نشریه علمی پدافند غیرعامل

سال سیزدهم، شماره ۱، بهار ۱۴۰۱، (پیاپی ۴۹): صص ۳۱-۱۹

علمی- پژوهشی

ارائه مدلی برای مدیریت جریان ورودی در شبکه‌های رایانه‌ای به‌منظور جلوگیری از حمله محروم‌سازی از سرویس بر اساس نظریه بازی‌ها

پژمان غلام نژاد[1*]

تاریخ دریافت: ۱۴۰۰/۰۴/۲۲
تاریخ پذیرش: ۱۴۰۱/۰۱/۱۶

چکیده

در حوادث رایانه‌ای، منافع استراتژی مهاجم (مدافع)، بستگی زیادی به عملکرد مدافع (مهاجم) دارد. بنابراین اثر بخشی سازوکار مدیریت بحران، به رفتارهای استراتژیک مدافع و مهاجم متکی است که به‌کارگیری یک ابزار مؤثر، بر پایه فناوری اطلاعات، در این امر، می‌تواند در افزایش راندمان این اثربخشی، چشمگیر باشد. حملات محروم‌سازی سرویس بر اساس کاهش پهنای باند، یک تهدید دائمی امنیت شبکه می‌باشند. روش‌های پیشنهادی به دلیل فقدان رویکردهای کمی در مدل‌سازی استراتژی‌های دفاعی در برابر این حملات، نمی‌توانند این مشکل را به‌صورت کارآمد برطرف کنند. نظریه بازی می‌تواند چارچوب کمی را برای مدل‌سازی چنین حملاتی فراهم می‌کند. یک مدل مبتنی بر تئوری بازی می‌تواند به‌عنوان یک سامانه پشتیبانی تصمیم برای مدافع عمل کند و قابلیت‌های آن را برای اتخاذ بهترین تصمیم‌ها برای حفظ سطح بهینه امنیت شبکه در برابر چنین حملاتی افزایش دهد. در این مقاله، یک مدل پیشنهادی برای واکنش به حملات محروم‌سازی سرویس، بر پایه نظریه بازی‌ها، به‌عنوان یک بازی بین مهاجم و مدافع ارائه می‌شود. همچنین شبکه مدل شده و بازده محاسبه می‌شود و بازی به تعادل نَش همگرا می‌شود. بهترین اقدام از استراتژی نَش استنباط می‌شود. نتایج به‌دست آمده با شبیه‌سازی و محاسبات عددی به نفع سازوکار دفاعی نظری بازی پیشنهادی است و از شایستگی استفاده از نظریه بازی برای دفاع در برابر حملات محروم‌سازی سرویس برای تقویت امنیت شبکه حمایت می‌کند.

کلید واژه‌ها: نظریه بازی‌ها، تیم واکنش به حوادث رایانه‌ای، حملات شبکه، امنیت سامانه‌های رایانه‌ای

[1] دکترای تخصصی کامپیوتر هوش مصنوعی، دانشگاه علوم و فنون هوایی شهید ستاری، دانشکده مهندسی رایانه و فناوری اطلاعات، تهران، ایران
(pezhman.gholamnezhad@gmail.com)- نویسنده مسئول

۱- مقدمه

۱-۱- ضرورت و اهمیت پژوهش

حوادث امنیتی سایبری می‌تواند پیامدهای شدیدی را برای افراد، مشاغل و سازمان‌ها داشته باشد و دامنه این مسئله در حال گسترش روزافزون می‌باشد. زیرا مهاجمان به تدریج ابزارها و مهارت‌های پیچیده سایبری را توسعه می‌دهند. امروزه با وجود سازوکارهای دفاعی بسیار و فناوری پیشرفته، حملات محروم‌سازی سرویس از نظر اندازه و تعداد در حال افزایش است. افزایش اندازه و تعداد این نوع از حملات، تشخیص و دفاع را دشوارتر نموده است. این مشکل به دلیل ساختارهای شبکه با سرعت بالا، پیچیده، توزیعی و وابسته به هم، همچنان یک مسئله باز و تهدید امنیتی شدید در سراسر جهان است. سازوکارهای مبتنی بر جریان می‌توانند میزان افزایش نرخ جریان بسته‌ها را تشخیص دهند، اما نحوه انتخاب آستانه برای هر جریان را به‌صورت پویا برای جلوگیری از حملات محروم‌سازی سرویس پیشنهاد نمی‌کنند. راه حل‌های امنیتی دیگر شبکه مانند دیواره آتش و سامانه‌های تشخیص نفوذ یا سامانه‌های پیشگیری از نفوذ نیز فاقد چارچوب تصمیم‌گیری کمی برای پیکربندی نرخ جریان هستند. اجتناب از چنین حملاتی به دلیل تغییر رفتار حمله مهاجم، پیشرفت‌های مبتنی بر فناوری‌های نوین، شیوه سازماندهی شده برای حمله و مکان‌های فیزیکی دور از دسترس بسیار دشوار است.

رویکرد دفاعی موجود، انگیزه‌های مهاجم و تجزیه و تحلیل مبادله آن برای شروع حمله را در نظر نمی‌گیرد. برای دفاع در برابر حملات محروم‌سازی سرویس، در چنین محیطی نیازمند سازوکار های دفاعی مبتنی بر یک چارچوب کمی است که بتواند هدف مهاجم و انگیزه‌های آن را به‌صورت ریاضی مدل‌سازی کند.

۱-۲- بیان مسئله

پاسخ یک تیم واکنش به حوادث سایبری در دفاع یا تهاجم، بستگی زیادی به عملکرد مهاجم یا مدافع دارد. استفاده از رویکردهای مبتنی بر نظریه بازی، به‌منظور تجزیه و تحلیل تاکتیکی، و بررسی موقعیت‌های تصمیم‌گیری استراتژیک مدافع و یا تجزیه و تحلیل انگیزه‌های مهاجمان، از اهمیت بالایی برخوردار است. با توجه به غلبه رویکرد نظریه بازی بر راه حل‌های سنتی در حوزه سایبری (ریاضیات اثبات شده، دفاع قابل اعتماد، اقدام به موقع و راه حل‌های توزیع شده)، بیان نقش تئوری بازی در دستیابی به یک استراتژی تعادل برای زنده ماندن از حملات غیر منتظره، می‌تواند در تصمیم‌گیری‌های آتی، بسیار اثربخش باشد.

این پژوهش یک سازوکار دفاعی مبتنی بر نظریه بازی را پیشنهاد می‌نماید که به عنوان یک سامانه پشتیبانی تصمیم برای مدافعان شبکه، در برابر حملات محروم‌سازی سرویس کار می‌کند و به تنظیم یک حد بالا یا آستانه بهینه در ترافیک ورودی در هر جریان به‌صورت پویا کمک می‌کند. در واقع در این مقاله، وضعیت، به‌صورت یک بازی دو نفره مدل می‌شود و بهینه‌سازی بر اساس نقاط زین یا تعادل نَش بازی با استفاده از شبیه‌سازی و محاسبات عددی انجام می‌شود.

در سازوکار پیشنهادی نه تنها پارامترهای شبکه بلکه انگیزه، مقاصد و اهداف مهاجم را برای درک سناریوی حمله واقعی به روشی دقیق و کارآمد نیز کمیت می‌شوند و ترافیک حمله را مدل‌سازی می‌کند، احتمالات جریان‌های حمله را کمتر یا مساوی با آستانه بهینه تعیین شده توسط یک مدافع محاسبه می کند، و بازده یا توابع هدف مربوطه مهاجم و مدافع را هر دو تعریف می‌نماید.

۱-۳- پیشینه پژوهش

نظریه بازی‌ها در انواع مختلف شبکه به‌کار گرفته شده است. در سال ۲۰۰۶، مدلی برای پیشگیری از حمله محروم‌سازی از سرویس[1] در شبکه حسگر[2] با استفاده از تئوری بازی تکراری ارائه شد [۱]. در این مدل، یک پروتکل مبتنی بر نظریه بازی ارائه شد که تشخیص وجود گره‌هایی را انجام می‌دهد که موافقت خود را برای ارسال بسته‌ها اعلام نموده، اما در انجام آن موفق نمی‌شوند. در سال ۲۰۱۲، برای جلوگیری از حمله محروم‌سازی از سرویس، از روش پازل مشتری[3] که مبتنی بر ایده خسته شدن محاسباتی یک کاربر مخرب هنگام تلاش برای حمله است، به همراه بازی‌های مبتنی بر همکاری[4]، استفاده شد [۲]. در سال ۲۰۱۲، به بررسی کاربردهای نظریه بازی در شبکه‌های حسگر بی‌سیم پرداخته شد [۳] و برخی از زمینه‌های تحقیقاتی برای اطمینان از امنیت شبکه‌های حسگر بی‌سیم بر اساس نظریه بازی‌ها، از جمله اعتبار ایستگاه پایگاه، کارآیی سامانه تشخیص نفوذ، تحرک شبکه‌های حسگر بی‌سیم، کیفیت خدمات، قابلیت استفاده در دنیای واقعی، مصرف انرژی، یادگیری گره‌های حسگر و گسترش برنامه‌های کاربردی نظریه بازی ارائه شد. در سال ۲۰۱۶، به بررسی روش‌های نظریه بازی در کاربردهای امنیت سایبری بر اساس طبقه‌بندی‌های امنیتی پرداخته شد [۴] که در جدول (۱) بیان شده است.

[1] Denial of Service Attacks (DoS)
[2] Sensor Network
[3] Client Puzzle
[4] Cooperative Game

جدول (۱): روش‌های نظریه بازی در کاربردهای امنیت سایبری

مسائل امنیتی	مدل‌های بازی		
امنیت شبکه‌های موردی[1] موبایل	مدل‌های بازی ایستا		بازی‌های مبتنی بر همکاری
تشخیص نفوذ	مدل‌های بازی ایستا		بازی‌های مبتنی بر عدم همکاری
بهینه‌سازی سرمایه‌گذاری امنیتی			
بهینه‌سازی سرمایه‌گذاری امنیتی	مدل‌های بازی پویا	مدل‌های بازی مبتنی بر اطلاعات کامل	
سازوکار تشویق امنیتی			
تجزیه و تحلیل حمله- دفاع سایبری		مدل‌های بازی مبتنی بر اطلاعات ناقص	

در سال ۲۰۱۷، یک راه حل امنیتی بر اساس نظریه بازی دو نفره[2] برای تشخیص حملات محروم‌سازی از سرویس و جلوگیری از مشکلات خدمات شبکه اینترنت اشیاء پیشنهاد شد [۵]. در سال ۲۰۱۷، رویکردهای نظریه بازی برای امنیت سایبری و مسائل مربوط به حریم خصوصی بررسی شد [۶] که در جدول (۲) بیان شده است.

جدول (۲): رویکردهای نظریه بازی برای امنیت سایبری و مسائل مربوط به حریم خصوصی

مسائل امنیت و حریم خصوصی	مدل‌های بازی
حریم خصوصی در شبکه‌های اجتماعی موبایل	بازی معضل زندانیان ایستا
تداخل و استراق سمع	بازی ایستا مجموع- صفر
امنیت سایبری و فیزیکی و یکپارچگی داده‌ها و در دسترس بودن	بازی استکلبرگ[3]
ارسال بسته‌ها در شبکه	بازی ائتلافی
امنیت سایبری و فیزیکی امن	بازی تصادفی با مجموع- صفر
حریم خصوصی مسیر	بازی بیزین
حریم خصوصی مسیر	بازی پویا
خودخواهی در ارسال بسته‌ها	بازی تکراری
پیکربندی سامانه تشخیص نفوذ	بازی مارکو
خودخواهی در شبکه‌های موردی خودرو	بازی تکاملی

در سال ۲۰۱۷، به‌منظور بهینه‌سازی، مدل الگوریتم‌های تکاملی مبتنی بر نظریه بازی تکاملی معرفی شد [۷] که در واقع سازوکاری برای تبدیل یک بازیکن به تصمیم گیرنده منطقی است. در سال ۲۰۱۹، یک مدل نظری بازی ارائه شد که از تعادل نش[4] برای نشان دادن تلاش حمله دشمن و تأیید سازوکار دفاعی در برابر همان حمله استفاده می‌کند [۸]. در این کار، ترکیبی از تئوری- بیز با الگوریتم خوشه بندی k-میانگین[5]، برای ارزیابی داده‌های بدون برچسب و کشف حملات بدافزار استفاده می‌شود. در سال ۲۰۱۹، یک بررسی مقایسه‌ای برای مسیریابی مبتنی بر نظریه بازی برای شبکه‌های حسگر بی‌سیم انجام شد [۹] که در آن از بازی‌های مبتنی بر همکاری، بازی‌های مبتنی بر عدم همکاری و بازی‌های تکاملی استفاده شده است. در سال ۲۰۱۹، به بررسی کاربردهای نظریه بازی در بلاک چین[6] پرداخته شد[۱۰] که در آن از بازی‌های مبتنی بر عدم همکاری، بازی‌های تصادفی و بازی‌های تکراری استفاده شده است. در سال ۲۰۱۹، به نقش نظریه بازی، برای به اشتراک گذاری منابع در سامانه‌های توزیع شده بزرگ پرداخته شد [۱۱] که بر اساس بازی‌های مبتنی بر همکاری و بازی‌های مبتنی بر عدم همکاری است. در سال ۲۰۲۰، به بررسی نظریه بازی‌ها در الگوریتم‌های توزیع شده به‌منظور تولید بازی‌های مبتنی بر موبایل پرداخته شد [۱۲] که در آن الگوریتم‌های توزیع شده برای رسیدن به تعادل نش مورد مطالعه قرار گرفته و مدل‌های هم‌زمان و غیر هم‌زمان برای بزاری‌های چند نفره در نظر گرفته شده است. در سال ۲۰۲۱، تجزیه و تحلیل پایداری سامانه‌های کنترل شبکه تحت حملات محروم‌سازی از سرویس مورد مطالعه قرار گرفته است [۱۳] که نظریه بازی برای ایجاد یک بازی غیر همکار بین مدافع و مهاجم معرفی شده است.

۱-۴- هدف پژوهش

هدف اصلی این مقاله ارائه الگویی مناسب در برابر حوادث امنیتی سایبری بر اساس نظریه بازی‌ها در شبکه‌های رایانه‌ای می‌باشد که در قالب روشی برای مدیریت جریان ورودی به‌منظور جلوگیری از حمله محروم‌سازی سرویس ارائه شده است که از این ساختار و الگو می‌توان در برابر حوادث رایانه‌ای در مدیریت بحران استفاده نمود. در واقع این پژوهش یک سازوکار دفاعی مبتنی بر نظریه بازی را پیشنهاد می‌نماید که به‌عنوان یک سامانه پشتیبانی تصمیم برای مدافعان شبکه، در برابر حملات محروم‌سازی سرویس کار می کند و به تنظیم یک حد بالا یا آستانه بهینه در ترافیک ورودی در هر جریان به‌صورت پویا کمک می‌کند. در واقع در این مقاله، وضعیت، به‌صورت یک بازی دو نفره مدل می‌شود و بهینه‌سازی بر اساس نقاط زین یا تعادل نَش بازی با استفاده از شبیه‌سازی و محاسبات عددی انجام می‌شود.

[1] Ad Hoc Mobile Network
[2] Two-player Game
[3] Stackelberg Game
[4] Nash Equilibrium
[5] K-means
[6] Block Chain

۲- روش تحقیق و ابزارها

رویکرد حل مسئله یکی از اساسی‌ترین بخش‌های یک پژوهش است که این مهم به این بخش اختصاص یافته است. با توجه به تعریف و مدل ریاضی مسئله این پژوهش، روش حلی برای آن در نظر گرفته شده است. به‌منظور حل مسئله روش حل دقیق پیشنهاد شده است. نرم‌افزار شبیه ساز ان اس۳[1] یک ابزار قدرتمند در زمینه شبکه و نسخه جدید شبیه ساز اان اس۲[2] برای شبیه‌سازی شبکه‌های رایانه‌ای است که یک پروژه منبع باز و در حال توسعه می‌باشد که از سال ۲۰۰۶ شروع شده است. این نرم‌افزار برای سکوهای[3] شبیه‌سازی شبکه باز قابل توسعه بوده و ارائه شده به‌منظور پژوهش و آموزش در زمینه شبکه می‌باشد. در واقع، شبیه‌ساز ان اس۳، مدل کار بسته‌های اطلاعاتی شبکه را ارائه داده و یک موتور شبیه‌سازی قوی را برای انجام آنالیزهای شبیه‌سازی فراهم می‌سازد. پروژه ان اس۳ به‌عنوان یک سامانه کتابخانه نرم‌افزار که با یکدیگر کار می‌کنند، ساخته شده است. برنامه‌های کاربر می‌تواند به این کتابخانه‌ها لینک (یا وارد[4]) شود. برنامه‌های کاربر همچنین می‌تواند در زبان برنامه نویسی سی پلاس پلاس[5] یا پایتون[6] نوشته شود. این نرم‌افزار مبنای حل دقیق برای مدل پیشنهادی این پژوهش است. این رویکرد در حقیقت به‌منظور حل مثال‌های واقعی طراحی نشده، بلکه هدف اعتبارسنجی مدل است. در بخش تئوری و محاسبات، مدل پیشنهادی با روش دقیق و با استفاده از این نرم‌افزار اعتبارسنجی خواهد شد. تیم‌های تحقیقاتی معمولاً از ماژول‌های[7] مختلف برای شبیه‌سازی‌های تحقیقات خود استفاده می‌کنند. فلو مانیتور[8] یکی از این مدل‌ها می‌باشد که برای کنترل جریان بسته‌ها استفاده می‌شود که متأسفانه در شرایط آزمایش‌های این پژوهش قابل استفاده نبود، زیرا به جای بازرسی، کاملاً به خروجی ردیابی شده بسته‌های داده[9] وابسته است و نمی‌تواند بسته‌ها را در هنگام عبور از پشته پروتکل[10] ان اس۳، بررسی کند. در حالی که نیاز به یک ماژول فیلترینگ بسته‌ها، بر اساس مدل نظریه بازی‌ها می‌باشد که بتواند آمار مربوط به آن را جمع‌آوری کند. بدین منظور از یک قلاب شبکه[11] استفاده می‌شود که برای مشاهده اطلاعات جریان بسته به‌کار برده می‌شود. البته از آنجا که در ادبیات مدلی مانند مدل ارائه شده، با مفروضات موجود ارائه نشده است، مقادیر تعدادی از پارامترهای مدل به‌صورت فرضی و تجزیه و تحلیل از عملکرد مدل ارائه شده است.

این تحقیق از نظر هدف توسعه‌ای می‌باشد، چون به دنبال یافتن روشی علمی مناسب برای حل یک مسئله است. از نظر ماهیت داده‌ها آمیخته (کمی و کیفی) و از نظر روش گردآوردی داده‌ها نیز توصیفی است. روش تحقیق در این پژوهش بر اساس ماهیت و نحوه گردآوری داده‌های آن، توصیفی (موردی و زمینه‌ای) است. با رویکرد آمیخته (کمی و کیفی) است. چون قرار است در یک مورد خاص (استفاده از نظریه بازی در مدیریت بحران) عمیقاً پژوهش به عمل آید. برای گرد آوری داده‌ها از منابع و مآخذ معتبر کتابخانه‌ای و اینترنت استفاده شده است.

۳- مفاهیم نظریه‌های مربوطه و فرضیه‌ها

۳-۱- معرفی نظریه بازی‌ها و انواع آن

یک بازی شامل مجموعه‌ای از بازیکنان، مجموعه‌ای از حرکت‌ها یا راهبردها و نتیجه مشخصی برای هر ترکیب از راهبردها می‌باشد. پیروزی در هر بازی تنها تابع شانس نیست، بلکه اصول و قوانین ویژه خود را دارد و هر بازیکن در طی بازی سعی می‌کند با به‌کارگیری آن اصول، خود را به برد نزدیک کند. بنابراین هر بازیکن هنگام تصمیم‌گیری برای انجام حرکت بهینه، می‌بایست تمامی واکنش‌های بازیکان دیگر را نسبت به حرکت خود، در نظر بگیرد، در حالی که حرکات سایر بازیکنان را با قطعیت نمی‌داند. اما درباره حرکت خود می‌بایست تصمیم‌گیری منطقی انجام دهد. در واقع برای هر بازی، ۳ بخش زیر ضروری است: ۱- بازیکنان، ۲- استراتژی بازیکان (در حیطه قواعد بازی) و ۳- دریافت‌ها و میزان بهینگی.

در هر بازی باید بازیکنان و عملکرد هر کدام از آن‌ها تعیین و مشخص شود. استراتژی بازیکنان برای سایر بازیکنان حریف نامشخص است و بر اساس احتمالات تعیین می‌شود. سپس بر اساس احتمالات، پیش‌بینی و درخت تصمیم ایجاد می‌شود. همچنین هر بازی تحت قواعدی مشخص می‌باشد و استراتژی بازیکنان و حریف، بر این اساس مشخص می‌شود. انتظار می‌رود بر اساس قواعد بازی، بازیکنان استراتژی‌های خود را چنان انتخاب کنند که بهترین نتیجه (بهینگی) حاصل شود.

در حالت کلی بازی‌ها را می‌توان به ۳ گروه زیر دسته‌بندی نمود: ۱- بازی‌های مهارتی، ۲- بازی‌های شانسی و ۳- بازی‌های استراتژیک.

بازی‌های مهارتی، بازی‌های یک نفره‌ای هستند که در آن، بازیکن، کنترل تمام پیامدها را بر عهده دارد، مانند جلسه آزمون. بازی‌های شانسی، بازی‌های یک نفره‌ای هستند که در آن بر

[1] NS3
[2] NS2
[3] Platform
[4] Import
[5] C++
[6] Python
[7] Module
[8] Flow monitor
[9] Packet Data
[10] Protocol Stack
[11] Network Hook

خلاف بازی‌های مهارتی، بازیکن کنترل کاملی بر پیامدها ندارد و در واقع بخشی از رخدادهای بازی‌های شانسی، مبتنی بر انتخاب بازیکنان است و در واقع مبتنی بر عدم قطعیت می‌باشند. بازی‌های استراتژیک، بازی‌های دو یا چند نفره‌ای هستند که در آن هر بازیکن، کنترل جزئی بر روی نتایج دارد. این نوع از بازی، به گروه‌های زیر دسته‌بندی می‌شوند:

- بازی‌های ایستا و پویا[1]: در بازی‌های ایستا، حرکت بازیکنان به‌صورت ترتیبی می‌باشد، مانند شطرنج. اما در بازی‌های پویا، بازی با حرکت هم‌زمان چند بازیکنان انجام می‌شود و هیچکدام از بازیکنان در مورد نحوه بازی حریف، اطلاعی ندارند.

- بازی‌های با همکاری یا بدون همکاری[2]: در بازی‌های با همکاری، بازیکنان می‌توانند در هنگام بازی و یا قبل از آن، ارتباط آزاد داشته باشند، در صورتی که در بازی‌های بدون همکاری این امکان وجود ندارد. این نوع بازی‌ها دارای ساختار پیچیده‌ای هستند.

- بازی با اطلاع کامل و ناقص[3]: در بازی با اطلاعات کامل، تصمیم هر بازیکن مبتنی بر تمام حرکات قبلی سایر بازیکنان است، مانند شطرنج. اما اگر بازیکن به دلایلی، مجموعه‌ای از اطلاعات را در اختیار نداشته باشد، آن بازی با اطلاعات ناقص نامیده می‌شود.

- بازی با اطلاعات متقارن و نامتقارن[4]: در بازی با اطلاعات متقارن، هیچکدام از بازیکنان، اطلاعات بیشتری نسبت به سایرین ندارند و با جابه‌جایی استراتژی دو بازیکن، رخدادهای آن‌ها تغییر نمی‌کند، اما در بازی با اطلاعات نامتقارن، تعدادی از بازیکنان اطلاعات بیشتری نسبت به سایرین دارند.

- بازی‌های دو نفره و چند نفره[5]: در بازی‌های دو نفره تنها دو بازیکن مشغول رقابت هستند، اما در بازی‌های چند نفره، گروهی از افراد در حال رقابت با یکدیگر هستند.

- بازی‌های با مجموع صفر و مجموع غیر صفر[6]: در بازی‌های با مجموع صفر، ارزش بازی در فرآیند بازی، ثابت می‌ماند (کاهش یا افزایش نمی‌یابد) و سود یک بازیکن با زیان بازیکن دیگر همراه است. اما در بازی‌های مجموع غیر صفر، راهبردهایی موجود است که برای تمامی بازیکنان سودمند است.

- بازی‌های تصادفی و غیر تصادفی[7]: در بازی‌های غیر تصادفی، فرآیند بازی به‌صورت منطقی دنبال می‌شود اما در بازی‌های تصادفی، فرآیند بازی مبتنی بر تصادفی و اتفاقی می‌باشد.

- بازی‌های محدود و نامحدود[8]: در بازی‌های محدود، تعداد بازیکنان و استراتژی هر بازیکن محدود می‌باشد. اما در بازی‌های نامحدود بازیکنان استراتژی‌های نامحدودی دارند.

برای نمایش فضای بازی و حرکات بازیکنان، از سه روش زیر استفاده می‌شود:

شکل گسترده[9]، شکل متعارف[10] و شکل تابع مشخصه[11].

نمایش بازی در شکل گسترده، با استفاده از درخت، انجام می‌شود. در این روش، مجموعه گره‌های ممکن که بازیکن حرکت خود را از آن انتخاب می‌کند، مجموعه اطلاعاتی نامیده می‌شود. نمایش بازی در شکل متعارف، شامل بازی‌های دو نفره بدون همکاری است که هر دو بازیکن به‌صورت هم‌زمان، بازی می‌کنند. در این شکل نمایش، از ماتریس استفاده می‌شود. شکل تابع مشخصه، برای نمایش بازی‌های چند نفره مبتنی بر همکاری، مورد استفاده قرار می‌گیرد و حرکات بر اساس تابع مشخصه، نمایش داده می‌شوند.

۳-۲- حملات محروم‌سازی از سرویس[12]

در شبکه‌های رایانه‌ای، حمله محروم‌سازی از سرویس، به حملاتی گفته می‌شود که در آن نفوذگر با ارسال درخواست‌های بسیار زیاد به یک سرور یا رایانه، باعث استفاده بیش از حد منابع آن، مانند پردازنده سرور، بانک‌های اطلاعاتی، پهنای باند و... می‌شود، به‌طوری که منجر به از دسترس خارج شدن ماشین و منابع شبکه از دسترس کاربران می‌شود.

حملات محروم‌سازی از سرویس در دو قالب کلی زیر قرار می‌گیرند: حملاتی که خدمات و سرویس‌ها را خراب می‌کنند و حملاتی که خدمات و سرویس‌ها را با بسته‌های سیل‌آسا[13] مختل می‌سازند.

جدی‌ترین حملات، توزیع شده می‌باشند. در حملات محروم‌سازی از سرویس، نفوذگر از یک سامانه، به‌صورت مستقیم، برنامه خود را اجراء و درخواست‌ها را ارسال می‌نماید، اما در حملات توزیع شده محروم‌سازی از سرویس[14]، نفوذگر از چندین سامانه مختلف در شبکه، برای اجرای برنامه‌های خود استفاده می‌کند.

[1] Static and Dynamic Game Theory
[2] Cooperative and Non-Cooperative Game Theory
[3] Complete and Incomplete Information Game Theory
[4] Symmetric and Asymmetric Information Game Theory
[5] Two-person and N-person Game
[6] Zero and Non-Zero Sum Game
[7] Random and Non-Random Game
[8] Finite and Non-Finite Game
[9] Extensive
[10] Normal
[11] Functional
[12] Denial of Service Attacks (DoS)
[13] Flood
[14] Distributed Denial of Service (DDoS)

برخی از انواع حملات محروم‌سازی از سرویس به شرح زیر می‌باشند:

۱- حملات حجمی[1]: در این نوع حمله، تمامی پهنای باند شبکه مصرف می‌شود و سرویس گیرندگان[2] نمی‌توانند تمامی پهنای باند شبکه را مصرف کنند. این امر با طغیان پژواک[3] بسته‌های درخواست-پاسخ[4] در سویچ‌ها اتفاق می‌افتد.

۲- حملات سیل‌آسای اس وای اان[5]: در این نوع حمله از بسته‌های سیل‌آسای اس وای ان استفاده می‌شود که آدرس فرستنده‌های آن جعلی می‌باشد. در ساختار بسته‌های پروتکل کنترل انتقال (تی پی سی)[6] یکسری بیت‌های پرچم[7] وجود دارد که یکی از آن‌ها بیت اس وای ان[8] است که از رایانه مبدأ به رایانه مقصد، برای برقراری ارتباط بین آن‌ها ارسال می‌شود. اگر این بیت توسط رایانه مقصد دریافت شود، یک بیت تصدیق[9] از رایانه مقصد به رایانه مبدأ ارسال می‌شود.

۳- حملات تکه تکه شدن[10]: حملاتی هستند که از جمع‌آوری مجدد[11] بسته‌ها جلوگیری می‌کنند. تکه تکه شدن آی پی[12]، یک فرآیند در پروتکل آی پی[13] است که بسته‌ها را به قطعات کوچک‌تر تقسیم‌بندی می‌کند. این قطعات توسط میزبان، دوباره جمع‌آوری می‌شوند.

۴- حملات لایه کاربرد[14]: مهاجم با استفاده از خطاهای برنامه‌نویسی در برنامه، باعث انکار سرویس می‌شود. این امر با ارسال درخواست‌های کاربردی متعدد به هدف برای خسته کردن منابع هدف به‌دست می‌آید. بنابراین قادر به سرویس‌دهی به هیچ مشتری معتبری نیست.

۵- حملات شلیک[15]: در این نوع از حملات با ارسال به‌روزرسانی‌های جعلی، باعث آسیب دائمی به سخت‌افزار و در نتیجه غیر قابل استفاده بودن آن‌ها می‌شود.

۳-۳- بات نت

بات نت[16]، شبکه‌هایی هستند که با در اختیار گرفتن مجموعه‌ای از رایانه‌ها که بات[17] نامیده می‌شوند، تشکیل می‌شوند [۱۴]. این شبکه‌ها توسط یک چند مهاجم برای انجام فعالیت‌های مخرب کنترل می‌شوند.

۳-۴- تعادل نَش

تعادل نَش[18] یک مفهوم راه حل است که شرایط بازی پایدار بازی را توصیف می‌کند. هیچ بازیکنی ترجیح نمی‌دهد استراتژی خود را تغییر دهد، زیرا با توجه به اینکه سایر بازیکنان به استراتژی تعیین شده پایبند هستند، بازدهی او را کاهش می‌دهد. در واقع در تئوری بازی، تعادل نَش راه حلی شامل دو یا چند بازیکن است، که در آن فرض بر آگاهی هر بازیکن به استراتژی تعادل بازیکنان دیگر است و بدون هیچ بازیکنی که فقط برای کسب سود خودش با تغییر استراتژی یک جانبه عمل کند. اگر هر بازیکنی استراتژی را انتخاب کند هیچ بازیکنی نمی‌تواند با تغییر استراتژی خود در حالی که نفع بازیکن دیگر را بدون تغییر نگه داشته باشد عمل کند، سپس مجموعه انتخاب‌های استراتژی فعلی و بهره‌مندی مربوطه، تعادل نش را تشکیل می‌دهد. به‌عنوان مثال، علی و حسن در تعادل نَش است اگر علی در حال انجام بهترین تصمیم‌گیری که او می‌تواند با توجه به تصمیم‌گیری حسن داشته باشد و همچنین حسن بهترین تصمیمی که می‌تواند با توجه به تصمیم‌گیری علی داشته باشد. به همین ترتیب یک گروه از بازیکنان در تعادل نَش است اگر هر یک در حال انجام بهترین تصمیم‌گیری باشند که آن‌ها می‌توانند، با توجه به تصمیمات دیگران داشته باشند. با این حال، تعادلی که نَش است لزوماً به معنای بهترین بهره‌وری کل برای همه بازیکنان مربوطه نمی‌باشد، در بسیاری از موارد ممکن است تمام بازیکنان بهره‌وری خود را بهبود بخشند در صورتی که چگونه بتوانند به توافق بر روی استراتژی‌های مختلف از تعادل نَش برسند.

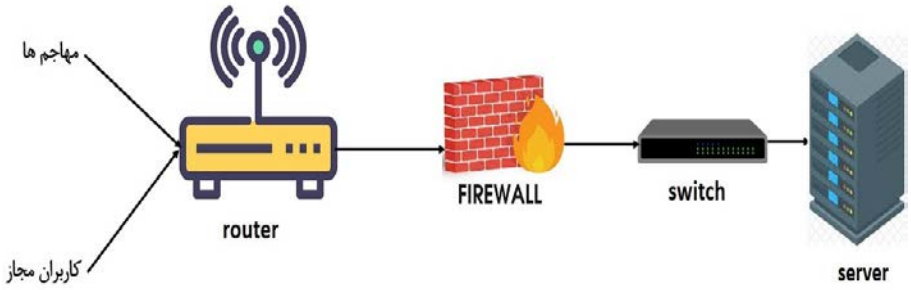
۴- یافته‌های تحقیق

۴-۱- مدل عمومی مسئله

این پژوهش، بر روی حملات محروم‌سازی از سرویس متمرکز می‌شود و تعامل بین مدافع (مدیر شبکه) و مهاجم را به‌عنوان یک بازی دو نفره در نظر می‌گیرد و اقدامات متقابل مبتنی بر نظریه بازی‌ها را اعمال می‌کند.

برای حملات محروم‌سازی از سرویس، یک مدل بازی ایستا ارائه شده است. در مدل بازی ایستا، هیچ بازیکنی مجاز به تغییر استراتژی نیست. مهاجم در تلاش است تا بیشترین نرخ ارسال بات نت را داشته باشند. چالش مدافع، تعیین تنظیمات بهینه برای دیواره آتش[19] برای جلوگیری از فعالیت‌های مخرب است.

[1] Volumetric Attacks
[2] Clients
[3] Echo
[4] Request/Reply Packets
[5] SYN flooding
[6] Transmission Control Protocol (TCP)
[7] Flag Bits
[8] SYN (Synchronize)
[9] ACK (Acknowledge)
[10] Fragmentation Attacks
[11] Reassembling
[12] IP Fragmentation
[13] Internet Protocol (IP)
[14] Application Layer Attacks
[15] Plashing Attacks
[16] Botnet
[17] Bot
[18] Nash Equilibrium
[19] Firewall



شکل (۱): توپولوژی عمومی مسئله

در این پژوهش از تعادل نش[1]، که بهترین استراتژی هر بازیکن را نشان می‌دهد، استفاده می‌شود. در مدل پویا، به هر بازیکن اجازه داده می‌شود تا استراتژی خود را در طول بازی، تغییر دهد.

برای بیان مسئله، یک توپولوژی عمومی شبکه در نظر گرفته شده است که مطابق شکل (۱) در آن یک سرور[2]، از طریق سویچ[3]، دیواره آتش و مسیریاب[4]، به اینترنت شده است. همچنین پهنای باند بین سویچ و دیواره آتش محدود است و در معرض حملات محروم‌سازی از سرویس قرار دارد.

کنترل مدافع، در دیواره آتش انجام می‌شود. هیچ کاربر مجاز که نیاز به برقراری ارتباط با سرور را داشته باشد، وجود ندارد. مهاجم، گره‌های حمله کننده را کنترل می‌کند که می‌توانند بسته‌های جعلی را ارسال کنند.

در مدل بازی پیشنهادی، اقدامات متقابل مهاجم و مدافع (مدیر شبکه)، به‌عنوان یک بازی دو نفره در نظر گرفته می‌شود و وجود تعادل در این بازی مورد بررسی قرار گرفته می‌شود. در مدل پیشنهادی مهاجم در تلاش است تا مؤثرترین میزان مدافع، انجام بهترین تنظیمات بر روی دیواره آتش در مقابل حملات مهاجم باشد. در یک بازی، هر بازیکن در حالی که اقدامات منطقی سایر بازیکنان را پیش‌بینی می‌کند، اقداماتی را انتخاب می‌کند که منجر به بهترین پاداش ممکن برای خود شود. یک استراتژی برای یک بازیکن یک برنامه کامل از اقدامات در تمام شرایط ممکن در طول بازی است.

تعادل نش[5] یک مفهوم راه حل است که شرایط بازی پایدار بازی را توصیف می‌کند. هیچ بازیکنی ترجیح نمی‌دهد استراتژی خود را تغییر دهد، زیرا با توجه به این که سایر بازیکنان به استراتژی تعیین شده پایبند هستند، بازدهی او را کاهش می‌دهد.

۴-۲- مفروضات مدل

همچنین پیش‌فرض‌های زیر در نظر گرفته می‌شود:

یک مهاجم تمامی گره‌های حمله کنندگان را کنترل می‌کند که هر یک از آن‌ها بسته‌های جعلی را به سرور می‌فرستند. بین مسیریاب و دیواره آتش، پهنای باند بالایی وجود دارد که می‌تواند تمامی بسته‌های ورودی را پردازش کند.

مدافع هیچگونه اطلاعی از این که جریان از طرف یک کاربر مجاز یا یک مهاجم است، ندارد. با افزایش نرخ جریان، اعتقاد دیواره آتش به درستی جریان کاهش می‌یابد.

زمانی که سرعت جریان ورودی بیشتر از پهنای باند موجود باشد، بسته‌های جریان در دیواره آتش رها می‌شوند.

در یک جریان، مهاجم، یک آدرس منحصر به فرد را برای هر کدام از بسته‌ها، جعل نمی‌کند.

۴-۳- پارامترهای مدل

نمادهای استفاده شده در مدل پیشنهادی، در جدول (۳) بیان شده است.

جدول (۳): نمادهای استفاده شده در مدل پیشنهادی

نماد	معنا
S	سرور
R	مسیریاب
F	دیواره آتش
SW	سویچ
B	پهنای باند بین دیواره آتش و سویچ
N	تعداد کاربران مجاز
M	تعداد گره‌های مهاجم
r_l	نرخ بیت مورد انتظار از یک جریان مجاز
σ_l	انحراف معیار نرخ جریان مجاز
r_A	نرخ بیت جریان حمله
γ	حداقل نرخ بیتی که برای یک جریان زنده در نظر گرفته شده است

[1] Nash Equilibrium
[2] Server
[3] Switch
[4] Router
[5] Nash Equilibrium

۴-۴- بیان ریاضی مسئله

در مدل پیشنهادی، تعداد n کاربر مجاز را که می‌خواهند با سرور S ارتباط برقرار کنند، در نظر گرفته می‌شوند و میزان ارسال یک کاربر مجاز با یک متغیر تصادفی، نمایش داده می‌شود که با انتخاب n نمونه از یک توزیع نرمال، میزان ارسال کاربر مجاز نمایش داده می‌شود:

$$x_i \sim N\left(r_l, \sigma_l^2\right), i = 1,2,\ldots,n$$

که در آن، x_i نشان دهنده میزان ارسال کاربر i-ام است و r_l میانگین مقدار نرخ ارسال کاربر مجاز است و σ_l انحراف استاندارد[1] (انحراف معیار نرخ جریان مجاز) است. بنابراین نرخ جریان ورودی در حالت بدون انجام شدن حمله برابر است با:

$$T^{na} = X_1 + X_2 + \ldots + X_n$$

بنابر قانون پایه احتمال:

$$T^{na} \sim N\left(n.r_l, n.\sigma_l^2\right)$$

همچنین فرض می‌شود که پهنای باند B، با احتمال بالا به گونه‌ای در نظر گرفته شده که $T^{na} < B$.

در ابتدا مدل بازی استاتیک در نظر گرفته می‌شود که در آن یک مهاجم، تمامی گره‌های حمله کننده را کنترل می‌کند (در حملات محروم‌سازی از سرویس، تنها یک گره حمله کننده وجود دارد، در حالی که در حملات توزیع شده محروم‌سازی از سرویس، چندین گره حمله کننده وجود دارد). در مدل پیشنهادی، تعداد m گره حمله کننده وجود دارد. در این تحقیق اگر $m = 1$ باشد، سناریوی حملات محروم‌سازی از سرویس، در نظر گرفته می‌شود.

در یک بازی استاتیک، هنگامی که یک بازیکن، استراتژی خود را در نظر می‌گیرد، شانس دیگری برای تغییر آن ندارد و پاداش مهاجم لزوماً از نظر ارزش، با مدافع برابر نیست، یعنی می‌تواند یک بازی با جمع صفر یا یک بازی با جمع غیر صفر باشد. تنها اقداماتی که برای مهاجم در دسترس است، تنظیم میزان ارسال و انتخاب تعداد گره‌های حمله (m) است. فرض می‌شود که نرخ ارسال برای همه جریان‌های حمله یکسان است که توسط r_A نشان داده می‌شود. در هنگام حمله، نرخ جریان برابر است با:

$$T = \left(X_1 + X_2 + \ldots + X_n\right) + m.r_A$$

اگر $T > B$، انکار سرویس اتفاق می‌افتد. زمانی که سازوکار دفاعی وجود نداشته باشد، تمامی بسته‌های جریان، از دیواره آتش عبور می‌کنند. اگر $T > B$، فقط بخشی از هر جریان می‌تواند از دیواره آتش به سویچ برود. α، این مقدار را مشخص می‌کند که برای هر جریان یکسان است. می‌دانید که $(1-\alpha)$ مقدار از هر جریان در خروجی دیواره آتش کاهش می‌یابد. اگر نرخ بیت جریان، r باشد، فقط مقدار نرخ بیت αr، به سرور می‌رسد. فرض می‌شود که پهنای باند به روشی عادلانه تقسیم‌بندی می‌شود و $\alpha = \frac{B}{T}$. γ، حداقل نرخ بیتی است که برای یک جریان زنده در نظر گرفته شده است که به پروتکل ارتباطی خاص استفاده شده بستگی دارد و n_g، میانگین تعداد جریان‌های مجاز است که می‌توانند به سرور دسترسی پیدا کنند.

در این تحقیق، $n_g = n.P\left[X_i > \frac{\gamma}{\alpha}\right]$ که n برابر با تعداد جریان‌های مجاز است و عبارت $P\left[X_i > \frac{\gamma}{\alpha}\right]$ احتمال آن است که مقدار متغیر تصادفی X بزرگ‌تر از x است. به‌طور مشابه، α، مقداری از هر جریان حمله است که در خروجی دیواره آتش کاهش یافته است. بنابراین میانگین نرخ مصرف پهنای باند (توسط مهاجم) به‌صورت زیر محاسبه می‌شود:

$$v_b^{nd} = \frac{m.\alpha.r_a}{B} = \frac{m.r_A}{n.r_l + m.r_A} \quad (۱)$$

نسبت کاربران از دست رفته به تعداد کل کاربران به‌طور متوسط به‌صورت زیر محاسبه می‌شود:

$$v_n^{nd} = \frac{n - n_g}{n} = P\left[X_i < \frac{\gamma}{\alpha}\right] = P\left[X_i < \frac{\gamma\left(n.r_l + m.r_A\right)}{B}\right] \quad (۲)$$

هدف مهاجمان، افزایش v_b^{nd} و v_n^{nd} است که به‌عنوان پاداش در نظر گرفته می‌شود. همچنین فرض می‌شود که مهاجم برای کنترل گره حمله باید هزینه‌ای را متحمل شود. فرض می‌شود که هزینه کل مهاجم، یعنی v_c، متناسب با تعداد گره‌های حمله به‌کار رفته، یعنی m، می‌باشد: $v_c = m$. بازده خالص مهاجم را به‌عنوان یک جمع وزنی از سه مقدار فوق تعریف می‌شود:

$$V^a = w_b^a v_b^{nd} + w_n^a v_n^{nd} - w_c^a v_c \quad (۳)$$

که در آن، w_b^a، w_n^a و w_c^a ضرایب وزنی مهاجمان هستند.

از طرفی دیگر، بازده خالص مدافع به‌صورت مجموع وزنی، به‌صورت زیر محاسبه می‌شود:

$$V^d = -w_b^d v_b^{nd} - w_n^d v_n^{nd} + w_c^d v_c \quad (۴)$$

که در آن، w_b^d، w_n^d و w_c^d، ضرایب وزنی مدافع هستند.

[1] Standard Deviation

۵- پیاده‌سازی و تحلیل

۵-۱- روش حل

دیواره آتش عامل دفاعی مدیر شبکه است و بسته‌های یک جریان ورودی با یک احتمال که وابسته به نرخ جریان است، را کاهش می‌دهد. در این تحقیق برای نمایش این میزان کاهش، از یک تابع سیگموئید[1] استفاده شده است:

$$F(x) = \frac{1}{\left(1 + e^{-\beta\frac{(x-M)}{B}}\right)} \qquad (۵)$$

که در آن، پارامتر m، نمایش دهنده میزان جریان است که مقدار آن توسط مدافع کنترل می‌شود و نرخ کاهش برای آن برابر با ۰/۵ است و B یک پارامتر پیمایش است. دیواره آتش بسته‌های یک جریان با نرخ r را با احتمال $F(r)$ کاهش می‌دهد.

در بخش قبل بیان شد که r_l نشان دهنده نرخ مورد انتظار یک جریان مجاز است. میانگین نرخ جریان‌های مجاز عبور شده از دیواره آتش را با $r_l^{'}$ نمایش داده می‌شود و برابر است با:

$$r_l^{'} = r_l.\left(1-F\left(r_l\right)\right) \qquad (۶)$$

همچنین میانگین نرخ جریان‌های حمله که از دیواره آتش عبور کرده‌اند، برابر است با:

$$r_A^{'} = r_A.\left(1-F\left(r_A\right)\right) \qquad (۷)$$

اگر r_A را با $r_A^{'}$، و r_l را با $r_l^{'}$، در فرمول‌های (۱ و ۲)، جایگزاری کنید، نتایج زیر حاصل می‌شود:

$$v_b = \frac{m.r_A^{'}}{n.r_l^{'} + m.r_A^{'}} \qquad (۸)$$

$$v_n = P\left[X_i < \frac{\gamma\left(n.r_l + m.r_A\right)}{B}\right] \qquad (۹)$$

که در آن، v_b نرخ متوسط مصرف پهنای باند توسط مهاجم است و v_n نسبت کاربران از دست رفته به کل کاربران است.

همچنین می‌توان بازده V^a و V^d را از فرمول‌های (۳ و ۴)، با جایگزین کردن v_b^{nd} با v_b و v_n^{nd} با v_n، محاسبه نمود.

می‌توان از مفهوم تعادل نش برای تعیین بهترین مشخصات استراتژی این دو بازیکن استفاده نمود. هر بازیکن باید هدف خود را به حداکثر برساند. مهاجم باید مقادیر بهینه را برای m و r_A انتخاب کند و مدافع باید بهترین مقدار M را برای تابع سیگموئید انتخاب کند تا توسط دیواره آتش استفاده شود. تعادل نش این بازی به‌عنوان یک زوج استراتژی تعریف شده که به‌طور هم‌زمان دو رابطه زیر را برآورده می‌کند:

$$\forall r_A, m \; v^{a}_{\left(r_A^*, m^*, M^*\right)} \geq v^{a}_{\left(r_A, m, M^*\right)}$$

$$\forall M \; v^{d}_{\left(r_A^*, m^*, M^*\right)} \geq v^{d}_{\left(r_A, m, M^*\right)}.$$

۵-۲- پیاده‌سازی مدل پیشنهادی

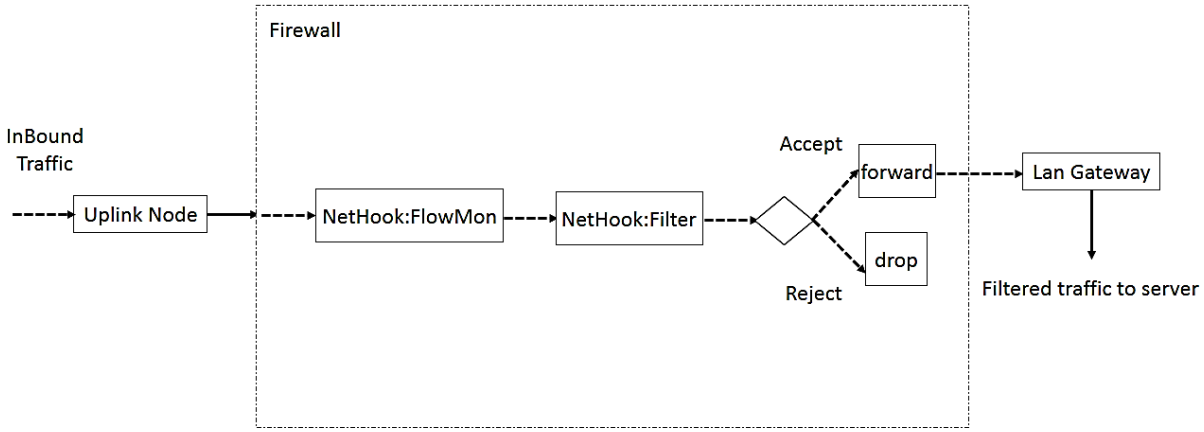
برای پیاده‌سازی مدل پیشنهادی از یک قلاب شبکه[2] استفاده می‌شود که برای مشاهده اطلاعات جریان بسته به‌کار برده می‌شود. در برنامه نویسی رایانه‌ای، اصطلاح قلاب‌سازی[3] طیف وسیعی از روش‌ها را برای تغییر یا تقویت رفتار سیستم عامل، برنامه‌ها یا سایر مؤلفه‌های نرم‌افزار با رهگیری مکالمات عملکردی یا پیام‌ها یا رویدادهای منتقل شده بین اجزای نرم‌افزار به‌کار می‌برد. کدی که چنین تماس‌های عملکردی، رویدادها یا پیام‌های رهگیری را کنترل می‌کند، قلاب نامیده می‌شود. این مفهوم در هسته لینوکس[4]، برای فیلتر کردن بسته‌ها، نَت[5] (ترجمه آدرس شبکه) و بسته‌های صف برای بازرسی از کاربر به‌طور گسترده‌ای مورد استفاده قرار گرفته است. نت فیلتر لینوکس[6] (چارچوبی است که توسط هسته لینوکس ارائه شده است و اجازه می‌دهد عملیات مختلف مربوط به شبکه در قالب کنترل کننده‌های سفارشی پیاده‌سازی شود) پیگیری اتصال را از طریق استفاده از قلاب‌های مختلف در کد شبکه هسته امکان پذیر می‌کند. این قلاب‌ها، مکان‌هایی هستند که کد هسته، به‌صورت ایستا یا به‌صورت ماژول قابل بارگیری، می‌تواند توابع را برای فراخوانی رویدادهای خاص شبکه در مکان‌های از پیش تعریف شده درون پشته پروتکل ثبت کند.

نت فیلتر لینوکس، قلاب‌ها را هنگام عبور بسته از طریق پشته پروتکل در مکان‌های زیر پیاده سازی می‌کند: پیش مسیریابی[7]، تحویل محلی[8]، جلو و بعد از مسیریابی[9]. هر قلاب مربوط به مکان‌هایی است که ممکن است فردی در آن رد شود و بسته را رد کند. متأسفانه، این مؤلفه هنوز دران اس۳ وجود ندارد. برای غلبه بر این محدودیت، در این پژوهش، یک ماژول ان اس۳

[1] Sigmoid

[2] Network Hook
[3] Hooking
[4] Linux Kernel
[5] NAT (Network Address Translate)
[6] Linux Net-Filter
[7] Pre-Routing
[8] Local Deliver
[9] Forward and Post-Routing

جدید به نام قلاب شبکه ایجاد شده که می‌تواند در هر گره با پشته پروتکل شبکه جمع شود و توسعه دهنده می‌تواند ماژول بازرسی خود را ادغام کند. این ماژول جدید قابلیت دستکاری بسته‌ها را در هر مکان درون پشته پروتکل فراهم می‌کند. شکل (۲) پیاده‌سازی قلاب شبکه را در مدل پیشنهادی نشان می‌دهد.



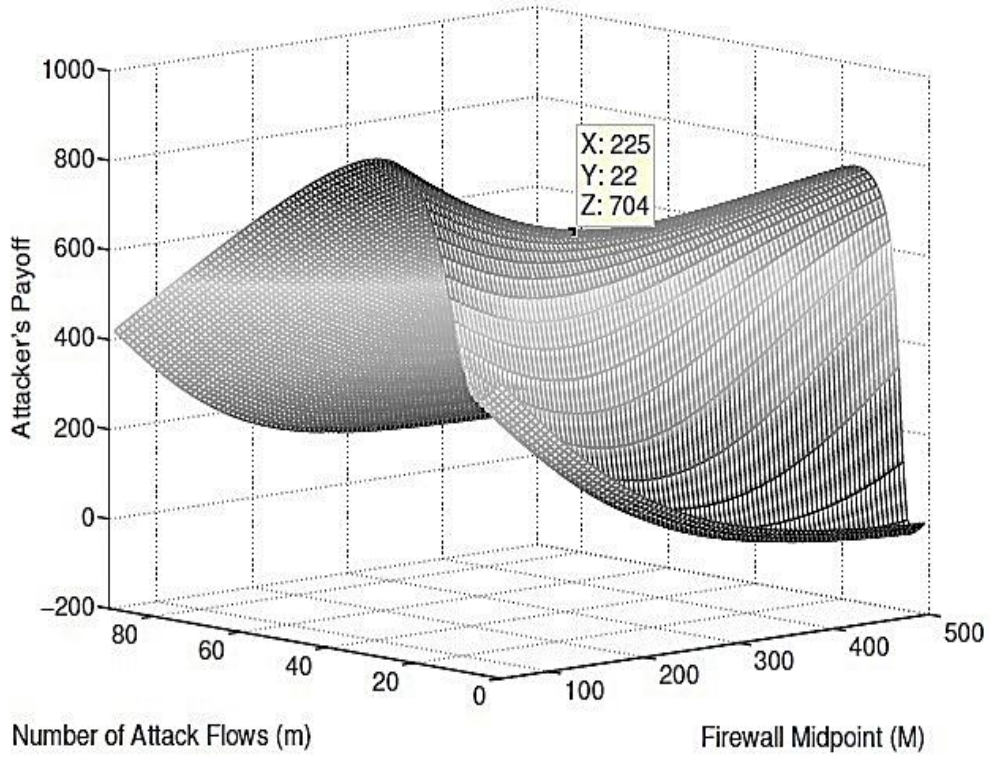
شکل (۲): پیاده‌سازی قلاب شبکه در مدل پیشنهادی

۵-۳- حل مسئله نمونه

در مدل پیشنهادی، به‌عنوان مثال، اگر مدافع و مهاجم، ضرایب وزنی یکسانی داشته باشند، یعنی: $V^{a}=-V^{d}$ و $w_{b}^{a}=w_{b}^{d}$ و $w_{n}^{a}=w_{n}^{d}$، می‌توان با مقداردهی پارامترهای مورد نیاز به‌صورت زیر، تعادل نَش را محاسبه نمود:

$$w_{b}^{a}=1000, w_{n}^{a}=1000, w_{c}^{a}=10,$$
$$B=2000, n=20, r_{l}=60, \sigma_{l}=20,$$

با استفاده از تابع سیگموئید، مطابق شکل (۳) و قرار دادن پارامترهای فوق در معادلات (۳، ۴، ۸ و ۹) می‌توان تعداد جریان‌های مهاجم یعنی m^{*}، در تعادل نَش را به‌دست آورد.



شکل (۳): تابع سیگموئید و تعادل نَش با پارامترهای مشخص

در شکل (۳): مشاهده می‌شود که نقطه زینی برابر است با: $m^{*}=22, M^{*}=225$. در واقع بازده مهاجم برای تعداد مختلف حملات یعنی m، و مقادیر مختلف دیواره آتش یعنی M، در این شکل نمایش داده شده است که نقطه زینی همان تعادل نَش می‌باشد.

۵-۴- نتایج و بحث

برای بررسی ویژگی‌های مدل پیشنهادی، می‌بایست آن را با روش‌های مبتنی بر هوش مصنوعی و هوش محاسباتی، از قبیل یادگیری ماشین، شبکه‌های عصبی و... مقایسه نمود. استفاده از روش‌های یادگیری ماشین در تیم واکنش به حوادث رایانه‌ای، می‌تواند نتایج تشخیص را بهبود دهد. با آموزش یک مدل، با داده‌های تولید شده در زمان واقعی از دستگاه‌های مختلف در شبکه، این سامانه‌ها می‌توانند فعالیت‌های مشکوک را به‌طور مؤثرتری تشخیص دهند. البته این آموزش، نیاز به یک مجموعه داده[1] از محیط دارد که ریسک آموزش بر اساس داده‌های مشاهده شده با امکان توسعه مدل، در ورودی‌های دارای خطا، افزایش می‌یابد [۱۵]. بنابراین سامانه‌ها نمی‌توانند حملات در حال انجام را شناسایی کنند و الگوریتم‌های یادگیری ماشین نمی‌توانند تمام حملات را از هم تفکیک کنند. در حالی که مدل پیشنهادی نیازی به مجموعه داده نیست و به‌صورت هوشمند، بر اساس میزان حملات، واکنش مناسب ارائه می‌شود.

به‌منظور نمایش قابلیت‌های مدل پیشنهادی، یک مقایسه با یک مدل مشابه که اخیراً انجام شده، صورت می‌پذیرد که در آن از نظریه بازی دفاع در برابر حملات محروم‌سازی سرویس استفاده شده است [۱۶]. در این مدل مقایسه‌ای، فرآیند پیشنهادی مبتنی بر بازی دو نفره است که حمله محروم‌سازی سرویس را بر اساس کاهش پهنای باند در نظر می‌گیرد که در آن مهاجم می‌خواهد حداکثر پهنای باند با ظرفیت محدود را اشغال کند. مهاجم این کار را با سیل‌آسا نمودن شبکه با جریان‌های ناخواسته یا مخرب انجام می‌دهد. مهاجم باید نرخ حمله مؤثر در هر جریان را تعیین نماید. همچنین برای حمله مقرون به صرفه باید اندازه بهینه بات‌نت را انتخاب کند. قبل از حمله، تجزیه و تحلیل مبادله را انجام می‌دهد. اگر بازده یا سود به‌دست آمده کمتر از هزینه حمله باشد، از انجام چنین حمله محروم‌سازی سرویس پر هزینه‌تری خودداری می‌شود. از سوی دیگر، برای تعیین یک کران بالایی در ترافیک شبکه، مدافع باید یک آستانه بهینه برای هر جریان تنظیم کند تا حداکثر جریان حمله یا حذف شود. تنظیم خودسرانه یک آستانه برای نرخ جریان نیز می‌تواند باعث از بین رفتن جریان‌های قانونی شود. مدافع مقدار آستانه بهینه را با برآورد دقیق انتخاب می‌نماید تا از دست دادن جریان‌های قانونی به حداقل برسد. مدافع آستانه را به گونه‌ای تعیین می‌نماید که بتواند بازده مهاجم را به حداقل برساند. این مسئله بهینه‌سازی به‌عنوان یک بازی بین مهاجم و مدافع ارائه می‌شود. مجموعه‌های فعالیت و توابع هدف هر دو بازیکن، با استفاده از تابع توزیع پواسن تعریف شده است که نیازمند تنظیم پارامترهای مربوطه می‌باشد که در رابطه (۱۰) بیان شده است:

$$p\left(r_i^a \square \tau\right)=\frac{\lambda^{\tau}e^{-\lambda}}{\tau!} \qquad (۱۰)$$

که در آن، نرخ جریان حمله r_i^a برابر با آستانه تعیین شده τ ، در فرآیند پیشنهادی می‌باشد و λ میانگین مقدار نرخ جریان حمله است.

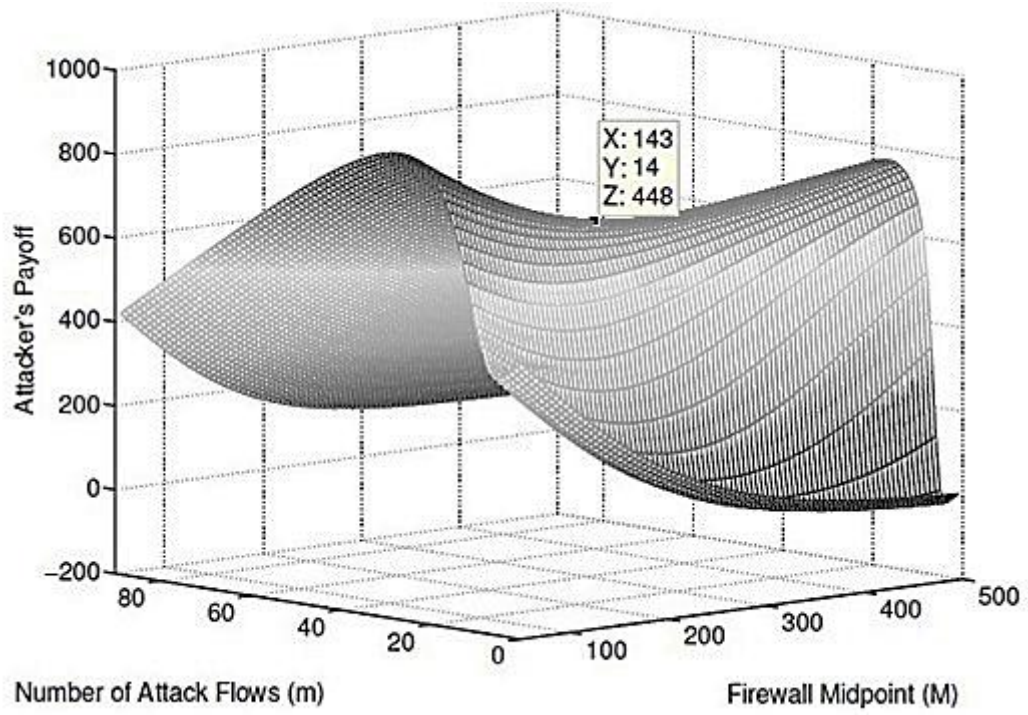
در این مقاله، در فرآیند پیشنهادی از توابع سیگموئید استفاده شده است. توابع سیگموئید دامنه‌ای از تمام اعداد واقعی را در بر می‌گیرد و با مقدار بازگشتی (پاسخ) معمولاً به‌طور یکنواخت افزایش می‌یابد، اما می‌تواند مقدار آن کاهش یابد. همچنین، تابع سیگموئید اغلب یک مقدار بازگشتی (محور y) را در محدوده ۰ تا ۱ نشان می‌دهد که این مقدار می‌تواند فرآیند تصمیم‌گیری را در مسئله بیان شده مشخص سازد. در حالی که یک مدل پواسن شبیه یک رگرسیون خطی معمولی است، با این تفاوت که مدل پواسن فرض می‌کند که میانگین و واریانس خطاها برابر است. اما معمولاً در عمل، واریانس خطاها بزرگ‌تر از میانگین است (اگرچه می‌تواند کوچک‌تر نیز باشد). در واقع به‌کارگیری توابع سیگومئید به جای فرآیند پواسن، می‌تواند به‌عنوان ارتقای یک رگرسیون خطی به رگرسیون غیر خطی در نظر گرفته شود.

شکل (۴) حل مسئله نمونه با پارامترهای مطرح شده در بخش ۵-۳ را بر اساس به‌کارگیری تابع پواسن، نمایش می‌دهد. مشاهده می‌شود که به‌کارگیری تابع پواسن، دارای تأثیرپذیری کمتری نسبت به مدل پیشنهادی دارد. در واقع بازده مهاجم برای تعداد مختلف حملات یعنی m، و مقادیر مختلف دیواره آتش یعنی M، در این شکل، نسبت به شکل (۳) دارای مقادیر کمتری می‌باشد. همچنین مرتبه اجرایی[2] مدل پیشنهادی به دلیل عدم نیاز به آموزش، کمتر از روش‌های مبتنی بر آموزش و نمونه‌برداری[3] در یادگیری ماشین می‌باشد.

[1] Data Set

[2] Order

[3] Training and Sampling



شکل (۴): تابع پواسن و تعادل نَش با پارامترهای مشخص

۶- نتیجه‌گیری

در این تحقیق، یک مدل پیشنهادی برای مدیریت بحران، در یک شبکه در برابر حملات محروم‌سازی از سرویس، بر اساس نظریه بازی‌ها ارائه شده است که در آن اقدامات متقابل مهاجم و مدافع (مدیر شبکه)، به‌عنوان یک بازی دو نفره استاتیک، در نظر گرفته شد و وجود تعادل در این بازی مورد بررسی قرار گرفت که می‌توانند در یک تیم واکنش به حوادث سایبری مورد استفاده قرار گیرد. واکنش این تیم‌ها معمولاً مبتنی بر عملکرد انسانی می‌باشد که به‌کارگیری مدل پیشنهادی، می‌تواند در موقعیت‌های تصمیم‌گیری استراتژیک مدافع و یا تجزیه و تحلیل انگیزه‌های مهاجمان، نسبت به تصمیم‌گیری‌های انسانی که ممکن است دچار خطا شوند، تأثیرگذاری بهینه‌تری داشته باشد.

در مدل پیشنهادی، بازده هر بازیکن به مؤلفه‌های زیر بستگی دارد:

- درصد پهنای باند مصرف شده توسط گره‌های مجاز و حمله کننده.

-مقداری از گره‌های مجاز فعال با نرخ بیت‌های مختلف یا یکسان، در شبکه ارسال می‌شوند.

با استفاده از تعادل نَش در شبکه، بر مبنای به‌کارگیری تابع سیگموئید، می‌توان از اثربخشی حملات مهاجم جلوگیری نمود. مهاجم می‌تواند برای عبور از دیواره آتش، تعداد گره‌های حمله کننده را افزایش دهد در حالی که نرخ بیت هر گره کاهش می‌یابد. بنابراین در این مدل، مدافع با انتخاب یک نقطه‌زینی مناسب، در حالی که ترافیک حمله را انکار می‌کند، هم‌زمان به بیشترین میزان ترافیک مجاز، اجازه عبور دهد.

در کارهای آتی، می‌توان یک مدل پیشنهادی بر اساس بازی‌های پویا برای حملات توزیع شده محروم‌سازی از سرویس ارائه نمود.

۷- مراجع

[1] A. Agah, M. Asadi, and S. K. Das, "Prevention of DoS Attack in Sensor Networks Using Repeated Game Theory," in ICWN, 2006, pp. 29-36.

[2] A. Michalas, N. Komninos, and N. R. Prasad, "Cryptographic Puzzles and Game Theory Against Dos and Ddos Attacks in Networks," Int. J. of Computer Research, vol. 19, no. 1, pp. 79, 2012.

[3] H.-Y. Shi, W.-L. Wang, N.-M. Kwok, and S.-Y. Chen, "Game Theory for Wireless Sensor Networks: A Survey," Sensors, vol. 12, no. 7, pp. 9055-9097, 2012.

[4] Y. Wang, Y .Wang, J. Liu, Z. Huang, and P. Xie, "A survey of Game Theoretic Methods for Cyber Security," in 2016 IEEE First Int. Conf. on Data Sci. in Cyberspace (DSC), IEEE, pp. 631-636,2016.

[5] F. Yazdankhah and A. R. Honarvar, "An Intelligent Security Approach Using Game Theory to Detect DoS attacks in IoT," Int. J. Adv. Comput. Sci. Appl., vol. 8, pp. 313-318, 2017.

[6] C. T. Do et al., "Game theory for cyber security and privacy," ACM Computing Surveys (CSUR), vol. 50, no. 2, pp. 1-37, 2017.

[7] G .Yang, "Game theory-inspired evolutionary algorithm for global optimization," Algorithms, vol. 10, no. 4, p. 111, 2017.

[8] L. Gao, Y. Li, L. Zhang, F. Lin, and M. Ma, "Research on detection and defense mechanisms of DoS attacks based on BP neural network and game theory," IEEE Access, vol. 7, pp. 43018-43030, 2019.

[9] M. A. Habib and S. Moh, "Game theory-based routing for wireless sensor networks: A comparative survey," Applied Sciences, vol. 9, no. 14, p. 2896, 2019.

[10]Z. Liu, NC Luong, W Wang, D Niyato, P Wang., "A Survey on Applications of Game Theory in Blockchain," arXiv Preprint arXiv:1902.10865, 2019.

[11]S. Riahi and A. Riahi, "Game Theory for Resource Sharing in Large Distributed Systems," Int. J.l of Electrical & Computer Eng. (2088-8708), vol. 9 ,no. 2, pp. 78-89, 2019.

[12]M. Zargaryan and D. Gevorgyan, "Distributed Algorithms and Game Theory".

[13]L. Cheng, H. Yan, X. Zhan, S. Fan, and K. Shi, "Stability Analysis of Networked Control Systems under DoS Attacks in Frequency Domain via Game Theory Strategy ",Int. J. of Systems Sci.,vol. 52, no. 14, pp. 1-13, 2021.

[14]M. Antonakakis T April, M Bailey, M Bernhard., "Understanding the Mirai Botnet," In 26th {USENIX} security Symposium ({USENIX} Security 17), pp. 1093-1110, 2017.

[15]R. Gore, S. Y. Diallo, J. Padilla, and B. Ezell, "Assessing Cyber-Incidents Using Machine Learning," Int. J. of Information and Computer Security, vol. 10, no. 4, pp. 341-360, 2018.

[16]B. Kumar and B. Bhuyan, "Using Game Theory to Model DoS Attack and Defence," Sādhanā, vol. 44, no. 12 ,pp. 1-12, 2019.

A Model for Managing Input Stream in Computer Networks to Prevent Denial-of-Service Attack Based on Game Theory

P. Gholamnezhad*

Abstract

In computer incidents, the benefits of the attacker's (defender) strategy depend heavily on the performance of the defender (attacker). Thus, the effectiveness of the crisis management mechanism relies on the strategic behaviors of the defender and the attacker, and the use of an effective tool, based on information technology can lead to a significant increase in the efficiency. The DoS attacks based on bandwidth reduction are a constant threat to network security. The proposed methods, due to the lack of quantitative approaches in modeling defense strategies against these attacks, cannot solve the problem effectively. Game theory can provide a framework for modeling such attacks. A game theory-based model can act as a decision support system for the defender and enhance its ability to make the best decisions to maintain an optimal level of network security against such attacks. In this paper, a proposed model for responding to the DoS attacks, based on game theory, is presented as a game between attacker and defender. The network is also modeled and the efficiency is calculated. The results show that the game converges to the Nash equilibrium and the best action is inferred from this strategy. The results obtained by simulation and numerical calculations are in favor of the proposed theoretical defense mechanism of the game and support the merit of using game theory to defend against DoS attacks to strengthen network security.

Key Words: *Game Theory, Computer Incident Response Team, Network Attacks, Computer Systems Security*

* Ph.D. Faculty of Computer Engineering and Information Technology, Shahid Sattari University of Aeronautical Sciences and Technology, Tehran, Iran. (pezhman.gholamnezhad@gmail.com) - Writer-in-Charge