
بسم الله الرحمن الرحيم

بسمه تعالی

دانشگاه صنعتی امیرکبیر

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

پایان نامه کارشناسی ارشد گرایش هوش مصنوعی

سیستم تشخیص نفوذ توزیع شده مبتنی بر عامل های متحرک

Mobile agent based Distributed intrusion detection system

نگارش

مجید اسدپور ۸۱۱۳۱۵۸۹

استاد راهنما

آقای دکتر بروجردی

تابستان ۸۴

به نام پروردگار یگانه

اکنون که با عنایت به پروردگار متعال و همت و مساعدت استاد ارجمندم موفق به اتمام پروژه شده ام بر خود فـرض می دارم ازکلیه عزیزانی که در این راه یاری ام نموده اند سپاسگزاری کنم خصوصـا از اسـتاد بزرگـوارم جنـاب آقـای دکتر بروجردی که با دقت و حوصله زیاد راهنمایی این پروژه را بر عهده داشته اند و با نظرات ارزشمند خود بر غنای علمی پایان نامه افزوده اند و قدم به قدم همیار من بوده اند نهایت تشکر و سپاسگزاری را دارم .

به نام پروردگار یگانه

این پایان نامه بر اساس شماره قرارداد ۵۰۰/۱۰۰۷۲/ت مورخه ۸۳/۹/۲۱ تحت حمایت مالی مرکز تحقیقات مخابرات ایران انجام شده است.

فهرست مطالب

فهرست شکل ها

فهرست جداول

چکیده

حملات توزیع شده در شبکه های کامپیوتری، حملاتی هستند که از نقاط متعدد یک یا چند سیستم کامپیوتری را تهدید می کنند. سیستم تشخیص نفوذ توزیع شده (DIDS) سیستمی است که می تواند علاوه بر تشخیص حملات محلی، حملاتی که به صورت توزیع شده هستند را نیز تشخیص دهد. به عبارت دیگر چنین سیستمی می تواند با مشاهده آثار حمله توزیع شده در مکانهای مختلف و به صورت مستقل، آنها را به یکدیگر مرتبط سازد.

این پایان نامه یک سیستم تشخیص نفوذ توزیع شده با استفاده از عامل های متحرک را توصیف می کند. این سیستم به دلیل استفاده از عامل های متحرک مبتنی بر جاوا نسبت به سیستم های تشخیص نفوذ قدیمی برتری دارد.

در معماری جدیدی که در این پایان نامه معرفی شده است، عامل های متحرک به صورت هماهنگ اطلاعات میزبانهای شبکه را پردازش کرده و نهایتاً اطلاعات نفوذ را استخراج میکنند.

بسته نرم افزاری Aglet که توسط IBM توسعه داده شده است به عنوان پایه معماری عامل مورد استفاده قرار گرفته است. نمونه ای از این سیستم پیاده سازی شده است که نتایج ارزیابی آن ارائه میگردد. این ارزیابی ها نشان میدهد که این سیستم دارای مزایای تشخیص حملات توزیع شده، مقاوم در برابر خرابی، توسعه پذیری و سربار کم میباشد.

۱- مقدمه

با رشد سریع اینترنت ، حوادث مربوط به امنیت نیز افزایش یافته است زیرا تکنولوژی های نفوذ به روشهای پیچیده ای از قبیل حملات گروهی و هماهنگ شده توسعه یافته اند. در چنین وضعیتی اساساً به نرم افزارهایی نیاز داریم که به صورت اتوماتیک بتوانند اکثر نفوذها را تشخیص دهند. سیستم های IDS بعنوان نگهبان شبکه باید قادر باشند تا نفوذها را پس از وقوع در مدت زمان کوتاه تشخیص دهند. بعضی مشکلات IDS های موجود به قرار زیر است [۷] و [۱۱] .

۱. اکثر IDS ها حملات را از طریق تحلیل اطلاعات در یک نقطه مرکزی تشخیص میدهند که این نقطه مرکزی ممکن است یک میزبان و یا یک اینترفیس شبکه باشد. مولفه های IDS قادر به برقراری ارتباط و همکاری با یکدیگر نیستند و این محدودیت مانع از تشخیص حملات وسیع و توزیع شده میگردد.

۲. اکثر IDS های تجاری دارای معماری سلسله مراتبی هستند که سیستم کنترل کننده در بالای ساختار سلسه مراتب قرار دارد .واحدهای جمع کننده اطلاعات در نودهای میانی و واحدهای سنسور در نودهای پایین و در پایین ساختار سلسله مراتب قرار دارند. در چنین سیستمی انتقال حجم وسیع داده از طریق شبکه منجر به تراکم در شبکه میگردد.

۳. به خاطر اتکا به ساختارهای سلسله مراتبی، اکثر IDS ها هر لحظه ممکن است مورد حمله قرار بگیرند. قطع یک شاخه از این ساختار باعث از بین رفتن ساختار IDS و از کار افتادن این سیستم میگردد. بعلاوه تکنیک های مقاوم از قبیل متحرک بودن ، افزونگی و ترمیم شدن به صورت پویا در این گونه سیستم ها وجود ندارند.

۴. اکثر IDS های فعلی نمیتوانند از آلارم های نفوذ گذشته، رفتارهای نفوذی آینده را تحلیل کنند. به عنوان مثال اگر سیستم IDS بتواند چندین نفوذ را از میزبانهای مختلف و از منبع یکسان اما در زمانهای مختلف تشخیص بدهد نمیتواند این حملات را به یکدیگر مرتبط کند.

برای حل مشکلات مطرح شده میتوان از معماری عامل متحرک معرفی شده در این پایان نامه بهره برد. عامل برنامه ای است که به صورت خودمختار و مستقل و در جهت یک هدف حرکت میکند و همچنین با عامل های دیگر تعامل برقرار میکند. عامل متحرک نوع به خصوصی از عامل است که قادر به جابجایی از یک میزبان به میزبان دیگر است. عامل متحرک دارای ویژگی های کاهش بار شبکه، کاهش تاخیر شبکه، اجرای همزمان و غیر همزمان، مقاوم در برابر خرابی ، قابلیت گسترش و همچنین قابلیت اجرا در محیط های مختلف و ناهمگن است. نهایتاً اینکه تکنولوژی عامل متحرک برای حل مشکلات مذکور کاملاً مناسب میباشد [۹] .

فصل ۲ این پایان نامه درباره کارهای انجام شده مرتبط بحث میکند. کارهایی که به نوعی به تشخیص نفوذ خصوصا تشخیص نفوذ توزیع شده برمی گردد در این فصل در مورد آنها بحث می گردد. البته کارهایی که به نوعی از تکنولوژی عامل ها ، ثابت و یا متحرک، بهره می برند. فصل ۳ حملات موجود را دسته بندی میکند و ساختار قابل درکی از حملات را به شما نشان میدهد. برای آنکه بتوان با حملات مبارزه کرد شناخت آنها ضروری است در غیر این صورت نمی توان تحلیل درستی از تشخیص و یا عدم تشخیص حملات داشته باشیم. در فصل ۴، عامل های متحرک، مزایای آنها، ساختار و دلیل استفاده آن در پروژه انجام شده را بیان میکند. به طور کل مزایای استفاده از عامل های متحرک در سیستم های توزیع شده در قالب چند دلیل اصلی بیان می گردد. در فصل ۵ Snort که به عنوان یک IDS محلی در این پروژه مورد استفاده قرار گرفته است تشریح میگردد. Snort از قوی ترین ابزار های رایگان است که در به صورت تشخیص نفوذ محلی عمل می کند. در این پروژه سعی کرده ایم تا با استفاده از چندین IDS محلی در شبکه و نحوه چینش آنها و نوع همکاری ما بین آنها یک سیستم تشخیص نفوذ توزیع شده با پارامتر های بهینه توسعه دهیم. فصل ۶ به تشریح ابزارAglet، بستر اجرایی عامل متحرک میپردازد. در این فصل API[1] های موجود در این بستر که برای پیاده سازی پروژه مورد استفاده قرار گرفته است به تفصیل مورد بررسی قرار می

[1] Application Program Interface

گیرد. در فصل ۷ معماری پیشنهادی و نحوه پیاده سازی آن همراه با جرئیات شرح داده میشود و در فصل ۸ که بخش پایانی این پایان نامه محسوب میگردد، نتایج ارزیابی پروژه و مقایسه آن با دیگر پروژه ها مورد بحث و بررسی قرار میگیرد. برای ارزیابی و مقایسه دو کار شاخص دیگر را که به نوعی با کار اینجانب مرتبط بوده اند را انتخاب کرده ام. یکی کار بازرس های متحرک است که در دانشگاه امیرکبیر در سال ۱۳۸۱ به انجام رسیده است و دیگری MA-IDS که در فصل مورد نظر در مورد جزئیات آنها شرح کافی داده خواهد شد. در فصل پایانی نتایج مثبت و منفی کار پیشنهادی و همچنین پیشنهاداتی جهت ادامه کار فوق داده شده است.

۲- کارهای انجام شده

با افزایش سرعت کارآیی تعداد و ارتباط کامپیوترهای در دهه ۱۹۷۰ نیاز به سیستمهای امنیتی رشد بسیاری پیدا کرد. در سالهای ۱۹۷۷ و ۱۹۷۸ سازمان بین المللی استاندارد، جلسه ای را مابین دولت ها و ارگانهای بازرسی EDP تشکیل داد که نتیجه آن جلسه، تهیه گزارشی از وضعیت امنیت، بازرسی و کنترل سیستم ها در آن زمان بود. در همیم زمان وزارت نیروی کشود آمریکا به علت نگرانی از اوضاع امنیتی سیستم های خود، تحقیق بسیار دقیقی را در مورد بازرسی و امنیت سیستم ها ی کامپیوتری شروع کرد. این کار توسط فردی به نام Anderson انجام شد.

Anderson اولین فردی است که مقاله ای در رابطه با لزوم بازرسی خودکار امنیت سیستم ها ارائه داد. گزارش Anderson که در سال ۱۹۸۰ تهیه شد را میتوان به عنوان هسته اولیه مفاهیم تشخیص نفوذ معرفی کرد. در این گزارش مکانیزم هایی برای بازرسی امنیت سیستم ها معرفی شد و همچنین مشخص شده است که در صورت بروز خرابی در سیستم چگونه با آن مقابله شود.

در سالهای ۱۹۸۴ تا ۱۹۸۶ Denning و Neumann تحقیقاتی در زمینه امنیت سیستمهای کامپیوتری انجام دادند که نتیجه آن تولید یک سیستم تشخیص نفوذ به صورت Real Time بود که بر اساس سیستمهای خبره عمل میکرد. این سیستم IDES نامگذاری شد. در این پروژه ترکیبی از تشخیص ناهنجاری و تشخیص سوء استفاده مورد برسی قرار گرفته بود. ایده مطرح شده در این پروژه به عنوان پایه خیلی از سیستم های تشخیص نفوذ که از آن به بعد ایجاد شدند مورد استفاده قرار گرفت.

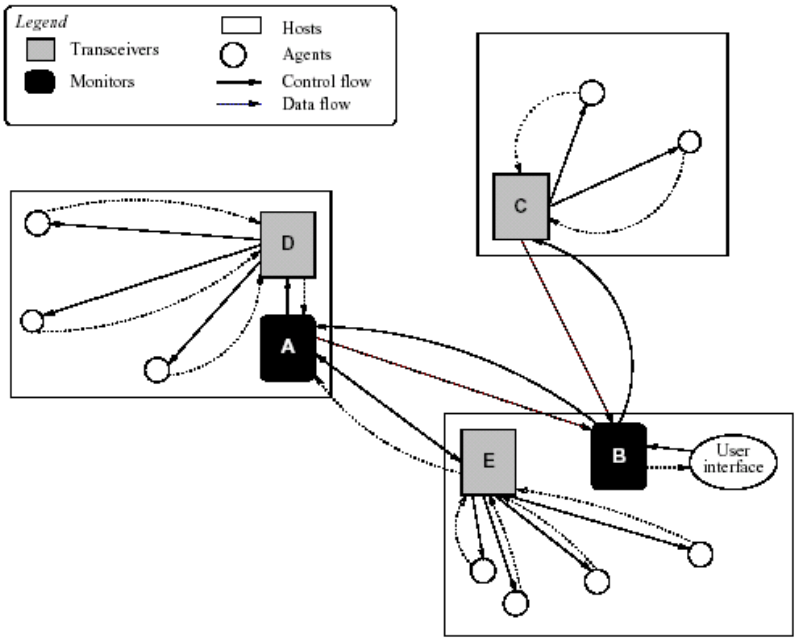
گزارش Anderson و تحقیقاتی که بر روی پروژه IDS صورت گرفت ، شروع کننده زنجیره ای از تحقیقات در رابطه با سیستم های تشخیص نفوذ بودند. در ادامه تعدادی از سیستم های مطرح که از آن تاریخ به بعد به وجود آمدند پرداخته می شود.

۲-۱- AAFID [۱۱]

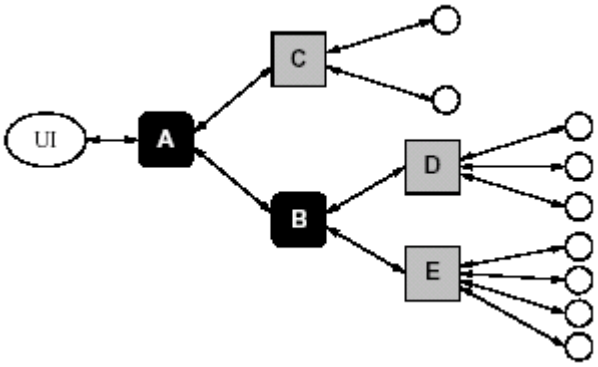
این ساختار از سه جزء اصلی تشکیل شده است: عامل، Transceiver و محافظ (شکل ۲-۱). یک سیستم AAFID میتواند بین هر تعداد از میزبانهای یک شبکه توزیع گردد. هر میزبان میتواند هر تعدادی عامل داشته باشد که وقایع نامترقبه را کنترل نماید. تمامی عامل ها در یک میزبان یافته هایشان را به یک Transceiver گزارش میکنند. Transceiver ها جزیی از هر میزبان هستند که عملیات تمامی عامل های فعال در آن میزبان را زیر نظر دارند. آنها کنترل عامل های فعال در آن میزبان را در دست دارند و قادر هستند که عامل ها را راه اندازی کرده یا آنها را از ادامه فعالیت باز نگهدارند و یا حتی دستورات پیکربندی جدید را برای آنها ارسال نمایند. همچنین ممکن است باعث ساده سازی داده های رسیده از عاملها گردند. در نهایت Transceiver ها نتایج خود را به یک یا چند محافظ گزارش میکنند. هر محافظ عملیات چندین Transceiver را زیر نظر دارد. محافظ ها بصورت گسترده تری به داده های شبکه دسترسی دارند و بنابراین قادرند تهاجماتی که چندین میزبان درگیر آن هستند را کشف نمایند.

محافظها در یک روش سلسله مراتبی سازماندهی می گردند بطوریکه هر محافظ به محافظهای سطح بالاتری گزارش میدهد. همچنین یک Transceiver ممکن است به بیشتر از یک محافظ گزارش دهد تا در صورت عمل نکردن یکی از محافظها مشکلی پیش نیاید. بالاخره یک محافظ مسئول مهیا کردن اطلاعات و گرفتن دستورات کنترلی از یک رابط کاربر میباشد. یک عامل یک جزء مستقل در اجرا است که ابعاد بخصوصی از یک میزبان را کنترل کرده و رفتارهای نابهنجار یا جالب را به Transceiver مناسب گزارش میکند. برای مثال، یک عامل ممکن است تعداد زیادی از اتصالات telnet را در یک میزبان محافظت شده مورد جستجو قرار داده و وقایع مشکوک را مورد بررسی قرار دهد. سپس عامل گزارشی تهیه میکند که به یک Transceiver مناسب فرستاده میشود. عامل این اجازه را ندارد که مستقیما یک اخطار تولید کند. معمولا یک Transceiver یا یک مانیتور براساس اطلاعات رسیده از یک یا چند عامل یک اخطار تولید میکند. بوسیله ترکیب

گزارشهای عامل های مختلف، Transceiver ها تصویری از حالت میزبانشان و مانیتورها تصویری از حالتهای شبکه ای که تحت کنترل است میسازند. عاملها مستقیما با یکدیگر در ساختارAAFID ارتباط ندارند و تنها اطلاعاتشان را به Transceiver میفرستند. Transceiver تصمیم میگیرد که با توجه به اطلاعات رسیده چه کاری انجام دهد.



شکل ۲-۱- ساختار کلی سیستم AAFID



شکل ۲-۲- ارتباط بین بخش‌های مختلف سیستم

نسخه اول این IDS بنام AAFID1 با استفاده از Java و نسخه دوم آن بنام AAFID2 با استفاده از Perl در سیستم عامل Linux پیاده سازی شده است.

۲-۲- MAIDS [۷] [1]

پروژه MAIDS یک ایده بلند پروازانه برای ایجاد یک سیستم تشخیص نفوذ کارا و مقاوم در برابر خطا میباشد که هر واحدش با واحدهای همتایش در دیگر سیستمهای تشخیص منطبق بوده و همچنین به سادگی قابل استفاده و پیکر بندی میباشد. این طرح در سال ۲۰۰۱ توسط دکتر هلمر و همکارانش در دانشگاه lowa state پیاده سازی شد و کلیه مستندات مربوط به آن در حال حاضر در سایت http://latte.cs.iastate.edu موجود میباشد. کاربر با یک توصیف سطح بالا از ضعفهای سیستم شروع کرده و آنها را در غالب یک درخت خطای نرم افزاری مینویسد. این درخت به یک CPN که تشکیل دهنده طرح سیستم تشخیص نفوذ میباشد تبدیل میگردد.

تکنیک مدل SFT به طور رایج در مهندسی امنیت استفاده میگردد. تحلیلSFT[2] ترکیب رویدادهایی که موجب از کار افتادن سیستم میشود را بررسی میکند. بصورت خاص، رویدادهای بنیادی به عنوان گره های برگ و رویدادهای شکست بعنوان گره ریشه در درخت خطا در نظر گرفته میشوند. ارتباط گره های SFT گیت های AND و OR رایج میباشد. از این رو هنگامی که ترکیبی از گره های بنیادی بصورت منطقی مقدار درست را برای شکست تلقی مینماید، گره ریشه نیز فورا " درست " در نظر گرفته میشود.

یک CPN یک گراف جهت دار دو قسمتی است که هر گره از آن یا یک مکان[3] و یا یک انتقال[4] میباشد. داده ها که در اینجا token نامیده میشوند در مکانها قرار میگیرند. Token از یک مکان به مکان دیگری از طریق انتقالها جابجا میشوند. رنگ یک token همانند نوع یک داده میباشد. انتقالها قوانین یکسان سازی دارند که میزان مصرف token های رسیده از کمانهای ورودی و با یک رنگ مشخص را با میزان token های جدید آزاد شده از طریق کمانهای خروجی را اداره میکند.

SFT مزایای بسیاری دارد که موجب شده است تا در MAIDS مورد استفاده قرار گیرد.

---

[1] Mobile Agent Intrusion Detection System
[2] Colored Petri Net
[3] Place
[4] Transition

۱) عموما به سادگی قابل استفاده و قابل فهم هستند.

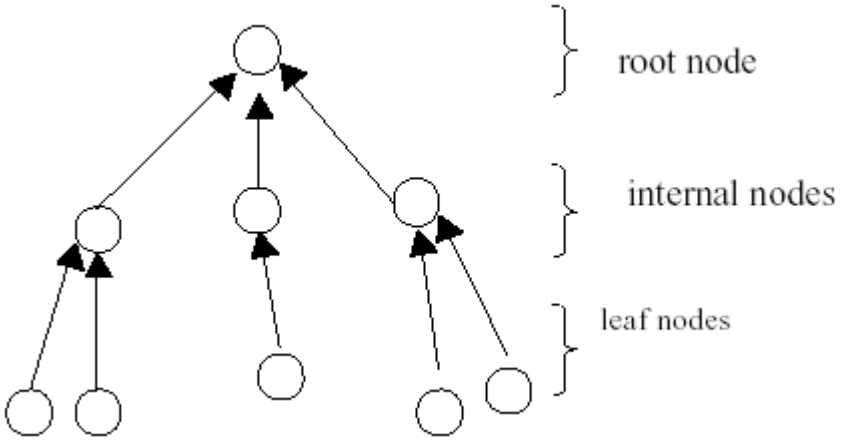
۲) با اصلاح و بهبود تدریجی موافق هستند. به محض بوجود آمدن آسیب در سیستم، زیر درختها میتوانند دو برابر شده و یا بسته به باقیمانده درخت خود را بهبود بخشند.

۳) بر خلاف CPN ها حملات را با یک روش مستقیم مدل میکنند یعنی با دقت بسیاری دامنه تشخیص نفوذ قالب ریزی میشود.

۴) تحلیل های SFT برای ایجاد یک درک بهتر در مورد امنیت، حتی در خارج از قلمرو تشخیص نفوذ مفید است.

۲-۳- مدل Sentil Sellih

در [۳۹] یک مدل سلسله مراتبی برای IDS پیشنهاد شده است که از سه لایه اصلی (شکل ۲-۳) تشکیل شده است:



شکل ۲-۳- معماری سلسله مراتبی سیستم تشخیص مزاحم توزیع شده

۱) گره ریشه که به عنوان تصمیم گیرنده مرکزی عمل مینماید.

۲) گره های میانی که وظیفه آنالیز داده ها و کاهش آنها را برعهده دارند.

۳) گره های برگ که کار جمع آوری داده ها را انجام میدهند.

گره ریشه یک سرویس دهنده مرکزی میباشد که کلیه اطلاعات لازم را با استفاده از گره های میانی گردآوری کرده تا یک تصمیم کلی در مورد وقوع یا عدم وقوع یک حمله گرفته شود. از آنجایی که

تنها یک گره ریشه وجود دارد، فرض میکنیم که بصورت معقول و مناسبی بتواند برخی از متدهای موجود در برابر تخلفات امنیتی اصلی از خود محافظت نماید.

مسئله اصلی مورد توجه، امنیت گره های برگ و بخشهای میانی است چرا که آنها بین شبکه های گوناگون و احتمالا ناامن توزیع شده اند و باعث گردیده اند که در مقابل حملات سیستم آسیب پذیر گردد. در این پروژه ادعا میشود که با امن نگه داشتن مناسب این گره ها یک IDS مقاوم در برابر حملات بوجود می آید که قادر است در یک محیط توزیع شده بزرگ کار کند. همچنین بر متدلوژی تاکید میشود که در آن یک نظارت و تضمین اضافی برای اجزاء میانی در سلسله مراتب IDS فراهم میباشد. این روش بر تحرک گره های میانی تاکید دارد. برای این منظور اجزاء میانی با استفاده از فن آوری عاملهای متحرک طراحی گردیده است. عاملهای متحرک مقاوم در برابر حملات در یک ساختاری عمل میکنند که در آن گره های برگ وظیفه جمع آوری داده ها را عهده دارند. این گره های برگ که - در این پروژه از آنها با عنوان مانیتورها یاد شده است - ترافیک شبکه را مشاهده کرده و هر گونه رفتار مشکوک را به عاملها یعنی اجزاء میانی گزارش میکنند. در کل، گروههای مختلفی از عاملها مسئول پردازش داده های رسیده از مانیتورهای مختلف هستند. عاملها سعی میکنند تا یک دانش رو به افزایش از فعالیتها در شبکه هایی که تحت نظارت آنهاست، بسازند. داده های آنالیز شده به گره ریشه که مسئول تشخیص وقوع نفوذ است فرستاده میشود. شکل ۲-۴ یک مثال از معماری سیستم را نشان میدهد.

محیط توزیع شده ای که این IDS در آن بکار گرفته شده است شامل محیطهای زیر بنایی عاملهای متحرک مازاد بر احتیاجی میباشد که در بین شبکه های مختلف توزیع شده اند. این محیطهای زیر بنایی بطور یکسان قادر به میزبانی از عاملهای متحرک بوده و تمامی منابع مورد نیاز جهت یک اجرای مناسب را فراهم می آورند.

تحرک اجزاء این IDS مستقیما باعث حذف برخی خطرات بوجود آمده توسط مهاجمین میگردد. جابجایی دائم عاملها را قادر میسازد که بصورت غیر مستقیم مکانهایشان را مخفی نموده و از