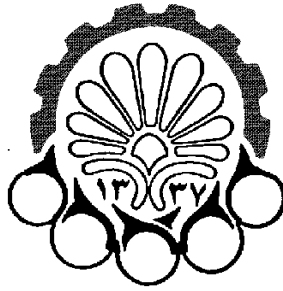


رسالة محمد



دانشگاه صنعتی امیرکبیر

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

پایان نامه 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 میدی

آذرماه ۱۳۸۷



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

بسمه تعالی

تاریخ:

شماره:

فرم اطلاعات پایان نامه

کارشناسی - ارشد و دکترا

معاونت پژوهشی

فرم پروژه تحصیلات تکمیلی ۷

مشخصات دانشجو:

نام و نام خانوادگی: فرناز ابطی
شماره دانشجویی: ۸۵۱۳۱۰۴۳
دانشگاه: مهندسی کامپیوتر و فناوری اطلاعات
رشته تحصیلی: مهندسی کامپیوتر
گروه: هوش مصنوعی

مشخصات استاد راهنما:

نام و نام خانوادگی: محمدرضا میبیدی
نام و نام خانوادگی:
رتبه و رتبه: استاد دانشکده مهندسی کامپیوتر
رتبه و رتبه:

مشخصات استاد مشاور:

نام و نام خانوادگی:
نام و نام خانوادگی:
رتبه و رتبه:
رتبه و رتبه:

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

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

نوع پروژه: کارشناسی ارشد
کاربردی بنیادی
دکترای توسعه‌ای
سال تحصیلی: ۸۷-۸۸ 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

تعداد صفحات:	تعداد مراجع:	تعداد صفحات:	مشخصات ظاهری
۴۴ ضمیمه:	۸۳	۱۸۰	تصویر <input checked="" type="radio"/> جدول <input checked="" type="radio"/> نمودار <input type="radio"/> نقشه <input type="radio"/> واژه‌نامه <input type="radio"/>
انگلیسی <input checked="" type="radio"/>	فارسی <input checked="" type="radio"/>	انگلیسی <input type="radio"/>	فارسی <input checked="" type="radio"/> چکیده
زبان متن			
یادداشت			

نظرها و پیشنهادهای به منظور بهبود فعالیت‌های پژوهشی دانشگاه

استاد:

دانشجو:

تاریخ:

امضاء استاد راهنما:

تقدیم به پدر، مادر و خواهر عزیزم

که در تمام مراحل زندگی حامی و پشتیبانم
بودند.

با تشکر از استاد گرانقدر، جناب آقای دکتر میبیدی

که حمایت‌ها و راهنمایی‌های ارزشمند ایشان راه‌گشای من در جهت
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

۱	مقدمه	۱
۱-۱	عامل‌ها و سیستم‌های چندعامله	۲
۱-۱-۱	تعریف عامل	۲
۱-۱-۲	تعریف سیستم چندعامله	۵
۱-۱-۳	مدل‌های سیستم‌های چندعامله	۸
۱-۱-۳-۱	فرآیند تصمیم‌گیری مارکف چندعامله (MMDP)	۸
۱-۱-۳-۲	مسائل تصمیم‌گیری مارکف قابل مشاهده جزئی (POMDP)	۱۰
۱-۱-۳-۳	فرآیند تصمیم‌گیری تیمی چندعامله (MTDP)	۱۱
۱-۱-۳-۴	بازی‌های غیرقطعی قابل مشاهده جزئی (POSG)	۱۲
۱-۱-۳-۵	مسائل ارضاء محدودیت توزیع‌شده (DCSP)	۱۳
۱-۱-۴	زمینه‌های کاربردی سیستم‌های چندعامله	۱۴
۱-۱-۵	هماهنگی در سیستم‌های چندعامله	۱۶
۱-۱-۵-۱	روش‌های ایجاد هماهنگی در سیستم‌های چندعامله	۱۷
۱-۲	هماهنگی در سیستم‌های چندعامله با استفاده از یادگیری	۲۱
۱-۲-۱	یادگیری تقویتی	۲۲
۱-۲-۱-۱	یادگیری تقویتی تک‌عامله	۲۵
۱-۲-۱-۲	یادگیری Q	۲۷
۱-۲-۲	یادگیری تقویتی چندعامله	۲۹
۱-۲-۲-۱	یادگیری مستقل	۳۲
۱-۲-۲-۲	یادگیری عمل جمعی	۳۲
۱-۲-۲-۳	اتوماتای یادگیر	۳۴

- ۳۶..... ۱-۲-۲-۱ ویژگی های اتوماتای یادگیر
- ۳۷..... ۳-۲-۱ اتوماتای یادگیر اتصالی
- ۳۸..... ۱-۳-۲-۱ اتوماتای اتصالی همگام
- ۳۸..... ۱-۱-۳-۲-۱ بازی اتوماتا
- ۴۰..... ۲-۳-۲-۱ اتوماتای اتصالی ترتیبی
- ۴۰..... ۱-۲-۳-۲-۱ اتوماتای یادگیر سلسله مراتبی
- ۴۱..... ۲-۲-۳-۲-۱ شبکه اتوماتای یادگیر
- ۴۱..... ۳-۲-۳-۲-۱ اتوماتای یادگیر توزیع شده
- ۴۲..... ۳-۳-۲-۱ اتوماتای اتصالی ناهمگام
- ۴۲..... ۴-۲-۱ فعالیت های انجام شده در زمینه استفاده از اتوماتای یادگیر در سیستم های چندعامله
- ۴۵..... ۳-۱- مفهوم امنیت و تشخیص نفوذ
- ۴۷..... ۱-۳-۱ تعاریف اولیه
- ۴۸..... ۲-۳-۱ انواع حملات و متدولوژی آنها
- ۴۸..... ۳-۳-۱ حملات شبکه ای و کامپیوتری
- ۴۹..... ۱-۳-۳-۱ دسته بندی حملات براساس متدولوژی حمله
- ۵۰..... ۴-۳-۱ دسته بندی حملات براساس رفتار
- ۵۱..... ۴-۱- مقابله با حملات کامپیوتری
- ۵۲..... ۱-۴-۱ دیواره آتش
- ۵۳..... ۲-۴-۱ سیستم های ممانعت از نفوذ (IPS)
- ۵۴..... ۳-۴-۱ سیستم های تشخیص نفوذ (IDS)
- ۵۵..... ۱-۳-۴-۱ لزوم وجود سیستم های تشخیص نفوذ
- ۵۵..... ۲-۳-۴-۱ وظایف یک سیستم تشخیص نفوذ
- ۵۶..... ۳-۳-۴-۱ تکنیک های مورد استفاده در سیستم های تشخیص نفوذ به منظور تشخیص و کلاس بندی

۵۶	۱-۳-۳-۴-۱- تشخیص سوءاستفاده
۵۸	۱-۳-۳-۴-۲- تشخیص ناهنجاری
۶۰	۱-۳-۴-۴- مدل عمومی یک سیستم تشخیص نفوذ (IDS)
۶۴	۱-۳-۴-۵- استفاده از سیستم‌های چندعامله و یادگیری تقویتی چندعامله برای تشخیص نفوذ
۶۵	۱-۵- هدف پروژه
۶۷	۱-۶- جمع‌بندی
۶۹	۲- حل مسئله هماهنگی در سیستم‌های چندعامله به کمک اتوماتای یادگیر
۶۹	۲-۱- مقدمه
۶۹	۲-۲- مروری بر تئوری بازی
۷۰	۲-۲-۱- بازی‌های ماتریسی (استراتژیک)
۷۱	۲-۲-۲- بازی‌های تصادفی
۷۲	۲-۲-۳- بازی‌های هماهنگی
۷۳	۲-۳- پیاده‌سازی چند نمونه بازی با استفاده از اتوماتاهای یادگیر
۷۳	۲-۳-۱- بازی Blotto
۷۶	۲-۳-۱-۱- یافتن استراتژی غالب در بازی Blotto با استفاده از اتوماتای یادگیر
۸۱	۲-۳-۲- بازی شکار گوزن
۸۳	۲-۳-۲-۱- استفاده از اتوماتاهای یادگیر برای پیاده‌سازی بازی شکار گوزن
۸۶	۲-۴- حل فرآیند تصمیم‌گیری مارکف چندعامله با استفاده از اتوماتای یادگیر
۸۷	۲-۴-۱- کنترل فرآیند تصمیم‌گیری مارکف چندعامله با استفاده از اتوماتاهای یادگیر
۹۶	۲-۵- حل مسائل ارضاء محدودیت توزیع شده به کمک اتوماتای یادگیر
۹۶	۲-۵-۱- حل یک نمونه از مسئله n -وزیر به کمک اتوماتاهای یادگیر
۹۹	۲-۶- جمع‌بندی

۳- تشخیص نفوذ به کمک سیستم‌های چندعامله مبتنی بر اتوماتای یادگیر	۱۰۱
۳-۱- مقدمه	۱۰۱
۳-۲- مجموعه داده‌های KDD99	۱۰۱
۳-۳- روش ارزیابی	۱۰۴
۳-۴- مدل پیشنهادی برای تشخیص نفوذ	۱۰۶
۳-۵- ارزیابی	۱۱۶
۳-۶- مزایای مدل پیشنهادی	۱۱۹
۳-۷- الگوریتم AdaBoost	۱۲۲
۳-۸- جمع‌بندی	۱۲۳
۴- جمع‌بندی و کارهای آینده	۱۲۵
۴-۱- مقدمه	۱۲۵
۴-۲- نتایج به دست آمده در این پروژه	۱۲۶
۴-۳- پیشنهادات	۱۲۹
مراجع	۱۳۱
پیوست‌ها	۱۳۷
۱- زمینه‌های کاربردی سیستم‌های چندعامله [۱۰]	۱۳۷
الف- عامل‌های مجسم	۱۳۷
ب- محیط‌های مبتنی بر تئوری بازی	۱۴۱
ج- مسائل دنیای واقعی	۱۴۳
۲- انواع الگوریتم‌های یادگیری تقویتی در سیستم‌های چندعامله	۱۴۷
الف- الگوریتم یادگیری Minimax-Q	۱۴۷

۱۴۸	ب- الگوریتم یادگیری Nash-Q
۱۵۰	ج- الگوریتم یادگیری Friend-or-Fo Q (FFQ)
۱۵۱	د- الگوریتم یادگیری rQ
۱۵۳	پیوست ۳- شرح پیاده‌سازی و راهنمای استفاده از برنامه
۱۵۳	الف- بازی‌ها و مدل‌های سیستم‌های چندعامله
۱۷۲	ب- سیستم تشخیص نفوذ پیشنهادی

فهرست اشکال

- شکل ۱-۱- ساختار عامل [۱] ۴
- شکل ۲-۱- ساختار سیستم چندعامله [۱] ۶
- شکل ۳-۱- مدل عامل‌ها در DCSP [۱۰] ۱۴
- شکل ۴-۱- روش‌های مختلف ایجاد هماهنگی بین عامل‌ها در سیستم‌های چندعامله [۱] ۱۷
- شکل ۵-۱- مدل یادگیری تقویتی [۱۸] ۲۴
- شکل ۶-۱- مقادیر $Q(s, a)$ ، $V^*(s)$ و خط‌مشی بهینه حاصل از هر یک از آن‌ها [۱۸] ۲۸
- شکل ۷-۱- شبه‌کد محاسبه مقادیر $Q(s, a)$ با استفاده از روش Q-Learning [۱۹] ۲۹
- شکل ۸-۱- مدل یادگیری تقویتی چندعامله [۱۴] ۳۰
- شکل ۹-۱- ارتباط بین اتوماتای یادگیر و محیط [۱۶] ۳۵
- شکل ۱۰-۱- طبقه‌بندی اتوماتای یادگیر اتصالی [۲۰] ۳۸
- شکل ۱۱-۱- بازی اتوماتا [۲۰] ۳۹
- شکل ۱۲-۱- اتوماتای یادگیر سلسله‌مراتبی [۲۰، ۲۱] ۴۰
- شکل ۱۳-۱- شبکه اتوماتای یادگیر [۲۰، ۲۱] ۴۱
- شکل ۱۴-۱- اتوماتای یادگیر توزیع‌شده [۲۳] ۴۲
- شکل ۱۵-۱- تعداد وقایع گزارش شده توسط CERT/CC در سال‌های ۱۹۹۵ تا ۲۰۰۲ [۳۳] ۴۵
- شکل ۱۶-۱- روال تغییرات پیچیدگی حملات و دانش مهاجمان در سال‌های ۱۹۸۰ تا ۲۰۰۰ [۳۳] ۴۶
- شکل ۱۷-۱- نمونه‌ای از به‌کارگیری سیستم ممانعت از نفوذ در شبکه [۳۶] ۵۴
- شکل ۱۸-۱- مدل عمومی یک سیستم تشخیص نفوذ [۳۵] ۶۱
- شکل ۱۹-۱- ساختار سلسله‌مراتبی عامل‌ها برای مدیریت امنیت شبکه [۵۸] ۶۴

- شکل ۱-۲- تغییرات احتمال انتخاب عمل بهینه توسط بازیکن دارای اتوماتای یادگیر با نرخ یادگیری (الف) ۰/۱ و (ب) ۰/۰۱، درحالتی که فقط یکی از بازیکنان از اتوماتای یادگیر استفاده نماید. ۷۷
- شکل ۲-۲- تغییرات احتمال انتخاب عمل بهینه توسط (الف) بازیکن ۱ و (ب) بازیکن ۲ با نرخ یادگیری ۰/۱، در حالتی که هر دو بازیکن از اتوماتای یادگیر استفاده نمایند. ۷۸
- شکل ۳-۲- تغییرات احتمال انتخاب عمل بهینه توسط (الف) بازیکن ۱ و (ب) بازیکن ۲ با نرخ یادگیری ۰/۱، در حالتی که هر دو بازیکن از اتوماتای یادگیر استفاده نمایند. ۷۸
- شکل ۴-۲- درصد دفعات همگرایی به هریک از سه استراتژی غالب در ۱۰۰۰۰ بار اجرای الگوریتم با احتمال اولیه برابر برای تمام اعمال ۸۰
- شکل ۵-۲- درصد دفعات همگرایی به هریک از سه استراتژی غالب در ۱۰۰۰۰ بار اجرای الگوریتم پس از افزایش جزئی احتمال اولیه عمل (۱،۲،۲) ۸۱
- شکل ۶-۲- تغییرات احتمال انتخاب عمل بهینه توسط (الف) بازیکن ۱ و (ب) بازیکن ۲ با نرخ یادگیری ۰/۳ ۸۴
- شکل ۷-۲- تغییرات احتمال انتخاب عمل بهینه توسط (الف) بازیکن ۱ و (ب) بازیکن ۲ با نرخ یادگیری ۰/۱ ۸۵
- شکل ۸-۲- درصد دفعات همگرایی به هریک از دو تعادل در ۱۰۰۰۰ بار اجرای الگوریتم ۸۵
- شکل ۹-۲- درصد دفعات همگرایی به هریک از دو تعادل در ۱۰۰۰۰ بار اجرای الگوریتم پس از افزایش جزئی احتمال اولیه عمل Stag ۸۶
- شکل ۱۰-۲- فرآیند تصمیم‌گیری مارکف چندعامله مورد استفاده در آزمایش [۷۱،۲۵] ۸۹
- شکل ۱۱-۲- نمودار تغییرات احتمال انتخاب مسیر بهینه برای عامل اول با استفاده از الگوریتم ۱ ۹۱
- شکل ۱۲-۲- نمودار تغییرات احتمال انتخاب عمل حرکت به بالا در خانه شروع به ازاء نرخ یادگیری (الف) ۰/۱ و (ب) ۰/۰۱ اتوماتای یادگیر ۱ ۹۲
- شکل ۱۳-۲- نمودار تغییرات احتمال انتخاب مسیر بهینه برای عامل اول با استفاده از الگوریتم ۲ ۹۴

شکل ۲-۱۴- نمودار تغییرات احتمال انتخاب مسیر بهینه برای عامل اول با استفاده از اتوماتای یادگیر اتصالی
 ۹۵

شکل ۲-۱۵- یک پاسخ برای مسئله ۴-وزیر [۱۰] ۹۷

شکل ۲-۱۶- تعریف متغیرهای مسئله ۴-وزیر مورد استفاده ۹۷

شکل ۲-۱۷- تغییرات احتمال اعمال اتوماتای یادگیر در طول فرآیند حل مسئله ۴-وزیر ۹۹

شکل ۳-۱- شمای کلی فرآیند دسته‌بندی و تشخیص نفوذ ۱۰۸

شکل ۳-۲- مدل پیشنهادی برای تشخیص نفوذ ۱۱۱

شکل ۳-۳- تغییرات حد آستانه (T) در طول مرحله آموزش مدل ۱۱۷

شکل ۳-۴- شبه‌کد الگوریتم AdaBoost [۸۳] ۱۲۳

شکل پ-۱- الگوریتم یادگیری Minimax-Q [۱۸] ۱۴۸

شکل پ-۲- الگوریتم یادگیری Nash-Q [۱۸] ۱۵۰

شکل پ-۳- الگوریتم یادگیری rQ [۱۸] ۱۵۲

فهرست جداول

- جدول ۱-۲- ماتریس نتیجه یک نمونه بازی هماهنگی ساده ۷۳
- جدول ۲-۲- ماتریس نتیجه برای بازیکن اول در یک نمونه بازی ۷۵
- جدول ۳-۲- ماتریس نتیجه برای بازیکن اول در یک نمونه بازی Blotto ۷۹
- جدول ۴-۲- ماتریس نتیجه بازی شکار گوزن در حالت کلی [۷۰] ۸۲
- جدول ۵-۲- ماتریس نتیجه برای یک نمونه بازی شکار گوزن ۸۲
- جدول ۶-۲- تعداد متوسط دفعات تکرار برای رسیدن احتمال مسیر بهینه به حد آستانه (۰/۹۵) با نرخ یادگیری ۰/۰۱ برای عامل ۱ ۹۶
- جدول ۱-۳- تعداد رکوردهای مجموعه‌های 10_percent و corrected به تفکیک نوع حمله/نرمال [۷۵،۷۴] ۱۰۳
- جدول ۲-۳- تعداد رکوردهای مجموعه‌های 10_percent و corrected به تفکیک نوع حمله [۷۵،۷۴] .. ۱۰۳
- جدول ۳-۳- نام و نوع ویژگی‌های مجموعه داده KDD99 [۷۵،۷۴] ۱۰۵
- جدول ۴-۳- مقادیر ویژگی‌های یک رکورد از مجموعه داده KDD99 پیش و پس از گسسته‌سازی ۱۰۹
- جدول ۵-۳- چند نمونه مشاهده در مدل ظرف و گوی با ۵ ظرف و چهار گوی ۱۰۹
- جدول ۶-۳- بردار احتمال اتوماتاهای یادگیر پس از مرحله آموزش ۱۱۸
- جدول ۷-۳- مقایسه کارایی مدل پیشنهادی با چند روش تشخیص نفوذ دیگر ۱۱۹

۱- مقدمه

امروزه در بسیاری از کاربردها و در زمینه‌های مختلف صنعتی، نظامی، مخابراتی، اطلاعاتی، اجتماعی و...، از سیستم‌های پیچیده و توزیع شده چندعامله استفاده فراوانی می‌شود. یک سیستم چندعامله، جامعه‌ای از عامل‌هاست که در یک محیط درکنار یکدیگر در حال 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 بازماند. به همین علت، هماهنگی یکی از مباحث مهم در حوزه سیستم‌های چندعامله می‌باشد.

به طور کلی می‌توان گفت هماهنگی فرآیندی است که از طریق آن، عامل در راه عمل یکپارچه جامعه عامل‌ها و تضمین این انسجام، درباره اعمال خود و سایر عامل‌ها استتاج 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. در مقابل، در سیستم‌های رقابتی، روش مذاکره مورد استفاده قرار می‌گیرد. در این گونه 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 به دست آمده، روشی دو مرحله‌ای را برای متوقف کردن حملات برگزید. اول این که

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 نمی‌گنجد، 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 قرار خواهیم 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 توزیع شده 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 شده است که به طور کلی 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^۱ 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^۲ نشان می‌دهد.
- عامل، پیش‌فعال^۳ می‌باشد، یعنی نه تنها 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^۴ انجام می‌دهد. برای این کار، براساس تجربیات قبلی رفتار خود را طوری تغییر می‌دهد که نتیجه بهتری نسبت به گذشته حاصل شود.
- عامل دارای قابلیت سازگاری^۵ است و می‌تواند با استفاده از روش‌های یادگیری، اعمال خود را با اهداف سیستم تطبیق دهد.
- یکی از ویژگی‌های مهم عامل، اجتماعی بودن^۶ است. عامل از طریق زبان‌های ارتباط میان عامل‌ها^۷، 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. در غیر 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^۸ 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

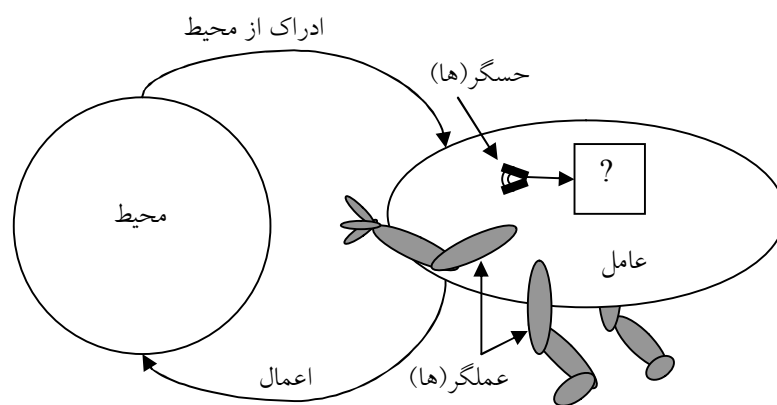
⁵ Adaptability

⁶ Sociality

⁷ Agent Communication Language (ACL)

⁸ Rationality

- عامل دارای تحرک^۹ است و می‌تواند بر روی یک شبکه، حرکت کرده و جابه‌جا شود. از دیگر ویژگی‌های عامل، صداقت^{۱۰} است، به این معنا که عمداً اطلاعات غلط را در اختیار سایر عامل‌ها قرار نمی‌دهد.
 - عامل دارای ویژگی خیرخواهی^{۱۱} 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 به صورت 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، از طریق 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 به صورت $Ag = \langle L, Act, see, do, \tau_a, S_0 \rangle$ تعریف می‌شود که در آن:

$L = \{I_1, I_2, \dots\}$ مجموعه وضعیت‌های محلی عامل است.

⁹ Mobility

¹⁰ Veracity

¹¹ Benevolence

$Act = \{a_1, a_2, \dots\}$ مجموعه اعمال عامل می باشد.

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

$Act \rightarrow do$ تابع انتخاب عمل عامل است که وضعیت های محلی را به اعمال تصویر می نماید.

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

S_0 وضعیت اولیه عامل می باشد.

عامل همواره در حال تعامل با محیط عملیاتی است. محیط عملیاتی در سیستم های مبتنی بر عامل دارای ویژگی های متفاوتی است و براساس این ویژگی ها می توان محیط ها را به چندین صورت متفاوت دسته بندی نمود. این دسته بندی ها که در [۱] به تفصیل به آن ها اشاره شده عبارتند از:

- محیط قابل دستیابی / غیر قابل دستیابی^{۱۲}
- محیط قطعی / غیر قطعی^{۱۳}
- محیط مقطعی / غیر مقطعی^{۱۴}
- محیط ایستا / پویا^{۱۵}
- محیط گسسته / پیوسته^{۱۶}

۱-۱-۲- تعریف سیستم چندعامله

از دیدگاه هوش مصنوعی توزیع شده، 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 عامل ها هماهنگ یا متضاد باشد. خصوصیات سیستم های چندعامله شامل موارد زیر می باشد: [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