Sharif Industrial Engineering and Management Journal (2025), 41(1), 109-121

Sharif University of Technology

https://sjie.journals.sharif.edu/

Research Article

Game-Theoretic Approach for Pricing Cloud Computing and Determining the Security Level of Security Provider Companies

Mahdie Sadeghian, Morteza Rasti-Barzoki* and Hossein Khosroshahi

Department of Industrial and Systems Engineering, Isfahan University of Technology, Isfahan

* corresponding author: (rasti@cc.iut.ac.ir)

Article Info

Article history:

Received:15 June 2024

Revised:17 August 2024

Accepted:31 August 2024

Keywords:

Pricing,
investment,
black hat hacker,
cybersecurity,
game theory.

Abstract

Since hardware may experience sudden failure and software solutions are often costly, users need an environment to perform computational and data storage tasks without expensive hardware and software. Cloud computing can provide this capability, but the presence of cyber hackers and their attacks raises user concerns about their data security. As information is precious, losing it can result in significant costs for the information owner. To address this problem, companies have emerged to ensure the safety of cloud computing services, and cloud users can entrust their information security to them. This article aims to examine the competition between security provider companies and cyber hackers using game theory and determine the strategies of each player to determine the game structure. These structures are based on the leader's decision to determine the security level initially or after an attack has occurred. The company decides what price to offer the user based on the value of the information, the amount of effort needed to return the information after a successful attack, the security level it needs to maintain, and the power structure. Similarly, the hacker decides how much effort to put in based on the value of the information. The results show that the price decreases linearly based on the information value when the company is the leader. In addition to the results obtained about the company's profit, it shows that in general, the company's profit, when it is a leader, is more than when it is a follower, and in particular, the company's profit based on the percentage of returned information in the leader's position is much higher than in the position of the follower. The level of security provided is also different according to the position of the company, and when the company is the leader, it is much higher than when the company is the follower, based on the hacker's credibility and the value of the returned information.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

To Cite this article:

Sadeghian, M., Rasti-Barzoki, M. and Khosroshahi, H. 2025. A game-theoretic approach for pricing cloud computing and determining the security level of security provider companies, Sharif Industrial Engineering and Management Journal, 41(1), 109-121. https://doi.org/10.24200/j65.2024.64530.2406

مجله علمی مهندسی صنایع و مدیریت شریف

https://sjie.journals.sharif.edu

مقاله‌ی پژوهشی

یک رویکرد نظریه‌ی بازی برای قیمت‌گذاری رایانش ابری و تعیین سطح امنیت شرکت‌های ارائه‌دهنده‌ی امنیت

مهدیه صادقیان، مرتضی راستی برزکی* و حسین خسروشاهی

دانشکده‌ی مهندسی صنایع و سیستم‌ها، دانشگاه صنعتی اصفهان، اصفهان، ایران.

*نویسنده مسئول (rasti@cc.iut.ac.ir)

اطلاعات مقاله

تاریخ دریافت : ۱۴۰۳/۰۳/۲۶

تاریخ اصلاحیه : ۱۴۰۳/۰۵/۲۷

تاریخ پذیرش : ۱۴۰۳/۰۶/۱۰

واژگان کلیدی:

قیمت‌گذاری،

سرمایه‌گذاری،

هکر کلاه سیاه،

امنیت سایبری،

نظریه‌ی بازی.

چکیده

سخت‌افزارها ممکن است دچار خرابی‌های ناگهانی شوند و راه‌حل‌های نرم‌افزاری اغلب پرهزینه‌اند، بنابراین کاربران به محیطی نیاز دارند که بتوانند بدون نیاز به سخت‌افزار و نرم‌افزار گران‌قیمت، محاسبات و ذخیره‌سازی داده‌ها را انجام دهند. رایانش ابری این امکان را فراهم می‌کند، اما نگرانی‌هایی درباره‌ی امنیت داده‌ها در برابر حملات سایبری وجود دارد. شرکت‌های امنیتی با تعیین سطح امنیت و قیمت‌گذاری براساس ارزش اطلاعات و درصد بازیابی می‌توانند از داده‌های کاربران محافظت کنند. آن‌ها می‌توانند راهبردهای متفاوتی مانند پیشگیری از حملات (ساختار رهبر) یا انتظار برای وقوع حمله و سپس مقابله (ساختار پیرو) را انتخاب کنند. در پژوهش حاضر، دو ساختار ذکرشده با حضور هکر کلاه سیاه بررسی شده است. نتایج نشان داده‌اند که ساختار قدرت، تأثیر زیادی در مقدار قیمت نداشته است، اما سود را به‌شدت تحت تأثیر قرار داده است. همچنین مشخص شده است که ارزش اطلاعات و کاهش اعتبار شرکت در اثر حمله‌ی موفق، در سود و میزان تقاضا تأثیر زیادی دارد.

۱. مقدمه

چاک رابینز[1]، مدیرعامل سیسکو، می‌گوید اگر جرایم سایبری به‌عنوان یک کشور در نظر گرفته شوند، سومین اقتصاد بزرگ جهان را خواهند داشت[2]. با افزایش تهدیدهای سایبری، انتظار می‌رود تا سال ۲۰۳۱، هر دو ثانیه یک حمله‌ی سایبری رخ دهد. براساس گزارش‌های ارائه‌شده، مهاجمان سایبری بیش از ۴ میلیارد رکورد را در سال ۲۰۲۱ به سرقت برده‌اند[2]. به همین علت، تمرکز شرکت‌ها به‌طورفزاینده‌ای بر روی توسعه‌ی اقدام‌های امنیت سایبری است.[۱] در این راستا، سرمایه‌گذاری در امنیت سایبری با هدف کمینه‌سازی آسیب ناشی از حملات انجام می‌گیرد.[۲] ارائه‌دهندگان امنیت، مسئول ایجاد امنیت برای سایر شرکت‌ها هستند.[۳] شرکت‌های ارائه‌دهنده‌ی امنیت می‌توانند با تعیین سطح امنیت برای جلوگیری از حمله و سپس تعیین قیمت براساس ارزش اطلاعات و درصد قابل بازیابی اطلاعات، رهبری ساختار قدرت را در اختیار بگیرند. از طرف دیگر، شرکت‌های مذکور می‌توانند با انتظار برای وقوع یک حمله، موقعیت پیرو را بگیرند و سپس سطح امنیتی را براساس مهارت هکر و ارزش اطلاعات تعیین کنند. در این حالت، حمله در حال وقوع است و هکر برای دستیابی به اطلاعات تلاش می‌کند و شرکت در حال رسیدگی و ایجاد امنیت است. آمارهای اخیر نشان می‌دهند که فقط ۰/۰۵٪ از شرکت‌ها مایل به گرفتن موقعیت رهبری هستند[2].

در سال‌های اخیر، مطالعات گسترده‌ای در مورد امنیت سایبری، راهبردهای شرکت‌ها و هکرها، مسائل سرمایه‌گذاری و قیمت‌گذاری در امنیت سایبری انجام شده است.[۴] قیمت‌گذاری از مسائل مهمی است که نه فقط در حوزه‌ی امنیت سایبری، بلکه در حوزه‌های مختلف دیگری، از جمله: حوزه‌ی زنجیره‌ی تأمین چندکاله صورت می‌گیرد.[۵] چن[3] و همکاران (۲۰۲۲)،[۶] به قیمت‌گذاری زنجیره‌ی تأمین چندکاله با استفاده از قرارداد تقسیم درآمد پرداخته‌اند. در حوزه‌ی امنیت سایبری نیز، بارتلوما[4] (۲۰۱۸)،[۷] مدل شای (۲۰۰۱)،[۸] را توسعه داده است، که در سه سطح گسترش یافته است. در مدل ذکرشده، شرکت قیمت را در سطح اول ارائه می‌کند و سپس براساس آن، اندازه‌ی شبکه تعیین می‌شود.[۹] در زمینه‌ی قیمت‌گذاری، ابتدا مدلی ارائه می‌شود، که قیمت براساس تقاضا و عرضه‌ی واقعی ابر تعیین می‌شود.

[1] Chuck Robbins
[2] cybersecurityventures.com
[3] Chen
[4] Bartholomae

استناد به این مقاله:

صادقیان ، مهدیه، راستی برزکی، مرتضی، و خسروشاهی، حسین، ۱۴۰۴. **یک رویکرد نظریه‌ی بازی برای قیمت‌گذاری رایانش ابری و تعیین سطح امنیت شرکت‌های ارائه‌دهنده‌ی امنیت**. مهندسی صنایع و مدیریت شریف ، ۴۱(۱)، صص.۱۰۹-۱۲۱. https://doi.org/10.24200/j65.2024.64530.2406

شاپا الکترونیکی: ۲۶۷۶-۴۷۵X

ماهیت جرایم سایبری در مقایسه با گذشته به‌دلیل پیچیدگی روزافزون هکرها پیچیده‌تر شده است. چنگ[1] و همکاران (۲۰۲۲)،[۱۰] هکرها را به ۱۳ نوع دسته‌بندی کرده‌اند. سپس، ۷ انگیزه و راهبرد مرتبط با آن‌ها را بررسی و از آن به‌عنوان چارچوبی برای کمک به تحلیل‌گران و مهندسان امنیتی استفاده کرده‌اند. طبقه‌بندی دیگر هکرها مربوط به سه دسته‌ی: کلاه سفید، کلاه خاکستری، و کلاه سیاه است. کالدول[2] (۲۰۱۱)،[۱۱] در مورد هکرهای اخلاقی یا کلاه سفید، بحث کرده و آن‌ها را برخلاف هکرهای کلاه سیاه دانسته‌اند، که به بهبود شرکت‌ها و افزایش امنیت با افزایش قابلیت‌های آن‌ها کمک می‌کنند. کهن[3] و همکاران (۲۰۲۲)،[۱۲] همکاری و عدم همکاری هکرهای کلاه خاکستری تصمیم به همکاری با ارائه‌ی جزئیات آسیب‌پذیری به شرکت ارائه‌دهنده‌ی امنیت می‌کند، شرکت مذکور نیز مایل است تا با هکر همکاری کند و آسیب‌پذیری خود را کاهش دهد.

یکی از راه‌های بررسی سطوح امنیت و اشتراک‌گذاری اطلاعات، استفاده از رویکرد نظریه‌ی بازی است.[۱۳] نظریه‌ی بازی، پتانسیل بالایی برای ایجاد یک محیط تحلیلی در حوزه‌ی امنیتی دارد، که با درنظرگرفتن حملات و دفاع، تعاملات بین هکر و شرکت را بررسی می‌کند.[۱۴] همچنین، طبق یک نظرسنجی، نظریه‌ی بازی می‌تواند درک پژوهشگران از مسائل امنیتی و حریم خصوصی را تسهیل کند،[۱۵] و چارچوبی است که به مهندسان امنیتی کمک می‌کند تا راهبردهای بهینه را برای کاهش آسیب حملات سایبری به‌کار گیرند.[۱۶] در این حوزه، پژوهش‌های بسیاری انجام شده است.[۷، ۸، ۱۲، و ۱۷-۱۹]

در برخی پژوهش‌های پیشین، کاربر ابری به‌عنوان بازیکنی بوده است که بین دو راهبرد اشتراک و عدم اشتراک اطلاعات خود، تصمیم‌گیری کرده است؛ در صورتی که ارزش اطلاعات آن مشاهده نشده است.[۱۹] علاوه‌بر این، اگرچه بارتلوما (۲۰۱۸)،[۷] بازی هکر و شرکت را با استفاده از رویکرد استکلبرگ حل کرده است، اما فقط موقعیت رهبر برای شرکت بیان شده است. در صورتی که براساس گزارش‌های اعلام‌شده[۲]، شرکت می‌تواند در جایگاه پیرو نیز باشد. همچنین در نوشتارهای ارائه‌شده، نوع هکر نیز مطرح نبوده است.

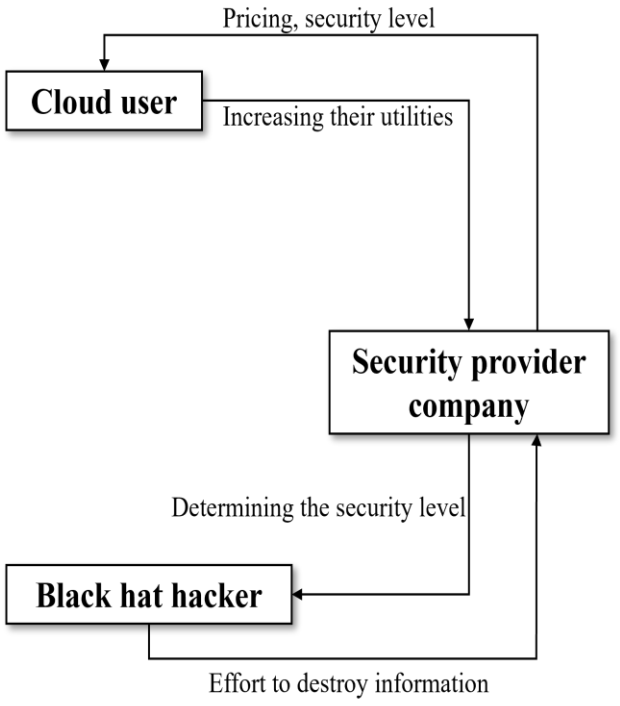
نوآوری پژوهش حاضر، وجود کاربر ابری به‌عنوان بازیکن خارجی است، که ارزش اطلاعات وی در به‌دست‌آمدن مقدار تقاضا مؤثر است. علاوه‌بر این، نوشتار حاضر ارزش اطلاعات از دست‌رفته را در تعیین موقعیت یک شرکت براساس میزان تلاش هکر در نظر می‌گیرد. همچنین نوع هکر و میزان تلاش او برای دستیابی به اطلاعات نیز مد نظر بوده است؛ تا توابع سود، دقیق‌تر مدل‌سازی شوند. وجود دو ساختار قدرت برای قیمت‌گذاری و تعیین سطح امنیت نیز از دیگر نوآوری‌های پژوهش حاضر به حساب می‌آیند. سؤال‌های پژوهش که بررسی شده‌اند، به این شرح هستند:

- قیمت تعادلی و سطح امنیت برای زمانی که شرکت تأمین‌کننده‌ی امنیت، رهبر باشد، چقدر است؟
- قیمت تعادلی و سطح امنیت برای زمانی که شرکت تأمین‌کننده‌ی امنیت، پیرو باشد، چقدر است؟
- درصد اطلاعات بازگشت‌شده پس از حمله‌ی موفق و ارزش اطلاعات کاربر ابری چه تأثیری در سود شرکت دارد؟

در ادامه‌ی پژوهش حاضر، در بخش ۲، مسئله‌ی بررسی‌شده تشریح و نمادها تعریف شده‌اند. در ادامه، مدل‌سازی مربوط به هر بازیکن صورت گرفته و جواب‌های تعادلی ارائه شده است. در بخش ۳، با استفاده از مثال عددی، به تجزیه‌وتحلیل مسئله پرداخته شده و نتیجه‌گیری صورت گرفته است. درنهایت در بخش ۰ نتیجه‌گیری کلی و پیشنهادهای آتی بیان شده است.

۲. بیان مسئله و مدل‌سازی

ساختارهای قدرت بازی موردمطالعه به گونه‌ای است که در ابتدا کاربر با افزایش مطلوبیت خود، اهمیت امنیت اطلاعات خود را مشخص می‌کند. در واقع، کاربر، یک بازیکن خارجی[4] است. سپس زمانی که مطلوبیت کاربر مثبت شود، تقاضا به‌دست می‌آید، که این مطلوبیت از توزیع یکنواخت پیروی می‌کند. متعاقباً، برای قیمت‌گذاری، هکر و شرکت تأمین‌کننده‌ی امنیت درگیر یک بازی استکلبرگ[5] می‌شوند، که در آن شرکت تأمین‌کننده‌ی امنیت به‌عنوان رهبر عمل می‌کند یا برعکس؛ و این مسئله به روش استقرا به عقب[6] حل می‌شود. مسئله‌ی بررسی‌شده، شامل دو گروه بازیکن است: گروه اول، شامل هکرهایی است که با حملات خود، امنیت سرویس ابری را مختل می‌کنند و به‌دنبال به‌دست‌آوردن اطلاعات کاربر هستند. گروه دوم، شامل شرکت‌های ارائه‌ی دهنده امنیت است، که قصد مبارزه با حملات هکرها را دارند. هر چه شرکت‌ها در ایجاد امنیت سرمایه‌گذاری بیشتری کنند، سطح امنیت بیشتر می‌شود و تعداد کاربرانی که از خدمات آن‌ها استفاده می‌کنند، افزایش می‌یابد و باعث افزایش سود شرکت می‌شود. درشکل ۱، توپولوژی مسئله و فعالیت هر بازیکن مشاهده می‌شود. این تذکر لازم است که در نوشتار حاضر، فقط به بررسی هکرهای کلاه سیاه پرداخته شده است.



شکل ۱. شماتیک مسئله.

[1] Chng
[2] Caldwell
[3] Cohen
[4] exogenous player
[5] Stackelberg game
[6] backward induction

۱.۲. نمادها

در ابتدا نمادهای به کاررفته در مسئله معرفی شده‌اند.

- اندیس‌ها

C اندیس کاربر ابری

F اندیس شرکت تأمین‌کننده‌ی امنیت

H اندیس هکر کلاه سیاه

- پارامترها

V متغیر تصادفی مربوط به ارزش بیشینه‌ی اطلاعات کاربر است، که از یک توزیع یکنواخت پیروی می‌کند (واحد پولی).

δ درصد آسیب واردشده به اطلاعات بعد از حمله‌ی موفق (بدون واحد).

$d(p)$ تقاضای کاربر ابری.

M کل پولی که هکر برای هک‌کردن دریافت می‌کند.

y درصد پولی که هکر قبل از حمله دریافت می‌کند (بدون واحد).

O اعتبار هکر با توجه به اطلاعاتی که در سایت تور [1] از آن هکر موجود است.

λ درصد افزایش اعتبار هکر بعد از یک حمله‌ی موفق که در بازه‌ی ۰ و ۱ است (بدون واحد).

θ درصد اطلاعاتی که شرکت بعد از حمله‌ی موفق می‌تواند بازیابی کند (بدون واحد).

N تعداد کاربران ابری.

k ضریب تبدیل هزینه‌ی سطح امنیت در تابع سود شرکت.

k_1 ضریب تبدیل هزینه‌ی تلاش هکر در تابع سود هکر.

μ ضریب تبدیل موفقیت حمله به واحد پولی.

α ضریب کاهش اعتبار شرکت در صورت موفقیت حمله.

γ ضریب تبدیل اعتبار هکر به واحد پولی.

- متغیرهای تصمیم

q سطح امنیت ایجادشده، که عددی بین ۰ و ۱ است.

p قیمتی که شرکت به کاربر ابری ارائه می‌دهد (واحد پولی).

e میزان افزایش تلاش هکر برای هک موفق، که تابعی از زمان و عددی بین ۰ و ۱ است.

- توابع وابسته

u_c تابع مطلوبیت کاربر ابری (واحد پولی).

u_F تابع سود شرکت تأمین‌کننده‌ی امنیت (واحد پولی).

u_H تابع سود هکر (واحد پولی).

۲.۲. مفروضات مسئله

در مورد مدل مربوط به کاربران ابری، متغیر تصمیم‌گیری وجود ندارد و فقط مطلوبیت مثبت تعیین می‌شود، که باعث می‌شود امنیت خود را به شرکت ارائه‌دهنده‌ی امنیت بسپارند. تقاضا برای شرکت تأمین‌کننده‌ی امنیت پس از تصمیم‌گیری در مورد این محدوده و درنظرگرفتن توزیع یکنواخت به‌دست می‌آید. در مدل هکر، از آنجایی که هکرهای کلاه سیاه موردتوجه هستند؛ متغیر تصمیم، میزان تلاش موردنیاز برای به‌دست‌آوردن اطلاعات براساس ارزش اطلاعات کاربر است. مدل نهایی مربوط به شرکت تأمین‌کننده‌ی امنیت، دو متغیر تصمیم دارد. متغیر تصمیم اول، با قیمتی مرتبط است که کاربران ابری باید ارائه دهند تا امنیت خود را تضمین کنند و متغیر تصمیم دوم، سطح امنیت ایجادشده است. هکرها اعتبار دارند و به ازاء هر هک موفق، اعتبار آن‌ها افزایش می‌یابد و بالعکس.

۳.۲. تابع مطلوبیت و سود بازیکنان

رابطه‌ی ۱، تابع مطلوبیت کاربر ابری را نشان می‌دهد، که به‌طورکلی شامل سطح امنیت ایجادشده برای حفظ اطلاعات کاربر و هزینه‌ای است که باید برای ایجاد آن بپردازد.

$$u_c = V - p - (1-q+e)(1-\theta)\delta V \qquad (۱)$$

که در آن، V متغیر تصادفی است که بیشینه‌ی ارزش اطلاعات کاربر را نشان می‌دهد و از یک توزیع یکنواخت پیروی می‌کند.[۲۰] p هزینه‌ای است که کاربر برای برقراری سطح امنیت به شرکت می‌پردازد. پارامتر q سطح امنیت ایجادشده در یک شرایط عادی را نشان می‌دهد، که براساس نوشتار فنگ و همکاران،[۱۸] عددی بین ۰ و ۱ خواهد داشت. پارامتر e نشانگر تلاش اضافی موردنیاز یک هکر برای افزایش احتمال یک حمله‌ی موفق است. بخش‌های اول و دوم تابع ۱، بیشینه‌ی ارزش و پولی را که کاربر باید پرداخت کند، نشان می‌دهند. بخش سوم، مربوط به موفقیت حمله است، که باعث آسیب به اطلاعات و کاهش رضایت مشتری و در نتیجه کاهش مطلوبیت می‌شود. کاهش مطلوبیت به‌علت حمله‌ی موفق زمانی اتفاق می‌افتد که مشتریان از حمله مطلع شوند و این در صورتی است که اطلاعات‌شان آسیب ببیند یا از بین برود و بازیابی نشود. حمله در صورتی موفق است که هکر تلاش کند و سطح امنیت شکسته شود یا به‌عبارتی برقرار نشود. برقراری سطح امنیت با متغیر تصمیم q نشان داده می‌شود و چون عددی بین ۰ و ۱ است، عدم برقراری آن به‌صورت $1-q$ خواهد بود. تلاش هکر نیز چون مؤثر است، به احتمال اخیر اضافه می‌شود. تمامی این بخش به‌صورت $1-q+e$ نوشته شده است. حال در صورت موفقیت حمله، شرکت تلاش می‌کند تا اطلاعات آسیب‌دیده را بازیابی کند. درصد اطلاعات بازیابی‌شده با پارامتر θ نشان داده شده است و در نتیجه، عدم بازیابی اطلاعات $1-\theta$ خواهد بود. پس اگر حمله موفق باشد و اطلاعات بازیابی نشود، با توجه به درصد آسیب اطلاعات، که با δ نشان داده شده است، تقاضا کاهش می‌یابد. این استدلال منجر به تشکیل بخش سوم تابع مطلوبیت کاربر می‌شود. این تذکر لازم است که درصد δ در بیشینه‌ی ارزش کل ضرب می‌شود تا میزان آسیب اطلاعات به‌دست آید.

[1] The Onion Router

کاربر زمانی امنیت اطلاعات خود را به شرکت تأمین‌کننده‌ی امنیت می‌سپارد که مطلوبیت مثبتی داشته باشد. بنابراین لازم است تا $u_c \geq 0$ باشد و سپس V از روش اخیر به‌دست آورده شود. کمترین حالتی که ممکن است کاربر امنیت خود را به شرکت تأمین‌کننده‌ی امنیت بسپارد، در حالت $u_C = 0$ است. در نتیجه، مطابق رابطه‌ی ۲، تقاضا مشخص می‌شود. معادله‌ی ۳، میزان تقاضا برای شرکت تأمین‌کننده‌ی امنیت را نشان می‌دهد؛ که براساس روابط موجود در کتاب فیلیپس (۲۰۲۱)،[۲۱] نوشته شده است؛ که در آن، برای به‌دست‌آوردن تابع تقاضا، از تمایل مشتری برای خرید استفاده می‌شود و برای سادگی فرض می‌شود که تمایل مشتری به پرداخت، دقیقاً برابر قیمت است؛ که این مقدار، حد پایین انتگرال را خواهد داد و سپس با به‌دست‌آوردن تابع تجمعی مربوط به تابع چگالی احتمال یکنواخت، تقاضا به‌دست می‌آید.

$$u_c = 0$$

$$V = \frac{p}{1-\delta-e\delta+q\delta+2\delta\theta+2e\delta\theta-2q\delta\theta} \quad (۱)$$

$$V \sim U(0,1) \quad (۲)$$

$$d(p) = N\int_{V\to\frac{p}{1-\delta-e\delta+q\delta+2\delta\theta+2e\delta\theta-2q\delta\theta}}^{1} dx = 1-\frac{p}{1+(1+e-q)\delta(-1+2\theta)} \quad (۳)$$

در ادامه، براساس رابطه‌ی اخیر، تابع سود شرکت مطابق معادله‌ی ۴ به‌دست می‌آید. برای سهولت حل، در ادامه، تعداد کاربران ابری نرمال و N، ۱ در نظر گرفته شده است. معادله‌ی ۵، تابع سود هکر با توجه به موفقیت و عدم موفقیت حمله را نشان می‌دهد. برای تبدیل توابع سود به واحد پولی، نیاز به ضرایب تبدیل است. بدین منظور ضرایب تبدیل برای هر عبارت به توابع اضافه شده‌اند، که در بخش ۱.۲. **نمادها** نیز معرفی شده‌اند.

$$u_F = d(p) * p - \frac{(kq^2)}{2} - (1-q+e)\alpha\mu \quad (۴)$$

$$u_H = My + (۱-q+e)(۱-y)M + (۱-q+e)\lambda O\gamma - (q-e)(۱-\lambda)O\gamma - \frac{(k_۱e^۲)}{۲} \quad (۵)$$

حال باید با توجه به ساختارهای مختلف، مسئله را حل کرد. در ابتدا فرض بر این است که تأمین‌کننده‌ی امنیت، تصمیم‌گیر اول و رهبر است و در مورد سطح امنیت موردنیاز، تصمیم و قیمت را به کاربر اعلام می‌کند. مقادیر تعادلی براساس اثبات‌های صورت‌گرفته در ۱۰ و با روش استقرا به عقب به‌دست آمده است. روابط ۶ الی ۸، مقادیر تعادلی را نشان می‌دهند.

$$p^* = \frac{1}{8}\left(4+\frac{\delta(-1+2\theta)(4k-\delta+2\delta\theta-4\alpha\mu)}{k} - \frac{4\delta(-1+2\theta)(M(-1+y)-O\gamma\lambda)}{k_1}\right) \quad (۶)$$

$$q^* = \frac{\delta-2\delta\theta+4\alpha\mu}{4k} \quad (۷)$$

$$e^* = \frac{M-My+O\gamma\lambda}{k_1} \quad (۸)$$

برای بررسی ساختار قدرت دیگر بازی، باید هکر در ابتدا تصمیم‌گیرنده باشد و شرکت تأمین‌کننده‌ی امنیت به عنوان پیرو عمل کند. مقادیر تعادلی براساس اثبات‌های صورت‌گرفته در پیوست ۱ و با روش استقرا به عقب به‌دست آمده است. روابط ۹ الی ۱۱، مقادیر تعادلی در این ساختار قدرت را نشان می‌دهند.

$$p^* = \frac{1}{8}\left(4+\frac{\delta(-1+2\theta)(4k+\delta(-1+2\theta)+4\alpha(-1+\theta)\mu)}{k} - \frac{4\delta(-1+2\theta)(M(-1+y)+O\gamma(-1+\lambda))}{k_1}\right) \quad (۹)$$

$$q^* = \frac{\delta-2\delta\theta+4\alpha\mu-4\alpha\theta\mu}{4k} \quad (۱۰)$$

$$e^* = \frac{M-My+O\gamma-O\gamma\lambda}{k_1}) \quad (۱۱)$$

۳. مثال عددی و تحلیل حساسیت

در ادامه، با استفاده از مثال عددی سعی شده است تا مسئله‌ی موردنظر تحلیل شود. شایان ذکر است علاوه‌بر مثال عددی اخیر، ۱۹ مثال عددی دیگر بررسی شده است، تا راستی‌آزمایی به‌دست‌آمده بررسی شود. برای بررسی میزان تفاوت مقادیر سود در نمونه‌های مختلف، از آزمون آماری فریدمن استفاده شده است. براساس نتیجه‌ی آزمون فریدمن و مقایسه با مقدار p-value که برابر ۰/۰۰۹۵۵ بوده است، فرض تفاوت بین نتایج، رد شده و در نتیجه بین مقادیر سود، تفاوت چشم‌گیری براساس نمونه‌های ایجادشده وجود نداشته است. محاسبات مربوط به این آزمون در ۲۰ ارائه شده است.

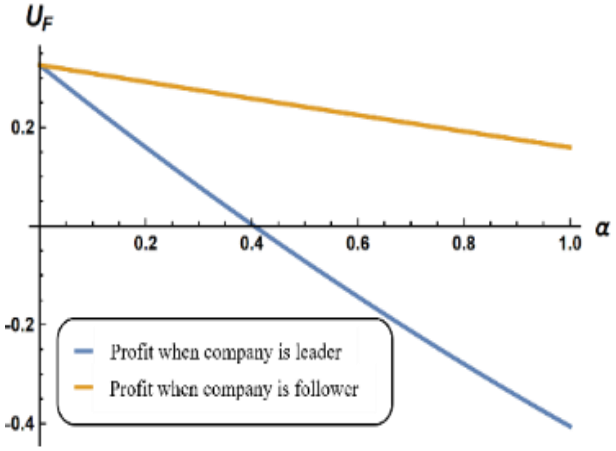
۱.۳. مثال عددی

جهت فهم بهتر مسئله، یک مثال عددی از مسئله ارائه و سپس به تحلیل حساسیت توابع سود نسبت به پارامترهای مختلف پرداخته و نکات مهم آن بیان شده است. در جدول ۱، مقادیر استفاده‌شده برای پارامترها ارائه شده‌اند. شایان ذکر است برای اینکه تمام مقادیر یک واحد شوند، با توجه به منابع هر یک، نرمال شده‌اند.

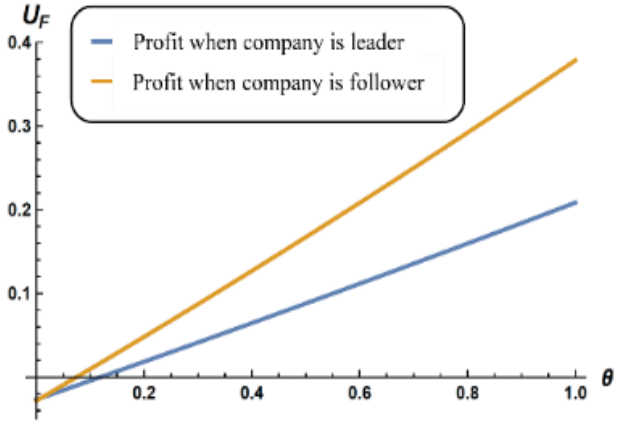
با حل مسئله‌ی حاصل از پارامترهایی که مقادیر آن در جدول ۱ ارائه شده است، این نتایج به‌دست آمده است: در شکل ۲، سود شرکت در دو سناریو براساس پارامتر ضریب کاهش اعتبار شرکت مشاهده می‌شود؛ که مطابق آن، براساس پارامتر مذکور، سود شرکت در حالت پیروبودن بیشتر است. در شکل ۳، سود شرکت براساس درصد بازگشت اطلاعات مشاهده می‌شود. در این حالت نیز سود شرکت در جایگاه پیرو بیشتر بوده و هر چه درصد بازگشت اطلاعات بیشتر بوده

جدول ۱. مقادیر در نظر گرفته‌شده برای پارامترها در مثال‌ها و تحلیل حساسیت‌ها.

Parameter	Value	Ref
k	1	[22]
α	3	Interview
k_1	3	[22]
O	0.4	[22]
γ	0.2	[22]
δ	0.3	[22]
λ	0.2	Interview
μ	1.5	Interview
M	4	[16]
y	0.5	Interview

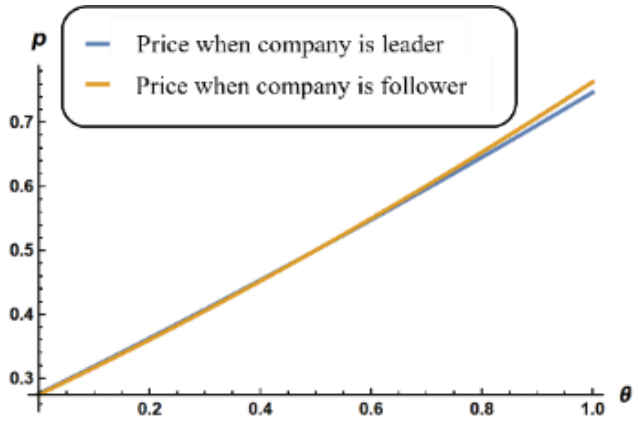


شکل۲. مقایسه‌ی سود شرکت براساس کاهش اعتبار شرکت در حمله‌ی موفق.

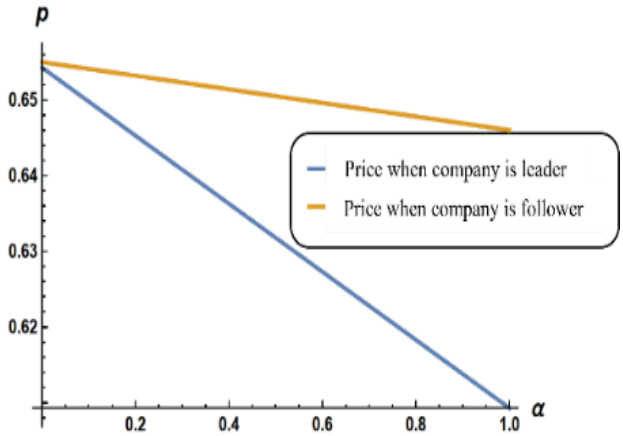


شکل۳. مقایسه‌ی سود شرکت براساس درصد اطلاعات بازگشتی.

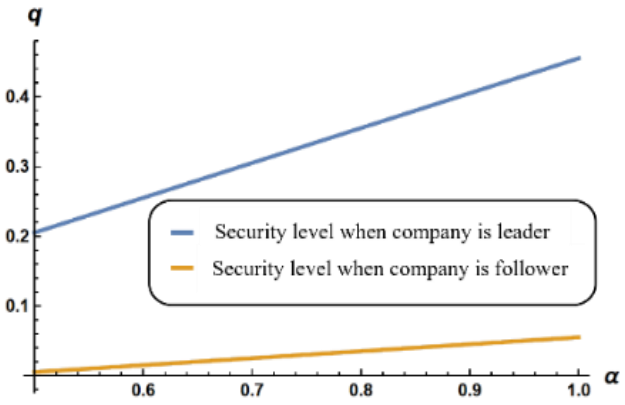
است، سود افزایش یافته است. درشکل ۴، مقایسه‌ی قیمت در دو ساختار قدرت مشاهده می‌شود. همان‌طور که مشخص است، قیمت‌ها در دو ساختار مذکور، تقریباً یکسان تعیین شده است. در ادامه، در شکل ۵، قیمت براساس ضریب کاهش اعتبار شرکت مشاهده می‌شود؛ که مطابق آن، براساس پارامتر مذکور، قیمت تعیین‌شده در وضعیتی که شرکت رهبر است، کمتر از حالتی بوده است که شرکت پیرو باشد. در شکل ۶، متغیر تصمیم سطح امنیت ایجادشده براساس



شکل ۴. قیمت شرکت براساس درصد اطلاعات بازگشتی.



شکل ۵. قیمت تعیین‌شده توسط شرکت براساس کاهش اعتبار شرکت هنگام حمله‌ی موفق.



شکل ۶. سطح امنیت تعیین‌شده براساس کاهش اعتبار شرکت هنگام حمله‌ی موفق.

ضریب کاهش شرکت مشاهده می‌شود. بدیهی است که هر چقدر ضریب کاهش شرکت بیشتر باشد، لازم است تا سطح امنیت بالاتری تعیین شود تا اعتبار شرکت کمتر آسیب ببیند.

براساس نمودارهای اخیر و همچنین تحلیل‌های صورت‌گرفته، این نتایج به‌دست آمده است:

۱) با توجه به نمونه‌های مختلف شبیه‌سازی‌شده و مقادیر به‌دست‌آمده و همچنین نمونه‌ی ارائه‌شده در پژوهش حاضر، دو پارامتر درصد بازیابی اطلاعات

و ضریب کاهش اعتبار شرکت، دو پارامتر اساسی در مقدار سود هستند. شرکت‌های تأمین‌کننده‌ی امنیت، با توجه به دو پارامتر مذکور و اهمیت هر یک، می‌توانند ساختار قدرت و قیمت خود را تعیین کنند.

۲) در شکل ۴ مشاهده می‌شود زمانی که تصمیم براساس درصد اطلاعات بازیابی شده باشد، قیمت تعیین‌شده توسط شرکت، در درصد بازیابی پایین در دو ساختار تفاوتی ندارند. هر چه درصد بازیابی افزایش یابد، قیمت تعیین‌شده در حالت پیرو، بیشتر خواهد بود؛ اما این تغییر زیاد نیست و می‌توان گفت قیمت در دو ساختار تقریباً یکسان تعیین می‌شود. با وجود این، مطابق شکل ۳، سود شرکت براساس پارامتر اخیر، در ساختار رهبربودن شرکت، تفاوت زیادی با سود در حالت پیرو دارد. این تغییر با وجود یکسان‌بودن تقریبی قیمت‌ها، ناشی از تفاوت سطح امنیت ایجادشده و تلاش هکر در دو ساختار است. تفاوت سطح امنیت ایجادشده در سود شرکت مطابق با نتایج مطالعه‌ی بارتلوما (۲۰۱۸)،[۷] است.

۳) درشکل ۵، قیمت تعیین‌شده براساس پارامتر ضریب کاهش اعتبار شرکت در صورت موفقیت حمله مشاهده می‌شود؛ که مطابق آن مشخص است که هر چه میزان کاهش اعتبار بیشتر باشد، قیمت کاهش یافته است. زیرا با توجه به کاهش اعتبار، شرکت محبوبیت کمتری در بین مشتریان خود خواهد داشت. بنابراین، لازم است شرکت برای جذب مشتری، قیمت خود را کاهش دهد و از این طریق، زیان وارده را جبران کند. همچنین در شکل اخیر مشاهده می‌شود که قیمت در حالت رهبربودن، بسیار کمتر تعیین شده است. درشکل ۲، تفاوت سود براساس پارامتر کاهش اعتبار در دو ساختار مشاهده می‌شود؛ که مطابق آن، سود در حالت رهبربودن نیز کاهش بسیاری نسبت به حالت پیروبودن داشته است.

۴) سطح امنیت تعیین‌شده براساس پارامتر ضریب کاهش اعتبار شرکت، زمانی که شرکت پیرو باشد، بسیار کمتر از زمانی است که شرکت رهبر باشد. این امر به وضوح در شکل ۶ مشاهده می‌شود. این نتیجه، یکی دیگر از دلایلی است که باعث می‌شود سود در حالت رهبربودن کمتر از حالت پیروبودن باشد؛ زیرا سطح امنیت در حالت رهبربودن شرکت، بالاتر است و در نتیجه، هزینه‌ای که شرکت برای تأمین سطح امنیت متحمل می‌شود، بسیار بیشتر است و باعث کاهش سود می‌شود.

۵) بالاتربودن سطح امنیت ایجادشده در حالت رهبربودن شرکت، به این علت است که شرکت باید قبل از حمله و بدون اطلاع از وضعیت حمله و مهارت هکر، سطح امنیت را ایجاد کند و قیمت را ارائه دهد.[۷] بنابراین، لازم است تا در حد امکان با توجه به ارزش اطلاعات، امنیت ایجاد شود و در نتیجه ممکن است سطح امنیت بسیار بالاتر از حد موردنیاز تعیین شود و این می‌تواند دلیل دیگری باشد که فقط ۰/۰۵٪ از شرکت‌ها ساختار اخیر را انتخاب می‌کنند[۲].

۶) تحلیل پارامتریک متغیر تصمیم مربوط به سطح امنیت ایجادشده نشان می‌دهد اگر تمامی پارامترهای موجود در متغیر تصمیم مذکور، مثبت باشد، همواره سطح امنیت ایجادشده در حالت رهبربودن شرکت، بیشتر از حالت پیروبودن آن است.

۷) تحلیل پارامتریک متغیر تصمیم تلاش هکر نشان می‌دهد اگر $\lambda > \frac{۱}{۲}$ و بقیه‌ی پارامترها مثبت باشد، تلاش هکر زمانی که شرکت رهبر باشد، بیشتر از زمانی است که شرکت پیرو باشد.

۴. نتیجه‌گیری و پیشنهادهای آتی

در نوشتار حاضر، به بررسی رابطه‌ی بین هکرها و یک شرکت ارائه‌دهنده‌ی امنیت پرداخته شده است، تا قیمت و سطح امنیتی موردنیاز شرکت بسته به ساختار قدرت تعیین کند. پس از مدل‌سازی و بررسی ساختارهای مختلف قدرت و با استفاده از داده‌های موجود در ادبیات و مصاحبه با کارشناسان امنیت سایبری، قیمت‌ها و سود در موقعیت‌های مختلف شرکت مقایسه شده‌اند. نتایج نشان می‌دهند جایگاه شرکت در ساختار قدرت، تأثیر زیادی در قیمت ارائه‌شده براساس درصد بازیابی اطلاعات ندارد. با وجود این، سود در حالت پیروبودن براساس همین پارامتر و همچنین پارامتر ضریب کاهش اعتبار شرکت، همواره بالاتر از جایگاه رهبر است.

از محدودیت‌های پژوهش حاضر، درنظرگرفتن فقط یک نوع هکر و یک شرکت است. همچنین نوع تابع تقاضا در نظر گرفته‌شده، خطی بوده است و فقط از تعدادی از پارامترهای تأثیرگذار تبعیت می‌کند. برای مطالعات آینده، علاوه‌بر پوشش‌دادن محدودیت‌های این مسئله، می‌توان بودجه‌ی کاربر ابری برای سرمایه‌گذاری امنیت سایبری را در نظر گرفت و آن را به‌عنوان محدودیت وارد مسئله کرد. همچنین درنظرگرفتن انواع دیگر هکر، برای نوشتن توابع سود می‌تواند نتایج متفاوتی را ارائه دهد. به‌عنوان مثال، هکرهای کلاه خاکستری را در نظر گرفت که می‌توانند راهبردهای افشا یا همکاری با شرکت را داشته باشند. درنهایت در این مسئله می‌توان به جای درنظرگرفتن درصد بازگشت اطلاعات، از بیمه‌ی ابری استفاده کرد، که در صورت حمله و آسیب به اطلاعات کاربر، شرکت مبلغی را به‌عنوان بیمه به کاربر پرداخت کند. این مورد نیز در توابع سود مربوط به شرکت و کاربر تأثیر خواهد داشت.

References- منابع

1. O'Connor, S., Hasshu, S., Bielby, J., Colreavy-Donnelly, S., Kuhn, S., Caraffini, F. and Smith, R., 2021. Scips: A serious game using a guidance mechanic to scaffold effective training for cyber security, *Information Sciences, 580,* pp.524-540 DOI: https://doi.org/10.1016/j.ins.2021.08.098.
2. Chronopoulos, M., Panaousis, E. and Grossklags, J., 2017. An options approach to cybersecurity investment, *IEEE Access, Vol. 6*, pp. 12175 – 12186 DOI: 10.1109/ACCESS.2017.2773366
3. Whaiduzzaman, M. and Gani, A., 2013, Measuring security for cloud service provider: A third party approach, in *2013 International Conference on Electrical Information and Communication Technology (EICT)*, pp. 1-6. IEEE. DOI: 10.1109/EICT.2014.6777855
4. Che, J., Duan, Y., Zhang, T. and Fan, J., 2011. Study on the security models and strategies of cloud computing, *Procedia Engineering, Vol. 23*, pp. 586-593 DOI: https://doi.org/10.1016/j.proeng.2011.11.2551.

5. Hsieh, C., Chang, Y. and Wu, C., 2014. Competitive pricing and ordering decisions in a multiple-channel supply chain, *International journal of production economics, Vol. 154*, pp. 156-165 DOI: https://doi.org/10.1016/j.ijpe.2014.04.024.

6. Chen, Z., Wu, S., Govindan, K., Wang, J., Chin, K. and Martíınez, L., 2022, Optimal pricing decision in a multi-channel supply chain with a revenue-sharing contract, *Annals of Operations Research, Vol. 318*, pp. 67-102, DOI: https://doi.org/10.1007/s10479-022-04748-7.

7. Bartholomae, F., 2018, Cybercrime and cloud computing. A game theoretic network model, *Managerial and Decision Economics, Vol. 39*, pp. 297-305, DOI: https://doi.org/10.1002/mde.2904.

8. Shy, O., 2001, The economics of network industries, *Cambridge university press*, DOI: https://doi.org/10.1007/978-3-662-04623-4_17.

9. Cong, P., Li, L., Zhou, J., Cao, K., Wei, T., Chen, M. and HU., S, 2018, Profit-driven dynamic cloud pricing for multiserver systems considering user perceived value, *IEEE Trans. Parallel Distrib. Syst, Vol. 29*, pp. 2742-2756, DOI: 10.1109/TPDS.2018.2843343.

10. Chng, S., Lu, H.Y., Kumar, A. and Yau, D., 2022, Hacker types, motivations and strategies: A comprehensive framework, *Computers in Human Behavior Reports, Vol. 5,* pp. 100167, DOI: https://doi.org/10.1016/j.chbr.2022.100167

11. Caldwell, T., 2011, Ethical hackers: Putting on the white hat, *Network Security, Vol. 2011*, pp. 10-13, DOI: https://doi.org/10.1016/S1353-4858(11)70075-7.

12. Cohen, D., Elalouf, A. and Zeev, R., 2022, Collaboration or separation maximizing the partnership between a “gray hat” hacker and an organization in a two-stage cybersecurity game, *International Journal of Information Management Data Insights, Vol. 2*, pp. pages 100073, DOI: https://doi.org/10.1016/j.jjimei.2022.100073.

13. Rachamalla, S. and Fatima, S.H., 2020, Game theory and cyber security, *Annual Workshop on Cyber Security*, *Vol. 2,* pp. 978- 990, DOI: https://doi.org/10.1145/1852666.1852704.

14. Shiva, S., Roy, S. and Dasgupta, D., 2010. Game theory for cyber security, in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, pp. 1-4, [In Persian] DOI: https://doi.org/10.1145/1852666.1852704,

15. Do, C., Tran, N., Hong, C., Kamhoua, C.A., Kwiat, K.A., Blasch, E. and Lyengar., S., 2017. Game theory for cyber security and privacy, *ACM Computing Surveys (CSUR), Vol. 50*, pp. 1-37, DOI: https://doi.org/10.1145/3057268.

16. Hyder, B. and Govindarasu, M., 2020. Optimization of cybersecurity investment strategies in the smart grid using game-theory, in *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1-5, DOI: 10.1109/ISGT45199.2020.9087634.

17. Xiao, P. and Tang, Z., 2015, Game theory–based resource pricing model in cloud platforms, *International Journal of Communication Networks and Distributed Systems, Vol. 14*, pp. 256-271, DOI: https://doi.org/10.1504/IJCNDS.2015.068666.

18. Feng, S., Xiong, Z., Niyato, D., Wang, P., Wang, S., and Shen, S., Joint pricing and security investment in cloud security service market with user interdependency, *IEEE Transactions on Services Computing, Vol. 15*, pp. 1461-1472, DOI: 10.1109/TSC.2020.2996382.

19. Ge, H., Zhao, L., Yue, D., Xie, X., Xie, L., Gorbachev, S., Corovin., I. and Ge., Y., 2024, A game theory based optimal allocation strategy for defense resources of smart grid under cyber-attack, *Information Sciences, Vol. 652,* pp. 1197-1220, DOI: https://doi.org/10.1016/j.ins.2023.119759.

20. Huang, J., Leng, M. and Parlar, M., 2021, Demand functions in decision modeling: A comprehensive survey and research directions, *Decision Sciences, Vol. 44,* pp. 557-609, DOI: https://doi.org/10.1111/deci.12021

21. Phillips, R., 2021, *Pricing and revenue optimization*, Stanford university press, 2021. In Electrical, DOI: https://doi.org/10.1515/9781503614260

22. Gao, X., Qiu, M., Wang, Y. and Wang, X., 2023, Information security investment with budget constraint and security information sharing in resource-sharing environments, *Journal of the Operational Research Society, Vol. 74,* pp. 1520-1535, DOI: https://doi.org/10.1080/01605682.2022.2096506 .

پیوست ۱

در ادامه، اثبات مربوط به حل مسئله براساس ساختار قدرت اول، یعنی رهبربودن شرکت تأمین‌کننده‌ی امنیت، بیان شده است.

در ابتدا لازم است مشخص شود که تابع مقعر است. در صورت منفی‌بودن مشتق دوم تابع، می‌توان با استفاده از مشتق اول، نقاط تعادلی را به‌دست آورد. با توجه به اینکه از روش استقرا به عقب برای حل مسئله استفاده شده است، لازم است تا ابتدا تابع مربوط به پیرو حل شود. سپس با قراردادن مقادیر به‌دست‌آمده در تابع رهبر، مسئله‌ی مربوط به رهبر حل شود (روابط ۱۲ الی ۱۵):

$$\frac{\partial^2 u_H}{\partial e^2} = -k \tag{۱۲}$$

$$\frac{\partial u_H}{\partial e} = M\left(1-y\right) + O\gamma\lambda - ek_1 \tag{۱۳}$$

$$4M\left(1-y\right) + O\gamma\lambda - ek_1 = 0 \tag{۱۴}$$

$$e^* = \frac{M - My + O\gamma\lambda}{k_1} \tag{۱۵}$$

با قراردادن مقدار اخیر (e^*) در تابع رهبر، تابع رهبر جدید ساخته می‌شود. سپس با درنظرگرفتن ماتریس هسین مربوط به تابع رهبر، می‌توان راجع به مقعربودن آن نظر داد. با فرض $2\theta > 1$، مینور اول ماتریس هسین منفی خواهد بود. با محاسبه‌ی مینور دوم ماتریس هسین رابطه‌ی ۲۱ به‌دست خواهد آمد. با توجه به مثبت‌بودن قسمت‌های مختلف رابطه‌ی اخیر و همچنین مثبت‌بودن مخرج کسر، می‌توان با ساده‌سازی آن را به رابطه‌ی ۲۲ تبدیل کرد. با علم به آنکه تمامی پارامترهای موجود در رابطه‌ی ۲۲ مثبت هستند، با فرض $k\left(Y\right)^3 > 3S + J\left(U\right)$، مینور دوم ماتریس هسین منفی می‌شود و در نتیجه تابع مقعر است. شایان ذکر است در مقداردهی پارامترهای مسئله، این مورد درنظر گرفته شده است. در ادامه، با توجه به مقعربودن توابع سود، با استفاده از مشتق اول مقادیر تعادلی مطابق روابط ۱۶ الی ۲۵ به‌دست می‌آیند.

$$u_F = p\left(1 - \frac{p}{1+\delta\left(-1+2\theta\right)\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right)}\right) - \alpha\mu\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right) - \frac{kq^2}{2} \tag{۱۶}$$

$$\frac{\partial^2 u_F}{\partial p^2} = -\frac{2}{1+\delta\left(-1+2\theta\right)\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right)} \tag{۱۷}$$

$$\frac{\partial^2 u_F}{\partial q^2} = -k - \frac{2p^2\delta^2\left(-1+2\theta\right)^2}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right)\right)^3} \tag{۱۸}$$

$$\begin{pmatrix} -\frac{2}{1+\delta\left(-1+2\theta\right)\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right)} & -\frac{2p\delta\left(-1+2\theta\right)}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right)\right)^2} \\ -\frac{2p\delta\left(-1+2\theta\right)}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right)\right)^2} & -k - \frac{2p^2\delta^2\left(-1+2\theta\right)^2}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right)\right)^3} \end{pmatrix} \tag{۱۹}$$

$$\det = \frac{2\left(\begin{array}{l} -3p^2\delta^2\left(1-2\theta\right)^2 + k\left(1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)\right)^3 - \\ p^2\delta^3\left(-1+2\theta\right)^3\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right) \end{array}\right)}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)\right)^4} \quad (۲۰)$$

$$\frac{\partial u_F}{\partial p} = 1 - \frac{2p}{1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)} \quad (۲۱)$$

$$\det = 2\left(-3S + k\left(Y\right)^3 - J\left(U\right)\right) \quad (۲۲)$$

$$\frac{\partial u_F}{\partial q} = -kq + \alpha\mu - \frac{p^2\delta\left(-1+2\theta\right)}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)\right)^2} \quad (۲۳)$$

$$p^* = \frac{1}{8}\left(4 + \frac{\delta\left(-1+2\theta\right)\left(4k-\delta+2\delta\theta-4\alpha\mu\right)}{k} - \frac{4\delta\left(-1+2\theta\right)\left(M\left(-1+y\right)-O\gamma\lambda\right)}{k_1}\right) \quad (۲۴)$$

$$q^* = \frac{\delta - 2\delta\theta + 4\alpha\mu}{4k} \quad (۲۵)$$

با قراردادن مقادیر تعادلی در معادله‌ی ۱۵، مقدار تعادلی متغیر تصمیم هکر مطابق رابطه‌ی ۲۶ به‌دست خواهد آمد.

$$e^* = \frac{M - My + O\gamma\lambda}{k_1} .\square \quad (۲۶)$$

پیوست ۲

در ادامه، اثبات مربوط به حل مسئله براساس ساختار قدرت دوم یعنی پیروبودن شرکت تأمین‌کننده‌ی امنیت بیان شده است (روابط ۲۷ الی ۴۱).

در ابتدا لازم است تا مشخص شود تابع مقعر است. برای این منظور از ماتریس هسین استفاده شده است. برای منفی‌بودن مینور اول، همان فرض پیوست ۱ برای منفی‌بودن مینور اول در نظر گرفته شده است. با محاسبه‌ی مینور دوم ماتریس هسین، عبارت ۳۰ به‌دست خواهد آمد. با توجه به مثبت‌بودن قسمت‌های مختلف رابطه‌ی اخیر و همچنین مثبت‌بودن مخرج کسر، می‌توان با ساده‌سازی آن را به‌عبارت ۳۱ تبدیل کرد. با علم به آنکه تمامی پارامترهای موجود در رابطه‌ی اخیر مثبت هستند، با فرض $۲\left(kA\right)^۳ > B\left(C\right)$، مینور دوم ماتریس هسین منفی می‌شود و در نتیجه تابع مقعر است. شایان ذکر است در مقداردهی پارامترهای مسئله، این مورد در نظر گرفته شده است. با توجه به اینکه از روش استقرا به عقب برای حل مسئله استفاده شده است، لازم است تا ابتدا تابع مربوط به پیرو حل شود و سپس با قراردادن مقادیر به‌دست‌آمده در تابع رهبر، مسئله‌ی مربوط به رهبر حل شود. با قراردادن روابط ۳۴ و ۳۵ در تابع هدف هکر (رابطه‌ی ۶) تابع هدف هکر به‌دست خواهد آمد. سپس با جای‌گذاری رابطه‌ی ۴۱ در روابط ۳۴ و ۳۵ مقادیر تعادلی شرکت به‌دست می‌آیند.

$$\frac{\partial^2 u_F}{\partial p^2} = -\frac{2}{1+\left(1+e-q\right)\delta\left(-1+2\theta\right)} \quad (۲۷)$$

$$\frac{\partial^2 u_F}{\partial q^2} = -k - \frac{2p^2\delta^2\left(-1+2\theta\right)^2}{\left(1+\left(1+e-q\right)\delta\left(-1+2\theta\right)\right)^3} \tag{۲۸}$$

$$\begin{pmatrix} -\frac{2}{1+\left(1+e-q\right)\delta\left(-1+2\theta\right)} & -\frac{2p\delta\left(-1+2\theta\right)}{\left(1+\left(1+e-q\right)\delta\left(-1+2\theta\right)\right)^2} \\ -\frac{2p\delta\left(-1+2\theta\right)}{\left(1+\left(1+e-q\right)\delta\left(-1+2\theta\right)\right)^2} & -k-\frac{2p^2\delta^2\left(-1+2\theta\right)^2}{\left(1+\left(1+e-q\right)\delta\left(-1+2\theta\right)\right)^3} \end{pmatrix} \tag{۳۹}$$

$$\det = \frac{2\left(k\left(1+\left(1+e-q\right)\delta\left(-1+2\theta\right)\right)^3 - p^2\delta^2\left(1-2\theta\right)^2\left(3+\left(1+e-q\right)\delta\left(-1+2\theta\right)\right)\right)}{\left(1+\left(1+e-q\right)\delta\left(-1+2\theta\right)\right)^4} \tag{۳۰}$$

$$\det = 2\left(kA\right)^3 - B\left(C\right) \tag{۳۱}$$

$$\frac{\partial u_F}{\partial p} = 1 - \frac{2p}{1+\left(1+e-q\right)\delta\left(-1+2\theta\right)} \tag{۳۲}$$

$$\frac{\partial u_F}{\partial q} = -kq - \frac{p^2\delta\left(-1+2\theta\right)}{\left(1+\left(1+e-q\right)\delta\left(-1+2\theta\right)\right)^2} + \alpha\left(1-\theta\right)\mu \tag{۳۳}$$

$$p = \frac{k\left(4+4\left(1+e\right)\delta\left(-1+2\theta\right)\right)+\delta\left(-1+2\theta\right)\left(\delta\left(-1+2\theta\right)+4\alpha\left(-1+\theta\right)\mu\right)}{8k} \tag{۳۴}$$

$$q = \frac{\delta - 2\delta\theta - 4\alpha\left(-1+\theta\right)\mu}{4k} \tag{۳۵}$$

$$p^* = \frac{1}{8}\begin{pmatrix} 4+\frac{\delta\left(-1+2\theta\right)\left(4k+\delta\left(-1+2\theta\right)+4\alpha\left(-1+\theta\right)\mu\right)}{k} - \\ \frac{4\delta\left(-1+2\theta\right)\left(M\left(-1+y\right)+O\gamma\left(-1+\lambda\right)\right)}{k_1} \end{pmatrix} \tag{۳۶}$$

$$q^* = \frac{\delta - 2\delta\theta + 4\alpha\mu - 4\alpha\theta\mu}{4k} \tag{۳۷}$$

$$u_H = My - \frac{O\gamma\lambda\left(\delta-2\delta\theta+4\alpha\mu-4\alpha\theta\mu\right)}{4k} + M\left(1-y\right)\left(1+e-\frac{\delta-2\delta\theta+4\alpha\mu-4\alpha\theta\mu}{4k}\right) + O\gamma\left(1-\lambda\right)\left(1+e-\frac{\delta-2\delta\theta+4\alpha\mu-4\alpha\theta\mu}{4k}\right) - \frac{e^2k_1}{2} \tag{۳۸}$$

$$\frac{\partial^2 u_H}{\partial e^2} = -k_1 \tag{۳۹}$$

$$\frac{\partial u_H}{\partial e} = M\left(1-y\right) + O\gamma\left(1-\lambda\right) - ek_1 \tag{۴۰}$$

$$e^* = \frac{M - My + O\gamma - O\gamma\lambda}{k_1} .\square \tag{۴۱}$$

پیوست ۳

آزمون فریدمن

در پژوهش حاضر، ۱۹ نمونه‌ی دیگر با توجه به محدودیت‌های هر پارامتر، ایجاد شده و براساس آن‌ها مقادیر تابع هدف به‌دست آمده است. سپس با استفاده از آزمون فریدمن، نتایج ارزیابی شده است. آزمون فریدمن، یک آزمون آماری ناپارامتریک است، که توسط میلتون فریدمن توسعه یافته است. روش مذکور، هر سطر را رتبه‌بندی می‌کند و سپس رتبه‌بندی در ستون‌ها را در نظر می‌گیرد. در ادامه، روند انجام آزمون فریدمن ارائه شده است.

فرض صفر، تفاوت بین نتایج در نظر گرفته شده است. برای انجام آزمون فریدمن و رد یا تأیید فرض صفر، ۱۹ نمونه در نظر گرفته شده‌اند، که با تغییر هر یک از پارامترها ایجاد شده‌اند. به‌عنوان مثال، در نمونه‌ی اول، درصد آسیب اطلاعات در حمله‌ی موفق، کم، در نمونه‌ی دوم، متوسط، و در نمونه‌ی سوم در حد بالا مقداردهی شده است. بقیه‌ی نمونه‌ها نیز با تغییر مقدار پارامترها به کم، متوسط و زیاد ایجاد شده و مقادیر تابع سود در دو سناریو به‌دست آمده است. مقادیر سود در جدول ارائه شده است. سپس براساس روند انجام آزمون فریدمن، مقادیر سود، رتبه‌بندی و رتبه‌ها در هر ستون با یکدیگر جمع شده‌اند. میانگین رتبه‌ها به‌دست آمده و براساس آماره‌ی آزمون فریدمن که در رابطه‌ی ۴۲ نشان داده شده است، مقدار آماره‌ی اخیر به‌دست آمده است (جدول ۳).

$$Q = \frac{12n}{k(k+1)} \sum_{j=1}^{k} (\bar{r}_j - \frac{(k+1)}{2})^2 \qquad (۴۲)$$

که در آن، n تعداد نمونه‌ها و k تعداد سناریوهای بررسی‌شده است. پس از به‌دست‌آوردن آماره‌ی Q، مقدار p-value محاسبه و برابر ۰/۰۰۹۵۵ شده است، که برای p-value ، مقدار کمی بوده و درنتیجه فرض صفر رد شده است.

جدول ۲. مقادیر سود با نمونه‌های مختلف.

Sample	Leader structure	Follower structure
1	0.090479	0.066986
2	0.184317	0.121533
3	0.278779	0.189106
4	0.288779	0.167106
5	0.692112	-0.720228
6	0.296279	0.150606
7	0.300215	0.256686
8	0.267487	0.103126
9	0.283679	0.177886
10	0.283729	0.177996
11	0.388867	0.276893
12	0.325139	0.216946
13	0.284713	0.177592
14	0.284312	0.177812
15	0.284179	0.177886
16	0.283979	0.177996
17	0.203759	-0.160794

جدول ۳. رتبه‌بندی مقادیر سود و محاسبه‌ی میانگین.

Average	Sum	Follower structure	Leader structure	Sample
0.45	5	4	1	1
0.72	8	6	2	2
1.81	20	14	6	3
2	22	8	14	4
1.81	20	1	19	5
2	22	7	15	6
2.9	32	16	16	7
0.9	10	5	5	8
1.72	19	12	7	9
1.9	21	13	8	10
3.18	35	17	18	11
2.9	32	15	17	12
2	22	10	12	13
2.09	23	11	12	14
2.09	23	12	11	15
2.09	23	13	10	16
0.45	5	2	3	17
0.63	7	3	4	18
1.63	18	9	9	19