دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

تشخیص حمله کانال جانبی بر اساس ماشین بردار پشتیبان بهبودیافته

دانیال جعفری[1]*، علیرضا موحدیان[2]

[1]دانشجو کارشناسی ارشد نرم افزار، آزمایشگاه سامانه های امن و بلاکچین دانشگاه امام رضا،jafaridaniel18@gmail.com

دانشجو کارشناسی ارشد نرم افزار، آزمایشگاه سامانه های امن و بلاکچین - دانشگاه بین المللی امام رضا علیه السلام،
movahedian@imamreza.ac.ir

چکیده:

در حوزه تشخیص حملات کانال جانبی، استفاده از تکنیک‌های یادگیری ماشین به‌ویژه ماشین بردار پشتیبان (SVM) به‌عنوان یکی از روش‌های موثر مورد توجه قرار گرفته است. در تحقیقات اخیر، بهبود عملکرد SVM با بهره‌گیری از الگوریتم بازپخت شبیه‌سازی‌شده به‌منظور تنظیم بهینه پارامترها بررسی شده است. تنظیم مناسب پارامترهایSVM ، که یکی از چالش‌های کلیدی در این زمینه محسوب می‌شود، یک مسئله NP-Hard است بنابراین استفاده از روش‌های فرابتکاری برای حل آن پیشنهاد می‌شود. در این پژوهش، الگوریتم فراابتکاری یوزپلنگ که دارای قدرت همگرایی بالاتری نسبت به سایر روش‌های بهینه‌سازی مانند بازپخت شبیه‌سازی‌شده است، برای اولین‌بار به‌منظور بهبود عملکرد SVM در تشخیص حملات کانال جانبی به کار گرفته شده است. نتایج شبیه‌سازی روی مجموعه داده DPA Contest v4 نشان می‌دهد که روش پیشنهادی توانسته دقت تشخیص را در مقایسه با SVMاستاندارد و نسخه بهبودیافته آن با الگوریتم بازپخت شبیه‌سازی‌شده، به میزان 1 درصد افزایش دهد. این بهبود عملکرد نشان‌دهنده ظرفیت بالای الگوریتم یوزپلنگ در بهینه‌سازی مسائل پیچیده و حساس مانند تشخیص حملات کانال جانبی است.

مقدمه:

هنگامی که الگوریتم‌های رمزنگاری بر روی دستگاه‌های الکتریکی پیاده سازی می‌شوند، مدار سخت‌افزاری، اطلاعات فیزیکی مرتبط مانند: زمان [1]، تابش الکترومغناطیسی [2]، مصرف انرژی، اپتیک [3]، آکوستیک [4] و غیره را به صورت غیر مستقیم افشا می‌کنند. تجزیه و تحلیل کانال جانبی (SCA) بدون نیاز به تحلیل مستقیم خود الگوریتم رمزنگاری، از این اطلاعات فیزیکی نشت کرده استفاده می‌کند. تجزیه و تحلیل کانال جانبی معمولاً کلید اصلی را به چند کلید فرعی تقسیم می‌کند و اطلاعات فیزیکی لو رفته را مهاجم می‌تواند ضبط کند. در نهایت مهاجم با ترکیب این اطلاعات و استفاده از دانش مرتبط، کلید اصلی را بازیابی می کند.

زمانی که پل کوچر اولین حمله کانال جانبی شناخته شده عمومی (حمله کانال جانبی) را بر روی چندین سیستم رمزنگاری[5] منتشر کرد، جذابیت زیادی در جامعه امنیتی برای بردارهای حمله فیزیکی مانند زمان بندی، مصرف انرژی[6]، تشعشعات الکترومغناطیسی (EM) [7] و صدا [8] ایجاد شد. در مقابل تحلیل های رمزنگاری سنتی که به شناسایی ضعف های نظری در ساختار الگوریتم های رمزنگاری می پردازند، حملات کانال جانبی بر شناسایی نقاط ضعف در پیاده سازی واقعی الگوریتم ها، در بخش نرم افزار و سخت افزار متمرکز هستند. این نوع حملات با بهره گیری از اطلاعات فیزیکی یا اجرایی نشت کرده، تلاش می کنند تا کلید مخفی را بازیابی کنند.

اگرچه بیشتر مطالعات در زمینه حملات کانال جانبی بر نفوذ به سیستم‌های رمزنگاری متمرکز شده‌اند، تحقیقات نشان داده است که اصول اساسی این نوع حملات می‌توانند انواع دیگری از تهدیدات را نیز به وجود آورند. برای مثال، حملات صوتی به صفحه‌کلید می‌توانند متن تایپ‌شده را افشا کنند [9]، یا تجزیه و تحلیل توان مصرفی پردازنده‌های تعبیه‌شده می‌تواند اطلاعاتی درباره دستورالعمل‌های اجراشده را بازیابی کنند.[10]

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

در تنظیمات رایج این نوع حملات، از روش‌هایی مانند بازرسی بصری آثار فیزیکی، تحلیل‌های آماری و تئوری اطلاعات استفاده می‌شود. حملات کانال جانبی مبتنی بر توان مصرفی را می‌توان به دو دسته اصلی تقسیم کرد: حملات غیر پروفایل (مانند: تجزیه و تحلیل توان ساده یا دیفرانسیلی[6]) و حملات پروفایل (شامل حملات مبتنی بر الگو یا رویکردهای تصادفی[11]) تقسیم کرد.
این دسته‌بندی نشان‌دهنده تنوع تکنیک‌ها و روش‌های موجود برای بهره‌برداری از اطلاعات فیزیکی نشت‌کرده در سیستم‌های محاسباتی است.
سیستم‌های یادگیری ماشین به طور کلی با افزایش تجربه در یک وظیفه خاص، عملکرد خود را بهبود می‌بخشند [12]. در مسائل طبقه‌بندی، این سیستم‌ها معمولاً با نمونه‌های آموزشی متشکل از بردارهای داده‌های ورودی (ویژگی‌ها) و خروجی‌های مرتبط (برچسب‌ها) آموزش داده می‌شوند،که این رویکرد به‌عنوان یادگیری نظارت‌شده شناخته می‌شود. در فرآیند آموزش، الگوریتم بر اساس داده‌های ورودی، پیش‌بینی‌هایی انجام می‌دهد و در صورت تطابق نداشتن این پیش‌بینی‌ها با برچسب‌های مورد انتظار، پارامترهای مدل اصلاح می‌شوند. هدف نهایی، ایجاد مدلی است که بتواند به طور مؤثر روی داده‌های دیده‌نشده تعمیم یابد؛ به این معنا که پیش‌بینی‌های دقیقی برای ورودی‌هایی که در داده‌های آموزشی حضور نداشته‌اند ارائه کند.
در مقابل، یادگیری بدون نظارت به وظایفی اشاره دارد که در آن برچسب‌های نتیجه در دسترس نیستند. در این حالت، الگوریتم سعی می‌کند ساختارهای زیربنایی یا ویژگی‌های پنهان مجموعه داده‌های ورودی را شناسایی کند، مثلاً با خوشه‌بندی داده‌ها به گروه‌های مختلف این کار را انجام می دهد.
یادگیری نیمه‌نظارت‌شده بین این دو دسته قرار می‌گیرد و حالتی را توصیف می‌کند که در آن برچسب‌های خروجی تنها برای بخشی از نمونه‌های آموزشی موجود است. این رویکرد تلاش می‌کند تا از ترکیب داده‌های برچسب‌دار و بدون برچسب برای بهبود عملکرد مدل بهره گیرد و ساختاری بهینه برای تحلیل مجموعه داده‌های ناقص ارائه دهد.

یادگیری ماشین به طور گسترده در بسیاری از حوزه‌ها مانند پردازش زبان طبیعی، تشخیص تصویر یا روباتیک استفاده می‌شود و اهمیت بیشتری برای سیستم‌های خودمختار آینده پیدا می‌کند [13]. علاوه بر این، تعداد زیادی مقاله نیز در سال‌های گذشته ارائه شده است که تکنیک‌های یادگیری ماشین را با تحلیل حملات کانال جانبی ترکیب کرده اند. جاپ و همکاران در یک بررسی، بخشی از تحقیقات مرتبط را که به کاربرد یادگیری ماشین در تحلیل توان مصرفی یا کانال‌های جانبی تشعشعات الکترومغناطیسی در پیاده‌سازی‌های رمزنگاری پرداخته‌اند، خلاصه کردند [14].
آنها خاطرنشان کردند که یک تشابه قوی بین مشکلات یادگیری ماشین نظارت شده و حمله‌های کانال جانبی نمایه شده و همچنین بین یادگیری ماشین بدون نظارت و حمله‌های کانال جانبی بدون پروفایل وجود دارد. در یکی از آخرین مقالات این حوزه [15] یک سیستم تحلیل کانال جانبی پیشنهاد شده است که در آن از روش بازپخت شبیه‌سازی‌شده و روش ماشین بردار پشتیبان برای تشخیص استفاده کرده است.

در این مقاله با توجه به عملکرد مناسب ماشین بردار پشتیبان در حمله کانال جانبی به ارائه روشی جدید از این روش یادگیری ماشین با تنظیم پارامترهای آن پرداخته شده است. تنظیم پارامتر ماشین بردار پشتیبان با روش بهینه‌سازی یورپلنگ [16] انجام می‌شود رویکردی که تاکنون مورد استفاده قرار نگرفته است. دلیل انتخاب الگوریتم بهینه‌سازی یوزپلنگ، توانایی بالای آن در همگرایی به نقطه بهینه حتی در مسائلی با ابعاد بالا است. این ویژگی باعث می‌شود که مدل پیشنهادی بتواند مقادیر دقیق و بهینه‌ای را برای پارامترهای ماشین بردار پشتیبان پیدا کند، که به طور مستقیم بر دقت و کارایی سیستم تشخیص حملات کانال جانبی تأثیر می‌گذارد.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

الگوریتم بهینه‌ساز یوزپلنگ [16] در سال 2022 معرفی شده است، بر اساس رفتار طبیعی یوزپلنگ در شکار طراحی شده و به عنوان الگوریتمی با قدرت جست‌وجوی بالا شناخته شده است. مطالعات نشان داده‌اند که این الگوریتم در آزمایش‌های انجام‌شده بر روی توابع تست، از نظر دقت همگرایی عملکرد بهتری نسبت به سایر روش‌ها داشته است. بر همین اساس، به نظر می‌رسد جایگزینی الگوریتم یوزپلنگ به جای روش بازپخت شبیه‌سازی‌شده که در مقاله [15] استفاده شده بود، می‌تواند منجر به افزایش صحت تشخیص در سیستم‌های تحلیل کانال جانبی شود. این ویژگی به خصوص در مسائل پیچیده‌ای که نیازمند جست‌وجوی دقیق و همگرایی سریع هستند، اهمیت بیشتری پیدا می‌کند.

بنابراین، با توجه به اینکه از روش ماشین بردار پشتیبان برای تشخیص حملات کانال جانبی استفاده شده است و همچنین به این نکته اشاره شده که تنظیم بهینه پارامترهای این روش می‌تواند تأثیر زیادی بر عملکرد آن داشته باشد، لازم به ذکر است که تاکنون چنین بهبودی در استفاده از ماشین بردار پشتیبان برای تشخیص حملات کانال جانبی صورت نگرفته است. به همین دلیل، در این پژوهش با هدف افزایش دقت تشخیص نفوذ، از طریق بهبود عملکرد ماشین بردار پشتیبان با استفاده از الگوریتم بهینه‌ساز یوزپلنگ، یک رویکرد جدید برای تشخیص نفوذ در شبکه‌های اینترنت اشیا ارائه می‌شود. این رویکرد می‌تواند به بهبود دقت و کارایی سیستم‌های تشخیص نفوذ کمک کند و در نهایت، تهدیدات امنیتی را در این شبکه‌ها کاهش دهد.

مرور ادبیات:

یکی از اولین مقالاتی که به کاربرد تکنیک‌های یادگیری ماشین در حمله‌های کانال جانبی پیاده سازی رمزنگاری می‌پردازد توسط هوسپودر و همکاران ارائه شد [17]. آنها از یک نوع ماشین بردار پشتیبان به نام ماشین بردار پشتیبانی حداقل مربع (LS-SVM) برای تشخیص رد قدرت یک نرم افزار محافظت نشده استفاده کردند. آنها نشان دادند که انتخاب پارامترهای LS-SVM به طور قابل توجهی بر عملکرد طبقه بندی تأثیر می‌گذارد، در حالی که اندازه مجموعه آموزشی اهمیت کمتری دارد.

هوسر و زونر نیز اولین کسانی بودند که از طبقه‌بندی چند کلاسه ماشین بردار پشتیبان برای تحلیل وزن های همینگ HW[1] یک بایت در پیاده‌سازی استاندارد رمزگذاری پیشرفته AES[2] که روی میکروکنترلر ATMega اجرا می‌شود، استفاده کردند [18]. آنها نشان دادند که حمله ماشین بردار پشتیبان نسبت به حمله الگو برای ردیابی قدرت با سطح نویز بالا مناسب‌تر است، زیرا این فرض را که داده‌ها زیربنای یک توزیع گاوسی چند متغیره هستند، راحت‌تر می‌کند. این مبنای کار بارتکوویتز و لمکه-راست یک سال بعد را فراهم کرد، که ماشین‌های بردار پشتیبانی احتمالی چند کلاسه را به همان روشی که در حملات الگو مشابه انجام می‌شد طراحی کنند [19]. همچنین در مقاله [20] مقادیر مطلق بردار وزن w تعیین می‌کند که آیا یک ویژگی متناظر تأثیر قابل توجهی بر عملکرد طبقه بندی دارد یا خیر؟ بنابراین، مقادیر وزنی با مقدار مطلق کوچک برای نادیده گرفتن ویژگی‌های بی‌اهمیت روی صفر تنظیم می‌شوند. کارایی روش بر اساس به اصطلاح آنتروپی حدس کلیدی (KGE) اندازه‌گیری شد، تکنیکی که دشواری بازیابی مقدار صحیح یک کلید را با توجه به تعداد مورد نیاز ردیابی کمیت می‌کند. آنها مشاهده کردند که هسته خطی در حملات قالب مبتنی بر ماشین بردار پشتیبان عملکرد مناسبی ندارد زیرا مشکل طبقه‌بندی خطی را ایجاد می‌کند، در حالی که هسته RBF برای مسائل غیرخطی مناسب‌تر است.

[1] Hamming Weight
[2] advanced encryption standard

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

بانکو و همکاران چندین طبقه‌بندی کننده را در زمینه حملات تک ردیابی بررسی کردند [3]. این نوع حملات دشمنی را فرض می‌کنند که تنها به یک رد حمله دسترسی دارد. هنگام هدف قرار دادن رمزهای متقارن، حملات باید دارای تحمل خطا باشند به این معنا که اطلاعات نشت کانال جانبی برای یک مقدار میانی می‌تواند مجموعه‌ای از مقادیر ممکن باشد. نمونه‌هایی از ادبیات آنالیز توان ساده عمل‌گرایانه [21] است که مجموعه‌ای از پنج حدس وزن همینگ را تحمل می‌کند، در حالی که حمله‌های کانال جانبی جبری [22] به سه مقدار وزن همینگ ممکن محدود می‌شوند. در این مطالعه، الگوها، ماشین بردار پشتیبان، شبکه عصبی، درخت تصمیم و جنگل تصادفی برای خروجی فهرست رتبه‌بندی وزن‌های همینگ با توجه به ردپای مصرف انرژی به‌دست‌آمده از اجرای استاندارد رمزگذاری پیشرفته در حال اجرا بر روی دو پلتفرم آزمایشی در نظر گرفته شدند.

در [23] یک مطالعه اضافی اهمیت تنظیم پارامترهای مناسب را هنگام استفاده از تکنیک‌های یادگیری ماشین (قابل پارامترسازی) برای تجزیه و تحلیل کانال جانبی نشان داد. از مجموعه طبقه‌بندی‌کننده‌های نظارت‌شده، بررسی‌شده بهترین نتایج (از نظر دقت طبقه‌بندی با استفاده از اعتبارسنجی متقاطع ده‌برابر) از طریق تنظیم پارامتر برای ماشین بردار پشتیبان به‌دست آمد. با این حال، جنگل تصادفی با تنظیمات بهینه خود فقط کمی بدتر عمل کردند، اما نسبت به تغییرات مقدار پارامتر بسیار قوی‌تر بودند. علاوه بر این نشان داده شده است که یک الگوریتم با دقت تنظیم شده قادر است به دقت نسبتاً بالایی (بیش از 70٪ در هنگام داشتن نویز کم) برسد، حتی اگر فقط تعداد کمی از ویژگی‌های مرتبط استفاده شود (در اینجا 20٪).

در تحقیق [24] با عنوان یک سیستم تشخیص حمله کانال جانبی با استفاده از رویدادهای هسته پردازشگر و یک ماشین بردار پشتیبان به این موضوع اشاره دارد که توانسته روشی برای تشخیص و سرکوب حملات کانال باند جانبی با استفاده از یادگیری ماشین و رویدادهای هسته پردازشگر پیشنهاد کند. یک مدل یادگیری نظارت شده در پیاده‌سازی یک سیستم مبتنی بر شمارنده‌های رویداد سخت‌افزاری برای شناسایی اکسپلویت‌های مخرب مانند انواع SPECTER که در یک فرآیند و در یک سیستم مبتنی بر لینوکس -که به عنوان یک دستگاه محاسباتی Edge اجرا می‌شوند-، استفاده می‌شود. این رویکرد از سخت‌افزار موجود بر روی تراشه به منظور شناسایی انواع سوءاستفاده‌های مخرب در میان سایر فرآیندهای برنامه و تعلیق فرآیند متخلف استفاده می‌کند. در این تحقیق انواع مختلف حمله کانال جانبی تجزیه و تحلیل شده و نشان داده می شود که چگونه در سیستم تشخیص، برای شناسایی و واکنش همزمان چندین حمله به طور همزمان آموزش داده می‌شود و چگونه از تکنیک‌های کاهش ابعاد و تکنیک‌های انتخاب ویژگی از مجموعه بزرگی از داده‌های شمارنده برای بهبود نتایج عملکرد استفاده شده است؟

در تحقیق [25] با عنوان یادگیری ماشینی برای حملات کانال جانبی پین بر اساس حسگرهای حرکتی گوشی‌های هوشمند، به این موضوع اشاره دارد که حسگرهای حرکتی در تمام دستگاه‌های تلفن همراه ادغام شده‌اند و اطلاعات مفیدی را برای اهداف مختلف ارائه می‌دهند. با این حال، این داده‌های حسگر را می‌توان توسط هر برنامه و وب‌سایتی که از طریق مرورگر قابل دسترسی باشد، بدون نیاز به مجوزهای امنیتی خواند. در این مقاله، نشان داده شده است که اطلاعات مربوط به حرکات تلفن هوشمند می‌تواند منجر به شناسایی شماره شخصی تایپ شده توسط کاربر شود. برای کاهش میزان داده‌های لو رفته، از رویکرد رویداد محور استفاده می‌کند که در آن حسگرهای حرکتی فقط زمانی که یک کلید فشار داده می‌شود نمونه‌برداری می‌شوند. داده‌های به‌دست‌آمده برای آموزش الگوریتم یادگیری ماشین برای طبقه‌بندی ضربه‌های کلید به شیوه‌ای تحت نظارت استفاده می‌شوند. همچنین کاربران هر بار که احراز هویت مورد نیاز است، پین یکسانی را وارد می‌کنند که منجر به اطلاعات بیشتر کانال جانبی در دسترس مهاجم می‌شود. نتایج عددی امکان‌پذیری حملات سایبری پین را بر اساس حسگرهای حرکتی، بدون محدودیت در طول پین و ترکیب‌های رقمی ممکن، نشان می‌دهد.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

در تحقیق [26] با عنوان تشخیص نفوذ در محیط‌های IoT از طریق تکنیک‌های کانال جانبی و یادگیری ماشین با اشاره به این موضوع که ظهور فناوری اینترنت اشیا (IoT) در دهه گذشته منجر به کاربردهای متعدد در زمینه‌های مختلف شده است. برخی از داده‌های پردازش شده با استفاده از این فناوری می‌توانند حساس بوده و دستگاه‌های درگیر می‌توانند مستعد حملات سایبری باشند، که منجر به افزایش علاقه به حوزه امنیت اطلاعات اعمال شده در اینترنت اشیا شده است. این مطالعه روشی را برای تجزیه و تحلیل یک شبکه اینترنت اشیا برای شناسایی حملات با استفاده از تکنیک‌های کانال جانبی ارائه می‌کند که نظارت مصرف برق دستگاه‌ها را بر عهده دارد و نشان می‌دهدکه می‌توان از یک سیستم مانیتورینگ مجهز به یادگیری ماشین برای تشخیص نفوذ بدون تداخل با رفتار عادی دستگاه‌ها استفاده کرد. آزمایش‌ها تحت سناریوهای مختلف، مانند استفاده از مجموعه داده‌های سفارشی، شناسایی حملات جدیدی که مدل با آن‌ها آموزش ندیده است، یا شناسایی حملاتی که به صورت زنده اتفاق می‌افتند، نتایج مثبتی را به همراه دارد. مزایای اصلی سیستم پیشنهادی سادگی، تکرارپذیری آن (هم کد و هم داده در دسترس هستند) و قابل حمل بودن است، زیرا می‌توان آن را در بسیاری از دستگاه‌ها مستقر کرد و نیاز زیادی به منابع ندارد. با توجه به ساختار شبکه اینترنت اشیا و محدودیت‌های قدرت دستگاه‌ها، استراتژی‌های استقرار مختلفی را پیشنهاد می‌کند.

در تحقیق [27] با عنوان سیستم تشخیص نفوذ کانال جانبی برای وسایل نقلیه هوایی بدون سرنشین حیاتی ماموریت، به این موضوع اشاره می کند که تروجان‌های سخت افزاری به تدریج در حال تبدیل شدن به یک تهدید رو به رشد در چشم انداز اینترنت اشیا هستند. این نوع حمله می‌تواند منجر به حوادث فاجعه بار برای وسایل نقلیه هوایی بدون سرنشین شود. نمونه‌هایی از این حوادث می‌تواند نشت اطلاعات، نقص در عملکرد پهپاد، که منجر به سقوط می‌شود و مسائل مربوط به یکپارچگی داده‌ها در اطلاعات جمع آوری شده توسط حسگرها باشد. مقالات دیگر سعی کرده‌اند این مشکل را با تمرکز بر تقویت رمزگذاری و سخت‌تر کردن ویژگی‌های فیزیکی دستگاه برای محدود کردن نشت اطلاعات حل کنند. با این حال، هدف این تحقیق نشان دادن اثربخشی تکنیک تشخیص نفوذ مبتنی بر کانال جانبی است و نشان می‌دهد که چگونه این تکنیک سیستم تشخیص نفوذ به طور موثر حوادث مربوط به اجرای وسایل نقلیه هوایی بدون سرنشین در پهپادها را شناسایی می‌کند و اختلافات در امپدانس سیستم را تحلیل می‌کند.

در تحقیق [28] با عنوان یک رویکرد چند هدفه برای تشخیص تروجان سخت افزاری مبتنی بر کانال جانبی با استفاده از ردیابی قدرت، به این موضوع اشاره می کند که شناسایی تروجان‌های سخت افزاری در گذشته به طور گسترده مورد مطالعه قرار گرفته است. در این مقاله، یک تکنیک تحلیل کانال جانبی پیشنهاد می‌شود که از تکنیک انتخاب ویژگی مبتنی بر پوشش برای تشخیص تروجان سخت‌افزاری استفاده می‌کند. الگوریتم بهینه‌سازی نهنگ برای استخراج دقیق بهترین زیرمجموعه ویژگی‌ها اصلاح شده است. هدف تکنیک پیشنهادی چند هدفه است: بهبود دقت و به حداقل رساندن تعداد ویژگی‌ها. تثبیت کننده روش انتخاب ویژگی به ایجاد یک مبادله متقابل بین پارامترهای دقت و فراخوان کمک می‌کند و در نتیجه تعداد منفی‌های کاذب را به حداقل می‌رساند.

همانطور که اشاره شد کوچر و همکاران [29] حمله مصرف برق را پیشنهاد کردند. این شاخه‌ای از حملات کانال جانبی است که دستگاه‌ها را با اندازه گیری مصرف انرژی مورد هدف قرار می‌دهد. آنان پیشنهاد کردند که تحلیل توان دیفرانسیل کلاسیک با موفقیت کلید الگوریتم را شکسته است و دریافتند که بین مصرف انرژی و داده‌ها هنگام رمزگذاری دستگاه ارتباط وجود دارد. علاوه بر این، این رابطه حاوی داده‌های کلید دستگاه رمزگذاری شده است که می‌تواند برای شکستن کلید استفاده شود. با تجزیه و تحلیل مصرف برق یک دستگاه در هنگام رمزگذاری یا رمزگشایی، می‌توان کلید استفاده شده را استنباط کرد. برای انجام این نوع حمله، یک کامپیوتر از یک دستگاه رمزگذاری استفاده و مجموعه‌ای از متن‌های ساده شناخته شده را برای رمزگذاری به دستگاه وارد می‌کند. همانطور که دستگاه، رمزگذاری را انجام می‌دهد، یک اسیلوسکوپ میزان مصرف انرژی را اندازه گیری می‌کند و در نتیجه ردیابی نیرو را به دست می‌آورد. به دنبال این رویکرد، روش‌های حمله تحلیل قدرت بیشتری توسعه یافتند که می‌توان آن‌ها را به طور کلی به عنوان حملات پروفایل و حملات غیرپروفایل طبقه‌بندی کرد. حملات غیرپروفایل شامل تجزیه و تحلیل اطلاعات متقابل [30] و

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

حملات برخوردی [31] و تجزیه و تحلیل توان همبستگی [32] و حملات پروفایل شامل حملات قالب [33] و حملات کانال جانبی مبتنی بر یادگیری ماشینی، مانند پرسپترون چندلایه [34]، جنگل‌های تصادفی [35] و روش نزدیک‌ترین همسایگان [36] ، شبکه‌های عصبی کانولوشن [37] و ماشین‌های بردار پشتیبان [38-41] است.

حملات غیرپروفایل ساده در برابر تداخل محیطی آسیب پذیر هستند. در مقابل، تکنیک‌های حمله پروفایل در برابر نویزهای محیطی انعطاف‌پذیرتر هستند، زیرا به کنترل کامل دستگاهی که مشابه دستگاه هدف است نیاز دارند. مهاجم از دستگاه متعلق به خود برای ایجاد یک مدل نشت کانال جانبی بر اساس تعداد زیادی نمونه استفاده می‌کند که با استفاده از این حمله، امکان شکستن کلید آسان‌تر روی دستگاه مورد نظر را فراهم می‌کند. هوسپودار و همکاران [38] برای اولین‌بار مدل LS-SVM را در حملات تجزیه و تحلیل مصرف انرژی اعمال کردند. یافته‌ها نشان داد که انتخاب پارامتر یادگیری ماشین تأثیر قابل‌توجهی بر عملکرد طبقه‌بندی دارد. هوسر و زونر و همکاران [39] با در نظر گرفتن مقادیر میانی برای طبقه‌بندی پروفایل‌های مصرف برق و کاهش پیچیدگی فضایی، مدل بیت را به مدل وزن همینگ گسترش و نشان دادند که حملات مبتنی بر ماشین بردار پشتیبان حملات قالب‌های معمولی را در موقعیت‌های نویز بالا شکست می‌دهند. هوو و همکاران [40] از یک ماشین بردار پشتیبان مبتنی بر هسته موجک برای بازیابی مقادیر افست و کلیدهای یک الگوریتم AES پوشانده استفاده کرده و نشان دادند که ماشین‌های بردار هسته موجک ماشین‌های بردار هسته گاوسی را شکست می‌دهند. پیک و هوسر و همکاران [41] از الگوریتم SMOTE برای رسیدگی به مشکل داده‌های نامتعادل در طول آموزش ماشین بردار پشتیبان استفاده کردند. این روش قادر به استخراج ویژگی‌هایی است که مهم‌ترین اطلاعات را از ردیابی نیرو حفظ می‌کند و در عین حال نویز را کاهش می‌دهد که پس از آن برای طبقه‌بندی ماشین بردار پشتیبان استفاده می‌شود. مشارکت‌های بالا نشان می‌دهد که ماشین بردار پشتیبان‌ها از سایر روش‌های یادگیری ماشین بهتر عمل می‌کند. با این حال، مشکل انتخاب پارامتر در ماشین بردار پشتیبان‌ها هنوز با روش‌های آنها حل نشده باقی مانده است.

بهینه‌سازی هایپرپارامتر با مسئله انتخاب مدل نیز مرتبط است. این به فرآیند یافتن تنظیمات پارامتر بهینه برای یک الگوریتم در نظر گرفته شده اشاره دارد که دقت آن را به حداکثر می‌رساند. از نظر یک شبکه عصبی، به عنوان مثال، تعداد لایه‌های پنهان یا نوع تابع فعال‌سازی مورد استفاده برای نورون‌های یک لایه مشخص است. متغیرهایی مانند موارد فوق معمولاً تأثیر زیادی بر ظرفیت بازنمایی یک تکنیک یادگیری ماشین دارند. با این حال، اهمیت این مرحله توسط همه نویسندگان مقالات بررسی شده تشخیص داده نشده (یا برای گزارش آن مهم تلقی نشده است). به طور خاص، تنها دو مشارکت وجود دارد که به صراحت تأثیر تنظیم پارامترهای مناسب را بر اثربخشی حمله‌های کانال جانبی بررسی کردند [43]. با این حال، دامنه تکنیک‌های مورد استفاده، از استفاده از مقادیر استاندارد برگرفته از ادبیات [44] در جستجوی شبکه [17] تا روش‌های پیشرفته مانند گروه ذرات [45] و الگوریتم‌های ژنتیک [46] پیش می‌رود. هنگام انتخاب یک الگوریتم مناسب، باید این نکته را نیز در نظر گرفت که الگوریتم‌های ساده‌تر یادگیری ماشین یا ابزارهای تحلیل کانال جانبی استاندارد به سربار بهینه‌سازی کمتری نیاز دارند.

الگوریتم‌های ابتکاری به طور گسترده در مسائل بهینه‌سازی استفاده می‌شود. چندین محقق از الگوریتم‌های اکتشافی برای استخراج این ویژگی استفاده کرده‌اند. وانگ و همکاران [47] چارچوبی از GA-CPA را پیشنهاد کردند که الگوریتم‌های ژنتیک و CPA را ترکیب می‌کرد. این چارچوب از الگوریتم‌های ژنتیک برای استخراج مقادیر مشخصه و به دنبال آن یک حمله CPA استفاده می‌کند. وانگ و همکاران [48] یک الگوریتم شبکه عصبی را توصیف کردند که از بهینه‌سازی ازدحام ذرات (PSO) برای شناسایی تروجان‌های سخت افزاری استفاده می‌کند. نتایج تجربی نشان می‌دهد که دقت تشخیص روش شبکه عصبی مبتنی بر گروه ذرات از روش‌های شبکه عصبی با روش پس انتشارخطای معمولی پیشی می‌گیرد. چندین محقق از الگوریتم‌های اکتشافی برای بهینه‌سازی پارامتر استفاده کرده‌اند که با روش‌های حل دقیق سنتی در اولویت‌بندی جستجو در فضای حل تقریبی متفاوت است. چندین الگوریتم اکتشافی برای بهینه‌سازی پارامترهای ماشین بردار پشتیبان مورد مطالعه قرار گرفته است، مانند الگوریتم‌های ژنتیک [49]،

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

بهینه‌سازی ازدحام ذرات [50]، بهینه‌سازی کلونی مورچه‌ها [51] و بازپخت شبیه‌سازی‌شده [52]. این مطالعات، دقت طبقه بندی بهبود یافته را در مقایسه با روش‌های دیگر مانند جستجوی شبکه‌ای نشان داده‌اند. الگوریتم ژنتیک، نزدیک به بهترین راه حل است، اما رمزگذاری مسئله و سپس رمزگشایی راه حل دشوار است. الگوریتم گروه ذرات دارای متغیرهای کمتری برای تغییر دادن و یک اصل ساده است، اما قابلیت جستجوی محلی ضعیف و دقت جستجوی کافی ندارد. روش کلونی مورچگان به آرامی همگرا می‌شود و تمایل دارد به بهینه محلی بیفتد. علاوه بر این، کلونی مورچگان نمی‌تواند مسائل بهینه‌سازی مداوم فضا را مدیریت کند و فقط برای مسائل گسسته مناسب است. بازپخت شبیه‌سازی‌شده کشف مقادیر حداکثر یا حداقل را با امکان انتخاب تصادفی راه حل‌های زیر بهینه امکان پذیر و فرار از بهینه محلی را آسان‌تر می‌کند.

در مطالعه [15]، روش بازپخت شبیه‌سازی‌شده و ماشین بردار پشتیبان برای ایجاد یک مدل SA-SVM ترکیب شدند، که ایجاد و برای تحلیل توان کانال جانبی اعمال شد. آزمایش بر روی مجموعه داده عمومی DPA انجام شد. ابتدا ضریب پیرسون برای انتخاب مقادیر ویژه مجموعه داده ردپای قدرت به کار گرفته شد سپس مدل HW به عنوان برچسب برای مدل SA-SVM مورد استفاده قرار گرفت. مدل SA-SVM از احتمال معینی برای پذیرش افزایش‌های منفی استفاده می‌کند تا از بهینه محلی خارج شود و پارامترهای بهینه را راحت‌تر پیدا کند. اما روش بازپخت شبیه‌سازی‌شده در ابعاد بالای مسائل بهینه‌سازی دارای دقت بالایی نیست زیرا فرایند اکتشاف در این الگوریتم ضعیف است. پیشنهاد این طرح نامه و پروپوزال مبنی بر استفاده از الگوریتم یوزپلنگ برای ماشین بردار پشتیبان یک راهکار باقدرت اکتشاف و استخراج بالا است که می‌تواند در ابعاد بالای مسئله با دقت همگرا شود.

روش پیشنهادی:

روش پیشنهادی در این مقاله، ماشین بردار پشتیبان بهبودیافته با الگوریتم بهینه‌سازی یوزپلنگ است. از چالش‌های روش پیشنهادی این است که چگونه می‌توان تشخیص حملات کانال جانبی را با دقت بالاتری انجام داد و چگونه روش ماشین بردار پشتیبان بهبود یافته به کمک الگوریتم بهینه ساز یوزپلنگ، در تشخیص حملات کانال جانبی می‌تواند نسبت به روش ماشین بردار پشتیبان استاندارد بوده و نسخه بهبودیافته آن با روش بازپخت شبیه‌سازی‌شده دقت بالاتری داشته باشد.

بنابراین هدف روش پیشنهادی در تشخیص حملات کانال جانبی، بالا بردن صحت تشخیص حملات است و این هدف با این مفروضات تحقیق شده است که الگوریتم بهینه‌سازی یوزپلنگ نسبت به الگوریتم بازپخت شبیه‌سازی‌شده دارای دقت بهینه‌سازی بالاتری است. همچنین روش ماشین بردار پشتیبان در صورتی که با الگوریتم بهینه‌سازی یوزپلنگ در حوزه تشخیص حملات کانال جانبی بهبود داده شود می‌تواند به دقت بالاتری دست پیدا کند.

چارچوب تشخیص حملات کانال جانبی شامل سه قسمت است:

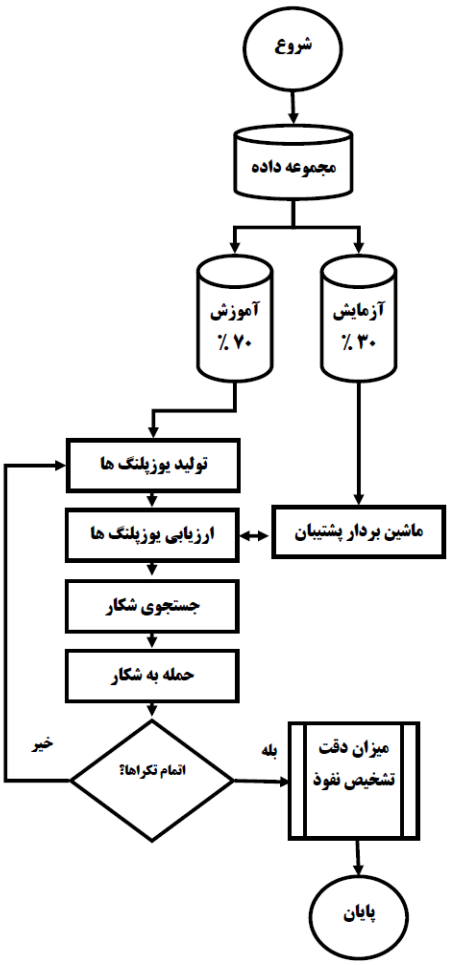
1. ماژول جمع آوری داده‌ها
2. ماژول آموزش طبقه بند
3. ماژول تست

1. ماژول جمع‌آوری داده‌ها: در این ماژول، مجموعه داده‌ها استخراج شده از DPA Contest v4 آماده سازی می‌شود.
2. ماژول تشخیص با آموزش طبقه بند: داده‌ها به عنوان ورودی برای طبقه بند ماشین بردار پشتیبان کار می‌کنند. ماشین بردار پشتیبان در این ماژول آموزش دیده تا الگوی داده‌ها را یاد بگیرد.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

3. ماژول تست: از داده‌های تست روی مدل برای ارزیابی عملکرد مدل برای تشخیص حملات کانال جانبی استفاده شده و میزان صحت تشخیص حملات بررسی می‌شود.

مراحل کلی روش پیشنهادی در فلوچارت شکل 1 آمده است:



شکل 1: مراحل تنظیم پارامتر ماشین بردار پشتیبان با الگوریتم یوزپلنگ

در ماژول آموزش طبقه بند (SVM-CO) ماشین بردار پشتیبان با استفاده از داده‌های نرمال و مخرب، آموزش داده می‌شود. داده‌ها به بخش‌های آموزشی و آزمایشی تقسیم می‌شوند. بهبود روش ماشین بردار پشتیبان با استفاده از الگوریتم یوزپلنگ به این صورت است که در الگوریتم یوزپلنگ، هر یوزپلنگ (جواب ممکن) یک مقدار تصادفی برای متغیر C و w در روش ماشین بردار پشتیبان در معادله 1 تولید می‌شود، پارامتر C تنظیم‌کننده حاشیه است که وظیفه آن برقراری تعادل بین حداکثر کردن حاشیه و حداقل کردن خطای دسته‌بندی بوده و همواره بزرگ‌تر از صفر است و پارامتر w هم وزن است به علت آنکه در روش ماشین بردار پشتیبان به‌صورت تصادفی تولید می‌شود و ممکن است در بهترین مقدار خود قرار نگیرد، ازاین‌رو به دست آوردن مقدار مناسب C و w در روش ماشین

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

بردار پشتیبان یک مسئله بهینه‌سازی است که الگوریتم یوزپلنگ بهترین مقدار را برای آن به دست می‌آورد. در ماشین بردار پشتیبان پیدا کردن بهترین w و C با کمینه‌سازی معادله 1 محقق می‌شود:

$$\min \frac{1}{2} \|w\|^2 + C \sum_i \varepsilon_i \quad (1)$$

که در بهینه‌سازی آن باید شرط معادله 2 در نظر گرفته شود:

$$y_i(<w.x_i>+b) \geq 1-\varepsilon_i \, , \varepsilon_i \geq 0 \;\; \forall i \quad (2)$$

در معادله 2 پارامتر b بایاس، x_i ویژگی داده و y_i کلاس داده است. در الگوریتم یوزپلنگ با استفاده از اپراتورهای خود، هر جواب ممکن (مقداری برای پارامتر C و w) را می‌یابد تا درنهایت به بهترین مقدار این پارامترها دست یابد. برای محاسبه برازندگی هر جواب در این الگوریتم از تابع برازندگی میزان صحت طبقه‌بندی از معادله 3 استفاده می‌شود.

$$accuracy = \frac{TN+TP}{TN+FN+TP+FP} \quad (3)$$

هر یک از عناصر ماتریس به شرح ذیل است:

TN: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها منفی بوده و الگوریتم دسته بندی نیز دسته آن‌ها را به‌درستی منفی تشخیص داده است.

TP: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها مثبت بوده و الگوریتم دسته بندی نیز دسته آن‌ها را به‌درستی مثبت تشخیص داده است.

FP: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها منفی بوده و الگوریتم دسته بندی دسته آن‌ها را به اشتباه مثبت تشخیص داده است.

FN: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها مثبت بوده و الگوریتم دسته بندی دسته آن‌ها را به اشتباه منفی تشخیص داده است.

در مسئله تنظیم پارامترهای ماشین بردار پشتیبان، هر جواب ممکن در الگوریتم بهینه‌سازی یک ارایه به‌صورت حقیقی است که نشان دهنده مقدار عددی برای دو پارامتر W و C در ماشین بردار پشتیبان است:

C	W
0.45	0.74

شکل 2: ساختار یک یوزپلنگ در تنظیم پارامترهای ماشین بردار پشتیبان

در شکل 2 هر یوزپلنگ نشان دهنده دو پارامتر اصلی در ماشین بردار پشتیبان است. به‌علت آنکه اعداد حقیقی هستند دیگر نیاز به تبدیل همانند انتخاب ویژگی نیست. میزان برازندگی هر یوزپلنگ با استفاده از دقت ماشین بردار پشتیبان که در معادله 3 به ازاء پارامترها است.

حرکات یوزپلنگ در الگوریتم بهینه‌سازی یوزپلنگ شامل:

- جستجوکردن: یوزپلنگ‌ها برای یافتن طعمه خود نیاز به جستجو دارند از جمله اسکن یا جستجوی فعال در قلمرو خود (فضای جستجو) یا اطراف آن.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

- نشستن و انتظار: پس از شناسایی طعمه، اما وضعیت مناسب، یوزپلنگ‌ها ممکن است بنشینند و منتظر نزدیک شدن طعمه یا بهتر شدن وضعیت باشند.
- هجوم بردن: این استراتژی دو مرحله اساسی دارد:
  - عجله: زمانی که یوزپلنگ تصمیم به حمله می‌گیرد، با حداکثر سرعت به سمت طعمه می‌شتابد.
  - گرفتن: یوزپلنگ از سرعت و انعطاف پذیری برای گرفتن طعمه با نزدیک شدن به طعمه استفاده می‌کند.
- شکار را رها کند و به خانه برگردد: برای این استراتژی دو حالت در نظر گرفته شده است. (1) اگر یوزپلنگ در شکار طعمه ناموفق باشد، باید موقعیت خود را تغییر دهد یا به قلمرو خود بازگردد. (2) در مواردی که شکار موفقی در یک بازه زمانی انجام نشود، موقعیت خود را به آخرین شکار کشف شده ببرد و جستجو را در اطراف آن انجام دهد.

استراتژی جستجو: یوزپلنگ‌ها از دو طریق به دنبال طعمه می‌گردند: در حالت نشسته یا ایستاده محیط را پایش و یا به طور فعال در اطراف آن گشت زنی می‌کنند. حالت پایش زمانی مناسب‌تر است که طعمه در حال راه رفتن در دشت متراکم و چرا باشد. از طرفی انتخاب حالت فعال که نیاز به انرژی بیشتری نسبت به حالت پایش دارد در صورتیکه طعمه پراکنده و فعال باشد بهتر است. بنابراین، در طول دوره شکار، با توجه به وضعیت طعمه، پوشش منطقه و وضعیت خود یوزپلنگ‌ها، زنجیره‌ای از این دو حالت جستجو است. معادله جستجوی تصادفی برای به روزرسانی موقعیت جدید یوزپلنگ در معادله 4 آمده است که موقعیت فعلی با گام حرکتی شکل می گیرد:

$$X_{i,j}^{t+1} = X_{i,j}^{t} + \hat{r}_{i,j}^{-1}.\alpha_{i,j}^{t} \qquad (4)$$

در معادله 4 $X_{i,j}^{t+1}$ موقعیت بعدی یوزپلنگ و $X_{i,j}^{t}$ موقعیت فعلی آن است و $\hat{r}_{i,j}^{-1}$ پارامتر تصادفی با توزیع نرمال استاندارد است و $\alpha_{i,j}^{t}$ طول گام برای حرکت است و بیشتر از 0 است و حالت پیش فرض آن $0.001 \times \frac{t}{T}$ است به این معنی که یوزپلنگ در حال جستجوی آهسته است. همچنین ممکن است در مواجهه با شکارها و یا دشمنان دیگر، به سرعت حرکت کرده و تغییر جهت حرکت داشته باشد. $\alpha_{i,j}^{t}$ حرکتی بین یوزپلنگ و دیگر همسایه ها و یا رهبر است. رهبر به بهترین جواب پیدا شده در هر تکرار بهینه‌سازی گفته می‌شود.

استراتژی نشستن و منتظر ماندن: در طول حالت جستجو، طعمه ممکن است در میدان دید یوزپلنگ قرار گیرد. در این شرایط هر حرکت یوزپلنگ ممکن است طعمه را از حضور خود آگاه کند و منجر به فرار طعمه شود. برای جلوگیری از این نگرانی، یوزپلنگ ممکن است تصمیم بگیرد (با دراز کشیدن روی زمین یا پنهان شدن در میان بوته‌ها) کمین کند تا به اندازه کافی به طعمه نزدیک شود. بنابراین، در این حالت، یوزپلنگ در موقعیت خود باقی می‌ماند و منتظر می‌شود تا طعمه نزدیک‌تر شود، معادله 5 برای این منظور در نظر گرفته شده است:

$$X_{i,j}^{t+1} = X_{i,j}^{t} \qquad (5)$$

در معادله 5 $X_{i,j}^{t+1}$ موقعیت بعدی یوزپلنگ و $X_{i,j}^{t}$ موقعیت فعلی آن است و در واقع به‌روزرسانی در موقعیت یوزپلنگ‌ها رخ نمی‌دهد.

استراتژی حمله: یوزپلنگ‌ها از دو عامل مهم برای حمله به طعمه خود استفاده می‌کنند: سرعت و انعطاف پذیری. وقتی یوزپلنگ تصمیم به حمله می‌گیرد، با سرعت تمام به سمت طعمه می‌رود. پس از مدتی طعمه متوجه حمله یوزپلنگ می‌شود و شروع به فرار می کند. به عبارت دیگر، یوزپلنگ موقعیت شکار را دنبال و جهت حرکت خود را به گونه‌ای تنظیم می‌کند که در یک نقطه راه شکار را مسدود می سازد. از آنجایی که یوزپلنگ با حداکثر سرعت به فاصله کمی از طعمه رسیده است، طعمه باید فرار کند و موقعیت خود را به طور ناگهانی تغییر دهد تا زنده بماند. یعنی موقعیت بعدی یوزپلنگ نزدیک آخرین موقعیت شکار است.

در معادله 6 استراتژی حمله آمده است:

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

$$X_{i,j}^{t+1} = X_{B,j}^{t} + \check{r}_{i,j}.\beta_{i,j}^{t} \quad (6)$$

که در آن $X_{B,j}^{t}$ موقعیت فعلی شکار است و در واقع بهترین موقعیت فعلی در الگوریتم است. $\check{r}_{i,j}$ عامل چرخش و $\beta_{i,j}^{t}$ برعامل همکنش یوزپلنگ است. $X_{B,j}^{t}$ برای نزدیک شدن به طعمه که در واقع بهترین جواب مسئله است در نظر گرفته شده و $\beta_{i,j}^{t}$ نشان دهنده تعامل یوزپلنگ‌ها با دیگر یوزپلنگ‌ها و یا رهبر است. $\check{r}_{i,j}$ عامل چرخش نیز یک حرکت تصادفی با معادله 7 است که در آن $r_{i,j}$ توزیع نرمال استاندارد است.

$$\check{r}_{i,j} = |r_{i,j}|^{\exp(\frac{r_{i,j}}{2})} sin(2\pi r_{i,j}) \quad (7)$$

در این الگوریتم برای حرکت‌های تصادفی از پارامترهای تصادفی r و همچنین مقدار H با معادله 8 استفاده می‌شود که در آن r_1 یک عدد تصادفی یکنواخت بین $[0و1]$ است.

$$H = e^{2\left(1-\frac{t}{T}\right)}(2r_1 - 1) \quad (8)$$

شبه کد روش پیشنهادی به‌صورت زیر است:

1- تعریف مسئله با تابع برازندگی (معادله 1)، مشخص کردن ابعاد مسئله (2 بعد برای دو پارامتر W و C) تعیین تعداد جمعیت اولیه یوزپلنگ‌ها
2- ارزیابی هر یوزپلنگ با تابع برازندگی تولید جمعیت اولیه با معادله 1
3- مشخص کردن یوزپلنگ‌ها، رهبر و طعمه با توجه به برازندگی آنها
4- بیشترین تکرارهای الگوریتم تعیین شود و مشخص کردن مقدار T تا وقتیکه به تکرار نهایی نرسیده است مراحل زیر انجام شود:
    4-2-1- انتخاب تعداد تصادفی یوزپلنگ‌ها و برای هر یوزپلنگ مراحل زیر انجام شود
    4-2-2- مشخص کردن همسایه‌های هر یوزپلنگ
        4-2-2-1- انجام عملگرهای حرکتی در هر بعد یوزپلنگ‌ها
        4-2-2-2- محاسبه $\alpha, \beta, \hat{r}, \check{r},$ و H
        4-2-2-3- r_2, r_3 به‌صورت تولید تصادفی توزیع غیریکنواخت بین 0 و 1
        4-2-2-4- **اگر** $r_2 \leq r_3$
        4-2-2-5- تولید تصادفی توزیع غیریکنواخت بین 0 و 3 برای r_4 و **اگر** $H \geq r_4$
        انجام جستجو توسط هر یوزپلنگ با معادله 4 در غیر این صورت انجام حرکت حمله به سمت شکار با معادله 6
        4-2-2-6- **اگر** $H < r_4$ منتظر ماندن و حرکت نکردن با معادله 5

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

4-2-3- به‌روزرسانی رهبر

4-2-4- شماره t یک عدد اضافه شود و اگر $t > rand \times T$ آنگاه رها کردن شکار و برگشت به خانه

5- برگشت رهبر به‌عنوان بهترین عامل جستجو و جواب مسئله (بهترین مقادیر برای دو پارامتر W و C)

نتایج:

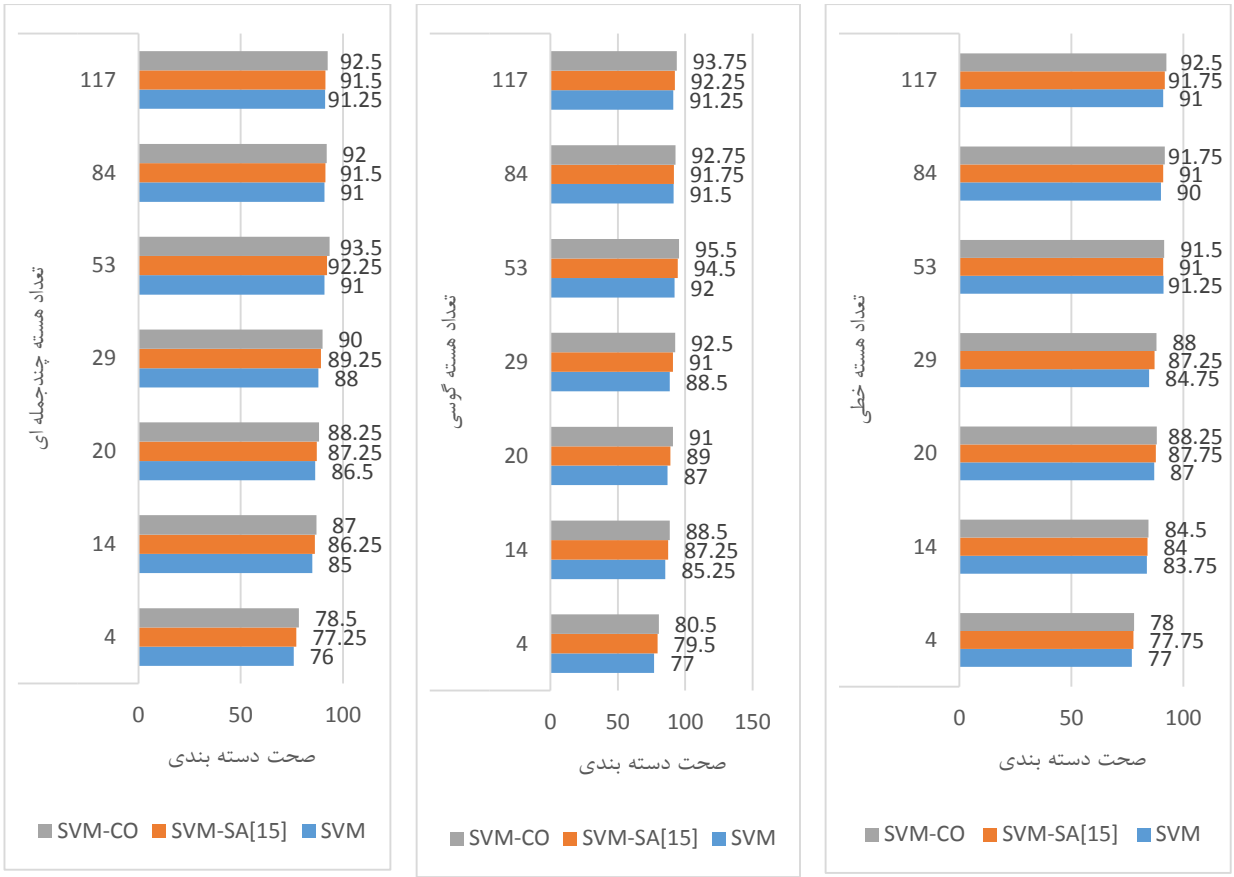
مجموعه داده آزمایشات از مسابقه DPA در زمینه امنیت رمزنگاری و آخرین نسخه آن DPA Contest v4 است [53]. از آنجایی که در این آزمایش از رمزگذاری کامل استفاده نشده نسخه DPA Contest v 4.1 به عنوان مجموعه داده انتخاب شده است که مشترک بین تحقیق حاضر و تحقیق [15] است. برای مقایسه پذیر بودن روش پیشنهادی، شبیه‌سازی بر روی مجموعه داده کامل انجام شد که شامل 1000 نمونه با 435000 ویژگی در هر نمونه است.

نتایج صحت تشخیص حمله با معیارصحت دسته بندی معادله 3 برای سه روش مبتنی بر ماشین بردار پشتیبان آمده است، که شامل:

- آزمایش با ماشین بردار پشتیبان با هسته گوسی، چندجمله ای و خطی
- آزمایش با ماشین بردار پشتیبان بهبود یافته با روش بازپخت شبیه‌سازی‌شده [15] با هسته گوسی، چندجمله ای و خطی
- آزمایش با ماشین بردار پشتیبان بهبود یافته با روش یوزپلنگ با هسته گوسی، چندجمله ای و خطی

در شکل 3 نتایج سه روش مبتنی بر ماشین بردار پشتیبان با تغییر تعداد هسته‌های مختلف آمده است.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603



شکل 3: نتایج صحت دسته بندی در هسته‌های مختلف ماشین بردار پشتیبان

Svm : ماشین بردار پشتیبان، Svm-Sa : ماشین بردار پشتیبان بهبودیافته با روش بازپخت شبیه‌سازی‌شده [15]، Svm-Co : ماشین بردار پشتیبان بهبودیافته با روش یوزپلنگ

همانطور که از شکل 3 مشخص است بیشترین مقدار صحت دسته بندی مربوط به روش ماشین بردار پشتیبان بهبودیافته با روش یوزپلنگ و سپس روش ماشین بردار پشتیبان بهبودیافته با روش بازپخت شبیه‌سازی‌شده [15] است. در شکل 4 میزان بهبود نتایج در روش پیشنهادی و روش مقاله [15] آمده است. بالاترین میزان صحت نتایج عدد 95. درصد با هسته گوسی در روش ماشین بردار پشتیبان بهبودیافته با روش یوزپلنگ است.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

شکل 4: میزان بهبود نتایج در مقایسه با روش پیشنهادی (SVM-CO) و روش (SVM-SA) [15]

همانطور که از شکل 4 مشخص است بیشترین میزان بهبود نتایج 2.25 درصد و کمترین آن 0.32 است. بطور میانگین در آزمایشات انجام شده میزان بهبود نتایج روش پیشنهادی (SVM-CO) و روش مقاله(SVM-SA) [15] در شکل 5 آمده است.

شکل 5: میانگین میزان بهبود نتایج در مقایسه با روش پیشنهادی (SVM-CO) و روش (SVM-SA) [15] در هسته‌های مختلف

همانطور که از شکل 5 مشخص است، بیشترین مقدار بهبود در هسته گوسی بوده است و در حالت کلی روش پیشنهادی توانسته در مجموعه آزمایشات نسبت به روش مقاله [15] نتایج بالاتری داشته باشد. نتایج نشان می‌دهد که ماشین بردار پشتیبان با هسته گوسی بهترین عملکرد را در روش پیشنهادی داشته است و توانسته به بهبود 1.48 درصدی نسبت به روش مقاله(SVM-SA) [15] برسد، ولی در هسته خطی و چندجمله ای این میزان بهبود مشاهده نشده است. درواقع تاثیر الگوریتم بهینه‌سازی یوزپلنگ نسبت به الگوریتم بازپخت شبیه‌سازی‌شده در بهبود ماشین بردار پشتیبان وقتیکه هسته گوسی انتخاب شده باشد، بیشتر است زیرا

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

خط جداساز در هسته گوسی وابستگی بیشتری به تنظیم پارامتر W و C در ماشین بردار پشتیبان دارد ولی در هسته خطی این تاثیر کمتر است زیرا در هسته خطی، خط جداساز مانند هسته چندجمله ای و گوسی قدرت خمیدگی و جداسازی کلاس‌ها را ندارد.

نتیجه گیری:

تحقیقات در زمینه تشخیص حمله‌های کانال جانبی به منظور جلوگیری از شکستن سیستم‌های رمزنگاری انجام می‌شود. حمله‌های کانال جانبی مبتنی بر قدرت شامل حملات غیرپروفایل، از جمله تجزیه و تحلیل توان ساده/دیفرانسیل، و حملات پروفایل، از جمله حملات الگو و رویکردهای تصادفی می‌شوند. تشخیص این حملات با استفاده از روش‌های یادگیری ماشین انجام شده است که یکی از روش‌های کارا در این زمینه، ماشین بردار پشتیبان (SVM) است. با توجه به اینکه ماشین بردار پشتیبان یک راهکار مناسب برای تشخیص حملات کانال جانبی محسوب می‌شود ولی پارامترهای آن به‌خوبی تنظیم نشده است و این مسئله بر صحت دسته‌بندی آن تأثیر می‌گذارد.

در این مقاله، با توجه به عملکرد مناسب ماشین بردار پشتیبان در تشخیص حمله کانال جانبی، به ارائه روشی جدید از این روش یادگیری ماشین با تنظیم پارامترهای آن با استفاده از روش فرابتکاری یوزپلنگ پرداخته شده است. نتایج بر روی مجموعه داده استخراج‌شده از DPA Contest v4 در مقایسه با دو روش دیگر از ماشین بردار پشتیبان با هسته‌های مختلف ارزیابی شد. نتایج نشان داد که بهترین نتیجه با استفاده از هسته گوسی به‌دست آمده است، در حالی که تنظیم پارامترها با روش بازپخت شبیه‌سازی‌شده در بهترین حالت 94.5 درصد صحت دسته‌بندی را به همراه داشت، تنظیم پارامترها با استفاده از روش یوزپلنگ 95.5 درصد صحت دسته‌بندی را بهبود بخشید.

بعنوان اقدامات آینده، می‌توان به استفاده از الگوریتم‌های فرابتکاری برای تنظیم تعداد هسته‌های ماشین بردار پشتیبان اشاره کرد. نتایج نشان می‌دهند که با تغییر هسته‌های ماشین بردار پشتیبان، نتایج صحت دسته‌بندی تغییر می‌کند، بنابراین، تعیین دقیق تعداد هسته‌ها یک مسئله بهینه‌سازی است که می‌تواند با استفاده از الگوریتم‌های بهینه‌سازی بهبود یابد.

منابع:

[1] Kocher, P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Proceedings of the 16th Annual International Cryptology Conference (CRYPTO 96), Santa Barbara, CA, USA, 18–22 August 1996; pp. 104–113.
[2] Wang, R.; Wang, H.; Dubrova, E. Far Field EM Side-Channel Attack on AES Using Deep Learning. In Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security, online, 13 November 2020; pp. 35–44.
[3] Ferrigno, J.; Hlavá˘c, M. When AES Blinks: Introducing Optical Side Channel. IET Inf. Secur. 2008, 2, 94.
[4] Genkin, D.; Shamir, A.; Tromer, E. Acoustic Cryptanalysis. J. Cryptol. 2017, 30, 392–443.
[5] Kocher, P.C.: Timing attacks on implementations of DiffieHellman, RSA, DSS, and other systems. Advances in Cryptology– CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara. California, USA August 18–22, 1996 Proceedings, pp. 104–113. Springer, Berlin (1996)
[6] Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. Advances in Cryptology–CRYPTO' 99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999. Proceedings, pp. 388–397. Springer, Berlin (1999)
[7] Quisquater, J.J., Samyde, D.: Electromagnetic analysis (EMA): measures and counter-measures for smart cards. Smart Card Programming and Security: International Conference on Research in Smart Cards, E-smart 2001 Cannes, France, September 19–21, 2001. Proceedings, pp. 200–210. Springer, Berlin (2001)
[8] Genkin, D., Shamir, A., Tromer, E.: Acoustic cryptanalysis. J. Cryptol. 30(2), 392–443 (2017)
[9] Zhuang, L., Zhou, F., Tygar, J.D.: Keyboard acoustic emanations revisited. ACM Trans. Inf. Syst. Secur. 13(1), 3:1–3:26 (2009)

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

[10] Eisenbarth, T., Paar, C., Weghenkel, B.: Building a side channel based disassembler. Transactions on Computational Science X: Special Issue on Security in Computing, Part I, pp. 78–99. Springer, Berlin (2010)
[11] chindler, W., Lemke, K., Paar, C.: A stochastic model for differential side channel cryptanalysis. In: Rao, J.R., Sunar, B. (eds.) Cryptographic Hardware and Embedded Systems—CHES 2005: 7th International Workshop, Edinburgh, UK, August 29– September 1, 2005. Proceedings, pp. 30–46. Springer, Berlin (2005)
[12] Hastie, T., Tibshirani, R., Friedman, J.: The Elements of Statistical Learning: Data Mining, Inference and Prediction, 2nd edn. Springer, Berlin (2009)
[13] Jordan, M.I., Mitchell, T.M.: Machine learning: trends, perspectives, and prospects. Science 349(6245), 255–26
[14] Jap, D., Breier, J.: Overview of machine learning based sidechannel analysis methods. In: 2014 International Symposium on Integrated Circuits (ISIC), pp. 38–41 (2014)
[15] *Ying Zhang , Pengfei He , Han Gan , Hongxin Zhang ,Pengfei Fan: Side-Channel Power Analysis Based on SA-SVM.in:2023 applted sciences* 3:1–3:26 (2023)
[16] *Mohammad Amin Akbari, Mohsen Zare, Rasoul Azizipanah‑abarghooee,Seyedali Mirjalil & Mohamed Deriche1 . (2022). The cheetah optimizer:a nature.inspired metaheuristic algorithm for large.scale optimization problems . Scientific Reports.10953.*
[17] Hospodar, G., Gierlichs, B., De Mulder, E., Verbauwhede, I., Vandewalle, J.: Machine learning in side-channel analysis: a first study. J. Cryptogr. Eng. 1(4), 293 (2011)
[18] Heuser, A., Zohner, M.: Intelligent machine homicide. In: Schindler, W., Huss, S.A. (eds.) Constructive Side-Channel Analysis and Secure Design: Third International Workshop, COSADE 2012, Darmstadt, Germany, May 3–4, 2012. Proceedings. Springer, Berlin (2012)
[19] Bartkewitz, T., Lemke-Rust, K.: Efficient template attacks based on probabilistic multi-class support vector machines. In: Mangard, S. (ed.) Smart Card Research and Advanced Applications: 11th International Conference, CARDIS 2012, Graz, Austria, November 28–30, 2012, Revised Selected Papers, pp. 263–276. Springer, Berlin (2013)
[20] Standaert, F.X., Malkin, T.G., Yung, M.: A unified framework for the analysis of side-channel key recovery attacks. In: Joux, A. (ed.) Advances in Cryptology—EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26–30, 2009. Proceedings. Springer, Berlin (2009)
[21] Mangard, S.: A simple power-analysis (SPA) attack on implementations of the AES key expansion. In: Lee, P.J., Lim, C.H. (eds.) Information Security and Cryptology—ICISC 2002: 5th International Conference Seoul, Korea, November 28–29, 2002. Revised Papers, pp. 343–358. Springer, Berlin (2003)
[22] Renauld, M., Standaert, F.X.: Algebraic side-channel attacks. In: Bao, F., Yung, M., Lin, D., Jing, J. (eds.) Information Security and Cryptology: 5th International Conference, Inscrypt 2009, Beijing, China, December 12–15, 2009. Revised Selected Papers, pp. 393– 410. Springer, Berlin (2010)
[23] Picek, S., Heuser, A., Jovic, A., Ludwig, S.A., Guilley, S., Jakobovic, D., Mentens, N.: Side-channel analysis and machine learning: A practical perspective. In: 2017 International Joint Conference on Neural Networks (IJCNN), pp. 4095–4102 (2017)
[24] *Rob Oshana.: A Side Channel Attack Detection System Using Processor Core Events and a Support Vector Machine. In:2022 Mediterranean Conference on Embedded Computing (MECO).* (2022)
[25] *MATTEO NERINI.: Machine Learning for PIN Side-Channel Attacks Based on Smartphone Motion Sensors. In: IEEE Access.* (2023)
[26] *ALEJANDRO DOMÍNGUEZ CAMPOS.: Intrusion detection on IoT environments through side-channel and Machine Learning techniques. In: IEEE Access.* (2024)
[27] *Alejandro Almeida, Muneeba Asif.: Side-Channel-Driven Intrusion Detection System for Mission Critical Unmanned Aerial Vehicles. In: IEEE Access.* (2023)
[28] *PRIYADHARSHINI MOHANRAJ .: A Multiobjective Approach for Side-Channel Based Hardware Trojan Detection Using Power Traces In IEICE TRANS.* (2024)
[29] Goos, G.; Hartmanis, J.; van Leeuwen, J.; Kocher, P.; Jaffe, J.; Jun, B. Differential Power Analysis. In Proceedings of the 19th Annual International Cryptology Conference (CRYPTO 99), Santa Barbara, CA, USA, 15–19 August 1999; pp. 388–397.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

[30] Gierlichs, B.; Batina, L.; Tuyls, P.; Preneel, B. Mutual Information Analysis. In Cryptographic Hardware and Embedded Systems— CHES 2008; Oswald, E., Rohatgi, P., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5154, pp. 426–442. ISBN 978-3-540-85052-6.
[31] Niu, Y.; Zhang, J.; Wang, A.; Chen, C. An Efficient Collision Power Attack on AES Encryption in Edge Computing. IEEE Access 2019, 7, 18734–18748.
[32] Han, J.; Kim, Y.-J.; Kim, S.-J.; Sim, B.-Y.; Han, D.-G. Improved Correlation Power Analysis on Bitslice Block Ciphers. IEEE Access 2022, 10, 39387–39396.
[33] Choudary, M.O.; Kuhn, M.G. Efficient, Portable Template Attacks. IEEE Trans. Inf. Forensic Secur. 2018, 13, 490–501
[34] Golder, A.; Das, D.; Danial, J.; Ghosh, S.; Sen, S.; Raychowdhury, A. Practical Approaches Toward Deep-Learning-Based Cross-Device Power Side-Channel Attack. IEEE Trans. VLSI Syst. 2019, 27, 2720–2733.
[35] Picek, S.; Heuser, A.; Jovic, A.; Legay, A. Climbing Down the Hierarchy: Hierarchical Classification for Machine Learning Side-Channel Attacks. In Proceedings of the 9th International Conference on Cryptology in Africa (AFRICACRYPT 2017), Dakar, Senegal, 24–26 May 2017; pp. 61–78.
[36] Liu, J.; Zhang, S.; Luo, Y.; Cao, L. Machine Learning-Based Similarity Attacks for Chaos-Based Cryptosystems. IEEE Trans. Emerg. Top. Comput. 2021, 10, 824–837
[37] Martinasek, Z.; Hajny, J.; Malina, L. Optimization of Power Analysis Using Neural Network. In Proceedings of the 10th IFIP WG 8.8/11.2 International Conference (CARDIS 2011), Leuven, Belgium, 14–16 September 2011; pp. 94–107.
[38] Hospodar, G.; Gierlichs, B.; De Mulder, E.; Verbauwhede, I.; Vandewalle, J. Machine Learning in Side-Channel Analysis: A First Study. J. Cryptogr. Eng. 2011, 1, 293–302.
[39] Heuser, A.; Zohner, M. Intelligent Machine Homicide. In Proceedings of the 10th International Workshop, COSADE 2019, Darmstadt, Germany, 3–5 April 2019; pp. 249–264.
[40] Hou, S.; Zhou, Y.; Liu, H.; Zhu, N. Wavelet Support Vector Machine Algorithm in Power Analysis Attacks. Radioengineering 2017, 26, 890–902.
[41] Picek, S.; Heuser, A.; Jovic, A.; Bhasin, S.; Regazzoni, F. The Curse of Class Imbalance and Conflicting Metrics with Machine Learning for Side-Channel Evaluations. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018, 2019, 209–237
[42] Tran, N.Q.; Hur, J.; Nguyen, H.M. Effective Feature Extraction Method for SVM-Based Profiled Attacks. Comput. Inf. 2021, 40, 1108–1135.
[43] Martinasek, Z., Zeman, V., Malina, L., Martinasek, J.: k-Nearest neighbors algorithm in profiling power analysis attacks. Radioengineering 25(2), 365–382 (2016
[44] Lerman, L., Bontempi, G., Markowitch, O.: A machine learning approach against a masked AES. J. Cryptogr. Eng. 5(2), 123–139 (2015)
[45] Duan, L., Hongxin, Z., Qiang, L., Xinjie, Z., Pengfei, H.: Electromagnetic side-channel attack based on PSO directed acyclic graph SVM. J. China Univ. Posts Telecommun. 22(5), 10–15 (2015)
[46] Maghrebi, H., Portigliatti, T., Prouff, E.: Breaking cryptographic implementations using deep learning techniques. In: Carlet, C., Hasan, M.A., Saraswat, V. (eds.) Security, Privacy, and Applied Cryptography Engineering: 6th International Conference, SPACE 2016, Hyderabad, India, December 14–18, 2016. Proceedings, pp. 3–26. Springer, Cham (2016)
[47] Wang, A.; Li, Y.; Ding, Y.; Zhu, L.; Wang, Y. Efficient Framework for Genetic Algorithm-Based Correlation Power Analysis. IEEE Trans. Inf. Forensics Secur. 2021, 16, 4882–4894.
[48] Wang, C.X.; Zhao, S.Y.; Wang, X.S.; Luo, M.; Yang, M. A Neural Network Trojan Detection Method Based on Particle Swarm Optimization. In Proceedings of the 14th International Conference on Solid-State and Integrated Circuit Technology (ICSICT), Qingdao, China, 31 October–3 November 2018; pp. 1–3.
[49] Huang, C.-L.; Wang, C.-J. A GA-Based Feature Selection and Parameters Optimizationfor Support Vector Machines. Expert Syst. Appl. 2006, 31, 231–240.
[50] Lin, S.-W.; Ying, K.-C.; Chen, S.-C.; Lee, Z.-J. Particle Swarm Optimization for Parameter Determination and Feature Selection of Support Vector Machines. Expert Syst. Appl. 2008, 35, 1817–1824.
[51] Zhang, X.; Chen, X.; He, Z. An ACO-Based Algorithm for Parameter Optimization of Support Vector Machines. Expert Syst. Appl. 2010, 37, 6618–6628.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055
DOI: 10.71623/joins.2025.1143603

[52] Sartakhti, J.S.; Afrabandpey, H.; Saraee, M. Simulated Annealing Least Squares Twin Support Vector Machine (SA-LSTSVM) for Pattern Classification. Soft Comput. 2017, 21, 4361–4373.
[53] Yin, Z.; Zheng, J.; Huang, L.; Gao, Y.; Peng, H.; Yin, L. SA-SVM-Based Locomotion Pattern Recognition for Exoskeleton Robot. Appl. Sci. 2021, 11, 5573.
[54] DPA Contest V4. Available online: https://www.dpacontest.org/v4/rsm_doc.php (accessed on 20 March 2023).