ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

طرح یک سیستم تشخیص نفوذ سلسله مراتبی کارا در شبکه‌های سیار موردی مبتنی بر نظریه بازیها

مهدی خلیل‌زاده[۱]، محمود فتحی[۲]

دانشگاه علم و صنعت ایران، مرکز آموزش الکترونیک، گروه فناوری اطلاعات و ارتباطات[۱]

دانشگاه علم و صنعت ایران، دانشکده مهندسی کامپیوتر[۲]

{mkhalilzadeh, mahfathy}@iust.ac.ir

چکیده

در این مقاله طرح یک سیستم تشخیص نفوذ سلسله‌مراتبی کارا در شبکه‌های سیار موردی با استفاده از نظریه بازیها ارائه شده است. در طرح ارائه شده با ارائه یک مدل بازی دو نفره بین مهاجم و هر سطح سیستم تشخیص نفوذ سلسله مراتبی، استراتژی بهینه هر سطح در پاسخگویی یا ارسال گزارش به سطح بالاتر تعیین شده است. در تعیین این استراتژی نرخ تشخیص نفوذ هر سطح، نرخ خطای هشدار، هزینه تشخیص، هزینه ارسال به لایه بعد و مهلت پاسخگویی و انجام واکنش مناسب در نظر گرفته شده است.

واژه‌های کلیدی

سیستم تشخیص نفوذ سلسله‌مراتبی، نظریه بازیها، بازی بیزین(Bayesian game)، مدافع، مهاجم

۱- مقدمه

سیستم‌های تشخیص نفوذ سیستم‌های نرم‌افزاری یا سخت‌افزاری هستند که فرآیند نظارت بر رخدادها در شبکه یا سیستم‌های کامپیوتری را بطور خودکار انجام می‌دهند و با جمع آوری اطلاعات فعالیت‌ها و تحلیل آنها تشخیص می‌دهند که آیا فعالیتی غیر عادی یا مطابق با یک حمله از پیش تعریف شده رخ داده است یا خیر و در صورت بروز رخداد غیر معمول با تولید هشدار مناسب، مدیر سیستم را خبر می‌کنند. سیستمهای تشخیص و مقابله با نفوذ امکان پاسخگویی مناسب به فعالیتهای مخرب را نیز فراهم می‌نمایند[۱،۲].

معماری سیستمهای تشخیص نفوذ به زیرساخت شبکه وابسته است. در شبکه‌های سیمی ترافیک شبکه از طریق سوئیچها، روترها و دروازه‌ها انتقال می‌یابد. بنابراین امکان استفاده از سیستم تشخیص نفوذ در کنار این دستگاه‌ها یا پیاده‌سازی آن در داخل آنها وجود دارد. این در حالیست که در در شبکه‌های سیار موردی چنین دستگاه‌هایی بکار گرفته نمی‌شود. علاوه بر آن رسانه باز و قابل دسترس این شبکه‌ها امکان دسترسی کاربران خرابکار را در کنار سایر کاربران فراهم می‌کند. این ویژگی به همراه توپولوژی پویا و متغیر شبکه باعث می‌شود تمایز بین فعالیت‌های عادی و غیرعادی کاربران در محیط سیار بسیار مشکل گردد. بنابراین معماری سیستم‌های تشخیص نفوذ بکارگرفته شده در شبکه‌های سیمی قابل استفاده مستقیم در شبکه‌های سیار موردی نخواهد بود.

زیرساخت شبکه‌های سیار موردی برحسب کاربرد ممکن است مسطح یا چندلایه‌ای باشد. در زیرساخت مسطح همه گره‌ها معادل در نظر گرفته می‌شوند، در حالیکه در زیرساخت لایه‌ای بعضی گره‌ها با سایرین متفاوت هستند. در این زیرساخت، گره‌ها با استفاده از مفهوم خوشه‌بندی به چندین خوشه[۱] تقسیم می‌شوند (خوشه‌های سطح اول)، و هر خوشه یک سرخوشه دارد (سرخوشه-های سطح اول). سرخوشه‌های سطح اول نیز از مفهوم خوشه‌بندی برای سازماندهی بین خودشان و انتخاب سرخوشه‌های سطح دوم استفاده می‌کنند. این رویه تا جایی ادامه پیدا می‌کند که کلیه گره‌های شبکه در ساختار سلسله مراتبی قرار گیرند. ارتباط بین گره‌ها در داخل خوشه‌ها به صورت مستقیم و ارتباط بین خوشه‌ها از طریق سرخوشه‌ها صورت می‌گیرد.

[1] Cluster

در شبکه‌های سیار موردی، معماری سیستم‌های تشخیص نفوذ براساس زیرساخت به سه دسته مستقل[1]، "توزیع شده و همکارانه"[2] و سلسله‌مراتبی[3] تقسیم می‌شود[۳].

در معماری مستقل، بر روی هر گره به صورت مستقل یک سیستم تشخیص نفوذ اجرا می‌شود. تصمیمات گرفته شده در هر گره بر اساس اطلاعاتی است که در همان گره جمع‌آوری می‌شود و هیچگونه همکاری بین گره‌های شبکه صورت نمی‌گیرد. این معماری در شبکه‌هایی که در آن همه گره‌ها قادر به نصب و اجرای یک سیستم تشخیص نفوذ هستند مناسب است. همچنین استفاده از آن در شبکه‌های مسطح کاراتر از شبکه‌های چندلایه‌ای است. با اینحال به دلیل اینکه اطلاعات گره‌های مستقل برای تشخیص‌نفوذ کافی نیست این معماری کارایی زیادی ندارد.

در معماری توزیع شده و همکارانه، هر گره با اجرای یک عامل تشخیص نفوذ در مکانیزم تشخیص نفوذ و پاسخ شرکت می‌کند. عاملهای تشخیص نفوذ مسئول جمع‌آوری و تحلیل اطلاعات محلی هر گره و بروز عکس‌العمل مناسب در برابر نفوذهای احتمالی هستند. در اینحالت زمانیکه شواهد کافی جهت تصمیم گیری قطعی وجود نداشت عاملهای تشخیص نفوذ همسایه در یک مکانیزم تشخیص نفوذ سراسری و همکارانه شرکت می‌کنند. همانند معماری مستقل، استفاده از این معماری نیز در شبکه‌های مسطح مناسبتر از شبکه‌های چندلایه‌ای است.

معماری سلسله‌مراتبی بسط معماری توزیع شده است که برای شبکه‌های چندلایه‌ای مناسب است. در این معماری گره‌ها در هر خوشه مسئول جمع‌آوری و تحلیل اطلاعات محلی خود و بروز عکس‌العمل مناسب در برابر نفوذهای تشخیص داده شده هستند. سرخوشه‌ها علاوه بر جمع‌آوری و تحلیل اطلاعات محلی خود، مسئول جمع‌آوری و تحلیل اطلاعات خوشه خود نیز هستند. زمانیکه شواهد کافی جهت تصمیم گیری قطعی در هر خوشه وجود نداشت اطلاعات آن خوشه از طریق سرخوشه به خوشه سطح بالاتر ارسال می‌گردد، این روند تا رسیدن به نرخ تشخیص قابل قبول ادامه می‌یابد.

۲- کارهای مرتبط

امروزه بسیاری روش‌های مبتنی بر نظریه بازیها در حوزه کامپیوتر و امنیت شبکه، به منظور مدل‌کردن، تحلیل و بهینه‌سازی عملکرد و کارایی سیستم‌های تشخیص نفوذ در شبکه‌های سیمی و بی‌سیم مورد استفاده قرار گرفته است.

Kodialam و Lakshman در [۴] مدل سیستم تشخیص نفوذی به صورت یک بازی ۲ نفره بین فراهم‌کننده سرویس و نفوذگر ارائه داده‌اند. در این مدل نفوذ زمانی با موفقیت صورت می‌گیرد که بسته مخرب به مقصد مورد نظر برسد. در بازی، هدف نفوذگر انتخاب مسیری خاص بین گره مبدا و مقصد است، و هدف فراهم-کننده سرویس انتخاب مجموعه لینک‌های مناسب برای نمونه-برداری و تشخیص نفوذ است. بازی بصورت یک بازی ۲ نفره با جمع صفر[4] تعریف شده است. فراهم‌کننده سرویس سعی می‌کند با افزایش احتمال تشخیص، مطلوبیتش را حداکثر کند و نفوذگر سعی می‌کند احتمال تشخیص را به حداقل برساند. راه‌حل بهینه برای هر دو بازیکن استراتژی minmax است.

محدودیت این بازی شرط داشتن اطلاعات کامل[5] است. به این معنا که نفوذگر اطلاعات قابل توجهی راجع به شبکه دارد و قادر است با انتخاب مسیر بهینه استراتژی minmax را بازی کند. علاوه بر آن استفاده از بازیهای با جمع صفر برای مدل کردن سیستم-های تشخیص نفوذ به این معناست که بین هزینه تشخیص و هزینه نفوذ رقابت متقابل شدیدی وجود دارد. این فرض در حالت کلی درست نیست. مثلا در [۴] هزینه نمونه‌برداری از چندین لینک، بسیار بیشتر از هزینه ارسال بسته مخرب در یک مسیر خاص است.

Patcha و Park در [۵] تعامل بین مهاجم و سیستم تشخیص نفوذ را به صورت یک بازی پویای چندمرحله‌ای دونفره با اطلاعات ناقص[6] مدل کرده‌اند. در این بازی هدف مهاجم ارسال پیام‌های مخرب به گره هدف به قصد حمله به آن است. حمله زمانی موفقیت‌آمیز است که پیام مخرب بدون اینکه توسط سیستم تشخیص نفوذ تشخیص داده شود به گره هدف برسد. اگر سیستم تشخیص نفوذ تشخیص دهد که پیام دریافتی مخرب است گره مهاجم بلوکه و حمله متوقف می‌شود. در این مدل هدف سیستم تشخیص نفوذ انتخاب استراتژی بهینه در پاسخ به پیامهای دریافتی از فرستنده است. انتخاب استراتژی بر اساس اعتقادات قبلی صورت می‌گیرد و بهره موثر با به حداقل رساندن هزینه پیامهای هشدار اشتباه و نفوذهای تشخیص داده نشده حداکثر می‌گردد.

این مدل کاملا نظری است و در آن مشخص نشده سیستم تشخیص نفوذ چگونه استراتژی مهاجم را تخمین می‌زند و چگونه اعتقاداتش را بروزرسانی می‌کند.

بسیاری مدل‌ها برای حل مساله خودخواهی و همکاری گره‌ها در شبکه‌های موردی ارائه شده است(بعنوان مثال [۶-۱۰]). در اکثر این مدل‌ها استراتژی هر گره جلورانی یا عدم جلورانی بسته‌ها با در نظرگرفتن هزینه(مصرف انرژی)، منفعت(گذردهی شبکه) و میزان همکاری گره‌های همسایه است. این مدل‌ها نشان می‌دهند با

[1] Stand-alone IDS
[2] Distributed and Cooperative IDS
[3] Hierarchical IDS

[4] Zero-sum game
[5] Perfect Information
[6] Two player multi-stage dynamic game with incomplete information

اعمال مکانیزم‌های همکاری گره‌های خودخواه گذردهی کمتری از شبکه دریافت می‌کنند. با اینحال حل مساله خودخواهی به تنهایی مشکل امنیت را حل نمی‌کند. یک گره بداندیش[1] بسیار مخربتر از یک گره خودخواه است.

Agah و همکاران در [۱۱] و Alpcan و Basar در [۱۲] یک مدل بازی دونفره با جمع غیرصفر برای شبکه حسگرها ارائه داده‌اند. محدودیت بزرگ این مدل‌ها فرض داشتن اطلاعات کامل است. به این معنا که سیستم تشخیص نفوذ بطور قطع می‌داند که بازیکن مقابل مهاجم است. در حالیکه در شبکه‌های واقعی چنین فرضی درست نیست و سیستم تشخیص نفوذ اطلاعات کاملی از ماهیت مهاجم ندارد.

Yu Liu و همکاران در [۱۳] از نظریه بازیها برای تعیین استراتژی دفاعی موثر و کارا در شبکه‌ای با چندین سیستم تشخیص نفوذ(یا سیستم تشخیص نفوذی با چندین روش تشخیص) استفاده کرده‌اند. آنها تعاملات بین مهاجم و مدافع را بصورت دوبازی با جمع صفر و جمع غیرصفر مدل کرده‌اند.

در بازی با جمع صفر، هدف مدافع حداکثرکردن منفعت مورد انتظار و هدف مهاجم حداقل کردن هزینه مورد انتظار است. این مدل برای شبکه‌های با محدودیت انرژی مناسب نیست. به همین دلیل در [۱۳] مدل بازی دیگری با جمع غیرصفر با در نظرگرفتن هزینه پایش[2] و هزینه حمله ارائه شده است. در این مدل مدافع با در نظر گرفتن هزینه پایش(مثلا منابع حافظه و مصرف توان)، نرخ تشخیص و نرخ خطای هشدار، مجموعه مناسبی از روشهای تشخیص نفوذ را برای مقابله با حمله مهاجم تعیین می‌کند. محدودیت بزرگ این مدل نیز فرض داشتن اطلاعات کامل راجع به مهاجم است.

Yu Liu و همکاران در [۱۴] شبکه‌ای مسطح با N گره سیار را در نظر گرفته‌اند که سیستم تشخیص نفوذ بر روی هر گره آن در حال اجرا است. سپس تعاملات بین مهاجم و مدافع را بصورت یک بازی دونفره بیزین[3] در دو حالت ایستا و پویا مدل کرده‌اند. در این مدل یک بازیکن مهاجم بالقوه است و بازیکن دیگر مدافع است. نوع[4] بازیکن مهاجم با θ_i نمایش داده می‌شود و جزء اطلاعات خصوصی آن محسوب می‌شود، به این معنا که مدافع از بداندیش بودن یا نبودن بازیکن مقابل باخبر نیست. $\theta_i=0$ به معنای عادی بودن و $\theta_i=1$ به معنای بداندیش بودن مهاجم است. نوع بازیکن مدافع با $\theta_j=0$ نمایش داده می‌شود و به معنای عادی بودن آن است. بازیکن مهاجم از نوع بازیکن مدافع باخبر است.

اگر بازیکن i از نوع بداندیش باشد استراتژی آن Attack یا Not attack و اگر از نوع عادی باشد استراتژی‌اش Not attack است. استراتژی بازیکن j(مدافع) Monitor یا Not monitor است. c_a هزینه حمله مهاجم است. ω ارزش امنیتی منابع است. به این معنا که در صورت موفقیت مهاجم در دسترسی به منابع، خسارتی معادل $-\omega$ به مدافع وارد می‌شود. c_m هزینه پایش، α نرخ تشخیص و β نرخ خطای هشدار است.

در نمایش درختی مدل بازی ارائه شده، عدم قطعیت در مورد نوع بازیکن i با اضافه کردن گره N(به معنای Nature) نشان داده شده است. μ_0 احتمال بداندیش بودن بازیکن i و $1-\mu_0$ احتمال عادی بودن آن است. μ_0 جزء اطلاعات عمومی بازی است به این معنا که بازیکن j به آن اعتقاد دارد و بازیکن i نیز از اعتقاد بازیکن j باخبر است و بازیکن j می‌داند که بازیکن i از این موضوع باخبر است. در حالت ایستا مقدار μ_0 مقداری ثابت است ولی در حالت پویا در پایان هر مرحله تکرار بازی، بازیکن j اعتقاد خود را در مورد نوع بازیکن i با استفاده از قانون بیز و براساس رفتار بازیکن i در آن مرحله و پیشینه رفتارش در مراحل قبل بهبود می‌بخشد.

حل بازی منجر به تعیین استراتژی بهینه هر بازیکن در برابر بازیکن مقابل خواهد بود. در مدل مذکور استراتژی بهینه مهاجم حمله با احتمال $p^*=\frac{\beta\omega+c_m}{(2\alpha+\beta)\omega\mu_0}$ و استراتژی بهینه مدافع پایش با احتمال $q^*=\frac{\omega-c_a}{2\alpha\omega}$ است. همانطور که ذکر شد این مدل در شبکه‌های سیار موردی با معماری مسطح کاربرد دارد.

مدل بازیهای ارائه شده مذکور جهت بکارگیری در شبکه‌های مسطح مناسب است و امکان استفاده از آنها در شبکه های چندلایه وجود ندارد. علاوه بر آن، در معماری سیستم‌های تشخیص نفوذ سلسله مراتبی معمول هنگام ارسال گزارش از سطوح پایین به سطوح بالا، به دو مساله مهم توجه نشده است: مساله اول اینکه اگرچه ارسال گزارش به لایه‌های بالاتر منجر به تشخیص با دقت بیشتری می‌گردد، در مقابل سربار و هزینه تشخیص بیشتری نیز به همراه دارد، و مساله دوم اینکه ارسال به لایه‌های بالاتر نیاز به زمان بیشتری دارد و ممکن است مهلت پاسخگویی و انجام واکنش مناسب سپری شود. این مساله در شبکه‌هایی همچون شبکه خودروها[5]، که بخشی از حملات مربوط به ایمنی خودرو و سرنشینان آن می‌شود بسیار حائز اهمیت است. ما در ادامه با ارائه مدلی مبتنی بر نظریه بازیها به حل مسائل فوق در سیستم‌های تشخیص نفوذ سلسله مراتبی در شبکه‌های سیار موردی می‌پردازیم و در مدل بازی ارائه شده به فرض عدم قطعیت مدافع در مورد ماهیت مهاجم و نحوه بروزرسانی اعتقاداتش توجه می‌کنیم.

[1] Malicious
[2] Monitoring
[3] Bayesian game
[4] Type
[5] Vehicular Ad hoc Network(VANET)

۳- مدل بازی پیشنهادی

تعاملات بین مهاجم و سیستم تشخیص نفوذ را بصورت یک بازی دونفره پویای بیزین مدل می‌کنیم. در نظریه بازیها، بازی بیزین بازی است که در آن حداقل یک بازیکن اطلاعات کاملی راجع به بازیکن مقابل ندارد. در این حالت هر بازیکن راجع به نوع بازیکن مقابل یک توزیع احتمال اختصاص می‌دهد[۱۵].

انتخاب بازی بیزین، به دلیل ماهیت تعاملات بین سیستم تشخیص نفوذ و گره‌های شبکه است. در واقع این تعاملات به صورت یک "بازی با اطلاعات ناتمام"[1] است که در آن سیستم تشخیص نفوذ در مورد نوع بازیکن مقابل قطعیت ندارد. بازی بیزین این امکان را برای سیستم‌تشخیص نفوذ فراهم می‌کند تا بر اساس اعتقادش راجع به نوع بازیکن مقابل، استراتژی مناسب را انتخاب کند.

در مدل بازی ارائه شده یک بازیکن مهاجم احتمالی است و با i نشان داده می‌شود، بازیکن دیگر مدافع است و با j نشان داده می‌شود. بازیکن i دو نوع دارد: نوع عادی[2] که با $\theta_i=0$ مشخص می‌شود و نوع بداندیش که با $\theta_i=1$ مشخص می‌شود. نوع بازیکن i جزء اطلاعات خصوصی‌اش بحساب می‌آید. به عبارت دیگر بازیکن j از بداندیش بودن یا نبودن بازیکن i با خبر نیست. نوع بازیکن j عادی است و با $\theta_j=0$ نشان داده می‌شود. نوع بازیکن j جزء اطلاعات عمومی بازی است، به این معنا که هر دو بازیکن از آن باخبرند.

نوع بداندیش بازیکن i دو استراتژی خالص Attack و Not attack را بازی می‌کند و نوع عادی آن تنها استراتژی Not Attack را بازی می‌کند. بازیکن j نیز دو استراتژی خالص Deliver to Response Module و Deliver to Next Layer را بازی می‌کند.

مهاجم یک حمله چندمرحله‌ای را با اجرای مرحله اول حمله آغاز می‌کند. سپس با مشاهده واکنش مدافع تصمیم به توقف یا انجام مراحل بعدی حمله می‌گیرد. استراتژی مهاجم در ادامه یا توقف هر مرحله حمله به نحویست که بیشترین بهره مورد انتظار نصیبش گردد و احتمال تشخیصش به حداقل برسد.

مدافع در سطح صفر وقوع یا عدم وقوع حمله را تشخیص می‌دهد. در صورت وجود شواهد کافی پاسخگویی می‌کند و در غیر اینصورت اقدام به ارسال گزارش به سطح یک می‌نماید. علاوه بر آن هنگام دریافت اولین گزارش یک حمله احتمالی، حداکثر مهلت انجام واکنش مناسب در برابر آن حمله را محاسبه می‌نماید و زمان پاسخگویی را به نحوی تنظیم می‌کند که مهلت مقرر سپری نشود. سطح یک با تحلیل رفتار مهاجم، استراتژی پاسخگویی یا ارسال گزارش به سطح بعدی را بنحوی انتخاب می‌کند که بیشترین بهره مورد انتظار نصیبش گردد. این رویه در هر سطح تکرار می‌شود و ارسال گزارش به سطوح بعدی تا انتخاب استراتژی پاسخگویی در سطح مطلوب ادامه می‌یابد. در واقع مدافع سعی در رسیدن به بیشترین نرخ تشخیص با کمترین هزینه ممکن دارد.

$\Omega=\{\omega_1,\omega_2,...,\omega_k\}$ بردار ارزش امنیتی[3] منابع و دارایی‌های[4] سیستم است و $\forall\omega\in\Omega$، $-\omega$ میزان خسارت وارده به سیستم است. مقادیر ω بر اساس سیاستهای امنیتی هر سیستم تعیین می‌گردند. همچنین فرض می‌کنیم ارتباط متقارنی بین میزان منفعت و زیان مدافع و مهاجم وجود دارد. این فرض در تعامل با گره‌های بداندیش در شبکه معقول است.

بردار $C_a=\{c_{a1},c_{a2},...,c_{am}\}$ برداز هزینه مهاجم به ازاء هر یک از حملات نوع ۱ تا m است و $\forall c_a\in C_a\ c_a>0$ است.

بردار $A=\{\alpha_1,\alpha_2,...,\alpha_n\}$ بردار نرخ تشخیص سیستم تشخیص نفوذ در سطوح ۱ تا n است. $\alpha_i\in A$ نرخ تشخیص سیستم تشخیص نفوذ در سطح i است و $\forall i\ \alpha_i\in[0,1],\alpha_i\le\alpha_{i+1}$ است.

بردار $B=\{\beta_1,\beta_2,...,\beta_n\}$ بردار نرخ خطای هشدار سیستم تشخیص نفوذ در سطوح ۱ تا n است. $\beta_i\in B$ نرخ خطای هشدار سیستم تشخیص نفوذ در سطح i است و $\forall i\ \beta_i\in[0,1],\beta_i\ge\beta_{i+1}$ است.

فرض‌های $\alpha_i\le\alpha_{i+1}$ و $\beta_{i+1}\le\beta_i$ در شرایطی صدق می‌کنند که سیستم‌های تشخیص نفوذ در هر سطح نسبت به سطح پایین‌تر خود، نرخ تشخیص بیشتر و نرخ خطای هشدار کمتری داشته باشند. وجود این شرایط در سیستمهای تشخیص نفوذ سلسله‌مراتبی معقول است.

c_{R_i} هزینه پاسخگویی مدافع و c_{d_i} هزینه تشخیص مدافع در سطح i است. c_{d_i} از رابطه (۱) بدست می‌آید:

$$c_{d_i}=\sum_{k=1}^{i}(\lambda_1 c_{s_k}+\lambda_2 c_{p_k}) \qquad (۱)$$

در رابطه فوق c_{s_k} هزینه ارسال از سطح k-1 به سطح k و c_{p_k} هزینه پردازش در سطح k است. همچنین λ_1 و λ_2 ضرایبی برای تطبیق مقیاس[5] و بعد[6] است.

t_i زمان سپری شده از لحظه دریافت اولین گزارش حمله احتمالی تا پاسخگویی در سطح i است. t_i از رابطه (۲) محاسبه می‌شود:

$$t_i=\sum_{k=1}^{i}(t_{s_k}+t_{p_k})+t_{R_i} \qquad (۲)$$

در رابطه فوق t_{s_k} زمان ارسال از سطح k-1 به سطح k، t_{p_k} زمان پردازش در سطح k و t_{R_i} زمان لازم برای پاسخگویی در سطح i است.

---

[1] Incomplete information game
[2] Regular
[3] Security value
[4] Asset
[5] Scale
[6] Dimension

جدول ۱: بازیکن i بداندیش است

	Deliver to Response Module (D.to.R.)	Deliver to Next Layer (D.to.N.)	
Attack	$(1-2\alpha_i)\omega-c_a, (2\alpha_i-1)\omega-\alpha_i c_{R_i}-c_{d_i}$	$(1-2\alpha_{i+1})\omega-c_a, (2\alpha_{i+1}-1)\omega-\alpha_{i+1}c_{R_{i+1}}-c_{d_{i+1}}$	$t_{i+1}\le\tau$
		$\omega-c_a, -\omega-\alpha_{i+1}c_{R_{i+1}}-c_{d_{i+1}}$	$t_{i+1}>\tau$
Not Attack	$0, \omega-\beta_i c_{R_i}-c_{d_i}$	$0, \omega-\beta_{i+1}c_{R_{i+1}}-c_{d_{i+1}}$	

جدول۲: بازیکن i عادی است

	Deliver to Response Module (D.to.R.)	Deliver to Next Layer (D.to.N.)
Not Attack	$0, \omega-\beta_i c_{R_i}-c_{d_i}$	$0, \omega-\beta_{i+1}c_{R_{i+1}}-c_{d_{i+1}}$

τ حداکثر مهلت انجام واکنش مناسب توسط مدافع است. بعنوان مثال در شبکه خودروها، زمانیکه خودرویی با سرعت متوسط $\bar{v}$ در حال حرکت است و گزارشی مربوط به وقوع رخدادی در مکانی مشخص دریافت می‌کند باید پیش از رسیدن به مکان فوق از صحت یا عدم صحت گزارش دریافتی اطمینان حاصل کند و در صورت صحت گزارش، واکنش مناسب (مثلا کاهش سرعت، توقف، تغییر مسیر و ...) را بروز دهد. در این شبکه مقدار τ از رابطه (۳) بدست می‌آید:

$$\tau=\frac{d}{\bar{v}} \qquad (۳)$$

در رابطه فوق d فاصله تخمینی از مکان دریافت اولین گزارش تا مکان انجام واکنش مناسب توسط خودرو است، این فاصله بر اساس نوع رخداد، مکان وقوع آن و نوع واکنش مناسب در برابر آن محاسبه می‌گردد. $\bar{v}$ سرعت متوسط خودرو است.

مقدار $\omega>c_a,c_d$ است، زیرا در غیراینصورت نه مهاجم انگیزه‌ای برای حمله دارد و نه مدافع انگیزه‌ای برای تشخیص و پاسخگویی دارد.

هزینه تشخیص و حمله ممکن است تابعی از انرژی، زمان و یا هزینه دریافت سرویس از اپراتور شبکه باشد.

جدول (۱) و (۲) ماتریس بهره بازی به شکل استراتژیک را نمایش می‌دهد:

در جدول (۱) برای ترکیب استراتژی (Attack , D.to.R.) بهره مدافع برابر منفعت مورد انتظار[1] از تشخیص حمله در سطح i منهای هزینه تشخیص و پاسخگویی حمله در سطح i است.

منفعت مورد انتظار تشخیص حمله در سطح i به نرخ تشخیص در سطح i، α_i، بستگی دارد. رابطه (۴) نحوه بدست آوردن بهره مدافع را نشان می‌دهد:

$$\alpha_i(\omega-c_{R_i})-(1-\alpha_i)\omega-c_{d_i}=(2\alpha_i-1)\omega-\alpha_i c_{R_i}-c_{d_i} \qquad (۴)$$

در رابطه فوق $(1-\alpha_i)$ نرخ خطا در تشخیص است. براساس رابطه (۴) منفعت مورد انتظار مهاجم از حمله برابر $-(2\alpha_i-1)\omega$ است، لذا بهره مهاجم برابر $(1-2\alpha_i)\omega-c_a$ خواهد بود.

برای ترکیب استراتژی (Attack , D.to.N.) در حالتی که $t_{i+1}\le\tau$ است مشابه رابطه (۴) بهره مدافع برابر $(2\alpha_{i+1}-1)\omega-\alpha_{i+1}c_{R_{i+1}}-c_{d_{i+1}}$ و بهره مهاجم برابر $(1-2\alpha_{i+1})\omega-c_a$ می‌شود. در حالتی که $t_{i+1}>\tau$ است ارسال به سطح بعد موجب انقضای مهلت پاسخگویی مدافع می‌شود، لذا بهره مهاجم برابر $\omega-c_a$ و بهره مدافع برابر $-\omega-\alpha_{i+1}c_{R_{i+1}}-c_{d_{i+1}}$ می‌شود.

در حالتی که استراتژی بازیکن i، Not attack است(جدول (۱) و (۲))، بهره مدافع برابر مقدار ω منهای هزینه تشخیص و هزینه خطای هشدار در سطح i است. هزینه خطای هشدار به نرخ خطای هشدار در سطح i، β_i، بستگی دارد. رابطه (۵) نحوه بدست آوردن بهره مدافع را نشان می‌دهد:

$$\beta_i(\omega-c_{R_i})+(1-\beta_i)\omega-c_{d_i}=\omega-\beta_i c_{R_i}-c_{d_i} \qquad (۵)$$

بهره مهاجم در این‌حالت برابر مقدار صفر است.

[1] Expected benefit

۴- تحلیل تعادل نش بیزین[1]

شکل (۱) نمایش درختی مدل بازی بیزین ارائه شده است. در شکل گره N نمایش دهنده "Nature" است و نوع بازیکن i را مشخص می‌کند. فرض می‌کنیم بازیکن j با احتمال اولیه μ_0 بازیکن i را بداندیش در نظر می‌گیرد و بازیکن i از این موضوع باخبر است.

بازیکنان عاقل[2] هستند و هدف هر دو به حداکثر رساندن بهره مورد انتظارشان است، در واقع بازیکن i با اجرای استراتژی بیزین خود سعی در به حداقل رساندن احتمال تشخیصش دارد و بازیکن j با اجرای استراتژی بیزین خود سعی در به حداکثر رساندن احتمال تشخیص با کمترین هزینه ممکن دارد.

برای تحلیل بازی ۳ حالت مختلف درنظر می‌گیریم:

حالت۱- اگر بازیکن i استراتژی خالص (Attack if malicious, Not attack if regular) را بازی کند، آنگاه بهره مورد انتظار بازیکن j با اجرای استراتژی خالص D.to.R. از رابطه (۶) بدست می‌آید:

$$Eu_j(D.to.R.) = \mu((2\alpha_i - 1)\omega - \alpha_i c_{R_i} - c_{d_i}) + (1-\mu)(\omega - \beta_i c_{R_i} - c_{d_i}) \quad (۶)$$

همچنین بهره مورد انتظار بازیکن j با اجرای استراتژی خالص D.to.N. از رابطه (۷) و (۸) بدست می‌آید:

$$Eu_j(D.to.N.) = \mu((2\alpha_{i+1} - 1)\omega - \alpha_{i+1} c_{R_{i+1}} - c_{d_{i+1}}) + (1-\mu)(\omega - \beta_{i+1} c_{R_{i+1}} - c_{d_{i+1}}) \quad if\ t_{i+1} \le \tau \quad (۷)$$

$$Eu_j(D.to.N.) = \mu(-\omega - \alpha_{i+1} c_{R_{i+1}} - c_{d_{i+1}}) + (1-\mu)(\omega - \beta_{i+1} c_{R_{i+1}} - c_{d_{i+1}}) \quad if\ t_{i+1} > \tau \quad (۸)$$

۱-۱- در اینحالت اگر داشته باشیم:

$$Eu_j(D.to.R.) > Eu_j(D.to.N.),\ t_{i+1} \le \tau$$

یا بعبارتی

$$\mu > \frac{(c_{d_i} - c_{d_{i+1}}) + \beta_i c_{R_i} - \beta_{i+1} c_{R_{i+1}}}{2\omega(\alpha_i - \alpha_{i+1}) + (\beta_i - \alpha_i) c_{R_i} - (\beta_{i+1} - \alpha_{i+1}) c_{R_{i+1}}},\ t_{i+1} \le \tau \quad (۹)$$

آنگاه بهترین پاسخ بازیکن j اجرای استراتژی خالص D.to.R. است. با اینحال در صورت اجرای استراتژی خالص D.to.R. توسط بازیکن j، بازیکن i استراتژی خالص Attack را با شرط زیر بازی خواهد کرد:

$$(1-2\alpha_i)\omega - c_a > 0 \Rightarrow 0 < c_a < (1-2\alpha_i)\omega \quad (۱۰)$$

بنابراین با برقراری شرط (۹) و (۱۰) استراتژی ((Attack if malicious , Not attack if regular) , D.to.R.) یک تعادل نش بیزین با استراتژی خالص خواهد بود.

۱-۲- اگر داشته باشیم:

$$Eu_j(D.to.R.) < Eu_j(D.to.N.),\ t_{i+1} \le \tau \quad (۱۱)$$

یا بعبارتی

$$\mu < \frac{(c_{d_i} - c_{d_{i+1}}) + \beta_i c_{R_i} - \beta_{i+1} c_{R_{i+1}}}{2\omega(\alpha_i - \alpha_{i+1}) + (\beta_i - \alpha_i) c_{R_i} - (\beta_{i+1} - \alpha_{i+1}) c_{R_{i+1}}},\ t_{i+1} \le \tau \quad (۱۲)$$

آنگاه بهترین پاسخ بازیکن j اجرای استراتژی خالص D.to.N. است. با اینحال در صورت اجرای استراتژی خالص D.to.N. توسط بازیکن j، بازیکن i استراتژی خالص Attack را با شرط زیر بازی خواهد کرد:

$$(1-2\alpha_{i+1})\omega - c_a > 0 \Rightarrow 0 < c_a < (1-2\alpha_{i+1})\omega \quad (۱۳)$$

بنابراین با برقراری شرط (۱۲) و (۱۳) استراتژی ((Attack if malicious , Not attack if regular) , D.to.N.) یک تعادل نش بیزین با استراتژی خالص خواهد بود.

۱-۳- اگر داشته باشیم $t_{i+1} > \tau$ آنگاه بهترین پاسخ بازیکن j اجرای استراتژی خالص D.to.R. است و بازیکن i نیز با شرط (۱۰) استراتژی خالص Attack را بازی خواهد کرد.

بنابراین با برقراری شرط $t_{i+1} > \tau$ و (۱۰) استراتژی ((Attack if malicious , Not attack if regular) , D.to.R.) یک تعادل نش بیزین با استراتژی خالص خواهد بود.

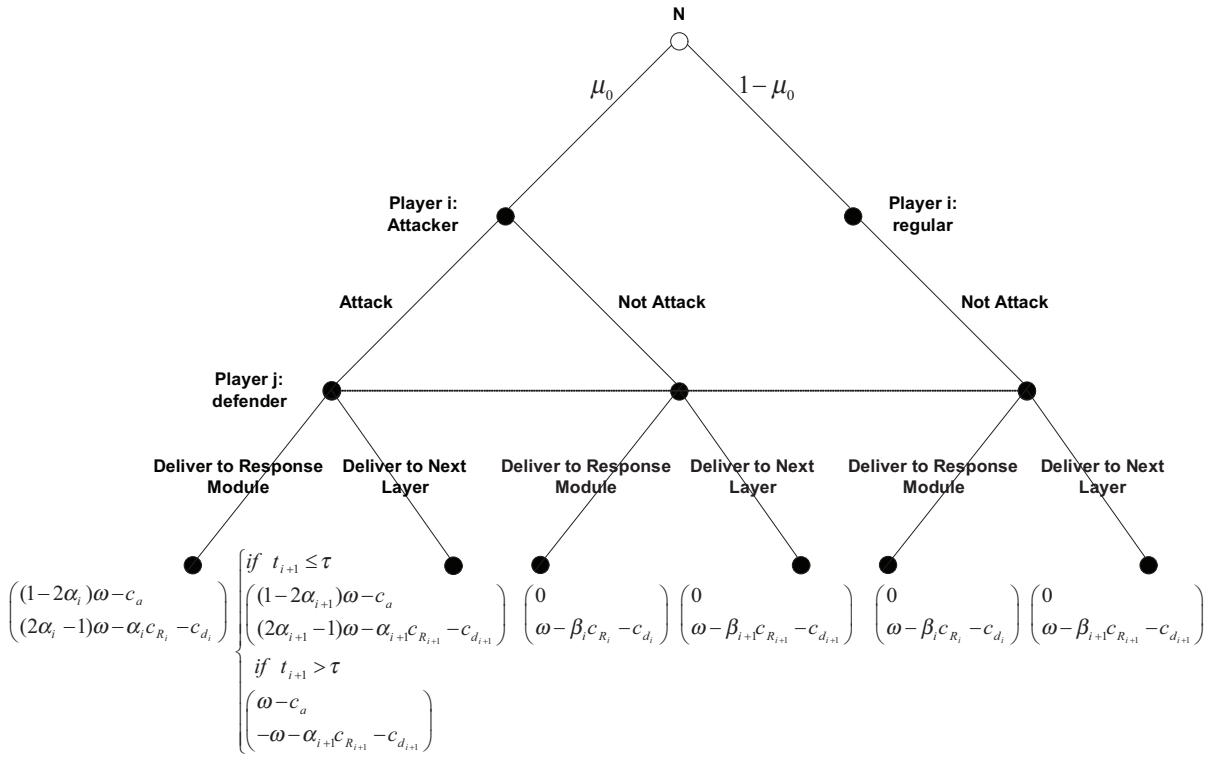
حالت۲- اگر بازیکن i استراتژی خالص (Not attack if malicious, Not attack if regular) را بازی کند، آنگاه بهره مورد انتظار بازیکن j با اجرای استراتژی خالص D.to.R. مستقل از مقدار μ است و از رابطه (۱۴) بدست می‌آید:

$$Eu_j(D.to.R.) = \omega - \beta_i c_{R_i} - c_{d_i} \quad (۱۴)$$

همچنین بهره مورد انتظار بازیکن j با اجرای استراتژی خالص D.to.N. مستقل از مقدار μ است و از رابطه (۱۵) بدست می‌آید:

$$Eu_j(D.to.N.) = \omega - \beta_{i+1} c_{R_{i+1}} - c_{d_{i+1}} \quad (۱۵)$$

[1] Bayesian Nash Equilibrium(BNE)
[2] Rational



شکل ۱: نمایش درختی مدل بازی ارائه شده

۲-۱- در اینحالت اگر داشته باشیم:

$$Eu_j(D.to.R.)>Eu_j(D.to.N.),\ t_{i+1}\le\tau \qquad (۱۶)$$

یا بعبارتی

$$\beta_i c_{R_i}-\beta_{i+1}c_{R_{i+1}}<c_{d_{i+1}}-c_{d_i},\ t_{i+1}\le\tau \qquad (۱۷)$$

آنگاه بهترین پاسخ بازیکن j اجرای استراتژی خالص D.to.R. است. با اینحال در صورت اجرای استراتژی خالص D.to.R. توسط بازیکن j، بازیکن i استراتژی خالص Not attack را با شرط زیر بازی خواهد کرد:

$$(1-2\alpha_i)\omega-c_a<0 \Rightarrow c_a>(1-2\alpha_i)\omega \qquad (۱۸)$$

بنابراین با برقراری شرط (۱۷) و (۱۸) استراتژی خالص ((Not attack if malicious , Not attack if regular) , D.to.R.) یک تعادل نش بیزین با استراتژی خالص خواهد بود.

۲-۲- اگر داشته باشیم:

$$Eu_j(D.to.R.)<Eu_j(D.to.N.),\ t_{i+1}\le\tau \qquad (۱۹)$$

یا بعبارتی

$$\beta_i c_{R_i}-\beta_{i+1}c_{R_{i+1}}>c_{d_{i+1}}-c_{d_i},\ t_{i+1}\le\tau \qquad (۲۰)$$

آنگاه بهترین پاسخ بازیکن j اجرای استراتژی خالص D.to.N. است. با اینحال در صورت اجرای استراتژی خالص D.to.N. توسط بازیکن j، بازیکن i استراتژی خالص Not attack را با شرط زیر بازی خواهد کرد:

$$(1-2\alpha_{i+1})\omega-c_a<0 \Rightarrow c_a>(1-2\alpha_{i+1})\omega \qquad (۲۱)$$

بنابراین با برقراری شرط (۲۰) و (۲۱) استراتژی خالص ((Not attack if malicious , Not attack if regular) , D.to.N.) یک تعادل نش بیزین با استراتژی خالص خواهد بود.

۲-۳- اگر داشته باشیم $t_{i+1}>\tau$ آنگاه بهترین پاسخ بازیکن j اجرای استراتژی خالص D.to.R. است و بازیکن i نیز با شرط (۱۸) استراتژی خالص Not attack را بازی خواهد کرد.

بنابراین با برقراری شرط $t_{i+1}>\tau$ و (۱۸) استراتژی خالص ((Not attack if malicious , Not attack if regular) , D.to.R. , (μ یک تعادل نش بیزین با استراتژی خالص خواهد بود.

حالت۳- نشان می‌دهیم در صورت برقراری شرطهای (۲۶)، (۲۷) و (۳۳) بازی تعادل نش بیزین با استراتژی آمیخته نیز دارد.

فرض می‌کنیم p احتمال اجرای استراتژی (attack if malicious) توسط بازیکن i و q احتمال اجرای استراتژی D.to.R. توسط بازیکن j است. آنگاه بهره مورد انتظار بازیکن j با اجرای استراتژی D.to.R. از رابطه (۲۲) بدست می‌آید:

$$Eu_j(D.to.R.) = p\mu((2\alpha_i - 1)\omega - \alpha_i c_{R_i} - c_{d_i}) + (1-p)\mu(\omega - \beta_i c_{R_i} - c_{d_i}) + (1-\mu)(\omega - \beta_i c_{R_i} - c_{d_i}) = p\mu(2\omega(\alpha_i - 1) + c_{R_i}(\beta_i - \alpha_i)) + (\omega - \beta_i c_{R_i} - c_{d_i}) \quad (۲۲)$$

همچنین بهره مورد انتظار بازیکن j با اجرای استراتژی خالص D.to.N. از رابطه (۲۳) بدست می‌آید:

$$Eu_j(D.to.N.) = p\mu((2\alpha_{i+1} - 1)\omega - \alpha_{i+1} c_{R_{i+1}} - c_{d_{i+1}}) + (1-p)\mu(\omega - \beta_{i+1} c_{R_{i+1}} - c_{d_{i+1}}) + (1-\mu)(\omega - \beta_{i+1} c_{R_{i+1}} - c_{d_{i+1}}) = p\mu(2\omega(\alpha_{i+1} - 1) + c_{R_{i+1}}(\beta_{i+1} - \alpha_{i+1})) + (\omega - \beta_{i+1} c_{R_{i+1}} - c_{d_{i+1}}) \quad (۲۳)$$

با مساوی قرار دادن $Eu_j(D.to.N.) = Eu_j(D.to.R.)$ مشخص می‌شود استراتژی تعادلی آمیخته بازیکن i استراتژی attack با احتمال زیر است:

$$p^* = \frac{(c_{d_{i+1}} - c_{d_i}) + \beta_{i+1} c_{R_{i+1}} - \beta_i c_{R_i}}{\mu(2\omega(\alpha_{i+1} - \alpha_i) + c_{R_i}(\alpha_i - \beta_i) - c_{R_{i+1}}(\alpha_{i+1} - \beta_{i+1}))} \quad (۲۴)$$

از طرفی داریم:

$$0 \le p^* \le 1 \quad (۲۵)$$

بنابراین:

$$p^* \le 1 \Rightarrow \mu \ge \frac{(c_{d_{i+1}} - c_{d_i}) + \beta_{i+1} c_{R_{i+1}} - \beta_i c_{R_i}}{(2\omega(\alpha_{i+1} - \alpha_i) + c_{R_i}(\alpha_i - \beta_i) - c_{R_{i+1}}(\alpha_{i+1} - \beta_{i+1}))} \quad (۲۶)$$

$$p^* \ge 0 \Rightarrow \begin{cases} (c_{d_{i+1}} - c_{d_i}) \ge \beta_i c_{R_i} - \beta_{i+1} c_{R_{i+1}} \\ 2\omega(\alpha_{i+1} - \alpha_i) > (\alpha_{i+1} - \beta_{i+1}) c_{R_{i+1}} - (\alpha_i - \beta_i) c_{R_i} \\ OR \\ (c_{d_{i+1}} - c_{d_i}) \le \beta_i c_{R_i} - \beta_{i+1} c_{R_{i+1}} \\ 2\omega(\alpha_{i+1} - \alpha_i) < (\alpha_{i+1} - \beta_{i+1}) c_{R_{i+1}} - (\alpha_i - \beta_i) c_{R_i} \end{cases} \quad (۲۷)$$

به طریق مشابه بهره مورد انتظار بازیکن i با اجرای استراتژی خالص attack از رابطه (۲۸) بدست می‌آید:

$$Eu_i(Attack) = q\mu((1-2\alpha_i)\omega - c_a) + (1-q)\mu((1-2\alpha_{i+1})\omega - c_a) = \mu q\omega(2\alpha_{i+1} - 2\alpha_i) + \mu((1-2\alpha_{i+1})\omega - c_a) \quad (۲۸)$$

همچنین بهره مورد انتظار بازیکنi با اجرای استراتژی Not attack از رابطه (۲۹) بدست می‌آید:

$$Eu_i(Not\ attack) = 0 \quad (۲۹)$$

با مساوی قرار دادن $Eu_i(Attack) = Eu_i(Not\ attack)$ مشخص می‌شود استراتژی تعادلی آمیخته بازیکن j استراتژی D.to.R. با احتمال زیر است:

$$q^* = \frac{(2\alpha_{i+1} - 1)\omega + c_a}{2\omega(\alpha_{i+1} - \alpha_i)} \quad (۳۰)$$

از طرفی داریم:

$$0 \le q^* \le 1 \Rightarrow 0 \le \frac{(2\alpha_{i+1} - 1)\omega + c_a}{2\omega(\alpha_{i+1} - \alpha_i)} \le 1 \quad (۳۱)$$

بنابراین:

$$q^* \le 1 \Rightarrow c_a \le (1-2\alpha_i)\omega$$
$$q^* \ge 0 \Rightarrow c_a \ge (1-2\alpha_{i+1})\omega \quad (۳۲)$$

در نتیجه:

$$(1-2\alpha_{i+1})\omega \le c_a \le (1-2\alpha_i)\omega \quad (۳۳)$$

بنابراین با برقراری شرطهای (۲۶)، (۲۷) و (۳۳) استراتژی آمیخته((p^* if malicious , Not attack if regular) , q^*) یک تعادل نش بیزین با استراتژی آمیخته خواهد بود.

۵- بروزرسانی اعتقادات بر اساس قانون بیز

تعیین مقدار دقیق احتمال اولیه μ_0 کار بسیار مشکلی است. لذا در این بخش از قانون بیز برای بروزرسانی اعتقاد بازیکن j استفاده می‌کنیم[۱۵ p۳۳۲].

فرض می‌کنیم بازی در دوره‌های زمانی $t=0,1,...,T$ بین مهاجم و مدافع در هر سطح تکرار می‌گردد. افق تکرار بازی نامحدود است، زیرا هیچ بازیکنی نمی‌داند بازیکن مقابل چه موقع بازی را ترک خواهد کرد. همچنین فرض می‌کنیم هویت بازیکنان در طول بازی ثابت و قابل تشخیص است. این فرض مستلزم وجود مکانیزمهای احراز هویت برای مقابله با حملات جعل هویت همچون حمله Sybil است.

در اولین تکرار بازی، $t=0$، اعتقاد بازیکن j در مورد نوع بازیکن i با مقدار اولیه μ_0 (مثلا $\mu_0=\frac{1}{2}$) مشخص می‌گردد. در ادامه، در پایان هر مرحله تکرار بازی، بازیکن j اعتقاد خود را در مورد نوع بازیکن i با استفاده از قانون بیز و براساس عمل مشاهده شده

بازیکن i در آن مرحله و پیشینه اعمالش در مراحل قبل بهبود می‌بخشد. رابطه (۳۴) نحوه انجام این کار را نشان می‌دهد:

$$\mu_j(\theta_i \mid (h^t, a^t)) = \frac{\mu_j(\theta_i \mid h^t) P(a_i{}^t \mid h^t, \theta_i)}{\sum_{\tilde{\theta}_i} \mu_j(\tilde{\theta}_i \mid h^t) P(a_i{}^t \mid h^t, \tilde{\theta}_i)} \quad (۳۴)$$

در رابطه فوق $a_i{}^t$ عمل بازیکن i در دوره t است، بردار $a^t = (a_i{}^t, a_j{}^t)$، بردار عمل بازیکنان در دوره t است، $h^t = (a^0, a^1, ..., a^{t-1})$ پیشینه عمل بازیکنان در شروع دوره t است و $P(a_i{}^t \mid h^t, \theta_i)$ احتمال مشاهده عمل a_i در دوره t با معلوم بودن θ_i و h^t است.

۶- مثال عددی

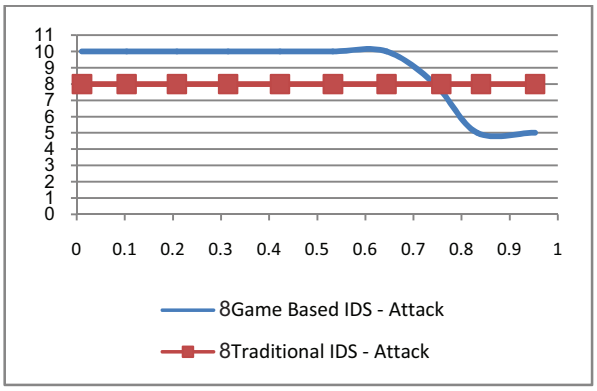
در این بخش با یک مثال عددی تعادل بدست آمده در طرح ارائه شده را نمایش می‌دهیم.

فرض می‌کنیم سیستم تشخیص نفوذ سلسله‌مراتبی ۱۰ سطح دارد. حملات بر اساس نرخ تشخیص سطوح به ۱۰ گروه A_1 تا A_{10} تقسیم می‌شوند. سطح ۱ حملات گروه A_1 را با نرخ قابل قبولی تشخیص می‌دهد. سطح ۲ علاوه بر حملات گروه A_1 حملات گروه A_2 را نیز تشخیص می‌دهد و به همین ترتیب تا سطح ۱۰، که کلیه حملات گروه A_1 تا A_{10} را تشخیص می‌دهد.

بردار $C_{a/\omega} = \{.01, .02, .03, .04, .05, .06, .07, .08, .09, .1\}$ بردار نسبت هزینه حمله مهاجم به ارزش امنیتی منابع است. بردار $A = \{.33, .34, .42, .43, .51, .52, .60, .61, .69, .70\}$ بردار نرخ تشخیص سیستم تشخیص نفوذ در سطوح ۱ تا ۱۰ و بردار $B = \{.80, .72, .64, .56, .48, .40, .32, .24, .16, .08\}$ بردار نرخ خطای هشدار سیستم تشخیص نفوذ در سطوح ۱ تا ۱۰ به ازای حملات گروه A_8 است.

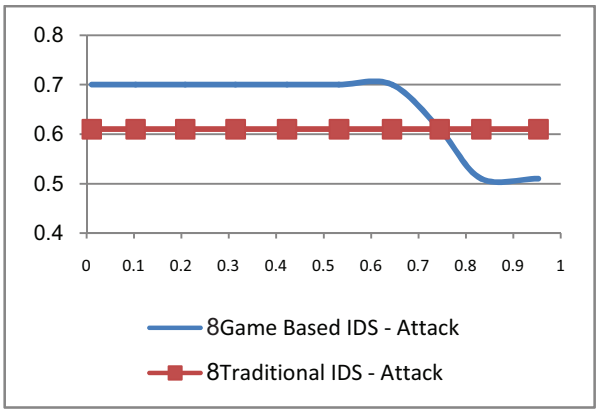
سناریوی فوق در نرم‌افزار MATLAB پیاده شده است. کلیه مقادیر عددی ورودی از طریق فایل ورودی خوانده می‌شود و نتایج خروجی در فایل خروجی ذخیره می‌گردد.

شکل (۲) تغییرات سطح تصمیم‌گیری در طرح ارائه شده را در تشخیص حمله‌ای از گروه A_8 با افزایش هزینه تشخیص(نسبت هزینه تشخیص به ارزش امنیتی) نشان می‌دهد. هزینه تشخیص از .01 تا .95 افزایش می‌یابد. همانطور که در شکل مشخص است در هزینه‌های کمتر از .64 تصمیم‌گیری در سطح ۱۰ انجام می‌شود. با افزایش هزینه از مقدار .64 سطح تصمیم‌گیری کاهش می‌یابد به نحوی که در هزینه .83 تصمیم‌گیری در سطح ۵ انجام می‌شود. تغییرات سطوح تصمیم‌گیری با هدف به حداکثر رساندن بهره سیستم تشخیص نفوذ انجام می‌شود.

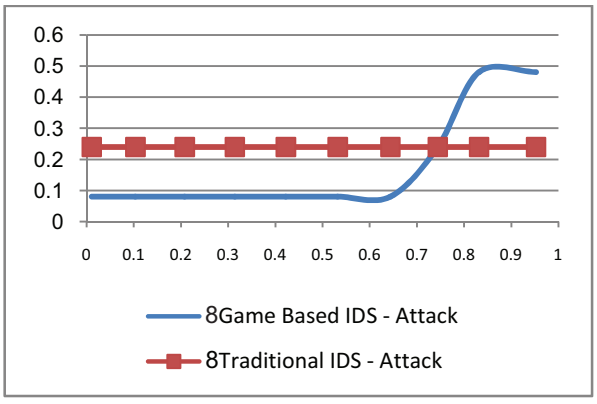


شکل ۲: تغییرات سطح تصمیم گیری در طرح ارائه شده در مقایسه با سیستم‌های تشخیص نفوذ معمول

شکل ۳ تغییرات نرخ تشخیص و شکل (۴) تغییرات نرخ خطای هشدار در طرح ارائه شده را در تشخیص حمله‌ای از گروه A_8 با افزایش هزینه تشخیص نشان می‌دهد. این تغییرات در اثر تغییرات سطح تصمیم‌گیری و با هدف به حداکثر رساندن بهره سیستم تشخیص نفوذ انجام می‌شود. همانطور که در شکل مشخص است افزایش هزینه تشخیص تاثیری در نرخ تشخیص و نرخ خطای هشدار سیستمهای تشخیص نفوذ معمول ندارد.

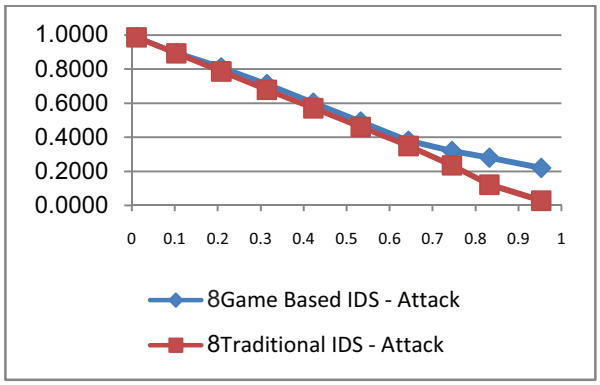


شکل ۳: تغییرات نرخ تشخیص با افزایش هزینه تشخیص در طرح ارائه شده در مقایسه با سیستم‌های تشخیص نفوذ معمول



شکل ۴: تغییرات نرخ خطای هشدار با افزایش هزینه تشخیص در طرح ارائه شده در مقایسه با سیستم¬های معمول

شکل ۵ مقایسه بین تغییرات بهره سیستم تشخیص نفوذ در طرح ارائه شده با سیستمهای تشخیص نفوذ معمول است.



شکل ۵: تغییرات بهره سیستم تشخیص نفوذ در طرح ارائه شده در مقایسه با سیستم‌های تشخیص نفوذ معمول

۷- نتیجه‌گیری

اکثر سیستم‌های تشخیص نفوذ سلسله مراتبی بر اساس روند ذکرشده در بخش ۱ عمل می‌کنند. در این سیستم‌ها هر گره وظیفه پایش، ثبت وقایع، تحلیل، پاسخ‌دهی به نفوذهای تشخیص داده شده (در صورت وجود دلایل کافی) و هشدار یا گزارش‌دهی به سطوح بالاتر را دارد. ارسال گزارش نفوذهای احتمالی از سطوح پایین به سطوح بالاتر تا رسیدن به نرخ تشخیص قابل قبول ادامه می‌یابد. اگرچه ارسال گزارش به لایه‌های بالاتر منجر به تشخیص با دقت بیشتری می‌گردد، در مقابل سربار و هزینه تشخیص بیشتری نیز به همراه دارد. علاوه بر آن در شبکه‌هایی همچون شبکه خودروها، که بخشی از حملات مربوط به ایمنی خودرو و سرنشینان آن می‌شود تشخیص حمله و واکنش سیستم در مهلت زمانی مناسب ضروری است. در طرح ارائه شده در این مقاله ویژگیهای زیر مورد توجه قرار گرفته است:

- در ارسال گزارش به لایه‌های بالاتر علاوه بر دقت تشخیص، هزینه و سربار ناشی از آن نیز در نظر گرفته می‌شود. در واقع تعادلی بین دقت تشخیص بالاتر و هزینه تشخیص پایین‌تر ایجاد می‌شود.
- در پاسخگویی به حملات، حداکثر مهلت انجام واکنش مناسب محاسبه و در نظرگرفته می‌شود.
- رفتار مهاجم در دوره‌های زمانی مختلف پیش‌بینی و تحلیل می‌شود و استراتژی دفاعی مناسب در برابر آن اتخاذ می‌گردد.

ویژگی‌های مذکور وجه تمایز و نوآوری بکاررفته در طرح ارائه شده در مقایسه با کارهای مرتبط در این زمینه است.

مراجع

[1] R. Bace and P. Mell, *"NIST special publication on intrusion detection systems,"* SP800-31, NIST, Gaithersburg, MD, 2001.

[2] K. Scarfone and P. Mell, *"Guide to intrusion detection and prevention systems (idps),"* NIST Special Publication, vol. 800, p. 94, 2007.

[3]]Y. Xiao, X. Shen, and D. Z. Du, *"A Survey on Intrusion Detection in Mobile Ad Hoc Networks,"* in Wireless/Mobile Network Security: Springer US, 2006, pp. 170 - 196.

[4] T. V. Lakshman and M. Kodialam, *"Detecting network intrusions via sampling: a game theoretic approach,"* IEEE INFOCOM. San Francisco, California, USA, 2003.

[5] A. Patcha and J. M. Park, *"A game theoretic formulation for intrusion detection in mobile ad hoc networks,"* International Journal of Network Security, vol. 2, pp. 146-152, 2006.

[6] J. Cai and U. Pooch, *"Allocate fair payoff for cooperation in wireless ad hoc networks using shapley value,"* in Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'04), 2004.

[7] P. Nurmi, *"Modelling routing in wireless ad hoc networks with dynamic Bayesian games,"* in 1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks (IEEE SECON), 2004, pp. 63-70.

[8] V. Srinivasan, P. Nuggehalli, C. F .Chiasserini, and R. R. Rao, *"An analytical approach to the study of cooperation in wireless ad hoc networks,"* IEEE Transactions on Wireless Communications, vol. 4, pp. 722-733, 2005.

[9] A. Urpi, M. Bonuccelli, and S. Giordano, *"Modeling Cooperation in Mobile Ad Hoc Networks: a Formal Description of Selfishness,"* In Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2003.

[10] Y. Xiao, X. Shan, and Y. Ren, *"Game theory models for IEEE 802.11 DCF in wireless ad hoc networks,"* IEEE Radio Communications, March, vol. 43, pp. S22-S26, 2005.

[11] A. Agah, S. K. Das, K. Basu, and M. Asadi, *"Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach,"* in Proceedings of the Third IEEE International Symposium on Network Computing and Applications (NCA'04), 2004, pp. 343-346.

[12] T. Alpcan and T. Basar, *"A game theoretic approach to decision and analysis in network intrusion detection,"* in Proceeding of the 42nd IEEE Conference on Decision and Control (CDC), 2003.

[13] Y. Liu, H. Man ,and C. Comaniciu, *"A game theoretic approach to efficient mixed strategies for intrusion detection,"* in Proceeding of the 2006 IEEE International Conference on Communications (ICC 2006), 2006.

[14] Y. Liu, C. Comaniciu, and H. Man, *"A Bayesian game approach for intrusion detection in wireless ad hoc networks,"* in Proceedings of the GameNets06. ACM,, 2006.

[15] D. Fudenberg and J. Tirole. *"Game Theory,"*. The MIT Press, Cambridge, Massachusetts, 1991.