دانشگاه پیام نور مرکز شمیرانات

دانشکده فنی و مهندسی

پایان نامه برای دریافت مدرک کارشناسی ارشد

رشته مهندسی کامپیوتر

گروه مهندسی کامپیوتر و فناوری اطلاعات

# ارائه یک روش ترکیبی برای تشخیص حملات انکار سرویس توزیع شده (DDoS) با استفاده از روش های محاسباتی نرم

علی شریفی بروجردی

استاد راهنما:

دکتر سید سعید آیت

استاد مشاور:

دکتر مهدی باطنی

شهریورماه ۱۳۹۲

تاریخ: ...../...../.....

شماره: .....

بسمه تعالی

# صورتجلسه دفاع از پایان نامه دوره کارشناسی ارشد

جلسه دفاع از پایان نامه دوره کارشناسی ارشد

آقای **علی شریفی بروجردی**

دانشجوی رشته **مهندسی کامپیوتر** به شماره دانشجویی **۹۰۰۰۱۰۴۲۷**

تحت عنوان (( **ارائه یک روش ترکیبی برای تشخیص حملات انکار سرویس توزیع شده با استفاده از روش های محاسباتی نرم** ))

با حضور هیات داوران در روز چهارشنبه مورخ ۱۳۹۲/۶/۲۷ ساعت ۱۰ صبح در محل ساختمان ..... برگزار شد و هیات داوران پس از بررسی، پایان نامه مذکور را شایسته نمره به عدد ..... به حروف ..... با درجه ..... تشخیص داد.

| ردیف | نام و نام خانوادگی | هیات داوران | مرتبه دانشگاهی | دانشگاه / موسسه | امضاء |
|---|---|---|---|---|---|
| ۱ | | استاد راهنما | | | |
| ۲ | | استاد مشاور | | | |
| ۳ | | استاد داور | | | |
| ۴ | | نماینده تحصیلات تکمیلی | | | |

# گواهی اصالت، نشر و حقوق مادی و معنوی اثر

اینجانب **علی شریفی بروجردی** دانشجوی ورودی سال **۱۳۹۰** مقطع کارشناسی ارشد رشته **مهندسی کامپیوتر** گواهی می نمایم، چنانچه در پایان نامه خود از فکر، ایده و نوشته دیگری بهره گرفته‌ام با نقل قول مستقیم یا غیرمستقیم منبع و ماخذ آن را نیز در جای مناسب ذکر کرده ام. بدیهی است مسئولیت تمامی مطالبی که نقل‌قول دیگران نباشد بر عهده خویش می‌دانم و جوابگوی آن خواهم بود.

دانشجو تأیید می‌نماید که مطالب مندرج دراین پایان نامه نتیجه تحقیقات خودش می باشد و در صورت استفاده از نتایج دیگران مرجع آن را ذکر نموده است.

نام و نام خانوادگی دانشجو: **علی شریفی بروجردی**

تاریخ و امضاء:

اینجانب **علی شریفی بروجردی** دانشجوی ورودی سال **۱۳۹۰** مقطع کارشناسی ارشد رشته **مهندسی کامپیوتر** گواهی می‌نمایم، چنانچه براساس مطالب پایان‌نامه خود اقدام به انتشار مقاله، کتاب، و .... نمایم، ضمن مطلع نمودن استاد راهنما، با نظر ایشان نسبت به نشر مقاله، کتاب، و ... به صورت مشترک و با ذکر نام استاد راهنما مبادرت نمایم.

نام و نام خانوادگی دانشجو: **علی شریفی بروجردی**

تاریخ و امضاء:

(کلیه حقوق مادی مترتب از نتایج مطالعات، آزمایشات و نوآوری ناشی از تحقیق موضوع این پایان نامه متعلق به دانشگاه پیام نور می باشد.)

# تقدیم

به پدر، مادر و همسرم،

که آتش پرفروغ مهرشان، هماره، گرمابخش لحظه لحظه‌های زندگی‌ام بوده‌است

و

آنان که جان شیرینِ شان را در راه پاسداشت این مرز و بوم، دلاورانه بر کف نهادند.

# تشکر و قدردانی

سپاس خدای را که سخنوران، در ستودن او بمانند و شمارندگان، شمردن نعمت های او ندانند و کوشندگان، حق او را گزاردن نتوانند.

در این مهلت اندک، گاه آن است که از اساتید گرامی و ارجمند خویش، جناب آقای دکتر سید سعید آیت که در تمامی مراحل گردآوری این پایان‌نامه با دقت و ژرف نگری و دلسوزی، مرا از رهنمون‌های ارزشمند خود بهره‌مند ساختند و نیز استاد بزرگوار، جناب آقای دکتر مهدی باطنی که مشورت‌های سودمندشان چراغ راهم بود و همچنین جناب آقای دکتر محمد رضا حیدری نژاد که زحمت داوری این پایان نامه را بر عهده داشتند، صمیمانه سپاسگزاری نمایم.

# چکیده

با توسعه همه جانبه استفاده از شبکه های کامپیوتری، تهدیدات ناشی از اجرای حملات انکار سرویس توزیع شده در حال افزایش است به شکلی که این دسته از اختلالات به راحتی می توانند منابع ارتباطی و محاسباتی سیستم یا سیستم های قربانی را در مدت زمان کوتاهی از ارائه خدمت به کاربران قانونی خود باز دارند. در این تحقیق، مجموعه ای خلاقانه از تفکیک کننده های فازی–عصبی نوع سوگنو برای تشخیص حملات انکار سرویس توزیع شده ارائه گردیده است که برای تجمیع نتایج آن ها از روش Bagging استفاده می شود. دقت تشخیص و هشدارهای مثبت نادرست، مقیاس هایی هستند که در این تحقیق از آن ها برای تحلیل کارایی روش پیشنهادی بهره گرفته شده است. نتایج آزمایشات صورت پذیرفته بر روی زیر مجموعه ای بهینه و تصادفی از مجموعه داده NSL-KDD Dataset، نشان دهنده این امر می باشد که مجموعه طراحی شده از تفکیک کننده های پیشنهادی، طی فرآیند تشخیص حملات، به نرخ دقت بالاتری (٪۹۶) در مقایسه با سایر روش های پرکاربرد یادگیری ماشین دست یافته است. علاوه بر این، هشدارهای نادرست صادره توسط سیستم تشخیص نفوذ، با بکارگیری روش ارائه شده به شکل چشم گیری کاهش یافته است.



# واژگان کلیدی

حملات انکار سرویس توزیع شده، سیستم های استنتاج فازی–عصبی، بگینگ، مجموعه ی تفکیک کننده ها، هشدارهای مثبت نادرست، یادگیری ماشین، سیستم تشخیص نفوذ.

## فهرست مطالب

# فهرست جداول

# فهرست اشکال

## مقدمه

با افزایش روزافزون کاربرد شبکه های کامپیوتری به ویژه اینترنت به عنوان ابزارهای نوین ارتباط جمعی از سوی اقشار مختلف جامعه، تامین امنیت اطلاعات مبادله شده بر بستر این رسانه های نوظهور، از اهمیت ویژه ای برخوردار گردیده است. امروزه، ارتباطات درونی سیستم های کامپیوتری در این شبکه ها چنان گسترده و پیچیده شده است که درک کامل چگونگی عملکرد آن ها از حیطه توانایی های تکنیکی متخصص ترین افراد نیز خارج است. از سویی دیگر، بر توانایی های پردازشی کامپیوترهای شخصی روزبه روز افزوده می گردد و این در حالی است که امکان اتصال افراد غیرحرفه ای با سرعت بالا به اینترنت و شبکه های کامپیوتری به امری معمول مبدل گشته است. با وجود این که ارائه خدمات بر خط مالی و بانکی[1] موجبات تسهیل امور جاری زندگی مردم را فراهم می سازد، بر مخاطرات پیش روی مسئولین تامین امنیت این شبکه ها نیز، لحظه به لحظه افزوده می گردد. روزانه تریلیون ها دلار تراکنش مالی در سطح اینترنت صورت می پذیرد که بروز اختلال در این روند صدمات مالی و حیثیتی جبران ناپذیری بر شرکت های فعال در این حوزه وارد می سازد. امروزه، بیش از هر زمان دیگر، ارائه کنندگان خدمات سایبری در معرض حملات متعدد قرار دارند. در این فضای رقابتی و پر مخاطره تنها سازمان ها و موسساتی که بتوانند با ملحوظ نمودن تمهیدات امنیتی مناسب موجبات استمرار ارائه خدمات خود را در محیط مجازی فراهم نمایند، از مزایای بی شمار حضور در این عرصه پر منفعت بهره مند خواهند گردید.

هر فعالیت سایبری که با هدف تخریب و یا استفاده غیر قانونی از منابع موجود در یک سیستم و یا شبکه رایانه ای صورت می پذیرد، نفوذ[2] نامیده می شود. تقریباً تمامی سیستم های رایانه ای از آسیب پذیری های امنیتی[3] شناخته شده و ناشناخته رنج می برند. در عمل، تمامی افراد به مجموعه بزرگی از داده ها یا همان شبکه جهانی اینترنت متصل هستند که دستیابی به هر نوع اطلاعاتی را برای هر شخص و در هر جا مقدور می سازد. در این اثناء، وب سایت های متعددی ابزارها و دانش لازم

[1] On-line Financial and Banking Services
[2] Intrusion
[3] Security Vulnerabilities

برای ساماندهی حملات سایبری را در اختیار عموم قرار می دهند تا جایی که افرادی با سطح معلومات متوسط نیز می توانند با بهره گیری از آن ابزارها و اطلاعات، به ساماندهی و انجام حملات سایبری بپردازند. علاوه بر این، اینترنت به جهت غیر قابل پیش بینی بودن گسترش کاربرد آن از روز نخست، با تمرکز بر ملاحظات امنیتی طراحی نگردیده و دارای نواقص امنیتی متعددی است.

در این آشفتگی بزرگ، قابل درک است که یک کاربر نافرمان به راحتی و بدون هرگونه جلب توجه خواهد توانست فعالیت های مخرب و مخاطره آمیزی را در بستر اینترنت به انجام برساند. برای جبران کمبودهای امنیتی موجود در پروتکل های مورد استفاده در شکل گیری اینترنت، متخصصین امنیتی، ابزارهای امنیتی متعددی از جمله آنتی ویروس ها[1] و دیواره های آتش[2] را طراحی نموده اند که امروزه به شکل گسترده ای از سوی کاربران شبکه جهانی اینترنت مورد استفاده قرار می گیرند. در چنین شرایطی، ابزارهای منفعل امنیتی همچون دیواره های آتش، فاقد قابلیت مواجهه موثر با فعالیت های متعدد و متنوع این خرابکاران سایبری می باشند. اخیراً با هدف رفع نواقص ابزارهای امنیتی مورد اشاره، استفاده از نرم افزارهای گمراه کننده[3] که با شبیه سازی برخی از سرویس ها، مهاجمین را در دستیابی به منابع شبکه گمراه می سازند مورد توجه مسئولین امنیتی شبکه ها قرار گرفته است (مدیری و یزدان پرست، ۱۳۸۹).

بنا بر اهمیت موضوع در بسیاری از کشورها تیم های واکنش سریع با تحلیل روش های مختلف حمله به سیستم ها و شناسایی آسیب پذیری های موجود به مشکلات امنیتی پاسخ می دهند. چنین تیم هایی باید از مشکلات امنیتی مطرح در حوزه فناوری اطلاعات آگاهی داشته و با اطلاع رسانی و ارائه خدمات امنیتی، مشکلات را مرتفع نموده و خطرات را قبل از وقوع گسترده آن ها گوشزد نمایند (مدیری و شاه ولایتی، ۱۳۹۰).

سیستم های تشخیص نفوذ[4]، ابزارهای نظارتی موثری هستند که برای ممانعت از وقوع اقدامات خرابکارانه در یک شبکه کامپیوتری، به دیواره های امنیتی افزوده می شوند. این سیستم ها، ترافیک

[1] Anti-Viruses
[2] Firewalls
[3] Spoofing Softwares
[4] Intrusion Detection Systems (IDSs)

ورودی و خروجی یک شبکه را مورد نظارت مستمر قرار می دهند تا فعالیت های تهدیدکننده را از همتایان عادی و قانونی شان متمایز سازند. . علاوه بر آن، این سیستم ها باید توانایی تولید هشدارهای لازم را برای آگاه سازی مسئولین امنیتی شبکه از مخاطرات تهدید کننده محیط خود، دارا باشند. نسل اول این سیستم ها با استفاده از روش تحلیل متمرکز داده ها به تشخیص نفوذ می پرداختند که در حال حاضر شیوه ای آسیب پذیر قلمداد می گردد (خلج، ۱۳۸۱).

این روزها، سیستم های تشخیص نفوذ تجاری، از مجموعه ای از قوانین به نام الگوها[1] برای تشخیص حملاتی که یک شبکه و یا سیستم کامپیوتری را مورد حمله قرار می دهند، بهره می برند. این شیوه تشخیص حملات، در حال حاضر دقیق ترین شیوه تشخیص و در عین حال گریز پذیرترین شیوه برای اخلاگران حرفه ای می باشد زیرا مجموعه بزرگی از اقدامات خرابکارانه سایبری از دید این سیستم ها به علت وجود تفاوت های جزئی در الگوهای عملکرد آن ها با حملات شناخته شده، بی خطر قلمداد گردیده و اجازه عبور دریافت می دارند. علاوه بر این، حملاتی که از آسیب پذیری های امنیتی روز صفرِ[2] (اخیراً کشف شده) سیستم های ارتباطی، برای نفوذ استفاده می کنند نیز به سبب ناشناخته بودن الگوهای مورد استفاده آن ها برای سیستم های تشخیص نفوذ مبتنی بر الگو، قابلیت عبور از سیستم های امنیتی و رسیدن به اهداف خرابکارانه خود را به دست می آورند.

از این رو، لزوم ابداع شیوه هایی که به سیستم های تشخیص نفوذ، قابلیت فراگیری خودکار روش های تشخیص حملات ناشناخته را می دهند، مورد تاکید قرار دارد. تکنیک های یادگیری ماشین[3]، برای نجات متخصصین امنیتی از موقعیت بغرنج بیان شده، طراحی گردیده اند. یک سیستم تشخیص نفوذ بهینه، لزوماً باید توانایی تشخیص کلیه حملات شناخته شده و ناشناخته را بدون امکان وقوع نقص در عملکردش داشته باشد. در واقع، چنین سیستم تشخیص نفوذی، باید بطور همزمان علاوه بر عدم صدور مجوز برای عبور اخلالگران از دیواره های امنیتی شبکه، از صدور هشدارهای

[1] Signatures
[2] Zero Day Vulnerabilities
[3] Machine Learning

امنیتی نادرست در مواجهه با ترافیک عادی و قانونی شبکه خودداری نماید. چنین پیش نیازهایی موجب افزایش ظرافت و پیچیدگی عملکرد الگوریتم های یادگیری ماشین می گردد. در مقابل، سایر حوزه هایی که از مزایای الگوریتم های یادگیری ماشین بهره جسته اند، نیاز به چنین دقت خارق العاده ای در عملکرد این دسته از الگوریتم ها ندارند. لذا، تاکنون چنین ملاحظاتی مانع استفاده عملی از الگوریتم های یادگیری ماشین در محصولات تجاری مرتبط با تشخیص نفوذ در شبکه های کامپیوتری گردیده است. بر خلاف ملاحظات بیان شده، در سال های اخیر، متخصصان فعال در حوزه یادگیری ماشین، با ارائه مقالات و انجام پژوهش های متعدد در حوزه های امنیتی و تشخیص نفوذ، عملکردی در خور تحسین به نمایش گذاشته اند. مانع دیگری که در روند استفاده از الگوریتم های یادگیری ماشین در فرآیند تشخیص نفوذ خودنمایی می کند، فقدان مجموعه داده های علامت گذاری شده[1] است. تنها مجموعه داده علامت گذاری شده در این خصوص مجموعه داده KDD99 است که حاوی نسخه ای بهینه شده از مجموعه داده DARPA98 می باشد که در سال ۱۹۹۸ توسط آژانس پروژه های تحقیقاتی پیشرفته دفاعی[2] ایالات متحده تولید و در اختیار محققان قرار گرفته است. این در حالی است که قابلیت استناد مجموعه داده مورد اشاره از سوی محققین به شدت مورد تردید قرار دارد.

در مواجهه با چنین مشکلاتی، در سال های اخیر شیوه های نوینی از کاربرد الگوریتم های یادگیری ماشین در فرآیند تشخیص نفوذ معرفی گردیده اند که از آن جمله می توان به روش های بکارگیری مجموعه ای از تفکیک کننده ها[3] برای تشخیص حملات سایبری نام برد. در واقع روش های مجموعه ای، شیوه ای نسبتاً نوین از کاربرد ترکیبی الگوریتم های یادگیری ماشین در حوزه های متعدد علمی است که هدف نهایی آن بهره گیری از نقاط قوت هر یک از الگوریتم های بکار رفته در این ساختار با هدف ارتقاء عملکرد کلی مجموعه نهایی می باشد. علاوه بر این، روش مذکور در مواردی که مسائل پیش رو قابلیت تقسیم شدن به زیر مساله های متعدد را دارند نیز عملکرد مطلوبی خواهد داشت. در این موارد هر قسمت از مجموعه اصلی که از همکاری و تعامل یک یا چند

[1] Labeled Datasets
[2] Defense Advanced Research Projects Agency ( DARPA)
[3] Ensemble of Classifiers

الگوریتم یادگیری ماشین تشکیل گردیده است، مسولیت حل یکی از زیر مساله های مطروحه را خواهد داشت. مجموعه داده مورد استفاده در ارزیابی عملکرد روش های ارائه شده برای تشخیص حملات سایبری، دارای ۴۱ ویژگی متمایز می باشد که هر یک از این ویژگی ها نمایان کننده یکی از صفات مهم جریانی از داده ها[1] است که حملات سایبری در بستر آن صورت می پذیرد. در این تحقیق، تمرکز ما بر ارائه روشی بهینه برای تشخیص حملات انکار سرویس با استفاده از مجموعه های متعددی از ویژگی های قابل استفاده معطوف خواهد بود. کاربرد تعداد کمتری از ویژگی های تعریف شده برای اتصالات شبکه جهت پیاده سازی فرآیند تشخیص حملات، از زمان لازم برای پردازش این داده ها خواهد کاست و در مجموع امکان تشخیص سریع تر حملات سایبری را فراهم می آورد.

[1] Data flow

# فصل اول

# کلیات تحقیق

## ۱–۱ امنیت

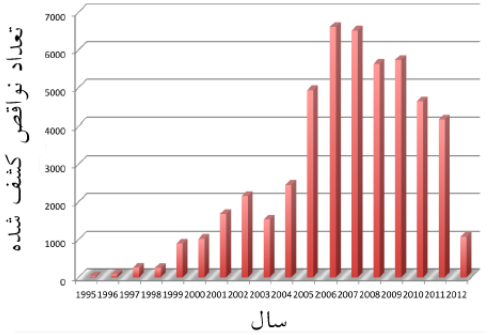
### ۱–۱–۱ سیستم های تشخیص نفوذ

از سیستم های تشخیص نفوذ، به عنوان ابزارهایی امنیتی- نظارتی، جهت تشخیص نفوذهای غیر قانونی به سیستم ها و شبکه های کامپیوتری استفاده می گردد. نفوذ، مجموعه ای غیر قانونی و مخرب از فعالیت هایی است که به شکل متوالی و مرتبط با هم و با هدف تسلط بر یک سیستم هدف صورت می پذیرد (کروگل[1] و همکاران، ۲۰۰۵). سیستم تشخیص نفوذ، ابزاری ضروری برای یک مسئول امنیت شبکه است چرا که بدون استفاده از آن، مسئول امنیت نخواهد توانست حجم وسیع اطلاعاتی را در هر ثانیه به شبکه وارد و یا از آن خارج می شوند کنترل کرده و مورد بررسی دقیق و موشکافانه قرار دهد. احتمال وقوع حملات در شبکه های کامپیوتری همیشگی است چرا که در ابزارهای اصلی موجود در شبکه ها (همچون مسیریاب ها، سوئیچ ها، کامپیوترهای میزبان) از نرم افزارهایی استفاده می گردد که همواره دارای نواقص متعدد ساختاری و امنیتی می باشند. بنابراین، راه حل بهینه برای پیشگیری از حملات سایبری، استفاده از نرم افزارهایی است که فاقد چنین نواقصی باشند. علاوه بر این با افزایش دانش عموم در رابطه با چگونگی عملکرد شبکه ها و نرم افزارهای متعدد، اخلالگران قادر خواهند بود به راحتی نواقص سیستم ها را شناسایی و از آن ها برای نفوذ به شبکه بهره برداری نمایند (مظلوم، ۱۳۸۱). متاسفانه، پیش بینی تمام راه های سوء استفاده موجود در یک نرم افزار از سوی توسعه دهندگان آن غیر ممکن خواهد بود. به علاوه، استفاده ناشیانه و نادرست از امکانات نرم افزاری از سوی توسعه دهندگان در فرآیند تولید نرم افزار، مانند آنچه در

[1] Kruegel

تعریف ساختار داخلی دستورات در زبان های سی و سی پلاس پلاس به وقوع پیوسته است و مشکل عمده ای بنام سرریز میانگیر[1] را به ارمغان آورده نیز غیر قابل اجتناب می نماید.

شکل ۱-۱ تعداد نواقص شناخته شده در نرم افزارها را بر اساس گزارش پایگاه داده نواقص ملی[2] ایالات متحده (NVD، ۲۰۱۳) در بازه زمانی سال های ۱۹۹۵ تا ۲۰۱۲ میلادی به تصویر می کشد. چنین حجمی از نواقص موجود در نرم افزارهای پرکاربرد کنونی را متخصصین حوزه امنیت شبکه وضعیتی انفجاری توصیف می نمایند که خود از عمق وخامت اوضاع خبر می دهد.




شکل ۱-۱ تعداد نواقص نرم افزاری کشف شده از سال ۱۹۹۵ تا ۲۰۱۲

علاوه بر این، ابزارهای متحرک[3] و محاسبات ابری[4] نیز در حال تبدیل شدن به کابوس بزرگ متخصصین امنیتی شبکه های کامپیوتری هستند. این در حالی است که نرم افزارهایی چون سیستم عامل Mac OS X که تا پیش از این بدون نقص و دارای ضریب امنیت بالا قلمداد می شده اند نیز به تازگی مورد حمله گسترده اخلالگران سایبری قرار گرفته اند. تمامی این موارد بر اهمیت ارتقاء جایگاه امنیت و ملاحظات امنیتی در روند تولید و توسعه نرم افزارها صحه می گذارند. امروزه، ارتقاء جایگاه سیستم های تشخیص نفوذ در کنار ابداع روش های نوین رمزنگاری و بهبود عملکرد دیواره های آتش، سه راهکار عمده بهبود شاخص های امنیتی شبکه های کامپیوتری قلمداد می گردند.

[1] Buffer Overflow
[2] National Vulnerabilities Database (NVD)
[3] Mobile Devices
[4] Cloud Computing