost among manned planes, they are more favorable for world armies. The availability of advanced navigation and satellite communication technologies has revolutionized the use of drones, making them more versatile. They can now endure missions by 40 hours, far beyond the capabilities of human crew. With in-flight refueling and ultra-efficient solar power, the drones can provide an even greater range of operation. Meanwhile, in order to deter drone threats, diverse actions have done in the world, called "Counter-drone technologies or systems". Counter-drone technology encompasses a wide range of ways that allow you to detect, classify, and mitigate unmanned aerial vehicles. Parallel of using drones in the world, developing of counter-drone technologies is on process. More of these technologies are based on electronic and cyber defense methods.

Corresponding author (Email: mojtabarezvani313@gmail.com)

The growth of counter-drone technology is related to the increase in concerns about the threat that drones pose to civilian and military infrastructures. Counter drone systems have become essential for the safety and security of critical infrastructures. Counter-drone systems detect and intercept the unknown drones by taking into account their flight path, physical properties such as size and kinetic energy, the number of swarming drones, and the likely damage which could be caused. Counter-drone systems are fixed or preferably portable and have the capability of defending the facilities like military establishments and sites, airports, petroleum facilities, etc. by quickly detecting multiple drones at sufficient distances.

Drone detection technology works to detect drones in the airspace. The most popular ways to detect drones electronic and cyber defense are: acoustic sensors, electro-optical and infra-red sensors, RADAR and radio frequency sensors. Acoustic sensors can involve one or multiple microphones and software. These technologies can detect drones by engine sound to calculate distance and direction. Optical sensors (cameras) utilize multiple wavelengths (thermal, infrared, etc.) for day or night drone detection, and the technology is evolving quickly to extend range and intelligence with AI capabilities. Radar uses radio waves to determine distance and speed of objects. It is accurate and identifies hundreds of targets simultaneously, including all drone types (piloted or autonomous) in many weather conditions. RF sensors consist of one or multiple antennas of various ranges to detect communications between and drone and its controller (human operator). Although for drone mitigation or interception, the best are electromagnetic pulse (EMP) or high power microwave (HPM), laser guns, electromagnetic field, jamming and spoofing.

This research aimed to develop prioritized solutions of electronic and cyber defense in drone detection and defense.

In this research, which is applicable in nature, the most popular methods in electronic and cyber defense were identified and analyzed using of a mixed methodology after a literature review on drone detection and defense systems. Then by using of library studies and expert opinions, 11 criteria were gathered and prioritized using AHP method. These 11 criteria were: response time, cost, side-effects, operator skills, ability to detect autonomous drones, range, accuracy, intensity of effect, ability to drone landing, ability to build in the country, accessibility to system details.

In this process, it was known that performance accuracy and functional range of detection systems have the best points. Then each of drone detection and defense was marked and by multiplying scores in weight of each criterion, final scores of each drone detection and defense system was identified in order to prioritize them.

At last, it became clear that for drone detection based on determined criteria the best method is RADAR based method and for defense is HPM. Thus, using of laser systems and cyber spoofing with a slight difference were on next steps of drone defense.

مجلـــه شهـــر ایمـــن
شاپا الکترونیکی: 2676-556X
Journal Homepage: www.ispdrc.ir

مقاله پژوهشی

راهکارهای اولویت‌بندی شده پدافند الکترونیک و پدافند سایبری در شناسایی و مقابله با تهدیدات پهپادی با استفاده از روش تحلیل سلسله‌مراتبی

مجتبی عراقی زاده*، غلامرضا جلالی فراهانی، حمید فروزان

۱- پژوهشیارمجتمع دانشگاهی مهندسی و پدافند غیر عامل
۲- دانشیار دانشگاه عالی دفاع ملی
۳- استادیار گروه مدیریت راهبردی دانشگاه عالی دفاع ملی

واژگان کلیدی

تحلیل سلسله‌مراتبی، تهدیدات پهپادی، شناسایی، مقابله، پدافند الکترونیک، پدافند سایبری

چکیده

پژوهش حاضر با هدف ارائه راهکارهای اولویت‌بندی‌شده پدافند الکترونیک و پدافند سایبری برای شناسایی و مقابله با تهدیدات پهپادی به انجام رسیده است. در پژوهش حاضر که از نظر ماهیت، کاربردی می‌باشد با بهره-گیری از روشی ترکیبی پس از یک مطالعه مروری بر روی روش‌های شناسایی و مقابله با تهدیدات پهپادی، مرسوم‌ترین این روش‌ها از جدیدترین منابع شناسایی و ارزیابی گردیدند. در ادامه با بهره‌گیری از مطالعات کتابخانه‌ای و نظر خبرگان، ۱۱ معیار برای رتبه‌بندی این روش‌ها احصاء و با روش تحلیل سلسله‌مراتبی رتبه-بندی گردیدند. سپس هریک از روش‌های شناسایی و مقابله بر اساس معیارهای شناسایی شده بر اساس ویژگی‌ها و محدودیت‌های احصاء شده در بخش ادبیات پژوهش برای هریک از روش‌های شناسایی و مقابله با تهدیدات پهپادی، نمره‌گذاری گردیدند و با ضرب نمودن امتیازهای به‌دست‌آمده در وزن هر معیار، امتیاز نهایی هریک از روش‌های شناسایی و مقابله با تهدیدات پهپادی حاصل گردید تا از این طریق بتوان آنها را رتبه‌بندی نمود. در پایان مشخص گردید برای شناسایی پهپادها، بهترین روش بر اساس معیارهای تعیین‌شده، روش‌های مبتنی بر سامانه‌های راداری بوده و برای مقابله با پهپادها، بهترین روش، بهره‌گیری از پالس الکترومغناطیسی می‌باشد. همچنین بهره‌گیری از سامانه‌های لیزری و ایجاد فریب سایبری برای پهپاد با اختلاف ناچیزی در رتبه بعدی روش‌های مقابله با تهدیدات پهپادی قرار گرفتند.

*. نویسنده مسئول Email: mojtabarezvani313@gmail.com

۱- کلیات

۱-۱- طرح مسئله

گسترش روزافزون دامنه تهدیدات پهپادهای جاسوسی و تهاجمی علیه منافع ملی کشور توسط کشورهای فرامنطقه‌ای ایجاب می‌کند که نظام دفاعی کشور برای مقابله با آنها به بازبینی و بهینه‌سازی فرایندهای عملیاتی خود در این زمینه بپردازد (حبیبی، ۱۳۹۳: سخن آغازین). علت توجه به پرنده-های بدون سرنشین این است که در بخش‌های نظامی، از آن زمان که بشر خود را شناخته، از جنگ تن‌به‌تن و گلاویز شدن دوری کرده است و لذا به‌طور تدریجی با ابداع ابزارها، فاصله انسان‌ها را در جنگ‌ها از یکدیگر بیشتر کرده است و این روند افزایش فاصله بین دو جبهه درگیری، یک اصل ثابت بوده است (رستمی، ۱۳۹۱). به‌علاوه، کارایی و اثربخشی هواپیماهای بدون سرنشین با توجه به توانمندی بسیار بالای آنها و سهولت کاربری، نگهداری، ساخت و تولید و همچنین ارزان‌قیمت بودن در مقایسه با هواپیماهای سرنشین‌دار، مورد توجه ارتش‌های جهان قرار گرفته است (شکوهی،۱۳۹۲:۱۳).

با وجود آنکه پهپادها کاربردهای نظامی و غیرنظامی بسیار مفیدی برای کشورها دارند و از سالیان پیش کاربردهای متعددی برای پهپادها در حوزه تجاری مطرح بوده است (کاظمی و الهیان، ۱۳۹۹:۴۸)، اما به‌موازات بهره-گیری از منافع، تهدیدات آنها نیز به‌شدت علیه دارایی‌ها و زیرساخت‌های کشورها گسترش یافته است. در واقع در جنگ‌های آینده ترکیبی از هواپیماهای با سرنشین و بدون سرنشین به‌کار گرفته خواهد شد (حبیبی، ۱۳۹۳: مقدمه). پهپادها دسته‌بندی‌های گوناگونی دارند که مهم‌ترین و رایج‌ترین دسته‌بندی پهپادها در جهان عبارتند از دسته‌بندی بر اساس اندازه و وزن، دسته‌بندی بر اساس چگونگی کنترل پرواز و دسته‌بندی بر اساس نوع مأموریت پهپاد (خرم فعال، ۱۳۹۹:۱۷). بر اساس اندازه و وزن به سه دسته راهبردی، عملیاتی و تاکتیکی، بر اساس چگونگی کنترل پرواز سه دسته پیش برنامه‌ریزی‌شده، کنترل از راه دور و کنترل بر اساس هوش مصنوعی و بر اساس نوع مأموریت به پنج دسته شناسایی، مراقبت، انتحاری، تهاجمی و هدف تقسیم‌بندی می‌شوند (همان:۵۶).

در این میان برای مقابله با تهدیدات پهپادی اقدامات مختلفی در دنیا تحت عنوان فناوری‌های ضد پهپاد صورت گرفته است. فناوری ضد پهپاد که به‌عنوان فناوری ضد سامانه‌های بدون سرنشین نیز شناخته می‌شوند به سامانه-هایی اشاره دارند که برای شناسایی و یا رهگیری هواپیماهای بدون سرنشین استفاده می‌شوند. درحالی‌که نگرانی از تهدیدهای امنیتی بالقوه از پهپادهای نظامی و نیز شخصی در حال رشد است یک بازار جدید برای فناوری ضد پهپاد به‌سرعت در حال ظهور است. تا به امروز حداقل ۲۳۵ عدد از محصولات ضد پهپاد در بازار و یا در حال تحقیق و توسعه برای ورود به بازار شناسایی شده‌اند (هالند (*Holland*)، ۲۰۱۸:۱) به نقل از (پدرام و همکاران، ۱۳۹۷:۱۴۷). این روش‌ها عمدتاً مبتنی بر پدافند الکترونیک و پدافند سایبری هستند. از جمله سامانه‌هایی که به‌عنوان آشکارساز و رهگیر پهپاد می‌توان به آنها اشاره کرد عبارتند از: رادار، امواج رادیویی، تصویری، مادون‌قرمز، صوتی و حسگرهای ترکیبی؛ بنابراین مسئله پژوهش حاضر، اولویت‌بندی راهکارهای شناسایی و مقابله با تهدیدات پهپادی چگونه می‌باشد.

۱-۲- محدودیت‌های تحقیق

ازآنجاکه این حوزه جزو حوزه‌های لبه دانشی و نوین در عرصه علوم نظامی می‌باشد، داده‌ها و اطلاعات به کار برده شده در این پژوهش از میان آخرین منابع در دسترس در بسترهای علمی گردآوری گردید. طبیعتاً ممکن است روش‌هایی ورای روش‌های ذکر شده در این پژوهش وجود

داشته باشد که هنوز به عرصه عمومی معرفی نشده باشند.

۱-۳- پیشینه و ادبیات موضوع

جنگ الکترونیک و جنگ سایبری در حال تبدیل شدن به عناصر کلیدی صحنه نبرد هستند، به‌خصوص زمانی که عملیات نظامی وابستگی بیشتری به تفوق اطلاعاتی داشته باشد. تسلط بر طیف الکترومغناطیسی و سامانه‌های اطلاعاتی، فرمانروایی مطلق در میدان جنگ را به ارمغان خواهد آورد و مخاطرات ناشی از وابستگی عناصر صحنه نبرد به شبکه‌های ارتباطی و سامانه‌های اطلاعاتی را کاهش می‌دهد. وجوه اشتراکات جنگ سایبری و جنگ الکترونیک در اصول و فرآیند اجرا و همچنین تأثیرات و پیامدهای نسبتاً مشابه آنها در سازمان‌های نظامی، سبب همگرایی بین دو عرصه شده است. استفاده مؤثر و هماهنگ از قابلیت‌های این دو حوزه، عامل برتری‌ساز و تعیین کننده در نبردهای آینده خواهد بود. کشورهای بهره‌مند از این دو عامل قادر خواهند بود تا نبردها را با حداقل تلفات انسانی و کمترین هزینه به نفع خود به پایان برسانند (فرحبخت و دهقانی، ۱۳۹۸:۲۰۰).

در سال‌های اخیر توجه به روش‌های شناسایی و مقابله با تهدیدات پهپادی به روش‌های پدافند الکترونیک و پدافند سایبری بسیار مورد توجه قرار گرفته است. چیپر (*Chiper*) و همکاران (۲۰۲۲) در مقاله‌ای مروری و ارزشمند، با بررسی ۱۸۶ منبع علمی در رابطه با روش‌های شناسایی و مقابله با این تهدیدات پرداخته‌اند. آنها معتبرترین روش‌ها را شناسایی کرده و به بیان ویژگی‌ها و نقاط ضعف هریک از روش‌ها پرداخته‌اند و در انتها سامانه پیشنهادی خود را معرفی کرده‌اند (چیپر و همکاران، ۲۰۲۲). پدرام و همکاران نیز (۱۳۹۸) در پژوهشی با عنوان آینده‌پژوهی در حوزه محصولات ضد پهپاد با استفاده از اولویت‌گذاری پابرجا پس از معرفی روش‌ها و فناوری‌های مختلف ضد پهپاد و ارائه نقاط مثبت و منفی آنها، تلاش نموده‌اند با روشی جدید، نسبت به اولویت‌گذاری فناوری‌های آتی در این حوزه تمرکز داشته باشند و به این ترتیب رویکردهای پیشنهادی خود را در زمینه محصولات ضد پهپادی بیان کرده‌اند. در این پژوهش تفکیک مابین روش‌های سخت مقابله و روش‌های پدافند الکترونیک و سایبری صورت نپذیرفته است (احمدیان و مزلقانی: ۱۳۹۷). کراتکی (*Kratky*) و فارلیک (*Farlik*) (۲۰۱۸) در مقاله‌ی مقابله با پهپادها- جلوبرنده تحقیقات در فناوری‌های نظامی که با هدف تأکید بر ایجاد زمینه‌های علمی جدید در ارتباط با فناوری‌های ضدپهپادی به انجام رسیده است، به بیان رشته‌ها و حوزه‌های علمی که باید در ارتباط با مقابله با پهپاد فعال شده و می‌توانند اقدامات مؤثری انجام دهند، پرداخته‌اند. در ادامه نیز مهم‌ترین فناوری‌های شناسایی و مقابله را معرفی کرده‌اند اما بیشترین تأکید این مقاله بر لزوم آغاز یک حرکت علمی وسیع در زمینه مقابله با تهدیدات پهپادی است (کراتکی و فارلیک، ۲۰۱۸). براست (*Brust*) و همکاران (۲۰۱۸) در پژوهشی با عنوان دفاع در برابر نفوذ پهپادهای مهاجم با استفاده از شبکه‌ای از پهپادهای دفاعی به ارائه راه‌حلی خلاقانه برای مقابله با تهدیدات پرداخته‌اند که طی آن به مجرد تشخیص نزدیک شدن پهپاد مهاجم، شبکه‌ای منسجم از پهپادهای مدافع اقدام به محاصره پهپاد مهاجم از سه جهت نموده و امکان حرکت را از آن سلب می‌نمایند و در نهایت نیز آن پهپاد را به خارج از محیط حفاظت‌شده هدایت می‌کنند. این روش از الگوریتم‌های خاص و پیچیده‌ای برای شناسایی، محاصره و هدایت جهت‌دار پهپاد مهاجم بهره برده و امکان و هزینه‌های پیاده‌سازی آن برای زیرساخت‌های مختلف باید مورد بررسی قرار گیرد (براست و همکاران، ۲۰۱۸). فارلیک و همکاران (۲۰۱۹) در مقاله‌ای با عنوان شناسایی چند طیفی پهپادهای تجاری که حاصل کار پژوهشی چهار سال‌های بوده است روش‌های شناسایی پهپادها بر اساس طیف‌های مختلف

الکترومغناطیسی را تحلیل کرده‌اند و راه‌حل‌های راداری را برای شناسایی پهپادها مناسب دانسته‌اند. هرچند به این مسئله نیز اذعان کرده‌اند که هیچ راه‌حل جامع و کاملی برای شناسایی پهپادها وجود ندارد و باید مطالعات بسیار بیشتری در این زمینه صورت پذیرد (فارلیک و همکاران، ۲۰۱۹). همچنین نوروزی (۱۳۹۴) در مقاله‌ای با عنوان بررسی حملات الکترونیک علیه پهپادها، حملات الکترونیک علیه سیستم‌های ارتباط رادیویی، ماهواره‌ای و شبکه ارتباطی پهپادها را مورد بررسی قرار داده و راهکارهای متناسب هریک از حملات را پیشنهاد داده است. در این مقاله علاوه بر حملات الکترونیکی علیه پهپادها، حملات سایبری علیه آنها نیز به دو شکل سخت‌افزاری و نرم‌افزاری مورد توجه قرار گرفته است (نوروزی، ۱۳۹۴)، لکن در این مقاله نیز مانند مقالات یاد شده پیشین موضوع اولویت‌بندی و رتبه‌بندی روش‌های دفاع الکترونیک و سایبری در برابر تهدیدات پهپادی رخ نداده است.

آنچه به‌عنوان جمع‌بندی از پیشینه‌های ذکر شده در این مقاله و سایر پیشینه‌هایی که از ذکر آنها صرف‌نظر شده است حاصل می‌شود این است که فناوری‌های متعدد شناسایی و مقابله با تهدیدات پهپادی به‌خوبی شناسایی و معرفی شده‌اند و مزایا و معایب هر یک نیز بیان گردیده‌اند اما با توجه به اینکه هر یک از روش‌های یاد شده از مزایا و معایبی برخوردار هستند، نوعی و اولویت‌بندی برای انتخاب سامانه برتر شناسایی و مقابله با تهدیدات پهپادی به انجام نرسیده است. به‌عبارت‌دیگر انتخاب سامانه برای انتخاب‌گران غیرحرفه‌ای در شرایط فعلی دشوار است که این مقاله به دنبال برطرف نمودن این چالش است.

۱-۴- انواع سیستم‌های شناسایی و دفاع در برابر تهدیدات پهپادی از نظر محل قرارگیری

- زمین‌پایه ثابت
- زمین‌پایه متحرک (روی خودرو)
- دستی (قابل‌حمل با دست)
- نصب‌شده بر روی یک پهپاد
- نصب‌شده بر روی چند پهپاد

۱-۵- انواع فناوری‌های شناسایی

از مهم‌ترین فناوری‌های شناسایی پهپادهای مهاجم می‌توان به موارد زیر اشاره کرد:

۱-۵-۱- آکوستیک (صوتی)

حسگرهای آکوستیک یکی از گزینه‌های مطرح برای کشف ریزپرنده‌ها هستند این حسگرها به صداهای محیطی گوش می‌دهند و صدای خاص ریز پرنده‌ها را از میان صداهای موجود تشخیص می‌دهند. حسگر به‌محض آنکه صدایی را می‌شنود آن را با صداهای موجود در بانک داده خود مقایسه می‌کنند تا صدای ریز پرنده را شناسایی و نوع پرنده را تشخیص دهد. در این حالت هشدار امنیتی برای عوامل مربوطه صادر می‌شود. در شرایطی که رادارهای فعال و غیرفعال ناکارآمد هستند می‌توان از حسگرهای آکوستیک در این خصوص استفاده کرد. این حسگرها مقرون‌به‌صرفه بوده و کار با آنها ساده است، البته این حسگرها به‌عنوان تنها گزینه نباید به کار روند و همواره باید در ترکیبی از گزینه‌ها به کار گرفته شوند. چالش‌های پیش روی حسگرهای آکوستیک در این است که باید مبتنی بر بانک داده فعالیت کنند و چنانچه کتابخانه داده آنها به‌روز نباشد قادر به کشف ریز پرنده نخواهند بود در نتیجه به‌روزرسانی کتابخانه حسگر آکوستیک با صداهای ریزپرنده در صنعتی که هر روز نوآوری دارد یک چالش اساسی است که هیچ‌گاه به پوشش ٪۱۰۰ نمی‌رسد (کافی، ۱۴۰۰: ۲۲۰). این فناوری حاوی آرایه‌ای از میکروفون‌ها هستند که پایگاه داده‌ای از صداهای تولیدی از روتورهای پهپادها را دارند و با مقایسه صدای پهپادهای

نزدیک‌شونده با این پایگاه داده، حضور آنها را تشخیص می‌دهند (چیپر و همکاران، ۷:۲۰۲۲). برای شناسایی محل پهپاد به تعداد بیشتری از این میکروفون‌ها نیاز است (همینگا و همکاران: ۲۰۲۲).

۱-۵-۲- سنجنده‌های تصویربرداری

این سنجنده‌ها شامل دو نوع دوربین الکترواپتیکال (EO) و مادون‌قرمز (IR) هستند.

- دوربین اپتیکی (EO): این نوع سنجنده‌ها را می‌توان در کنار سایر سنجنده‌ها نظیر رادار و RF نیز به‌کار برد و با گرفتن تصویر پهپاد، ویژگی‌های آن را تعیین کرد. بزرگ‌ترین مشکل این سنجنده‌ها آن است که در محیط‌های تاریک و مه‌آلود قابلیت استفاده پایینی دارند. به‌علاوه کیفیت تصاویر بستگی دارد به کیفیت لنزها و زاویه تصویربرداری (نیاز ضروری به خط دید).
- دوربین حرارتی: در این روش بر اساس حرارت تولید شده از موتور، باتری و پردازنده‌ها پهپاد شناسایی می‌شود. این روش محدودیت‌هایی شامل محدوده پایین شناسایی و حساسیت‌های محیطی که امکان تشخیص اختلاف دمای پهپاد و محیط اطراف را به وجود می‌آورد، دارد.

۱-۵-۳- رادار (شناسایی بر اساس سطح مقطع راداری)

سامانه‌ای است که از امواج راداری برای شناسایی اشیاء استفاده می‌کند. رادار یک سیگنال ارسال و بازگشت آن را دریافت می‌کند و از این طریق، جهت حرکت، فاصله و موقعیت پهپاد را تعیین می‌کند. بیشتر رادارها برای شناسایی اهداف بزرگ‌مقیاس طراحی شده‌اند و توانایی تشخیص پرنده‌های کوچک را ندارند. راه‌حل راداری یک راه‌حل اکتیو یا عامل است که می‌توان با استفاده از آن، محدوده، زاویه و سرعت پهپاد را شناسایی کرد. رادار شامل فرستنده، گیرنده و پردازنده است (همینگا و همکاران: ۲۰۲۲).

برای انتخاب رادار کشف باید ملاحظات زیر را در نظر گرفت: (کافی،۲۱۹:۱۴۰۰)

- مسافت مورد نیاز برای کشف
- مکان به‌کارگیری رادار
- ابعاد دارایی مورد پوشش
- درجه اهمیت دارایی مورد پوشش به‌منظور تعیین هزینه‌های قابل قبول

می‌توان از ترکیبی از رادارهای فعال و غیرفعال استفاده کرد. رادارهای فعال به‌عنوان گیرنده امواج پراکنده در فضا مانند امواج مخابراتی عمل می‌کنند و از نظر هزینه ابعاد قطعات مکانیکی و نیازهای تعمیراتی در مقایسه با رادارهای فعال در مرتبه پایین‌تری قرار دارند.

۱-۵-۴- تحلیل‌گر امواج رادیویی (RF)

برای کشف ریزپرنده‌ها از سامانه فرکانس رادیویی مانند تحلیلگر طیف فرکانس رادیویی و یا نرم‌افزار استفاده می‌شود تا طیف فرکانسی پرنده کشف شود و لینک بین فرماندهی و کنترل و پرنده و لینک بارگذاری ویدیو مشخص شود. با کشف و لینک فرکانس رادیویی می‌توان به سایر اطلاعات مانند سازنده و پرنده و یا نوع آن پی برد. این اطلاعات در ارزیابی تحلیل بسیار مفید است. بسیاری از سامانه‌های فرکانس رادیویی تنها قادر به کشف پرنده هستند اما با اتکای به راه‌حل‌های فناورانه مانند استفاده از آنتن‌های مولتی استاتیک متعدد می‌توان اطلاعات کاملی شامل مثلث جغرافیایی پرنده و موقعیت کاربر را مشخص نمود (کافی،۲۱۸:۱۴۰۰).

این تحلیل‌گرها شامل یک یا چند آنتن برای دریافت امواج رادیویی است و یک پردازشگر نیز برای تحلیل طیف-های فرکانس‌های رادیویی دارد. در این روش از فرکانس‌های رادیویی (RF) میان پهپاد و پایگاه کنترل آن استفاده می‌شود و سیگنال‌های انتقالی میان پهپاد و کنترل‌کننده آن

شناسایی و تحلیل می‌شود. این سیگنال‌ها گاهی بالارونده و گاهی پایین‌رونده هستند (همینگا و همکاران: ۲۰۲۲).

۱-۵-۵- ترکیبی

۱-۶- مهم‌ترین روش‌های مقابله یا سرنگونی پدافند الکترونیک و پدافند سایبری

مهم‌ترین روش‌های مقابله یا سرنگونی پهپادهای مهاجم عبارتند از:

۱-۶-۱- پالس الکترومغناطیسی (*EMP*)

این سامانه‌ها، پالس الکترومغناطیسی تولید می‌کنند که می‌تواند در تجهیزات الکترومغناطیسی اخلال به وجود آورد. پالس‌های الکترومغناطیسی با لینک‌های رادیویی ایجاد اختلال نموده و گاهی مدارهای الکترونیکی پهپاد را از بین می‌برد. (حتی ممکن است مدارات سایر تجهیزات الکترونیکی پیرامونی را به خاطر ولتاژهای مخرب بالا و جریان‌های الکتریکی زیادی که به وجود می‌آورند از بین ببرد.)

سامانه‌های امواج ماکروویو با انرژی بالا (*HPM*) ممکن است شامل آنتنی برای متمرکز کردن پالس‌های الکترومغناطیسی در یک‌جهت مشخص با هدف کاهش پیامدهای جانبی داشته باشد (همینگا و همکاران: ۲۰۲۲).

۱-۶-۲- لیزر

سامانه‌ای اپتیکی با انرژی بالا که پرتو نور پر انرژی تولید کرده و می‌تواند آسیب جدی به ساختار پهپاد و مدارات الکترونیکی آن وارد نماید.

۱-۶-۳- ایجاد میدان مغناطیسی

این روش به‌تازگی توسط مجموعه‌ای در کشور امارات متحده عربی به‌کار گرفته شده است که طی آن از آهن‌رباهای بسیار قوی برای ایجاد یک میدان مغناطیسی که دور کننده پهپادها می‌باشد استفاده می‌شود (چیپر و همکاران، ۸:۲۰۲۲).

۱-۶-۴- جمر با فرکانس رادیویی (*RF/GSNS*)

جمر با فرکانس رادیویی وسیله‌ای قابل‌حمل است که حجم بالایی از امواج رادیویی را از خود ساطع می‌کند و به سمت هدف می‌تاباند و با این کار، سیگنال‌های مابین کنترل کننده پهپاد و خود پهپاد را مورد اختلال و پوشش قرار می‌دهد. در چنین شرایطی یکی از چهار حالت زیر پدید می‌آید:

- پهپاد یک فرود کنترل شده در موقعیت خود خواهد داشت
- پهپاد به سمت موقعیت از پیش تعیین شده‌اش بازمی‌گردد. (این موقعیت ممکن است موقعیت هدف مورد نظر باشد نه مبدأ اصلی)
- به شکل غیرکنترل شده‌ای به زمین می‌افتد.
- به سمت نامعلومی به شکل غیرکنترل شده‌ای به پرواز درمی‌آید.

۱-۶-۵- فریب‌دهنده‌های سامانه موقعیت‌یاب جهانی (GPS Spoofer)

این سامانه، سیگنال جدیدی را به سمت پهپاد می‌فرستد که ارتباط میان سامانه موقعیت‌یاب جهانی (*GPS*) و ماهواره را جایگزین می‌کند و با این کار، پهپاد دچار فریب شده و به مکان دیگری می‌رود. با تغییر دائمی مختصات جی چی اس پهپاد به‌صورت در لحظه، موقعیت پهپاد توسط فریب‌دهنده کنترل می‌شود و بنابراین می‌توان پهپاد را در نقطه مطلوب فرود آورد (همینگا و همکاران: ۲۰۲۲).

۱-۶-۶- ترکیبی

در این روش، ترکیبی از سامانه‌های یاد شده مورد استفاده و بهره‌برداری قرار می‌گیرند

جدول ۱- ویژگی‌ها و محدودیت‌های روش‌های شناسایی پهپادها (چیپر و همکاران، ۲۰۲۲)، (همینگا و همکاران، ۲۰۲۲)، (پـدرام مزلقانی و همکاران، ۱۳۹۵) (تجمیع و گرداوری شده توسط نگارندگان، ۱۴۰۲)

روش	ویژگی‌ها	محدودیت‌ها
آکوستیک (صوتی)	- از طیف ۲۰ هرتز تا ۲۰ کیلوهرتز را پوشش می‌دهد. - پایگاه داده علائم صوتی دستگاه به‌راحتی قابل به‌روزرسانی است. - سبک‌وزن است و به‌راحتی می‌توان از آن در کنار سایر سنجنده‌ها بهره برد. - توانایی شناسایی پهپادهای خودکار و غیرخودکار را در ارتفاع پایین دارند. - در محیط‌های ناهموار می‌توان آنها را قرار داد و از آنها استفاده کرد. - به‌صورت غیرفعال (پسیو) عمل می‌کنند.	- برد محدود - آسیب‌پذیر در برابر نویزهای محیط (در محیط‌های پر نویز جوابگو نیستند) - مستعد فریب است. - سرعت پایین‌تر نسبت به روش‌های نوری
- تصویربرداری	- کلیه طیف‌های بصری و مادون‌قرمز را پوشش می‌دهد. (۳۰۰ گیگاهرتز - تا ۳ مگاهرتز) - دوربین‌های IR می‌توانند در کلیه شرایط آب و هوایی و شب و روز کار کنند. - می‌توان از فناوری‌های رایانه‌ای نیز کمک گرفت. - امکان تشخیص جهت و سرعت - قابلیت شناسایی محموله پهپادها را دارند. - می‌توانند عکس تهیه کنند و برای تحقیقات بعدی از آنها استفاده شود.	- تصاویر دو بعدی فراهم می‌کنند. - محدودیت عملکرد در شرایط خاص دمایی و آب و هوایی برای دوربین EO - وابستگی به داده‌های زمین‌مرجع - وابستگی به خط دید - به‌تنهایی قابلیت استفاده ندارند. - خطای نسبتاً بالایی دارند.
رادار	- محدوده باند مورد استفاده: ۳۰۰ گیگاهرتز تا ۳ مگاهرتز - کارکرد در کلیه شرایط آب و هوایی و دمایی و شب و روز - سنجش اطلاعات مربوط به‌سرعت هدف - امکان شناسایی علائم ریز - سطح پوشش بالا - دقت بالا - حجم محدود و قابل‌حمل که آن را برای کاربردهای تاکتیکی قابل استفاده می‌کند. - قابلیت اعتماد و اتکاء بالا - برد بالا - رصد دائمی - تعیین موقعیت دقیق - هم‌زمان توانایی شناسایی صدها هدف را دارد - توان شناسایی انواع مختلف پهپادها اعم از خودکار و غیرخودکار را دارد.	- نیاز به سطح مقطع راداری بالا - تشخیص تفاوت پهپادها و پرنده‌ها به‌سختی - محدودیت عملکرد در ارتفاع‌ها و سرعت‌های پایین. - در برخورد با اشیاء کوچک بخصوص پرندگان دچار اختلالاتی می‌شود. - وابستگی به خط دید - هزینه بالا - به‌کارگیری از آن نیازمند مجوز بوده و باید کنترل فرکانسی برای جلوگیری از تداخلات صورت پذیرد.
تحلیل‌گر امواج راداری (RF)	- گرفتن طیف‌های ارتباطی و سیگنال‌های میان پهپاد و اپراتور آن - پیچیدگی پایین و سادگی در اجرا یا پیاده‌سازی - کارکرد در کلیه شرایط آب و هوایی و دمایی و شب و روز - سادگی نصب به خاطر مدولار بودن و دریافت سیگنال‌های دیجیتال - امکان در اختیار گرفتن کنترل خلبان - قیمت نسبتاً پایین - توانایی شناسایی هم‌زمان چند پهپاد - به‌صورت غیرفعال (پسیو) عمل می‌کنند.	- نیاز به دانش مربوط به ارتباطات پهپادی - تشخیص دشوار زاویه رسیدن - عدم امکان استفاده در محیط‌های شهری به خاطر پدیده fading و مسیرهای چندگانه - آسیب‌پذیر در برابر فرکانس‌های رادیویی غیرمجاز که ظرفیت دریافت‌کننده آن را بیش‌ازحد اشغال می‌کند. - تأثیر منفی بر نیروهای خودی - قابلیت آشکارسازی و انهدام با موشک‌ها و پهپادهای ضدتشعشع - عدم امکان شناسایی پهپادهای خودکار - عدم شناسایی همیشه محل دقیق پهپادها - برای محدوده‌های ارتفاعی پایین کاربرد دارد.

جدول ۲- ویژگی‌ها و محدودیت‌های روش‌های مقابله با پهپادها (چیپر و همکاران، ۲۰۲۲)، (همینگـا و همکـاران، ۲۰۲۲)، (پـدرام مزلقانی و همکاران، ۱۳۹۵) (تجمیع و گرداوری شده توسط نگارندگان، ۱۴۰۲)

روش	ویژگی‌ها	محدودیت‌ها
پالس‌های الکترومغناطیسی (EMP)	- می‌تواند مدارها و تجهیزات داخلی پهپادها را بسوزاند. - در دامنه‌های کوتاه و بلند قابلیت استفاده دارد.	- ضروری بودن جهت‌گیری دقیق برای جمینگ - دشوار بودن شناسایی میزان اثرگذاری جمینگ - هزینه بالا - ریسک اختلالات غیرعمدی بسیار بالاست و امکان تخریب تجهیزات الکترونیکی پیرامونی است. - پهپاد خاموش می‌شود و ممکن است در جایی خارج از کنترل نیروهای خودی فرود آید.
لیزر	- در قدرت‌های پایین می‌تواند دوربین پهپاد را از کار بیندازد و در قدرت‌های بالا به‌طورکلی پهپاد را از کار بیندازد. - به‌راحتی می‌توان هدف را دنبال کرد. - امن‌تر از روش‌های فیزیکی حذف یا به‌کارگیری از پرتابه‌هاست. - امکان رهگیری اهداف متعدد - زمان عکس‌العمل پایین - دقت و برد بالا	- حساس به شرایط آب و هوایی - نیاز به اطلاعات دقیق از موقعیت هدف - لیزر با قدرت بالا امکان تداخل با سایر سیستم‌ها را دارد. - هزینه بالا - فناوری بالای لیزر پرتوان - شناسایی آسان توسط دشمن (به دلیل خط آتش مستقیم)
ایجاد میدان مغناطیسی	- مقرون‌به‌صرفه - پاسخگویی در برابر تهدیدات جمعی پهپادها	- کوچک بودن حوزه مورد حفاظت - امکان ایجاد تداخل با سایر سیستم‌ها
جمر با فرکانس رادیویی RF/GNSS	- می‌تواند حمله پهپادهای جمعی که به‌طور هم‌زمان حمله کرده‌اند را خنثی کنند و سیگنال‌های دریافتی آنها را کاهش دهند. - امکان جهت‌دهی و اعمال جمینگ به‌صورت مستقیم در جهت‌های دلخواه	- ناکارآمدی در برابر پهپادهای خودکار - ناکارآمدی در برابر پهپادهایی که سامانه ناوبری داخلی دارند. - ناکارآمدی در برابر پهپادهایی که سامانه ارتباطی رمزنگاری شده دارند. - جوابگویی صرفاً در فواصل کوتاه - امکان ایجاد تداخل با سایر تجهیزات - برد کم - امکان پدید آمدن رفتارهای غیرقابل‌پیش‌بینی برای پهپاد وجود دارد. - امکان برخورد پهپاد به هدف مورد نظر به شکل غیرعامدانه‌ای وجود دارد.
فریب‌دهنده‌های سامانه موقعیت‌یاب جهانی (Spoofing)	- امکان کپی و بازتولید سیگنال‌های ارتباطی با استفاده از الگوریتم‌های هوش مصنوعی و پردازش سیگنال‌های دیجیتال - امکان کشف آسیب‌پذیری‌های سیستم‌های مختلف پهپادی	- نیاز به داشتن تحلیل‌های ثابت و دقیق از فرکانس‌های عملیاتی پهپاد هدف - نیاز به سیستم سنجش طیف‌های مختلف - برد کم - امکان اثرگذاری بر سایر سامانه‌های ارتباطاتی

۲- روش تحقیق

در این پژوهش که در زمره پژوهش‌های کاربردی می‌باشـد و با روش تحلیلی توصیفی به انجام رسـیده اسـت، بـر اسـاس مطالعات مروری اسناد مرتبط، داده‌ها و اطلاعات مـورد نیـاز گردآوری شده است. سپس بر اساس یافته‌ها و تحلیـل‌هـای محقق از یافته‌های تحقیقاتی و کسب نظر از جامعه خبرگان

پژوهش، مؤلفه‌های ارزیابی و اولویت‌بندی راهکارها تعیین گردید. در مرحله بعد با بهره‌گیری از تکنیک تحلیل سلسله‌مراتبی (*AHP*)، این معیارها با کسب نظر مجدد از جامعه خبرگان پژوهش و با بهره‌گیری از نرم‌افزار *Expert Choice11* رتبه‌بندی گردید. در مرحله بعد با اختصاص امتیاز به هریک از راهکارهای شناسایی و مقابله با تهدیدات پهپادی بر اساس مؤلفه‌های تعیین شده و تشکیل رابطه میانگین وزنی برای هریک از راهکارها، امتیاز نهایی هریک از راهکارها تعیین و امکان اولویت‌بندی فراهم می‌گردد.

شایان ذکر است فرایند اختصاص امتیاز به راهکارهای شناسایی و مقابله با تهدیدات پهپادی در بازه‌ای سه‌گانه (کم: ۱، متوسط: ۲ و زیاد: ۳) و بر اساس اطلاعات موجود در منابع تحقیق صورت پذیرفته است. با این تفاسیر رویکرد این تحقیق، آمیخته (کمی-کیفی) بوده است.

با توجه به تخصصی بودن موضوع پژوهش و محدودیت افراد خبره در این زمینه، خبرگان پژوهش به روش نمونه‌گیری هدفمند به تعداد ۱۰ نفر انتخاب شده‌اند.

۳- مؤلفه‌های مؤثر در اولویت‌بندی روش‌های شناسایی و مقابله با تهدیدات پهپادی

با مطالعه و تحلیل اسناد یاد شده در بخش ادبیات پژوهش و همچنین سایر اسنادی که مرتبط با موضوع بوده‌اند و همچنین کسب نظر از خبرگان پژوهش، تعداد ۱۲ مؤلفه به‌عنوان مؤلفه‌های برترساز در انتخاب روش‌های شناسایی و مقابله با تهدیدات پهپادی شناسایی شدند که به شرح زیر می‌باشند:

۱. سرعت واکنش سامانه
۲. هزینه به‌کارگیری سامانه
۳. اثرات جانبی بر تجهیزات و افراد
۴. مهارت لازم جهت به‌کارگیری
۵. امکان شناسایی پهپادهای خودکار (از پیش برنامه‌ریزی شده)
۶. محدوده یا برد عملکرد
۷. عملکرد در شرایط مختلف آب و هوایی و روشنایی
۸. دقت عملکرد
۹. شدت اثر بر هدف
۱۰. امکان فرونشاندن پهپاد
۱۱. قابلیت بومی‌سازی در کشور در زمان کوتاه
۱۲. دسترسی به اطلاعات آشکار و پنهان سامانه

۳-۱- روش *AHP*

فرایند تحلیل سلسله‌مراتبی (*AHP*)، روش تصمیم‌گیری چند معیاره‌ای است که توسط پروفسور ساعتی در دهه ۱۹۷۰ میلادی معرفی گردید (زبردست، ۱۳۸۰). این روش به دلیل ویژگی‌های ریاضی مطلوبی که دارد و این موضوع که اطلاعات ورودی به این روش به‌راحتی به‌دست می‌آید مورد توجه بسیاری از محققان است. این روش از ساختاری چند سطحی و سلسله‌مراتبی از اهداف، معیارها، زیرمعیارها و گزینه‌ها استفاده می‌کند و اطلاعات از مقایسه‌های زوجی به دست می‌آیند (کوسالیا (*Kousalya*) ، ۲۰۱۲).

۳-۲- تشکیل مقایسات زوجی

هنگامی‌که سلسله‌مراتب تشکیل گردید، گام بعدی آن است که اولویت‌های هریک از اجزاء سطوح تعیین گردند. مجموعه‌ای از ماتریس‌های مقایسه‌ای کلیه اجزاء دریک سطح، به‌ترتیب از بالاترین اولویت‌ها ساخته می‌شود. مقایسات بر این اساس شکل می‌گیرد که به‌عنوان نمونه، المان «الف» چه مقدار اهمیت بیشتری نسبت به المان «ب» دارد.

تقدم اهمیت بر اساس جدولی ۹ مقیاسی در جدول ۳ نشان داده شده است.

جدول ۳- مقیاس نه‌تایی شدت اهمیت و توضیحات مربوطه

میزان اهمیت	تعریف
۱	اهمیت برابر
۳	اهمیت نسبتاً بیشتر
۵	اهمیت با شدت بیشتر
۷	اهمیت با شدت خیلی بیشتر
۹	اهمیت فوق‌العاده بیشتر
۲، ۴، ۶، ۸	مقادیر متوسط

فرایند به دست آوردن وزن (ضریب اهمیت) گزینه‌ها نسبت به هریک از زیرمعیارها شبیه تعیین ضریب اهمیت معیارها نسبت به هدف است. در هر دو حالت، قضاوت‌ها بر مبنای مقایسه دودویی معیارها یا گزینه‌ها و بر اساس مقیاس ۹ کمیتی ساعتی صورت پذیرفته و نتیجه در ماتریس مقایسه دودویی معیارها یا گزینه‌ها ثبت شده و از طریق نرمالیزه کردن میانگین هندسی ردیف‌های این ماتریس‌ها، ضرایب اهمیت مورد نظر به‌دست می‌آید. در مقاله حاضر از نرم‌افزار *Expert Choice 11* برای تحلیل ماتریس‌ها استفاده می‌گردد.

اولین گام در اولویت‌بندی روش‌های مقابله با تهدیدات پهپادی رتبه‌بندی مؤلفه‌های بالا بوده که با روش تحلیل سلسله‌مراتبی این اقدام صورت می‌پذیرد.

جدول ۴- جدول خام تحلیل سلسله‌مراتبی

	سرعت واکنش	هزینه	اثرات جانبی	نیاز به مهارت	محدوده یا برد عملکرد	عملکرد در شرایط مختلف آب و هوایی	دقت عملکرد	شدت اثر بر هدف	امکان فرونشاندن پهپاد	قابلیت بومی‌سازی در کشور در زمان کوتاه	دسترسی به اطلاعات آشکار و پنهان سامانه
سرعت واکنش											
هزینه											
اثرات جانبی											
نیاز به مهارت											
محدوده یا برد عملکرد											
عملکرد در شرایط مختلف آب و هوایی											
دقت عملکرد											
شدت اثر بر هدف											
امکان فرونشاندن پهپاد											
قابلیت بومی‌سازی در کشور در زمان کوتاه											
دسترسی به اطلاعات آشکار و پنهان سامانه											

۴- ویژگی‌های جامعه خبرگان

با توجه به تخصصی بودن موضوع روش‌های شناسایی و مقابله با تهدیدات پهپادی از افراد مطلع و صاحب‌نظر در این زمینه کسب نظر گردید. لذا همان‌طور که پیش‌تر نیز اشاره شد روش انتخاب جامعه خبرگان، روش نمونه‌گیری هدفمند قضاوتی بوده است. ویژگی‌های جامعه خبرگان پژوهش به شکل زیر است:

- تعداد: ۱۰ نفر
- جنسیت: ۱۰ نفر مرد- صفر نفر زن
- مدرک تحصیلی: ۷ نفر دکتری- ۳ نفر کارشناسی ارشد
- تخصص: ۵ نفر حوزه دفاع الکترونیک - ۳ نفر حوزه حفاظت از زیرساخت‌های حیاتی- ۲ نفر حوزه دفاع سایبری

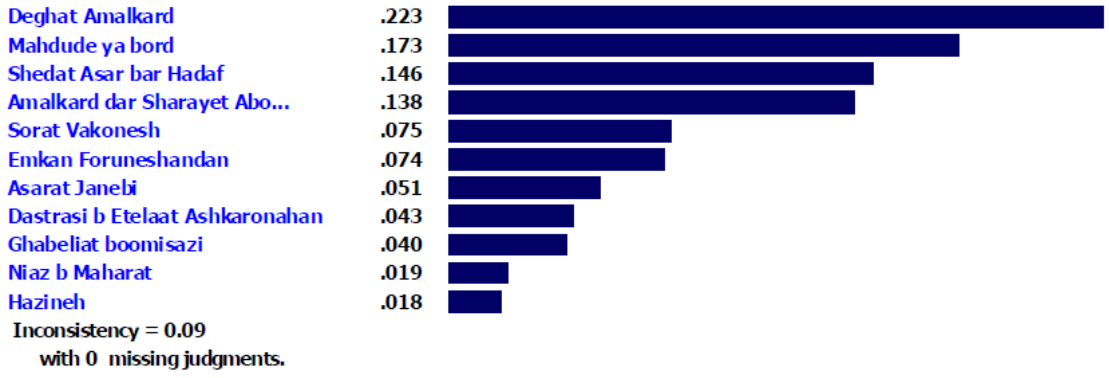
نتیجه تحلیل سلسله‌مراتبی صورت گرفته با استفاده از نرم‌افزار *Expert Choice11* به‌قرار زیر است:

در این تحلیل ضریب ناسازگاری ۰/۰۹ بوده و ازآنجاکه کمتر از ۰/۱ می‌باشد مورد تائید می‌باشد؛ بنابراین اولویت‌بندی معیارهای تعیین شده به‌صورت زیر است:

بر این اساس، دقت عملکرد سامانه با اختلاف معناداری بالاترین درجه اهمیت را نسبت به سایر معیارها دارد. بدین معنا که سامانه باید کمترین خطا را داشته و به شکل دقیقی ویژگی‌های پهپاد مهاجم را شناسایی نماید. پس از آن، معیار محدوده یا برد عملکردی سامانه می‌باشد که هر اندازه بیشتر باشد بهتر است. شدت اثرگذاری سامانه مقابله با هدف نیز حائز سومین رتبه اهمیت می‌باشد. دو معیار هزینه و نیاز به مهارت نیز به‌ترتیب حائز کمترین امتیازها می‌باشند. تفسیر این موضوع آن است که برای تأمین امنیت یک زیرساخت حیاتی در برابر تهدیدات پهپادی موضوع هزینه در برابر آنچه به دست می‌آید موضوع کم‌اهمیتی است. نیاز به مهارت کاربران نیز موضوعی نیست که به خاطر آن نوع سامانه شناسایی و مقابله نیاز به تغییر داشته باشد.

جدول ۵- رتبه‌بندی معیارهای رتبه‌بندی روش‌های شناسایی و مقابله با تهدیدات پهپادی

ردیف	رتبه‌بندی	امتیاز
۱	دقت عملکرد	۰/۲۲۳
۲	محدوده یا برد عملکرد	۰/۱۷۳
۳	شدت اثر بر هدف	۰/۱۴۶
۴	عملکرد در شرایط مختلف آب و هوایی و روشنایی	۰/۱۳۸
۵	سرعت واکنش	۰/۰۷۵
۶	امکان فرونشاندن پهپاد	۰/۰۷۴
۷	اثرات جانبی	۰/۰۵۱
۸	دسترسی به اطلاعات آشکار و پنهان سامانه	۰/۰۴۳
۹	قابلیت بومی‌سازی در کشور در زمان کوتاه	۰/۰۴
۱۰	نیاز به مهارت	۰/۰۱۹
۱۱	هزینه	۰/۰۱۸



نمودار ۱- نمودار میله‌ای رتبه‌بندی معیارهای رتبه‌بندی

در مرحله بعد، هریک از سامانه‌های معرفی شده در بخش اول پژوهش بر اساس معیارهای یاد شده امتیازدهی شده و امتیاز کلی هر روش بر اساس حاصل‌ضرب ضریب اهمیت معیار در امتیاز اختصاص داده شده به آن معیار برای هریک از روش‌ها محاسبه می‌گردد.

۵- تجزیه‌وتحلیل یافته‌ها

۵-۱- امتیازدهی به روش‌های شناسایی تهدیدات پهپادی

در این بخش بر اساس یافته‌های حاصل از ادبیات پژوهش به هریک از روش‌های شناسایی تهدیدات پهپادی امتیازی از ۱ تا ۳ اختصاص داده می‌شود. به‌نحوی‌که ۳ مناسب‌ترین وضعیت و ۱ نامناسب‌ترین وضعیت می‌باشد.

۵-۲- محاسبه امتیازات

۵-۲-۱- روش‌های شناسایی

=آکوستیک
3*0.075+3*0.018+3*0.051+3*0.019+1*0.173+1*0.138+1*0.223+3*0.04+3*0.043=1.27

= تصویربرداری
3*0.075+2*0.018+3*0.051+3*0.019+2*0.173+3*0.138+2*0.223+3*0.04+3*0.043=1.93

جدول ۶- امتیازات اتخاذ داده شده به هریک از روش‌های شناسایی پهپادها

	سرعت واکنش	هزینه	اثرات جانبی	نیاز به مهارت	محدوده یا برد عملکرد	عملکرد در شرایط مختلف آب و هوایی	دقت عملکرد	قابلیت بومی‌سازی در کشور در زمان کوتاه	دسترسی به اطلاعات آشکار و پنهان سامانه
آکوستیک (صوتی)	۳	۳	۳	۳	۱	۱	۱	۳	۳
تصویربرداری	۳	۲	۳	۳	۲	۳	۲	۳	۳
رادار	۳	۱	3	۱	۳	۳	۳	۳	۳
RF	۲	۱	۲	۱	۲	۳	۱	۳	۳

جدول ۷- امتیازات اتخاذ داده شده به هریک از روش‌های مقابله با پهپادها

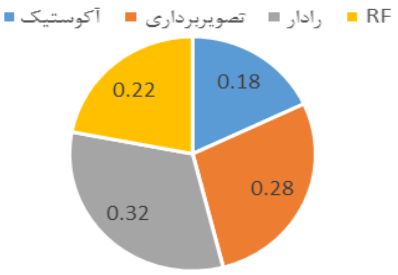
	سرعت واکنش	هزینه	اثرات جانبی	نیاز به مهارت	محدوده یا برد عملکرد	عملکرد در شرایط مختلف آب و هوایی	دقت عملکرد	شدت اثر بر هدف	امکان فرونشاندن پهپاد	قابلیت بومی‌سازی در کشور در زمان کوتاه	دسترسی به اطلاعات آشکار و پنهان سامانه
پالس‌های الکترومغناطیسی (EMP)	۲	۱	۱	۱	۳	۳	۲	۳	۲	۳	۲
لیزر	۳	۱	۱	۱	۳	۱	۳	۳	۱	۲	۲
ایجاد میدان مغناطیسی	۱	۳	۱	۳	۱	۳	۲	۳	۲	۲	۱
جمینگ RF/GNSS	۲	۱	۱	۱	۲	۳	۱	۲	۳	۳	۱
اسپوفینگ (Spoofing)	۲	۲	۱	۱	۲	۲	۳	۲	۳	۳	۳

رادار
=3*0.075+1*0.018+3*0.051+3*0.019+3*0.127+3*0.138+3*0.223+3*0.04+3*0.043= 2.27
RF
=2*0.075+1*0.018+2*0.051+1*0.019+2*0.127+3*0.138+1*0.223+3*0.04+3*0.043= 1.52

در این مرحله به‌منظور نرمال‌سازی اعداد به‌دست‌آمده، جمع جبری کلیه امتیازات محاسبه شده و امتیاز هر روش تقسیم بر جمع جبری به‌دست‌آمده شده تا امتیاز نرمال شده هر روش به دست آید. جمع جبری امتیازات نرمال شده باید عدد ۱ باشد.

جدول ۸- امتیازات نرمال شده روش‌های شناسایی پهپادها

نام روش	امتیاز خام	امتیاز نرمال شده
آکوستیک	۱,۲۷	۰,۱۸
تصویربرداری	۱,۹۳	۰,۲۸
رادار	۲,۲۷	۰,۳۲
RF	۱,۵۲	۰,۲۲
مجموع	۶,۹۹	۱



نمودار۲- امتیاز نرمال شده روش‌های شناسایی

نتایج حاصل از این جدول بیانگر آن است که روش‌های شناسایی مبتنی بر رادار، بهترین روش برای شناسایی پهپادها می‌باشد؛ زیرا این روش علاوه بر آنکه توانایی شناسایی پهپادهای خودکار را دارد، دقت عملکردی بالایی نیز داشته و در کشور امکان ساخت آن وجود دارد. نکته قابل‌تأمل آن است که پهپادهای کوچک یا ریزپرنده‌ها با رادارهای اختصاصی و سه‌بعدی باید شناسایی شوند. پس از آن روش‌های تصویربرداری اپتیکال و حرارتی در رتبه بعدی قرار دارند و روش آکوستیک یا سنجنده‌های صوتی حائز پایین‌ترین امتیاز می‌باشد که عمده علت آن دقت و برد عملکردی پایین می‌باشد.

۵-۲-۲- روش‌های مقابله

پالس‌های الکترومغناطیسی
=2*0.075+1*0.018+1*0.051+1*0.019+3*0.127+3*0.138+2*0.223+3*0.146+2*0.074+3*0.04+2*0.043=2.41
لیزر =
3*.075+1*0.018+1*.051+1*0.019+3*0.127+1*0.138+3*0.223+3*0.146+1*0.074+2*0.04+2*0.043=2.32
ایجاد میدان الکترومغناطیسی =
1*0.075+3*0.018+1*0.051+3*0.019+1*0.127+3*0.138+2*0.223+3*0.146+2*0.074+2*0.04+1*0.043= 1.98
جمینگ =
2*.075+1*0.018+1*0.051+1*0.019+2*0.127+3*0.138+1*0.223+2*0.146+3*0.074+3*0.04+1*0.043= 1.9
اسپوفینگ =
2*.075+2*0.018+1*0.051+1*0.019+2*0.127+2*0.138+3*0.223+2*0.146+3*0.074+3*0.04+3*0.043= 2.31

جدول ۹- امتیازات نرمال شده روش‌های مقابله با پهپادها

نام روش	امتیاز خام	امتیاز نرمال شده
پالس‌های الکترومغناطیسی	۲,۴۱	۰,۲۲
لیزر	۲,۳۲	۰,۲۱
ایجاد میدان مغناطیسی	۱,۹۸	۰,۱۸
جمینگ	۱,۹	۰,۱۷
اسپوفینگ	۲,۳۱	۰,۲۱
مجموع	۱۰,۹۱	۱

نمودار۳- امتیاز نرمال شده روش‌های مقابله

نتـایج حاصـل از ارزیـابی جـدول روش‌هـای مقابلـه با تهدیدات پهپـادی حـاکی از آن اسـت کـه بهـره‌گیـری از پالس‌های الکترومغناطیسی (*EMP*) بهترین روش مقابلـه بـا تهدیدات پهپادی می‌باشد؛ زیرا این روش علاوه بر آنکه برای مقابله با پهپادهای خودکار و غیرخودکار مناسب است، امکان انجام حملات فوجی یا سوارمینگ (*Swarming*) را از دشمن گرفته و امنیت خوبی را برای زیرسـاخت فـراهم مـی‌آورنـد. روش جمینگ از آنجا که صـرفاً بـرای مقابلـه بـا پهپادهـای غیرخودکار طراحی شده، حائز کمترین امتیـاز بـوده و روش ایجاد میدان الکترومغناطیسی نیز محدوده اثـر بسـیار کـم و سطح اثرگذاری غیرروشنی را دارد.

۶- نتیجه‌گیری

پژوهش حاضر با هدف شناسایی و اولویت‌بندی روش‌های شناسایی و مقابله با تهدیدات پهپادی به انجام رسید. در نتیجه انجام بخش مروری این پژوهش، شناخته‌شده‌تـرین روش‌هـای شناسایی و مقابله بـا تهدیـدات پهپـادی از معتبرتـرین منـابع معرفی و مزایا و معایب هریک از آنها بیان گردید. در ادامه طی یک فرایند تحلیل محتوا، ۱۱ معیار برای رتبـه‌بنـدی روش‌هـا تدوین و با بهره‌گیری از روش تحلیل سلسله‌مراتبی رتبه‌بنـدی گردیدنـد. در نتیجـه ایـن تحلیـل مشـخص گردیـد از میـان معیارهای متفاوتی کـه بـرای انتخـاب سـامانه‌هـای شناسـایی و مقابلـه بـا تهدیـدات پهپـادی پـیش روی تصـمیم‌سـازان و تصمیم‌گیران این حوزه در زیرساخت‌های مختلف وجـود دارد، دقت عملکردی این سامانه‌ها، محدوده یا برد عملکردی آنهـا و همچنین شدت اثرگذاری بر هدف، حـائز بیشـترین اهمیـت و هزینه سامانه حائز کمترین اهمیت می‌باشند. سپس هریـک از روش‌هـای شناسـایی و مقابلـه در جـداولی مجـزا امتیـازدهی شدند. از حاصل‌ضرب امتیازهای به‌دست‌آمده در وزن معیارهـا، امتیاز نهایی هر روش اکتساب گردید. بر ایـن اسـاس از میـان روش‌های متعدد شناسایی و مقابلـه بـا تهدیـدات پهپـادی در حوزه پدافند الکترونیک و پدافند سایبری، در حوزه شناسـایی بهره‌گیری از سامانه‌های راداری بهترین روش بـرآورد گردیـد. همچنـین روش سـنجنده‌هـای صـوتی یـا آکوسـتیک نیـز پایین‌ترین امتیاز را کسب نمود.

در حوزه مقابله نیز بهره‌گیری از پـالس الکترومغناطیسـی بهترین روش مقابله با تهدیدات پهپـادی تشـخیص داده شـد. روش جمینگ نیز هرچنـد روشـی مرسـوم و قـدیمی در ایـن حوزه محسوب می‌شود اما از آنجا که کارایی چنـدانی در برابـر پهپادهای خودکار ندارد، حائز کمترین امتیاز می‌باشـد. نتیجـه عملیاتی محقق از این پژوهش آن است که باید از سامانه‌هـای شناسایی و مقابله ترکیبی استفاده نمود؛ یعنی سـامانه حـاوی حـداقل دو روش بـرای شناسـایی و دو روش بـرای مقابلـه بـا تهدیدات پهپادی باشد.

۷- مراجع

پدرام، عبدالرحیم؛ احمدیان، مهدی؛ امیرمزلقانی، یوسف (۱۳۹۷). آینده‌پژوهی در حوزه محصولات ضد پهپاد با استفاده از اولویت‌گذاری پابرجا .*آینده‌پژوهی دفاعی، شماره ۱۱، ۱۴۳-۱۶۴*

حبیبی، نیک‌بخش (۱۳۹۳). *پهپاد در عملیات هوایی*. تهران: انتشارات راهبردی نهاجا.

خرم فعال، حسین (۱۳۹۹). *تهدیدات ریزپرنده‌ها و راه‌های مقابله با آن. معاونت آموزش و پژوهش ستاد کل نیروهای مسلح*

رستمی، محمد (۱۳۹۱). آشنایی با هواپیماهای بدون سرنشین (پهپاد) .تهران: انتشارات مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی.

زبردست، ا. (۱۳۸۰). کاربرد فرایند تحلیل سلسله‌مراتبی در برنامه‌ریزی شهری و منطقه‌ای، نشریه هنرهای زیبا، شماره ۱۰، تهران.

شکوهی، حسین (۱۳۹۲). نقش *پهپادها در جنگ‌های آینده (صحنه نبرد ناهمگون)* .تهران: دانشگاه عالی دفاع ملی.

فرحبخت، احمدرضا؛ دهقانی، مهدی (۱۳۹۸). همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی. *فصلنامه امنیت ملی، شماره ۳۱*، ۱۹۹-۲۱۹.

کافی، سعید (۱۴۰۰). درس آموخته‌های جنگ قره‌باغ. تهران: دانشگاه جامع امام حسین علیه‌السلام.

کاظمی، حمید؛ و الهیان، سمانه (۱۳۹۹). توسعه پهپادهای غیرنظامی و چالش‌های پیش روی آن. فصلنامه فناوری در مهندسی هوافضا، ۴۵-۶۴.

نوروزی، احمد (۱۳۹۴). بررسی حملات الکترونیکی علیه پهپادها. *چهارمین همایش سراسری علوم و مهندسی دفاعی در سپاه*. تهران.

Brust, M., Danoy, G., Bouvry, P., Gashi, D., Pathak, H., & Gonc¸alves, M. (2018). Defending against Intrusion of Malicious UAVs with Networked UAV Defense Swarms.

Chiper, F.-L., Martian, A., Vladeanu, C., Marghescu,, I., Craciunescu, R., & Fratu, O. (2022). Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution. *Sensors*.

Farlik, J., Kratky, M., Casar, J., & Stary, V. (2019). Multispectral Detection of Commercial Unmanned Aerial Vehicles. *Sensors*.

Hamminga, S., Claasen, T. & Verdonk, M. (2022). *Counter-Drone Technologies to Detect and Stop Drones Today. Retrieved from*: https://www.robinradar.com/

Holland, M.A. (2018). Counter-Drone Systems. Center for the Study of the Drone at Bard College, Feburary http://dronecenter.bard.edu/counter-drone-systems./

Kratky, M., & Farlik, J. (2018). Countering UAVs – the Mover of Research in Military Technology. *Defence Science Journal*, 460-466.

Kousalya, P. (2012). Analytical Hierarchy Process approach – An application. Mathematica Aeterna, 2(10), 861-878.