Journal of Electronical & Cyber Defence
Vol. 10, No. 1, Spring 2022, Serial No. 37

A method to detect intrusion into the Internet of Things using the game theory

S. Siadat*, M. Ghafary, M. Rezvanmadani

* Associate professor, Faculty of Electrical and Computer Engineering, University of Birjand, Birjand, Iran

(Received: 23/04/2021, Accepted: 19/01/2022)

ABSTRACT

The Internet of Things is an emerging technology that integrates the Internet and physical intelligent objects; objects that cover a wide range of areas such as smart homes and cities, industrial and military processes, human health, business and agriculture. The IoT technology deepens the presence of Internet-connected devices in our day-to-day operations, bringing many benefits to the quality of life, as well as security-related challenges. Accordingly, the IoT security solutions should be developed and like other networks, the IoT intrusion detection systems are considered the most important means of providing security. In the present study, a method is proposed to detect any IoT intrusion, using the game theory. In the proposed method, the attacker security attack game and the behavior of the intrusion detection system in a two-player, non-participatory game are analyzed dynamically and with complete information, and the equilibrium solutions are obtained for specific sub-games. The analysis of best response parameters using the game theory and Nash equilibrium definitions indicates the need to use cloud-fog-based IoT intrusion detection systems. This is realized in the proposed model through providing optimal strategies and maximizing the attack reports by the smart node network..

Keywords: IoT ; intrusion detection ; game theory.

* Corresponding Author Email: safieh.siadat@gmail.com

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۱، بهار ۱۴۰۱، ص ۳۱-۲۱

علمی-پژوهشی

روشی جهت تشخیص نفوذ در اینترنت اشیا با استفاده از نظریه‌ی بازی‌ها

سیده صفیه سیادت[1*]، محسن انگورج غفاری[2]، محمدرضوان مدنی[3]

۱- استادیار، ۲و۳- دانشجوی کارشناسی ارشد، گروه مدیریت فناوری اطلاعات، دانشگاه پیام نور، تهران، ایران

(دریافت: ۱۴۰۰/۰۲/۰۳، پذیرش: ۱۴۰۰/۱۰/۲۹)

چکیده

اینترنت اشیا، فناوری نوظهوری است که اینترنت و اشیای هوشمند فیزیکی را ادغام می‌کند، اشیایی که به دامنه‌های گسترده‌ای از قبیل خانه‌ها و شهرهای هوشمند، فرآیندهای صنعتی و نظامی، نظارت بر بهداشت و سلامت انسان، کسب‌وکار و کشاورزی تعلق دارد. فناوری اینترنت اشیا، حضور وسایل متصل به اینترنت را در فعالیت‌های روزانه‌ی ما عمیق‌تر می‌کند و مزایای زیادی را در کیفیت زندگی به همراه دارد و از طرفی چالش‌های مرتبط با مسائل امنیتی نیز ایجاد کرده است. براین‌اساس، راه‌حل‌های امنیتی برای اینترنت اشیا باید توسعه داده شود؛ همانند سایر شبکه‌ها، سیستم‌های تشخیص نفوذ برای اینترنت اشیا نیز، مهم‌ترین ابزار امنیتی به حساب می‌آید. در پژوهش حاضر، طرح روشی برای تشخیص نفوذ در اینترنت اشیا با استفاده از نظریه‌ی بازی‌ها ارائه شده است. در روش ارائه‌شده، بازی حمله‌ی امنیتی مهاجم و رفتار سیستم تشخیص نفوذ در بازی دو نفره، غیرمشارکتی پویا و با اطلاعات کامل تحلیل می‌شود و راه‌حل‌های تعادلی نش برای زیربازی‌های خاص را به دست می‌دهد. تحلیل پارامترهای بهترین پاسخ با استفاده از تعاریف نظریه‌ی بازی‌ها و تعادل نش و شبیه‌سازی در نرم‌افزار MATLAB، حاکی از لزوم بهره‌گیری از سیستم‌های تشخیص نفوذ در شبکه‌ی اینترنت اشیا است. این بهره‌گیری مبتنی بر ابرمه از طریق ارائه‌ی استراتژی‌های بهینه و گزارش حداکثری حملات از سوی شبکه‌ی گره‌های هوشمند در مدل پیشنهادی انجام می‌شود.

کلیدواژه‌ها: اینترنت اشیا ، تشخیص نفوذ، نظریه‌ی بازی‌ها

۱- مقدمه

پیشرفت فناوری‌های مختلف از قبیل حسگرها، ارتباطات بی‌سیم، محاسبات نهفته، شناسایی و ردیابی خودکار، دسترسی گسترده به اینترنت و سرویس‌های توزیع‌شده، پتانسیل ادغام اشیا هوشمند را در زندگی روزانه‌ی ما از طریق اینترنت افزایش می‌دهد. همگرایی اینترنت و اشیا هوشمندی که می‌تواند به برقراری ارتباط و تعامل با یکدیگر بپردازند، اینترنت اشیا را تعریف می‌کند. این نمونه جدید به‌عنوان یکی از مهم‌ترین عوامل در صنعت فناوری اطلاعات و ارتباطات در سال‌های آینده تشخیص داده شده است [۲۴].

هدف فناوری اینترنت اشیا توانمندسازی اشیا برای اتصال در هر زمان و مکان، با هر چیزی و هر شخصی است که از هر مسیر یا شبکه و خدمت به‌صورت مطلوب استفاده می‌کند. اینترنت اشیا تکامل جدیدی از اینترنت است. اینترنت اشیا فناوری جدیدی است که به حضور نافذ محیطی توجه می‌کند و از تنوع اشیا هوشمند با اتصالات بی‌سیم و سیم‌دار به محاوره با یکدیگر می‌پردازد. این اشیا برای ایجاد کاربردها یا خدمات جدید و دستیابی به اهداف مشترک با یکدیگر همکاری می‌کنند و درواقع چالش‌های توسعه برای ایجاد جهانی هوشمند و بزرگ به شمار می‌روند. جهانی که به شکل واقعی، دیجیتال و مجازی است و به سمت شکل‌گیری محیط‌های هوشمند، همگرا می‌شود و حوزه‌های هوشمندتر انرژی، حمل‌ونقل، سلامت، شهرها و بسیاری دیگر را به وجود می‌آورد [۴].

بااین‌حال، ادغام اشیا هوشمند موجود در دنیای واقعی با اینترنت می‌تواند تهدیدات امنیتی را نیز در بسیاری از فعالیت‌های روزانه‌ی ما به همراه داشته باشد [۵].

با توجه به استانداردها و پشته‌های ارتباطی گسترده، توان محدود محاسباتی و تعداد بالای وسایل به هم متصل، اقدامات رایج امنیتی در برابر تهدیدات نمی‌تواند در سیستم‌های اینترنت اشیا به‌طور مؤثری عمل کند. به همین دلیل، توسعه‌ی راه‌حل‌های امنیتی خاص برای اینترنت اشیا ضروری است، تا به کاربران سازمان‌ها اجازه دهد، تمام ضعف سیستم را شناسایی کنند [۳۳].

* رایانامه نویسنده مسئول: siadat@pnu.ac.ir

ناشر: دانشگاه جامع امام حسین (ع)

برخی از پروژه‌های در حال انجام برای تکامل امنیت اینترنت اشیا شامل روش‌هایی است که محرمانگی داده‌ها و احراز هویت، کنترل دسترسی در داخل شبکه‌ی اینترنت اشیا، حریم خصوصی و اعتماد میان کاربران و اشیا، و اجرای سیاست‌های امنیت و حریم خصوصی را ارائه می‌دهد[۳۴]. بااین‌حال، حتی با وجود این روش‌ها نیز شبکه‌های اینترنت اشیا در برابر حمله‌های متعدد آسیب‌پذیر است. حمله‌هایی که با هدف اختلال و از بین بردن این شبکه‌ها طراحی می‌شود. به همین دلیل، روش دفاعی موردنیاز، طراحی روش‌هایی است که مهاجمان را تشخیص دهد. سیستم‌های تشخیص نفوذ برای انجام این هدف است.

توسعه‌ی فناوری‌های مبتنی بر وب و محاسبات ابری، انقلاب آینده در فناوری‌های دیجیتال را رقم خواهد زد و افزایش سلامت، بهره‌وری، سهولت و طیف گسترده‌ای از اطلاعات مفید برای افراد و سازمان‌ها را در پی خواهد داشت. از طرفی چالش‌هایی در حیطه‌ی محرمانگی شخصی، پیچیدگی فناوری، نفوذ و ایجاد شکاف دیجیتال خواهد شد [۲۶].

دنیای دیجیتال، با داده‌های شخصی، اشتراکی و ثبت‌شده‌ی افراد اشباع شده است و نگرانی‌هایی در زمینه‌ی امنیت و حفاظت از اطلاعات افراد و دولت‌ها فراهم کرده است. مشکلات ناشی از انتقال و پردازش داده‌های ناخواسته، موجب نگرانی‌های کاربران و مسائل قانونی شده است. با رشد سریع کاربردهای فناوری اینترنت اشیا مفاهیم امنیتی مورد توجه قرار می‌گیرد. نگرانی‌هایی در زمینه‌ی نفوذ، محرمانگی و ناتوانی مردم در کنترل زندگی شخصی‌شان شکل می‌گیرد. اگر فعالیت روزانه‌ی افراد نظارت شود و آن‌ها تولیدکننده‌ی خروجی‌های اطلاعاتی باشند، فعالیت‌های سیاسی، اقتصادی و اجتماعی تحت تأثیر قرار می‌گیرند. در صورت نقض امنیت، رخداد حمله و اختلال در عملکرد، مزایای فناوری اینترنت اشیا کمرنگ می‌شود [۱۲].

برقراری امنیت شاید بزرگ‌ترین چالش در شبکه‌ی اینترنت اشیا باشد. امنیت در اینترنت فعلی هم یک چالش بزرگ به شمار می‌آید، اما در اینترنت اشیا این مسئله ابعاد بزرگ‌تری پیدا می‌کند. توزیع‌شدگی شبکه و به‌تبع آن نقاط ورود بیشتر به سیستم، یکی از دلایل این موضوع است. همچنین اشیایی که قرار است به اینترنت متصل شود، معمولاً ساختار و معماری ساده‌تری نسبت به کامپیوترها دارد و این پیاده‌سازی ابزارهای امنیتی را در آن دشوار می‌سازد. فناوری اینترنت اشیا خیلی بیشتر از اینترنت فعلی به زندگی واقعی نزدیک شده است؛ درواقع نفوذ به چنین شبکه‌ای معادل نفوذ به زندگی روزمره کاربران خواهد بود [۳۳].

با توجه به چالش‌های امنیتی در دنیای مجازی و فناوری نوظهور اینترنت اشیا و هم‌چنین وجود چالش‌های نفوذ به این سیستم‌ها، ارائه یک روش بهینه به‌منظور کشف نفوذ صورت‌گرفته و حفظ امنیت در این سیستم‌ها بسیار ضروری و حائز اهمیت است [۲۷].

به‌همین‌جهت به‌منظور مقابله بانفوذگران و مهاجمان به سیستم‌ها و شبکه‌های رایانه‌ای، روش‌های متعددی تحت عنوان روش‌های تشخیص نفوذ ایجاد گردیده است که عمل نظارت بر وقایع اتفاق‌افتاده در یک سیستم یا شبکه‌ی رایانه‌ای را بر عهده دارد. در پژوهش حاضر، به‌منظور تحقق اهداف و ارائه مدل ریاضی کارآمد در سیستم‌های تشخیص نفوذ، بخش‌های ذیل در نظر گرفته شده است. پیشینه‌ی پژوهش در بخش دوم و بیان مسئله در بخش سوم آورده شده است. مدل‌سازی و تعاریف پارامترهای بازی، اطلاعات و داده‌های مورداستفاده در بخش چهارم بیان شده است. بخش پنجم نیز با بهره‌گیری از یافته‌های به دست آمده ضمن تجزیه و تحلیل، نهایت به ارائه‌ی نتایج و پیشنهادهای مؤثر در بخش ششم منتهی می‌شود.

۲- پیشینه‌ی پژوهش

در طی سال‌های اخیر، مقالات و روش‌های مختلفی مبتنی بر نظریه‌ی بازی در حوزه‌ی امنیت شبکه‌های کامپیوتری، به‌منظور مدل کردن، تحلیل و بهینه‌سازی عملکرد و کارایی سیستم‌های تشخیص نفوذ در فناوری‌های مرتبط با اینترنت اشیا از قبیل شبکه‌های اقتضایی متحرک (کومار و دوتا[1] [۱۸])،میشرا و همکاران[2] [۲۳])، شبکه‌های حسگر بی‌سیم (بوتن و همکاران[3] [۶])، محاسبات ابری (مودی و همکاران[4] [۲۵]) و سیستم‌های سایبری فیزیکی (میتچل و چن[5] [۲۰]) منتشر شده‌اند.

گزارش مودی و همکاران [۲۵]، نفوذهای مختلفی را ارائه داد؛ که بر دسترس‌پذیری، محرمانگی و یکپارچگی در محاسبات ابری تأثیر می‌گذارد. نویسندگان این مرجع، فناوری سیستم‌های تشخیص نفوذ استفاده شده در ابر را به سه دسته مبتنی بر میزبان، مبتنی بر شبکه و مبتنی بر هایپروایز (ناظر ماشین مجازی) تقسیم کرده‌اند. همچنین در مورد مزایا و معایب هر پروتکل بحث و چالش‌هایی را شناسایی کردند، تا محاسبات ابری را به‌صورت بستر قابل‌اعتمادی برای ارائه سرویس‌های اینترنت اشیا درآورند.

[1] Kumar & Dutta
[2] Mishra et al
[3] Butan et al
[4] Modi et al
[5] Mitchell & Chen

نتیجه‌ی پژوهش میدی و همکاران[1] [۲۳] نشان می‌دهد کـه یک سیستم تشخیص نفوذ قادر به نظارت و کنترل پروتکـل‌هـای ارتباط چندگانـه، ترکیـب قـوانین امضـا و فرآینـدهای تشـخیص ناهنجاری است.

بوتون و همکاران **[۶]** به بررسی گسترده‌ای در مورد سیستم‌های تشخیص نفوذ در شبکه‌های حسـگر بی‌سیم پرداخته؛ و تحـلیل مقایسه‌ای را بین سیستم‌های تشخیص نفوذ ارائه‌شده برای شبکه‌های حسگر بی‌سیم با توجـه به معـماری شبکه و روش تشخیص ارائه کرده است.

گرانجال و همکاران[2] **[۱۴]** یک تحلیل امنیتی جامع از چندین پروتکل اینترنت ارائه می‌کنند. به‌طور دقیق‌تر، آن‌ها مسائل امنیتی IEEE802.15.4 را روی شبکه‌های منطقه‌ای بی‌سیم قدرت پایین(6LoWPAN)، پروتکل مسیریابی IPv**6** برای شبکه‌های قدرت پایین و سست(RPL[3])، پروتکل امنیت لایه‌ی انتقال(DTLS[4]) و پروتکل برنامه‌های محدود(CoAP[5]) را بررسی کردند.

کومار و دوتا [**۱۸**]روش‌های تشخیص نفـوذ ارائـه‌شـده بـرای شبکه‌های اقتضایی متحرک را با تمرکز بر روی الگوریتم تشخیص آن‌ها بررسی نموده‌اند. یک دسته‌بندی درختی را برای روش‌هـای تشخیص نفوذ معرفـی کـرده‌انـد کـه بـا توجـه بـه ماهیـت روش پردازشی استفاده‌شده در روش تشخیص صورت گرفته است.

لی و همکـاران[6] [**۲۹**] یـک سیسـتم تشـخیص نفـوذ بـرای شبکه‌هـای **6**LOWPAN-RPL ارائـه مـی‌دهنـد کـه قـادر اسـت حمـلات Sinkhole، Sybil و Selective را بـا اسـتفاده از رویکـرد ترکیبی که پارامترهای متفاوتی را متصل می‌کند، شناسایی کند.

آتلی و همکاران[7] [**۳**] یک سیستم تشخیص نفوذ را بر اسـاس ویژگی با ناظر و استفاده از شبکه‌ی عصبی پیشرو ارائه داده است. در این مقاله انتخـاب ویژگـی روی داده‌هـای ISCX-IDS **2012** وAndroid CIC ، انجام‌شده است. به‌منظور انجـام فـاز، انتخـاب ویژگی از SVM با یادگیری افزایشـی اسـتفاده شـده اسـت؛ کـه رتبه‌بندی انجام‌شده از ۴۳ ویژگی موجـود در مجموعـه داده، ۲۰ ویژگی با بالاترین رتبه انتخـاب شـده‌انـد و سـپس بـا اسـتفاده از شبکه‌ی عصبی، تشخیص نهایی با دقت ۹۴٪ تـا ۹۸/۷ ٪ صـورت پذیرفت.

شیگن شن و همکاران[8] **[۳۲]**چـارچوبی بهینـه بـرای نشـان دادن کاربرد بالقوه و عملی سرکوب انتشار بدافزار به‌منظور حفـظ حریم خصوصی اشیا هوشمند در شبکه‌های اینترنت اشیا از طریق یک سیستم تشخیص نفوذ با محاسبه‌ی تئوریـک بـازی بیـزین را ارائه کرده است.

کلمپوس و همکاران[9] **[۱۷]**، امنیت اینترنت اشیا، چـالش‌هـا، تهدیدها و راه‌حل‌هـای آن را مـورد بررسـی قـرار دادنـد. پـس از بررسی و ارزیـابی تهدیـدات بـالقوه و تعیـین اقـدامات و الزامـات امنیتی در زمینه‌ی اینترنت اشیا، آنالیز ریسـک کمـی و کیفـی را اجرا کردند که به بررسی تهدیدات امنیتی در هر لایه می‌پردازد.

دوستی مطلق و همکاران **[۲۷]**، به بررسی طرحـی جدیـد بـا استفاده از ترکیب رمزنگاری کلاسیک و رمزنگاری کوانتومی برای ارتقای امنیت شبکه‌ی اینترنت پرداخته است.

عنوان پژوهشی مرتبط با سیستم‌های تشخیص نفـوذ مبتنـی بر ناهنجاری، آروا و همکاران[10] **[۳]**، با تجزیه و تحلیل راه‌حل‌ها و مطالعات تجربی و با بهره‌گیری نقش یادگیری عمیق در تشخیص نفوذ، کارایی و اثربخشی روش‌های پیشنهادی را بحث مـی‌کنـد و با شناسـایی چـالش‌هـای تحقیقـات گذشـته، دسـتورالعمل‌هـا و شناسه‌های مبتنی بر یادگیری عمیق توصیه می‌شود.

موراسی و همکاران**[۱]**، در پژوهشی علاوه بر ارائه‌ی مدل بـر اساس ترکیب شبکه‌های عصبی مصنوعی به‌منظور تشخیص نفوذ، روشی را برای استخراج ویژگی‌های بهینه، بـر روی مجموعـه داده Cup KDD ، کـه مجموعـه داده‌ی اسـتاندارد جهـت آزمـایش روش‌های تشخیص نفوذ در شـبکه‌هـای کـامپیوتری اسـت، ارائـه می‌نماید.

کوشش‌های تحقیقاتی در زمینه‌ی دستگاه‌های تشخیص نفوذ برای شبکه‌ی اینترنت اشیا آغاز و شتاب گرفته اسـت. بـا در نظـر گرفتن پیشینه‌ی پژوهش ارائـه‌شـده، ایـن نکتـه مهـم اسـت کـه راه‌حل‌های ارائه‌شده، نقـاط ضـعف و قـوت هـر روش تشـخیص و استراتژی قرار دادن را به‌طـور عمیقـی بررسـی نکـرده‌انـد. اغلـب نویسندگان بر روی انواع کمی از حمله‌ها و فناوری‌هـای اینترنـت اشیا تمرکز کرده‌اند. درنهایت، استراتژی‌های اعتبارسـنجی بسـیار ساده، زمینه را برای بازتولید رویکردهای پیشنهادی دیگـر فـراهم ساخته است.

۳- بیان مسئله

تشخیص نفوذ، انجام اقداماتی جهـت تشخـیص نفـوذگران و مهاجمان به داخل سیستم‌های اطلاعاتی است. این اقـدامات، کـه

[1] Midi et al
[2] Granjal et al
[3] Routing Protocol for Low-Power and Lossy Networks
[4] Datagram Transport Layer Security
[5] Constrained Application Protocol
[6] Le et al
[7] Atli et al
[8] Shigen Shen et al
[9] Klempous
[10] Ara et al

به‌عنوان نفوذ شناخته می‌شود، با هدف دسترسی غیرمجاز به سیستم‌های کامپیوتری صورت می‌گیرد. نفوذگران ممکن است کاربران داخلی یا خارجی باشند. نفوذگران داخلی درواقع کاربرانی در داخل شبکه با درجه‌های مختلف اجازه‌ی دسترسی هستند که تلاش می‌کنند درجه‌ی سطح دسترسی و امتیازات خود را برای سوءاستفاده از امتیازات غیرمجاز افزایش دهند. نفوذگران خارجی درواقع کاربرانی خارج از شبکه‌ی هدف هستند که تلاش می‌کنند تا دسترسی غیرمجازی به اطلاعات سیستم داشته باشند. **[۳۵]**.

سیستم تشخیص نفوذ شامل حسگرها، موتور تحلیل و سیستم گزارش‌دهی است. حسگرها در مکان یا میزبان‌های مختلف شبکه مستقر می‌شوند. وظیفه این حسگرها جمع‌آوری داده‌های شبکه یا میزبان از قبیل آمارهای ترافیکی ، سرآیند بسته‌ها، درخواست‌های سرویس و فراخوان‌های سیستم‌عامل است، که طبق معماری شبکه آن را در مکان‌های مختلف قرار می‌دهند. حسگرها داده‌های جمع‌آوری‌شده را به موتور تحلیل ارسال می‌کنند، که مسئولیت بررسی داده‌های جمع‌آوری‌شده و تشخیص نفوذهای در حال انجام را با رویکردهای مختلف مبتنی بر امضا، مبتنی بر ناهنجاری، مبتنی بر مشخصه و مبتنی بر روش ترکیبی دارد. وقتی موتور تحلیل، نفوذی را تشخیص می‌دهد، سیستم گزارش‌دهی، را با اطلاعات نفوذ شامل شناسایی نفوذکننده، محل نفوذ، زمان نفوذ و نوع نفوذ مجهز می‌کند و این سیستم هشداری را برای مدیر شبکه تولید می‌کند **[۳۲]**.

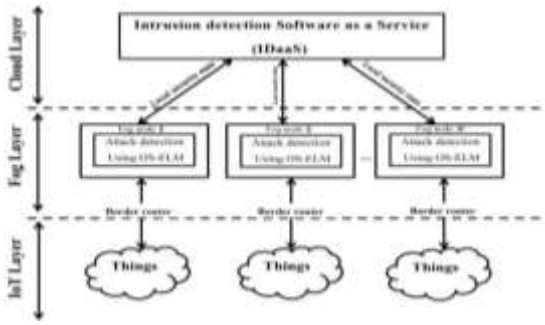
در شبکه‌های اینترنت اشیا، سیستم تشخیص نفوذ می‌تواند در استراتژی‌های مختلف، در یک یا چند میزبان اختصاصی، یا در هر شیء فیزیکی قرار بگیرد و در قالب سه استراتژی طبقه‌بندی می‌شود: به‌صورت متمرکز، به‌صورت توزیع‌شده و به‌صورت ترکیبی.

در حالت متمرکز، عوامل سیستم تشخیص نفوذ، در یک جزء متمرکز به‌عنوان‌مثال مسیریاب مرزی یا یک میزبان اختصاصی مستقر می‌شود.

بااین‌وجود، این حالت به جهت نیاز عوامل سیستم تشخیص نفوذ به جمع داده‌های زیادی از اشیا هوشمند، باعث ایجاد ارتباط بین اشیا هوشمند و مسیریاب مرزی می‌شود.

در حالت استراتژی قرارگیری توزیع‌شده، سیستم‌های تشخیص نفوذ در هر شیء فیزیکی قرار داده می‌شود که به‌طور بدیهی می‌تواند ارتباط فوق را کاهش دهد و درعین‌حال گنجایش مصرف منابع محدودشده‌ی اشیا هوشمند را افزایش دهد. اما برخلاف دو حالت اشاره‌شده، عوامل سیستم تشخیص نفوذ در حالت ترکیبی در گره‌ها یا نودهای نظارت به‌عنوان‌مثال گره نگهبان، مستقرشده است تا از مزایای استراتژی‌های متمرکز و توزیع‌شده بهره ببرد و از نقاط ضعف آن‌ها پیشگیری کند. این راه‌حل می‌تواند الزامات موردنیاز برای ارتباطات میان اشیا هوشمند و مسیریاب مرزی را کمتر و ظرفیت پردازش بیشتر را برآورده کند**[۳۲]**.

شکل (۱)، لایه‌های مستقل، سخت‌افزارها و نرم‌افزارهای عامل و نحوه‌ی قرار گرفتن و استراتژی‌های سیستم‌های تشخیص نفوذ را نشان می‌دهد که بیانگر این نکته است که سیستم‌های تشخیص نفوذ در شبکه‌های اینترنت اشیا مبتنی بر ابر- مه می‌توانند در مسیریاب مرزی در یک یا چند میزبان اختصاصی، یا در هر شیء فیزیکی قرار بگیرند.



شکل۱. زیرساخت‌های سیستم تشخیص نفوذ برای شبکه‌های اینترنت اشیا

امروزه برای برقراری امنیت و ارتباطات و تبادل اطلاعات در فضای مجازی اقدامات متنوعی از قبیل رمزنگاری اطلاعات، طراحی پروتکل‌های امن، به‌کارگیری دیواره‌های[1] آتش و سیستم‌های ردیابی و جلوگیری از نفوذ از طریق سیستم‌های تشخیص نفوذ انجام شده است. در برخی از روش‌های تأمین امنیت در شبکه‌ها مانند استفاده از سیستم‌های ردیابی نفوذ و یا دیواره‌های آتش نیاز است که بر اساس برخی داده‌ها تصمیم‌گیری صورت بگیرد و طبق آن یک سیاست خاص امنیتی در شبکه اتخاذ شود. برای انجام این‌گونه فرآیندها در سیستم‌های امنیتی شبکه و بهینه کردن آن‌ها تاکنون از ابزارهای گوناگون ریاضی چون روش‌های آماری آزمون فرض، نظریه‌ی تصمیم، روش شناسایی الگو، یادگیری ماشین، نظریه‌ی گراف، نظریه‌ی کنترل استفاده شده است. اما ازآنجاکه در بسیاری از حوادث امنیتی ایجادشده در شبکه، مهاجم یک انسان و یا یک برنامه‌ی هوشمند است، نیاز به روشی است که بتواند نحوه‌ی تصمیم‌گیری یک مهاجم هوشمند را، که به‌تناسب اقدامات پیشگیرانه و متقابل مدافعین، استراتژی‌هایش را تغییر می‌دهد،

[1] Firewall

مدل کند. بـه همـین دلیـل در دهـه‌ی اخیـر تـلاش‌هـایی بـرای به‌کارگیری نظریه بازی‌ها در حوزه‌ی امنیت شبکه آغاز شده است.

نظریه‌ی بازی‌ها، ازآنجاکه اصولاً برای مدل‌کردن و بهینه‌سازی تصمیم در شرایطی که چند عامل هوشمند به تقابل یا تعامـل بـا هم می‌پردازند ابداع‌شده است، ابزاری مناسـب بـرای اسـتفاده در بسیاری از مسائل مطرح در امنیت شـبکه اسـت. تـاکنون از ایـن نظریه در مسائلی چون تخصیص بهینه‌ی منابع، نحـوه‌ی طراحـی امن توپولوژی شبکه، پیکربندی بهینه سیستم‌های ردیابی نفـوذ و دیواره‌های آتش استفاده شده است.

با توجه به حجم انبوه داده‌هایی کـه یـک سیسـتم تشـخیص نفوذ با آن روبه‌رو است، به‌کـارگیری یـک ابـزار قـوی کـه بتوانـد سیستم تشخیص نفـــوذ را قادر سازد، با کـــاوش در میان حجـم انبـوه داده‌هـای شـبکه، نتـــیجه‌ی مطلـــوب را حاصـل کنـــد، اجتنـاب‌ناپـذیر اسـت. یکـی از ابزارهـای قدرتمنـد، اسـتـفاده از سیسـتم‌های مبتنی بر نظریه‌ی بازی است. نظریـه بـازی در حـل بهینه‌سازی منابع و هزینه‌ها در حوزه‌ی اقتصادی موفقیت بزرگـی کسب کـرده اسـت، به همین دلیل در سـال‌های اخیـر موردتوجه محقـقان سایر زمینه‌ها نیز قرارگرفته است [۱].

نظریه‌ی بازی مبتنی بر رفتار هر بازیکن است و می‌توانـد بـر اساس همکـــاری یا نداشتن همکاری در یک بـازی مشـــارکتی باشد [۳۰].

در چنـد سـال اخیـر ارائـه‌ی اسـتنتاج‌هـای ریاضـــی بـرای شـــبکه‌های بی‌سیم بـا اسـتفاده از روش‌هـای نظـــریه‌ی بـازی بسیار موردتوجه قرارگرفته است. ازآنجایی‌کـه نظـــریـــه بـازی‌هـا یـک ابـزار طبیـــعی و قابـل‌انعطـاف بـرای مطالعـه‌ی کـاربران هـوشـمند و تصمیم‌گیرنده اسـت، بنـابراین تقابـل و همکـــاری کاربران خودکار در شبکه‌های بی‌سیم نیز می‌تواند بـا ایـن ابـــزار بررسی شود[۱۱]. بنابراین اگر مسئله‌ی امنیت و تشخیـص نفوذ از دیدگاه نظریه‌ی بازی‌ها مورد بررسی قرار گیرد، به نقاط مشترکی بین این مسئله و مدل‌های موجود در این نظریه مـی‌تـوان دسـت یافت.

در این پژوهش قصد داریم تعاملات بین مهاجمان و سیسـتم تشخیص نفوذ را به‌صورت یک بازی دو نفره‌ی پویا مدل کنیم. در نظریـه‌ی بـازی‌هـا، بـازی غیرمشـارکتی، بـازی اسـت کـه در آن بازیکنان به‌هیچ‌وجه نمی‌توانند با هم تبادل یـا مـذاکره‌ای داشـته باشند و به توافقی برسند و یا به ائتلافی دست بزنند.

انتخاب و بهره‌گیری از بازی غیرمشارکتی، بـه دلیـل ماهیـت تعاملات بین سیستم تشخیص نفـوذ و زیرسیسـتم‌هـای شـبکه‌ی اینترنت اشیا است. درواقع ایـن تعاملات به‌صورت یک بازی پویا با اطلاعات کامل است، که در آن سیستم تشـخیص نفـوذ در مـورد نوع عملـکرد بازیکن مقابل قطعیت ندارد.

۴- اطلاعات و داده‌ها

عناصر اصلی در نظریه‌ی بازی‌ها شامل بازیکنان، عمل‌هـا، سـود و اطلاعات است که مجموعه‌ی این عناصـر بـه‌عنـوان قواعـد بـازی شناخته می‌شود.

در مدل‌سازی با استفاده از نظریه‌ی بازی‌هـا، هـدف طراحـی شرایطی بر اساس قواعد بازی است، تا بیان شـود کـه در شـرایط خاص، چه اتفاقاتی رخ خواهد داد. نظریه‌ی بـازی‌هـا، مبتنـی بـر رفتار هر بازیکن است و بازیکنان با تلاش برای افزایش سود خـود در بازی، تصمیماتی را اتخاذ می‌کنند که به آن‌ها استراتژی گفتـه می‌شود[۱۹]. به همین جهت، نظریه‌ی بازی‌ها را می‌توان به‌عنوان علم مدل‌سازی و بررسی سیستم‌های تصمیم‌گیرنده تعریف کرد.

در پژوهش حاضر، مدل‌سازی بازی پویا بر اساس زمان، کامل بر اساس اطلاعات و به‌صورت استراتژیک تعریف می‌شود. دو شرط زیر را در مدل پیشنهادی رعایت کرده و مدنظر قرار داده‌ایم:

[۱] بازیکنان نسـبت بـه تمـامی پارامترهـا و قواعـد بـازی آگاهی و دانش کامل دارند.

[۲] حداقل یکـی از بازیکنـان از اسـتراتژی بـازیکن دیگـر بی‌اطلاع است و این‌گونه، ابتدا بازیکن اول حرکت خـود را انجـام می‌دهد، سپس بازیکن دوم با اطلاع از عمـل انتخـابی بازیکـــن اوّل حرکت (عملگر) خود را انتخاب می‌کند.

یکی از مهم‌ترین عناصر در توصیف بازی، تعریـف بازیکنـان و تعیین ترجیحات بازیکنان از طریق تابع سود اسـت. در مدل بازی پیشنهادی ارائه‌شده، یک بازیکن مهاجم احتمالی است و بـازیکن دیگر، مدافع، سیستم تشخیص نفوذ است.

$\mathcal{N} = \{$سیستم تشخیص نفوذ , مهاجم احتمالی$\}$ بازیکنان

$\mathcal{S}_1 = \{$عدم حمله , حمله$\}$ استراتژی بازیکن اوّل

$\mathcal{S}_2 = \{$عدم هشدار , هشدار به واسطه تشخیص$\}$ استراتژی بازیکن دوّم

با توجه به تعاریف ارائه‌شده، سیستم تشخیص نفوذ با شبکه‌ی گره‌های هوشمند $S = \{s_1, s_2, \dots, s_P\}$ را در نظـر مـی‌گیـریم کـه گره‌های هوشمند به‌عنوان یک نرم‌افزار عامل تعریف‌شـده اسـت و حملات احتمالی در زیرسیستم بزرگ اینترنت اشیا را با استفـاده از رویکـــردهای مختلف مبتنی بر امـضا، مبتـــنی بر ناهنجاری، مبتنـی بـر مشخصـه و بـه روش ترکـــیبی گـزارش مـی‌کنـد. هشدارهای گزارش‌شده از طریـق سیستـــم تشـخیص نفـــوذ را می‌توان به‌صورت مجموعه‌ای از زیرسیستم‌ها شـامل برنامـه‌هـای کامپیوتری یا اجزای شبکه و فرایندهای مستقل توزیـع‌شـده روی میزبان‌های متعدد به‌صورت $A = \{a_1, a_2, \dots, a_M\}$ نمایش داد، که هـــدف یـک مهـاجم اسـت. مجموعـه‌ی $T = \{t_1, t_2, \dots, t_K\}$ را به‌عنوان مجموعـه‌ای از تهدیـدهای ثبـت‌شـده‌ی قابـل‌تشـخیص تـعریف می‌کنیم که هـر عضـو مجموعـه، یـک نفـوذ مـــمکن را

نـــشان می‌دهد. خصوصیات یکی از عناصر Tرا با تخصیص آن به یک یا چند کلاس تابع میان $\{F_1, F_2, \dots\}$ می‌توان توصـیف نمـود که هر کلاس تابعF ، معرف یک خصوصیت مشترک از اعـضایش است.

به جهت توانایی تشخیص بیش از یک نفوذ از طریق گره‌های هوشمند، با نگاشت از مجموعه‌ی S به مجموعه‌ی $T \cup \{0\}$ ، بردار خروجـی شـبکه‌ی گـره‌هـای هوشـمند $d = \{d_1, d_2, \dots, d_L\}$ را تعریف کنیم به‌طوری‌که $L \geq P$. عنصر i اُم، بردار خروجی مـرتبط با گره هوشمند $s_j \in S$ ، به شـکل $d_i(s_j)$ برابـر بـا یـک اسـت، درصورتی‌که گره هوشمند، نفوذ ممکن $t_k \in T$ را تشـخیص داده باشد؛ در غیر این صورت، $d_i(s_j) = 0$.

بنابراین با توجه به استدلال بالا، و در نظر گرفتن این‌کـه هـر حسگر هوشمند قادر به گزارش حداکثر یکی از هر نوع نفوذهـای ممکن است، خواهیم داشت:

$$d_i(s_k) \neq d_j(s_k) \perp i, j, k > 0 , s_k \epsilon S \quad (۱)$$

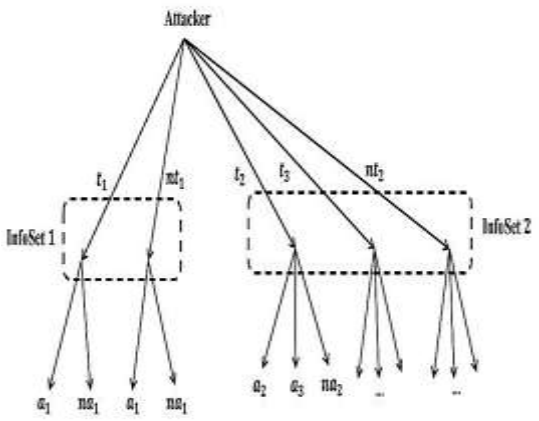
مگر درصورتی‌که:

$$d_i(s_k) \neq d_j(s_k) \quad (۲)$$

حال با بهره‌گیری از تعاریف و فرضـیات موجـود بـازی ، مـاتریس سیستم M را با توصیف رابطه‌ی بین بردار خروجی گره هوشمندj و زیرسیستم ابه‌صورت ماتریس (۳) تعریف می‌کنیم:

$$M_{i,j} = \begin{cases} 1 & \text{گره هوشمند } j \text{، نفوذ ممکن } i \text{ را تشخیص و هشدار دهد} \\ 0 & \text{گره هوشمند } j \text{، هشداری برای نفوذ } i \text{ را ندهد} \end{cases} \quad (۳)$$

در درخت بازی شکل (۲)، پارامترهای t_1، t_2 و t_3 بـه‌عنـوان تهدیدهای هدف زیرسیستم‌های ۱، ۲ و ۳ از سـوی مهـاجم، nt_1 وnt_2 معـرف عملگـر عـدم حملـه از سـوی مهـاجم، a_1، a_2 و a_3 هشدارهای سیستم تشخیص نفوذ برای زیرسیستم‌های مربـوط و na_1 و na_2 تعیین نکردن یک هشدار از سوی سیستم تشـخیص نفوذ را نشان می‌دهد.



شکل (۲): فـرم بسط‌یافته‌ی بازی پیشنـهادی با دو مجموعه‌ی اطـلاعاتی و سه زیرسیستم

درخت مدل‌سازی شده در شکل (۲) را که بیانگر نمونـه‌ای از بازی پیشـــنهادی با دو مجموعه‌ی اطلاعـاتی و سـه زیرسیسـتم اسـت مـی‌تـوان بـه روش بازگشـتی موردمطالعـه قـرارداد. در مجموعه‌ی اطلاعاتی اول ، کـه تهدیـد تعریـف‌شـده t_1 از سـوی مهاجم، زیرسـیستم اول را هـدف قرار می‌دهـد، یـا کـاری انجـام نمی‌دهـد (nt_1). مـجموعه‌ی اعمـال سیسـتم تشـخیص نفـوذ، گزارش هشدار برای زیرسیستم اول با معرف a_1 یا ارسال نکـردن هشدار با معرف a_2 است. درنتیجه با بهره‌گیـری از درخـت بـازی شکل (۲) و تعـاریف مـی‌تـوان ماتریسـی 2×2 بـازی و نحـوه‌ی عملکرد استراتژی‌ها را در جدول (۱) نمایش داد.

جدول (۱): توصیف پارامتری استراتژی‌های نظیربه‌نظیر مجموعه‌ی اطلاعاتی اول

Q_{Attack}	t_1	β_h	$-\beta_s$
	nt_1	0	0
		a_1	na_1

Q_{IDS}	t_1	$-\alpha_h$	α_m
	nt_1	α_f	0
		a_1	na_1

همواره $\alpha, \beta \geq 0$

که پارامترهای تعریف‌شـده Q_{IDS} و Q_{Attack}در جـدول (۱)، مقادیر تابع سود هریک از بازیکنان را نشان می‌دهـد و سـطرها و ستون‌های نظیربه‌نظیر مـاتریس، عملکـرد و فضـاهای اسـتراتژی بازیکنان، سیستم تشخیص نفوذ و مهاجم است. مقدار $-\alpha_h$بهره‌ی سیستم تشخیص نفوذ بـه‌ازای گـزارش هشـدار تشـخیص هـدف است. از طرف دیگر، α_f وα_m هزینه‌های سیستم تشـخیص بـرای هشدار غلط و از دست دادن حمله را نشان مـی‌دهـد. هزینـه β_h مجازات تشخیص برای مهاجم و $-\beta_s$ بهره‌ی حاصل از یک نفـوذ تشخیص داده نشده را نشان می‌دهد.

درنتیجه، استراتژی‌های بازیکن سیستم تشخیص نفوذ به مقادیر نسبی α_f وα_m و هشدار غلط و هزینه‌های از دست دادن یک حمله و تهدید بستگی دارد. اگر $\alpha_f > a_m$ ، آنگاه سیستم تشخیص نفوذ هشداری را نخواهد داشت (معرف$n\alpha$) و در حالت دیگر اگر $\alpha_f < a_m$، آنگاه سیستم تشخیص نفوذ همواره یک هشدار را مشخص می‌کند (معرفα).

۵- یافتن بهترین پاسخ ، تجزیه وتحلیل تعادل نش بازی

وجـود تعـادل نـش در مـاتریسQ_{IDS} را مـورد پـژوهش قـرار

مـی‌دهـیم. بـا در نظـر گـرفتن اسـتراتژی‌هـای نظیربـه‌نظیـر بازیکنـان تعریـف‌شـده بـه‌صـورت توزیـع‌هـای احتمـال روی فضای استراتژی‌هـای معـین، نتـایج را توسـعه مـی‌دهـیم. فـرض مـی‌کنـیم P_1و $P_1 - 1$ احتمـالات اسـتراتژی‌هـای t_1 و nt_1 بـازیکن مهـاجم هسـتند و هـم‌چنـین فـرض مـی‌کنـیم q_1 و $1 - q_1$ احتمـالات اسـتراتژی‌هـای a_1 و na_1 سیسـتم تشخیص نفـوذ باشـند. حـال زوج (P^*, q^*) یـک‌راه حـل تعـادل نـش غیرهمکـاری بـرای عملگـر بـازی مـاتریس 2×2، (Q_{Attack}, Q_{IDS}) ارائـه مـی‌دهـد بـه شرطـی کـه نامساوی‌های (۴) و (۵) درست باشند:

$$p_1^*(\beta_h q_1^* - \beta_s(1 - q_1^*)) \le p_1(\beta_h q_1^* - \beta_s(1 - q_1^*)) \quad (۴)$$

$$\begin{aligned} \mathrm{p_1^* a_m} + \mathrm{q_1^*[a_f - (a_f + a_h + a_m)p^*]} \\ \le \mathrm{p_1^* a_m} \\ + \mathrm{q_1[a_f - (a_f + a_h + a_m)p^*]} \end{aligned} \quad (۵)$$

که : $0 \le p_1, q_1 \le 1$.

تنها راه‌حل برای مجموعه‌ی نامساوی‌های ارائه‌شده بـه‌عنـوان پارامترهای بهترین پاسخ، تشکیل تعادل نش منحصربه‌فـرد بـازی که از طریق رابطه‌های (۶) و (۷) به دست می‌آید:

$$p_1^* = \frac{a_f}{a_f + a_h + a_m} \quad (۶)$$

$$q_1^* = \frac{\beta_s}{\beta_h + \beta_s} \quad (۷)$$

و هم‌چنین هزینه‌های تعادلی مهاجم Q^*_{Attack} و سیستم تشخیص نفوذQ^*_{IDS} برای ماتریس زیر بازی طراحی‌شده جدول (۱)، از رابطه‌های (۸) و (۹) به دست می‌آید:

$$Q^*_{Attack} = [p_1^*(1 - p_1^*)]Q_{Attack}[q_1^*(1 - q_1^*)]^T \quad (۸)$$

$$Q^*_{IDS} = [p_1^*(1 - p_1^*)]Q_{IDS}[q_1^*(1 - q_1^*)]^T \quad (۹)$$

با توجه به رابطـه‌هـای تعـادل نـش (۶) و (۷) و پارامترهـای بهتـرین پاسـخ رابطـه‌هـای (۸) و (۹)، احتمـال اینکـه مهـاجم، زیرسیستم اوّل را در نقطه تعادل نش موردحمله و هدف خود قرار دهد، با کاهش a_f، کاهش می‌یابد، زیرا هرچه هزینه‌های گـزارش نشدن هشدار برای سیستم تشخیص نفوذ کمتر باشـد، بـه همـان نسبت بیشتر گرایش به تعیین یک هشدار و گیر انداختن مهـاجم پیدا می‌کند. پس به طبـع، افـزایش a_h و a_m نقـش بازدارنـده‌ای برای مهاجم ایفا می‌کنـد و هـم‌چنـین ، احتمـال اینکـه سیسـتم تشخیص نفوذ، یک هشـدار را مشـخص کنـد، تحـت تـأثیر سـود مهاجم از نفوذ موفق، $-\beta_s$ است.

تحلیل پارامتری برای مجموعه‌اطلاعات دوم را با برقراری ارتباط بین هزینه‌ها در زیرسیستم‌های دو و سه و در قالب ماتریسی 2×2، جدول (۲) بررسی می‌کنیم:

جدول (۲) توصیف پارامتری استراتژی‌های نظیربه‌نظیر مجموعه اطلاعاتی دوم

	t_2	β_h	$-\beta_d$	β_s
Q_{Attack}	t_3	$-\beta_d$	$-\beta_h$	$-\beta_s$
	nt_2	۰	۰	۰
		a_2	a_3	na_2
	t_2	$-\alpha_h$	α_d	α_m
Q_{IDS}	t_3	α_d	$-\alpha_h$	α_m
	nt_2	α_f	α_f	۰
		a_2	a_3	na_2

همواره $\alpha, \beta \ge 0$

در جدول (۲) α_d و $-\beta_d$ هزینه‌ی فریب برای سیستم تشخیص نفوذ و مهاجم است. می‌توان این‌گونه فرض نمود $a_d > a_m$ و $\beta_d > \beta_s$، زیرا هشدار ندادن سیستم تشخیص نفوذ بسیار هزینه‌بردارتر از حمله نکردن است و با فریب سیستم تشخیص نفوذ ، مهاجم، مکانیسم‌های امنیتی را درگـیر اختلال می‌کند. فرض می‌کنیم $\bar{p}_1$ ، $\bar{p}_2$ و $1 - \bar{p}_1 - \bar{p}_2$ احتمالات استراتژی‌های t_2 ، t_3 و nt_2 مهاجم و هم‌چنین فرض می‌کنیم $\bar{q}_1$ ، $\bar{q}_2$ و $1 - \bar{q}_1 - \bar{q}_2$ احتمالات مربوط به استراتژی‌های a_1 ، a_2 و na_2 سیستم تشخیص نفوذ است. استراتژی عملگر سیستم تشخیص نفوذ با مقادیر نسبی هم چون رابطه‌های (۱۰) و (۱۱) ارائه می‌شود.

$$\bar{p}_1^* = \bar{p}_2^* = \frac{a_f}{2a_f + 2a_m + a_h - a_d} \quad (۱۰)$$

$$\bar{q}_1^* = \bar{q}_2^* = \frac{\beta_f}{2\beta_s + \beta_h - \beta_d} \quad (۱۱)$$

درصورتی‌که $\beta_d < \beta_h$ و $a_d < 2a_f + 2a_m + a_h$.

درنهایت ، استراتژی تعادل سیستم تشخیص نفوذ را می‌توان به شکل رابطه (۱۲) ارائه کرد :

$$\begin{cases} a_1 \; With \; Probability \; q_1^* \\ na_1 \; With \; Probability \; 1 - q_1^* \\ \\ a_2 \; With \; Probability \; \bar{q}_1^* \\ a_3 \; With \; Probability \; \bar{q}_2^* \\ na_1 \; With \; Probability \; 1 - \bar{q}_1^* - \bar{q}_2^* \end{cases} \quad (۱۲)$$

۶- ارزیابی و اعتبار مدل بازی پیشنهادی

معماری تشخیص نفوذ امروز، یک الگوی پردازش اطلاعات غیرفعال است. بااین‌حال، با وفور و پیچیدگی بیشتر حملات امنیتی، سیستم‌های تشخیص نفوذ قادر به تمایز قصد و نیت حقیقی و هدف مهاجمیان نیست. برای شناسایی و تشخیص درست هدف یک حمله، سیستم‌های تشخیص نفوذ باید توانایی پردازش اطلاعات حمله در متن را داشته باشد. با استقرار شبکه‌ی حسگرها در سیستم و از طریق تحلیل نظریه بازی داده‌های خروجی حسگر، می‌توان رفتار، نیت و هدف مهاجم را مدل‌سازی نمود. به‌علاوه، به خاطر انعطاف‌پذیری مدل بازی پیشنهادی، نه‌تنها حملاتی که بخش‌های خاصی از شبکه را هدف قرار می‌دهد، ، بلکه هم‌چنین اهداف مجردی نظیر فرآیندهای توزیع‌شده روی زیرسیستم‌های فیزیکی متعدد را می‌توان به دست آورد. علاوه بر مدل‌سازی رفتار و نیت مهاجم، از چارچوب نظریه بازی با محاسبه روابط جانشینی امنیت و نکات آماری می‌توان برای تحلیل و مدل‌سازی فرایند پاسخ سیستم تشخیص نفوذ نیز استفاده نمود. اعمال پاسخ و واکنش سیستم تشخیص نفوذ از تنظیم هشدار ساده تا پیکره‌بندی مجدد هزینه‌بر سیستم متغیر بوده و شامل خاموش کردن سرویس‌های نسبتاً کم‌اهمیت‌تر در سیستم می‌شود.

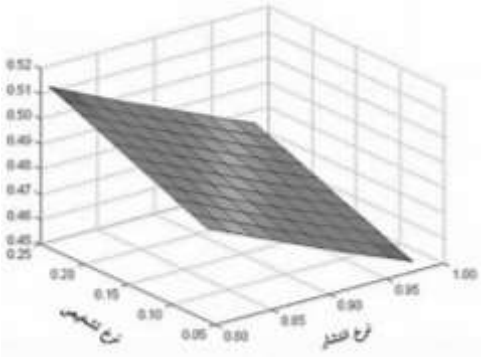
در این بخش، ابتدا با انجام آزمایش‌های عددی در محیط نرم‌افزاری متلب، چارچوب نظری و تئوریک بازی پیشنهادی خود را از قبل اعتبار بخشیدیم و برای پژوهش و تشریح تعادل نش نمونه‌های عددی، در استراتژی‌های مختلط و رفتاری، بین بردار مهاجم با اعمال$[t_1, t_2, t_3, nt_1, nt_2]$ و بردار سیستم تشخیص نفوذ با اعمال $[a_1, a_2, a_3, na_1, na_2]$ ارتباط برقرار کردیم و طبق روابط ۶، ۷، ۱۰ و ۱۱ به محاسبه تعادل نش پرداختیم. سپس با واردکردن مدل بازی پیشنهادی به شبکه‌های اینترنت اشیا با استفاده از IDSaaS مبتنی بر ابر-مه، یک برنامه‌ی بالقوه ارائه می‌دهیم.

همان‌طور که در مدل بازی پیشنهادی، سیستم تشخیص نفوذ و مهاجم احتمالی در چند استراتژی مختلف تقابل و بازی می‌کنند، در هر مرحله نتایج بازی نیز مشاهده و ضبط شده است. از این نتایج به‌دست‌آمده، چند نکته‌ی آماری را ارائه و محاسبه می‌کنیم.

معیارهای نرخ بهینه‌ی شیء هوشمند به‌عنوان مهاجم با انتخاب انتشار و احتمال آلودگی‌های بعدی موردتوجه قرارگرفته است. دلیل انتخاب این معیار، می‌تواند پارامترهای مؤثری بر رفتار یک شی هوشمند در شبکه را مشخص کند و هم‌چنین اصول قضاوت به هنگام درباره این‌که شیء هوشمند مهاجم آلوده است یا خیر.

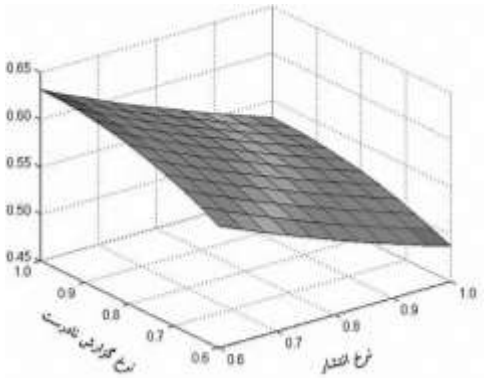
در آزمایش در محیط نرم‌افزاری، پارامترهای استراتژی‌های مختلف بازی به‌طور خاص مقداردهی شده است، اگرچه مقادیر این پارامترها را به‌طور منطقی تغییر دهیم، می‌توانیم به روندهای مشابه به سمت نقاط آماری برسیم. بنابراین اعتقاد بر این است که نتایج عددی بعدی برای نشان دادن خصوصیات مدل بازی پیشنهادی، با توجه به پارامترهای استراتژی‌های مختلف، مفید است و می‌تواند به‌راحتی برای موقعیت‌های خاص‌تر دوباره تولید شود.

گرایش نرخ بهینه انتشار یک شی هوشمند را از نظر میزان آشکارسازی رفتار شی هوشمند با تعریف مؤلفه‌های، نرخ تشخیص، نرخ گزارش نادرست و نرخ انتشار نشان می‌دهیم. بدیهی است، نرخ تشخیص بالاتر و نرخ گزارش نادرست پایین‌تر، به IDSaaS اجازه می‌دهد تا یک شیء هوشمند مهاجم را راحت‌تر به دام بیاندازد، که درنتیجه همان‌طور که در شکل ۵-۱ مشخص است، این امر باعث می‌شود بدافزار موجود در شیء هوشمند مهاجم تلاش کمتری برای انتشار خود کند و ازاین‌رو نیز، باعث کاهش نرخ انتشار می‌شود.



شکل (۱): نرخ انتشارشی هوشمند مهاجم بر اساس در نظر گرفتن پارامتر نرخ تشخیص

علاوه‌براین، نرخ گزارش اشتباه بیشتر به معنای آن است که نرخ تشخیص کاهش می‌یابد و نمی‌توان با توجه به اهداف پژوهش، از حریم خصوصی بیشتری در شبکه‌های اینترنت اشیا محافظت کرد و نتیجه می‌شود که یک شیء هوشمند مهاجم، انتشار را با نرخ بالاتر پیش می‌گیرد، زیرا با احتمال کمتری سیستم تشخیص نفوذ می‌تواند آن را شناسایی کند. همان‌طور که انتظار می‌رود، گرایش‌های واقعی پیاده‌سازی در شکل، تحلیل ارائه‌شده را تأیید می‌کند.



شکل (۲): نرخ انتشارشی هوشمند مهاجم بر اساس در نظر گرفتن پارامتر نرخ گزارش نادرست

بااین‌وجود عوامل مختلف تأثیرات متفاوتی در بازیکنان مـدل بازی پیشنهادی دارد که بر نرخ استراتژی‌های مختلف تشخیص و نرخ انتشار اثرگذار است. به عنوان مثال هنگامی‌که در مـدل بـازی پیشنهادی بـا افـزایش نـرخ گـزارش نادرسـت از ۰/۵۵ بـه ۰/۹۹ روبه‌رو می‌شـویم، تغییـرات نـرخ انتشـار از ۰/۵۸۳۹ بـه ۰/۶۵۲۸ افزایش می‌یابد، افزایش تا ۱۱/۵۷٪؛ و هم‌چنـین زمـانی کـه نـرخ تشخیص از ۰/۹۹ به ۰/۵۵ ارائه می‌شود، تغییـرات نـرخ انتشـار از ۰/۴۶۲۱ به ۰/۸۷۰۸ افزایش می‌یابد، یعنی افـزایش تـا ۸۸/۴۴٪. این مسئله در پیاده‌سـازی نشـان مـی‌دهـد کـه کـاهش در نـرخ تشخیص باعث می‌شود شیء هوشمند آلوده نرخ انتشار بالاتری را از افزایش نرخ گزارش نادرست ارائه دهد.

۷- یافته‌های پژوهش، جمع‌بندی و نتیجه‌گیری

در پژوهش حاضـر یـک مـدل بـازی اسـتراتژیک ، پویـا و کامـل به‌منظور تشخیص نفوذ حملات در شـبکه‌هـای اینترنـت اشـیا در سیستم تشخیص نفوذ توزیـع‌شـده تعریـف‌شـده اسـت. پـژوهش تحلیلی بازی در قالـب زیربـازی‌هـای ماتریسـی 2 × 2 و یـافتن پارامترهای بهترین پاسخ در تعادل نش، بیـنش‌هـای ارزشـمندی برای مهاجم و رفتار تشخیص نفوذ به ارمغان مـی‌آورد. بـه‌عـلاوه، برای دسـتیابی بـه سـناریوهای واقـع‌گرایانـه‌تـر، فرضـیات سـاده مطرح‌شده جهت دستیابی به نتایج تحلیلی را، به‌راحتی مـی‌تـوان بسـط و توسـعه داد و سیسـتم تشـخیص نفـوذ بـا حسـگرهای هوشمند، که به‌عنوان یک نرم‌افزار عامل تعریف‌شده است، حملات در زیرسیستم بزرگ اینترنت اشـیا را بـا اسـتفاده از رویکردهـای مختلف مبتنی بر امضا، مبتنی بر ناهنجاری، مبتنی بر مشخصـه و به روش ترکیبی گزارش می‌کند .بنابراین می‌توان این‌گونه مطـرح کرد که با توجه به راه‌حل‌های تعادلی و هزینه‌های هر زیربازی در ماتریس‌های ارائه‌شده، سیستم تشخیص نفوذ و مهـاجم، عملکـرد استراتژی‌های خود را مـشخص می‌کننـد. وجـه تمـایز و نـوآوری به‌کاررفته در مقایسه با کارهای مرتبط نیز، ارائه‌ی یک مدل بازی برای تشخیص حملات در اینترنت اشیا مابین گره‌هـای حسـگر و سـرور پلتفـرم اسـت کـه بـا هـدف تشـخیص تعـداد بیشـتری از کلاس‌های حملات، نرخ تشخیص درست و به حداقل رساندن نرخ تشخیص اشتباه مورد استفاده قرار گرفته است.

درنتیجه این نکته حائز اهمیت را از پژوهش حاضر مـی‌تـوان دریافت که دیگر اقدامات امنیتی رایج و معمول و هم‌چنین اجرای حریم خصوصی نمی‌تواند به‌طور مستقیم به فناوری‌های اینترنـت اشیا اعمال شود. به همین جهت توسـعه‌ی راه‌حـل‌هـای امنیتـی خاص همچون سیستم‌های تشخیص نفـوذ ضـروری اسـت تـا بـه کاربران و سازمان اجازه دهد تمام نقاط ضعف و حملات سیسـتم خود را شناسایی و ترمیم کنند.

۷- منابع

[1] A. Marosi, E. Zabah, H. Ataee khabaz.,2020. Network intrusion detection using a combination of artificial neural networks in a hierarchical manner (in Persian), Journal of Electronical & Cyber Defence ,Vol 8, pp. 89-99.

[2] Abduvaliyev, A., Pathan, A.S.K., Jianying, Z., Roman, R., Wai-Choong, W., 2013. On the vital areas of intrusion detection systems in wireless sensor networks. IEEE 15 (3), 1223–1237.

[3] Arwa Aldweesh, Abdelouahid Derhab., 2020. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems. Vol 189.

[4] Atzori, L. Iera, A., Morabiti, G., 2010. The internet of things: A survey, computer Network, V54, 15, 2787-2805.

[5] Borgia, E., 2014. The Internet of Things vision: key features, applications and open issues. Comput Commun.54, 1-31.

[6] Butun, I., Morgera, S., Sankar, R., 2014. A survey of intrusion detection systems in wireless sensor networks. Commun. Surv. Tutor. IEEE 16 (1), 266–282.

[7] Butun, I., Morgera, S.D., Sankar, R., 2014. A survey of intrusion detection systems in wireless sensor networks. IEEE Commun. Surv. Tutor. 16 (1), 266–282.

[8] Cervantes, C., Poplade, D., Nogueira, M., Santos, A., 2015. 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), 606–611.

[9] Dewan, F., Nouri, H., & Mohammad, R., 2010, Combining Native Bayes and Decision tree for Adaptive Intrusion Detection. International Journal of Network Its Security & Application, 2, 12-25.

[10] D. Midi, A. Rullo, A. Mudgerikar, E. Bertino, Kalis., 2017. A system for knowledge-driven adaptable intrusion detection for the internet of things, in: Proceed- ings of the IEEE Thirty-Seventh International Conference on Distributed Computing System(ICDCS), 2017, 656-666.

[11] Fotini, Pavlidov, Georgios Koltsidas., 2010. Game theory for routing modeling in communication networks – a survey, Journal of Communications and Network, 10(30), 268-286.

[12] Jin, Du., 2012 .Application of IOT in electronic commerce, Journal of Digital Content Technology and its Application,6.

[13] Granjal, E.Monteiro, J.s. Silva., 2015. Security for the internet of things: a survey of existing protocols and open research issues. iEEE.17(3), 1294-1312.

[14] Granjal, J., Monteiro, E., Silva, J.S., 2012. On the effectiveness of end-to-end security for Internet-integrated sensing applications. In: Green Computing and Communications (GreenCom), IEEE, 87–93.

[15] Kim, A.N., Hekland, F., Petersen, S., Doyle, P., 2008. When HART goes wireless: understanding and implementing the WirelessHART standard, In: 2008 IEEE International Conference on Emerging Technologies and Factory Automation, 899–907.

[16]] Kim, D., Ro, W.W., 2014. A malicious pattern detection engine for embedded security systems in the Internet of Things. Sensors 14 (12), 24188–24211.

[17] Klempous, Ryszard, et al., 2007. Adaptive misbehavior detection in wireless sensors network based on local community agreement. 14th Annual IEEE International Conference and Workshops on the Engineering of Computer- Based System.

[18] Kumar, S., Dutta, K., 2016. Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges. Secur. Commun. Netw. 9 (14), 2484–2556.

[19] [19] M. Foroghi, A. Akrami zadeh, M. Bagheri.,2018. The decision model in a cyber-conflict with injury, with a game theory approach (in Persian), Journal of Electronical & Cyber Defence ,Vol 8, pp. 89-99.

[20] Mitchell, R., Chen, I.-R., 2014. A survey of intrusion detection techniques for cyberphysical systems. ACM Comput. Surv. (CSUR) 46 (4), 55.

[21] Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I., 2012. Internet of things: vision, applications and research challenges. Ad Hoc Netw. 10 (7), 1497–1516.

[22] Mishra, A., Nadkarni, K., Patcha, A., 2004. Intrusion detection in wireless ad hoc networks. IEEE Wirel. Commun. 11 (1), 48–60.

[23] Midi, S., Krishna, P., Agarwal, H., Saxena, A., Obaidat, M., 2011. A learning automata based solution for preventing Distributed Denial of Service in Internet of Things. In: Internet of Things (iThings/CPSCom), International Conference on and Proceedings of the 4th International Conference on Cyber, Physical and Social Computing, 114–122.

[24] Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I., 2012. Internet of Things: vision, applications and research challenges. Ad Hoc Netw.10(7).1497-1516.

[25] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., Rajarajan, M., 2013. A survey of intrusion detection techniques in Cloud. J. Netw. Comput. Appl. 36 (1), 42–57.

[26] Mudgerikar, A., Sharma, p., & Bertino, E.,2019. A system- level Intrusion Detection System for IoT Devices. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, 493-500.

[27] N. Dosti.,2019. New mechanism to enhance IoT network security using quantum and classical cryptography (in Persian), Journal of Electronical & Cyber Defence ,Vol 4.

[28] Pongle, P., Chavan, G., 2015. Real time intrusion and wormhole attack detection in Internet of Things. Int. J. Comput. Appl. 121 (9), 1–9.

[29] Le, A., Loo, J., Chai, K.K., Aiash, M., 2016. A specification-based IDS for detecting attacks on RPL-based network topology. Information 7 (2), 25.

[30] Ramesh, T., and S. Shaleni Priya., 2018. A Review on Game Theory Based Congestion Control in Wireless Sensor Network. Journal of Network Communications and Emerging Technologies.

[31] S. Reza, L. Wallgren, T. Voigt., 2013. real-time intrusion detection in the internet of things, Ad Hoc Netw.11,2661-2674.

[32] Shigen Shen, Longjun Huang, Haiping Zhou, Shui Yu,. 2018. Multistage Signaling Game-based

[33] Optimal Detection Strategies for Suppressing Malware Diffusion in Fog-Cloud-based IoT Networks, IEEE Internet of Things Journal.

[34] Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisini, A., 2015. Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. 76 (0), 146–164.

[35] S. Sicari and A. Rizzardi and L. A. Grieco and A.Coenporisini., 2014, Security, privacy and trust in Iot: The road ahead, Computer Network.

[36] Vacca, J., 2013. Computer and Information Security Handbook. Morgan Kaufmann, Amsterdam.