





دانشگاه پیام نور

مرکز تهران

پایان نامه برای دریافت درجه کارشناسی ارشد

در رشته مهندسی کامپیوتر - نرم افزار

دانشکده فنی و مهندسی

گروه علمی مهندسی کامپیوتر و فناوری اطلاعات

عنوان پایان نامه:

ارائه یک روش مبتنی بر ناهنجاری جهت کشف حملات

DDoS

نگارش:

ریحانه کریم آزاد

استاد راهنما:

دکتر مقصود عباسپور

استاد مشاور:

دکتر احمد فراهی

بهمن ۱۳۹۰



جمهوری اسلامی ایران
وزارت علوم، تحقیقات و فناوری

مرکز شمیرانات



دانشگاه پیام نور

دانشگاه پیام نور استان تهران

تصویب نامه

پایان نامه کارشناسی ارشد رشته مهندسی کامپیوتر (نوم افزار)

تحت عنوان:

"ارائه یک روش مبتنی بر ناهنجاری جهت کشف حملات DDoS"

تاریخ دفاع: ۱۳۹۰/۱۱/۲۶ ساعت: ۱۳-۱۲

نمره:۱۹...
درجه ارزشیابی: ...بسیار عالی

هیات داوران:

امضاء	مرتبۀ علمی	نام و نام خانوادگی	داوران
		دکتر مقصود عباسپور	استاد راهنما
	استاد	دکتر احمد فراهی	استاد راهنمای همکار
		دکتر آرش قربان نیا دلاور	استاد داور
		دکتر محمد هادی معظم	نماینده گروه

تهران- بزرگراه ارتش-انتهای

بلوار شهید مژدی (اوشان)

خیابان شهید پیروز شفیعی

خیابان یاران-خیابان یاران دوم

دانشگاه پیام نور مرکز شمیرانات

تلفن: ۴-۲۲۱۹۵۳۰۳

دورنگار: ۲۲۴۸۴۸۳۴

www.shemiranat.tpu.ac.ir

shemiranat@tpu.ac.ir

گواهی اصالت نشر و حقوق مادی و معنوی اثر

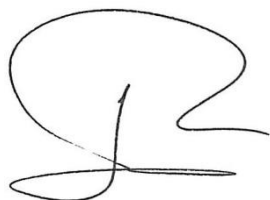
اینجانب ریحانه کریم آزاد دانشجوی ورودی سال ۱۳۸۶ مقطع کارشناسی ارشد رشته مهندسی کامپیوتر گرایش نرم افزار گواهی می‌نمایم چنانچه در پایان نامه‌ی خود از فکر، ایده و نوشته دیگری بهره گرفته‌ام با نقل قول مستقیم یا غیر مستقیم، منبع و ماخذ آن را نیز در جای مناسب ذکر کرده‌ام. بدیهی است مسئولیت تمامی مطالبی که نقل قول دیگران نباشد؛ برعهده خویش می‌دانم و جوابگوی آن خواهم بود.

دانشجو تایید می‌نماید که مطالب مندرج در این پایان نامه، نتیجه تحقیقات خودش می‌باشد و در صورت استفاده از نتایج دیگران، مراجع آن را ذکر نموده است.

ریحانه کریم آزاد

نام و نام خانوادگی دانشجو:

تاریخ و امضاء: ۱۳۹۰/۱۱/۲۶

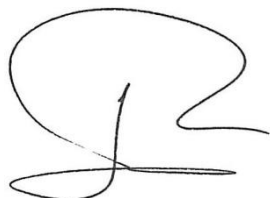


اینجانب ریحانه کریم آزاد دانشجوی ورودی سال ۱۳۸۶ مقطع کارشناسی ارشد رشته مهندسی کامپیوتر گرایش نرم افزار گواهی می‌نمایم چنانچه براساس مطالب پایان نامه‌ی خود، اقدام به انتشار مقاله، کتاب و ... به صورت مشترک و با ذکر نام استاد راهنما مبادرت نمایم.

ریحانه کریم آزاد

نام و نام خانوادگی دانشجو:

تاریخ و امضاء: ۱۳۹۰/۱۱/۲۶



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

بهمن ۱۳۹۰

تقدیم به :

مادر دلسوز و همسر مهربانم

تشکر و قدردانی

سپاس و ستایش خداوند را که به من توفیق داد که به یاری و مدد او این پایان نامه را به پایان رسانم.

بر خود واجب می دانم که:

از استاد راهنمای بزرگوام جناب آقای دکتر عباسپور که با دانش خود همواره مرا در تکمیل این پژوهش راهنمایی کردند،

از استاد مشاور ارجمندم جناب آقای دکتر فراهی که در طول انجام مراحل این پایان نامه با آگاهی و دقت نظر خاص راهنمایی های ارزشمندشان را از من دریغ نمودند،

از خانواده عزیزم، به ویژه برادر مهربانم که همواره یاور و پشتیبان من بوده اند،
و از تمام کسانی که در طول دوران تحصیل با راهنمایی های ارزشمند علمی و معنوی خود، مرا یاری نمودند سپاس گذاری نموده و از خداوند برای این عزیزان آرزوی توفیق و سربلندی می نمایم.

ریحانه کریم آزاد

چکیده

حملات DDoS یکی از مهم‌ترین تهدیدات برای در دسترس بودن سرویس‌های اینترنت برای کاربران می‌باشد. در این نوع از حملات، مهاجم با استفاده از میلیون‌ها عامل تعداد بسیار زیادی بسته ایجاد کرده و به سیستم قربانی ارسال می‌کند و به این ترتیب تمام منابع محاسباتی و ارتباطی سیستم قربانی را در مدت زمان بسیار کوتاهی مصرف می‌کند. با این کار سیستم قربانی قادر به پاسخگویی به کاربران قانونی خود نخواهد بود. روش‌هایی که برای کشف حملات DDoS وجود دارند به دو دسته روش‌های مبتنی بر امضاء و روش‌های مبتنی بر ناهنجاری تقسیم می‌شوند. در روش‌های مبتنی بر امضاء از الگوهای مشخصی که برای انواع مختلف حملات وجود دارند برای شناسایی حمله استفاده می‌شود. بنابراین مهم‌ترین اشکال این گروه از روش‌ها این است که قادر به شناسایی حملات جدید نمی‌باشند. به این دلیل که الگوی آن‌ها در سیستم موجود نیست. در روش‌های مبتنی بر ناهنجاری از مقایسه رفتار ترافیک شبکه با رفتار نرمال برای تشخیص حمله استفاده می‌شود. بنابراین این روش‌ها نیازی به دانستن الگوی حملات نداشته و قادر به شناسایی حملات جدید نیز می‌باشند. سیستم‌های مختلفی برای کشف حملات DDoS پیشنهاد شده‌اند که از روش‌های متفاوتی برای آنالیز بسته‌های ورودی به شبکه استفاده می‌کنند. برخی از این روش‌ها شامل الگوریتم‌های یادگیری ماشین و سیستم‌های خبره می‌باشند. در این تحقیق روشی برای کشف حملات DDoS پیشنهاد نموده‌ایم که از بررسی ناهنجاری‌های ایجاد شده در ترافیک شبکه در زمان حمله برای شناسایی حملات استفاده می‌کند. سیستم پیشنهادی با بررسی ترافیک ورودی به شبکه، تعدادی ویژگی، که از شباهت‌های رفتاری بسته‌های حمله بدست آمده، را محاسبه کرده و سپس با کمک رابطه بدست آمده بین این ویژگی‌ها با استفاده از روش ابرصفحه و همچنین روش شبکه‌های عصبی RBF، حملات DDoS را کشف می‌کند. برای ارزیابی سیستم پیشنهادی از شاخص‌های False Positive، False Negative، True Positive و True Negative و همچنین میزان دقت روش پیشنهادی در کشف حملات DDoS استفاده می‌شود. در این تحقیق از پایگاه داده‌های UCLA و DARPA و همچنین شبکه شبیه‌سازی شده با استفاده از ابزارهای Trino و TFN2K برای ارزیابی سیستم پیشنهادی استفاده شده است. در مرحله نهایی سیستم پیشنهادی با سیستم‌های (Oke & Loukas, 2007) و (Lee et al., 2008) مقایسه می‌شود.

کلمات کلیدی

حملات DDoS، روش‌های کشف حملات مبتنی بر ناهنجاری، شبکه‌های عصبی RBF، امنیت شبکه، ابرصفحه

فهرست مطالب

۱	مقدمه	۱
۲	۱-۱ مقدمه	۲
۳	۲-۱ تعریف مسئله و سئوالات اصلی تحقیق	۳
۴	۳-۱ سابقه و ضرورت انجام تحقیق	۴
۵	۴-۱ فرضیه‌ها	۵
۶	۵-۱ اهداف تحقیق	۶
۶	۶-۱ نوآوری تحقیق	۶
۶	۷-۱ روش تحقیق	۶
۷	۸-۱ مراحل انجام تحقیق	۷
۷	۹-۱ ساختار پایان نامه	۷
۹	۲ بررسی حملات DDoS	۹
۱۰	۱-۲ مقدمه	۱۰
۱۱	۲-۲ ساختار توزیع شده حملات DDoS	۱۱
۱۴	۳-۲ روش‌های حملات DDoS	۱۴
۱۴	۱-۳-۲ روش‌های مبتنی بر نفوذپذیری‌های نرم‌افزار	۱۴
۱۵	۲-۳-۲ روش‌های مبتنی بر مصرف منابع	۱۵
۱۶	۴-۲ جعل IP	۱۶
۱۷	۵-۲ انواع حملات DDoS مبتنی بر سیلاب	۱۷
۲۰	۱-۵-۲ حمله Smurf	۲۰
۲۱	۲-۵-۲ حمله TCP SYN مبتنی بر سیلاب	۲۱
۲۳	۳-۵-۲ حمله DNS Amplification	۲۳
۲۵	۶-۲ ابزارهای حمله DDoS	۲۵
۲۶	۱-۶-۲ ابزارهای حملات DDoS مبتنی بر عامل	۲۶

۲۸	ابزارهای حملات DDoS مبتنی بر IRC	۲-۶-۲
۲۹	نتیجه‌گیری	۷-۲
۳۰	بررسی سیستم‌های کشف حملات DDoS	۳
۳۱	مقدمه	۱-۳
۳۲	کشف حملات DDoS بر اساس روش کشف	۲-۳
۳۲	روش‌های کشف مبتنی بر امضاء	۳-۳
۳۴	روش‌های کشف مبتنی بر ناهنجاری	۴-۳
۳۶	کشف حملات DDoS با استفاده از روش‌های مبتنی بر ویژگی‌های IP	۱-۴-۳
۳۷	کشف حملات DDoS با استفاده از روش‌های یادگیری ماشین	۲-۴-۳
۳۹	بررسی روش ارائه شده در سیستم MLDRNN	۱-۲-۴-۳
۳۹	بررسی روش ارائه شده در سیستم DMCA	۲-۲-۴-۳
۴۱	سیستم‌های کشف حملات DDoS بر اساس محل قرارگیری	۵-۳
۴۲	نتیجه‌گیری	۶-۳
۴۴	سیستم پیشنهادی برای کشف حملات DDoS	۴
۴۵	مقدمه	۱-۴
۴۶	مفاهیم پایه	۲-۴
۴۶	شبکه‌های عصبی RBF	۱-۲-۴
۴۸	ابرفحه	۲-۲-۴
۴۸	واریانس، آنتروپی و انحراف مطلق میانه	۳-۲-۴
۵۰	معماری سیستم پیشنهادی	۳-۴
۵۱	ماژول Packet Capturing	۱-۳-۴
۵۱	ماژول DDoS Detection	۲-۳-۴
۵۲	ماژول Filtering	۳-۳-۴
۵۳	ماژول Attack Notification	۴-۳-۴
۵۴	ماژول DDoS Detection	۴-۴

۵۴	Feature Extraction	ماژول	۱-۴-۴
۵۷	Correlation Engine	ماژول	۲-۴-۴
۵۹	DDoS	کشف حملات	۵-۴
۶۰		محل فرارگیری شبکه در سیستم	۶-۴
۶۱		نتیجه‌گیری	۷-۴
۶۲	پیااده‌سازی و ارزیابی سیستم پیشنهادی		۵
۶۳		مقدمه	۱-۵
۶۴		پیااده‌سازی سیستم پیشنهادی	۲-۵
۶۴	Feature Extraction	ماژول	۱-۲-۵
۶۷	RBF	پیااده‌سازی شبکه‌های عصبی	۲-۲-۵
۶۸		پیااده‌سازی ابرصفحه	۳-۲-۵
۶۹		ارزیابی سیستم پیشنهادی	۳-۵
۷۰	UCLA	پایگاه داده	۱-۳-۵
۷۱	DARPA	پایگاه داده	۲-۳-۵
۷۲		ساختار شبکه شبیه‌سازی شده	۳-۳-۵
۷۳		معیارهای ارزیابی	۴-۳-۵
۷۵		ارزیابی کارایی سیستم پیشنهادی	۵-۳-۵
۷۵	RBF	ارزیابی سیستم پیشنهادی با استفاده از شبکه‌های عصبی	۱-۵-۳-۵
۷۷		ارزیابی رابطه بدست آمده با استفاده از ابرصفحه	۲-۵-۳-۵
۷۸	RBF	ارزیابی رابطه بدست آمده با استفاده از ابرصفحه و شبکه‌های عصبی	۳-۵-۳-۵
۸۳	DMCA و MLDRNN	مقایسه کارایی سیستم پیشنهادی با سیستم‌های	۶-۳-۵
۸۶		نتیجه‌گیری	۴-۵
۸۸	نتیجه‌گیری و پیشنهادها		۶
۸۹		مقدمه	۱-۶
۸۹		نتیجه‌گیری	۲-۶

۹۱ ۳-۶ پیشنهادها

۹۲ منابع و مراجع

۹۷ واژه‌نامه انگلیسی به فارسی

۱۰۰ واژه‌نامه فارسی به انگلیسی

فهرست جداول

- جدول ۵-۱. نمونه‌ای از ویژگی‌های محاسبه شده برای داده‌های نرمال ۶۷
- جدول ۵-۲. نمونه‌ای از ویژگی‌های محاسبه شده برای داده‌های حمله ۶۷
- جدول ۵-۳. معیارهای ارزیابی ۷۴
- جدول ۵-۴. نتایج بدست آمده در پنجره زمانی معادل ۱ ثانیه با روش RBF ۷۶
- جدول ۵-۵. نتایج بدست آمده در پنجره زمانی معادل ۳ ثانیه با روش RBF ۷۶
- جدول ۵-۶. نتایج بدست آمده در پنجره زمانی معادل ۵ ثانیه با روش RBF ۷۶
- جدول ۵-۷. نتایج بدست آمده در پنجره زمانی معادل ۱ ثانیه با روش ابرصفحه ۷۷
- جدول ۵-۸. نتایج بدست آمده در پنجره زمانی معادل ۳ ثانیه با روش ابرصفحه ۷۷
- جدول ۵-۹. نتایج بدست آمده در پنجره زمانی معادل ۵ ثانیه با روش ابرصفحه ۷۷
- جدول ۵-۱۰. نتایج بدست آمده در پنجره زمانی معادل ۵ ثانیه با روش ابرصفحه و RBF ۷۸
- جدول ۵-۱۱. نتایج بدست آمده در پنجره زمانی معادل ۵ ثانیه با روش ابرصفحه و RBF ۷۸
- جدول ۵-۱۲. نتایج بدست آمده در پنجره زمانی معادل ۵ ثانیه با روش ابرصفحه و RBF ۷۹
- جدول ۵-۱۳. مقایسه سیستم پیشنهادی و سیستم‌های MLDRNN ۸۳
- جدول ۵-۱۴. مقایسه سیستم پیشنهادی و سیستم‌های DMCA ۸۴

فهرست اشکال

- شکل ۱-۲. ساختار حملات DDOS معمولی (DOULIGERIS & MITROKOTSA, 2004) ۱۲
- شکل ۲-۲. ساختار حملات DDOS مدل بازتابنده (PAXON, 2001) ۱۳
- شکل ۳-۲. حمله DDOS مدل مستقیم مبتنی بر سیلاب (CHANG, 2002) ۱۸
- شکل ۴-۲. حمله DDOS مدل بازتابنده مبتنی بر سیلاب (CHANG, 2002) ۱۹
- شکل ۵-۲. مکانیزم حمله SMURF ۲۱
- شکل ۶-۲. مکانیزم برقراری اتصال TCP (WANG ET AL., 2002) ۲۲
- شکل ۷-۲. مکانیزم حملات TCP SYN مبتنی بر سیلاب (WANG ET AL., 2002) ۲۳
- شکل ۸-۲. مقایسه حمله SMURF و DNS AMPLIFICATION ۲۴
- شکل ۹-۲. مکانیزم حمله DNS AMPLIFICATION (VAUGHN & EVRON, 2006) ۲۵
- شکل ۱-۳. ساختار عمومی روش‌های مبتنی بر ناهنجاری (GARCI'A ET AL., 2009) ۳۵
- شکل ۱-۴. شمای کلی شبکه عصبی RBF (BOUCHACHIA, 2005; MOODY & DARKEN, 1989) ۴۷
- شکل ۲-۴. ابر صفحه‌ای برای جداسازی فضای R_1 و R_2 ۴۸
- شکل ۳-۴. معماری سیستم پیشنهادی جهت کشف حملات DDOS ۵۲
- شکل ۴-۴. مازول FILTERING ۵۳
- شکل ۵-۴. مازول کشف DDOS ۵۴
- شکل ۶-۴. الگوریتم کشف حملات DDOS ۵۹
- شکل ۷-۴. محل قرارگیری سیستم کشف حملات DDOS در شبکه ۶۰
- شکل ۱-۵. طرح پیاده‌سازی سیستم پیشنهادی ۶۴
- شکل ۲-۵. قطعه کد محاسبه آنتروپی پورت مقصد ۶۵
- شکل ۳-۵. قطعه کد محاسبه انحراف مطلق میانه بازه‌های زمانی ۶۵
- شکل ۴-۵. نمایش نمونه‌ای از داده‌های بسته‌های TCP ذخیره شده در پایگاه داده UCLA ۷۱
- شکل ۵-۵. نمایش نمونه‌ای از داده‌های DARPA DATASET ۷۲
- شکل ۶-۵. نمایش نمونه‌ای از بسته‌های حمله ایجاد شده توسط ابزار TRINOO ۷۳
- شکل ۷-۵. نمایش نمونه‌ای از بسته‌های حمله ایجاد شده توسط ابزار TFN2K ۷۳
- شکل ۸-۵. نمودار دقت کشف حملات TCP پایگاه داده DARPA ۷۹
- شکل ۹-۵. نمودار دقت کشف حملات TCP ایجاد شده توسط نرم‌افزار TFN2K ۸۰
- شکل ۱۰-۵. نمودار دقت کشف حملات UDP پایگاه داده UCLA ۸۰
- شکل ۱۱-۵. نمودار دقت کشف حملات ICMP ایجاد شده توسط نرم‌افزار TFN2K ۸۱
- شکل ۱۲-۵. نمودار دقت کشف حملات UDP ایجاد شده توسط نرم‌افزار TFN2K ۸۱

شکل ۵-۱۳. نمودار دقت کشف حملات UDP ایجاد شده توسط نرم‌افزار TRINOO..... ۸۲

شکل ۵-۱۴. نمودار مقایسه دقت کشف حملات توسط سیستم پیشنهادی و MLDRNN..... ۸۴

شکل ۵-۱۵. نمودار مقایسه دقت کشف حملات توسط سیستم پیشنهادی و DMCA..... ۸۵

فهرست علائم اختصاری

C&C	Command& Control
CIAC	Computer Incident Advisory Capability
DDoS	Distributed Denial of Service
DNS	Domain Name Server
DoS	Denial of Service
DMCA	Detection Method using Cluster Analysis
FN	False Negative
FNR	False Negative Rate
FP	False Positive
FPR	False Positive Rate
ICMP	Internet Control Message Protocol
IRC	Internet Relay Chat
IP	Internet Protocol
LASR	Labrotory of Advanced Systems Research
MAD	Median Absolute Deviation
MIT	Massachusetts Institue of Technology
MLDRNN	Maximum Likelihood & Random Neural Network
RBF	Redial Basis Function
TCP	Transmission Control Protocol
TN	True Negative
TNR	True Negative Rate
TP	True Positive
TPR	True Positive Rate
TTL	Time To Live
UCLA	University of California, Los Angeles
UDP	User Datagram Protocol

فصل اول

مقدمه

۱-۱ مقدمه

یکی از پایه‌های مهم امنیت سیستم‌های کامپیوتری، در دسترس بودن منابع آن‌هاست. حملات DoS^۱ از جمله خطرات امنیتی است که ممکن است برای یک سیستم اتفاق بیفتد. حمله DoS سبب می‌شود سیستم یا شبکه قربانی توانایی ارائه سرویس‌های نرمال به کاربران خود را نداشته باشد (Douligieris & Mitrokotsa, 2004). یک سیستم ممکن است در معرض حمله DoS قرار بگیرد و یا برای انجام حمله به قربانی دیگری در اینترنت تسخیر شود.

حملات DoS منابع شبکه را مصرف نموده و فعالیت‌های کامپیوترهای تسخیر شده را کند و یا مختل می‌کنند. قربانی ممکن است یک میزبان^۲، سرویس‌دهنده^۳، مسیریاب^۴ و یا هر موجودیت دیگری در شبکه باشد. این سیستم پس از حمله قادر به برقراری ارتباط عادی با کاربران نخواهد بود. از جمله حملات DoS، حملات DDoS^۵ می‌باشند. این حملات تعداد بسیار زیادی از کامپیوترهای موجود در اینترنت را تسخیر نموده و از آن‌ها به صورت هم‌زمان برای حمله به یک قربانی استفاده می‌کنند. استفاده از چندین سیستم به صورت هم‌زمان، کشف حملات DDoS را مشکل می‌سازد (Meyer & Penzhorn, 2004).

اولین حمله از این نوع در اواخر ژوئن و اوایل جولای ۱۹۹۹ مشاهده شد. در آگوست ۱۹۹۹ نیز یک حمله با نام Trinoo، ۲۲۷ سیستم را برای حمله به کامپیوترهای دانشگاه مینه سوتا به کار گرفت.

^۱Denial of Service

^۲Host

^۳Server

^۴Router

^۵Distributed Denial of Service

همچنین، Yahoo در هفتم فوریه ۲۰۰۰ و eBay، CNN، Amazon.com و Buy.com در هشتم فوریه و Excite و E*Trade، ZDNet در نهم فوریه با سیل این حملات مواجه شدند. حملات DDoS به دو گروه تقسیم می‌شوند: هدف گروه اول حملات مذکور این است که با استفاده از نفوذپذیری‌های نرم‌افزار و یا پروتکل، مانع سرویس دادن سیستم قربانی به کاربران قانونی شود (MölsÄa, 2004).

گروه دوم حملات DDoS برای از کار انداختن سیستم قربانی مقدار زیادی ترافیک حمله به آن ارسال می‌کنند. این گروه که حملات مبتنی بر سیلاب نامیده می‌شوند، تلاش می‌کنند منابع شبکه قربانی را با داده‌هایی که به ظاهر واقعی هستند، اشباع کنند. در نتیجه بسته‌های کاربران قانونی به دلیل کمبود منابعی مانند پهنای باند^۲ به قربانی نخواهند رسید (Douligeris & Mitrokotsa, 2004). در این تحقیق سیستمی برای کشف حملات DDoS ارائه می‌دهیم که بتواند به صورت غیرفعال^۳ این گروه از حملات را شناسایی کند. این سیستم از ناهنجاری‌های ایجاد شده در رفتار بسته‌ها در زمان حمله برای شناسایی ترافیک حمله استفاده می‌کند. در سیستم نهایی پیشنهادی، از شبکه‌های عصبی RBF و روش ابرصفحه^۴ برای ایجاد رابطه‌ای جهت آنالیز و دسته‌بندی ترافیک ورودی به دو دسته ترافیک نرمال و حمله استفاده شده است. جهت دستیابی به ساختار مناسب و منسجم برای تحقیق در ادامه فصل اصول و مبانی که در این تحقیق مورد نظر می‌باشد، ارائه می‌شود.

۲-۱ تعریف مسئله و سوالات اصلی تحقیق

طرح مورد نظر به صورت خلاصه عبارت است از:

«ارائه سیستمی مبتنی بر ناهنجاری و غیرفعال جهت کشف حملات DDoS که دارای درصد خطای پایین و دقت بالا در تشخیص حملات بوده و از روش‌های یادگیری ماشین و روش ابرصفحه برای شناسایی ترافیک حمله از ترافیک نرمال استفاده نماید».

¹Packet

²Bandwidth

³Passive

⁴HyperPlane

بنابراین در پایان این تحقیق ما به سوالات زیر پاسخ خواهیم داد :

۱. برای انجام حملات DDoS چه مراحل طی می‌شود؟
۲. در هر یک از مراحل حمله، ترافیک ارسالی به شبکه قربانی دارای چه ویژگی‌های است؟
۳. ترافیک شبکه در زمان حمله نسبت به حالت نرمال چه تغییری می‌کند؟
۴. بسته‌های حمله دارای چه ویژگی‌های مشترکی هستند؟

۱-۳ سابقه و ضرورت انجام تحقیق

برای محفوظ نگه داشتن شبکه‌ها در مقابل حملات DDoS، نیاز به سیستم‌هایی برای کشف این حملات می‌باشد. تحقیقات بسیاری در این زمینه انجام شده است. به طور کلی این سیستم‌ها را می‌توان به دو دسته تقسیم کرد (Garg & Chawla, 2011; Douligeris & Mitrokotsa, 2004):

- سیستم‌های مبتنی بر امضاء^۱:

این سیستم‌ها برای تشخیص حمله، ترافیک شبکه را با الگوهای موجود از حملات شناخته شده، مقایسه می‌کند. الگوها می‌توانند شامل ویژگی‌های بسته، شرطها، ترتیب و یا رابطه بین وقایع نشان‌دهنده سوءاستفاده، باشند. این روش مشابه نرم‌افزارهای آنتی ویروس است که فایل‌ها و حافظه را با الگوهای شناخته شده از ویروس‌ها مقایسه می‌کند. از جمله اشکالات این روش این است که نمی‌تواند حملات جدید را شناسایی کند.

- سیستم‌های مبتنی بر ناهنجاری^۲:

در این روش انحراف سیستم از رفتار نرمال مورد بررسی قرار می‌گیرد. در واقع این روش‌ها بر پایه یافتن رفتار غیرنرمال نسبت به استانداردهای نرمال می‌باشد. در این روش ترافیک شبکه مانیتور شده و با رفتار مبنا^۴ مقایسه می‌شود. رفتار مبنا نشان‌دهنده رفتار نرمال برای شبکه است. مزیت اصلی این روش نسبت به سیستم‌های مبتنی بر امضاء این است که با تغییر الگوی حملات، که به

¹Signature-based systems

²Pattern

³Anomaly-based systems

⁴Baseline

سادگی امکان پذیر است، دچار خطا در تشخیص نمی‌شوند و می‌توانند حملات جدید را شناسایی کنند.

در (Lee et al., 2008) با بررسی ویژگی‌های مراحل انجام حمله، پارامترهایی برای کشف حمله انتخاب شده است. سپس از الگوریتم خوشه‌بندی^۱ برای تشخیص ترافیک نرمال از مراحل مختلف حمله استفاده شده است. از معایب این سیستم می‌توان به این مورد اشاره کرد که این سیستم فقط در حالتی قابل استفاده است که مهاجم و قربانی در یک شبکه قرار داشته باشند. برای ارزیابی روش ارائه شده از پایگاه داده DARPA (MIT Lincoln Lab, 2000) استفاده شده است.

ضرورت:

در سال ۲۰۰۷ بسیاری از سایت‌ها از جمله سایت‌های دولتی و بانک‌ها در کشور استونی^۲ مورد حمله DDoS قرار گرفت و از آنجایی که بیشتر امور اداری این کشور از طریق وب سایت آن صورت می‌گیرد، این حمله مشکلات بسیاری را برای دولت ایجاد نمود (Guardian, 2007).

از آنجایی که بزودی در ایران شبکه ملی خواهیم داشت و فعالیت‌های IT روی این بستر صورت خواهد گرفت، پس باید از وقوع چنین حادثه‌ای روی شبکه ملی ایران جلوگیری کرد.

۴-۱ فرضیه‌ها

- با بررسی رفتار بسته‌های دریافتی و انتخاب ویژگی‌های بسته‌های حمله در سمت شبکه قربانی و آنالیز این ویژگی‌ها توسط الگوریتم‌های یادگیری ماشین، می‌توان ترافیک حمله را از ترافیک نرمال تشخیص داد.
- روش ابرصفحه می‌تواند در ایجاد رابطه بین ویژگی‌های بسته‌های حمله جهت کشف حملات DDoS مورد استفاده قرار گیرد.

¹Clustering

²Estonia