دانشگاه صنعتی امیرکبیر

دانشکده مهندسی برق

پایان نامه کارشناسی ارشد

عنوان:

طراحی سیستمی بخش باند پایه گیرنده تشخیص سیگنال باند وسیع

نگارش:

محمدرضا غفوری فرد

استاد راهنما:

جناب آقای دکتر حسن غفوری فرد

استاد مشاور:

جناب آقای دکتر ایاز قربانی

بهمن ۱۳۸۶

بسمه تعالی

شماره:

تاریخ:

فرم پروژه تحصیلات تکمیلی ۱

پیشنهاد پروژه تحصیلات تکمیلی

(رساله کارشناسی ارشد و دکترا)

۱- مشخصات دانشجو

نام و نام خانوادگی: **محمدرضا غفوری فرد** شماره دانشجوئی :**۸۴۲۲۳۱۰۱**

رشته تحصیلی: **الکترونیک** دانشکده: **برق**

آدرس: **پاسداران : بوستان ۱۰ – پلاک ۳۱** تلفن : **۲۲۵۸۷۷۳۵** مقطع: **کارشناسی ارشد**

۲-مشخصات استاد راهنمای اول

نام و نام خانوادگی: **دکتر حسن غفوری فرد** سمت، مرتبه علمی و محل خدمت: **دانشیار دانشکده برق ، دانشگاه صنعتی امیر کبیر**

آدرس: **پاسداران : بوستان ۱۰ – پلاک ۳۱**

تلفن:

۳-مشخصات استاد راهنمای دوم

نام و نام خانوادگی: سمت، مرتبه علمی:

تلفن :

۴-عنوان پایان نامه یا رساله

فارسی: طراحی سیستمی گیرنده تشخیص سیگنال باند وسیع

انگیسی: Systematic Design of A Wide Band Signal Classifier Receiver

نوع پروژه: کاربردی * ☐ بنیادی ☐ توسعه ای ☐ تعداد واحد ٦ ☐

۵- کلمات کلیدی فارسی: گیرنده پهن باند، شناسایی سیگنال، فرکانس یابی، آنالیز پالس

کلمات کلیدی انگلیسی: **Wide Band Receiver, Signal Classification, Frequency Measurement, Pulse Analysis**

***توضیحات:** لطفا تایپ شود.

چکیده

با توجه به گسترش انواع فرستنده‌های فرکانس بالا، امروزه تحقیقات وسیعی در جهت ساخت سیستم-های شناسایی متنوع انجام می‌پذیرد. کارکردهای اصلی یک سیستم شناسایی، آشکار سازی و تفکیک سیگنال‌های فرستنده‌های مختلف می‌باشد. اطلاع از وجود فرستنده‌ها و همچنین نوع سیگنال ارسالی آن‌ها به‌ویژه در مورد فرستنده‌های پالسی، اطلاعات بسیار حیاتی می‌باشند. فرستنده‌های پالسی عمدتاً در رادارها کاربرد دارند و به همین سبب از نظر استراتژیک، شناسایی و تفکیک فرستنده‌های پالسی منجر به شناسایی و تفکیک رادارهای موجود در منطقه می‌گردد. با توجه به تنوع فرکانسی این‌گونه فرستنده‌ها، لزوماً سیستم-های گیرنده باید در طیف فرکانسی وسیعی قابلیت فعالیت داشته باشند. به همین جهت در این پایان نامه طراحی و ساخت یک سیستم گیرنده تشخیص سیگنال باند وسیع انجام گرفت.

برای درک بهتر سیستم‌های شناسایی رادار، لازم است ابتدا با سیگنال‌های راداری و همچنین مشخصات این سیگنال‌ها، آشنایی پیداکرد. لذا در این پایان نامه علاوه بر مطالعه سیستم‌های راداری، انواع سیگنال‌های راداری، پارامترهای مختلف سیگنال‌های راداری و روش‌های آشکارسازی این پارامترها مورد بررسی قرارگرفت. به علاوه، برای درک بهتر از سیستم‌های راداری، یک نرم افزار شبیه ساز پالس‌های راداری نوشته شد. پالس راداری تولید شده توسط این شبیه ساز می تواند به برنامه شبیه ساز واحد استخراج پارامترهای پالس داده شود تا پالس به طور کامل بازشناسی شود.

در نهایت، نتایج اندازه گیری به دست آمده از ساخت سیستم در انتهای پایان نامه همراه با نمودارهای تولید شده آورده شده است.

فصل اول

مروری بر جنگ الکترونیک و سیستم های گیرنده سیگنال راداری

در این فصل با نگاهی کلی به جنگ الکترونیک و تعریف تقسیم بندی‌های آن، جایگاه سیستم-های گیرنده تشخیص سیگنال راداری در جنگ الکترونیک تبیین می‌شود. به علاوه نگاهی کلی به انواع این سیستم‌ها و کاربردهای هریک انجام می‌گیرد.

۱-۱- جنگ الکترونیک

جنگ الکترونیک[1] رویکردی سیستمی است برای به کارگیری و کنترل طیف الکترومغناطیسی در جهت مقابله با سیستم‌های مخابراتی دشمن. استفاده دشمن از طیف فرکانسی برای ایجاد ارتباطات مخابراتی، ناوبری و رادار می‌تواند با به کارگیری تکنیک‌ها و فناوری سیستم‌های الکترومغناطیسی به چالش کشیده شود. در کاربرد نظامی، جنگ الکترونیک ابزاری است برای مقابله با فعالیت‌های دشمن که از طیف الکترو مغناطیسی در آن‌ها استفاده می‌شود.

جنگ الکترونیک فضای الکترومغناطیسی را به وسیله حس کردن و تحلیل نحوه استفاده دشمن از طیف الکترومغناطیسی به کار می‌گیرد و اقدامات متقابلی را در جهت ناتوان ساختن دشمن در استفاده از طیف به اجرا در می‌آورد [۱].

سنسورهای جنگ الکترونیک وسیله‌ای هستند که به کمک آن‌ها نیروهای نظامی به جمع‌آوری اطلاعات تاکتیکی می‌پردازند. این سنسورها به همراه ضد اقدامات جنگ الکترونیک[2] کارایی سلاح-های کنترل شده به وسیله الکترو اپتیک/ طیف مادون قرمز و فرکانس رادیویی دشمن را کاهش می-دهند [۲].

نیروهای زمینی، دریایی و هوایی طیف فرکانسی را برای فرمان، کنترل، هدف قراردادن و هدایت سلاح‌ها به کار می‌گیرند.

جنگ الکترونیک، سه حوزه عملیاتی زیر را شامل می‌شود [۴-۳]:

---

[1]. Electronic Warfare (EW)
[2]. EW Countermeasures

- حمایت الکترونیکی[1]: اطلاعات مختلفی را که از تشعشعات الکترومغناطیسی محیط به دست آورده می‌شوند، جهت تحلیل در اختیار قرار داده تا با استفاده از آن‌ها نیروی رزمی در میدان نبرد حمایت شود.
- حمله الکترونیکی[2]: با استفاده از داده‌های جمع‌آوری شده از سیستم‌های حمایت الکترونیک، امکان ایجاد انواع اختلال و حملات الکترونیک، همچنین به کارگیری آتش را فراهم می‌سازد.
- حفاظت الکترونیکی[3]: تجهیزات و سکّوهای خودی را از تهدیدهایی که به صورت الکترونیکی کنترل می‌شوند، حفاظت می‌کند.

اینک به شرح هر یک از کارکردهای ذکر شده در بخش قبل می‌پردازیم.

۱-۱-۱- حمایت الکترونیکی (ES)

حمایت الکترونیکی به آن بخش از جنگ الکترونیک گفته می‌شود که در برگیرنده فعالیت‌هایی است که مستقیماً تحت هدایت نیروی عملیاتی برای شنود، شناخت و تعیین موقعیت منابع دشمن به کمک انرژی الکترومغناطیسی تشعشع شده آن انجام می‌گیرد. داده‌های به دست آمده از حمایت الکترونیکی ، اطلاعاتی در زمان مناسب در اختیار نیروی کاربر قرار می‌دهد که آن نیرو بر مبنای آن می‌تواند تصمیمات لازم را اتخاذ نماید. حمایت الکترونیکی به عنوان یکی از منابع جنگ اطلاعاتی، بر نیازهای اضطراری اپراتور تمرکز می‌کند تا نیت دشمن و اطلاعات هدف را به دست آورد. حمایت الکترونیکی به نوبه خود از چهار کارکرد پایه‌ای تشکیل شده است:

[1]. Electronic Support (ES)
[2]. Electronic Attack (EA)
[3]. Electronic Protection (EP)

- شنود[1]
- شناسایی[2]
- بهره برداری[3]
- تعیین موقعیت[4]

شنود تشعشعات ارتباطی و غیرارتباطی دشمن یکی از کارکردهای اصلی حمایت الکترونیکی است. این عمل خود از دو گام تشکیل شده است. ابتدا، اپراتور باید قابلیت بازشناسی سیگنال موردنظر را چه در یک جستجوی عمومی و چه در یک فرکانس مشخص داشته باشد. سپس، هنگامی که سیگنال مطلوب یافته شد، اپراتور باید به سرعت جهت ضبط سیگنال اقدام نماید و یا پارامترهای اندازه‌گیری شده آن ذخیره کند. (این امر می‌تواند به صورت خودکار و بدون هدایت اپراتور نیز انجام شود.)

کارکرد شناسایی در بر گیرنده شناسایی و طبقه‌بندی تشعشعات ارتباطی و غیر ارتباطی بر مبنای اندازه‌گیری‌های انجام گرفته روی پارامترهای خاص می‌باشد.

نتایج بهره‌برداری برای تعیین جهت آنتن‌های ایجاد اختلال (برای عملیات حمایت الکترونیکی یا حمله الکترونیکی)، حمایت از آتش به وسیله عناصر نبرد و توسعه اطلاعات در مورد موقعیت میدان جنگ استفاده می‌شود.

در تعیین موقعیت، با استفاده از سامانه‌های جهت یاب[5]، تجهیزات تابش کننده شناسایی می‌شود. جهت یاب مسؤولیت تعیین جهت سیگنال رادیویی دریافتی را به عهده دارد.

---

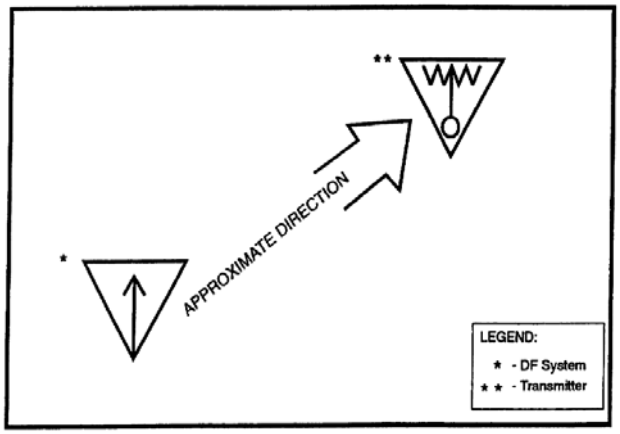
[1] . Intercept
[2] . Identify
[3] . Exploit
[4] . Locate
[5] . Direction Finding (DF)

عملیات جهت یابی نیازمند وجود پایگاه‌های متعدد درطول یک خط مبنا[1] می‌باشد. خط مبنای جهت یابی یک خط یا محور فرضی است که تجهیزات DF یک شبکه جهت یاب در طول آن قراردارند. طول خط مبنا فاصله مستقیم بین دو سامانه جهت یاب بیرونی‌تر در یک پایگاه است.

عمقی که در آن یک شبکه جهت یاب می‌تواند به صورت مؤثر موقعت فرستنده‌های دشمن را تشخیص دهد توسط طول خط مبنا مشخص می‌شود.

نقشه‌های به کارگیری و جابجایی واحدهای خودی که در منطقه عملیات آنها سامانه DF ایجاد شده است، به کارگیری تجهیزات این سامانه را تحت تاثیر قرار می‌دهد. ناحیه هدفی که قرار است آشکار شود، چیدمان خط مبنا را به نوعی دیکته می‌کند.

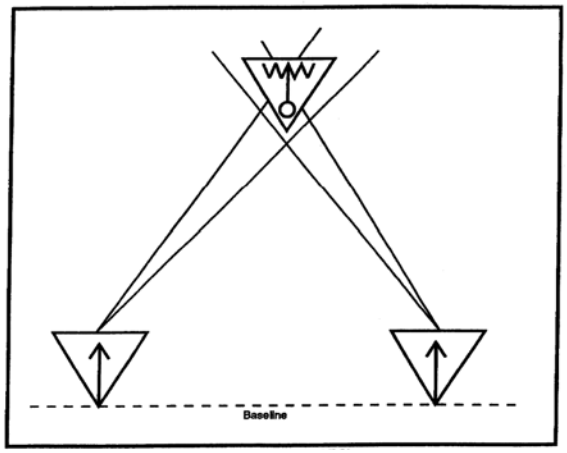
با استفاده از یک پایگاه DF زمینی، همان‌گونه که در **شکل ۱-۱** نشان داده شده است، خط زاویه به دست می‌آید که جهت فرستنده دشمن را نمایان می‌سازد.



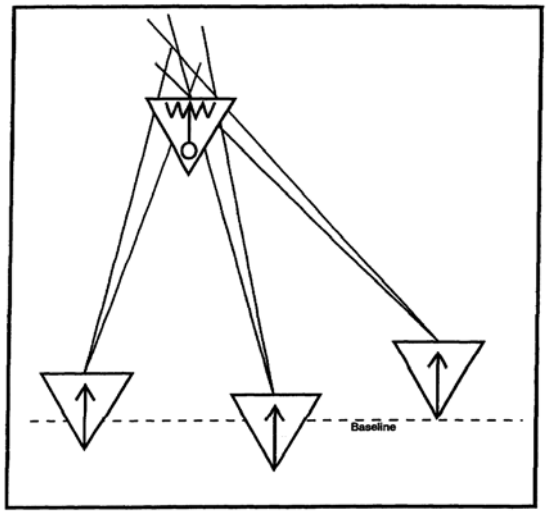
شکل ۱-۱: خط مبنا [۳]

[1] . Baseline

تخمین موقعیت[1] با استفاده از دو یا چند سامانه DF به کمک روش مثلثی امکان‌پذیر است. همان‌گونه که در **شکل ۱-۲** مشاهده می‌شود، مکان احتمالی فرستنده هدف، از تقاطع خطوط زاویه دو سامانه جهت‌یاب قابل استحصال است. اگر در تعیین موقعیت از سه سامانه جهت‌یاب استفاده شود، موقعیت با دقت بیشتری تعیین می‌شود. این امر در **شکل ۱-۳** به تصویر کشیده شده است.



شکل ۱-۲: دو سایت زمینی DF [۳]



شکل ۱-۳: سه سایت زمینی DF [۳]

[1] . Position Finding (PF)

همان‌گونه که پیش از این ملاحظه گردید، حمایت الکترونیک می‌تواند قابلیت شنود، شناسایی و تعیین موقعیت فرستنده‌های دشمن را در اختیار نیرو قرار دهد. این سیستم‌ها منبع اطلاعاتی مفیدی برای ایجاد اختلال، حفاظت خودی، هدف قراردادن و سایر کاربردهای نیروهای رزمی هستند. حمایت الکترونیک اختلال و نابودی فرامین، هدایت و ارتباطات دشمن را از طریق جمع-آوری و گزارش داده‌های هدف مهیا می‌سازد.

۱-۱-۲- حمله الکترونیکی (EA)

میزان اثرگذاری جنگ الکترونیک به درجه یکپارچگی آن با سیستم آتش بستگی دارد. حمله الکترونیک هنگامی که همراه با آتش به کار گرفته شود، اثرگذاری بیشتری خواهد داشت.

حمایت آتش نیازمند تعیین موقعیت دقیق‌تر هدف است لذا برای برخی اهداف، اختلال وسیله حمله مناسب‌تری به‌نظر می‌رسد. سایر عملیات‌های حمله الکترونیک در جهت برهم زدن فرامین و هدایت دشمن برنامه‌ریزی می‌شوند. تهیه اطلاعات از میدان نبرد درسرتاسر فرآیند برنامه‌ریزی حمله الکترونیکی استفاده می‌شود.

اقدامات متقابل فرمان، هدایت و ارتباطات[۱]، بخش‌های جدانشدنی از حمله الکترونیک هستند. عملیات امنیتی، اختلال و تخریب فیزیکی که به وسیله داده‌های جمع‌آوری شده قابل اجرا می‌باشند در جهت ممانعت از انتقال ارتباطات و یا کم اثر کردن فرامین، هدایت و یا ارتباط دشمن مورد استفاده قرار می‌گیرند.

حمله الکترونیک فرستنده‌های تهدیدکننده و سامانه‌های جمع‌آوری اطلاعات را مختل و یا کم اثر می‌کند. دو بخش حمله الکترونیک یعنی اختلال الکترومغناطیسی[۲] و فریب الکترومغناطیسی[۳]

[1] . Command, Control and Communications (C3)
[2] . Electromagnetic Jamming
[3] . Electromagnetic Deception

تنوع وسیعی از تجهیزات و تکنیک‌ها را پوشش می‌دهند. اختلال و فریب هنگامی که با هم به طور صحیح آمیخته شوند می‌توانند فرمان، هدایت و ارتباط دشمن را برهم بزنند.

اختلال الکترومغناطیسی عبارت است از تابش یا بازتابش انرژی الکترومغناطیسی برای ممانعت از یا کاهش دریافت اطلاعات توسط یک گیرنده. گیرنده‌های رادیویی و رادارهایی که در یک فرکانس داده شده، تنظیم شده‌اند به وسیله تابش توان بالاتر از دریافت سیگنال اصلی باز می‌مانند و بدین - وسیله مختل می‌شوند. به طور کلی میزان اثرگذاری اختلال به توان نسبی بین فرستنده و اخلال‌گر، فاصله نسبی بین فرستنده، اخلال‌گر و گیرنده و این‌که آیا گیرنده از آنتن جهت‌دار استفاده می‌کند یا نه بستگی دارد.

اختلال الکترومغناطیسی خود به سه گروه تقسیم می‌شود [۳-۵]:

- تابش[۱]
- تابش مجدد[۲]
- بازتابش[۳]

اختلال به وسیله تابش، آن دسته از تجهیزاتی را در بر می‌گیرد که انرژی الکترومغناطیسی ساطع می‌کنند. برای این کار تکنیک‌های مختلفی وجود دارد که به اختصار به آن‌ها می‌پردازیم.

- اختلال سد: این تکنیک عبارت است از اختلال تعدادی کانال مجاور و یا محدوده‌ای مشخص از طیف فرکانسی به طور همزمان. اختلال‌گرهای سد، توان بالایی را در یک محدوده وسیع فرکانسی تابش می‌کنند.

[1] . Radiation
[2] . Reradiation
[3] . Reflection

- اختلال موضعی: در این تکنیک، تنها یک فرکانس مشخص مورد اختلال قرار می‌گیرد.از آن‌جا که اختلال موضعی کمترین تزاحم و تداخل را با فرستنده‌های خودی ایجاد می-کند، این نوع اختلال پرکابرد ترین تکنیک در میان سایر روش‌های اختلال است.
- اختلال جاروبی: در این تکنیک، یک سیگنال اختلال با پهنای باند باریک با فرکانس مرکزی متغیر برای اختلال به کار گرفته می‌شود.

در روش تابش مجدد، اختلال با ترکیب فرستنده- گیرنده حاصل می‌شود. برای انجام چنین اختلالی، تکرار کننده‌ها سیگنال دشمن را شنود می‌کنند، سپس آن سیگنال را به گونه‌ای تغییر می-دهند، سیگنال تغییر داده شده را تقویت می‌نمایند و در نهایت آن را با هدف در هم گسیختن اطلاعات و یا به اشتباه انداختن دشمن به سمت گیرنده آن ارسال می‌کنند.

از روش بازتابش، برای سردرگم کردن رادارهای دشمن استفاده می‌شود. ابزارهای بازتابشی مانند پوسته[۱] (تشکیل شده از نوارهای باریک فلزی با طول‌ها و پاسخ‌های فرکانسی متفاوت)، ریسمان[۲] (یک رول فویل یا سیم فلزی طویل که برای پاسخ فرکانس پایین و پهن طراحی شده است) و بازتابنده‌های گوشه[۳] (شامل سطوح بازتابنده مسطح شکلی که در نهایت یک بازتابنده سه بعدی را تشکیل می‌دهند) با ایجاد اهداف اشتباه و یا پنهان کردن اهداف واقعی برای دشمن میزان اثرگذاری عملیات آن را کاهش می‌دهند.

[1] . Chaff
[2] . Rope
[3] . Corner Reflectors

۱-۱-۳- حفاظت الکترونیکی (EP)

حفاظت الکترونیکی به آن بخشی از جنگ الکترونیکی اطلاق می‌شود که در برگیرنده فعالیت‌هایی است که برای حصول اطمینان از استفاده مؤثر نیروی خودی از طیف الکترومغناطیسی علی‌رغم استفاده دشمن از جنگ الکترونیک انجام می‌شود.

حفاظت الکترونیکی خود شامل سیاست‌گذاری، فرآیند و طراحی است و هدف آن ناکام گذاشتن فعالیت‌های دشمن در حوزه حمایت الکترونیکی وحمله الکترونیکی می‌باشد. عناصر مختلف حفاظت الکترونیکی در **شکل ۱-۴** به تصویر کشیده شده است. در زیر به شرح هر یک از این اجزا خواهیم پرداخت.

شکل ۱-۴: عناصر مختلف EP

۱-۱-۳-۱- طراحی تجهیزات[1]: درطراحی تجهیزات باید اصولی را پیش از طراحی در نظرگرفت. برخی از مواردی که باید در این بخش مورد توجه قرار گیرند به این شرح می‌باشند:

[1] . Equipment Design

- تصمیمات لازم در مورد قابلیت‌های EP در مرحله ابتدایی ساخت سیستم انجام گیرد.
- توجه درست به تهدیدهای مورد انتظار از محیط در طول عمر عملیاتی سیستم مورد نظر قرار گیرد.
- نیازهای عملیاتی برای حفاظت در نظر گرفته شود.
- تصمیمات هوشمندانه در مورد سطح حفاظت مطلوب اتخاذ شود.

۱-۱-۳-۲- آموزش[1]: یک جزء حیاتی در به کارگیری موثر و قابل اعتماد حفاظت الکترونیکی، آموزش است. برخی تاکتیک‌های عملیاتی جهت کاهش آسیب‌پذیری سیستم در مقابل جنگ الکترونیک و حتی غلبه بر این فعالیت‌های دشمن از این قرارند :

- استفاده از سیستم در حداقل سطح توان و پهنای باند ممکن که کارکرد آن را دچار اختلال نکند.
- تمرین کنترل تشعشع[2] برای کاهش احتمال شنود توسط دشمن: این امر در واقع استفاده کنترل شده و هوشمندانه از فرستنده‌های الکترومغناطیسی، صوتی و ... در جهت بهینه کردن قابلیت‌های سیستم و در عین حال حداقل کردن احتمال آشکار شدن به وسیله حسگرهای دشمن است.
- سوئیچ کردن به مدارها، فرکانس‌ها و وسایل متغیر هنگامی که حمله الکترونیک مانع انجام عملیات موفق در وضعیت اصلی می‌شود.
- برنامه‌ریزی جهت به کارگیری، بهره‌برداری، مخفی‌کردن و یا جابجا کردن تأسیسات آسیب پذیر جهت حصول اطمینان از این که در هنگام نیاز می‌توان به طور موثر از آن‌ها استفاده کرد.

---
[1] . Training
[2] . Emission Control (EMCON)

۱-۱-۳-۳- امنیت سیگنال[1]: امنیت سیگنال موضوعی است که خود در برگیرنده امنیت ارتباطات[2] و امنیت الکترونیک[3] می‌شود.باید توجه کرد که امنیت سیگنال با حفاظت الکترونیک متفاوت است. در واقع امنیت سیگنال هدفش بی اثر کردن تداخلات دشمن در سیگنال است در حالی‌که هدف از حفاظت الکترونیک بی اثر کردن فعالیت‌های حمایت الکترونیک و حمله الکترونیک دشمن است. از طرف دیگر برخی از تاکتیک‌ها و تکنیک‌های عملیاتی حفاظت الکترونیک مشابه جنبه‌هایی از امنیت انتقال سیگنال می‌باشد. لذا در این حالت، حفاظت الکترونیک و امنیت سیگنال به هم مرتبط هستند و هر دو به استفاده مؤثر و مداوم طیف الکترومغناطیس توسط نیروهای خود مربوط می‌باشند.

۱-۱-۳-۴- مدیریت فرکانس[4]: این کار مسؤولیت افسر الکترونیک و مخابرات است که به استفاده نیروی خودی و همچنین دشمن از فضای فرکانسی نظاره کند. این افسر تخصیص فرکانس و استفاده از آن را مدیریت می‌کند.

۱-۲- کاربردهای سیستم گیرنده سیگنال راداری

سیستم گیرنده سیگنال راداری از تجهیزاتی است که می‌تواند در دو کارکرد حمایت الکترونیک (جهت جمع آوری اطلاعات از فرستنده‌های دشمن) و حمله الکترونیک (جهت هدایت آتش یا سیستم‌های اختلال کننده) مورد استفاده قرارگیرد.

---

[1] . Signal Security (SIGSEC)
[2] . Communication Security (COMSEC)
[3] . Electronic Security (ELSEC)
[4] . Frequency Management

برای کاربردهای سیستم تشخیص سیگنال راداری به طور مشخص، می‌توان به موارد زیر اشاره کرد [۶].

- استفاده در مرزهای کشور و یا شهرهای مهم برای تشخیص به موقع تهدید نظامی دشمن و نیز جمع‌آوری اطلاعات از سیگنال‌های ارسالی رادارهای فعال منطقه.
- استفاده در زیردریایی‌ها: به دلیل اینکه امواج الکترومغناطیسی در زیر آب امکان انتشار ندارند دستگاه‌های الکترومغناطیسی مانند رادار کارایی خود را از دست می‌دهند. در نتیجه زیردریایی زمانی که زیر آب است قادر به استفاده از رادار خود برای شناسایی منطقه نمی‌باشد. از مهم‌ترین خطراتی که زیردریایی را تهدید می‌کند این است که کشتی دشمن یا جنگنده‌های دشمن در منطقه حضور داشته باشند و زیردریایی بدون اطلاع از حضور آن‌ها به سطح آب بیاید. کاربرد سیستم تشخیص سیگنال راداری در این‌جا این است که زیردریایی قبل از بیرون آمدن از آب با استفاده از یک دکل آنتن‌های سیستم را به بیرون از آب می‌فرستد و با استفاده از آن از وجود یا عدم وجود رادارهای دشمن در بیرون از آب مطلع می‌شود و بعد می‌تواند نسبت به خروج از آب تصمیم صحیحی بگیرد. لازم به ذکر است که به علت وجود سیستم‌های شنود دشمن امکان استفاده از رادار در این شرایط وجود ندارد.
- استفاده در هواپیماهای جنگی: از مهم‌ترین تهدیدات نظامی، هواپیماهای جنگی و موشک-های زمین به هوا یا هوا به هوای هدایت شونده هستند. این موشک‌ها برای دنبال کردن و منهدم کردن هدف از رادار استفاده می‌کنند. برای شناسایی این تهدید و انجام اقدامات لازم توسط خلبان که می‌تواند اقدامات اختلال، مانور یا بیرون پریدن باشد، از سیستم تشخیص سیگنال راداری در هواپیما استفاده می‌شود. به دلیل حساسیت کار جنگنده و شرایط ویژه‌ای که دارد وجود سیستم تشخیص سیگنال راداری با دقت و سرعت بالا برای آن بسیار ضروری و پراهمیت است. این سیستم به دلیل این‌که پسیو است و از ماژول‌های حجیم فرستنده توان استفاده نمی‌کند دارای حجم

کوچکی است که به راحتی قابل نصب در جنگنده‌ها می‌باشد و آنتن‌های آن نیز در نوک بال‌ها نصب می‌گردند.

- نصب بر روی نفر: آنتن‌های کوچک سیستم تشخیص سیگنال راداری به راحتی قابل نصب بر روی کلاه سربازان می‌باشد و می‌تواند سربازان را نسبت به حضور تهدید نظامی در منطقه مطلع کند.

۱-۳- طبقه بندی سیستم‌های گیرنده تشخیص سیگنال راداری

سیستم‌های شناسایی سیگنال‌های راداری را به طور کلی می‌توان بسته به پیچیدگی و کاربرد در سه گروه طبقه‌بندی کرد. گروه اول که ساده‌ترین ساختار و عملکرد را دارد، هشداردهنده راداری[1] نامیده می‌شود. همان‌گونه که از نام آن بر می‌آید، سیستم RWR عمدتاً تنها برای دادن هشدار به کار می‌رود و نمی‌توان عملکرد خیلی پیچیده‌ای را از آن انتظار داشت. این سیستم که ممکن است روی دکل زیردریایی، بال هواپیمای نظامی و یا حتی نیروی پیاده نصب شده باشد، رادارهای منطقه تحت پوشش را برای کاربر آشکار کرده و اطلاعات اندکی را در مورد رادار در اختیار او قرار می‌دهد. ویژگی مهم این سیستم، سادگی، کوچکی و قابلیت حمل آن می‌باشد.

دسته دیگر را می‌توان در قالب سیستم‌های ESM[2] بررسی کرد. این سیستم‌ها، عموماً دارای پیچیدگی ساختاری و عملکردی بیشتری نسبت به سیستم‌های RWR هستند. البته همچنان از لحاظ ابعاد غالباً چندان حجیم نیستند. سامانه‌های ESM توانایی‌های بسیار گسترده‌ای دارند. آشکارسازی انواع پارامترهای پالس‌های دریافتی از رادار مانند پهنای پالس، نرخ تکرار پالس، فرکانس یا باند کاری رادار، دامنه پالس و سرعت چرخش رادار از قابلیت‌های این سامانه است. بسته به کلاس

[1]. Radar Warning Receiver (RWR)
[2]. Electronic Support Measures (ESM)