

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشکده : فنی و مهندسی

پایان نامه کارشناسی ارشد رشته: مهندسی فناوری اطلاعات

گرایش: تکنولوژی اطلاعات و ارتباطات

عنوان پایان نامه:

ارائه روش همبستگی هشدار برای سیستم تشخیص نفوذ

با استفاده از سیستم خبره فازی

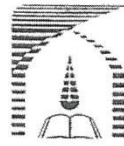
نام دانشجو:

زهرا اسدی

استاد راهنما:

دکتر علی یزدیان

آبان ۹۳



بسمه تعالی

تاییدیه اعضای هیات داوران حاضر در جلسه دفاع از پایان نامه

خانم زهرا اسدی پایان نامه ۶ واحدی خود را با عنوان همبستگی هشدار برای سیستم تشخیص نفوذ با استفاده از سیستم خبره فازی در تاریخ ۱۳۹۳/۸/۱۰ 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 محمدتقی حمیدی بهشتی	دانشیار	
استاد ناظر	دکتر حمید رضا اسکندری	استادیار	
استاد ناظر	دکتر محمد حسام تدین	استادیار	
مدیر گروه (یا نماینده گروه تخصصی)	دکتر حمید رضا اسکندری	استادیار	

این نسخه به عنوان نسخه نهایی پایان نامه ارساله مورد تایید است.
امضای استاد راهنما

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

مقدمه: با عنایت به سیاست‌های پژوهشی 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 هیات علمی، دانشجویان، دانش‌آموختگان و دیگر همکاران طرح، در مورد نتایج پژوهشهای علمی که تحت عناوین پایان‌نامه، رساله و طرحهای تحقیقاتی که با هماهنگی دانشگاه انجام شده است، موارد ذیل را رعایت نمایند:

ماده ۱- حقوق مادی و معنوی پایان‌نامه‌ها / رساله‌های مصوب دانشگاه متعلق به دانشگاه است و هرگونه بهره‌برداری از آن باید با ذکر نام دانشگاه و رعایت آیین‌نامه‌ها و دستورالعمل‌های مصوب دانشگاه باشد.

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 استاد راهنما مسئول مکاتبات مقاله 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 حاصل از نتایج پایان‌نامه / رساله و تمامی طرحهای تحقیقاتی دانشگاه باید با مجوز کتبی صادره از طریق حوزه پژوهشی دانشگاه و بر اساس آیین‌نامه‌های مصوب انجام می‌شود.

ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه 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 حوزه پژوهشی دانشگاه انجام گیرد.

ماده ۵- این دستورالعمل در ۵ ماده و یک تبصره در تاریخ ۱۳۸۴/۴/۲۵ در شورای پژوهشی دانشگاه به تصویب رسیده و از تاریخ تصویب لازم‌الاجرا است و هرگونه تخلف از مفاد این دستورالعمل، از طریق مراجع قانونی قابل پیگیری می‌شود.

نام و نام خانوادگی

امضاء

زهرا علی

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 / رساله دکتری نگارنده در رشته
سال در دانشکده
دانشگاه تربیت مدرس به راهنمایی سرکار خانم/جناب
آقای دکتر ، مشاوره سرکار خانم/جناب آقای دکتر
آقای دکتر 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 را به 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، تأمین نماید.

ماده ۶: اینجانب زهرا اری دانشجوی رشته ICT مقطع کارشناسی ارشد

تعهد فوق ضمانت اجرایی آن را قبول کرده، به آن ملتزم می شوم.

نام و نام خانوادگی: زهرا اری
تاریخ و امضا:

من به سرچشمه خورشیدنه خود بروم راه ذره‌ای بودم و مهر تو مرا بالا برد

پاس به پیشگاه حضرت دوست که هر چه داریم از اوست.

باشکر از زحمات بی دریغ استاد ارجمند، جناب آقای دکتر علی نیردیان که بارها سمانی‌های ارزشمند خود، همواره اینجانب را

یاری نمودند.

باشکر از پدر و مادر عزیزم، مهربان فرشتگانی که سخات ناب باور بودن، لذت و غرور دانستن، جسارت خواستن،

عظمت رسیدن و تمام تجربه‌های یکتا و زیبای زندگی ام، مدیون حضور سبز آن‌هاست.

باشکر از همسر عزیزم، که سایه مهربانی اش سایه ساز زندگی ام می‌باشد، و بی او این نوشتار رانه آغازی بود و نه پایانی

تقدیم به فرزند دل‌بندم آریتا، که با لبخندهای شیرینش، سختی راه را بر من هموار نمود و مشوق و مایه آرامش من گردید.

چکیده

سیستم‌های تشخیص نفوذ یکی از ابزارهای پرکاربرد در امنیت شبکه‌های کامپیوتری هستند. تعداد زیاد هشدارهایی که توسط سیستم‌های تشخیص نفوذ ایجاد می‌شوند، کاذب و تکراری بودن اکثر این هشدارها و عدم توانایی اپراتورهای امنیتی در تجزیه و تحلیل آن‌ها یکی از مشکلات اساسی سیستم‌های تشخیص نفوذ است. یکی از روش‌های مقابله با این مشکلات استفاده از روش‌های همبستگی هشدارهاست که به ما امکان می‌دهد هشدارهای کاذب و تکراری را از بین برده و اطلاعات مفید و سطح بالا را استخراج نماییم. در این پایان‌نامه ضمن بررسی روش‌های موجود برای همبسته سازی هشدارها به معماری‌ای خواهیم پرداخت که روش‌های مبتنی بر سیستم ایمنی مصنوعی را با سیستم خبره فازی ترکیب کرده تا بر اساس اولویت‌ها و دانش اپراتورهای امنیتی عمل نمایش و استدلال را انجام دهد. در ابتدا فرآیند همبسته سازی هشدارها شامل چندین مؤلفه ارائه شده است. در مدل پیشنهادی فرآیند نرمال سازی و پیش پردازش روی تمامی هشدارها اعمال می‌شود. پس از نرمال سازی، هشدارها نام و ساختار استاندارد دارند که توسط سیستم همبسته ساز شناخته می‌شود. سیستم‌های تشخیص نفوذ سپس هشدارهای خود را به روی یک سرور مرکزی فرستاده و آن‌ها را در پایگاه داده خود ذخیره می‌کنند. در مرحله بعد هشدارهای تکراری حذف می‌شوند. با استفاده از الگوریتم سیستم ایمنی مصنوعی و همچنین با بهبود تولید ابر هشدارها با استفاده از قوانین فازی هم نرخ تشخیص هشدارهای مربوط به حملات و هم نرخ خطای مثبت کاذب به حد قابل قبولی رسید. در نهایت نتایج استفاده توأم این دو مؤلفه را به دست آورده و با کارهای معتبر دیگر در این زمینه جهت اعتبار سنجی مدل نهایی مقایسه کردیم. مقایسه نشان‌دهنده مطلوبیت بالای میزان خطای مثبت کاذب و نتایج طبقه‌بندی حملات بوده است.

کلمات کلیدی: همبستگی هشدارها، تشخیص نفوذ، سیستم خبره فازی، سیستم ایمنی مصنوعی، مثبت کاذب

فهرست مطالب

صفحه	عنوان
۱	فصل ۱- کلیات تحقیق
۱	۱-۱- مقدمه
۲	۲-۱- بیان مسئله
۴	۱-۲-۱- اهمیت و ضرورت انجام تحقیق
۴	۲-۲-۱- اهداف تحقیق
۵	۳-۲-۱- وجه تمایز پژوهش با سایر پژوهش‌ها
۵	۳-۱- سؤالات و فرضیات پژوهش
۵	۱-۳-۱- بخش بندی تحقیق
۷	۲-۳-۱- ساختار پژوهش
۸	فصل ۲- ادبیات و پیشینه پژوهش
۸	۱-۲- مقدمه
۱۰	۱-۱-۲- گراف‌های حمله شبکه
۱۰	۲-۲- طبقه‌بندی حملات شبکه
۱۱	۱-۲-۲- حملات پویش پورت
۱۱	۲-۲-۲- حمله انکار سرویس
۱۳	۳-۲-۲- حمله راه دور به ماشین محلی
۱۴	۴-۲-۲- حمله کاربر به ریشه
۱۶	۳-۲- تاریخچه تشخیص نفوذ
۱۸	۴-۲- سیستم تشخیص نفوذ
۱۹	۱-۴-۲- سیستم‌های تشخیص نفوذ بر اساس معماری منبع

- ۲۰ ۱-۱-۴-۲ سیستم‌های تشخیص نفوذ مبتنی بر میزبان (HIDS)
- ۲۱ ۲-۱-۴-۲ سیستم‌های تشخیص نفوذ مبتنی بر شبکه (NIDS)
- ۲۳ ۳-۱-۴-۲ سیستم تشخیص نفوذ توزیع شده (DIDS)
- ۲۴ ۲-۴-۲ سیستم‌های تشخیص نفوذ بر اساس روش تشخیص
- ۲۵ ۱-۲-۴-۲ تشخیص ناهنجاری
- ۲۷ ۲-۲-۴-۲ تشخیص مبتنی بر امضاء
- ۲۸ ۵-نتیجه‌گیری
- ۲۹ فصل ۳-مروری بر همبسته سازی هشدارها
- ۲۹ ۱-۳-مقدمه
- ۳۰ ۲-۳-تاریخچه پیدایش و تکامل
- ۳۱ ۳-۳-هدف همبستگی هشدارها
- ۳۲ ۴-۳-رویکرد جامع به همبسته سازی هشدارها
- ۳۳ ۱-۴-۳-نرمال سازی
- ۳۴ ۲-۴-۳-تجمیع
- ۳۵ ۳-۴-۳-کاهش هشدارهای نادرست
- ۳۵ ۴-۴-۳-بازسازی ریسمان حمله
- ۳۵ ۵-۴-۳-بازسازی نشست حمله
- ۳۶ ۶-۴-۳-تشخیص تمرکز
- ۳۷ ۷-۴-۳-همبسته سازی چندمرحله‌ای
- ۳۷ ۸-۴-۳-تحلیل اثر
- ۳۸ ۹-۴-۳-اولویت بندی هشدارها
- ۳۸ ۵-۳-تکنیک‌های مورد استفاده همبسته سازی هشدار
- ۴۰ ۱-۵-۳-همبستگی علائم هشدار بر اساس شباهت مشخصه
- ۴۰ ۲-۵-۳-همبسته سازی مبتنی بر سناریو
- ۴۰ ۳-۵-۳-همبسته سازی مبتنی بر رابطه پیش شرط و نتیجه

۴۱ ۳-۵-۴-همبسته سازی مبتنی بر قانون
۴۱ ۳-۵-۵-همبسته سازی زمانی
۴۲ ۳-۵-۶-همبسته سازی آماری
۴۳ ۳-۵-۷-تکنیک‌های آماری و داده‌کاوی
۴۴ ۳-۶-ماتریس همبستگی علائم هشدار (ACM)
۴۸ ۳-۷-آشنایی با نظریه منطق فازی
۴۹ ۳-۸-نتیجه‌گیری
۵۰ فصل ۴-معماری پیشنهادی سیستم همبستگی هشدارها
۵۰ ۴-۱-مقدمه
۵۱ ۴-۲-معرفی مدل همبستگی پیشنهادی
۵۲ ۴-۲-۱-تجمیع
۵۲ ۴-۲-۲-نرمالسازی
۵۲ ۴-۲-۳-پیش‌پردازش هشدارها
۵۳ ۴-۲-۴-ادغام هشدارها
۵۴ ۴-۳-طبقه‌بندی هشدارها به کمک سیستم خبره فازی
۵۴ ۴-۴-الگوریتم فازی مورداستفاده در سیستم همبستگی هشدار پیشنهادشده
۵۷ ۴-۵-انتخاب ویژگی
۶۰ ۴-۶-قوانین فازی
۶۱ ۴-۷-چرخه زندگی ابر هشدارهای حافظه
۶۲ ۴-۷-۱-تطبیق‌دهنده جریان هشدارها با ابر هشدارها
۶۴ ۴-۸-نتیجه‌گیری
۶۵ فصل ۵-پیاده‌سازی معماری پیشنهادی
۶۵ ۵-۱-مقدمه
۶۶ ۵-۲-پیاده‌سازی سیستم همبستگی هشدار
۶۷ ۵-۳-توصیف مجموعه داده

۶۸KDD CUP 99	۱-۳-۵- خصوصیات مجموعه داده های
۷۰	۲-۳-۵- مشکلات ذاتی در مجموعه داده ها
۷۱ KDD'99	۳-۳-۵- داده های تکراری در مجموعه داده های
۷۲	۴-۵- کارایی سیستم همبسته سازی هشدارها
۷۳ AIS	۱-۴-۵- کارایی مؤلفه همبسته سازی با استفاده از قوانین فازی و کلاس بندی به روش
۷۷	۲-۴-۵- عملکرد کلی سیستم
۸۰	۵-۵- نتیجه
۸۲	۶- نتیجه گیری و پیشنهادها
۸۲	۱-۶- مقدمه
۸۲	۲-۶- مروری بر فصول گذشته
۸۴	۳-۶- دستاوردهای پژوهش
۸۴	۴-۶- سهم پژوهشی
۸۵	۵-۶- نقاط قوت و ضعف مدل پیشنهادی
۸۵	۱-۵-۶- نقاط قوت
۸۵	۲-۵-۶- نقاط ضعف
۸۶	۶-۶- پیشنهادهایی برای ادامه این پژوهش
۸۷	۷-۶- نتیجه گیری
۸۸	منابع

فهرست جداول

صفحه	عنوان
۱۱	جدول ۱-۲ خلاصه‌ای از حملات پویش پورت (Kendall, 1999)
۱۳	جدول ۲-۲ خلاصه‌ای از حملات انکار سرویس (Kendall, 1999)
۱۴	جدول ۳-۲ خلاصه‌ای از حملات راه دور به کاربر (Kendall, 1999)
۱۵	جدول ۴-۲ خلاصه‌ای از حملات کاربر به ریشه (Kendall, 1999)
۶۰	جدول ۱-۴ قوانین تعریف شده نمونه
۶۷	جدول ۱-۵ فراوانی ۱۰ درصد تصحیح شده داده‌های KDD Cup 1999
۶۷	جدول ۲-۵ فراوانی داده‌های آموزشی
۶۸	جدول ۳-۵ جدول فراوانی داده‌های آزمون
۷۲	جدول ۴-۵ آمار داده‌های تکراری در مجموعه داده‌های آموزشی KDD'99
۷۲	جدول ۵-۵ آمار داده‌های تکراری در مجموعه داده‌های آزمون KDD'99
۷۴	جدول ۶-۵ نرخ تشخیص مؤلفه تولید ابر هشدارها با استفاده از قوانین فازی و الگوریتم AIS بر اساس وزن‌های مختلف اهداف
۷۸	جدول ۷-۵ مقایسه روش پیشنهاد شده با روش‌های معروف

فهرست شکل ها

صفحه	عنوان
۶	شکل ۱-۱ فازهای انجام تحقیق
۷	شکل ۲-۱ ساختار پژوهش
۹	شکل ۱-۲ تجزیه و تحلیل آسیب پذیری یک شبکه (Sheyner, 2004 #140)
۱۹	شکل ۲-۲ خصوصیات سیستم های تشخیص نفوذ (Wu&Banzhaf, 2010)
	شکل ۳-۲ نمودار تشخیص حملات بر اساس به روز بودن حملات و منابع مورد نیاز برای رویکردهای
۲۵	مختلف تشخیص نفوذ (Kendall, 1999)
	شکل ۱-۳ مؤلفه های سیستم همبسته ساز با رویکرد جامع والیر و همکارانش (Valeur et al., 2004)
۳۳
۴۵	شکل ۲-۳ ماتریس همبستگی علائم هشدار
۵۲	شکل ۱-۴ معماری مدل همبستگی پیشنهادی
۵۶	شکل ۲-۴ معماری مؤلفه های سیستم طبقه بندی هشدار توسط سیستم فازی و AIS
۶۱	شکل ۳-۴ نمایش قوانین تعریف شده نمونه با استفاده از سیستم خبره فازی
۶۲	شکل ۴-۴ دوره زندگی یک ابر هشدار
۶۴	شکل ۵-۴ الگوریتم AIS در زمان اجرا
	شکل ۱-۵ نرخ تشخیص هشدارهای نامرتب توسط سیستم پیشنهادی بر اساس وزن های مختلف
۷۵	ضریب عمومیت
	شکل ۲-۵ نرخ تشخیص ارتباط های حمله توسط مؤلفه سیستم پیشنهادی بر اساس وزن های مختلف
۷۶	ضریب عمومیت
	شکل ۳-۵ نرخ تشخیص حملات به تفکیک نوع حمله توسط سیستم پیشنهادی بر اساس وزن های
۷۷	مختلف ضریب عمومیت
۸۰	شکل ۴-۵ مقایسه روش پیشنهاد شده با دیگر روش های مشهور

فصل اول

کلیات تحقیق

۱-۱- مقدمه

با روند رو به رشد استفاده از شبکه‌های کامپیوتری به‌خصوص اینترنت و مهارت رو به رشد کاربران و مهاجمان این شبکه‌ها و وجود نقاط آسیب‌پذیری مختلف در نرم‌افزارها، ایمن‌سازی سیستم‌ها و شبکه‌های کامپیوتری، نسبت به گذشته از اهمیت بیشتری برخوردار شده است. تأمین امنیت در هر سیستم یا شبکه کامپیوتری در واقع به معنای تأمین سه بعد اساسی محرمانگی، جامعیت و دسترس‌پذیری در آن است. (آذرکسب&قیداری، ۱۳۸۷)

سیستم‌های تشخیص نفوذ، بر اساس منبع تأمین‌کننده داده‌های ورودی به دودسته سیستم‌های مبتنی بر میزبان و سیستم‌های مبتنی بر شبکه تقسیم می‌گردند. بر اساس روش تحلیل و تشخیص نیز سیستم‌های تشخیص نفوذ به دودسته عمده سیستم‌های تشخیص مبتنی بر امضاء و سیستم‌های تشخیص ناهنجاری تقسیم می‌شوند. در سیستم‌های تشخیص مبتنی بر امضاء، تشخیص حمله بر اساس اطلاعات موجود از الگوهای حمله‌های شناخته‌شده صورت می‌پذیرد. درحالی‌که در سیستم‌های

تشخیص ناهنجاری ابتدا نمایه‌هایی از رفتارهای نرمال و هنجار (سیستم، شبکه و یا کاربران آن) تولید و سپس رفتارهای ناهنجار و مهاجمانه با تخطی و انحراف از این نمایه‌های نرمال تشخیص داده می‌شوند. (آذرکسب & قیداری، ۱۳۸۷)

۱-۲- بیان مسئله

تشخیص نفوذ^۱ روند نظارت بر حوادث رخ داده در یک سیستم کامپیوتری یا شبکه و تجزیه و تحلیل آن‌ها برای نشانه‌هایی از حوادث احتمالی منجر به نقض یا تهدید سیاست‌های امنیتی کامپیوتر است. مطالعه رفتار حمله، کار چالش‌برانگیزی است. زیرا مهاجمین^۲ معمولاً رفتار خود را تغییر می‌دهند تا قابل شناسایی نباشند. از آنجایی که آسیب‌پذیری‌ها، مرتباً در حال کشف و شناسایی هستند، حملات نیز از استراتژی‌های حمله جدید، استفاده می‌کنند. یکی از روش‌های مطالعه استراتژی‌های حمله، استخراج آن‌ها از طریق هشدارهایی است که توسط سیستم‌های تشخیص نفوذ تولید می‌شوند. (Zhu&Ghorbani, 2006b)

همه تکنیک‌های کشف نفوذ، نقاط قوت و ضعفی دارند. به عنوان مثال، کشف نفوذ مبتنی بر امضا، دارای نرخ مثبت کاذب^۳ پایین‌تری است، اما برای کشف حملات شناخته شده، مورد استفاده قرار می‌گیرد. کشف مبتنی بر ناهنجاری، می‌تواند حملات جدید را کشف کند، اما از نرخ بالای مثبت کاذب رنج می‌برد. علاوه بر این، تعریف رفتار نرمال یک سیستم نیز کار سختی است. سیستم‌های تشخیص نفوذ نمی‌توانند حملات چندمرحله‌ای را تشخیص دهند. برای مقابله با این مشکلات سیستم همبستگی هشدار^۴ پیشنهاد شده است. همبستگی هشدار فرایندی است که شامل چندین مؤلفه است و هدف این مؤلفه‌ها، آنالیز علائم هشدار و ارائه یک دید سطح بالا در مورد وضعیت امنیتی شبکه تحت نظارت است. (Zhu&Ghorbani, 2006b)

1 Intrusion Detection

2 Attacker

3 False Positive

4 Alert Correlation System

این بخش ، شامل تجزیه و تحلیل هشدارهای ایجاد شده توسط سیستم‌های کشف نفوذ و ابزارهای امنیتی دیگر، جهت کشف طرح‌های حمله، شناسایی هشدارهای کاذب و موارد دیگر است و به ما امکان می‌دهد تا هشدارهای تکراری و کاذب را از بین ببریم و آن‌ها را مطابق با اولویت‌ها و میزان خطر آفرینی فعالیت‌های شناسایی شده، اولویت بندی نماییم. (Tabia et al., 2011a)

یکی از کاربردهای مهم همبستگی هشدار، شناسایی استراتژی‌ها یا طرح‌های نفوذهای مختلف و درک هدف حملات است. اگر بتوانیم گام بعدی یا هدف نهایی یک مهاجم را با مطالعه الگوی رفتار نفوذگرانه شناسایی کنیم، در نتیجه می‌توانیم از افزایش حمله جلوگیری نموده و آسیب وارده به سیستم را به حداقل برسانیم. (Zhu&Ghorbani, 2006b)

روش‌های همبستگی هشدار، یا باعث کاهش تعداد هشدارهای صادر شده از طریق حذف هشدارهای تکراری و بی‌ربط می‌شوند و یا باعث کشف حملات چندمرحله‌ای می‌گردند (Tabia et al., 2011a)

آروموسو همبستگی هشدار را این‌گونه تعریف می‌کند: "به معنای واقعی کلمه همبستگی نفوذ تعریف شده است که تفسیر، ترکیب و تجزیه و تحلیل اطلاعات از تمام منابع در دسترس درباره فعالیت سیستم مقصد به منظور تشخیص نفوذ و پاسخ اشاره شده است." (Kabiri&Ghorbani, 2007)

حملات انکار سرویس یک سلاح برای اخاذی و خرابکاری است که موجب خساراتی در حد میلیون‌ها دلار به سایت‌های تجاری و دولتی شده‌اند. ترکیبی از نیروی حمله و ابزار حمله به‌عنوان سناریوی حمله^۱ تعریف می‌شود. روش‌های جاری مقابله با حملات انکار سرویس^۲ در پیشگیری از حملات، تشخیص و پاسخ متمرکز شده است. پیشگیری از حملات انکار سرویس شامل تکنیک‌هایی است که یکپارچگی میزبان‌ها را حفظ می‌کند و تکنیک‌هایی برای تشخیص و میزان محدودیت فعالیت

1 Attack Scenario

2 Denial of Service

شبکه غیرطبیعی است. تشخیص حمله به طور معمول بر اساس تکنیک‌هایی مانند تطبیق امضاء^۱ یا تشخیص ناهنجاری^۲ است. پاسخ به حملات انکار سرویس به طور معمول شامل فیلتر کردن بسته‌های حمله است. (Hussain et al., 2006)

تکنیک‌های هوش مصنوعی، محاسبات نرم و سیستم خبره فازی، روش‌های نوینی هستند که می‌توان در همبستگی بین علائم هشدار سیستم‌های تشخیص نفوذ از آن‌ها استفاده کرد. تکنیک‌های هوش مصنوعی ضریب اطمینان سیستم را بالا می‌برد و این توانایی را به سیستم می‌دهد که در مقابل رشد تقاضاها پاسخگو باشد. (Özyer et al., 2007)

۱-۲-۱ - اهمیت و ضرورت انجام تحقیق

یکی از مهم‌ترین چالش‌های پیش روی سیستم‌های تشخیص نفوذ تعداد زیاد هشدارهای تولیدشده است. مدیر سیستم با این هشدارها تحت الشعاع قرار خواهد گرفت هنگامی که او نمی‌تواند این هشدارها را استفاده و مدیریت کند. بهترین راه حل شناخته شده این است که هشدارهای سطح پایین، به یک حمله سطح بالاتر همبسته شوند و سپس یک هشدار سطح بالا از آن‌ها تولید شود. (Batani et al., 2013)

۱-۲-۲ - اهداف تحقیق

با توجه به مشکلات مطرح شده در بالا، هدف این تحقیق طراحی روشی جهت بالا بردن کیفیت اطلاعات هشدارها و ارائه گزارش‌های کامل مدیریتی به کارشناسان و مدیران امنیت شبکه می‌باشد تا از این طریق بتوان هشدارهای تکراری را تجمیع و همبسته نمود و با بررسی روابط بین حوادث و هشدارها، الگوها و یا استراتژی‌های حمله را استخراج کرد.

1 Signature matching

2 Anomaly detection

۱-۲-۳- وجه تمایز پژوهش با سایر پژوهش‌ها

با توجه به بررسی‌های انجام‌شده و مشکلات موجود در سیستم‌های تشخیص نفوذ، همبستگی هشدارها و ترکیب روش‌های مختلف در طراحی سیستم‌های تشخیص نفوذ کمک مؤثری در مدیریت زمان و بهبود کارایی سیستم‌های تشخیص نفوذ دارد. لذا در این تحقیق روشی بر اساس سیستم خبره فازی برای یادگیری درجه همبستگی بین هشدارها در تشخیص و استخراج سناریوی حمله ارائه می‌شود. در این روش سیستم پیشنهادی سعی در پیدا کردن همبستگی هشدارهای جدید با هشدارهای قبلی بر اساس قواعد فازی می‌نماید. در صورت عدم همبستگی قاعده جدیدی ارائه می‌گردد.

۱-۳-۳- سوالات و فرضیات پژوهش

- چه رفتارهایی به‌عنوان حمله شناخته می‌شوند؟
- راه‌های پیشگیری، تشخیص و پاسخ در برابر حملات چیست؟
- هوش مصنوعی شامل سیستم خبره فازی چگونه به تشخیص حملات کمک می‌کند؟
- همبستگی هشدارها به چه روش‌هایی قابل پیاده‌سازی است؟

۱-۳-۱- بخش بندی تحقیق

انجام تحقیق از ۳ فاز مطالعاتی، پیاده‌سازی و مستندسازی تشکیل خواهد شد. که در شکل ۱-۱ اقدامات هر فاز مشاهده می‌شود.

فاز پیاده سازی

- تحلیل نیاز مندی‌ها جهت پیاده سازی
- طراحی سیستم پیاده سازی
- تهیه ابزارهای پیاده سازی
- آغاز پیاده سازی (شبیه سازی شبکه، شبیه سازی سیستم همبستگی هشدار برای تشخیص حملات از جمله حملات انکار سرویس)
- آزمایش

- مطالعه سناریوهای حملات

- مطالعه روش های موجود برای تشخیص حملات
- مطالعه سیستم های تشخیص نفوذ و نقاط ضعف و قوت آنها
- مطالعه همبستگی هشدارها
- مطالعه روش های همبستگی هشدارها
- مطالعه تکنیک سیستم خبره فازی جهت تشخیص حملات

فاز مطالعاتی

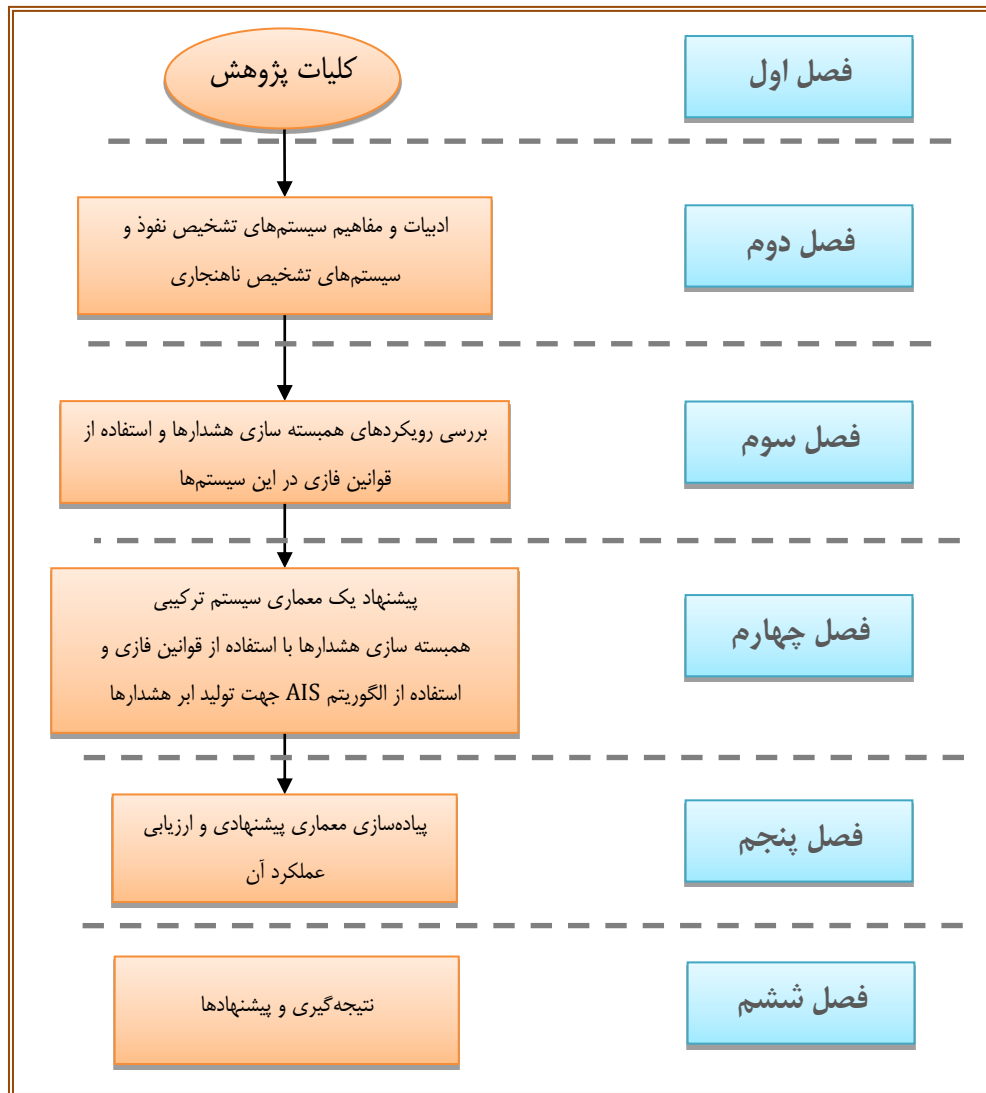
- مستندسازی فاز مطالعاتی
- مستندسازی فاز پیاده سازی و نتایج حاصل از آن

فاز مستندسازی

شکل ۱-۱ فازهای انجام تحقیق

۲-۳-۱- ساختار پژوهش

ساختار کلی پژوهش به صورت کلی در شکل ۲-۱ بیان شده است.



شکل ۲-۱ ساختار پژوهش