نشریه علمی-تخصصی
پژوهش های نوین علوم مهندسی
ISSN: 2538-3809
سال هفتم، شماره ۵ (پیاپی: ۴۱)، زمستان ۱۴۰۱

مقابله با حملات سایبری-الکترونیکی در سیستم‌های راداری نیروی دریایی

محمدمهدی نوروزیان[۱]

تاریخ دریافت: ۱۴۰۱/۱۰/۲۷
تاریخ پذیرش: ۱۴۰۱/۱۲/۱۰
کد مقاله: ۴۹۸۰۱

چکـیده

مقاله حاضر جنبه های مرتبط با حملات ترکیبی شامل جنگ سایبری و جنگ الکترونیک در سیستم های راداری نیروی دریایی را مورد بحث قرار می دهد. این مقاله به چگونگی پیاده سازی چنین حملاتی می پردازد و نشان می دهد که حملات الکترونیکی (Electronic Attacks) می تواند برای راه اندازی از راه دور یک تهدید سایبری میزبانی شده در یک سیستم محاسباتی راداری مورد استفاده قرار گیرد. این مفهوم از طریق شبیه سازی هایی نشان داده می شود که در آن از یک تکنیک تطبیق الگو برای تصدیق حملات الکترونیکی و در نتیجه، راه اندازی تهدید سایبری استفاده می شود. نتایج نشان دهنده تاثیرگذاری و قدرت این تکنیک به عنوان یک ابزار برای فعالسازی کدهای مخرب نصب شده در سیستم‌های راداری است.

واژگـان کلـیدی: تهدید سایبری، حملات ترکیبی، جنگ الکترونیک، سیستم های راداری دریایی

۱- دانش آموخته کارشناسی شبکه های کامپیوتری، دانشگاه فنی و حرفه ای، دانشکده شهید شمسی پور تهران
norouzianmm97@gmail.com

۱- مقدمه

جنگ سایبری[1] که به دنبال کشف و دستکاری اطلاعات دیجیتال است، به طور فزاینده ای در زمینه بین المللی گسترش می یابد. حملات سایبری پیشرفته مستند شده اند و مطالعاتی که برای درک آن ها انجام شده است، امکان توسعه دیگران را حتی قدرتمندتر و با پتانسیل بالا برای دستیابی به اهداف استراتژیک نشان می دهد (S. McLaughlin et al., 2016). از جمله این حملات می توان به بدافزارها مثل کدهای مخربی (G. Liang et al., 2017) که هدف آن ها اختلال در عملکرد سیستم ها است اشاره کرد. استاکس نت (R. Langner, 2011)، نمونه ای از بدافزاری که ظاهرا توسط حکومت های یک ملیتی تولید شده بود، توانست برنامه هسته ای یک کشور را تا چند سال به تاخیر بیندازد (K. Zetter, 2014). در عملیات نظامی باغ میوه[2] ، نیروی هوایی اسرائیل بدون شناسایی شدن با استفاده از مکانیسم سایبری مخرب نصب شده در سیستم راداری سوریه، به تاسیسات سوریه حمله کرد (R. R. Dipert, 2013).

یکی از فرضیه هایی که در مقالات مطرح شده است، به احتمال حمله الکترونیکی (Electronic Attack) مربوط می شود؛ یعنی حمله ای که در طیف الکترومغناطیسی انجام می شود، برای آزاد کردن یک حمله سایبری با قابلیت ممانعت از فرآیند محاسباتی رادار مورد استفاده قرار می گیرد. چنین تلفیقی از حملات الکترونیکی و سایبری خود را به عنوان یک روند جدید در جنگ های مدرن نشان می دهد، که در آن حملات الکترونیک سایبری حاصل، کلاس جدیدی از تهدیدات را نشان می دهد که باید مورد توجه قرار گیرند.

در بخش نیروی تنفنگداری دریایی، سیستم های راداری به عنوان سنسورهای مربوطه برای ایمنی ناوبری یا به عنوان منبع اطلاعات برای سیستم های ناوبری یکپارچه استفاده می شوند. توجه داشته باشید که یک سیستم راداری به خطر افتاده ممکن است منجر به خطرات جدی برای ایمنی کشتی ها و ناوها شود، که با اثرات احتمالی در طیف گسترده ای از حوزه ها (مانند اقتصادی، زیست محیطی، دفاعی و غیره) همراه است. به همین دلیل، مهم است که چگونگی پیاده سازی چنین حملات سایبری را بررسی کنیم و به دنبال اقدامات متقابل احتمالی باشیم. این مقاله نشان می دهد که چگونه می توان از یک تکنیک تطبیق الگو در یک حمله سایبری برای تشخیص الگوهای خاص حمله الکترونیکی (EA) استفاده کرد و در نتیجه، از این اطلاعات برای راه اندازی یک فرآیند سایبری مخرب در یک سیستم رادار استفاده کرد.

هدف اصلی این مقاله نشان دادن مکانیزمی است که می تواند به عنوان پیوندی بین حمله الکترونیکی و سلاح سایبری مورد استفاده قرار گیرد. به طور خاص تر، این مکانیزم برای اجازه دادن به حمله الکترونیکی برای راه اندازی یک سلاح سایبری که قبلا در سیستم رادار دریایی نصب شده بود، استفاده می شود. اثربخشی مکانیزم پیشنهادی از طریق شبیه سازی ها در پایتون ارزیابی می شود، جایی که هدف یک سیستم راداری عمومی است که برای ناوبری دریایی استفاده می شود. بقیه این کار به شرح زیر سازماندهی شده است: بخش دوم کارهای مرتبط را ارایه می دهد. بخش سوم مکانیسم پیشنهادی در این کار را توصیف می کند تا امکان ارتباط بین حمله الکترونیکی و حمله سایبری در یک سیستم رادار را فراهم کند. بخش چهارم نتایج شبیه سازی را ارایه می دهد. در نهایت، بخش پنجم نتیجه گیری می کند.

۲- پژوهش های مرتبط

افشای بدافزار استاکس نت در سال ۲۰۱۰ جزئیات یک کرم با سطح شگفت انگیزی از پیچیدگی را نشان داد. پالایش آن نگرانی هایی را در مورد توسعه سلاح های سایبری تخصصی، با مهارت بالا و پیچیده، با طراحی چند رشته ای ایجاد کرد. ادبیات نشان می دهد که توسعه چنین سلاح پیچیده ای بدون پشتیبانی فنی گسترده از منابع انسانی بسیار واجد شرایط در زمینه های مختلف فنی (مانند فن آوری اطلاعات و ارتباطات، مهندسی کنترل و مهندسی هسته ای)ممکن نخواهد بود. این سازمان توسط نهاده ای دولتی برای دستیابی به اهداف استراتژیک در محیط بین المللی ایجاد می شد (K. Zetter, 2014).

هدف استاکس نت سایت های غنی سازی هسته ای ایران بود که عملیات آن مختل کردن و به تاخیر انداختن برنامه هسته ای این کشور بود. امروزه، مطالعات متعددی در مورد آن در دسترس است که نشان می دهد چنین مدل حمله ای می تواند به عنوان الهام و انگیزه ای برای افرادی با مقاصد مخرب علیه اهداف مهم دیگر مورد استفاده قرار گیرد.

همین مفهوم حمله چند رشته ای می تواند برای آسیب رساندن به پلتفرم های دیگر از جمله سیستم ها و سنسورهای مورد استفاده در محدوده پایگاه های دریایی که ممکن است آسیب پذیری های سایبری به صورت عمدی در آن ها کاشته شده باشد یا خیر، مورد استفاده قرار گیرد.

1 Cyber Warfare
2 Operation Orchard

نویسنده در مورد مفاهیم حملات ترکیبی در حوزه قدرت دریایی بحث می کنند، جایی که جنگ سایبری، الکترونیکی و جنبشی می توانند برای انجام اهداف تاکتیکی و استراتژیک خاص ادغام شوند. کاربرد جداگانه این نوع جنگ در عملیات های نظامی مدرن معمول بوده است، با این حال مشاهده می شود که گرایشی برای ادغام این ابعاد جنگ وجود دارد به طوری که اقدامات در یکی از آن ها باعث اثرات در دیگری می شود. مثالی از حمله ترکیبی در جایی که نویسنده یک حمله الکترونیکی (EA[1]) (به طور خاص یک حمله جعل GPS) را نشان می دهند که قادر به ایجاد یک اثر کینتیک در ناوبری کشتی است. از جمله انواع احتمالی حملات ترکیبی که در این مقاله به آن ها می پردازیم، می توان به حملات سایبرالکترونیک اشاره کرد. به ویژه، به یک حمله خاص علیه سیستم های رادار دریایی می پردازد که تا جایی که ما می دانیم، در بیشینه مورد بررسی قرار نمی گیرد.

طبق (R. A. Clarke, 2014)، حمله الکترونیکی سایبری حمله‌ای است که در آن اقدامات جنگ الکترونیک (Electronic Warfare) نه تنها به دنبال دستکاری اطلاعات تاکتیکی به دست آمده از طریق طیف الکترومغناطیسی (مانند EW[2]) سنتی هستند، بلکه به دنبال دستکاری فرآیند محاسباتی سیستم هدف نیز هستند. در (Y. M. Tavares, 2018)، نویسنده یک تکنیک حمله الکترونیکی (EA) ارائه می دهند که قادر به ایجاد چندین هدف کاذب، با محدوده های مختلف، در محدوده تشخیص رادار است. هدف تکنیک آن ها تولید چندین هدف ساختگی است و در نتیجه باعث می شود اپراتور رادار نتواند بین هدف واقعی و اهداف کاذب تمایز قائل شود.توجه داشته باشید که در مورد آن ها، اطلاعات تشخیص هدف دستکاری می شود، اما فرآیند محاسباتی رادار به طور معمول ادامه می یابد.برای اینکه چنین حمله الکترونیکی (EA) بتواند فرآیند محاسباتی را دستکاری کند، لازم است که در سیستم رادار مکانیزمی برای تایید اطلاعات غلط تولید شده توسط حمله الکترونیکی به عنوان یک دستور برای راه اندازی مکانیزم سایبری مخرب مسئول دستکاری رفتار سیستم وجود داشته باشد.

توجه داشته باشید که برای چنین حمله سایبری، لازم است که یک مولفه سایبری قبلا در سیستم محاسبات راداری تعبیه شده باشد.در این زمینه، مقالات آسیب پذیری های کاشته شده در سیستم های شکاف هوایی را گزارش می کنند (که اغلب در مورد سیستم های رادار دریایی است). این آسیب پذیری ها را می توان در نرم افزار، مانند استاکس نت (N. Falliere, 2010) یا در سخت افزار از طریق حملات زنجیره تامین مانند (J. Robertson, 2018) پیاده سازی شود.باید توجه ویژه ای به عملیات اورچارد شود.

طبق (S. Adee, 2008)، ریزپردازنده های تجاری خارج از شبکه موجود در رادار سوریه ممکن است به صورت هدفمند با یک در پشتی سخت افزاری مخفی (که به عنوان سوئیچ کشنده شناخته می شود) ساخته شده باشند که با دریافت یک کد از پیش برنامه ریزی شده، عملکردهای آن مختل شده و موقتا رادار را مسدود می کند. در این زمینه، هدف از این کار نشان دادن هدف آگاهی از چگونگی ارتباط جنگ الکترونیک و سایبری است. در این مقاله، نویسنده سرنخ هایی را در مورد ایجاد یک آسیب پذیری سایبری برای تحت تاثیر قرار دادن سیستم های راداری ارائه می دهد، اما توضیح نمی دهد که چگونه چنین آسیب پذیری می تواند به عنوان راحتی مهاجم ایجاد شود، به خصوص اگر رایانه های راداری دچار شکاف هوایی شوند و تنها مسیر ارسال دستورها به یک آسیب پذیری که قبلا نصب شده است، از طریق آنتن راداری باشد. در این مقاله ما مکانیزمی را نشان می دهیم که می تواند برای اتصال حوزه های جنگ الکترونیک و سایبری به یک عنصر کلیدی برای ساخت یک حمله سایبری الکترونیک مورد استفاده قرار گیرد.

۳- مکانیزم حمله سایبری-الکترونیک

در حمله سایبرالکترونیک که در این مقاله به آن پرداخته می شود، فرض بر این است که طیف الکترومغناطیسی توسط مهاجم برای ارسال دنباله ای از پالس های جعلی به گیرنده رادار مورد استفاده قرار می گیرد. پس از تایید فرمان، مولفه سایبری حمله می تواند شروع به دستکاری فرآیند محاسباتی رادار برای انجام اقدامات مخرب، مانند تنظیم مجدد سیستم، توقف به روزرسانی شاخص موقعیت برنامه (PPI)، یا حتی ثبت و بازپخش سناریوها کند.

تمرکز این کار بر روی تولید پژواک های راداری جعلی نیست (عمل در دامنه EW نشان داده شده در شکل ۱ نشان داده شده)، نه در جزئیات مربوط به دستکاری فرآیند محاسباتی راداری (عمل در دامنه Cyber Warfare در شکل ۱ نشان داده شده).

تمرکز این کار بر روی مکانیزم پیوندی است که بین هر دو حوزه قرار دارد تا یک حمله سایبری - الکترونیک را در یک سیستم رادار دریایی امکان پذیر کند.

مکانیزمی که در اینجا برای ای در حمله سایبرالکترونیک که در این مقاله به آن پرداخته می شود، فرض بر این است که طیف الکترومغناطیسی توسط مهاجم برای ارسال دنباله ای از پالس های جعلی به گیرنده رادار مورد استفاده قرار می گیرد.

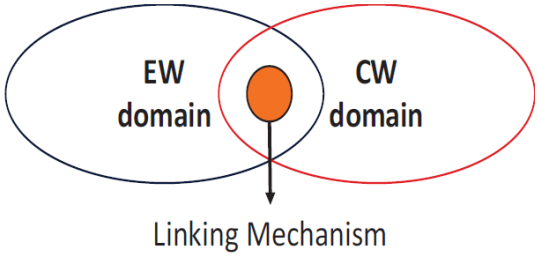
1 Electronic Attack
2 Electronic Warfare

پس از تایید فرمان، مولفه سایبری حمله می تواند شروع به دستکاری فرآیند محاسباتی رادار برای انجام اقدامات مخرب، مانند تنظیم مجدد سیستم، توقف به روزرسانی شاخص موقعیت برنامه (PPI[1])، یا حتی ثبت و بازپخش سناریوها کند.

تمرکز این کار بر روی تولید پژواک های راداری جعلی نیست (عمل در دامنه EW نشان داده شده در شکل ۱ نشان داده شده)، نه در جزئیات مربوط به دستکاری فرآیند محاسباتی راداری (عمل در دامنه CW[2] در شکل ۱ نشان داده شده).

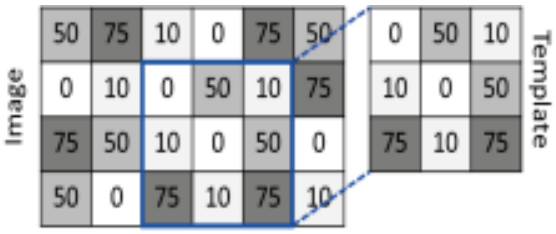
تمرکز این کار بر روی مکانیزم پیوندی است که بین هر دو حوزه قرار دارد تا یک حمله سایبری – الکترونیک را در یک سیستم رادار دریایی امکان پذیر کند.

مکانیزمی که در اینجا برای این کار پیشنهاد شده است براساس تکنیک تطبیق الگو می باشد. ن کار پیشنهاد شده است براساس تکنیک تطبیق الگو می باشد.



شکل ۱- مکانیزم اتصال دهنده بین دامنه های EW و CW

تکنیک تطبیق الگو در پردازش تصویر برای یافتن بخش های کوچکی از یک تصویر که متناظر با یک تصویر مدل است، استفاده می شود. برای این کار، یک الگو تعریف می شود که باید در یک تصویر اصلی جستجو شود. تصویر اصلی در تحلیل و الگو در پیکسل ها تقسیم می شوند، همانطور که در شکل ۲ نشان داده شده است. سپس قالب در یک فرآیند جستجو در تمام قسمت های تصویر اصلی، روی تصویر اصلی جابه جا می شود. برای هر موقعیت فرض شده توسط الگو در این فرآیند اسکن بر روی تصویر اصلی، یک شاخص شباهت محاسبه می شود. شاخص شباهت، شباهت بین قالب و قطعه تصویر اصلی مقایسه شده را کمی می کند. اگر شاخص بالاتر از آستانه تعریف شده قبلی باشد، تصویر الگو در تصویر اصلی تشخیص داده می شود.این عملیات جستجوی جامع نیازمند یک هزینه محاسباتی قابل توجه، متناسب با اندازه تصاویر است.از سوی دیگر، درجه بالایی از اثربخشی را در جستجوی الگوها در تصاویر فراهم می کند.



شکل۲- مثالی از تطبیق الگو

درجه شباهت بین الگو و یک تکه از تصویر اصلی با مقایسه مقادیر شدت هر یک از پیکسل های آن ها ایجاد می شود.از جمله روش های موجود برای محاسبه ضریب تشابه می توان به موارد زیر اشاره کرد:

مجموعه تفاوت های مطلق (SAD)، مجموعه تفاوت های مربعی (SSD)، و همبستگی متقاطع نرمال شده.

در این مقاله از همبستگی عرضی پیرسون (PCC) (Y. M. Tavares, 2018) استفاده شده است (۱):

$$corr = \frac{\sum_{i=1}^{N}(p_i + p)(a_i - a)}{\sqrt{\sum_{i=1}^{N}(p_i - p)^2}\sqrt{\sum_{i=1}^{N}(a_i - a)^2}} \qquad (1)$$

در جایی که PI شدت پیکسل i در الگو؛ p شدت متوسط پیکسل های الگو؛ AI شدت پیکسل i در قطعه تصویر؛ a شدت متوسط پیکسل ها در قطعه تصویر؛ N تعداد پیکسل ها است.توجه داشته باشید که این روش یک عبارت نرمال سازی در مخرج

1 Plan Position Indicator
2 Cyber Warfare

ارائه می دهد، که آن را نسبت به تغییرات جهانی در روشنایی تغییر می دهد، و نتایج همیشه در یک محدوده تعریف شده [۱, ۱-] قرار می گیرند.

۴- نتایج

مکانیزم حمله سایبرالکترونیک شرح داده شده در بخش ۳ از طریق شبیه سازی بر روی یک کامپیوتر با پردازنده i7 اینتل ۲,۵ گیگا بایت حافظه رم DDR3، اجرای ویندوز ۱۰، ۶۴ بیت ارزیابی شد. محیط رادار در شبیه ساز رادار سینماتیک ۲,۰۷. شبیه سازی شد و مکانیزم تطبیق الگو برای حمله سایبرالکترونیک پیاده سازی و در پایتون شبیه سازی شد.

فرض بر این است که مولفه سایبری حمله (بدافزار) در حال حاضر در رادار نصب شده است، با توجه به اینکه مکانیزم های بهره برداری برای نصب آن در سیستم محاسباتی رادار خارج از محدوده این مقاله است. همچنین، با توجه به اینکه پیاده سازی مولفه EA حمله در محدوده این مقاله نیست، فرض بر این است که فرمان از راه دور (توالی صداهای های کاذب) از طریق یک فرکانس رادیویی دیجیتال (فرکانس رادیویی دیجیتال)تولید و منتقل می شود.

این دستور توسط رادار دریافت و پردازش می شود و به صورت یک تصویر در صفحه نمایش PPI نمایش داده می شود، مانند هر انعکاس دریافت شده دیگر.

در شبیه سازی های ارائه شده، کد پایتون رابط گرافیکی (PPI) تولید شده توسط شبیه ساز رادار را اسکن می کند تا دستورها حمله دریافت شده از مولفه EA حمله را شناسایی کند. برای ارزیابی اثربخشی مکانیزم پیشنهادی، در این کار، دستور حمله انتخابی شامل یک توالی از پنج تکرار اشتباه است، که یک توالی از پنج نقطه نمایش داده شده در جهتی که فرستنده DRFM قرار دارد را تولید می کند. پس از شناسایی این الگو، می توان از آن برای راه اندازی یک اقدام مخرب در سیستم رادار دریایی استفاده کرد.

در جایی که PI شدت پیکسل i در الگو؛ p شدت متوسط پیکسل های الگو؛ AI شدت پیکسل i در قطعه تصویر؛ a شدت متوسط پیکسل ها در قطعه تصویر؛ N تعداد پیکسل ها است. توجه داشته باشید که این روش یک عبارت نرمال سازی در مخرج ارائه می دهد، که آن را نسبت به تغییرات جهانی در روشنایی تغییر می دهد، و نتایج همیشه در یک محدوده تعریف شده قرار می گیرند.

شکل ۳- مثالی از صفحه رادار مورد استفاده در شبیه سازی ها نشان می دهد

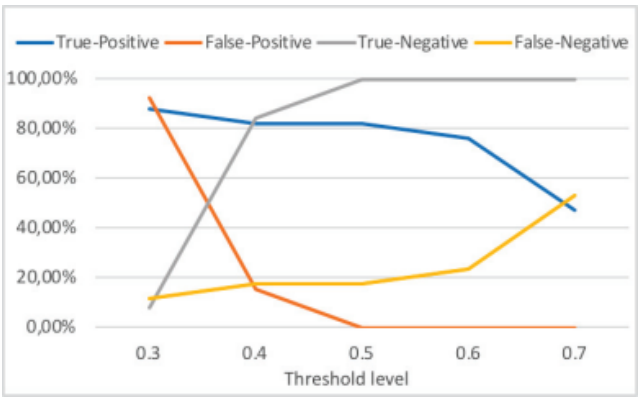
لازم به ذکر است که مهاجم در حال انتقال سیگنال EA است که دستور راه اندازی نشان داده شده در صفحه نمایش را تولید می کند و بسته به محل فرستنده DRFM، سیگنال می تواند از هر جهتی باشد. بنابراین لازم است زوایای مختلفی را در نظر گرفت که از آن ها می توان فرمان راه اندازی را دریافت کرد. به خاطر سادگی، تغییرات ۱ درجه در نظر گرفته می شود، بنابراین مهاجم می تواند از جهت ۰۰۰۱،۰۰۱،۰۰۲،۰۰۳ و غیره منتشر کند. با در نظر گرفتن این زوایای مختلف ممکن از ورود، الگوی حاوی الگوی فرمان راه اندازی نیز در طول فرآیند جستجو در سراسر PPI در مراحل ۱ درجه ای چرخش داده می شود. این جستجوی تطبیق الگو در تمام صفحه PPI اجرا می شود تا زمانی که الگوریتم یک تطابق را پیدا کند یا تا زمانی که تمام احتمالات در طول صفحه آزمایش شوند. این کار برای از بین بردن تغییرات رنگی احتمالی انجام می شود و تنها تجزیه و تحلیل شدت پیکسل ها را انجام می دهد. این الگو نیز در مقیاس خاکستری برای مقایسه پردازش می شود. برای پیاده سازی الگوریتم، کتابخانه های NumPy، ۲cv و Pillow مورد استفاده قرار گرفتند.

```
import numpy as np
import cv2
from PIL import Image

import time

ini = time.time()

for i in range(179):

 print (i)

 colorImage = Image.open('tamplate.png')

 rotated = colorImage.rotate(i)

 rotated.save('tamplate 2.png')

 img_bgr = cv2.imread('Imagem teste 5.png')
 img_gray = cv2.cvtColor(img_bgr, cv2.COLOR_BGR2GRAY)

 template = cv2.imread('tamplate 2.png',0)
 w, h = template.shape[::-1]

 res = cv2.matchTemplate(img_gray,template,cv2.TM_CCOEFF_NORMED)
 threshold = 0.7
 loc = np.where(res >= threshold)

for pt in zip(*loc[::-1]):
     cv2.rectangle(img_bgr, pt, (pt[0]+w, pt[1]+h), (0,255,255), 2)
     cv2.imshow('detected', img_bgr)

fim = time.time()

print ("Tempo de execução: ", fim-ini)
```

شکل ٤- پیاده سازی مکانیزم تحریک در پایتون

پنج سطح آستانه ارزیابی شدند: ۰,۳، ۰,۴، ۰,۵، ۰,۶، ۰,۷. به خاطر داشته باشید که PCC های محاسبه شده با سطوح آستانه مقایسه می شوند تا تصمیم بگیرند که آیا یک تطابق پیدا شده است یا نه (بخش ۳). هر سطح آستانه با استفاده از مجموعه ۳۰ سناریوی مختلف ارزیابی شد. مقادیر متناظر با ماتریس سردرگمی برای هر سطح آستانه در جدول ۱.

عملکرد مکانیسم ماشه برای هر سطح آستانه نیز در شکل ۵ نشان داده شده است.



شکل ۵-عملکرد مکانیزم تحریک

وضعیت مثبت صحیح (True-Positive) به حالتی اشاره دارد که در آن دستور راه اندازی در PPI وجود دارد و تطابقی با الگو وجود دارد. مثبت غلط (False-Positive) حالتی است که در آن دستور راه اندازی در PPI وجود ندارد، اما تطابقی با الگو وجود دارد. منفی حقیقی زمانی رخ می دهد که دستور راه اندازی در PPI وجود نداشته باشد و تطابقی با الگو وجود نداشته باشد. در نهایت، منفی غلط (False-Negative) زمانی رخ می دهد که دستور راه اندازی در PPI باشد اما شناسایی نشود. براساس نتایج، کاهش آستانه نرخ TP را افزایش می دهد، اما نرخ FP را نیز افزایش می دهد (که ممکن است باعث فعال سازی حمله تصادفی و ناخواسته شود). با توجه به نتایج، بهترین آستانه از دیدگاه مهاجم ۰,۵ است.

توجه داشته باشید که با این آستانه مهاجم می تواند حداکثر نرخ TP (۸۲,۳۵٪) را بدون مثبت کاذب به دست آورد. به این معنی که با این آستانه، با در نظر گرفتن سناریوهای ارزیابی شده، احتمال فعال سازی حمله تصادفی به ۰٪ (که برای جلوگیری از افشای حمله مهم است) می رسد و مهاجم ۸۲,۳۵ ٪ احتمال فعال سازی موفقیت آمیز مولفه سایبری حمله در اولین تلاش را دارد.توجه داشته باشید که با دو بار تلاش احتمال فعال شدن درست حمله در حداقل یکی از تلاش ها به ۹۶,۸۸ ٪ افزایش می‌یابد.

جدول ۱- میزان عملکرد

Threshold	TP	FP	TN	FN
0.3	88.24%	92.31%	7.69%	11,76%
0.4	82.35%	15.38%	84.62%	17,65%
0.5	82.35%	0%	100%	17,65%
0.6	76.47%	0%	100%	23,53%
0.7	47.06%	0%	100%	52,94%

۵- نتیجه گیری

با در نظر گرفتن چارچوب نظری ارائه شده و شبیه سازی های انجام شده، می توان دریافت که EA و حملات سایبری می‌توانند با یکدیگر در ارتباط باشند و یک حمله الکترونیکی سایبری با قابلیت تاثیر بر سیستم های رادار دریایی را شکل دهند. این حمله از این حقیقت بهره می برد که رادار، به عنوان یک سنسور، می تواند یک در باز برای دستورها در نظر گرفته شود. استفاده از تکنیک های پردازش تصویر برای راه اندازی یک کد مخرب که قبلا بر روی یک سیستم رادار دریایی با دقت و اثربخشی خوب نصب شده است، با حفظ ایمنی لازم در برابر فعال سازی های تصادفی امکان پذیر است. حتی باوجود تمام ابزارهای امنیت اطلاعات، همه سیستم های کامپیوتری در معرض خطر آلوده شدن به بدافزار قرار دارند. این مکانیزم می تواند به نفع یک عملیات دریایی استفاده شود، که در مناسب ترین لحظه برای نیروی مهاجم فعال می شود. برای کارهای آینده قصد داریم عملکرد مکانیزم پیشنهادی را در یک سیستم واقعی ارزیابی کنیم و اقدامات متقابل برای کاهش این تهدید مانند ابزارهایی برای تایید یکپارچگی نرم افزار مورد استفاده در رادارهای دریایی را بررسی کنیم.

منابع

1. A. Almslmany, C. Wang and Q. Cao, "Advanced deceptive jamming model based on DRFM SubNyquist sampling," 2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, 2016, pp. 727-730.
2. A. O. de Sá, L. F. R da C. Carmo, R. C. S. Machado, “Bio-inspired Active System Identification: a Cyberphysical Intelligence Attack in Networked Control Systems,” in Mobile Networks and Applications, pp. 1-14, October 2017.
3. A. O. Sá, R. C. S. Machado, N. N. Almeida, “The Convergence of Cyber, Electronic and Kinetic Warfare Within the Scope of Sea Power”, Journal of the Brazilian Naval War College, vol. 25, pp. 89- 128, 2018.
4. G. Liang et al., “The 2015 Ukraine Blackout: Implications for False Data Injection Attacks,” in IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317-3318, July 2017.
5. J. Bhatti, T. Humphreys, “Hostile Control of Ships via False GPS Signals: Demonstration and Detection”, Navigation, vol. 64, pp.51-66, 2017.
6. J. Robertson, M. Riley, “The big hack: how China used a tiny chip to infiltrate US companies”, Bloomberg Businessweek, vol. 4, 2018.
7. K. Zetter, “Countdown to Zero Day: Stuxnet and the launch of the world’s first digital weapon”, Broadway books, 2014.
8. N. Falliere, L. O. Murchu, E. Chien, “W32. Stuxnet dossier”, Symantec, 2010.
9. R. A. Clarke, R. K. Knake, “Cyber war”, Old Saybrook: Tantor Media, Incorporated, 2014.
10. R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," in IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, May-June 2011.
11. R. R. Dipert, “Other-than-Internet (OTI) cyberwarfare: challenges for ethics, law, and policy”, Journal of Military Ethics, vol. 12, no. 1, pp. 34-53, 2013.
12. S. Adee, "The Hunt For The Kill Switch", in IEEE Spectrum, vol. 45, no. 5, pp. 34-39, May 2008.
13. S. McLaughlin et al., "The Cybersecurity Landscape in Industrial Control Systems," in Proceedings of the IEEE, vol. 104, no. 5, pp. 1039-1057, May 2016.
14. Y. M. Tavares, N. Nedjah, L. M. Mourelle, “Embedded implementation of template matching using correlation and particle swarm optimization”, International Journal of Bio-Inspired Computation, 2018 Vol.11 No.2, pp.102 – 109.