دانشگاه تربیت مدرس

دانشکده مهندسی برق و کامپیوتر

گروه کامپیوتر

پایان نامه کارشناسی ارشد کامپیوتر - معماری کامپیوتر

تشخیص رفتار غیرعادی در شبکه های VoIP مبتنی بر پروتکل های SIP/RTP

نگارش

محبوبه شاکری میاندره

استاد راهنما

دکتر سعید جلیلی

استاد مشاور

دکتر مهدی آبادی

پائیز ۱۳۹۱

دانشگاه تربیت مدرس
دانشکده مهندسی برق و کامپیوتر

بسمه تعالی

تاییدیه اعضای هیات داوران حاضر در جلسه دفاع از پایان نامه کارشناسی ارشد

خانم محبوبه شاکری میاندره پایان نامه ۶ واحدی خود را با عنوان **تشخیص رفتار غیر عادی در شبکه های VoIP مبتنی بر پروتکل های SIP/RTP** در تاریخ ۱۳۹۱/۸/۱۷ ارائه کردند.

اعضای هیات داوران نسخه نهایی این پایان نامه را از نظر فرم و محتوا تایید کرده، پذیرش آنرا برای اخذ درجه کارشناسی ارشد مهندسی کامپیوتر-معماری سیستمها پیشنهاد می کنند.

عضو هیات داوران	نام و نام خانوادگی	رتبه علمی	امضا
استاد راهنما	دکتر سعید جلیلی	دانشیار	
استاد مشاور	دکتر مهدی آبادی	استادیار	
استاد ناظر	دکتر بهزاد اکبری	استادیار	
استاد ناظر	دکتر رسول جلیلی	دانشیار	
مدیر گروه (یا نماینده گروه تخصصی)	دکتر بهزاد اکبری	استادیار	

دانشکده مهندسی برق و کامپیوتر

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/ رساله دکتری نگارنده در رشته مهندسی کامپیوتر است که در سال ۱۳۹۱ در دانشکده مهندسی برق و کامپیوتر دانشگاه تربیت مدرس به راهنمایی جناب آقای دکتر سعید جلیلی و مشاوره جناب آقای دکتر مهدی آبادی 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 محبوبه شاکری میاندره دانشجوی رشته مهندسی کامپیوتر-معماری سیستم‌ها مقطع کارشناسی ارشد تعهد فوق وضمانت اجرایی آن را قبول کرده، به آن ملتزم می شوم.

نام و نام خانوادگی: محبوبه شاکری میاندره

تاریخ و امضا: ۹۶

دانشکده مهندسی برق و کامپیوتر

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، دانش آموختگان 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 پایان نامه‌ها / 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 پایان نامه/ 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 دانش آموختگی 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 پایان نامه / رساله و تمامی طرحهای تحقیقاتی دانشگاه باید با مجوز کتبی صادره از طریق حوزه پژوهشی دانشگاه و بر اساس آئین نامه های 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 پایان نامه/ رساله و تمامی طرح‌های تحقیقاتی دانشگاه باید با هماهنگی اسناد 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 لازم الاجرا است و هرگونه تخلف از مفاد این دستورالعمل، از طریق مراجع قانونی قابل پیگیری می شود.

نام و نام خانوادگی: محمدرضا شاکری سعیدی

تاریخ و امضا:

تقدیم به

آنان که وجودم جز هدیه وجودشان نیست

پدر و مادر عزیزم

سپاس بی کران

پروردگار یکتا را که هستی مان بخشید

و به طریق علم و دانش رهنمونمان شد

و به همنشینی رهروان علم و دانش مفتخرمان نمود

و خوشه چینی از علم و معرفت را روزیمان ساخت.

و سپاس

او را که آموخت مرا تا بیاموزم

استاد گرامی جناب آقای دکتر سعید جلیلی

چکیده

امروزه فناوری انتقال صوت روی اینترنت (VoIP) به عنوان یک مولفه مهم و جایگزین کم هزینه برای شبکه‌های تلفنی سویچ عمومی (PSTN) در صنعت ارتباطات است. به تدریج با گسترش و محبوبیت سرویس‌های VoIP، امنیت در آن‌ها به یکی از مسائل مورد توجه محققان تبدیل شده است. روش‌های مختلفی برای تشخیص ناهنجاری در شبکه‌های VoIP پیشنهاد شده است که اغلب آن‌ها دارای محدودیت‌هایی هم‌چون نیاز داشتن به نمونه‌های ناهنجاری در مرحله یادگیری، ردیابی تنها یک زوج ویژگی مشخص برای تشخیص ناهنجاری و یا عدم به‌کارگیری یک رویکرد جامع برای شناسایی حملات مختلف VoIP می‌باشند. در این پژوهش، یک روش تشخیص ناهنجاری جامع بر روی شبکه‌های VoIP با استفاده از ماشین بردار پشتیبان تک کلاسی پیشنهاد می‌شود که از سه تابع هسته متفاوت به صورت موازی بهره می‌گیرد. در این روش چند پارامتر (هم‌چون پارامتر کنترل کننده خطا و پارامتر هسته) وجود دارد که به طور قابل ملاحظه‌ای بر روی دقت تشخیص ناهنجاری تاثیر گذاشته و نیازمند هستند که به درستی تنظیم شوند. برای این منظور روش پیشنهادی از مزیت‌های الگوریتم بهینه‌سازی انبوه ذرات برای تنظیم پارامترها بهره می‌گیرد. همچنین در این پژوهش، یک تابع برازندگی متناسب پیشنهاد می‌شود که هر دو مسایل بیش‌برازندگی و کم‌برازندگی را هنگام ارزیابی مقادیر کاندید شده برای پارامترها در نظر می‌گیرد. روش پیشنهادی از یک استراتژی وزن‌دهی مبتنی بر مکانیزم تشویق و تنبیه بهره می‌گیرد تا نتایج بدست آمده از توابع مختلف هسته را ترکیب کرده و با وزن‌دهی مناسب به آن‌ها، دقت روش پیشنهادی را برای تشخیص ناهنجاری‌های VoIP افزایش دهد. نتایج آزمایش‌های انجام شده برای ارزیابی کارآیی روش پیشنهادی نشان می‌دهند که این روش قادر است ناهنجاری‌های شبکه VoIP را با نرخ تشخیص بالا و نرخ هشدار نادرست پایین تشخیص دهد.

کلمات کلیدی- انتقال صوت روی اینترنت، تشخیص ناهنجاری، هم‌جوشی هسته‌های وزن‌دار، ماشین بردار پشتیبان تک‌کلاسی، بهینه‌سازی انبوه ذرات.

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

فهرست اختصارات

DBA2	Distribution-Based Artificial Anomaly
DoS	Denial of Service
DR	Detection Rate
FPR	False Positive Rate
OCSVM	One-Class Support Vector Machine
PSO	Particle Swarm Optimization
PSTN	Public Switched Telephone Network
RBF	Radial Basis Function
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SIP	Session Initiation Protocol
SPIT	SPam over Internet Telephony
SVM	Support Vector Machine
UAC	User Agent Client
UAS	User Agent Server
VoIP	Voice over IP

فصل اول:

کلیات

۱-۱- مقدمه

مهاجرت از شبکه تلفن سویچ عمومی[1] (PSTN) قدیمی به ارتباطات با استفاده از شبکه‌های مبتنی بر IP، باعث توسعه بسیار سریع کاربردها با ویژگی‌های پیچیده و در عین حال هزینه کم شده است. انتقال صوت روی IP[2] (VoIP) که با نام تلفن اینترنتی نیز شناخته می‌شود، یکی از این کاربردها است که اتصالات جهانی را با هزینه کم فراهم می‌کند. VoIP شکلی از ارتباط است که به کاربر اجازه می‌دهد تا تماس‌های تلفنی خود را بر روی پهنای باند گسترده اینترنت به‌جای خطوط تلفنی آنالوگ برقرار کند [۱]. شبکه VoIP برای برقراری چنین ارتباطی از اجزای مختلفی همچون پایانه‌ها، مدیر تماس، سرویس‌دهنده سیگنالینگ، سرویس‌دهنده رسانه، و عناصر مرزی نشست بهره می‌گیرد. برای این‌که محصولات سازندگان مختلف قادر باشند تا با یکدیگر ارتباط برقرار کنند، یک مجموعه از پروتکل‌های استاندارد صنعتی توسط سازمان‌هایی هم‌چون IETF، IEEE، 3GPP و ITU-T تعریف شده است. VoIP با استفاده از پروتکل‌های مختلف سیگنالینگ و رسانه پیاده‌سازی می‌شود. پروتکل‌های سیگنالینگ برای برقراری، نگهداری و خاتمه اتصال بین دو نقطه انتهایی به‌کار می‌رود. پروتکل‌های سیگنالینگ برای مذاکره نوع کدگذاری رسانه مورد استفاده برای تبدیل سیگنال‌های صدای آنالوگ به بسته‌های دیجیتالی به‌کار می‌روند. پروتکل‌های رسانه نیز برای انتقال محتوای واقعی بین نقاط انتهایی بر روی شبکه به‌کار می‌روند. به‌خاطر نیاز به بی‌درنگ بودن،

[1] Public Switched Telecommunication Network
[2] Voice over IP

پروتکل‌های رسانه اغلب از انتقال غیرقابل اطمینان (UDP)[1] در لایه انتقال استفاده می‌کنند. رایج‌ترین پروتکلی که برای انتفال جریان‌های بلادرنگ مورد استفاده قرار می‌گیرد، پروتکل انتقال بی‌درنگ[2] (RTP) است.

به‌طور سنتی، PSTN به عنوان یک شبکه مورد اعتماد در نظر گرفته می‌شود، زیرا یک شبکه بسته است. از طرفی هر سرویس یا برنامه کاربردی که از اینترنت استفاده می‌کند در معرض حملات عام اینترنت و دیگر انواع خاص برروی آن می‌باشد. در بیشتر مواقع حملات نوع دوم (یعنی حملات خاص آن سرویس)، از آسیب‌پذیری موجود در پیکربندی سرویس ارائه شده و یا پروتکل به‌کاررفته در آن، سوءاستفاده می‌کنند. در نتیجه، VoIP به جهت که بر بستر اینترنت پیاده‌سازی می‌شود و شامل پروتکل‌هایی است که به‌طور بالقوه آسیب‌پذیرند، در معرض تهدیدات زیادی قرار دارد. این تهدیدات را می‌توان به دو دسته تقسیم کرد: تهدیدات جلوگیری از سرویس (ناشی از ارسال سیل‌آسا، دستکاری بدنه پیام و دستکاری جریان پیام) و تهدیدات اجتماعی[3] (هم‌چون هرزتماس) است. اکثر حملات بر روی VoIP سعی بر نقض سرویس‌های امنیتی محرمانگی، صحت[4]، و دسترس‌پذیری[5] را دارند که به دلیل وجود آسیب‌پذیری‌های ناشی از عیوب طراحی، پیاده‌سازی، و پیکربندی می‌باشند.

۱-۲- مسأله تشخیص ناهنجاری در شبکه VoIP

از آن‌جا که شبکه‌های VoIP بر روی بستر باز اینترنت برپا شده و از حساسیت بالایی نسبت به تاخیر و کیفیت سرویس برخوردار هستند، مورد هدف حملات مختلفی قرار می‌گیرند. بنابراین، با گسترش و محبوبیت این شبکه‌ها، امنیت در آن به یکی از مهم‌ترین دغدغه‌ها تبدیل شده است. برای تشخیص حملات بر روی شبکه VoIP روش‌های مختلفی پیشنهاد شده است که می‌توان آن‌ها را به طور عمده به دو دسته تشخیص مبتنی بر امضاء و تشخیص مبتنی بر ناهنجاری تقسیم کرد.

[1] User Datagram Protocol
[2] Real-time Transport Protocol
[3] Social Threats
[4] Integrity
[5] Availability

در چند سال اخیر بسیاری از پژوهش‌های انجام شده برای تشخیص نفوذ به شبکه‌های VoIP به سمت رویکرد تشخیص ناهنجاری سوق پیدا کرده است. در روش‌های مبتنی بر تشخیص ناهنجاری، ابتدا یک نما[1] از رفتار هنجار پروتکل ایجاد می‌شود. سپس هر ترافیکی که از نمای ایجاد شده انحراف داشته باشد به عنوان ناهنجاری تشخیص داده می‌شود. مزیت این روش‌ها در شناسایی حملات ناشناخته به شبکه VoIP علاوه بر حملات شناخته شده است.

تاکنون اغلب روش‌های پیشنهادی برای تشخیص ناهنجاری‌ها در شبکه‌های VoIP، تنها بر روی یک پروتکل خاص اعمال شده و یا از ردیابی یک زوج ویژگی مشخص برای تشخیص ناهنجاری استفاده کرده‌اند. در این پژوهش برای حل این مشکلات یک روش جامع برای تشخیص ناهنجاری‌های VoIP ارائه می‌شود که با در نظر گرفتن رفتار پروتکل‌های SIP و RTP به ساخت یک مدل ترکیبی هنجار از شبکه می‌پردازد.

۱-۳- رویکردهای تشخیص

برای تشخیص حملات بر روی شبکه VoIP روش‌های مختلفی پیشنهاد شده است که می‌توان آن‌ها را به طور عمده به دو دسته تشخیص مبتنی بر الگو و تشخیص مبتنی بر ناهنجاری تقسیم کرد.

در روش‌های تشخیص مبتنی بر الگو رفتار ترافیکی شبکه VoIP با الگوهای حملات شناخته شده مقایسه و در صورت تطبیق، هشدار داده می‌شود. اگرچه این دسته از روش‌ها در شناسایی حملات شناخته شده مؤثر و کارآمد هستند، اما در شناسایی حملات جدیدی که الگوی آن‌ها ناشناخته است، با شکست مواجه می‌شوند. در سویی دیگر، روش‌های تشخیص ناهنجاری نمایی از رفتار هنجار و مورد انتظار شبکه VoIP ساخته و هرگونه رفتاری که به طور قابل ملاحظه از نمای ساخته شده انحراف داشته باشد را به عنوان رفتار ناهنجار تشخیص می‌دهند. مزیت این روش‌ها عدم نیاز به دانش قبلی از حملات مختلف قابل انجام بر روی شبکه‌های VoIP است. بنابراین، این روش‌ها قادرند تا حملات جدید را نیز شناسایی کنند.

از طرفی این روش‌ها می‌توانند بر اساس نوع کلاس حملاتی که مورد هدف قرار می‌دهند به چهار بخش روش‌های تشخیص حملات ارسال سیل‌آسا، روش‌های تشخیص ارسال پیام‌های بدخواهانه (حملات

[1] Profile

دستکاری بدنه پیام و حملات دستکاری جریان پیام)، روش‌های تشخیص حملات هرزتماس و روش‌های تشخیص چندین کلاس حمله تقسیم شوند.

۱-۴- اهداف پایان نامه

در این پژوهش روشی برای تشخیص ناهنجاری‌های شبکه VoIP پیشنهاد می‌شود. هدف این روش، تشخیص ناهنجاری‌ها در یک شبکه تحت نظارت است. این کار با استفاده از تحلیل غیر فعال ترافیک VoIP در شبکه تحت نظارت صورت می‌گیرد. روش پیشنهادی در این پژوهش به طور مشخص اهداف زیر را دنبال می‌کند:

- روش پیشنهادی با استفاده از یادگیری غیرنظارتی و بدون استفاده از نمونه‌های ناهنجاری مدل هنجار را از روی شبکه VoIP ساخته و با استفاده از آن ناهنجاری‌ها را شناسایی کند.
- روش پیشنهادی در ساخت نمای هنجار شبکه VoIP ، رفتار عادی هر دو پروتکل SIP و RTP را در بر گیرد، تا با یک رویکرد جامع ناهنجاری‌ها را در سطح هر دوی این پروتکل‌ها شناسایی کرده و حملات مختلف را تشخیص دهد.
- روش پیشنهادی از نرخ تشخیص بالا و نرخ هشدار نادرست پایینی برخوردار باشد.

۱-۵- نوآوری های پایان نامه

جنبه‌های نوآوری پژوهش حاضر در ادامه فهرست شده‌اند:

- استفاده از رویکرد ترکیبی که در آن الگوریتم ماشین بردار پشتیبان تک‌کلاسی با سه هسته مختلف که به صورت موازی اجرا می‌شود.
- ارائه یک تابع برازندگی مناسب که قادر است مقادیر پارامترهای الگوریتم ماشین بردار پشتیبان تک‌کلاسی را به خوبی ارزیابی کرده و با استفاده از آن بهترین مقادیر را تنظیم نمود.
- ارائه یک روش وزن‌دهی وفق‌پذیر که قادر است وزن هر هسته را با در نظر گرفتن دقت پیش‌بینی‌های قبلی‌اش با بهره‌گیری از سیاست تنبیه/تشویق تنظیم کرده و از آن برای ترکیب

نتایج آن‌ها بهره گیرد. این مسأله باعث می‌شود که بتوان از نقاط قوت هر هسته به صورت مجتمع استفاده نمود.

- پیاده‌سازی روش پیشنهادی بر روی یک شبکه VoIP شبیه‌سازی شده به این منظور که عملکرد آن در برابر تشخیص ناهنجاری‌های شبکه VoIP مورد ارزیابی قرار گیرد. نتایج آزمایش‌ها نشان می‌دهد که روش پیشنهادی قادر است تا ناهنجاری‌ها را با نرخ تشخیص ۹۸/۱ درصد و نرخ هشدار نادرست ۰/۸ درصد تشخیص دهد.

۱-۶- مروری بر فصول پایان‌نامه

در این فصل به کلیات پژوهش شامل مسأله تشخیص ناهنجاری شبکه VoIP، رویکردهای تشخیص، اهداف پایان‌نامه و جنبه‌های نوآوری آن پرداخته شد.

ادامه پژوهش پیش‌رو بدین صورت سازماندهی شده که در فصل دوم به بیان مفاهیم پایه پرداخته می‌شود. در این فصل ابتدا به معماری VoIP پرداخته شده و سپس پروتکل‌های آن معرفی می‌شود. در ادامه این فصل نیز نمونه‌ای از عملکرد ترکیبی پروتکل‌های SIP و RTP در شبکه VoIP بیان خواهد شد. انتهای این فصل به طبقه‌بندی حملات موجود در VoIP پزداخته می‌شود که هر یک به تفصیل مورد بررسی قرار خواهند گرفت. در فصل سوم نیز رویکردهای تشخیص نفوذ به شبکه VoIP بیان می‌شود و پس از دسته‌بندی روش‌های ارائه شده، مهم‌ترین آن‌ها با جزئیات بیان خواهد شد. فصل چهارم نیز به ارائه روش پیشنهادی اختصاص دارد. در این فصل، روش پیشنهادی برای تشخیص ناهنجاری‌های VoIP به تفصیل بیان شده و مراحل مختلف آن تشریح خواهد شد.

فصل پنجم به ارزیابی روش‌های پیشنهادی اختصاص دارد. بدین صورت که ابتدا مشخصات ترافیک و شبکه شبیه‌سازی شده مورد ارزیابی تشریح می‌شود. سپس نتایج آزمایش‌های مختلف انجام شده به همراه تحلیل آن‌ها ارائه می‌شود. در این آزمایش‌ها تاثیر پارامترهای مختلف بر روی روش پیشنهادی نشان داده می‌شود و تحلیلی از میزان حساسیت این روش نسبت به مقادیر مختلف پارامترها ارائه می‌شود. در انتهای این فصل، معیارهای مقایسه‌ای متناسب معرفی شده و روش‌های پیشنهادی با سایر روش‌ها مقایسه می‌شود.

در فصل ششم از تمامی مطالب ذکر شده در این پژوهش نتیجه‌گیری شده و در نهایت پژوهش‌های آتی برای توسعه روش پیشنهادی بیان می‌شود.