

ارائه مدلی جهت استفاده از عاملهای متحرک در سیستم‌های تشخیص نفوذ توزیع شده مبتنی بر تئوری بازی

*آمین نظارت
**مهدی رجا
***غلامحسین دستغیبی فرد

* استادیار، گروه کامپیوتر و فناوری اطلاعات، دانشگاه پیام نور، ایران
** بخش مهندسی و علوم کامپیوتر، دانشگاه شیراز
*** دانشیار، بخش مهندسی و علوم کامپیوتر، دانشگاه شیراز

تاریخ دریافت: ۹۲/۰۸/۰۱ تاریخ پذیرش: ۹۵/۰۸/۲۳

چکیده

سیستم‌های تشخیص نفوذ در شبکه، ابزارهایی هستند که به منظور محافظت از منابع شبکه در مقابل حملات استفاده می‌شوند. با توجه به گستردگی حملات در فضای اینترنت و تغییر در شکل و نوع حملات از حالت متمرکز به توزیع شده، معماری اینگونه سیستم‌ها نیز به سمت توزیع‌شدگی حرکت می‌کند. در این مقاله روشی مبتنی بر عاملهای متحرک که به عنوان سنسورهای تشخیص‌دهنده حرکات غیر معتبر عمل می‌کنند پیشنهاد شده است. عاملهای متحرک تشخیص‌دهنده حمله^۱ به صورت پراکنده در شبکه در حال جابجایی از یک گره به گره دیگر می‌باشند و در هر زمان یک شبکه فوقانی^۲ امنیتی را ساخته و با استفاده از نوعی بازی همکارانه و برقراری ارتباط با یکدیگر، پس از رسیدن به مقدار شیبلی می‌توانند میزان و منشاء حمله را تشخیص و گزارش دهند. در این مقاله روشی پیشنهاد شده است که WGA در یک بازی غیرهمکارانه با عنصر مهاجم سعی در برقراری یک ارتباط مکاشفای جهت محاسبه مقدار نش و رسیدن به حداکثر سودمندی را دارد تا بتواند ضمن تفکیک حملات و یا درخواستهای واقعی، میزان و شدت حمله را با کمک سایر WGA بدست آورد.

واژه‌های کلیدی: عاملهای متحرک، IDS، تئوری بازی، سیستم چند عاملی، تعادل نش، مقدار شیبلی، امنیت شبکه

^۱ White Globule Agents
^۲ Overlay Network

۱- مقدمه

حملات و آسیب‌پذیری شبکه‌های کامپیوتری روز به روز چه از بعد پیچیدگی و چه تکنولوژی در حال گسترش می‌باشند. تا جایی که بعضی از این حملات به راحتی شرکت‌های تجارت الکترونیکی را از گردونه تجارت خارج می‌کنند. سیستم‌های تشخیص نفوذ می‌بایستی بتوانند در کاهش آسیب‌ها و حملات به شبکه‌ها پیشنهادات مناسبی را ارائه نمایند. برای رسیدن به این هدف سازمانها و موسسات تجاری و دولتی اقدام به تاسیس مراکز عملیات امنیت جهت آنالیز و رصد گزارشات و حوادث نفوذ نموده‌اند.

به عنوان مثال یکی از ابزارهای امنیتی شرکت Symantec با عنوان Threat con warning Sys با اندازه‌گیری میزان آسیب‌پذیری شبکه درجه آنرا به مدیر شبکه گزارش می‌دهد [۱] و مدیر شبکه می‌تواند براساس آسیب‌پذیری، تمهیدات لازم را در نظر بگیرد. البته این سیستم از یک ساختار اندازه‌گیری دقیق استفاده می‌کند و معیارهای آن مبتنی بر روشهای ریاضی و محاسباتی نیست، که این امر می‌تواند مدیر شبکه را به اشتباه اندازد. علاوه بر این اندازه‌گیری مربوط مبتنی بر پایش داده‌های رد و بدل شده بین حمله‌کننده و دفاع‌کننده نیست. سیستم‌های تشخیص نفوذ اخیر را می‌توان به دو گروه تقسیم بندی کرد [۲]:

- ۱- واکنشی (Reactive) (مبتنی بر تشخیص تمضا یا مجوز جهت اجازه ورود یا خروج)
- ۲- کنشی (Proactive) (سرویسهای فوقانی امن، شبکه proxy و ...)

سرویسهای فوقانی امن^۳ دارای معماری هستند که برای جلوگیری از حملات و ایجاد آمادگی قبلی در مقابل حملات توزیع شده DOS استفاده می‌شود. اما روشی که در این معماری برای برقراری ارتباط با گره‌ها استفاده می‌شود مبتنی بر ارتباط دائمی است که سربار زیادی را بر روی شبکه تحمیل می‌نماید و این موضوع مانعی است در

مقابل گسترش بیشتر معماری [۳]. اگرچه روش کنشی بسیار کاراتر از مدل واکنشی است اما هنوز مسائل زیادی در پیاده‌سازی کارایی در این معماری باقی مانده است. سیستم‌های IDS متمرکز بسیار مستعد خطای تک نقطه^۴ هستند و می‌توانند توسط مهاجمین کشف و مورد تهاجم قرار گیرند. برای حل این مشکل می‌توان از تعداد بیشتری IDS استفاده کرد تا بتوان میزان حملات تشخیص داده نشده را کاهش داد. که البته این مسئله مستلزم پرداخت هزینه بیشتر می‌باشد.

قدرت یک سیستم تشخیص نفوذ در ایجاد یک تعادل بین تعداد مدافعان و میزان تشخیص‌های خطا یا عدم تشخیص‌ها می‌باشد. به همین منظور جهت مدل کردن حملات برای اندازه‌گیری درجه ریسک امنیتی (تهدید یک حمله) و کمک به تصمیم‌گیری در پاسخ مناسب به حملات ضروری به نظر می‌رسد که از یک روش توزیع شده تشخیص نفوذ بهره گرفته شود. عاملهای متحرک می‌توانند به عنوان مدافعانی در گره‌های شبکه در نظر گرفته شوند که به صورت خود مختار بین گره‌ها جابجا شوند و مجموعه‌ای از آنها تشکیل یک شبکه فوقانی از یک سیستم چند عامله را می‌دهند. هر عامل متحرک می‌تواند به منظور ایجاد درک بهتر از یک حمله امنیتی و تشخیص میزان خطر آن وارد یک تعامل با حمله‌کننده شود.

به منظور افزایش دقت در تصمیم‌گیری و کشف حمله می‌توان از تئوری بازیها در تعامل عامل تشخیص‌دهنده و مهاجم استفاده کرد. سپس هر یک عاملهای تشخیص‌دهنده می‌توانند در یک بازی دیگر به منظور بررسی میزان دقت نتیجه حاصله وارد یک مذاکره^۵ با سایر عاملهای درون شبکه فوقانی شوند. این بازی از نوع بازیهای همکارانه جهت رسیدن به یک توافق در خصوص میزان درجه ریسک امنیتی^۶ حمله مربوطه می‌باشد. در بازی اول که بین عامل متحرک WGA به عنوان مدافع و یک مهاجم صورت می‌گیرد، یک تعامل دوطرفه

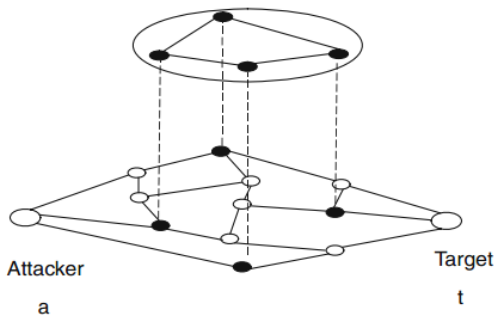
^۴ Single Point of Failure

^۵ Negotiate

^۶ Security Risk value

^۳ Secure Overlay Network

هر یک از این گروه‌ها میزبان یک عامل سیار است. این عاملها بایستی در هر لحظه به نحوی در گره‌های شبکه قرار گیرند که حداکثر پوشش امنیتی برقرار باشد و با توجه به سیار بودن آنها، حیطة حرکت عامل محافظ می-بایست به نحوی باشد که تجمع عاملها و یا خلا در شبکه بوجود نیاید. به همین دلیل و به منظور کاهش نرخ تشخیص خطا، افزایش نرخ تشخیص و کاهش مصرف پهنای باند شبکه، بایستی عواملی از جمله تعداد عاملهای محافظ، محیط تحت پوشش هر یک و درجه حساسیت امنیتی آنها مشخص و در طی زمان اصلاح و اعلام گردد. در این تحقیق به منظور افزایش مراقبت از شبکه و مقابله با مهاجمان معماری جهت شبکه فوقانی و مدیریت حرکت عاملها و همچنین بازی امنیتی جهت رسیدن به درجه حساسیت عامل (مقدار شیپلی) مورد بررسی و پیشنهاد قرار گرفته شده است [۴].



شکل ۱: شبکه فوقانی

۳- معماری مدل پیشنهادی سیستم چند عاملی محافظ

نظر به گستردگی شبکه‌های کامپیوتری و افزایش حجم مبادلات و ارتباطات درون شبکه‌ها و افزایش بار آنها، ایجاد ارتباطات دائمی و نگهداری آنها می‌تواند باعث افزایش سربار شبکه و ایجاد اختلال در کار اصلی نرم‌افزارهای موسسات گردد. سیستم‌های امنیتی و نظارتی بایستی بتوانند با کمترین اختلال در شبکه و حداقل سربارکاری به وظایف خود عمل نمایند.

یکی از انواع عاملها، نوع سیار آنها می‌باشد. یک عامل سیار، نوعی نرم‌افزار خود مختار، کنشی و متحرک می‌باشد که می‌تواند با جابجایی درون شبکه و بدون نیاز به کنترل مستمر توسط سرور اصلی، اقدام به انجام وظایف خود اعم از جمع‌آوری اطلاعات، مقابله با حملات، خرید و فروش یا مذاکره با سایر عاملها نماید و سپس نتایج حاصله را به

برقرار می‌شود که یک بازی از نوع غیرهمکارانه دونفره می‌باشد. هر دوطرف بازی به دنبال بیشینه کردن منافع و سودمندی خود می‌باشند. حمله‌کننده قصد نفوذ به شبکه و تخریب یا جمع‌آوری اطلاعات را دارد و مدافع نیز قصد مقابله و کشف تعدا بیشتری حملات به شبکه را دارد. هر دو بازیکن دارای یک تابع سودمندی^۷ هستند که در یک نقطه به تعادل کنش خواهند رسید که در آن نقطه هر دو بازیکن، نوعی از بازی خودرا که در آن تمایل به تغییر بازی ندارند را انجام می‌دهند. در این نقطه عامل متحرک مدافع به مقداری خواهد رسید که آن مقدار درجه امنیتی حمله را مشخص می‌نماید.

برای اطمینان از اینکه حمله‌ای صورت گرفته است یا خیر و جلوگیری از ارسال هشدارهای اشتباه در بازی دیگری از نوع همکارانه با سایر عاملهای مدافع در محیط چند عاملی اقدام به مذاکره می‌نماید. در این بازی عاملها می‌توانند جهت جلوگیری از ایجاد سربار در شبکه به صورت گروههای چند نفره تشکیل ائتلاف دهند. در هر ائتلافه با موضوع یک حمله تشکیل می‌شود عاملها پس از مذاکره به یک مقدار تفاهمی مشترک به نام مقدار شیپلی^۸ می‌رسند که این مقدار درجه نهایی امنیت شبکه و نوع تصمیم در مقابل حمله صورت گرفته را مشخص می‌نماید. با توجه به عدد بدست آمده می‌توان شدت و میزان برخورد را مشخص نمود.

۲- شبکه فوقانی چند عامله^۹

نوع توزیع عاملهای متحرک و نحوه قرارگیری آنها در هر زمان برای تحت پوشش قرار دادن بخش عمده‌ای از شبکه، یکی از مسائل مهم در تشکیل شبکه فوقانی و از عوامل تاثیرگذار در تصمیم هر عامل برای جابجایی در شبکه است.

به عنوان مثال: در شکل ۱ فرض شده که یک مهاجم قصد ارسال یک بسته از میزبان α (مهاجم) به میزبان t (مقصد) را دارد و یک شبکه فوقانی چند عاملی از گره‌های $MA = \{MA_1, MA_2, \dots, MA_n\}$ تشکیل شده است.

^۷ Utility function

^۸ Shaply value

^۹ Multi Agent overlay network

اطلاع سرور فرستنده عامل برساند بدون اینکه نیاز به بازگشت به سرور و اشغال پهنای باند داشته باشد و یا حتی نیاز به ارسال کلیه اطلاعات داشته باشد [۵].

امروزه کاربردهای فراوانی از سیستمهای مبتنی بر عاملها وجود دارد. عامل ها می‌توانند با تشکیل اجتماعات چند عاملی و برقراری ارتباطات هم‌افزا با یکدیگر به نتایج بسیار سریع و با کمترین دخالت انسانی برسند. عاملها همچنین می‌توانند یاد گرفته و تغییر شکل دهند و استراتژی اولیه را بهبود بخشند. در این مقاله از خصوصیت مذاکره عاملها استفاده شده و معماری پیشنهادی ارائه شده است.

به منظور جلوگیری از بزرگ شدن عاملها و درگیر شدن آنها در بررسی بسته‌های شبکه‌های کامپیوتری در این تحقیق از یکی از IDS های شناخته شده و Open source به نام SNORT استفاده شده است [۶].

SNORT یک IDS خوب و پرکاربرد می‌باشد که با بررسی بسته‌های شبکه و مطابقت آنها با سناریوهای حمله موجود در بانک دانش خود می‌تواند حملات را تشخیص دهد و پیام هشدار مناسب را ارائه نماید. اما همانگونه که قبلاً نیز اشاره شد این سیستم یک IDS مرکزی است و برای اینکه بتواند مجموعه‌ای از حملات به گره‌های مختلف شبکه را تشخیص دهد می‌بایستی در نقاط مختلف شبکه نصب شده و همچنین امکان برقراری ارتباط با یکدیگر را نیز داشته باشند. در حال حاضر این سیستم از چنین قابلیت‌هایی برخوردار نمی‌باشد و برای تحقق این امر بایستی تمامی log های حملات به سایر IDS مرکزی منتقل و ادغام کرده تا بتوان کل حمله را به درستی تشخیص داد. که در حال حاضر چنین امکانی وجود ندارد.

در مدل پیشنهادی که ترکیبی است از عاملهای متحرک، از یک سرور مرکزی به منظور تولید عاملها استفاده می‌شود. در اینجا از مدل دفاعی بدون الهام گرفته شده است. تعدادی عامل متحرک به عنوان گلوبولهای سفید در گره‌های شبکه مستقر شده و در زمانهای خاصی جابجا می‌شوند. ترکیب سرور شامل اجزاء زیر است:

- کارخانه تولید عاملهای گلوبولهای سفید^{۱۰}

- کارخانه تولید عاملهای خنثی کننده^{۱۱}

- SNORT

- پایگاه دانش حملات^{۱۲}

- کارخانه تولید عاملهای گلوبول سفید

این عامل وظیفه تولید عاملهای جدید مدافع را برعهده دارد. در ابتدای شروع به کار سیستم تعدادی محل WGAهایی که بایستی تولید شوند از قبل توسط مدیر شبکه تعیین می‌شوند و این عامل پس از تولید هر WGA آنها به گره‌ای از شبکه ارسال می‌کند. نوع حرکت عامل WGA به گره‌های شبکه از نوع جابجایی‌پذیری قوی^{۱۳} می‌باشد و در هر زمان وضعیت کلیه وقایع قبلی و نتیجه حاصله از آنها را به همراه دارد. هر عامل WGA به صورت دوره‌ای با این عامل ارتباط برقرار می‌کند و گزارشی از مشاهدات خود را اعلام می‌نماید. در هر لحظه این عامل می‌داند که هر WGA کجاست. تفاوت WGAهای تولید شده در این عامل این است که یک عامل WGA به همراه خود خلاصه‌ای از سناریوهای انواع حملات در شبکه‌ها را دارد و با کمک ابزار تشخیص نفوذ

SNORT، رفتارهای مشکوک در شبکه را شناسایی می‌کند. پس از شناسایی یک رفتار مشکوک با سایر عاملهای WGA مذاکره کرده و دانش خود را تکمیل یا تصحیح می‌نماید. این عامل از چندین عامل دیگر تشکیل شده است که هر یک وظیفه‌ای را بر عهده دارند:

عامل AMS^{۱۴}: مدیر اصلی عاملهاست و به هر عامل یک شماره اختصاصی انتساب می‌دهد. وظیفه ایجاد، حذف، جابجایی و ... عاملها را بر عهده دارد.

عامل DF^{۱۵}: این عامل اطلاعات کاملی از کلیه عاملهای ایجاد شده و در حال اجرا را در اختیار دارد. نام عامل، محل عامل، مشخصات و تاریخچه آن را می‌داند. زمانی که یکی از عاملهای WGA قصد برقراری ارتباط با سایر

^{۱۱} Lymphocit Agent Factory

^{۱۲} IDS knowledge

^{۱۳} Strong mobility

^{۱۴} Agent Management System

^{۱۵} Directory Facilitator

^{۱۰} White Global Agent Factory

شبکه امکان اعمال قوانینی را به کاربر می‌دهد. در این ابزار از تعدادی قانون جهت شناسایی حملات استفاده می‌شود و زمانی که سناریوی موجود در قوانین محقق شود عکس‌العمل مناسب را نشان می‌دهد. در این مقاله از SNORT جهت مطابقت سناریو با بسته‌های شبکه استفاده شده است.

پایگاه دانش حملات: در این پایگاه دانش سناریوهای مربوط به حملات امنیتی در شبکه درج شده است تا هر عامل WGA بدانند که در زمان بروز یک تهدید امنیتی (که با خواندن Log فایل SNORT قابل تشخیص است) چه اقدامی را انجام دهد. از آنجا که یک عامل WGA بایستی در زمانی که یک تهدید را حس می‌کند اقدام به تعامل با حمله‌کننده نماید، با استفاده از این دانش درون این پایگاه می‌داند که در مرحله بعدی چه عملی را بایستی انجام دهد تا حمله‌کننده قسمت بعدی حمله را به اجرا گذارد، لذا با شبیه‌سازی یک آسیب‌پذیری می‌تواند تهدید را تشخیص دهد.

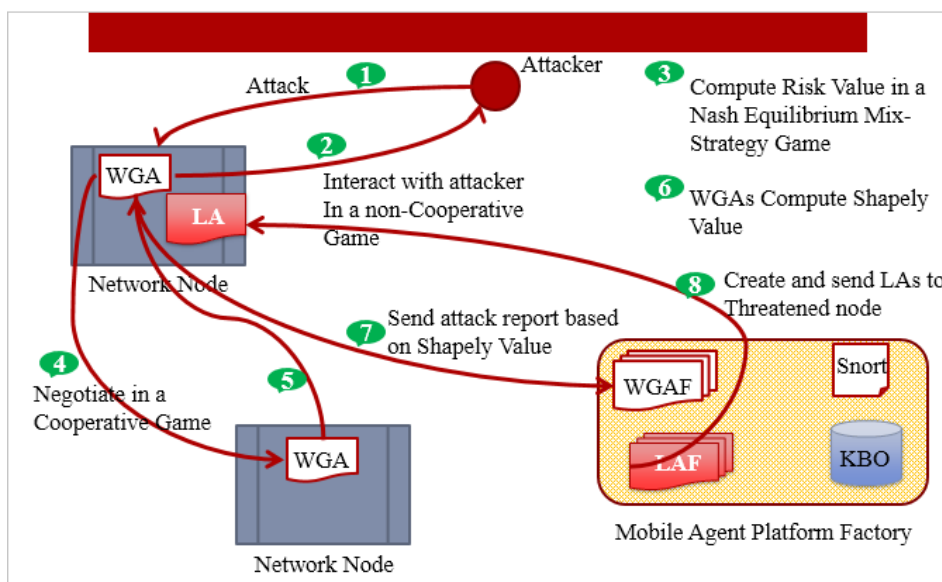
عاملها را داشته باشد، درخواست خود را به این عامل ارسال می‌نماید.

- کارخانه تولید عاملهای خنثی‌کننده (LAF)

یکی از وظایف سیستم‌های تشخیص نفوذ، جمع‌آوری اطلاعات و شناسایی حملات جهت گزارش‌دهی به سیستم‌های مقابله با حمله یا IDSها می‌باشد. در این مدل نوعی عامل در نظر گرفته شده است که وظیفه مقابله با حملات و از بین بردن حمله‌کننده را بر عهده دارد. پس از شناسایی و تایید یک حمله توسط ائتلافی از WGA گزارشی به WGAF ارسال می‌شود که درجه ریسک امنیتی این حمله را مشخص می‌نماید.

WGAF نیز با استفاده از درجه امنیتی، تقاضایی را برای این عامل ارسال می‌نماید و عامل مذکور بر همین اساس تعداد عاملهای LA و محلهایی که بایستی ارسال شوند را تشخیص می‌دهد.

- SNORT: یک ابزار متن باز IDS می‌باشد که با بررسی بسته‌های رد و بدل شده در شبکه و Sniff کردن



شکل ۲: مدل پیشنهادی سیستم توزیع شده تشخیص نفوذ

۴- روش کار مدل پیشنهادی

همانگونه که اشاره شد این مدل امنیتی از اجزاء مختلفی تشکیل شده است. در این بخش به نحوه کار مدل و روش اجرای آن پرداخته می‌شود. عامل WGAF تعدادی عامل WGA را ایجاد کرده و به گره‌های شبکه ارسال می‌کند. در صورت حمله یک عامل خارجی، WGA مستقر در آن گره شروع به تعامل با attacker می‌نماید. این عامل از نوع یک بازی غیر همکارانه می‌باشد. عامل WGA با کمک KB و اطلاعات حاصل شده از تعامل با مهاجم یک استراتژی آمیخته را پیش می‌گیرد تا بتواند به یک نقطه تعادلی نش برسد. این نقطه تعادلی نش به عنوان مقدار ریسک آن حمله در نظر گرفته می‌شود.

برای افزایش دقت مقدار ریسک و تشخیص این موضوع که آیا مشابه با این حمله در سایر گره‌های شبکه نیز شناسایی شده است یا خیر، عامل WGA اقدام به تشکیل یک ائتلاف با تعدادی از عامل‌های WGA دیگر می‌کند و در بازی همکارانه با آنها مذاکره می‌نماید تا در نهایت از مقادیر ریسک امنیتی بدست آمده در سایر WGAها به یک مقدار مورد توافق به نام مقدار شیپلی برسند. پس از محاسبه مقدار شیپلی، عامل WGA این مقدار را برای WGAF ارسال می‌نماید. این عدد به عنوان مقدار ریسک امنیتی شبکه که مورد توافق ائتلافی از WGAها می‌باشد در نظر گرفته شده و WGAF آن را به LAF گزارش می‌دهد و همچنین می‌تواند با توجه به این درجه امنیتی تصمیم به افزایش یا کاهش WGAها و یا تغییر مکان آنها بگیرد.

عامل LAF با دریافت درجه امنیتی جدید شبکه عامل-های خنثی‌کننده LA را ساخته و به گره‌های تهدید شده ارسال می‌کند. به هر گره تهدید شده یک عامل LA ارسال می‌شود و به وی تعداد تکثیرهای بعدی از خود را اعلام می‌کند. برای جلوگیری از اشغال پهنای باند شبکه، هر عامل LA پس از رسیدن به مقصد، خود را به میزان لازم تکثیر می‌کند تا بتواند با توجه به درجه امنیتی گزارش شده مقابله مناسب با حمله را داشته باشد.

با توجه به درجه امنیتی جدید بدست آمده برای شبکه، تعداد و محل قرارگیری WGAها توسط WGAF مورد بازنگری قرار گرفته و تعداد و محل‌های جدید اعلام می‌شود و در نهایت یک شبکه فوقانی از عامل‌های سیار و یک

محیط چند عاملی جدید ساخته می‌شود. ملاک‌های این تصمیم‌گیری بر مبنای پارامترهای: گره‌های تهدید شده، درجه تهدید هر گره، مسیر طی شده توسط یک مهاجم، تغییر درجه امنیتی نسبت به قبل و ... می‌باشد.

۵- بازی ریسک امنیتی

در حالت کلی، ریسک امنیتی به تعداد نفوذهایی که احتمال رخداد آنها وجود دارد گفته می‌شود (نرخ نقض امنیت). نفوذ امنیتی زمانی رخ می‌دهد که یک مهاجم بتواند از نواقص امنیتی استفاده کرده و وارد سیستم شود [۷] [۸]:

$$\text{Security risk} = \text{امنیت نقض تعداد نرخ}$$

$$\text{نفوذ هر هزینه میانگین} *$$

در این مقاله هدف تعیین میزان ریسک امنیتی است تا بتوان با استفاده از آن سیستم تشخیص نفوذ توزیع شده^{۱۶} را تنظیم کرد. در بازی امنیتی پیشنهادی نقش‌های زیر وجود دارد.

- مهاجم

- WGAgent

مهاجم: بطور دائم یک شبکه به کاربران مختلفی در حال سرویس‌دهی می‌باشد که بعضی از آنها می‌توانند به عنوان یک مهاجم باشند. هدف یک مهاجم نفوذ به درون شبکه و اجرای اهداف از قبل تعیین شده می‌باشد [۹]. اگر حمله یک مهاجم تشخیص داده نشود معادل b_1 هزینه پرداختی آن مهاجم می‌باشد. در صورت تشخیص حمله این هزینه معادل b_2 می‌باشد. همچنین اگر فرض می‌شود که $b_1 - b_2 < 0$ است یعنی مهاجم در صورتی که تشخیص داده شود یک سودمندی مثبت بدست می‌آورد و در صورتی که $b_1 - b_2 > 0$ باشد، سودمندی مهاجم منفی خواهد بود. در صورتی که یک مهاجم به WGA با شماره i که بر روی یکی از گره‌های شبکه قرار دارد حمله کند. دو پارامتر \hat{I}_1 , \hat{I}_2 را در نظر می‌گیریم که اولی میزان گسترش مهاجم از و دومی مربوط به پهنای باندی است که مهاجم برای حمله به عامل i ام اشغال می‌کند. این پارامتر توسط [۱۰] پیشنهاد

^{۱۶} Distributed IDS

جدول ۲: هزینه عایدی مهاجم

Attacker	نتیجه	هزینه
	نفوذ	$-b_1$
	عدم نفوذ	b_2

در نهایت هریک از دو بازیگر (WGA_i , attacker) یک مقدار سودمندی $payoff$ را متصور هستند که به صورت زیر برای هر یک محاسبه می‌شود. برای attacker میزان نتیجه بدین صورت است:

$$payoff_{att} = r_1 [p_d b_2 - b_1 (1 - p_d)]$$

که r_1 احتمال اینکه یک attacker رفتار خرابکارانه داشته و قصد نفوذ به سیستم را داشته باشد. مقدار بازده مورد انتظار WGA در IDS نیز به صورت زیر محاسبه می‌شود:

$$payoff_{WGA} = r_1 c_2 + p_d c_2 - r_1 p_d (c_1 + c_2 + c_3)$$

حال به بازی غیر همکارانه با استراتژی آمیخته بین دو بازیگر (WGA , attacker) می‌پردازیم مجموعه استراتژی‌هایی که هر یک از بازیگران می‌توانند داشته باشند بدین صورت است:

$$S_{attacker} = \{u_1, u_2, u_3\}$$

$$S_{WGA} = \{d_1, d_2\}$$

u_1 نشان‌دهنده یک حمله کامل‌تر توسط مهاجم با احتمال r_1 می‌باشد که قبلاً "عنوان گردید. u_2 را به عنوان استراتژی تکثیری یک حمله توسط مهاجم به نحوی که با احتمال r_2 به صورت گسترده اقدام به تکثیر خود نماید در نظر می‌گیریم.

u_3 نشان می‌دهد که با احتمال $1-r_1-r_2$ حمله‌ای صورت نمی‌گیرد. برای عامل نیز استراتژی d_1 نشان‌دهنده تشخیص یک نفوذ با احتمال q و اعلام هشدار لازم می‌باشد. استراتژی d_2 نیز حالتی را نشان می‌دهد که عامل هیچ عکس‌العملی را در مقابل حمله انجام نمی‌دهد. احتمال d_2 را با $1-q$ نشان می‌دهیم. با توجه به استراتژی‌های فرض شده میزان بازده مورد انتظار $payoff$ مهاجم و عامل را به صورت زیر بسط می‌دهیم. دلیل بسط بازده نوع بازی انتخابی است که از نوع استراتژی آمیخته در نظر گرفته شده است و برای اینکه بتوان احتمال کلیه استراتژی‌های فرض شده را در بازده نهایی لحاظ کرد جدول زیر را q -mix بازده انتظاری

شده‌اند. می‌توان نتیجه گرفت که یک حمله گسترش یافته λf_i از پهنای باند را اشغال می‌کند.

WGAgents: مجموعه‌ای از عامل‌های تشخیص‌دهنده WGA به صورت $N = \{WGA_1, WGA_2, \dots, WGA_n\}$ نمایش داده می‌شوند می‌باشد. این عاملها بر روی گره‌های شبکه مستقر شده و یک شبکه فوقانی چند عامله را برای تشخیص نفوذ و تشکیل یک IDS توزیع شده را می‌دهند. وظیفه این عاملها این است که با بررسی بسته‌های انتقالی درون شبکه کاربران عادی را از مهاجمین تشخیص دهند. فرض کنید که m_i نشان‌دهنده نرخ تحرک^{۱۷} عامل WGA_i در حرکت از یک میزبان به میزبان دیگر می‌باشد. عامل WGA_i بطور معمول می‌تواند دچار دو دسته خطا شود: دسته‌بندی مهاجم به عنوان کاربر عادی یا دسته‌بندی کاربر عادی به عنوان مهاجم. در این مدل به دنبال برقراری یک تعادل بین اینگونه هشدارها و هشدارهای صحیح می‌باشیم.

برای عامل WGA_i نرخ تشخیص نفوذ را با p_d (احتمال تشخیص) و نرخ عدم تشخیص را با $(1-p_d)$ نشان می‌دهیم و p_f را به عنوان احتمال تشخیص اشتباه حمله در نظر می‌گیریم. هزینه C_1 برای تشخیص یک حمله توسط WGA_2 و C_2 و C_3 به ترتیب هزینه‌هایی که IDS بابت تشخیص اشتباه و عدم تشخیص بایستی بپردازد فرض می‌کنیم.

جدول ۱: احتمالات شناسایی نفوذ توسط عامل.

WGA_i	P_d	احتمال تشخیص نفوذ	هزینه IDS
	$1-P_d$	احتمال عدم تشخیص نفوذ	$-C_1$
	P_f	احتمال تشخیص نفوذ اشتباه	C_2

از طرف دیگر مهاجم در صورت نفوذ به سیستم هزینه b_1 را بدست می‌آورد و در صورت عدم موفقیت در نفوذ هزینه b_2 را بایستی بدهد. هشدار اشتباه هزینه صفر را برای مهاجم در بردارد.

^{۱۷} Mobility

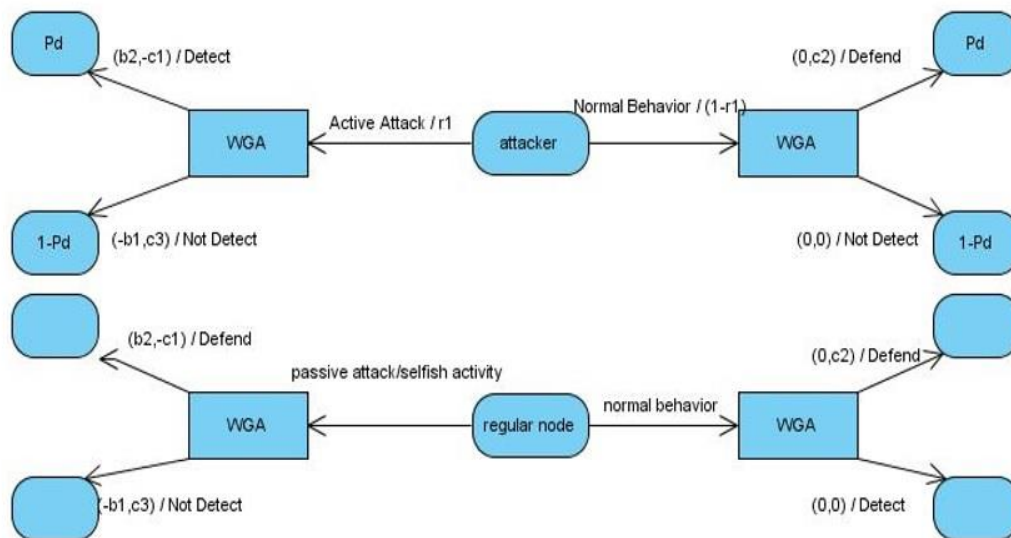
عامل) و r-mix (بازده انتظاری مهاجم) نشان می‌دهد در نظر می‌گیریم [۱۱].

جدول ۳: ماتریس payoff

attack	WGA _i		
	d _۱	d _۲	q - mix
u _۱	$b_1 f_i, -c_1(1 + p_d + m_i)$	$-b_2 f_i, c_2(1 + (1 - p_d))$	$b_1 f_i q - b_2 f_i(1 - q)$
u _۲	$b_1(1 + \lambda f_i + l_i), -c_1(1 + p_d + l_i + m_i)$	$b_2(1 + \lambda f_i + l_i), -c_2(1 + l_i + (1 - p_d))$	$b_1(1 + \lambda f_i + l_i) q - b_2(1 + \lambda f_i + l_i)(1 - q)$
u _۳	$\cdot, c_2(1 + p_f + m_i)$	$\cdot \cdot \cdot$	\cdot
r - mix	$-c_1(1 + p_d + m_i)r_1 - c_1(1 + p_d + l_i + m_i)(r_2) + c_2(1 + p_f + m_i)(1 - r_1 - r_2)$	$c_2(1 + (1 - p_d))r_1 + c_2(1 + l_i + (1 - p_d))r_2$	

حرکت بازیگر دیگر هستند. عبارتی عامل مدافع دارای یک باور از حرکت خود و پاسخ متقابل مهاجم می‌باشد. در شکل ۴ نحوه این تعامل نشان داده شده است.

ماتریس بازده دو بازیگر در حالات مختلف انتخاب استراتژی را نشان می‌دهد. فرض بر این است که هر دو بازیگر چنین ماتریسی را داشته و قادر به محاسبه حالت



شکل ۴: وضعیت های مختلف تشخیص

نش) برسد. این نقطه که با (r^*, q^*) نمایش داده می‌شود از ماتریس ۳*۳ جدول بدست می‌آید.

در این مرحله هر بازیکن بایستی بازی را انجام دهد که در آن حالت هیچ انگیزه ای برای تغییر بازی خود نداشته باشد و بازیکن مقابل نیز به همین نقطه (تعادل

$$q^*[-c_1(1+p_d+m_i)r_1^* - c_1(1+p_d+l_i+m_i)(r_2^*) + c_2(1+p_f+m_i)(1-r_2^*-r_1^*)] + (1 - q^*)[c_3(1+(1-p_d))r_1^* + c_3(1+l_i+(1-p_d))r_2^*] \\ \leq q[-c_1(1+p_d+m_i)r_1^* - c_1(1+p_d+l_i+m_i)(r_2^*) + c_2(1+p_f+m_i)(1-r_2^*-r_1^*)] + (1 - q^*)[c_3(1+(1-p_d))r_1^* + c_3(1+l_i+(1-p_d))r_2^*]$$

بعد از حل نامساوی، اگر فرض کنیم که $r_2=1-r_1$ باشد خواهیم داشت (برای مهاجم دو حالت کلی در نظر گرفته شود)

عبارت بالا نشان می‌دهد که بهترین استراتژی که بازیکن مقابل انتخاب می‌کند بایستی در هر حالتی از استراتژی انتخابی بازیکن کمتر باشد. q, r هر دو بین صفر و یک هستند $0 \leq q, r \leq 1$.

$$\text{if } -c_1(1+p_d+m_i)r - c_1(1+p_d+l_i+m_i)(1-r) = c_3(1+(1-p_d))r + c_3(1+l_i+(1-p_d))(1-r) \text{ and } b_1f_iq - b_2f_i(1-q) = b_1(1+\lambda f_i+l_i)q - b_2(1+\lambda f_i+l_i)(1-q) \text{ then}$$

$$r^* = \frac{c_1(1+p_d+l_i+m_i) + c_3(1+l_i+(1-p_d))}{-c_1(1+p_d+m_i) + c_1(1+p_d+l_i+m_i) - c_3(1+l_i+(1-p_d)) + c_3(1+(1-p_d))} \\ q^* = \frac{-b_2(1+\lambda f_i+l_i) + b_2f_i}{b_1(1+\lambda f_i+l_i) + b_2(1+\lambda f_i+l_i) + (b_1+b_2)f_i}$$

$$\text{if } -c_1(1+p_d+m_i)r + c_2(1+p_f+m_i)(1-r) = c_3(1+l_i+(1-p_d))(r) \text{ and } b_1f_iq - b_2f_i(1-q) = 0 \text{ then}$$

$$r^* = \frac{c_2(1+p_f+m_i)}{c_1(1+p_d+m_i) + c_2(1+p_f+m_i) + c_3(1+l_i+(1-p_d))} \\ q^* = \frac{b_2f_i}{(b_1+b_2)f_i}$$

$$\text{if } c_2(1+p_f+m_i)(1-r) - c_1(1+p_d+l_i+m_i)(r) = c_3(1+l_i+(1-p_d))(r) \text{ and } b_1(1+\lambda f_i+l_i)q - b_2(1+\lambda f_i+l_i)(1-q) = 0 \text{ then}$$

$$r^* = \frac{c_2(1+p_f+m_i)}{c_2(1+p_f+m_i) + c_1(1+p_d+l_i+m_i) + c_3(1+l_i+(1-p_d))} \\ q^* = \frac{b_2(1+\lambda f_i+l_i)}{b_1(1+\lambda f_i+l_i) + b_2(1+\lambda f_i+l_i)}$$

$\{d_1, d_2\}$ عامل مدافع بدست می‌آید.

فرض می‌کنیم v_i مقدار ریسک امنیتی عامل i ام (WGA_i) باشد آنگاه:

$$v_i = \frac{q_i^*(d_1)}{q_i^*(d_1)} + \frac{r_i^*(u_1) + r_i^*(u_2)}{r_i^*(u_r)} \quad i \in N$$

پس از محاسبه استراتژی‌های بهینه و تعادل نش بازی بردار احتمالی $r^* = \{r^*(u_1), r^*(u_2), r^*(u_r)\}$ برای مهاجم زمانی که استراتژی‌های $\{u_1, u_2, u_3\}$ را انتخاب می‌کند بدست می‌آید و بردار احتمالی $q^* = \{q^*(d_1), q^*(d_2), q^*(d_r)\}$ برای استراتژی‌های

۶- بازی همکارانه عاملها با یکدیگر

در این بخش بازی همکارانه عاملهای WGA برای تشکیل ائتلاف و تشخیص مقدار شیپلی با استفاده از نقطه تعادل نش یا همان SRV محاسبه شده در بخش قبلی توضیح داده خواهد شد. مقدار شیپلی یک اشاره‌گر قدرتمند برای مسئله انتساب هزینه است [۱۲]. بازی همکارانه که در آن همه بازیگران ($WGAS$) طی یک سری مذاکره با یکدیگر به دنبال افزایش میزان سودمندی گروه و ائتلاف تشکیل شده می‌باشند، راه حل مناسبی برای تشخیص میزان درجه امنیتی شبکه فوقانی است.

ابتدا تابع $R: V \rightarrow R^+$ به عنوان یک تابع یک به یک از اعداد حقیقی را به صورتی که هر عنصر از V ، I به صورت $V = \{v_1, v_2, \dots, v_j\}$ تعریف می‌شود. سطح امنیتی IDS پیشنهادی برای استفاده از L تعریف می‌کنیم. L به نحوی تعریف می‌شود که

$$L = \{l_1, \dots, l_L\} \text{ when } 0 < k_1 < k_2 < \dots < k_L$$

به عنوان مقادیر حد آستانه در نظر گرفته می‌شوند. در رابطه زیر حالات مختلف سطح امنیتی با کمک بردار خروجی عاملها V نشان داده شده است.

$$SL = \begin{cases} l_1 & \text{if } \sum_{i=1}^N R(v_i) \geq k_1 \\ l_j & \text{if } \sum_{i=1}^N R(v_i) \geq k_j \\ l_{j+1} & \text{if } \sum_{i=1}^N R(v_i) \geq k_{j+1} \\ l_L & \text{if } \sum_{i=1}^N R(v_i) \geq k_L \end{cases}$$

زمانی که

$$k_1 = v_{min} + k_{in} \quad , \quad k_j = v_{min} + j k_{in} \quad , \quad k_{j+1} = v_{min} + (j+1)k_{in} \quad , \dots \quad , \quad k_H = v_{min} + Lk_{in}$$

$$k_{in} = \frac{v_{max} + v_{min}}{L + 1}$$

عاملهای $WGAS$ را با استفاده از سطح امنیتی که توسط هر یک بدست آمده (k_j) در یکی از گروهها دسته‌بندی می‌کنیم SRV عامل را می‌توان بوسیله یک بازی N نفره با $X = \{1, 2, \dots, n\}$ مدل‌سازی کرد، که در آن مجموعه‌ای از بازیگران می‌باشد و می‌توان هر زیر مجموعه‌ای از آن را به صورت $V \subset N$ بدست آورد، به

نحوی که $\forall j \in V$ و $v_j \neq 0$ به عنوان یک ائتلاف شناخته می‌شود [۱۳] [۱۴]. ائتلاف X عامل در یک گروه با حد آستانه K از سطوح امنیتی، نشان‌دهنده یک الگوی حمله و سطح امنیتی L در گروه می‌باشد. مقدار مجموع ائتلاف^{۱۸} از جمع مقادیر SRV اعضا ائتلاف به صورت $R(c) = \sum_{i \in c} R(v_i)$ محاسبه می‌شود و به آن تابع ائتلاف گفته می‌شود. فرض کنید $R(c) = \sum_{i \in c} R(v_i)$ ، $v_i \in V$ ، $c \subset X$ با تعداد اعضا C می‌باشد. آنگاه مقدار شیپلی از I بین عضو بردار عاملها به صورت زیر تعریف می‌شود.

عاملهای $WGAS$ را با استفاده از سطح امنیتی که توسط هر یک بدست آمده (k_j) در یکی از گروهها دسته‌بندی می‌کنیم SRV عامل را می‌توان بوسیله یک بازی N نفره با $X = \{1, 2, \dots, n\}$ مدل‌سازی کرد، که در آن مجموعه‌ای از بازیگران می‌باشد و می‌توان هر زیر مجموعه‌ای از آن را به صورت $V \subset N$ بدست آورد، به نحوی که $\forall j \in V$ و $v_j \neq 0$ به عنوان یک ائتلاف شناخته می‌شود [۱۳] [۱۴]. ائتلاف X عامل در یک گروه با حد آستانه K از سطوح امنیتی، نشان‌دهنده یک الگوی حمله و سطح امنیتی L در گروه می‌باشد. مقدار مجموع ائتلاف^{۱۹} از جمع مقادیر SRV اعضا ائتلاف به صورت $R(c) = \sum_{i \in c} R(v_i)$ محاسبه می‌شود و به آن تابع ائتلاف گفته می‌شود. فرض کنید $R(c) = \sum_{i \in c} R(v_i)$ ، $v_i \in V$ ، $c \subset X$ با تعداد اعضا C می‌باشد. آنگاه مقدار شیپلی از I بین عضو بردار عاملها به صورت زیر تعریف می‌شود.

$$SP(i) = \sum_{c \subset X} \sum_{i \in c} \frac{(c-1)! (n-c)!}{n!} [R(c) - R(c - \{i\}w)]$$

پس از محاسبه $sp(i)$ برای هر یک از عاملها که با استفاده از عضویت آنها در ائتلاف بدست آمده است می‌توان سطح ریسک امنیتی حمله صورت گرفته به آن عامل را با استفاده از مقادیر مختلف k_j در گروههای مختلف

^{۱۸} aggregate

^{۱۹} aggregate

امنیتی L قرار دهیم. بدین منظور ۴ حد آستانه برای L در نظر گرفته و عاملها را در هر یک از این دسته‌ها (ائتلاف) قرار می‌دهیم. از محاسبه مقادیر NE بردار v_i برای ۲۰ عامل $WGAS$ بدست می‌آید. سپس با استفاده از k_{in} حد آستانه ۴ گروه ائتلافی را محاسبه کرده و با استفاده از آن و مقادیر v_i مقدار دقیق شیپلی را بدست می‌آوریم. پس از محاسبه مقدار SP برای هر عامل می‌توان با کمک k_{in} های محاسبه شده برای ۴ سطح مورد نظر امنیتی، سطح تهدید برای هر عامل را در یکی از این ۵ گروه دسته‌بندی کرده و میزان خطر هر حمله را تشخیص داد. پس از دسته‌بندی عاملها در هر یک از گروهها مدیر سیستم می‌تواند با توجه به اطلاعات بدست آمده یا تصمیم‌گیری لازم را داشته باشد. مقادیر آستانه مربوط به سطح امنیتی می‌تواند به مرور زمان توسط مدیر سیستم تغییر کرده به نحوی که دسته‌بندی واقعی آن ارائه نماید.

امنیتی قرار دارد و مطابق با قرارگیری در هر گروه $l_1, l_2, \dots, l_{j+1}, l_j, l_1$ برای هر عامل یک درجه امنیتی تعیین نمود.

۷- شبیه‌سازی

به منظور شبیه‌سازی کارایی مدل پیشنهادی نیاز به یک مثال عددی وجود دارد ابتدا ۲۰ عدد فرضی به صورت تصادفی در یک ماتریس برای ۲۰ عامل تولید می‌کنیم. در این ماتریس به ازاء هر یک از عاملها اعدادی را نیز به عنوان پارامترهای حمله‌کننده برای پارامترهای مختلف آن از قبیل b_1, b_2, \dots و به صورت تصادفی تولید می‌نماییم. در ادامه با استفاده از نرم‌افزار شبیه‌سازی بازی به نام $GAMBIT$ [۱۵][۱۶] نقطه تعادل نش را برای هر یک از عاملها و حمله‌کننده بدست آورده و در جدول درج می‌کنیم. سپس برای محاسبه مقدار شیپلی از نرم‌افزار $MATLAB$ استفاده کرده و سعی می‌کنیم که مقدار SRV هر عامل را مشخص کرده و در یکی از

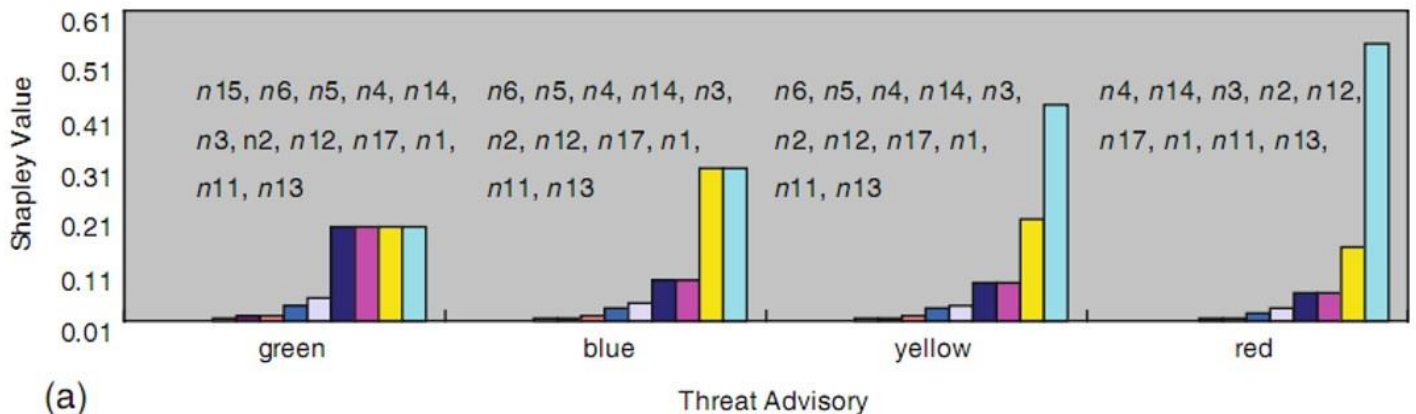
جدول ۴: پارامترهای عامل مهاجم و نقطه تعادل نش هر یک

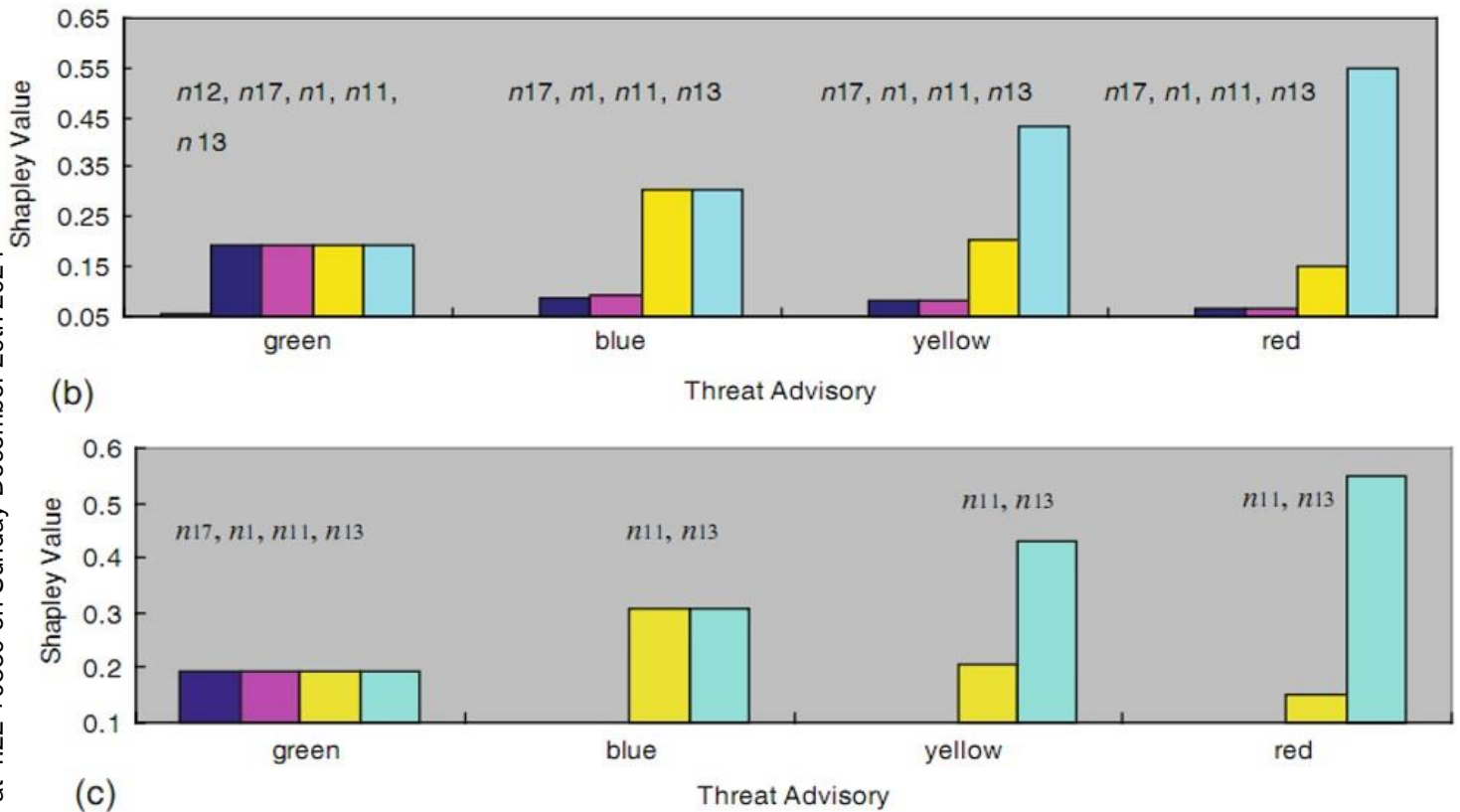
Agent	Attacker and Agent's params										Nash v_i
	b_1	$-b_2$	$f_i\%$	$-c_1$	c_2	c_3	$l_i\%$	$m_i\%$	$p_d\%$	$p_f\%$	
N_1	۱۰	- ۹۰	۰,۴ ۹	- ۲۵	۷۱	۵۵	۰,۸	۰,۳ ۵	۰,۵	۰, ۷	۱۰,۷ ۳۲
N_2	۲۰	- ۱۰۰	۰,۴ ۴	- ۸۱	۲۰	۱۰	۰,۳	۰,۹	۰,۸	۰, ۲	۳,۹۷
N_3	۳۰	- ۵۰	۰,۵ ۵	- ۵۰	۳۱	۳۶	۰,۳	۰,۴ ۵	۰,۸	۰, ۳	۲,۳۱
N_4	۴۰	- ۷۰	۰,۳ ۵	- ۷۰	۴۰	۵۰	۰,۴	۰,۷	۰,۷	۰, ۴	۲,۱۱
N_5	۵۰	- ۵۰	۰,۲ ۵	- ۵۰	۶۰	۴۰	۰,۶	۰,۵	۰,۸	۰, ۶	۱,۵۸ ۹
N_6	۶۰	- ۹۰	۰,۲ ۹	- ۶۰	۵۰	۶۰	۰,۵	۰,۶	۰,۶	۰, ۵	۲,۵۴ ۷
N_7	۷۰	- ۴۰	۰,۶ ۴	- ۴۰	۹۰	۷۰	۰,۸	۰,۵	۰,۷	۰, ۴	۳,۲۰
N_8	۸۰	- ۵۰	۰,۷ ۹	- ۹۰	۶۰	۵۰	۰,۷	۰,۴	۰,۸	۰, ۳	۱,۲۳ ۵
N_9	۹۰	- ۹۰	۰,۳ ۹	- ۸۰	۷۰	۹۰	۰,۱ ۵	۰,۲	۰,۷	۰, ۹	۲,۲۳ ۱
N_{10}	۱۰	- ۱۱	۰,۰ ۵	- ۵	۱۰	۹۰	۱	۰,۱	۰,۴	۰, ۲	۰,۰۰ ۸۷

Agent	Attacker and Agent's params										Nash
	b_1	$-b_2$	$f_i\%$	$-c_1$	c_2	c_3	$l_i\%$	$m_i\%$	$p_d\%$	$p_f\%$	v_i
N13	۲۵	- ۹۱	۰,۴ ۴	- ۸۱	۱۵	۱۴	۰,۰ ۵	۰,۹ ۹	۰,۵	۰, ۱	۵,۷
N14	۳۵	- ۹۸	۰,۳ ۴	- ۱,۵	۹۸	۱۰	۰,۹ ۱	۰,۹ ۹	۰,۵	۰, ۱	۴۹,۰ ۱
N15	۴۵	- ۵۵	۰,۲ ۱	- ۶۵	۳۳	۳۱	۰,۳ ۵	۰,۶ ۵	۰,۷	۰, ۲	۲,۳۸ ۵
N16	۵۵	- ۴۱	۰,۲	- ۴۱	۵۵	۵۰	۰,۵ ۵	۰,۴ ۵	۰,۷ ۹	۰, ۴۵	۱,۴۵
N17	۶۵	- ۱۰۰	۰,۴	- ۱۰	۷۱	۸۵	۰,۸ ۱	۰,۲ ۱	۰,۵	۰, ۳	۱۰,۰ ۲
N18	۷۵	- ۲۵	۰,۷	- ۳۰	۷۴	۷۹	۰,۷ ۵	۰,۲ ۵	۰,۸	۰, ۲۵	۱,۰۹ ۳
N19	۸۵	- ۱۰	۰,۰ ۵	- ۸۰	۱۵	۱۵	۰,۱ ۴	۰,۸ ۵	۰,۵	۰, ۵	۰,۳۸ ۱
N20	۱۰	- ۱۰	۰,۰ ۱	- ۷۰	۲۰	۵۴	۰,۹	۰,۹	۰,۹	۰, ۲	۴,۰۲ ۱
N13	۲۵	-	۰,۴	-	۱۵	۱۴	۰,۰	۰,۹	۰,۵	۰, ۱	۵,۷

چهارم قرار میگیرند. لذا ائتلافی بدین صورت تشکیل می شود و می توان سطح امنیتی این گروهها را معادل یکدیگر در نظر گرفت. با تغییر در مقدار شیپلی می توان این دسته بندی ها را تغییر داد و شبکه فوقانی مختلفی را برای دفاع در مقابل حملات تشکیل داد. در شکل زیر چندین مقدار شیپلی برای حالات مختلف در نظر گرفته شده که تشکیل ائتلاف در سه وضعیت را نشان می دهند.

مقدار حد آستانه برای هر یک از گروه ۴ را محاسبه کرده و مقادیر $\{۴۰,۷۲, ۲۰,۱, ۳,۰۲, ۹,۰۸\}$ برای k_{in} بدست می آید که مقادیر نش محاسبه شده را در چهار گروه دسته بندی می کند. سپس با استفاده از فرمول مقدار شیپلی و مقادیر k_{in} امکان محاسبه دقیق $SP(i)$ میسر می شود. عاملهای $\{n3, n4, n5, n6, n8, n9, n10, n11, n15, n16, n18, n19\}$ در گروه اول و $\{n2, n13, n20\}$ در گروه دوم و $\{n1, n12, n17\}$ در گروه سوم و $\{n14\}$ در گروه





شکل ۵- سه حالت پیکر بندی ائتلاف برای مقادیر شیپلی (a) بزرگتر از ۰,۷ و (b) بزرگتر از ۰,۸ و (c) بزرگتر از ۰,۹

۷. نتیجه گیری

از شبکه را پوشش دهد. علاوه بر این در صورت تشخیص ضعیف یا اشتباه، عاملها با تشکیل ائتلاف و محاسبه SRV تجمیعی (مقدار شیپلی) درصد خطای تشخیص و هشدارهای غیر صحیح (false alarm) را به حداقل می-رساند. در این مدل مقادیر حد آستانه براساس تشخیص-های عامل WGA (v_i) به روز می‌شود (k_{in}) و در هر بار تشکیل ائتلاف این مقادیر تغییر می‌کند و در عمل سیستم در هر بار از دوره‌های محاسبه SRV گروه‌بندی جدیدی را انجام می‌دهد. برای ادامه این تحقیق، محققین قصد دارند با استفاده از روشهای یادگیری از جمله Reinforcement Learning محاسبه k_{in} را به صورت تدریجی محاسبه کرده و در هر بار محاسبه از داده‌های مراحل قبل نیز بهره برده شود.

در این مقاله یک مدل امنیتی توزیع شده برای تشخیص نفوذ به شبکه DIDS مبتنی بر تئوری بازیها ارائه شده است. در سیستم‌های سنتی IDS مدیران سیستم می‌بایستی دائماً به رصد سیستم پرداخته و کلیه اتفاقات و سناریوهای ممکن را بررسی و پایش نمایند. در این تحقیق، ما مدلی را مبتنی بر تئوری بازیها در فرم گسترده به دو صورت همکارانه و غیر همکارانه پیشنهاد کردیم که در نوع غیر همکارانه (رقابتی) مقدار ریسک امنیتی با استفاده از تعادل نش توسط هر کدام از عاملها محاسبه شده و در بازی همکارانه عاملهایی که در یک گروه قرار می‌گیرند با تشکیل ائتلاف و محاسبه مقدار شیپلی درجه امنیتی ائتلاف را محاسبه می‌نماییم. نظر به اینکه در این مدل عاملهای $WGAs$ درون شبکه گسترده شده‌اند، با تشکیل یک شبکه فوقانی تشخیص نفوذ می‌توانند عمده تراکنش‌ها و داده‌های رد و بدل شده در شبکه را رصد کرده و به صورت توزیع شده بخش عمده‌ای

۹. D. S. P. J. M. R. K. G. Shaw "Inside the minds of the insider", Security Management, جلد ۴۳, p. ۳۴-۴۴, ۱۹۹۹.
۱۰. T. B. T. Alpcan "A game theoretic approach to decision and analysis in network intrusion detection", IEEE Conference on Decision and Control, p. ۲۵۹۵-۲۶۰۰, ۲۰۰۳.
۱۱. C.-K. W. Yi-Ming Chen "A Game Theoretic Framework for Multi-agent Deployment in Intrusion Detection Systems", Security Informatics, Annals of Information Systems, pp. ۱۱۷-۱۳۳, ۲۰۱۰.
۱۲. D. R. B. Mishra "Cost sharing in a job scheduling problem using the Shapley value", ۲۰۰۵.
۱۳. P. Z. Liu "Incentive-based modeling and inference of attacker intent, objectives and strategies", ACM Transactions on Information and System Security, جلد ۸, p. ۷۸-۱۱۸, ۲۰۰۵.
۱۴. A. S. S. Dixit "Games of Strategy", ۲۰۰۱.
۱۵. R. D. M. A. M. a. T. T. L. McKelvey, "Gambit: Software Tools for Game Theory", ۲۰۰۷, Available: <http://econweb.tamu.edu/gambit>.
۱۶. GAMBIT "GAMBIT", ۲۰۱۳, Available: <http://www.gambit-project.org/>
۱. C. Symantec "Symantec Corporation", ۲۰۱۳, ۰۸, ۱۰, Available: <http://www.symantec.com/index.jsp>.
۲. P. H. V. L. R. J. Z. H. M. Mel "An Overview of Issues in Testing Intrusion Detection Systems", NIST, Gaithersburg, MD, ۲۰۰۲.
۳. A. D. V. M. R. D. Keromytis, "SOS: An architecture for mitigating DDoS attacks," *IEEE Communications*, vol. ۲۲, p. ۱۷۶-۱۸۸, ۲۰۰۴.
۴. G. V. S. Suryawanshi "Mobile Agent for Distributed Intrusion detection System in Distributed System", *International Journal of Artificial Intelligence and Computational Research (IJAICR.)*, p. ۲۰۱۰.
۵. M. A. M. S. M. A. K. & M. R. M. I. Kamaruzaman Maskat "Mobile Agents in Intrusion Detection System: Review and Analysis", *Modern Applied Science*, شماره ۵, جلد ۵, pp. ۲۱۸-۲۳۱, Dec ۲۰۱۱.
۶. R. B. a. P. Mell "Intrusion detection systems", ۲۰۱۲, Available: <http://www.snort.org/docs/nistids.pdf>.
۷. S. E. Schechter, "Computer Security Strength and Risk: A Quantitative Approach," *PhD Thesis, Harvard University*, ۲۰۰۴.
۸. S. E. Schechter "Toward econometric models of the security risk from remote attacks", *IEEE Security & Privacy*, شماره ۱, جلد ۳, p. ۴۰-۴۴, ۲۰۰۵.

دسته‌بندی داده‌های دو رده‌ای با ابرمستطیل موازی محورهای مختصات