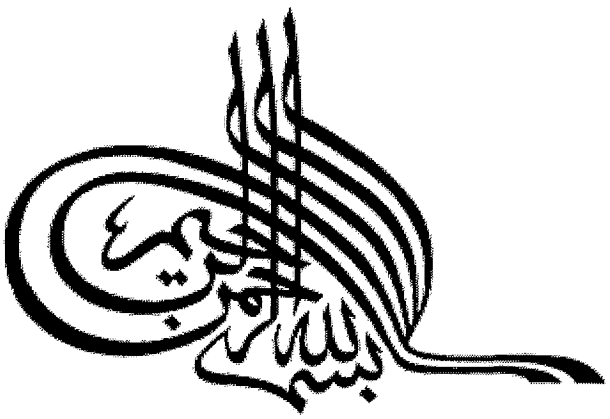


دانشگاه اصفهان

دانشکده فنی

گروه کامپیوتر

پایان نامه‌ی کارشناسی ارشد رشته‌ی کامپیوتر گرایش نرم‌افزار

امنیت سیستمهای چندعاملی به کمک عاملهای بی‌خبر و بی‌نشان

استاد راهنما:

دکتر بهروز ترک لادانی

استاد مشاور:

دکتر مهدی برنجکوب

پژوهشگر:

فاطمه راجی

اسفند ماه ۱۳۸۶

دانشگاه اصفهان

دانشکده فنی

گروه کامپیوتر

پایان نامه‌ی کارشناسی ارشد رشته‌ی کامپیوتر گرایش نرم‌افزار خانم فاطمه راجی

تحت عنوان

امنیت سیستمهای چندعاملی به کمک عاملهای بی‌خبر و بی‌نشان

در تاریخ ۱۴/۶/۱۳۸۷ توسط هیأت داوران زیر بررسی و با درجه ..عالی..... به تصویب نهایی رسید.

۱- استاد راهنمای پایان نامه دکتر بهروز ترک لادانی با مرتبه‌ی علمی استادیار امضاء

۲- استاد مشاور پایان نامه دکتر مهدی برنجکوب با مرتبه‌ی علمی استادیار امضاء

۳- استاد داور داخل گروه دکتر احمد براآنی با مرتبه‌ی علمی استادیار امضاء

۴- استاد داور خارج از گروه دکتر محمد دخیل‌علیان با مرتبه ی علمی استادیار امضاء

امضای مدیر گروه

۱۳۸۷/۶/۱۸

تشکر و قدردانی

پروردگار یکتا را شکرگزارم که به من توان به پایان رساندن مرحله دیگر از زندگیم را عطا فرمود. اکنون که در پایان این راه و آغاز مرحله‌ای دیگر قرار دارم، بر خود لازم می‌دانم که از زحمات کلیه اساتید بزرگواری که مرا در رسیدن به این مرحله یاری داده‌اند، سپاسگزاری نمایم.

بدینوسیله مراتب قدردانی خود را از جناب آقای دکتر بهروز ترک‌لادانی که به عنوان استاد راهنما، با رهنمودها و دلسوزی‌های خود سهم عمده‌ای در انجام این پایان‌نامه داشته‌اند، اعلام می‌دارم. بی‌شک راهنمائیها و حمایتهای ایشان مشوق اینجانب در انجام این پایان‌نامه بوده است. از جناب آقای دکتر مهدی برنجکوب، استاد مشاور پایان‌نامه که در انجام تحقیق از راهنمائیهای ارزشمندشان استفاده نمودم و بدینوسیله بر غنای آن افزودند، کمال تشکر و قدردانی را دارم.

همچنین از مدیر گروه محترم گروه کامپیوتر جناب آقای دکتر کمال جمشیدی که دلسوزانه از هیچ مساعدتی دریغ نورزیدند و دیگر استادان عزیز و گرانقدر بویژه جناب آقای دکتر احمد براآنی و جناب آقای دکتر محمد دخیل‌علیان که زحمت داوری این پایان‌نامه را پذیرفتند، تشکر و قدردانی می‌نمایم.

فاطمه راجی

اسفند ۱۳۸۶

تقدیم به حضرت دوست که هرچه دارم از اوست.

تقدیم به پدر و مادر عزیزم، به آنان که هرچه دارم از آنها و دعای خیرشان است.

تقدیم به همسر مهربانم، به او که همراهی‌اش بهانه‌ای برای ادامه راه من است و

تقدیم به تمامی جویندگان دانش.

چکیده

عامل متحرک قطعه برنامه‌ای است که توانائی حرکت از یک میزبان به میزبان دیگری را دارد. در مورد فناوری عاملهای متحرک مسائل زیادی وجود دارد که یکی از مهمترین آنها, مسأله امنیت است. از آنجائیکه عامل متحرک شامل کد و اطلاعات است, لذا تأمین امنیت عامل در برابر میزبانهای بدخواه مهمترین بحث امنیتی این فناوری است. از طرف دیگر همواره نیازمندی اصلی مالک در کاربردهای مختلف آن است که عامل بتواند بصورت بی‌نشان در شبکه حرکت کند بطوریکه هویت مالک و سفرنامه عامل حتی برای یک تحلیلگر ترافیک شبکه هم پنهان بماند.

در این پایان‌نامه, پس از بیان برخی از پروتکلهای مهم تأمین امنیت و بی‌نشانی عامل, دو پروتکل پیشنهاد شده است. در پروتکل پیشنهادی اول سعی بر این است که با فراهم کردن ویژگی بی‌نشانی برای عامل و مقاوم کردن آن در مقابل حمله‌های تحلیل ترافیک, امنیت یک عامل متحرک فراهم شود. در این پروتکل جهت فراهم کردن ویژگی بی‌نشانی از یک سیستم بی‌نشان کننده عمومی استفاده شده که متشکل از تعدادی میزبان مورد اعتماد به نام Mixer است. عامل در هر سفر به یک میزبان سفرنامه بصورت رمزشده از بین Mixerها عبور می‌کند. Mixerها به عنوان واسط ارتباطی در هر گام سفر عامل، بی‌نشانی مالک و سفرنامه عامل و همچنین مقاومت عامل در مقابل حمله‌های تحلیل ترافیک را فراهم می‌کنند. علاوه بر این, عامل می‌تواند پس از اتمام سفر با حفظ ویژگی بی‌نشانی به خانه برمی‌گردد تا سفرنامه و نتایج اجرای خود در میزبانها را به مالک تحویل دهد.

در پروتکل پیشنهادی دوم با توسعه پروتکل پیشنهادی اول, ویژگی بی‌خبری به عامل بی‌نشان اضافه شده است تا صحت و محرمانگی کد عامل تحت کنترل مالک باشد. به این صورت که مالک می‌تواند پس از ارسال عامل به محیط در هر زمان که مایل باشد, مأموریت جدیدی را بصورت رمزشده به همراه شرایط محیطی لازم جهت رمزگشائی آن به عامل ابلاغ می‌کند. در این پروتکل, مالک جهت حفظ بی‌نشانی, از طریق سیستم بی‌نشان کننده بر روی یک تخته سیاه کامپیوتری مأموریت عاملش را می‌نویسد. در این حالت عامل در صورت برقراری شرایط رمزگشائی می‌تواند با مأموریت جدید به میزبان سفرنامه بعدی سفر کند.

کلید واژه‌ها:

عامل متحرک, سیستمهای چندعاملی, امنیت, رمزنگاری, بی‌خبری, بی‌نشانی

فهرست مطالب

عنوان **صفحه**

عنوان ..... **صفحه**

عنوان ..... صفحه

فصل پنجم: عامل بی‌خبر و بی‌نشان

عنوان ..... **صفحه**

فهرست شکلها

عنوان **صفحه**

فصل اول: کلیات

فصل دوم: امنیت عامل متحرک

فصل سوم: بی‌نشانی

عنوان..... صفحه

فصل چهارم: پروتکلی جهت برقراری بی‌نشانی مالک و سفرنامه عامل

فصل پنجم: عامل بی‌خبر و بی‌نشان

فهرست جدولها

عنوان **صفحه**

فصل اول: کلیات

۱-۱ مقدمه

یکی از فناوریهائی که در سالهای اخیر بسیار مورد توجه محققین قرار گرفته، فناوری عاملهای متحرک است. در یک سیستم مبتنی بر عامل متحرک، عامل بطور واقعی در شبکه حرکت کرده و با میزبانهای[1] مختلفی ارتباط برقرار می‌کند و پس از انجام دادن مجموعه وظایفی که صاحبش به او محول کرده به خانه بر می‌گردد. بنابراین عامل بطور مستقیم سرویس موردنظر خود را از میزبان درخواست می‌کند و همین ویژگی مزایای زیادی از جمله کیفیت و کارائی بالا در انجام درخواستها و استفاده موثر از پهنای باند شبکه را به ارمغان می‌آورد.

بطورکلی خصوصیات گوناگونی برای یک عامل تعریف شده است [25] همانند:

- واکنش‌پذیری[2]: توانائی عامل در پاسخ به تغییرات محیط خود
- خودمختاری[3]: توانائی عامل در کنترل کامل عملیات خود در جهت رسیدن به هدف
- اجتماعی‌بودن[4]: توانائی عامل در تعامل با عاملها یا کاربران
- متحرک‌بودن[5]: توانائی عامل در انتقال خود از یک محیط به محیط دیگر
- یادگیری و نتیجه‌گیری[6]: توانائی عامل در تغییر رفتارهای خود براساس تجربیات قبلی و تعامل با محیط

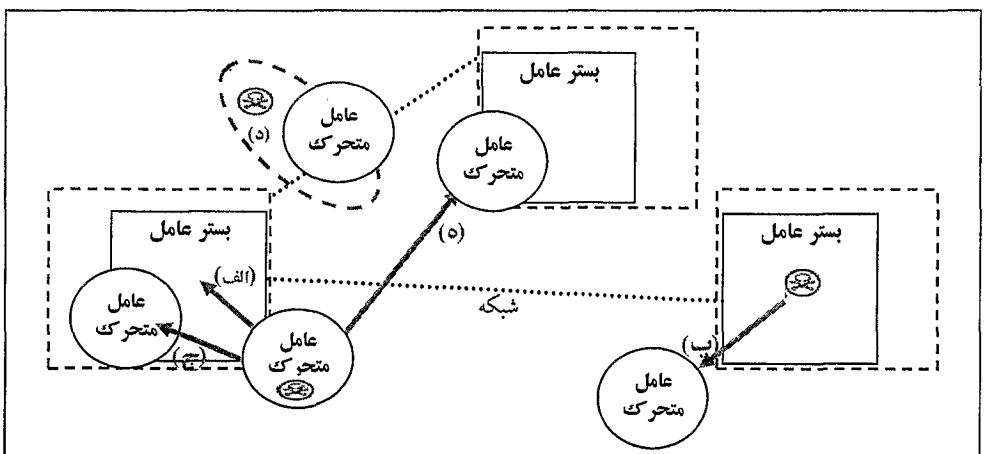
---

[1] Host
[2] Reactivity
[3] Autonomy
[4] Socialibility
[5] Mobility
[6] Inference

هر عامل دو خصیصه اول از خصوصیات بالا را دارا می‌باشد و بقیه خصوصیات برای افزودن ویژگیهائی به عاملها تعریف شده‌اند. عاملها با بهره‌گیری از این ویژگیها در زمینه‌های گوناگونی همچون تجارت الکترونیک و یا مدیریت شبکه استفاده می‌شوند [24].

۱-۲ مسائل امنیتی مطرح در مورد عاملهای متحرک

ویژگی تحرک در عاملهای متحرک، حساسیت مسائل امنیتی آنها را افزایش می‌دهد. در معماری عامل متحرک مسئله امنیت از دو دیدگاه قابل بررسی است، دیدگاه عامل و دیدگاه بستر[1] یا میزبان آن. در واقع امنیت در این معماری می‌بایست عامل یا بستر آن را در مقابل یکدیگر مصون نگه دارد. همانطورکه در شکل ۱-۱ مشاهده می‌شود یک عامل بدخواه[2] می‌تواند به میزبانی که در آن است و از منابع محاسباتی‌اش استفاده می‌کند، حمله کند.



(الف): عاملهای بدخواه می‌توانند به میزبان خود حمله کنند.
(ب): میزبانهای بدخواه می‌توانند به عاملها حمله کنند.
(ج): عاملهای بدخواه می‌توانند به عاملهای دیگر موجود در میزبانهایشان حمله کنند.
(د): میزبانهای بدخواه می‌توانند به عاملها در حین انتقال در شبکه حمله کنند.
(ه): عاملهای بدخواه می‌توانند به عاملهای دیگر موجود در میزبانهای دیگر حمله کنند.

شکل ۱-۱: حمله‌های مربوط به یک سیستم مبتنی بر عامل

[1] Platform
[2] Malicious

علاوه بر این عامل بدخواه می‌تواند به عاملهای موجود در میزبان خود و هم به عاملهای میزبانهای دیگر صدمه برساند. از طرف دیگر یک میزبان بدخواه می‌تواند به عاملهای موجود در بستر خود و یا بسترهای دیگران حمله کند. البته چنین میزبانی ممکن است در حین سفر عامل از یک میزبان به میزبان دیگر به آن عامل حمله کند.

تاکنون راه‌حلهای مختلفی در جهت تأمین امنیت میزبان در مقابل عاملها ارائه شده که با پیاده سازی آنها در یک سیستم مبتنی بر عامل امنیت نسبتاً خوبی برای میزبان فراهم شده است [36]. بنابراین هم اکنون توجه محققین عمدتاً بر روی تأمین امنیت عامل در مقابل میزبانهای راه دور معطوف است. در همین راستا، امنیت عامل از چهار دیدگاه مورد بررسی قرارمی‌گیرد [2]:

۱) **صحت**[1]: حفظ صحت و درستی اجزای تشکیل‌دهنده عامل(کد، حالت) در طول سفر

۲) **محرمانگی**[2]: دسترسی میزبان به کد یا حالت عامل بطور مشروع

۳) **در دسترس بودن**[3]: محدودیت نداشتن عامل معتبر از دسترسی به منابع مشروع خود در محیط اجرائی میزبان (بستر)

٤) **احراز اصالت**[4]: شناسائی هویت میزبان توسط عامل متحرک

نقض هر یک از چهار نیاز امنیتی بالا، یک حمله به عامل محسوب می‌شود. به این صورت که در حمله به صحت و محرمانگی عامل، اطلاعات خصوصی موجود در کد یا حالت عامل مورد بهره‌برداری غیرمجاز قرار می‌گیرد. این حمله‌ها به همراه حمله به احراز اصالت عامل، نشان دهنده تلاش گروه بدخواهی جهت استفاده از عامل بدون متوقف کردن اجرای آن است. در حمله به در دسترس بودن، عامل از دسترسی به منابع موردنیازش منع شده و اطلاعات غلطی برای او فراهم می‌شود یا عامل بدون اجرا شدن یا حتی مهاجرت به یک میزبان دیگر نابود می‌شود.

۱-۳ انگیزه

در هر یک از مکانیزمهای تأمین امنیت عامل در مقابل میزبانها، برخی از نیازمندیهای امنیتی عامل (صحت، محرمانگی، در دسترس بودن و احراز اصالت) برقرار می‌شود. مثلاً در یکی از مهمترین آنها عامل با کد

---

[1] Integrity
[2] Privacy
[3] Availability
[4] Authentication

(مأموریت) رمز شده به محیط فرستاده می‌شود بطوریکه خودش هم از هدف مأموریتش بی‌خبر است. به همین دلیل به این نوع عامل اصطلاحاً عامل بی‌خبر[1] گفته می‌شود. عامل در محیط به کمک طرف سوم مطمئنی[2] کلید رمزگشائی کدش را بدست می‌آورد و از مأموریت خود باخبر می‌شود. در این روش نیازمندی صحت و محرمانگی کد عامل در طول سفر حفظ می‌شود [2].

در اینجا اگر فرض کنیم که محرمانگی کد و حالت عامل را با استفاده از مکانیزم فوق تأمین کردیم باز هم یک شنودگر[3] می‌تواند بدون دانستن محتوای کد و حالت عامل از طریق جریان پیامهای مبادله شده بین عامل با میزبانها و یا مالکش به مضمون فعالیتهای عامل پی ببرد و محرمانگی کد عامل را به مخاطره اندازد.

همچنین در بسیاری از مواقع لازم است که مالک سعی در مخفی نگه داشتن نام خود نماید. مثلاً ممکن است یک مالک بخواهد در مورد موضوع حساسی همچون اطلاعات سیاسی به جستجو در وب بپردازد یا بدون آنکه نام خود را فاش کند و نگران تغییر کد عاملش باشد، عاملی را به محیط بفرستد تا در خرید و فروشهای بی‌نشان[4] شرکت کند [3]. بنابراین در این حالت عامل بصورتی در شبکه حرکت می‌کند که بی‌نشانی مالک آن فراهم شود.

در سیستمهای مبتنی بر عامل متحرک می‌توان نوع دیگری از بی‌نشانی یعنی بی‌نشانی سفرنامه[5] را مطرح کرد. سفرنامه عامل همان مسیر حرکت عامل و لیست بسترهائی است که عامل در آنها اجرا شده است. در حالت بی-نشانی سفرنامه فقط مالک از سفرنامه عامل مطلع می‌شود و هیچ‌کس حتی تحلیلگر ترافیک شبکه و میزبانهای سفرنامه هم نمی‌توانند از آن مطلع شوند [38].

برای درک اهمیت ویژگی بی‌نشانی مالک و بی‌نشانی سفرنامه عامل در یک سیستم مبتنی بر عامل فرض کنید یک شرکت تجاری خواهان آن باشد که عاملی را به شبکه بفرستد تا اطلاعاتی راجع به موجودی و قیمت کالاهای شرکتهای رقیب جمع‌آوری نماید. در این حالت لازم است بی‌نشانی مالک و بی‌نشانی سفرنامه عامل فراهم شود. زیرا شرکتهای رقیب با دانستن هویت مالک عامل یا هویت شرکتهائی که عامل قبلاً در آنها به جستجو پرداخته و یا در آینده آنها را ملاقات خواهد کرد، روی چنین عاملی حساس شده و اطلاعات غلطی را به او می‌دهند تا هم مالک (شرکت رقیب) و هم شرکتهای رقیبی که عامل در آینده آنها را ملاقات خواهد کرد را فریب دهند.

---

[1] Clueless Agent
[2] Trusted Third Party
[3] Eavesdropper
[4] Anonymous
[5] Itinerary

با اینکه تحقیقات زیادی در زمینه برقراری بی‌نشانی در ارتباطات شبکه صورت گرفته، ولی در مورد برقراری آن در سیستمهای مبتنی بر عامل متحرک کمتر کار شده است. همچنین راه‌حلی وجود ندارد که هم به تأمین جنبه‌های امنیت عامل اهمیت دهد و هم به برقراری ویژگی بی‌نشانی برای عامل بپردازد. در حالیکه می‌توان با مخفی نگه داشتن هویت مالک عامل، سفرنامه عامل و همچنین مأموریت آن، حساسیت میزبانها نسبت به عامل را کاهش دهیم و از بی‌نشانی به عنوان ابزاری در جهت تأمین امنیت عامل استفاده کنیم.

بطور خلاصه، برقراری صحت و محرمانگی کد عامل در شبکه کار بسیار ارزشمندی است زیرا یک میزبان بدخواه می‌تواند براساس اهداف خود کد عامل را تغییر داده و به صحت کد لطمه وارد سازد و یا کد عامل را مورد تحلیل قرار داده و به هدف مأموریت او پی ببرد و محرمانگی کد نقض شود. بنابراین استفاده از عاملهای بی-خبر در یک شبکه خطر فریب خوردن عامل را کاهش می‌دهد.

همچنین اگر توزیع چنین عاملهائی در شبکه و ارتباطشان با مالک با استفاده از کانالهای بی‌نشان انجام پذیرد، مالک می‌تواند عاملش را بدون هیچ ترس و واهمه‌ای از فاش شدن نام و مکان خود به مأموریتهای مختلفی بفرستد زیرا نه تنها میزبانهای عامل بلکه هیچ یک از شنودگرهای بین راه هم نمی‌توانند با تحلیل ترافیک شبکه به فعالیتهای او پی ببرند.

چنین عاملی با داشتن سپر محکمی در جهت حفاظت خود (خصوصیت بی‌خبری) و نقابی جهت مخفی نگه-داشتن نام خود (خصوصیت بی‌نشانی) به میزبانهای شبکه سفر می‌کند. این عامل می‌تواند در زمینه‌های مختلفی همچون تجارت الکترونیک، درمان الکترونیکی، مذاکره‌های[1] الکترونیکی و حراجهای الکترونیکی و کاربردهای نظامی نقش مهمی را ایفا کند.

۱-٤ مروری بر ساختار پایان نامه

ساختار پایان نامه به این ترتیب است. در فصل دوم ابتدا سیستمهای مبتنی بر عامل متحرک معرفی شده و سپس مسئله امنیت در این سیستمها و راهکارهای ارائه شده جهت تأمین آن بطور مبسوط بیان خواهد شد. در فصل سوم ویژگی بی‌نشانی و کارهای انجام شده در زمینه تأمین بی‌نشانی در شبکه و در سیستمهای مبتنی بر عامل متحرک بررسی خواهد شد.

---

[1] Negotiation

در فصل چهارم پروتکل پیشنهادی اول توضیح داده خواهد شد. در این پروتکل با الهام گرفتن از روشهای تأمین بی‌نشانی در شبکه، بی‌نشانی مالک و بی‌نشانی سفرنامه عامل تأمین می‌شود. همچنین حرکت این عامل در شبکه بصورتی است که در مقابل حمله‌های مختلف مقاوم بماند.

در فصل پنجم پروتکل پیشنهادی دوم با استفاده از عامل بی‌خبر و بی‌نشان بیان می‌شود. به این صورت که علاوه بر تأمین بی‌نشانی مالک و سفرنامه عامل، صحت و محرمانگی کد عامل با استفاده از مکانیزم صفحه اعلانات برقرار می‌شود.

مقاوم بودن پروتکلهای پیشنهادی در مقابل حمله‌های مرسوم در سیستمهای مبتنی بر عامل در انتهای فصلهای مربوط به آنها مورد بررسی قرار گرفته است. در نهایت در فصل ششم پس از بیان نتایج، با ارائه پیشنهادات بحث را به پایان می‌بریم.