Journal of Electronical & Cyber Defence
Vol. 9, No. 4, 2022, Serial No. 36

The Improvement of the GMCR Model Based on Statistical Analysis of the Game' Graph (Case Study: Malwares and Countermeasures Actions Based on Detection-Independent and Deductive Evidence)

M. Abbasi[1], M. Ghayoori Sales[2*]

*Imam Hossein Comprehensive University, Tehran, Iran

(Received: 21/08/2021, Accepted: 25/09/2021)

ABSTRACT

The GMCR model is one of the approaches used for modeling and analyzing the real-world conflicts based on the game theory. In this model, as the number of players' options increases, the number of game states (problem state space) increases exponentially. As the number of feasible game states increases, so does the number of game equilibrium states. Extracting favorable equilibrium states and effective options is one of the requirements of applying the GMCR model in view of the widespread conflicts such as malware games and countermeasures. In this paper, based on the GMCR, a MAG architecture with four processing layers is presented. The MAG's architecture was evaluated and analyzed based on methods of detecting and analyzing detection-independent and deductive evidence of malware and countermeasures in the form of three related games. The evaluation results show that among the attacker options, the option of "fileless cyber-attacks" and among the defense options, the options of "network communication disconnection," "path exploration techniques" and "symbolic execution," at a rate of 100%, are the effective options of the actors. Reducing the game state space by using the game abstraction algorithm, scenario-based and repeated games, extracting effective actions and favorable equilibrium states of the players are some of the advantages of MAG architecture. The MAG architecture can be used in the cyber operations decision support systems and the tabletop cyber wargames to make the right decisions and respond appropriately .

Keywords: Graph Model, Conflict Analysis, Game Theory, MAG Architecture, Malware Analysis, Detection-Independent and deductive evidence, Effective Options

* Corresponding Author Email: ghayoori@ihu.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۴، زمستان ۱۴۰۰، ص ۱۲۳- ۹۹

علمی- پژوهشی

بهبود مدل گرافِ تحلیل مناقشه مبتنی بر تحلیل آماری گرافِ بازی
مطالعه موردی: اقدامات بدافزارها و مقابله‌کنندگان بر اساس شواهد غیرمحیطی و قیاسی

مصطفی عباسی[۱]، مجید غیوری ثالث[۲*]

۱- دانشجوی دکتری، ۲- استادیار، دانشگاه جامع امام حسین(ع)، تهران، ایران

(دریافت: ۱۴۰۰/۰۵/۳۰، پذیرش: ۱۴۰۰/۰۷/۰۳)

چکیده

یکی از رویکردهای مدل‌سازی و تحلیل مناقشه‌های دنیای واقعی مبتنی بر نظریه بازی، مدل گرافِ تحلیل مناقشه است در این مدل با افزایش تعداد گزینه‌های بازیگران، تعداد وضعیت‌های بازی به‌صورت نمایی افزایش یافته و با افزایش تعداد وضعیت‌های بازی، تعداد وضعیت‌های تعادلی نیز زیاد می‌شود. با توجه به گستردگی اقدامات بدافزارها و راهکارهای مقابله‌ای، استخراج گزینه‌های تاثیرگذار بازیگران و وضعیت‌های تعادلی مطلوب بازی، از نیازمندی‌های ضروری به‌کارگیری مدل گرافِ تحلیل مناقشه در حوزه تحلیل حملات بدافزاری است. در این مقاله مبتنی بر مدل گرافِ تحلیل مناقشه، معماری به‌نام مگ ارایه شده است. معماری مگ بر اساس روش‌های تشخیص و تحلیل شواهد غیرمحیطی و قیاسی بدافزارها و مقابله‌کنندگان در قالب سه بازی مرتبط، ارزیابی و تحلیل گردید. نتایج ارزیابی نشان داد از بین گزینه‌های مهاجم، گزینه حملات سایبری بدون فایل و از بین گزینه‌های مدافع، گزینه‌های قطع ارتباطات شبکه‌ای و تکنیک‌های اکتشاف مسیر و اجرای نمادین، با میزان مشارکت ۱۰۰ درصدی، گزینه‌های تاثیرگذار بازیگران هستند. کاهش فضای حالت بازی با استفاده از الگوریتم انتزاع‌سازی بازی، ارایه بازی‌های سناریو محور و تکرارپذیر، استخراج اقدامات موثر و وضعیت‌های تعادلی مطلوب بازیگران، از مزایای معماری مگ هست. از معماری مگ می‌توان در سامانه‌های بازی جنگ و تصمیم‌یار عملیات سایبری جهت تصمیم‌سازی صحیح و اتخاذ پاسخ مناسب استفاده کرد.

کلمات کلیدی: مدل گراف، تحلیل مناقشه، نظریه بازی، معماری مگ، تحلیل بدافزار، تشخیص غیرمحیطی و قیاسی، گزینه‌های تاثیرگذار

۱- مقدمه

با توجه به گسترش زیرساخت‌های سایبری نظامی و غیرنظامی و حملات بدافزاری به این زیرساخت‌ها، مدل‌سازی و تحلیل حملات و ارایه راهکارهای مقابله‌ای از ضروریات این حوزه است [۱- ۳]. بدافزارها برای شناسایی زیرساخت هدف و سامانه‌های دفاعی از تکنیک‌های متنوعی استفاده می‌نمایند؛ این تکنیک‌ها را می‌توان به دودسته کلی (۱) شناسایی محیط هدف بر اساس شواهد محیطی[۱] به‌صورت مستقیم[۲] (۲) روش‌های تشخیص و تحلیل شواهد غیر محیطی[۳] و قیاسی[۴] تقسیم کرد [۴] و این دسته‌بندی برای شناسایی رفتارهای بدافزارها توسط سامانه‌های دفاعی و مقابله‌کنندگان نیز قابل‌بیان هست [۷- ۵]. با توجه به رقابت همیشگی بین بدافزارها و سامانه‌های دفاعی [۱۰- ۸]، تعارض منافع بین بازیگران[۵] این حوزه وجود داشته است؛ به‌نحوی که تصمیم‌گیری یکی بر تصمیم دیگران اثرگذار هست. لذا مساله بدافزار و مقابله‌کنندگان را می‌توان با رویکردهای نظریه بازی مدل‌سازی و تحلیل کرد [۱۱]. مدل گراف تحلیل مناقشه (GMCR)[۶]، یکی از رویکردهای مدل‌سازی و تحلیل بازی‌ها است [۱۲]. در مدل گراف تحلیل مناقشه، فضای حالت مساله متاثر از گزینه‌های بازیگران[۷] و وضعیت‌های بازی[۸] است. تعداد وضعیت‌های بازی در مدل GMCR، دو به توان کل گزینه‌های بازیگران است و اعمال محدودیت‌هایی به بازی، وضعیت‌های غیرممکن بازی حذف و تعداد وضعیت‌های ممکن بازی[۹] کاهش می‌یابد. در بازی بدافزارها و مقابله‌کنندگان، با توجه به تنوع بازیگران و گزینه‌های آن‌ها، در صورتی که تعداد گزینه‌های بازیگران زیاد و شرایط محدودکننده بازی کم باشد، وضعیت‌های ممکن بازی و وضعیت‌های تعادلی بازی افزایش یافته و درنتیجه

*رایانامه نویسنده مسئول: ghayoori@ihu.ac.ir

[1] Detection-Dependent
[2] Direct Detection
[3] Detection-Independent
[4] Deductive Detection
[5] Conflict of Interest of the Players
[6] Graph Model for Conflict Resolution(GMCR)
[7] Players'Options
[8] Game States
[9] Feasible States

ناشر: دانشگاه جامع امام حسین (ع)

تفسیر نتایج بازی، مشکل خواهد بود. از چالش‌های دیگر بازی بدافزار و مقابله‌کنندگان، نبود شناخت کافی بازیگران نسبت به رقیب است؛ لذا باید راهکاری جهت مدل‌سازی شرایط عدم قطعیت مساله ارایه کرد تا متناسب مدل‌سازی و تحلیل بازی به‌صورت مرحله‌ای و سناریو محور، از افزایش شناخت بازیگران نسبت به شرایط بازی استفاده کرد؛ بنابراین هدف مقاله ارایه یک معماری جهت بهبود مدل گراف تحلیل مناقشه برای استفاده در بازی بدافزارها و مقابله‌کنندگان بوده تا بر اساس آن، گزینه‌های تاثیرگذار بازیگران و وضعیت‌های تعادلی مطلوب در بازی استخراج شود.

در بخش ۲ این مقاله، ادبیات موضوع و پیشینه تحقیق بیان شده و در آن کاربردهای گراف در حملات سایبری و کاربردهای نظریه بازی به‌خصوص مدل GMCR در حوزه‌های مختلف امنیتی و دفاعی عنوان گردیده است. در بخش ۳، معماری پیشنهادی توسعه مدل گراف تحلیل مناقشه و ارزش‌گذاری اقدامات بدافزارها و مقابله‌کنندگان و پارامترهای آن‌ها تشریح می‌گردد. در ادامه ارزیابی معماری ارایه شده بر اساس رفتارها و اقدامات غیر وابسته به محیط هدف بازیگران، در بخش ۴ بیان شده و در پایان نیز نتیجه‌گیری مقاله عنوان می‌شود.

۲- ادبیات موضوع و پیشینه تحقیق

با توجه به موضوع مقاله، در این بخش مروری بر ادبیات موضوع و کاربردهای گراف، مدل گراف تحلیل مناقشه در حملات سایبری و رویکردهای تحلیل و شناسایی بدافزار، ارایه می‌گردد.

۲-۱- گراف حمله و کاربردها

مفهوم گراف‌های حمله برای اولین بار توسط فیلیپس و سوییلر مطرح شد [۱۳]. هر گراف حمله مجموعه‌ای از سناریوهای نفوذ به یک شبکه کامپیوتری یا زیرساخت هدف را نمایش می‌دهد. در این گراف جهت‌دار، هر مسیر کامل از یک گره ابتدایی به یک گره هدف با یک سناریوی نفوذ مطابقت دارد [۱۴]. در زمینه به‌کارگیری مدل گراف در حملات سایبری تحقیقات متنوعی صورت گرفته [۱۵] و در حوزه شناسایی و تحلیل بدافزارها، نیز کاربردهایی داشته است [۱۶، ۱۷]. در تحقیق زنگ[1] و همکاران [۱۵] در سال ۲۰۱۹، روش‌های مختلف تولید و تحلیل گراف حمله با رویکردهای الگوریتم گراف[2]، شبکه بیزی[3]، مدل مارکوف[4] و الگوریتم‌های بهینه‌سازی هزینه[5]، بررسی شده و مزایا و معایب و پیچیدگی زمانی، روش‌های مختلف باهم مقایسه گردیده است. میشرا[6] و همکاران در سال ۲۰۱۸، چارچوب پشتیبان تصمیمی برای بررسی حملات سایبری با استفاده از مدل گراف ارایه نموده‌اند و بر اساس نظریه بازی کلاسیک، تعادل نش بازی مهاجم و مدافع جهت بهره‌برداری از آسیب‌پذیری را استخراج نموده‌اند [۱۸]. در مقاله مروری هوساک[7] و همکاران در سال ۲۰۱۸، دسته‌بندی جامعی از روش‌های پیش‌بینی و تجسم حملات در امنیت سایبری ارایه شده و مدل‌های مارکوف، شبکه‌های بیزین و گراف‌های حمله و بخشی از نظریه بازی را در دسته‌بندی مدل‌های گسسته رخداد[8] قرار داده است [۲]. در مقاله باکداش[9] و همکاران [۹] در سال ۲۰۱۸، با پیش‌بینی تشخیص تحلیلگر رخدادهای سایبری، با بهره‌گیری از مدل فضای حالت بیزین، وضعیت بدافزار در آینده را بررسی نموده است. در تحقیق دونیکووا[10] و همکاران [۱۹] در سال ۲۰۱۸، برای بهبود وظایف نظارت امنیت سایبری، افزایش مدل‌های حمله در قالب گراف‌های حمله را بررسی نموده و به کاربرد مدل‌های گراف حمله و راهکارهای مبتنی بر آن توجه ویژه‌ای شده است و ابزاری برای انتخاب راهکارهای دفاعی متناسب با حملات پیاده‌سازی گردیده است. در پژوهش آنجلینی[11] و همکاران [۲۰] در سال ۲۰۱۸، آشکارساز حملات چندمرحله‌ای برخط مبتنی بر مدل گراف حمله را ارایه نموده‌اند؛ موتور همبسته ساز برخط و موتور مصورسازِ پیشرفته حملات در زیرساخت هدف، از مولفه‌های اصلی این آشکارساز بوده و وجود مصالحه بین دقت تشخیص و زمان تشخیص از نتایج ارزیابی آن است.

۲-۲- روش‌های تشخیص و تحلیل شواهد غیرمحیطی[12] و قیاسی بدافزارها و مقابله‌کنندگان

در پژوهش‌های مختلفی، روش‌های شناسایی و تحلیل بدافزارهای به روش‌های ایستا، پویا و ترکیبی بررسی و دسته‌بندی شده‌اند [۲۳- ۲۱]. عموما بدافزارها از راهکارهایی جهت شناسایی و دورزدن سامانه‌های تحلیل و کشف بدافزارها استفاده می‌کنند. سامانه‌های دفاعی و امنیتی ضمن بهره‌گیری از روش‌های متنوع برای شناسایی بدافزارها، از راهکارهایی جهت مخفی سازی شواهد محیطی و غیر محیطی خود از بدافزارها، استفاده می‌کنند [۲۴، ۲۵].

روش‌های تشخیص و تحلیل شواهد غیر محیطی و قیاسی، روش‌هایی است که مستقیما به دنبال نشانه‌های بدافزارها یا

[1] Zeng
[2] Graph Algorithm
[3] Bayesian Network
[4] Markov Model
[5] Cost Optimization Algorithm
[6] Mishra
[7] Husák
[8] Discrete Models
[9] Bakdash
[10] Doynikova
[11] Angelini
[12] Detection-Independent

سامانه‌های دفاعی هدف نیست بلکه به‌صورت غیرمستقیم از آن نشانه‌ها برای تشخیص هدفمند، بهره‌گیری می‌نماید [۴]. بدافزارها با بهره‌گیری از تکنیک‌های خود اشکال‌زدایی، توقف پردازنده، مخفی‌سازی نخ‌ها و تکنیک‌های چند نخی، جریان کنترلی پردازه‌ها را دست‌کاری[1] نموده و پیامد آن مخفی‌سازی اقدامات بدافزارها و دور زدن سامانه‌های دفاعی و اشکال‌زدا است و راهکارهای مقابله‌ای تنظیم درگاه اشکال‌زدایی و نقطه شکست[2]، مسدودسازی و قلاب‌اندازی به توابع سیستمی[3] مرتبط در سطوح مختلف امنیتی سیستم‌عامل است [۳۰- ۲۶]. در برخی از موارد بدافزارها با قفل‌کردن سخت‌افزارهای ورود اطلاعات کاربر یا ساخت میزکارهای مختلف و مخفی، دستورات را به‌صورت پنهانی اجرا می‌نمایند و از رصد و قفل‌های اشکال‌زداها فرار[4] می‌کنند [۳۰- ۲۶] و راهکار مقابله‌ای، مسدودسازی و قلاب‌اندازی به توابع سیستمی مرتبط است. به تعویق انداختن فعالیت‌های اصلی بدافزارها با بهره‌گیری از روش‌های تاخیر[5] در اجرای کد هدف و پردازش زمان اجرای یک دستور مشخص و پردازش ساختمان داده‌های مرتبط با زمان اجرای برنامه در واحد پردازش مرکزی[6] با بهره‌گیری از توابع سیستمی، نمونه‌هایی از روش‌های شناسایی محیط‌های شبیه‌سازی شده و غیرواقعی هدف بدافزارها است [۳۶- ۳۱]؛ تغییر مدت زمان تحلیل و پردازش بدافزارها به‌صورت پویا، وصله کردن آسیب‌پذیری‌های سطح هسته جهت جلوگیری از دسترسی‌های غیرمجاز با مسدودسازی و قلاب‌اندازی به توابع سیستمی، از راهکارهای مقابله‌ای با این تکنیک‌های بدافزار است. از دیگر تکنیک‌های غیر وابسته به محیط، فعال‌سازی قابلیت‌های اصلی و مخرب بدافزار مبتنی بر محرک‌های محیطی[7] مثل فعال‌سازی در یک زمان مشخص، وارد نمودن یک کلیدواژه مشخص، ورودی یا ارتباط مشخص درون‌شبکه‌ای است. از راهکارهای مقابله‌ای با این تکنیک‌ها، بهره‌گیری از روش‌های کشف مسیر[8] و اجرای نمادین[9] برای تعیین شرایط و مسیر فعال‌سازی کدهای مخرب هست [۳۹- ۳۷]. بهره‌جویی از آسیب‌پذیری‌های سیستم هدف (مبتنی بر وب و سطوح سیستم[10]) [۲۹، ۳۰]، جهت تزریق مستقیم کد مخرب در حافظه و اجرای کدهای مخرب به‌صورت بدون فایل[11]، از تکنیک‌های بدافزارها جهت دور زدن سامانه‌های دفاعی و مقابله‌کنندگان است [۴۰، ۴۱]؛ وصله نمودن آسیب‌پذیری‌های مرتبط با آسیب‌پذیری سیستم هدف، استفاده از سیستم‌های تشخیص مبتنی بر ناهنجاری، قلاب‌اندازی به توابع سیستمی و بارگذاری فیلتر درایور از راهکارهای مقابله‌ای با حملات بدون فایل است.

۲-۳- مدل گراف تحلیل مناقشه و کاربردها:

بررسی و تحلیل، حملات سایبری به زیرساخت‌های سایبری [۱, ۸] و شبکه‌های کامپیوتری [۴۲] با استفاده از نظریه بازی در طول سال‌های مختلف، مورد توجه محققین و پژوهشگران بوده است. مدل گراف تحلیل مناقشه، یکی از رویکردهای نظریه بازی است؛ این مدل، یک متدولوژی مدل‌سازی و تحلیل مناقشه راهبردی مبتنی بر روش تحقیق توصیفی- تحلیلی، ارائه می‌کند. این مدل، به‌آسانی قابل‌استفاده بوده و منعطف است [۱۲, ۴۳]. این مدل هنر خود را در تحلیل مسائل پیچیده دنیای واقعی به‌خوبی نشان داده است. به‌منظور پیش‌بینی محتمل‌ترین نتایج مورد انتظار در مناقشه و منازعه قدرت‌های منطقه‌ای و بین‌المللی در سوریه [۴۴]، مسائل هسته‌ای ایران [۴۵]، چالش‌های اجتماعی تقسیم ارث [۴۶] و مدل‌سازی و تحلیل راهبردی مناقشه نویسندگان بدافزار و تحلیل‌گران سامانه‌های امنیتی [۱۱] استفاده شده است.

در سال ۲۰۰۵ کیلگور[12] و هایپل[13] [۱۲]، مراحل توسعه و تکمیل GMCR و قابلیت و نواقص نرم‌افزارهای تولیدشده برای آن را بررسی و ارایه نمودند؛ ارایه تعاریف و ساختارهای جدید در موضوعات عدم قطعیت در ترجیح گذاری، مدل گراف سلسله مراتبی، وضعیت‌های تعادلی محکم و تعریف پایداری‌های نوین از پیشنهادهای این پژوهش برای پژوهشگران بوده است. مدل GMCR، در طی سال‌های مختلف توسط پژوهشگران توسعه داده شده است. در سال ۲۰۱۵ کینسارا[14]، ابزار +GMCR را جهت برطرف کردن برخی از نواقص نرم‌افزار GMCRII ارایه کرد. کینسارا، رویکرد تعیین رتبه‌بندی ترجیحات بازیگران جهت دستیابی به وضعیت پایداری و تعادل هدف و مصورسازی گراف بازی را، به مدل گراف تحلیل مناقشه اضافه کرد[۴۷]. ترجیح‌گذاری فازی فاصله[15] در خصوص وضعیت‌های مناقشه را، بشر[16] و همکاران در سال ۲۰۱۸ ارایه نمودند [۴۸]. در

[1] Control Flow Manipulation
[2] Set Debug Port and Breakpoint
[3] Skip and Hooking API Function
[4] Lockout Evasion
[5] Stalling
[6] CPU RDTSC (Read Time Stamp Counter)
[7] Trigger-Based
[8] Path Exploration
[9] Symbolic execution
[10] Web-based and System-level exploits
[11] Fileless Attack(Advanced Volatile Threat)
[12] Kilgour
[13] Hipel
[14] Kinsara
[15] Interval Fuzzy Preferences
[16] Bashar

پژوهش‌های حی[1] و همکاران [۴۹]، [۵۰]، در سال‌های ۲۱۰۹ و ۲۰۲۰، مدل گراف سه سطحی و دوسطحی برای تحلیل مناقشه ارایه نمودند؛ در مدل ارایه شده، بازیگران، پایداری و ترجیحات بازیگران[2] در مدل پیشنهادی تعریف شده و آن را با موضوع چالش دولت‌ها با مساله تغییرات آب‌وهوا مدل‌سازی و ارزیابی نموده است. در پژوهش هوانگ[3] و همکاران [۵۱] در سال ۲۰۲۰، رویکرد جدیدی برای تولید راهکار[4] در صحنه نبرد، با استفاده از مدل گراف تحلیل مناقشه ارایه شده است. هایپل در سال ۲۰۲۰، بازتاب سه دهه توسعه مدل GMCR، مبانی نظری و کاربردهای آن را بررسی و ارایه نموده است [۵۲].

۲-۴- مدل پایه‌ای GMCR

بررسی مبانی نظری و کارهای پیشین مقاله نشان داد که از مدل GMCR در دفاع سایبری به‌صورت محدود استفاده شده است. در خصوص توسعه و بهبود مدل گراف نیز مجموعه پژوهش‌هایی صورت گرفته است اما پژوهشی در زمینه، توسعه مدل گراف مبتنی بر تحلیل آماری نتایج بازی به‌خصوص در حوزه تحلیل رفتارهای بدافزارها تا زمان نگارش مقاله، انجام نشده است. برخی از دلایل انتخاب مدل پایه‌ای GMCR برای تحلیل بازی بدافزارها و مقابله‌کنندگان، به شرح زیر است:

- ✓ وجود شرایط مدل‌سازی و شبیه‌سازی گسسته رخداد[5] در اقدامات و رفتارهای بازیگران
- ✓ توالی و وابستگی بین اقدامات و رفتارهای بازیگران در مراحل مختلف حمله و دفاع و منطبق بودن بر شرایط مدل گراف تحلیل مناقشه
- ✓ مطابقت مراحل و شرایط و تعامل بازیگران در بازی با ویژگی‌های رویکردهای وضعیت محور

با توجه به گستردگی رفتار بدافزارها و مقابله‌کنندگان، برای بهره‌برداری مناسب از مدل GMCR در تحلیل رفتار بدافزارها و مقابله‌کنندگان، نیاز است بهبودی در این مدل انجام گیرد. دلایل توسعه GMCR، برای بازی بدافزارها و مقابله‌کنندگان به شرح زیر بیان می‌شود:

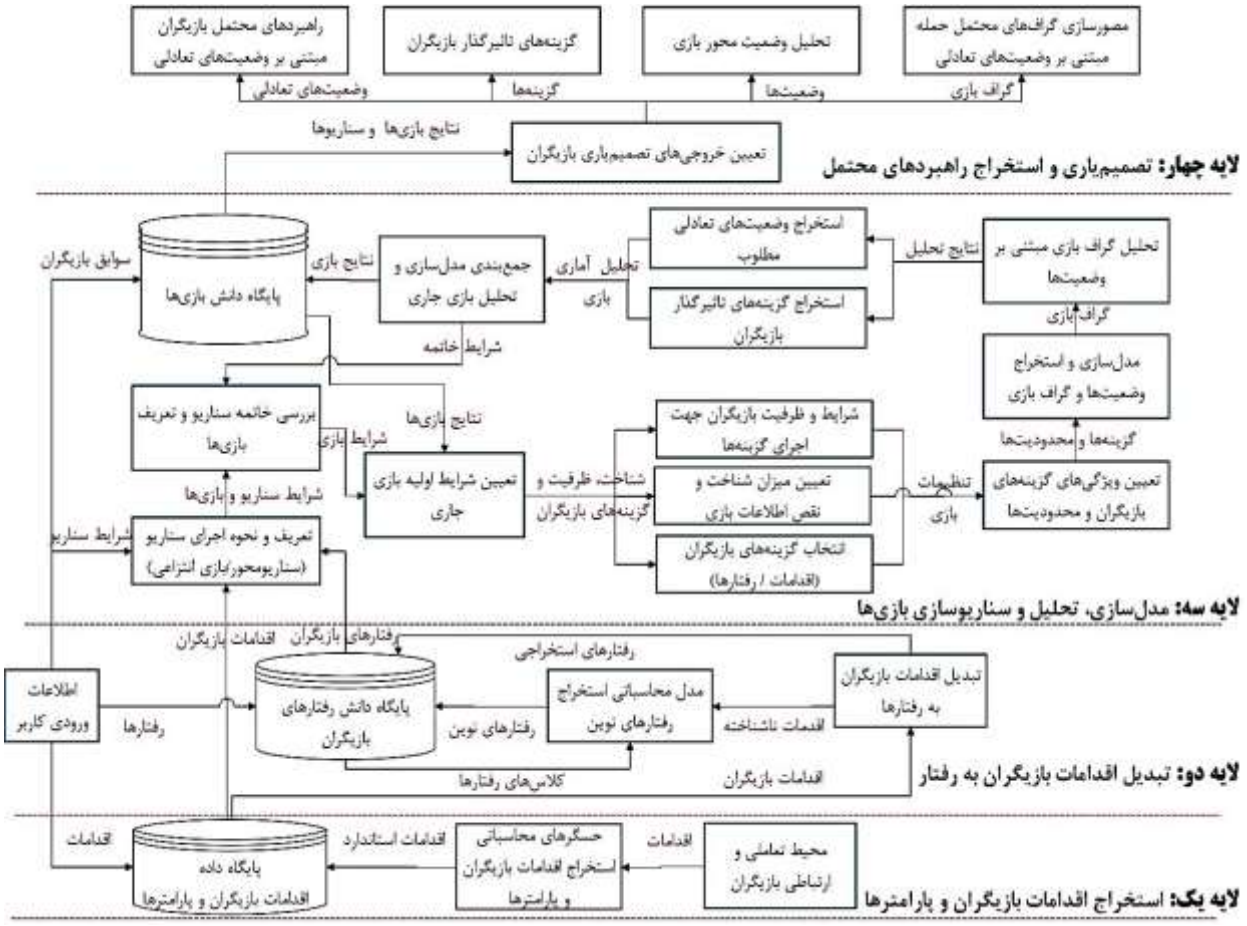
- ✓ گستردگی اقدامات و رفتارهای بازیگران و نیازمندی به انتزاع‌سازی اقدامات
- ✓ نداشتن شناخت و اطلاعات کامل بازیگران نسبت به یکدیگر و نحوه مدل‌سازی و پیاده‌سازی عدم قطعیت
- ✓ نحوه ارزش‌گذاری محاسباتی بازیگران نسبت به وضعیت‌های ممکن بازی با توجه به گستردگی وضعیت‌های ممکن بازی
- ✓ گستردگی وضعیت‌های تعادلی بازی بر اساس منطق‌های پایداری و استخراج وضعیت تعادلی مطلوب

بهبود صورت گرفته در این مقاله مبتنی بر تحلیل آماری نتایج بازی، شامل ۱) تعریف معیارهای استخراج گزینه‌های تاثیرگذار بازیگران و الگوریتم آن ۲) ارایه الگوریتم سناریوسازی بازی‌ها ۳) معرفی الگوریتم انتزاع‌سازی بازی‌ها است.

۳- معماری مگ[6] - بهبود مدل گراف تحلیل مناقشه مبتنی بر تحلیل آماری

با توجه به دلایل انتخاب و توسعه مدل GMCR برای تحلیل اقدامات و رفتارهای بازیگران که در بخش مبانی نظری عنوان شد، بهبود مدل گراف تحلیل مناقشه مبتنی بر تحلیل آماری در قالب یک معماری به‌نام مگ، مطابق با شکل (۱)، ارائه شده است؛ در معماری مگ، لایه‌ها، مولفه‌ها و ارتباطات بین آن‌ها ارایه شده است. مولفه‌های معماری مگ جهت ارزش‌گذاری گزینه‌ها بازیگران مبتنی بر پارامترهای تعریف‌شده، معیارهای استخراج وضعیت‌های تعادلی و گزینه‌های تاثیرگذار، الگوریتم مدل‌سازی و تحلیل بازی، الگوریتم سناریوسازی بازی‌ها و الگوریتم انتزاع‌سازی بازی‌ها، در قالب چهار لایه مجزا، تعریف و به‌کارگیری شده‌اند.

[1] He
[2] Plaayers' Preferences
[3] Huang
[4] Course of Action
[5] Discrete event modeling and simulation
[6] Malware Analysis GMCR(MAG)



شکل (۱): معماری مگ، لایه‌ها و مولفه‌ها

در معماری مگ، چهار لایه پردازشی شامل ۱) استخراج اقدامات بازیگران و پارامترها ۲) تبدیل اقدامات بازیگران به رفتارها ۳) مدل‌سازی، تحلیل بازی‌ها و سناریوسازی ۴) تصمیم‌سازی و استخراج راهبردها و رفتارهای محتمل بازیگران و وضعیت‌های تعادلی، وجود دارد. پایگاه داده اقدامات بازیگران و پارامترهای آن‌ها و پایگاه دانش بازیگران در معماری مگ، به‌صورت محاسباتی توسط حسگرها و مدل‌های محاسباتی استخراج اقدامات و رفتارها و پارامترها و ورود دستی اطلاعات توسط بهره‌بردار و کاربر، قابل تنظیم و به‌روزرسانی است. لایه مدل‌سازی و تحلیل بازی و سناریوسازی، متناسب با گزینه‌های استخراجی بازیگران و پارامترهای آن‌ها، بازی‌ها مدل‌سازی و تحلیل می‌گردند. با توجه به نقص اطلاعات بازیگران نسبت به وضعیت‌ها و ترجیحات یکدیگر و همچنین فرآیند انتزاع سازی اقدامات بازیگران و تولید رفتارها، در این لایه با رویکرد سناریو محور بازی‌های مختلف و وابسته به هم مدل‌سازی و تحلیل می‌گردد تا بر اساس نتایج آن‌ها، مناسب‌ترین و محتمل‌ترین گزینه‌ها و وضعیت‌های تعادلی بازیگران استخراج شود. در لایه تصمیم‌سازی و استخراج راهبردهای محتمل، متناسب با نتایج لایه سه، گزینه‌های تاثیرگذار، راهبردهای محتمل بازیگران، تحلیل وضعیت محور و گراف‌های وضعیت‌های بازی ارایه می‌گردد.

با توجه به اهمیت شرایط تعادلی در مدل‌های مبتنی بر نظریه بازی، موارد تصمیم‌یاری ارایه شده در لایه چهارم، مبتنی بر گزینه‌های تاثیرگذار و وضعیت‌های تعادلی مطلوب استخراجی بر اساس معیارهای تعریف‌شده (جدول (۳) و (۴) از پیوست مقاله) است.

بازیگران قابل تعریف در معماری مگ حداقل دو بازیگر بوده اما بازیگران در این مقاله به‌صورت مفروض، مهاجم و مدافع هستند؛ مهاجم بیان‌کننده رفتارهای بدافزارها و مدافع، نشان‌دهنده راهکارهای مقابله‌ای با رفتارهای بدافزارها است. در ادامه نحوه تعریف گزینه‌های بازیگران و توابع ارزش‌گذاری، معیارهای استخراج گزینه‌های تاثیرگذار و الگوریتم‌های انتزاع‌سازی و سناریوسازی مرتبط با معماری مگ تشریح می‌گردد.

۳-۱- گزینه‌های بازیگران و ارزش‌گذاری

در مدل *GMCR*، تعریف بازیگران، گزینه‌های بازیگران و ترجیحات بازیگران نسبت به وضعیت‌های بازی از مولفه‌های اصلی بازی است. گزینه‌های بازیگران و ترجیحات آن‌ها به‌صورت داده‌های ورودی دستی یا محاسباتی قابل تعریف است. در این مقاله گزینه‌های بازیگران و وابستگی و ارتباط گزینه‌ها به‌صورت دستی تهیه و تنظیم می‌گردد. پارامترهای گزینه‌های بازیگران و مقادیر آن‌ها، متناسب با ویژگی‌های گزینه‌ها، تعیین می‌شود. در این مقاله، پارامترها را به دودسته کلی پارامترهای وابسته به گزینه‌ها و وابسته به بهره‌بردار گزینه‌ها، تقسیم می‌شوند. مقادیر پارامترهای گزینه‌های بازیگران به‌صورت توصیفی و عددی قابل‌تعریف هستند؛ مقادیر توصیفی و عددی پارامترها، متناسب با سطوح امنیتی عنوان‌شده در جدول (۱) بیان می‌گردند. مقادیر جدول (۱)، بر اساس سطوح امنیتی سیستم‌عامل و معماری پردازنده [۵۳]، [۵۴] و دسته‌بندی اقدامات بدافزارها و سامانه‌های تحلیل بدافزارها و مقایسه آن‌ها [۴]، [۲۵]، [۵۵]، [۵۶]، استخراج شده است. بازه مقادیر عددی و کمی پارامترها با الگوبرداری از بازه تقسیم‌بندی طیف لیکرت[1] و سیستم امتیازدهی آسیب‌پذیری‌ها مشترک[2] [۵۷]، [۵۸] طیف اعداد ۰ تا ۱۰، تعیین شده است.

جدول (۱): سطوح امنیتی مرتبط با گزینه‌های بازیگران حوزه بدافزار

ردیف	عنوان سطح امنیتی	طیف مقادیر
۱	سطح کاربری سیستم‌عامل[3]	۲-۰
۲	سطح هسته سیستم‌عامل[4]	۴-۲
۳	سطح مجازی‌سازی و تقلید[5]	۶-۴
۴	سطح فلز لخت[6]	۸-۶
۵	سطح ثابت‌افزار و سخت‌افزار[7]	۱۰-۸

در پژوهش افیانیان و همکاران [۴]، پارامترهای پیچیدگی[8]، تاب‌آوری[9]، سطح اثربخشی[10] و فراوانی[11] به‌عنوان پارامترهای اقدامات بدافزارها به‌صورت کیفی معرفی و تشریح شده است. در این پژوهش، علاوه بر کمی و کیفی‌سازی پارامترهای ارایه شده در پژوهش افیانیان و توسعه آن‌ها، دسته‌بندی جدیدی از پارامترهای مقابله‌کنندگان بدافزارها با رویکرد شواهد غیر محیطی و تحلیل و تشخیص قیاسی، نیز ارایه شده است. پارامترهای پیچیدگی، تاب‌آوری، سطح اثربخشی، فراوانی وابسته به گزینه‌های بازیگران و پارامتر قابلیت بهره‌برداری وابسته به بهره‌بردار است. پارامترهای گزینه‌های بازیگران در سطح بالاتر با رویکرد انتزاع‌سازی گزینه‌ها[12]، بر اساس پارامترهای سطح پایین‌تر گزینه‌های بازیگران تعیین می‌شود.

منظور از پیچیدگی پیاده‌سازی، تعداد خط کدهایی موردنیاز برای پیاده‌سازی، اجرا و پردازش نتایج گزینه مدنظر و سطح پیاده‌سازی کدها متناسب با لایه‌بندی امنیتی سیستم‌عامل است. این سطح امنیتی از کد نویسی و پیاده‌سازی در سطح کاربری سیستم‌عامل تا سطح ثابت‌افزار، قابل تقسیم‌بندی و مقداردهی است. یکی دیگر از ویژگی‌های این پارامتر، دسترس بودن دانش و فناوری پیاده‌سازی گزینه موردنظر است که متناسب با آن مقدار کمی پیچیدگی پیاده‌سازی تغییر می‌کند.

پارامتر تاب‌آوری، میزان سختی مقابله با گزینه بازیگر توسط رقیب را نمایش می‌دهد؛ هرچه راهکارهای مقابله‌ای رقیب از سمت ثابت‌افزار به سمت سطح کاربری سیستم‌عامل تمایل بیشتری داشته باشد میزان تاب‌آوری گزینه موردنظر و ارزش آن، کمتر و راهکارهای دور زدن آن بیشتر است. این تاب‌آوری متناسب با سطوح امنیتی سیستم‌عامل و سطح پیچیدگی پیاده‌سازی متفاوت است.

پارامتر سطح اثربخشی، میزان اثربخشی گزینه بازیگر بر راهکارهای مقابله‌ای رقیب را بر اساس سطوح امنیتی سیستم‌عامل، نشان می‌دهد. هرچه سطح اثرگذاری گزینه بازیگر به سطح ثابت‌افزار و سخت‌افزار نزدیک‌تر باشد میزان اثربخشی و ارزش آن بیشتر و راهکارهای مقابله‌ای با آن سخت‌تر است.

پارامتر فراوانی به‌کارگیری، میزان فراوانی استفاده از گزینه بازیگر بر اساس تاریخچه و سوابق را، نشان می‌دهد. مقادیر این پارامتر بر اساس منابع مرتبط و نظر خبرگان مقداردهی شده است. تمایل این پارامتر به سمت یک، نشان‌دهنده عمومی‌تر بودن و تمایل به سمت ده، نشانه جدید و ناشناخته بودن گزینه بازیگر را بیان می‌کند.

[1] Likert spectrum
[2] Common Vulnerability Scoring System(CVSS)
[3] User-mode
[4] Kernel-mode
[5] Virtualization and emulation
[6] Bare-metal
[7] Framware and Hardware
[8] Complexity
[9] Resistance
[10] Efficacy-Level
[11] Pervasiveness
[12] Abstraction of Options

پارامتر قابلیت بهره‌برداری، میزان توانمندی‌های بازیگران برای بهره‌برداری از گزینه مدنظر را بیان می‌دارد. هرچه منابع مالی، نیروی انسانی متخصص، سامانه‌های نرم‌افزاری پایه بومی، تجهیزات زیرساختی بومی و دسترسی به دانش و فناوری بازیگران مناسب‌تر باشد قابلیت بهره‌برداری از گزینه بیشتر بوده و مقدار این پارامتر به سمت عدد ده میل می‌کند. ضریب پارامتر، میزان اهمیت آن پارامتر را نسبت به سایر پارامترهای گزینه‌ها، بیان می‌کند؛ جهت ساده‌سازی و به‌صورت مفروض در این مقاله، مقدار ضریب پارامترها ثابت و یک در نظر گرفته شده است. ظرفیت و توانمندی اجرای گزینه توسط بازیگر، بر اساس شرایط بازیگر (شامل منابع مالی، نیروی انسانی متخصص، سامانه‌های نرم‌افزاری پایه بومی، تجهیزات زیرساختی بومی و دسترسی به دانش و فناوری) و پارامترهای مرتبط با گزینه آن (شامل پیچیدگی پیاده‌سازی، تاب‌آوری، سطح اثربخشی و فراوانی به‌کارگیری) طبق رابطه (۱) محاسبه می‌گردد. مقدار کمی و کیفی هر یک از شرایط بازیگران شامل یکی از موارد: ۵-خیلی خوب ۴- خوب ۳-متوسط ۲ – ضعیف ۱- خیلی ضعیف است.

$$Ex_k^p = \left(\sum_{i=1..I, j=1..J, k=1..K} x_{ki} * S_{ki}^p + y_{kj} * P_{kj}^p \right) \Big/ 60 \qquad (۱)$$

در رابطه (۱)، Ex_k^p نشان‌دهنده، توانمندی بهره‌برداری بازیگر p (مهاجم یا مدافع) از گزینه k است. x_{ki} ضریب ثابت شرایط بازیگر و S_{ki}^p مقدار شرایط i ام بازیگر p در گزینه k است؛ y_{kj} ضریب ثابت پارامترهای گزینه بازیگر و P_{kj}^p مقدار پارامتر j ام بازیگر p در گزینه k است. ضریب ثابت شرایط بازیگر شامل منابع مالی، نیروی انسانی متخصص، سامانه‌های نرم‌افزاری پایه بومی، تجهیزات زیرساختی بومی و دسترسی به دانش و فناوری به ترتیب ۱,۲۵، ۱,۲۵، ۰,۷۵، ۰,۷۵ و ۱ و ضریب ثابت پارامترهای گزینه بازیگر شامل پیچیدگی پیاده‌سازی، تاب‌آوری، سطح اثربخشی و فراوانی به‌کارگیری به ترتیب ۳، ۳، ۳ و ۱، بر اساس تحقیق و پژوهش و خبره سنجی با مدل AHP تعیین شده است. علت تقسیم نتایج بر ۶۰، نرمال‌سازی جواب به عدد ۱۰ یعنی حداکثر مقدار پارامترهای گزینه بازیگر است.

توابع $F_{At}^A(i)$ و $F_{Df}^A(i)$، مقدار ارزش یک اقدام برای بازیگران را، بر اساس میانگین حسابی پارامترهای آن، طبق رابطه (۲)، محاسبه می‌نمایند. A_{At} و A_{Df} به ترتیب بیانگر مجموعه اقدامات مهاجم و مدافع است؛ به‌نحوی‌که مجموعه اقدامات مهاجم و مدافع باهم اشتراکی نداشته و اجتماع آن‌ها مجموعه اقدامات بازیگران را تشکیل می‌دهند.

$$F_{At}^A(i) = \frac{\sum_{j=1}^N V_{At}^A(i,j) \ * \ W_{At}^A(i,j)}{\sum_{j=1}^N W_{At}^A(i,\ j)}$$
$$F_{Df}^A(i) = \frac{\sum_{j=1}^N V_{Df}^A(i,j) \ * \ W_{Df}^A(i,j)}{\sum_{j=1}^N W_{Df}^A(i,j)} \qquad (۲)$$

در رابطه (۲)، $W_{At}^A(i,j)$ و $V_{At}^A(i,j)$ اعضاء پارامترهای مجموعه اقدامات مهاجم (A_{At}) و $W_{Df}^A(i,j)$ و $V_{Df}^A(i,j)$ اعضاء پارامترهای مجموعه اقدامات مدافع (A_{Df}) است. مقدار عایدی یک اقدام برای مهاجم و مدافع به ترتیب بر اساس توابع $U_{At}^A(i)$ و $U_{Df}^A(i)$ مطابق با رابطه (۳)، محاسبه می‌گردد.

$$U_{At}^A(i) = F_{At}^A(i) - \sum_{j=1}^{N} F_{Df}^A(j)$$
$$U_{Df}^A(i) = F_{Df}^A(i) - \sum_{j=1}^{N} F_{At}^A(j) \qquad (۳)$$

مطابق رابطه (۳)، عایدی بازیگر برای یک اقدام مشخص، از کسر مقادیر ارزش راهکارهای مقابله‌ای رقیب از ارزش اقدام بازیگر محاسبه می‌گردد؛ لذا هرچه ارزش راهکارهای مقابله‌ای رقیب در برابر اقدام بازیگر کمتر یا رقیب شناخت کمتری نسبت به اقدام بازیگر، داشته باشد، ارزش بهره‌برداری از آن اقدام در وضعیت‌های مختلف بازی بیشتر خواهد بود. در مدل‌سازی و تحلیل بازی مبتنی بر *GMCR*، ترجیح‌گذاری وضعیت‌های ممکن بازی، با مرتب‌سازی ترتیبی وضعیت‌ها مبتنی بر ارزش آن‌ها، صورت می‌گیرید؛ لذا منفی‌شدن ارزش برخی از اقدامات و وضعیت‌ها، مشکلی در مدل‌سازی و تحلیل بازی به وجود نمی‌آورد.

مجموعه رفتارهای بازیگران نیز با مجموعه اقدامات بازیگران ارتباط دارند و پارامترهای مرتبط با رفتارها بر اساس پارامترهای اقدامات منتسب به رفتارها، محاسبه می‌گردد. روابط حاکم بر محاسبات مقدار ارزش رفتارها، شبیه به محاسبات اقدامات است.

$$V_{At}^B(i,j), W_{At}^B(i,j) \epsilon B_{At}$$
$$V_{At}^A(m,n), W_{At}^A(m,n) \in A_{At}$$
$$V_{At}^B(i,j) = \frac{\sum_{m \epsilon M, n \in N} V_{At}^A(m,n) * W_{At}^A(m,n)}{\sum_{m \epsilon M, n \in N} W_{At}^A(m,n)}$$
$$W_{At}^B(i,j) = \frac{\sum_{m \epsilon M, n \in N} W_{At}^A(m,n)}{sizeof\left(W_{At}^A(m,n)\right)} \qquad (۴)$$

در رابطه (۴) نحوه استخراج پارامترهای رفتارهای مهاجم بر اساس اقدامات مهاجم ارایه شده است. در این رابطه، B_{At} مجموعه رفتارهای مهاجم و $W_{At}^B(i,j)$ و $V_{At}^B(i,j)$ به ترتیب بیان‌کننده وزن و مقدار پارامتر i ام رفتار j ام مهاجم و $sizeof()$ تعداد

عناصر یک مجموعه را محاسبه می‌کند. در رابطه (۴)، m شماره اقدام مرتبط با رفتار و n شماره پارامتر همان اقدام هست. نحوه محاسبه پارامترهای رفتارهای مدافع، شبیه به رابطه (۴) مربوطه به مهاجم است. رابطه (۵)، نحوه محاسبه پاداش مدافع (تابع $P_{Df}^{B}(k)$) در وضعیت k (از وضعیت‌های ممکن بازی) را بر اساس رفتارهای بازیگران، در این وضعیت نشان می‌دهد. y_i^K و x_j^k به ترتیب نشان‌دهنده استفاده مهاجم و مدافع از رفتارهای خود در وضعیت k بوده و در صورت استفاده از رفتار، مقدار یک و در غیر این صورت با صفر مقداردهی می‌گردد. در این رابطه مقدار ارزش رفتارهای مهاجم از مدافع کسر و بر میانگین هارمونیک[1] تعداد رفتارهای بازیگران تقسیم می‌گردد. با توجه رابطه بین رفتارهای مهاجم و مدافع در وضعیت مذکور(k)، مقدار تابع پاداش مدافع با قرینه پاداش مهاجم برابر است. در صورتی که مدافع از وضعیت k_1 به وضعیت k_2 تغییر وضعیت دهد، مقدار ارزش جابجایی آن از طریق $P_{Df}^{B}(k_1,k_2)$ محاسبه می‌گردد که این مقدار از تفریق پاداش دو وضعیت برای بازیگر به دست می‌آید. در رابطه (۵)، m و n به ترتیب تعداد رفتار مهاجم و مدافع است؛ نحوه محاسبه عایدی مهاجم در یک وضعیت مشخص، شبیه به مدافع هست(رابطه(۵)).

$$P_{Df}^{B}(k) = \frac{(\Sigma_{i=1}^{m} y_i^K * F_{Df}^{B}(i)/\Sigma_{j=1}^{m} y_j^k) - (\Sigma_{j=1}^{n} x_j^k * F_{At}^{B}(j)/\Sigma_{i=1}^{n} x_i^k)}{\frac{2*\Sigma_{i=1}^{n} x_i^k * \Sigma_{j=1}^{m} y_j^k}{\Sigma_{i=1}^{n} x_i^k + \Sigma_{j=1}^{m} y_j^k}}$$
$$P_{Df}^{B}(k) = -P_{At}^{B}(k) \qquad (۵)$$
$$P_{Df}^{B}(k_1,k_2) = P_{Df}^{B}(k_2) - P_{Df}^{B}(k_1)$$

تعریف پارامترهای گزینه‌های بازیگران و نحوه ارزش‌گذاری آن‌ها، متناسب با شرایط حوزه بدافزار بوده اما می‌توان این روابط، دسته‌بندی و طیف مقادیر پارامترهای گزینه‌ها را در سایر حوزه‌ها، متناسب با شرایط بازی و توسط بهره‌بردار، سفارشی کرد.

۳-۲- معیارهای استخراج وضعیت‌های تعادلی مطلوب بازی و گزینه‌های تاثیرگذار بازیگران

استخراج وضعیت تعادلی مطلوب بازی از بین وضعیت‌های متنوع و گسترده تعادلی، یکی از چالش و نیازهای معماری مگ است. یکی از راهکارهای انتخاب مناسب‌ترین وضعیت‌های تعادلی، انتخاب وضعیت‌هایی است که گزینه‌های تاثیرگذار بیشتری در آن نقش داشته باشند. برای استخراج گزینه‌های تاثیرگذار، نیاز به معیارهای استخراج گزینه‌های تاثیرگذار بازی است. در جدول (۲)، معیارهای ارزیابی و انتخاب گزینه‌های تاثیرگذار بازیگران در بازی به‌صورت معیارهای اصلی و فرعی ارایه شده و مقادیر این معیارها بر اساس روابط ارایه شده در جدول‌های (۳) و (۴) از پیوست مقاله، محاسبه و ارایه می‌گردد.

پس از محاسبه مقادیر هرکدام از ۵۰ معیار تعریف‌شده، بر اساس روابط حاکم بر آن‌ها، در هر معیار، حداکثر مقدار معیار گزینه‌ها در آن معیار استخراج می‌گردد. هدف از انتخاب حداکثر مقدار معیار، انتخاب گزینه‌های تاثیرگذار در آن معیار هست. جهت افزایش دقت انتخاب گزینه‌ها و جلوگیری از حذف گزینه‌های نزدیک به حداکثر مقدار در هر معیار، گزینه‌هایی که مقادیر آن‌ها بیشتر از ۹۵٪ حداکثر مقدار آن معیار باشد نیز به‌عنوان گزینه برتر انتخاب می‌گردند. حد آستانه ۹۵٪، بر اساس نتایج مدل‌سازی و شبیه‌سازی مختلف، به‌عنوان حد آستانه مناسب تعیین شده و با این حد آستانه درصد قابل قبولی از گزینه‌های بازیگران به‌عنوان گزینه‌های تأثیرگذار انتخاب می‌شوند و بر مبنای آن‌ها، تعداد مناسبی وضعیت‌های تعادلی مطلوب استخراج می‌شود. درصورتی‌که حد آستانه صددرصدی (حداکثر مقدار معیار) مدنظر باشد؛ برای هر بازیگر در هر معیار فقط یک گزینه به‌عنوان گزینه تاثیرگذار لحاظ می‌گردد و سایر گزینه‌های مشابه به گزینه تاثیرگذار حذف می‌شوند. اگر حد آستانه کمتر در نظر گرفته شود و ویژگی‌های پارامتری و شناخت بازیگران از گزینه‌ها شبیه به هم باشند؛ گزینه‌های تاثیرگذار زیاد شده واگرایی نتایج به وجود آمده و گزینه‌های تاثیرگذار واقعی به‌صورت مناسب استخراج نمی‌شود.

در جدول (۲)، معیار ۱ و ۲، نشان‌دهنده ارزش هرکدام از گزینه‌های بازیگران بر اساس پارامترهای آن و گزینه‌های مقابله رقیب است (رابطه (۳)). معیارهای ۳ تا ۶ نشان‌دهنده تعداد و شرایط الگوهای حذف وضعیت‌های غیرممکن بازی مرتبط با گزینه‌های بازیگران با شرط الزام بودن گزینه در الگوهای حذف وضعیت‌های غیرممکن است. معیار ۳ نشان‌دهنده تعداد الگوهای شامل گزینه بازیگران به تفکیک گزینه‌ها و معیار ۴ و ۵ به ترتیب بیان‌کننده نسبت مقدار معیارهای ۳ گزینه‌های بازیگران به تعداد الگوهای حذف مرتبط با بازیگر و کل بازیگران بازی است؛ معیار ۶ از میانگین معیار ۴ و ۵ به تفکیک گزینه‌های بازیگران محاسبه می‌گردد.

[1] Harmonic Mean

جدول (۲): معیارهای اصلی و فرعی تحلیل آماری نتایج بازی

ردیف	عنوان معیارهای اصلی	شماره معیارهای فرعی	معیار موثر
۱	ارزش گزینه‌های بازیگران (کیفیت ارزش)	۱ تا ۲	۲
۲	الزام بودن گزینه در الگوهای حذف وضعیت‌های غیرممکن (کیفیت الزام استفاده)	۳ تا ۶	۶
۳	الزام نبودن گزینه در الگوهای حذف وضعیت‌های غیرممکن (کیفیت الزام عدم استفاده)	۷ تا ۱۰	۱۰
۴	شناخت بازیگران از گزینه‌ها (کیفیت شناخت)	۱۱	۱۱
۵	مشارکت گزینه‌های بازیگران در وضعیت‌های بازی (کیفیت مشارکت)	۱۲ تا ۱۳	۱۳
۶	وضعیت‌های با عایدی کمتر نسبت به رقیب (کیفیت شکست)	۱۴ تا ۱۷	۱۷
۷	وضعیت‌های با عایدی برابر با رقیب (کیفیت برابری)	۱۸ تا ۲۱	۲۱
۸	وضعیت‌های با عایدی بیشتر نسبت به رقیب (کیفیت برتری)	۲۲ تا ۲۵	۲۵
۹	وضعیت پایداری بازیگر (کیفیت پایداری)	۲۶ تا ۲۹	۲۹
۱۰	وضعیت تعادل *Nash* (کیفیت تعادل *Nash*)	۳۰ تا ۳۳	۳۳
۱۱	وضعیت تعادل *SEQ* (کیفیت تعادل *SEQ*)	۳۴ تا ۳۷	۳۷
۱۲	وضعیت تعادل *GMR* (کیفیت تعادل *GMR*)	۳۸ تا ۴۱	۴۱
۱۳	وضعیت تعادل *SMR* (کیفیت تعادل *SMR*)	۴۲ تا ۴۵	۴۵
۱۴	میانگین وضعیت‌های تعادلی (*Nash, SEQ, GMR, SMR*) (کیفیت تعادل‌های پایه)	۴۶ تا ۴۸	۴۸
۱۵	تعادل مطلوب *BestEQ* (کیفیت تعادل مطلوب)	۴۹ تا ۵۰	۵۰

معیارهای ۷ تا ۱۰ نشان‌دهنده تعداد و شرایط الگوهای حذف وضعیت‌های غیرممکن بازی مرتبط با گزینه‌های بازیگران با شرط الزام نبودن گزینه در الگوهای حذف وضعیت‌های غیرممکن است و تفسیر معیارهای فرعی آن شبیه معیارهای فرعی ۳ تا ۶ است.

معیار شماره ۱۱ نشان‌دهنده، کیفیت شناخت گزینه بازیگر و بهره‌گیری و تاثیر آن در بازی است و بر اساس میانگین معیارهای ۶ و ۱۰ محاسبه می‌شود. معیار ۱۲ تا ۱۳ کیفیت مشارکت گزینه‌های بازیگران در بازی را ارزیابی می‌کند و نشان‌دهنده وضعیت‌های ممکنی از بازی است که در آن وضعیت‌ها از گزینه‌های بازیگران استفاده شده است؛ معیار ۱۲ نشان‌دهنده تعداد وضعیت‌های شامل گزینه بازیگر و معیار ۱۳ بیان‌کننده نسبت مقدار معیار ۱۲ به‌کل وضعیت‌های بازی است.

معیارهای فرعی ۱۴ تا ۲۵، شرایط عایدی بازیگران در وضعیت‌های مختلف بازی را در قالب سه دسته معیار اصلی با عایدی کمتر، عایدی برابر و عایدی بیشتر نسبت به رقیب بررسی می‌کنند؛ معیارهای ۱۴، ۱۸ و ۲۲، به ترتیب تعداد وضعیت‌های با عایدی کمتر، برابر و بیشتر نسبت به رقیب را به تفکیک گزینه‌های بازیگران محاسبه می‌کند. معیارهای ۱۵، ۱۹ و ۲۳، به ترتیب نسبت معیارهای ۱۴، ۱۸ و ۲۲ به مشارکت گزینه‌های بازیگران را بیان می‌کند. معیارهای ۱۶، ۲۰ و ۲۴، به ترتیب نسبت معیار ۱۴ به‌کل گزینه‌های با عایدی کمتر، معیار ۱۸ به‌کل گزینه‌های با عایدی برابر و معیار ۲۲ به‌کل گزینه‌های با عایدی بیشتر به تفکیک گزینه‌ها را بیان می‌کند. معیار ۱۷ بر اساس میانگین معیارهای ۱۵ و ۱۶، معیار ۲۱ بر اساس میانگین ۱۹ و ۲۰ و معیار ۲۵ بر اساس میانگین معیار ۲۴ و ۲۳ محاسبه می‌شود. معیارهای ۲۶ تا ۴۵ در قالب چهار دسته معیارهای اصلی، وضعیت پایداری، وضعیت‌های تعادلی بازیگران منطبق بر منطق‌های *Nash*، *SEQ*، *GMR* و *SMR* را بررسی می‌کند. هر دسته از این معیارهای اصلی، چهار معیار فرعی دارد: ۱) معیار فرعی اول- تعداد وضعیت‌های گزینه‌های بازیگران بر اساس پایداری یا منطق‌های تعادلی ۲) معیار فرعی دوم - نسبت معیار فرعی اول به معیار ۱۲ گزینه بازیگر ۳) معیار فرعی سوم - نسبت معیار فرعی اول به تعداد کل وضعیت‌های پایداری یا منطق‌های تعادلی ۴) معیار فرعی چهارم - میانگین معیارهای فرعی سوم و چهارم.

معیار ۴۶ نشان‌دهنده میانگین حسابی معیارهای ۱۳، ۳۵، ۳۹ و ۴۳ مربوطه به وضعیت‌های تعادلی (*Nash*، *SEQ*، *GMR* و *SMR*) است. معیارهای ۴۷ و ۴۸ نیز شبیه به معیار ۴۶، محاسبه می‌شوند.

وضعیت‌هایی از بازی که تعادل *GMR* و *SMR* بوده و در آن وضعیت‌ها از گزینه‌های تاثیرگذار بازیگران استفاده شده باشد به‌عنوان وضعیت‌های تعادلی مطلوب (*BestEQ*) معرفی می‌شوند. معیار ۴۹ تعداد مشارکت گزینه‌های بازیگران در وضعیت تعادلی مطلوب را محاسبه می‌نماید. معیار ۵۰ نسبت مشارکت گزینه‌های بازیگران در وضعیت‌های تعادلی مطلوب را نسبت به سایر گزینه‌ها

نشان می‌دهد. گزینه‌های تاثیرگذاری که بیشترین مشارکت در وضعیت‌های تعادلی مطلوب را داشته به‌عنوان گزینه‌های تاثیرگذار نهایی معرفی می‌گردند (معیار ۵۰). در جدول (۲)، از بین ۵۰ معیار عنوان‌شده، معیارهای موثرتر و استخراج‌کننده گزینه‌های تاثیرگذار بازیگران بازی، در ستون معیار موثر جدول مذکور، ارایه شده است. هدف از ارایه و بررسی معیارهای عنوان‌شده، بررسی رابطه بین وضعیت‌های تعادلی مطلوب و گزینه‌های تاثیرگذار بازی با شرایط و کیفیت معیارهای اصلی گزینه‌های بازیگران است.

یکی از خروجی‌های مهم تحلیل یک مناقشه مبتنی بر مدل *GMCR*، گراف بازی شامل وضعیت‌های ممکن (نودهای گراف) و ماتریس ارتباطی وضعیت‌ها (یال‌های گراف) است. محاسبات پایه‌ای مدل *GMCR* شامل گراف بازی، منطق‌های پایداری و وضعیت‌های تعادلی در پژوهش‌ها و مقالات پایه‌ای آن به‌صورت ریاضی اثبات شده است ([۱۲], [۴۷], [۵۲]). هدف از معیارهای اصلی ارایه شده در این مقاله (شامل بررسی ارزش گزینه‌های بازیگران، میزان شناخت بازیگران از گزینه‌های رقیب، میزان مشارکت گزینه‌های بازیگران در وضعیت‌های ممکن بازی، شرایط عایدی بازیگران از گزینه‌ها و بررسی وضعیت‌های تعادلی مختلف)، استخراج گزینه‌های تاثیرگذار و وضعیت‌های تعادلی مطلوب بازی است. کاربرد و شرح معیارها، به‌صورت توصیفی، رسمی و روابط ریاضی در این بخش مقاله و جدول‌های ۳ و ۴ پیوست مقاله به‌طور کامل شرح داده شده است.

۳-۳- الگوریتم استخراج وضعیت‌های تعادلی بازی و گزینه‌های تاثیرگذار بازیگران

مطابق الگوریتم (۱)، وضعیت‌های تعادلی مطلوب و گزینه‌های تاثیرگذار بازیگران در بازی، در ۵ مرحله، بررسی و استخراج می‌گردد.

مراحل الگوریتم (۱) شامل ۱) استخراج وضعیت‌های ممکن بازی ۲) استخراج بردار ترجیحات بازیگران نسبت به وضعیت‌های بازی و حرکت و بهبودهای یک‌جانبه بازیگران ۳) بررسی پایداری انفرادی بازیگران و وضعیت‌های تعادلی و تحلیل آماری آن‌ها ۴) استخراج ۵۰ معیارهای اثرگذار بازی با تحلیل گراف بازی ۵) استخراج وضعیت‌های تعادلی مطلوب و گزینه‌های تاثیرگذار نهایی بازیگران است. ورودی‌های الگوریتم (۱)، گزینه‌های بازیگران و الگوهای حذف وضعیت‌های غیرممکن بازی بوده و خروجی آن، وضعیت‌های تعادلی بازی منطبق بر منطق‌های مختلف پایداری، وضعیت‌های تعادلی مطلوب و گزینه‌های تاثیرگذار بازیگران است.

الگوریتم (۱): مدل‌سازی و تحلیل بازی

Input:
playerOptions:set of player Options
infeasiblePatterns: set of patterns to delete infeasible states

Output:
NashStates, SEQStates, GMRStates, SMRStates, BestEQStates: set of fesiblestates
PlayersEffectiveoptions: set of player Options

#Step 1: Create binary form and infeasible state of Game
1: *AllGameStates*= 2^(count(*attackerOptions*) + count(*DefenderOptions*))
2: *GameFeasibleStates* =0
3: **For** each *ID* in range(0,*AllGameStates*):
4: create currenState'binaryForm for current *ID*
5: If currenState'binaryForm is in infeasiblePatterns:
6: Break
7: Else:
8: calculate Attacker and Defender Option'Values
9: update gameResultMatrix
10: *GameFeasibleStates*++
#Step 2: Calculate ordinal prefrences and UI(unilateral improvement) and UM(unilateral movement) of States
11: **For** each *state* in GameFeasibleStates:
12: calculate ordinal prefrences for Attacker and Defender
13: **For** each *state* in GameFeasibleStates:
14: calculate UI and UM for Attacker and Defender
15: update gameResultMatrix
#Step 3: Calculate Indivitual stability and equilibrium for Feasible States
16: **For** each *state* in GameFeasibleStates:
17: calculate Indivitual stability for Attacker and Defender for *state*
18: **For** each *state* in GameFeasibleStates:
19: calculate Nash, SEQ, GMR And SMR equilibrium for state
20: **For** each *state* in GameFeasibleStates:
21: calculate count of Nash, SEQ, GMR And SMR equilibrium
22: update gameResultMatrix
23: check gameSensitivity by minimum change in game' prefrences
#Step 4: Extract Players Effective options
24: **For** each *options* in playerOptions:
25: **For** each *ID* in range (1,50):
26: calculate *Measures[ID] by using gameResltMatrix and table4*
27: calculate PlayersEffectiveoptions by using measures
#Step 5: Calculate BestEQ of Game and final PlayersEffectiveoptions
28: calculate and show BestEQ and PlayersEffectiveoptions

۴-۳- الگوریتم سناریوسازی بازی‌ها

به‌دلیل عدم شناخت کافی بازیگران از یکدیگر، نحوه مدل‌سازی و بررسی تاثیر اطلاعات ناقص بازیگران یکی از موضوعات مهم در طرح‌ریزی و اجرای یک بازی است. قابلیت سناریوسازی و تحلیل نتایج سناریوهای تولیدی و تصمیم‌گیری در خصوص شرایط بازی‌ها، از اهداف شبه کد سناریوسازی بازی‌ها است. (۱) تغییر

پارامترهای گزینه‌های بازیگران، (۲) تغییر در ارتباطات گزینه‌های بازیگران بازی به دلیل عدم شناخت کافی بازیگران از یکدیگر و (۳) تغییر در ارتباطات گزینه‌های بازیگران بازی به دلیل عدم شناخت کافی بازیگران از یکدیگر از راهکارهای اعمال شناخت ناقص و عدم قطعیت در سناریوسازی بازی‌ها است.

تغییر پارامترهای گزینه‌های بازیگران، نتیجه آن تغییر ارزش گزینه‌های بازیگران است. با تغییر ارزش گزینه‌های بازیگران در مدل گراف، تعداد و ساختار وضعیت‌های ممکن بازی تغییر نخواهد کرد؛ اما ترجیحات بازیگران و حرکت و بهبود یک‌جانبه آن‌ها در وضعیت‌های ممکن بازی تغییر می‌کند و نتیجه آن تغییر وضعیت‌های تعادلی و گزینه‌های تاثیرگذار بازی است. الگوهای حذف وضعیت‌های غیرممکن بازی و ارزش گزینه‌های بازیگران، با ارتباطات گزینه‌های بازیگران، ارتباط مستقیم دارد. تغییر در ارتباطات گزینه‌های بازیگران نسبت به یکدیگر، باعث تغییر در وضعیت‌های ممکن بازی و ترجیحات و حرکت و بهبود یک‌جانبه بازیگران می‌گردد و نتیجه آن تغییر وضعیت‌های تعادلی و گزینه‌های تاثیرگذار بازی است. شبیه به تغییر در ارتباطات گزینه‌های بازیگران، تغییر در تعداد گزینه‌های بازیگران، باعث تغییر در وضعیت‌های ممکن بازی، ترجیحات، حرکت و بهبود یک‌جانبه بازیگران می‌گردد که نتیجه آن تغییر وضعیت‌های تعادلی و گزینه‌های تاثیرگذار بازی است.

الگوریتم (۲): مدل‌سازی، تحلیل و استخراج وضعیت‌های تعادلی مطلوب و گزینه‌های تاثیرگذار بازیگران به‌صورت سناریو محور

Input:
playerOptions:set of players options for each game
infeasiblePatterns: set of patterns to delete infeasible states for each game

Output:
PlayersEffectiveoptions: Set of Players options
NashStates, SEQStates, GMRStates, SMRStates: Set of feasible states of games

1:**For** each game in games
2: model and analysis game by using players'option and infeasibilePatterns
3: calculate NashStates, SEQStates, GMRStates, SMRStates
4: calculate PlayersEffectiveoptions for game by using Effective measures(table 4)
5: calculate BestEQ and final PlayersEffectiveoptions for current game(table 4)
6: add gameResult to gamesResultMatrix
7:calculate average of Effective measures for games in gamesResultMatrix
8:calculate final PlayersEffectiveoptions
9: **For** each game in games:
10: extend Players Effective options to current game
11: update and show BestEQ and PlayersEffectiveoptions for current game

مطابق با الگوریتم (۲)، با ایجاد تغییرات در شرایط مختلف بازی شامل تغییر ویژگی‌های گزینه‌های بازیگران و اضافه یا حذف آن‌ها، مدل‌سازی و تحلیل بازی به‌صورت سناریو محور انجام می‌شود. در خط ۱ شبه کد، برای تمام بازی‌ها، مراحل مدل‌سازی، تحلیل و استخراج وضعیت‌های تعادلی، استخراج وضعیت‌های تعادلی مطلوب و گزینه‌های تاثیرگذار و بروز رسانی ماتریس نتایج بازی صورت می‌گیرد؛ در ادامه میانگین میزان مشارکت گزینه‌های بازیگران در وضعیت‌های تعادلی مطلوب به تفکیک بازی‌ها محاسبه و گزینه‌های تاثیرگذار نهایی استخراج می‌شود. در خطوط ۲ تا ۵ نتایج بازی‌های مختلف تجمیع شده و گزینه‌های نهایی تاثیرگذار استخراج می‌گردد. در کدهای خط ۵، نتایج استخراج گزینه‌های نهایی به بازی‌های مختلف اعمال می‌گردد. در پایان شبه کد در خطوط ۶ تا ۷، گزینه‌های نهایی تاثیرگذار بازی‌ها و ارایه پیشنهادها به بازیگران، انجام می‌شود.

۳-۵- الگوریتم انتزاع سازی بازی‌ها

یکی از چالش‌های مهم در معماری مگ انفجار فضای حالت متناسب با افزایش گزینه‌های بازیگران است. انتزاع سازی و تجمیع گزینه‌های بازیگران و تبدیل آن‌ها به گزینه‌های سطح بالاتر، یکی از راهکارهای مقابله به انفجار فضای حالت بازی است. نحوه نگاشت گزینه‌های بازی پایه به بازی انتزاع یافته و نحوه نگاشت گزینه‌های تاثیرگذار بازی انتزاع یافته به بازی دو چالش عمده این معماری است.

الگوریتم (۳): مدل‌سازی و تحلیل بازی‌ها به‌صورت انتزاع یافته

Input:
playerOptions:Set of Players options for each game
infeasiblePatterns:set of patterns to delete infeasible states

Output:
PlayersEffectiveoptions: Set of Players options
NashStates, SEQStates, GMRStates, SMRStates:Set of feasible states
#Modelling, Analysis, Extract Effective options and BestEQ of originalGame

1: model and analysis originalGame by using players'option and infeasibilePatterns
2: calculate NashStates, SEQStates, GMRStates, SMRStates
3: calculate PlayersEffectiveoptions for originalGame by using Effective measures(table 4)
4: add originalgameResult to gamesResultMatrix
#Modelling, Analysis, Extract Effective options and BestEQ of abstractedGame
5: convert originalgame to abstractedgame
6: model and analysis abstractedgame by using players'option and infeasibilePatterns
7: calculate NashStates, SEQStates, GMRStates, SMRStates
8: calculate PlayersEffectiveoptions for abstractedgame by using Effective measures(table 4)
9: add abstractedgameResult to gamesResultMatrix
#Compare originalGame And abstractedGame
10:compare PlayersEffectiveoptions'originalgame with abstractedgame
11: **For** each game in games
12: calculate and show BestEQ and PlayersEffectiveoptions for current game

با توجه به معماری مگ در شکل (۱)، تبدیل گزینه‌ها در سطح اقدامات بازیگران و پارامترهای آن‌ها به گزینه‌ها در سطح رفتارها و استخراج وابستگی‌های بین اقدام و رفتار، یکی از مصادیق انتزاع‌سازی بازی پایه (فضای گسترده بازیگران حملات سایبری مبتنی بر بدافزار) است. در آن فضای حالت محیط پیچیده بازی اصلی به فضای محدود و کوچک‌تر بازی انتزاع شده، تبدیل می‌گردد. بازی انتزاع شده بر اساس معماری مگ، تحلیل شده و نتایج تحلیلی مبتنی بر فرآیند تبدیل گزینه‌ها (از سطح اقدام به رفتار) به فضای اصلی و واقعی بازی نگاشت می‌گردد.

مطابق با الگوریتم (۳)، ابتدا مراحل مدل‌سازی و تحلیل هرکدام از بازی‌ها صورت گرفته و برای هر بازی به‌صورت مجزا وضعیت تعادلی مطلوب و گزینه‌های تاثیرگذار انتخاب می‌گردد. با مقایسه نتایج بازی پایه و انتزاع یافته، گزینه‌های تاثیرگذار نهایی استخراج و مبتنی بر گزینه‌های انتخاب‌شده در هر بازی وضعیت تعادل مطلوب بازی‌ها مجدداً انتخاب می‌گردد؛ مبتنی بر نتایج بازی‌ها می‌توان ارتباطات بین گزینه‌ها را به نحو مطلوب‌تر تعیین کرد.

۳-۶- مقایسه معماری مگ با سایر مدل‌های مرتبط

چارچوب اولیه برای مدل گراف برای حل مناقشه در سال ۱۹۹۹ توسط هایپل و همکاران ارایه گردید که ابزار طراحی‌شده آن‌ها دارای اشکالات متعددی بوده و انعطاف‌پذیری لازم بخصوص برای سیستم‌های پویا و یادگیر را نداشته است [۴۳]. محدودیت‌های در تعریف بازیگر و گزینه‌های آن‌ها و محدودیت در تعداد وضعیت‌های بازی و نحوه ترجیح گذاری بازیگران در وضعیت‌های بازی، از نواقص ابزار و چارچوب موردنظر است. مدل *GMCR+* توسط رامی و همکاران که در سال ۲۰۱۵ ارایه شده، آخرین نسخه بروز شده مدل *GMCR II* بوده که علاوه بر رفع برخی از محدودیت‌های مدل قبلی (تعداد وضعیت‌های بازی)، قابلیت‌های ارایه گرافیکی وضعیت مختلف بازی، طراحی مکانیسم برای بازی و توصیف کیفی وضعیت‌های تعادلی را به ابزار مدنظر اضافه نموده است [۴۷].

جدول (۵): مقایسه معماری مگ با سایر مدل‌ها

ردیف	شاخص/مدل‌ها	*GMCR* [۴۳]	*GMCR+* [۴۷]	*MAG* (پیشنهادی)
۱	تعریف بازیگران	محدود / دستی	نامحدود / دستی	نامحدود / دستی، سیستمی
۲	تعریف اقدامات بازیگران	محدود / دستی	نامحدود / دستی	نامحدود / دستی، سیستمی
۳	منطق‌های تعادلی	*Nash, SEQ, GMR, SMR,*	*Nash, SEQ, GMR, SMR*	*Nash, SEQ, GMR, SMR,BestEQ*
۴	وضعیت‌های ائتلافی	دارد	دارد	ندارد
۵	معیارهای استخراج گزینه‌های تاثیرگذار	ندارد	ندارد	دارد
۶	تحلیل نتایج بازی مبتنی بر مدل آماری	ندارد	ندارد	دارد
۷	استخراج گزینه‌های تاثیرگذار در بازی	ندارد	ندارد	دارد
۸	استخراج وضعیت‌های مطلوب بازی	ندارد	ندارد	دارد
۹	بازی سناریو محور	ندارد	ندارد	دارد
۱۰	انتزاع سازی بازی	ندارد	ندارد	دارد

از چالش‌ها و نواقص به‌کارگیری مدل *GMCR II* و *GMCR+* در محیط‌های پویا شبیه به حوزه بدافزار، تعداد و تنوع ویژگی‌های رفتارهای بازیگران بوده که متناسب با شرایط و پارامترهای مختلف رقابت، شرایط مدل‌سازی و شبیه‌سازی تغییر می‌نماید. در جدول (۵)، معماری مگ با سایر مدل‌های مرتبط، بر اساس چند شاخص مقایسه و ارزیابی شده است. با توجه به اهداف بداندیش در حوزه بدافزار به‌خصوص زمانی که دو بازیگر مهاجم و مدافع به‌صورت غیرهمکارانه، در نظر گرفته می‌شوند، عموما ائتلاف معنی ندارد. بر اساس فرض غیرهمکارانه بودن بازی‌ها در مطالعه موردی این مقاله (بازی بدافزارها و مقابله‌کنندگان)، وضعیت‌های ائتلافی در معماری پیشنهادی بررسی نشده است. با توجه به قابلیت بررسی بازی همکارانه در مدل *GMCR*، در معماری مگ، امکان اضافه نمودن بررسی وضعیت‌های ائتلافی وجود دارد.

۴- ارزیابی معماری مگ - مطالعه موردی: بازی تشخیص و تحلیل قیاسی رفتارهای بازیگران

مطالعه موردی برای ارزیابی معماری مگ، بازی بدافزارها و مقابله‌کنندگان با رویکرد روش‌های تشخیص و تحلیل شواهد غیرمحیطی و قیاسی است. سناریو اصلی این است که مهاجمان قصد دارند حمله بدافزاری بر اساس مراحل مدل زنجیره کشتار

سایبری[1] یا مدل حمله میتره[2]، طراحی کنند. پس از شناسایی هدف و جمع‌آوری اطلاعات اولیه، قصد نفوذ و بهره‌برداری از سیستم هدف را دارند لذا مطابق برخی از اقدامات و رفتارهای مراحل نفوذ[3] و بهره‌برداری[4] مدل زنجیره کشتار سایبری یا دسترسی اولیه[5]، اجرا[6] و پایداری[7] مدل میتره اقدام می‌کنند. لذا از روش‌های شناسایی، تشخیص و تحلیل شواهد محیطی و غیرمحیطی اهداف استفاده می‌کنند. مهاجم در نظر دارند ابتدا با بهره‌گیری از روش‌های تشخیص و تحلیل شواهد غیرمحیطی و قیاسی، به سیستم هدف نفوذ کرده و متناسب با شرایط سیستم هدف اقداماتی انجام دهد و مراحل آتی حمله را اجرایی نمایند. لذا در این مرحله از حمله، طراحان بدافزار تمایل دارند تا شرایط حمله را با توجه از شناخت راهکارهای مقابله‌ای مقابله‌کنندگان تحلیل و ارزیابی نمایند. لذا طراحان، رفتارهای مهاجم را از مجموعه رفتارهای مرتبط با روش‌های تشخیص و تحلیل شواهد غیرمحیطی و قیاسی انتخاب می‌کنند و اقدامات و رفتارهای مقابله‌کنندگان را متناسب راهکارهای شناسایی و مقابله با رفتارهای مهاجمان، تعیین می‌کنند. به دلیل کامل نبودن اطلاعات بازیگران نسبت به توانمندی و راهکارهای مقابله‌ای رقیب، شناخت بازیگران از شرایط بازی با عدم قطعیت همراه بوده و در نتیجه، نتایج و تصمیم سازی معماری مگ متناسب با نیاز بازیگران، متنوع است. متناسب با شناخت بازیگران و عدم قطعیت‌های عنوان‌شده، بازی‌های متنوعی در این مطالعه موردی قابل تعریف است و هرکدام از این بازی‌ها به‌صورت منفرد مدل‌سازی و تحلیل می‌شوند. در مطالعه موردی این مقاله، سه بازی مطابق با جدول (۹) تعریف‌شده و بر اساس الگوریتم‌های سناریوسازی و انتزاع سازی بازی‌ها و ارتباطات و وابستگی‌های گزینه‌های بازیگران در بازی‌های مختلف، نتایج بازی‌ها تجمیع و تحلیل واقعی‌تر از سناریو مطالعه موردی ارایه گردیده است.

قابلیت و توانمندی بهره‌برداری بازیگران جهت اجرای گزینه‌ها در بازی‌های این مطالعه موردی، به‌صورت مفروض مطابق با جدول (۶)، در نظر گرفته شده و پارامترهای آن منابع مالی، نیروی انسانی متخصص، سامانه‌های نرم‌افزاری پایه بومی، تجهیزات زیرساختی بومی و دسترسی به دانش و فناوری است. ظرفیت بهره‌برداری از هر گزینه برای هر بازیگر در هر بازی بر اساس شرایط و ظرفیت بازیگران و پارامترهای گزینه‌ها طبق رابطه (۱) محاسبه می‌گردد.

[1] Cyber Kill Chain
[2] MITRE ATT@CK
[3] Intrusion
[4] Exploitation
[5] Initial Access
[6] Execution
[7] Persistence

جدول (۶): شرایط و ظرفیت بازیگران جهت اجرای گزینه‌ها

ردیف	عنوان پارامتر	مهاجم	مدافع
۱	منابع مالی	متوسط	متوسط
۲	نیروی انسانی متخصص	خوب	خوب
۳	سامانه‌های نرم‌افزاری پایه بومی	خوب	خوب
۴	تجهیزات زیرساختی بومی	ضعیف	ضعیف
۵	دسترسی به دانش و فناوری	متوسط	متوسط

۴-۱- مشخصات بازی‌ها و مدل‌سازی

در این مطالعه موردی، گزینه‌های بازیگران شامل رفتارهای مهاجم و مدافع بوده و این رفتارها بر اساس اقدامات بدافزارها و راهکارهای مقابله‌ای با آن‌ها که در بخش مبانی نظری بیان‌شده، استخراج گردیده است. گزینه‌های مهاجم در جدول (۷) و بر اساس رفتارهای تشخیص محیط‌های تحلیل و اشکال‌زدایی هدف بر اساس تحلیل قیاسی و شواهد غیر وابسته به محیط احصاء شده است؛ گزینه‌های مدافع مرتبط با رفتارهای خنثی‌سازی تشخیص قیاسی محیط اشکال‌زدا توسط بدافزارها و در قالب جدول (۸) بیان گردید.

جدول (۷): گزینه‌های مهاجم و ویژگی‌های آن‌ها

ردیف	عنوان گزینه	مراجع	پارامترهای رفتارها			
			پیچیدگی	تاب‌آوری	اثربخشی	فراوانی
۱	دست‌کاری جریان کنترلی پردازه‌های مرتبط با رفتارهای بدافزار	[۱۲]، [۲۳]، [۴۰]، [۴۳]، [۵۹]، [۶۰]	۶	۶	۷	۷
۲	فرار از قفل‌های اشکال‌زداها با قفل‌کردن سیستم	[۳۲]، [۲۷]	۷	۷	۸	۸
۳	نفوذ بدافزار مبتنی بر تکنیک بدون فایل جهت دور زدن تکنیک‌های ضد اشکال‌زدایی و دفاعی	[۲۹]، [۳۰]، [۴۰]، [۴۱]	۷	۸	۸	۸
۴	به تعویق انداختن رفتارهای اصلی و مخرب بدافزار	[۳۱]، [۳۳]–[۳۶]، [۵۹]، [۶۰]	۲	۵	۲	۷
۵	فعال‌سازی قابلیت‌های اصلی و مخرب بدافزار مبتنی بر محرک‌های محیطی	[۳۷]–[۳۹]	۴	۶	۳	۵
۶	دور زدن سامانه‌های نظارتی و جعبه‌شن با بهره‌گیری آسیب‌پذیری‌ها با رویکرد تکنیک‌های حمله بدون فایل	[۲۹]، [۴۱]	۹	۹	۸	۸
۷	دور زدن سامانه‌های نظارتی با تزریق کد مخرب در پردازه‌های هدف مبتنی بر حمله بدون فایل	[۲۹]، [۴۱]	۹	۸	۷	۷

اقدامات و پارامترهای بازیگران، با روش تحقیقی و اکتشافی از منابع علمی شامل گزارش‌های امنیتی، مقالات، بررسی مجموعه داده و تحلیل بدافزارهای مرتبط و نتایج تجربی و آزمایشگاهی

محققین و خبرگان حوزه بدافزار، استخراج گردیده‌اند. علاوه بر اینکه اقدامات و رفتارهای بازیگران و پارامترهای آن‌ها از منابع علمی معتبر تهیه و تدوین شده‌اند؛ توسط جمعی از پژوهشگران و خبرگان حوزه بدافزار به‌صورت خبره سنجی ارزیابی و تایید گردیده‌اند. نحوه خبره‌سنجی به این صورت بوده که ابتدا گزینه‌های بازیگران و مقادیر پارامترهای آن‌ها از منابع علمی استخراج و سپس نتایج در اختیار خبرگان قرار گرفت. جمع‌بندی نتایج خبره سنجی در قالب جدول رفتارهای (جداول (۷) و (۸)) ارایه شد. تجمیع‌سازی و انتزاع‌سازی اقدامات و تبدیل آن‌ها به رفتارها بر اساس رابطه (۴)، انجام شده است.

در جدول (۹)، مشخصات بازی‌های مطالعه موردی ارایه شده است. شناخت بازیگران نسبت به اقدامات یکدیگر در همه بازی‌ها، در قالب ستون " گزینه‌های مقابله‌ای" لحاظ شده است. تغییرات بازی (۲) نسبت به بازی (۱)، تغییر در مقادیر پارامترهای گزینه‌های بازیگران و متناسب با آن تغییر ارزش گزینه بازیگران است. در بازی (۳)، در میزان شناخت گزینه‌های مقابله‌ای رقیب، نسبت به بازی (۲)، تغییر ایجاد شده است. در جدول (۹)، ارزش گزینه‌های بازیگران بر اساس پارامترهای آن‌ها و مطابق با روابط (۲) و (۳) محاسبه شده است.

جدول (۸): گزینه‌های مدافع و ویژگی‌های آن‌ها

ردیف	عنوان گزینه	پارامترهای رفتارها			
		پیچیدگی	تاب‌آوری	اثربخشی	فراوانی
۱	مقابله با دست‌کاری جریان کنترلی اجرای بدافزار	۹	۸	۷	۸
۲	مقابله با تکنیک قفل‌کردن محیط اشکال‌زدا	۸	۷	۶	۸
۳	قطع ارتباطات و تعاملات شبکه‌ای و بازیابی زیرساخت هدف	۹	۷	۱۰	۸
۴	بهره‌گیری از تکنیک‌های مقابله با تعویق رفتارهای مخرب بدافزار	۶	۴	۶	۵
۵	بهره‌گیری از تکنیک‌های اکتشاف مسیر و اجرای نمادین برای آشکارسازی محرک‌های فعال‌ساز محیطی بدافزار	۸	۹	۷	۸
۶	بهره‌گیری از تکنیک‌های قلاب اندازی به توابع و وصله نمودن آسیب‌پذیری‌های هدف	۶	۷	۴	۶

جدول (۹): مشخصات بازی‌ها در مطالعه موردی

شماره گزینه	مهاجم						مدافع					
	بازی ۱		بازی ۲		بازی ۳		بازی ۱		بازی ۲		بازی ۳	
	ارزش گزینه‌ها	گزینه‌های مقابله‌ای	ارزش گزینه‌ها	گزینه‌های مقابله‌ای	ارزش گزینه‌ها	گزینه‌های مقابله‌ای	ارزش گزینه‌ها	گزینه‌های مقابله‌ای	ارزش گزینه‌ها	گزینه‌های مقابله‌ای	ارزش گزینه‌ها	گزینه‌های مقابله‌ای
۱	۳۳	۰	۳۳	۰	۲۹	۰	۴۰	۰	۴۰	۰	۳۷	۰
۲	۳۷	۱	۳۷	۱	۳۷	۱	۳۶		۳۶	۱	۳۳	
۳	۳۹		۳۹	۲	۳۶		۴۲	۲	۴۲	۲	۳۵	۲
۴	۲۰		۲۰		۱۹		۲۷		۲۷		۲۷	
۵	۲۳	۴	۲۳	۴	۲۳	۴	۴۰	۴	۴۰	۴	۴۰	۴
۶	۴۲		۴۲	۵	۳۶		۲۹	۶	۲۹	۶	۲۹	۶
۷	۳۹	۵	۳۹	۵	۳۵	۵						

الگوهای حذف وضعیت‌های غیرممکن بازی‌ها مطابق با جدول (۱۰)، بر اساس محدودیت‌های "استفاده از حداقل یکی از گزینه‌ها "، "وابستگی گزینه‌های بازیگران " و "نبود قابلیت پیاده‌سازی و اجرا توسط بازیگر "، تعیین گردیده است. با بررسی ظرفیت و توانمندی بازیگران جهت اجرای گزینه‌ها در این مطالعه موردی، مطابق جدول (۱۰) در بازی‌های (۱) و (۲) از گزینه‌های مهاجم و مدافع به ترتیب ۲ و ۱ گزینه، حذف گردیده است؛ با تغییر پارامترهای گزینه‌های بازیگران در بازی (۳)، ظرفیت و توانمندی اجرای همه گزینه‌ها برای بازیگران فراهم شده است. سایر الگوهای حذف وضعیت‌های غیرممکن بازی‌ها بر اساس روابط و شناخت گزینه‌های بازیگران به یکدیگر ارایه گردید.

جدول (۱۰): الگوهای حذف وضعیت‌های غیرممکن بازی‌ها

ردیف	عنوان الگو/بازی	بازی ۱		بازی ۲		بازی ۳	
		مهاجم	مدافع	مهاجم	مدافع	مهاجم	مدافع
۱	استفاده حداقل یکی از گزینه‌ها	۱	۱	۱	۱	۱	۱
۲	وابستگی گزینه‌های بازیگران	۴	۴	۶	۵	۴	۴
۳	نبود قابلیت پیاده‌سازی و اجرا توسط بازیگر	۲	۱	۲	۱	۰	۰

در جدول (۱۱)، خلاصه مشخصات بازیگران در بازی‌های این مطالعه موردی، شامل تعداد گزینه‌های بازیگران و پارامترهای آن‌ها، وابستگی گزینه‌ها و الگوهای حذف وضعیت غیرممکن بازی، وضعیت‌های ممکن بازی‌ها، بر اساس مراحل مدل‌سازی معماری مگ، ارایه شده است.

جدول (۱۱): مشخصات و شرایط مدل‌سازی بازی‌های مطالعه موردی

بازی‌ها / شماره ویژگی‌ها	بازی ۱		بازی ۲		بازی ۳	
	مهاجم	مدافع	مهاجم	مدافع	مهاجم	مدافع
۱	۷	۶	۷	۶	۷	۶
۲	۴	۴	۴	۴	۴	۴
۳	۶/۶	۷/۱	۶/۶	۷/۱	۶/۱	۶/۶
۴	۱	۱	۱	۱	۱	۱
۵	۶/۶	۷/۰	۶/۶	۷/۰	۶/۲	۶/۶
۶	۷	۶	۹	۷	۵	۵
۷	۸۱۹۲		۸۱۹۲		۸۱۹۲	
۸	۸۰۷۱		۸۱۶۳		۷۶۳۸	
۹	۱۲۱		۲۹		۵۵۴	
۱۰	۹۸/۶		۹۹/۶۵		۹۳/۲۴	
۱۱	۸		۸		۱۶	
۱۲	۴۴		۸		۳۲۶	
۱۳	۸		۸		۲۳	
۱۴	۸		۸		۱۶	
۱۵	۷		۷		۱۶	

در جدول (۱۱) عنوان ویژگی‌های مرتبط با شماره ویژگی‌ها شامل (۱) تعداد گزینه‌های بازیگر، (۲) تعداد پارامترهای گزینه‌ها، (۳) میانگین پارامترهای گزینه‌ها، (۴) تعداد پارامترهای بهره‌بردار، (۵) میانگین پارامترهای بهره‌بردار (۶) تعداد الگوهای حذف وضعیت‌های غیرممکن، (۷) تعداد کل وضعیت‌های بازی‌ها، (۸) تعداد وضعیت‌های غیرممکن بازی‌ها، (۹) تعداد وضعیت‌های ممکن بازی‌ها، (۱۰) درصد کاهش تعداد وضعیت‌های بازی، (۱۱) تعداد تعادل *Nash*، (۱۲) تعداد تعادل *SEQ*، (۱۳) تعداد تعادل *GMR*، (۱۴) تعداد تعادل *SMR*، (۱۵) تعداد تعادل *BestEQ* هستند. ویژگی‌های شماره (۱۱) تا (۱۵) از جدول (۱۱)، بیان‌کننده وضعیت‌های تعادلی به تفکیک سه بازی مطالعه موردی است. حداقل تعداد وضعیت‌های تعادلی مربوط به بازی شماره (۲) بوده و تعداد وضعیت‌های تعادلی غیر از منطق تعادلی *BestEQ*، در سایر منطق‌های تعادلی یکسان است. با اعمال محدودیت‌های بیشتری به بازی‌ها، ضمن کاهش تعداد وضعیت‌های ممکن بازی، تعداد وضعیت‌های تعادلی نیز کاهش می‌یابد.

۴-۲- بحث و تحلیل نتایج بازی‌ها

در جدول (۱۲)، نتایج سه بازی مطالعه موردی، جهت استخراج گزینه‌های تاثیرگذار بر اساس الگوریتم (۲)، ارایه شده است. مطابق جدول (۱۲)، گزینه ۱، ۳، ۵ و ۷ مهاجم و گزینه‌های ۱، ۲، ۵ و ۶ مدافع به‌عنوان گزینه‌های تاثیرگذار مطالعه موردی معرفی گردیده است. گزینه ۳ مهاجم و گزینه‌های ۱ و ۵ مدافع نسبت به بقیه گزینه‌های تاثیرگذار بازیگران فراوانی بیشتری در وضعیت‌های تعادلی مطلوب داشته‌اند.

جدول (۱۲): نتایج بازی‌ها در استخراج گزینه‌های تاثیرگذار

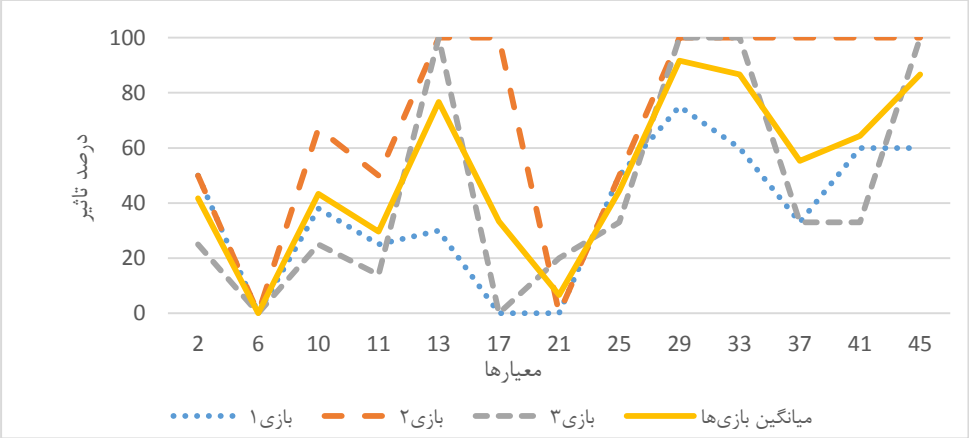
معیارها	گزینه‌های مهاجم								گزینه‌های مدافع								درصد مشارکت بازیگران
	۱	۲	۳	۴	۵	۶	۷	درصد مشارکت	۱	۲	۳	۴	۵	۶	درصد مشارکت		
۲	۰	۱	۱	۰	۰	۳	۰	۲۵	۲	۰	۲	۰	۳	۰	۴۲		۳۳
۶	۱	۳	۰	۰	۱	۱	۱	۷۵	۱	۰	۳	۰	۱	۱	۷۵		۷۵
۱۰	۳	۱	۳	۰	۳	۰	۳	۴۲	۲	۲	۰	۰	۲	۳	۷۱		۵۶
۱۱	۲	۲	۰	۰	۲	۰	۲	۳۸	۲	۲	۰	۰	۲	۳	۷۱		۵۴
۱۳	۲	۰	۲	۱	۲	۰	۲	۶۲	۲	۲	۰	۱	۲	۲	۷۵		۶۹
۱۷	۰	۰	۰	۰	۳	۰	۰	۸	۰	۰	۰	۱	۰	۳	۸		۸
۲۱	۱	۰	۱	۰	۰	۰	۰	۵۰	۱	۰	۱	۱	۰	۰	۲۵		۳۸
۲۵	۰	۰	۱	۰	۰	۰	۳	۳۳	۰	۰	۰	۰	۳	۰	۱۷		۲۵
۲۹	۱	۰	۲	۰	۱	۰	۱	۱۰۰	۲	۱	۰	۰	۲	۲	۸۸		۹۴
۳۳	۱	۰	۲	۰	۱	۰	۱	۱۰۰	۲	۲	۰	۰	۲	۲	۷۵		۸۸
۳۷	۱	۰	۰	۱	۲	۰	۱	۶۲	۱	۱	۰	۲	۱	۱	۱۰۰		۸۱
۴۱	۱	۰	۲	۰	۱	۰	۱	۱۰۰	۳	۱	۰	۰	۳	۲	۷۱		۸۵
۴۵	۱	۰	۲	۰	۱	۰	۱	۱۰۰	۲	۲	۰	۰	۲	۲	۷۵		۸۸
۴۸	۱	۰	۲	۰	۱	۰	۱	۱۰۰	۲	۱	۰	۰	۲	۱	۱۰۰		۱۰۰
۵۰	۱	۰	۲	۰	۱	۰	۱	۶۴	۲	۱	۰	۰	۲	۱	۶۴		۶۴

در جدول (۱۳) گزینه‌های تاثیرگذار هر بازی به تفکیک ارایه شده و بر اساس آن، گزینه‌های تاثیرگذار بازی (۱) شامل گزینه ۳ مهاجم و گزینه ۱ و ۵ مدافع، گزینه‌های تاثیرگذار بازی (۲) شامل گزینه‌های ۱، ۵ و ۷ مهاجم و گزینه‌های ۱، ۵ و ۶ مدافع و گزینه‌های تاثیرگذار بازی (۳) شامل گزینه ۳ مهاجم و گزینه ۲ مدافع است.

جدول (۱۳): گزینه‌های تاثیرگذار بازیگران به تفکیک بازی

گزینه‌ها / بازی‌ها	گزینه‌های تاثیرگذار مهاجم							گزینه‌های تاثیرگذار مدافع					
	۱	۲	۳	۴	۵	۶	۷	۱	۲	۳	۴	۵	۶
بازی ۱	۰	۰	۱	۰	۰	۰	۰	۱	۰	۰	۰	۱	۰
بازی ۲	۱	۰	۰	۰	۱	۰	۱	۱	۰	۰	۰	۱	۱
بازی ۳	۰	۰	۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰

در نمودار شکل (۲)، وضعیت معیارهای موثر بر گزینه‌های تاثیرگذار مطالعه موردی به تفکیک بازی‌های آن و میانگین بازی‌ها، ارایه شده است. هدف از ارایه این نمودار، بررسی و انتخاب موثرترین معیارها در انتخاب گزینه‌های تاثیرگذار بازیگران و وضعیت‌های تعادلی بازی است.



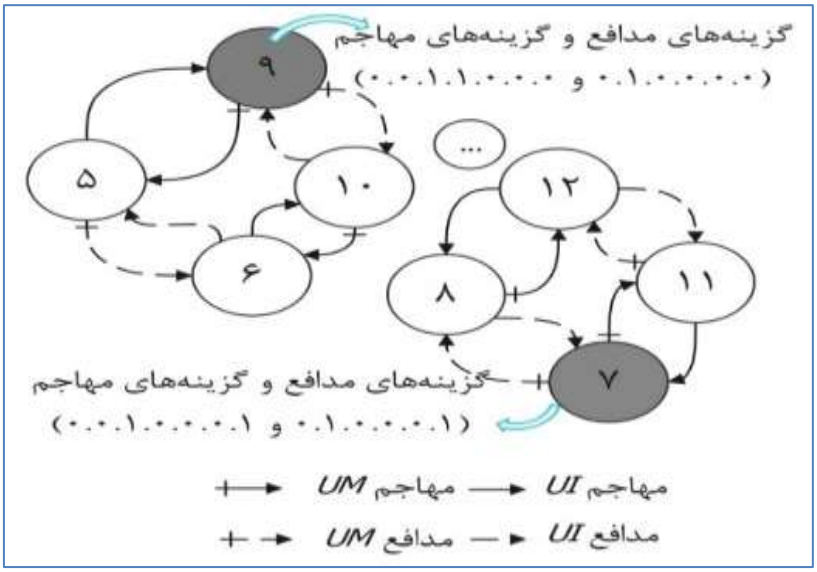
شکل (۲): نمودار تاثیر معیارها بر وضعیت‌های تعادلی مطلوب

مطابق با جدول (۱۲)، (۱۳) و نمودار شکل (۲)، تحلیل میزان مشارکت گزینه‌های بازیگران بر اساس پارامترهای موثر در استخراج گزینه‌های تاثیرگذار بازیگران، قابل تفسیر است.

معیار شماره ۲ مرتبط با ارزش گزینه‌های بازیگران، مشارکت ۳۳ درصدی داشته که این مشارکت، نشان‌دهنده قوی و قابل‌قبول بودن این معیار نیست. میانگین معیارهای ۶، ۱۰ و ۱۱ مرتبط با میزان شناخت بازیگران از گزینه‌ها، به ترتیب مشارکت ۶۲ درصدی داشته و این میزان مشارکت، در بازی‌های مرتبط با مطالعه موردی نیز پایین است. علت پایین بودن مشارکت این معیار، کثرت و پراکندگی گزینه‌های تاثیرگذار بازی‌های مطالعه موردی در مهاجم و مدافع بوده است. معیار شماره ۱۳ مرتبط با مشارکت گزینه‌های بازیگران در بازی، مشارکت ۶۹ درصدی در استخراج گزینه‌های تاثیرگذار بازی‌ها داشته است. معیار ۱۷ مرتبط باکیفیت مشارکت گزینه‌های بازیگر در وضعیت‌های بازی با عایدی کمتر بازیگران، مشارکت ۸ درصدی در استخراج گزینه‌های تاثیرگذار داشته و این موضوع به دلیل عدم تمایل بازیگران به حضور در وضعیت شکست و ناپایدار بودن در چنین وضعیت‌هایی، منطقی و قابل پیش‌بینی بوده است.

معیار ۲۱ مرتبط با کیفیت مشارکت گزینه‌های بازیگر در وضعیت‌های بازی با عایدی برابر بازیگران، تاثیر ۳۸ درصدی در استخراج گزینه‌های تاثیرگذار بازی‌ها داشته و این موضوع با منطق پایداری و تعادل بازیگران در وضعیت‌های بازی همخوانی دارد اما مقدار این معیار پایین است. علت پایین بودن مشارکت این معیار، کثرت و پراکندگی گزینه‌های تاثیرگذار بازی‌های مطالعه موردی در مهاجم و مدافع بوده است. معیار ۲۵ مرتبط با کیفیت مشارکت گزینه‌های بازیگر در وضعیت‌های بازی با عایدی بیشتر بازیگران، تاثیر ۲۵ درصدی در استخراج گزینه‌های تاثیرگذار بازی‌ها داشته است. معیار ۲۹ مرتبط با کیفیت پایداری گزینه‌های بازیگر، مشارکت ۹۴ درصدی در تعیین گزینه‌های تاثیرگذار داشته‌اند که بیان‌کننده موضوع است که اکثریت وضعیت‌های شامل گزینه‌های تاثیرگذاری بازیگران مطابق با منطق نش، وضعیت تعادل بوده‌اند. میانگین معیارهای مرتبط با وضعیت تعادلی شامل معیارهای ۳۳، ۳۷، ۴۱، ۴۵ و ۴۸ تاثیر ۸۹ درصدی داشته و نشان‌دهنده این است که گزینه‌های تاثیرگذار استخراجی بازی به‌طور میانگین در ۸۹ درصد وضعیت‌های مرتبط با تعادلی مطلوب مشارکت داشته‌اند. علت اصلی بالابودن مقدار این معیار، بالا بودن مقدار معیار مرتبط با کیفیت پایداری گزینه‌های بازیگر است. میانگین درصد مشارکت همه معیارها، در تعیین گزینه‌های تاثیرگذار ۸۱ درصد محاسبه گردید. این مقدار برای مهاجم و مدافع به ترتیب ۶۲ و ۱۰۰ درصد است که نشان‌دهنده همگرا بودن مشخصات مدافع نسبت به مهاجم در بازی‌ها، بوده است. هرکدام از وضعیت‌های تعادلی و غیرتعادلی بازی‌های این مطالعه موردی، متناسب با بهره‌گیری بازیگران از گزینه‌های خود در آن وضعیت، قابل تفسیر است. تعداد وضعیت‌های تعادلی مطلوب بازیگران در بازی‌های (۱)، (۲) و (۳) به ترتیب ۷، ۷ و ۱۶ مورد و عموما وضعیت‌های تعادلی مطلوب، وضعیت‌های تعادلی *Nash* بودند. در بازی (۲) از ۲۹ وضعیت ممکن بازی، وضعیت‌های (۰)، (۷)، (۹)، (۱۴)، (۱۵)، (۲۱) و (۲۳) وضعیت تعادلی مطلوب بازی بوده و همه این وضعیت‌ها، بر اساس منطق‌های تعادلی *Nash*، *SEQ*، *GMR* و *SMR* نیز وضعیت تعادلی هستند. در همه وضعیت‌های تعادلی مطلوب ذکرشده در بازی (۳)، از گزینه‌های تاثیرگذار مهاجم و مدافع استفاده شده و همین شرایط در بازی‌های (۱) و (۲) نیز وجود دارد.

در شکل (۳)، بخشی از گراف بازی (۲)، ارایه گردیده و همان‌طور که در شکل (۳) نشان داده شده، در وضعیت تعادلی مطلوب ۷ مهاجم از گزینه‌های ۱ و ۵ و مدافع از گزینه‌های ۱ و ۵ بهره‌برداری نموده و در وضعیت ۹ مهاجم از گزینه‌های ۴ و ۵ و مدافع از گزینه ۵ استفاده کرده است.



شکل (۳): بخشی از گراف بازی (۲)

در جدول (۱۴)، از بین گزینه‌های تاثیرگذار مهاجم به دلیل فراوانی تکرار گزینه ۳ در معیار ۴۹ و تکرار در سایر معیارهای تاثیرگذار، این گزینه به‌عنوان گزینه برتر نهایی انتخاب می‌گردد؛ همین شرایط در گزینه ۳ و ۵ مدافع، نیز صدق می‌کند. متناسب با ارتباطات تعریف‌شده بین گزینه‌های بازیگران در سطح رفتار با اقدام در معماری مگ و بر اساس الگوریتم (۳)، در خصوص بازی انتزاع یافته، ارتباطات بین گزینه‌های بازیگران در قالب جدول (۱۴)، بیان گردیده است.

جدول (۱۴): ارتباط گزینه‌های تاثیرگذار بازیگران در سطح رفتار با گزینه‌های در سطح اقدام

بازیگر	شماره گزینه	عنوان گزینه در سطح رفتار	عنوان گزینه در سطح اقدام
مهاجم	۳	نفوذ بدافزار مبتنی بر تکنیک بدون فایل جهت دور زدن تکنیک‌های ضد اشکال‌زدایی و دفاعی	بهره‌برداری از آسیب‌پذیری‌های مبتنی بر وب جهت حمله بدون فایل به اشکال‌زدا
			بهره‌برداری از آسیب‌پذیری‌های سطح هسته جهت حمله بدون فایل به اشکال‌زدا
مدافع	۳	قطع ارتباطات و تعاملات شبکه‌ای و بازیابی زیرساخت هدف	قطع دسترسی شبکه و وب تا زمان وصله کردن آسیب‌پذیری هدف
			نبود راهکار مناسب در منابع آشکار، بازیابی اطلاعات سیستم هدف و مسدودسازی درگاه‌های ورود
	۵	بهره‌گیری از تکنیک‌های اکتشاف مسیر و اجرای نمادین برای آشکارسازی محرک‌های فعال‌ساز محیطی بدافزار	بهره‌گیری از تکنیک کشف مسیر برای تعیین شرایط و مسیر فعال‌سازی بدافزار: با کلید مشخص، در زمان مشخص، بر اساس ورودی‌های متنوع شبکه‌ای و برنامه‌های کاربردی

با توجه به توانایی‌ها و قابلیت‌های مهاجم و مدافع و همچنین مدل‌سازی و تحلیل بازی، مهاجم از گزینه " اجرای رفتارهای اصلی بدافزار مبتنی بر تکنیک بدون فایل جهت مقابله با تکنیک‌های ضد اشکال‌زدایی "، استفاده می‌نماید. با توجه به فرضیات مساله و جدید بودن حملات بدون فایل و بهره‌برداری مهاجم از آسیب‌پذیری‌های نوین وب، مدافع توانایی‌های لازم جهت مقابله با این نوع حمله را ندارد. زمانی که مدافع نشانه‌هایی از حمله دریافت کرد نیاز است ارتباطات شبکه‌ای زیرساخت خود

را قطع و ضمن وصله نمودن آسیب‌پذیری‌های موجود زیرساخت، با استفاده از تکنیک‌های بازیابی اطلاعات، زیرساخت هدف را مجدداً راه‌اندازی نماید. حمله اخیر به زیرساخت‌های بندرهای جنوب کشور ایران در مهرماه سال ۹۹ و گزارش‌ها شرکت‌های امنیتی، تأکید کننده، شرایط و نتایج این بازی است. لذا توصیه می‌گردد مدافع توانایی خود جهت شناسایی و مقابله با حملات بدون فایل را افزایش دهد.

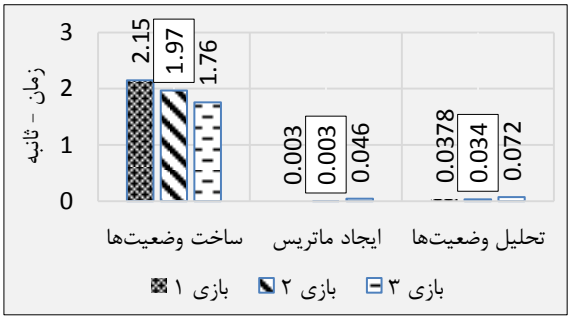
۴-۳- تحلیل حساسیت بازی‌ها و مطالعه موردی

یکی از روش‌های تعیین قابل‌اعتماد بودن معماری پیشنهادی، تحلیل حساسیت بازی است؛ بدین‌صورت که با تغییر جزئی اولویت‌های بازیگران نباید نتایج مدل‌سازی و وضعیت‌های تعادل به‌صورت گسترده‌ای تغییر کند. در این بازی‌های این مطالعه موردی، با تغییر اندک در پارامترهای گزینه‌های بازیگران و شناخت بازیگران نسبت به گزینه‌های مقابله‌ای رقیب، تغییرات جزئی در اولویت‌های بازیگران نسبت به وضعیت‌های بازی پایه صورت گرفت؛ اما در نتایج مدل‌سازی و تحلیل، یعنی وضعیت‌های تعادلی مطالعه موردی تغییر جدی صورت نگرفت؛ افزون بر این، گزینه‌های تاثیرگذار استخراجی و وضعیت‌های تعادلی مطالعه موردی، بر مبنای سه بازی متفاوت و مرتبط بوده و وضعیت‌های تعادلی بر اساس ۵ منطق تعادلی (*Nash, SEQ, GMR, SMR, BestEQ*) استخراج شده است. لذا، می‌توان نتیجه گرفت که وضعیت‌های تعادلی به‌دست‌آمده وضعیت‌های تعادلی قابل‌اعتمادی هستند.

۴-۴- مدت زمان مدل‌سازی، شبیه‌سازی و تحلیل بازی‌های مطالعه موردی:

در شکل (۴)، نمودار مدت زمان مدل‌سازی و شبیه‌سازی بازی‌های مطالعه موردی برحسب ثانیه، در سه بخش، ارایه شده است.

۱- مدت زمان ساخت وضعیت‌های ممکن بازی و استخراج حالت گزینه‌ای وضعیت‌ها (گزینه‌های به‌کارگیری شده در وضعیت)، محاسبه عایدی و ترجیح گذاری بازیگران نسبت به وضعیت‌های ممکن بازی که به‌عنوان ساخت وضعیت‌ها در نمودار شکل (۴) عنوان شده است. این زمان با تعداد گزینه‌های بازیگران ارتباط مستقیم دارد و هرچه تعداد گزینه‌های بازیگران بیشتر باشد زمان ساخت وضعیت‌ها به‌صورت نمایی افزایش می‌یابد؛ هر چه تعداد و الگوهای حذف وضعیت‌های غیرممکن بازی بیشتر باشد، تعداد وضعیت‌های قابل‌حذف افزایش یافته و زمان ساخت وضعیت‌های بازی کمتر می‌گردد.



شکل (۴): نمودار مدت زمان مدل‌سازی و تحلیل بازی‌ها

۲- مدت زمان استخراج بهبود و حرکت‌های یک‌جانبه بازیگران در وضعیت‌های ممکن بازی که با عنوان "ایجاد ماتریس انتقال " بازی، بیان گردیده است. این زمان با تعداد وضعیت‌های ممکن بازی ارتباط مستقیم دارد و هرچه تعداد وضعیت‌ها بیشتر باشد زمان محاسبه نیز افزایش خواهد یافت. هرچه ارتباطات بین وضعیت‌های بازی (یال‌های بین گره‌های گراف بازی) کمتر باشد مدت زمان استخراج بهبود و حرکت‌های یک‌جانبه بازیگران کمتر خواهد شد.

۳- مدت زمان تحلیل و استخراج گزینه‌های تاثیرگذار و تعادلی بازی، از مجموع مدت زمان استخراج پایداری فردی و تعادلی بازیگران بر مبنای منطق‌های *Nash, SEQ, GMR, SMR* و *BestEQ* و محاسبه مقادیر معیارهای موثر در تعیین گزینه‌های اثرگذار بازیگران به دست می‌آید. هرچه تعداد وضعیت‌های ممکن بازی کمتر و تعداد وضعیت‌های پایداری بازیگران (به‌خصوص پایداری *Nash*) بیشتر باشد، مدت زمان تحلیل و استخراج گزینه‌های تاثیرگذار و تعادلی بازی کمتر می‌گردد.

۴-۵- یافته‌های مقاله مبتنی بر معماری مگ:

در جدول (۱۵)، گزاره‌های[1] استخراجی از نتایج مدل‌سازی و تحلیل بازی‌های مطالعات موردی در قالب یافته‌های مقاله ارایه شده است. بر اساس نتایج جدول (۱۵)، می‌توان تحلیل و درک مناسب‌تری به شرایط بازی، قبل از مدل‌سازی و شبیه‌سازی آن داشت؛ این گزاره‌ها در بازی‌های سناریو محور و تکرارپذیر، قابلیت به‌کارگیری و بهره‌برداری بیشتری دارد.

نظریه بازی یکی از ابزارهای مهم تصمیم‌گیری در بازی جنگ هست و همه موضوعات عنوان‌شده در این مقاله مبتنی بر نظریه بازی و تحلیل مناقشه بوده؛ لذا یکی از کاربردهای معماری مگ، بهره‌گیری از آن در سامانه بازی جنگ است. مدل *GMCR*، یکی از مصادیق سامانه‌های تصمیم‌یار بوده و معماری مگ مبتنی بر توسعه مدل *GMCR* است؛ بنابراین معماری مگ نیز مصداق

[1] Proposition

معماری یک سامانه تصمیم‌یار است. در این مقاله کاربردی بودن معماری مگ در حوزه بدافزار بررسی و ارزیابی شد؛ لذا می‌توان از آن در سامانه‌های بازی جنگ و تصمیم‌یار عملیات سایبری استفاده کرد.

جدول (۱۵): گزاره‌های استخراجی مبتنی بر تحلیل نتایج بازی‌ها

ردیف	عنوان گزاره	نتیجه گزاره	پیامدهای گزاره
۱	افزایش ارزش پارامترهای گزینه	افزایش ارزش گزینه	افزایش کیفیت برتری، کیفیت تعادلی، احتمال گزینه تاثیرگذار بودن
۲	کاهش ارتباطات گزینه بازیگر به گزینه‌های رقیب	افزایش ارزش گزینه، کاهش کیفیت شناخت	افزایش کیفیت برتری، کیفیت تعادلی، احتمال گزینه تاثیرگذار بودن
۳	افزایش ارتباطات گزینه‌های بازیگران	افزایش کیفیت شناخت، کاهش وضعیت‌های ممکن	محدودتر و قابل توصیف‌تر شدن نتایج بازی، کاهش زمان مدل‌سازی و تحلیل بازی
۴	افزایش پایداری فردی بازیگران	افزایش کیفیت تعادل نش	کاهش زمان تحلیل بازی، افزایش احتمال گزینه تاثیرگذار بودن
۵	افزایش مشارکت در وضعیت‌های تعادلی	افزایش کیفیت مشارکت تعادلی	افزایش کیفیت تعادل‌ها، افزایش احتمال گزینه تاثیرگذار بودن
۶	افزایش آستانه استخراج گزینه‌های تاثیرگذار	افزایش گزینه‌های تاثیرگذار	افزایش کیفیت تعادلی، افزایش پراکندگی نتایج
۷	افزایش ریسک‌پذیری بازیگر	افزایش وضعیت‌های تعادلی *GMR* و *SMR*	افزایش کیفیت تعادلی مطلوب

۵- نتیجه‌گیری

در این مقاله معماری مگ برای بهبود مدل گرافِ تحلیل مناقشه ارایه شده است. برای ارزیابی معماری مگ، از مطالعه موردی مرتبط با تشخیص و تحلیل قیاسی رفتار بدافزارها و مقابله‌کنندگان، استفاده شده است. نتایج حاصل از ارزیابی به‌صورت انتزاع سازی و سناریو محور نشان می‌دهد در این مطالعه موردی، مهاجم تمایل دارد از تکنیک‌های حملات سایبری بدون فایل استفاده نماید و از آن‌جایی که مدافع توانایی کافی مقابله با این نوع حملات را ندارد، عموما وضعیت‌هایی که شامل این گزینه باشند جزء وضعیت‌های تعادلی بازی هستند. معماری مگ محدودیتی از نظر تعداد بازی‌های سناریو محور نداشته و در ارزیابی مقاله تنها سه نوع بازی برای ارزیابی استفاده گردید. تجمیع نتایج بازی‌های سناریو محور مقاله نشان داد میزان مشارکت ۵۰ معیار پیشنهادی در استخراج گزینه‌های تاثیرگذار مهاجم و مدافع، ۶۴ درصد بوده است. میزان تایید معیارهای مرتبط با وضعیت‌های تعادلی بازی برای گزینه‌های تاثیرگذار مهاجم و مدافع ۱۰۰ درصد محاسبه شد. تعداد وضعیت‌های تعادلی مطلوب بازیگران در بازی‌های (۱)، (۲) و (۳) به ترتیب ۷، ۷ و ۱۶ مورد و عموما وضعیت‌های تعادلی مطلوب، وضعیت‌های تعادلی نش بودند. نتایج و یافته‌های مدل‌سازی و تحلیل بازی‌های مطالعه موردی، به‌عنوان گزاره‌های استخراجی ارایه شده است. معماری مگ، معیارهای استخراج وضعیت‌های تعادلی و گزینه‌های تاثیرگذار، الگوریتم‌های انتزاع‌سازی و بازی سناریو محور از نوآوری‌های این مقاله بوده است. استخراج محاسباتی رفتارهای بازیگران و پارامترهای ارزش‌گذاری رفتارها، تحلیل و استخراج رفتارهای تاثیرگذار بازیگران با رویکردهای فازی، بهبود معیارهای استخراج گزینه‌های تاثیرگذار و بررسی شرایط ائتلاف در مناقشه‌های حوزه بدافزار را می‌توان به‌عنوان کارهای آتی این مقاله بیان کرد.

۶- منابع

[1] J. Pawlick, E. Colbert, and Q. Zhu, "A Game-Theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy," ACM Comput. Surv., vol. 52, no. 4, 2019,

[2] M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," IEEE Commun. Surv. Tutorials, vol. 21, no. 1, pp. 640–660, 2019,

[3] H. Akbari, S. M. Safavi, and R. Khandani, "The Distributed Denial of Service Attacks Situation Awareness Based on The Prediction of Battle Scene Using Dempster-Shefer Evidences Theories and Bayesian Rules," Electron. Cyber Def., vol. 7, no. 1, pp. 77–94, 2019, [Online]. Available: https://ecdj.ihu.ac.ir/article_204480.html

[4] A. Afianian, S. Niksefat, B. Sadeghiyan, and D. Baptiste, "Malware Dynamic Analysis Evasion Techniques: A Survey," CoRR, vol. abs/1811.0, 2018.

[5] A. Bulazel and B. Yener, "A survey on automated dynamic malware analysis evasion and counter-evasion: PC, Mobile, and Web," ACM Int. Conf. Proceeding Ser., pp. 1–21, 2017,

[6] Y. Huang, U. Verma, C. Fralick, G. Infantec-Lopez, B. Kumar, and C. Woodward, "Malware Evasion Attack and Defense," pp. 34–38, 2019,

[7] S. Ghasemi and S. Parsa, "An Effective Method to Detect Environment-Aware Malware Based on the Behavioral Distances Comparison," Electron. Cyber Def., vol. 6, no. 4, pp. 123–133, 2019.

[8] C. Kiennert, Z. Ismail, H. Debar, and J. Leneutre, "A Survey on Game-Theoretic Approaches for Intrusion Detection and Response Optimization," ACM Comput. Surv., vol. 51, no. 5, Aug. 2018,

[9] J. Z. Bakdash et al., "Malware in the future? Forecasting of analyst detection of cyber events," J. Cybersecurity, vol. 4, no. 1, Jan. 2018,

[10] H. Zhang et al., "Defense Against Advanced Persistent Threats: Optimal Network Security Hardening Using Multi-stage Maze Network Game," in 2020 IEEE Symposium on Computers and Communications (ISCC), 2020, pp. 1–6.

[11] M. Abbasi, M. Sheikhmohamadi, and M. Ghaioory, "Modeling and Analysis of competition between malware authors and security analysts, using game theory," Strateg. Stud. public policy, vol. 7, no. 23, pp. 19–41, 2017.

[12] D. M. Kilgour and K. W. Hipel, "The graph model for conflict resolution: past, present, and future," Gr. Decis. Negot., vol. 14, no. 6, pp. 441–460, 2005,

[13] C. Phillips and L. P. Swiler, "A Graph-Based System for Network-Vulnerability Analysis," in Proceedings of the 1998 Workshop on New Security Paradigms, 1998, pp. 71–79.

[14] O. M. Sheyner, "Scenario graphs and attack graphs," CARNEGIE-MELLON UNIV PITTSBURGH PA SCHOOL OF COMPUTER SCIENCE, 2004.

[15] J. Zeng, S. Wu, Y. Chen, R. Zeng, and C. Wu, "Survey of attack graph analysis methods from the perspective of data and knowledge processing," Secur. Commun. Networks, vol. 2019, 2019.

[16] A. Mpanti, S. D. Nikolopoulos, and I. Polenakis, "A Graph-Based Model for Malicious Software Detection Exploiting Domination Relations between System-Call Groups," in Proceedings of the 19th International Conference on Computer Systems and Technologies, 2018, pp. 20–26.

[17] S. D. Nikolopoulos and I. Polenakis, "A graph-based model for malware detection and classification using system-call groups," J. Comput. Virol. Hacking Tech., vol. 13, no. 1, pp. 29–46, 2017,

[18] P. K. Mishra and G. Tyagi, "Game Theory based Attack Graph Analysis for Cyber War Strategy".

[19] E. Doynikova and I. Kotenko, "Improvement of Attack Graphs for Cybersecurity Monitoring: Handling of Inaccuracies, Processing of Cycles, Mapping of Incidents and Automatic Countermeasure Selection," SPIIRAS Proc., vol. 2, p. 211, Apr. 2018,

[20] M. Angelini, S. Bonomi, E. Borzi, A. Del Pozzo, S. Lenti, and G. Santucci, "An Attack Graph-Based On-Line Multi-Step Attack Detector," 2018.

[21] A. Souri and R. Hosseini, "A state-of-the-art survey of malware detection approaches using data mining techniques," Human-centric Computing and Information Sciences, vol. 8, no. 1. 2018.

[22] R. Sihwail, K. Omar, and K. A. Z. Ariffin, "A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 4–2, pp. 1662–1671, 2018,

[23] S. Karandikar, M. Amin, S. Deshpande, and Y. Khalid, "Network-based malware detection." Google Patents, May 23, 2017.

[24] C. S. Veerappan, P. L. K. Keong, Z. Tang, and F. Tan, "Taxonomy on malware evasion countermeasures techniques," in IEEE World Forum on Internet of Things, WF-IoT 2018 - Proceedings, May 2018, vol. 2018-Janua, pp. 558–563.

[25] Ö. A. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," IEEE Access, vol. 8, pp. 6249–6271, 2020,

[26] M. V. Yason and Ncent, "The Art of Unpacking," Black Hat 2007, 2007. https://wikileaks.org/hbgary-emails//fileid/21224/6926

[27] Walter Kong, "Unlocking LockScreen," 2013. https://www.virusbulletin.com/virusbulletin/2013/07/unlocking-lockscreen

[28] "Overview of the Kronos banking malware rootkit," Lexi Security Hub, 2014. https://www.lexsi.com/securityhub/overview-kronos-banking-malware-rootkit/?lang=en

[29] V. L. Le, I. Welch, X. Gao, and P. Komisarczuk, "Anatomy of drive-by download attack," in Proceedings of the Eleventh Australasian Information Security Conference-Volume 138, 2013, pp. 49–58.

[30] D. Ugarte, D. Maiorca, F. Cara, and G. Giacinto, "PowerDrive: Accurate De-obfuscation and Analysis of PowerShell Malware," in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2019, pp. 240–259.

[31] Y. Oyama, "Trends of anti-analysis operations of malwares observed in API call logs," J. Comput. Virol. Hacking Tech., vol. 14, no. 1, pp. 69–85, 2018,

[32] The Cylance Threat Research Team, "threat-spotlight-satan-raas," 2017. [Online]. Available: https://threatvector.cylance.com/en_us/home/threat-spotlight-satan-raas.html

[33] B. Bencsáth, G. Pék, L. Buttyán, and M. Felegyhazi, "The cousins of stuxnet: Duqu, flame, and gauss," Futur. Internet, vol. 4, no. 4, pp. 971–1003, 2012.

[34] Arunpreet Singh and Clemens Kolbitsch, "Not so fast my friend – Using Inverted Timing Attacks to Bypass Dynamic Analysis," 2014. https://www.lastline.com/labsblog/not-so-fast-my-friend-using-inverted-timing-attacks-to-bypass-dynamic-analysis/

[35] R. Paleari, L. Martignoni, G. F. Roglia, and D. Bruschi, "A fistful of red-pills: How to automatically generate procedures to detect CPU emulators," in Proceedings of the USENIX Workshop on Offensive Technologies (WOOT), 2009, vol. 41, p. 86.

[36] M. Lindorfer, C. Kolbitsch, and P. M. Comparetti, "Detecting Environment-Sensitive Malware Diplom-Ingenieurin," in International Workshop on Recent Advances in Intrusion Detection, 2011, pp. 338–357.

[37] R. Rubira Branco, G. Negreira Barbosa, P. Drimel Neto, R. R. Branco, G. N. Barbosa, and P. D. Neto, "Scientific but Not Academical Overview of Malware Anti-Debugging, Anti-Disassembly and Anti- VM Technologies," Black Hat, 2012, [Online]. Available: internal-pdf://117.26.35.53/BH_US_12_Branco_Scientific_Academic_WP.pdf

[38] N. Falliere, L. O. Murchu, and E. L. B. Chien, "W32. stuxnet dossier," White Pap. Symantec Corp., Secur. Response, vol. 5, p. 29, 2011,

[39] D. Brumley, C. Hartwig, Z. Liang, J. Newsome, D. Song, and H. Yin, "Automatically identifying trigger-based behavior in malware," in Botnet Detection, Springer, 2008, pp. 65–88.

[40] A. Kapravelos, Y. Shoshitaishvili, M. Cova, C. Kruegel, and G. Vigna, "Revolver: An automated approach to the detection of evasive web-based malware," in Presented as part of the 22nd {USENIX} Security Symposium ({USENIX} Security 13), 2013, pp. 637–652.

[41] A. Kapravelos, M. Cova, C. Kruegel, and G. Vigna, "Escape from monkey island: Evading high-interaction honeyclients," in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2011, pp. 124–143.

[42] S. Shiva, S. Roy, and D. Dasgupta, "Game theory for cyber security," in Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, 2010, p. 34.

[43] K. W. Hipel, D. M. Kilgour, L. Fang, and X. Peng, "The decision support system GMCR II in negotiations over groundwater contamination," in IEEE SMC'99 Conference Proceedings. 1999 IEEE International Conference on Systems, Man, and Cybernetics (Cat. No. 99CH37028), 1999, vol. 5, pp. 942–948.

[44] M. Sheikhmohammady, H. Bitalebi, A. Moatti, and K. W. Hipel, "Formal Strategic Analysis of the Conflict over Syria," in Proceedings of the 2013 IEEE International Conference on Systems, Man, and Cybernetics, 2013, pp. 2442–2447.

[45] M. Sheikhmohammady, K. W. Hipel, H. Asilahijani, and D. Marc Kilgour, "Strategic analysis of the conflict over Iran's nuclear program," in Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics, 2009, pp. 1911–1916.

[46] M. Sheikhmohammadi and M. Abbasi, "Game Theory Approach to Modeling and Analyzing Inheritance Allocation of a Passed-away Couple," Econ. Model., vol. 10, no. 33, pp. 23–48, 2016.

[47] R. A. Kinsara, O. Petersons, K. W. Hipel, and D. M. Kilgour, "Advanced Decision Support for the Graph Model for Conflict Resolution," J. Decis. Syst., vol. 24, no. 2, pp. 117–145, 2015,

[48] M. A. Bashar, K. W. Hipel, D. M. Kilgour, and A. Obeidi, "Interval Fuzzy Preferences in the Graph Model for Conflict Resolution," Fuzzy Optim. Decis. Mak., vol. 17, no. 3, pp. 287–315, Sep. 2018,

[49] S. He, K. W. Hipel, H. Xu, and Y. Chen, "A Two-Level Hierarchical Graph Model for Conflict Resolution with Application to International Climate Change Negotiations," J. Syst. Sci. Syst. Eng., vol. 29, no. 3, pp. 251–272, Jun. 2020,

[50] S. He, D. M. Kilgour, and K. W. Hipel, "A Three-Level Hierarchical Graph Model for Conflict Resolution," IEEE Trans. Syst. Man, Cybern. Syst., pp. 1–10, 2019,

[51] Y. Huang, B. Ge, B. Zhao, and K. Yang, "Course of Action Generation Using Graph Model for Conflict Resolution," in 2020 IEEE 15th International Conference of System of Systems Engineering (SoSE), 2020, pp. 249–254.

[52] K. W. Hipel, L. Fang, and D. M. Kilgour, "The Graph Model for Conflict Resolution: Reflections on Three Decades of Development," Gr. Decis. Negot., vol. 29, no. 1, pp. 11–60, 2020,

[53] RealWorldCyberSecurity, "Negative Rings in Intel Architecture: The Security Threats That You've Probably Never Heard Of." https://medium.com/swlh/negative-rings-in-intel-architecture-the-security-threats-youve-probably-never-heard-of-d725a4b6f831 (accessed Jun. 22, 2021).

[54] D. Reference, "Report on AES implementation with speed and side channel immunity improvements," no. 783163, 2021.

[55] O. Or-Meir, N. Nissim, Y. Elovici, and L. Rokach, "Dynamic Malware Analysis in the Modern Era—A State of the Art Survey," ACM Comput. Surv., vol. 52, no. 5, Sep. 2019,

[56] D. Javaheri and M. Hosseinzadeh, "A Framework for Recognition and Confronting of Obfuscated Malwares Based on Memory Dumping and Filter Drivers," Wirel. Pers. Commun., vol. 98, no. 1, pp. 119–137, 2018,

[57] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," IEEE Secur. Priv., vol. 4, no. 6, pp. 85–89, 2006.

[58] M. Keramati, "A Security Model Based Approach for Dynamic Risk Assessment of Multi-Step Attacks in Computer Networks," Electron. Cyber Def., vol. 9, no. 1, pp. 157–173, 2021.

[59] A. Singh, "Malware Evasion Techniques: Same Wolf – Different Clothing," 2017. https://www.lastline.com/labsblog/malware-evasion-techniques/

[60] D. Kirat, G. Vigna, and C. Kruegel, "Barecloud: bare-metal analysis-based evasive malware detection," in 23rd {USENIX} Security Symposium ({USENIX} Security 14), 2014, pp. 287–301.

پیوست‌ها:

جدول (۱ پیوست): روابط پایه‌ای انتخاب گزینه‌های تاثیرگذار بازیگران

ردیف	تعریف و ویژگی‌های روابط
۱	$P = \{At, Df\}, \quad At = Attacker, \quad Df = Defender, \quad p \in P$
۲	$Y_p = \begin{cases} sizeof(B_{At}) \ \ if\ P = At \\ sizeof(B_{Df}) \ \ if\ P = Df \end{cases}, \quad y = Y_p$
۳	$Psets = \left\{ \bigcup_{x \in Psets} x \middle\| \begin{matrix} x^k(p) == p \ and \ x \in PB(U_B) \\ ,0 \le k \le sizeof(Psets) \end{matrix} \right\}$ $Pset^{p,y} = \left\{ \bigcup_{x \in Psets} x \middle\| \begin{matrix} x_y^k(p) == p \\ ,0 \le k \le sizeof(Psets) \end{matrix} \right\}$ $Ptypes = \{Requ, Optional, Notneed\}, Pty \in Ptypes$ $Pset_{Pty}^{p,y} = \left\{ \bigcup_{x \in Psets} x \middle\| \begin{matrix} if\ Pty == Requ\ then\ \ x_y^k(p)\ must\ be\ 1 \\ if\ Pty == Optional\ then\ \ x_y^k(p)\ must\ be\ 0 \\ if\ Pty == Notneed\ then\ \ x_y^k(p)\ must\ be\ -1 \\ ,0 \le k \le sizeof(Psets) \end{matrix} \right\}$
۴	$Puty = \{Low, Equ, High\}, Uty \in Puty$ $Cnt_y^p = \left\{ \bigcup_{x \in U_{\bar{B}}} x \middle\| x_y^k(p) \ne 0, 0 \le k \le sizeof(U_{\bar{B}}) \right\}$ $Cnt_{Uty}^p = \left\{ \cup_{x \in U_{\bar{B}}} x \middle\| \begin{matrix} if\ (p = At\ And\ Uty = low)\ then\ P_{At}^B(k) < P_{Df}^B(k) \\ if\ (p = At\ And\ Uty = High)\ then\ P_{At}^B(k) > P_{Df}^B(k) \\ if\ Uty = Equ\ then\ P_{Df}^B(k) = P_{At}^B(k) \\ if\ (p = Df\ And\ Uty = low)\ then\ P_{Df}^B(k) < P_{At}^B(k) \\ if\ (p = Df\ And\ Uty = High)\ then\ P_{Df}^B(k) > P_{At}^B(k) \\ ,0 \le k \le sizeof(U_{\bar{B}}) \end{matrix} \right\} s$ $Cnt_{Uty}^{p,y} = \left\{ \bigcup_{x \in U_{\bar{B}}} x \middle\| \begin{matrix} if\ (p = At\ And\ Uty = low)\ then\ P_{At}^B(k) < P_{Df}^B(k) \\ if\ (p = At\ And\ Uty = High)\ then\ P_{At}^B(k) > P_{Df}^B(k) \\ if\ Uty = Equ\ then\ P_{Df}^B(k) = P_{At}^B(k) \\ if\ (p = Df\ And\ Uty = low)\ then\ P_{Df}^B(k) < P_{At}^B(k) \\ if\ (p = Df\ And\ Uty = High)\ then\ P_{Df}^B(k) > P_{At}^B(k) \\ x_y^k(p) \ne 0, 0 \le k \le sizeof(U_{\bar{B}}) \end{matrix} \right\}$
۵	$Stb_N^{p,y} = \left\{ \bigcup x \middle\| x \in ST_N^p, x_y^k(p) \ne 0, 0 \le k \le sizeof(U_{\bar{B}}) \right\}$ $Stb_N^p = \left\{ \bigcup x \middle\| x \in ST_N^p, x^k(p) \ne 0, 0 \le k \le sizeof(U_{\bar{B}}) \right\}$
۶	$Eqtype = \{Nash, SEQ, GMR, SMR, Best\}, Eq \in Eqtype,$ $EQ_{Eq}^{p,y} = \left\{ \bigcup x \middle\| x \in EQ_{Eq}^{U_{\bar{B}}}, x_y^k(p) \ne 0, 0 \le k \le sizeof(U_{\bar{B}}) \right\}$ $EQ_{Eq}^p = \left\{ \bigcup x \middle\| x \in EQ_{Eq}^{U_{\bar{B}}}, x^k(p) \ne 0, 0 \le k \le sizeof(U_{\bar{B}}) \right\}$
۷	$Max_i^{p,y} = \left\{ \bigcup_{y \in B_p} y \middle\| m_i^p(y) \ge 0.95 * max(M_i^p) \right\}$

جدول (۲ پیوست): روابط معیارهای تعیین گزینه‌های تاثیرگذار بازیگران در بازی

شماره معیار اصلی	شماره معیار فرعی	نحوه محاسبه معیار
۱	۱	$M_1^P = \left\{ \bigcup_{y=0}^{Y_p} m_1^p(y) \middle\| m_1^p(y) = U_P^B(y) \right\}$
	۲	$M_2^P = \left\{ \bigcup_{y=0}^{Y_p} m_2^p(y) \middle\| m_2^p(y) = \left(U_P^B(y) / \sum m_1^p(y) \right) * 100 \right\}$
۲	۳	$M_3^p = \left\{ \bigcup_{y=0}^{Y_p} m_3^p(y) \middle\| m_3^p(y) = sizeof\left(Pset_{Requ}^{p,y} \right) \right\}$
	۴	$M_4^p = \left\{ \bigcup_{y=0}^{Y_p} m_4^p(y) \middle\| m_4^p(y) = (M_3^p / sizeof(Pset^{p,y}) * 100) \right\}$
	۵	$M_5^p = \left\{ \bigcup_{y=0}^{Y_p} m_5^p(y) \middle\| m_5^p(y) = (M_3^p / sizeof(Psets) * 100) \right\}$
	۶	$M_6^p = \left\{ \bigcup_{y=0}^{Y_p} m_6^p(y) \middle\| m_6^p(y) = ((M_4^p + M_5^p)/2) * 100) \right\}$
۳	۷	$M_7^p = \left\{ \bigcup_{y=0}^{Y_p} m_7^p(y) \middle\| m_7^p(y) = sizeof\left(Pset_{Notneed}^{p,y} \right) \right\}$
	۸	$M_8^p = \left\{ \bigcup_{y=0}^{Y_p} m_8^p(y) \middle\| m_8^p(y) = (M_7^p / sizeof(Pset^{p,y}) * 100) \right\}$
	۹	$M_9^p = \left\{ \bigcup_{y=0}^{Y_p} m_9^p(y) \middle\| m_9^p(y) = (M_7^p / sizeof(Psets) * 100) \right\}$
	۱۰	$M_{10}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{10}^p(y) \middle\| m_{10}^p(y) = ((M_8^p + M_9^p)/2) * 100) \right\}$
۴	۱۱	$M_{11}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{11}^p(y) \middle\| m_{11}^p(y) = ((M_6^p + M_{10}^p)/2) * 100) \right\}$
۵	۱۲	$M_{12}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{12}^p(y) \middle\| m_{12}^p(y) = sizeof\left(Cnt_y^p \right) \right\}$
	۱۳	$M_{13}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{13}^p(y) \middle\| m_{13}^p(y) = (m_{12}^p(y) / sizeof(U_B)) * 100 \right\}$
۶	۱۴	$M_{14}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{14}^p(y) \middle\| m_{14}^p(y) = sizeof\left(Cnt_{Low}^{p,y} \right) \right\}$
	۱۵	$M_{15}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{15}^p(y) \middle\| m_{15}^p(y) = (m_{14}^p(y) / m_{12}^p(y)) * 100 \right\}$
	۱۶	$M_{16}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{16}^p(y) \middle\| m_{16}^p(y) = \left(m_{14}^p(y) / sizeof\left(Cnt_{Low}^p \right) \right) * 100 \right\}$
	۱۷	$M_{17}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{17}^p(y) \middle\| m_{17}^p(y) = ((M_{15}^p + M_{16}^p)/2) * 100) \right\}$
۷	۱۸	$M_{18}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{18}^p(y) \middle\| m_{18}^p(y) = sizeof\left(Cnt_{Equ}^{p,y} \right) \right\}$
	۱۹	$M_{19}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{19}^p(y) \middle\| m_{19}^p(y) = \left(m_{18}^p(y) / m_{12}^p(y) \right) * 100 \right\}$
	۲۰	$M_{20}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{20}^p(y) \middle\| m_{20}^p(y) = \left(m_{18}^p(y) / sizeof\left(Cnt_{Equ}^p \right) \right) * 100 \right\}$
	۲۱	$M_{21}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{21}^p(y) \middle\| m_{21}^p(y) = ((M_{20}^p + M_{19}^p)/2) * 100) \right\}$
۸	۲۲	$M_{22}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{22}^p(y) \middle\| m_{22}^p(y) = sizeof\left(Cnt_{High}^{p,y} \right) \right\}$
	۲۳	$M_{23}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{23}^p(y) \middle\| m_{23}^p(y) = (m_{22}^p(y) / m_{12}^p(y)) * 100 \right\}$
	۲۴	$M_{24}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{24}^p(y) \middle\| m_{24}^p(y) = \left(m_{22}^p(y) / sizeof\left(Cnt_{High}^p \right) \right) * 100 \right\}$
	۲۵	$M_{25}^p = \left\{ \bigcup_{y=0}^{Y_p} m_{25}^p(y) \middle\| m_{25}^p(y) = ((M_{23}^p + M_{24}^p)/2) * 100) \right\}$

ادامه جدول (۲ پیوست): روابط معیارهای تعیین گزینه‌های تاثیرگذار بازیگران در بازی

۹	۲۶	$M_{26}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{26}^{p}(y)\ \middle\vert\ m_{26}^{p}(y)=sizeof(Stb_N^{p,y})\right\}$
	۲۷	$M_{27}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{27}^{p}(y)\ \middle\vert\ m_{27}^{p}(y)=\left(m_{26}^{p}(y)/m_{12}^{p}(y)\right)*100\right\}$
	۲۸	$M_{28}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{28}^{p}(y)\ \middle\vert\ m_{28}^{p}(y)=\left(m_{26}^{p}(y)/sizeof(Stb_N^{p})\right)*100\right\}$
	۲۹	$M_{29}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{29}^{p}(y)\ \middle\vert\ m_{29}^{p}(y)=((M_{27}^{p}+M_{28}^{p})/2)*100)\right\}$
۱۰	۳۰	$M_{30}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{30}^{p}(y)\ \middle\vert\ m_{30}^{p}(y)=sizeof\left(EQ_{Nash}^{p,y}\right)\right\}$
	۳۱	$M_{31}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{31}^{p}(y)\ \middle\vert\ m_{31}^{p}(y)=\left(m_{30}^{p}(y)/m_{12}^{p}(y)\right)*100\right\}$
	۳۲	$M_{32}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{32}^{p}(y)\ \middle\vert\ m_{32}^{p}(y)=\left(m_{30}^{p}(y)/sizeof\left(EQ_{Nash}^{p}\right)\right)*100\right\}$
	۳۳	$M_{33}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{33}^{p}(y)\ \middle\vert\ m_{33}^{p}(y)=((M_{31}^{p}+M_{32}^{p})/2)*100)\right\}$
۱۱	۳۴	$M_{34}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{34}^{p}(y)\ \middle\vert\ m_{34}^{p}(y)=sizeof\left(EQ_{SEQ}^{p,y}\right)\right\}$
	۳۵	$M_{35}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{35}^{p}(y)\ \middle\vert\ m_{35}^{p}(y)=\left(m_{34}^{p}(y)/m_{12}^{p}(y)\right)*100\right\}$
	۳۶	$M_{36}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{36}^{p}(y)\ \middle\vert\ m_{36}^{p}(y)=\left(m_{34}^{p}(y)/sizeof\left(EQ_{SEQ}^{p}\right)\right)*100\right\}$
	۳۷	$M_{37}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{37}^{p}(y)\ \middle\vert\ m_{37}^{p}(y)=((M_{35}^{p}+M_{36}^{p})/2)*100\right\}$
۱۲	۳۸	$M_{38}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{38}^{p}(y)\ \middle\vert\ m_{38}^{p}(y)=sizeof\left(EQ_{GMR}^{p,y}\right)\right\}$
	۳۹	$M_{39}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{39}^{p}(y)\ \middle\vert\ m_{39}^{p}(y)=\left(m_{38}^{p}(y)/m_{12}^{p}(y)\right)*100\right\}$
	۴۰	$M_{40}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{40}^{p}(y)\ \middle\vert\ m_{40}^{p}(y)=\left(m_{38}^{p}(y)/sizeof\left(EQ_{GMR}^{p}\right)\right)*100\right\}$
	۴۱	$M_{41}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{41}^{p}(y)\ \middle\vert\ m_{41}^{p}(y)=((M_{39}^{p}+M_{40}^{p})/2)*100\right\}$
۱۳	۴۲	$M_{42}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{42}^{p}(y)\ \middle\vert\ m_{42}^{p}(y)=sizeof\left(EQ_{SMR}^{p,y}\right)\right\}$
	۴۳	$M_{43}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{43}^{p}(y)\ \middle\vert\ m_{43}^{p}(y)=(m_{42}^{p}(y)/m_{12}^{p}(y))*100\right\}$
	۴۴	$M_{44}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{44}^{p}(y)\ \middle\vert\ m_{44}^{p}(y)=\left(m_{42}^{p}(y)/sizeof\left(EQ_{SMR}^{p}\right)\right)*100\right\}$
	۴۵	$M_{45}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{45}^{p}(y)\ \middle\vert\ m_{45}^{p}(y)=((M_{43}^{p}+M_{44}^{p})/2)*100\right\}$
۱۴	۴۶	$M_{46}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{46}^{p}(y)\ \middle\vert\ m_{46}^{p}(y)=\left(m_{31}^{p}(y)+m_{35}^{p}(y)+m_{39}^{p}(y)+m_{43}^{p}(y)\right)/4\right\}$
	۴۷	$M_{47}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{47}^{p}(y)\ \middle\vert\ m_{47}^{p}(y)=\left(m_{32}^{p}(y)+m_{36}^{p}(y)+m_{40}^{p}(y)+m_{44}^{p}(y)\right)/4\right\}$
	۴۸	$M_{48}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{48}^{p}(y)\ \middle\vert\ m_{48}^{p}(y)=\left(m_{33}^{p}(y)+m_{37}^{p}(y)+m_{41}^{p}(y)+m_{45}^{p}(y)\right)/4\right\}$
۱۵	۴۹	$M_{49}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{49}^{p}(y)\ \middle\vert\ m_{49}^{p}(y)=sizeof\left(EQ_{Best}^{p,y}\right)\right\}$
	۵۰	$M_{50}^{p}=\left\{\bigcup_{y=0}^{Y_p} m_{50}^{p}(y)\ \middle\vert\ m_{50}^{p}(y)=\left(m_{49}^{p}(y)/\sum m_{49}^{p}(y)\right)*100\right\}$