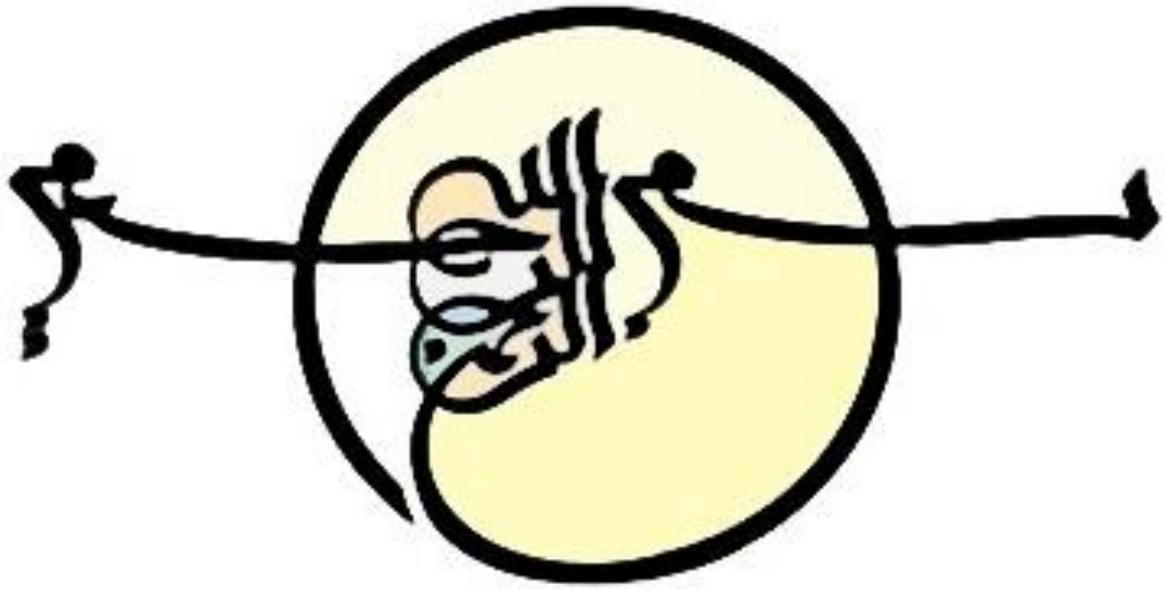


مرکز تهران

پایان‌نامه برای دریافت درجه کارشناسی ارشد

در رشته مهندسی کامپیوتر - نرم‌افزار

دانشکده فنی و مهندسی

گروه علمی مهندسی کامپیوتر و فناوری اطلاعات

عنوان پایان‌نامه:

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

تاریخ .....
شماره .....
پیوست .....

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 (نرم 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:** ..عالی..

هیات داوران:

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

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.tpnu.ac.ir
shemiranat@tpnu.ac.ir

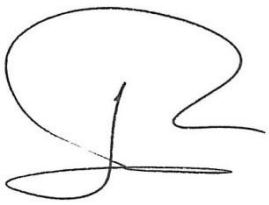
گواهی اصالت نشر و حقوق مادی و معنوی اثر

اینجانب **ریحانه کریم‌آزاد** 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.

نام و نام خانوادگی دانشجو: **ریحانه کریم‌آزاد**

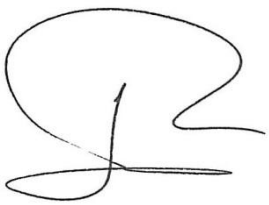
تاریخ و امضاء: **۱۳۹۰/۱۱/۲۶**



اینجانب **ریحانه کریم‌آزاد** 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.

نام و نام خانوادگی دانشجو: **ریحانه کریم‌آزاد**

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 پایان‌نامه را به پایان رسانم.

بر خود واجب می‌دانم که:

از استاد راهنمای بزرگوارم 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 راهنمایی‌های ارزشمندشان را از من دریغ ننمودند،

از خانواده عزیزم، به ویژه برادر مهربانم که همواره یاور و پشتیبان من بوده‌اند،

و از تمام کسانی که در طول دوران تحصیل با راهنمایی‌های ارزشمند علمی و معنوی خود، مرا یاری نمودند سپاس‌گذاری نموده و از خداوند برای این عزیزان آرزوی توفیق و سربلندی می‌نمایم.

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 می‌کندو 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 روش‌های 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 رابطهٔ 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 Trinoo 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

فهرست جداول

فهرست اشکال

فهرست علائم اختصاری

C&C	Command& Control
CIAC	Computer Incident Advisory Capability
DDoS	Distributed Denial of Sevice
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	Massachusette 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[1] 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 (Douligeris &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[2]، سرویس‌دهنده[3]، مسیریاب[4] 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[5] 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.

[1] Denial of Service
[2] Host
[3] Server
[4] Router
[5] Distributed Denial of Service

همچنین، Yahoo در هفتم فوریهٔ ۲۰۰۰ و Amazon.com، CNN، eBay و Buy.com در هشتم فوریه و ZDNet، E*Trade وExcite 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 (MÄolsÄa, 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 کند. در نتیجه بسته[1]های کاربران قانونی به دلیل کمبود منابعی مانند پهنای باند[2] به قربانی نخواهند رسید(Douligeris &Mitrokotsa, 2004).

در این تحقیق سیستمی برای کشف حملات DDoS ارائه می‌دهیم که بتواند به صورت غیرفعال[3] 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[4] برای ایجاد رابطه‌ای جهت آنالیز ودسته‌بندی ترافیک ورودی به دو دستهٔ 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.

۱-۲ 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».

[1] Packet
[2] Bandwidth
[3] Passive
[4] HyperPlane

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

۱. برای انجام حملات DDoS چه مراحلی 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[1]:**

این سیستم‌ها برای تشخیص حمله، ترافیک شبکه را با الگو[2]های موجود از حملات شناخته شده، مقایسه می‌کند. الگوها می‌توانند شامل ویژگی‌های بسته، شرط‌ها، ترتیب و یا رابطهٔ بین وقایع نشان‌دهندهٔ 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[3]:**

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[4] مقایسه می‌شود. رفتار مبنا نشان‌دهندهٔ رفتار نرمال برای شبکه است. مزیت اصلی این روش نسبت به سیستم‌های مبتنی بر امضاء این است که با تغییر الگوی حملات، که به

[1] Signature-basedsystems
[2] Pattern
[3] Anomaly-based systems
[4] Baseline

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[1]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 دادهٔ DARPA (MIT Lincoln Lab, 2000) استفاده شده است.

ضرورت:

در سال ۲۰۰۷ بسیاری از سایت‌ها از جمله سایت‌های دولتی و بانک‌ها در کشور استونی[2] 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.

۱-۴ 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.

[1]Clustering
[2]Estonia