
بسم الله الرحمن الرحیم

دانشگاه شیخ بهایی

دانشکده مهندسی کامپیوتر

پایان‌نامه کارشناسی ارشد رشته مهندسی کامپیوتر – نرم افزار

تشخیص حمله توزیع شده منع سرویس در لایه کاربرد

پژوهشگر:

اسماعیل یلمه ها

استاد راهنما:

دکتر محمدرضا خیام باشی

شهریور ۱۳۹۳

شکر شایان نثار ایزد منان که توفیق را رفیق راهم ساخت تا این پایان‌نامه را به پایان برسانم و از استاد فاضل و اندیشمند جناب آقای **دکتر محمدرضا خیام باشی** که راهنمایی کم‌نظیر ایشان کمک این‌جانب بود و همواره لطف و محبت ایشان چراغ راه در پیمودن این مسیر بود، تقدیر و تشکر می‌نمایم.

تقدیم به

آقا **امام زمان (عج)** به امید آنکه روزی جهان با نهضت علمی‌اش، به عالی‌ترین مراتب نیکی برسد.

و تقدیم به پدر و مادر عزیزم که بی‌شک عزیزترین‌اند.

چکیده

دسترسی‌پذیری منابع در اینترنت از اهمیت ویژه‌ای برخوردار است. یکی از حملاتی که می تواند تهدیدی برای دسترسی پذیری منابع باشد، حملات منع سرویس است. این حملات شامل ارسال حجم زیادی از بسته‌ها به سمت سرویس‌دهنده قربانی است تا جایی که سرویس‌دهنده نتواند سرویس‌دهی مورد انتظار را به کاربران مجاز ارائه نماید. گونه‌ای از این حملات که به مشکل عمده‌ای تبدیل‌شده، حملات منع سرویس در لایه کاربرد است. وجه تمایز حملات منع سرویس در لایه کاربرد با دیگر حملات، استفاده حمله‌کنندگان از ارتباطات مجاز برای انجام حمله است.

در این پایان‌نامه با استفاده از نرخ درخواست‌ها و نرخ اطلاعات ردوبدل شده، روشی برای شناسایی حملات منع سرویس در لایه کاربرد ارائه شده است. در این روش برای تفکیک بهتر الگوهای موجود در این نرخ ها از الگوریتم امیدریاضی-بیشینه‌سازی استفاده‌شده است. با استفاده از این الگوریتم می‌توان خوشه هایی همپوشان را ایجاد نمود تا اشتراکات رفتاری کاربران و حمله‌کنندگان به گونه ای بهتر پوشش داده‌شود. از سوی دیگر برای انعطاف پذیرتر کردن استفاده از خوشه ها در برابر تغییرات موقتی ایجادشده در شبکه‌ها، از الگوریتم ژنتیک کمک گرفته شده‌است. پیاده سازی این روش و آزمایش آن بر روی مجموعه‌ی داده‌ای که از ترافیک یک وب سایت تحت حمله منع سرویس جمع آوری شده، انجام شده است و نتایج بهبودی نسبت به پژوهش قبلی که از مجموعه داده مشابه‌ی استفاده نموده را نشان می‌دهد.

لغات کلیدی: حمله توزیع شده منع سرویس، الگوریتم امید ریا ضی-بیشینه سازی، الگوریتم ژنتیک، دسترسی‌پذیری

فهرست مطالب

فهرست شکل‌ها

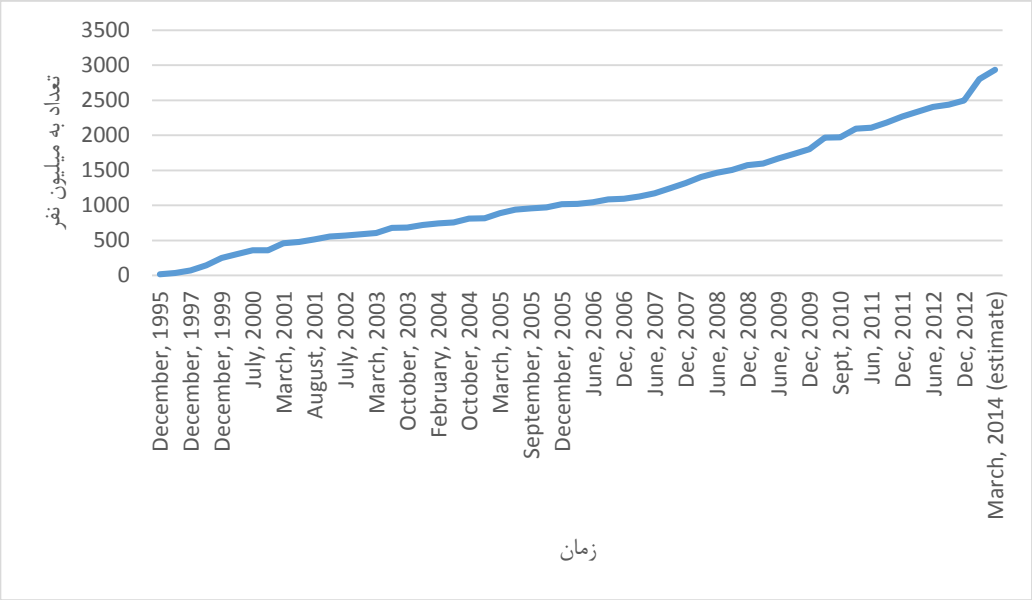
فهرست جداول

فصل ۱:

مقدمه

۱-۱ انگیزه تحقیق

اینترنت در عرصه‌های مختلف نقش به سزایی را ایفا می‌کند[۱-۴]. در یک دهه اخیر استفاده از منابع اینترنتی رشد پانصد درصدی داشته‌اند[۵]. شکل ۱- ۱ این روند گسترش را از سال ۱۹۹۵ تاکنون نشان می‌دهد؛ اما در کنار این پیشرفت‌ها، عامل‌های مخرب زیادی نیز در این محیط به وجود آمده و در حال فعالیت هستند. از همین روی نگاه به رویکردهای امنیتی از سه دیدگاهِ قابلیت اعتماد[۱]، جامعیت[۲] و دسترسی‌پذیری[۳] حائز اهمیت است. قابلیت اعتماد بیان‌کننده ارائه‌ی رویکردی برای دسترسی افراد مجاز به سیستم‌ها و داده‌ها است. جامعیت به مفهوم یکپارچگی داده‌ها و عدم تناقض در آن‌ها است و دسترسی‌پذیری، دسترسی به‌مجرد تقاضا را تشریح می‌کند[۶].



شکل ۱- ۱: *تعداد استفاده‌کنندگان از اینترنت [۵].*

[1] Confidentiality
[2] Integrity
[3] Availability

حملات منع سرویس[1] ازجمله خطرات تهدید کننده دستر سی‌پذیری می‌باشند که شکل پیشرفته‌تر این حملات در قالب توزیع‌شده[2] ظهور کرده است و با عنوان حملات DDoS شناخته می‌شوند. این حملات یکی از تهدیدهای مهم سرویس‌های اینترنتی به شمار می‌روند که باوجود پیشرفت‌های جاری، همچنان یکی از روش‌های پرقدرت برای مصرف منابع شبکه به شمار می‌آیند[۷]. سناریو حملات DDoS شامل ارسال بسته‌های ساختگی به‌سوی سیستم قربانی از چندین (هزاران یا صدها هزار) نقطه‌ی توزیع‌شده در اینترنت است افزایش این بسته‌ها باعث توقف جریان بسته‌های مجاز[3] از ترافیک یک شبکه می‌شود. در اغلب موارد سیستم‌های ارسال‌کننده نیز خود قربانی یک حمله قرارگرفته‌اند و با عنوان زامبی[4] شناخته می‌شوند. این حملات با ارسال ترافیک به گونه انفجاری[5] نیز ارتباط دارند که البته شناسایی و تمایز این دو وضعیت از یکدیگر بسیار سخت است[۸].

۱-۲ طرح مسئله

حملات منع سرویس به دودسته حملات لایه شبکه[6] و لایه کاربرد[7] تقسیم می‌شوند. در حملات لایه شبکه بسته های جعلی زیادی به سوی سرویس دهنده قربانی ارسال می شوند و معمولا حمله‌کنندگان از آدرس های IP[8] جعلی استفاده می نمایند. در حالی که حمله کنندگان در لایه کاربرد با استفاده از جریانی از درخواست‌های مجاز اقدام به حمله می نمایند. زامبی ها در این روش با استفاده از آدرس IP مجاز به ایجاد ارتباط می‌پردازند چرا که در غیراینصورت ارتباط TCP برقرار نخواهد شد. برخی از این حملات شامل درخواست برای تصاویر سنگین یا صفحاتی می باشد که ایجاد آنها نیازمند اجرای پرسوجوهای متعددی است[۱۰,۹]. این چنین

[1] Denial of Service (DoS) attacks
[2] Distributed Denial of Service (DDoS) attacks
[3] Legitimate packet
[4] Zombie
[5] Bursting traffic
[6] Network layer
[7] Application layer
[8] Internet protocol

درخواست‌هایی مشابه رفتار کاربران مجاز با سرویس دهنده می باشد. کاربران مجاز نیز اقدام به درخواست برای مشاهده ی صفحات، دریافت فایل ها و تصاویر را می نمایند. همین شباهت رفتاری در نوع درخواست های صادر شده برای سرویس دهنده، باعث سخت شدن تمایز کاربران عادی از حمله کنندگان می شود.

ا ستراتژی های مقابله با حملات DDoS در لایه کاربرد را می‌توان به فعال[1] و واکن شی[2] د سته‌بندی کرد. اســتراتژی فعال با زیر نظر قرار دادن ترافیک شــبکه، تلاش می‌کند قبل از این‌که حمله‌ای صــورت بگیرید با آن مقابله کند. درحالی‌که اســتراتژی واکنشــی پاســخ‌گویی را به زمان شــناســایی یک حمله انتقال می‌دهد تا میزان خسارات کاهش پیدا کند. درواقع چندین روش مقابله‌ای در این استراتژی، بر پایه‌ی حد آستانه[3] عمل می‌کنند و درصورتی‌که میزان ترافیک بر روی سیستم از حد آستانه عبور کند مکانیزم دفاعی شروع به کار می‌کند. هرچند استراتژی فعال یک استراتژی گران‌تر و پرهزینه‌تر، نسبت به استراتژی واکنشی است اما به‌هرحال وقتی حمله‌ای بزرگ اتفاق می‌افتد فوراً می‌تواند مشــکلات متعددی را برای قســمت‌های مختلف شــبکه بوجود آورد، قبل از این‌که رویکرد واکنشی حتی شانس پاسخ پیدا کند[۱۲,۱۱,۷].

اســـتفاده از هر یک از این موارد در مقابله با حملات DDoS، نیاز به تمایز دو وضـــعیت عادی و تحت حمله را در بطن خود دارد. عملیات دسته‌بندی دودویی[4]، داده‌ها را به دو کلاس دسته‌بندی می‌نماید. با توجه به ایجاد ارتباطات مجاز، انجام این دسته‌بندی در لایه کاربرد سخت تر است. در واقع باید بر رفتار کاربران متمرکز شد و الگوهایی که رفتار آنها را از کاربران مجاز متمایز می کند را شناسایی نمود و با استفاده از آنها به شناسایی حملات DDoS در لایه کاربرد پرداخت. البته موارد متعددی باعث اشـــتراک در الگوها و در هم تنیدگی رفتار کاربران مجاز و حمله کنندگان می گردد. از جمله آنها می توان به رفتار تصـــادفی و کاوشـــگرایانه کاربران در تعامل با یک وب ســایت را عنوان کرد که باعث شــباهت آن به یک حمله کننده با رفتار تصــادفی می‌شــود. از

[1] Proactive
[2] Reactive
[3] Threshold-based
[4] Binary Classification

سوی دیگر یک حمله کننده نیز می تواند با درخواست برای منابع پر استفاده (همچون بخش مطالب پر بازدید یک سایت) تلاش نماید که الگوی مصرف منابع خود را نزدیک به کاربران مجاز نماید.

۱-۳ اهداف

با توجه به افزایش خطرات و اهمیت توجه بیشتر به حملات DDoS در لایه کاربرد، این پایان نامه قصد دارد با استفاده از نرخ تبادل اطلاعات و نرخ درخواست های ارسال شده توسط کاربران به سرویس دهنده، به شناسایی این حملات بپردازد. برای نیل به این هدف نیاز به استفاده از یک الگوریتم مناسب برای تفکیک الگوهای موجود در این ویژگی ها برای تمایز بیشتر ترافیک حمله از ترافیک مجاز می باشد. یکی از این الگوریتم ها، الگوریتم امیدریاضی-بیشنه سازی[1] است.

به صورت مشخص این پایان نامه به دنبال پاسخ به این سوال است که: آیا با استفاده از الگوریتم امیدریاضی-بیشینه‌سازی بر روی ویژگی هایی همچون نرخ تبادل اطلاعات و نرخ درخواست ها، می توان با دقت بهتری ترافیک حمله را از ترافیک مجاز تفکیک کرد؟ دقت مناسب در اینجا با توجه به مقالاتی که در این زمینه انجام شده است، با رعایت اصول مقایسه، قابل تبیین است. البته باید توجه داشت که هر چه روش ارائه شده برای شناسایی حمله کنندگان نیاز به ذخیره اطلاعات بیشتری داشته باشد، می تواند نتایج بدتری را در پی داشته باشد چرا که ایجاد سربار بیشتر توسط روش مقابله، خود به مفهوم وجود یک عامل داخلی برای منع سرویس است.

۱-٤ ساختار پایان‌نامه

ساختار پایان‌نامه در فصول بعد بدین شرح است که فصل دوم به‌صورت ویژه به بررسی ابعاد مختلف امنیت به‌ویژه حملات منع سرویس پرداخته است. در این فصل برخی انواع حملات مورد بررسی قرارگرفته و حملات

[1] Expectation-Maximization (EM)

DDoS در لایه کاربرد تبیین شده است. فصل سوم با ارائه تحقیقات انجام شده در زمینه شناسایی و مقابله با این حملات، به برخی از ویژگی‌های استفاده شده برای این منظور پرداخته است.

فصل چهارم به شرح روش پیشنهادی این پایان نامه برای شناسایی حملات DDoS در لایه کاربرد پرداخته است و به طور مفصل جزئیات آن مورد بررسی قرار گرفته است. فصل پنجم، به بحث پیاده‌سازی و بررسی نتایج اختصاص داده‌شده است و نتایج کسب‌شده با مقاله ای در این زمینه مقایسه شده است. پس از این فصل نتیجه‌گیری کلی و پیشنهادها برای انجام کارهای آینده ارائه شده است که می‌توان از این پیشنهادها برای توسعه‌ی روش ارائه‌شده استفاده کرد.

فصل ۲:

امنیت اطلاعات و

حملاتDDoS در لایه کاربرد

۲-۱ مقدمه

استفاده‌کنندگان از اینترنت به‌منظور استفاده از دستاوردها و مزایای فن‌آوری اطلاعات و ارتباطات، ملزم به رعایت اصـولی خاص و اهتمام جدی به‌تمامی مؤلفه‌های تأثیرگذار در تداوم ارائه خدمات در یک سـیسـتم کامپیوتری می‌باشند. امنیت اطلاعات و ایمن سازی شبکه‌های کامپیوتری ازجمله این مؤلفه‌ها بوده که نمی‌توان آن را مختص یک فرد و یا سازمان در نظر گرفت.

در این فصـل به تشـریح برخی از انواع حملات و خطرات تهدیدکننده امنیت اطلاعات پرداخته می‌شـود پس‌ازآن حملات DDoS در لایه کاربرد با جزئیات بیشتری ارائه خواهد شد. بخش انتهایی این فصل به تشریح برخی از روش‌ها و الگوریتم‌های مورداسـتفاده در این پایان‌نامه برای شـناسـایی این‌گونه حملات اختصـاص داده‌شده است.

۲-۲ انواع حملات

تاکنون حملات متعددی متوجه شبکه‌های کامپیوتری بوده که می‌توان آنها را به سه گروه عمده تقسیم نمود:

- حملات شناسایی
- حملات دستیابی
- حملات منع سرویس

که در ادامه شرح مختصری از هر یک ارائه خواهد شد.

۲-۲-۱ حملات شناسایی

در این نوع حملات، مهاجمان اقدام به جمع‌آوری و شناسایی اطلاعات با هدف تخریب و آسیب رساندن به کاربران یا سیستم ها می‌نمایند. برای نیل به این منظور از نرم‌افزارهای پویشگر[1] برای شناسایی نقاط ضعف و آسیب‌پذیری آنها استفاده می شود. در این رابطه برخی تولیدکنندگان، نرم‌افزارهائی را با هدف کمک به مدیران شبکه‌ها طراحی و پیاده‌سازی نموده‌اند که متأسفانه از آنان در جهت اهداف مخرب نیز استفاده می‌شود. به‌عنوان نمونه، به‌منظور تشخیص و شناسایی رمزهای عبور، نرم‌افزارهای متعددی طراحی و پیاده سازی شده است. نرم‌افزارهای فوق باهدف کمک به مدیران شبکه، افراد و کاربرانی که رمز عبور خود را فراموش کرده و یا آگاهی از رمز عبور افرادی که سازمان خود را بدون اعلام رمز عبور ترک نموده‌اند، استفاده می‌گردند. به‌هرحال وجود این نوع نرم‌افزارها واقعیتی انکارناپذیر بوده که می‌تواند به‌منزله یک سلاح مخرب در اختیار مهاجمان قرار گیرد.

یک مهاجم با استقرار یک پویشگر در شبکه، قادر به جمع‌آوری و آنالیز تمامی ترافیک شبکه خواهد بود. اطلاعات مربوط به نام و رمز عبور عموماً به‌صورت متن معمولی و رمز نشده ارسال می‌گردد و این بدان معنی است که با آنالیز بسته‌های اطلاعاتی، امکان مشاهده این‌گونه اطلاعات حساس وجود خواهد داشت. شبکه های محلی که با استفاده از هاب[2] پیکر بندی شده اند می توانند هدف مناسبی برای این گونه حملات باشند. هاب بسته‌های ورودی را به تمام خروجی‌های خود ارسال می‌کند و این وظیفه‌ی دریافت‌کننده است که اگر آدرس مقصد با آدرس خودش یکسان نبود، از آن استفاده نکند. در این‌چنین شبکه‌ای با قرارگیری یک حمله‌کننده دریکی از این خروجی‌ها، تمام اطلاعات شبکه در معرض خطر قرار می گیرد. برخی از انواع این نرم افزار ها عبارتند از[۱۳]:

[1] Scanner
[2] Hub