فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال پنجم، شماره دو، تابستان 1400

مدلی برای تشخیص نفوذ در اینترنت اشیاء بااستفاده‌از بازی شراکت

علی سلیمی[1]، مجید غیوری‌ثالث[2]

تاریخ دریافت: 1400/05/12 **تاریخ پذیرش**: 1400/09/17

چکیده

یکی از چالش‌های موجود در سیستم‌های تشخیص نفوذ در اینترنت اشیاء چالش منابع است که دسترسی محدود به منابع و همچنین مصرف بالای منابع را شامل می‌شود. برای غلبه بر این چالش، دسته‌ای از پژوهش‌ها به راه‌حل فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ در اینترنت اشیاء نظر داشته‌اند. در این مسیر، ارتباطات میان مدافعین و مهاجمین در قالب یک بازی، با استفاده از نظریه‌ی بازی، مدل‌سازی می‌شود و سپس گره مدافع تصمیم می‌گیرد که چه زمان یا میزانی سیستم تشخیص نفوذ خود را فعال کند. در پژوهش‌های پیشین اما، همواره بازی میان یک تک‌گره مدافع و مهاجم برقرار است و ارتباطات میان گره‌های مدافع در شبکه، در مدل‌های ارائه‌شده درنظر گرفته نمی‌شود. به باور ما، درنظرگرفتن ارتباطات میان مدافعین برای اتخاذ تصمیم عقلانی اهمیت دارد. ما در این پژوهش، به‌منظور فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ در اینترنت اشیاء، روشی را برای مدل‌سازی ارتباطات میان گره‌های مدافع با استفاده از بازی شراکت ارائه داده‌ایم. در این روش، گره مدافع با درنظرگرفتن رفتار گره‌های مدافع دیگر و همچنین درآمد حاصل از امنیت و هزینه وارد از مصرف منابع، تلاش می‌کند برای میزان فعالسازی سیستم تشخیص نفوذ خود تصمیم صحیحی بگیرد. در نهایت نشان داده‌ایم که در این روش، گره‌های مدافع، با همکاری یکدیگر، می‌توانند هزینه‌ی منابع خود را به طور معقول کاهش دهند.

واژگان کلیدی: اینترنت اشیاء، بازی شراکت، تشخیص نفوذ، چالش منابع، نظریه‌ی بازی

[1] دانشجوی کارشناسی‌ارشد، دانشگاه جامع امام‌حسین(ع)، alisalimi@ihu.ac.ir

[2] استادیار دانشکده‌ی کامپیوتر و قدرت سایبری، دانشگاه جامع امام‌حسین(ع)، ghayoori@ihu.ac.ir

نویسنده‌ی مسئول: مجید غیوری‌ثالث

1. مقدمه

در سال 1999، عبارت اینترنت اشیاء[1] به‌وسیله‌ی کوین اشتون[2]، در طی فعالیت او در بخش بهینه‌سازی زنجیره‌ی تأمین شرکت پراکتر-اند-گمبل[3] ابداع شد[1]. تاکنون تعاریف و نگرش‌های متفاوتی برای اینترنت اشیاء ارائه‌شده است که ازجمله‌ی آن می‌توان به یکپارچه‌سازی دنیای مجازی و دنیای فیزیکی اشاره‌کرد[2]. امروزه کاربرد اینترنت اشیاء در حوزه‌های مختلفی مانند شهر هوشمند، سلامت هوشمند، کشاورزی هوشمند و خانه هوشمند قابل ردگیری است. اینترنت اشیاء در کنار فواید بیشمار خود، چالش‌های متعددی را نیز در جنبه‌های مختلف، با خود همراه‌کرده‌است؛ مانند چالش‌های استانداردسازی، مدیریت، بصری‌سازی، مصرف منابع، و البته امنیت[4][3].

آلابا و همکارانش[5] تهدیدات و آسیب‌پذیری‌های امنیتی در اینترنت اشیاء را به سه دسته‌ی تهدیدات سخت‌افزار[4]، تهدیدات شبکه[5] و تهدیدات کاربرد هوشمند[6] تقسیم‌بندی کرده‌اند. این تهدیدات حملات مختلفی را مانند انکار خدمت[7]، استراق سمع[8] و جعل[9] سبب می‌شود. چالش برقراری امنیت و مقابله با این تهدیدات در اینترنت اشیاء دلایل متفاوتی دارد. وجود پروتکل‌ها، استانداردها، سخت‌افزارها، و نرم‌افزارهای مختلف یا به طور کلی ناهمگونی[10] در اینترنت اشیاء ازجمله‌ی این دلایل است. اما یکی از اصلی‌ترین چالش‌های پیش‌روی برقراری امنیت در شبکه‌ی اینترنت اشیاء، به‌خصوص در لایه‌ی ادراکی[11] این شبکه، چالش منابع است[5].

به‌دلیل خصوصیت ویژه‌ی اینترنت اشیاء که با جهان فیزیکی ارتباط و تبادل تنگاتنگی دارد و همچنین ویژگی همه‌جاحاضری[12] این شبکه و نیاز به استفاده‌ی گسترده از دستگاه‌های تعبیه‌شده با حسگرها[13] و عملگرها[14]، اینترنت اشیاء مملو است از دستگاه‌هایی با ظرفیت پایین[15] در پایین‌ترین لایه‌ی این شبکه که به آن لایه‌ی ادراکی گویند. مصرف بالای منابع به دلیل گستردگی فیزیکی لایه‌ی ادراکی و دسترسی محدود به منابع به دلیل وجود دستگاه‌هایی با منابع کم در لایه‌ی ادراکی، دو روی سکه‌ی چالش منابع در اینترنت اشیاء است. چنین شرایطی یک شبکه‌ی کم‌توان و پراتلاف[16] را نتیجه‌می‌دهد که استفاده از روش‌های پیشین تأمین امنیت موجود در شبکه‌های قراردادی[17] در آن ممکن نیست و نیاز به روش‌ها، مدل‌ها و نگرش‌های جدیدی را مطرح می‌کند که ویژگی اصلی آن نسبت به روش‌های پیشین، مصرف معقول منابع است.

تشخیص نفوذ[18] درکنار مفاهیم دیگری چون دیوار آتش و رمزنگاری، یکی از راه‌حل‌های برقراری امنیت در شبکه‌های کامپیوتری‌ست. اما چنان که بیان‌شد، چالش منابع، نیاز به سیستم‌ها، مدل‌ها و نگرش‌های تشخیص نفوذ جدیدی را در اینترنت اشیاء مطرح می‌کند. درواقع مسئله این است که چگونه با مصرف معقول‌تر منابع کار تشخیص نفوذ را انجام دهیم. تلاش‌های بسیاری ازسوی محققین برای انطباق و ارائه‌ی سیستم‌های تشخیص نفوذی[19] متناسب با نیازمندی‌ها و شرایط اینترنت اشیاء ارائه‌شده‌است. این تلاش‌ها را می‌توان به شاخه‌های مختلفی تقسیم‌بندی کرد، ازجمله: تلاش درجهت بهینه‌سازی سخت‌افزار و منابع انرژی، ارائه‌ی الگوریتم‌های کم‌وزن برای تشخیص نفوذ، جایگذاری بهینه‌ی سیستم‌های تشخیص نفوذ در لایه‌ی ادراکی اینترنت اشیاء، و فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ.

در تحقیقات معدودی به رویکرد فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ در لایه‌ی ادراکی اینترنت اشیاء پرداخته‌شده‌است. در این تحقیقات، با استفاده از نظریه‌ی

[1] Internet of Thing
[2] Kevin Ashton
[3] Procter&Gamble
[4] Hardware Threats
[5] Network Threats
[6] Smart Application Threat
[7] Denial of Servic (DoS)
[8] Eavesdropping
[9] Counterfeiting
[10] Heterogeneity
[11] Perceptual Layer
[12] Ubiquitous
[13] Sensor
[14] Actuator
[15] Low-weight Devices
[16] Low-power and Lossy Network (LLN)
[17] Conventional Networks
[18] Intrusion Detection
[19] Intrusion Detection System (IDS)

بازی[1] روابط میان گره‌های شبکه و حمله‌کنندگان مدل‌سازی شده‌است. این مدل‌سازی در قالب یک بازی میان گره مدافع[2] و حمله‌کننده[3] و با درنظرگرفتن درآمد حاصل از امنیت و هزینه‌ی تحمیل‌شده از مصرف منابع انجام‌شده‌است. درنهایت، با استفاده از مدل‌های ایجادشده، تصمیم عقلانی[4] برای چگونگی فعال‌سازی مکانیزم تشخیص نفوذ اتخاذ شده‌است که موضوع تصمیم، گاهی زمان فعال‌سازی و گاهی میزان فعال‌سازی و نوع سیستم تشخیص نفوذ برای فعال‌سازی است.

اما در پژوهش‌های پیشین، ارتباط میان گره‌های مدافع مختلف در لایه‌ی ادراکی و در مقابل و علیه حمله‌کننده نادیده گرفته‌شده‌است. در مدل‌های ارائه‌شده، گره مدافع در مقابل حمله‌کننده تنهاست و بدون درنظرگرفتن رفتار سایر گره‌های مدافع تصمیم‌گیری می‌کند. به باور ما، درنظرگرفتن ارتباط میان گره‌های مدافع مختلف برای تحلیل عقلانی شرایط اهمیت دارد و می‌تواند سبب اتخاذ تصمیم صحیح‌تر شود؛ چنان که وجود یک گره مدافع در شبکه تفاوت می‌کند با وجود چند گره مدافع. ما در این پژوهش با مدل‌کردن ارتباط میان گره‌های موجود در اینترنت اشیاء در تشخیص نفوذ، با استفاده از بازی شراکت[5] یا بازی هم‌افزایی[6] مدلی را برای فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ ارائه‌داده‌ایم. با استفاده از مدل ارائه‌شده، هر گره مدافع با درنظرداشتن گره‌های مدافع دیگر در شبکه و همچنین درآمد حاصل از برقراری امنیت و هزینه‌ی حاصل از مصرف منابع، می‌تواند تصمیم عقلانی برای چگونگی فعال‌سازی سیستم تشخیص نفوذ خود اتخاذکند.

درادامه ابتدا مفاهیم پایه (بخش 2) و کارهای پیشین (بخش 3) شرح داده‌شده‌است. سپس مدل پیشنهادی ارائه شده (بخش 4) و در بخش بعدی در یک مطالعه‌ی موردی شبیه‌سازی شده و مورد ارزیابی قرار گرفته‌است (بخش 5). در گام بعدی تفاوت مدل‌های ارائه‌شده با پژوهش‌های پیشین مورد بحث قرارگرفته (بخش 6) و نتایج (بخش 7) بیان شده‌است.

2. مفاهیم پایه

در این بخش سه مفهوم اینترنت اشیاء، سیستم تشخیص نفوذ، و نظریه‌ی بازی به طور مختصر بیان می‌شود.

2-1. اینترنت اشیاء

تاکنون برای اینترنت اشیاء تعاریف متعدد و متنوعی بیان‌شده‌است. اما پیش از نقل‌قول این تعاریف باید یادآور این نکته شد که عبارت "اینترنت اشیاء" به خودی‌خود نکات مهمی را درباره‌ی چیستی این مفهوم روشن می‌کند. نکته‌ی اول قابل‌برداشت این است که اینترنت اشیاء در وهله‌ی اول، اینترنت است یا به عبارت دیگر مرحله‌ی جدیدی از شبکه‌ی اینترنت موجود و می‌دانیم که اینترنت عبارت‌است از شبکه‌ای از شبکه‌های کامپیوتری که بزرگترین شبکه‌ی کامپیوتری موجود است. با توجه به این مسئله می‌توان به این نکته پی‌برد که یک شبکه محلی از اشیاء مانند خانه‌ی هوشمند که از طریق شبکه‌ی اینترنت دسترس‌پذیر[7] نیست در مفهوم اینترنت اشیاء جای ندارد و عبارت "شبکه‌ی اشیاء"[8] برای چنین شبکه‌ای مناسب‌تر به‌نظرمی‌رسد.

نکته‌ی دوم قابل برداشت این است که این شبکه‌ی اینترنت جدید، شبکه‌ی اشیاء است. پیش از این، اینترنت تنها برای ارتباط انسان‌ها مورد استفاده قرار می‌گرفت و تنها موجودیت‌های دو سر ارتباط، انسان‌ها بودند (رایانه‌ها نیز جزو واسطه‌ها درنظر گرفته‌شده‌اند). اما با ورود مفهوم اینترنت اشیاء، موجودیت دیگری به نام شیء[9] (که هرچیزی یک شیء است) وارد شبکه‌ی اینترنت شد که نتیجه‌ی آن افزودن انواع ارتباط شیء-به-شیء و انسان-به-شیء به نوع ارتباط انسان-به-انسان بود.

اینک دو تعریف ارائه‌شده برای اینترنت اشیاء را بیان می‌کنیم:

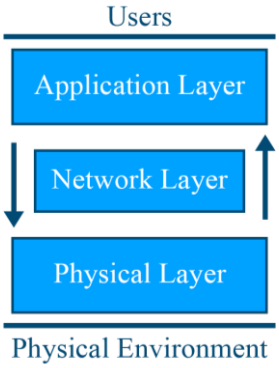
[1] Game Theory
[2] Defender
[3] Attacker
[4] Rational
[5] Partnership Game
[6] Synergistic Game
[7] Available
[8] Network of Things
[9] Thing

تعریف اول: یکپارچه‌سازی بدون‌درز انسان‌ها و دستگاه‌ها به منظور همگرایی دنیای فیزیکی و محیط‌های مجازی ساخت بشر[2].

تعریف دوم: یک طرح‌واره‌ی میان‌شبکه‌ای[1] میسرشده به‌وسیله‌ی پشته‌ی فناوری[2] که یک ارتباط بدون‌درز را میان اشیاء فیزیکی و اشیاء مجازی ارائه می‌کند؛ برای تسهیل توسعه‌ی سرویس‌ها و کاربردهای هوشمند با قابلیت خودپیکربندی[3]. پشته‌ی فناوری ترکیبی است از فناوری‌های مختلف که این فرآیندها و همچنین یک اتصال بدون‌درز "در هرزمان، هرمکان، به‌وسیله‌ی هرکس و هرچیز" را میسر می‌کند[4].

امروزه اینترنت اشیاء در حوزه‌های مختلفی به‌کار گرفته‌می‌شود که از جمله‌ی آن می‌توان به حوزه‌های مراقبت‌های بهداشتی، انرژی، حمل‌ونقل، خودکارسازی ساختمان، شهرهای هوشمند، کشاورزی، صنعت، و حوزه‌ی نظامی[4] اشاره‌کرد[6].

در یک نگرش سطح‌بالا، می‌توان معماری اینترنت اشیاء را در سه بخش لایه‌ی فیزیکی[5] یا لایه‌ی ادراکی، لایه‌ی شبکه[6] و لایه‌ی کاربرد[7] خلاصه‌کرد (شکل 1). لایه‌ی فیزیکی یا لایه‌ی ادراکی شامل دستگاه‌های تعبیه‌شده با حسگرها و عملگرها است که وظیفه‌ی آن تبادل با محیط فیزیکی‌ست. وظیفه‌ی لایه‌ی شبکه انتقال داده‌ها میان گره‌های شبکه و همچنین انتقال اطلاعات در بستر اینترنت است. لایه‌ی کاربرد نیز وظیفه‌ی بهره‌برداری از این داده‌ها و مدیریت گره‌های شبکه را برعهده دارد. از جنبه‌ی دیگر، عملیات اینترنت اشیاء در سه مرحله تقسیم‌بندی می‌شود: مرحله‌ی جمع‌آوری[8] مرحله‌ی انتقال[9] و مرحله‌ی پردازش، مدیریت و بهره‌برداری[10] در مرحله‌ی جمع‌آوری، هدف اصلی جمع‌آوری داده‌های مربوط به محیط فیزیکی است که این داده‌ها در مرحله‌ی انتقال، به کاربردها، و نهایتا به کاربران منتقل می‌شوند. در مرحله‌ی پردازش، مدیریت، و بهره‌برداری، این داده‌ها توسط کاربردها به‌منظور کسب اطلاعات مفید پردازش می‌شوند که هدف، تصمیم‌گیری بر پایه‌ی این اطلاعات و کنترل اشیاء فیزیکی موجود درون محیط فیزیکی است[7].



شکل 1- معماری سطح‌بالای اینترنت اشیاء

درنهایت، ظرفیت محدود دستگاه‌های لایه‌ی ادراکی یا مرحله‌ی جمع‌آوری، گستردگی فیزیکی، وجود فناوری‌ها و پروتکل‌های مختلف، و به‌طورکلی وجود ناهمگونی از ویژگی‌های اصلی اینترنت اشیاء و سبب تمایز آن با شبکه‌های قراردادی پیشین به‌شمار می‌روند[7][5][2]. این ویژگی‌ها چالش‌های مختلفی را سبب می‌شوند، ازجمله: استانداردسازی، مدیریت، بصری‌سازی، مصرف منابع، و امنیت[4][3].

2-2. سیستم تشخیص نفوذ

تشخیص نفوذ عبارت است از فرآیند پایش رخدادها روی سیستم کامپیوتری یا شبکه و تحلیل آن جهت به دست آوردن نشانه‌هایی از اتفاقاتی که خط‌ومشی‌ها و استانداردهای امنیتی را نقض می‌کنند. به سیستم نرم‌افزاری که فرآیند تشخیص نفوذ را به‌طور خودکار انجام می‌دهد سیستم تشخیص نفوذ گویند[8]. یک سیستم تشخیص نفوذ از سه بخش حسگرها، موتور تحلیل[11] و سیستم گزارش‌دهی[12] تشکیل می‌شود[7]. بخش حسگرها داده‌های شبکه یا سیستم میزبان را جمع‌آوری می‌کند،

[1] Inter-networking Paradigm
[2] Technology Stack
[3] Self-configuring
[4] Military
[5] Physical Layer
[6] Network Layer
[7] Application Layer
[8] Collection Phase
[9] Transmission Phase
[10] Processing, Management and Utilization phase
[11] Analysis Engine
[12] Reporting System

سپس این داده‌ها در بخش موتور تحلیل به منظور کشف نفوذ ارزیابی می‌شوند، و درنهایت، در هنگام کشف نفوذ، سیستم گزارش‌دهی، هشدارها و گزارش‌های لازم را به مدیر شبکه یا سیستم ارسال می‌کند.

سیستم‌های تشخیص نفوذ، برحسب نوع اطلاعات جمع‌آوری شده در بخش حسگرها، به دو دسته‌ی مبتنی‌بر میزبان[1]و مبتنی‌بر شبکه[2]تقسیم‌بندی می‌شوند. سیستم تشخیص نفوذ مبتنی‌بر میزبان[3]به یک دستگاه/میزبان ضمیمه می‌شود و به منظور کشف فعالیت‌های مخرب، وقایع درون سیستم را نظارت می‌کند. سیستم تشخیص نفوذ مبتنی‌بر شبکه[4]به یک یا چند بخش از شبکه متصل می‌شود و به منظور کشف اقدامات مخرب، بر ترافیک شبکه نظارت می‌کند[9]. به طور کلی، می‌توان گفت، در سیستم‌های تشخیص نفوذ مبتنی‌بر میزبان توجه به وقایع درون یک سیستم مشخص و در سیستم‌های تشخیص نفوذ مبتنی‌بر شبکه توجه به وقایع درون شبکه است. به سیستم تشخیص نفوذی که به هر دو دسته از وقایع توجه دارد سیستم تشخیص نفوذ ترکیبی[5]گویند.

سیستم‌های تشخیص نفوذ، برحسب روش[6]اتخاذشده برای تشخیص ناهنجاری در بخش موتور تحلیل، به سه دسته‌ی مبتنی‌بر امضاء،[7] مبتنی‌بر ناهنجاری،[8] و مبتنی‌بر تعیین مشخصات[9] تقسیم‌بندی می‌شوند[11][10][9][7]. در روش مبتنی بر امضاء، رفتارهای موجود در شبکه یا میزبان با الگوها/امضاءهای رفتارهای مخرب موجود در پایگاه‌داده‌ی سیستم تشخیص نفوذ مقایسه می‌شود و درصورت تطابق، رفتار مخرب کشف‌می‌شود. در روش مبتنی‌بر ناهنجاری، میزان انحراف هر رفتار موجود در شبکه یا میزبان از رفتار عمومی موجود ارزیابی می‌شود و رفتارهای مغایر با رفتارهای عمومی، به عنوان رفتار مخرب شناسایی می‌شوند. روش مبتنی‌بر تعیین مشخصات، شامل مجموعه‌ای از قوانین[10]و حدود آستانه[11]است که رفتار مورد انتظار در شبکه یا میزبان را تعریف می‌کنند و هر رفتارهای مغایر با رفتارهای مورد انتظار تعریف‌شده، به عنوان رفتار مخرب شناسایی می‌شوند. یک سیستم تشخیص نفوذ، در موتور تحلیل خود، می‌تواند ترکیبی از روش‌های مطرح‌شده را به‌کارگیرد که به چنین روشی، روش ترکیبی گویند.

سیستم‌های تشخیص نفوذ، ازجمله تمهیداتی است که برای تأمین امنیت در اینترنت اشیاء به‌کارگرفته می‌شود. درهنگام ایجاد و ارائه‌ی یک سیستم تشخیص نفوذ در اینترنت اشیاء، مجموعه‌ای از تصمیمات اتخاذ می‌شود؛ به عبارت دیگر می‌توان سیستم‌های تشخیص نفوذ در اینترنت اشیاء را با برخی ویژگی‌های مشخص عنوان نمود. علاوه بر نوع سیستم تشخیص نفوذ و روش تشخیص نفوذ مورد استفاده که پیش‌تر بیان شد، تصمیم/ویژگی دیگری که از اهمیت بالایی برخوردار است مکان سیستم تشخیص نفوذ در اینترنت اشیاء است که گاهی به آن معماری سیستم تشخیص نفوذ در اینترنت اشیاء نیز اطلاق می‌شود. سیستم‌های تشخیص نفوذ در اینترنت اشیاء برحسب مکان جایگذاری به سه دسته‌ی توزیع‌شده،[12]متمرکز[13]و ترکیبی تقسیم می‌شوند. در دسته‌ی توزیع‌شده، سیستم‌های تشخیص نفوذ در تمام اشیاء فیزیکی اینترنت اشیاء جایگذاری می‌شوند. در دسته‌ی متمرکز، سیستم تشخیص نفوذ درون یک مولفه‌ی متمرکز جایگذاری می‌شود. دسته‌ی ترکیبی، مفاهیم دو روش پیشین را ترکیب می‌کند به طریقی که در این دسته، سیستم‌های تشخیص نفوذ در برخی از دستگاه‌های اینترنت اشیاء (نه یک دستگاه و نه تمام دستگاه‌ها) جایگذاری می‌شوند. فناوری‌های[14] موردنظر سیستم تشخیص نفوذ ارائه‌شده و همچنین حملات[15] موردنظر ازجمله تصمیم/ویژگی‌های دیگر سیستم‌های تشخیص نفوذ در اینترنت اشیاء است. در نهایت می‌توان نحوه‌ی

[1]Host-based
[2]Network-based
[3]HIDS
[4]NIDS
[5]Hybrid
[6]Method
[7]Signature-based
[8]Anomaly-based
[9]Specification-based
[10]Rules
[11]Thresholds
[12]Distributed
[13]Centralized
[14]Technologies
[15]Attacks

اعتبارسنجی[1]سیستم تشخیص نفوذ ارائه‌شده را به عنوان آخرین تصمیم/ویژگی سیستم‌های تشخیص نفوذ در اینترنت اشیاء دانست[7].

2-3. نظریه‌ی بازی

نظریه‌ی بازی شاخه‌ای از علم ریاضیات و علمی برای تحلیل موقعیت‌های استراتژیک[2] است. به‌طورکلی، بازی[3] را می‌توان شرایطی تعریف کرد که در آن سودمندی[4]هرکدام از بازیکنان، علاوه بر رفتار/استراتژی[5]خود، به رفتار/استراتژی بازیکنان دیگر نیز بستگی‌دارد. نظریه‌ی بازی از جنبه‌های مختلف کاربرد دارد: تحلیل چرایی رفتارهای بازیکنان در یک موقعیت استراتژیک، پیش‌بینی رفتار بازیکنان، و توصیه‌ی استراتژی عقلانی به بازیکنان یک بازی. امروزه، نظریه‌ی بازی در دامنه‌ی گسترده‌ای از علوم کاربرد دارد؛ مانند علوم سیاسی، جامعه‌شناسی، روانشناسی، علوم کامپیوتری، و امنیت.

مفاهیم، روش‌ها، و نظریه‌های مختلفی در نظریه‌ی بازی وجوددارد. به عنوان یکی از اساسی‌ترین این مفاهیم می‌توان به مفهوم بهترین پاسخ[6]اشاره‌کرد. بهترین پاسخ عبارت است از بهترین استراتژی یا استراتژی‌های یک بازیکن که در پاسخ به استراتژی‌های اتخاذشده به‌وسیله‌ی بازیکنان دیگر، بیشترین سودمندی را برای آن بازیکن به عمل می‌آورد. این مفهوم، پایه‌ای است برای دو نظریه‌ی مهم در این حوزه: نظریه‌ی عقلانیت[7]و نظریه‌ی تعادل نش.[8] نظریه عقلانیت تلاشی است برای حذف مجموعه استراتژی‌های یک بازیکن که در هیچ‌صورتی (در پاسخ به هیچ‌یک از استراتژی‌های بازیکنان دیگر) بهترین پاسخ نیستند. نظریه‌ی دیگر، نظریه‌ی تعادل نش، به نقاطی از فضای بازی[9] اشاره می‌کند که در آن تمام بازیکنان در پاسخ به استراتژی بازیکنان دیگر بهترین پاسخ را اتخاذ کرده‌اند که به این نقاط، نقاط تعادل[10] بازی گویند. منظور از نقاط بازی، تلاقی استراتژی‌های تمام بازیکنان یک بازی است که به آن نمایه‌ی استراتژی[11]گویند و همچنین فضای بازی یعنی تمام تلاقی‌های استراتژیک ممکن. گاهی بازیکنانی که در نقطه‌ی تعادل بازی قرارگرفته‌اند، به طور جمعی (و نه فقط یک بازیکن) با انتخاب استراتژی‌های دیگری به غیر از تعادل می‌توانند سودمندی خود را افزایش دهند اما چنین نقاطی به دلیل تعادل نبودن ناپایدارند. زیرا حداقل یک بازیکن وجوددارد که در این نقطه می‌تواند با اتخاذ استراتژی دیگری سودمندی خود را افزایش داده و بازی را از این نقطه خارج کند. همین امر مفهوم قرارداد[12]را در نظریه‌ی بازی به‌وجود می‌آورد. با استفاده از قرارداد بازیکنان می‌توانند بر انتخاب استراتژی بخصوصی از بازی قرارداد کنند[12].

همچنین باید یادآور این نکته شد که بازی‌ها انواع و شرایط مختلفی دارند که از آن جمله می‌توان به تقسیم‌بندی کلی بازی‌های ایستا[13]و بازی‌های پویا[14]اشاره‌کرد. در بازی‌های ایستا، بازیکنان، همگی، به‌یکباره[15]استراتژی خود را انتخاب می‌کنند اما در بازی‌های پویا انتخاب‌ها به‌صورت متوالی انجام‌می‌شود[12].

گاهی در شرایط استراتژیک مختلف، روابط میان بازیکنان شباهت‌های بنیادینی با یکدیگر دارد که این مسئله برخی مدل‌های اساسی بازی را معرفی می‌کند به‌طوری‌که می‌توان رد این مدل‌های بازی را در شرایط استراتژیک مختلف مشاهده‌کرد؛ مانند بازی معمای زندانی،[16]جمع صفر،[17]و البته بازی شراکت. بازی شراکت یا بازی هم‌افزایی، مدلی برای بیان ارتباطات بازیکنان در یک پروژه مشترک است؛ مانند شرایطی که چند

[1] Validation
[2] Strategic Setting
[3] Game
[4] Utility
[5] Strategy
[6] Best Response
[7] Rationalizability
[8] Nash Equilibrium
[9] Strategy Space
[10] Equilibrium
[11] Strategy Profile
[12] Contract
[13] Static
[14] Dynamic
[15] One-shot
[16] Prisoner's Dilemma
[17] Zero-sum

همکار در تولید یک محصول دارند. چنان‌که روشن است، در این بازی یک پروژه[1]و چند شریک[2]وجوددارد. سودی که از تلاش هریک از شرکا حاصل می‌شود به سود کلی پروژه اختصاص دارد که هرکدام از شرکا سهم مشخصی از این سود دارند. اما هزینه‌ای که هر شریک برای این تلاش صرف می‌کند متوجه خود اوست. نکته‌ی دیگر این بازی این است که تلاش جمعی شرکا ممکن است درآمد افزوده‌ای برای پروژه حاصل کند به این معنا که ممکن است تلاش چند شریک باهم ارجح باشد بر تلاش یک شریک تنها که این مسئله را در این بازی، مکملیت[3] گویند و با تابع مکملیت[4] وجود یا عدم‌وجود و چگونگی آن قابل‌تعریف است[12].

3. پژوهش‌های مرتبط

در این بخش به بیان مختصری از پژوهش‌هایی که در جهت به‌کارگیری سیستم‌های تشخیص نفوذ در اینترنت اشیاء انجام‌شده‌است پرداخته‌ایم. این تلاش‌ها به مسیرها و دسته‌های مختلفی قابل تقسیم‌بندی است: بهینه‌سازی سخت‌افزار و منابع انرژی، ارائه‌ی الگوریتم‌های کم‌وزن برای تشخیص نفوذ، جایگذاری بهینه سیستم‌های تشخیص نفوذ در لایه‌ی ادراکی اینترنت اشیاء، و فعال‌سازی بهینه سیستم‌های تشخیص نفوذ. البته ممکن است یک پژوهش در بیش از یک دسته جای گیرد. پیش از مرور باید یادآور این نکته شد که حوزه‌ی سخت‌افزاری مورد توجه ما نیست و در مقابل، تمرکز ما دسته‌ی فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ است.

ارائه‌ی الگوریتم‌های بهینه، معمولا یکی از سه حالت ممکن است: ارائه‌ی یک الگوریتم جدید، ارائه‌ی یک کاربرد جدید برای الگوریتم موجود، یا ارائه‌ی یک ترکیب جدید از الگوریتم‌های موجود که البته خود زیرشاخه‌ای از دسته‌ی دوم است. همچنین بهینگی می‌تواند در جهت پردازش و/یا حافظه باشد. برای نمونه، در جهت ارائه‌ی یک الگوریتم جدید، اوه و همکارانش[13] یک الگوریتم کم‌وزن برای بررسی تطبیق امضاءها در مکانیزم تشخیص نفوذ مبتنی بر امضاء ارائه‌داده‌اند. این الگوریتم با دربرداشتن یک مکانیزم پَرِش نیاز به بررسی جزئی بخشی از داده‌ها را از میان می‌برد. الگوریتم ارائه‌شده از نظر پردازش و حافظه، نسبت به الگوریتم سنتی تطابق امضاء بهینه‌تر است. در جهت ارائه‌ی یک کاربرد جدید برای الگوریتم‌های موجود، بختیار و همکارانش[14] با توجه به وجود حملات انکار خدمت در حوزه‌ی سلامت هوشمند در اینترنت اشیاء، با استفاده از الگوریتم یادگیری ماشین J48، یک سیستم تشخیص نفوذ مناسب برای دستگاه‌هایی با ظرفیت کم برای مقابله با این حملات ارائه‌داده‌اند. همچنین لیو و همکارانش[15] یک روش تشخیص نفوذ بهینه با استفاد از الگوریتم خوشه‌بندی SFC[5]ارائه کرده‌اند که در این روش از الگوریتم PCA[6]برای کاهش ابعاد استفاده شده‌است. پاتل و جینوالا[16] نیز با استفاده از تکنولوژی زنجیره‌ی بلوکی[7] یک سیستم تشخیص نفوذ برای تشخیص حملات انکار خدمت در پروتکل مسریابی RPL معرفی کرده‌اند. در این روش، با توجه به محدودیت منابع، با استفاده از ریززنجیره[8] از یک زنجیره‌ی بلوکی بهینه از جنبه‌ی فضا استفاده شده‌است. درنهایت، در جهت ارائه‌ی یک ترکیب جدید از الگوریتم‌های موجود، پاریمالا و کایالویژی[17] با ارائه‌ی یک الگوریتم انتخاب ویژگی با استفاده از ترکیب دو الگوریتم CRF[9] و SMO[10]و همچنین استفاد از الگوریتم CNN[11]در یادگیری عمیق، به گفته‌ی خود، یک سیستم تشخیص نفوذ بهینه از نظر زمان و کارآمد از نظر دقت معرفی کرده‌اند.

در مسیر و دسته‌ی پژوهشی بعدی، جایگذاری بهینه‌ی سیستم‌های تشخیص نفوذ در لایه‌ی ادراکی اینترنت اشیاء، روش جایگذاری را می‌توان به سه روش متمرکز، توزیع‌شده، و ترکیبی تقسیم‌کرد. برای نمونه، کاسینثان و همکارانش[19][18] برای

[1] Project
[2] Partner
[3] Complementarity
[4] Complementarity Function
[5] Suppressed Fuzzy Clustering
[6] Principal Component Analysis
[7] Block Chain
[8] Microchain
[9] Conditional Random Field
[10] Spider Monkey Optimization
[11] Convolutional Neural Network

حل مشکل گره‌های کم‌توان، یک روش جایگذاری متمرکز را پیشنهاد داده‌اند که در آن سیستم تشخیص نفوذ در یک سیستم میزبان قدرتمند جایگذاری می‌شود به‌طوری که بخش حسگرهای تشخیصی این سیستم به‌صورت سیمی[1] در پهنه‌ی شبکه‌ی لایه‌ی ادراکی توزیع شده‌اند. همچنین آبهیشک و همکارانش[20] با قرار دادن مکانیزم تشخیص نفوذ خود در یک نقطه‌ی دسترسی[2] امن، سعی در شناسایی دروازه‌های[3] مخرب[4] در شبکه‌ی خوشه‌بندی‌شده‌ی اینترنت اشیاء داشته‌اند.[5] سادیکین و همکارانش[21] نیز با اتخاذ یک رویکرد متمرکز، یک سیستم تشخیص نفوذ ترکیبی (مبتنی بر امضاء و مبتنی بر ناهنجاری) در پروتکل زیگبی[6] ارائه داده‌اند. از جمله تلاش‌های صورت گرفته در این تحقیق استفاده از امکانات پروتکل زیگبی برای جمع‌آوری بهینه و امن داده‌های مورد نیاز سیستم تشخیص نفوذ است. اسکندری و همکارانش[22] با فرض اینکه پیاده‌سازی یک سیستم تشخیص نفوذ مبتنی بر امضاء در دستگاه‌هایی با محدودیت منابع کاری دشوار است، یک مکانیزم متمرکز مبتنی بر ناهنجاری معرفی کرده‌اند. در این سیستم از یک تکنیک طبقه‌بندی تک‌کلاسه کم‌وزن استفاده شده‌است. همچنین با پیاده‌سازی سیستم در یک سخت‌افزار Raspberry Pi 3، سیستم در دو سناریوی متمرکز ارزیابی شده‌است: قراردادن سیستم در دروازه‌ی شبکه و در یک دستگاه، جدای دستگاه‌های دیگر در شبکه. در مقابل، سروانتس و همکارانش[23] از رویکرد توزیع‌شده برای جایگذاری مکانیزم تشخیصی استفاده کرده‌اند به‌گونه‌ای که در آن وظایف برحسب ظرفیت هر گره به گره‌ها انتصاب می‌شود. آموری و همکارانش[24] نیز یک مکانیزم تشخیص نفوذ دولایه را ارائه‌داده‌اند، شامل لایه‌ی محلی[7] و سراسری؛[8] در لایه‌ی محلی، وظایف کم‌وزن تشخیص نفوذ توسط گره‌های کم‌وزن انجام می‌شود و سپس در لایه‌ی سراسری، داده‌های مورد نیاز به یک فراگره[9] برای انجام وظایف سنگین‌تر تشخیص نفوذ ارسال می‌شود. نکته‌ی دیگر این که در لایه‌ی محلی از الگوریتم کم‌وزن C4.5 برای طبقه‌بندی[10] استفاده شده‌است. ارشد و همکارانش[25] نیز از یک رویکرد همکارانه برای ارائه‌ی یک مکانیزم تشخیص نفوذ مقرون‌به‌صرفه در اینترنت اشیاء صنعتی[11] استفاده کرده‌اند. در چهارچوب ارائه‌شده، مکانیزم تشخیص نفوذ شامل مؤلفه‌ی سطح دستگاه و مؤلفه‌ی مسریاب است. مؤلفه‌ی سطح دستگاه که شامل دستگاه‌های اینترنت اشیاء است، وظیفه‌ی تشخیص در سطح دستگاه و همچنین نظارت بر اتفاقاتی را که در این سطح قابل مشاهده است برعهده دارد. در سوی دیگر مؤلفه‌ی مسریاب که در واقع مسریاب حاضر در شبکه است، وظیفه‌ی پردازش داده‌های جمع‌آوری‌شده توسط مؤلفه‌ی سطح دستگاه، اتخاذ تصمیم درباره‌ی مخرب یا غیرمخرب بودن اتفاقات مشاهده‌شده، و همچنین ارسال نتایج به دستگاه‌های اینترنت اشیاء را برعهده دارد. برخلاف دو جایگذاری پیشین، آمارال و همکارانش[26] از یک رویکردی میانی یا ترکیبی استفاده کرده‌اند که در آن گره‌های لایه‌ی ادراکی اینترنت اشیاء به خوشه‌های[12] مختلفی تقسیم‌بندی می‌شوند و در هر خوشه قدرتمندترین گره، مسئولیت تشخیص نفوذ در آن خوشه را به‌عهده‌دارد.

در مسیر و دسته‌ی پژوهشی بعدی، فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ در لایه‌ی ادراکی اینترنت اشیاء (که مسیر پژوهش ما نیز هست)، سدجلماسی و همکارانش[28][27] با مدل‌کردن ارتباط میان گره مدافع و حمله‌کننده در قالب یک بازی روشی را برای فعال‌سازی بهینه ارائه‌کرده‌اند. در این بازی، بازه‌ی زمانی به برش‌های کوچکی تقسیم می‌شود و مدافع تصمیم می‌گیرد که در کدام یک از این برش‌های زمانی سیستم تشخیص نفوذ خود را فعال کند. این مدل برای فعال‌سازی سیستم

[1] Wired
[2] Access Point
[3] Gateway
[4] Malicious
[5] در یک شبکه‌ی خوشه‌بندی شده‌ی اینترنت اشیاء، معمولا در هر خوشه یک گره با منابع بیشتر به عنوان دروازه برای ارتباط سایر گره‌ها با نقاط دیگر شبکه استفاده می‌شود.
[6] Zigbee
[7] Local
[8] Global
[9] Super Node
[10] Classification
[11] Industrial Internet of Things (IIoT)
[12] Clusters

تشخیص نفوذ مبتی‌بر ناهنجاری استفاده می‌شود و قسمت مبتنی‌بر امضاء این سیستم همواره فعال است. مدل پیشنهادی در یک جایگذاری توزیع‌شده‌ی سیستم‌های تشخیص نفوذ استفاده شده‌است. ژو و همکارانش[29] نیز، ارتباط میان گره مدافع و حمله‌کننده را در قالب یک بازی مدل کرده‌اند. در این مدل، گره مدافع در یک ظرف زمانی کلی، میان اینکه چه‌کسری مکانیزم مبتنی‌بر امضاء و چه‌کسری مکانیزم مبتنی بر ناهنجاری را فعال‌کند، تصمیم‌گیری می‌کند و هیچ‌گاه سیستم تشخیص نفوذ در گره مدافع غیرفعال نمی‌شود. مدل پیشنهادی در یک جایگذاری ترکیبی (یک شبکه‌ی خوشه‌بندی‌شده) استفاده‌شده‌است.

مسیر و دسته‌ی پژوهشی ما برای حل چالش منابع و مدیریت منابع در اینترنت اشیاء، از میان مسیرهای بیان‌شده، مانند دو پژوهش پیشین، فعال‌سازی بهینه و عقلانی سیستم‌های تشخیص نفوذ با استفاده از نظریه‌ی بازی است؛ یعنی با در نظرگرفتن درآمد حاصل از امنیت هنگام فعال‌سازی سیستم تشخیص نفوذ و هزینه‌ی وارد از مصرف منابع هنگام فعال‌سازی سیستم تشخیص نفوذ، دریابیم که سیستم‌های تشخیص نفوذ موجود در گره‌های شبکه را چگونه فعال‌سازی کنیم. در دو روش پیشین در این مسیر، تنها ارتباط میان گره مدافع و حمله‌کننده برای اتخاذ تصمیم درنظر گرفته‌شده‌است و در این مدل‌ها ارتباط میان گره‌های مدافع نادیده گرفته‌شده‌است. به باور ما در نظرگرفتن این ارتباطات در چنین موقعیت استراتژیکی برای اتخاذ تصمیم درست اهمیت دارد. ما در این پژوهش، برخلاف دو روش پیشین، مدلی را برای فعال‌سازی بهینه‌ی سیستم تشخیص نفوذ در اینترنت اشیاء ارائه‌کرده‌ایم که در آن ارتباط میان گره‌های مدافع در مقابل حمله‌کننده درنظر گرفته‌شده‌است.

4. مدل پیشنهادی

چنان‌که در بخش‌های پیشین گفتیم، مسئله‌ی ما در این پژوهش فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ یا به عبارت دیگر مدیریت منابع در تشخیص نفوذ در اینترنت اشیاء است. در روش پیشنهادی ما برای مدیریت منابع، ارتباطات میان گره‌های مدافع در قالب بازی مدل‌سازی شده‌اند. در این بخش، مدل پیشنهادی خود را ارائه‌کرده‌ایم.

در مدل ارائه‌شده که مدلی مبتنی بر بازی شراکت است، رابطه‌ی میان گره‌های مدافع در قالب یک بازی همکارانه[1]مدل شده‌است؛ با این فرض که برقراری امنیت در شبکه توسط یک گره مدافع، علاوه بر خود گره برای سایر گره‌های مدافع نیز سودمند است. یعنی تنها بخشی از درآمد حاصل از برقراری امنیت توسط یک گره مدافع برای خود اوست و باقی برای سایرین. چنان که اگر حمله‌کننده‌ای توسط یک گره مدافع شناسایی شود تمام گره‌های شبکه از جمله خود آن گره مدافع از آسیب آن حمله‌کننده مصون می‌شوند.

در مدل ارائه‌شده، گره‌های مدافع با درنظرگرفتن درآمد حاصل از برقراری امنیت، هزینه‌ی وارد از مصرف منابع، و همچنین با درنظرگرفتن رفتار سایر گره‌های مدافع در مدل پیشنهادی، درباره‌ی میزان فعال‌سازی سیستم تشخیص نفوذ خود تصمیم‌گیری می‌کنند. "میزان" در عبارت "میزان فعال‌سازی"، می‌تواند به میزان در ابعاد مختلفی دلالت داشته‌باشد. ملموس‌ترین این ابعاد بعد زمانی است؛ یعنی چه کسری از بازه‌ی زمانی سیستم تشخیص نفوذ فعال باشد. به عنوان مثال دیگر می‌توان به میزان تلاش برای تطبیق امضاءها در سیستم مبتنی بر امضاء اشاره کرد؛ یعنی چه کسری از پایگاه‌داده‌ی امضاءها بررسی شود.

در ادامه، به‌ترتیب، مدل پیشنهادی را توصیف و تعریف کرده‌ایم و سپس نحوه‌ی کاربست آن را در شبکه نیز بیان‌کرده‌ایم.

4-1. توصیف

در بازی شراکت یک پروژه مشترک و چند شریک وجوددارد. درآمدی که از تلاش هریک از شرکا حاصل می‌شود به درآمد کلی پروژه اختصاص دارد که هرکدام از شرکا سهم مشخصی از این درآمد دارند. درمقابل، هزینه‌ای که هر شریک برای این تلاش صرف می‌کند متوجه خود اوست. ما تشخیص نفوذ را پروژه مشترک و گره‌های مدافع را شریکان این پروژه در

[1]Cooperative

نظرگرفته‌ایم؛ با این فرض که کشف حمله به‌وسیله‌ی یک گره برای گره‌های دیگر و تمام شبکه سودمند خواهدبود.

در این مدل، هربازیکن مجموعه‌ای از میزان‌های ممکن برای فعال‌سازی سیستم تشخیص نفوذ خود را به عنوان مجموعه استراتژی‌های خود در اختیار دارد. درآمدی که هر بازیکن برای پروژه به ارمغان می‌آورد، با میزان فعال‌سازی سیستم و نرخ تشخیص[1]سیستم ارتباط مستقیم دارد. ارزش امنیت برقرارشده، به‌عنوان ضریب، مؤلفه‌ی دیگر تابع درآمد[2]بازیکن است. در سوی دیگر، هزینه‌ی هر بازیکن عبارت است از هزینه‌ی منابع مصرف‌شده توسط سیستم تشخیص نفوذ آن بازیکن که این هزینه با میزان فعال‌سازی سیستم رابطه دارد. البته هزینه در رابطه با میزان فعال‌سازی، می‌تواند به‌صورت غیر خطی تغییرکند. ارزش هزینه‌ی صرف‌شده برای امنیت، به‌عنوان ضریب، مؤلفه‌ی دیگر تابع هزینه‌ی[3]بازیکن است.

درآمد کلی پروژه برابر است با مجموع درآمدهای بازیکنان به‌علاوه‌ی ارزش افزوده‌ی همکاری بازیکنان درصورتی که بازی دارای ویژگی مکملیت[4]باشد. چگونگی این ارزش یا درآمد افزوده با تابع مکملیت مشخص می‌شود. در سوی دیگر، هزینه‌ی کلی پروژه برابر است با مجموع هزینه‌هایی که بازیکنان متحمل شده‌اند.

در نهایت، هربازیکن سهم مشخصی از درآمد کلی پروژه کسب می‌کند و هزینه‌ی صرف‌شده توسط خود بازیکن، از آن کاسته می‌شود که این مسئله با تابع سودمندی[5]بازیکن مشخص شده‌است. سودمندی کلی پروژه نیز عبارت است درآمد کلی پروژه با کاهش هزینه‌ی کلی پروژه از آن.

2-4. تعریف

در این بخش مدل پیشنهادی خود برمبنای بازی شراکت را تعریف کرده‌ایم. در ادامه عبارت "بازی" هم بر بازی و هم بر پروژه‌ی مشترک دلالت دارد و عبارت "بازیکن" هم بر بازیکن و هم بر شریک. حال عناصر این مدل را مرحله‌به‌مرحله بیان می‌کنیم:

1- $\boldsymbol{n}$ را به‌عنوان تعداد بازیکنان در نظر می‌گیریم.

2- برای هربازیکن $\boldsymbol{i}$:

$$E_i \subset \mathbb{R}^+ \cup \{0\} \quad (1)$$

$\boldsymbol{E_i}$ عبارت است از مجموعه‌ی سطوح مختلف تلاش (مجموعه استراتژی‌های بازیکن) که زیر مجموعه‌ای از اعداد حقیقی غیرمنفی است و

$$e_i \in E_i \quad (2)$$

$\boldsymbol{e_i}$ عبارت است از سطح تلاش انتخاب‌شده (استراتژی انتخاب‌شده) به‌وسیله‌ی بازیکن از مجموعه استراتژی‌های موجود.

3- برای بازی:

$$E = E_1 \times \dots \times E_n \quad (3)$$

$\boldsymbol{E}$ عبارت است از فضای استراتژی بازی (تمام تلاقی‌های ممکن استراتژی‌های تمامی بازیکنان) و

$$e = (e_1, \dots, e_n) \in E \quad (4)$$

$\boldsymbol{e}$ عبارت است از نمایه‌ی استراتژی بازی که نشانگر استراتژی‌های انتخاب‌شده به‌وسیله‌ی تمام بازیکنان است از میان تمام تلاقی‌های ممکن است.

4- برای هربازیکن $\boldsymbol{i}$:

$$r_i(e_i) = e_i A_i V_i^r \quad (5)$$

$\boldsymbol{r_i}$ عبارت است از تابع درآمد حاصل برای بازی به‌وسیله‌ی بازیکن که تابعی از استراتژی انتخاب‌شده‌ی بازیکن است و در آن $\boldsymbol{1 \geq A_i \geq 0}$ نرخ تشخیص گره و $\boldsymbol{V_i^r \geq 0}$ ارزش تشخیص نفوذ یا ضریب تابع درآمد است. همچنین

$$c_i(e_i) = v(e_i) V_i^c \quad (6)$$

$\boldsymbol{c_i}$ عبارت است از تابع هزینه‌ی بازیکن که تابعی از استراتژی انتخاب‌شده‌ی بازیکن است و در آن تغییرات هزینه با استفاده از

[1] Detection Rate . یعنی چه‌کسری از حملات موجود توسط سیستم تشخیص نفوذ شناسایی می‌شود.

[2] Revenue Function

[3] Cost Function

[4] ویژگی مکملیت بازی شراکت در بخش مفاهیم پایه بیان شده‌است.

[5] Utility Function

تابع $\boldsymbol{v(e_i)}$ به صورت تابع میزان مصرف مدل شده‌است[1] همچنین $\boldsymbol{V_i^c \geq 0}$ ارزش منابع مصرف‌شده یا ضریب تابع هزینه است.

5- برای بازی:

$$r(e) = \sum_{i=1}^{n} r_i(e_i) + f(e) \quad (7)$$

$\boldsymbol{r}$ عبارت است از درآمد کلی حاصل از تلاش تمام بازیکنان برای بازی که در آن تابع $\boldsymbol{f(e)}$ همان تابع مکملیت بازی است. همچنین

$$c(e) = \sum_{i=1}^{n} c_i(e_i) \quad (8)$$

$\boldsymbol{c}$ عبارت است از هزینه مجموعی که بازیکنان بازی متحمل شده‌اند.

6- برای هربازیکن $\boldsymbol{i}$:

$$l_i \in [0,1] \quad (9)$$

$\boldsymbol{l_i}$ سهم بازیکن از درآمد بازی است (یعنی چه کسری از درآمد کلی پروژه برای بازیکن است) و درنهایت

$$u_i(e) = l_i r(e) - c_i(e_i) \quad (10)$$

$\boldsymbol{u_i}$ عبارت است از تابع سودمندی بازیکن.

7- برای بازی:

$$l = (l_1, \dots, l_n) \in L \quad (11)$$

$\boldsymbol{l}$ عبارت است نمایه‌ی سهم[2]بازی که نمایشگر چگونگی سهم تمام بازیکنان است و

$$L = \{(l_1, \dots, l_n) | \sum_{i=1}^{n} l_i = 1\} \quad (12)$$

$\boldsymbol{L}$ عبارت است از فضای سهم[3]بازی که شامل تمام بردارهای $\boldsymbol{n}$تایی‌ست که حاصل جمع عناصر آن برابر با $\boldsymbol{1}$ است. در نهایت

$$u(e) = r(e) - c(e) \quad (13)$$

$\boldsymbol{u}$ عبارت است از تابع سودمندی بازی.

3-4. کاربست

در ادامه نحوه‌ی به‌کارگیری مدل ارائه‌شده را در شبکه‌ی اینترنت اشیاء، مرحله به مرحله بیان کرده‌ایم:

1- $\boldsymbol{N}$ را به عنوان مجموعه‌ی تمام گره‌های موجود در شبکه تعریف می‌کنیم.

2- $\boldsymbol{D}$ را به عنوان مجموعه‌ی تمام پروژه‌های مشترک تشخیص نفوذ تعریف می‌کنیم. هر پروژه مشترک نشانگر یک بازی‌ست. یعنی می‌توان پروژهای مشترک مختلفی با اهداف تشخیصی مختلف در یک شبکه تعریف کرد. برای مثال شبکه را به خوشه‌های مختلفی تقسیم می‌کنیم و برای هر خوشه یک پروژه مشترک تشخیص نفوذ یا به عبارت دیگر بازی جداگانه تعریف می‌کنیم.

3- تابع $\boldsymbol{assign}$ را به‌صورت زیر تعریف می‌کنیم:

$$assign: D \to (2^{N \times \mathbb{R}^{\geq 0} \times R \times C} \times F \times L) - \{\emptyset\} \quad (13)$$

که در آن $\boldsymbol{R}$ یعنی مجموعه توابع سود، $\boldsymbol{C}$ یعنی مجموعه توابع هزینه، $\boldsymbol{F}$ یعنی مجموعه توابع مکملیت، و $\boldsymbol{L}$ یعنی مجموعه‌ی تمام بردارهایی که جمع عناصر آن برابر با 1 است. درواقع، در این مرحله مشخص می‌کنیم در هر پروژه تشخیص نفوذ یا در هر بازی چه گره‌هایی از شبکه با چه استراتژی‌ها، چه تابع درآمد و چه تابع هزینه‌ای حضور دارند و همچنین برای پروژه، تابع مکملیت چگونه تعریف می‌شود و سهم هر بازیکن از درآمد پروژه چقدر است.

4- بازی‌ها را تحلیل می‌کنیم. در این مرحله تصمیم‌ها برای چگونگی فعال‌سازی سیستم تشخیص نفوذ اتخاذ می‌شود؛ با استفاده از تحلیل بازی با تئوری‌های عقلانیت و تعادل نش.

5. مطالعه‌ی موردی

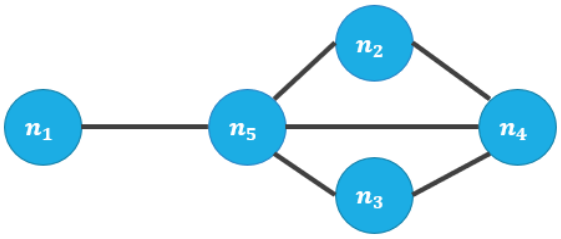
در این بخش چگونگی به‌کارگیری مدل ارائه‌شده و همچنین نتایج حاصل از آن در یک مطالعه‌ی موردی تشریح شده‌است. ابتدا چگونگی به‌کارگیری را بیان کرده‌ایم و سپس فاز ارزیابی به

[1] گاهی قیمت یک محصول با میزان مصرف تغییرمی‌کند، مانند تعرفه برق در ایران که شامل افزایش قیمت و همچنین تخفیف است. این مسئله را می‌توان به دو روش مدل کرد: تابع قیمت ($c_i(e_i) = e_i V_i^c(e_i)$) و تابع میزان مصرف ($c_i(e_i) = v(e_i)V_i^c$). برای مثال اگر قیمت دوبرابر شود از سوی دیگر می‌توان فرض کرد که گویی مصرف دوبرابر استنباط شده‌است.

[2] Lot Profile

[3] Lot Space

روش شبیه‌سازی انجام و ارائه شده‌است. شبکه‌ی مورد مطالعه از پنج گره تشکیل می‌شود که توپولوژی آن در شکل 2 نمایش داده‌شده‌است. در این شبکه، فرض کرده‌ایم که گره‌ها یکسان هستند. دیگر اینکه، در این مطالعه‌ی موردی میزان تلاش یا میزان فعال‌سازی سیستم تشخیص نفوذ در بعد زمانی مدنظر است؛ یعنی گره‌ها چه کسری از بازه‌ی زمانی، سیستم تشخیص نفوذ خود را فعال کنند.



شکل 2. توپولوژی شبکه‌ی مطالعه‌ی موردی

5-1. کاربست

کاربست مدل ارائه‌شده و نتایج حاصل به شرح زیر است:

مرحله‌ی اول) $\boldsymbol{N = \{n_1, n_2, n_3, n_4, n_5\}}$ را به عنوان مجموعه‌ی تمام گره‌های شبکه تعریف می‌کنیم.

مرحله‌ی دوم) $\boldsymbol{D = \{d_1, d_2, d_3, d_4, d_5\}}$ را به عنوان مجموعه‌ی تمام پروژه‌های تشخیص نفوذ در شبکه تعریف می‌کنیم به طوری که $\boldsymbol{d_i}$ عبارت است از تشخیص نفوذ علیه $\boldsymbol{n_i}$.

مرحله‌ی سوم) برای هر $\boldsymbol{d_i}$ داریم:

1. بازیکنان، گره‌های همسایه‌ی $\boldsymbol{n_i}$ هستند.
2. برای هر گره $\boldsymbol{j}$: $\boldsymbol{E_j = [0,1]}$، $\boldsymbol{V_j^r = V^r}$، $\boldsymbol{V_j^c = V^c}$، $\boldsymbol{A_j = A}$ و $\boldsymbol{l_j = 1/n}$ برقرار است که $\boldsymbol{n}$ نمایشگر تعداد بازیکنان بازی است (فرض یکسان بودن گره‌ها). توجه کنید که در $\boldsymbol{E_j = [0,1]}$، $\boldsymbol{0}$ نشان‌دهنده‌ی حداقل تلاش و $\boldsymbol{1}$ نشان‌دهنده‌ی حداکثر تلاش است. برای مثال اگر گرهی استراتژی $\boldsymbol{0.5}$ را انتخاب کند باید در نیمی از مواقع مکانیزم تشخیص نفوذ خود را فعال کند یا به عبارت دیگر با احتمال $\boldsymbol{0.5}$ تشخیص نفوذ انجام دهد.
3. تابع میزان مصرف را به صورت زیر تعریف می‌کنیم (شکل 3):

$$v(e_i) = (2e_i)^2/2 \quad (10)$$

در این تابع، بازیکن در مصرف پایین (نیمه‌ی اول تابع) مشمول تخفیف می‌شود و در مصرف بالا (نیمه‌ی دوم تابع) مشمول جریمه (هزینه‌ی اضافه). نقطه‌ی میانی تابع نقطه‌ای است که بازیکن نه مشمول تخفیف و نه مشمول جریمه است.

4. تابع مکملیت را به صورت زیر تعریف می‌کنیم:

$$f(e) = 0 \quad (11)$$

یعنی فرض کرده‌ایم که بازی فاقد ویژگی مکملیت است.

(توجه کنید که مرحله‌ی سوم همان مرحله‌ی تعریف تابع $\boldsymbol{assign}$ است.)

مرحله‌ی چهارم) برای هر $\boldsymbol{d_i}$، پس از تحلیل، نتایج زیر حاصل شده‌اند:

1. نقطه‌ی تعادل بازی عبارت است از:

$$e^* = \left(\frac{AV^r}{4nV^c}, \dots, \frac{AV^r}{4nV^c}\right) \quad (12)$$

2. اگر بازیکنان بر بیشینگی تابع سودمندی پروژه قرارداد کنند، نقطه‌ی قرداد بازی عبارت است از:

$$e^c = \left(\frac{AV^r}{4V^c}, \dots, \frac{AV^r}{4V^c}\right) \quad (13)$$

3. احتمال میانگین تشخیص تک‌حمله در بازی عبارت است از:

$$\bar{p}_d = \frac{A\sum_{i=1}^{n} e_i}{n} \quad (14)$$

4. هزینه‌ی منابع در بازی عبارت است از:

$$c_e = \sum_{i=1}^{n} c_i(e_i) \quad (15)$$

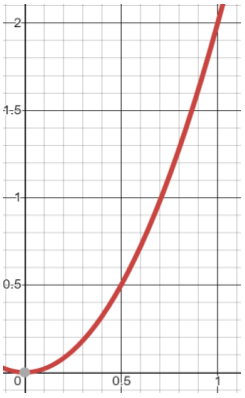
5. با در نظرگرفتن $\boldsymbol{\bar{p}_d^a}$، $\boldsymbol{\bar{p}_d^*}$ و $\boldsymbol{\bar{p}_d^c}$ به‌عنوان احتمال تشخیص تک‌حمله زمانی که گره‌ها به‌ترتیب نقطه‌ی بیشینه‌ی فعال‌سازی، نقطه‌ی تعادل، و نقطه‌ی قرارداد را بازی می‌کنند، داریم $\boldsymbol{\bar{p}_d^* \leq \bar{p}_d^a}$ و $\boldsymbol{\bar{p}_d^c \leq \bar{p}_d^a}$.

6. با در نظرگرفتن c_e^c، c_e^*، و c_e^a به‌عنوان هزینه‌ی منابع زمانی که گره‌ها به‌ترتیب نقطه‌ی بیشینه‌ی فعال‌سازی، نقطه‌ی تعادل، و نقطه‌ی قرارداد را بازی می‌کنند، داریم $c_e^* \le c_e^c \le c_e^a$.
7. همچنین می‌توان با فرض این مسئله که گره‌ها نقطه‌ی تعادل را بازی می‌کنند، تابع سودمندی پروژه را با تنظیم نمایه‌ی سهم ($l = (l_1, l_2, \dots, l_n)$) بیشینه کرد:

$$u(l) = \frac{V^r A}{n}\sum_{i=1}^{n} e_i^*(l_i) - \frac{V^c}{2}\sum_{i=1}^{n}\left(2e_i^*(l_i)\right)^2 \quad (16)$$

که در آن:

$$e_i^*(l_i) = \frac{l_i A V^r}{4V^c} \quad (17)$$



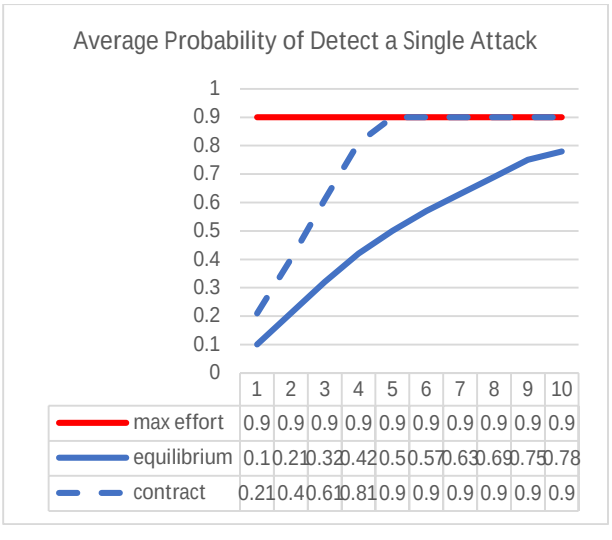
شکل 3. تابع میزان مصرف: توجه‌کنید که مصرف‌کننده در نقطه‌ی میانی (0,5) به همان مقدار که مصرف کرده‌است هزینه می‌پردازد و نیمه‌ی پیش از آن (0 تا 0,5) بازه‌ی تخفیف و نیمه‌ی پس از آن (0,5 تا 1) بازه‌ی جریمه است.

5-2. ارزیابی

برای شبیه‌سازی مدل‌های ارائه‌شده در مطالعه‌ی موردی از یک برنامه‌ی توسعه‌داده‌شده با زبان برنامه‌نویسی پایتون[1] استفاده کرده‌ایم. فرآیند شبیه‌سازی 50000 بار تکرار می‌شود و هر بار تا زمانی ادامه پیدا می‌کند که گره حمله‌کننده شناسایی شود. در هر بار به طور تصادفی (با احتمال 0,2 برای هرگره) یک گره از میان پنج گره شبکه به عنوان حمله‌کننده انتخاب می‌شود. گره‌ها با احتمال 0,5 تصمیم می‌گیرند که آیا به همسایگان خود بسته ارسال کنند یا خیر و همچنین حمله‌کننده با احتمال 0,5 تصمیم می‌گیرد که آیا حمله انجام دهد یا خیر.

در شکل‌های 4، 5، 6 و 7 نتایج استراتژی بازیکنان در هر یک از حالت‌های بازی حداکثر تلاش، بازی تعادل، و بازی قرداد، با فرض $V^c = 1$ و $A = 0.9$ و تغییر V^r نمایش داده شده‌است؛ به‌ترتیب از جنبه‌های احتمال میانگین تشخیص تک‌حمله، هزینه‌ی منابع، شناسایی حمله‌کننده در چندمین حمله، و نسبت سود به هزینه. یعنی در شرایطی که نرخ تشخیص گره‌ها 90 درصد است و ضریب تابع هزینه یا ارزش منابع 1، با تغییر ضریب تابع درآمد یا ارزش امنیت، یا به عبارت دیگر با تغییر نسبت ارزش منابع به ارزش امنیت، حالت‌ها را با یکدیگر مقایسه کرده‌ایم.

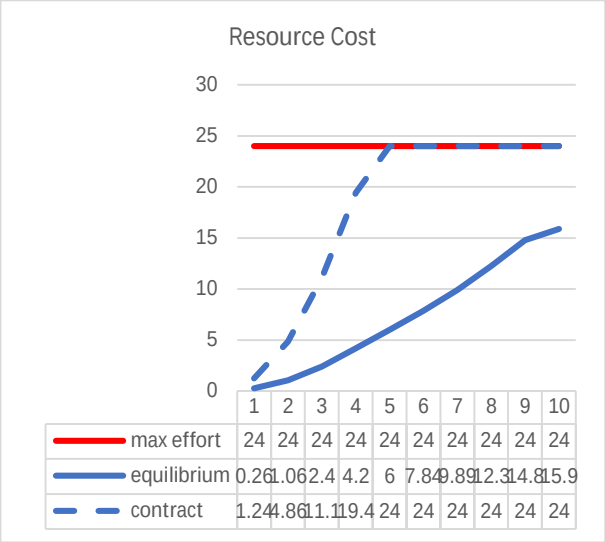
چنان که در شکل 4 مشاهده می‌کنید، از جنبه‌ی احتمال میانگین تشخیص تک‌حمله، همواره قرارداد بهتر از تعادل عمل می‌کند. همچنین با افزایش ارزش امنیت نسبت به ارزش هزینه (مانند شبکه‌هایی که امنیت در آن‌ها بحرانی است)، این احتمال در هر دو حالت افزایش میابد.



شکل 4. احتمال میانگین تشخیص تک‌حمله با فرض $V^c = 1$ و $A = 0.9$، و با تغییر V^r.

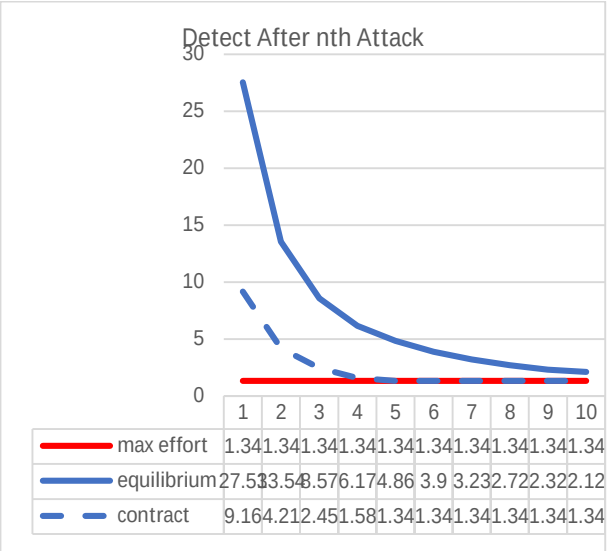
[1] Python

چنان که در شکل 5 مشاهده می‌کنید، از جنبه‌ی هزینه‌ی منابع، همواره قرارداد بدتر از تعادل عمل می‌کند. همچنین با افزایش ارزش امنیت نسبت به ارزش هزینه، این هزینه در هر دو حالت افزایش میابد.



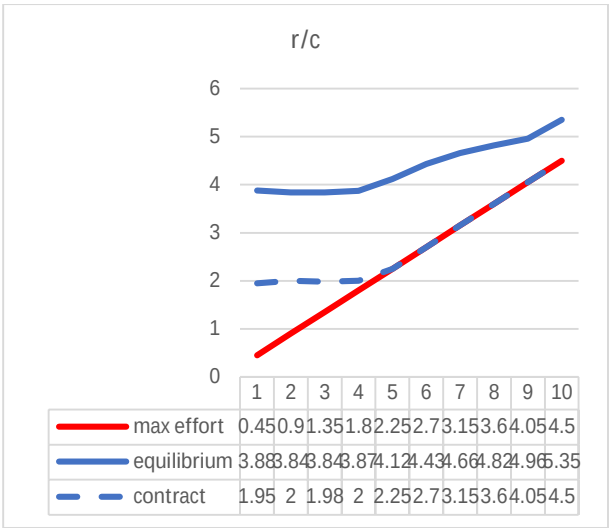
شکل 5. هزینه‌ی منابع با فرض $V^c = 1$ و $A = 0.9$، و با تغییر V^r.

با توجه به شکل 6، از جنبه‌ی سرعت شناسایی حمله‌کننده، قرارداد همواره بهتر از تعادل عمل‌می‌کند. همچنین با افزایش ارزش امنیت نسبت به ارزش هزینه، این سرعت در هر دو حالت افزایش میابد.



شکل 6. شناسایی حمله‌کننده در چندمین حمله با فرض $V^c = 1$ و $A = 0.9$، و با تغییر V^r.

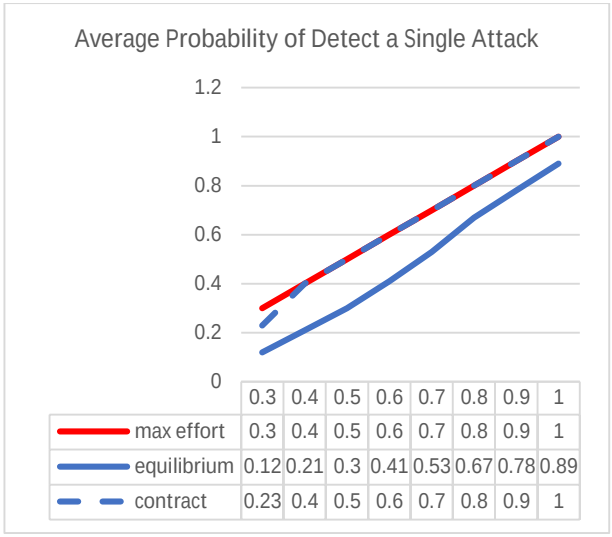
با توجه به شکل 7، از جنبه‌ی نسبت سود به هزینه، قرارداد همواره بدتر از تعادل عمل می‌کند. همچنین با افزایش ارزش امنیت نسبت به ارزش هزینه، این نسبت در هر دو حالت افزایش میابد.



شکل 7. نسبت سود به هزینه با فرض $V^c = 1$ و $A = 0.9$، و با تغییر V^r.

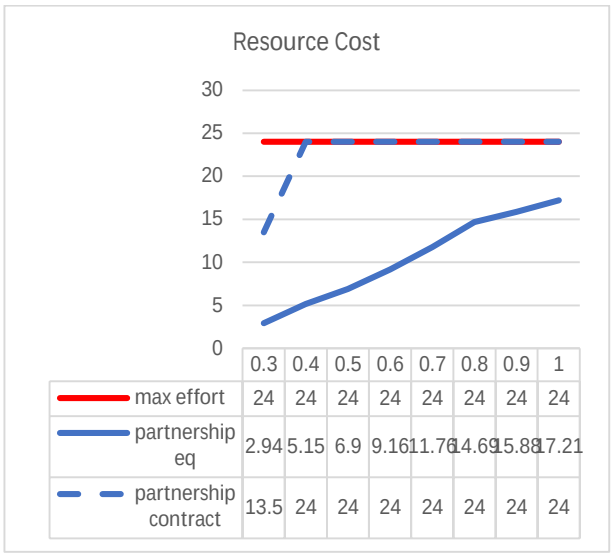
در شکل‌های 8، 9، 10 و 11 نتایج استراتژی بازیکنان در هر یک از حالت‌های بازی حداکثر تلاش، بازی تعادل، و بازی قرداد با فرض $\boldsymbol{V^c = 1}$ و $\boldsymbol{V^r = 10}$ و تغییر $\boldsymbol{A}$ نمایش داده شده‌است؛ به‌ترتیب از جنبه‌های احتمال میانگین تشخیص تک‌حمله، هزینه‌ی منابع، شناسایی حمله‌کننده در چندمین حمله، و نسبت سود به هزینه. یعنی در شرایطی که نسبت ارزش امنیت به ارزش منابع 10 به 1 است، با تغییر نرخ تشخیص گره‌ها حالت‌ها را با یکدیگر مقایسه کرده‌ایم.

چنان که در شکل 8 مشاهده می‌کنید، از جنبه‌ی احتمال میانگین تشخیص تک‌حمله، همواره قرارداد بهتر از تعادل عمل می‌کند. همچنین با افزایش نرخ تشخیص (یعنی زمانی که نرخ تشخیص سیستم‌های تشخیص نفوذ بالا است)، این احتمال در هر دو حالت افزایش میابد.



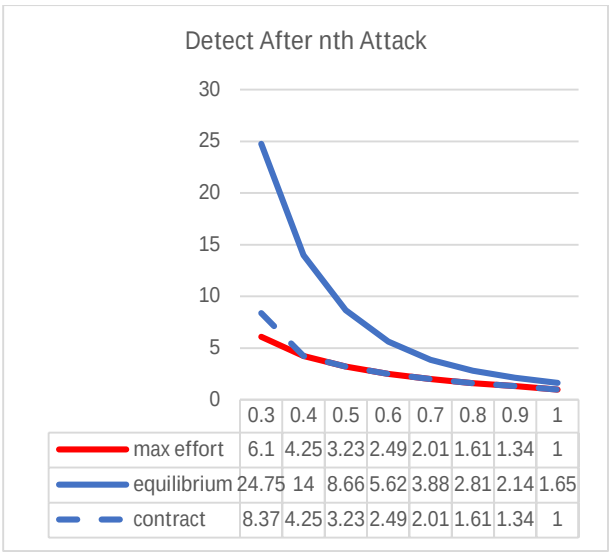
شکل 8. احتمال میانگین تشخیص تک‌حمله با فرض $V^c = 1$ و $V^r = 10$، و با تغییر A.

چنان که در شکل 9 مشاهده می‌کنید، از جنبه‌ی هزینه‌ی منابع، همواره قرارداد بدتر از تعادل عمل می‌کند. همچنین با افزایش نرخ تشخیص، این هزینه در هر دو حالت افزایش میابد.



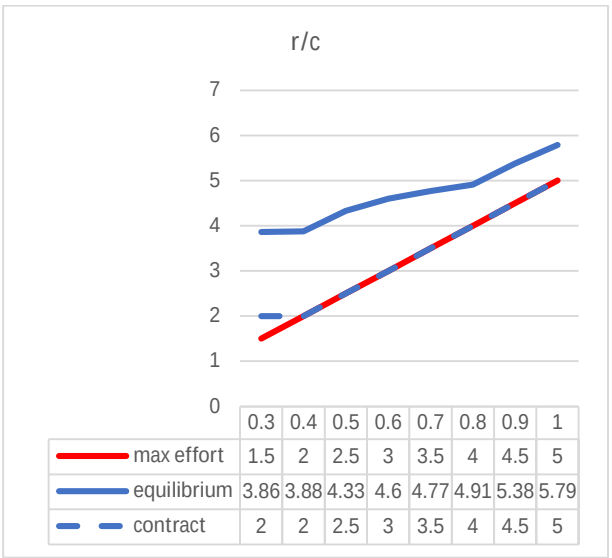
شکل 9. هزینه‌ی منابع با فرض $V^c = 1$ و $V^r = 10$، و با تغییر A.

با توجه به شکل 10، از جنبه‌ی سرعت شناسایی حمله‌کننده، قرارداد همواره بهتر از تعادل عمل می‌کند. همچنین با افزایش نرخ تشخیص، این سرعت در هر دو حالت افزایش میابد.



شکل 10. شناسایی حمله‌کننده در چندمین حمله با فرض $V^c = 1$ و $V^r = 10$، و با تغییر A.

با توجه به شکل 11، از جنبه‌ی نسبت سود به هزینه، قرارداد همواره بدتر از تعادل عمل می‌کند. همچنین با افزایش نرخ تشخیص، این نسبت در هر دو حالت افزایش میابد.



شکل 11. نسبت سود به هزینه با فرض $V^c = 1$ و $V^r = 10$، و با تغییر A.

برای لمس بیشتر کارکرد مدل ارائه‌شده می‌توان به این مثال اشاره کرد: فرض کنید ارزش امنیت ده برابر ارزش هزینه‌ی منابع باشد (مثلا $\boldsymbol{V^c = 1}$ و $\boldsymbol{V^r = 10}$) و هچنین نرخ تشخیص سیستم‌های تشخیص نفوذ در گره‌های مدافع 90 درصد باشد

($A = 0.9$). در چنین وضعیتی می‌بینیم که این مدل با کاهش 34 درصدی هزینه‌ی منابع، به احتمال میانگین تشخیص تک‌حمله‌ی 0,78 می‌رسد (کاهش 12 درصدی) و به طور میانگین با 0,8 حمله دیرتر از حالتی که گره‌ها همواره سیستم تشخیص نفوذ خود را فعال می‌کنند، حمله‌کننده شناسایی می‌شود.

6. مقایسه با کارهای پیشین

چنان که پیشتر نیز بیان شد، اصلی‌ترین تفاوت مدل ارائه‌شده با کارهای پیشین در زمینه‌ی فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ در اینترنت اشیاء این است که در تحقیقات پیشین همواره بازی در رابطه‌ی میان یک تک‌گره مدافع و یک حمله‌کننده برقرار بود اما در مدلی که ارائه‌داده‌ایم بازی میان گره‌های مدافع در برابر حمله‌کننده برقرار است. مدل ارائه‌شده برخلاف مدل‌های پیشین، یک واقعیت دیگر موجود در شبکه را، یعنی رابطه‌ی میان مدافعان را که در تشخیص نفوذ اهمیت دارد مدنظر قرارداده‌است.

در تحقیقات پیشین، حمله‌کننده به‌صورت صریح[1] در بازی حضور دارد؛ یعنی رفتار یا استراتژی‌های حمله‌کننده به‌عنوان یک بازیکن در بازی مدل شده‌است. اما در مدل ما نقش حمله‌کننده ضمنی[2] است؛ یعنی حمله‌کننده به‌عنوان یک بازیکن در بازی مطرح نیست. بلکه ما فرضی درباره‌ی رفتار حمله‌کننده داریم (چنان‌که در بخش ارزیابی دیدیم) و نقش حمله‌کننده یا حمله‌کنندگان، یا به‌طورکلی حمله، با تعریف پروژه‌های تشخیص نفوذ در کاربست مدل مدنظر قرارگرفته‌است.

سدجلماسی و همکارانش[28][27]، بازی را برروی سیستم تشخیص نفوذ مبتنی‌بر ناهنجاری به‌کارگرفته‌اند و ژو و همکارانش[29] برروی سیستم تشخیص نفوذ مبتنی‌بر امضاء و مبتنی‌بر ناهنجاری به طور همزمان. اما در مدل ما این آزادی وجوددارد که با تعریف پروژه‌های تشخیص نفوذ مختلف، بازی‌ها را به‌طور جداگانه برروی مکانیزم‌های تشخیص نفوذ مختلف، حملات مختلف، و حتی خوشه‌های مختلف شبکه به طور دیگرگون به‌کار گرفت. چنان‌که می‌دانیم، ممکن است مکانیزم‌های تشخیص نفوذ مختلفی برای شرایط مختلف شبکه، خوشه‌های مختلف شبکه، یا حتی حملات مختلف شبکه به‌کار گرفته‌شود که ویژگی ناهمگونی اینترنت اشیاء این مسئله را پررنگ‌تر نیز می‌کند. به طور خلاصه، یعنی از جمله ویژگی‌های مدلی که ارائه کرده‌ایم، برخلاف کارهای پیشین، حمایت از ویژگی ناهمگونی اینترنت اشیاء است که می‌توان با توجه به شرایطی که هر شبکه اینترنت اشیاء یا حتی هر بخش از شبکه‌ی اینترنت اشیاء دارد، بازی متناسب با آن را تعریف نمود.

ازجمله تفاوت‌های دیگر این است که، در مدل سدجلماسی و همکارانش[28][27]، میزان فعال‌سازی سیستم تشخیص نفوذ به‌وسیله‌ی گره از پیش مشخص است و راهبردی برای تعیین این میزان مشخص نشده‌است و تنها بازی به این که چه زمانی این فعال‌سازی انجام شود کمک می‌کند. همچنین در مدل ژو و همکارانش[29]، میزان فعال‌سازی مکانیزم تشخیص نفوذ، به‌طورکلی، "همواره" است و سیستم تشخیص نفوذ گره هیچ‌گاه خاموش نمی‌شود و تنها سهم دو نوع سیستم تشخیص نفوذ مبتنی‌بر ناهنجاری و مبتنی‌بر امضاء از میزان فعال‌سازی کلی مشخص می‌شود. اما در مدل ما، برخلاف دو مدل پیشین، بازی، میزان را به گره‌ها پیشنهاد می‌دهد.

به‌عنوان تفاوت آخر می‌توان به این نکته اشاره‌کرد که در مدل‌های پیشین تکیه‌ی بهینه‌سازی فعال‌سازی برروی بعد زمان است اما در مدلی که ما ارائه‌داده‌ایم تلاش گره علاوه بر میزان فعال‌سازی از نظر زمانی می‌تواند بر مسائل و ابعاد دیگری مانند فضای حافظه دلالت داشته باشد؛ برای نمونه میزان بررسی تطابق امضاءها از پایگاه‌داده امضاء (اینکه چه بخشی از پایگاه‌داده بررسی شود) در سیستم‌های تشخیص نفوذ مبتنی‌بر امضاء. چنان‌که می‌دانیم تنها منابع انرژی در اینترنت اشیاء چالش‌برانگیز نیست و منابع دیگری نیز مانند حافظه و منابع پردازشی مورد بحث است (نظر به وجود گره‌هایی با ظرفیت پایین در اینترنت اشیاء). به‌طور خلاصه، ما در مدل خود، برخلاف مدل‌های پیشین، نظر جامع‌تری نسبت به منابع داشته‌ایم.

خلاصه‌ای از مقایسه‌های بیان‌شده در جدول 1 قابل مشاهده است.

[1] Explicit

[2] Implicit

جدول 1 – مقایسه‌ی مدل ارائه‌شده با کارهای پیشین

	Attacker as a Player	Attacker role	Relation between Defenders	Handling Heterogeneity	Enabling Amount	Dimension
Our Proposed Models	No	Implicit	Concern	High	Model Suggestion	Time and Anything Else
H. Sedjelmaci et al. [27][28]	Yes	Explicit	Ignored	Low	Predefined	Time
M. Zhou et al. [29]	Yes	Explicit	Ignored	Low	Totally Predefined (Max) But Model Suggest Share	Time

7. نتایج

در این پژوهش، در ابتدا تشریح کردیم که یکی از اصلی‌ترین موانع امنیت و بخصوص به‌کارگیری سیستم‌های تشخیص نفوذ در اینترنت اشیاء، چالش منابع یعنی گره‌هایی با منابع کم و همچنین مصرف بالای منابع است. سپس بیان کردیم، پژوهش‌هایی که در جهت رفع این چالش کوشیده‌اند، طرق مختلفی را گزیده‌اند مانند ارائه‌ی الگوریتم‌های بهینه، جایگذاری بهینه‌ی سیستم‌های تشخیص نفوذ در شبکه‌ی اینترنت اشیاء، و فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ. با بررسی تحقیقات انجام‌شده در مسیر فعال‌سازی بهینه، نشان دادیم که رابطه‌ی میان گره‌های مدافع در مدل‌های ارائه‌شده مغفول است. در ادامه با ارائه‌ی مدلی مبتنی‌بر بازی شراکت سعی کردیم با درنظرگرفتن ارتباط میان گره‌های مدافع، سیستم‌های تشخیص نفوذ را به طور بهینه فعال‌سازی کنیم. سپس مدل ارائه‌شده را در یک مطالعه‌ی موردی شبیه‌سازی و نتایج را بررسی کردیم. دیدیم که در مدل ارائه‌شده، گره‌ها می‌توانند با درنظرگرفتن درآمد حاصل از برقراری امنیت، هزینه‌ی وارد از مصرف منابع، و همچنین با درنظرگرفتن رفتار دیگر گره‌های مدافع تصمیم عقلانی درباره‌ی میزان فعال‌سازی سیستم تشخیص نفوذ خود اتخاذکنند. درنهایت نیز تفاوت‌های مدل ارائه‌شده با مدل‌های پیشین بررسی شد.

8. مراجع

[1] K. L. Lueth, “IoT Basics: Getting Started with the Internet of Things,” 2015. Available: https://iot-analytics.com/product/whitepaper-iot-basics-getting-started-with-the-internet-of-things/

[2] F. Khodadadi, A.V. Dastjerdi, and R. Buyya, “Internet of Things: An Overview,” *in Internet of Things Principles and Paradigms*, pp. 3-28, 2016.

[3] M. Marjani, F. Nasaruddin, A. Gani, A. Karim, I. A. T. Hashem, A. Siddiqa, and I. Yaqoob, “Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges,”, *IEEE Access*, vol. 5, pp. 5247-5261, 2017.

[4] A. Čolaković, and M. Hadžialić, “Internet of Things (IoT): A Review of Enabling Technologies, Challenges, and Open Research Issues,” *Computer Networks*, vol. 144, 2018.

[5] F. A. Alaba, M. Othman, I. A. T. Hashema, and F. Alotaibib. “Internet of Things security: A survey,” *Network and Computer Applications*, vol. 88, pp. 10-28, 2017.

[6] M. Ge, H. Bangui, and B. Buhnova, “Big Data for Internet of Things: A Survey,” *Future Generation Computer Systems*, vol. 87, pp. 601-614, 2018.

[7] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A Survey of Intrusion Detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25-37, 2017.
[8] E. Dubrova, "Fault-Tolerant Design," *Springer*, 2013.
[9] L. Santos, C. Rabadão, and R. Gonçalves, "Intrusion Detection Systems in Internet of Things: A Literature Review," *in 13th Iberian Conference on Information Systems and Technologies (CISTI)*, 2018.
[10] E. Benkhelifa, T. Welsh, and W. Hamouda, "A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Towards Universal and Resilient Systems," *IEEE Communications Surveys & Tutorials*, vol. 20, pp. 3496-3509, 2018.
[11] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion Detection Systems For IoT-based Smart Environments: A Survey," *Journal of Cloud Computing*, 2018.
[12] J. Watson, "Strategy: An Introduction to Game Theory," *W. W. Norton & Company*, 2013.
[13] D. Oh, D. Kim, and W. W. Ro, "A Malicious Pattern Detection Engine for Embedded Security Systems in the Internet of Things," *Sensors*, 2014.
[14] F. A. Bakhtiar, E. S. Pramukantoro, and H. Nihri, "A Lightweight IDS Based on J48 Algorithm for Detecting DoS Attacks on IoT Middleware," *in 2019 IEEE 1st Global Conference on Life Sciences and Technologies (LifeTech 2019)*, 2019.
[15] L. Liu, B. Xu, X. Zhang, and X. Wu, "An Intrusion Detection Method for Internet of Things Based on Suppressed Fuzzy Clustering," *EURASIP Journal on Wireless Communications and Networking*, 2018.
[16] H. B. Patel, and D. C. Jinwala, "6MID: Mircochain Based Intrusion Detection for 6LoWPAN Based IoT Networks," *Procedia Computer Science*, vol. 184, pp. 929-934, 2021.
[17] G. Parimala, and R. Kayalvizhi, "An Effective Intrusion Detection System for Securing IoT Using Feature Selection and Deep Learning," *in 2021 International Conference on Computer Communication and Informatics (ICCCI)*, 2021.
[18] P. Kasinathan, C. Pastrone, M. Spirito, and M. Vinkovits, "Denial-of-Service Detection in 6LoWPAN Based Internet of Things," *in 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 600–607, 2013.
[19] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "DEMO: An IDS Framework for Internet of Things Empowered by 6LoWPAN," *in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, pp. 1337–1340, 2013.
[20] N. V. Abhishek, T. J. Lim, B. Sikdar, and A. Tandon, "An Intrusion Detection System for Detecting Compromised Gateways in Clustered IoT Networks," *in 2018 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*, 2018.
[21] F. Sadikin, T. V. Deursen, and S. Kumar, "A Hybrid Zigbee IoT Intrusion Detection System Using Secure and Efficient Data Collection," *Internet of Things*, vol. 12, 2020.
[22] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An Intelligent Anomaly Based Intrusion Detection System for IoT Edge Devices," *IEEE Internet of Things Journal*, vol. 7, pp. 6882-6897, 2020.
[23] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of Sinkhole Attacks for Supporting Secure Routing on 6lowpan for Internet of Things," *in 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 606–611, 2015.
[24] A. Amouri, V. T. Alaparthy, and S. D. Morgera, "Cross Layer-based Intrusion Detection Based on Network Behavior for IoT," *in 2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON)*, 2018.
[25] J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, "An Intrusion Detection Framework for Energy Constrained IoT Devices," *Mechanical Systems and Signal Processing*, vol. 136, 2020.
[26] J. Amaral, L. Oliveira, J. Rodrigues, G. Han, and L. Shu, "Policy and Network-based Intrusion Detection System for IPv6-enabled Wireless Sensor Networks," *in 2014 IEEE International Conference on Communications (ICC)*, pp. 1796–1801, 2014.
[27] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, "A Lightweight Anomaly Detection Technique for LowResource IoT Devices: A Game-Theoretic Methodology," *in IEEE ICC 2016 - Mobile and Wireless Networking Symposium*, 2016.
[28] H. Sedjelmaci, S. M. Senouci, and T. Taleb, "An Accurate Security Game for Low-Resource IoT Devices," *in IEEE Transactions on Vehicular Technology*, 2017.
[29] M. Zhou, L. Han, H. Lu, and C. Fu, "Intrusion Detection System for IoT Heterogeneous Perceptual Network Based on Game Theory," *in International Conference on Security and Privacy in New Computing Environments*, 2019.