بسم الله الرحمن الرحيم

دانشکده ریاضی و کامپیوتر
بخش علوم کامپیوتر

پایان‌نامه تحصیلی برای دریافت درجه کارشناسی ارشد
رشته علوم کامپیوتر گرایش هوش مصنوعی

تشخیص حمله انکار سرویس توزیع شده با استفاده از روش‌های محاسبات نرم

مؤلف:
ندا کاظمی نژاد

استاد راهنما:
دکتر مرجان کوچکی رفسنجانی

استاد مشاور:
دکتر محمد مسعود جاویدی

بهمن ۱۳۹۳

این پایان‌نامه به عنوان یکی از شرایط درجه کارشناسی ارشد به

بخش علوم کامپیوتر

دانشکده ریاضی و کامپیوتر

دانشگاه شهید باهنر کرمان

تسلیم شده است و هیچگونه مدرکی به عنوان فراغت از تحصیل دوره مزبور شناخته نمی‌شود.

دانشجو : ندا کاظمی نژاد

استاد راهنما : دکتر مرجان کوچکی رفسنجانی

استاد مشاور : دکتر محمد مسعود جاویدی

داور ۱ : دکتر آرشام برومند سعید

داور۲ : دکتر مهدیه قزوینی

نماینده تحصیلات تکمیلی دانشکده :

معاون آموزشی و پژوهشی دانشکده :

تقدیم به خدایی که آفرید

جهان را، انسان را، عقل را، علم را، معرفت را، عشق را

و به کسانی که عشقشان را در وجودم دمید

به همسرم به صمیمیت باران، پدرم به استواری کوه، مادرم به زلالی چشمه

تشکر و قدردانی

سپاس خدای را که هر چه دارم از اوست. او که هستی‌مان بخشید و به طریق علم و دانش رهنمونمان شد. از همراه همیشگی و پشتوانه زندگیم، همسر عزیزم، همچنین پدر و مادر مهربان و فداکارم، به پاس محبت‌ها و حمایتشان، تشکر و قدردانی می‌کنم.

ازاستاد فرهیخته وارجمندم سرکارخانم دکتر مرجان کوچکی رفسنجانی و همچنین جناب آقای دکتر محمد مسعود جاویدی که با نکته‌های دلاویز و گفته‌های بلند، صحیفه‌های سخن را علم پرور نمودند و همواره راهنما و راه‌گشای اینجانب در اتمام و اکمال پایان‌نامه بوده‌اند تقدیر و تشکر می نمایم و همچنین تشکر خالصانه خدمت اساتید داور سرکار خانم دکتر مهدیه قزوینی و جناب آقای دکتر آرشام برومند سعید و همه کسانی که به نوعی مرا در به انجام رساندن این مهم یاری نموده‌اند، دارم.

چکیده

گسترش تکنولوژی اینترنت و خدمات آن، باعث گسترش روزافزون حملات به شبکه‌ها شده است. یکی از شایع‌ترین این حملات، حمله انکار سرویس (DoS)[1] و در حالت خطرناک‌تر حمله انکار سرویس توزیع شده (DDoS)[2] می‌باشد. با گسترش روز افزون حملات DoS و DDoS و با توجه به لزوم ارائه درست سرویس‌ها، نیاز به آشنایی با این حملات روز به روز افزایش می‌یابد. در این نوع حملات، به هنگام استفاده از سیستم برای اهداف قانونی، سیستم آنقدر مشغول است که نمی‌تواند به درخواست‌های مجاز کاربران پاسخ دهد. آنچه در حملات کامپیوتری مورد تأکید همگان است، تشخیص به موقع و در گام بعدی مقابله با آن می‌باشد.

در این پایان‌نامه، سعی شده که حمله DDoS با استفاده از روش‌های محاسبات نرم همچون سیستم‌های عصبی فازی تطبیقی (ANFIS)[3]، تشخیص داده شود. همچنین به منظور بهبود پارامترها و افزایش دقت تشخیص، در مرحله آموزش، از الگوریتم بهینه‌سازی ازدحام ذرات (PSO)[4] بهره برده‌ایم. درنهایت روش پیشنهادی (NFPBoost)[5] و روش‌های دیگر(Bagging، Boosting، RBPBoost، AdaBoost، NFBoost و NFBoost+CM) را در نرم افزار متلب شبیه‌سازی، مقایسه و ارزیابی کرده‌ایم. نتایج، حاکی از آن است که این روش توانایی بیشتری در تشخیص حمله DDoS دارد.

کلید واژه‌ها: حمله انکار سرویس، حمله انکار سرویس توزیع شده، محاسبات نرم، سیستم‌های عصبی فازی تطبیقی، هوش جمعی[6]، بهینه‌سازی ازدحام ذرات.

[1] Denial of Service (DoS)
[2] Distributed Denial of Service Attack (DDoS)
[3] Adaptive Neuro-Fuzzy Inference Systems (ANFIS)
[4] Particle Swarm Optimization (PSO)
[5] Neuro-Fuzzy Particle Swarm Optimization Boost (NFPBoost)
[6] Swarm Intelligence (SI)

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

فهرست نمودارها

فصل اول:

کلیات

۱-۱مقدمه

حمله انکار سرویس (DoS)[۱]، حمله‌ای است که از طریق یک مبدأ واحد راه‌اندازی می‌شود که هدف آن از کاراندازی سیستم قربانی[۲] با استفاده از هدر دادن منابع آن است بطوریکه سیستم سرویس‌دهنده[۳] دیگر توانایی پاسخگویی به کاربران مجازخود را نداشته باشد. تولید حملات انکار سرویس موفق، روی سیستم‌های قدرتمند امروزی، توسط یک سیستم واحد امکان‌پذیر نیست. همچنین پیگیری حمله‌ای که از چند مبدأ متفاوت صورت گرفته باشد، به مراتب دشوارتر از حمله‌ای است که فقط از یک مبدأ واحد صورت گرفته باشد. از طرفی دیگر، حملات تک منبعی به راحتی توسط بسیاری مکانیزم‌های دفاعی مقابله می‌شوند. از اینرو مهاجمان می‌توانند تعدادی از میزبان‌های سازش‌کننده با دشمن[۴] را که توسط ویروس‌ها یا برنامه‌های تروجان [۵] به‌خطر افتاده‌اند را برای راه‌اندازی یک حمله بکارگرفته و بوسیله آن هر سیستم قدرتمندی را نابود کنند. حمله انکار سرویس توزیع شده (DDoS)[۶] یک حمله هماهنگ شده از طریق بسیاری از میزبان‌های به‌خطر افتاده و آسیب‌پذیر است که هدف آن غیرقابل دسترسی کردن خدمات یک سیستم یا چندین سیستم قربانی می‌باشد. درحقیقت حمله DDoS از طریق چندین سیستم و بصورت توزیع شده، راه‌اندازی می‌شود [۱].

۱-۲ بیان مسئله و پیشینه تحقیق

امنیت شبکه یکی از مهم‌ترین بخش‌های دامنه امنیتی است. خدمات بحرانی در هر زیرساخت (سیمی[۷]، بی‌سیم[۸]، شبکه‌های حسگر[۹]) عمدتاً از طریق رابط وب قابل دسترسی است. این خدمات به خوبی توسط دیوار آتش[۱۰] و نرم افزار آنتی ویروس به عنوان سطح اول دفاعی محافظت می‌شوند. با توجه به پیشرفت تکنولوژی اینترنت، منابع اینترنتی و خدمات آن، از راه دور در یک محیط توزیع شده قابل دسترسی می‌باشند. این ویژگی هم برای کاربران مجاز و هم برای مهاجمان مفید می‌باشد. با رشد سریع اینترنت و در دسترس بودن ابزارهای حمله پیشرفته و آسیب‌پذیری پشته پروتکل TCP/IP، حملات امنیتی زیادی همچون حملات انکار سرویس توزیع شده (DDoS) به عنوان

[1] Denial of Service (DoS)
[2] Victim system
[3] Server
[4] Compromised host
[5] Trojan
[6] Distributed Denial of Service (DDoS)
[7] Wired
[8] Wireless
[9] Sensor networks
[10] Firewall

تهدیدی جدی پدیدار شدند. حمله DDoS یک حمله نسبتاً ساده و در عین حال قدرتمند برای حمله به منابع اینترنتی است که اولین بار در ژوئن ۱۹۹۸ ظاهر شد و به سرعت گسترش یافت. این حملات خسارات گسترده‌ای به بارآوردند. آنها به سایت‌های شناخته شده‌ای همچون yahoo، Amazon، CNN، Buy، eBay، Date و ... حمله کردند. اگر مهاجم از سیستم‌های زیادی بطور همزمان برای راه اندازی حملات علیه یک میزبان راه دور استفاده کند به عنوان حمله DDoS تلقی می‌شود. در روش DDoS معمولاً مهاجم سیستم‌های زیادی را آلوده کرده و به آنها همزمان فرمان می‌دهد. به سیستم‌های آلوده شده زامبی[1] و به شبکه‌ای از این سیستم‌ها که تحت کنترل یک شخص هستند، botnet گفته می‌شود. حمله انکار سرویس توزیع شده، تلاش برای خارج کردن سیستم و منابع شبکه از دسترس کاربران مجازش می‌باشد. اگرچه منظور از حمله DDoS و انگیزه انجام آن ممکن است متفاوت باشد، اما بطور کلی شامل تلاش برای قطع موقت یا دائمی و یا تعلیق خدمات یک میزبان متصل به اینترنت است. خسارات مالی و اقتصادی، تخریب عملکرد شبکه، غیر قابل دسترس بودن خدمات در زمان بحرانی و حیاتی، برخی عواملی هستند که انگیزه ما را برای حفاظت در برابر منابع شبکه و برنامه‌های کاربردی آن برمی‌انگیزد. ازآنجائیکه حمله DDoS باعث کارکرد نامناسب یک سیستم اطلاعاتی می‌شود و کاربران را از دسترسی به خدماتی که سرویس‌دهنده موردنظر ارائه می‌دهد محروم می‌کند، از شایع‌ترین انواع حمله‌هاست؛ بنابراین تشخیص این حملات امری ضروری است که روش‌های محاسبات نرم همچون شبکه‌های عصبی[2]، سیستم‌های استنتاج فازی (FIS)[3] و ترکیب این دو یعنی سیستم‌های عصبی فازی، در تشخیص این حملات، نتایج خوبی از خود نشان داده‌اند [۲].

در روشی جدید، گروهی از سیستم‌های عصبی فازی تطبیقی، فعالیت‌های شبکه را طبقه‌بندی کرده و نفوذ[4] را تشخیص می‌دهند. سپس یک ماژول استنتاج فازی، تصمیم نهایی در مورد اینکه فعالیت فعلی، فعالیتی نرمال یا نفوذی است را می‌گیرد. در نهایت به منظور بدست آوردن بهترین نتیجه، یک الگوریتم ژنتیک برای بهینه‌سازی ساختار سیستم تصمیم‌گیر فازی استفاده می‌شود که این روش نرخ تشخیص بالایی دارد [۳].

هال[5] و همکارانش [۴] با استفاده از سیستم‌های استنتاج عصبی فازی تطبیقی و الگوریتم Bagging یک گروه از طبقه‌بندی‌کننده[6]ها ایجاد کرده‌اند که برای تشخیص نفوذ مورد استفاده قرار می‌گیرد

[1] Zombie
[2] Neural network
[3] Fuzzy Inference System (FIS)
[4] Intrusion
[5] Hall
[6] Classifier

که دقت تشخیص بالایی نسبت به روش‌های دیگر دارد.

یک الگوریتم سه مرحله‌ای می‌تواند برای طراحی گروهی از سیستم‌های عصبی فازی استفاده شود. بعد از ایجاد گروه طبقه‌بندی‌کننده‌ها از طریق الگوریتم Bagging هر سیستم عصبی فازی پارامتر T-norm خودش را بروزرسانی می‌کند که به دنبال آن دقت بهبود می‌یابد و تعداد پارامترها کاهش می‌یابد [۵].

به منظور بهبود دقت، می‌توان سیستم‌های عصبی فازی را به صورت گروهی با استفاده از الگوریتم AdaBoost ترکیب کرد. زیرسیستم‌های فازی بوسیله یادگیری گرادیان آموزش داده شده‌اند و بوسیله الگوریتم خوشه‌بندی FCM [۱] مقداردهی اولیه می‌شوند. این تغییر، قابلیت تفسیر دانش را بوسیله ادغام پایگاه‌های قاعده زیرسیستم‌ها به یک پایگاه دانش، بهبود می‌دهند. شبیه‌سازی، عملکرد عالی سیستم‌های عصبی فازی را نشان می‌دهد [۶].

ژانگ[۲] و همکارانش [۷] گروهی از طبقه‌بندی‌کننده‌های عصبی فازی و الگوریتم رأی‌گیری[۳] را بکار برده‌اند بطوریکه کارایی آن در مقایسه با الگوریتم‌های موجود بهبود یافته است.

با استفاده از گروهی از طبقه‌بندی‌کننده‌های عصبی فازی و الگوریتم AdaBoost روش جدیدی پیشنهاد شده بطوریکه طبقه‌بندی، با ویژگی‌های ناشناخته و تعداد کمتر ویژگی‌ها انجام می‌شود [۸].

اسچرر و همکارانش [۹] یک گروه Boosting از سیستم‌های عصبی فازی ایجاد کرده‌اند. قواعد در سیستم‌های عصبی فازی رابطه‌ای، انعطاف‌پذیرتر از قواعد در سیستم‌های عصبی فازی زبانی می‌باشند که دلیل آن وزن‌های اضافی در تالی قواعد می‌باشد. این وزن‌ها از رابطه دودویی اضافی بدست می‌آیند. به پاس این، مجموعه‌های فازی ورودی و خروجی با یک درجه خاص با یکدیگر رابطه دارند. اندازه این رابطه بوسیله تعداد مجموعه‌های فازی ورودی و خروجی تعیین می‌شود. این روش عملکرد خوبی نسبت به دیگر روش‌ها دارد.

روشی برای ادغام پایگاه قواعد از چندین سیستم عصبی فازی که تشکیل‌دهنده یک گروه آموزش دیده بوسیله الگوریتم AdaBoost و الگوریتم پس‌انتشار[۴] می‌باشد، توسط مارسین و همکارانش ارائه شده است. این روش منجر به سیستم عصبی فازی ادغام شده می‌باشد که قابلیت تفسیر و امکان کاهش ویژگی‌ها را بوجود می‌آورد [۱۰].

برای تشخیص حمله انکار سرویس، روش‌های ترکیبی مختلفی از یک سیستم طبقه‌بندی چندگانه و ارزیابی عملکرد آنها، بکارگرفته شده است. نتایج نشان می‌دهد که روش ترکیبی شبکه عصبی

[1] Fuzzy C-Means clustering (FCM)
[2] Zhang
[3] Voting algorithm
[4] Backpropogation algorithm

نسبت به روش‌های دیگر با توجه به قابلیت تنظیم خودکار وزن‌هایش بدون فرضیات قبلی، بهترعمل می‌کند [۱۱].

یک روش جدید برای تشخیص حملات DDoS ارائه شده است. در این روش سیستم‌های عصبی فازی ترکیبی و تطبیقی (ANFIS) به عنوان یک طبقه‌بندی‌کننده پایه انتخاب شده است. در حقیقت این روش شامل دو مرحله پیش‌پردازش و طبقه‌بندی است. سپس خروجی گروه طبقه‌بندی‌کننده‌ها با الگوریتم میانگین وزندارشده[۱] ترکیب می‌شوند. تصمیم‌گیری نهایی بوسیله رأی‌گیری اکثریت[۲] که رأی هر گروه را شامل شده، انتخاب می‌شود [۱۲].

روش RBPBoost از طریق ترکیب خروجی گروه طبقه‌بندی‌کننده‌ها و استراتژی کمینه‌سازی هزینه نیمن پیرسون، برای تصمیم‌گیری طبقه‌بندی نهایی بدست آمده است. این روش یک مجموعه جامع از الگوریتم‌های یادگیری سیستم، برای انتخاب طبقه‌بندی‌کننده پایه استفاده می‌کند. در واقع سیستم پیشنهادی شامل مرحله جمع آوری داده، مرحله پیش‌پردازش، مرحله طبقه‌بندی و مرحله پاسخ می‌باشد [۱۳].

جلیلی و همکارانش [۱۴] روش جدیدی برای تشخیص حملات DDoS، بر اساس یک پیش‌پردازش‌گر آماری و شبکه‌های عصبی مصنوعی بدون ناظر[۳] معرفی کرده‌اند. در این روش ابتدا با درنظرگرفتن مجموعه بسته‌های موجود در یک بازه زمانی، ویژگی‌های آماری نشان‌دهنده رفتار این گونه حملات توسط پیش‌پردازش‌گر آماری، از آنان استخراج شده است. سپس با استفاده از شبکه‌های عصبی بدون ناظر، این ویژگی‌ها تحلیل و به صورت ترافیک نرمال یا حمله طبقه‌بندی شده‌اند.

یک تشخیص‌گر شبکه عصبی RBF [۴] برای حملات انکار سرویس توزیع شده (DDoS) در شبکه‌های عمومی بر اساس ویژگی‌های آماری از بسته‌های داده ورودی، ارائه شده است [۱۵].

یک روش برای تشخیص حملات انکار سرویس توزیع شده (DDoS) بوسیله ساخت یک برآوردگر فازی[۵] روی زمان میانگین بین وقایع شبکه، معرفی شده است که این مسئله به دو چالش تقسیم می‌شود؛ ابتدا تشخیص رخداد حمله انکار سرویس توزیع شده و دوم شناسایی IP آدرس متخلف [۱۶].

جدول ۱-۱ مزایا و معایب روش‌های مذکور را بطور خلاصه بیان می‌کند.

---

[1] Weighted mean
[2] Majority voting
[3] Unsupervised artificial neural networks
[4] Radial Basis Function (RBF)
[5] Fuzzy estimator