دانشگاه صنعتی امیرکبیر

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر

گرایش هوش مصنوعی

تشخیص نفوذ با استفاده از سیستم‌های چندعامله مبتنی بر اتوماتاهای یادگیر

نگارش:

فرناز ابطحی

استاد راهنما:

دکتر محمدرضا میبدی

آذرماه ۱۳۸۷

دانشگاه صنعتی امیرکبیر
(پلی‌تکنیک تهران)

بسمه تعالی

فرم اطلاعات پایان‌نامه

کارشناسی- ارشد و دکترا

تاریخ:
شماره:

معاونت پژوهشی
فرم پروژه تحصیلات تکمیلی ۷

مشخصات دانشجو:

نام و نام خانوادگی: فرناز ابطحی دانشجوی آزاد ● بورسیه ○ معادل ○

شماره دانشجوئی: ۸۵۱۳۱۰۴۳ دانشکده: مهندسی کامپیوتر و فناوری اطلاعات رشته تحصیلی: مهندسی کامپیوتر گروه: هوش مصنوعی

مشخصات استاد راهنما:

نام و نام خانوادگی: محمدرضا میبدی درجه و رتبه: استاد دانشکده مهندسی کامپیوتر

نام و نام خانوادگی: درجه و رتبه:

مشخصات استاد مشاور:

نام و نام خانوادگی: درجه و رتبه:

نام و نام خانوادگی: درجه و رتبه:

عنوان پایان‌نامه به فارسی: تشخیص نفوذ با استفاده از سیستم‌های چندعامله مبتنی بر اتوماتاهای یادگیر

عنوان پایان‌نامه به انگلیسی: Intrusion Detection using Learning Automata-based Multi-Agent Systems

نوع پروژه: کارشناسی ○ ارشد ● دکترا ○ سال تحصیلی: ۸۷-۸۸

کاربردی ● بنیادی ○ توسعه‌ای ○ نظری ○

تاریخ شروع : مهر ۸۶ تاریخ خاتمه : آذر ۸۷ تعداد واحد : ۶ سازمان تأمین کننده اعتبار :

واژه‌های کلیدی به فارسی: سیستم‌های چندعامله، هماهنگی، اتوماتای یادگیر، تشخیص نفوذ، دسته‌بندی

واژه‌های کلیدی به انگلیسی : Multi-Agent Systems, Coordination, Learning Automata, Intrusion Detection, Classification

مشخصات ظاهری	تعداد صفحات: ۱۸۰	تصویر ● جدول ● نمودار ○ نقشه ○ واژه‌نامه ○	تعداد مراجع: ۸۳	تعداد صفحات ضمائم: ۴۴
زبان متن	فارسی ●	انگلیسی ○	چکیده	فارسی ● انگلیسی ●
یادداشت				

نظرها و پیشنهادها به منظور بهبود فعالیت‌های پژوهشی دانشگاه

استاد:

دانشجو:

امضاء استاد راهنما: **تاریخ:**

۱ : ارائه به معاونت پژوهشی به همراه یک نسخه الکترونیکی از پایان‌نامه و فرم اطلاعات پایان‌نامه بصورت **PDF** همراه چاپ چکیده (فارسی انگلیسی) و فرم اطلاعات پایان‌نامه

تقدیم به پدر، مادر و خواهر عزیزم

که در تمام مراحل زندگی حامی و پشتیبانم بودند.

با تشکر از استاد گرانقدر، جناب آقای دکتر میبدی

که حمایت‌ها و راهنمایی‌های ارزشمند ایشان راه‌گشای من درجهت پیشبرد و انجام هرچه بهتر این پایان‌نامه بود.

چکیده

تا به حال فعالیت‌های کمی در زمینه استفاده از سیستم‌های چندعامله برای تشخیص نفوذ انجام شده است. در این پایان‌نامه، روشی مبتنی بر سیستم‌های چندعامله برای تشخیص نفوذهایی از نوع انکار سرویس که یکی از حملات مهم و شایع در سیستم‌های کامپیوتری است ارائه می‌گردد. از آن‌جایی که مسئله هماهنگی بین عامل‌ها در یک سیستم چندعامله بسیار حیاتی و حساس است، لازم است ابتدا روشی برای هماهنگ کردن عامل‌ها در سیستم‌های چندعامله ارائه گردد. تکنیکی که برای این منظور مورد استفاده قرار می‌دهیم، اتوماتای یادگیر می‌باشد. بنابراین، در این پایان‌نامه دو هدف مدنظر می‌باشد. ابتدا کارایی اتوماتای یادگیر در حل مسئله هماهنگی در سیستم‌های چندعامله مورد بررسی قرار گرفته و راه‌کارهایی برای این منظور ارائه می‌گردد. سپس با استفاده از نتایج این بررسی‌ها و مدل‌های به‌دست‌آمده، سیستم تشخیص نفوذی پیشنهاد می‌شود که مبتنی بر عامل‌های هوشمند بوده و در آن، عامل‌ها از اتوماتای یادگیر برای ایجاد هماهنگی بهره می‌گیرند. آزمایش‌ها نشان می‌دهند که روش‌های ارائه شده برای ایجاد هماهنگی، از کارایی لازم برخوردار بوده و سیستم تشخیص نفوذ پیشنهادی، در مقایسه با سیستم‌های مشابه، عملکرد مناسبی از لحاظ سرعت، نرخ تشخیص و نرخ خطای مثبت نادرست از خود نشان می‌دهد.

واژه‌های کلیدی: سیستم‌های چندعامله (Multi-Agent Systems)، هماهنگی (Coordination)، اتوماتای یادگیر (Learning Automata)، تشخیص نفوذ (Intrusion Detection)، دسته‌بندی (Classification).

فهرست مطالب

فهرست مطالب

فهرست مطالب

فهرست مطالب

فهرست مطالب

فهرست اشکال

فهرست اشکال

فهرست اشکال

فهرست جداول

۱- مقدمه

امروزه در بسیاری از کاربردها و در زمینه‌های مختلف صنعتی، نظامی، مخابراتی، اطلاعاتی، اجتماعی و...، از سیستم‌های پیچیده و توزیع‌شده چندعامله استفاده فراوانی می‌شود. یک سیستم چندعامله، جامعه‌ای از عامل‌هاست که در یک محیط درکنار یکدیگر درحال کار بوده و سعی در انجام کاری خاص و رسیدن به هدفی مشخص دارند. این عامل‌ها هوشمند و خودمختار هستند، بنابراین بدون وجود روشی برای ایجاد هماهنگی میان آن‌ها، ممکن است سیستم دچار هرج و مرج شده و از رسیدن به هدف نهایی بازبماند. به‌همین‌علت، هماهنگی یکی از مباحث مهم در حوزه سیستم‌های چندعامله می‌باشد.

به‌طور کلی می‌توان گفت هماهنگی فرآیندی است که ازطریق آن، عامل در راه عمل یکپارچه جامعه عامل‌ها و تضمین این انسجام، درباره اعمال خود و سایر عامل‌ها استنتاج و تصمیم‌گیری می‌نماید. هماهنگی در سیستم‌های چندعامله به دو روش کلی *همکاری* و *رقابت* صورت می‌گیرد. تکنیک‌های همکاری در سیستم‌هایی قابل استفاده است که عامل‌ها دارای هدف یکسان بوده و غیرمنفعت‌طلب باشند. درمقابل، در سیستم‌های رقابتی، روش *مذاکره* مورد استفاده قرار می‌گیرد. در این‌گونه سیستم‌ها، عامل‌ها در رقابت با یکدیگر بوده و هریک درصدد رسیدن به هدف و منفعت شخصی خود است و هدف کلی و مشترکی در سیستم وجود ندارد.

برای ایجاد هماهنگی در سیستم‌های چندعامله، روش‌های متعددی وجود دارد. یکی از این روش‌ها، استفاده از اتوماتای یادگیر است. اتوماتای یادگیر که یکی از تکنیک‌های یادگیری مبتنی بر محاسبات نرم بوده و براساس یادگیری تقویتی عمل می‌کند، ماشینی است که می‌تواند تعدادی متناهی عمل را انجام دهد. هر عمل انتخاب شده توسط یک محیط احتمالی ارزیابی شده، نتیجه ارزیابی در قالب سیگنالی مثبت یا منفی به اتوماتا داده می‌شود و اتوماتا از این پاسخ در انتخاب عمل بعدی تأثیر می‌پذیرد. هدف نهایی این است که اتوماتا یاد بگیرد تا از بین اعمال خود، بهترین عمل را انتخاب کند. بهترین عمل، عملی است که احتمال دریافت پاداش از محیط را حداکثر نماید.

تشخیص نفوذ عبارت است از فرآیند تشخیص تلاش‌هایی که جهت دسترسی غیرمجاز به یک شبکه یا کاهش کارایی آن انجام می‌شوند. در تشخیص نفوذ باید ابتدا درک صحیحی از چگونگی انجام حملات پیدا کرد. سپس بنابر درک به‌دست‌آمده، روشی دو مرحله‌ای را برای متوقف کردن حملات برگزید. اول این‌که

باید مطمئن شد که الگوی عمومی فعالیت‌های خطرناک تشخیص داده شده است و دوم این‌که اطمینان حاصل کرد که با حوادث مشخصی که در طبقه‌بندی مشترک حملات نمی‌گنجند، به سرعت رفتار می‌شود.

در این پایان‌نامه، هدف، ارائه سیستم‌های هوشمند چندعامله‌ای است که در آن‌ها عامل‌ها به‌منظور تصمیم‌گیری برای انجام اعمال خود، از اتوماتای یادگیر کمک می‌گیرند و از این طریق رفتار آن‌ها هماهنگ شده و سیستم در نهایت به هدف خود دست می‌یابد. برای بررسی نقاط قوت سیستم‌های چندعامله هوشمند مبتنی بر اتوماتای یادگیر، کاربرد آن‌ها را در تشخیص نفوذ که یکی از مباحث مهم در امنیت شبکه‌های کامپیوتری است، مورد مطالعه قرارخواهیم داد.

در رویکردی که سعی در ارائه آن خواهیم داشت، ساختاری متشکل از عامل‌ها را برای هماهنگی و یادگیری مکانیزم تشخیص نفوذ با استفاده از داده‌هایی از منابع توزیع‌شده به کار خواهیم برد که در آن، عامل‌ها از اتوماتای یادگیر به‌عنوان ابزاری برای کمک به فرآیند یادگیری و تصمیم‌گیری درمورد وقوع حمله یا عدم وقوع آن استفاده می‌نمایند. ساختار اتوماتای یادگیر به‌گونه‌ای است که می‌تواند خود را با تغییرات و رویدادهای جدید تطبیق دهد و از این رو به‌نظر می‌رسد که بتوان از آن به‌خوبی در تشخیص نفوذ بهره گرفت.

۱-۱- عامل‌ها و سیستم‌های چندعامله

۱-۱-۱- تعریف عامل

عامل در واقع نوعی سیستم نرم‌افزای است که دارای خصوصیات و هدف مشخصی می‌باشد. تا به حال تعاریف متعددی برای عامل ارائه شده‌است که به طورکلی می‌توان آن‌ها را در تعریف زیر خلاصه نمود:

تعریف ۱-۱: *عامل*، یک سیستم کامپیوتری است که در تعامل با محیطی که در آن قرار گرفته، در جهت رسیدن به اهداف خود، اعمالی را به‌صورت خودمختار و مستقل انجام می‌دهد.

بنابراین عامل دارای ویژگی‌های خاصی است که از جمله آن‌ها می‌توان به موارد زیر اشاره نمود: [۱]

- عامل، *خودمختار*[1] است، به این معنا که بدون دخالت فرد یا عامل دیگر، عمل می‌کند و بر روی وضعیت داخلی خود کنترل دارد.
- عامل وضعیت محیط خود را مشاهده کرده و نسبت به تغییراتی که در آن رخ می‌دهد از خود *واکنش*[2] نشان می‌دهد.
- عامل، *پیش‌فعال*[3] می‌باشد، یعنی نه‌تنها قادر است در پاسخ به محیط از خود واکنش نشان داده و عمل کند، بلکه می‌تواند رفتار هدف‌گرا از خود نشان دهد.
- عامل همواره سعی در بهبود کارایی خود دارد و این کار را از طریق *یادگیری*[4] انجام می‌دهد. برای این‌کار، براساس تجربیات قبلی رفتار خود را طوری تغییر می‌دهد که نتیجه بهتری نسبت به گذشته حاصل شود.
- عامل دارای *قابلیت سازگاری*[5] است و می‌تواند با استفاده از روش‌های یادگیری، اعمال خود را با اهداف سیستم تطبیق دهد.
- یکی از ویژگی‌های مهم عامل، *اجتماعی بودن*[6] است. عامل از طریق زبان‌های ارتباط میان عامل‌ها[7]، با سایر عامل‌ها ارتباط برقرار می‌کند. همانند جوامع انسانی، در جامعه‌ای از عامل‌ها نیز برای رسیدن به بسیاری از اهداف لازم است عامل‌ها با یکدیگر همکاری و یا مذاکره نمایند. درغیر این صورت ممکن است رسیدن به این اهداف برای یک عامل به‌تنهایی امکان‌پذیر نباشد. برای رسیدن به اهداف مشترک، عامل‌ها گاهی باید اعمالی را برخلاف اهداف شخصی خود انجام دهند.
- عامل دارای *عقلانیت*[8] است، یعنی همواره طوری عمل می‌کند که به اهداف خود نزدیک‌تر شود و اعمالی را که او را از رسیدن به هدف باز می‌دارند، انجام نمی‌دهد.

---

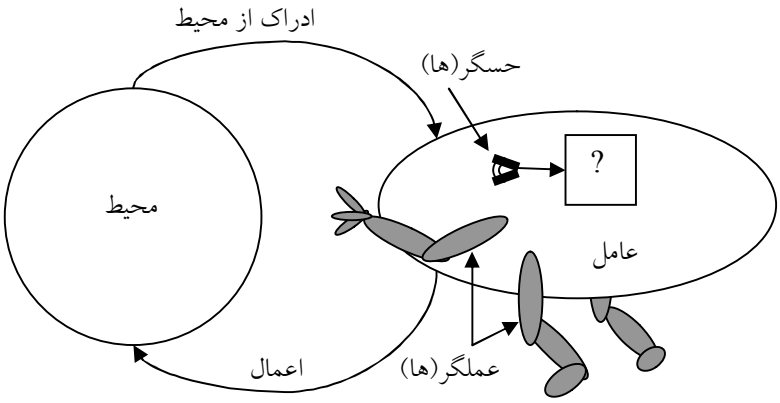
[1] Autonomous
[2] Reaction
[3] Proactive
[4] Learning
[5] Adaptability
[6] Sociality
[7] Agent Communication Language (ACL)
[8] Rationality

- عامل دارای تحرک[9] است و می‌تواند بر روی یک شبکه، حرکت کرده و جابه‌جا شود.

از دیگر ویژگی‌های عامل، *صداقت*[10] است، به این معنا که عمداً اطلاعات غلط را در اختیار سایر عامل‌ها قرار نمی‌دهد.

- عامل دارای ویژگی خیرخواهی[11] است، یعنی عامل‌ها اهداف متضادی را دنبال نمی‌کنند و همواره سعی دارند کاری را که از آن‌ها خواسته شده انجام دهند.

ساختار یک عامل را می‌توان به‌صورت شکل ۱-۱ توصیف نمود. [۱]



شکل ۱-۱- ساختار عامل [۱]

همان‌طور که در شکل ۱-۱ مشاهده می‌شود، عامل با استفاده از حسگرها وضعیت محیط را درک می‌کند و پس از انتخاب عمل مناسب با توجه به آنچه از محیط حس نموده، ازطریق عملگرهای خود بر روی محیط اثر می‌گذارد. بر این اساس می‌توان تعریف صوری زیر را برای عامل ارائه نمود: [۱]

تعریف ۱-۲: هر *عامل* با یک چندتایی به‌صورت $Ag =< L, Act, see, do, \tau_a, S_0 >$ تعریف می‌شود که در آن:

$L = \{l_1, l_2, ...\}$ مجموعه وضعیت‌های محلی عامل است.

---

[9] Mobility
[10] Veracity
[11] Benevolence

$Act = \{a_1, a_2, ...\}$ مجموعه اعمال عامل می‌باشد.

$Percept \rightarrow see : vis(E)$ تابع درک عامل است که دید عامل را به مشاهده آن از محیط تبدیل می‌کند.

$Act \rightarrow do$ تابع انتخاب عمل عامل است که وضعیت‌های محلی را به اعمال تصویر می‌نماید.

$\tau_a : L \times Percept \rightarrow L$ تابع تغییر وضعیت عامل است.

S_0 وضعیت اولیه عامل می‌باشد.

عامل همواره درحال تعامل با محیط عملیاتی است. محیط عملیاتی در سیستم‌های مبتنی بر عامل دارای ویژگی‌های متفاوتی است و براساس این ویژگی‌ها می‌توان محیط‌ها را به چندین صورت متفاوت دسته‌بندی نمود. این دسته‌بندی‌ها که در [۱] به تفضیل به آن‌ها اشاره شده عبارتند از:

- محیط قابل دستیابی/ غیر قابل دستیابی[۱۲]
- محیط قطعی/ غیرقطعی[۱۳]
- محیط مقطعی/ غیرمقطعی[۱۴]
- محیط ایستا/ پویا[۱۵]
- محیط گسسته/ پیوسته[۱۶]

۱-۱-۲- تعریف سیستم چندعامله

از دیدگاه هوش مصنوعی توزیع‌شده، سیستم چندعامله اجتماعی از تعدادی عامل مستقل است که با یکدیگر در تعامل هستند و هریک دارای هدفی است که ممکن است با اهداف سایر عامل‌ها هماهنگ یا متضاد باشد. خصوصیات سیستم‌های چندعامله شامل موارد زیر می‌باشد: [۱]

- دانش کافی و لازم برای حل مسئله در یک عامل وجود ندارد.

---

[12] Accessible/Inaccessible
[13] Deterministic/Non-Deterministic
[14] Episodic/Non-Episodic
[15] Static/Dynamic
[16] Discrete/Continuous