



دانشکده فنی و مهندسی
گروه مهندسی فناوری اطلاعات

پایان نامه 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

الله الرحمن الرحيم



بسمه تعالی

تاییدیه اعضای هیات داوران حاضر در جلسه دفاع از پایان نامه

آقای مهدی الهی پایان نامه ۶ 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 پایان نامه (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 می شوند:

ماده ۱: در صورت اقدام به چاپ پایان نامه (رساله) ی خود، مراتب را قبلاً به طور کتبی به «دفتر نشر آثار علمی» 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 هزینه های انتشارات دانشگاه، تعداد یک درصد شمارگان کتاب (در هر نوبت چاپ) را به «دفتر نشر آثار علمی» دانشگاه اهدا کند. دانشگاه می تواند مازاد نیاز خود را به نفع مرکز نشر در معرض فروش قرار دهد.

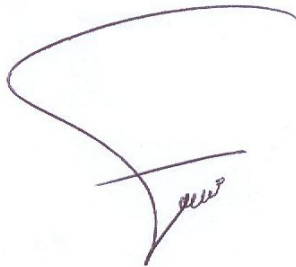
ماده ۴: در صورت عدم رعایت ماده ۳، ۵۰٪ بهای شمارگان چاپ شده رابه عنوان خسارت به دانشگاه تربیت مدرس، تأدیه کند.

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

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

نام و نام خانوادگی: **مهدی الهی**

تاریخ و امضا: ۹۱/۶/۲۴



آیین نامه 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.

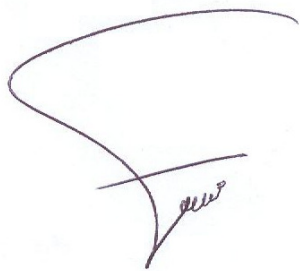
ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه یافته ها در جشنواره‌های ملی، منطقه‌ای و بین‌المللی که حاصل نتایج مستخرج از پایان‌نامه/ رساله و تمامی طرحهای تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق معاونت پژوهشی دانشگاه انجام گیرد.

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 کلیه 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 پیچ و اثره 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 خلقت 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 بی‌دینغ و ارزشمندشان تشکر کنم. اینجانب بر خود وظیفه میدانم که در ابتدا مراتب قدردانی خود را از استاد بزرگوارم جناب آقای دکتر علی‌زیدیان برای قبول راهنمایی این پامان‌نامه و نیز لطف و مساعدت همه‌جانبه ایشان را ابراز دارم، که انجام این پروژه تنها با همراهی بی‌دینغ و بی‌انگه‌های 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 خوش‌نیت، مهندس محمد جواد کارگر، مهندس مرتضی پرویزی و مهندس سینا رضاقلی زاده سودبرده‌ام که در اینجا زحمات بی‌دینغ‌شان تشکر می‌نمایم.

انجام بیچ‌کاری به‌ویژه تحصیل در دانشگاه بدون حمایت خانواده میسر نیست، از زحمات و کمک‌های مادرم، پدرم، همسر، برادران و خواهر بزرگوارم تشکر می‌کنم.

این تحقیق با حمایت مالی مرکز تحقیقات منجرات 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 نفوذ¹ (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 کاذب² 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 *Intrusion Detection Systems*

² *False positive*

فهرست مطالب

عنوان	صفحه
فهرست اشکال.....	ح
فهرست جداول.....	د
فصل ۱- کلیات پژوهش.....	۱
۱-۱- مقدمه.....	۱
۲-۱- تعریف مسئله.....	۲
۳-۱- اهمیت تحقیق.....	۲
۴-۱- فرضیه‌های پژوهش.....	۳
۵-۱- پرسشهای پژوهش.....	۴
۶-۱- اهداف پژوهش.....	۴
۷-۱- نوآوری پژوهش.....	۴
۸-۱- گام‌های روند پژوهش.....	۵
۹-۱- ساختار پژوهش.....	۷
فصل ۲- مفاهیم تشخیص نفوذ و سیستم‌های تشخیص ناهنجاری.....	۸
۱-۲- مقدمه ای بر تشخیص نفوذ.....	۸
۲-۲- تاریخچه تشخیص نفوذ.....	۹
۳-۲- انواع حملات با توجه به طریقه حمله.....	۱۰
۱-۳-۲- حملات از کار انداختن سرویس.....	۱۱
۲-۳-۲- حملات دسترسی به منابع شبکه.....	۱۱
۱-۲-۳-۲- حملات جهت دستیابی به داده.....	۱۱
۲-۲-۳-۲- حملات جهت دستیابی به سیستم.....	۱۱
۴-۲- سیستم‌های تشخیص نفوذ.....	۱۲
۵-۲- سیستم‌های تشخیص نفوذ بر اساس معماری منبع.....	۱۳
۱-۵-۲- سیستم‌های تشخیص نفوذ مبتنی بر میزبان (HIDS).....	۱۴

۱۵.....	مزایا و معایب HIDS	۱-۱-۵-۲
۱۶.....	سیستم‌های تشخیص نفوذ مبتنی بر شبکه (NIDS)	۲-۵-۲
۱۸.....	مزایا و معایب NIDS	۱-۲-۵-۲
۱۸.....	سیستم تشخیص نفوذ توزیع شده (DIDS)	۳-۵-۲
۱۹.....	مزایا و معایب DIDS	۱-۳-۵-۲
۱۹.....	روش‌های پاسخ به نفوذ	۶-۲
۲۰.....	پاسخ غیرفعال در سیستم تشخیص نفوذ	۱-۶-۲
۲۱.....	پاسخ فعال در سیستم تشخیص نفوذ	۲-۶-۲
۲۲.....	سیستم‌های تشخیص نفوذ بر اساس روش تشخیص	۷-۲
۲۳.....	تشخیص سوء رفتار	۱-۷-۲
۲۴.....	تشخیص رفتار ناهنجار	۲-۷-۲
۲۵.....	روش‌های تشخیص سوء استفاده	۸-۲
۲۵.....	الگوریتم ژنتیک (GA)	۱-۸-۲
۲۶.....	سیستم خبره	۲-۸-۲
۲۷.....	مدل پایه	۳-۸-۲
۲۷.....	آنالیز مرحله عبور	۴-۸-۲
۲۷.....	تطبیق الگوها	۵-۸-۲
۲۷.....	روش‌های تشخیص رفتار غیر عادی	۹-۲
۲۸.....	روش تحلیل آماری	۱-۹-۲
۲۹.....	روش یادگیری ماشین	۲-۹-۲
۳۰.....	شبکه‌های عصبی	۳-۹-۲
۳۰.....	داده کاوی	۴-۹-۲
۳۱.....	شبکه‌های بیزین	۱-۴-۹-۲
۳۱.....	ماشین‌های بردار پشتیبان (SVM):	۲-۴-۹-۲
۳۲.....	درخت تصمیم‌گیری	۳-۴-۹-۲
۳۲.....	مقایسه روند سیستم‌های IDS:	۱۰-۲
۳۴.....	نتیجه‌گیری	۱۱-۲

فصل ۳- بررسی رویکردهای سیستم ایمنی مصنوعی و ماشینهای بردار پشتیبان.....۳۵	
۳۵.....مقدمه	۱-۳-
۳۶.....انگیزه استفاده از روش دو مرحله ای در تشخیص ناهنجاری	۲-۳-
۳۹.....تشخیص ناهنجاری شبکه با رویکرد سیستم ایمنی مصنوعی	۳-۳-
۴۰.....بازبینی مختصری از سیستم ایمنی انسان	۱-۳-۳-
۴۴.....مدل سیستم ایمنی بدن مصنوعی برای تشخیص نفوذ	۲-۳-۳-
۴۶.....مدل تفکیک سیستم ایمنی مصنوعی خودی/غیر خودی	۳-۳-۳-
۴۸.....کاربرد سیستم ایمنی مصنوعی (AIS) در تشخیص ناهنجاری شبکه (NAD)	۴-۳-۳-
۴۸.....فاز آموزش در سیستم AD-AIS	۱-۴-۳-۳-
۴۹.....فاز تست در سیستم AD-AIS	۲-۴-۳-۳-
۵۰.....طبقه‌بندی فعالیت‌های ناهنجار در سیستم ترکیبی	۴-۳-
۵۱.....کاربرد سیستم مبتنی بر ماشین بردار پشتیبان برای طبقه بندی	۵-۳-
۵۲.....به دست آوردن ضرایب لاگرانژ	۲-۵-۳-
۵۲.....طبقه بندی با رویکرد SVM	۳-۵-۳-
۵۴.....ماشینهای بردار پشتیبان غیر خطی	۴-۵-۳-
۵۶.....ساخت جداکننده‌های خطی با استفاده از تابع کرنل	۵-۵-۳-
۵۸.....ماشین بردار پشتیبان چند کلاسی	۶-۵-۳-
۵۹.....نتیجه‌گیری	۶-۳-
فصل ۴- معماری پیشنهادی سیستم ترکیبی تشخیص ناهنجاری.....۶۱	
۶۱.....مقدمه	۱-۴-
۶۲.....فعالیت‌های زمان اجرای سیستم ترکیبی تشخیص ناهنجاری	۲-۴-
۶۳.....فرایند آموزش مؤلفه‌های سیستم تشخیص ناهنجاری ترکیبی	۱-۲-۴-
۶۴.....ساختار سیستم ایمنی مصنوعی برای تشخیص ناهنجاری	۳-۴-
۶۵.....سیستم ایمنی مصنوعی مبتنی بر الگوریتم انتخاب منفی	۱-۳-۴-
۶۷.....ارائه روش بهبود یافته سیستم ایمنی مصنوعی با استفاده از ژنتیک الگوریتم	۲-۳-۴-
۶۹.....معرفی تشخیص دهنده‌ها	۳-۳-۴-
۷۱.....قانون تطبیق تشخیص دهنده و آنتی ژن	۴-۳-۴-

۷۲.....	روش تولید تشخیص دهندهها	۵-۳-۴
۷۶.....	استخراج اطلاعات سطح بالاتر درباره ناهنجاریها با استفاده از بردار ماشین پشتیبان	۴-۴
۷۷.....	ساخت مدل طبقه‌بندی با استفاده از SVM	۱-۴-۴
۷۷.....	طبقه بندی با استفاده از توابع کرنل متفاوت در SVM	۵-۴
۷۷.....	طبقه بندی SVM با استفاده از تابع کرنل خطی	۱-۵-۴
۷۸.....	طبقه بندی SVM با استفاده از تابع کرنل چند جمله‌ای	۲-۵-۴
۷۹.....	طبقه بندی SVM با استفاده از تابع کرنل شعاعی	۳-۵-۴
۷۹.....	طبقه بندی SVM با استفاده از تابع تانژانت هذلولی	۴-۵-۴
۸۰.....	طبقه‌بندی حملات با استفاده از ماشینهای بردار پشتیبان چند کلاسی	۶-۴
۸۱.....	استخراج اطلاعات کلاس‌های طبقه بندی شده توسط SVM	۱-۶-۴
۸۳.....	مزایای استفاده از SVM برای طبقه بندی نوع حمله	۲-۶-۴
۸۴.....	فرآیند اجرای الگوریتم پیشنهادی تشخیص ناهنجاری به صورت مرحله به مرحله	۷-۴
۸۴.....	هدایت ترافیک شبکه به سیستم ورودی	۱-۷-۴
۸۵.....	کدگذاری بسته های شبکه	۲-۷-۴
۸۶.....	موتور تشخیص ناهنجاری	۳-۷-۴
۸۸.....	تولید تشخیص دهندههای جدید	۲-۳-۷-۴
۸۸.....	تطبیق دهنده تشخیص دهندهها با ارتباطات شبکه	۳-۳-۷-۴
۹۰.....	طبقه بندی حملات با استفاده از رویکرد SVM	۴-۷-۴
۹۰.....	نتیجه گیری	۸-۴
۹۱.....	فصل ۵- پیاده‌سازی معماری پیشنهادی و ارزیابی عملکرد آن	
۹۱.....	مقدمه	۱-۵
۹۲.....	پیاده سازی سیستم ترکیبی	۲-۵
۹۲.....	توصیف مجموعه داده	۳-۵
۹۴.....	خصوصیتهای مجموعه دادههای KDD CUP 99	۱-۳-۵
۹۶.....	مشکلات ذاتی در مجموعه دادهها	۲-۳-۵
۹۶.....	داده های تکراری در مجموعه دادههای KDD'99	۳-۳-۵
۹۷.....	کارایی سیستم تشخیص ناهنجاری ترکیبی	۴-۵

۹۷.....	کارایی مؤلفه سیستم ایمنی مصنوعی	۱-۴-۵
۱۰۳.....	کارایی طبقه بندی حملات تشخیص داده شده	۲-۴-۵
۱۰۴.....	عملکرد کلی سیستم	۳-۴-۵
۱۰۷.....	مقایسه عملکرد کلی سیستم با یک پژوهش مشابه	۵-۵
۱۰۹.....	نتیجه	۶-۵
۱۱۰.....	جمع بندی و نتیجه گیری	فصل ۶-۶
۱۱۰.....	مقدمه	۱-۶
۱۱۰.....	مروری بر فصول گذشته	۲-۶
۱۱۱.....	دستاورد های پژوهش	۳-۶
۱۱۲.....	سهام پژوهشی	۴-۶
۱۱۲.....	نقاط قوت و ضعف مدل پیشنهادی	۵-۶
۱۱۲.....	نقاط قوت	۱-۵-۶
۱۱۳.....	نقاط ضعف	۲-۵-۶
۱۱۳.....	پیشنهاد های برای ادامه این پژوهش	۶-۶
۱۱۴.....	نتیجه گیری	۷-۶
۱۱۵.....	پیوست	فصل ۷-۷
۱۱۵.....	پیوست الف: انواع حملات در شبکه های کامپیوتری	۱-۷
۱۱۶.....	حملات از نوع DoS	۱-۱-۷
۱۲۰.....	حملات از نوع Back door	۲-۱-۷
۱۲۳.....	پیوست ب: مجموعه داده iscX 2012	۲-۷

فهرست اشکال

عنوان	صفحه
شکل ۱-۲ سازماندهی عمومی یک سیستم تشخیص نفوذ.....	۱۲
شکل ۲-۲ خصوصیات سیستمهای تشخیص نفوذ.....	۱۳
شکل ۳-۲ معماری یک شبکه با سیستمهای تشخیص نفوذ مبتنی بر میزبان.....	۱۵
شکل ۴-۲ معماری یک شبکه با سیستمهای تشخیص نفوذ مبتنی بر شبکه.....	۱۷
شکل ۵-۲ معماری یک شبکه با سیستمهای تشخیص نفوذ توزیع شده.....	۱۹
شکل ۶-۲ نمودار تشخیص حملات بر اساس به روز بودن حملات و منابع مورد نیاز برای رویکردهای مختلف تشخیص نفوذ.....	۲۳
شکل ۱-۳ یک سیستم تشخیص نفوذ ترکیبی ناهنجاری با مؤلفه تولید کننده امضا.....	۳۷
شکل ۲-۳ سطوح مختلف بدن انسان که به صورت انتزاعی می‌توان در نظر گرفت.....	۴۱
شکل ۳-۳ الف- سلول B، آنتیبادی، اپیتوپ، پاراتوپ، ایدوتوپ و آنتیژن و نحوه تشخیص آنتیژن توسط آنتی بادی مشخص گردیده است ب- نحوه اتصال آنتیبادی به آنتیژن بیان گردیده است.....	۴۳
شکل ۴-۳ عملکرد تشخیص و نابود کردن آنتیژن‌ها توسط آنتی بادی‌ها و نگهداری دسته‌های از آنتی بادی‌های شناساگر به عنوان سلولهای حافظه.....	۴۴
شکل ۵-۳ استفاده از ضرایب لاگرانژ یک استراتژی برای پیدا کردن مینیمم یا ماکزیمم یک تابع.....	۵۲
شکل ۶-۳ نزدیک‌ترین داده‌های آموزشی به ابر صفحه‌های جدا کننده بردار پشتیبان نامیده میشوند.....	۵۳
شکل ۷-۳ یک مجموعه داده غیر قابل طبقه بندی به صورت خطی.....	۵۴
شکل ۸-۳ استفاده از توابع غیر خطی جهت نگاشت فضای ورودی به یک فضای بالاتر.....	۵۵
شکل ۹-۳ استفاده از توابع کرنل غیر خطی جهت ساخت جداکننده‌های خطی در فضای ویژگی.....	۵۸
شکل ۱-۴ بررسی اجمالی از فعالیتهای زمان اجرای سیستم تشخیص ناهنجاری ترکیبی.....	۶۳
شکل ۲-۴ دید کلی فرایند آموزش برای دو مؤلفه.....	۶۴
شکل ۳-۴ استفاده از الگوریتم ژنتیک در تولید آنتی بادی‌های حافظه.....	۶۸
شکل ۴-۴ دوره زندگی یک تشخیص دهنده.....	۷۶
شکل ۵-۴ طبقه بندی libsvm با استفاده از تابع کرنل خطی.....	۷۸
شکل ۶-۴ طبقه بندی libsvm با استفاده از تابع کرنل چند جمله‌ای.....	۷۸

- شکل ۷-۴ طبقه بندی libsvm با استفاده از تابع کرنل شعاعی ۷۹
- شکل ۸-۴ طبقه بندی libsvm با استفاده از تابع کرنل تانژانت هذلولی ۸۰
- شکل ۹-۴ طریقه هدایت ترافیک شبکه به سیستم ورودی و عملکرد مؤلفه‌های سیستم ۸۵
- شکل ۱۰-۴ ساختار کدگشایی پروتکل‌های شبکه در سیستم پیشنهادی ۸۶
- شکل ۱۱-۴ ساختار زیر سیستم‌های مؤلفه تشخیص ناهنجاری ۸۷
- شکل ۱۲-۴ الگوریتم تولید عامل‌های تشخیص دهنده جدید و طریقه جایگزینی آن‌ها با آنتی بادیه‌های حافظه ۸۸
- شکل ۱۳-۴ الگوریتم سیستم ایمنی مصنوعی در زمان اجرا ۸۹
- شکل ۱-۵ نرخ تشخیص ارتباط‌های نرمال توسط مؤلفه سیستم ایمنی مصنوعی بر اساس وزن‌های مختلف ضریب عمومیت ۱۰۰
- شکل ۲-۵ نرخ تشخیص ارتباط‌های حمله توسط مؤلفه سیستم ایمنی مصنوعی بر اساس وزن‌های مختلف ضریب عمومیت ۱۰۱
- شکل ۳-۵ نرخ تشخیص حملات به تفکیک نوع حمله توسط مؤلفه سیستم ایمنی مصنوعی ۱۰۲
- شکل ۴-۵ نمودار نرخ صحت طبقه‌بندی حملات با استفاده از مؤلفه SVM با تابع کرنل چند جمله‌ای ۱۰۴
- شکل ۵-۵ مقایسه روش پیشنهاد شده با دیگر روش‌های مشهور ۱۰۷
- شکل ۶-۵ مقایسه روش پیشنهاد شده با یک روش مشابه ۱۰۸

فهرست جداول

صفحه	عنوان
۷۱	جدول ۴-۱ دسته بندی پورت‌هایی که در سیستم پیشنهاد شده استفاده میشود.....
۸۳	جدول ۴-۲ تقسیم بندی حملات به ۴ دسته اصلی
۹۳	جدول ۵-۱ فراوانی ۱۰ درصد تصحیح شده داده های KDD Cup 1999
۹۳	جدول ۵-۲ فراوانی داده های آموزشی
۹۳	جدول ۵-۳ جدول فراوانی داده های تست
۹۷	جدول ۵-۴ آمار داده‌های تکراری در مجموعه داده‌های آموزشی KDD'99
۹۷	جدول ۵-۵ آمار داده‌های تکراری در مجموعه داده‌های تست KDD'99
۹۸	جدول ۵-۶ نرخ تشخیص مؤلفه سیستم ایمنی مصنوعی بر اساس وزنهای مختلف اهداف
۱۰۳	جدول ۵-۷ نرخ صحت طبقه بندی حملات با استفاده از مؤلفه SVM با تابع کرنل چند جمله ای به ازای درجه های مختلف
۱۰۵	جدول ۵-۸ مقایسه روش پیشنهاد شده با روشهای معروف
۱۰۸	جدول ۵-۹ مقایسه روش پیشنهاد شده با یک روش ترکیبی مبتنی بر AIS و SOM
۱۱۵	جدول ۷-۱ انواع حملات در شبکه‌های کامپیوتری
۱۱۸	جدول ۷-۲ متداولترین پورت های استفاده شده در حملات DoS
۱۲۳	جدول ۷-۳ خصوصیات مجموعه داده های iscx 2012

فصل اول

کلیات پژوهش

۱-۱- مقدمه

امروزه یکی از مهم‌ترین مکانیزم‌های ایجاد امنیت شبکه‌ها و سیستم‌های کامپیوتری، تشخیص و جلوگیری از نفوذ^۱ (IDP) 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^۲ (ASIC) و همچنین توسعه چشمگیری که در معماری‌های نوین در طراحی و تولید نرم‌افزارها ایجاد شده، امکان استفاده از IDS و 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 شبکه ها و سیستم های کامپیوتری شناخته می شود. سیستم تشخیص نفوذ یا همان IDS به سخت افزار، نرم افزار یا تلفیقی از هر دو اطلاق می گردد که وظیفه شناسایی تلاش هایی که برای نفوذ به شبکه صورت می گیرد و ایجاد اختلال احتمالی حملات را بر عهده دارد، که این سیستم می تواند یک شبکه ی محلی^۱ یا گسترده^۲ باشد. (Patcha and Park, 2007). لازم به ذکر است که IDS ها عموماً به گونه ای از پهنای باند شبکه استفاده می کنند که می تواند بدون تأثیر گذاشتن بر روی ترافیک و معماری شبکه به کار خود ادامه دهند. غالباً IDS ها در قبال مشاهده نفوذ فقط به یک هشدار و یا ثبت رویداد در یک فایل اکتفا می کنند و هیچ عملی جهت جلوگیری از نفوذ انجام نمی دهند. این خصیصه همان موضوعی است که قدرت تحلیل هوشمند ترافیک اطلاعات شبکه را ایجاد می کند. این ماهیت IDS را در جایگاهی مناسب جهت تشخیص موارد زیر قرار می دهد (Verwoerd and Hunt, 2002):

- حملات شناخته شده قدیمی از طریق امضاء^۳ آن ها
- تغییر در جهت و حجم ترافیک مدخل های 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 مهم تر چند ریختی^۵ و به روز شدن حملات و بد افزارها می باشد که نیازمند این است که سیستم های 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 گروه‌های 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^۱ 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).

۴-۱- فرضیه‌های پژوهش

فرضیه‌های اصلی این پژوهش عبارت است از:

الف) می‌توان با طراحی یک سامانه‌ی ترکیبی در سیستم‌های تشخیص نفوذ می‌توان علاوه داشتن مزایای سیستم‌های 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

۵-۱- پرسش‌های پژوهش

سوالاتی 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 می‌باشد؟
- 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 بخشید؟
- آیا ترکیب این دو روش ما را به مزایای هر دو رویکرد تشخیص نفوذ (تشخیص سوء رفتار و تشخیص ناهنجاری) می‌رساند؟
- تا چه اندازه معایب دو رویکرد در سیستم نهایی ما تأثیر می‌گذارد؟

۶-۱- 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 سیستم با یک سیستم طبقه بندی با استفاده از روش ماشین بردار پشتیبان بعضی از معایب سیستم‌های تشخیص ناهنجاری را حذف کنیم.

۷-۱- 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