(رویداد ملی سپر نوآوری)

"فرم معرفی ایده یا طرح خلاقانه"

عنوان ایده : معماری فریب تطبیقی چندلایه(LADA)

۱- معرفی تیم کاری:

نام و نام خانوادگی ارائه دهندگان (کامل)	تاریخ تولد	مقطع و رشته تحصیلی	پست الکترونیکی	تلفن همراه	محل اشتغال	استان
نیما بحرینی بهزادی	1355/10/09	دکتری	Pnunima2@gmail.com	09111954820	دانشگاه علوم دریایی امام خمینی(ره) نوشهر	مازندران

۲- تعریف مسئله (Problem Statement)

مشکل یا چالش موجود:

سیستم‌های دفاعی و پدافند غیرعامل سنتی دارای نقاط ضعف اساسی زیر در اصل مهم فریب هستند:

- رویکردهای فریب ایستا و تک‌باره است که پس از کشف، بی‌اثر شده و از کاربرد آن به اتمام می‌رسد؛
- در چنین شرایطی ناتوانی در ایجاد هزینه مستمر و فزاینده برای مهاجم بخشی از مکتب ذهنی فریب شده است؛
- یادگیری و تطبیق پویا با رفتار مهاجم در فریب لحاظ نمی‌شود؛
- تمرکز پارادایمیک بر جلوگیری از هرگونه خسارت است به جای حداکثرسازی هزینه مهاجم از طریق غرق راهبردی دشمن در فرآیند فریب.

اهمیت مسئله:

در محیط امنیتی پیچیده امروز، این محدودیت‌ها منجر به:

- هدررفت منابع دفاعی در رویکردهای واکنشی؛
- امکان شناسایی و دورزدن سیستم‌های دفاعی توسط مهاجمان حرفه‌ای؛
- عدم بازدارندگی مؤثر در برابر تهدیدات مستمر؛
- کاهش تاب‌آوری سیستم‌های حیاتی در برابر حملات پیشرفته خواهد شد.

[1] Layered Adaptive Deception Architecture

۳- محور ایده

طرح و ایده ی شما در کدام یک از زیر محورهای شش گانه رویداد قرار میگیرد؟ ارتقاء توان دفاعی در شرایط اضطرار

۴- راه‌حل(Solution)

معماری سه لایه پویا:

لایه اول: شکارگر(The Bait Layer)

- ایجاد طعمه‌های متنوع و باورپذیر؛
- سرورهای جعلی، مدارک ساختگی، آسیب‌پذیری‌های ظاهری؛
- جابجایی پویای طعمه‌ها بر اساس پروفایل تهدید.

لایه دوم: دام‌ساز(The Snare Layer)

- فعال‌سازی هنگام تعامل مهاجم با طعمه؛
- ایجاد سناریوهای پیچیده برای معتبرسازی فریب؛
- استفاده از یادگیری ماشین برای ترسیم نقشه ذهنی مهاجم.

لایه سوم: صحنه واکنش‌های زنجیره‌ای(The Chain Reaction Stage)

- ایجاد دنباله بی‌پایان از فریب‌های به هم پیوسته؛
- اجرای واکنش‌های دفاعی به ظاهر منطقی اما کاملاً جعلی؛
- هدایت مهاجم به سطوح عمیق‌تر فریب.

- **ارزش پیشنهادی(Value Proposition)**
- چه مزیت‌هایی راه‌حل شما نسبت به راه‌حل‌های موجود دارد؟

۱ .گذار از دفاع ایستا به فریب پویا

- **راه‌حل‌های موجود:** سیستم‌های دفاعی ایستا که پس از کشف بی‌اثر می‌شوند
- **راه‌حل ما:** چرخه فریب بی‌پایان که با هر تعامل مهاجم تقویت می‌شود
- **تمایز:** تبدیل دفاع از "رویداد تک‌باره" به "فرآیند مستمر"

۲ .ایجاد هزینه فزاینده برای مهاجم

- **راه‌حل‌های موجود:** تمرکز بر جلوگیری از نفوذ یا هر گونه تعامل
- **راه‌حل ما :** هدفمندسازی حداکثرسازی هزینه مهاجم برای هر واحد تعامل
- **تمایز:** تبدیل تهدید به فرصت برای خستگی راهبردی دشمن

۳ .یادگیری و تطبیق پویا

- **راه‌حل‌های موجود:** پاسخ‌های از پیش تعریف شده و ثابت
- **راه‌حل ما:** سیستم هوشمند که از رفتار مهاجم یادگیری می‌کند
- **تمایز:** توانایی تطبیق با تاکتیک‌های متغیر مهاجم

۴ .معماری چندلایه یکپارچه

- **راه‌حل‌های موجود:** راه‌حل‌های مجزا و غیرهماهنگ
- **راه‌حل ما:** یکپارچگی کامل بین لایه‌های شکارگر، دام‌ساز و واکنش زنجیره‌ای
- **تمایز:** ایجاد اثر تقویتی بین لایه‌های مختلف فریب

- چرا مشتریان یا کاربران باید از این راه‌حل استفاده کنند؟ به‌دلایل زیر:

۱. افزایش بازدارندگی

ایجاد ریسک بالا و غیرقابل پیش‌بینی مادی برای مهاجمان

افزایش چشمگیر هزینه عملیاتی برای دشمن

۲. افزایش بازدهی سرمایه‌گذاری دفاعی

۳. بهبود تاب‌آوری

حفظ قابلیت‌های عملیاتی تحت حملات پیشرفته

افزایش اطمینان پذیری سیستم‌های حیاتی

۴. مزیت اطلاعاتی

جمع‌آوری اطلاعات ارزشمند از تاکتیک‌های مهاجمان

درک بهتر نیت و توانایی‌های دشمن

- **تحلیل بازار(Market Analysis)**
- مخاطبان هدف شما چه کسانی هستند؟

۱. سازمان‌های نظامی و امنیتی

۲. زیرساخت‌های حیاتی

۳. بخش خصوصی حساس

- اندازه بازار چگونه است؟ چقدر پتانسیل رشد وجود دارد؟

سازمانهای و نهادهای دفاعی و امنیتی

پتانسیل رشد(Growth Potential)

محرک‌های رشد بازار با عنایت به موارد زیر گسترده برآورد می‌شود:

- افزایش تهدیدات سایبری پیچیده
- تأکید اسناد بالادستی بر پدافند غیرعامل
- نیاز فزاینده به راه‌حل‌های بومی امنیتی
- رشد سریع حملات سایبری پیشرفته
- افزایش تقاضا برای راه‌حل‌های دفاع فعال
- وابستگی روزافزون به زیرساخت‌های دیجیتال

۸- مزیت رقابتی(Competitive Advantage)

تطبیق کامل با نیازهای دفاعی و امنیتی ایران، ملاحضات امنیتی استفاده از راه‌کارهای وارداتی و دسترسی سریع به خدمات

- ویژگی‌های منحصربه‌فرد محصول یا خدمات شما چیست؟

۱.معماری سه لایه پویا و یکپارچه

- لایه شکارگر
- لایه دام‌ساز
- لایه واکنش زنجیره‌ای

۲. چرخه فریب بی‌پایان

- تبدیل دفاع از رویداد تک‌باره به فرآیند مستمر

- افزایش خودکار پیچیدگی فریب با هر تعامل مهاجم
- ایجاد مارپیچ هزینه فزاینده برای مهاجم

۳. هوش مصنوعی تطبیقی

- یادگیری از رفتار مهاجم در زمان واقعی
- تطبیق پویا تاکتیک‌های فریب بر اساس الگوهای حمله
- پیش‌بینی مراحل بعدی مهاجم و طراحی فریب پیشدستانه

۴. مدل ریاضی پیشرفته

- استفاده از نظریه بازی‌های سلسله مراتبی
- پیاده‌سازی تعادل استکلبرگ برای پیش‌بینی رفتار مهاجم
- بهینه‌سازی چندهدفه با توابع سود دوگانه

۵. تئاتر واکنشی زنجیره‌ای

- ایجاد سناریوهای باورپذیر و به هم پیوسته
- وادار کردن مهاجم به "جنگیدن با سایه خودش"
- تبدیل فریب به رقابت پویا به جای داستان از پیش نوشته شده

۶. شاخص‌های کمی پیشرفته

- اندازه‌گیری کارایی بر اساس بزرگترین مؤلفه همبند (LCC)
- پایش بلادرنگ هزینه-فایده فریب
- ارزیابی دقیق میزان موفقیت در خستگی راهبردی دشمن

۷. قابلیت یکپارچه‌سازی کامل

- سازگاری با زیرساخت‌های امنیتی موجود
- امکان پیاده‌سازی تدریجی بدون اختلال در عملیات
- انعطاف‌پذیری در تطبیق با معماری‌های مختلف

۸. مدیریت هوشمند منابع

- تخصیص خودکار منابع بر اساس سطح تهدید
- بهینه‌سازی هزینه‌های اجرایی فریب
- ایجاد تعادل بین باورپذیری و هزینه‌های عملیاتی

۹. گزارش‌گیری و تحلیل پیشرفته

- تولید خودکار گزارش‌های تحلیلی
- نمایش گرافیکی مراحل فریب و تعاملات
- ارائه بینش عملیاتی برای تصمیم‌گیری

۱۰. مقیاس‌پذیری و انعطاف‌پذیری

- توانایی پوشش از شبکه‌های کوچک تا زیرساخت‌های ملی
- پشتیبانی از چندین سناریو فریب همزمان

۱۱. آموزش و شبیه‌سازی

- قابلیت استفاده برای آموزش تیم‌های دفاعی
- شبیه‌سازی سناریوهای حمله پیچیده
- آزمون و ارزیابی راهبردهای دفاعی

۱۲. کنترل و نظارت متمرکز

- داشبورد یکپارچه برای مدیریت تمامی لایه‌ها
- قابلیت نظارت بلادرنگ بر تمامی تعاملات
- کنترل دقیق سطح فریب و واکنش‌ها

۱۳. قابلیت توسعه و سفارشی‌سازی

- امکان افزودن ماژول‌های جدید
- سفارشی‌سازی بر اساس نیازهای خاص سازمان
- پشتیبانی از توسعه الگوریتم‌های اختصاصی

۹ – مدل کسب و کار(Business Model)

۱) فروش لایسنس نرم‌افزار به سازمان‌های بزرگ
۲) ارائه سرویس مشاوره استراتژیک و پشتیبانی
۳) برگزاری دوره‌های آموزشی تخصصی

۱۰ – نقشه راه(Roadmap)

- مراحل توسعه محصول از حال حاضر تا زمان عرضه به بازار

۱) توسعه هسته مرکزی
۲) توسعه نمونه اولیه
۳) پایلوت و اعتبارسنجی
۴) عرضه به بازار و توسعه تجاری
۵) بلوغ و توسعه بین‌المللی

۱۱- چالش‌ها و ریسک‌ها

- چالش‌های فنی:

۱) پیچیدگی الگوریتم‌های یادگیری ماشین

- چالش‌های عملیاتی:

۱) احتمال شناسایی سیستم توسط مهاجمان

- برنامه شما برای غلبه بر این چالش‌ها چیست؟

۱) همکاری با متخصصان سطح اول
۲) مدیریت معکوس ریسک شناسایی

۱۲- نتیجه‌گیری و درخواست(Closing and Ask)

- خلاصه‌ای از طرح یا ایده و اهمیت آن.

این ایده نقطه کور بسیاری از راهبردهای متعارف فریب است که آن را به یک رویداد ایستا و تک‌فعلی تقلیل می‌دهند. رویکرد پیشنهادی تله فریب بی‌پایان، یک پارادایم تغییردهنده بازی است که مهاجم را در یک چرخه ویرانگر از هزینه‌گذاری و تحلیل اشتباه گرفتار می‌کند. هدف، ایجاد یک چرخه بی‌پایان از تعامل است که در آن، هر اقدام دفاعیِ به‌ظاهر منطقیِ مدافع، در واقع قلابی برای به دام انداختن عمیق‌تر مهاجم است. مهاجم باید این حس را داشته باشد که در حال مشاهده و بهره‌برداری از یک پاسخ دفاعی واقعی است، نه اینکه در حال تماشای یک نمایش مصنوعی است.

در مفاهیم پدافند غیرعامل، دشمن یک موجودیت هوشمند، کنجکاو و مبتنی بر تحلیل هزینه- فایده است. رویکردهای سنتی فریب(مانند یک سایت جعلی) پس از کشف، بی‌اثر می‌شوند لادا این امر را با این اصل اساسی بازتعریف می‌کند که هر تعامل دشمن با سیستم، یک داده ارزشمند برای تغذیه چرخه فریب بعدی است. در این ایده، هدف نهایی خستگی راهبردی دشمن و افزایش نامتناهی هزینه برای اوست. سیستم به یک موجود زنده و یادگیرنده تبدیل می‌شود که به رفتار مهاجم پاسخ می‌دهد و او را در یک مارپیچ بی‌پایان از شک و تردید فرو می‌برد. رویکرد «تئاتر واکنشی زنجیره‌ای» که در این ایده بکارگرفته می‌شود، فریب را به یک رقابت پویا و باورپذیر تبدیل می‌کند، نه یک داستان از پیش نوشته شده. در این روش، دشمن خودش را در نقش نابغه‌ای می‌بیند که در حال شکست دادن یک مدافع

زبردست است، در حالی که در واقعیت، تنها دارد در یک تئاتر طراحی‌شده توسط همان مدافع، نقش قهرمان تراژدی خودش را بازی می‌کند. این، نهایت هنر پدافند غیرعامل است: **وادار کردن دشمن به جنگیدن با سایه‌ای از خودش.**

از این‌رو مفهوم تابع سود در لادا تغییر کرده است. در اینجا سود، جلوگیری از حمله نیست، بلکه حداکثرکردن هزینه‌نهایی مهاجم در ازای هر واحد تعامل است. هدف مدافع بیشینه‌سازی تابع سود تا جایی است که تهدید به صورت اقتصادی یا عملیاتی برای او غیرقابل توجیه شود.

هر چه مهاجم بیشتر در این چرخه مشارکت کند، سود مدافع بیشتر می‌شود. مدافع با استفاده از یادگیری ماشین، رفتار مهاجم را تحلیل کرده و طعمه‌های لایه‌های بعدی را برنامه‌ریزی می‌کند تا مشارکت و هزینه او را به حداکثر برساند. معماری فریب تطبیقی چندلایه، پدافند غیرعامل را از یک حالت انفعالی به یک بازی تهاجمی فریب تبدیل می‌کند.

ساختار لادا بر سه لایه پویا و وابسته به هم استوار است که یک حلقه فریب بی‌پایان را تشکیل می‌دهند.

لایه ۱ شکارگر[2]: این لایه، سطح قابل مشاهده برای مهاجم است و شامل طعمه‌های کلاسیک اما متنوع می‌شود. سرورهای جعلی، مدارک ساختگی، نقشه‌های اشتباه، و آسیب‌پذیری‌های به‌ظاهر جذاب. این طعمه‌ها به صورت پویا و بر اساس پروفایل اولیه تهدید جابه‌جا و بازسازی می‌شوند. هیچ طعمه‌ای برای همیشه در یک جا نمی‌ماند. کشف هر طعمه توسط مهاجم، پرده اول تئاتر فریب را بالا می‌زند.

لایه ۲ دام‌ساز[3]: هنگامی که مهاجم با یک طعمه تعامل می‌کند، این لایه فعال می‌شود. هدف آن، معتبرسازی فریب اولیه و هدایت مهاجم به یک سناریوی پیچیده است. این لایه شامل خلاءهای جعلی از فعالیت‌های محرمانه، جریان‌های ترافیکی دروغین بین نودهای بی‌خطر و حتی کاربران جعلی در سیستم‌های چت داخلی است. این لایه، مهاجم را متقاعد می‌کند که در مسیر درستی قرار دارد و او را به سرمایه‌گذاری زمان و منابع بیشتر ترغیب می‌کند. استفاده از یادگیری ماشین و تحلیل رفتار، نقشه ذهنی مهاجم را ترسیم می‌کند. هنگامی که مطمئن شد مهاجم به‌طور کامل با طعمه لایه اول درگیر شده است، سناریوی کشف نفوذ را فعال می‌کند. این سناریو یک رویداد کاملاً باورپذیر باید باشد.

لایه ۳ صحنه‌ی واکنش‌های زنجیره‌ای[4]: ایجاد یک دنباله بی‌پایان و باورپذیر از فریب‌های به هم پیوسته، این لایه، هسته اصلی تئاتر است. بلافاصله پس از کشف نفوذ، یک سری واکنش‌های دفاعی به ظاهر منطقی اما کاملاً جعلی اجرا می‌شود. این لایه می‌تواند در حوزه پدافند سایبری به شکل زیر پیاده شوند:

۱) واکنش اول مهاجرت نمایشی: سیستم، یک انتقال اضطراری داده‌های حیاتی از طعمه اولیه به یک سرور جدید و امن‌تر را شبیه‌سازی می‌کند. این سرور جدید (طعمه دوم)، پیچیده‌تر و جذاب‌تر است و مسیرهای دسترسی به آن، عمداً به گونه‌ای طراحی شده که مهاجم احساس کند به طور تصادفی آن را کشف کرده است.

۲) واکنش دوم تقویت فریبنده: امنیت طعمه اولیه به طور نمایشی تقویت می‌شود، اما این تقویت عمداً دارای نقاط ضعفی است که مهاجم بتواند آنها را دور بزند.

۳) واکنش سوم ایجاد مسیرهای مخفی جعلی: مسیرهای ارتباطی جدیدی در شبکه ایجاد می‌شوند که به نظر می‌رسد برای تأمین امنیت بیشتر یا ارتباطات پشتیبان ایجاد شده‌اند. این مسیرها، در واقع دام‌های جدیدی هستند که مهاجم را به سمت طعمه‌های بعدی هدایت می‌کنند.

طعمه معتبرتر ⟵ تعامل ⟵ ایجاد هزینه جزئی برای مدافع ⟵ ارائه طعمه

کاربرد بازی جنگ و ریاضیات در معماری فریب تطبیقی چندلایه:

مدل‌های نظریه بازی با درنظرگرفتن ساختار سلسله‌مراتبی مدافع- مهاجم، به مدافعان اجازه می‌دهند راهبردهای دفاعی را پیش از اقدام مهاجم طراحی کنند. این مدل‌ها در شبکه‌های مدرن که وابستگی درونی بالایی دارند، کمک می‌کنند تا منابع دفاعی به‌صورت بهینه تخصیص یابند و آسیب‌پذیری کل سیستم کاهش یابد. هسته ریاضی این مدل‌ها بر پایه مفهوم تعادل در **بازی‌های سلسله مراتبی**[5]است که در آن مدافع، پاسخ عاقلانه مهاجم را پیش‌بینی و دفاع خود را براساس آن بهینه می‌سازد. ما در این ایده پارادایم یادشده بالا را چنان تغییر می‌دهیم که بازی جنگ یادشده در جهت فریب راهبردی مهاجم حرکت کند.

زیرساخت‌های حیاتی(مانند شبکه‌های انرژی، حمل‌ونقل، یا ارتباطات) اغلب به یکدیگر وابسته‌اند؛ به‌طوری‌که اختلال در یکی، می‌تواند به صورت آبشاری به دیگر بخش‌ها سرایت کند. در این بافتار، مهاجمان(مهاجمان سایبری، هواپیماهای مهاجم، تروریست‌ها و...) و مدافعان(سازمان‌های امنیتی، سکوهای پدافند موشکی و اپراتورها) در تعامل هستند. مهاجمان به‌دنبال حداکثرکردن آسیب به شبکه هستند و مدافعان می‌کوشند با تخصیص منابع محدود، از بخش‌های کلیدی آن محافظت کنند. این تقابل در محیطی پویا و با اطلاعات ناقص رخ می‌دهد. مدل‌های نظریه بازی در این حوزه معمولاً به‌صورت بازی‌های سلسله‌مراتبی طراحی می‌شوند. در این ساختار، مدافع(رهبر) نخست اقدام دفاعی خود را انتخاب می‌کند و مهاجم(پیرو) با مشاهده دفاع، حمله را بهینه می‌سازد. این ترتیب، بازتابی از واقعیت است که

---

[2] The Bait Layer
[3] The Snare Layer
[4] The Chain Reaction Stage
[5] hierarchical game

مدافعان معمولاً زیرساخت را مستقر می‌کنند و مهاجمان سپس آن را هدف قرار می‌دهند. مدافع از مجموعه‌ای از گره‌ها یا پیوندها در شبکه محافظت می‌کند و مهاجم تعدادی از اجزا را برای حمله انتخاب می‌کند. هزینه‌های دفاع/حمله به‌صورت تابعی از میزان اختلال در شبکه تعریف می‌شوند. به‌طور معمول، سود مهاجم برابر با آسیبِ واردشده و سود مدافع برابر با منفیِ آن آسیب است. مفهوم اصلی نهفته در این روش، تعادل استکلبرگ است که در آن مدافع با پیش‌بینی پاسخ بهینه مهاجم، اقدام دفاعی خود را به گونه‌ای انتخاب می‌کند که آسیب نهایی را کمینه کند. این مفهوم در شبکه‌های وابسته اهمیت بیشتری می‌یابد؛ زیرا هر گره ممکن است چندین مسیر خدماتی را پشتیبانی کند و حمله به یک گره، می‌توانند اثرات ثانویه در کل شبکه ایجاد کند.

در این ایده مدافع به جای شبکه‌ای حقیقی از شبکه فریب بهره می‌برد و سعی دارد با شکست نمایشی در بازی جنگ مهاجم را ترغیب به ادامه بازی کند تا به این وسیله مهاجم خود با سلسله اقداماتی که انجام می‌دهد به‌صورت مستمر هزینه خود را افزایش دهد.

مفاهیم اولیه:

شبکه: مجموعه‌ای از گره‌ها[6] که با یال‌ها[7] به یکدیگر متصل شده‌اند؛

گره: هر عنصر در شبکه که می‌تواند مورد حمله قرار گیرد یا دفاع شود(مثلاً سرورها، روترها، کامپیوترها در یک شبکه کامپیوتری)؛

بردار دفاع(d) : یک بردار n بعدی درنظر گرفته می‌شود که در آن d_i میزان دفاعی است که مدافع برای گره iام اختصاص می‌دهد. این می‌تواند شامل فایروال‌هایی که مهاجم در نهایت توان عبور از آن را داشته باشد، به‌روزرسانی‌های امنیتی ناقص، اهداف قابل دسترس زمینی یا دریایی برای مهاجم و غیره باشد.

بردار حمله(a): یک بردار n بعدی که در آن a_i میزان یا نوع حمله مهاجم به گره iام است. این می‌تواند شامل حملات هوایی، دریایی و زمینی، بدافزارها، فیشینگ و غیره باشد.

تابع سود[8]: در مفهوم شاخص کارایی شبکه یکی از رایج‌ترین شاخص‌ها، بزرگترین مؤلفه همبند[9]است. پس از یک حمله که باعث حذف یا غیرفعال‌شدن گره‌ها و یال‌ها می‌شود، اندازه بزرگترین مؤلفه همبند نشان‌دهنده میزان یکپارچگی و کارایی باقی‌مانده شبکه است. برای مهاجم هدف ممکن است کمینه کردن اندازه بزرگترین مؤلفه همبند باشد، به این معنی که شبکه را به قطعات کوچک و جدا از هم تقسیم کند؛ بنابراین، U_A ممکن است با منفی اندازه بزرگترین مؤلفه همبند یا میزان کاهش آن متناسب باشد.

بازی استکلبرگ: بازی استکلبرگ یک نوع بازی سلسله‌مراتبی است که در آن یک بازیکن رهبر ابتدا حرکت خود را انجام می‌دهد و بازیکن دیگر پیرو با مشاهده حرکت رهبر، بهترین پاسخ خود را می‌دهد. در اینجا رهبر همان مدافع و پیرو همان مهاجم است. این مدل برای موقعیت‌هایی مناسب است که یکی از طرفین(معمولاً مدافع) توانایی پیش‌بینی رفتار طرف مقابل را دارد و می‌تواند استراتژی خود را بر اساس این پیش‌بینی بهینه کند. مراحل تعادل استکلبرگ به شرح زیر است مدافع ابتدا یک بردار دفاعی را انتخاب می‌کند. این انتخاب، بر اساس انتظار مدافع از پاسخ مهاجم در مرحله بعد است. مهاجم، با مشاهده استراتژی دفاعی که توسط مدافع انتخاب شده است، به‌دنبال بهترین حمله‌ای می‌گردد که تابع سود خود را بیشینه کند. این به این معنی است که مهاجم، با توجه به دفاع موجود، حمله‌ای را انتخاب می‌کند که بیشترین آسیب را وارد کند یا بیشترین بهره را ببرد. این مرحله به عنوان مسئله بهینه‌سازی مهاجم شناخته می‌شود:

$$\arg\max_a U_A(a,d) = a^*(d)$$

مدافع این پاسخ را پیش‌بینی کرده و بردار بعدی را به‌گونه‌ای انتخاب می‌کند که تابع سود خود را بیشینه کند. مدافع هم با در نظر گرفتن اینکه مهاجم همیشه بهترین پاسخ a*(d) را به استراتژی دفاعی d او خواهد داد، *d را طوری انتخاب می‌کند که تابع سود خود را بیشینه کند. این مرحله به‌عنوان مسئله بهینه‌سازی مدافع شناخته می‌شود به عبارت دیگر، مدافع، دفاعی را انتخاب می‌کند که با در نظر گرفتن بهترین پاسخ مهاجم به آن دفاع، بیشترین امنیت یا کارایی را برای شبکه فراهم کند.

$$\arg\max_d U_D(a^*(d),d) = {}^*d$$

شاخص‌های همانند موارد زیر می‌توانند به عنوان شاخص کارایی شبکه به‌کار روند:

۱) **جریان** : در شبکه‌های انتقال داده، میزان داده‌ای که می‌تواند بین دو نقطه مشخص منتقل شود.

۲) **اتصال‌پذیری** : تعداد مسیرهای بین گره‌ها یا قطر شبکه.

۳) **تعداد گره‌های فعال**: تعداد گره‌هایی که پس از حمله همچنان فعال و عملیاتی هستند.

۴) **هزینه تعمیر و بازیابی**: هزینه‌هایی که برای بازگرداندن شبکه به حالت عادی پس از حمله لازم است.

[6] nodes
[7] edges
[8] Utility Function
[9] Largest Connected Component(LCC)

توابع سود در معماری فریب تطبیقی چندلایه:

در این ایده هدف برای مدافع در ظاهر بیشینه‌کردن اندازه بزرگترین مؤلفه همبند و در واقع تنها افزایش هزینه برای دشمن است که می‌توان نسبت آن را به هزینه فریب دادن دشمن به‌عنوان تابع سود واقعی تعریف کرد، به این معنی که مدافع دو تابع سود دارد یکی تابع سود فریب است که مهاجم اقدامات خود را بر اساس آن برنامه‌ریزی خواهد کرد یعنی تابعی از اقدامات که شبکه را تا حد امکان یکپارچه و متصل نگه دارد و دیگری تابع سود واقعی است که مدافع بر اساس هزینه فایده فریب مهاجم طراحی کرده و ادامه مراحل را منوط به مثبت بودن آن تعریف می‌کند؛ بنابراین، U^*_D ممکن است با اندازه بزرگترین مؤلفه همبند یا میزان حفظ آن متناسب باشد که مدافع به‌ظاهر سعی خواهد کرد که آن را به طور نسبی بیشینه کند. چنان که میزان خسارات وارده بر شبکه فریب تعادل میان هزینه-فایده مدافع را به‌سود هزینه برهم نزند. تابع سود مهاجم $U_A(a,d)$ میزان منفعتی که مهاجم از یک حمله خاص a در حضور دفاع d به‌دست می‌آورد. مهاجم می‌خواهد این تابع را که باز هم با اندازه بزرگترین مولفه همبند متناسب است، کمینه کند، این تابع را می‌توان با تابع U^*_D هماهنگ دانست. در نهایت تابع سود حقیقی مدافع $U_D(a,d)$ میزان منفعتی(هزینه دشمن) است که مدافع از وضعیت شبکه فریب پس از حمله a در حضور فریبدفاع d به‌دست می‌آورد. مدافع می‌خواهد این تابع را بیشینه کند. مدافع برای بیشینه کردن سود واقعی خود، مجبور است تابع سود فریب خود را در سطحی کنترل‌شده کمینه کند.(شبکه فریب باید آسیب ببیند)، اما نه آنقدر که شبکه کاملاً نابود شود یا مهاجم متوجه فریب شود. این یک بهینه‌سازی روی لبه تیغ است. چرا که جواب توابع سود فریب خود به‌عنوان متغیری در تابع سود واقعی قرار خواهد گرفت. مدیریت علمی این تابع مطابق آنچه مدافع احتیاج دارد با استفاده از روش‌های ریاضی ممکن است.

در صورتی که ایده یا طرح شما ماهیت نظامی / امنیتی یا دفاعی دارد ضمن عنوان کلیات و ثبت ایده در وبسایت جهت ارسال پروپوزال بهمراه جزییات ایده و به جهت راهنمایی بیشتر به شماره ۰۹۰۵۵۷۸۴۹۷۹ پیام تا با شما تماس حاصل شده و راهنمایی لازم صورت پذیرد.

آیا نمونه اولیه ایده یا طرح خود را ساخته اید؟ بلی ☐ خیر ☐

آیا آمادگی ارائه نمونه اولیه محصول یا خدمت خود را جهت بررسی داوران دارید؟ بلی ☐ خیر ☐

* لطفا فرم تکمیل شده را حداکثر تا تاریخ ۱۴۰۴/۰۸/۲۴ در آدرس وبسایت www.separnoavari.ir بارگذاری نمایید.

دبیرخانه مسابقات : استان مازندران – نوشهر – خیابان رازی- خیابان ۲۲ بهمن – کوچه مسجد- ساختمان مرکز رشد و نوآوری نوشهر
تلفن و نمابر دبیرخانه : ۵۲۱۴۱۱۷۳– ۰۱۱ کسب اطلاعات بیشتر از طریق پیام رسان های ایتا یا واتس آپ به شماره ۰۹۰۵۵۷۸۴۹۷۹ پیام نموده
یا با دبیرخانه رویداد (مهندس ترابی با شماره ۰۹۱۱۳۹۵۱۹۷۹) تماس حاصل نمایید.

لطفا فایل تکمیل شده در در دو قالب Word و PDF در آدرس وبسایت www.separnoavari.ir بارگذاری نمایید.