فصلنامه علمی مطالعات مدیریت راهبردی دفاع ملی
سال ششم، شماره ۲۱، بهار ۱۴۰۱، صفحات ۷۴-۳۳

مقاله پژوهشی:

مروری نظام‌مند بر کاربرد رویکرد بازی امنیتی در حفاظت راهبردی دارایی‌ها

زهره سادات گتمیری[۱]، مرتضی خاکزار بفروئی[۲]، علیرضا آخوندی[۳]

تاریخ دریافت:۱۴۰۰/۰۳/۲۳ **تاریخ پذیرش:۱۴۰۰/۰۸/۰۷**

چکیده

طی دو دهه اخیر، به‌ویژه پس از وقوع حوادث ۱۱ سپتامبر ۲۰۰۱، حوزه تحقیقاتی بازی امنیتی در مرکز توجه محققین قرار گرفته و انتشار تولیدات علمی در این زمینه، از رشد صعودی چشمگیری برخوردار بوده است. تحقیق حاضر، با هدف بررسی وضعیت و ترسیم نقشه تولیدات علمی در حوزه بازی امنیتی، به‌ویژه در حوزه موضوعی مهندسی، به‌منظور ایجاد بینش نسبت به این حوزه موضوعی برای انجام تحقیقات توسعه‌ای و جدید انجام شده است. جامعه آماری پژوهش، مقالات علمی منتشر شده به زبان انگلیسی در پایگاه داده علمی اسکوپوس بوده است. در این تحقیق، برای اولین بار در زمینه مرور نظام‌مند ادبیات بازی امنیتی، از رویکرد تحلیل کتاب‌شناختی استفاده شده و به‌همین‌منظور، نرم‌افزارهای Bibexcel و Gephi به‌کار گرفته شده است. نتایج تحلیل موضوعی شبکه هم-استنادی مراجع پُر استناد نشان می‌دهد که مسئله تخصیص بهینه منابع دفاعی به زیر ساخت‌ها و امنیت اطلاعات و ارتباطات، به ترتیب، حوزه‌های موضوعی اصلی است که در مقالات مورد بررسی، به آنها پرداخته شده است. این امر حاکی از آن است که در حال حاضر، با توجه به گستره وسیع انواع دارایی‌های راهبردی در معرض انواع مختلف تهدیدها، ظرفیت زیادی برای پرداختن به موضوع بازی امنیتی در حوزه مهندسی وجود دارد. در انتها نیز، با بررسی محتوایی مقالات خوشه اول، پیشنهادهایی برای تحقیقات آینده در مسئله تخصیص بهینه منابع دفاعی با رویکرد بازی امنیتی در حوزه موضوعی مهندسی ارائه شده است.

کلید واژه‌ها: بازی امنیتی، تخصیص بهینه منابع دفاعی، تحلیل کتاب‌شناختی، اسکوپوس.

---

۱ .پژوهشگر گروه پژوهشی مهندسی صنایع، پژوهشکده توسعه تکنولوژی جهاد دانشگاهی (ACECR)، تهران، ایران (نویسنده مسئول، رایانامه: z.gatmiry@gmail.com

۲ . دانشیار، عضو هیئت علمی گروه مهندسی صنایع دانشگاه علم و فرهنگ، تهران، ایران.

۳ . استادیار، عضو هیئت علمی گروه پژوهشی مهندسی صنایع، پژوهشکده توسعه تکنولوژی جهاد دانشگاهی (ACECR)، تهران، ایران.

مقدمه

حفاظت از دارایی‌ها در مقابل تهدیدها، همواره جزء اولویت‌های اول صاحبان آنها بوده است. در سطح ملی نیز حفظ امنیت منابع و زیر ساخت‌های ملی، اعم از نظام‌های فیزیکی و سایبر–فیزیکی در مقابل انواع تهدیدها، به‌ویژه تهدیدهای راهبردی تبلور می‌یابد، یک دغدغه اساسی برای کشورها به‌شمار می‌آید (رحالگو و همکاران، ۱۳۹۹). چگونگی بهترین دفاع از دارایی‌ها در مقابل حملات هوشمندانه، به‌ویژه پس از حوادث ۱۱ سپتامبر ۲۰۰۱ در آمریکا، در مرکز توجه محققین قرار گرفته است (بیر، کاکس، عزیز[۱] ۲۰۰۹). مدافع لازم است بداند که چگونه از دارایی‌هایش حفاظت کند و چگونه منابع خود را بین این دارایی‌ها به‌صورت بهینه توزیع کند (باساک[۲] و همکاران، ۲۰۱۶). در میان رویکردهای مختلف معرفی شده برای پرداختن به این مسئله، تئوری بازی، به‌عنوان یک رویکرد مناسب برای پاسخ به این دو سؤال مورد استفاده قرار گرفته است (جین، آن و تمب[۳] ۲۰۱۳). تئوری بازی، از اجتماع ریاضیات و منطق ایجاد شده و بر این اصل اساسی استوار است که بازیکنان به‌دنبال حداکثر سازی سود و حداقل‌سازی زیان خود هستند (عبادی زاده، ۱۳۹۸). الگوهای بازی که در کاربردهای امنیتی مورد استفاده قرار می‌گیرند، بازی‌های امنیتی[۴] نامیده می‌شوند. در رویکرد بازی امنیتی، مدافع و مهاجم، دو بازیکن هستند که مدافع به‌دنبال تخصیص منابع محدود خود به دارایی‌های (اهداف) کلیدی به‌منظور دفاع از آنهاست. مهاجم نیز در جستجوی یافتن هدف مناسب برای حمله است (ویلچینسکی، یاکوبیک و کوشودزیه[۵] ۲۰۱۶).

تمرکز محققین بر روی بازی امنیتی، منجر به رشد صعودی انتشارات علمی به‌ویژه در دو دهه اخیر شده است. این امر، پایش مستمر و تحلیل روند انتشارات در این زمینه، برای ایجاد بینش نسبت به ابعاد مختلف آن و جهت‌گیری برای تحقیقات آتی را ضروری می‌سازد. از سوی دیگر، با وجود گسترش رویکرد استفاده از فنون کتاب‌شناختی[۶] در تحلیل

---

۱. Bier, Cox, & Azaiez
۲. Basak
۳. Jain, An, & Tambe
۴. Security Games
۵. Wilczyński, Jakóbik, & Kołodziej
۶. Bibliometrics

و ترسیم نقشه انتشارات علمی در حوزه‌های مختلف، تاکنون از این روش‌ها در مرور ادبیات بازی امنیتی استفاده نشده است. در موارد اندکی، کارهای خوبی در زمینه مرور ادبیات حوزه‌هایی از بازی امنیتی، مانند کارهای سندلر و آرک[1] در سال ۲۰۰۳ و هاسکن و لویتین[2] در سال ۲۰۱۲، انجام شده است که می‌توان با تحلیل آنها مسیر تحقیقات آتی در آن حوزه‌ها را شناسایی کرد. سندلر و آرک در سال ۲۰۰۳، به‌منظور مروری بر چگونگی به‌کارگیری تئوری بازی در ادبیات تروریسم، به بررسی اجمالی ادبیات پرداخته و ضمن معرفی کاربردهای نو، به معرفی خطوط راهنما برای تحقیقات آتی در این زمینه پرداختند(سندلر و آرک، ۲۰۰۳). هاسکن و لویتین نیز در سال ۲۰۱۲، به مرور ادبیات الگوهای نظام‌های دفاع و حمله پرداختند (هاسکن و لویتین، ۲۰۱۲). آنها ۱۲۹ مقاله در این حوزه را بر اساس ساختار نظام، مقیاس‌های دفاعی و تاکتیک‌ها و شرایط حمله، دسته‌بندی کردند تا ضمن ایجاد دیدگاه کلی نسبت به این حوزه، حوزه‌های تحقیقاتی آتی را به محققین پیشنهاد دهند.

در مقاله حاضر، با به‌کارگیری فنون و ابزارهای کتاب‌شناختی، به استخراج نقشه ساختار ادبیات بازی امنیتی بر روی مقالات منتشر شده در پایگاه داده اسکوپوس[3] یکی از معتبرترین و جامع‌ترین پایگاه‌های داده‌های علمی، پرداخته شده است. این کار با هدف ایجاد بینش نسبت به موضوع تحقیقاتی بازی امنیتی بر اساس آخرین انتشارات، به‌ویژه در حوزه مهندسی، معرفی مجموعه مقالات حاوی دانش، مفاهیم، ابزار و فنون پایه در دسته‌های مختلف موضوعی و فراهم آوردن زمینه‌ای برای شناسایی زمینه‌های جدید تحقیق آتی در حوزه موضوعی مهندسی صورت گرفته است. برای دستیابی به این اهداف، نویسندگان، مجله‌ها و مقالات پر استناد، به‌عنوان واحدهای اصلی انتخاب شدند تا با تحلیل بر روی آنها به کمک رویکرد تحلیل کتاب‌شناختی، به سؤالات اصلی، که در ادامه آمده است، پاسخ داده شود. (۱) نویسندگان کلیدی در حوزه تحقیقاتی مورد بررسی چه کسانی هستند ؟ (۲) با توجه به شبکه هم–نویسندگی نویسندگان، ساختار همکاری بین نویسندگان

۱. Sandler & Arce
۲. Hausken & Levitin
۳. Scopus

به چه شکل است؟ آیا همکاری لازم بین نویسندگان کلیدی برای انتشار مقالات اثرگذار در حوزه تحقیقاتی مورد بررسی شکل گرفته است؟ (۳) وضعیت توزیع مقالات جامعه آماری، در مجله‌ها به چه صورت است و مجله‌های کلیدی مشارکت کننده در انتشار مقالات کدامند؟ با توجه به شبکه هم-استنادی مقالات پر استناد، حوزه‌های تحقیقاتی اصلی مورد تمرکز در مجموعه مقالات مورد بررسی کدامند؟ (۴) ظرفیت‌های تحقیقاتی آتی بازی امنیتی در حوزه موضوعی مهندسی کدامند؟

ساختار ادامه مقاله به این ترتیب است که در بخش دوم، مبانی نظری و پیشینه تحقیق آورده شده است. در بخش سوم، روش‌شناسی تحقیق معرفی شده و توضیح مختصری درباره جامعه آماری ارائه شده است. در بخش چهارم، ضمن ارائه نتایج تحلیل کتاب‌شناختی، ظرفیت‌های تحقیقات آتی معرفی شده و در آخر، جمع بندی صورت گرفته است.

مبانی نظری و پیشینه تحقیق

ادبیات نظری حوزه بازی امنیتی

تئوری بازی، علم تصمیم‌گیری در شرایط تعاملی بر پایه علم ریاضی است. دیدگاه بنیادی تئوری بازی، به‌کارگیری منطق بازی برای الگو کردن زندگی واقعی است که در آن، بازیکنان در مقابل راهبردهای یکدیگر به رقابت می‌پردازند (فاروقی و نیازی، ۲۰۱۶). بر این اساس، هر بازی، با چهار مؤلفه اصلی تعیین می‌شود: تصمیم‌گیرندگان (بازیکنان)، گزینه‌ها (راهبردها)یی که انتخاب می‌کنند، اهدافشان در انتخاب یک راهبرد و آنچه که درباره ساختار یک تعامل می‌دانند. هدف یک بازیکن، انتخاب یک راهبرد است که بیشترین مطلوبیت یا عایدی ممکن برایش حاصل شود (فوجی وارا-گرو[1] ۲۰۱۵).

یک دسته‌بندی از الگوهای تئوری بازی، تقسیم آنها به بازی‌های همکارانه و غیر همکارانه[2] است. تئوری بازی، میان موقعیت‌هایی که در آن تصمیم‌گیرنده، به‌صورت مستقل

۱. Fujiwara-Greve
۲. cooperative and non-cooperative games

از سایر تصمیم‌گیرندگان اقدام می‌کند و موقعیت‌هایی که چندین تصمیم‌گیرنده، به‌صورت یک گروه می‌توانند فعالیت کنند تمایز قائل می‌شود. دلیل این تمایز، وجود تفاوت قابل توجه در تصمیمات و اقدامات حاصله است. در بازی غیر همکارانه، تصمیم‌گیرندگان نمی‌توانند توافقی الزام‌آور مبنی بر اجبار طرف مقابل به انجام برخی اقدامات را ایجاد کنند اما این امکان در بازی همکارانه وجود دارد. هدف تئوری بازی غیر همکارانه، این است که دریابد وقتی افراد، تصمیمات مستقل و راهبردی می‌گیرند، در یک جامعه چه اتفاقی می‌افتد. اما هدف تئوری بازی همکارانه، تعیین میزان عایدی افراد در ائتلاف‌های مختلف است که به‌منظور بهبود رفاه جمعی ایجاد شده‌اند. به‌طور معمول، در ادبیات، از بازی‌های غیر همکارانه با عنوان بازی تعارض نیز یاد می‌شود (فوجی وارا-گرو، ۲۰۱۵؛ فاروقی و نیازی[۱] ۲۰۱۶). الگوهای بازی غیر همکارانه که در کاربردهای امنیتی مورد استفاده قرار می‌گیرند، بازی‌های امنیتی نامیده می‌شوند (تمب، ۲۰۱۲).

بازی‌های امنیتی، دسته خاصی از بازی‌ها هستند که به مطالعه تعاملات میان مدافعان و مهاجمان تخریب‌گر می‌پردازد. از تئوری بازی‌های امنیتی و راهکارهای آنها به‌عنوان مبنایی برای تصمیم‌گیری و توسعه الگوریتم و پیش‌بینی رفتار مهاجم استفاده می‌شود. بازی‌های امنیتی، بسته به نوع اطلاعات در دسترس تصمیم‌گیرندگان، فضای اقدام و اهداف تصمیم‌گیرندگان، می‌توانند فرمول ساده قطعی یا فرمول تصادفی پیچیده با اطلاعات محدود داشته باشند (منشائی[۲] و همکاران، ۲۰۱۳). اما مسائل در حوزه بازی امنیتی، عموماً بر مبنای الگوهای استکلبرگ الگوسازی شده‌اند. بازی استکلبرگ[۳] که یک برنامه ریاضی دوسطحی است، از نوع بازی با قدرت نامتقارن است که یک بازیکن، رهبر و سایر بازیکنان، به‌عنوان پیرو هستند و به همین جهت، بازی رهبر-پیرو نیز نامیده می‌شوند. رهبر، اول حرکت می‌کند و با آگاهی از مجموعه اقدامات (یا سبد راهبردهای) پیروها، بهترین اقدام (یا راهبرد) خود را انتخاب می‌کند. سپس، پیروها به اقدام رهبر، عکس‌العمل منطقی نشان داده و بهترین اقدام (یا راهبرد) پاسخ را انتخاب می‌کنند (کازوران-آمیلبورو، ۲۰۱۷).

۱. Farooqui & Niazi
۲. Manshaei
۳. Stackelberg Game

ادبیات رسمی در موضوع تئوری بازی را می‌توان در آثار وون نیومن و مورگنسترن[1] و با انتشار کتاب آنها در سال ۱۹۴۴ با عنوان «تئوری بازی و رفتار اقتصادی» (نیومن و مورگنسترن، ۱۹۴۴) جستجو کرد. هنگام انتشار، این کتاب مورد استقبال و توجه فراوان محققین قرار گرفت (زاگار[2] ۲۰۱۹). از دهه ۱۹۴۰ تاکنون، تئوری بازی هم در زمینه تعداد نتایج تئوریک و هم به لحاظ قلمرو و تنوع کاربردها رشد بی وقفه‌ای را تجربه کرده است. به‌ویژه، نیمه دوم قرن بیستم، دوران طلایی تئوری بازی بوده و انتشارات و رویدادهای مختلفی، تئوری بازی و کاربردهای آن را پوشش می‌دهند که تعداد آنها سال به سال رو به افزایش قابل توجه است (باسار[3]، ۲۰۱۲). اهداء چندین جایزه نوبل برای کار بر روی تئوری بازی، که اولین آنها در سال ۱۹۹۴ به جان هارسانی[4] و همکارانش به پاس تحلیل پیشگامانه آنها در زمینه تعادل در تئوری بازی‌های غیر همکارانه اختصاص یافت، نشان از حیات پر نشاط این حوزه دانشی دارد. آخرین جایزه نوبل اقتصادی نیز در سال ۲۰۲۰ به دو متخصص تئوری بازی، پائول میلگرام و رابرت ویلسون[5] برای ابداع قالب‌های جدید حراج اهدا شده است (پایگاه جوایز نوبل، بی تا).

اندکی پس از انتشار کتاب نیومن و همکارش، کاربردها، توسعه‌ها، اصلاحات و الگوهای مبتنی بر تئوری بازی در ادبیات مطالعات امنیتی بروز و ظهور پیدا کرد. از آن زمان، ادبیات رشد فزاینده‌ای یافت و اثر آن بر حوزه مطالعات امنیتی قابل توجه بوده است. به‌طوری‌که به اذعان محققین، بدون شک، اکنون مطالعات مبتنی بر تئوری بازی بخشی از ادبیات مطالعات امنیتی هستند. از جمله موضوعات مطالعات امنیتی که به شدت تحت تأثیر استدلال‌های مبتنی بر تئوری بازی قرار گرفته‌اند می‌توان به آغاز و شدت درگیری و جنگ بین ایالتی، پیامدهای اتحادها و الگوهای هم‌ترازی، اثربخشی نظام‌های دفاع موشکی، تاثیر سیاست داخلی بر درگیری‌های بین دولتی، پویایی مسابقات تسلیحاتی و عملکرد کنترل تسلیحات، گسترش تروریسم، پیامدهای دموکراسی بر دیپلماسی قهری، مشخصات چانه

---

۱. Von Neumann and Morgenstern
۲. Zagare
۳. Basar
۴. John Harsanyi
۵. Paul Milgrom and Robert Wilson

زنی بحران و عملیات سیاست‌های توازن قوا اشاره کرد. در این میان، در حوزه مطالعات امنیتی، مطالعات بازدارندگی، بیشترین تأثیر را از تئوری بازی گرفته است.

شاید به‌علت شدت جنگ سرد در آمریکا در اوایل دهه ۱۹۵۰ میلادی، تقریبا همه کاربردهای اولیه تئوری بازی در زمینه مطالعات امنیتی، درگیری‌های بین ایالتی را به‌عنوان بازی‌های مجموع صفر تجزیه و تحلیل کرده است. یک بازی مجموع صفر[1] بازی است که در آن، منافع طرفین در تضاد کامل باشد. به‌عنوان نمونه‌هایی از این نوع مطالعات، می‌توان به تحلیل نبردهای جنگ جهانی دوم توسط الیور هیوود[2] در سال ۱۹۵۴ و مطالعه راهبرد نظامی توسط مک دونالد و توکی[3] در سال ۱۹۴۹ اشاره کرد (زاگار، ۲۰۱۹). در مطالعات انجام شده توسط سرهنگ الیور هیوود، اهمیت تئوری بازی در تصمیم‌گیری فرماندهی نشان داده شده است. او در بررسی نبردهای مختلفی از جنگ جهانی دوم مبتنی بر رویکرد تئوری بازی نشان داد که تصمیم دکترین نظامی، مشابه با جواب به‌دست آمده از نظریه بازی است. ارزیابی‌های وی منجر به تشویق انجمن تحقیق در عملیات به استفاده بیشتر از تئوری بازی در تصمیم‌گیری‌های نظامی شد. امروزه نقش تئوری بازی در بازی‌های جنگی، کشف قوانین حاکم بر بازی نظامی و استفاده از آنها در پیش‌بینی نتیجه جنگ پر رنگ است. بازی‌های نظامی، به‌منظور آزمون سناریوهایی که نمی‌توان در صحنه واقعی جنگ مورد آزمون عملی قرار داد طراحی می‌شوند (خاتمی و انوشه، ۱۳۹۸). اقدامات کاربردی در زمینه‌های امنیت شبکه‌های کامپیوتری، تروریسم، سناریوهای دزد و پلیس و بازی مذاکرات هسته‌ای حاکی از استفاده گسترده از تئوری بازی در مسائل نظامی و امنیتی در دهه اخیر است(بیگدلی و طیبی ۱۳۹۶). بنابراین، با توجه به اهمیت بیش از پیش موضوع امنیت و به‌کارگیری گسترده تئوری بازی در حل مسائل این حوزه، پژوهش حاضر، پیرامون مرور ادبیات نظام‌مند در حوزه موضوعی مهندسی انجام شده است.

---

[1] zero-sum games
[2] A.G. Haywood
[3] McDonald and Tukey

ادبیات نظری حوزه مرور ادبیات نظام‌مند

مرور ادبیات نظام‌مند، صرفاً مروری بر مطالعات قبلی نیست و خود یک تلاش تحقیقاتی به‌شمار می‌آید. مرور ادبیات نظام‌مند شیوه شناسایی، ارزیابی و تفسیر همه تحقیقات موجود مرتبط به یک سؤال تحقیق، حوزه موضوعی یا پدیده مورد علاقه مشخص است. در واقع، در مرور ادبیات نظام‌مند، مطالعات موجود شناسایی می‌شود، نوآوری‌های آنها انتخاب و ارزیابی می‌شود، داده‌ها تحلیل و ترکیب می‌شود و شواهد به‌گونه‌ای گزارش می‌شود که نتیجه‌گیری معقول و روشن نسبت به آنچه که هست و آنچه که نامعلوم و ناشناخته است به دست آید (توماس، فیلیپ اسکاوردا و خوزه اسکاوردا، ۲۰۱۶). همه مطالعاتی که در مرور نظام‌مند شرکت داده می‌شوند، «مطالعات اولیه» و مرور نظام‌مند، یک «مطالعه ثانویه» نامیده می‌شوند. گام‌های اصلی مرور نظام‌مند عبارتند از: تعریف سؤالات تحقیق و پروتکل مرور، جستجوی مطالعات اولیه، غربال اطلاعات اولیه بر مبنای معیارهای ورود و خروج از پیش تعریف شده، استخراج داده‌ها با استفاده از طرح طبقه‌بندی و فرم جمع‌آوری داده و آمایش داده‌ها و ارائه نتایج.

در حالت ایده‌آل، فرایند مذکور به‌صورت متوالی انجام می‌شود اما در عمل، اغلب، با عمیق‌تر شدن درک محقق نسبت به موضوع، لازم است که به عقب برگشته و گام‌های قبلی به‌روز رسانی شوند (اکسلسون[1] ۲۰۱۹).

پیشینه تحقیق

در بحث مرور ادبیات کاربرد تئوری بازی در حوزه مهندسی، سوریانو[2](۲۰۰۳)، با مرور کلی ادبیات، به گردآوری کاربردهای تئوری بازی در حل مسائل مختلف مهندسی در سه حوزه عمران، صنایع و برق و الکترونیک پرداخته است. وی به مرور جامع ادبیات نپرداخته و با بررسی فقط تعدادی از انتشارات در این سه حوزه موضوعی، برخی از آخرین پیشرفت‌ها در این حوزه‌ها را معرفی کرده است. در تحقیق انجام شده توسط اکسلسون

1 Axelsson
2 Sanchez-Soriano

(۲۰۱۹) با هدف شناسایی کاربردهای تئوری بازی در مهندسی نظام نظام‌ها (SOS)[1] به مرور نظام‌مند ادبیات پرداخته شده است. نظام نظام‌ها به موقعیت‌هایی اشاره دارد که در آن، نظام‌هایی که هر کدام به‌طور مستقل عمل کرده و مدیریت می‌شوند، به‌منظور دستیابی به اهدافی که به‌صورت انفرادی قابل حصول نیست با هم همکاری می‌کنند. اما اکسلسون فقط به بررسی محتوای تعداد محدودی از مقالات انتخابی برای استخراج کاربردهای تئوری بازی در این حوزه موضوعی اکتفا کرده و به ارائه چند دسته‌بندی از کاربردها بسنده کرده است. گریگوریان و کالینز[2] (۲۰۲۱)، کاربرد الگوهای تئوری بازی در حوزه مهندسی نظام‌ها را مرور کردند. به‌همین‌منظور، محتوای مقالات مجله‌های با محتوای تئوری بازی و مهندسی نظامات را بررسی کردند تا نوآوری‌های بالقوه تئوری بازی در حل مسائل مهندسی نظامات را شناسایی و معرفی کنند.

در حوزه موضوعی امنیت، منشایی و همکاران (۲۰۱۳)، به مرور ادبیات ساخت یافته و جامع در زمینه کاربرد تئوری بازی در پرداختن به اشکال مختلف مسائل فنی امنیت و حفظ حریم خصوصی در شبکه‌های رایانه‌ای و اپلیکشن‌های موبایلی از منظر اقتصادی پرداختند. به همین منظور، آنها در ابتدا مسائل امنیتی مورد بحث را استخراج کرده و سپس، رویکردهای مبتنی بر تئوری بازی که برای حل آنها به کار گرفته شده و نتایج اصلی مستخرج از آنها را خلاصه کرده است. در مرور ادبیات کلی انجام شده توسط وانگ و همکارانش (۲۰۱۷)، روش‌های مبتنی بر تئوری بازی برای حل مسائل حوزه امنیت سایبری، توصیف و جهت‌گیری برای تحقیقات آتی در این زمینه، از دو منظر ریاضی و امنیتی ارائه شده است. وجه تمایز کار آنها با مرور ادبیات انجام شده توسط منشایی و همکارانش (۲۰۱۳) و لیانگ و شیائو[3] (۲۰۱۳) در زمینه کاربرد تئوری بازی در حل مسائل امنیت شبکه این است که مطالعاتش محدود به شبکه‌های ارتباطی رایانه‌ای نبوده و همه اشکال فضای سایبری را در برگرفته است. همچنین، روش‌ها از هر دو جنبه تئوری ریاضی و کاربرد امنیتی بررسی شده است. مروری بر کاربردهای تئوری بازی در مدیریت حوادث

۱. systems-of-systems engineering
۲. Grigoryan & Collins
۳. Liang & Xiao

طبیعی (سیبرگ، دوین و ژوانگ[1] ۲۰۱۷) و مروری بر بازی‌ها و الگوریتم‌های تخصیص منابع در حل مسائل امنیت عمومی (چنگ چنگ و جیانگ وی[2] ۲۰۲۰) نیز از جمله مطالعات مروری غیر نظام‌مند در حوزه موضوعی کاربرد تئوری بازی در حل مسائل امنیتی به‌شمار می‌روند.

روش‌شناسی تحقیق

پژوهش حاضر، مرور ادبیات نظام‌مند با استفاده از فنون و ابزارهای تحلیل کتاب‌شناختی انجام شده است. تحلیل کتاب‌شناختی، اغلب برای ارزیابی تحقیقات علمی از طریق مطالعات کمّی بر روی انتشارات تحقیقاتی به‌کار گرفته می‌شود. تحلیل‌های کتاب‌شناختی، مبتنی بر این فرض است که کشفیات علمی و نتایج تحقیقاتی در نهایت، در مجله‌های علمی بین‌المللی منتشر می‌شوند تا سایر محققان بتوانند آنها را بخوانند و به آنها استناد کنند. به کمک تحلیل‌های کتاب‌شناختی می‌توان شاخصه‌هایی از کمّیت و عملکرد تحقیقات و سنجه‌هایی از ارتباطات بین محققان و حوزه‌های تحقیقاتی را به‌دست آورد (کاتارینا[3] و همکاران، ۲۰۱۴).

ترسیم نقشه علم[4] یکی از موضوعات تحقیقاتی مهم در حوزه مطالعات کتاب‌شناختی است که به‌دنبال یافتن و ارائه نمایشی فضایی از ارتباطات میان اجزای یک نظام دانش علمی با ماهیت پویا و متغیر است. در ترسیم نقشه علم، تمرکز بر روی دیده‌بانی یک زمینه علمی و تعیین حدود حوزه‌های تحقیقاتی آن است. بازیابی و پیش‌پردازش داده، استخراج، ترسیم، تحلیل و تجسم دادن به شبکه، گام‌های اصلی جریان کار ترسیم نقشه علم هستند(کوبو[5] و همکاران، ۲۰۱۱).

رایج‌ترین راه جمع‌آوری داده برای تحلیل کتاب‌شناختی، بازیابی داده از پایگاه‌های داده موجود است. در حال حاضر، پایگاه‌های داده اطلاعات کتاب‌شناختی برخط مختلفی وجود دارد که مستندات علمی و استنادات آنها، در این پایگاه‌ها ذخیره می‌شوند. بی شک، پایگاه

---

۱. Seaberg, Devine & Zhaung
۲. Chengcheng & Xiagwei
۳. Catharina
۴. Science mapping
۵. Cobo

داده علمی اسکوپوس، یکی از مهم‌ترین این پایگاه‌های داده است (کارتارینا و همکاران، ۲۰۱۴). پایگاه داده اسکوپوس، با بیش از ۲۵۰۰۰ مجله علمی از بیش از ۵۰۰۰ منتشرکننده بین‌المللی، رشته‌های مختلفی از جمله مهندسی را پوشش می‌دهد (الزویر[1]، ۲۰۲۰). در این مقاله، داده‌ها، از پایگاه داده علمی اسکوپوس بازیابی شده‌اند. با جستجو در «عنوان، خلاصه، کلمات کلیدی» منابع پایگاه داده‌های علمی اسکوپوس و محدود کردن جستجو به مقالات علمی به زبان انگلیسی، ۱۹۱۸ مقاله در حوزه بازی امنیتی، جمع‌آوری و در فرمت RIS ذخیره‌سازی شدند. داده‌های ذخیره‌سازی شده، در گام پیش‌پردازش، به‌عنوان ورودی نرم‌افزار Bibexcel استفاده شده است. در این گام، کیفیت واحدهای تحلیل (عمدتاً نویسندگان و کلمات) به کمک ابزارهای نرم افزاری مختلف مانند Bibexcel بهبود می‌یابند تا در تحلیل نقشه علم، نتایج بهتری حاصل شود (کوبو و همکاران، ۲۰۱۱).

بر اساس دسته‌بندی موضوعی اسکوپوس، ۱۰ حوزه موضوعی برتر مجموعه مقالات بازیابی شده از نظر فراوانی، در جدول شماره ۱ نشان داده شده است. همانطور که در این جدول قابل مشاهده است، ۲۷٫۶٪ از مقالات (۵۳۰ مقاله) در حوزه موضوعی مهندسی تألیف شده است و پس از حوزه موضوعی علوم کامپیوتر، در رده دوم قرار گرفته است. این مقاله‌های در حوزه موضوعی مهندسی، از سال ۱۹۸۴ به چاپ رسیده است. پس از حوادث ۱۱ سپتامبر در سال ۲۰۰۱، که سرآغاز انجام اقدامات مهم و خطیر در مقابل اقدامات تروریستی شناخته می‌شود (کلانتری، ۱۳۹۸)، موضوع بازی امنیتی در مرکز توجه محققان قرار گرفت و به‌دنبال آن، تعداد انتشارات علمی در این زمینه، روند صعودی پیدا کرد که این روند رشد، در انتشارات حوزه موضوعی مهندسی نیز قابل مشاهده است.

۱. Elsevier

جدول شماره ۱: حوزه موضوعی برتر مجموعه مقالات بازیابی شده

حوزه موضوعی	درصد فراوانی
علوم کامپیوتر	۴۱,۴٪
مهندسی	۲۷,۶٪
علوم اجتماعی	۲۷,۲٪
ریاضیات	۱۴,۶٪
اقتصاد و مالی	۱۱,۶٪
مدیریت کسب و کار و حسابداری	۸,۶٪
علم تصمیم‌گیری	۷,۸٪
پزشکی	۵,۴٪
محیط زیست	۵,۳٪
هنر و علوم انسانی	۴,۷٪

بر مبنای واحد تحلیل انتخابی، رویکردهای مختلفی برای استخراج شبکه وجود دارد. نویسندگان، مجله‌ها و مقالات استناد شده، معمول‌ترین واحدهای تحلیل در ترسیم نقشه علم هستند (کوبو و همکاران، ۲۰۱۱) که در این مقاله نیز، به‌عنوان واحدهای تحلیل انتخاب شده‌اند. نتایج تحلیل این واحدها، زمینه‌ای برای شناسایی افراد، مجله‌ها و مقالات کلیدی در حوزه تحقیقاتی مورد مطالعه فراهم خواهد کرد. از دو رویکرد تحلیل هم- نویسندگی و تحلیل هم-استنادی، برای استخراج شبکه استفاده شده است. تحلیل هم-نویسندگی، به‌منظور بررسی شبکه همکاری میان نویسندگان ۵۳۰ مقاله در حوزه موضوعی مهندسی انجام شده است. تحلیل هم ـ استنادی نیز، با استفاده از اطلاعات هم ـ استنادی ۱۴۹۹۸ منبع مورد ارجاع در فهرست مراجع این مقالات و با هدف شناسایی خوشه‌های اصلی موضوعی و ظرفیت‌های تحقیقاتی آتی بازی امنیتی در حوزه مهندسی انجام شده است.

برای ترسیم شبکه هم- استنادی استخراج شده نیز، یکی از الگوریتم‌های فن خوشه‌بندی بیشینه‌سازی[1] با نام ForceAtlas2 به‌کار گرفته شده است. استخراج، ترسیم و تجسم دادن به شبکه با به‌کارگیری ابزار تحلیل شبکه Gephi انجام شده است. برای استخراج دانش مفید از شبکه ساخته شده، تحلیل‌های مختلفی می‌تواند انجام شود. یکی از

۱. modularity maximization

مهم‌ترین این تحلیل‌ها، تحلیل شبکه است که در این مقاله به‌کار گرفته شده است. در تحلیل شبکه، با انجام تحلیل آماری بر روی شبکه ایجاد شده، سنجه‌های مختلفی مثل تعداد گره‌ها، تعداد مؤلفه‌های با اتصال ضعیف، چگالی گراف و سنجه‌های کمّی و کیفی خوشه‌ها را می‌توان اندازه‌گیری کرده و بر مبنای مقادیر این سنجه‌ها، شبکه را تفسیر کرد (کوبو و همکاران، ۲۰۱۱).

تجزیه و تحلیل داده‌ها و یافته‌های تحقیق

الف: یافته های تحقیق

تحلیل مشارکت نویسندگان

۱۰ نویسنده برتر، از حیث فراوانی تعداد مقالات منتشر شده در جدول شماره ۲ آورده شده است. همان‌طور که در جدول شماره نیز قابل مشاهده است، رتبه این نویسندگان، از نظر شاخص تعداد انتشارات و شاخص جایگاه در فهرست نویسندگان مقالات، لزوماً یکسان نیستند؛ به‌عنوان مثال، بیر، وی. ام.[۱] از نظر تعداد مقالات منتشر شده، در رتبه دهم قرار دارد؛ ولی از نظر جایگاه در فهرست نویسندگان، در رتبه دوم قرار دارد؛ این بدین‌معنی است که در اغلب مقالات، او جزء اولین نویسندگان مقاله است. رتبه ژوانگ، جی.[۲] و زونگ، دبلیو.[۳] هم از نظر تعداد انتشارات و هم از نظر جایگاه در فهرست نویسندگان یکسان هستند و از این حیث، به ترتیب در جایگاه اول و سوم قرار دارند. البته ایفاء نقش موثر نویسندگان، علاوه بر تعداد انتشارات، به کیفیت مقالات منتشر شده نیز وابسته است که در بخش تحلیل شبکه مشخص شده است که اغلب این نویسندگان، از جمله ژوانگ، جی.، جزء نویسندگان مقالات با مقدار شاخص کیفی بالا در حوزه موضوعی مورد مطالعه بوده‌اند.

۱. Bier, V.M.
۲. Zhuang, J.
۳. Zhong, W.

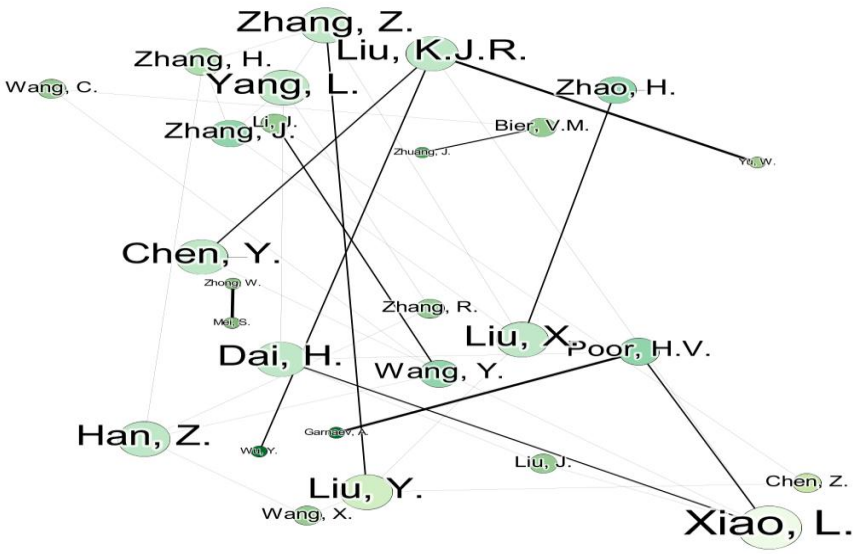
جدول شماره ۲: ۱۰نویسنده برتر از حیث تعداد مقالات منتشره

نویسندگان	جایگاه در فهرست نویسندگان	تعداد مقالات منتشر شده
ژوانگ. جی.	۴,۵	۹
لیو. وای[1]	۲,۴۴۸	۸
زونگ. دبلیو.	۲,۴۹۸	۷
لی. جی[2]	۱,۸۱۷	۷
وانگ، وای.	۲,۰۳۳	۷
لیو، کی. جی. آر[3]	۲,۳۳۳	۷
شیائو، ال.[4]	۱,۳۱۷	۶
پور، اچ. وی[5]	۱,۶۴۹	۶
هان، زد.[6]	۱,۵۹۳	۶
بیر، وی. ام.	۳,۱۶۶	۶

بررسی میزان مشارکت نویسندگان مقالات نشان داد که حدود ۱۵٪ از ۱۲۳۴ نویسنده، در تألیف بیش از یک مقاله مشارکت داشته‌اند. در شبکه هم-نویسندگی نویسندگانی که در تألیف حداقل ۴ مقاله مشارکت داشته‌اند (شکل شماره ۱)، هر گره، نماد یک نویسنده و هر یالِ متصل کننده دو گره، نمایانگر مشارکت دو نویسنده متناظر با دو گره در تألیف یک مقاله است. ضخامت هر یال، فراوانی مشارکت دو نویسنده و سایز هر گره، فراوانی همکاری نویسنده متناظر آن گره با سایر نویسندگان در تألیف مقالات را نشان می‌دهد. بر این اساس، مشاهده می‌شود که هر نویسنده، حداقل با یک نویسنده دیگر همکاری داشته است؛ اما نویسندگانی مانند ژوانگ. جی. که بیشترین مقالات بازی امنیتی در حوزه موضوعی مهندسی را تألیف کرده‌اند، همکاری پر رنگی با سایر نویسندگان دارای حداقل ۴ مقاله نداشته‌اند. بنابراین، تحلیل شبکه هم-نویسندگی نویسندگانی که در تألیف حداقل ۴ مقاله مشارکت داشته‌اند نیز نشان می‌دهد که تاکنون همکاری قوی بین نویسندگان شکل

۱. Liu, Y.
۲. Li, J.
۳. Liu, K.J.R
۴. Xiao, L.
۵. Poor, H.V.
۶. Han, Z.

نگرفته است و به‌نظر می‌رسد باید همکاری بیشتری بین محققان این حوزه تحقیقـاتی بـرای تألیف مقالات غنی و اثرگذار شکل بگیرد.



شکل شماره ۱: شبکه هم- نویسندگی نویسندگانی که در تألیف حداقل ۴ مقاله مشارکت داشته‌اند

وضعیت توزیع مقالات در مجله‌ها

بررسی آماری توزیع مقالات در مجله‌ها نشان می‌دهـد کـه ۲۲۸ مجلـه، در انتشـار ۵۳۰ مقاله مشارکت داشته‌اند. ۱۰ مجله برتر به شرح

جدول شماره ۳، ۱۲۹ مقاله (حدود ۲۵٪) از مجموع ۵۳۰ مقاله را به چاپ رسانده‌اند که حوزه موضوعی عمده این مجله‌ها، امنیـت اطلاعـات و ارتباطـات اسـت. همچنـین، مجلـه IEEE Transactions on Information Forensics and Security که بیشترین سـهم را در چـاپ مقالات دارد حدود ۳,۷۷٪ از کل مقالات را به چاپ رسـانده اسـت. همـه ۱۰ مجلـه برتـر، جزء مجلـه‌هـای معتبـر علمـی بـه‌شـمار مـی‌آینـد و اکثریـت آنهـا از درجـه تـأثیر[1] بـالایی برخوردارند. به‌نظر می‌رسد با توجه بـه گسـتره موضـوعی وسـیع مهندسـی و ماهیـت بـین رشته‌ای بازی امنیتی، سایر مجله‌های تخصصی و معتبر مهندسی می‌توانند نقـش فعـال‌تـری در انتشار مقالات این حوزه تحقیقاتی ایفاء کنند.

۱. impact factor

جدول شماره ۳: ۱۰ مجله برتر از حیث سهیم بودن در چاپ مقالات

نام علمی	تعداد مقالات چاپ شده
IEEE Transactions on Information Forensics and Security	۲۰
IEEE Transactions on Wireless Communications	۱۷
Risk Analysis	۱۷
IEEE Journal on Selected Areas in Communications	۱۵
Wireless Personal Communications	۱۴
Multimedia Tools and Applications	۱۱
Reliability Engineering and System Safety	۹
IEEE Communications Magazine	۹
International Journal of Distributed Sensor Networks	۹
International Journal of Information Security	۸

ب: تجزیه و تحلیل یافته ها

تحلیل شبکه هم-استنادی

به‌منظور شناسایی حوزه‌های تحقیقاتی اصلی در مجموعه مقالات مورد تحقیق، از تحلیل هم-استنادی استفاده شده است. هم- استنادی دو مقاله، به مفهوم حضور همزمان آنها در فهرست مراجع یک منبع علمی می‌باشد. مقالاتی که تعداد هم- استنادی بیشتری داشته باشند، با احتمال بیشتری به حوزه موضوعی یکسان مرتبط هستند. از آنجا که دو مقاله پر استناد نسبت به دو مقاله کم استناد، با احتمال بیشتری در چندین فهرست مراجع، حضور همزمان دارند، تحلیل هم- استنادی، معمولا خوشه‌هایی شامل مقالات پر استناد تولید می‌کند (کاتارینا و همکاران، ۲۰۱۴).

برای انجام این تحلیل، ابتدا به کمک نرم‌افزار Bibexcel، کلیه ۱۴۹۹۸ مرجع از فهرست مراجع ۵۳۰ مقاله مورد بررسی، استخراج شده است. پس از پالایش و آماده‌سازی داده‌ها، بر روی منابع اثرگذارتر، یعنی منابعی که حداقل پنج بار مورد ارجاع قرار گرفته بودند، به

کمک نرم‌افزار Gephi، تحلیل هم- استنادی انجام گرفته است. شبکه هم استنادی حاصل شده، شبکه‌ای با ۳۵۲ گره و ۸۵۸ یال است که برای ایجاد الگوی قابل فهم از آن، از الگوریتم ForceAtlas2، یکی از الگوریتم‌های طرح‌بندی[1] پیش فرض نرم افزار Gephi استفاده شده است. این الگوریتم، یک نظام فیزیکی را به‌منظور ایجاد یک تصویر سه بعدی از آن، شبیه‌سازی می‌کند. گره‌ها یکدیگر را مانند ذرات باردار دفع می‌کنند در حالی که یال‌ها مانند کش، گره‌هایشان را جذب می‌کنند. این نیروهای جاذبه و دافعه، جابجایی همگرا به وضعیت تعادل را ایجاد می‌کنند. در این نقشه، جایگاه هر گره، وابسته به سایر گره‌ها می‌باشد. این فرایند، فقط به اتصال‌های بین گره‌ها بستگی دارد. وجه تمایز ForceAtlas2 با سایر انواع الگوریتم‌های طرح‌بندی در این است که علاوه بر فراهم آوردن امکان تفسیر بصری از ساختار شبکه، نمایشی ماژولار از ساختار نیز ارائه می‌دهد که به تفسیر داده‌ها بر اساس پیکربندی نهایی شبکه کمک می‌کند (ژاکومی[2] و همکاران، ۲۰۱۴).

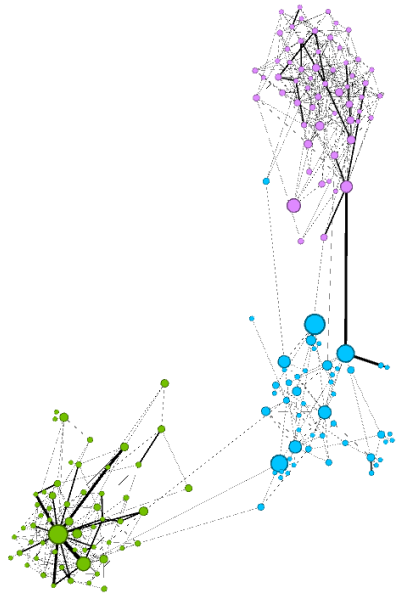
ماژول‌بندی شبکه حاصل به کمک ابزار ماژول‌بندی نرم‌افزار Gephi، این شبکه را به ۱۰ خوشه با شاخص ماژولاریتی ۰,۶۵ تقسیم بندی کرد که این مقدار ماژولاریتی، نشان‌دهنده ارتباط قوی بین گره‌های درون هر خوشه و ارتباط نسبتا قوی بین گره‌های خوشه‌های مختلف است. شاخص ماژولاریتی، عدد اسکالر بین ۱- و ۱+ است که تراکم اتصال‌های درون یک مجموعه از گره‌ها نسبت به اتصال‌های بین مجموعه‌ها را می‌سنجد. ابزار خوشه‌بندی در Gephi که بر پایه الگوریتم لووین[3] می‌باشد، تعداد بهینه خوشه‌ها، به گونه‌ای که شاخص ماژولاریتی بیشینه را به‌دست می‌دهد (فهیم نیا[4] و همکاران، ۲۰۱۵).

با توجه به اینکه هر یک از گره‌های این شبکه، حداقل ۵ بار مورد ارجاع قرار گرفته‌اند، در واقع، هر یک از خوشه‌ها، از گره‌هایی (مقالات) تشکیل شده‌اند که حاوی دانش، مفاهیم، نظریه‌ها، ابزار و یا فنون پایه در حوزه موضوعی مربوطه خود هستند.

---

۱. layout algorithm
۲. Jacomy
۳. Louvain
۴. Fahimnia

تعداد مقالات در هر خوشه متفاوت است. ۵۰٪ گره‌های (مقالات) شبکه، در سه خوشه اول، از حیث تعداد گره (مقاله)، قرار گرفته‌اند که نقشه آن در شکل شماره ۲ نشان داده شده است. بنابراین، این سه خوشه، در اولویت تحلیل هستند.



شکل شماره ۲: نقشه سه خوشه اول شبکه هم- استنادی

برای تعیین موضوع مورد تمرکز تحقیقاتی هر کدام از این سه خوشه، با الگو گرفتن از کار انجام شده توسط فهیم نیا و همکارانش (۲۰۱۵) ، محتوای ۵ مقاله دارای بیشترین تعداد هم- استنادی با مقالات پر استناد مورد بررسی قرار گرفت. در ادبیات کتاب‌شناختی، گفته می‌شود که این مقالات، از مقدار سنجه PageRank بالایی برخوردارند. در شبکه هم- استنادی، الگوریتم PageRank، تعداد دفعاتی که یک مقاله، با مقالات دیگر و با مقالات با هم- استنادی بالا، هم-استنادی داشته است را محاسبه می‌کند (فهیم نیا و همکاران، ۲۰۱۵). اطلاعات مربوط به این مقالات در جدول شماره ۴ آمده است.

جدول شماره ۴: پنج مقاله دارای بیشترین تعداد هم-استنادی با مقالات پر استناد در هر یک از سه خوشه اول

	نویسندگان، سال	عنوان مقاله	نام علمی
خوشه اول	نیکوفال و ژوانگ[۱] (۲۰۱۲)	تخصیص استوار بودجه دفاعی با در نظر گرفتن اطلاعات محرمانه مهاجم	Risk Analysis
	شان و ژوانگ[۲] (۲۰۱۳)	هزینه انصاف در تخصیص منابع امنیت ملی در مواجهه با دشمن راهبردی	Risk Analysis
	تالاریکو و همکاران[۳] (۲۰۱۵)	الگو تخصیص منابع امنیتی به شبکه حمل و نقل مواد شیمیایی چند-مُدی با تهدیدهای تطبیقی به کمک رویکرد تئوری بازی‌ها (MISTRAL)	Reliability Engineering and System Safety
	رنیرز[۴] (۲۰۱۲)	امنیت ترابری چند-مُدی مواد خطرناک: یافته‌های تجربی و تصمیمات آتی	Int. J. of Safety and Security Engineering
	هاسکن (۲۰۱۷)	دفاع و حمله اختصاصی و عمومی (از/به) اجزاء سری و موازی	Reliability Engineering and System Safety
خوشه دوم	موخرجی و همکاران[۵] (۲۰۱۴)	اصول امنیت لایه فیزیکی در شبکه‌های بیسیم چند کاربره: یک بررسی	IEEE Communications Surveys and Tutorials
	فکوریان و سویندلوهست[۶] (۲۰۱۳)	رقابت برای حفظ محرمانگی در کانال تداخلی MISO	IEEE Transactions on Signal Processing
	جیانگ و همکاران[۷] (۲۰۱۵)	انطباق نرخ محرمانگی در شبکه‌های حسگر بی‌سیم مبتنی بر بازی تکاملی	International Journal of Distributed Sensor Networks
	استانوژف و ینر[۸] (۲۰۱۳)	بهبود نرخ محرمانگی از طریق کاهش طیف برای جمینگ دوستانه	IEEE Transactions on Wireless Communications
	ژانگ و همکاران[۹]	تداخل امنیت PNY را برای شبکه‌های رادیو	IEEE Transactions on Information Forensics

۱. Nikoofal & Zhuang
۲. Shan & Zhuang
۳. Talarico et al.
۴. Reniers
۵. Mukherjee et al.
۶. Fakoorian & Swindlehurst
۷. Jiang et al.
۸. Stanojev & Yener
۹. Zhang et al.

	نویسندگان، سال	عنوان مقاله	نام علمی
	(۲۰۱۶)	شناختی بهبود می‌بخشد	and Security
خوشه سوم	وو و همکاران[1] (۲۰۱۲)	بازی‌های ضد جمینگ در شبکه‌های رادیو شناختی چند کاناله	IEEE J. on Selected Areas in Communications
	ترهو و همکاران[2] (۲۰۱۵)	یک بازی امنیتی استکلبرگ با راهبردهای تصادفی مبتنی رویکرد نظری خارج از مرز	Engineering Applications of Artificial Intelligence
	لی و همکاران[3](۲۰۱۵)	حملات جمینگ به تخمین وضعیت از راه دور در نظام‌های سایبری – فیزیکی: رویکرد تئوری بازی	IEEE Transactions on Automatic Control
	رحمان و همکاران[4] (۲۰۱۷)	تجمیع داده‌های ایمن و خصوصی برای زمانبندی مصرف انرژی در شبکه‌های هوشمند	IEEE Transactions on Dependable and Secure Computing
	تنگ و همکاران[5] (۲۰۱۳)	تشخیص هدف در شبکه‌های رادار بیستاتیک: تعیین گره و بازی امنیتی تکرار شونده	IEEE Transactions on Wireless Communications

بررسی محتوای مقالات خوشه‌ها نشان داد که حوزه موضوعی خوشه دوم و سوم، به‌طور عموم درباره تحلیل و بهبود امنیت اطلاعات و ارتباطات با رویکرد تئوری بازی می‌باشد. تمرکز اصلی مقالات خوشه اول نیز بر روی مسئله تخصیص بهینه منابع دفاعی با رویکرد الگوسازی مبتنی بر تئوری بازی است که به‌طور عمده، در حوزه امنیت ملی و امنیت زیرساخت‌ها مطرح شده است. زیر ساخت‌ها که به‌صورت بالقوه در مقابل حملات تروریستی یا سایر تهدیدهای هوشمند، در معرض آسیب قرار دارند، به‌طور عمده، شامل زیرساخت‌های شبکه‌ای (خطوط نفت و گاز طبیعی، شبکه‌های برق، تسهیلات و مسیرهای حمل و نقل، شبکه‌های ارتباط از دور، تامین آب و ...)، زیر ساخت‌های سازه‌ای (ساختمان‌های اداری، بیمارستان‌ها و ...)، زیر ساخت‌های اطلاعاتی (کنترل پرواز و ...) و زنجیره تأمین یا شبکه‌های تولید، پردازش و توزیع مواد غذایی می‌باشند (بیر، کاکس و عزیز، ۲۰۰۹). در ادبیات تئوری بازی، بازی امنیتی که برای

۱ Wu et al.
۲ Trejo et al.
۳ Li et al.
۴ Rahman et al.
۵ Tang et al.

الگوسازی مسئله حفاظت از اهداف زیر ساختی به کارمی‌رود، بازی امنیتی زیر ساخت[1] نامیده شده است (کار[2] و همکاران، ۲۰۱۸).

چالش اصلی در همه مسائل امنیتی، بهترین استفاده از منابع محدود برای ارتقاء امنیت، به‌ویژه در مواجهه با تهدیدهای تروریستی یا سایر تهدیدهای هوشمند است (باساک و همکاران، ۲۰۱۶). منابع محدود امنیتی باید به‌طور هوشمند و بر اساس اولویت‌های دارایی‌ها (اهداف) تخصیص داده شوند. اولویت‌بندی اهداف، بر اساس الزامات پوشش‌دهی امنیتی آنها، پاسخ‌های مهاجمان، عدم قطعیت‌ها در انواع مهاجمان و قابلیت‌ها، دانش و ترجیحات آنها تعیین می‌شوند. محققین رویکردهای مختلفی برای حل این مسئله داشته‌اند که از بین این رویکردها، بازی امنیتی به‌عنوان یک رویکرد مناسب به‌کار گرفته شده است(جین، آن و تمب، ۲۰۱۳). در جدول شماره ۵ توضیح مختصری از محتوای ۵ مقاله برتر خوشه اول که از بالاترین مقدار سنجه PageRank برخوردارند آورده شده است.

۱ Infrastructure Security Game (ISG)
۲ Kar

جدول شماره ۵: توصیف اجمالی از ۵ مقاله برتر خوشه اول

ردیف	عنوان مقاله	نویسندگان	علمی	نوع بازی					نوآوری
				نوع همکاری	جمعیت بازی کنندگان	افق زمانی	اطلاعات	دامنه تصمیم/عایدی	
۱	تخصیص استوار بودجه دفاعی با در نظر گرفتن اطلاعات محرمانه مهاجم	نیکوفال و ژوانگ (۲۰۱۲)	Risk Analysis	غیرهمکارانه	۲-نفره	همزمان و متوالی	ناکامل	پیوسته	الگوسازی عدم قطعیت در ارزشگذاری اهداف توسط دشمن با رویکرد تخصیص استوار منابع دفاعی
۲	هزینه انصاف در تخصیص منابع امنیتی در مواجهه با دشمن راهبردی	شان و ژوانگ (۲۰۱۳)	Risk Analysis	غیرهمکارانه	۲-نفره	متوالی	کامل	پیوسته	ایجاد موازنه بین انصاف و کارایی در تخصیص منابع امنیتی
۳	الگو تخصیص منابع امنیتی به شبکه حمل و نقل مواد شیمیایی چند-مُدی با تهدیدهای تطبیقی به کمک رویکرد تئوری بازی (MISTRAL)	تالاریکو و همکاران (۲۰۱۵)	Reliability Engineering and System Safety	غیرهمکارانه	۲-نفره	همزمان و متوالی	ناکامل	پیوسته	الگوسازی تصمیم راهبردی به کمک تئوری بازی و روش‌های مهندسی قابلیت اطمینان برای تخصیص بهینه اقدامات متقابل امنیتی به مسیرهای حمل و نقل با مُدهای متفاوت در زنجیره تأمین مواد خطرناک
۴	امنیت ترابری چند-قیدی مواد خطرناک: یافته‌های تجربی و تصمیمات آتی	رنیرز (۲۰۱۲)	Int. J. of Safety and Security Eng.	-	-	-	-	-	بررسی و معرفی روش‌ها و رویکردهای حل مسئله تخصیص منابع امنیتی به شبکه حمل و نقل مواد خطرناک
۵	دفاع و حمله اختصاصی و عمومی (از/به) اجزاء سری و موازی	هاسکن (۲۰۱۷)	Reliability Eng. and System Safety	غیرهمکارانه	۲-نفره	همزمان	کامل	پیوسته	تحلیل ۱۶ ترکیب مختلف از چگونگی تخصیص تلاش اختصاصی و عمومی توسط مدافع و مهاجم در نظام‌های سری و متوالی

در مقالات جدول شماره ۵، تمرکز اصلی بر روی بررسی همه جانبه مسئله تخصیص بهینه منابع دفاعی در مقابل دشمن راهبردی است. در ادبیات بازی امنیتی، دشمن هدف گرا[1] یا دشمن راهبردی، در مقابل دشمن فرصت‌طلب[2] مطرح می‌شود. دشمن فرصت‌طلب، هدف از پیش تعیین شده مشخصی ندارد و اقدام خود را بر اساس فرصت‌های به وجود آمده اتخاذ می‌کند (هاسکن، ۲۰۱۴). مهاجمان فرصت‌طلب، به جای برنامه‌ریزی راهبردی قبلی برای حملات، در جستجوی فرصت‌ها برای حمله هستند. آنها بازیکن با منطق محدود[3] به‌شمار می‌آیند و بر اساس پایش محدود[4] اقدام می‌کنند. به بیان دیگر، مهاجمان فرصت‌طلب، مشاهده محدودی از راهبرد دفاعی دارند و بنابراین، راهبرد حمله را بر مبنای اطلاعات و محاسبات محدود انتخاب می‌کنند که ممکن است به انتخاب راهبرد زیر-بهینه منجر شود (عباسی[5] ۲۰۱۶). مهاجم راهبردی، راهبرد بهینه حمله را بر مبنای سطوح دفاعی مشاهده شده اتخاذ می‌کند و بنابراین، تمایلی به حمله به اهداف با پوشش دفاعی بالاتر ندارد (هائو، جین و ژوانگ[6] ۲۰۰۹).

اهداف مورد دفاع، به‌طور عموم در سطح دفاع ملی و به‌طور اختصاصی از نوع زیر ساخت‌های شبکه‌ای می‌باشد. به‌طور عمده، الگوها توسعه یافته‌ی الگوهای پیشین و پایه است و سعی شده است که در الگوهای توسعه یافته، پارامترهای گوناگون، لحاظ شده و از ظرفیت انواع مختلف الگوهای تئوری بازی برای حل آنها استفاده شود. در همه این مقالات، الگوی طراحی شده، از نوع بازی غیر همکارانه است که البته با توجه به ماهیت مسئله، طبیعی است. یک بازی غیر همکارانه، وضعیت تعارض بین بازیکنان را الگوسازی می‌کند. در این وضعیت، بازیکنان، بدون تشکیل ائتلاف با سایر بازیکنان، به‌صورت مستقل تصمیم می‌گیرند (فوجی وارا-گرو، ۲۰۱۵). از نظر افق زمانی، هر دو نوع بازی ایستا و پویا و از

---

۱. Goal oriented
۲. Opportunistic attacker
۳. Bounded rationale
۴. Bounded surveillance
۵. Abbasi
۶. Hao, Jin, & Zhuang

نظر وجود اطلاعات نیز هر دو نوع بازی متقارن و غیر متقارن، در الگوسازی مسئله مورد بررسی قرار گرفته‌اند.

در بیشتر موارد، از فنون تحلیل ریسک و مهندسی قابلیت اطمینان نیز، به‌عنوان فنون اصلی، در الگوسازی و حل مسئله استفاده شده است. همانطور که ملاحظه می‌شود، اکثر این مقالات نیز در مجله‌های تخصصی ریسک و قابلیت اطمینان منتشر شده‌اند. نتایج جستجو در ادبیات نشان می‌دهد که محققان، در زمینه تحلیل امنیتی و مقابله با تروریسم توانسته‌اند به میزان قابل توجهی از ترکیب فنون مهندسی قابلیت اطمینان و تئوری بازی بهره ببرند (بیر، کاکس و عزیز، ۲۰۰۹؛ بریچا و نورالفتح[1] ۲۰۱۳؛ لینز و همکاران، ۲۰۱۳). تألیف‌ها تا سال ۲۰۱۲ در این زمینه، در مقاله هاسکن و لویتین (۲۰۱۲) مرور شده‌اند. در سال‌های اخیر، برخی کارهای مشابه دیگری در این زمینه به چاپ رسیده‌اند که در

جدول شماره ۶ آورده شده است. کاوناک و رابرسون[2] (۲۰۱۲)، به بررسی شرایط لازم برای وجود راهبرد تعادلی محض در الگوسازی دفاع از یک شبکه سری یا موازی در مقابل یک تهدید راهبردی پرداخته است. در الگوی طراحی شده توسط هاسکن (۲۰۱۳)، امکان تصمیم‌گیری بهینه در مورد انتخاب راهبرد دفاع تکی یا کلی از اجزاء یک شبکه سری، موازی و سری–موازی در مقابل یک تهدید راهبردی که ممکن است به یک جزء یا کل اجزاء شبکه حمله کند، فراهم شده است. لینز[3] و همکاران (۲۰۱۳)، تعامل بین یک مدافع و یک مهاجم راهبردی را طراحی کردند که اطلاعات ناکامل در خصوص ساختار نظام دارد. در این تعامل، مدافع، به‌دنبال طراحی بهینه ساختار یک نظام امنیتی به‌صورت سری –موازی و مهاجم، به‌دنبال حمله به یک زیر نظام مناسب با هدف بیشینه‌سازی خرابی در کل نظام است. آنها روش‌شناسی پیشنهادی خود را بر روی خطوط انتقال قدرت در جنوب برزیل که غالباً مورد هدف حمله مهاجمان قرار می‌گیرد به‌کار گرفتند. وانگ[4] و همکاران (۲۰۱۴)، چگونگی اثرگذاری راهبردهای دفاع و حمله بر قابلیت اطمینان نظام را در شرایطی که هر

---

۱. Bricha & Nourelfath
۲. Kovenock and Roberson
۳. Lins
۴. Wang

دو مدافع و مهاجم مقدار منابع ثابتی در اختیار دارند، بررسی کردند. مدافع از منابع خود فقط می‌تواند برای افزودن اجزاء استتار یا ارتقاء حفاظت سایبری اجزاء موجود استفاده کند. مهاجم نیز می‌تواند به زیرمجموعه‌ای از عناصر موجود حمله کند. آنها الگوریتمی پیشنهاد دادند که قابلیت ارائه راهبرد بهینه دفاعی را فراهم می آورد. مو[1] و همکاران (۲۰۱۵)، با توسعه الگوهای قبلی در خصوص راهبرد تخصیص بهینه منابع به حفاظت از اجزاء موجود یا ساخت اجزاء جدید، چارچوبی برای وارد کردن توزیع زمانی حملات عمدی در الگوی آسیب‌پذیری نظام فراهم کردند. رائو[2] و همکاران (۲۰۱۶)، از طریق فرموله کردن بازی بین یک متولی زیرساخت و یک مهاجم، به مطالعه نحوه حفاظت از زیرساخت‌های شامل تعدادی نظام به هم وابسته متشکل از اجزای گسسته که در معرض حملات سایبری یا فیزیکی قرار دارند، پرداختند. نتایج مطالعات تحلیل حساسیت، وابستگی تاب‌آوری زیرساخت به احتمال بقاء هر یک از نظام‌ها را اثبات کرد. هاسکن (a۲۰۱۷)، چگونگی حفاظت از یک نظام متشکل از دو جزء در دو حالت مستقل و وابسته و با ساختار سری و موازی در مقابل یک تهدید راهبردی را الگوسازی کرد. وی در مرحله بعد، الگوی خود را بر روی نظامی با ساختار پیچیده توسعه داد (هاسکن، ۲۰۱۹). نتایج تحلیل وی ثابت کرد که هر دو مدافع و مهاجم، تلاش خود را روی اجزایی از نظام متمرکز می‌کنند که وابستگی کمتری به سایر اجزاء نظام داشته باشند. وی، به کمک چارچوب پیشنهادی، نشان داد که چگونه وابستگی متقابل بین پالایشگاه‌های نفتی، استخراج نفت و گاز و حمل و نقل هوایی بر راهبردهای دفاع، حمله و مطلوبیت‌های مورد انتظار اثر می‌گذارد. گتمیری و همکاران (۲۰۲۱) نیز به بررسی چگونگی حفاظت پیشگیرانه از اکوسیستم های زیست محیطی در مقابل یک تهدید راهبردی پرداختند. آنها نشان دادند که چگونه منابع محدود دفاعی را باید به حفاظت از گونه‌های گیاهی و جانوری در یک اکوسیستم تخصیص داد به گونه‌ای که خطر حمله را برای مهاجم بالا ببرد تا حدی که مهاجم از حمله منصرف شود و یا در صورت حمله، حداقل خسارت ممکن به اکوسیستم وارد شود.

۱ Mo
۲ Rao

بررسی مقالات مذکور نشان داد که تمرکز اصلی این مطالعات، بر روی تخصیص بهینه منابع دفاعی به نظام‌های زیر ساختی در مقابل دشمنان راهبردی است. اغلب مسائل مذکور، به‌صورت یک برنامه‌ریزی ریاضی دو سطحی الگوسازی شده‌اند که در آن، مدافع در جستجوی بیشینه کردن بقاء نظام و مهاجم، در تلاش برای بیشینه کردن خرابی نظام می‌باشد. توابع عایدی به وسیله مفاهیم و فنون مهندسی قابلیت اطمینان نظام فرموله شده‌اند. بررسی قابلیت‌های کاربردی سایر فنون متنوع حوزه مهندسی در حل مسائل این حوزه نیز می‌تواند در فهرست تحقیقات آتی قرار گیرد.

جدول شماره ۶: ویژگی‌های مقالات اخیر منتشر شده که در آنها از ترکیب رویکرد بازی امنیتی و مفاهیم و فنون مهندسی قابلیت اطمینان برای الگوسازی استفاده شده است.

ردیف	نویسنده	نوع نظام		حوزه کاربرد
		پیکربندی (سری،موازی، سری-موازی، پیچیده)	وابستگی اجزا (مستقل، وابسته، چندحالته)	
۱	کاوناک و رابرسون(۲۰۱۲)	سری،موازی	مستقل	زیر ساخت
۲	هاسکن (۲۰۱۳)	سری،موازی، سری-موازی	مستقل	زیر ساخت
۳	لینز و همکاران (۲۰۱۳)	سری-موازی	مستقل	زیر ساخت
۴	وانگ و همکاران (۲۰۱۴)	پیچیده	مستقل	زیر ساخت
۵	مو و همکاران(۲۰۱۵)	موازی	مستقل	زیر ساخت
۶	رائو و همکاران (۲۰۱۶)	پیچیده	وابسته	زیر ساخت
۷	بن[1]و عزیز (۲۰۱۷)	-	-	مفهوم سازی (استفاده از مفهوم دسترس‌پذیری به جای قابلیت اطمینان در تابع بقاء)
۸	هاسکن (a۱۰۱۷)	پیچیده	وابسته	زیر ساخت
۹	هاسکن (۲۰۱۹)	کمپلکس	وابسته	زیر ساخت
۱۰	گتمیری و همکاران (۲۰۲۱)	سری، موازی، سری-موازی	مستقل	اکوسیستم

۱) Ben

امروزه در بحث چالش‌های امنیتی در سطح ملی، گستره اهدافِ در معرض تهدیدها، فراتر از زیر ساخت‌های فیزیکی و سایبری رفته و حفاظت از منابع زیستی و زیست محیطی در مقابل تهدیدهایی مانند تروریسم زیستی (از قبیل تهدیدهای بیولوژیکی)، بهره‌برداری غیر مجاز و حوادث طبیعی، به یکی از موضوعات کلیدی در مسئله امنیت پایدار در سطح جهان و کشورها تبدیل شده است. تهدیدهای زیست محیطی، نسبت به دیگر تهدیدهای نظامی، برای مهاجم بسیار کم هزینه است، اما این نوع تهدیدها به راحتی قابل انتشارند و می‌توانند باعث ایجاد خسارات و تبعات سنگینی شوند. در این موارد، عامل تهدید، ناشناس است، بنابراین شناسایی مهاجم و نیات و قابلیت‌های وی پیچیده است(متقی، کاویانی و نجفی، ۱۳۹۴).

حفاظت از جنگل‌ها و ذخایر گیاهی، آبزیان و حیات وحش در مقابل انواع تهدیدها، یک مسئله اساسی در پایداری محیط زیست به‌شمار می‌آید و خسارات اقتصادی ناشی از آسیب به این منابع برای کشورها، سالانه میلیاردها دلار است. بی‌شک، در کشورهای در حال توسعه، بودجه حفاظت از این منابع، اغلب خیلی محدود است. بنابراین، تخصیص کارای منابع دفاعی، کار سخت، حیاتی و مورد دغدغه این کشورهاست (مک کارتی[1] و همکاران، ۲۰۱۶). در کشور ما نیز مقابله با تهدیدات زیست محیطی و تقویت پدافند غیر عامل در حوزه زیرساخت حیاتی محیط زیست، به‌عنوان یکی از سیاست‌ها و اولویت‌های پژوهشی و فناوری کشور، تعریف و ابلاغ شده است (شورای عالی علوم تحقیقات و فناوری، ۱۳۹۶).

در سال‌های اخیر، با توجه به موفقیت کاربرد تئوری بازی در پرداختن به چالش تخصیص منابع امنیتی، محققان با الهام از این موفقیت، بر به‌کارگیری تئوری بازی در حوزه جدیدی به نام بازی امنیتی سبز[2] تمرکز کرده‌اند. حفاظت از جنگل‌ها در مقابل بهره‌برداری غیر مجاز، حفاظت از گونه‌های جانوریِ در معرض خطر انقراض، از شکار و حفاظت از گونه‌های دریایی در مقابل صید غیر مجاز، از مسائل مورد بررسی در حوزه تحقیقاتی بازی امنیتی سبز هستند. مسائل در حوزه بازی امنیتی سبز، به‌طور عمده، بر مبنای توسعه الگو

۱. McCarthy
۲. Green Security Game (GSG)

بازی استکلبرگ[1] الگوسازی شده و الگوریتم‌های متنوعی برای حل این الگوها طراحی و به‌کار گرفته شده است (فنگ و نگویان، ۲۰۱۶). البته همچنان، چالش‌های کلیدی در این حوزه توسط محققان به‌عنوان زمینه‌های تحقیقات آتی معرفی شده است. اما مروری کلی بر تحقیقات انجام شده در حوزه بازی امنیتی سبز نشان می‌دهد که در اکثر موارد، به حل مسئله دفاع از دارایی‌های زیست محیطی در مقابل تهدید فرصت‌طلبانه پرداخته شده است و به مواردی همچون بهینه‌سازی تخصیص منابع به اهداف (دارایی‌های) زیست محیطی، به‌منظور دفاع در مقابل تهدیدهای راهبردی و یا دفاع همزمان در مقابل انواع تهدیدهای عمدی و غیر عمدی کمتر پرداخته شده است. این در حالی است که در حال حاضر، شواهد متعددی مبنی بر تهدید بقاء دارایی‌های زیست‌محیطی توسط تهدید کنندگان راهبردی و حوادث طبیعی در مناطق مختلف جهان گزارش می‌شود.

در بحث تهدیدهای محیط زیست، حمله راهبردی در دسته اقدامات انسانی قرار می‌گیرد که از طریق بهره‌برداری و دستکاری غیر مجاز منابع طبیعی، باعث آسیب زدن به محیط زیست می‌شوند. به‌عنوان مثالی از این نوع تهدید، می‌توان به تررویسم زیست محیطی[2] اشاره کرد که شامل اقدام یا مجموعه‌ای از اقدامات غیر قانونی می‌شود که به‌منظور تخریب یا دستکاری عمدی منابع زیست محیطی و با اهداف سیاسی صورت می‌گیرد. مثالی دیگر، خرابه‌کاری عمدی در اکوسیستم[3] است که تخریب یا آسیب زدن به یک اکوسیستم با اهداف زیست محیطی-سیاسی تعریف می‌شود (آلپاس، برکوویچ و ارماکووا[4]، ۲۰۱۱). در سال‌های اخیر، آتش سوزی، به‌عنوان یکی از اصلی‌ترین فاکتورهای تهدید کننده حیات اکوسیستم‌های جنگلی به‌شمار می‌رود. این آتش سوزی‌ها، بر اثر عوامل انسانی، اعم از عمدی و غیر عمد و حوادث طبیعی مانند تغییرات اقلیمی به‌وجود می‌آید که عواملی مانند وزش باد موجب گسترش آتش‌سوزی و تشدید خسارات ناشی از آن می‌شود. به همین دلیل، یکی از اصلی‌ترین نگرانی‌ها از منظر زیست محیطی، اقتصادی، اجتماعی و امنیتی در

---

۱. Stackelberg Security Gmae
۲. Environmental terrorism
۳. Eco-Sabotage
۴. Alpas, Berkowicz, & Ermakova

ایران و بسیاری دیگر از کشورهای جهان به‌شمار می‌آید (محمدپور و دشتی، ۱۳۹۷). بر این اساس، پرداختن به مسئله بهینه‌سازی تخصیص منابع محدود به دارایی‌های زیست محیطی، مانند ذخایر گیاهی و جنگل‌ها، به‌منظور حفاظت همزمان در مقابل این مجموعه تهدیدها، بر پایه مفاهیم، دانش و ابزار و فنون ارائه شده در مقاله‌های حوزه بازی امنیتی زیر ساخت و توسعه آنها، به‌عنوان یکی از موضوعات مهم برای تحقیقات آتی پیشنهاد می‌شود. همانطور که در بند آخر نیز آورده شده است، به تازگی، محققان (گتمیری، حافظ الکتب و خاکزار[1]، ۲۰۲۱)، با به‌کارگیری دانش، مفاهیم و فنون مقالات خوشه اول و توسعه الگوهای پیشنهادی در آنها به مسئله بهینه‌سازی تخصیص منابع دفاعی به شبکه غذایی در مقابل تهدیدهای راهبردی پرداخته‌اند. به‌نظر می‌رسد با توسعه الگوهای پیشنهادی آنها بتوان به پوشش شکاف‌های تحقیقاتی در حوزه حفاظت از دارایی‌های زیست محیطی در مقابل انواع تهدیدها غنای بیشتری بخشید.

نتیجه‌گیری و پیشنهاد

این تحقیق، با هدف پوشش شکاف تحقیقاتی موجود در زمینه بررسی نظام‌مند روند انتشارات مجله‌های علمی و شناسایی و معرفی ظرفیت‌های تحقیقاتی بازی امنیتی در حوزه مهندسی با رویکرد تحلیل کتاب‌شناختی انجام شده است. جامعه آماری این تحقیق، محدود به مقاله‌های علمی به زبان انگلیسی مستخرج از پایگاه داده‌ای اسکوپوس است. اما، با وجود این محدودیت، نتایج آن، با توجه به جایگاه برتر این پایگاه داده در میان پایگاه‌های داده علمی معتبر، برای ایجاد دیدگاه کلی نسبت به مجموعه انتشارات علمی در این حوزه تحقیقاتی، قابل اتکاء است. همچنین، رویکرد آن در انجام مرور ادبیات، می‌تواند به‌عنوان الگویی پایه برای تعمیم دادن به مرور ادبیات جوامع آماری فراگیرتر مورد بهره‌برداری قرار گیرد.

نتایج تحلیل کتاب‌شناختی نشان داد که حوزه تحقیقاتی مهندسی، پس از حوزه تحقیقاتی علوم کامپیوتر، در جایگاه دوم قرار دارد. روند انتشارات در این حوزه، همگام با

[1] Gatmiry, Hafezalkotob & Khakzar

سایر انتشارات در موضوع بازی امنیتی، پس از حوادث ۱۱ سپتامبر ۲۰۰۱، از رشد صعودی چشمگیری برخوردار بوده است. در بخش تحلیل نویسندگان مقاله‌ها، نتایج حاکی از آن است که هنوز همکاری لازم بین محققین برای تألیف مقالات مشترک در این حوزه تحقیقاتی شکل نگرفته است. مجله‌های برتر، از حیث انتشار مقالات در این حوزه، همگی از مجله‌های معتبر انتشارات مطرح بین‌المللی هستند که نشان می‌دهد تاکنون مقالات با کیفیت مناسبی در این حوزه منتشر شده است.

تحلیل شبکه هم-استنادی مقاله‌های پر استناد نشان داد که تخصیص بهینه منابع دفاعی و امنیت اطلاعات و ارتباطات، موضوعات اصلی مقاله‌ها هستند و مسئله امنیت اطلاعات و ارتباطات، سهم قابل توجهی را به خود اختصاص داده‌اند. حوزه تخصصی ۸ مجله برتر منتشر کننده مقالات نیز مؤید این مطلب است. بررسی محتوای مقالات دارای بیشترین تعداد هم-استنادی با مقالات پر استناد در مسئله تخصیص بهینه منابع دفاعی نشان داد که حل مسئله الگوسازی عدم قطعیت در اولویت‌بندی اهداف توسط مهاجم، ایجاد موازنه بین انصاف و کارایی در تخصیص منابع دفاعی، الگوسازی تخصیص بهینه منابع امنیتی به مسیرهای شبکه حمل و نقل مواد خطرناک و الگوسازی مسئله انتخاب راهبرد تخصیص منابع دفاعی به اهداف تکی و یا کل اهداف در نظام‌های با ساختاربندی مختلف، موضوع مورد تمرکز تحقیقاتی بوده است.

در مسئله تخصیص بهینه منابع دفاعی، تمرکز اصلی مقالات بر روی دفاع در مقابل دشمن راهبردی بوده است که بازیکنی کاملا منطقی است و راهبرد بهینه حمله را بر مبنای پایش کامل و برنامه‌ریزی قبلی اتخاذ می‌کند. بررسی مقالات مذکور نشان داد که از مفاهیم و برخی فنون مهندسی قابلیت اطمینان برای الگوسازی نظام‌های مورد دفاع و توابع هدف بازیکنان به میزان قابل توجهی بهره گرفته شده است. این رویکرد مهندسی، امکان بررسی و تحلیل اثر راهبردهای انتخاب شده توسط مدافعان و مهاجمان بر روی احتمال بقاء، تاب‌آوری و دسترس‌پذیری نظام مورد دفاع را فراهم آورده است. بررسی قابلیت‌های کاربردی سایر فنون مهندسی قابلیت اطمینان و سایر مفاهیم، ابزارها و فنون متنوع حوزه مهندسی در حل مسائل این حوزه نیز می‌تواند در فهرست تحقیقات آتی قرار گیرد.

همچنین، بر روی انواع محدودی از دارایی‌های زیرساختی، به‌ویژه زیرساخت‌های شبکه‌ای تمرکز شده است. با توجه به اینکه در حال حاضر، حفاظت از دارایی‌های (اهداف) دیگری علاوه بر این نوع زیر ساخت‌ها، در مقابل انواع تهدیدها (اعم از راهبردی، فرصت‌طلبانه و طبیعی)، به موضوع مهمی در بحث امنیت پایدار برای کشورها تبدیل شده است، حل مسئله تخصیص بهینه منابع محدود دفاعی به این نوع دارایی‌ها (اهداف) نیز حائز اهمیت است. از جمله این دارایی‌ها، منابع طبیعی است که با وجود پرداختن به مسئله امنیت آنها در حوزه جدید بازی امنیتی سبز، همچنان به‌عنوان یک حوزه مهم و پر چالش تحقیقاتی به‌شمار می‌آید. نتایج بررسی‌ها نشان داد که اخیراً محققان با الگو گرفتن و توسعه الگوهای بازی امنیتی زیر ساخت در حوزه موضوعی مهندسی به حل مسئله حفاظت از اکوسیستم‌های زیست محیطی در مقابل تهدیدهای راهبردی پرداخته‌اند. به‌نظر می‌رسد توسعه الگوهای پیشنهادی آنها نقطه شروع خوبی برای غنا بخشیدن به تحقیقات در حوزه حفاظت از دارایی‌های زیست محیطی در مقابل انواع تهدیدها باشد.

فهرست منابع و مآخذ

الف. منابع فارسی

- بیگدلی، حمید و طیبی، جواد (۱۳۹۶)، ارائه یک الگو و روش حل بازی های امنیتی فازی و کاربرد آن در آینده پژوهی تهدیدات امنیتی، ***آینده پژوهی دفاعی***، ۲(۶)، ص ۷–۲۹.
- خاتمی، سیدمهدی و انوشه، ابراهیم (۱۳۹۸)، تحلیل منازعه ایران و رژیم صهیونیستی در زمینه برنامه هسته ای ایران با استفاده از نظریه بازی ها، ***آینده پژوهی دفاعی***، ۴(۱۳)، ص ۷–۳۹
- رحالگو، ناصر؛ کامکار، مهدی و یزدانیان، حمید (۱۳۹۹)، ویژگی های دفاع دانش بنیان از منظر مقام معظم رهبری، ***فصلنامه علمی مطالعات مدیریت راهبردی دفاع ملی***، ۴(۱۳)، ص ۲۹۷–۳۳۰.
- شورای عالی علوم تحقیقات و فناوری (۱۳۹۶)، **سیاست ها و اولویت های پژوهش و فناوری کشور در بازه زمانی ۹۶ تا ۱۴۰۰. ایران**.
- کلانتری، فتح الله، (۱۳۹۸)، مدیریت جنگ احتمالی آینده با توجه به روندها و پیشران های موجود، ***فصلنامه علمی مدیریت راهبردی دفاع ملی***، ۳(۱۲)، ص ۲۴۵–۲۷۲.
- عبادی زاده، حجت الله، (۱۳۹۸)، شبیه سازی ریاضی تعاملات و راهبردهای جمهوری اسلامی ایران و عربستان سعودی به کمک نظریه بازی‌ها، ***فصلنامه علمی مطالعات بین رشته ای دانش راهبردی***، ۹(۳۵)، ص ۳۵–۵۶.
- متقی، افشین، کاویانی، مراد و نجفی، سجاد، (۱۳۹۴)، رابطه امنیت زیست محیطی با امنیت ملی، ***فصلنامه مجلس و راهبرد***، ۲۲(۸۳)، ص ۷۵–۱۰۰.
- محمدپور، مطهره و دشتی، سولماز (۱۳۹۷)، شبیه سازی و پهنه بندی گسترش آتش سوزی در اکوسیستم جنگل به کمک الگو FARSITE (مطالعه موردی: جنگل های استان ایلام)، ***جغرافیا و مخاطرات محیطی***، ۳۲، ص ۸۷–۱۰۱.

ب. منابع انگلیسی

- Abbasi, Y. (2016). **Modeling Human Bounded Rationality in Opportunistic Security Games (Doctoral dissertation)**. University of Southern California.
- **All Nobel Prizes.** (n.d.). https://www.nobelprize.org/prizes/lists/all-nobel-prizes/
- Alpas, H., Berkowicz, S. M., & Ermakova, I. (Eds.). (2011). **Environmental Security and Ecoterorrism**. Springer.
- Axelsson, J. (2019). Game theory applications in systems-of-systems

engineering: A literature review and synthesis. ***Procedia Computer Science***, *153*, 154–165. https://doi.org/10.1016/j.procs.2019.05.066

- Basak, A., Fang, F., Nguyen, T. H., & Kiekintveld, C. (2016). Abstraction methods for solving graph-based security games. ***Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)***, *10003 LNAI*, 13–33. https://doi.org/10.1007/978-3-319-46840-2_2
- Basar, T. (2010). Lecture Notes on Game Theory. ***Game Theory Module of the Graduate Program in Network Mathematics***, 3–6.
- Ben Yaghlane, A., & Azaiez, M. N. (2017). Systems under attack-survivability rather than reliability: Concept, results, and applications. ***European Journal of Operational Research***, *258*(3), 1156–1164. https://doi.org/10.1016/j.ejor.2016.09.041
- Bier, V. M., Cox, L. A., & Azaiez, M. N. (2009). Why Both Game Theory and Reliability Theory Are Important in Defending Infrastructure against Intelligent Attacks. ***In Game theoretic risk analysis of security threats*** (pp. 1-11 TS-CrossRef). https://doi.org/10.1007/978-0-387-87767-9_1
- Bricha, N., & Nourelfath, M. (2013). Critical supply network protection against intentional attacks: A game-theoretical model. ***Reliability Engineering and System Safety***, *119*, 1–10. https://doi.org/10.1016/j.ress.2013.05.001
- Casorrán-Amilburu, C. (2017). **Formulations and Algorithms for General and Security Stackelberg Games (Doctoral dessertation)**. Université libre de Bruxelles.
- Catharina, R., Gortnitzki, C., Larsson, A., & Wadskog, D. (2014). Bibliometric Handbook for Karolinska Institutet. ***Research Evaluation***, 41. https://doi.org/10.1093/reseval/rvt018
- Chengcheng, H., & Xiagwei, Q. (2020). A review of games and resource allocation algorithms oriented public security. ***In 2020 International Conference on Computer Engineering and Application (ICCEA), IEEE,*** 373–378.
- Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011). Science mapping software tools: Review, analysis, and cooperative study among tools. ***Journal of the American Society for Information Science and Technology***, *62*(7), 1382–1402. https://doi.org/10.1002/asi.21525
- Elsevier. (2020). **Scopus Content Coverage Guide.** https://www.elsevier.com/__data/assets/pdf_file/0017/114533/Scopus_GlobalResearch_Factsheet2019_FINAL_WEB.pdf
- Fahimnia, B., Tang, C. S., Davarzani, H., & Sarkis, J. (2015). Quantitative models for managing supply chain risks: A review. ***European Journal of Operational Research,*** *247*(1), 1–15. https://doi.org/10.1016/j.ejor.2015.04.034
- Fakoorian, S. A. A., & Swindlehurst, A. L. (2013). Competing for secrecy in the MISO interference channel. ***IEEE Transactions on Signal Processing***,

61(1), 170–181. https://doi.org/10.1109/TSP.2012.2223689
- Fang, F., & Nguyen, T. (2016). Green security games: apply game theory to addressing green security challenges. ***ACM SIGecom Exchanges***, *15*(1), 78–83. https://doi.org/10.1145/2994501.2994507
- Farooqui, A. D., & Niazi, M. A. (2016). Game theory models for communication between agents: a review. In ***Complex Adaptive Systems Modeling*** (Vol. 4, Issue 1). Springer Berlin Heidelberg. https://doi.org/10.1186/s40294-016-0026-7
- Fujiwara-Greve, T. (2015). ***Non-Cooperative Game Theory***. Springer.
- Gatmiry, Z. S., Hafezalkotob, A., Khakzar bafruei, M., & Soltani, R. (2021). Food web conservation vs. strategic threats: A security game approach. ***Ecological Modelling***, *442*(May 2020), 109426. https://doi.org/10.1016/j.ecolmodel.2021.109426
- Grigoryan, G., & Collins, A. J. (2021). Game theory for systems engineering: A survey. ***International Journal of System of Systems Engineering***, *11*(2), 121–158. https://doi.org/10.1504/IJSSE.2021.116044
- Hao, M., Jin, S., & Zhuang, J. (2009). Robustness of Optimal Defensive Resource Allocations in the Face of Less Fully Rational Attacker. ***IIE Annual Conference***, 886–891.
- Hausken, K. (2013). Combined series and parallel systems subject to individual versus overarching defense and attack. ***Asia-Pacific Journal of Operational Research***, *30*(2). https://doi.org/10.1142/S021759591250056X
- Hausken, K. (2014). Choosing What to Protect When Attacker Resources and Asset Valuations are Uncertain. ***Operations Research and Decisions***, *24*(3), 23–44. https://doi.org/10.5277/ord140302
- Hausken, K. (2017a). Defense and attack for interdependent systems. ***European Journal of Operational Research,*** *256*(2), 582–591. https://doi.org/10.1016/j.ejor.2016.06.033
- Hausken, K. (2017b). Special versus general protection and attack of parallel and series components. ***Reliability Engineering and System Safety***, *165*(August 2016), 239–256. https://doi.org/10.1016/j.ress.2017.03.027
- Hausken, K. (2019). Defence and attack of complex interdependent systems. ***Journal of the Operational Research Society***, *70*(3), 364–376. https://doi.org/10.1080/01605682.2018.1438763
- Hausken, K., & Levitin, G. (2012). Review of systems defense and attack models. ***International Journal of Performability Engineering***, *8*(4), 355–366.
- Jacomy, M., Venturini, T., Heymann, S., & Bastian, M. (2014). ForceAtlas2, a continuous graph layout algorithm for handy network visualization designed for the Gephi software. ***PLoS ONE***, *9*(6), 1–12. https://doi.org/10.1371/journal.pone.0098679
- Jain, M., An, B., & Tambe, M. (2013). Security Games Applied to Real-World: Research Contributions and Challenges. In X. S. Wang (Ed.), ***Moving Target Defense II:Application of Game Theory and Adversarial Modeling*** (Vol. 100, pp. 15–39). Springer New York.

- Jiang, G., Shen, S., Hu, K., Huang, L., Li, H., & Han, R. (2015). Evolutionary game-based secrecy rate adaptation in wireless sensor networks. ***International Journal of Distributed Sensor Networks,*** *2015*. https://doi.org/10.1155/2015/975454
- Kar, D., Nguyen, T. H., Fang, F., Brown, M., Sinha, A., Tambe, M., & Jiang, A. X. (2018). Trends and applications in stackelberg security games. ***Handbook of Dynamic Game Theory***, 1223–1269. https://doi.org/10.1007/978-3-319-44374-4_27
- Kovenock, D., & Roberson, B. (2012). Strategic Defense and Attack for Series and Parallel Reliability Systems: Comment. ***Defence and Peace Economics***, *23*(5), 517–519. https://doi.org/10.1080/10242694.2012.660606
- Li, Y., Shi, L., Cheng, P., Chen, J., & Quevedo, D. E. (2015). Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. ***IEEE Transactions on Automatic Control,*** *60*(10), 2831–2836. https://doi.org/10.1109/TAC.2015.2461851
- Liang, X., & Xiao, Y. (2013). Game theory for network security. ***IEEE Communications Surveys and Tutorials***, *15*(1), 472–486. https://doi.org/10.1109/SURV.2012.062612.00056
- Lins, I. D., Rêgo, L. C., Moura, M. D. C., & Droguett, E. L. (2013). Selection of security system design via games of imperfect information and multi-objective genetic algorithm. ***Reliability Engineering and System Safety***, *112*, 59–66. https://doi.org/10.1016/j.ress.2012.11.021
- Manshaei, M. H., Zhu, Q., Alpcan, T., Basar, T., & Hubaux, J. P. (2013). Game theory meets network security and privacy. In ***ACM Computing Surveys*** (Vol. 45, Issue 3). https://doi.org/10.1145/2480741.2480742
- McCarthy, S., Tambe, M., Kiekintveld, C., Gore, M. L., & Killion, A. (2016). Preventing Illegal Logging: Simultaneous Optimization of Resource Teams and Tactics for Security. ***Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence***, 3880–3886. http://dl.acm.org/citation.cfm?id=3016450
- Mo, H., Xie, M., & Levitin, G. (2015). Optimal resource distribution between protection and redundancy considering the time and uncertainties of attacks. ***European Journal of Operational Research***, *243*(1), 200–210. https://doi.org/10.1016/j.ejor.2014.12.006
- Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. ***IEEE Communications Surveys and Tutorials***, *16*(3), 1550–1573. https://doi.org/10.1109/SURV.2014.012314.00178
- Neumann, V., & Morgenstern, O. (1944). **Theory of Games and Economic Behavior.**
- Nikoofal, M. E., & Zhuang, J. (2012). Robust Allocation of a Defensive Budget Considering an Attacker's Private Information. ***Risk Analysis***, *32*(5), 930–943. https://doi.org/10.1111/j.1539-6924.2011.01702.x
- Rahman, M. A., Manshaei, M. H., Al-Shaer, E., & Shehab, M. (2017). Secure and private data aggregation for energy consumption scheduling in

smart grids. ***IEEE Transactions on Dependable and Secure Computing***, *14*(2), 221–234. https://doi.org/10.1109/TDSC.2015.2446492

- Rao, N. S. V., Ma, C. Y. T., Hausken, K., He, F., & Zhuang, J. (2016). Defense strategies for infrastructures with multiple systems of components. *FUSION 2016 - **19th International Conference on Information Fusion, Proceedings, October***, 270–277.
- Reniers, G. L. L. (2012). Security of multimodal hazmat transports: Empirical findings and future directions. ***International Journal of Safety and Security Engineering***, *2*(1), 69–79. https://doi.org/10.2495/SAFE-V2-N1-69-79
- Sanchez-Soriano, J. (2013). An overview on game theory applications to engineering. ***International Game Theory Review***, *15*(3), 1–18. https://doi.org/10.1142/S0219198913400197
- Sandler, T., & Arce, D. G. M. (2003). Terrorism & game theory. ***Simulation and Gaming***, *34*(3), 319–337. https://doi.org/10.1177/1046878103255492
- Seaberg, D., Devine, L., & Zhuang, J. (2017). A review of game theory applications in natural disaster management research. ***Natural Hazards***, *89*(3), 1461–1483. https://doi.org/10.1007/s11069-017-3033-x
- Shan, X., & Zhuang, J. (2013). Cost of equity in homeland security resource allocation in the face of a strategic attacker. ***Risk Analysis***, *33*(6), 1083–1099. https://doi.org/10.1111/j.1539-6924.2012.01919.x
- Stanojev, I., & Yener, A. (2013). Improving secrecy rate via spectrum leasing for friendly jamming. ***IEEE Transactions on Wireless Communications***, *12*(1), 134–145. https://doi.org/10.1109/TWC.2012.120412.112001
- Talarico, L., Reniers, G., Sörensen, K., & Springael, J. (2015). MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries. ***Reliability Engineering and System Safety***, *138*, 105–114. https://doi.org/10.1016/j.ress.2015.01.022
- Tambe, M. (2012). Security and Game Theory. In ***cambridge university press***.
- Tang, L., Gong, X., Wu, J., & Zhang, J. (2013). Target detection in bistatic radar networks: Node placement and repeated security game. ***IEEE Transactions on Wireless Communications***, *12*(3), 1279–1289. https://doi.org/10.1109/TWC.2013.011713.120892
- Thomé, A. M. T., Scavarda, L. F., & Scavarda, A. J. (2016). Conducting systematic literature review in operations management. ***Production Planning and Control***, *27*(5), 408–420. https://doi.org/10.1080/09537287.2015.1129464
- Trejo, K. K., Clempner, J. B., & Poznyak, A. S. (2015). A Stackelberg security game with random strategies based on the extraproximal theoretic approach. ***Engineering Applications of Artificial Intelligence***, *37*, 145–153. https://doi.org/10.1016/j.engappai.2014.09.002
- Wang, L., Ren, S., Korel, B., Kwiat, K. A., & Salerno, E. (2014). Improving

system reliability against rational attacks under given resources. ***IEEE Transactions on Systems, Man, and Cybernetics: Systems***, *44*(4), 446–456. https://doi.org/10.1109/TSMC.2013.2263126

- Wang, Y., Wang, Y., Liu, J., Huang, Z., & Xie, P. (2017). A survey of game theoretic methods for cyber security. ***Proceedings - 2016 IEEE 1st International Conference on Data Science in Cyberspace***, *DSC 2016*, 631–636. https://doi.org/10.1109/DSC.2016.90
- Wilczyński, A., Jakóbik, A., & Kołodziej, J. (2016). Stackelberg security games: Models, applications and computational aspects. ***Journal of Telecommunications and Information Technology***, *2016*(3), 70–79.
- Wu, Y., Wang, B., Liu, K. J. R., & Clancy, T. C. (2012). Anti-jamming games in multi-channel cognitive radio networks. ***IEEE Journal on Selected Areas in Communications***, *30*(1), 4–15.
- Zagare, F. C. (2019). Game Theory and Security Studies. In ***Game Theory, Diplomatic History and Security Studies*** (Issue January, pp. 7–24). Oxford University Press. https://doi.org/10.1093/oso/9780198831587.003.0002

Zhang, H., Wang, T., Song, L., & Han, Z. (2016). Interference Improves PHY Security for Cognitive Radio Networks. ***IEEE Transactions on Information Forensics and Security***, *11*(3), 609–620. https://doi.org/10.1109/TIFS.2015.2500184.