فصلنامه علمی- پژوهشی
فناوری اطلاعات و ارتباطات ایران

سال هشتم، شماره‌های۲۷ و ۲۸، بهار و تابستان ۱۳۹۵
صص:۴۷-۶۰

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

[*]امین نظارت [**] مهدی رجا *** غلامحسین دستغیبی‌فرد
* 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 برعاملهای 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 شیپلی 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 مکاشفه‌ای 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 شیپلی، امنیت شبکه

نویسنده عهده‌دار مکاتبات: امین نظارت aminnezarat@pnu.ac.ir

[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 درجه 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.

سیستم های تشخیص نفوذ اخیر را می توان 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 گره ها استفاده می‌شود مبتنی بر ارتباط دائمی است که سربارزیادی را بر روی شبکه تحمیل می‌نماید و این موضوع مانعی است در مقابل گسترش بیشتر معماری[۳] .اگرچه روش کنشی بسیارکاراتر 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 تصیم‌گیری در پاسخ مناسب به حملات ضروری به نظر می‌رسد که از یک روش توزیع‌شده 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

---

[۳] Secure Overlay Network

[۴] Single Point of Failure

[۵] Negotiate

[۶] Security Risk value

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. هردو 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.

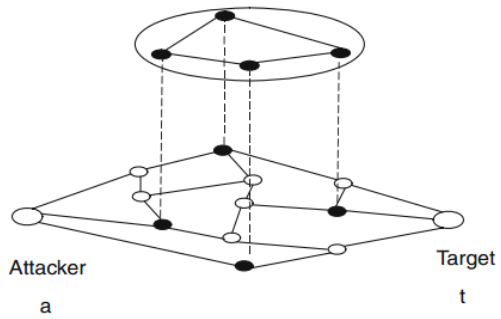
برای اطمینان از اینکه حمله‌ای صورت گرفته است یا خیر و جلوگیری از ارسال هشدارهای اشتباه در بازی دیگری از نوع همکارانه با سایر عاملهای مدافع در محیط چند عاملی اقدام به مذاکره می‌نماید. در این بازی عاملها می‌توانند جهت جلوگیری از ایجاد سربار در شبکه به صورت گروههای چند نفره تشکیل ائتلاف دهند. در هر ائتلافکه 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 $MA=\{MA_1, MA_2, \ldots, MA_2\}$ تشکیل شده است.

هر یک از این گره‌ها 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، حیطه حرکت عامل محافظ می‌بایست 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

---

[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 یکدیگربه 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 قبلا" نیز اشاره شد این سیستم یک IDSمرکزی 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 قابلیتی 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 حاضرچنین 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 گلبولهای سفید در گره‌های شبکه مستقر شده و در زمانهای خاصی جابجا می‌شوند. ترکیب سرور شامل اجزاء زیر است:

- کارخانه تولید عاملهای گلبولهای سفید[۱۰]
- کارخانه تولید عاملهای خنثی کننده[۱۱]
- SNORT
- پایگاه دانش حملات[۱۲]

- کارخانه تولید عاملهای گلبول 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 آنرا 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 می داند که هر WGAکجاست. تفاوت WGAهای تولید شده در این عامل این است که یک عامل WGA به همراه خود خلاصه ای از سناریوهای انواع حملات در شبکه ها 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 می نماید. این عامل از چندین عامل دیگر تشکیل شده است که هر یک وظیفه ای را بر عهده دارند:

عامل AMS[۱۴]: مدیر اصلی عاملهاست و به هر عامل یک شماره اختصاصی انتساب می دهد. 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 می داند. زمانی که یکی از عاملهای WGA قصد برقراری ارتباط با سایر

[۱۰] White Global Agent Factory

[۱۱] Lymphocit Agent Factory
[۱۲] IDS knowledge
[۱۳] Strong mobility
[۱۴] Agent Management System
[۱۵] Directory Facilitator

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

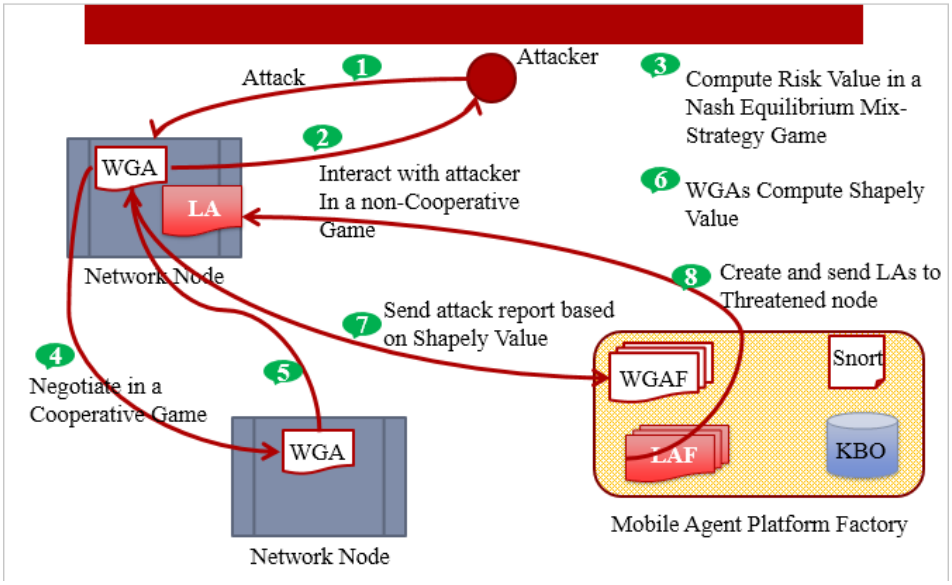
- کارخانه تولید عاملهای خنثی‌کننده (LAF)

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 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 WGAبداند 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 WGAبایستی 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.



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 می-باشد. 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 درنظر 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 ازاشغال 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 نست 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]:

$$Security\ risk = \text{امنیت نقض تعداد نرخ} * \text{نفوذ هر هزینه میانگین}$$

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_2 هزینه پرداختی آن مهاجم می‌باشد. در صورت تشخیص حمله این هزینه معادل b۱ می‌باشد. همچنین اگر فرض می شود 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 i_1 , i_2را 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

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-...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 درون‌شبکه کاربران عادی را از مهاجمین تشخیص دهند. فرض کنید که m_i نشان‌دهنده نرخ تحرک[17]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 (۱-p_d) نشان می‌دهیم و p_f را به عنوان احتمال تشخیص اشتباه حمله در نظر می‌گیریم. هزینه –c۱ 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.

هزینه IDS		احتمال تشخیص نفوذ	P_d	WGA_i
$-C_1$				
C_3		احتمال عدم تشخیص نفوذ	۱-P_d	
C_2		احتمال تشخیص نفوذ اشتباه	P_f	

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.

جدول ۲: هزینه عایدی مهاجم

	هزینه	نتیجه
Attacker	$-b_1$	نفوذ
	b_2	عدم نفوذ

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:

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

حال به بازی غیر همکارانه با استراتژی آمیخته بین دو بازیگر(attacker , WGA) 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 قبلا" 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 ۱-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 ۱-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 استراتژهای فرض شده را در بازده نهایی لحاظ کرد جدول زیر را q-mix بازده انتظاری

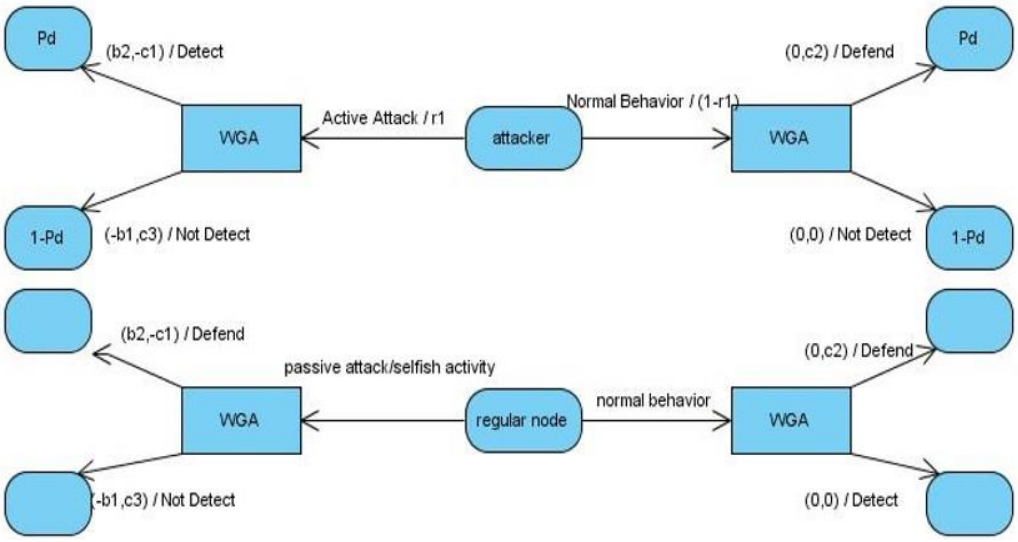
[17] Mobility

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

جدول ۳: ماتریس payoff.

	WGA_i		
$attack$	d_1	d_2	$q-mix$
u_1	$b_1 f_i \quad , \quad -c_1(1+p_d+m_i)$	$-b_2 f_i \quad , \quad c_3(1+(1-p_d))$	$b_1 f_i q \quad -b_2 f_i(1-q)$
u_2	$b_1(1+\lambda f_i+l_i)\ , \ -c_1(1+p_d+l_i+m_i)$	$b_2(1+\lambda f_i+l_i)\ , \ -c_3(1+l_i+(1-p_d))$	$b_1(1+\lambda f_i+l_i)\, q - b_2(1+\lambda f_i+l_i)(1-q)$
u_3	$0, c_2(1+p_f+m_i)$	$0,0$	0
$r-mix$	$-c_1(1+p_d+m_i)r_1 - c_1(1+p_d+l_i+m_i)(r_2) + c_2(1+p_f+m_i)(1-r_2-r_1)$	$c_3(1+(1-p_d))r_1 + c_3(1+l_i+(1-p_d))r_2$	

ماتریس بازده دو بازیگر در حالات مختلف انتخاب استراتژی را نشان می‌دهد. فرض بر این است که هر دو بازیگر چنـین ماتریسی را داشـته و قادر به محاسبه حالت حرکت بازیگر دیگر هستند. بعبارتی عامل مدافع دارای یک باور از حرکت خود و پاسخ متقابل مهاجم می‌باشد. در شکل ۴ نحوه این تعامل نشان داده شده است.



شکل ۴: وضعیت های مختلف تشخیص

در این مرحله هر بازیکن بایستی بازی را انجام دهد که در آن حالت هیچ انگیزه ای برای تغییر بازی خود نداشـته باشد و بازیکن مقابل نیز به همین نقطه (تعادل نش) برسد. این نقطه که با (r*, q*) نمایش داده می‌شود از ماتریس ۲*۳ جدول ۳ بدست می‌آید.

$$
\begin{aligned}
q^*[-c_1(1+p_d+m_i)r_1^*\square - c_1(1+p_d+l_i+m_i)(r_2^*) + c_2\big(1+p_f+m_i\big)(1-r_2^*-r_1^*)] + (1 \\
- q^*)\big[c_3\big(1+(1-p_d)\big)r_1^* + c_3(1+l_i+(1-p_d))r_2^*\big] \\
\leq\ q[-c_1(1+p_d+m_i)r_1^*\square - c_1(1+p_d+l_i+m_i)(r_2^*) \\
+ c_2\big(1+p_f+m_i\big)(1-r_2^*-r_1^*)] + (1 \\
- q^*)\big[c_3\big(1+(1-p_d)\big)r_1^* + c_3(1+l_i+(1-p_d))r_2^*\big]
\end{aligned}
$$

عبارت بالا نشان می‌دهد که بهترین استراتژی که بازیکن مقابل انتخاب می‌کند بایستی در هر حالتی از استراتژی انتخابی بازیکن کمتر باشد . r ,q هر دو بین صفر و یک هستند ۱=>r ,q = >۰ .

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)

$$
\begin{aligned}
\textbf{if}\ & -c_1(1+p_d+m_i)r\square - c_1(1+p_d+l_i+m_i)(1-r) \\
& = c_3(1+(1-p_d))\,r + c_3(1+l_i+(1-p_d))(1-r)\ \ \textbf{and}\ \ b_1 f_i q\square \\
& - b_2 f_i(1-q) = b_1(1+\lambda f_i+l_i)\,q - b_2(1+\lambda f_i+l_i)(1-q)\ \ \textbf{then}
\end{aligned}
$$

$$
r^* = \frac{c_1(1+p_d+l_i+m_i)+c_3(1+l_i+(1-p_d))}{-c_1(1+p_d+m_i)+c_1(1+p_d+l_i+m_i)-c_3(1+l_i+(1-p_d))+c_3(1+(1-p_d))}
$$

$$
q^* = \frac{-b_2(1+\lambda f_i+l_i)+b_2 f_i}{b_1(1+\lambda f_i+l_i)+b_2(1+\lambda f_i+l_i)+(b_1+b_2)f_i}
$$

$$
\begin{aligned}
\textbf{if}\ & -c_1(1+p_d+m_i)r\square + c_2(1+p_f+m_i)(1-r) \\
& = c_3(1+l_i+(1-p_d))(r)\ \ \textbf{and}\ \ b_1 f_i q\square - b_2 f_i(1-q^*) = 0\ \ \textbf{then}
\end{aligned}
$$

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

$$
q^* = \frac{b_2 f_i}{(b_1+b_2)f_i}
$$

$$
\begin{aligned}
\textbf{if}\ & c_2(1+p_f+m_i)(1-r\square) - c_1(1+p_d+l_i+m_i)(r) \\
& = c_3(1+l_i+(1-p_d))(r)\ \ \textbf{and}\ \ b_1(1+\lambda f_i+l_i)\,q - b_2(1+\lambda f_i+l_i)(1-q) \\
& = 0\ \ \textbf{then}
\end{aligned}
$$

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

$$
q^* = \frac{b_2(1+\lambda f_i+l_i)}{b_1(1+\lambda f_i+l_i)+b_2(1+\lambda f_i+l_i)}
$$

پس از محاسبه استراتژی های بهینه و تعادل نش بازی بردار احتمالی $r^* = \{r^*(u_1), r^*(u_2), r^*(u_3)\}$برای مهاجم زمانی که استراتژی های $\{u_1, u_2, u_3\}$ را انتخاب می کند بدست می‌آید و بردار احتمالی $q^* = \{q^*(d_1), q^*(d_2), q^*(d_3)\}$ برای استراتژی‌های $\{d_1, d_2\}$ عامل مدافع بدست می آید.

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

$$
v_i = \frac{q_i^*(d_1)}{q_i^*(d_1)} + \frac{r_i^*(u_1)+r_i^*(u_2)}{r_i^*(u_3)} \qquad i \in N
$$

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 $R: V \to R^+$ به عنوان یک تابع یک به یک از اعداد حقیقی را به صورتی که هر عنصر از v , r به صورت $V = \{v_۱, v_۲, \dots, v_j\}$ تعریف می‌شود. سطح امنیتی IDS پیشنهادی برای استفاده از L تعریف می-کنیم. L به نحوی تعریف می شود که

$L = \{l_۱, \dots, l_L\}$ $when$ $۰ < k_۱ < k_۱ < \cdots < k_L$

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.

$$SL = \begin{cases} l_۱ & if \sum_{i=۱}^{N} R(v_i) \geq k_۱ \\ l_j & if \sum_{i=۱}^{N} R(v_i) \geq k_j \\ l_{j+۱} & if \sum_{i=۱}^{N} R(v_i) \geq k_{j+۱} \\ l_L & if \sum_{i=۱}^{N} R(v_i) \geq k_L \end{cases}$$

زمانی که

$$k_۱ = v_{min} + k_{in} \ , \ k_j = v_{min} + j\,k_{in} \ , \ k_{j+۱} = v_{min} + (j+۱)k_{in} \ , \dots \ , \ k_H = v_{min} + Lk_{in}$$

$$k_{in} = \frac{v_{max} + v_{min}}{L + ۱}$$

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 Nنفره با $X = \{۱,۲,\dots, n\}$ مدل‌سازی کرد، که در آن X 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 $v_j \neq ۰$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 $R(c) = \sum_{i \epsilon c} R(v_i)$ محاسبه می‌شود و به آن تابع ائتلاف گفته می‌شود. فرض کنید $R(c) = \sum_{i \epsilon c} R(v_i) \ , v_i \epsilon V, c \subset X$ به عنوان مقدار ائتلاف C 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 Nنفره با $X = \{۱,۲,\dots, n\}$ مدل‌سازی کرد، که در آن X 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 $v_j \neq ۰$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 $R(c) = \sum_{i \epsilon c} R(v_i)$ محاسبه می‌شود و به آن تابع ائتلاف گفته می‌شود. فرض کنید $R(c) = \sum_{i \epsilon c} R(v_i) \ , v_i \epsilon V, c \subset X$ به عنوان مقدار ائتلاف C با تعداد اعضا C می‌باشد. آنگاه مقدار شیپلی از I بین عضو بردار عاملها به صورت زیر تعریف می‌شود.

$$SP(i) = \sum_{c \subset X \ i \, \epsilon \, c} \frac{(c-۱)! \ (n-c)!}{n!} [R(c) - R(c - \{i\}w)]$$

پس از محاسبه $sp\ (i)$ برای هر یک از عاملها که با استفاده از عضویت آنها در ائتلاف بدست آمده است می-توان 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 قرار دارد و مطابق با قرارگیری در هر گروه l_1, l_j, l_{j+1}, l_L برای هر عامل یک درجه امنیتی تعیین نمود.

۷- شبیه‌سازی

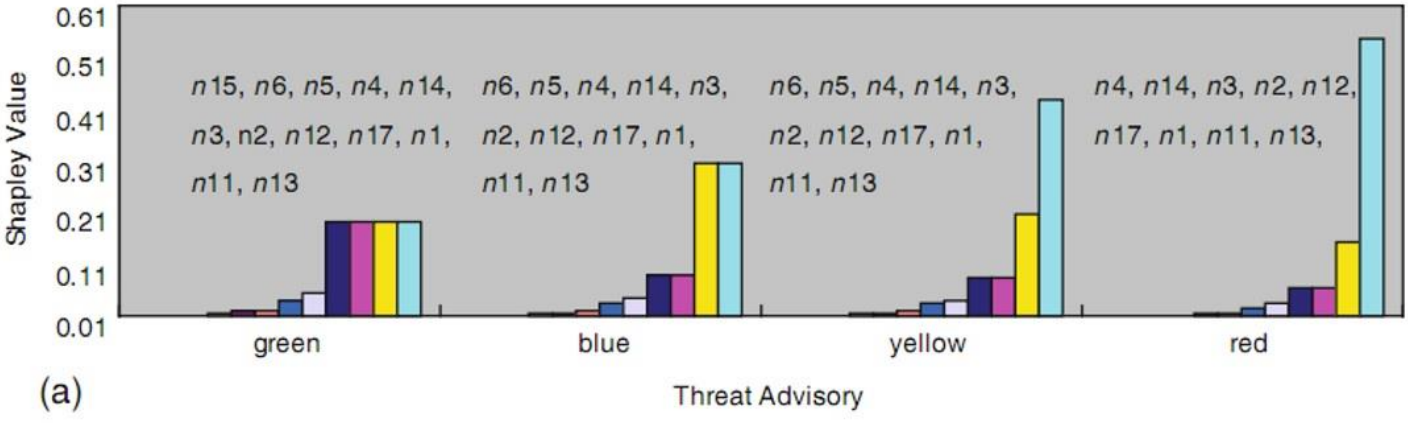
به منظور شبیه‌سازی کارایی مدل پیشنهادی نیاز به یک مثال عددی وجود دارد ابتدا ۲۰ عدد فرضی به صورت تصادفی در یک ماتریس برای ۲۰ عامل تولید می‌کنیم. در این ماتریس به ازاء هر یک از عاملها اعدادی را نیز به عنوان پارامترهای حمله‌کننده برای پارامترهای مختلف آن از قبیل b_1, b_2 و .... به صورت تصادفی تولید می‌نماییم. 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 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.

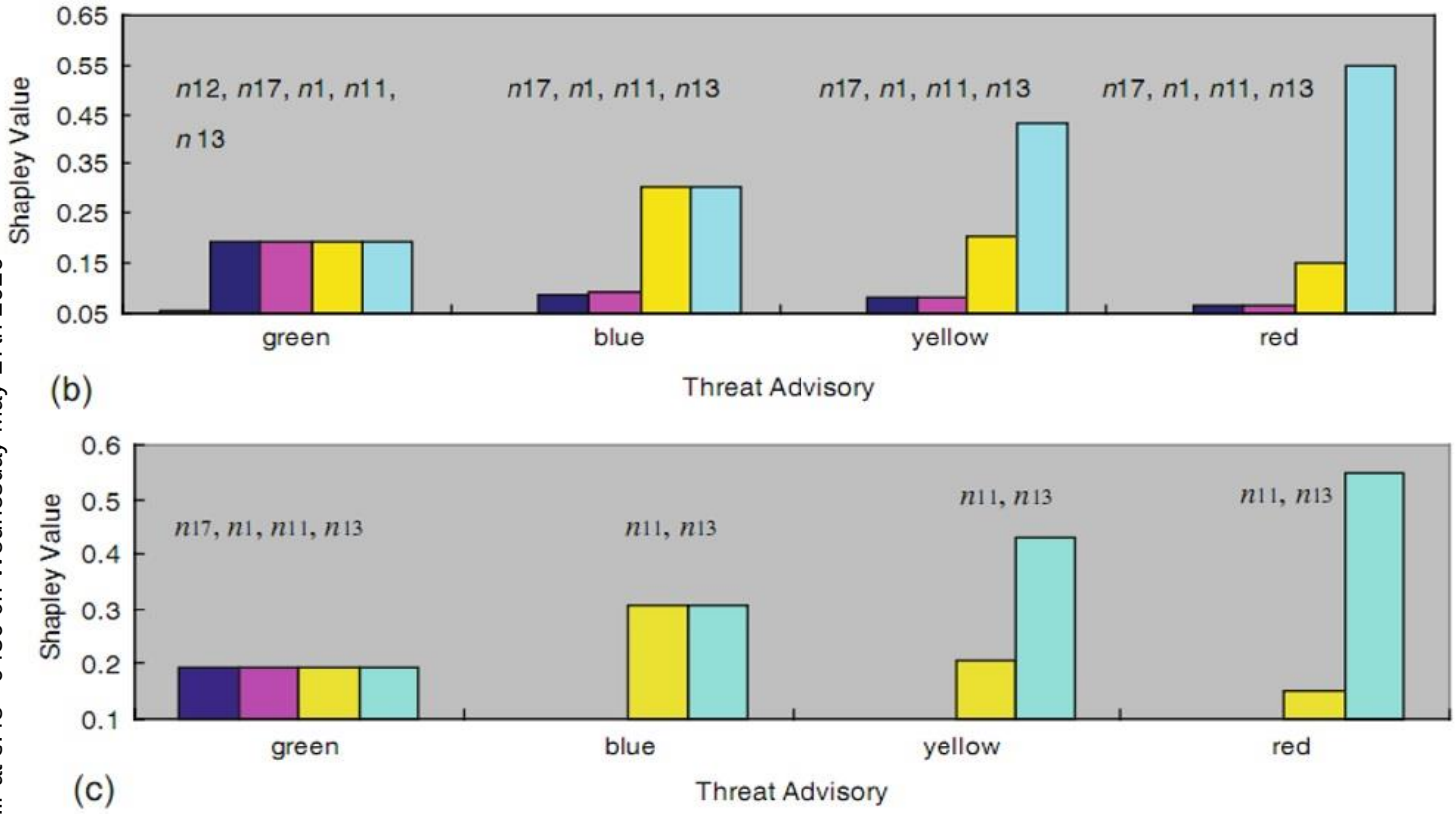
جدول ۴: پارامترهای عامل مهاجم و نقطه تعادل نش هریک

	Attacker and Agent's params										*Nash*
Agent	b_1	$-b_2$	$f_i\%$	$-c_1$	c_2	c_3	$l_i\%$	$m_i\%$	$p_d\%$	$p_f\%$	v_i
N۱	۱۰	-۹۰	۰,۴۹	-۲۵	۷۱	۵۵	۰,۸	۰,۳۵	۰,۵	۰,۷	۱۰,۷۳۲
N۲	۲۰	-۱۰۰	۰,۴۴	-۸۱	۲۰	۱۰	۰,۳	۰,۹	۰,۸	۰,۲	۳,۹۷
N۳	۳۰	-۵۰	۰,۵	-۵۰	۳۱	۳۶	۰,۳	۰,۴۵	۰,۸	۰,۳	۲,۳۱
N۴	۴۰	-۷۰	۰,۳۵	-۷۰	۴۰	۵۰	۰,۴	۰,۷	۰,۷	۰,۴	۲,۱۱
N۵	۵۰	-۵۰	۰,۲۵	-۵۰	۶۰	۴۰	۰,۶	۰,۵	۰,۸	۰,۶	۱,۵۸۹
N۶	۶۰	-۹۰	۰,۲	-۶۰	۵۰	۶۰	۰,۵	۰,۶	۰,۶	۰,۵	۲,۵۴۷
N۷	۷۰	-۴۰	۰,۶	-۴۰	۹۰	۷۰	۰,۸	۰,۵	۰,۷	۰,۴	۳,۲۰
N۸	۸۰	-۵۰	۰,۷	-۹۰	۶۰	۵۰	۰,۷	۰,۴	۰,۸	۰,۳	۱,۲۳۵
N۹	۹۰	-۹۰	۰,۳	-۸۰	۷۰	۹۰	۰,۱۵	۰,۲	۰,۷	۰,۹	۲,۲۳۱
N۱۰	۱۰۰	-۱۱۰	۰,۰۵	-۵	۱۰۰	۹۰	۱	۰,۱	۰,۴	۰,۲	۰,۰۰۸۷

	Attacker and Agent's params										*Nash*
Agent	b_1	$-b_2$	$f_i\%$	$-c_1$	c_2	c_3	$l_i\%$	$m_i\%$	$p_d\%$	$p_f\%$	v_i
N_{13}	۲۵	-۹۱	۰,۴	-۸۱	۱۵	۱۴	۰,۰۵	۰,۹	۰,۵	۰,۰۱	۵,۷
N_{14}	۳۵	-۹۸	۰,۳	-۱,۵	۹۸	۱۰۰	۰,۹۱	۰,۹	۰,۵	۰,۰۱	۴۹,۰۱
N_{15}	۴۵	-۵۵	۰,۲	-۶۵	۳۳	۳۱	۰,۳۵	۰,۶۵	۰,۷	۰,۰۲	۲,۳۸۵
N_{16}	۵۵	-۴۱	۰,۲	-۴۱	۵۵	۵۰	۰,۵۵	۰,۴۵	۰,۷۹	۰,۰۴۵	۱,۴۵
N_{17}	۶۵	-۱۰۰	۰,۴	-۱۰	۷۱	۸۵	۰,۸	۰,۲۱	۰,۵	۰,۰۳	۱۰,۰۲
N_{18}	۷۵	-۲۵	۰,۷	-۳۰	۷۴	۷۹	۰,۷۵	۰,۲۵	۰,۸	۰,۰۲۵	۱,۰۹۳
N_{19}	۸۵	-۱۰	۰,۰۵	-۸۰	۱۵	۱۵	۰,۱۴	۰,۸۵	۰,۵	۰,۰۵	۰,۳۸۱
N_{20}	۱۰۰	-۱۰	۰,۰۱	-۷۰	۲۰	۵۴	۰,۹	۰,۹	۰,۹	۰,۰۲	۴,۰۲۱
N_{13}	۲۵	-	۰,۴	-	۱۵	۱۴	۰,۰	۰,۹	۰,۵	۰,	۵,۷

مقدار حد آستانه برای هر یک از ۴ گروه را محاسبه کرده و مقادیر {۹,۰۸ ، ۳,۰۲ ، ۲۰,۱ ، ۴۰,۷۲} 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 {n۳,n۴,n۵,n۶,n۸,n۹,n۱۰,n۱۱,n۱۵,n۱۶,n۱۸,n۱۹} در گروه اول و {n۲,n۱۳,n۲۰} در گروه دوم و {n۱,n۱۲,n۱۷} در گـروه سـوم و {n۱۴} در گروه 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.





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

۷. نتیجه گیری

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 دائما" 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 شـده بخـش عمده‌ای 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 دورهای 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.

منابع

١. C. Symantec“ ,Symantec Corporation . .٢٠١٣ ٠٨ ١٠ ”, Available: http://www.symantec.com/index.jsp.

٢. P. H. V. L. R. J. Z. H. M. Mel“ ,An Overview of Issues in Testing Intrusion Detection Systems ”,NIST, Gaithersburg, MD, ٢٠٠٢.

٣. A. D. V. M. R. D. Keromytis, "SOS: An architecture for mitigating DDoS attacks," *IEEE Communications,* vol. ٢٢, p. ١٧٦–١٨٨., ٢٠٠٤.

٤. G. V. S. Suryawanshi“ ,Mobile Agent for Distributed Intrusion detection System in Distributed System ”, *International Journal of Artificial Intelligence and Computational Research (IJAICR.)* ,p .٢٠١٠ , .

٥. 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 ,٥ جلد , ,٦pp. ٢١٨-٢٣١, Dec ٢٠١١ .

٦. R. B. a. P. Mell“ ,Intrusion detection systems . ٢٠١٢ ”,Available: http://www.snort.org/docs/nistids.pdf.

٧. S. E. Schechter, "Computer Security Strength and Risk: A Quantitative Approach," *PhD Thesis, Harvard University*, ٢٠٠٤.

٨. S. E. Schechter“ ,Toward econometric models of the security risk from remote attacks ”,IEEE Security & Privacy ,١ شماره ,٣ جلد ,p. ٤٤–, ٢٠٠٥. ٤٠

٩. D. S. P. J. M. R. K. G. Shaw“ ,Inside the minds of the insider ”,Security Management ,٤٣ جلد ,p. ٣٤ ,.٤٤– .١٩٩٩

١٠. T. B. T. Alpcan“ ,A game theoretic approach to decision and analysis in network intrusion detection ”,IEEE Conference on Decision and Control , p. ٢٥٩٥ .٢٠٠٣ ,٢٦٠٠–

١١. 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. ١١٧-١٣٣, ٢٠١٠ .

١٢. D. R. B. Mishra“ ,Cost sharing in a job scheduling problem using the Shapley value .٢٠٠٥ ”,

١٣. P. Z. Liu“ ,Incentive-basedmodeling and inference of attacker intent, objectives and strategies ”,ACM Transactions on Information and System Security ,٨ جلد ,p. ٧٨ ,.١١٨– .٢٠٠٥

١٤. A. S. S. Dixit“ ,Games of Strategy ”, . .٢٠٠١

١٥. R. D. M. A. M. a. T. T. L. McKelvey , “Gambit: Software Tools for Game Theory . .٢٠٠٧ ”,,Available: http://econweb.tamu.edu/gambit.

١٦. GAMBIT“ ,GAMBIT . .٢٠١٣ ٧ ”, Available: http://www.gambit-project.org./