Journal of
Improvement Management
Vol.19 No. 2, Summer 2025(Serial 68)

Application of security games in modeling interdependent network disruptions

Milad Yari [1☎], Ramin Sadeghian [2], Meisam Jafari Eskandari [3]

1- Ph.D. Candidate in Industrial Engineering, Payame Noor University, Tehran, Iran.
2- Prof., Industrial Engineering Department, Payame Noor University, Tehran, Iran.
3- Associate Prof., Industrial Engineering Department, Payame Noor University, Tehran, Iran.

Abstract:

By expansion of the application of game theory in modeling various problems and the competitive nature of the real world, the use of this method in solving problems related to vital and important networks that affect the security of a country or society was introduced as security games.

In this research, an interdependent network has been studied under disruption, which, due to the dependence of its elements, a disruption in one component of the network affects other components and leads to sequential or cascading disruptions. The infrastructure and vital networks of a country, such as electricity distribution, transportation, telecommunications, finance and banking networks, have been studied. Given the nature of the subject under study, a game is formed between the attacker (disruptor) and the defender (network), each of which tries to optimize its strategies. The ultimate goal of the attacker is to collapse the network due to cascading disruptions, and the goal of the defender is to prevent the disruption or reduce its impact and ultimately maintain the stability of the network.

In this game, the attacker always makes the best decision to disrupt the current network flow, and the defender considers all the attacker's behaviors in previous iterations and acts to maximize the network flow. This iterative game continues until the goals of the two players converge.

Keywords: Disruptions, Game Theory, Interdependent Networks, Security Games.

DOI: 10.22034/jmi.2025.501405.3175

1. ☎ Corresponding Author: miladyari@student.pnu.ac.ir
2. sadeghian@pnu.ac.ir
3. meisam_jafari@pnu.ac.ir

کاربرد بازی‌های امنیتی در مدلسازی اختلالات شبکه‌های وابسته

دوره ۱۹ شماره ۲ (پیاپی ۶۸)
فصل تابستان ۱۴۰۴

نوع مقاله: پژوهشی (تاریخ دریافت: ۱۴۰۳/۱۱/۰۲ تاریخ پذیرش: ۱۴۰۴/۰۳/۲۶) صفحات ۱۳۸ تا ۱۶۵

میلاد یاری[1] دانشجوی دکتری مهندسی صنایع، دانشگاه پیام نور، تهران، ایران.
رامین صادقیان[2] استاد گروه مهندسی صنایع، دانشگاه پیام نور، تهران، ایران.
میثم جعفری اسکندری[3] دانشیار گروه مهندسی صنایع، دانشگاه پیام نور، تهران، ایران.

چکیده

با گسترش کاربرد نظریه بازی‌ها در مدلسازی مسائل مختلف و ماهیت رقابتی دنیای واقعی، استفاده از این روش در حل مسائل مربوط به شبکه‌های حیاتی و مهم که امنیت یک کشور یا جامعه را تحت شعاع قرار می‌دهد، به عنوان بازی‌های امنیتی معرفی گردید.

در این پژوهش، شبکه‌ای وابسته در زمان بروز اختلال مورد مطالعه قرار گرفته است که به دلیل وابستگی عناصر آن، اختلال در یک جزء از شبکه اجزای دیگر را تحت تاثیر قرار می‌دهد و منجر به اختلالات متوالی یا آبشاری می‌گردد. شبکه‌های زیرساختی و حیاتی یک کشور نظیر شبکه‌های توزیع برق، حمل‌ونقل، مخابراتی، مالی و بانکی مورد مطالعه قرار گرفته است. با توجه به ماهیت موضوع مورد بررسی، یک بازی میان مهاجم(عامل اختلال) و مدافع(شبکه) شکل می‌گیرد که هر کدام سعی در بهینه کردن استراتژی‌های خود دارند. هدف نهایی مهاجم، فروپاشی شبکه در اثر وقوع اختلالات آبشاری و هدف مدافع، ممانعت از بروز اختلال و یا کاهش اثر آن و نهایتاً حفظ پایداری شبکه است.

در این بازی، مهاجم همواره بهترین تصمیم به منظور ایجاد اختلال در جریان فعلی شبکه را اتخاذ می‌کند و مدافع تمام رفتارهای مهاجم در تکرارهای قبلی را در نظر گرفته و به منظور حداکثرسازی جریان شبکه عمل می‌کند و این بازی تکرارشونده تا همگرایی اهداف دو بازیکن به یکدیگر ادامه می‌یابد.

واژگان کلیدی: اختلالات، بازی‌های امنیتی، شبکه‌های وابسته، نظریه بازی‌ها.

۱. ☎مسئول مکاتبات: miladyari@student.pnu.ac.ir
۲. sadeghian@pnu.ac.ir
۳. meisam_jafari@pnu.ac.ir

۱- مقدمه

شبکه‌های وابسته به سیستم‌های پیچیده‌ای اشاره دارند که در آن‌ها چندین شبکه مختلف به یکدیگر وابسته هستند و عملکرد هر شبکه بر عملکرد شبکه‌های دیگر تاثیر می‌گذارد. این مفهوم در حوزه‌های مختلفی مانند مهندسی، علوم کامپیوتر، فیزیک و علوم اجتماعی کاربرد دارد. ویژگی اصلی شبکه‌های وابسته عبارتند از: ارتباط متقابل، پیچیدگی، حساسیت به اختلالات و کاربرد گسترده در دنیای واقعی.

بازی‌های امنیتی شاخه‌ای از نظریه بازی‌هاست که برای مدلسازی تعاملات استراتژیک بین مدافعان و مهاجمان در محیط‌های امنیتی استفاده می‌شوند. این بازی‌ها معمولا در حوزه‌هایی مانند امنیت سایبری، حراست فیزیکی، کنترل ترافیک هوایی، مبارزه با تروریسم و امنیت ملی کاربرد دارند. این بازی‌ها ابزاری قدرتمند برای مدیریت هوشمند تهدیدات در محیط‌های پیچیده هستند و سازمان‌ها می‌توانند با استفاده از این بازی‌ها، منافع امنیتی را بهینه توزیع کنند و استراتژی‌های دفاعی کارآمدی‌تری طراحی نمایند.

دارا بودن شبکه‌های زیرساختی وابسته‌بهم و قابل اعتماد برای دستیابی به جامعه ایمن و مولد، حیاتی و بسیار حائز اهمیت است. سیستم‌ها به دلیل وابستگی متقابل میان شبکه‌های مختلف، در برابر اختلالات یا از دست دادن عملکردشان بسیار آسیب پذیر هستند و هر اختلال قابلیت انتشار در کل سیستم را دارد. (Almoghathawi, González and Barker 2021)

موضوعاتی از قبیل امنیت ملی، رونق اقتصادی و رفاه اجتماعی به مجموعه ای از زیرساخت‌های بسیار مهم وابسته‌بهم بستگی دارد که این زیرساخت‌ها شامل مواردی نظیر شبکه سراسری توزیع نیروی برق، شبکه‌های مخابراتی و اطلاع‌رسانی، شبکه‌های حمل‌ونقل و سیستم‌های بانکی و مالی می‌باشد. اگرچه وابستگی روابط باعث بهبود و عملکرد مطلوب زیرساخت‌های مهم می‌شود، اما این سیستم‌های وابسته‌بهم در برابر اختلالات، حوادث طبیعی و حملات شکننده هستند. برای مثال، در صورت وجود حمله یا عدم موفقیت تصادفی در یک سیستم وابسته‌بهم، شکست در یک شبکه می‌تواند باعث خرابی گره‌های وابسته در سایر شبکه‌های مکمل شود و بالعکس. این روند ممکن است به صورت بازگشتی ادامه یابد و باعث ایجاد آبشاری از خرابی‌ها شود که به طور بالقوه می‌توانند کل سیستم را مختل کند. اختلال در شبکه‌های وابسته به مراتب پیچیده‌تر و مخرب‌تر از اختلال در یک شبکه ایزوله است، زیرا سیستم‌ها نه تنها در معرض تهدیدهای مربوط به شبکه خودشان بلکه در مقابل اختلالات آبشاری ناشی از سیستم‌های وابسته‌شان هستند. (Sun, Bocchini and Davison 2022)

درک رفتار این زیرساخت‌ها خصوصاً در زمان بروز اختلال در زمانی که سیستم‌های وابسته‌بهم به یک بخش جدایی‌ناپذیر از زندگی روزمره ما تبدیل شده‌اند، این سوال اساسی را در ذهن ما مطرح می‌کند که چگونه می‌توانیم آن‌ها را به شکلی استوار و مطمئن طراحی کنیم. کاربردهای بی‌شمار سیستم‌های

وابسته‌بهم در مباحث مربوط به امنیت ملی، سیستم‌های سلامت، نظارت و محافظت از منابع طبیعی، سیستم توزیع نیروی برق و خدمات اضطراری، عملکرد موفق و کارآمد آن‌ها در هسته فناوری‌هایی که برای ما حیاتی هستند را نشان می‌دهد. برای این منظور، باید تمرکز اصلی در درک آسیب‌پذیری‌های این شبکه‌ها و به ویژه علت اصلی بروز اختلالات آبشاری در مقیاس بزرگ از طریق توصیف دقیق و مدلسازی این وابستگی‌های ذاتی موردتوجه قرار گیرد. (Lehto 2022)

مدل‌ها و شبیه‌سازی‌ها می‌توانند درک مناسبی از ماهیت پیچیده رفتارها و ویژگی‌های عملیاتی شبکه‌های زیرساختی ارائه دهند و شامل روابط وابسته‌بهم باشند تا تصویر دقیقی از خصوصیات زیرساختی فعالیت‌ها و عملیات ارائه نمایند. علم شبکه سنتی در ارائه چنین ویژگی‌هایی دچار ضعف می‌باشد و علت آن تمرکز اصلی بر روی شبکه‌های منفرد بوده است، یعنی شبکه‌هایی که با هم ارتباط ندارند یا به شبکه دیگری وابسته نیستند. (Chen, Touati and Zhu 2021)

مدل‌سازی بازی‌های امنیتی در شبکه‌های وابسته‌بهم، اهمیت رویکرد چندوجهی را که شامل اصول نظریه بازی‌ها، عدم قطعیت و همکاری ذینفعان است، برجسته می‌کند. همانطور که تهدیدها تکامل می‌یابند و شبکه‌ها به طور فزاینده‌ای به هم متصل می‌شوند، تحقیقات مداوم برای افزایش استحکام و انعطاف‌پذیری استراتژی‌های امنیتی ضروری است. با پرداختن به چالش‌ها و بررسی روش‌های جدید، این زمینه می‌تواند به طور قابل توجهی به بهبود امنیت در سیستم‌های پیچیده کمک کند. (Wang et al 2022)

علیرغم برخی فعالیت‌های تحقیقاتی اخیر با هدف مطالعه شبکه‌های وابسته، تعداد کمی از آن‌ها جنبه‌های مهندسی شبکه‌های وابسته‌بهم را درنظر گرفته‌اند و تعداد کمی چگونگی طراحی چنین سیستم‌هایی برای داشتن حداکثر استواری تحت محدودیت‌های طراحی خاص را مطالعه کرده‌اند. ادبیات فعلی نیز فاقد مدل‌هایی از سیستم‌های وابسته‌بهم است که امکان مطالعه استواری سیستم‌های ادغام شده با رفتار ذاتی متفاوت را فراهم کند. بنابراین نیاز به توسعه رویکردهای جدید برای مدلسازی و تجزیه‌وتحلیل اختلالات آبشاری در سیستم‌های وابسته‌بهم و درنظرگرفتن جنبه‌های مهندسی بهبود استواری شبکه‌های وابسته‌بهم وجود دارد. (Shen et al 2024)

در این تحقیق بررسی و تحلیل یک شبکه را مدنظر داریم که این شبکه زیرساختی از تعدادی شبکه وابسته تشکیل شده است. به عنوان نمونه‌ای از این نوع شبکه‌ها، می توان به شبکه اطلاعات بانکی یک کشور اشاره نمود که متشکل از تعدادی شبکه وابسته از بانک‌های مختلف می‌باشد. شبکه‌های وابسته بعلت انعطاف‌پذیری و کارایی بالایی که دارند پیشرفت روزافزونی داشته‌اند اما روابط وابستگی متقابل آن‌ها منجر به تاثیرگذاری در شبکه‌های مکمل‌شان می‌گردد. بروز اختلالات آبشاری در این شبکه و انتشار خرابی در سیستم مربوطه را بررسی می‌کنیم که این اختلالات پی در پی ممکن است تا فروپاشی کامل شبکه پیش رود و به دنبال تشخیص و تقلیل اثرات ناشی از این گونه اختلالات و فعال ماندن شبکه هستیم. حملات سایبری مثالی معروف از بروز اختلال در این گونه شبکه‌هاست که با طراحی

استوار شبکه مربوطه در صدد مقابله با اثرات مخرب حملات هستیم و با استفاده از بازی‌های امنیتی و طراحی یک بازی میان مهاجم و مدافع در هنگام بروز حملات به مدلسازی این شبکه‌ها می‌پردازیم.

مطالعه درباره استواری شبکه‌ها مدتهاست که بر یک شبکه منفرد یا ایزوله که با شبکه‌های دیگر ارتباط ندارد، متمرکز شده است. با این حال، این شرایط درحال حاضر به‌ندرت در زندگی و جامعه ما اتفاق می‌افتد. زیرساخت‌های مدرن به طور قابل توجهی وابسته به یکدیگر هستند و تحلیل سیستم با شبکه‌های وابسته را پیچیده‌تر می‌کنند. ویژگی اساسی شبکه‌های وابسته این است که اختلال در یک شبکه می‌تواند به یک شبکه مکمل دیگر در آن سیستم سرایت نماید و تا خرابی بین شبکه خراب اولیه و شبکه‌های مکمل آن بطور رفت و برگشتی ادامه یابد و موجب فراگیر شدن اختلالات آبشاری در سراسر شبکه شود که این نوع از اختلال منجر به خسارات بسیار شدید خواهد شد. لذا مطالعه روابط میان شبکه‌های وابسته و مدلسازی دقیق ساختار این شبکه‌ها، منجر به کاهش آسیب‌پذیری زیرساخت‌های اساسی خواهد شد. (Zhu and Basar 2015)

درک آسیب‌پذیری‌ها و علت اصلی بروز غیرمنتظره شکست‌های آبشاری در مقیاس بزرگ از طریق توصیف دقیق و الگوبرداری ذاتی بین و در داخل اجزای مختلف شبکه میسر است و نیازمند مطالعات توپولوژی شبکه است. در واقعیت، شبکه‌هایی با عملکرد مشابه غالباً برای ساختن یک ساختار مشترک برای استواری بهتر و ریسک کمتر با یکدیگر همراه می‌شوند، به عنوان مثال شبکه‌های توزیع برق مناطق مختلف ممکن است باهم همراه باشند یا موسسات مالی مشابه ممکن است برای ریسک کمتر باهم در ارتباط باشند. بنابراین دستیابی به یک شبکه استوار در زمان بروز اختلال در زیرساخت‌های حیاتی از اهداف مهم و ضروری مدلسازی شبکه‌های وابسته می‌باشد که در این تحقیق درصدد دستیابی به این مهم هستیم.

۲- مبانی نظری و پیشینه پژوهش

ادبیات مدل‌سازی بازی‌های امنیتی در شبکه‌های وابسته، اهمیت رویکرد چندوجهی را که شامل اصول نظریه بازی‌ها، عدم قطعیت و همکاری ذینفعان است، برجسته می‌کند. همانطور که تهدیدها تکامل می‌یابند و شبکه‌ها به طور فزاینده‌ای بهم متصل می‌شوند، تحقیقات مداوم برای افزایش استحکام و انعطاف‌پذیری استراتژی‌های امنیتی ضروری است. با پرداختن به چالش‌ها و بررسی روش‌های جدید، این زمینه می‌تواند به طور قابل توجهی به بهبود امنیت در سیستم‌های پیچیده کمک کند. (Huang, Li and Cai 2023)

بازی‌های امنیتی تعاملات استراتژیکی هستند که در آن بازیکنان(مدافعان و مهاجمان) تصمیماتی اتخاذ می‌کنند و هدف نهایی این تصمیمات برای هر کدام از بازیکنان این است که عایدی خود را به حداکثر برسانند، که اغلب با استفاده از تئوری بازی‌ها مدلسازی می‌شوند. در جدول زیر طبقه‌بندی انواع بازی‌های امنیتی ارائه شده است. با طبقه‌بندی بازی‌های امنیتی به این دسته‌ها، پژوهشگران و

کارشناسان می‌توانند تعاملات استراتژیک موجود در سناریوهای امنیتی را بهتر درک کرده و سیاست‌ها و استراتژی‌های امنیتی مؤثرتری را توسعه دهند. هر طبقه‌بندی اطلاعاتی درباره ماهیت بازی مورد تجزیه و تحلیل و رویکردهای بهینه برای کاهش ریسک و افزایش امنیت ارائه می‌دهد. (Hunt and Zhuang 2024)

جدول ۱: طبقه‌بندی بازی‌های امنیتی

ردیف	نوع بازی	توضیح	منبع
۱	ایستا/پویا	بازی‌های ایستا: بازیکنان تصمیمات را به‌طور همزمان بدون آنکه از انتخاب‌های دیگر بازیکنان مطلع باشند، اتخاذ می‌کنند. استراتژی‌ها ثابت و بازی یک‌بار انجام می‌شود. بازی‌های پویا: بازیکنان در چندین دوره زمانی تصمیم‌گیری می‌کنند که در آن تصمیمات یک بازیکن می‌تواند بر تصمیمات آینده دیگران تأثیر بگذارد.	(Benchekroun and Long 2011)
۲	مجموع صفر/غیرصفر	بازی‌های مجموع صفر: سود یک بازیکن دقیقاً با ضررهای یک بازیکن دیگر متعادل می‌شود و کل عایدی‌ها ثابت باقی می‌ماند. بازی‌های مجموع غیرصفر: بازیکنان می‌توانند عایدی‌هایی داشته باشند که برای همه سودمند باشد و همکاری و منفعت متقابل را امکان‌پذیر می‌سازد.	(Fox 2010)
۳	اطلاعات کامل/ناقص	اطلاعات کامل: همه بازیکنان از ساختار بازی، عایدی‌ها و استراتژی‌های موجود برای سایر بازیکنان به‌طور کامل آگاه هستند. اطلاعات ناقص: بازیکنان از نوع، استراتژی‌ها یا عایدی‌های سایر بازیکنان اطلاعات محدودی دارند که منجر به عدم اطمینان در تصمیم‌گیری می‌شود.	(Gerardi 2004)
۴	همکارانه/غیرهمکارانه	بازی‌های همکارانه: بازیکنان می‌توانند ائتلاف‌هایی تشکیل و توافق‌های لازم را برای بهبود نتایج خود انجام دهند. بازی‌های غیرهمکارانه: بازیکنان به‌طور مستقل عمل می‌کنند و نمی‌توانند توافق‌های لازم را انجام دهند و بر استراتژی‌های فردی تمرکز دارند.	(Mirzaei-Nodoushan, Bozorg-Haddad and A. Loáiciga 2022)

ردیف	نوع بازی	توضیح	منبع
۵	ترتیبی/همزمان	بازی‌های ترتیبی: بازیکنان تصمیمات را یکی پس از دیگری می‌گیرند و به بازیکنان بعدی این امکان را می‌دهند که اقدامات قبلی را مشاهده کنند. بازی‌های همزمان: بازیکنان تصمیمات را در زمان واحدی بدون اینکه از انتخاب‌های دیگران مطلع باشند، اتخاذ می‌کنند.	Brocas, Carrillo and Sachdeva (2018)
مقاله حاضر	ترکیبی	یک بازی با ساختاری پویا، مجموع عایدی غیرصفر، اطلاعات ناقص طرفین، بصورت غیرهمکارانه و با تصمیمات ترتیبی	

استواری و آسیب‌پذیری سیستم‌های دنیای واقعی همواره مسئله‌ای حائز اهمیت بوده است و باتوجه به توسعه سریع فناوری‌های اطلاعات و پیشرفت‌های اخیر در شبکه‌ها، درحال‌حاضر شبکه‌ها نقش مهمتری در مدلسازی و تجزیه‌وتحلیل زیرساخت‌هایی که اصول زندگی و صنعت ما را تشکیل می‌دهند، دارند. شکست‌های آبشاری یکی از مهمترین موضوعاتی است که در استواری سیستم‌های مختلف مورد بررسی قرار گرفته است، از آنجا که تجزیه یک عنصر یا یک گروه بسیار کوچک از اجزا می‌تواند به دلیل پویایی توزیع مجدد جریان‌ها روی شبکه‌ها برای شکست کل سیستم کافی باشد. اختلالات آبشاری می‌تواند باعث ایجاد یک سری از خرابی‌ها یا تأثیرات بعدی در سیستم‌ها یا فرآیندهای بهم پیوسته شود که این مفهوم اغلب در زمینه‌هایی مانند مدیریت ریسک، مهندسی سیستم‌ها و واکنش به بلایا استفاده می شود. اختلالات را می توان بر اساس معیارهای مختلفی طبقه‌بندی کرد،(Soto et al 2022) مانند:

۱. منبع اختلال: طبیعی(مانند زلزله، سیل)، فناوری(مانند حملات سایبری، خرابی سیستم)، یا ناشی از انسان(مانند اعتصابات، خرابکاری).

۲. سطح تأثیر: اختلالات موضعی که بر یک منطقه کوچک تأثیر می‌گذارد یا اختلالات گسترده ای که بر چندین منطقه یا بخش تأثیر می‌گذارد.

۳. مدت زمان: اختلالات کوتاه مدتی که به سرعت برطرف می‌شوند در مقابل اختلالات طولانی مدت که نیازمند تلاش‌های قابل‌توجهی برای بازیابی هستند.

۴. ارتباط متقابل: چگونه اختلالات در یک حوزه می‌تواند منجر به شکست در سایر حوزه‌ها شود که اهمیت درک وابستگی‌های متقابل سیستم را برجسته می‌کند.

۵. قابلیت پاسخگویی: توانایی سیستم‌ها برای جذب، انطباق یا بازیابی از اختلالات.

مهمترین زیرساختی که در آن شکست‌های آبشاری می‌تواند خسارت بزرگی ایجاد کند، سیستم‌های توزیع نیروی برق یا شبکه‌های هوشمند است، از آنجا که خرابی سیستم نیرو می‌تواند اثرات دور از دسترس و مرتبه بالاتری بر اقتصاد مانند بیشتر جنبه های زندگی داشته باشد و همچنین موجب آسیب دیدن عملکرد دیگر زیرساخت‌های مهم گردد. علاوه بر سیستم‌های توزیع نیرو، شکست‌های آبشاری نیز در مناطق دیگر سیستم‌های اجتماعی و اقتصادی که قسمت بزرگی از زندگی ماست، رخ می‌دهد. برای مثال، خرابی‌های آبشاری عاملی اساسی است که بر سیستم‌های حمل‌ونقل تأثیر می‌گذارد، جایی که خرابی سیگنال و تعلیق مترو ممکن است رخ دهد که منجر به از بین رفتن ظرفیت شبکه راه‌های موقت می شود. (Mühlhofer et al 2023)

نیاز فزاینده‌ای برای توسعه مدل‌ها و ابزار تحلیلی برای مطالعه استواری سیستم‌های وابسته در هنگام وقوع شکست‌های آبشاری وجود دارد. بررسی خرابی‌های شبکه یا مقاومت شبکه‌ها در برابر حذف گره‌ها یا یال‌های ناشی از شکست‌های تصادفی یا حملات عمدی با خصوصیات ایستای شبکه آغاز می‌شود. این بدان معناست که چنین مطالعاتی بر حذف گروهی از گره‌ها و عواقب مربوط به عملکرد شبکه متمرکز است. براساس این شیوه، پیامدهای ناگواری که در شبکه وقتی که گروه قابل توجهی از گره‌ها حذف شوند رخ می‌دهد نشان داده شده است. اما در بسیاری از سیستم‌های دنیای واقعی مانند شبکه نیرو، خرابی گره‌های منفرد یا بسیار کمی از گره‌ها می‌توانند به دلیل پویایی توزیع مجدد جریان در شبکه، باعث سقوط در سطح کل سیستم شوند. بنابراین رویکردهای پویا برای در نظر گرفتن این پدیده توسعه یافته اند. (Zhang, Liu, Tu and Kong 2022)

در مقاله (Yang and Zhu 2024)، روش‌های مبتنی بر تئوری بازی‌ها جهت استواری، امنیت و انعطاف‌پذیری سیستم‌های کنترل فیزیکی-سایبری مورد مطالعه قرار گرفت. با افزایش سطح یکپارچگی سیستم‌های کنترل توسط فناوری‌های اطلاعاتی جدید، سیستم‌های کنترل جدید با عدم قطعیت نه تنها از جانب فضای فیزیکی بلکه از طرف اجزای سایبری شبکه مواجه هستند. عدم قطعیت‌های ناشی از سیستم سایبری اغلب غیرقابل پیش‌بینی و مخرب‌تر برای سیستم‌های کنترل هستند. واژه استواری اغلب به توانایی سیستم برای بقا با محدوده مشخصی از پارامترهای غیرقطعی اشاره دارد و امنیت توانایی سیستم را برای بقا و محافظت از رفتارهای نامطلوب و حوادث غیرقابل پیش‌بینی توصیف می‌کند.

در مدل پایه، یک سیستم شامل مجموعه‌ای از شبکه‌های وابسته را در نظر می‌گیریم که هرکدام دارای مقداری بار اولیه، مقداری ظرفیت خالی و با حداکثر ظرفیت مشخص می‌باشند. در زمان بروز حملات و اختلال در انتقال بار توسط خطوط آسیب دیده، بار خطوط آسیب دیده در شبکه اصلی یا شبکه مکملشان مجددا توزیع می‌گردد تا از بروز اختلالات آبشاری در سیستم و فروپاشی آن جلوگیری نماید که بصورت زیر مدلسازی می‌گردد:

جدول۲: نمادهای مورد استفاده در مدل پایه

نمادها	تعاریف
N	مجموعه کل شبکه‌های سیستم
l_i	خطوط شبکه i
$C_{k,i}$	حداکثر ظرفیت خط k در شبکه i
$L_{k,i}$	بار اولیه خط k در شبکه i
$S_{k,i}$	فضای خالی خط k در شبکه i
$P_{LS}(x,y)$	تابع چگالی احتمالی توزیع بار
a_{ij}	ضریب یکپارچگی توزیع بار

یک سیستم شامل **n** شبکه که باهم در ارتباط هستند درنظر می‌گیریم:**N={1 , … , n}** مجموعه کل شبکه‌های سیستم می‌باشد. برای **i∈N** فرض می‌کنیم شبکه **i** شامل N_i خط $l_{1,i}$, … , $l_{Ni,i}$ با بار اولیه $L_{1,i}$, … , $L_{Ni,i}$ می‌باشد. بنابراین حداکثر ظرفیت خط **k** در شبکه **i**:

$$C_{k,i} = L_{k,i} + S_{k,i} \quad , i \in N \, , \, k = 1,..., N_i \qquad (I)$$

که $S_{k,i}$ بعنوان فضای خالی خط **k** در شبکه **i** معرفی می‌شود(حداکثر بار اضافی قابل تحمل).

جفت فضای بدون بار $\{L_{k,i}, S_{k,i}\}_{k=1}^{N_i}$ بطور مستقل و مساوی از طریق زیر توزیع می‌شوند:

$$P_{L_i S_i}(x,y) = P[L_{k,i} \le x, S_{k,i} \le y] \quad , \quad k = 1,..., N_i \qquad (II)$$

تابع چگالی احتمالی جفت مرتبط عبارتست از:

$$p_{L_i S_i}(x,y) = \frac{\partial^2}{\partial x \, \partial y} P_{L_i S_i}(x,y) \quad , \; S_{k,i} > 0 \, , L_{k,i} > 0 \qquad (III)$$

در ابتدا $1\text{-}p_i$ قسمت از خطوط در شبکه **i** بصورت تصادفی مورد حمله قرار می‌گیرد. بار خطوط از دست رفته در شبکه اصلی یا شبکه‌های مکمل براساس قوانین مدیریت توزیع بار مجدداً توزیع می‌گردد. اختلال بیشتر درشبکه اولیه یا مکمل که بیش از ظرفیت‌شان بارگذاری شده‌اند بصورت متوالی منجر به آبشاری از اختلالات می‌گردد. اختلالات آبشاری همزمان درون و بین شبکه‌ها اتفاق افتاده و یک رفتار پویا و ارتباط پیچیده بین سطوح یکپارچگی و استواری کلی سیستم را منجر می‌شود. (Etesami and Başar 2019)

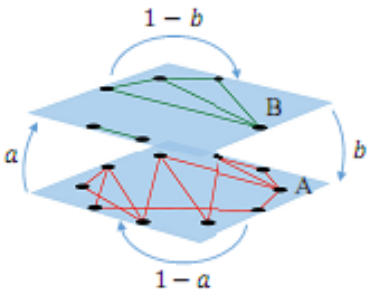
تعیین قسمتی از خطوط فعال هر شبکه در حالت پایدار(نقطه‌ای که اختلالات آبشاری متوقف می‌شود) یکی از اهداف این تحقیق است و در نهایت تحلیلی از عملکرد فرآیند پویای اختلالات آبشاری ارائه می‌دهیم. در این روش فرض می‌شود زمانی که یک خط از دست برود، جریان آن بین شبکه خودش

و شبکه دیگری با نسبتی که توسط ضریب یکپارچگی مشخص می‌شود، توزیع مجدد می‌گردد. نسبتی از بار خط ازدست رفته در شبکه **i** که به شبکه **j** می‌رسد توسط ضریب یکپارچگی a_{ij} تعیین می‌شود:

$$\sum_{j \in N} a_{ij} = 1 \quad for\ i \qquad \text{(IV)}$$

و نسبتی از بار که در شبکه **i** بصورت داخلی توزیع مجدد می‌شود عبارتست از :

$$1 - \sum_{j \in N - \{i\}} a_{ij} \qquad \text{(V)}$$



شکل ۱: مدل پایه‌ای دو شبکه وابسته A و B

زمانی که اختلال در شبکه **A** رخ می‌دهد، **a** قسمت از بار این شبکه به شبکه **B** منتقل می‌شود و **1-a** قسمت از بار باقیمانده بطور داخلی در شبکه **A** مجدداً توزیع می‌گردد. درمورد شبکه **B** نیز همین شرایط صادق است. **a , b □ [0,1]**

فرض کنیم **$1-p_1$** قسمت از خطوط شبکه **A** و **$1-p_2$** قسمت از خطوط شبکه **B** بطور تصادفی دچار اختلال گردد. حملات اولیه ممکن است منجر به اختلالات آبشاری گردد و اگر یکی از شبکه‌ها در طول فرآیند متلاشی شود، شبکه دیگر باقیمانده بار آن را متحمل می‌شود و بعنوان یک شبکه منفرد ازاین به بعد عمل می‌کند.

$\{1,\ldots,N_A\} \subset N_{s,A}$ مجموعه خطوطی که در حالت پایه شبکه هنوز فعال‌اند.**$n_{\infty,A}(p_1)$** قسمت نهایی انتظاری خطوط فعال شبکه زمانی که **$1-p_1$** قسمت از خطوط بطور تصادفی مورد حمله قرار گرفته است و استواری سیستم به وسیله رفتار **$n_{\infty,A}(p_1)$** و **$n_{\infty,B}(p_2)$** برای تمامی اندازه حملات ارزیابی می‌گردد.

$$n_{\infty,A}(p_1) = \lim_{N_A \to \infty} \frac{E[|N_{s,A}(p_1)|]}{N_A} \qquad \text{(VI)}$$

۳- روش‌شناسی

این مقاله از جهت روش‌شناسی در زمره تحقیقات کاربردی قرار دارد که با استفاده از نتایج تحقیقات بنیادی به منظور بهبود و به کمال رساندن رفتارها، روش‌ها، ابزارها، وسایل، تولیدات، ساختارها و الگوهای مورد استفاده جوامع انسانی، انجام شده است. در تحقیق حاضر از مطالعات کتابخانه‌ای در زمینه نظریه بازی‌ها، شبکه‌های وابسته و بحث اختلالات آبشاری استفاده شده است. (Pandey 2021)

داده‌ها و اطلاعات مربوط به تحقیق با استفاده از مطالعات کتابخانه‌ای و الگوبرداری از اطلاعات مربوط به شبکه‌های زیرساختی کشور نظیر شبکه‌های اطلاعاتی، شبکه‌های انتقال آب، شبکه‌های توزیع برق، شبکه‌های اطلاعات مالی و بانکی جمع‌آوری شده است. تجزیه‌وتحلیل و مقایسه اطلاعات قبل از اجرای مدل و نتایج حاصل از اجرای مدل در این تحقیق جهت اعتبارسنجی مدل مورد استفاده قرار می‌گیرد و در صورت لزوم از شبیه‌سازی و مدلسازی مسئله در ابعاد کوچک استفاده می‌کنیم. روش تحلیل و استفاده از بازی‌های امنیتی در مدل‌سازی اختلالات شبکه‌های وابسته معمولاً شامل مراحل زیر است:

۱. تعریف شبکه و سناریوهای اختلال: ساختار شبکه و انواع اختلالاتی که ممکن است رخ دهد، از جمله وابستگی‌های آنها را شناسایی می‌کنیم.

۲. مدلسازی بازی امنیتی: با تعریف بازیکنان(به عنوان مثال، مدافعان و مهاجمان)، استراتژی‌ها و بازده‌های مرتبط با اقدامات مختلف در پاسخ به اختلالات، بازی امنیتی را فرموله می‌کنیم.

۳. ادغام وابستگی‌ها: وابستگی‌های بین اجزای مختلف شبکه و اختلالات را در مدل بازی ادغام می‌کنیم و اطمینان حاصل کنیم که تعاملات به طور دقیق نشان داده می‌شوند.

۴. تجزیه‌وتحلیل استراتژی‌ها: از تجزیه‌وتحلیل نظریه بازی برای ارزیابی استراتژی‌های بهینه برای مدافعان با درنظرگرفتن اقدامات بالقوه مهاجمان و تأثیر اختلالات استفاده می‌کنیم.

۵. شبیه‌سازی و آزمایش: شبیه‌سازی سناریوهای مختلف برای آزمایش استواری استراتژی‌ها در شرایط مختلف اختلالات شبکه.

۶. تکرار و اصلاح: اجرا و تکرار مدل‌ها و اصلاح آن براساس نتایج و استراتژی‌های بهبود انعطاف‌پذیری در برابر اختلالات شبکه.

تجزیه و تحلیل و مقایسه اطلاعات قبل از اجرای مدل و نتایج حاصل از اجرای مدل در این تحقیق جهت اعتبارسنجی مدل مورد استفاده قرار می‌گیرد و در صورت لزوم از شبیه‌سازی و مدلسازی مسئله در ابعاد کوچک استفاده می‌کنیم.

همچنین به روش‌های مورد استفاده در پژوهش‌های انجام شده در زمینه مدلسازی اختلالات آبشاری در شبکه‌های وابسته با استفاده از نظریه بازی‌ها بطور مختصر در جدول ذیل اشاره شده است:

جدول۳: روش‌های حل مسئله

ردیف	راهکار مقابله و حل مسئله	منبع
۱	Perfect Bayesian equilibrium	(Gudmundsson, Hougaard and Sethuraman 2024)
۲	A repeated two-way signaling game	(Casey, Massey and Mishra 2021)
۳	hybrid game-theoretic framework	(Rao, Ma and He 2022)
۴	dynamic game-theoretic approach	(Cunningham and Tucker 2024)
۵	stochastic (Markov) security game	(Wu, Li and Steven Li. 2021)
۶	repeated Stackelberg Security Games	(Li et al 2024)
۷	a robust and adaptive network flow model	(Yang, Scoglio and Gruenbacher 2021)

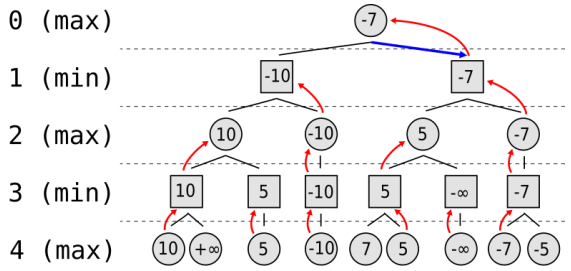
۳-۱ ساختار بازی

مدلسازی بازی در شبکه مورد مطالعه این پژوهش، به صورت یک توالی تکرارشونده از بهترین پاسخ‌های(تابع هدف) مدافع و مهاجم می‌باشد. در تکرار اول، مدافع فرض می‌کند حمله‌ای در سیستم رخ نداده است و مسیری که مقدار جریان ورودی به گره مقصد را ماکزیمم می‌کند، انتخاب کرده و جریان را ماکزیمم می‌کند. سپس، مهاجم حمله بهینه خود را در راستای تخریب حداکثری جریان فوق به کار می‌گیرد. در تکرار بعدی، مدافع تمام حملات آشکار شده در تکرارهای قبل را درنظر می‌گیرد و استراتژی جریان بهینه(استوار) علیه آن حملات را اتخاذ می‌کند و مهاجم همواره بهترین استراتژی ایجاد اختلال علیه جریان آشکار شده توسط مدافع در تکرار فعلی را محاسبه می‌نماید.

این فرایند تکرارشونده تا زمانی که تابع هدف دو بازیکن(مدافع و مهاجم) محدب است و به یک مقدار تعادلی همگرایی دارد، ادامه می‌یابد. لذا در این بازی که به صورت بازی‌های رهبر-پیرو مدلسازی شده است، دو طرف بازی به منظور رسیدن به یک مقدار تعادلی از اهداف خود وارد بازی می‌شوند و پس از طی مراحل تکراری به یک مقدار از برآورده سازی اهداف خود بسنده می‌کنند و بازی به تعادل می‌رسد.

در شکل زیر نمونه‌ای از یک درخت اقدامات دو بازیکن ارائه شده است. در پایین‌ترین لایه(۴) رهبر(مدافع) سعی در بیشینه کردن تابع هدف خود دارد، در لایه بالاتر(۳) پیرو(مهاجم) به منظور آسیب حداکثری به جریان شبکه سعی در کمینه کردن تابع هدف خود دارد و مقادیر کمتر را در هر سناریو

انتخاب می‌کند. مجددا مدافع با توجه به انتخاب مهاجم در لایه بالاتر(۲) سعی در بیشینه کردن جریان شبکه دارد و لذا مقادیر بیشتر در هر سناریو را انتخاب می‌کند و سپس در لایه بعدی(۱) مهاجم کمینه مقدار ممکن از دو سناریوی موجود را انتخاب می‌کند. نهایتا در لایه آخر(۰) دو بازیکن بر روی مقدار هدف (-7) عایدی‌شان به تعادل می‌رسد.



شکل۲: مثالی از درخت اقدامات بازیکنان

در واقع با یک مسئله بهینه‌سازی minmax مواجه هستیم که در آن مدافع بعنوان رهبر و شروع‌کننده بازی سعی در بیشینه‌سازی تابع هدف خود که همان عبور حداکثر جریان در شبکه است را دنبال می‌کند و مهاجم بعنوان پیرو سعی در کمینه‌سازی جریان عبوری در شبکه به منظور ایجاد حداکثر اختلال در شبکه دارد. لذا این توالی تا رسیدن به یک مقدار تعادلی ادامه یافته و پس از ارضای تابع هدف دو بازیکن متوقف می‌گردد.

۴– یافته‌ها

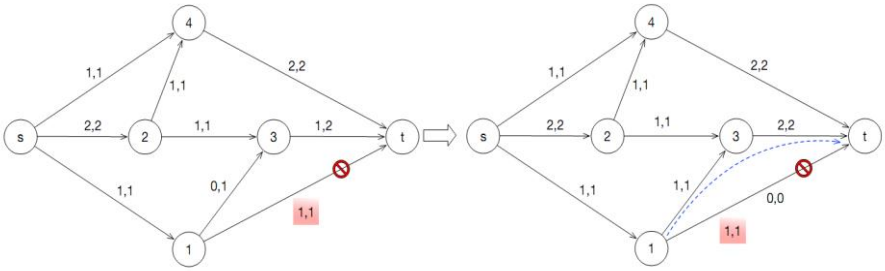
در بیان ویژگی‌های ذاتی شبکه‌های زیرساختی وابسته و مهم نظیر شبکه‌های توزیع سراسری انرژی برق، شبکه‌های مخابراتی، شبکه‌های حمل‌ونقل و شبکه‌های اطلاعات مالی، ذکر این موضوع حائز اهمیت است که این شبکه‌ها در عین حال که انعطاف‌پذیری و کارایی بالایی دارند، در برابر بروز اختلالات آسیب‌پذیر و شکننده‌اند. به دلیل وابستگی میان اجزای این شبکه‌ها، علاوه بر تاثیر تهدیدهای مرتبط با شبکه خودشان، اختلالات آبشاری ناشی از شبکه‌های وابسته‌شان نیز منجر به بروز شرایط مخرب‌تر و پیچیده‌تر از شبکه‌های ایزوله می‌شود. لذا درک رفتار این شبکه‌های زیرساختی خصوصاً در زمان بروز اختلالات، درک آسیب‌پذیری آن‌ها و مدلسازی این وابستگی‌های ذاتی بسیار مهم و چالش برانگیز است. (Zhe et al 2021)

مطالعه روابط میان شبکه‌های وابسته و مدلسازی دقیق ساختار این شبکه‌ها، منجر به کاهش آسیب‌پذیری زیرساخت‌های اساسی خواهد شد. درک آسیب پذیری‌ها و علت اصلی بروز غیرمنتظره اختلالات آبشاری در مقیاس بزرگ از طریق توصیف دقیق و الگوبرداری ارتباطات ذاتی میان و درون اجزای مختلف شبکه میسر می‌شود و لذا دستیابی به یک شبکه استوار در زمان بروز اختلال در زیرساخت‌های حیاتی و اساسی و تقلیل آسیب‌پذیری‌ها، دستاوردی مهم و ارزشمند است. (Pan et al 2021)

در این پژوهش، با محاسبه یک استراتژی جریان بیشینه و استوار از طریق توزیع جریان مجدد توسط یال‌های مجاور شبکه با استفاده از یک بازی تکرارشونده دونفره بین صاحب شبکه و مهاجم، مدلسازی اختلالات صورت پذیرفته است. توسعه مدل‌های بهینه‌سازی برای حل مسئله تصمیم‌گیری دو بازیکن در هر تکرار از بازی به این صورت است که در این مدل بهینه‌سازی، صاحب شبکه تمامی استراتژی‌های حمله مهاجم در تکرارهای قبلی را درنظر می‌گیرد و یک استراتژی جریان استوار که مقدار جریان عبوری شبکه در بدترین حالت حملات قبلی را ماکزیمم کند، محاسبه می‌کند. (Vatenmacher, Svoray, Tsesarsky and Isaac 2022)

حملات سایبری مثالی معروف از بروز اختلال در شبکه‌های وابسته و اساسی است که با طراحی استوار شبکه مربوطه درصدد مقابله با اثرات مخرب حملات هستیم و با استفاده از تئوری بازی‌ها و طراحی یک بازی میان مهاجم و مدافع در هنگام بروز حملات، به مدلسازی این شبکه‌ها می پردازیم و شرایط بازی‌های تکراری با اطلاعات کامل و ناقص را بررسی می‌کنیم. (Ho et al 2022)

همچنین، پارامترهای غیرقطعی را وارد مدل می‌کنیم و از مفاهیم بازی‌های امنیتی و بکارگیری انواع آن در این شبکه بخصوص در شرایط بروز اختلالات آبشاری به جهت نزدیکی به ماهیت این تحقیق بهره می گیریم. در این تحقیق درصدد بدست آوردن اندازه سیستم نهایی بعنوان تابعی از اندازه حملات اولیه، اندازه حمله بحرانی که منجر به فروپاشی کامل سیستم می‌شود و تعیین توزیع جریان بهینه که استواری را بیشینه می‌کند، هستیم.



شکل ۳: مثالی از توزیع مجدد جریان پس از بروز اختلال

برای مثال شکل فوق را در نظر می‌گیریم. در این مثال ۶گره و ۹یال داریم. مقدار اولیه x در شبکه چپ نشان داده شده است که هر جفت عدد روی یال‌ها به ترتیب نشان‌دهنده جریان روی یال و ظرفیت یال می‌باشد. فرض می‌کنیم که طرف مقابل(دشمن) می‌تواند حداکثر به یکی از یال‌های شبکه حمله کند(یال e1t). جریان یال e1t تنها از طریق یال‌های e13 و e3t می‌تواند مجدداً مسیریابی شود و جریان نهایی سایر یال‌ها ثابت می‌ماند. جریان نهایی پس از حمله در شبکه سمت راست نشان داده شده است.

یک شبکه حامل جریان به نام G در نظر می‌گیریم که شامل گره‌های v و یال‌های ε می‌باشد. گره‌های منبع و ترمینال را به ترتیب با s و t نمایش می‌دهیم. برای سهولت مدلسازی و درک بهتر مسئله نمادهای زیر را به اختصار تعریف می‌کنیم:

جدول۴: نمادهای مورد استفاده در مدلسازی مسئله

نمادها	تعاریف
$G =< v , \varepsilon >$	شبکه با دو مولفه گره و یال
$e \in \varepsilon$	یال
U_e	حداکثر ظرفیت یال
δ_v^+	مجموعه یال های ورودی به گره
δ_v^-	مجموعه یال های خروجی از گره
Λ_v	مجموعه کلیه مسیرها از گره v به گره t
$\Lambda_\sigma = \bigcup_{v \in \sigma} \Lambda_v$	مجموعه کلیه مسیرهای ممکن به گره t
Γ	حداکثر تعداد یال مورد حمله واقع شده
x_e	مقدار جریان اولیه یال
μ_e	سناریو حمله به یال
ψ	مجموعه سناریوهای ممکن برای حمله
p_e	هزینه مسیریابی(انتقال) یک واحد جریان از طریق یال
W	عایدی رسیدن موفق یک واحد جریان به گره t

در این شبکه، جریان یال‌های مورد حمله قرارگرفته از طریق یال‌های مجاور دارای ظرفیت، مجدداً مسیریابی و تحصیص می‌گردد. در واقع هدف یافتن یک استراتژی جریان استوار برای شبکه در برابر بدترین سناریو حمله می‌باشد.

جریان شبکه(x) که مقداری غیرمنفی می باشد به یال های شبکه براساس محدودیت های ظرفیت بصورت زیر تخصیص می یابد:

$$\sum_{e\in\delta_v^+} x_e - \sum_{e\in\delta_v^-} x_e = 0 \qquad \forall v \in V \setminus \{s\}$$
$$x_e \le U_e \qquad \forall e \in \varepsilon \qquad (1)$$
$$x_e \ge 0 \qquad \forall e \in \varepsilon$$

χ مجموعه کلیه سناریوهای ممکن جریان که محدودیت (۱) را ارضا می‌کند. سناریو حمله(μ) به این صورت است که اگر یال e مورد حمله قرار گیرد مقدارش برابر یک و در غیر این صورت مقدار صفر را می‌گیرد. مجموعه سناریوهای حمله توسط محدودیت زیر تعریف می گردد:

$$\psi = \sum_e \mu_e \le \Gamma \qquad (2)$$

در این شبکه، جریان یال‌های مورد حمله قرار گرفته از طریق یال‌های مجاور دارای ظرفیت، مجدداً مسیریابی و تحصیص می‌گردد. در واقع هدف یافتن یک استراتژی جریان استوار برای شبکه در برابر بدترین سناریو حمله می‌باشد.

برای تشریح بیشتر مسئله تنظیمات دیگری مورد نیاز می‌باشد. اگر یال e مورد حمله قرار گیرد(μ_e=۱) ظرفیت آن از U_e به m_e تغییر می‌یابد و اگر یال e کاملاً مسدود گردد m_e=0 می‌گردد. همچنین مجموع هزینه مسیریابی جریان(p_e) به نقطه مقصد نباید از W تجاوز کند به همین دلیل یک حد بالای W/2L برای آن در نظر می‌گیریم که L حداکثر تعداد یال‌های مسیر منبع تا مقصد می‌باشد.

جریان اولیه x و سناریو حمله μ را درنظر می‌گیریم. y_e مقدار نهایی جریان یال e و z_e مقدار جریان اضافی که مسیریابی مجدد از طریق یال e شده است. از طریق حل مسئله بهینه سازی خطی زیر، مقدار $M(x,\mu)$ که حداکثر مقدار توافقی x پس مسیریابی مجدد جریان‌ها برای شبکه می‌باشد، محاسبه می‌شود:

$$M(x,\mu) = \max\{Wy_{(t,s)} - \sum_e p_e z_e\} - \sum_e p_e x_e \qquad (3)$$

$s.t.$

$$\sum_{e\in\delta_v^+} y_e - \sum_{e\in\delta_v^-} y_e \ge 0 \qquad \forall v \in V \setminus s \qquad (4)$$
$$y_e = x_e \qquad \forall e \notin \Lambda_{\sigma_\mu} \qquad (5)$$
$$y_e \le (1-\mu_e)U_e + \mu_e m_e \qquad \forall e \in \Lambda_{\sigma_\mu} \qquad (6)$$
$$z_e \ge y_e - x_e \qquad \forall e \in \Lambda_{\sigma_\mu} \qquad (7)$$
$$y_e \ge 0; z_e \ge 0 \qquad \forall e \in \varepsilon \qquad (8)$$

برای حل مسئله تعریف شده در قسمت قبلی، یک توالی تکرارشونده از بهترین پاسخ‌های بازی میان طرف اول و دوم را تشریح می‌کنیم. در تکرار اول بازی، طرف اول فرض می‌کند که حمله‌ای در شبکه رخ نداده است و جریانی که مقدار ورودی به گره مقصد را حداکثر می‌سازد، محاسبه می‌کند. سپس طرف دوم سناریو حمله بهینه جهت مختل کردن جریان محاسبه شده توسط طرف اول را، می‌یابد. در تکرارهای بعدی، طرف اول کلیه سناریوهای حمله آشکارشده در تکرارهای قبلی را در نظر می‌گیرد و یک استراتژی استوار(maximin) در برابر آن حملات می‌یابد. طرف دوم همواره بهترین اختلال علیه جریان بدست آمده توسط طرف اول در تکرار جاری را محاسبه می‌کند. این فرآیند تکرارشونده تا زمانی که تابع هدف هردو بازیگر محدب باشد، ادامه می‌یابد.

$$\min_{\mu\in\psi}\{\max y_{(t,s)} - \sum_{e\in\varepsilon} p_e.z_e\} \qquad (11)$$

$s.t.$

$$\sum_{e\in\delta_v^+} y_e - \sum_{e\in\delta_v^-} y_e \geq 0 \qquad \forall v \in V \setminus s \qquad (12)$$

$$y_e \leq (1-\mu_e)U_e + \mu_e m_e \qquad \forall e\in\varepsilon \qquad (13)$$

$$y_e \leq (1-\pi_e)\bar{X}_e + \pi_e U_e \qquad \forall e\in\varepsilon \qquad (14)$$

$$\pi_e \leq \sum_{e'\in\rho_e} \mu_{e'} \qquad \forall e\in\varepsilon \qquad (15)$$

$$z_e \geq y_e - x_e \qquad \forall e\in\varepsilon \qquad (16)$$

$$\pi_e \in \{0,1\} \qquad \forall e\in\varepsilon \qquad (17)$$

$$y_e \geq 0; z_e \geq 0 \qquad \forall e\in\varepsilon \qquad (18)$$

متاسفانه مدل بهینه‌سازی فوق بصورت مستقیم بعنوان بهینه‌سازی خطی بعلت وجود تابع هدف minimax قابل حل نمی‌باشد. با توجه به این که متغیرهای مسئله ماکزیمم‌سازی درونی همگی پیوسته‌اند، می‌توانیم کل مسئله را به یک مسئله مینیمم‌سازی از طریق محاسبه دوگان مسئله داخلی تبدیل کنیم. برای این منظور ابتدا تابع لاگرانژ را بدست می‌آوریم که برای آزادسازی محدودیت‌های (۱۲)-(۱۷) از متغیرهای ηو$\beta,\gamma,\delta,\omega,\propto$ استفاده می‌کنیم.

$$L(\alpha,\beta,\gamma,\delta,\eta,\omega) = -y_{(t,s)} + \sum_{e\in\varepsilon} p_e z_e + \sum_{v\in N\setminus s} \alpha_v [\sum_{e\in\delta_v^-} y_e - \sum_{e\in\delta_v^+} y_e] + \sum_e \delta_e [\pi_e - \sum_{e'\in\rho_e} \mu_{e'}] \qquad (19)$$

$$+ \sum_{e\in\varepsilon} \gamma_e [y_e - \bar{X}_e - \pi_e (U_e - \bar{X}_e)] + \sum_e \eta_e [\pi_e - 1] + \sum_e \omega_e [y_e - z_e - \bar{X}_e] + \sum_{e\in\varepsilon} \beta_e [y_e - U_e + \mu_e (U_e - m_e)]$$

بنابراین مسئله بهینه‌سازی طرف دوم(مهاجم) با استفاده از مسئله دوگان تابع لاگرانژ، بصورت زیر نوشته می‌شود:

$$\min_{\alpha,\beta,\gamma,\delta,\eta,\omega,\mu} \sum_e \beta_e U_e - \sum_e \beta_e \mu_e (U_e - m_e) + \sum_e \gamma_e \bar{X}_e + \sum_e \delta_e \sum_{e' \in \rho_e} \mu_{e'} + \sum_e \eta_e + \sum_e \omega_e \bar{X}_e \quad (20)$$

$s.t.$

$$\beta_e + \gamma_e + \omega_e + \alpha_v - \alpha_w \geq 0 \qquad \forall e = (v,w) \qquad (21)$$

$$\delta_e + \eta_e - \gamma_e (U_e - \bar{X}_e) \geq 0 \qquad \forall e \in \varepsilon \qquad (22)$$

$$\omega_e \leq p_e \qquad \forall e \in \varepsilon \qquad (23)$$

$$\sum_e \mu_e \leq \Gamma \qquad (24)$$

$$\alpha_t = 1; \alpha_s = 0 \qquad (25)$$

$$\alpha_v, \beta_e, \gamma_e, \delta_e, \eta_e, \omega_e \geq 0; \mu_e \in \{0,1\} \qquad (26)$$

تابع هدف(۲۰) نقطه مینیمم توابع خطی μ را محاسبه می‌کند. می‌توانیم متغیر باینری μ بصورت پیوسته آزادسازی کنیم. اگرچه اگر متغیر μ باینری باشد، وجود این متغیر در تابع هدف (۲۰) منجر به مدل بهینه سازی mixed-integer می‌شود که با روش‌هایی نظیر CPLEX قابل حل می‌باشد.

در مسئله بهینه‌سازی طرف اول(مدافع)، هدف مدافع تعیین استراتژی جریان استوار است که مقدار تابع هدف در بدترین شرایط حمله را براساس عبارت(۱۰) ماکزیمم کند. از آنجا که فضای استراتژی دشمن گسترده است، سناریوهای آشکار شده از تکرار قبل در نظر گرفته می‌شود. با توجه به مجموعه k سناریو حمله آشکار شده در تکرارهای قبلی، مدافع استراتژی جریانی که حداقل مقدار جریان رسیده به مقصد را ماکزیمم کند، محاسبه می‌کند. μ^k سناریو حمله k و x استراتژی جریان استوار علیه حملات می‌باشد. همانطور که از عبارت(۳) مشخص است، عایدی طرف اول از اختلاف بین جریان رسیده به مقصد و هزینه‌های مسیریابی جریان اولیه و جریان‌های مجدد مسیریابی شده بدست می‌آید. بنابراین تابع هدف آن بشکل زیر است:

$$\max_k \min \hat{y}^k_{(t,s)} - \sum_e p_e [\hat{x}_e + \hat{z}^k_e] \qquad (27)$$

تابع هدف (۲۷) با استفاده از عبارت زیر خطی‌سازی می‌گردد که λ بدترین حالت تابع هدف تحت سناریو حمله k را نشان می‌دهد:

$$\max \quad \lambda$$

$$s.t. \qquad \lambda \leq \hat{y}^k_{(t,s)} - \sum_e p_e [\hat{x}_e + \hat{z}^k_e] \qquad \forall k \in K \qquad (28)$$

مسئله بهینه‌سازی خطی طرف اول(مدافع) بصورت زیر است:

$$\max \lambda \tag{29}$$

$$s.t.$$

$$\lambda \le \hat{y}^{k}_{(t,s)} - \sum_{e} p_e [\hat{x}_e + \hat{z}^{k}_{e}] \qquad \forall k \in K \tag{30}$$

$$\hat{z}^{k}_{e} \ge \hat{y}^{k}_{e} - \hat{x}^{k}_{e} \qquad \forall k \in K, e \in \varepsilon \tag{31}$$

$$\sum_{e \in \delta^{+}_{v}} \hat{x}_e - \sum_{e \in \delta^{-}_{v}} \hat{x}_e = 0 \qquad \forall v \in V \setminus s \tag{32}$$

$$\hat{x}_e \le U_e \qquad \forall e \in \varepsilon \tag{33}$$

$$\sum_{e \in \delta^{+}_{v}} \hat{y}^{k}_{e} - \sum_{e \in \delta^{-}_{v}} \hat{y}^{k}_{e} = 0 \qquad \forall k \in K, v \in V \setminus s \tag{34}$$

$$\hat{y}^{k}_{e} \le (1-\mu^{k}_{e}) U_e + \mu^{k}_{e} . m_e \qquad \forall k \in K, e \in \varepsilon \tag{35}$$

$$\hat{y}^{k}_{e} \le (1-\hat{\pi}^{k}_{e}) \hat{x}_e + \hat{\pi}^{k}_{e} . U_e \qquad \forall k \in K, e \in \varepsilon \tag{36}$$

$$\lambda \ge 0; \hat{x}_e \ge 0; \hat{y}_e \ge 0 \tag{37}$$

برای درک بهتر چارچوب کلی روش پیشنهادی ما برای حل این بازی، دو مسئله بهینه‌سازی مدافع و مهاجم در قسمت قبلی را با تشریح مراحل تکرارشونده الگوریتم زیر توضیح می‌دهیم:

اساسا این مسئله به عنوان یک بازی رهبر-پیرو که در آن مدافع به عنوان رهبر و مهاجم به عنوان پیرو در نظر گرفته شده است، مدلسازی می‌گردد که در آن مهاجم قدرتمندتر است و می‌تواند پس از مشاهده تصمیم مدافع، تصمیم‌گیری کند. در نتیجه مدافع نیازمند اتخاذ تصمیمی استوار با درنظر گرفتن کلیه حملات محتمل مهاجم است.

Algorithm

Initialize: $\boldsymbol{X} \leftarrow \{\}, \boldsymbol{\mu} \leftarrow \{\}, \mu_{old} \leftarrow \mathbf{0}, V^L \leftarrow 0, V^U \leftarrow \infty$;
while $(V^U \neq V^L)$ **do**
  $\tilde{\boldsymbol{x}}, V^U \leftarrow \text{ADMINSTRATORPROBLEM}(G, U, \boldsymbol{p}, \boldsymbol{\mu})$;
  μ
  $\boldsymbol{x}_p \leftarrow \tilde{\boldsymbol{x}} \cap \boldsymbol{X}$;
  $\boldsymbol{x}_c \leftarrow \tilde{\boldsymbol{x}} \setminus \boldsymbol{x}_p$;
  if $|\boldsymbol{x}_c| = 0$ **then**
    break ;
  else
    $x^* \leftarrow Random(\boldsymbol{x}_c)$;
    $\boldsymbol{X} \leftarrow \boldsymbol{X} \cup x^*$;
  $\tilde{\mu}, V^L \leftarrow \text{ADVERSARYPROBLEM}(G, U, \boldsymbol{p}, x^*, \Gamma)$;
  if $\tilde{\mu} \neq \mu_{old}$ **then**
    $\boldsymbol{\mu} \leftarrow \boldsymbol{\mu} \cup \tilde{\mu}$;
    $\mu_{old} \leftarrow \tilde{\mu}$;
  else
    break ;
return $\tilde{\boldsymbol{x}}, \boldsymbol{\mu}$

شکل۴: چارچوب کلی الگوریتم حل بازی مدافع و مهاجم

فرض می کنیم X و μ مقادیر تولیدشده جریان شبکه و سناریوهای حمله را به ترتیب در تکرارهای قبلی ذخیره می‌کند و در ابتدا هردو مجموعه خالی هستند. μ_{old} سناریو حمله آخرین تکرار را نگهداری می کند و مقدار آن در زمان ابتدایی در سناریو بدون حمله صفر است. V^L و V^U حد پایین و بالای بازی در نظر گرفته شده‌اند که در زمان اولیه به ترتیب مقدارشان صفر و بی نهایت است.

در هر تکرار از بازی، مدافع مسئله بهینه‌سازی خود را به گونه ای محاسبه می‌کند تا جریان استوار علیه سناریو حمله قبلی(μ) بهینه گردد. مسئله بهینه‌سازی مدافع می‌تواند چندین جواب بهینه داشته باشد که برای مثال در تکرار اول، مدافع ضرورتا یک مسئله حداکثر جریان با حداقل هزینه را حل می‌کند که چندین جواب بهینه با مقدار هدف بهینه دارد. X مجموعه راه‌حل‌های بهینه جریان استوار که در تکرار فعلی محاسبه شده است و حد بالای V^U به مقدار تابع هدف مدافع بروزرسانی می‌شود. از این مجموعه راه‌حل‌های جریان، مقدار x_c که قبلا اجرایی نشده بود مشخص می‌کنیم و اگر تمام جواب‌های X قبلا اجرا شده بود، فرایند تمام و هر جواب از مجموعه X یک جریان استوار علیه حملات ممکن Ψ

می‌باشد. به بیان دیگر اگر یک جریان x^* از مجموعه x_c بصورت تصادفی انتخاب و اجرا کنیم، این جریان جدید x^* به استخری از جواب‌های X اضافه می‌گردد.

اگر مدافع جریان x^* را تولید و اجرا نماید، مهاجم بهترین سناریو حمله $\tilde{\mu}$ را محاسبه کرده به طوریکه جریان x^* با حل تابع هدف خود مختل نماید و حد پایین V^L به مقدار تابع هدف مهاجم بروزرسانی می‌شود. اگر مهاجم سناریو حمله تکرارهای قبل را مجدد تکرار نکند، سناریو جدید $\tilde{\mu}$ به استخر جواب μ اضافه می‌شود و μ_{old} به سناریو جدید $\tilde{\mu}$ بروزرسانی می‌شود. در مقابل اگر مهاجم سناریو حمله تکرارهای قبل را مجدد تکرار کند، فرایند به x^* به عنوان سناریو جریان استوار علیه $\tilde{\mu}$ میل می‌کند.

مشخصا مقادیر هدف دو بازیکن به یک عدد همگرا می‌شود و می‌توان تایید کرد اگر مدافع جریان x^* را اجرا کند، حد پایین هدف مقداری خواهد بود که اهداف دو بازیکن همگرا می‌شود. نکته حائز اهمیت این است که مسئله بهینه‌سازی مدافع می‌تواند تعداد زیادی از جواب با مقدار هدف بهینه داشته باشد که اهداف دو بازیکن همگراست و برای اجتناب از این حالت، زمانی که حد بالا و پایین بازی همگرا می‌شود فرایند را پایان می‌دهیم. به بیان دیگر اگر مسائل بهینه سازی بازیکنان به صورت زیربهینه حل شود، ممکن است حد بالا و پایین بازی همگرا نشود اگرچه بازیکنان استراتژی‌های گذشته‌شان را تکرار نمایند.

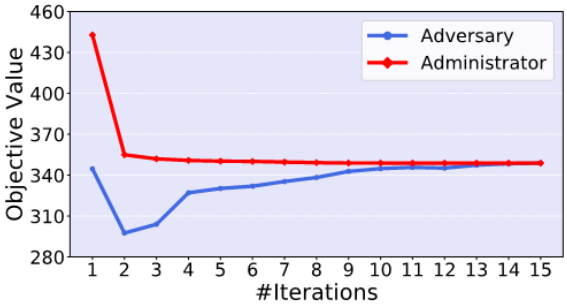
جدول۵: جدول عایدی مدافع و مهاجم در تکرارهای بازی

تکرار	مقدار جریان شبکه(X)	سناریو حمله(μ)	V^L	V^U
قبل از شروع	–	–	۰	∞
اول تا قبل از توقف الگوریتم	x	ψ	پاسخ تابع هدف مهاجم	پاسخ تابع هدف مدافع
آخر	x^*	$\tilde{\mu}$	V^U	V^L

۴-۱ حل مدل در مقیاس‌های کوچک و بزرگ

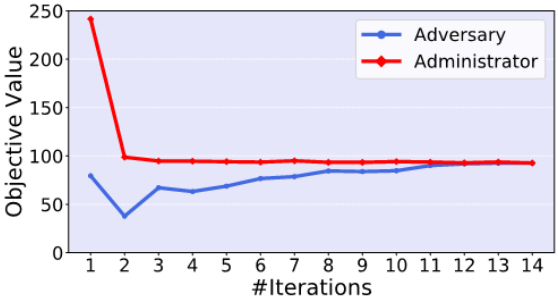
به عنوان یک مسئله موردی، داده‌های مربوط به یک شبکه جمل‌ونقل محدود را درنظر می‌گیریم. در شکل زیر همگرایی بازی تکرارشونده پیشنهادی ما برای مسئله فوق که شامل ۳۵ نقطه(گره) توزیع بار با ظرفیت فعال ۰٫۴(چهل درصد) با بودجه ۵(حداکثر بروز اختلال در پنج خط ارتباطی) در نظر گرفته شده است. محور افقی(X) تعداد تکرار بازی و محور عمودی(Y) مقدار تابع هدف بازیکنان را نشان می‌دهد. همانطور که انتظار می‌رود، تابع هدف مالک شبکه(مدافع/رهبر) با گذشت تکرارهای متوالی بطور یکنواخت کاهش می‌یابد و همانطور که پاسخ‌ها همگرا می‌شوند، توانایی مهاجم(پیرو) در ایجاد اختلال در جریان شبکه نیز کاهش می‌یابد. تابع هدف پس از ۱۵ تکرار بازی به عدد ۳۴۹ میل می‌کند

و می‌توان ادعا کرد که حداقل تابع هدف مورد انتظار مدافع برای هر سناریو حمله(Ψ) عدد ۳۴۹ خواهد بود.



شکل۵: حل مدل در مقیاس کوچک(Γ=5)

در مثالی دیگر مطابق شکل زیر، شبکه‌ای شامل ۲۰ نقطه(گره) توزیع بار با ظرفیت فعال۰,۸(هشتاد درصد) با بودجه ۱۰(حداکثر بروز اختلال در ده خط ارتباطی) در نظر گرفته شده است که پس از ۱۴ تکرار بازی، همگرا می‌شود. با توجه به نتایج حاصل از آزمایش ما با تغییر پارامترهای فوق، در کلیه مسائل مشابه با تکرار حداکثر ۲۰دور بازی میان بازیکنان، توابع هدف به یک مقدار همگرا می‌گردند و بازی به تعادل می‌رسد.



شکل۶: حل مدل در مقیاس کوچک(Γ=10)

برای حل مدل در مقیاس واقعی از راه حل ابتکاری تشریح شده در شکل۴ بهره می‌گیریم، همچنین تعریف سه واژه ذیل و بررسی عملکرد راه حل پیشنهادی ما براساس این مفاهیم حائز اهمیت است:

۱. راه حل حداکثر جریان[۱](MF): در این روش، فرض می‌کنیم مدافع از هیچ حمله‌ای خبر ندارد و حداکثر جریان را از طریق شبکه انتقال می‌دهد.

۲. طرح‌ریزی یک مرحله‌ای[۲](OSP): در این بازی یک مرحله‌ای، مدافع ابتدا حداکثر جریان را محاسبه کرده و پس از آن مهاجم حمله بهینه را صورت می‌دهد تا حداکثر جریان را مختل کند. سرانجام مدافع جریان بهینه را برای شبکه آسیب دیده از حمله مهاجم اتخاذ می‌کند.

[۱] Max-Flow solution
[۲] One Step Planning

۳. راه حل جریان استوار(RF): در این روش، یک جریان استوار را محاسبه می‌کنیم که در آن فرض می‌شود کل جریان خطوط آسیب دیده از دست رفته است. (Bertsimas et al 2013) یک مدل بهینه‌سازی برای محاسبه جریان استوار در شرایطی که حداکثر جریان ورودی دچار اختلال و شکست می‌گردد، ارائه داده است و ما با تغییر این مدل بهینه‌سازی به حالتی که حداکثر خطوط شبکه مورد حمله قرار می‌گیرد، از آن استفاده کرده‌ایم.

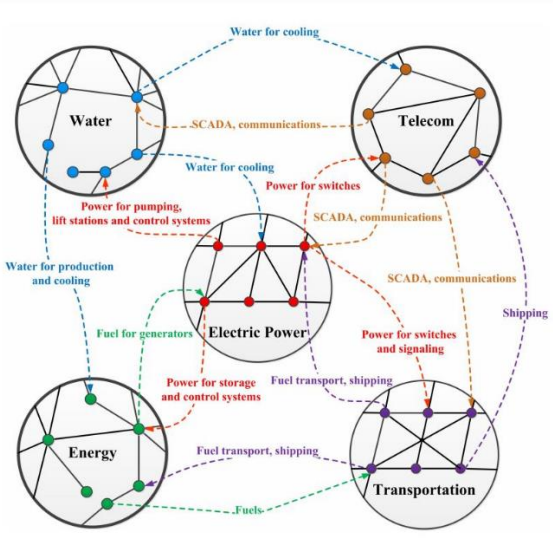
جدول۶: مصداق‌های بروز اختلالات آبشاری در شبکه‌های زیرساختی

مشخصه‌های شبکه				راه حل		
شماره نمونه	تعداد گره	ظرفیت یال	بودجه(Γ)	MF	OSP	RF
۱	۱۴	۲۲	۲	۱۸۲۸	۱۶۰۲	۱۷۹۶
۲	۱۷	۳۱	۳	۲۸۷۱۱	۵۰۰۰	۱۲۰۰۰
۳	۱۶۳	۳۹۹	۵	۴۵۱۲	۴۱۴۲	۴۵۱۲
۴	۳۹	۸۰	۵	۴۵۰۷	۳۵۴۵	۴۳۱۴
۵	۱۲	۵۰	۵	۳۶۵۷	۱۱۵۵	۳۶۲۶
۶	۱۳	۵۴	۵	۳۰۱۳	۱۳۶۱	۲۷۵۰
۷	۱۳	۴۹	۵	۴۶۵۳	۱۸۶۹	۴۳۷۷
۸	۲۷	۶۰	۵	۴۵۰۲	۲۹۱۲	۴۲۳۶
۹	۲۴	۴۸	۵	۴۶۳۳	۳۸۴۰	۴۴۶۷
۱۰	۵۲	۱۰۹	۵	۴۳۳۸	۳۹۸۹	۴۱۴۸
۱۱	۴۱	۱۸۹	۵	۴۷۱۰	۱۴۸۸	۴۴۴۷
۱۲	۳۷	۹۷	۵	۴۴۸۹	۳۴۲۱	۴۲۹۰
۱۳	۱۴	۲۶	۳	۲۶۹۵	۱۹۰۸	۲۶۷۲
۱۴	۲۹	۶۴	۵	۴۱۰۰	۲۳۲۱	۳۸۱۷
۱۵	۱۳	۴۱	۵	۴۲۸۳	۱۴۲۲	۴۰۳۹
۱۶	۴۲	۱۰۶	۵	۴۲۸۳	۱۴۲۲	۴۰۳۹
۱۷	۲۹	۱۱۵	۵	۴۵۵۲	۲۹۱۸	۴۳۲۴
۱۸	۲۶	۶۶	۵	۴۵۵۲	۲۹۱۸	۴۳۲۴
۱۹	۶۷	۱۳۸	۵	۳۸۴۶۴	۱۵۷۷۶	۲۵۲۰۰
۲۰	۵۶	۱۰۸	۵	۴۷۸۶	۴۳۷۸	۴۶۷۱

[1]Robust Flow solution

۵– بحث و نتیجه‌گیری

زیرساخت‌های مهم که اقتصاد و امنیت ملی را تهدید می‌کنند از قبیل سیستم‌های توزیع نیروی برق، توزیع آب و حمل‌ونقل، بیش از پیش به یکدیگر وابسته شده‌اند. اگرچه این سیستم‌ها پیشرفت‌های بی سابقه‌ای در زمینه‌های انعطاف پذیری و کارایی داشته‌اند، شکست در یک شبکه به علت روابط وابستگی متقابل آن‌ها منجر به گسترش و تاثیر در عملکرد شبکه‌های وابسته آن می‌گردد. شکست‌های آبشاری یکی از این پدیده‌هاست که که شکست‌های چشمگیری را به زیرساخت‌های مهم وارد می‌کند. در جایی که یک اختلال کوچک اولیه می‌تواند منجر به شکست‌های پیچیده در وابسته‌های شبکه و نتیجتاً شکست و فروپاشی سراسر سیستم گردد. موضوع و چالش اصلی، درک و تقلیل دلایل اصلی شکست‌های آبشاری غیرمنتظره در ابعاد بزرگ از طریق توصیف و مدلسازی وابستگی‌های درونی بین شبکه‌های مختلف است.



شکل۷: مثالی از شبکه‌های زیرساختی وابسته در یک کشور

مدلسازی بازی‌های امنیتی در شبکه‌های وابسته، اهمیت رویکرد چندوجهی را که شامل اصول نظریه بازی‌ها، عدم قطعیت و همکاری ذینفعان است، برجسته می‌کند. همانطور که تهدیدها تکامل می‌یابند و شبکه‌ها به طور فزاینده‌ای به هم متصل می‌شوند، تحقیقات مداوم برای افزایش استحکام و انعطاف‌پذیری استراتژی‌های امنیتی ضروری است. با پرداختن به چالش‌ها و بررسی روش‌های جدید، این زمینه می‌تواند به طور قابل توجهی به بهبود امنیت در سیستم‌های پیچیده کمک کند.

در پژوهش (کریمی، حسن‌پور و مصدق‌خواه ۱۴۰۳) مشخص گردید مولفه‌های مدیریت منابع انسانی، اختلال طبیعی، آگاهی و اختلال اقتصادی بر مولفه‌های امنیت و اختلال عملیاتی تاثیر می‌گذارند. براساس نتایج حاصله، مشخص گردید مدیریت دانش و درک ساختارهای زنجیره تامین و منابع انسانی، بلوک‌های سازنده برای ایجاد یک زنجیره تامین تاب‌آور هستند. از این رو، زنجیره تامین تاب‌آور با پرورش مدیریت دانش در مرحله پیش از اختلال از طریق اقداماتی مانند آموزش و تمرین، ایجاد فرهنگ مدیریت ریسک زنجیره تامین و زنجیره تأمین تاب‌آور و اقدامات زنجیره تامین و شبیه سازی بهبود می‌یابد.

همچنین پژوهش(ابراهیم‌پور و فرجود چوکامی ۱۴۰۲) اهمیت شاخص استواری زنجیره تأمین را طبق نظر خبرگان پژوهش نشان می‌دهد. از جمله پیشنهادها برای مدیران در این زمینه میتوان تمرکز بیشتر بر روی استوار ساختن زنجیره تأمین برای افزایش تاب‌آوری زنجیره تأمین و حفظ شرایط در زمان بروز اختلال با افزایش قابلیت دید و افزونگی در زنجیره تأمین اشاره کرد.

با مشاهده اختلالات شبکه از دریچه بازی‌های امنیتی، تحلیلگران می‌توانند اثرات آبشاری حملات یا خرابی‌ها در سیستم‌های به هم پیوسته را بهتر درک و پیش‌بینی کنند. این مدل را می توان در حوزه های مختلفی از جمله سرورهای ابری توزیع شده، شبکه های داده و سیستم های انرژی هوشمند اعمال کرد. با مطالعه ساختار شبکه‌ها درمی‌یابیم که مدتهاست بررسی‌ها و تحلیل‌های موجود بر شبکه‌های منفرد یا ایزوله که با شبکه‌های دیگر ارتباط ندارد، متمرکز شده است. با این حال، براساس شواهد و واقعیت‌های موجود در شبکه‌های کنونی، این شرایط به ندرت در زندگی و جامعه ما اتفاق می‌افتد. زیرساخت‌های مدرن به طور قابل توجهی وابسته به یکدیگر هستند و تحلیل سیستم با شبکه‌های وابسته را پیچیده‌تر می‌کنند. ویژگی اساسی شبکه‌های وابسته این است که اختلال در یک شبکه می‌تواند به یک شبکه مکمل دیگر در آن سیستم سرایت نماید و تا خرابی بین شبکه خراب اولیه و شبکه‌های مکمل آن بطور رفت و برگشتی ادامه یابد و موجب فراگیر شدن اختلالات آبشاری در سراسر شبکه شود که این نوع از اختلال منجر به خسارات بسیار شدید خواهد شد. لذا مطالعه روابط میان شبکه های وابسته و مدلسازی دقیق ساختار این شبکه‌ها، منجر به کاهش آسیب‌پذیری زیرساخت‌های اساسی خواهد شد.

درک آسیب‌پذیری‌ها و علت اصلی بروز غیرمنتظره اختلالات آبشاری در مقیاس بزرگ از طریق توصیف دقیق و الگوبرداری ذاتی بین و در داخل اجزای مختلف شبکه میسر است و نیازمند مطالعات توپولوژی شبکه است. در واقعیت، شبکه‌هایی با عملکرد مشابه غالباً برای ساختن یک ساختار مشترک برای استواری بهتر و ریسک کمتر با یکدیگر همراه می‌شوند، به عنوان مثال شبکه‌های توزیع برق مناطق مختلف ممکن است با هم همراه باشند یا موسسات مالی مشابه ممکن است برای ریسک کمتر با هم در ارتباط باشند. بنابراین دستیابی به یک شبکه استوار در زمان بروز اختلال در زیرساخت‌های حیاتی از اهداف مهم و ضروری مدلسازی شبکه‌های وابسته می‌باشد که در این تحقیق در صدد دستیابی به این مهم هستیم.

از زمینه‌های کاربردی این تحقیق، درنظرگرفتن وابستگی میان شبکه‌های مختلف زیرساختی می‌باشد که ماهیت غیرقابل انکار شبکه‌های امروزی است. همچنین وقوع اختلالات احتمالی در این شبکه‌ها که در دنیای واقعی بسیار محتمل است و منجر به تاثیر در شبکه‌های وابسته و مکمل می‌گردد، بررسی شده است. علاوه بر این، درک و کاهش اثرات مخرب اختلالات آبشاری و طراحی استوار شبکه‌های مکمل که نیاز بسیار مهم در راستای بقای شبکه‌ها در دنیای کنونی است، مدنظر قرار گرفته است.

نتایج این تحقیق مورد استفاده در شبکه‌های زیرساختی و مهم نظیر نظام بانکی و مالی کشور می‌باشد که در آن سیستم‌های اطلاعاتی وابسته در برابر اختلالات ناشی از حملات سایبری بسیار آسیب‌پذیرند. لذا طراحی استوار این شبکه اطلاعاتی که متشکل از چند شبکه وابسته بهم است و درک و تقلیل آسیب‌پذیری این شبکه‌ها بسیار حائز اهمیت است. بروز اختلالات آبشاری در شبکه و انتشار اختلالات را بررسی می‌کنیم که این اختلالات آبشاری ممکن است تا فروپاشی کامل شبکه پیش رود و به دنبال تشخیص و تقلیل اثرات ناشی از این گونه اختلالات و فعال ماندن شبکه هستیم. حملات سایبری مثالی معروف از بروز اختلال در این گونه شبکه‌هاست که با طراحی استوار شبکه مربوطه درصدد مقابله با اثرات مخرب حملات هستیم و با استفاده از تئوری بازی‌ها و طراحی یک بازی میان مهاجم و مدافع در هنگام بروز حملات به مدلسازی این شبکه‌ها می‌پردازیم و پارامترهای غیرقطعی را وارد مدل می‌کنیم و از مفاهیم بازی‌های امنیتی و بکارگیری انواع آن در این شبکه بخصوص بازی‌های آبشاری به جهت نزدیکی به ماهیت این تحقیق بهره می‌گیریم. مدلسازی و تحلیل استواری شبکه‌های وابسته در برابر اختلالات آبشاری از طریق تعیین مشخصه‌های دقیق وابستگی اجزای شبکه صورت می‌گیرد که بررسی و درک علت ریشه‌ای این اختلالات در مقیاس بزرگ و در شرایط تصادفی بسیار حائز اهمیت است. علاوه بر این، بدست آوردن اندازه سیستم نهایی بعنوان تابعی از اندازه حملات اولیه و اندازه حمله بحرانی که منجر به فروپاشی کامل شبکه می‌شود و تعیین توزیع بار بهینه که استواری را بیشینه می‌کند، بسیار ارزشمند و ضروریست.

جدول۷: مصداق‌های بروز اختلالات آبشاری در شبکه‌های زیرساختی

ردیف	شبکه زیرساختی مورد مطالعه	منبع
۱	شبکه‌های انتقال قدرت	(Cadini et al 2024)
۲	شبکه‌های کامپیوتری	(Li et al 2024)
۳	شبکه‌های مالی و اقتصادی	(Ramirez et al 2023)
۴	شبکه‌های ارتباطی	(Ren et al 2018)
۵	شبکه‌های توزیع آب	(Yao and Fan. 2023)
۶	شبکه‌های حمل‌ونقل	(Sun et al 2024)

همچنین در مسیرهای آینده این تحقیق، علاقه فزاینده‌ای به ادغام تکنیک‌های یادگیری ماشین و هوش مصنوعی با مدل‌های بازی امنیتی برای افزایش قابلیت‌های پیش‌بینی و تطبیق استراتژی‌ها براساس داده‌های زمان واقعی وجود دارد و تحقیقات آینده می‌تواند بر توسعه معیارهایی برای تعیین کمیت انعطاف‌پذیری شبکه‌های وابسته به یکدیگر تمرکز کند که امکان ارزیابی بهتر اثربخشی استراتژی‌های امنیتی را فراهم می‌کند.

در پژوهش (صادقی و مزروعی ۱۴۰۴) برای اولین بار چالش‌های هم‌رقابتی را در زنجیره تأمین بررسی کرده است و با توجه به لزوم بکارگیری هم‌رقابتی در زنجیره تأمین(برای رفع کمبود در منابع و تخصیص)، می‌تواند برای تهیه نقشه راهی برای مقابله با چالش‌های احتمالی، مفید واقع شود. همچنین، تشویق به همکاری میان ذینفعان برای به اشتراک گذاشتن اطلاعات در مورد آسیب‌پذیری‌ها و تهدیدات، می‌تواند وضعیت امنیتی کلی شبکه‌های وابسته را افزایش دهد. استفاده از بینش‌های حوزه‌های مختلف مانند اقتصاد، جامعه‌شناسی و مهندسی برای غنی‌سازی فرآیند مدل‌سازی و درک رفتار انسان، انگیزه‌های اقتصادی و محدودیت‌های فنی می‌تواند به مدل‌های جامع‌تری منجر شود.

منابع

ابراهیم پور، مصطفی، و زینب فرجود چوکامی. ۱۴۰۲. "شناسایی و رتبه بندی شاخص‌های تاب‌آوری زنجیره‌تأمین در ابعاد چهارگانه با استفاده از روش سوآرا در صنعت مواد غذایی." فصلنامه بهبود مدیریت ۱۷(۲): ۵۹-۳۳.

کریمی، امیرمسعود، حسینعلی حسن‌پور، و مسعود مصدق خواه. ۱۴۰۳. "ارائه الگوی تحلیل اختلالات و تاب‌آوری زنجیره تامین مواد غذایی." فصلنامه بهبود مدیریت ۱۸(۲): ۷۳-۴۸.

صادقی آرانی، زهرا، و اسماعیل مزروعی نصرآبادی. ۱۴۰۴. "شناسایی و مدل‌سازی چالش‌های هم‌رقابتی در زنجیره تأمین بهداشت و درمان: رویکرد مدل‌سازی ساختاری-تفسیری فراگیر فازی." فصلنامه بهبود مدیریت ۱۹(۱): ۵۹-۳۶.

Almoghathawi, Yasser, Andrés D. González, and Kash Barker. "Exploring recovery strategies for optimal interdependent infrastructure network resilience." *Networks and Spatial Economics* 21 (2021): 229-260.

Benchekroun, Hassan, and N. V. Long. "Game theory: Static and dynamic games." *Research tools in natural resource and environmental economics* (2011): 89-140.

Bertsimas, Dimitris, Ebrahim Nasrabadi, and Sebastian Stiller. "Robust and adaptive network flows." Operations Research 61, no. 5 (2013): 1218-1242.

Brocas, Isabelle, Juan D. Carrillo, and Ashish Sachdeva. "The path to equilibrium in sequential and simultaneous games: A mousetracking study." *Journal of Economic Theory* 178 (2018): 246-274.

Cadini, Francesco, Luca Lomazzi, and Enrico Zio. "Vulnerability Analysis of Power Transmission Grids Subject to Cascading Failures." Electronics 13, no. 5 (2024): 943.

Casey, William, Steven E. Massey, and Bud Mishra. "How signalling games explain mimicry at many levels: from viral epidemiology to human sociology." *Journal of the Royal Society Interface* 18, no. 175 (2021): 20200689.

Chen, Juntao, Corinne Touati, and Quanyan Zhu. "A dynamic game approach to designing secure interdependent IoT-enabled infrastructure network." *IEEE Transactions on Network Science and Engineering* 8, no. 3 (2021): 2601-2612.

Cunningham, James D., and Conrad S. Tucker. "Mitigating adversarial cascades in large graph environments." *Expert Systems with Applications* 258 (2024): 125243.
De Soto, Borja García, Alexandru Georgescu, Bharadwaj Mantha, Ziga Turk, Abel Maciel, and Muammer Semih Sonkor. "Construction cybersecurity and critical infrastructure protection: new horizons for Construction 4.0." *J. Inf. Technol. Constr.* 27 (2022): 571-594.
Etesami, S. Rasoul, and Tamer Başar. "Dynamic games in cyber-physical security: An overview." *Dynamic Games and Applications* 2019, no. 4 (Etesami and Başar): 884-913.
Fox, William P. "Teaching the applications of optimisation in game theory's zero sum and non-zero sum games." *International Journal of Data Analysis Techniques and Strategies* 2, no. 3 (2010): 258-284.
Gerardi, Dino. "Unmediated communication in games with complete and incomplete information." *Journal of Economic Theory* 114, no. 1 (2004): 104-131.
Gudmundsson, Jens, Jens Leth Hougaard, and Jay Sethuraman. "Managing cascading disruptions through optimal liability assignment." *arXiv preprint arXiv:2408.07361* (2024).
Ho, Edwin, Arvind Rajagopalan, Alex Skvortsov, Sanjeev Arulampalam, and Mahendra Piraveenan. "Game Theory in defence applications: A review." *Sensors* 22, no. 3 (2022): 1032.
Huang, Yan, Yi Joy Li, and Zhipeng Cai. "Security and privacy in metaverse: A comprehensive survey." *Big Data Mining and Analytics* 6, no. 2 (2023): 234-247.
Hunt, Kyle, and Jun Zhuang. "A review of attacker-defender games: Current state and paths forward." *European Journal of Operational Research* 313, no. 2 (2024): 401-417.
Lehto, Martti. "Cyber-attacks against critical infrastructure." In *Cyber security: Critical infrastructure protection*, pp. 3-42. Cham: Springer International Publishing, 2022.
Li, Haitao, Lixin Ji, Yingle Li, and Shuxin Liu. "Robustness Analysis of Multilayer Infrastructure Networks Based on Incomplete Information Stackelberg Game: Considering Cascading Failures." *Entropy* 26, no. 11 (2024): 976.
Li, Qiyuan, Yumeng Wang, Donghai Tian, Chong Yuan, and Changzhen Hu. "Component-based modeling of cascading failure propagation in directed dual-weight software networks." Computer Networks 255 (2024): 110861.
Mirzaei-Nodoushan, Fahimeh, Omid Bozorg-Haddad, and Hugo A. Loáiciga. "Evaluation of cooperative and non-cooperative game theoretic approaches for water allocation of transboundary rivers." *Scientific Reports* 12, no. 1 (2022): 3991.
Mühlhofer, Evelyn, Elco E. Koks, Chahan M. Kropf, Giovanni Sansavini, and David N. Bresch. "A generalized natural hazard risk modelling framework for infrastructure failure cascades." *Reliability Engineering & System Safety* 234 (2023): 109194.
Pan, Shouzheng, Hai Yan, Jia He, and Zhengbing He. "Vulnerability and resilience of transportation systems: A recent literature review." *Physica A: Statistical Mechanics and its Applications* 581 (2021): 126235.
Pandey, Prabhat, and Meenu Mishra Pandey. *Research methodology tools and techniques*. Bridge Center, 2021.
Ramirez, Stefanny, Marcelle Van Den Hoven, and Dario Bauso. "A stochastic model for cascading failures in financial networks." IEEE Transactions on Control of Network Systems 10, no. 4 (2023): 1950-1961.
Rao, Nageswara SV, Chris YT Ma, and Fei He. "Game-theoretic strategies for cyber-physical infrastructures under component disruptions." *IEEE Transactions on Reliability* 72, no. 2 (2022): 483-497.
Ren, Wendi, Jiajing Wu, Xi Zhang, Rong Lai, and Liang Chen. "A stochastic model of cascading failure dynamics in communication networks." IEEE Transactions on Circuits and Systems II: Express Briefs 65, no. 5 (2018): 632-636.
Shen, Yi, Huang Yang, Gang Ren, and Bin Ran. "Model cascading overload failure and dynamic vulnerability analysis of facility network of metro station." *Reliability Engineering & System Safety* 242 (2024): 109711.
Sun, Jingran, Kyle Bathgate, Shidong Pan, and Zhanmin Zhang. "Network-based method for assessing multi-modal transportation network vulnerability to cascading failures." Sustainability Analytics and Modeling 4 (2024): 100034.

Sun, Wenjuan, Paolo Bocchini, and Brian D. Davison. "Overview of interdependency models of critical infrastructure for resilience assessment." *Natural Hazards Review* 23, no. 1 (2022): 04021058.
Vatenmacher, Michael, Tal Svoray, Michael Tsesarsky, and Shabtai Isaac. "Performance-driven vulnerability analysis of infrastructure systems." *International Journal of Disaster Risk Reduction* 76 (2022): 103031.
Wang, Gang, Yuechao Chao, Yong Cao, Tieliu Jiang, Wei Han, and Zeshao Chen. "A comprehensive review of research works based on evolutionary game theory for sustainable energy development." *Energy Reports* 8 (2022): 114-136.
Wu, Gongyu, Meiyan Li, and Zhaojun Steven Li. "A stochastic modeling approach for cascading failures in cyberphysical power systems." *IEEE Systems Journal* 16, no. 1 (2021): 723-734.
Yang, Qihui, Caterina M. Scoglio, and Don M. Gruenbacher. "Robustness of supply chain networks against underload cascading failures." *Physica A: Statistical Mechanics and its Applications* 563 (2021): 125466.
Yang, Ya-Ting, and Quanyan Zhu. "Game-Theoretic Foundations for Cyber Resilience Against Deceptive Information Attacks in Intelligent Transportation Systems." *arXiv preprint arXiv:2412.04627* (2024).
Yao, Chen, and Bo Fan. "Spatiotemporal Vulnerability Analysis of Large-Scale Infrastructure Systems under Cascading Failures: Case of Water Distribution Networks." Journal of Infrastructure Systems 29, no. 2 (2023): 04023008.
Zhang, Xi, Dong Liu, Haicheng Tu, and Chi Kong Tse. "An integrated modeling framework for cascading failure study and robustness assessment of cyber-coupled power grids." *Reliability Engineering & System Safety* 226 (2022): 108654.
Zhu, Quanyan, and Tamer Basar. "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems." *IEEE Control Systems Magazine* 35, no. 1 (2015): 46-65.
Zhu, Yuan, Kaan Ozbay, Hong Yang, Fan Zuo, and Di Sha. "Modeling and simulation of cascading failures in transportation systems during hurricane evacuations." *Journal of advanced transportation* 2021, no. 1 (2021): 5599073.