دانشکده فنی و مهندسی

گروه مهندسی فنّاوری اطلاعات

پایان‌نامه دوره کارشناسی ارشد مهندسی فناوری اطلاعات

تشخیص ناهنجاری‌های شبکه با استفاده از روش ترکیبی سیستم دفاعی مصنوعی و یادگیری ماشین SVM

استاد راهنما:

دکتر علی یزدیان

دانشجو:

مهدی الهی

زمستان ۱۳۹۰


بسم الله الرحمن الرحيم

بسمه تعالی

تاییدیه اعضای هیات داوران حاضر در جلسه دفاع از پایان نامه

آقای مهدی الهی پایان نامه ٦ واحدی خود را **با عنوان تشخیص ناهنجاری های شبکه با استفاده از روش ترکیبی سیستم دفاعی مصنوعی و یادگیری ماشین** در تاریخ ۱۳۹۰/۱۲/۲۱ ارائه کردند.

اعضای هیات داوران نسخه نهایی این پایان نامه را از نظر فرم و محتوا تایید کرده و پذیرش آنرا برای تکمیل درجه کارشناسی ارشد مهندسی فناوری اطلاعات – سیستمهای اطلاعاتی پیشنهاد می کنند.

عضو هیات داوران	*نام و نام خانوادگی*	*رتبه علمی*	*امضا*
استاد راهنما	دکتر علی یزدیان ورجانی	استادیار	
استاد ناظر	دکتر مهدی آبادی	استادیار	
استاد ناظر	دکتر غلامعلی منتظر	دانشیار	
استاد ناظر	دکتر حسین قرایی	استادیار	
مدیر گروه (یا نماینده گروه تخصصی)	دکتر غلامعلی منتظر	دانشیار	

آیین نامه چاپ پایان‌نامه (رساله)های دانشجویان دانشگاه تربیت مدرس

نظر به اینکه چاپ و انتشار پایان نامه (رساله)های تحصیلی دانشجویان دانشگاه تربیت مدرس، مبین بخشی از فعالیتهای علمی – پژوهشی دانشگاه است بنابراین به منظور آگاهی و رعایت حقوق دانشگاه،دانش آموختگان این دانشگاه نسبت به رعایت موارد ذیل متعهد می‌شوند:

ماده ۱: در صورت اقدام به چاپ پایان نامه (رساله)ی خود، مراتب را قبلاً به طور کتبی به «دفتر نشر آثارعلمی» دانشگاه اطلاع دهد.

ماده ۲: در صفحه سوم کتاب (پس از برگ شناسنامه) عبارت ذیل را چاپ کند:

«کتاب حاضر، حاصل پایان نامه کارشناسی ارشد نگارنده در رشته **مهندسی فناوری اطلاعات** است که در سال **۱۳۸۸** در دانشکده **فنی و مهندسی** دانشگاه تربیت مدرس به راهنمایی جناب آقای دکتر **علی یزدیان** ، از آن دفاع شده است.»

ماده ۳: به منظور جبران بخشی از هزینه‌های انتشارات دانشگاه، تعداد یک درصد شمارگان کتاب (در هر نوبت‌چاپ) را به «دفتر نشر آثارعلمی» دانشگاه اهدا کند. دانشگاه می‌تواند مازاد نیاز خود را به نفع مرکز نشر درمعرض فروش قرار دهد.

ماده ۴: در صورت عدم رعایت ماده ۳، ۵۰٪ بهای شمارگان چاپ شده رابه عنوان خسارت به دانشگاه تربیت‌مدرس، تأدیه کند.

ماده ۵: دانشجو تعهد و قبول می کند در صورت خودداری از پرداخت بهای خسارت، دانشگاه می‌تواندخسارت مذکور را از طریق مراجع قضایی مطالبه و وصول کند؛ به علاوه به دانشگاه حق می‌دهد به منظور استیفای حقوق خود، از طریق دادگاه، معادل وجه مذکور در ماده ۴ را از محل توقیف کتابهای عرضه شده‌نگارنده برای فروش، تامین نماید.

ماده ۶: اینجانب **مهدی الهی** دانشجوی رشته **مهندسی فناوری اطلاعات** مقطع **کارشناسی ارشد** تعهد فوق وضمانت اجرایی آن را قبول کرده، به آن ملتزم می شوم.

نام و نام خانوادگی: **مهدی الهی**

تاریخ و امضا: ۹۱/۶/۲۴

آیین‌نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهشهای علمی دانشگاه تربیت مدرس

مقدمه: با عنایت به سیاست‌های پژوهشی و فناوری دانشگاه در راستای تحقق عدالت و کرامت انسانها که لازمه شکوفایی علمی و فنی است و رعایت حقوق مادی و معنوی دانشگاه و پژوهشگران، لازم است اعضای هیأت علمی، دانشجویان، دانش‌آموختگان و دیگر همکاران طرح، در مورد نتایج پژوهشهای علمی که تحت عناوین پایان‌نامه، رساله و طرحهای تحقیقاتی با هماهنگی دانشگاه انجام شده است، موارد زیر را رعایت نمایند:

ماده ۱- حق نشر و تکثیر پایان نامه/ رساله و درآمدهای حاصل از آنها متعلق به دانشگاه می باشد ولی حقوق معنوی پدید آورندگان محفوظ خواهد بود.

ماده ۲- انتشار مقاله یا مقالات مستخرج از پایان‌نامه/ رساله به صورت چاپ در نشریات علمی و یا ارائه در مجامع علمی باید به نام دانشگاه بوده و با تایید استاد راهنمای اصلی، یکی از اساتید راهنما، مشاور و یا دانشجو مسئول مکاتبات مقاله باشد. ولی مسئولیت علمی مقاله مستخرج از پایان نامه و رساله به عهده اساتید راهنما و دانشجو می باشد.

تبصره: در مقالاتی که پس از دانش‌آموختگی بصورت ترکیبی از اطلاعات جدید و نتایج حاصل از پایان‌نامه/ رساله نیز منتشر می‌شود نیز باید نام دانشگاه درج شود.

ماده ۳- انتشار کتاب، نرم افزار و یا آثار ویژه (اثری هنری مانند فیلم، عکس، نقاشی و نمایشنامه) حاصل از نتایج پایان‌نامه/ رساله و تمامی طرحهای تحقیقاتی کلیه واحدهای دانشگاه اعم از دانشکده ها، مراکز تحقیقاتی، پژوهشکده ها، پارک علم و فناوری و دیگر واحدها باید با مجوز کتبی صادره از معاونت پژوهشی دانشگاه و براساس آئین نامه های مصوب انجام شود.

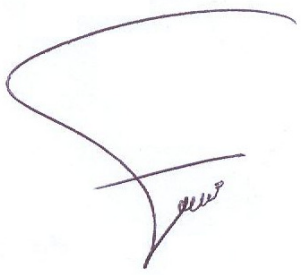
ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه یافته ها در جشنواره‌های ملی، منطقه‌ای و بین‌المللی که حاصل نتایج مستخرج از پایان‌نامه/ رساله و تمامی طرح‌های تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق معاونت پژوهشی دانشگاه انجام گیرد.

ماده ۵- این آیین‌نامه در ۵ ماده و یک تبصره در تاریخ ۸۷/۴/۱ در شورای پژوهشی و در تاریخ ۸۷/۴/۲۳ در هیأت رئیسه دانشگاه به تایید رسید و در جلسه مورخ ۸۷/۷/۱۵ شورای دانشگاه به تصویب رسیده و از تاریخ تصویب در شورای دانشگاه لازم‌الاجرا است.

«اینجانب **مهدی الهی** دانشجوی رشته **مهندسی فناوری اطلاعات** ورودی سال تحصیلی **۱۳۸۸** مقطع **کارشناسی ارشد** دانشکده **فنی و مهندسی** متعهد می شوم کلِیه نکات مندرج در آئین نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهش های علمی دانشگاه تربیت مدرس را در انتشار یافته های علمی مستخرج از پایان نامه / رساله تحصیلی خود رعایت نمایم. در صورت تخلف از مفاد آئین نامه فوق الاشعار به دانشگاه وکالت و نمایندگی می دهم که از طرف اینجانب نسبت به لغو امتیاز اختراع بنام بنده و یا هر گونه امتیاز دیگر و تغییر آن به نام دانشگاه اقدام نماید. ضمناً نسبت به جبران فوری ضرر و زیان حاصله بر اساس برآورد دانشگاه اقدام خواهم نمود و بدینوسیله حق هر گونه اعتراض را از خود سلب نمودم»

امضا: ***مهدی الهی***

تاریخ: ۹۱/۶/۲۴



تقدیم به

پدر و مادر مهربانم که با هیچ واژه ای نمی توان مهر و محبت شان را توصیف کرد

تقدیم به

همسر عزیز و مهربانم که در کنار او آرزوی بهترین روزها را دارم

تقدیر و تشکر

پروردگار مهربان را سپاسگزارم که به من هستی بخشید. به من فرصت داد به امید آنکه بتوانم در راه جلب رضایت او قدم بردارم و توفیق خدمت شایسته به خلقش داشته باشم.

در طی انجام این تحقیق بزرگواران زیادی بنده را هدایت و یاری نموده‌اند. کمترین کاری که می‌توان کرد این است که با ذکر نام آنها از کمک‌ها و راهنمایی‌های بی دریغ و ارزشمندشان تشکر کنم. اینجانب بر خود وظیفه میدانم که در ابتدا مراتب قدردانی خود را از استاد بزرگوارم جناب آقای دکتر علی یزدیان برای قبول راهنمایی این پایان نامه و نیز لطف و مساعدت همه جانبه ایشان را ابراز دارم، که انجام این پروژه تنها با همراهی بی دریغ و بیان نکته‌های راه‌گشای ایشان میسر بود.

در نگارش و ویرایش علمی و ادبی رساله و مقاله‌های مستخرج از آن از کمک‌ها و مشاوره‌های دوستان بزرگوارم آقایان مهندس حسام خوش نیت، مهندس محمد جواد کارگر، مهندس مرتضی پرویزی و مهندس سینا رضا قلی زاده سود برده‌ام که در اینجا از زحمات بی دریغ‌شان تشکر می‌نمایم.

انجام هیچ کاری به ویژه تحصیل در دانشگاه بدون حمایت خانواده میسر نیست، از زحمات و کمک‌های مادرم، پدرم، همسرم، برادران و خواهر بزرگوارم تشکر می‌کنم.

این تحقیق با حمایت مالی مرکز تحقیقات مخابرات ایران انجام گرفته است که بدینوسیله از این مرکز محترم قدردانی می‌کنیم.

چکیده

با استفاده روز افزون از اینترنت و به اشتراک گذاری اطلاعات، تشخیص دسترسی غیر مجاز و همچنین نفوذ در شبکه تبدیل به یکی از اصلی‌ترین نگرانی‌های مدیران شبکه شده است. سیستم‌های تشخیص نفوذ[1] (IDS) عموماً جهت شناسایی و مقابله با نفوذ در سیستم‌های کامپیوتری پیاده سازی می‌شوند. در این سیستم‌ها از دو روش پرکاربرد *تشخیص ناهنجاری* و *تشخیص سوءاستفاده* برای شناسایی نفوذ استفاده می‌شود. یک سیستم تشخیص ناهنجاری در ابتدا روی مثال‌هایی از شرایط نرمال آموزش می‌بیند و بعد از آن پتانسیل تشخیص حملات جدید را دارد. گرچه بسیاری از سیستم‌های تشخیص ناهنجاری به آسانی فعالیت‌های ناهنجار را تشخیص می‌دهند، اما اطلاعاتی سطح بالا و کاربردی برای مسئول شبکه ایجاد نمی‌کنند، و از طرفی دیگر تشخیص بر اساس سوءاستفاده الگوهای شناخته شده را با اطلاعات کافی و جزئیات تشخیص می‌دهد اما توانایی تشخیص حملات جدید را ندارد. در این پایان نامه یک سیستم ترکیبی با هدف دستیابی به مزایای دو روش بیان شده بررسی خواهد شد. در ابتدا ارتباط‌هایی به عنوان ناهنجاری با استفاده از سیستم AIS تشخیص داده می‌شوند، سپس این ارتباط به عنوان یک ناهنجاری در سیستم SVM طبقه بندی می‌شود که اطلاعات سطح بالاتری را به صورت قرار گرفتن در یک نوع کلاس خاص از آن می‌توان استخراج کرد. نتایج بدست آمده روی مجموعه داده مشهور KDD 1999 در این مدل پیشنهاد شده نشان از پایین بودن نرخ خطای مثبت کاذب[2] و تشخیص حملات به خوبی یا بهتر از دیگر مدل‌های مطرح نشان خواهد داد.

کلمات کلیدی: امنیت شبکه، تشخیص نفوذ، تشخیص ناهنجاری، سیستم ایمنی مصنوعی، ماشین بردار پشتیبان

---

[1] *Inrusion Detection Systems*

[2] *False positive*

فهرست مطالب

عنوان **صفحه**

فهرست اشکال

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

فصل اول

کلیّات پژوهش

۱-۱- مقدمه

امروزه یکی از مهم‌ترین مکانیزم‌های ایجاد امنیت شبکه‌ها و سیستم‌های کامپیوتری، تشخیص و جلوگیری از نفوذ (IDP[1]) می‌باشد. این ایده برای اولین بار تنها مورد استقبال مراکز نظامی و محیط‌های تجاری مهم قرار گرفت و دلیل آن بار پردازشی فراوان آن سیستم‌ها بوده است. امروزه با پیشرفتی که در طراحی و تولید سخت‌افزارها و مدارهای مجتمع با کاربرد خاص[2] (ASIC) و همچنین توسعه چشمگیری که در معماری‌های نوین در طراحی و تولید نرم‌افزارها ایجاد شده، امکان استفاده از IDSو IPS برای طیف گسترده‌ای از سیستم‌های کامپیوتری امکان‌پذیر شده است(Debar et al., 1999).

در گذشته سیستم‌های تشخیص نفوذ به عنوان سیستم‌هایی مجزا در نظر گرفته می‌شد در حالی که امروزه این سیستم‌ها را به عنوان زیرسیستم‌هایی از تجهیزات شبکه، سیستم عامل‌ها و حتی سرویس‌ها می‌شناسیم. در این پایان‌نامه هدف بررسی این تکنولوژی به عنوان یکی از راه‌های مطمئن در تأمین امنیت و مدیریت سیستم‌های کامپیوتری در حال و آینده‌ای نزدیک است. در این فصل به کلیات این پژوهش پرداخته می‌شود و در آن به معرفی موضوع، روش اجرای پژوهش، اهداف پژوهش، نوآوری‌های پژوهش، گام‌های روند پژوهش و ساختار مطرح شده در این نوشتار اشاره می‌شود. مفاهیم و انواع سیستم‌های تشخیص نفوذ را در فصل بعدی بررسی خواهیم کرد. در فصل سوم بررسی رویکردهای سیستم ایمنی مصنوعی و ماشین‌های بردار پشتیبان دو رویکردی که در مؤلفه‌های سیستم پیشنهادی استفاده خواهند شد را به صورت مفصل بحث و بررسی خواهیم کرد. در فصل چهارم معماری پیشنهادی سیستم ترکیبی تشخیص ناهنجاری ارائه می‌شود و در نهایت در

---

[1] *Intrusion Detection and Prevention*

[2] *Application Specific Integrated Circuit*

فصل پنجم این معماری پیاده سازی شده و عملکرد آن مورد ارزیابی قرار خواهد گرفت. در فصل ششم هم جمع بندی نهایی و نتیجه گیری کلی خود را از پژوهش انجام شده بیان خواهیم کرد.

۱-۲- تعریف مسئله

امروزه تشخیص و جلوگیری از نفوذ در شبکه های کامپیوتری به عنوان یکی از راهکارهای اصلی در تأمین امنیت شبکه‌ها و سیستم‌های کامپیوتری شناخته می‌شود. سیستم تشخیص نفوذ یا همان IDS به سخت‌افزار، نرم‌افزار یا تلفیقی از هر دو اطلاق می‌گردد که وظیفه‌ی شناسایی تلاش‌هایی که برای نفوذ به شبکه صورت می‌گیرد و ایجاد اخطار احتمالی حملات را بر عهده دارد، که این سیستم می‌تواند یک شبکه‌ی محلی[۱] یا گسترده[۲] باشد. (Patcha and Park, 2007). لازم به ذکر است که IDSها عموماً به گونه ای از پهنای باند شبکه استفاده می‌کنند که می‌تواند بدون تأثیر گذاشتن بر روی ترافیک و معماری شبکه به کار خود ادامه دهند. غالباً IDSها در قبال مشاهده نفوذ فقط به یک هشدار و یا ثبت رویداد در یک فایل اکتفا می‌کنند و هیچ عملی جهت جلوگیری از نفوذ انجام نمی‌دهند. این خصیصه همان موضوعی است که قدرت تحلیل هوشمند ترافیک اطلاعات شبکه را ایجاد می‌کند. این ماهیت IDS را در جایگاهی مناسب جهت تشخیص موارد زیر قرار می‌دهد(Verwoerd and Hunt, 2002):

- حملات شناخته شده قدیمی از طریق امضاء[۳] آن‌ها
- تغییر در جهت و حجم ترافیک مدخل‌های شبکه با استفاده از قوانین پیچیده و تحلیل آماری[۴]
- تغییر در الگوی رفتاری ترافیک شبکه با استفاده از تحلیل جریان
- تشخیص فعالیت ناهنجار با استفاده از تحلیل انحراف معیار
- تشخیص فعالیت مشکوک با استفاده از آنالیز آماری، تحلیل جریان ترافیک شبکه و انحراف از آستانه

۱-۳- اهمیت تحقیق

یک مشکلی که در تشخیص نفوذ وجود دارد وسعت و دامنه حملات و از همه مهم‌تر چند ریختی[۵] و به روز شدن حملات و بد افزارها می‌باشد که نیازمند این است که سیستم‌های تشخیص نفوذ همگام با این حملات به روز شوند، که این کار نیز

---

[1] *Local network*
[2] *Distribute*
[3] *Signature*
[4] *Statistical Analysis*
[5] *polymorphism*

مشکلات خاص خود را دارد. روشی که معمولاً در سیستم‌های تشخیص نفوذ جهت انتفاع این مشکل به کار می‌رود، استفاده از روش تشخیص ناهنجاری‌های شبکه می‌باشد که این کار مشکل نیازمندی به روز شدن سیستم تشخیص نفوذ را در برابر حملات جدید برطرف می‌کند و توانایی تشخیص حملات جدید به وجود می‌آید (Markou and Singh, 2003). این روش در تشخیص حملات ناشناخته بسیار مفید است. از آنجایی که حملات ممکن است با هیچ کدام از الگوهای حمله مطابقت نداشته باشند روش ذکر شده این قابلیت را دارد که حملات ناشناخته را نیز تشخیص دهد.

در این روش برای هر کاربر یا گروه های کاربری مدل رفتار عادی بدست می‌آید. در صورتی که کاربری بر خلاف الگوی رفتاری عادی خود عمل کند سیستم IDS پیام هشدار خواهد داد بنابراین با استفاده از این روش تشخیص نفوذ می‌توانیم نفوذ گران داخلی را تشخیص دهیم(Chen et al., 2010).

از آنجایی که این روش مبتنی بر رفتار و یا پروفایل عادی کاربران است برای نفوذ گران کشف رفتارهای عادی کاربران و یا رفتارهایی که باعث بروز هشدار از طرف IDS نشود بسیار مشکل است (Depren et al., 2005).

از نقاط ضعف این روش اعلام هشدارهای نادرست از جانب IDS می‌باشد به نحوی که رفتار عادی کاربران به عنوان حمله و یا نفوذ به عنوان یک رفتار عادی در نظر گرفته می‌شود. یا به عبارتی دیگر مشکل بزرگ این روش بالا بودن نرخ خطای مثبت کاذب[1] آن می‌باشد. که بهبود بخشیدن این خصیصه یکی از مسائلی است که نیاز بررسی و پژوهش بیشتری در آن احساس می‌شود(Powers and He, 2008).

۱-۴- فرضیه‌های پژوهش

فرضیه‌های اصلی این پژوهش عبارت است از:

الف) می‌توان با طراحی یک سامانه‌ی ترکیبی در سیستم‌های تشخیص نفوذ می‌توان علاوه داشتن مزایای سیستم-های تشخیص نفوذ بر پایه تشخیص ناهنجاری به برخی از مزایای این سیستم‌های بر پایه تشخیص سوءاستفاده رسید.

ب) استفاده از روش تقسیم و غلبه در سیستم‌های تشخیص نفوذ باعث به دست آوردن کارایی بالاتر می‌گردد.

علاوه بر این پیش فرض‌های این تحقیق به شرح زیر است :

الف) امکان یادگیری سیستم تشخیص ناهنجاری در یک محیط عاری از نفوذ برای ساخت یک مدل رفتار نرمال وجود دارد.

[1] *False positive*

ب) یک پایگاه داده از حملات جهت آموزش سیستم طبقه بندی حملات وجود دارد

۱-۵- پرسش‌های پژوهش

سؤالاتی که در این تحقیق به دنبال پاسخ گویی به آن‌ها هستیم:

- آیا استفاده از سیستم ایمنی مصنوعی برای تشخیص ناهنجاری نسبت به دیگر روش‌های رایج، روش کارایی می-باشد؟
- آیا می‌توان عملکرد سیستم ایمنی مصنوعی برای تشخیص ناهنجاری را بهبود بخشید؟
- آیا می‌توان با استفاده از روش SVM معایب سیستم‌های تشخیص ناهنجاری مانند عدم ارائه اطلاعات سطح بالا و نرخ بالای خطای مثبت کاذبی را بهبود بخشد؟
- آیا ترکیب این دو روش ما را به مزایای هر رو رویکرد تشخیص نفوذ (تشخیص سوء رفتار و تشخیص ناهنجـاری) می‌رساند؟
- تا چه اندازه معایب دو رویکرد در سیستم نهایی ما تأثیر می‌گذارد؟

۱-۶- اهداف پژوهش

در این تحقیق به دنبال دست‌یابی و پیاده سازی به یک روش ترکیبی سیستم‌های تشخیص نفوذ مبتنی بر میزبان با استفاده از روش تشخیص ناهنجاری می‌باشیم. که در این سیستم قصد بر این است که با استفاده از رویکرد سیستم ایمنی مصنوعی مدل رفتاری کاربران را بدست آورده و ناهنجاری‌ها را تشخیص دهیم. علاوه بر این سعی شده تا با ترکیب این سیسـتم بـا یک سیستم طبقه بندی با استفاده از روش ماشین بردار پشتیبان بعضی از معایب سیستم‌های تشخیص ناهنجاری را حـذف کنیم.

۱-۷- نوآوری پژوهش

امروزه کاربرد روش‌های مختلف هوشمند در جهت تشخیص ناهنجاری افزایش چشمگیری داشته است و سیستم‌های تشخیص نفوذ با استفاده از روش‌های هوش مصنوعی و یادگیری ماشین و دیگر الگوریتم‌های بهینه سازی سعی در بهبود کارایی خود داشته‌اند. بنابراین تشخیص ناهنجاری‌های شبکه، ارائه اطلاعات سطح بالاتری از اطلاعاتی که سیستم‌های تشخیص ناهنجاری ارائه می‌دهند و همچنین ارائه راهکارهایی جهت برخورد با ناهنجاری و آگاهی از تأثیرهای آن و پایین