Electronic & Cyber Defense
Vol. 14, No.1, 2026 (Serial No. 35) .pp.35-52
ISSN: 2322-4347, E-ISSN: 2980-8979

Investigating and feasibility of cyber war game using game theory

R. Roohi-Seraji[1] , N.Doustimotlagh[2*]

[1] Researcher, Supreme National Defense university, Tehran, Iran. *rroohi@iasbs.ac.ir*

[2] Assistant Professor, Supreme National Defense University, Tehran, Iran (*Correspondence: *doustimotlagh@chmail.ir*)

ARTICLE INFO

Article history:

Article Type: Research paper

Received: 07 January 2026

Revised: 15 February 2026

Accepted: 27 February 2026

Available online: 07 April 2026

Keywords:

Cyber Wargame

Game Theory

ynamic Cyber Wargame

Nash Equilibrium Point

Cyber Security

ABSTRACT

This paper focuses on the study of cybersecurity based on a cyberwar game by proposing a dynamic attack-defense algorithm for the interaction between attackers and defenders, where both parties are intelligent and dynamically adjust their attack or defense strategies according to the opponent's actions to achieve victory. The phenomenon of "cyberwar" exists in most real-world cybersecurity incidents, which requires special research and analysis. First, a theoretical framework of a zero-sum non-cooperative dynamic game is reviewed for data analysis, and then several different modes are generalized and examined, and finally a simulated scenario is presented based on it, and the results are analyzed in terms of the success rate of defense and the energy of the entire system. The decisions of attackers/defenders to have different attack/defense levels based on cost or benefit are modeled. An attempt is made to generalize the initial idea, and a three-sided dynamic cyberwar game is examined. A dynamic threshold cyberwar game (T,p) is presented. Finally, a cyberattack scenario on the infrastructure of the Ministry of Roads is addressed and the effectiveness of the proposed model is reported.

Cite this article: Roohi-Seraji, R., Doustimotlagh, N. (2026). Investigating and feasibility of cyber war game using game theory. *Electronic and Cyber Defense*,14(1),35-52.2026.

DOI: https://dor.isc.ac/dor/20.1001.1.23224347.1405.14.1.3.5

Publisher: Imam Hossein University.

«پدافند الکترونیک و سایبری»
سال چهاردهم، شماره ۱، بهار ۱۴۰۵؛ ص ۵۲-۳۵
شاپا الکترونیکی: ۸۹۷۹-۲۹۸۰ شاپا چاپی: ۴۳۴۷-۲۳۲۲

بررسی و امکان‌سنجی بازی جنگ سایبری با استفاده از نظریه بازی‌ها

رضا روحی سراجی[۱]، نصیب الله دوستی مطلق[۲*]

[۱] پژوهشگر، دانشگاه عالی دفاع ملی، تهران ، ایران.*rroohi@iasbs.ac.ir*

۲ استادیار، دانشگاه عالی دفاع ملی، تهران، ایران (نویسنده مسئول: *doustimotlagh@chmail.ir*)

چکیده

این مقاله به امنیت سایبری از دریچه بازی‌های جنگ سایبری می‌پردازد و یک الگوریتم دفاع - حمله با تعامل پویا را بین مهاجمان و مدافعان هوشمند پیشنهاد می‌کند. در این رویکرد، هر دو طرف به‌صورت پویا استراتژی‌های خود را بر اساس اقدامات حریف تنظیم می‌کنند تا به پیروزی دست یابند. باتوجه‌به وجود پدیده «جنگ سایبری» در اغلب حوادث واقعی امنیت سایبری، ابتدا یک چارچوب نظری بازی پویا غیر همکاری مجموع صفر برای تحلیل این تعاملات بررسی می‌شود. مدل‌سازی بر اساس هزینه یا سود تصمیمات مهاجمان/مدافعان برای اعمال سطوح مختلف حمله/دفاع صورت می‌گیرد. ایده اولیه تعمیم داده شده و حالت‌های پیچیده‌تری از جمله بازی جنگ سایبری پویای سه‌جانبه و بازی جنگ سایبری پویای آستانه‌ای (T,p) مورد بررسی قرار می‌گیرند. همچنین برای سنجش اثربخشی، یک سناریوی شبیه‌سازی بر مبنای مدل‌های پیشنهادی ارائه شده و نتایج شبیه‌سازی بر اساس معیارهایی چون نرخ موفقیت در دفاع و میزان انرژی کل سیستم تحلیل می‌گردد. در نهایت، اثربخشی مدل پیشنهادی با استفاده از یک سناریوی حمله سایبری به زیرساخت‌های وزارت راه مورد سنجش و گزارش قرار می‌گیرد.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۴/۱۰/۱۷

بازنگری: ۱۴۰۴/۱۱/۲۶

پذیرش: ۱۴۰۴/۱۲/۰۸

ارائه آنلاین: ۱۴۰۵/۰۱/۱۸

کلید واژه ها:

بازی جنگ سایبری

نظریه بازی‌ها

بازی جنگ سایبری پویا

نقطه تعادل نش

امنیت سایبری

استناد: روحی سراجی، رضا، دوستی مطلق، نصیب الله. (۱۴۰۵). بررسی و امکان‌سنجی بازی جنگ سایبری با استفاده از نظریه بازی‌ها. *پدافند الکترونیکی و سایبری*، ۱۴(۱)، ۵۲-۳۵.DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1405.14.1.3.5

ناشر: دانشگاه جامع امام حسین(ع)

۱. مقدمه

امروزه دنیا شاهد عصری از حملات سایبری بی‌سابقه است. اطمینان از سه عامل مهم محرمانه بودن، یکپارچگی و دردسترس‌بودن (CIA[1]) داده‌ها، بسیار حیاتی است. این موضوع در محیط‌های با منابع محدود انرژی، محاسبات و منابع ارتباطی، عاملی تعیین‌کننده و چالش‌برانگیزتر می‌شود.

اکثر تحقیقات دانشگاهی معمولاً بر روی یک مدل ایستا با یک حمله یا دفاع خاص بدون درنظرگرفتن شدت حمله، شرایط محیطی و تعاملات میان مهاجمان و مدافعان ارائه می‌شود؛ بنابراین، برای یافتن عملکرد دفاعی مناسب طراحی یک الگوریتم دفاعی با سیستمی پویا همراه راهبُردها مختلف، درخور اهمیت است. هدف از این تحقیق مطالعه نمونه‌های قبل و ارتقا مدل‌های قبلی و طراحی یک چارچوب بازی جنگ سایبری است که ریشه در نظریه بازی‌ها دارد که کنش‌های پویا بین مهاجمان و مدافعان را در نظر می‌گیرد.

سازوکاری دفاعی در برابر چندین نوع حمله در شبکه‌ها معرفی می‌شود. سازوکاری دفاعی که محدودیت منابع و همچنین ارزش امنیتی دارایی شبکه را در نظر می‌گیرد موردمطالعه قرار می‌گیرد. این مدل بر اساس شدت حملات و هزینه نسبی برای راه‌اندازی آن‌ها، پاسخ‌های مناسبی را برای یک مدافع ارائه می‌دهد. یک بازی مهاجم - مدافع مجموع صفر غیر همکاری ارائه می‌شود.

به‌طورکلی، حمله یا دفاع به سه دسته طبقه‌بندی می‌شود: سطح صفر، سطح یک و سطح دو. مهاجم می‌تواند بین این سه استراتژی به طور متناوب تغییر کند، سطح صفر نشان‌دهنده عدم حمله، سطح یک نشان‌دهنده شدت کم حمله و سطح دو نشان‌دهنده شدت حمله بالا است. به همین ترتیب، اقدامات مدافع نیز در سه سطح دفاعی متناظر طبقه‌بندی می‌شود که سطوح بالاتر دفاع به محاسبات، توان باتری یا حافظه بیش‌تری نیاز دارد، اما شانس موفقیت بیش‌تری در برابر حملات به دست می‌آورد. لازم به ذکر است در بخش بهبود نتایج سعی بر آن است که یکی از مدل‌های مدنظر برای بهبود عملکرد الگوریتم پیشنهادی، افزایش سطوح در حمله و متعاقباً دفاع باشد.

ساختار مقاله در ادامه بدین صورت است. در بخش ۲ کارهای مرتبط بیان شده است. در بخش ۳ مدل بازی جنگ سایبری دوجانبه پویا توضیح داده شده است. در بخش بعدی یعنی بخش ۴ سعی شده است تا مدلی پیچیده‌تر، یعنی بازی جنگ سایبری سه‌جانبه پویا با دخالت یک عامل سوم خارجی مورد بررسی قرار گیرد و نتایج با مدل قبل مقایسه شود. در بخش ۵ نیز سعی شده است تا نوع دیگری از مدل بازی جنگ سایبری پویا با آستانه (T,p) ارائه و بررسی شود.

در بخش ۶ به تحلیل شبیه‌سازی‌های رایانه‌ای و در بخش ۷ نیز به ارزیابی عملکرد مدل پیشنهادی بر اساس یک سناریو سایبر محور مرتبط با وزارت راه و شهرسازی جمهوری اسلامی ایران و تبیین الگوریتم برنامه‌نویسی مربوطه پرداخته می‌شود. بخش‌های ۸ و ۹ به نتایج بحث و مقایسه می‌پردازد. نهایتاً در بخش ۱۰ به نتیجه حاصل پرداخته می‌شود.

۲. کارهای مرتبط

۲-۱. تاریخچه‌ای از کارهای پیشین

مشکلات در حوزه سایبری را می‌توان از طریق روش‌های برآمده از نظریه بازی‌ها به‌منظور کنترل و خنثی‌کردن تهدیدات آینده بررسی کرد. استفاده از نظریه بازی‌ها در امنیت سایبری از جمله شبکه‌های ارتباطی را می‌توان در [۳-۱] مشاهده کرد. به‌خصوص در شبکه و برنامه‌های تلفن همراه توسط [۴]، دفاع در برابر حملات انکار سرویس در شبکه و یک راه‌حل دفاعی مبتنی بر جورچین در [۵] و رویکرد بازی بیزی برای تشخیص نفوذ در شبکه‌های بی‌سیم در [۶]. مفهوم تعادل نش در هر دو سناریو ایستا و پویا استفاده می‌شود. یک بازیکن می‌تواند یک گره مخرب یا معمولی باشد. در [۷]، یک پروتکل مسیریابی امن با مدل‌سازی تعامل گره‌ها در شبکه‌های حسگر بی‌سیم[2] و سیستم تشخیص نفوذ به‌عنوان یک فرمول بازی بیزی پیشنهاد شده است. برخلاف اکثر سازوکارهای امنیتی که بر یک حمله یا دفاع خاص تمرکز می‌کنند، در این کار یک سیستم دفاعی پویا ارائه می‌شود که تنوع در شدت حمله و دفاع را در نظر می‌گیرد.

۲-۲. توصیف بازی غیر همکاری

در این بخش بازی امنیتی به‌عنوان یک بازی مجموع صفر غیر همکاری فرموله می‌شود. علاوه بر این، راهبُردها نیز توصیف می‌شوند. مهاجم برای بهترین کنش رقابت می‌کند و هدف او به حداکثر رساندن سودمندی خود است؛ بنابراین، حریفان ملزم به همکاری با یکدیگر نیستند. در مقابل، مدافع همچنین دوست دارد یک استراتژی مناسب برای به حداکثر رساندن شانس محافظت خود در برابر حریفان بدون صرف انرژی یا محاسبات بیش از حد اتخاذ کند.

در اکثر مدل‌سازی‌های قبلی بر اساس نظریه بازی‌ها که می‌توان نمونه‌هایی از آن‌ها را در [۲-۱] و [۴] مشاهده کرد، مهاجمان و مدافعان را تنها با دو استراتژی، مدل می‌کردند. به‌منظور ارائه مدلی کاراتر و گسترده‌تر سعی بر آن شده تا طرفین بازی استراتژی‌های حمله/دفاع خود را با شدت‌های مختلف به صورتی پویا تنظیم کنند.

مهاجمان و مدافعان برای دستیابی به موفقیت، نسبت هزینه به سود متفاوتی را محاسبه می‌کنند؛ بنابراین، هر طرف بازی به جای‌داشتن تنها دو سطح (صفر یا یک)، دارای سطوح مختلف استراتژی هستند.

[1]. Confidentiality, Integrity and Availability

[2]. Wireless Sensor Networks

۲-۳. روش تحقیق

ابتدا سعی بر آن شد که با استفاده از بنیان‌های نظری موجود در نظریه بازی‌ها به شرح بازی جنگ سایبری دوجانبه پویا پرداخته شود. بعد با رعایت اصول و بنیان کارهای قبل به توسعه دیدگاه اولیه و بهبود مدل قبل و از دید نظری و شبیه‌سازی‌های رایانه‌ای به بازی جنگ سایبری سه‌جانبه پویا و بازی جنگ سایبری با آستانه (T, p) پرداخته شود.

نتایج بسیار رضایت‌بخش و ملموس بود. بعد به پیاده‌سازی مدل پیشنهادی بازی جنگ سایبری دوجانبه به وسیله‌ی نمونه‌ای داخلی پرداخته شد و نتایج منطبق بر اصول بحث شده که بر کارایی مدل پیشنهادی تأکید داشت، گزارش شدند.

۳. مدل بازی جنگ سایبری دوجانبه

یک بازی دونفره غیر همکاری مجموع صفر

$$G =< (N), (S), (U) >$$

ارائه می‌شود که در آن دو بازیکن مهاجم و مدافع $N=\{A,D\}$ هستند: بازیکن A گره حمله‌کننده و بازیکن دیگر D مدافع در نظر گرفته می‌شود. $S = \{a_r, d_r | r \in \{0, 1, 2\}\}$ فضای استراتژی است که مجموعه اقداماتی است که برای هر بازیکن در دسترس است و ابزارهای آن‌ها توسط U به آن‌ها نسبت داده می‌شود.

برای مهاجم، سطح صفر یعنی حمله نکند، a_0 =*no-Attack*، سطح یک یعنی شدت کم حمله، a_1 =*Attack-1*. و سطح دو شدت حمله بالا است که با a_2 =*Attack-2* نشان داده می‌شود. به‌طورکلی، از دید مهاجم در مقایسه با استراتژی *Attack-1*، استراتژی *Attack-2* در ایجاد حمله موفق مؤثرتر است، اما برای اجرای حمله منابع یا هزینه بیش‌تری را می‌طلبد. به همین ترتیب، برای مدافع d_0 = *No-Defend*، d_1=*Defend-1* و d_2 =*Defend-2* در نظر گرفته می‌شود.

فرض می‌شود که ارزش دارایی‌های محافظت شده توسط مدافع D برابر با ω_n باشد، جایی که $\omega_n > 0$ و $n \in \{1,2\}$ است. ω_1 ارزش دارایی است که توسط استراتژی *Attack-1* و ω_2 ارزش دارایی‌هایی است که توسط استراتژی *Attack-2* به خطر افتاده است. باتوجه‌به بازی حاصل‌جمع صفر، ω_n سود مهاجم است درصورتی‌که استراتژی او *Attack-n* موفقیت‌آمیز باشد و $-\omega_n$ نشان‌دهنده از دست‌دادن مدافع است. مقدار این آسیب با معیارهایی چون میزان اتلاف انرژی، از دست‌دادن یکپارچگی داده‌ها و تعداد گره‌های در معرض خطر و غیره، تعیین می‌شود.

برای مهاجم: c_{a1} هزینه به‌کارگیری استراتژی *Attack-1* و c_{a2} هزینه به‌کارگیری استراتژی *Attack-2* است. به همین ترتیب، برای مدافع: c_{d1} هزینه به‌کارگیری استراتژی *Defend-1* و c_{d2} هزینه استقرار استراتژی *Defend-2* است.

۱-۳. مفروضات بازی جنگ سایبری دوجانبه پویا

مفروضات زیر برای مدل استراتژی حمله / دفاع سه سطحی پیشنهادی ارائه می‌شود:

- ارزش دارایی‌های امنیتی همیشه بیش‌تر از هزینه دفاع یا حمله به آن‌ها است، زیرا در غیر این صورت مدافع یا مهاجم به ترتیب انگیزه‌ای برای دفاع یا حمله ندارند. به عبارتی، برای $n \in \{1,2\}$ داریم $\omega_n > c_{an}, c_{dn}$.
- هزینه استراتژی a_1 کم‌تر از هزینه استراتژی a_2 است. چون a_2 یک استراتژی تهاجمی‌تر و مؤثرتر از a_1 است و مستلزم تلاش و هزینه بیش‌تر. (یعنی $c_{a1} < c_{a2}$).
- هزینه استراتژی دفاعی d_1 کم‌تر از هزینه استراتژی d_2 برای مدافع است. باز هم به این دلیل که d_2 یک استراتژی دفاعی مؤثرتر از d_1 است. (یعنی $c_{a1} < c_{d2}$).
- به‌طورکلی، بر اساس تعریف ω_n در بخش قبلی می‌توان فرض کرد که ($\omega_2 \geq \omega_1$). جدول (۱) ماتریس بازده بازی را به شکل استراتژیک نشان می‌دهد.

جدول (۱). شکل استراتژیک بازی پویای دوجانبه حمله - دفاع

	d_0	d_1	d_2
a_0	*0, 0*	$c_{d1}, -c_{d1}$	$c_{d2}, -c_{d2}$
a_1	$\omega_1 - c_{a1}$, $c_{a1} - \omega_1$	$c_{d1} - c_{a1}$, $c_{a1} - c_{d1}$	$c_{d2} - c_{a1}$, $c_{a1} - c_{d2}$
a_2	$\omega_2 - c_{a2}$, $c_{a2} - \omega_2$	$\omega_2 + c_{d1} - c_{a2}$, $c_{a2} - c_{d1} - \omega_2$	$c_{d2} - c_{a2}$, $c_{a2} - c_{d2}$

فرضیات زیر در مورد نتایج بازی در نظر گرفته می‌شوند:

- حمله تحت این سناریوها موفقیت‌آمیز است: برای *Attack-1* در مقابل *No-Defend* و *Attack-2* در مقابل *Defend-1* یا *No-Defend*.
- دفاع در این سناریوها موفق است: *Defend-1* در مقابل *Attack-1* یا *No-Attack* و *Defend-2* در مقابل *Attack-2* یا *Attack-1* یا *No-Attack*.
- وقتی هیچ حمله‌ای وجود ندارد و هیچ دفاعی به کار نمی‌رود، یعنی بدون حمله در مقابل بدون دفاع، سود یا ضرر صفر است.

۲-۳. نقطه تعادل نش

می‌توان نشان داد هیچ جفت استراتژی قطعی وجود ندارد که برای هر دو بازیکن کار کند؛ بنابراین، استراتژی مختلط تعادل نش[1] *(MSNE)* برای مدل پیشنهادی استفاده می‌شود.

[1]. Mixed Strategy Nash Equilibrium

تعریف ۱:

استراتژی مختلط تعادل نش برای یک بازی امنیتی، به‌صورت توزیع احتمال $\hat{p}$ بر روی مجموعه استراتژی‌های خالص S برای هر بازیکن است به‌طوری که:

فرض کنید p_{a0} احتمال بازی استراتژی a_0، p_{a1} احتمال بازی استراتژی a_1، و $p_{a2} = 1 - p_{a0} - p_{a1}$ احتمال بازی استراتژی a_2 برای مهاجم باشد. به همین ترتیب، برای مدافع نیز p_{d0} احتمال بازی استراتژی d_0، p_{d1} احتمال بازی استراتژی d_1، و $p_{d2} = 1 - p_{d0} - p_{d1}$ احتمال بازی استراتژی d_2 باشد.

طبق تعریف *MSNE*، با برابر کردن بازده موردانتظار، طرفین در مورد انتخاب استراتژی‌های خود بی‌تفاوت می‌شوند؛ بنابراین سود موردانتظار از بازی استراتژی‌های a_0، a_1 و a_2 برای مهاجم و استراتژی‌های d_0، d_1، و d_2 برای مدافع برابر در نظر گرفته می‌شود. یعنی:

$$EU(p_{a0}) = EU(p_{a1}) = EU(p_{a2})$$
$$EU(p_{d0}) = EU(p_{d1}) = EU(p_{d2})$$

سپس، از جدول (۱)، ابزار موردانتظار مهاجم برای بازی استراتژی a_0، a_1 و a_2 به‌عنوان تابعی از استراتژی ترکیبی به دست می‌آید که همانند [۲۲] توزیع احتمال p_{d0}، p_{d1} و p_{d2} برای مدافع حاصل می‌شود:

$$p_{d0} = \frac{c_{a1}}{\omega_1}, \quad p_{d1} = \frac{c_{a2}}{\omega_2} - \frac{c_{a1}}{\omega_1}, \quad p_{d2} = 1 - \frac{c_{a2}}{\omega_2} \qquad (۱)$$

به طور مشابه، سود موردانتظار مدافع برای بازی استراتژی d_0، d_1، و d_2 تابعی از استراتژی ترکیبی است که همانند [۲۲]، توزیع احتمال p_{a0}، p_{a1} و p_{a2} برای مهاجم به دست می‌آید:

$$p_{a0} = 1 - \left(\frac{c_{d2} - c_{d1}}{\omega_2} + \frac{c_{d1}}{\omega_1}\right), \; p_{a1} = \frac{c_{d1}}{\omega_1}, \quad p_{a2} = \frac{c_{d2} - c_{d1}}{\omega_2} \qquad (۲)$$

بنابراین، استراتژی مختلط تعادل نش برای بازی امنیتی غیر همکاری با توزیع $\{p_{a0}, p_{a1}, p_{a2}\}$ و $\{p_{d0}, p_{d1}, p_{d2}\}$ در معادلات (۱) و (۲) ارائه شده است. به این معنا که هر بازیکن انتخاب خود را تصادفی انجام خواهد داد. در نتیجه، حریفان در بازی نسبت به نتایج بازی بی‌تفاوت خواهند بود.

تذکر ۱:

اگر $c_{a2} << \omega_2$ طبق رابطه (۱) ممکن است $p_{d1} < 0$ باشد. این غیرممکن است. از سوی دیگر این احتمال منفی نشان می‌دهد که مدافع اصلاً انگیزه‌ای برای به‌کارگیری استراتژی d_1 ندارد و انگیزه قوی دارد تا همیشه استراتژی d_2 را بازی کند. در مقابل، بنا به رابطه (۲) مهاجم هیچ انگیزه‌ای برای بازی استراتژی a_2 (سطح ۲ حمله) ندارد؛ بنابراین، دو استراتژی a_2 و d_1 می‌توانند به طور کامل از فضای استراتژی حذف شوند. در نتیجه، بازی به ۲ استراتژی برای هر بازیکن با *MSNE* جدید کاهش می‌یابد. برای جزئیات بیش‌تر [۲۲] را ببینید.

۳-۳. چند نمونه از به‌کارگیری مدل پیشنهادی

در این بخش، سه سناریوی احتمالی در [۲۲] برای درک بهتر مطلب به‌اختصار بیان می‌شود تا نشان داده شود که چگونه استراتژی‌های حمله - دفاع و تعاملات پویای آن‌ها را می‌توان از طریق چارچوب نظری بازی مدل‌سازی کرد (برای جزئیات بیش‌تر به [۲۲] مراجعه شود). در بخش انتهایی، سناریوی مدنظر خود را معرفی و بر اساس همین مدل به بیان نتایج پرداخته می‌شود.

۳-۳-۱. سیستم دفاعی در برابر حمله سیلاب *Hello*

حمله سیلاب *Hello*[1] [۹] یکی از حملات رایج در لایه شبکه است که یک شبکه حسگر بی‌سیم می‌تواند با آن روبرو شود، جایی که مهاجم می‌تواند توهم همسایگی با گره‌های دیگر یا توهم ایستگاه پایه را ایجاد کند.

استراتژی‌های حمله: در حمله سطح یک با شدت کم، گره دشمن پیام *Hello* را به گره‌های حسگر می‌فرستد و آن‌ها را متقاعد می‌کند که یکی از همسایگان آن‌هاست. در حمله سطح دو با شدت بالا، گره دشمن بسته درخواست مسیر دریافتی[2] (*RREQ*) را باقدرت بالا به تعداد زیادی گره می‌فرستد و گره‌ها را متقاعد می‌کند که گره مهاجم ایستگاه پایه آن‌هاست.

استراتژی‌های دفاعی: در مقابل، دفاع سطح یک بر اساس زمان، با یک آستانه زمانی از پیش تعریف شده برای دریافت پاسخ است [۱۰-۱۱]. استراتژی دفاعی سطح دوم یک فن تشخیص پیشرفته‌تر و نیازمند توان محاسباتی بیش‌تر است. این سطح می‌تواند قدرت سیگنال پیام‌های *Hello* مبتنی بر طرح جورچین مشتری[3] *(MBCP)* باشد که برای بررسی اعتبار از جورچین‌های مشتری کوتاه استفاده می‌شود [۱۲]. روش دیگری که می‌تواند

[1]. Hello flood attack
[2]. Route Request Packet
[3]. Message Based Client Puzzles

به‌عنوان دفاع سطح دو به کار رود، طرح تأیید مکان با فیلترکردن حریصانه توسط طرح تأیید مکان ماتریسی است [۱۳].

به طور خلاصه، استراتژی‌های این بازی حمله و دفاع به شرح زیر است:

- مهاجم : a_1 مانند یک همسایه دروغین رفتار کنید
- مهاجم: a_2 مانند یک ایستگاه پایه دروغین رفتار کنید
- مدافع : d_1طرح زمان‌بندی پاسخ
- مدافع : d_2 قدرت سیگنال و طرح جورچین مشتری مبتنی بر پیام *Hello* (*MBCP*). یا طرح تأیید مکان.

۳-۳-۲. سیستم دفاعی در برابر حمله بدافزار

بدافزار یکی از تهدیدهای اصلی دنیای سایبری است. در طول جنگ سایبری، بدافزارها برای مختل کردن عملیات تجاری، سرقت اطلاعات حساس، دستیابی به دسترسی غیرمجاز یا هر رفتار هدفمند دیگری استفاده می‌شوند [۱۴].

استراتژی‌های حمله: حمله سطح یک، ایجاد بدافزار با استفاده مجدد از کدهای مخرب موجود است. حمله بدافزار سطح دوم مخرب‌تر و دفاع در برابر آن سخت‌تر است، جایی که بدافزار با استفاده از فن‌های چندشکلی یا دگرگونی تولید می‌شود [۱۵-۱۶].

استراتژی‌های دفاعی: دفاع سطح یک، مبتنی بر امضا و معروف به تجزیه‌وتحلیل استاتیک است؛ مانند نرم‌افزارهای ضدویروس [۱۵]. دفاع سطح دو می‌تواند استراتژی پیشرفته‌تری باشد که نیازمند قدرت محاسباتی، اتصالات اینترنتی، زمان پاسخ شناسایی، و مهارت/دانش کارکنان امنیتی و غیره باشد. به‌عنوان‌مثال فن‌های تجزیه‌وتحلیل بدافزارهای پویا مانند *Sandbox* [۱۷-۱۸].

به طور خلاصه، استراتژی‌های نظریه بازی‌ها برای این بازی حمله و دفاع به شرح زیر است:

- مهاجم a_1 : بدافزاری که با استفاده از کد مخرب موجود تولید می‌شود.
- مهاجم a_2 : بدافزاری که با استفاده از آسیب‌پذیری روز صفر، فن‌های کدگذاری چندشکلی یا دگرگونی تولید می‌شود.
- مدافع d_1 : تجزیه‌وتحلیل استاتیک (یعنی سیستم امنیتی مبتنی بر امضا[1]).
- مدافع d_2 : فن‌های تحلیل بدافزار پویا (مانند *Sandbox*).

۳-۳-۳. سیستم دفاعی در برابر حمله حدس رمز عبور

اکثر سیستم‌های سایبری دنیای واقعی برای احراز هویت به رمز عبور متکی هستند. یک تهدید رایج برای احراز هویت مبتنی بر رمز عبور، حمله حدس‌زدن رمز عبور است.

استراتژی‌های حمله: حمله سطح اول با شدت کم است، آزمایش‌های حدس رمز عبور که به هیچ مهارتی نیاز ندارد. حمله سطح دوم، شدت بالایی از آزمایش‌های حدس با استفاده از طرح چند مشتری مجازی است [۱۹]. با استفاده از چنین طرحی، یک مهاجم می‌تواند مشتریان مجازی زیادی را با یک دستگاه محاسباتی ایجاد کند.

استراتژی‌های دفاعی: سطح یک دفاع، تعداد تلاش‌های ناموفق برای ورود را محدود می‌کند [۲۰]. سطح دو دفاع، سیستم تشخیص نفوذ است که سازوکاری کارآمد است و سرعت تشخیص بالایی دارد. مدافع می‌تواند با استخراج اثر انگشت دستگاه[2]، منبع واقعی درخواست‌های مهاجم را تعیین کند [۲۱].

به طور خلاصه، استراتژی‌های نظریه بازی‌ها این بازی حمله و دفاع به شرح زیر است:

- مهاجم a_1: مانند یک کاربر عادی هر بار یک درخواست ورود به سیستم ارسال می‌کند.
- مهاجم a_2: از فن‌های کاربرهای مجازی برای ارسال هم‌زمان تعداد زیادی درخواست‌های ورود در یک‌زمان استفاده می‌کند.
- مدافع d_1 : طرح تلاش برای احراز هویت (مانند محدودیت در تعداد تلاش‌ها)
- مدافع d_2 : یک سیستم تشخیص پیشرفته که منابع واقعی درخواست ورود را شناسایی کند (مانند درخواست اثر نگشت دستگاه)

۴. تغییر مدل پیشنهادی از حالت بازی دوجانبه به بازی سه‌جانبه

در این بخش سعی می‌شود مدل پیشنهادی در مرحله قبل با بررسی و ارزیابی دخالت یک عامل خارجی در تعامل مهاجم - مدافع بهینه شود. هرچند این عمل به پیچیدگی مدل پیشنهادی و افزایش محاسبات مربوطه منجر می‌شود، ولی در واقع مدل بازی پیشنهادی را کاراتر و به واقعیت نزدیک‌تر می‌کند.

مدل جدید بر این فرض استوار است: هنگامی که مهاجم A به مدافع D حمله می‌کند عامل ناشناس دیگری مانند X، حال به مهاجم یا در همکاری با مهاجم به مدافع، حمله می‌کند؛ لذا در حالت اول یک بازی غیر همکاری مجموع صفر و در حالت دوم یک بازی همکاری مدنظر است. مدل این بازی به شرح زیر است:

$$G = < (N), (S), (U) >$$

که در آن $N = \{A, D, X\}$ و فضای استراتژی به‌صورت

$$S = \{ Y_{ar}^{K}, K_{ar}^{Y} \mid r \in \{0,1,2\}, \quad Y \in \{A, X\}, \quad K \in \{A, D\}, \quad Y \neq K \}$$

و U همان تابع تعریف شده در بالاست که ابزارهای مناسب را به هر بازیکن نسبت می‌دهد.

[1]. Signature-based security systems

[2]. device fingerprint

۴-۱. شرح بازی جنگ سایبری سه‌جانبه پویا

مدل پیشنهادی نظری در قالب یک بازی جنگ سایبری سه‌جانبه رخ می‌دهد که در آن مهاجم A و مدافع D مفروض هستند. به طور ناگهانی یک عامل خارجی ناشناس دیگر مانند مهاجم X به A یا D حمله می‌کند.

دقت شود که هر مدل‌سازی ریاضی در نظریه بازی‌ها بر اساس قواعد و مفروضات از پیش تعیین شده بنا و پی‌ریزی می‌شود. این مجموعه قوانین نقشی اساسی در ساختن چهارچوب بازی پیشنهادی و نتایج حاصل از آن داشته و زیر بنای مدل را تشکیل می‌دهند؛ لذا مفروضات زیر نیز برقرار است:

1) درآن‌واحد، هر بازیکن تنها می‌تواند به یک بازیکن دیگر حمله کند.

2) عامل خارجی X، همواره به‌عنوان مهاجم در نظر گرفته می‌شود.

3) بازیکن D، همواره به‌عنوان مدافع در نظر گرفته می‌شود.

4) هر مهاجم/ مدافع سه سطح برای انتخاب نوع استراتژی بازی خود دارد.

5) ارزش منابعی که از آن‌ها محافظت می‌شود به‌صورت ω_{nY} نمایش داده می‌شود که $n \in \{1,2\}$ و $Y \in \{A, D\}$. همچنین، هزینه حمله (دفاع) به‌صورت $C_{K_{an}^{Y}}$ (و $C_{Y_{dn}^{K}}$) که $K \in \{A, X\}$ (و $Y \in \{A, D\}$) نشان داده می‌شود.

6) ارزش منابع همواره از هزینه حمله/دفاع بیش‌تر در نظر گرفته می‌شود، تا مهاجم/مدافع انگیزه‌ای برای انجام حمله/دفاع خود داشته باشد. یعنی:

$$\omega_{nY} > C_{K_{an}^{Y}}, C_{Y_{dn}^{K}} \ : \ Y \in \{A, D\} \text{ و } K \in \{A, X\}$$

7) برای به‌صرفه‌بودن انتخاب استراتژی‌های بازی نسبت به یکدیگر فرض می‌شود:

علاوه بر این‌ها، مدل بازی ما را ملزم می‌کند زمانی که مهاجم یا مدافع یک استراتژی خاص را اجرا می‌کنند، نتیجه‌ای مشخص حاصل شود؛ لذا فرضیات زیر در مورد نتایج بازی در نظر گرفته می‌شود:

- حمله تحت این سناریوها موفقیت‌آمیز است: برای *Attack-1* در مقابل *No-Defend* و *Attack-2* در مقابل *Defend-1* یا *No-Defend*.
- دفاع در این سناریوها موفق است: *Defend-1* مقابل *Attack-1* یا *No-Attack* و *Defend-2* در مقابل *Attack-2* یا *Attack-1* یا *No-Attack*.
- وقتی هیچ حمله‌ای وجود ندارد و هیچ دفاعی به کار نمی‌رود، یعنی بدون حمله در مقابل بدون دفاع، سود یا ضرر صفر است.

مفروضات فوق به این معنی است که استراتژی دفاعی شدیدتر، *Defend-2*، در برابر همه حملات ایمن است. بااین‌حال، استراتژی دفاعی سطح پایین، *Defend-1*، برای حمله سطح پایین، *Attack-1* خوب است، اما همچنان برای مقابله با حمله شدیدتر *Attack-2* آسیب‌پذیر است.

تذکر ۲.

دقت شود معنای نمادها به‌صورت زیر بیان می‌شود .برای $K, Y \in \{A, D, X\}$ و $n \in \{0,1,2\}$ داریم:

$Y_{an}^{K} =$ حمله Y به K با استراتژی در سطح n صورت پذیرفته است

$Y_{dn}^{K} =$ دفاع Y برابر K با استراتژی در سطح n صورت پذیرفته است

$C_{Y_{an}^{K}} =$ هزینه حمله Y به K که در سطح n صورت پذیرفته است

$C_{Y_{dn}^{K}} =$ هزینه دفاع Y برابر K که در سطح n صورت پذیرفته است

۴-۲. جداول استراتژیک بازی جنگ سایبری سه‌جانبه

برای مدل ذکر شده فوق دو حالت می‌توان متصور شد:

۴-۲-۱. حالت اول: X به A و A به D حمله کند.

جداول استراتژیک مربوط به حالت ۱ در نظر گرفته می‌شود: یعنی زمانی که Xبه Aو A به D حمله کند. توجه شود که در این حالت خواسته یا ناخواسته X به D در برابر حمله A کمک می‌کند. به‌عبارت‌دیگر هر بار که X به A حمله می‌کند حداقل به‌اندازه $C_{X_{an}^{A}}$ از منابع و باطری بازیکن (سیستم) A می‌کاهد که این یعنی به همین اندازه به بازیکن (سیستم) D کمک می‌کند. به‌نوعی یک بازی همکاری بین X و D است. برای درک بهتر به شکل (۱) مراجعه شود. $\omega_{1Y} \leq \omega_{2Y} \leq C_{K_{a1}^{Y}} \leq C_{K_{a2}^{Y}} \leq C_{Y_{d1}^{K}}$

شکل (۱). A به D و X نیز به A حمله می‌کند

۴-۲-۱-۱. حمله Xبه A:

در این مرحله جدول (۲) استراتژیک زیر در نظر گرفته می‌شود.

جدول (۲). شکل استراتژیک بازی حمله X به A

	A^X_{d0}	A^X_{d1}	A^X_{d2}
X^A_{a0}	*0, 0*	$c_{A^X_{d1}}, -c_{A^X_{d1}}$	$c_{A^X_{d2}}, -c_{A^X_{d2}}$
X^A_{a1}	$i=0: X^A_{a0}$ و D^A_{d0}، $\omega_{1A} - c_{X^A_{a1}}$، $c_{X^A_{a1}}$ $i=1: X^A_{a1}$ و D^A_{d0}، $c_{X^A_{a1}} - \omega_{1A}$، $\omega_{1A} - c_{X^A_{a1}}$ $i=2: X^A_{a2}$ و D^A_{d0}، $c_{X^A_{a2}} - \omega_{2A}$، $\omega_{2A} - c_{X^A_{a2}}$	X^A_{a0} و D^A_{d1}، $c_{A^X_{d1}} - c_{X^A_{a1}}$، $c_{X^A_{a1}}$ X^A_{a1} و D^A_{d1}، $c_{X^A_{a1}} - c_{A^X_{d1}}$، $c_{A^X_{d1}} - c_{X^A_{a1}}$ X^A_{a2} و D^A_{d1}، $c_{X^A_{a2}} - c_{A^X_{d1}} - \omega_{2A}$، $\omega_{2A} + c_{A^X_{d1}} - c_{X^A_{a2}}$	X^A_{a0} و D^A_{d2}، $c_{A^X_{d2}} - c_{X^A_{a1}}$، $c_{X^A_{a1}}$ X^A_{a1} و D^A_{d2}، $c_{X^A_{a1}} - c_{A^X_{d2}}$، $c_{A^X_{d2}} - c_{X^A_{a1}}$ X^A_{a2} و D^A_{d2}، $c_{X^A_{a2}} - c_{A^X_{d2}}$، $c_{A^X_{d2}} - c_{X^A_{a2}}$

مانند محاسبات حالت بازی دوجانبه برای به‌دست‌آوردن احتمالات موردنیاز برای استراتژی‌های حمله و دفاع نتایج زیر حاصل می‌شود:

$$p_{A^X_{d0}} = \frac{c_{X^A_{a1}}}{\omega_{1A}}, p_{A^X_{d1}} = \frac{c_{X^A_{a2}}}{\omega_{2A}} - \frac{c_{X^A_{a1}}}{\omega_{1A}}, \quad p_{A^X_{d2}} = 1 - \frac{c_{X^A_{a2}}}{\omega_{2A}} \tag{۳}$$

$$p_{X^A_{a0}} = 1 - \left(\frac{c_{A^X_{d2}} - c_{A^X_{d1}}}{\omega_{2A}} + \frac{c_{A^X_{d1}}}{\omega_{1A}}\right), \quad p_{X^A_{a1}} = \frac{c_{A^X_{d1}}}{\omega_{1A}}, p_{X^A_{a2}} = \frac{c_{A^X_{d2}} - c_{A^X_{d1}}}{\omega_{2A}} \tag{۴}$$

۴-۲-۱-۲. حمله A به D (هم‌زمان با حمله X به A در سطح a_i)

برای $i \in \{0,1,2\}$ ابتدا جدول (۳) استراتژیک زیر مورد بررسی واقع می‌شود.

جدول (۳). شکل استراتژیک حمله A به D و X به A در سطح a_i

	D^A_{d0} و X^A_{ai}	D^A_{d1} و X^A_{ai}	D^A_{d2} و X^A_{ai}
A^D_{a0}	$c_{X^A_{ai}}$، $-c_{X^A_{ai}}$	$c_{D^A_{d1}} + c_{X^A_{ai}}$، $-\left(c_{D^A_{d1}} + c_{X^A_{ai}}\right)$	$c_{D^A_{d2}} + c_{X^A_{ai}}$، $-\left(c_{D^A_{d2}} + c_{X^A_{ai}}\right)$
A^D_{a1}	$\left(\omega_{1D} + c_{X^A_{ai}}\right) - c_{A^D_{a1}}$، $c_{A^D_{a1}} - \left(\omega_{1D} + c_{X^A_{ai}}\right)$	$\left(c_{D^A_{d1}} + c_{X^A_{ai}}\right) - c_{A^D_{a1}}$، $c_{A^D_{a1}} - \left(c_{D^A_{d1}} + c_{X^A_{ai}}\right)$	$\left(c_{D^A_{d2}} + c_{A^X_{ai}}\right) - c_{A^D_{a1}}$، $c_{A^D_{a1}} - \left(c_{D^A_{d2}} + c_{A^X_{ai}}\right)$
A^D_{a2}	$\left(\omega_{2D} + c_{X^A_{ai}}\right) - c_{A^D_{a2}}$، $c_{A^D_{a2}} - \left(\omega_{2D} + c_{X^A_{ai}}\right)$	$\omega_{2D} + \left(c_{X^A_{ai}} + c_{D^A_{d1}}\right) - c_{A^D_{a2}}$، $c_{A^D_{a2}} - \omega_{2D} - \left(c_{X^A_{ai}} + c_{D^A_{d1}}\right)$	$\left(c_{D^A_{d2}} + c_{X^A_{ai}}\right) - c_{A^D_{a2}}$، $c_{A^D_{a2}} - \left(c_{D^A_{d2}} + c_{X^A_{ai}}\right)$

تذکر ۳.

جدول شماره (۳) تلفیقی از ۳ جدول جداگانه است. به‌عبارت‌دیگر سطر یک جدول (۳) را می‌توان به شکل زیر در نظر گرفت:

برای $i,j \in \{0,1,2\}$، سود موردانتظار ا ز بازی استراتژی‌های a_i و d_j برای مدافعان X^A_{ai} و D^A_{dj} یکسان در نظر گرفته می‌شود، یعنی

$$EU\left(p_{D^A_{d0}}, x^A_{ai}\right) = EU\left(p_{D^A_{d1}}, x^A_{ai}\right) = EU\left(p_{D^A_{d2}}, x^A_{ai}\right) \tag{۵}$$

باتوجه‌به جدول (۳)، ابزار موردانتظار مدافعان برای بازی استراتژی X^A_{ai} و D^A_{d0} به‌صورت زیر خواهد بود:

$$EU\left(p_{D^A_{d0}}, x^A_{ai}\right) = p_{A^D_{a0}}\left(-c_{X^A_{ai}}\right) + p_{A^D_{a1}}\left(c_{A^D_{a1}} - \omega_{1D} - c_{X^A_{ai}}\right) + p_{A^D_{a2}}\left(c_{A^D_{a2}} - \omega_{2D} - c_{X^A_{ai}}\right) \tag{۶}$$

$$EU\left(p_{D^A_{d1}}, x^A_{ai}\right) = p_{A^D_{a0}}\left(-c_{D^A_{d1}} - c_{X^A_{ai}}\right) + p_{A^D_{a1}}\left(c_{A^D_{a1}} - c_{D^A_{d1}} - c_{X^A_{ai}}\right) + p_{A^D_{a2}}\left(c_{A^D_{a2}} - \omega_{2D} - c_{X^A_{ai}} - c_{D^A_{d1}}\right) \tag{۷}$$

$$EU\left(p_{D^A_{d2}}, x^A_{ai}\right) = p_{A^D_{a0}}\left(-c_{D^A_{d2}} - c_{X^A_{ai}}\right) + p_{A^D_{a1}}\left(c_{A^D_{a1}} - c_{D^A_{d2}} - c_{X^A_{ai}}\right) + p_{A^D_{a2}}\left(c_{A^D_{a2}} - c_{D^A_{d2}} - c_{X^A_{ai}}\right) \tag{۸}$$

باتوجه‌به تعریف ۱ و جای‌گذاری (۶)، (۷) و (۸) در (۵) توزیع احتمال $p_{A^D_{a0}}$، $p_{A^D_{a1}}$ و $p_{A^D_{a2}}$ برای مهاجم A به شرح زیر خواهد بود:

$$p_{A^D_{a0}} = 1 - \left(\frac{c_{D^A_{d1}}}{\omega_{1D}} + \frac{c_{D^A_{d2}} - c_{D^A_{d1}}}{\omega_{2D}}\right), \quad p_{A^D_{a1}} = \frac{c_{D^A_{d1}}}{\omega_{1D}}, \quad p_{A^D_{a2}} = \frac{c_{D^A_{d2}} - c_{D^A_{d1}}}{\omega_{2D}} \tag{۹}$$

۴-۲-۱-۳. دفاع D در برابر A (هم‌زمان با دفاع A برابر X در سطح d_j).

برای $j \in \{0,1,2\}$، جدول استراتژیک بازی در این حالت به فرم جدول (۴) زیر است.

جدول (۴). شکل استراتژیک بازی دفاع D برابر A و دفاع A برابر X در سطح d_j

	D^A_{d0}	D^A_{d1}	D^A_{d2}
A^D_{a0} و A^X_{dj}	$-c_{A^X_{dj}}$, $c_{A^X_{dj}}$	$c_{D^A_{d1}} - c_{A^X_{dj}}$, $c_{A^X_{dj}} - c_{D^A_{d1}}$	$c_{D^A_{d2}} - c_{A^X_{dj}}$, $c_{A^X_{dj}} - c_{D^A_{d2}}$
A^D_{a1} و A^X_{dj}	$\omega_{1D} - \left(c_{A^D_{a1}} + c_{A^X_{dj}}\right)$, $\left(c_{A^D_{a1}} + c_{A^X_{dj}}\right) - \omega_{1D}$	$c_{D^A_{d1}} - \left(c_{A^D_{a1}} + c_{A^X_{dj}}\right)$, $\left(c_{A^D_{a1}} + c_{A^X_{dj}}\right) - c_{D^A_{d1}}$	$c_{D^A_{d2}} - \left(c_{A^D_{a1}} + c_{A^X_{dj}}\right)$, $\left(c_{A^D_{a1}} + c_{A^X_{dj}}\right) - c_{D^A_{d2}}$
A^D_{a2} و A^X_{dj}	$\omega_{2D} - \left(c_{A^D_{a2}} + c_{A^X_{dj}}\right)$, $\left(c_{A^D_{a2}} + c_{A^X_{dj}}\right) - \omega_{2D}$	$\omega_{2D} + c_{D^A_{d1}} - \left(c_{A^D_{a2}} + c_{A^X_{dj}}\right)$, $\left(c_{A^D_{a2}} + c_{A^X_{dj}}\right) - \omega_{2D} - c_{D^A_{d1}}$	$c_{D^A_{d2}} - \left(c_{A^D_{a2}} + c_{A^X_{dj}}\right)$, $\left(c_{A^D_{a2}} + c_{A^X_{dj}}\right) - c_{D^A_{d2}}$

تذکر ۴.

لازم به ذکر است، جدول شماره (۴) تلفیقی از ۳ جدول جداگانه است. به‌عبارت‌دیگر به‌ازای $j \in \{0,1,2\}$، ستون یک جدول (۴) را می‌توان به شکل زیر در نظر گرفت:

$$j=0,\ \begin{cases} A^D_{a0} \text{ و } A^X_{d0} \\ A^D_{a1} \text{ و } A^X_{d0} \\ A^D_{a2} \text{ و } A^X_{d0} \end{cases} \quad j=1,\ \begin{cases} A^D_{a0} \text{ و } A^X_{d1} \\ A^D_{a1} \text{ و } A^X_{d1} \\ A^D_{a2} \text{ و } A^X_{d1} \end{cases} \quad j=2,\ \begin{cases} A^D_{a0} \text{ و } A^X_{d2} \\ A^D_{a1} \text{ و } A^X_{d2} \\ A^D_{a2} \text{ و } A^X_{d2} \end{cases}$$

به طور مشابه،

$$U\left(p_{A^D_{a0}, A^X_{dj}}\right) = EU\left(p_{A^D_{a1}, A^X_{dj}}\right) = EU\left(p_{A^D_{a2}, A^X_{dj}}\right) \qquad (۱۰)$$

Eو ابزار موردانتظار مهاجمان برای بازی استراتژی A^X_{dj} و A^D_{ai} باتوجه‌به جدول (۴) به شکل زیر محاسبه می‌شود:

$$EU\left(p_{A^D_{a0}, A^X_{dj}}\right) = p_{D^A_{d0}}\left(-c_{A^X_{dj}}\right) + p_{D^A_{d1}}\left(c_{D^A_{d1}} - c_{A^X_{dj}}\right) + p_{D^A_{d2}}\left(c_{D^A_{d2}} - c_{A^X_{dj}}\right) \qquad (۱۱)$$

$$EU\left(p_{A^D_{a1}, A^X_{dj}}\right) = p_{D^A_{d0}}\left(\omega_{1D} - c_{A^D_{a1}} - c_{A^X_{dj}}\right) + p_{D^A_{d1}}\left(c_{D^A_{d1}} - c_{A^D_{a1}} - c_{A^X_{dj}}\right) + p_{D^A_{d2}}\left(c_{D^A_{d2}} - c_{A^D_{a1}} - c_{A^X_{dj}}\right) \qquad (۱۲)$$

$$EU\left(p_{A^D_{a2}, A^X_{dj}}\right) = p_{D^A_{d0}}\left(\omega_{2D} - c_{A^D_{a2}} - c_{A^X_{dj}}\right) + p_{D^A_{d1}}\left(\omega_{2D} + c_{D^A_{d1}} - c_{A^D_{a2}} - c_{A^X_{dj}}\right) + p_{D^A_{d2}}\left(c_{D^A_{d2}} - c_{A^D_{a2}} - c_{A^X_{dj}}\right) \qquad (۱۳)$$

و لذا باتوجه‌به تعریف ۱ و جای‌گذاری (۱۱)، (۱۲) و (۱۳) در (۱۰) توزیع احتمال $p_{D^A_{d0}}$، $p_{D^A_{d1}}$ و $p_{D^A_{d2}}$ برای مدافع D به دست خواهد آمد:

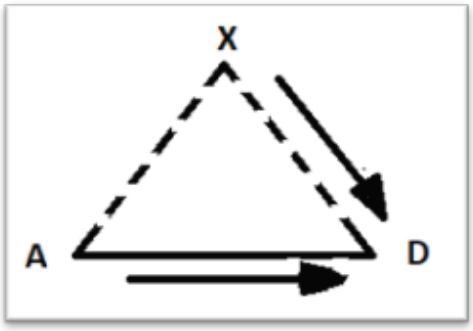
$$p_{D^A_{d0}} = \frac{c_{A^D_{a1}}}{\omega_{1D}}, \qquad p_{D^A_{d1}} = \frac{c_{A^D_{a2}}}{\omega_{2D}} - \frac{c_{A^D_{a1}}}{\omega_{1D}}, \qquad p_{D^A_{d2}} = 1 - \frac{c_{A^D_{a2}}}{\omega_{2D}} \qquad (۱۳)$$

$$p_{D^A_{d0}} = \frac{c_{A^D_{a1}}}{\omega_{1D}}, \qquad p_{D^A_{d1}} = \frac{c_{A^D_{a2}}}{\omega_{2D}} - \frac{c_{A^D_{a1}}}{\omega_{1D}}, \qquad p_{D^A_{d2}} = 1 - \frac{c_{A^D_{a2}}}{\omega_{2D}} \qquad (۱۴)$$

نهایتاً در این حالت استراتژی مختلط تعادل نش با توزیع، $\{p_{X^A_{a0}}, p_{X^A_{a1}}, p_{X^A_{a2}}\}$ و $\{p_{A^D_{a0}}, p_{A^D_{a1}}, p_{A^D_{a2}}\}$ در معادلات (۳)، (۹) و (۱۴) ارائه شده است.

۴-۲-۲. حالت دوم: X و A هم‌زمان به D حمله کنند.

شکل (۲) زیر در نظر گرفته می‌شود:



شکل (۲). A و X نیز به D حمله کنند

جداول مربوط به حالت ۲ در نظر گرفته می‌شود: دقت شود که در این حالت X و A نیز به طور خواسته یا ناخواسته همکاری کرده و D نیز باید در دو سطح مختلف در برابر هر دو حمله دفاع کند.

۴-۲-۲-۱. فرض کنید A به D حمله کند (هم‌زمان D در برابر X نیز دفاع می‌کند)

با درنظرگرفتن $j \in \{0,1,2\}$، برای جدول (۵) نتایج زیر حاصل می‌شود.

جدول (۵). شکل استراتژیک بازی حمله A به D و دفاع هم‌زمان D در برابر X

	D_{d0}^{A} و D_{dj}^{X}	D_{d1}^{A} و D_{dj}^{X}	D_{d2}^{A} و D_{dj}^{X}
A_{a0}^{D}	$c_{D_{dj}^{X}}$, $-c_{D_{dj}^{X}}$	$c_{D_{d1}^{A}}+c_{D_{dj}^{X}}$, $-\left(c_{D_{d1}^{A}}+c_{D_{dj}^{X}}\right)$	$c_{D_{d2}^{A}}+c_{D_{dj}^{X}}$, $-\left(c_{D_{d2}^{A}}+c_{D_{dj}^{X}}\right)$
A_{a1}^{D}	$\left(\omega_{1D}+c_{D_{dj}^{X}}\right)-c_{A_{a1}^{D}}$, $c_{A_{a1}^{D}}-\left(\omega_{1D}+c_{D_{dj}^{X}}\right)$	$\left(c_{D_{d1}^{A}}+c_{D_{dj}^{X}}\right)-c_{A_{a1}^{D}}$, $c_{A_{a1}^{D}}-\left(c_{D_{d1}^{A}}+c_{D_{dj}^{X}}\right)$	$\left(c_{D_{d2}^{A}}+c_{D_{dj}^{X}}\right)-c_{A_{a1}^{D}}$, $c_{A_{a1}^{D}}-\left(c_{D_{d2}^{A}}+c_{D_{dj}^{X}}\right)$
A_{a2}^{D}	$\left(\omega_{2D}+c_{D_{dj}^{X}}\right)-c_{A_{a2}^{D}}$, $c_{A_{a2}^{D}}-\left(\omega_{2D}+c_{D_{dj}^{X}}\right)$	$\omega_{2D}+\left(c_{D_{d1}^{A}}+c_{D_{dj}^{X}}\right)-c_{A_{a2}^{D}}$, $c_{A_{a2}^{D}}-\omega_{2D}-\left(c_{D_{d1}^{A}}+c_{D_{dj}^{X}}\right)$	$\left(c_{D_{d2}^{A}}+c_{D_{dj}^{X}}\right)-c_{A_{a2}^{D}}$, $c_{A_{a2}^{D}}-\left(c_{D_{d2}^{A}}+c_{D_{dj}^{X}}\right)$

تذکر ۵.

لازم به ذکر است، جدول شماره (۵) تلفیقی از ۳ جدول جداگانه است. به‌عبارت‌دیگر سطر یک جدول (۵) را می‌توان به شکل زیر در نظر گرفت: به‌ازای $j\in\{0,1,2\}$ داریم.

	D_{dj}^{A} و D_{dj}^{X}
A_{a0}^{D}	$c_{D_{dj}^{X}}$, $-c_{D_{dj}^{X}}$
A_{a1}^{D}	$\left(\omega_{1D}+c_{D_{dj}^{X}}\right)-c_{A_{a1}^{D}}$, $c_{A_{a1}^{D}}-\left(\omega_{1D}+c_{D_{dj}^{X}}\right)$
A_{a2}^{D}	$\left(\omega_{2D}+c_{D_{dj}^{X}}\right)-c_{A_{a2}^{D}}$, $c_{A_{a2}^{D}}-\left(\omega_{2D}+c_{D_{dj}^{X}}\right)$

حال استراتژی مختلط نقطه تعادل نش برای جدول شماره (۵) به کار گرفته می‌شود: سود موردانتظار از بازی استراتژی‌های d_i و d_j توسط مدافع برابر باشند. یعنی

$$EU\left(p_{D_{d0}^{A},D_{dj}^{X}}\right)=EU\left(p_{D_{d1}^{A},D_{dj}^{X}}\right)=EU\left(p_{D_{d2}^{A},D_{dj}^{X}}\right) \quad (۱۵)$$

باتوجه‌به جدول (۵) سود موردانتظار مدافع برای بازی استراتژی D_{di}^{A} و D_{dj}^{X} به شکل زیر محاسبه می‌شود:

$$\begin{aligned}EU\left(p_{D_{d0}^{A},D_{dj}^{X}}\right)&=p_{A_{a0}^{D}}\left(-c_{D_{dj}^{X}}\right)\\&+p_{A_{a1}^{D}}\left(c_{A_{a1}^{D}}-\omega_{1D}-c_{D_{dj}^{X}}\right)\\&+p_{A_{a2}^{D}}\left(c_{A_{a2}^{D}}-\omega_{2D}-c_{D_{dj}^{X}}\right)\end{aligned} \quad (۱۶)$$

$$\begin{aligned}EU\left(p_{D_{d1}^{A},D_{dj}^{X}}\right)&=p_{A_{a0}^{D}}\left(-c_{D_{d1}^{A}}-c_{D_{dj}^{X}}\right)\\&+p_{A_{a1}^{D}}\left(c_{A_{a1}^{D}}-c_{D_{d1}^{A}}-c_{D_{dj}^{X}}\right)\end{aligned} \quad (۱۷)$$

$$\begin{aligned}&+p_{A_{a2}^{D}}\left(c_{A_{a2}^{D}}-c_{D_{d1}^{A}}-c_{D_{dj}^{X}}\right)\\EU\left(p_{D_{d2}^{A},D_{dj}^{X}}\right)&=p_{A_{a0}^{D}}\left(-c_{D_{d2}^{A}}-c_{D_{dj}^{X}}\right)\\&+p_{A_{a1}^{D}}\left(c_{A_{a1}^{D}}-c_{D_{d2}^{A}}-c_{D_{dj}^{X}}\right)\\&+p_{A_{a2}^{D}}\left(c_{A_{a2}^{D}}-c_{D_{d2}^{A}}-c_{D_{dj}^{X}}\right)\end{aligned} \quad (۱۸)$$

باتوجه‌به تعریف ۱ و جایگزینی (۱۶)، (۱۷) و (۱۸) در (۱۵) توزیع احتمال $p_{A_{a0}^{D}}$، $p_{A_{a1}^{D}}$ و $p_{A_{a2}^{D}}$ برای مهاجم A به‌صورت زیر است:

$$\begin{aligned}p_{A_{a0}^{D}}&=1-\frac{c_{D_{d1}^{A}}}{\omega_{1D}}-\frac{c_{D_{d2}^{A}}-c_{D_{d1}^{A}}}{\omega_{2D}},\\p_{A_{a1}^{D}}&=\frac{2\,c_{D_{d1}^{A}}-c_{D_{d2}^{A}}}{\omega_{1D}},\ p_{A_{a2}^{D}}=\frac{c_{D_{d2}^{A}}-c_{D_{d1}^{A}}}{\omega_{2D}}\end{aligned} \quad (۱۹)$$

۲-۲-۴. فرض X به D حمله کند (هم‌زمان D در برابر A نیز دفاع می‌کند):

همانند حالت قبل خواهیم داشت:

$$\begin{aligned}p_{X_{a0}^{D}}&=1-\frac{c_{D_{d1}^{A}}}{\omega_{1D}}-\frac{c_{D_{d2}^{A}}-c_{D_{d1}^{A}}}{\omega_{2D}},\\p_{X_{a1}^{D}}&=\frac{2\,c_{D_{d1}^{A}}-c_{D_{d2}^{A}}}{\omega_{1D}},\ p_{X_{a2}^{D}}=\frac{c_{D_{d2}^{A}}-c_{D_{d1}^{A}}}{\omega_{2D}}\end{aligned} \quad (۲۰)$$

۲-۲-۳. فرض A و X به D حمله کنند:

با توجه به جدول $i,j\in\{0,1,2\}$ حاصل خواهد شد.

	D_{d0}^{A}	D_{d1}^{A}	D_{d2}^{A}
A_{a0}^{D} و X_{ai}^{D}	$-c_{X_{ai}^{D}}$, $c_{X_{ai}^{D}}$	$c_{D_{d1}^{A}}-c_{X_{ai}^{D}}$, $-\left(c_{D_{d1}^{A}}-c_{X_{ai}^{D}}\right)$	$c_{D_{d2}^{A}}-c_{X_{ai}^{D}}$, $-\left(c_{D_{d2}^{A}}-c_{X_{ai}^{D}}\right)$
A_{a1}^{D} و X_{ai}^{D}	$\omega_{1D}-\left(c_{A_{a1}^{D}}+c_{X_{ai}^{D}}\right)$, $\left(c_{A_{a1}^{D}}+c_{X_{ai}^{D}}\right)-\omega_{1D}$	$c_{D_{d1}^{A}}-\left(c_{A_{a1}^{D}}+c_{X_{ai}^{D}}\right)$, $\left(c_{A_{a1}^{D}}+c_{X_{ai}^{D}}\right)-c_{D_{d1}^{A}}$	$c_{D_{d2}^{A}}-\left(c_{A_{a1}^{D}}+c_{X_{ai}^{D}}\right)$, $\left(c_{A_{a1}^{D}}+c_{X_{ai}^{D}}\right)-c_{D_{d2}^{A}}$
A_{a2}^{D} و X_{ai}^{D}	$\omega_{2D}-\left(c_{A_{a2}^{D}}+c_{X_{ai}^{D}}\right)$, $\left(c_{A_{a2}^{D}}+c_{X_{ai}^{D}}\right)-\omega_{2D}$	$\omega_{2D}+c_{D_{d1}^{A}}-\left(c_{A_{a2}^{D}}+c_{X_{ai}^{D}}\right)$, $\left(c_{A_{a2}^{D}}+c_{X_{ai}^{D}}\right)-\omega_{2D}-c_{D_{d1}^{A}}$	$c_{D_{d2}^{A}}-\left(c_{A_{a2}^{D}}+c_{X_{ai}^{D}}\right)$, $\left(c_{A_{a2}^{D}}+c_{X_{ai}^{D}}\right)-c_{D_{d2}^{A}}$

جدول (۶): شکل استراتژیک بازی حمله A و X به D

سود موردانتظار از بازی استراتژی‌های a_i و a_j توسط مهاجمان X و A برابر باشند. یعنی

$$EU\left(p_{A_{a0}^D, X_{ai}^D}\right) = EU\left(p_{A_{a1}^D, X_{ai}^D}\right) = EU\left(p_{A_{a2}^D, X_{ai}^D}\right) \quad (۲۱)$$

به طور مشابه، ابزار موردانتظار مهاجمان برای بازی استراتژی X_{ai} و A_{aj} با استفاده از جدول (۶) به شکل زیر محاسبه می‌شود:

$$EU\left(p_{A_{a0}^D, X_{ai}^D}\right) = p_{D_{d0}^A}\left(-c_{X_{ai}^D}\right) + p_{D_{d1}^A}\left(c_{D_{d1}^A} - c_{X_{ai}^D}\right) + p_{D_{d2}^A}\left(c_{D_{d2}^A} - c_{X_{ai}^D}\right) \quad (۲۲)$$

$$EU\left(p_{A_{a1}^D, X_{ai}^D}\right) = p_{D_{d0}^A}\left(\omega_{1D} - c_{A_{a1}^D} - c_{X_{ai}^D}\right) + p_{D_{d1}^A}\left(c_{D_{d1}^A} - c_{A_{a1}^D} - c_{X_{ai}^D}\right) + p_{D_{d2}^A}\left(c_{D_{d2}^A} - c_{A_{a1}^D} - c_{X_{ai}^D}\right) \quad (۲۳)$$

$$EU\left(p_{A_{a2}^D, X_{ai}^D}\right) = p_{D_{d0}^A}\left(\omega_{2D} - c_{A_{a2}^D} - c_{X_{ai}^D}\right) + p_{D_{d1}^A}\left(\omega_{2D} - c_{A_{a2}^D} - c_{X_{ai}^D}\right) + p_{D_{d2}^A}\left(c_{D_{d2}^A} - c_{A_{a2}^D} - c_{X_{ai}^D}\right) \quad (۲۴)$$

$$C_{a1}^X = C_{d1}^A = C_{a1}^A = C_{d1}^D = 50$$
$$C_{a2}^X = C_{d2}^A = C_{a2}^A = C_{d2}^D = 150$$
$$\omega_{1A} = \omega_{1D} = 200, \quad \omega_{2A} = \omega_{2D} = 400$$

باتوجه‌به تعریف ۱ و جایگزینی (۲۲)، (۲۳) و (۲۴) در (۲۱) توزیع احتمال $p_{D_{d0}^A}$، $p_{D_{d1}^A}$ و $p_{D_{d2}^A}$ برای مدافع D به شرح زیر خواهد بود:

$$p_{D_{d0}^A} = \frac{c_{A_{a1}^D}}{\omega_{1D}}, \qquad p_{D_{d1}^A} = \frac{c_{A_{a2}^D}}{\omega_{2D}} - \frac{c_{A_{a1}^D}}{\omega_{1D}}, \qquad p_{D_{d2}^A} = 1 - \frac{c_{A_{a2}^D}}{\omega_{2D}} \quad (۲۵)$$

استراتژی مختلط تعادل نش نهایتاً در این حالت با توزیع $\{p_{A_{a0}^D}, p_{A_{a1}^D}, p_{A_{a2}^D}\}$، $\{p_{X_{a0}^D}, p_{X_{a1}^D}, p_{X_{a2}^D}\}$ و $\{p_{D_{d0}^A}, p_{D_{d1}^A}, p_{D_{d2}^A}\}$ در معادلات (۱۹)، (۲۰) و (۲۵) ارائه شده است. به این معنا که هر بازیکن انتخاب خود را تصادفی انجام خواهد داد. در نتیجه حریفان در بازی نسبت به نتایج بازی بی‌تفاوت خواهند بود.

۴-۳. نتایج شبیه‌سازی رایانه‌ای بازی جنگ سایبری سه‌جانبه پویا

در این بخش به بررسی نتایج حاصل از مدل پیشنهادی بازی جنگ سایبری سه‌جانبه با استفاده از مدل رایانه‌ای و کدنویسی حاصل از زبان برنامه‌نویسی پایتون[1] پرداخته می‌شود و سعی می‌شود مزایا و معایب مدل پیشنهادی بررسی شود:

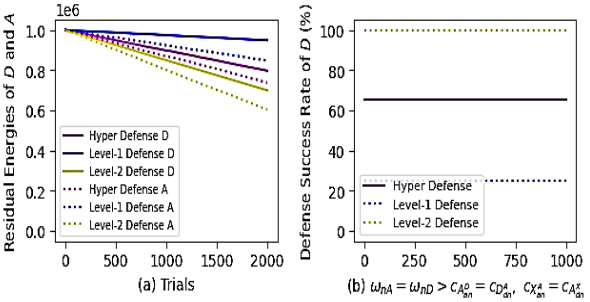
برای بررسی این حالت سعی می‌شود آزمایش را 10^3 دور[2] و در هر دور به تعداد 10^2 مرتبه تکرار[3] شود. سپس با استفاده از میانگین[4] پیروی/شکست به بررسی و مقایسه نتایج پرداخته می‌شود. لازم به ذکر است، مقادیر اولیه و پارامترهای آغازین در نتایج به‌دست‌آمده تأثیرگذار خواهند بود.

۴-۳-۱. حالتی که X به A و A به D حمله کند.

باتوجه‌به فرمول‌های به‌دست‌آمده در معادلات (۳)، (۹) و (۱۴) می‌توان همان نتایج به‌دست‌آمده در حالت بازی دوجانبه را برای این حالت نیز در نظر گرفت. ولی منابع و انرژی سیستم بازیکن A به دلیل حمله از یک سو و دفاع ازسوی‌دیگر نسبت به حالت بازی دوجانبه دارای افت بیش‌تری شده و از این نظر تحت‌فشار قرار خواهد گرفت.

الف. زمانی که $\omega_{nA} = \omega_{nD}$ از C_{an}^A و C_{dn}^D و C_{an}^X بیش‌تر و همچنین C_{an}^A با C_{dn}^D و C_{an}^X با C_{dn}^Aبرابر باشد. مثلاً به‌ازای مقادیر اولیه

برای حمله A به D و حمله X به A وضعیت سیستم بازیکنان D و A به شکل زیر خواهد بود.



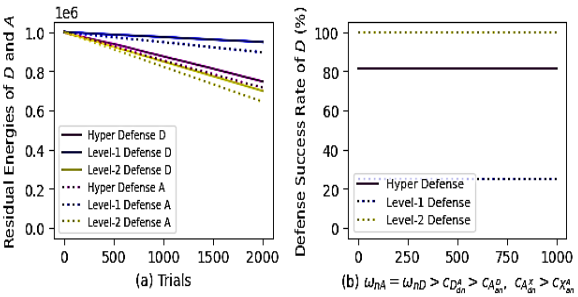
شکل (۳): *وضعیت سیستم بازیکنان D و A*

برای دفاع D در برابر A در شکل (۳) (b)، ابر دفاع پیشنهادی بازده بالاتر نسبت به دفاع ایستای سطح یک دارد و از نظر مصرف انرژی در شکل (۳) (a)، در وضعیت متوسط نسبت به دو حالت دیگر دفاع ایستا قرار دارد. همان‌طور که در شکل (۳) (a) دیده می‌شود، به علت حمله X به A وضعیت سیستم بازیکن A از نظر پایایی انرژی در فشار بیش‌تری نسبت به بازیکن D است که می‌تواند به ناپایداری وضعیت آن دست یابد و انرژی سیستم بازیکن A را زودتر به صفر برساند. علت این امر حمله و دفاع هم‌زمان بازیکن A است.

[1]. Python

[2]. Trial
[3]. terate
[4]. Mean

ب. زمانی که ω_{nD} و ω_{nA} از C_{an}^{A} و C_{dn}^{D} و C_{an}^{X} بیش‌تر و نیز C_{an}^{A} از C_{dn}^{D} و C_{an}^{X} از C_{dn}^{A} کم‌تر باشد؛ مثلاً به‌ازای مقادیر اولیه

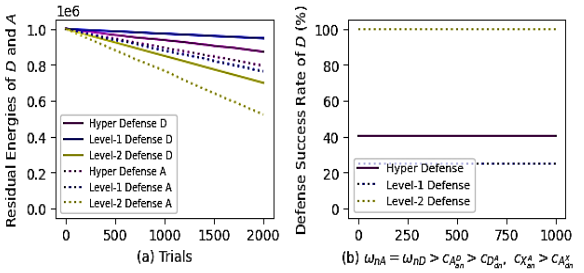


شکل (۴): *وضعیت سیستم بازیکنان D و A*

دقت شود برای دفاع D در برابر A در شکل (۴) (b)، ابر دفاع بازده مناسب ۸۰ درصد (80%) موفقیت را ثبت کرده که نسبت به دفاع ایستای سطح یک با متوسط موفقیت زیر ۳۰ درصد (30%) قابل‌ملاحظه است. از نظر مصرف انرژی در شکل (۴) (a)، ابر دفاع پیشنهادی همچنان در وضعیت متوسط نسبت به دو حالت دیگر دفاع ایستا قرار دارد، هرچند به انرژی مصرفی دفاع ایستای سطح یک نزدیک‌تر است که نشان می‌دهد سامانه ابر دفاع پیشنهادی این مقادیر اولیه بیش‌تر سطح دفاع را برمی‌گزیند.

همان‌طور که در شکل (۴) (a) دیده می‌شود، در حمله X به A با همان مقادیر اولیه، سیستم بازیکن A از نظر سطح انرژی در حالت ابر دفاع، مصرف انرژی بیش‌تری نسبت به حالت ابر دفاع بازیکن D و نزدیک به سطح دفاع ایستای سطح ۲ بازیکن D دارد. این امر نشان‌دهنده این واقعیت است که با این مقادیر اولیه، سیستم ابر دفاع A میل به استفاده از دفاع ایستای سطح ۲ دارد و لذا مصرف انرژی بیش‌تری خواهد داشت؛ ولی در حالت دفاع ایستای سطح ۲ دچار مصرف انرژی بیش‌تری نسبت به بازیکن D می‌شود که می‌تواند به ناپایداری وضعیت آن دست یابد و انرژی سیستم بازیکن A را زودتر به صفر برساند.

ج. زمانی که ω_{nD} و ω_{nA} از C_{an}^{A} و C_{dn}^{D} و C_{an}^{X} بیش‌تر و نیز C_{an}^{A} از C_{dn}^{D} و C_{an}^{X} از C_{dn}^{A} بیش‌تر باشد. مثلاً به‌ازای مقادیر اولیه



شکل (5): *وضعیت سیستم بازیکنان D و A*

همان‌گونه که در شکل (۵) مشهود است، همانند دو حالت قبل دوباره ابر دفاع بازیکن D در برابر حمله A در حالت بهتری نسبت به حالت دفاع ایستای سطح یک است و سطح مصرف انرژی آن از سطح دفاع ایستای یک بیش‌تر و از سطح دفاع ایستای دو کم‌تر است. سطح مصرف انرژی بازیکن A نیز همان‌طور که انتظار می‌رود در تمام حالات دفاع بیش‌تر است.

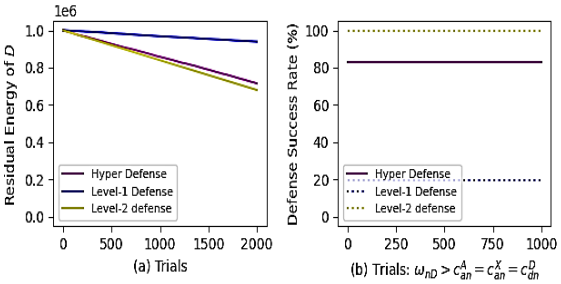
۴-۳-۲. حالتی که X و A به D حمله کنند.

دقت شود در این حالت، زمانی که دفاع D در برابر X و A به طور هم‌زمان موفق باشد آنگاه دفاع موفق نامیده می‌شود.

الف. زمانی که ω_{nD} از C_{an}^{A} و C_{dn}^{D} و C_{an}^{X} بیش‌تر و C_{an}^{A} با C_{dn}^{D} C_{an}^{X} برابر باشند. یعنی به‌ازای مقادیر اولیه

$$C_{a1}^{X} = C_{a1}^{A} = C_{a1}^{D} = 50, \quad C_{a2}^{X} = C_{a2}^{A} = C_{a2}^{D} = 80, \quad \omega_{1D} = 100, \omega_{2D} = 300$$

لذا بعد از اجرای برنامه مربوطه با مقادیر اولیه فوق که احتمالات را برای ما مشخص می‌کند، شکل (۶) حاصل خواهد شد.

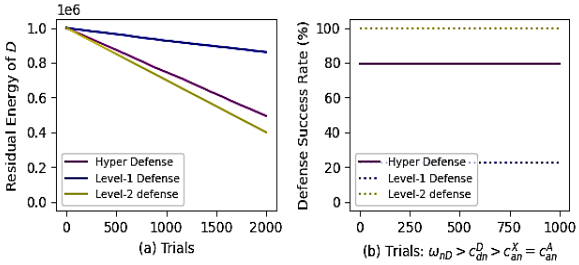


شکل (۶): زمانی که ω_{nD} از C_{an}^{A} و C_{dn}^{D} و C_{an}^{X} بیش‌تر، و C_{dn}^{D} با C_{an}^{X} و C_{an}^{A} برابر باشد.

دوباره درصد موفقیت ابر دفاع D در بازی جنگ سایبری سه‌جانبه پویا به بالاتر از ۸۰ درصد (80%) ارتقا می‌یابد. ولی در سطح دفاع ایستای سطح یک بازیکن D نرخ موفقیت نزدیک به ۲۰ درصد (20%) دیده می‌شود. مصرف انرژی ابر دفاع ما در این حالت بسیار نزدیک به سطح مصرف انرژی دفاع ایستای سطح ۲ است که نشان‌دهنده این امر است که سامانه ابر دفاع ما در این حالت بیش‌تر تمایل به انتخاب دفاع ایستای سطح ۲ دارد.

$$C_{a1}^{X} = 30 > C_{a1}^{A} = 20, \quad C_{a1}^{A} = 20 > C_{d1}^{D} = 15,$$
$$C_{a2}^{X} = 250 > C_{a2}^{A} = 200, \quad C_{a2}^{A} = 210 > C_{d2}^{D} = 200$$
$$\omega_{1A} = 300, \omega_{2A} = 500, \quad \omega_{1D} = 200, \omega_{2D} = 280$$

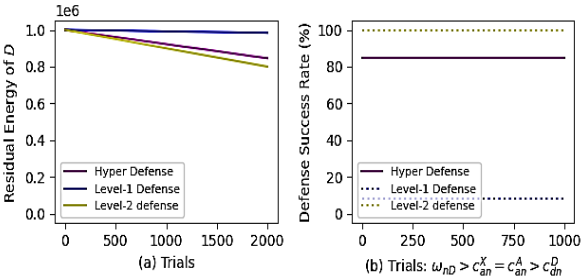
ب. زمانی که ω_{nD} از C_{an}^{A} و C_{dn}^{D} و C_{an}^{X} بیش‌تر و C_{dn}^{X} کم‌تر از C_{dn}^{D} باشد، یعنی با مقادیر اولیه



شکل (۷): زمانی که ω_{nD} از C_{an}^{A} و C_{dn}^{D} و C_{an}^{X} بیش‌تر، و C_{an}^{A} و C_{dn}^{D} کم‌تر از C_{an}^{X}

در این حالت همان‌طور که در شکل (۷) دیده می‌شود نرخ موفقیت ابر دفاع D در بازی جنگ سایبری سه‌جانبه پویا نزدیک به ۸۰ درصد (۸۰٪) است. در دفاع ایستای سطح یک بازیکن D نیز نرخ بالای ۲۰ درصد (۲۰٪) دیده می‌شود و مصارف انرژی سیستم‌ها همچنان همانند قبل عمل می‌کند.

ج. زمانی که ω_{nD} از C_{an}^{A} و C_{dn}^{D} بیش‌تر و C_{an}^{X} و C_{dn}^{D} نیز از C_{dn}^{D} بیش‌تر باشد، یعنی با مقادیر اولیه



شکل (۸): زمانی که ω_{nD} از C_{an}^{A} و C_{dn}^{D} و C_{an}^{X} بیش‌تر، و C_{dn}^{D} از C_{dn}^{X} و C_{dn}^{A} کم‌تر است

در شکل (۸) نرخ موفقیت ابر دفاع D در بازی جنگ سایبری سه‌جانبه پویا بالاتر از ۸۰ درصد (80%) و همچنان بالاتر از حالت دفاع ایستا سطح یک است. منتها سطح یک دفاع ایستای بازیکن D شاهد افت نرخ موفقیت به زیر ۲۰ درصد (20%) است.

تذکر ۶.

دقت شود در تمام موارد بازی جنگ سایبری سه‌جانبه نرخ موفقیت ابر دفاع پیشنهادی از دفاع ایستای سطح یک بیش‌تر است و مصرف انرژی آن بین مصرف انرژی دفاع ایستای سطح یک و مصرف انرژی دفاع ایستای سطح دو است.

۵. بهبود مدل پیشنهادی با بازی جنگ سایبری با آستانه (T, p)

در این بخش سعی می‌شود تعداد موفقیت یا عدم آن در بازی جنگ سایبری نیز در انتخاب سطح استراتژی انتخابی توسط بازیکنان اثر داده شود.

۵-۱. شرح بازی جنگ سایبری با آستانه (T, p)

برای اجرای بازی جنگ سایبری آستانه‌ای (T, p) با n سطح استراتژی، عددی صحیح چون T به‌عنوان تکرار آزمایش، ملاک تغییر استراتژی بازیکنان قرار داده می‌شود. به‌عبارت‌دیگر در T بار انجام بازی، برای i که $i \leq n$، اگر در حمله A با سطوح $\{a_i, \cdots, a_1, a_0\}$ به D با سطوح دفاعی $\{d_n, \cdots, d_1, d_0\}$، درصد موفقیت حمله از مقدار معین $p\%$ کم‌تر باشد، سعی می‌شود یک سطح به استراتژی‌های حمله اضافه شود تا با امکان انتخاب سطوح بالاتر و شدیدتر $\{a_{i+1}, a_i, \cdots, a_1, a_0\}$ به مدافع D حمله شود. بالعکس، اگر درصد موفقیت از مقدار مفروض $p\%$ بیش‌تر بود، فرض بر این گذاشته می‌شود که احتمالاً می‌توان با سطوح حمله کم‌هزینه‌تر نیز به هدف مطلوب دست‌یافت؛ لذا سعی می‌شود برای صرفه‌جویی در انرژی سیستم و جلوگیری از اتلاف منابع، با استراتژی در سطوح پایین‌تر $\{a_{i-1}, \cdots, a_1, a_0\}$ به D حمله شود. لازم به ذکر است، به طور هم‌زمان، همین روش در انتخاب سطوح استراتژی‌های دفاعی برای بازیکن D نیز می‌تواند در نظر گرفته شود.

$$C_{a1}^{X} = C_{a1}^{A} = 50, \quad C_{d1}^{D} = 30, \quad \omega_{1D} = 200$$
$$C_{a2}^{X} = C_{a2}^{A} = 80, \quad C_{d2}^{D} = 50, \quad \omega_{2D} = 300$$

تذکر ۷.

دقت شود تفاوت این مدل بازی جنگ سایبری و نتایج آن در کدنویسی و شبیه‌سازی رایانه‌ای مشهود است. به‌عبارت‌دیگر از دید نظری و قوانین همان بازی جنگ سایبری دوجانبه و یا حتی سه‌جانبه را می‌توان با این روش تلفیق کرد، منتها فرق اساسی این مدل بازی با آستانه (T, p) را می‌توان در کدنویسی و نتایج شبیه‌سازی شده منتج از آن‌ها جستجو کرد.

تذکر ۸.

لازم به ذکر است، با انتخاب یک درصد معین مثلاً $p\%$، می‌توان تعداد راهبُردها (سطوح) موردنیاز نسبت به آن را با انجام چندین‌باره آزمایش به دست آورد. به‌عبارت‌دیگر، با این روش بازی می‌توان تعداد استراتژی‌های بهینه موردنیاز در یک بازی جنگ سایبری، برای به‌دست‌آوردن درصد معینی از پیروزی را یافت.

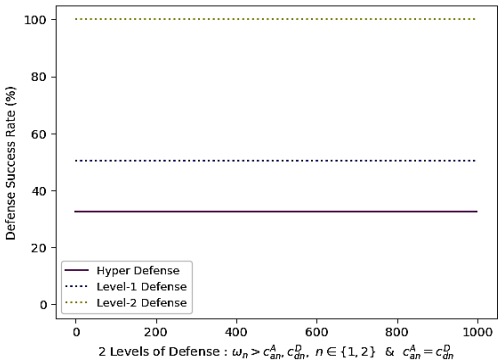
۵-۲. شبیه‌سازی رایانه‌ای بازی جنگ سایبری با آستانه (T, p)

در این بخش بازی سایبری دوجانبه یعنی یک مهاجم A و یک مدافع D در نظر گرفته می‌شود. ابتدا دقت شود که انتخاب سطح

صفر در دفاع برای دست‌یافتن به درصد معینی از موفقیت، بدین معناست که استراتژی ابر دفاع معادل سطح یک دفاع ایستا در نظر گرفته شود؛ لذا برای شروع تعداد سطوح دفاع از عدد دو آغاز می‌شود. یعنی برای انجام آزمایش نخست سطوح دفاع صفر و یک برای سامانه ابر دفاع در نظر می‌شود.

هدف: دست‌یافتن به $p = 50\%$ درصد موفقیت در دفاع با حداقل سطوح، در $T = 10^3$ تکرار.

معادلات موجود در رابطه‌های (۱) و (۲) را در نظر گرفته و ابتدا سطح دفاع صفر و سطح دفاع یک برای مدافع D انتخاب می‌شوند و مهاجم A در انتخاب هر سه سطح آزاد است. قوانین و مفروضات بازی همانند آنچه قبلاً گفته شد در نظر گرفته می‌شود. همچنین فرض بر این است که ω_{nD} از C_{an}^{A} و C_{dn}^{D} بیش‌تر و C_{an}^{A} با C_{dn}^{D} برابر باشد؛ یعنی به‌ازای مقادیر اولیه



شکل (۹): دو سطح دفاع برای مدافع D و آستانه $T = 10^3$ تکرار و درصد موفقیت هدف $p = 50\%$

در شکل (۹) دیده می‌شود که با دو سطح دفاع، نرخ موفقیت سامانه ابر دفاع به زیر ۴۰ درصد می‌رسد درحالی‌که دفاع ایستای سطح یک به نرخ موفقیت بالای ۵۰ درصد رسیده است. یعنی با این مقادیر اولیه برای متغیرها در رابطه (۲۶)، با اینکه سامانه ابر دفاع به موفقیت حدود ۴۰٪ رسیده؛ ولی اتخاذ دفاع ایستای سطح یک با موفقیت $p = 50\%$، بهتر عمل خواهد کرد که خود می‌تواند سطح انرژی سیستم را حفظ و به پایایی آن کمک کند.

۶. تحلیل شبیه‌سازی‌های رایانه‌ای

آنچه از کدهای شبیه‌سازی شده و نتایج حاصل از آن در بخش‌های قبل یعنی بازی‌های جنگ سایبری سه‌جانبه پویا و نیز بازی جنگ سایبری آستانه‌ای (T, p) حاصل می‌شود آن است که هرچند در اکثر موارد سامانه ابر دفاع (پویا) عملکرد بهتری نسبت به دفاع ایستا دارد، اما نتایج بسیار به مقادیر اولیه متغیرها وابسته است؛ لذا یافتن عملکرد بهتر در دفاع یا حمله، نیازمند آزمایش‌های بیش‌تر باتوجه‌به شرایط مسئله موردنظر و عوامل و شرایط محیطی است.

۷. ارزیابی عملکرد بازی پویای دوجانبه با سناریوی حمله به جمهوری اسلامی ایران

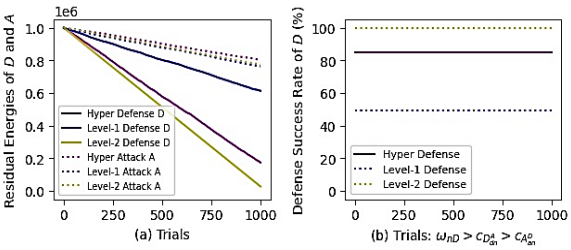
در این بخش، مدل بازی جنگ سایبری دوجانبه را برای سناریوی حمله به وزارت راه و شهرسازی جمهوری اسلامی ایران توسط رژیم متخاصم شبیه‌سازی کرده و به مقایسه نرخ موفقیت سامانه ابر دفاع پویا و دو سیستم دفاع ثابت "همیشه روشن" پرداخته می‌شود تا اعتبارسنجی دقیقی از عملکرد مدل توسعه داده شده صورت گیرد. اولین سیستم دفاع ثابت همیشه از دفاع با شدت کم (سطح) استفاده می‌کند که مؤلفه‌های دفاعی کم‌تری را در بر می‌گیرد و دومین سیستم دفاع ثابت همیشه از دفاع با شدت بالا (سطح دو) استفاده می‌کند که ~~$C_{dn}^{A} = C_{dn}^{D} = 50$~~ یعنی دارای مؤلفه‌های دفاعی بیش‌تر و بالطبع هزینه‌گذاری بیش‌تر است.

~~$\omega_{1D} = 100$~~ ~~$\omega_{2D} = 200$~~ (26)

مهاجم از فن‌حمله مایتره[1] استفاده کرده و زیرساخت‌های انرژی و اساسی وزارت راه و شهرسازی و اهداف بالقوه را در نظر می‌گیرد. کد شبیه‌سازی دارای دو بخش اصلی است: در مرحله نخست، اهداف بالقوه باتوجه‌به ارزش آن‌ها وزن‌دهی شده و احتمال انتخاب هر کدام مشخص می‌شود، سپس ماتریس حمله با ابعاد $n \times 3$ انتخاب می‌شود که n تعداد مؤلفه‌های موجود در حمله مایتره است به قسمی که ستون اول مؤلفه‌های حمله، ستون دوم احتمالات مربوط به هر مؤلفه و ستون آخر هزینه استفاده از آن مؤلفه است. حال ماتریس دفاع با ابعاد $m \times 3$ انتخاب می‌شود که همانند ماتریس حمله است با این تفاوت که m تعداد مؤلفه‌های موجود در توان دفاعی جمهوری اسلامی ایران است. در مرحله بعد هدف، مؤلفه‌های دفاع و حمله انتخاب و سطوح و هزینه‌های مرتبط با هر کدام مشخص می‌شود. سرانجام باتوجه‌به هزینه‌های به‌دست‌آمده و ارزش منابع، به تطبیق مدل پیشنهادی پویا با حمله سناریوی مدنظر پرداخته و در انتها نتایج بازی گزارش می‌شود.

مدل حمله - دفاع پیشنهادی سعی در دستیابی به یک استراتژی دفاعی مناسب برای سیستم با نظر گرفتن محدودیت منابع دارد. عملکرد سیستم با شناسایی دو معیار ارزیابی می‌شود: میانگین انرژی باقیمانده و نرخ موفقیت دفاعی. علاوه بر این، در مورد مقادیر اولیه فقط حالت c_{an} کم‌تر از c_{dn} در نظر گرفته می‌شود و ارزش اهداف نیز متناظر با ω_n است. تعداد مؤلفه‌های حمله یا دفاع مشخص‌کننده سطوح حمله یا دفاع است، به عبارتی سطح یک حمله تعداد مؤلفه کم‌تری نسبت به سطح دو حمله دارد و برای دفاع نیز به همین صورت.

[1] MITRE



شکل (۱۰): نتیجه حمله شبیه‌سازی شده و وضعیت سیستم D

دفاع سطح یک ثابت مقدار انرژی کم‌تری مصرف می‌کند، اما متوجه می‌شویم که میزان موفقیت دفاعی آن در مقایسه با مدل پیشنهادی ابر دفاع پایین‌تر است. ابر دفاع در مقایسه با دفاع سطح یک ثابت، نرخ موفقیت دفاعی خوبی ایجاد می‌کند (بالای ۸۰٪). همان‌طور که در شکل‌های (۱۰) نشان‌داده‌شده دستیابی به انرژی باقیمانده بالاتر در مقایسه با رویکرد دفاعی سطح ۲ ثابت، از مزایای دیگر ابر دفاع در این سناریو است.

۷-۱. شرح دقیق حمله شبیه‌سازی شده بر اساس مدل رایانه‌ای

در شکل‌های زیر نتیجه حاصل از حمله شبیه‌سازی شده بر اساس کد نوشته شده ارائه می‌شود تا تصویری شفاف‌تر از نوع بازی و نتیجه آن به دست آید. لازم به ذکر است عکس‌های موجود در این بخش از محیط برنامه‌نویسی استخراج شده است.

۷-۱-۱. مرحله اول برنامه

در این مرحله سطوح حمله و دفاع به همراه مؤلفه‌های آن‌ها مشخص می‌شود.

```
Description:

 This Model has 3 levels of attacks such that

 Level-0 Attack = No-Attack.

 Level-1 Attack = ['Impact: Data Destruction', 'Persistence: Event Triggered Execution', 'Discovery: Permission Groups Discover
y', 'Defense Evasion: Rootkit', 'Execution: Exploitation for Client Execution', 'Privilege Escalation: Abuse Elevation Control
Mechanism', 'Defense Evasion: Masquerading', 'Persistence: Account Manipulation', 'Execution: Shared Modules', 'Discovery: Syst
em Network Connections Discovery', 'Impact: Data Encrypted for Impact', 'Resource Development (Enterprise, ICS): Compromise Acc
ounts', 'Lateral Movement: Remote Service Session Hijacking', 'Execution: Inter-Process Communication', 'Persistence: Server So
ftware Component', 'Resource Development (Enterprise, ICS): Obtain Capabilities', 'Exfiltration (Enterprise, Mobile): Automated
Exfiltration', 'Persistence: Browser Extentions', 'Execution: Inter-Process Communication', 'Collection: Email Collection', 'Re
source Development (Enterprise, ICS): Develop Capabilities', 'Execution: Container Administration Command', 'Execution: Exploit
ation for Client Execution', 'Discovery: System Service Discovery', 'Defense Evasion: Signed Binary Proxy Execution', 'Defense
Evasion: Domain Policy Modification', 'Collection: Data from Local System', 'Execution: Shared Modules', 'Impact: Fireware Corr
uption', 'Impact: Service Stop', 'Defense Evasion: Domain Policy Modification', 'Execution: Software Deployment Tools', 'Defens
e Evasion: Indicator Removal on Host', 'Persistence: Modify Authentication Process', 'Discovery: Peripheral Device Discovery',
'Command and Control: Proxy', 'Initial Access: Exploit Public-Facing Application', 'Defense Evasion: Traffic Signaling', 'Defen
se Evasion: Weaken Encryption', 'Privilege Escalation: Access Token Manipulation', 'Impact: Data Manipulation', 'Impact: Data M
anipulation', 'Impact: Data Destruction', 'Impact: Fireware Corruption', 'Initial Access: Trusted Relationship', 'Discovery: Vi
rtualization/Sandbox Evasion', 'Persistence: Browser Extentions', 'Impact: System Shutdown/Reboot', 'Defense Evasion: Unused/Un
supported cloud Region', 'Command and Control: Non-Standard Port', 'Defense Evasion: Domain Policy Modification', 'Defense Evas
ion: Indirect Command Execcution', 'Discovery: System Location Discovery', 'Exfiltration (Enterprise, Mobile): Exfiltartion Ove
r Other Network Medium', 'Defense Evasion: Indicator Removal on Host', 'Initial Access: External Remote Services', 'Execution:
Container Administration Command', 'Execution: Software Deployment Tools', 'Defense Evasion: Masquerading', 'Command and Contro
l: Multi-Stage Channels', 'Discovery: Network Share Discovery', 'Defense Evasion: Exploitation for Defense Evasion', 'Defense E
vasion: File and Directory Permission Modification', 'Credential Access (Enterprise, Mobile): Network Sniffing', 'Discovery: Pe
rmission Groups Discovery', 'Lateral Movement: Software Development Tools', 'Reconnaissance (Enterprise, ICS): Phishing for Inf
ormation', 'Persistence: Account Manipulation'].

 Level-2 Attack = ['Impact: Data Destruction', 'Persistence: Event Triggered Execution', 'Discovery: Permission Groups Discover
y', 'Defense Evasion: Rootkit', 'Execution: Exploitation for Client Execution', 'Privilege Escalation: Abuse Elevation Control
Mechanism', 'Defense Evasion: Masquerading', 'Persistence: Account Manipulation', 'Execution: Shared Modules', 'Discovery: Syst
em Network Connections Discovery', 'Impact: Data Encrypted for Impact', 'Resource Development (Enterprise, ICS): Compromise Acc
ounts', 'Lateral Movement: Remote Service Session Hijacking', 'Execution: Inter-Process Communication', 'Persistence: Server So
ftware Component', 'Resource Development (Enterprise, ICS): Obtain Capabilities', 'Exfiltration (Enterprise, Mobile): Automated
Exfiltration', 'Persistence: Browser Extentions', 'Execution: Inter-Process Communication', 'Collection: Email Collection', 'Re
source Development (Enterprise, ICS): Develop Capabilities', 'Execution: Container Administration Command', 'Execution: Exploit
ation for Client Execution', 'Discovery: System Service Discovery', 'Defense Evasion: Signed Binary Proxy Execution', 'Defense
Evasion: Domain Policy Modification', 'Collection: Data from Local System', 'Execution: Shared Modules', 'Impact: Fireware Corr
uption', 'Impact: Service Stop', 'Defense Evasion: Domain Policy Modification', 'Execution: Software Deployment Tools', 'Defens
e Evasion: Indicator Removal on Host', 'Persistence: Modify Authentication Process', 'Discovery: Peripheral Device Discovery',
'Command and Control: Proxy', 'Initial Access: Exploit Public-Facing Application', 'Defense Evasion: Traffic Signaling', 'Defen
se Evasion: Weaken Encryption', 'Privilege Escalation: Access Token Manipulation', 'Impact: Data Manipulation', 'Impact: Data M
anipulation', 'Impact: Data Destruction', 'Impact: Fireware Corruption', 'Initial Access: Trusted Relationship', 'Discovery: Vi
rtualization/Sandbox Evasion', 'Persistence: Browser Extentions', 'Impact: System Shutdown/Reboot', 'Defense Evasion: Unused/Un
supported cloud Region', 'Command and Control: Non-Standard Port', 'Defense Evasion: Domain Policy Modification', 'Defense Evas
ion: Indirect Command Execcution', 'Discovery: System Location Discovery', 'Exfiltration (Enterprise, Mobile): Exfiltartion Ove
r Other Network Medium', 'Defense Evasion: Indicator Removal on Host', 'Initial Access: External Remote Services', 'Execution:
Container Administration Command', 'Execution: Software Deployment Tools', 'Defense Evasion: Masquerading', 'Command and Contro
l: Multi-Stage Channels', 'Discovery: Network Share Discovery', 'Defense Evasion: Exploitation for Defense Evasion', 'Defense E
vasion: File and Directory Permission Modification', 'Credential Access (Enterprise, Mobile): Network Sniffing', 'Discovery: Pe
rmission Groups Discovery', 'Lateral Movement: Software Development Tools', 'Reconnaissance (Enterprise, ICS): Phishing for Inf
ormation', 'Persistence: Account Manipulation', 'Defense Evasion: Deploy Container', 'Lateral Movement: Taint Shared Content'].

 At the same time we have 3 levels of defenses such that

 Level-0 Defend = No-Defend.

 Level-1 Defend = ['Monitoring in the Security Operations Center (SOC): Cyber Event Monitoring', 'Eradication: Malware Analysis
Operations', 'Cybersecurity and Crisis Management Steering Committee: Education of DucumentCybersecurity and Crisis Management
Steering Committee: DRP Document', 'Monitoring (Identifying Anomaly Patterns): Incident Handling', 'Eradication: Malware Analys
is Operations', 'Monitoring in the Security Operations Center (SOC): Cyber Event Monitoring', 'Identification: Level 1 Expert',
'Eradication: Review the Intruders Actions', 'Identification: Level 2 Expert', 'Identification: Service Manager', 'Eradication:
Attacker Access Cut Off', 'War Room: Operational roles', 'Eradication: Identify All Compromised Systems', 'War Room: Evaluatio
n', 'War Room: Operational roles', 'War Room: Operational roles'].

 Level-2 Defend = ['Monitoring in the Security Operations Center (SOC): Cyber Event Monitoring', 'Eradication: Malware Analysis
Operations', 'Cybersecurity and Crisis Management Steering Committee: Education of DucumentCybersecurity and Crisis Management
Steering Committee: DRP Document', 'Monitoring (Identifying Anomaly Patterns): Incident Handling', 'Eradication: Malware Analys
is Operations', 'Monitoring in the Security Operations Center (SOC): Cyber Event Monitoring', 'Identification: Level 1 Expert',
'Eradication: Review the Intruders Actions', 'Identification: Level 2 Expert', 'Identification: Service Manager', 'Eradication:
Attacker Access Cut Off', 'War Room: Operational roles', 'Eradication: Identify All Compromised Systems', 'War Room: Evaluatio
n', 'War Room: Operational roles', 'War Room: Operational roles', 'War Room: Decision Making', 'Recovery: Change Security Tools
Settings', 'Recovery: Installing Security Patches', 'Activating the CSIRT Team: Containment', 'Monitoring in the Security Opera
tions Center (SOC): Anomaly Detection', 'War Room: Decision Making'].
```

شکل (۱۱): توضیح مؤلفه‌ها و سطوح حمله/دفاع

همان‌طور که در شکل (۱۱) دیده می‌شود، ۳ سطح حمله که هر سطح شامل مؤلفه‌های حمله (اهداف مورد هجوم) است. همچنین ۳ سطح دفاع نیز مشخص شده است که هر سطح دفاع شامل مؤلفه‌های دفاع (توانایی‌های مدافع) است.

۷-۱-۲. مرحله دوم برنامه

در این مرحله به گزارشی از نوع حمله، مهاجم، مدافع، اهداف و تعداد مؤلفه‌های حمله و دفاع در همه سطوح، هزینه‌ها و ارزش منابع به‌دست‌آمده در محاسبات و بررسی‌های حین حمله پرداخته می‌شود.

```
The Report of Game:

 The Expriment was executed in The date: 2024-12-09 00:47:49.764713. It was a 'MITRE' attack. The Attacker is 'The Unite 8200 o
f Regime' and The Defender is the 'The Counter Cyber Attack of Iran, Islamic Republic of' the targets of attack were:

 Targets of Attack = ['Deputy for Legal Affairs of the Parliament and Provinces', 'Deputy of Urban Planning and Architecture',
'Housing Bank', 'The Supreme Council for Organizing Authorized Entry and Exit Points of the Country', 'Office of Performance Ma
nagement and Citizens Rights', 'Supreme Aviation Council of Iran', 'Security Center', 'Deputy for Management Development and Hu
man Resources'] that overal worth was 2290.

 The attack was consist of: level-0 attack with 0-number components, level-1 attack with 68-number components and level-2 attac
k with 70-number components such that respectively, the cost of attacks were 0, 344 and 353. Consequently, it had level-0 defen
d with 0-number components, level-1 defend with 16-number components and level-2 defend with 22-number components such that the
cost of defends were 0, 569 and 973.
```

شکل (۱۲): گزارش بازی مهاجم/مدافع

همان‌طور که در شکل (۱۲) دیده می‌شود، گزارش بازی به شرح زیر است:

حمله در تاریخ ۰۹-۱۲-۲۰۲۴ در ساعت ۰۰:۴۷:۴۹ رخداده است. این یک حمله از نوع مایتره است. مهاجم «واحد ۸۲۰۰ رژیم» و مدافع «واحد ضد حمله سایبری جمهوری اسلامی ایران است». اهداف حمله عبارت‌اند از:

اهداف حمله= [«معاونت حقوقی مجلس و استان‌ها»، «معاونت شهرسازی و معماری»، «بانک مسکن»، «شورای‌عالی ساماندهی مبادی ورودی و خروجی مجاز کشور»، «دفتر مدیریت عملکرد و حقوق شهروندی»، «شورای‌عالی هواپیمایی کشور»، «مرکز حراست»، «معاونت توسعه مدیریت و منابع انسانی»] که ارزش کل اهداف مورد حمله ۲۲۹۰ واحد است.

حمله شامل: سطح-۰ با ۰ مؤلفه، سطح-۱ با ۶۸ مؤلفه و سطح-۲ با ۷۰ مؤلفه است به قسمی که هزینه‌های سطوح حمله به ترتیب ۰، ۳۴۴ و ۳۵۳ است. متعاقباً، در دفاع: سطح-۰ با ۰ مؤلفه، سطح-۱ با ۱۶ مؤلفه و سطح-۳ با ۲۲ مؤلفه دفاع است به قسمی که هزینه‌های سطوح دفاع به ترتیب ۰، ۵۶۰ و ۹۷۳ است.

۷-۱-۳. مرحله سوم برنامه

نهایتاً تحلیل به‌دست‌آمده بر اساس شکل (۱۱) ارائه می‌شود.

```
The Result:

 As we can see in the Figure: In 1000 times executing the expriment, the Hyper defend has 84% success rate, static level-1 defe
nd 49% success rate and static level-2 defend 100% success rate. Hyper defend system energy consuming is more than static level
-1 defend and less than static level-2 defend.
```

شکل (۱۳): نتیجه حاصل از حمله/دفاع بر اساس شکل (۱۱)

بر اساس شکل (۱۳) نتیجه بازی به شرح زیر است:

در ۱۰۰۰ دور انجام آزمایش، سامانه ابر دفاع دارای نرخ موفقیت ۸۴٪، دفاع ثابت سطح-۱ دارای نرخ موفقیت ۴۹٪ و دفاع ثابت سطح-۲ دارای نرخ موفقیت ۱۰۰٪ است. میزان مصرف انرژی سامانه ابر دفاع بیش‌تر از دفاع ثابت سطح-۱ و کم‌تر از دفاع ثابت سطح-۲ است.

۸. نتایج و بحث

سیستم ابر دفاع پیشنهادی در همه موارد ذکر شده به‌جای روشن‌کردن همیشه سیستم دفاعی، به‌ویژه برای شبکه‌ای که بر بهره‌وری انرژی تأکید دارد، در انرژی صرفه‌جویی می‌کند و به میزان موفقیت بالایی دست می‌یابد. این سیستم دفاعی بر تعاملات پویا بین مهاجم و مدافع استوار است.

باتوجه‌به روش بکار رفته در مراحل فوق می‌توان این مدل را برای هر سیستم موجود پیاده‌سازی کرد و باتوجه‌به عوامل محیطی مختص به آن سیستم نیز آن را بهینه کرد.

۹. مقایسه

برای مطالعه بیش‌تر در موضوع امنیت سایبری و نیز کاربرد نظریه بازی‌ها در آن به منابع [۳۰-۲۳] مراجعه شود. برای وضوح بیش‌تر توضیحات زیر ارائه می‌شود:

در منبع [۲۳] به تعداد ۱۵ مقاله کامل موجود است که این مقالات در بخش‌های موضوعی: امنیت سیستم‌ها، اقتصاد، نقطه تعادل و کنترل، فریب سایبری، شبکه و حریم خصوصی، یادگیری ماشینی خصمانه و سیستم‌های سایبری - فیزیکی تقسیم‌بندی شده‌اند.

در منبع [۲۴] بر این امر تصریح شده است که در زمینه تضمین امنیت سیستم‌های اطلاعاتی، فن شکار تهدید سایبری، ابزاری حیاتی برای شناسایی چنین تهدیدهایی است. آنچه موردنیاز است یک ابزار شکار تهدید سایبری مستقل است که بتواند به طور فراگیرتری اجرا شود و رقابت را به میزان قابل‌توجهی در زمان، هزینه و البته منابع تحلیلی محدود کاهش دهد. با استفاده از نظریه بازی‌ها (بازی‌های زنجیره‌ای [1]) توسعه الگوریتم‌های مناسب برای اطلاع‌رسانی به یک قابلیت شکار تهدید کاملاً مستقل، شرح داده شده است. مجموعه‌ای از بازی‌ها که در آنها استراتژی‌های شکار تهدید می‌توانند ارزیابی و اصلاح شوند.

در منبع [۲۵] یک روش تخصیص بهینه منابع دفاعی برای دفاع پیشگیرانه در برابر حملات سایبری بالقوه در شبکه هوشمند بر اساس مدل بازی تکاملی [2] برای توصیف رفتار بازی مهاجمان و مدافعان و فرمول تعادل پاسخ کوانتومی برای محاسبه احتمال حمله ارائه شده است. یک مدل بازی دولایه برای به‌دست‌آوردن طرح تخصیص بهینه منابع دفاعی به‌جای یک استراتژی تعادل نش ساده نیز پیشنهاد شده است.

در منبع [۲۶] سعی بر شناسایی عوامل مؤثر بر فرهنگ و آگاهی امنیت سایبری با استفاده از تحلیل مضمون است. داده‌های پژوهش در حوزه فرهنگ و آگاهی امنیت سایبری در داخل و خارج کشور است که با بهره‌گیری از روش تحلیل مضمون، در چارچوب نرم‌افزار *MAXQDA* مورد بررسی قرار گرفته است. تا به‌گونه‌ای منطقی و اصولی به کاهش جرائم سایبری و حل مشکلات مرتبط با آن بپردازد.

منبع [۲۷] به ارزشیابی مطلوبیت امنیت اطلاعات و شبکه سایبری در بندر امام خمینی (ره) از منظر پدافند غیرعامل با استفاده از پانزده گویه/شاخص پرداخته است. از آزمون کلموگروف - اسمینروف به‌منظور نرمال بودن داده‌ها و جهت بررسی وضعیت متغیرهای پژوهش از آزمون بارتلت و *KMO* و همچنین برای رتبه‌بندی شاخص‌ها از مدل فریدمن استفاده شده است.

در منبع [۲۸] از مدل مارکوف برای مدل‌سازی و نمایش تفاوت ذاتی عملکرد کاربران و نفوذگران شبکه استفاده شده، با این تفاوت که مدل ارائه‌شده با وصله خودکار و روند موران متفاوت بود و بیشتر به مدل رأی‌دهندگان شباهت دارد. مدل سیستم دینامیکی ارائه‌شده بر اساس تقریب میانگین میدان است که به طور هدفمند کارایی دفاع سایبری فعال را مشخص می‌نماید.

در منبع [۲۹] چارچوبی چهارلایه جهت استخراج اقدامات اثرگذار بازیگران حوزه‌ی بدافزار با رویکرد نظریه‌ی بازی ارائه شده است. چارچوب پیشنهادی، بر اساس یک مطالعه موردی شامل ۱۲ فعالیت مهاجم و ۱۲ فعالیت مدافع در قالب سه بازی، مدل‌سازی و ارزیابی شده است. کاهش فضای حالت بازی، ارزش‌گذاری اقدامات و استخراج اقدامات مؤثر و وضعیت‌های تعادلی مطلوب بازیگران از مزایای چارچوب پیشنهادی است.

منبع [۳۰] به حل چالش اصلی تخصیص منابع محاسباتی در رایانش مه می‌پردازد. با استفاده از الگوریتم ترکیبی تعادل نش و الگوریتم مزایده، تخصیص منابع بهبودیافته است. در هر مرحله از الگوریتم هر بازیکن بر اساس راهبرد سایر بازیکنان بهترین راهبرد را تولید می‌کند. نتایج پژوهش نشان از برتری بهره‌وری گره مه و بهره‌وری اپراتور خدمات داده در روش پیشنهادی در مقایسه با الگوریتم بازی استکلبرگ دارد.

۱۰. نتیجه‌گیری

آنچه از کدهای شبیه‌سازی شده و نتایج حاصل از آن در بخش‌های قبل، یعنی بازی‌های جنگ سایبری سه‌جانبه پویا و نیز بازی جنگ سایبری آستانه‌ای (T, p) حاصل می‌شود آن است که هرچند در اکثر موارد سامانه ابر دفاع (پویا)

[1] Chain Games
[2] Evolutionary Game

عملکرد بهتری نسبت به دفاع ایستا دارد؛ اما نتایج بسیار به مقادیر اولیه متغیرها وابسته است؛ لذا یافتن عملکرد بهتر در دفاع یا حمله نیازمند آزمایش‌های بیش‌تر باتوجه‌به شرایط مسئله موجود و عوامل محیطی است.

چالش‌های پیش رو این است که مدل حمله - دفاع پیشنهادی سعی در دستیابی به یک استراتژی دفاعی مناسب برای سیستم موردنظر با درنظرگرفتن محدودیت منابع دارد. عملکرد سیستم با شناسایی دو معیار ارزیابی شد: میانگین انرژی باقیمانده و نرخ موفقیت دفاعی.

نتایج به‌دست‌آمده مطلوب و موید مدل پیشنهادی است. آنچه در تمام موارد به‌عنوان یک چالش است و باید در نظر گرفته شود، حالات و مقادیر اولیه سیستم مورد آزمایش است که چه در بخش دفاع و چه در بخش حمله باید موردتوجه قرار گیرد که به بررسی دقیق نوع مسئله و ابعاد مختلف آن وابسته است.

از مزایای مدل پیشنهادی این است که هرچند برای یک سناریوی مدنظر در وزارت راه و شهرسازی مورد آزمایش و تحلیل قرار گرفت؛ ولی به‌وضوح قابل آزمایش و بهره‌وری در سایر بخش‌های موردنیاز کشور است و می‌تواند نتایج خوبی در بخش آموزش برای آمادگی قبل از حمله سایبری و یا بهبود عملکرد یک سیستم بعد از وقوع تهدید سایبری داشته باشد.

همچنین از مزایای دیگر ارائه شده در این تحقیق معرفی بازی جنگ سایبری سه‌جانبه پویاست که با افزایش حالات استراتژی نسبت به بازی جنگ سایبری دوجانبه به ارتقا مدل پیشنهادی قبل در [۲۲] منجر شده است. همان‌گونه که قبلاً بیان شد در مدل‌سازی‌های قبلی بر اساس نظریه بازی‌ها [۲-۱] و [۴]، مهاجمان و مدافعان را تنها با دو استراتژی، مدل می‌کردند، اما مدل‌سازی بر اساس سطوح مختلف و تأکید بر پویایی مدل از مزایای دیگر این طرح است که با معرفی بازی جنگ سایبری آستانه‌ای (T,P)به بهینه‌سازی تعداد این سطوح حمله/دفاع نیز توجه شده است که باتوجه‌به درنظرگرفتن محدودیت منابع بسیار حائز اهمیت است.

۱۱. منابع

[1] Y. Wang, Y. Wang, J. Liu, Z. Huang, and P. Xie, "A survey of game theoretic methods for cyber security," in IEEE First International Conference on Data Science in Cyberspace (DSC), June 2016.

[2] .S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in 43rd Hawaii International Conference on System Sciences, pp. 1–10, Jan 2010.

[3] A. E. Chukwudi and I. C. Eze Udoka, "Game theory basics and its application in cyber security," Advances in Wireless Communications and Networks, vol. 3, no. 4, pp. 45–49, 2017.

[4] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacs¸ar, and J.-P. Hubaux, "Game theory meets network security and privacy," ACM Computing Surveys (CSUR), vol. 45, no. 3, p. 25, 2013.

[5] M. Fallah, "A puzzle-based defense strategy against flooding attacks using game theory," IEEE Transactions on Dependable and Secure Computing, vol. 7, pp. 5–19, Jan 2010.

[6] Y. Liu, C. Comaniciu, and H. Man, "A bayesian game approach for intrusion detection in wireless ad hoc networks," in Proceeding from the 2006 workshop on Game theory for communications and networks, p. 4, ACM, 2006.

[7] M. Mohi, A. Movaghar, and P. M. Zadeh, "A bayesian game approach for preventing dos attacks in wireless sensor networks," in Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on, vol. 3, pp. 507–511, IEEE, 2009.

[8] D. Fudenberg and J. Tirole, "Game theory. 1991," Cambridge, Massachusetts, vol. 393, 1991.

[9] V. P. Singh, S. Jain, and J. Singhai, "Hello flood attack and its countermeasures in wireless sensor networks," IJCSI International Journal of Computer Science Issues, vol. 7, no. 11, pp. 23–27, 2010.

[10] A. Dubey, D. Meena, and S. Gaur, "A survey in hello flood attack in wireless sensor networks," Int. J. Eng. Res. Technol, vol. 3, 2014.

[11] M. S. Haghighi and K. Mohamedpour, "Securing wireless sensor networks against broadcast attacks," in Telecommunications, 2008. IST 2008. International Symposium on, pp. 49–54, IEEE, 2008.

[12] R. Singh, D. J. Singh, and D. R. Singh, "Hello flood attack countermeasures in wireless sensor networks," 2016.

[13] R. S. Hassoubah, S. M. Solaiman, and M. A. Abdullah, "Intrusion detection of hello flood attack in wsns using location verification scheme," International Journal of Computer and Communication Engineering, vol. 4, no. 3, p. 156, 2015.

[14] R. Rehman, G. Hazarika, and G. Chetia, "Malware threats and mitigation strategies: a survey," Journal of Theoretical and Applied Information Technology, vol. 29, no. 2, pp. 69–73, 2011.

[15] I. You and K. Yim, "Malware obfuscation techniques: A brief survey," in 2010 International Conference on Broadband, Wireless Computing, Communication and Applications, pp. 297–300, Nov 2010.

[16] A. Sharma and S. K. Sahay, "Evolution and detection of polymorphic and metamorphic malwares: A survey," arXiv preprint arXiv:1406.7061, 2014.

[17] J. Kim, S. Lee, J. M. Youn, and H. Choi, "A study of simple classification of malware based on the dynamic api call counts," in International Conference on Computer Science and its Applications, pp. 944–949, Springer, 2016.

[18] M. Egele, T. Scholte, E. Kirda, and C. Kruegel, "A survey on automated dynamic malware-analysis techniques and tools," ACM computing surveys (CSUR), vol. 44, no. 2, p. 6, 2012.

[19] O. Nakhila and C. Zou, "Parallel active dictionary attack on ieee 802.11 enterprise networks," in MILCOM IEEE Military Communications Conference, pp. 265–270, Nov 2016.

[20] V. Goyal, V. Kumar, M. Singh, A. Abraham, and S. Sanyal, "Compchall: addressing password guessing

attacks," in Information Technology: Coding and Computing, ITCC. International Conference on, vol. 1, pp. 739–744, IEEE, 2005.

[21] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," IEEE Communications Surveys Tutorials, vol. 18, pp. 94–104, Firstquarter 2016.

[22] A. Attiah, M. Chatterjee and C. C. Zou, "A Game Theoretic Approach to Model Cyber Attack and Defense Strategies," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO,USA,2018,pp.17,doi:10.1109/ICC.2018.8422719

[23] A. Sinha, J. Fu, Q. Zhu, T. Zhang, "Decision and Game Theory for Security" 15th International Conference, GameSec, New York City, NY, USA, October 16–18, 2024, Proceedings. Doi: https://doi.org/10.1007/978-3-031-74835-6, 2024

[24] Groce, P.,: Using Game Theory to Advance the Quest for Autonomous Cyber Threat Hunting. Carnegie Mellon University, Software Engineering Institute's Insights (blog), Accessed June 3, 2025, https://insights.sei.cmu.edu/blog/Using-Game Theory -to-Advance-Cyber-Threat-Hunting

[25] Hui Ge, Lei Zhao, Dong Yue, Xiangpeng Xie, Linghai Xie, Sergey Gorbachev, Iakov Korovin, Yuan Ge, "A game theory based optimal allocation strategy for defense resources of smart grid under cyber-attack", Information Sciences, Volume 652, 19759, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2023.119759. 2024.

[26] Heydari, S., Barzegar, M., Mohammad Davoodi, A. H. (2023). 'Identify the Factors Affecting the Culture and Awareness of Cyber Security Using Theme Analysis', Electronic and Cyber Defense, 11(1), pp. 67-80 , 2023. DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1402.11.1.6.7 (in persian)

[27] Khouzestani, L., Maroofnezhad, A. 'Assessment of Desirability of Information Security and Cyber Network Indices in Ports with Emphasis on Passive Defense (Case Study: Imam Khomeini Port Complex) ', Electronic and Cyber Defense, 12(4), 2025. DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.4.8 (in persian)

[28] Dadashtabar Ahmadi, K., mahmoudbabouei, M. 'The Presentation of an Active Cyber Defense Model for Application in Cyber Deception Technology', Electronic and Cyber Defense, 9(4), pp. 125-140. 2022. DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1400.9.4.10.3 (in persian)

[29] Abbasi, M., Ghayoori, M. 'A Framework for Evaluating Malware and Countermeasures with an Analytical Approach based on the Game Theory Case Study: Actors' Actions Based on Environmental Evidence', Electronic and Cyber Defense, 10(1), pp. 47-71. 2022. DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1401.10.1.5.9 (in persian)

[30] mohammady talvar, H., haj seyyed javadi, S. H., Navidi, H., rezakhani, A. (2022). 'The IoT Resource Allocation Improvement in Fog Computing Using Non-Cooperative Game Theory', Electronic and Cyber Defense, 9(4), pp. 147-158. 2022. DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1400.9.4.12.5 (in perssian)