

## مدلی برای تشخیص نفوذ در اینترنت اشیاء با استفاده از بازی شراکت

علی سلیمی<sup>۱</sup>، مجید غیوری<sup>۲</sup> ثالث<sup>۲</sup>

تاریخ پذیرش: 1400/09/17

تاریخ دریافت: 1400/05/12

### 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 در نظر گرفته نمی‌شود. به باور ما، در نظر گرفتن ارتباطات میان مدافعین برای اتخاذ تصمیم عقلانی اهمیت دارد. ما در این پژوهش، به منظور 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 در نظر گرفتن 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

<sup>۱</sup> دانشجوی کارشناسی‌ارشد، دانشگاه جامع امام حسین (ع)، [alisalimi@ihu.ac.ir](mailto:alisalimi@ihu.ac.ir)

<sup>۲</sup> استادیار دانشکده‌ی کامپیوتر و قدرت سایبری، دانشگاه جامع امام حسین (ع)، [ghayoori@ihu.ac.ir](mailto:ghayoori@ihu.ac.ir)

نویسنده‌ی مسئول: مجید غیوری ثالث

## 1. مقدمه

مملو است از دستگاه‌هایی با ظرفیت پایین<sup>15</sup> 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 اشیا است. چنین شرایطی یک شبکه‌ی کم‌توان و پراتلاف<sup>16</sup> را نتیجه‌می‌دهد که استفاده از روش‌های پیشین تأمین امنیت موجود در شبکه‌های قراردادی<sup>17</sup> 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<sup>18</sup> در کنار مفاهیم دیگری چون دیوار آتش و رمزنگاری، یکی از راه‌حل‌های برقراری امنیت در شبکه‌های کامپیوتری است. اما چنان که بیان شد، چالش منابع، نیاز به سیستم‌ها، مدل‌ها و نگرش‌های تشخیص نفوذ جدیدی را در اینترنت اشیا مطرح می‌کند. در واقع مسئله این است که چگونه با مصرف معقول‌تر منابع کار تشخیص نفوذ را انجام دهیم. تلاش‌های بسیاری از سوی محققین برای انطباق و ارائه‌ی سیستم‌های تشخیص نفوذی<sup>19</sup> متناسب با نیازمندی‌ها و شرایط اینترنت اشیا ارائه‌شده است. این تلاش‌ها را می‌توان به شاخه‌های مختلفی تقسیم‌بندی کرد، از جمله: تلاش در جهت بهینه‌سازی سخت‌افزار و منابع انرژی، ارائه‌ی الگوریتم‌های کم‌وزن برای تشخیص نفوذ، جایگذاری بهینه‌ی سیستم‌های تشخیص نفوذ در لایه‌ی ادراکی اینترنت اشیا، و فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ.

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

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

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

به دلیل خصوصیت ویژه‌ی اینترنت اشیا که با جهان فیزیکی ارتباط و تبادل تنگاتنگی دارد و همچنین ویژگی همه‌جاحاضری<sup>12</sup> این شبکه و نیاز به استفاده‌ی گسترده از دستگاه‌های تعبیه‌شده با حسگرها<sup>13</sup> و عملگرها<sup>14</sup>، اینترنت اشیا

<sup>1</sup> Perceptual Layer 1

<sup>2</sup> Ubiquitous 2

<sup>3</sup> Sensor 3

<sup>4</sup> Actuator 4

<sup>5</sup> Low-weight Devices 5

<sup>6</sup> Low-power and Lossy Network (LLN) 6

<sup>7</sup> Conventional Networks 7

<sup>8</sup> Intrusion Detection 8

<sup>9</sup> Intrusion Detection System (IDS) 9

<sup>1</sup> Internet of Thing

<sup>2</sup> Kevin Ashton

<sup>3</sup> Procter&Gamble

<sup>4</sup> Hardware Threats

<sup>5</sup> Network Threats

<sup>6</sup> Smart Application Threat

<sup>7</sup> Denial of Serviv (DoS)

<sup>8</sup> Eavesdropping

<sup>9</sup> Counterfeiting

<sup>1</sup> Heterogeneity

مدلی برای تشخیص نفوذ در اینترنت اشیا با استفاده از بازی شراکت

## 2. مفاهیم پایه

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

### 2-1. اینترنت اشیا

تاکنون برای اینترنت اشیا تعاریف متعدد و متنوعی بیان شده‌است. اما پیش از نقل قول این تعاریف باید یادآور این نکته شد که عبارت "اینترنت اشیا" به خودی خود نکات مهمی را درباره‌ی چیستی این مفهوم روشن می‌کند. نکته‌ی اول قابل برداشت این است که اینترنت اشیا 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 پی برد که یک شبکه محلی از اشیا مانند خانه‌ی هوشمند که از طریق شبکه‌ی اینترنت دسترس پذیر<sup>7</sup> نیست در مفهوم اینترنت اشیا جای ندارد و عبارت "شبکه‌ی اشیا"<sup>8</sup> برای چنین شبکه‌ای مناسب‌تر به نظر می‌رسد.

نکته‌ی دوم قابل برداشت این است که این شبکه‌ی اینترنت جدید، شبکه‌ی اشیا 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 در نظر گرفته شده‌اند). اما با ورود مفهوم اینترنت اشیا، موجودیت دیگری به نام شیء<sup>9</sup> (که هر چیزی 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 ارائه شده برای اینترنت اشیا را بیان می‌کنیم:

بازی<sup>1</sup> روابط میان گره‌های شبکه و حمله‌کنندگان مدل‌سازی شده‌است. این مدل‌سازی در قالب یک بازی میان گره مدافع<sup>2</sup> و حمله‌کننده<sup>3</sup> و با در نظر گرفتن درآمد حاصل از امنیت و هزینه‌ی تحمیل شده از مصرف منابع انجام شده‌است. در نهایت، با استفاده از مدل‌های ایجاد شده، تصمیم عقلانی<sup>4</sup> 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 گرفته شده‌است. در مدل‌های ارائه شده، گره مدافع در مقابل حمله‌کننده تنهاست و بدون در نظر گرفتن رفتار سایر گره‌های مدافع تصمیم‌گیری می‌کند. به باور ما، در نظر گرفتن 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 مدل کردن ارتباط میان گره‌های موجود در اینترنت اشیا در تشخیص نفوذ، با استفاده از بازی شراکت<sup>5</sup> یا بازی هم‌افزایی<sup>6</sup> مدلی را برای فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ ارائه داده‌ایم. با استفاده از مدل ارائه شده، هر گره مدافع با در نظر داشتن 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 اتخاذ کند.

در ادامه ابتدا مفاهیم پایه (بخش 2) و کارهای پیشین (بخش 3) شرح داده شده‌است. 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 ارائه شده با پژوهش‌های پیشین مورد بحث قرار گرفته (بخش 6) و نتایج (بخش 7) بیان شده‌است.

<sup>6</sup>Synergistic Game

<sup>7</sup>Available

<sup>8</sup>Network of Things

<sup>9</sup>Thing

<sup>1</sup> Game Theory

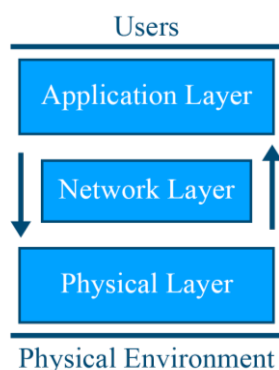
<sup>2</sup> Defender

<sup>3</sup> Attacker

<sup>4</sup> Rational

<sup>5</sup>Partnership Game

می‌شوند که هدف، تصمیم‌گیری بر پایه‌ی این اطلاعات و کنترل اشیاء فیزیکی موجود درون محیط فیزیکی است [7].



شکل 1- معماری سطح بالای 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، از جمله: 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<sup>11</sup> و سیستم گزارش‌دهی<sup>12</sup> تشکیل می‌شود [7]. بخش حسگرها داده‌های شبکه یا سیستم میزبان را جمع‌آوری می‌کند،

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

**تعریف دوم:** یک طرح‌واره‌ی میان‌شبکه‌ای<sup>1</sup> میسر شده به‌وسیله‌ی پشته‌ی فناوری<sup>2</sup> که یک ارتباط بدون‌درز را میان اشیاء فیزیکی و اشیاء مجازی ارائه می‌کند؛ برای تسهیل توسعه‌ی سرویس‌ها و کاربردهای هوشمند با قابلیت خودپیکربندی<sup>3</sup>. پشته‌ی فناوری ترکیبی است از فناوری‌های مختلف که این فرآیندها و همچنین یک اتصال بدون‌درز "در هر زمان، هر مکان، به‌وسیله‌ی هرکس و هر چیز" را میسر می‌کند [4].

امروزه اینترنت اشیاء در حوزه‌های مختلفی به‌کار گرفته می‌شود که از جمله‌ی آن می‌توان به حوزه‌های مراقبت‌های بهداشتی، انرژی، حمل‌ونقل، خودکارسازی ساختمان، شهرهای هوشمند، کشاورزی، صنعت، و حوزه‌ی نظامی<sup>4</sup> اشاره کرد [6].

در یک نگرش سطح‌بالا، می‌توان معماری اینترنت اشیاء را در سه بخش لایه‌ی فیزیکی<sup>5</sup> یا لایه‌ی ادراکی، لایه‌ی شبکه<sup>6</sup> و لایه‌ی کاربرد<sup>7</sup> خلاصه کرد (شکل 1). لایه‌ی فیزیکی یا لایه‌ی ادراکی شامل دستگاه‌های تعبیه‌شده با حسگرها و عملگرها است که وظیفه‌ی آن تبادل با محیط فیزیکی است. 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<sup>8</sup>، مرحله‌ی انتقال<sup>9</sup> و مرحله‌ی پردازش، مدیریت و بهره‌برداری<sup>10</sup>. در مرحله‌ی جمع‌آوری، هدف اصلی جمع‌آوری داده‌های مربوط به محیط فیزیکی است که این داده‌ها در مرحله‌ی انتقال، به کاربردها، و نهایتاً به کاربران منتقل می‌شوند. در مرحله‌ی پردازش، مدیریت، و بهره‌برداری، این داده‌ها توسط کاربردها به‌منظور کسب اطلاعات مفید پردازش

<sup>7</sup>Application Layer

<sup>8</sup>Collection Phase

<sup>9</sup>Transmission Phase

<sup>10</sup>Processing, Management and Utilization phase

<sup>11</sup>Analysis Engine

<sup>12</sup>Reporting System

<sup>1</sup>Inter-networking Paradigm

<sup>2</sup>Technology Stack

<sup>3</sup>Self-configuring

<sup>4</sup>Military

<sup>5</sup>Physical Layer

<sup>6</sup>Network Layer

مدلی برای تشخیص نفوذ در اینترنت اشیاء با استفاده از بازی شراکت

سپس این داده‌ها در بخش موتور تحلیل به منظور کشف نفوذ ارزیابی می‌شوند، و در نهایت، 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 مبتنی بر میزبان<sup>1</sup> و مبتنی بر شبکه<sup>2</sup> تقسیم‌بندی می‌شوند. سیستم تشخیص نفوذ مبتنی بر میزبان<sup>3</sup> به یک دستگاه/میزبان ضمیمه می‌شود و به منظور کشف فعالیت‌های مخرب، وقایع درون سیستم را نظارت می‌کند. سیستم تشخیص نفوذ مبتنی بر شبکه<sup>4</sup> 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 مبتنی بر میزبان توجه به وقایع درون یک سیستم مشخص و در سیستم‌های تشخیص نفوذ مبتنی بر شبکه توجه به وقایع درون شبکه است. به سیستم تشخیص نفوذی که به هر دو دسته از وقایع توجه دارد سیستم تشخیص نفوذ ترکیبی<sup>5</sup> گویند.

سیستم‌های تشخیص نفوذ، برحسب روش<sup>6</sup> اتخاذ شده برای تشخیص ناهنجاری در بخش موتور تحلیل، به سه دسته‌ی مبتنی بر امضاء<sup>7</sup>، مبتنی بر ناهنجاری<sup>8</sup> و مبتنی بر تعیین مشخصات<sup>9</sup> تقسیم‌بندی می‌شوند [10][11][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 در صورت تطابق، رفتار مخرب کشف می‌شود. در روش مبتنی بر 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 مبتنی بر تعیین مشخصات، شامل

مجموعه‌ای از قوانین<sup>10</sup> و حدود آستانه<sup>11</sup> است که رفتار مورد انتظار در شبکه یا میزبان را تعریف می‌کند و هر رفتارهای مغایر با رفتارهای مورد انتظار تعریف شده، به عنوان رفتار مخرب شناسایی می‌شوند. یک سیستم تشخیص نفوذ، در موتور تحلیل خود، می‌تواند ترکیبی از روش‌های مطرح شده را به کارگیرد که به چنین روشی، روش ترکیبی گویند.

سیستم‌های تشخیص نفوذ، از جمله تمهیداتی است که برای تأمین امنیت در اینترنت اشیاء به کار گرفته می‌شود. در هنگام 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، تصمیم‌گیری 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 توزیع شده<sup>12</sup>، متمرکز<sup>13</sup> و ترکیبی تقسیم می‌شوند. در دسته‌ی توزیع شده، 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<sup>14</sup> موردنظر سیستم تشخیص نفوذ ارائه شده و همچنین حملات<sup>15</sup> موردنظر از جمله تصمیم‌گیری‌های دیگر سیستم‌های تشخیص نفوذ در اینترنت اشیاء است. در نهایت می‌توان نحوه‌ی

<sup>9</sup>Specification-based

<sup>1</sup>Rules

<sup>1</sup>Thresholds

<sup>1</sup>Distributed

<sup>1</sup>Centralized

<sup>1</sup>Technologies

<sup>1</sup>Attacks

<sup>1</sup>Host-based

<sup>2</sup>Network-based

<sup>3</sup>HIDS

<sup>4</sup>NIDS

<sup>5</sup>Hybrid

<sup>6</sup>Method

<sup>7</sup>Signature-based

<sup>8</sup>Anomaly-based

اعتبارسنجی<sup>1</sup> سیستم تشخیص نفوذ ارائه شده 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<sup>2</sup> است. به‌طور کلی، بازی<sup>3</sup> را می‌توان شرایطی تعریف کرد که در آن سودمندی<sup>4</sup> هرکدام از بازیکنان، علاوه بر رفتار/استراتژی<sup>5</sup> خود، به رفتار/استراتژی بازیکنان دیگر نیز بستگی دارد. 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 وجود دارد. به عنوان یکی از اساسی‌ترین این مفاهیم می‌توان به مفهوم بهترین پاسخ<sup>6</sup> اشاره کرد. بهترین پاسخ عبارت است از بهترین استراتژی یا استراتژی‌های یک بازیکن که در پاسخ به استراتژی‌های اتخاذ شده به وسیله‌ی بازیکنان دیگر، بیشترین سودمندی را برای آن بازیکن به عمل می‌آورد. این مفهوم پایه‌ای است برای دو نظریه‌ی مهم در این حوزه: نظریه‌ی عقلانیت<sup>7</sup> و نظریه‌ی تعادل نش<sup>8</sup>. نظریه عقلانیت تلاشی است برای حذف مجموعه استراتژی‌های یک بازیکن که در هیچ صورتی (در پاسخ به هیچ یک از استراتژی‌های بازیکنان دیگر) بهترین پاسخ نیستند. نظریه‌ی دیگر، نظریه‌ی تعادل نش، به نقاطی از فضای بازی<sup>9</sup> اشاره می‌کند که در آن تمام بازیکنان در پاسخ به استراتژی

بازیکنان دیگر بهترین پاسخ را اتخاذ کرده‌اند که به این نقاط، نقاط تعادل<sup>10</sup> بازی گویند. منظور از نقاط بازی، تلاقی استراتژی‌های تمام بازیکنان یک بازی است که به آن نمایه‌ی استراتژی<sup>11</sup> گویند و همچنین فضای بازی یعنی تمام تلاقی‌های استراتژیک ممکن. گاهی بازیکنانی که در نقطه‌ی تعادل بازی قرار گرفته‌اند، به طور جمعی (و نه فقط یک بازیکن) با انتخاب استراتژی‌های دیگری به غیر از تعادل می‌توانند سودمندی خود را افزایش دهند اما چنین نقطه‌ی به دلیل تعادل نبودن ناپایدارند. زیرا حداقل یک بازیکن وجود دارد 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<sup>12</sup> را در نظریه‌ی بازی به وجود 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<sup>13</sup> و بازی‌های پویا<sup>14</sup> اشاره کرد. در بازی‌های ایستا، بازیکنان، همگی، به یکباره<sup>15</sup> استراتژی خود را انتخاب می‌کنند اما در بازی‌های پویا انتخاب‌ها به صورت متوالی انجام می‌شود [12].

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

<sup>1</sup>Equilibrium

<sup>2</sup>Strategy Profile

<sup>3</sup>Contract

<sup>4</sup>Static

<sup>5</sup>Dynamic

<sup>6</sup>One-shot

<sup>7</sup>Prisoner's Dilemma

<sup>8</sup>Zero-sum

<sup>1</sup>Validation

<sup>2</sup>Strategic Setting

<sup>3</sup>Game

<sup>4</sup>Utility

<sup>5</sup>Strategy

<sup>6</sup>Best Response

<sup>7</sup>Rationalizability

<sup>8</sup>Nash Equilibrium

<sup>9</sup>Strategy Space

مدلی برای تشخیص نفوذ در اینترنت اشیاء با استفاده از بازی شراکت

همکار در تولید یک محصول دارند. چنان که روشن است، در این بازی یک پروژه<sup>1</sup> و چند شریک<sup>2</sup> وجود دارد. سودی که از تلاش هر یک از شرکا حاصل می شود به سود کلی پروژه اختصاص دارد که هر کدام از شرکا سهم مشخصی از این سود دارند. اما هزینه ای که هر شریک برای این تلاش صرف می کند متوجه خود اوست. نکته ی دیگر این بازی این است که تلاش جمعی شرکا ممکن است درآمد افزوده ای برای پروژه حاصل کند به این معنا که ممکن است تلاش چند شریک با هم ارجح باشد بر تلاش یک شریک تنها که این مسئله را در این بازی، مکملیت<sup>3</sup> گویند و با تابع مکملیت<sup>4</sup> وجود یا عدم وجود و چگونگی آن قابل تعریف است [12].

### 3. پژوهش های مرتبط

در این بخش به بیان مختصری از پژوهش هایی که در جهت به کارگیری سیستم های تشخیص نفوذ در اینترنت اشیاء انجام شده است پرداخته ایم. این تلاش ها به مسیرها و دسته های مختلفی قابل تقسیم بندی است: بهینه سازی سخت افزار و منابع انرژی، ارائه ی الگوریتم های کم وزن برای تشخیص نفوذ، جایگذاری بهینه سیستم های تشخیص نفوذ در لایه ی ادراکی اینترنت اشیاء، و فعال سازی بهینه سیستم های تشخیص نفوذ. البته ممکن است یک پژوهش در بیش از یک دسته جای گیرد. پیش از مرور باید یادآور این نکته شد که حوزه ی سخت افزاری مورد توجه ما نیست و در مقابل، تمرکز ما دسته ی فعال سازی بهینه ی سیستم های تشخیص نفوذ است.

ارائه ی الگوریتم های بهینه، معمولاً یکی از سه حالت ممکن است: ارائه ی یک الگوریتم جدید، ارائه ی یک کاربرد جدید برای الگوریتم موجود، یا ارائه ی یک ترکیب جدید از الگوریتم های موجود که البته خود زیرشاخه ای از دسته ی دوم است. همچنین بهیگی می تواند در جهت پردازش و/یا حافظه باشد. برای نمونه،

در جهت ارائه ی یک الگوریتم جدید، اوه و همکارانش [13] یک الگوریتم کم وزن برای بررسی تطبیق امضاءها در مکانیزم تشخیص نفوذ مبتنی بر امضاء ارائه داده اند. این الگوریتم با دربرداشتن یک مکانیزم پُرش نیاز به بررسی جزئی بخشی از داده ها را از میان می برد. الگوریتم ارائه شده از نظر پردازش و حافظه، نسبت به الگوریتم سنتی تطابق امضاء بهینه تر است. در جهت ارائه ی یک کاربرد جدید برای الگوریتم های موجود، بختیار و همکارانش [14] با توجه به وجود حملات انکار خدمت در حوزه ی سلامت هوشمند در اینترنت اشیاء، با استفاده از الگوریتم یادگیری ماشین J48، یک سیستم تشخیص نفوذ مناسب برای دستگاه هایی با ظرفیت کم برای مقابله با این حملات ارائه داده اند. همچنین لیو و همکارانش [15] یک روش تشخیص نفوذ بهینه با استفاده از الگوریتم خوشه بندی SFC<sup>5</sup> ارائه کرده اند که در این روش از الگوریتم PCA<sup>6</sup> برای کاهش ابعاد استفاده شده است. پاتل و جینوالا [16] نیز با استفاده از تکنولوژی زنجیره ی بلوکی<sup>7</sup> یک سیستم تشخیص نفوذ برای تشخیص حملات انکار خدمت در پروتکل مسریابی RPL معرفی کرده اند. در این روش، با توجه به محدودیت منابع، با استفاده از ریززنجیره<sup>8</sup> از یک زنجیره ی بلوکی بهینه از جنبه ی فضا استفاده شده است. در نهایت، در جهت ارائه ی یک ترکیب جدید از الگوریتم های موجود، پاریمالا و کایالوویژی [17] با ارائه ی یک الگوریتم انتخاب ویژگی با استفاده از ترکیب دو الگوریتم CRF<sup>9</sup> و SMO<sup>10</sup> و همچنین استفاده از الگوریتم CNN<sup>11</sup> در یادگیری عمیق، به گفته ی خود، یک سیستم تشخیص نفوذ بهینه از نظر زمان و کارآمد از نظر دقت معرفی کرده اند.

در مسیر و دسته ی پژوهشی بعدی، جایگذاری بهینه ی سیستم های تشخیص نفوذ در لایه ی ادراکی اینترنت اشیاء، روش جایگذاری را می توان به سه روش متمرکز، توزیع شده، و ترکیبی تقسیم کرد. برای نمونه، کاسینتان و همکارانش [19][18] برای

<sup>7</sup>Block Chain

<sup>8</sup>Microchain

<sup>9</sup>Conditional Random Field

<sup>10</sup>Spider Monkey Optimization

<sup>11</sup>Convolutional Neural Network

<sup>1</sup>Project

<sup>2</sup>Partner

<sup>3</sup>Complementarity

<sup>4</sup>Complementarity Function

<sup>5</sup>Suppressed Fuzzy Clustering

<sup>6</sup>Principal Component Analysis

حاصل مشکل گره‌های کم‌توان، یک روش جایگذاری متمرکز را پیشنهاد داده‌اند که در آن سیستم تشخیص نفوذ در یک سیستم میزبان قدرتمند جایگذاری می‌شود به طوری که بخش حسگرهای تشخیصی این سیستم به صورت سیمی<sup>1</sup> در پهنه‌ی شبکه‌ی لایه‌ی ادراکی توزیع شده‌اند. همچنین آبپیشک و همکارانش [20] با قرار دادن مکانیزم تشخیص نفوذ خود در یک نقطه‌ی دسترسی<sup>2</sup> امن، سعی در شناسایی دروازه‌های مخرب<sup>4</sup> در شبکه‌ی خوشه‌بندی‌شده‌ی اینترنت اشیا داشته‌اند.<sup>5</sup> سادیکن و همکارانش [21] نیز با اتخاذ یک رویکرد متمرکز، یک سیستم تشخیص نفوذ ترکیبی (مبتنی بر امضاء و مبتنی بر ناهنجاری) در پروتکل زیگی<sup>6</sup> ارائه داده‌اند. از جمله تلاش‌های صورت گرفته در این تحقیق استفاده از امکانات پروتکل زیگی 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 شده است. همچنین با پیاده‌سازی سیستم در یک سخت‌افزار Raspberry Pi 3، سیستم در دو سناریوی متمرکز ارزیابی شده است: قراردادن سیستم در دروازه‌ی شبکه و در یک دستگاه، جدای دستگاه‌های دیگر در شبکه. در مقابل، سروانتس و همکارانش [23] از رویکرد توزیع شده برای جایگذاری مکانیزم تشخیصی استفاده کرده‌اند به گونه‌ای که در آن وظایف برحسب ظرفیت هر گره به گره‌ها انتصاب می‌شود. آموری و همکارانش [24] نیز یک مکانیزم تشخیص نفوذ دولایه را ارائه داده‌اند، شامل لایه‌ی محلی<sup>7</sup> و سراسری<sup>8</sup> در لایه‌ی محلی، وظایف کم‌وزن تشخیص نفوذ توسط گره‌های کم‌وزن انجام می‌شود و سپس در لایه‌ی

سراسری، داده‌های مورد نیاز به یک فراگره<sup>9</sup> برای انجام وظایف سنگین تر تشخیص نفوذ ارسال می‌شود. نکته‌ی دیگر این که در لایه‌ی محلی از الگوریتم کم‌وزن C4.5 برای طبقه‌بندی<sup>10</sup> استفاده شده است. ارشد و همکارانش [25] نیز از یک رویکرد همکارانه برای ارائه‌ی یک مکانیزم تشخیص نفوذ مقرون به صرفه در اینترنت اشیا صنعتی<sup>11</sup> استفاده کرده‌اند. در چهارچوب ارائه شده، مکانیزم تشخیص نفوذ شامل مؤلفه‌ی سطح دستگاه و مؤلفه‌ی مسریاب است. مؤلفه‌ی سطح دستگاه که شامل دستگاه‌های اینترنت اشیا 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 جمع‌آوری شده توسط مؤلفه‌ی سطح دستگاه، اتخاذ تصمیم درباره‌ی مخرب یا غیرمخرب بودن اتفاقات مشاهده شده، و همچنین ارسال نتایج به دستگاه‌های اینترنت اشیا 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 اشیا به خوشه‌های<sup>12</sup> مختلفی تقسیم‌بندی می‌شوند و در هر خوشه قدرتمندترین گره، مسئولیت تشخیص نفوذ در آن خوشه را به‌عهده دارد.

در مسیر و دسته‌ی پژوهشی بعدی، فعال‌سازی بهینه‌ی سیستم‌های تشخیص نفوذ در لایه‌ی ادراکی اینترنت اشیا (که مسیر پژوهش ما نیز هست)، سدجلماسی و همکارانش [27][28] با مدل‌کردن ارتباط میان گره مدافع و حمله‌کننده در قالب یک بازی روشی را برای فعال‌سازی بهینه ارائه کرده‌اند. 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

<sup>6</sup>Zigbee<sup>7</sup>Local<sup>8</sup>Global<sup>9</sup>Super Node<sup>10</sup>Classification<sup>11</sup>Industrial Internet of Things (IIoT)<sup>12</sup>Clusters<sup>1</sup>Wired<sup>2</sup>Access Point<sup>3</sup>Gateway<sup>4</sup>Malicious

<sup>5</sup> در یک شبکه‌ی خوشه‌بندی شده‌ی اینترنت اشیا، معمولاً در هر خوشه یک گره با منابع بیشتر به عنوان دروازه برای ارتباط سایر گره‌ها با نقاط دیگر شبکه استفاده می‌شود.

مدلی برای تشخیص نفوذ در اینترنت اشیاء با استفاده از بازی شراکت

تشخیص نفوذ مبتنی بر ناهنجاری استفاده می‌شود و قسمت مبتنی بر امضاء این سیستم همواره فعال است. مدل پیشنهادی در یک جایگذاری توزیع‌شده‌ی سیستم‌های تشخیص نفوذ استفاده شده است. 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 چه کسری مکانیزم مبتنی بر امضاء و چه کسری مکانیزم مبتنی بر ناهنجاری را فعال کند، تصمیم‌گیری می‌کند و هیچ‌گاه سیستم تشخیص نفوذ در گره مدافع غیرفعال نمی‌شود. مدل پیشنهادی در یک جایگذاری ترکیبی (یک شبکه‌ی خوشه‌بندی‌شده) استفاده شده است.

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 نظر گرفتن 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 در نظر گرفته شده است و در این مدل‌ها ارتباط میان گره‌های مدافع نادیده گرفته شده است. به باور ما در نظر گرفتن 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 ارائه کرده‌ایم که در آن ارتباط میان گره‌های مدافع در مقابل حمله‌کننده در نظر گرفته شده است.

#### 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 ارائه کرده‌ایم.

در مدل ارائه شده که مدلی مبتنی بر بازی شراکت است، رابطه‌ی میان گره‌های مدافع در قالب یک بازی همکارانه<sup>1</sup> مدل شده است؛ 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. چنان‌که 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 ارائه شده، گره‌های مدافع با در نظر گرفتن درآمد حاصل از برقراری امنیت، هزینه‌ی وارد از مصرف منابع، و همچنین با در نظر گرفتن 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 داشته باشد. 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، به ترتیب، مدل پیشنهادی را توصیف و تعریف کرده‌ایم و سپس نحوه‌ی کاربست آن را در شبکه نیز بیان کرده‌ایم.

#### 4-1. توصیف

در بازی شراکت یک پروژه مشترک و چند شریک وجود دارد. 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. در مقابل، 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

<sup>1</sup>Cooperative

و هم بر شریک. حال عناصر این مدل را مرحله به مرحله بیان می‌کنیم:

1-  $n$  را به عنوان تعداد بازیکنان در نظر می‌گیریم.

2- برای هر بازیکن  $i$ :

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

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

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

$e_i$  عبارت است از سطح تلاش انتخاب شده (استراتژی انتخاب شده) به وسیله‌ی بازیکن از مجموعه استراتژی‌های موجود.

3- برای بازی:

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

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

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

$e$  عبارت است از نمایه‌ی استراتژی بازی که نشانگر استراتژی‌های انتخاب شده به وسیله‌ی تمام بازیکنان است از میان تمام تلاقی‌های ممکن است.

4- برای هر بازیکن  $i$ :

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

$r_i$  عبارت است از تابع درآمد حاصل برای بازی به وسیله‌ی بازیکن که تابعی از استراتژی انتخاب شده‌ی بازیکن است و در آن  $1 \geq A_i \geq 0$  نرخ تشخیص گره و  $V_i^r \geq 0$  ارزش تشخیص نفوذ یا ضریب تابع درآمد است. همچنین

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

$c_i$  عبارت است از تابع هزینه‌ی بازیکن که تابعی از استراتژی انتخاب شده‌ی بازیکن است و در آن تغییرات هزینه با استفاده از

نظر گرفته‌ایم؛ با این فرض که کشف حمله به وسیله‌ی یک گره برای گره‌های دیگر و تمام شبکه سودمند خواهد بود.

در این مدل، هر بازیکن 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<sup>1</sup> سیستم ارتباط مستقیم دارد. ارزش امنیت برقرار شده، به عنوان ضریب، مؤلفه‌ی دیگر تابع درآمد<sup>2</sup> بازیکن است. در سوی دیگر، هزینه‌ی هر بازیکن عبارت است از هزینه‌ی منابع مصرف شده توسط سیستم تشخیص نفوذ آن بازیکن که این هزینه با میزان فعال‌سازی سیستم رابطه دارد. البته هزینه در رابطه با میزان فعال‌سازی، می‌تواند به صورت غیر خطی تغییر کند. ارزش هزینه‌ی صرف شده برای امنیت، به عنوان ضریب، مؤلفه‌ی دیگر تابع هزینه<sup>3</sup> بازیکن است.

درآمد کلی پروژه برابر است با مجموع درآمدهای بازیکنان به علاوه‌ی ارزش افزوده‌ی همکاری بازیکنان در صورتی که بازی دارای ویژگی مکملیت<sup>4</sup> 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، هر بازیکن سهم مشخصی از درآمد کلی پروژه کسب می‌کند و هزینه‌ی صرف شده توسط خود بازیکن، از آن کاسته می‌شود که این مسئله با تابع سودمندی<sup>5</sup> بازیکن مشخص شده است. سودمندی کلی پروژه نیز عبارت است از درآمد کلی پروژه با کاهش هزینه‌ی کلی پروژه از آن.

#### 2-4. تعریف

در این بخش مدل پیشنهادی خود بر مبنای 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

<sup>3</sup>Cost Function

<sup>4</sup>ویژگی مکملیت بازی شراکت در بخش مفاهیم پایه بیان شده است.

<sup>5</sup>Utility Function

<sup>1</sup> Detection Rate. یعنی چه کسری از حملات موجود توسط سیستم تشخیص نفوذ شناسایی می‌شود.

<sup>2</sup>Revenue Function

مدلی برای تشخیص نفوذ در اینترنت اشیا با استفاده از بازی شراکت

تابع  $v(e_i)$  به صورت تابع میزان مصرف مدل شده است.<sup>1</sup> همچنین  $V_i^c \geq 0$  ارزش منابع مصرف شده یا ضریب تابع هزینه است.

5- برای بازی:

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

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

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

$c$  عبارت است از هزینه مجموعی که بازیکنان بازی متحمل شده‌اند.

6- برای هر بازیکن  $i$ :

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

$l_i$  سهم بازیکن از درآمد بازی است (یعنی چه کسری از درآمد کلی پروژه برای بازیکن است) و در نهایت

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

$u_i$  عبارت است از تابع سودمندی بازیکن.

7- برای بازی:

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

$l$  عبارت است نمایه‌ی سهم بازی که نمایشگر چگونگی سهم تمام بازیکنان است و

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

$L$  عبارت است از فضای سهم بازی که شامل تمام بردارهای  $n$  تایی است که حاصل جمع عناصر آن برابر با 1 است. در نهایت

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

$u$  عبارت است از تابع سودمندی بازی.

#### 4-3. کاربرت

<sup>1</sup> گاهی قیمت یک محصول با میزان مصرف تغییر می‌کند، 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

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

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

2-  $D$  را به عنوان مجموعه‌ی تمام پروژه‌های مشترک تشخیص نفوذ تعریف می‌کنیم. هر پروژه مشترک نشانگر یک بازی است. یعنی می‌توان پروژه‌های 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  $assign$  را به صورت زیر تعریف می‌کنیم:

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

که در آن  $R$  یعنی مجموعه توابع سود،  $C$  یعنی مجموعه توابع هزینه،  $F$  یعنی مجموعه توابع مکملیت، و  $L$  یعنی مجموعه‌ی تمام بردارهایی که جمع عناصر آن برابر با 1 است. در واقع، 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

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.

<sup>2</sup>Lot Profile

<sup>3</sup>Lot Space

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 *assign* است.)

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

1. نقطه‌ی تعادل بازی عبارت است از:

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

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

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

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

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

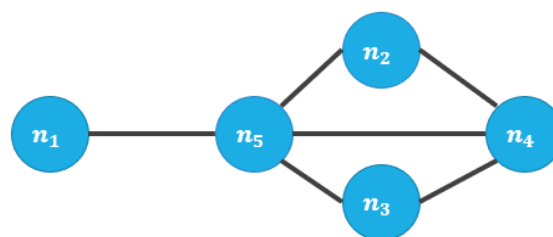
4. هزینه‌ی منابع در بازی عبارت است از:

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

5. با در نظر گرفتن  $\bar{p}_d^c$ ،  $\bar{p}_d^*$  و  $\bar{p}_d^a$  به‌عنوان احتمال

تشخیص تک‌حمله زمانی که گره‌ها به‌ترتیب نقطه‌ی بیشینه‌ی فعال‌سازی، نقطه‌ی تعادل، و نقطه‌ی قرداد را بازی می‌کنند، داریم  $\bar{p}_d^* \leq \bar{p}_d^c \leq \bar{p}_d^a$

روش شبیه‌سازی انجام و ارائه شده‌است. شبکه‌ی مورد مطالعه از پنج گره تشکیل می‌شود که توپولوژی آن در شکل 2 نمایش داده شده‌است. 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. کاربرد

کاربست مدل ارائه‌شده و نتایج حاصل به شرح زیر است: مرحله‌ی اول)  $N = \{n_1, n_2, n_3, n_4, n_5\}$  را به عنوان مجموعه‌ی تمام گره‌های شبکه تعریف می‌کنیم. مرحله‌ی دوم)  $D = \{d_1, d_2, d_3, d_4, d_5\}$  را به عنوان مجموعه‌ی تمام پروژه‌های تشخیص نفوذ در شبکه تعریف می‌کنیم به طوری که  $d_i$  عبارت است از تشخیص نفوذ علیه  $n_i$

مرحله‌ی سوم) برای هر  $d_i$  داریم:

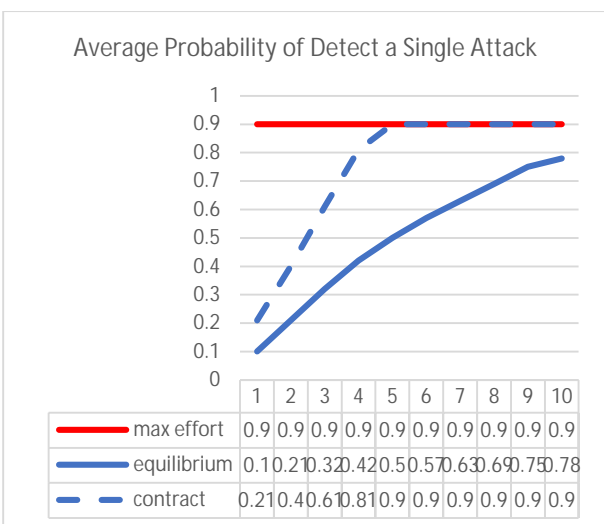
1. بازیکنان، گره‌های همسایه‌ی  $n_i$  هستند.
2. برای هر گره  $j$ :  $E_j = [0, 1]$ ،  $V_j^r = V^r$ ،  $V_j^c = V^c$ ،  $A_j = A$  و  $l_j = 1/n$  برقرار است که  $n$  نمایشگر تعداد بازیکنان بازی است (فرض یکسان بودن گره‌ها). توجه کنید که در  $E_j = [0, 1]$ ، نشان‌دهنده‌ی حداقل تلاش و  $1$  نشان‌دهنده‌ی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

مدلی برای تشخیص نفوذ در اینترنت اشیاء با استفاده از بازی شراکت

پنج گره شبکه به عنوان حمله کننده انتخاب می شود. گره ها با احتمال 0,5 تصمیم می گیرند که آیا به همسایگان خود بسته ارسال کنند یا خیر و همچنین حمله کننده با احتمال 0,5 تصمیم می گیرد که آیا حمله انجام دهد یا خیر.

در شکل های 4، 5، 6 و 7 نتایج استراتژی بازیکنان در هر یک از حالت های بازی حداکثر تلاش، بازی تعادل، و بازی قرارداد، با فرض  $V^c = 1$  و  $A = 0.9$  و تغییر  $V^r$  نمایش داده شده است؛ به ترتیب از جنبه های احتمال میانگین تشخیص تک حمله، هزینه منابع، شناسایی حمله کننده در چندمین حمله، و نسبت سود به هزینه. یعنی در شرایطی که نرخ تشخیص گره ها 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، حالت ها را با یکدیگر مقایسه کرده ایم.

چنان که در شکل 4 مشاهده می کنید، از جنبه ی احتمال میانگین تشخیص تک حمله، همواره قرارداد بهتر از تعادل عمل می کند. همچنین با افزایش ارزش امنیت نسبت به ارزش هزینه (مانند شبکه هایی که امنیت در آن ها بحرانی است)، این احتمال در هر دو حالت افزایش میابد.



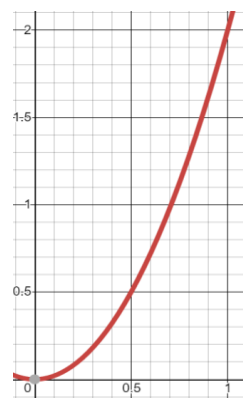
شکل 4. احتمال میانگین تشخیص تک حمله با فرض  $V^c = 1$  و  $A = 0.9$ ، و با تغییر  $V^r$ .

6. با در نظر گرفتن  $C_e^a$ ،  $C_e^*$  و  $C_e^c$  به عنوان هزینه ی منابع زمانی که گره ها به ترتیب نقطه ی بیشینه ی فعال سازی، نقطه ی تعادل، و نقطه ی قرارداد را بازی می کنند، داریم  $C_e^* \leq C_e^c \leq C_e^a$ .
7. همچنین می توان با فرض این مسئله که گره ها نقطه ی تعادل را بازی می کنند، تابع سودمندی پروژه را با تنظیم نمایه ی سهم  $(l = l_1, l_2, \dots, l_n)$  بیشینه کرد:

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

که در آن:

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



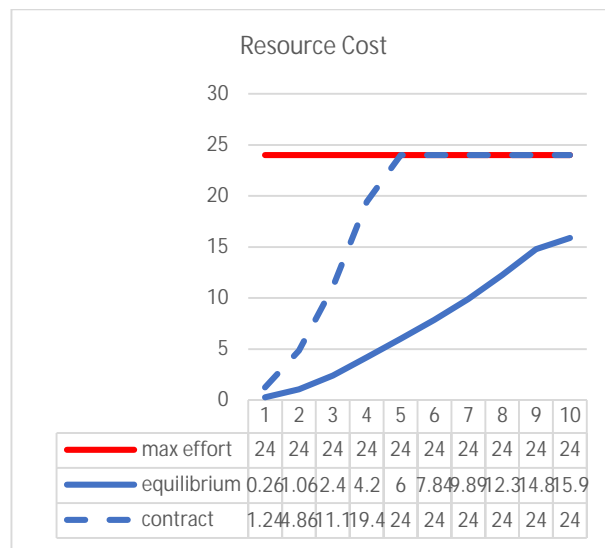
شکل 3. تابع میزان مصرف: توجه کنید که مصرف کننده در نقطه ی میانی (0,5) به همان مقدار که مصرف کرده است هزینه می پردازد و نیمه ی پیش از آن (0 تا 0,5) بازه ی تخفیف و نیمه ی پس از آن (0,5 تا 1) بازه ی جریمه است.

## 5-2. ارزیابی

برای شبیه سازی مدل های ارائه شده در مطالعه ی موردی از یک برنامه ی توسعه داده شده با زبان برنامه نویسی پایتون<sup>1</sup> استفاده کرده ایم. فرآیند شبیه سازی 50000 بار تکرار می شود و هر بار تا زمانی ادامه پیدا می کند که گره حمله کننده شناسایی شود. در هر بار به طور تصادفی (با احتمال 0,2 برای هر گره) یک گره از میان

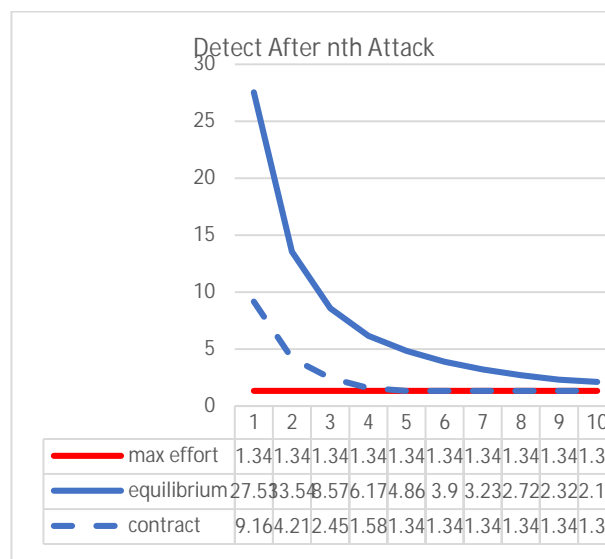
<sup>1</sup>Python

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 می‌یابد.



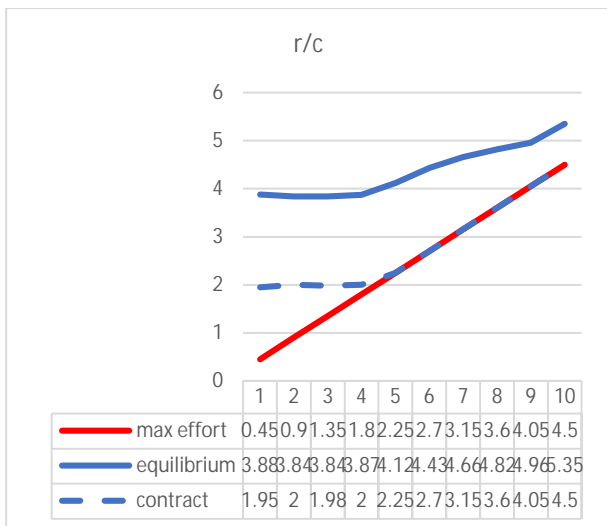
شکل 5. هزینه‌ی منابع با فرض  $V^c = 1$  و  $A = 0.9$  و با تغییر  $V^r$ .

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



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

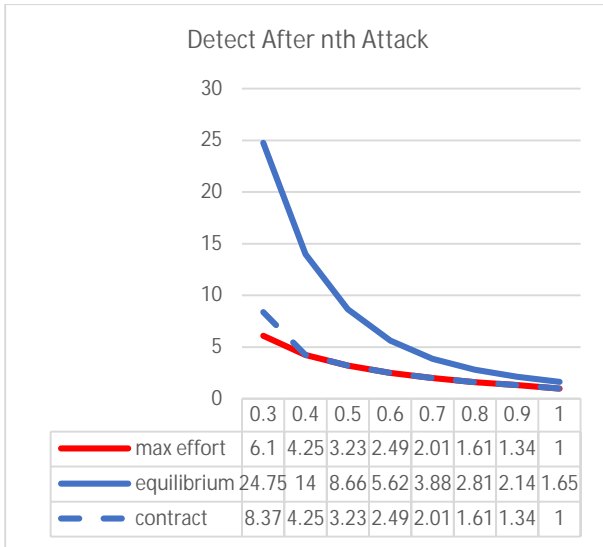
با توجه به شکل 7، از جنبه‌ی نسبت سود به هزینه، قرارداد همواره بدتر از تعادل عمل می‌کند. همچنین با افزایش ارزش امنیت نسبت به ارزش هزینه، این نسبت در هر دو حالت افزایش می‌یابد.



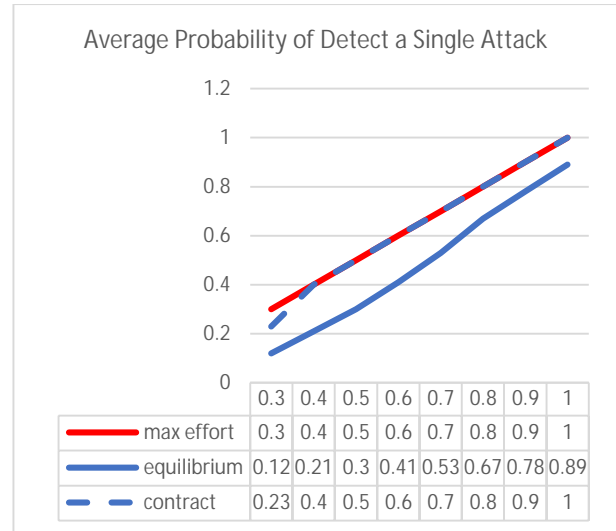
شکل 7. نسبت سود به هزینه با فرض  $V^c = 1$  و  $A = 0.9$  و با تغییر  $V^r$ .

در شکل‌های 8، 9، 10 و 11 نتایج استراتژی بازیکنان در هر یک از حالت‌های بازی حداکثر تلاش، بازی تعادل، و بازی قرارداد با فرض  $V^c = 1$  و  $V^r = 10$  و تغییر  $A$  نمایش داده شده‌است؛ به ترتیب 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 می‌یابد.

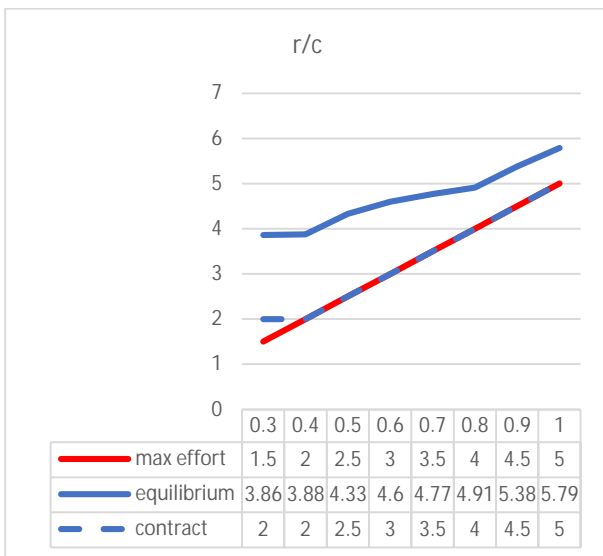


شکل 10. شناسایی حمله کننده در چندمین حمله با فرض  $V^c = 1$  و  $V^r = 10$ ، و با تغییر  $A$ .



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

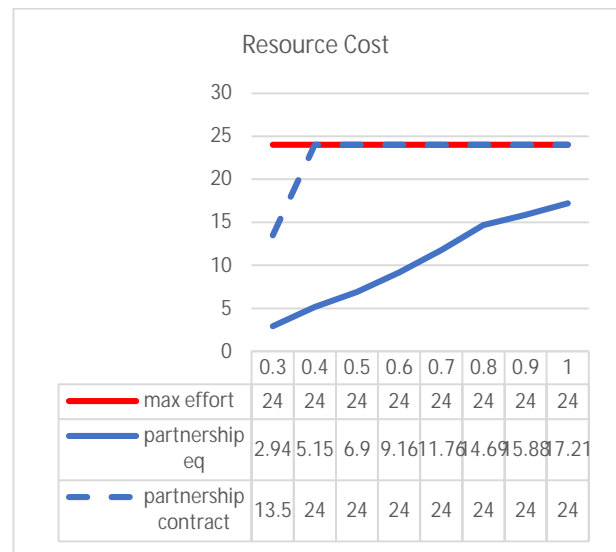
با توجه به شکل 11، از جنبه‌ی نسبت سود به هزینه، قرارداد همواره بدتر از تعادل عمل می‌کند. همچنین با افزایش نرخ تشخیص، این نسبت در هر دو حالت افزایش می‌یابد.



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

برای لمس بیشتر کارکرد مدل ارائه شده می‌توان به این مثال اشاره کرد: فرض کنید ارزش امنیت ده برابر ارزش هزینه‌ی منابع باشد (مثلاً  $V^c = 1$  و  $V^r = 10$ ) و همچنین نرخ تشخیص سیستم‌های تشخیص نفوذ در گره‌های مدافع 90 درصد باشد

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 می‌یابد.



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 حمله کننده، قرارداد همواره بهتر از تعادل عمل می‌کند. همچنین با افزایش نرخ تشخیص، این سرعت در هر دو حالت افزایش می‌یابد.

( $A = 0.9$ ). 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 اشیا 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 قرار داده‌است.

در تحقیقات پیشین، حمله‌کننده به‌صورت صریح<sup>1</sup> در بازی حضور دارد؛ یعنی رفتار یا استراتژی‌های حمله‌کننده به‌عنوان یک بازیکن در بازی مدل شده‌است. اما در مدل ما نقش حمله‌کننده ضمنی<sup>2</sup> 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 به‌طور کلی حمله، با تعریف پروژه‌های تشخیص نفوذ در کاربست مدل مدنظر قرار گرفته‌است.

سدجلماسی و همکارانش [28][27]، بازی را بر روی سیستم تشخیص نفوذ مبتنی بر ناهنجاری به‌کار گرفته‌اند و ژو و همکارانش [29] بر روی سیستم تشخیص نفوذ مبتنی بر امضاء و مبتنی بر ناهنجاری به‌طور همزمان. اما در مدل ما این آزادی وجود دارد که با تعریف پروژه‌های تشخیص نفوذ مختلف، بازی‌ها را به‌طور جداگانه بر روی مکانیزم‌های تشخیص نفوذ مختلف، حملات مختلف، و حتی خوشه‌های مختلف شبکه به‌طور 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 اشیا این مسئله را پررنگ‌تر نیز می‌کند. به‌طور خلاصه، یعنی از جمله ویژگی‌های مدلی که ارائه کرده‌ایم، برخلاف کارهای پیشین، حمایت از ویژگی ناهمگونی اینترنت اشیا است که می‌توان با توجه به شرایطی که هر شبکه اینترنت اشیا یا حتی هر بخش از شبکه‌ی اینترنت اشیا دارد، بازی متناسب با آن را تعریف نمود.

از جمله 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، به‌طور کلی، "همواره" است و سیستم تشخیص نفوذ گره هیچ‌گاه خاموش نمی‌شود و تنها سهم دو نوع سیستم تشخیص نفوذ مبتنی بر ناهنجاری و مبتنی بر 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 اشاره کرد که در مدل‌های پیشین تکیه‌ی بهینه‌سازی فعال‌سازی بر روی 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 مبتنی بر امضاء. چنان‌که می‌دانیم تنها منابع انرژی در اینترنت اشیا چالش‌برانگیز نیست و منابع دیگری نیز مانند حافظه و منابع پردازشی مورد بحث است (نظر به وجود گره‌هایی با ظرفیت پایین در اینترنت اشیا). 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.

<sup>2</sup>Implicit

<sup>1</sup>Explicit

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

اتخاذکنند. در نهایت نیز تفاوت‌های مدل ارائه‌شده با مدل‌های پیشین بررسی شد.

## 7. نتایج

در این پژوهش، در ابتدا تشریح کردیم که یکی از اصلی‌ترین موانع امنیت و بخصوص به‌کارگیری سیستم‌های تشخیص نفوذ در اینترنت اشیا، 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 اشیا، 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 مبتنی بر بازی شراکت سعی کردیم با در نظر گرفتن 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 در نظر گرفتن درآمد حاصل از برقراری امنیت، هزینه‌ی وارد از مصرف منابع، و همچنین با در نظر گرفتن رفتار دیگر گره‌های مدافع تصمیم عقلانی درباره‌ی میزان فعال‌سازی سیستم تشخیص نفوذ خود

## 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. Siddiq, 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.

- 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. Alaparthi, 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.
- [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