

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ



دانشکده ریاضی و کامپیوتر
بخش علوم کامپیوتر

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

تشخیص حمله انکار سرویس توزیع شده با استفاده از روش های
محاسبات نرم

مؤلف:

ندا کاظمی نژاد

استاد راهنما:

دکتر مرجان کوچکی رفسنجانی

استاد مشاور:

دکتر محمد مسعود جاویدی

بهمن ۱۳۹۳



این پایان نامه 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 نمی شود.

دانشجو: ندا کاظمی نژاد

استاد راهنما: دکتر مرجان کوچکی رفسنجانی

استاد مشاور: دکتر محمد مسعود جاویدی

داور ۱: دکتر آرشام برومند سعید

داور ۲: دکتر مهدیه قزوینی

نماینده تحصیلات تکمیلی دانشکده:

معاون آموزشی و پژوهشی دانشکده:

حق چاپ محفوظ و مخصوص به دانشگاه شهید باهنر کرمان است.

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 هستی مان 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.

از استاد فرهیخته و ارجمندم 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 می‌نمایم 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 روزافزون 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. در نهایت روش پیشنهادی (NFPBoost)⁵ و روش‌های دیگر (Boosting, Bagging)، 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 جمعی⁶، 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

۱	فصل اول: کلیات
۲	۱-۱: مقدمه
۲	۲-۱: بیان مسئله و پیشینه تحقیق
۷	۳-۱: چالش‌های مهم تحقیق و اهداف تحقیق
۸	۴-۱: مروری بر فصل‌های پایان نامه
۹	فصل دوم: مقدمه‌ای بر حمله انکار سرویس توزیع شده
۱۰	۱-۲: مقدمه
۱۰	۲-۲: امنیت
۱۱	۳-۲: اینترنت و امنیت
۱۲	۴-۲: مؤلفه‌های امنیت
۱۳	۵-۲: مهاجمان و انگیزه‌های آنها
۱۳	۶-۲: انواع حملات شبکه
۱۳	۶-۲-۱: انواع حملات شبکه با توجه به موقعیت مهاجم
۱۳	۶-۲-۱-۱: حملات انجام شده توسط کاربر مورد اعتماد (خودی)
۱۴	۶-۲-۱-۲: حملات انجام شده توسط افراد غیر معتمد (خارجی)
۱۴	۶-۲-۲: انواع حملات شبکه با توجه به هدف مهاجم
۱۴	۶-۲-۱-۲: حملات انکار سرویس
۱۴	۶-۲-۲: حملات دسترسی به منابع شبکه
۱۵	۶-۲-۳: انواع حملات شبکه با توجه به نحوه اثرگذاری
۱۵	۶-۲-۳-۱: حملات غیرفعال
۱۵	۶-۲-۳-۲: حملات فعال
۱۶	۷-۲: تاریخچه حمله انکار سرویس توزیع شده
۱۷	۸-۲: معرفی حمله انکار سرویس
۱۷	۹-۲: دسته‌بندی انواع حملات

- ۱۷..... ۲-۹-۱: حمله سطح ابزار شبکه
- ۱۷..... ۲-۹-۲: حمله سطح سیستم عامل
- ۱۸..... ۲-۹-۳: حمله سطح برنامه‌های کاربردی
- ۱۸..... ۲-۹-۴: حمله سطح انتشار سیل آسای داده
- ۱۸..... ۲-۹-۵: حمله سطح خصوصیت پروتکل
- ۱۸..... ۲-۱۰-۱: حمله انکار سرویس توزیع شده (DDoS)
- ۱۹..... ۲-۱۱-۱۱: ساختار کلی حمله انکار سرویس توزیع شده
- ۲۰..... ۲-۱۱-۱: فاز کنترل
- ۲۰..... ۲-۱۱-۱-۱: انتخاب عامل‌ها
- ۲۰..... ۲-۱۱-۱-۲: مصالحه کردن
- ۲۱..... ۲-۱۱-۱-۳: ارتباط برقرار کردن
- ۲۱..... ۲-۱۱-۲: فاز حمله
- ۲۱..... ۲-۱۲-۱۲: دسته‌بندی حملات DDoS
- ۲۲..... ۲-۱۲-۱-۱: دسته‌بندی حملات DDoS براساس معماریشان
- ۲۲..... ۲-۱۲-۱-۱-۱: حمله DDoS مبتنی بر راه‌انداز-عامل
- ۲۳..... ۲-۱۲-۱-۲: حمله DDoS مبتنی بر کانال‌های IRC
- ۲۴..... ۲-۱۲-۲: دسته‌بندی حملات DDoS بر اساس توپولوژی شبکه
- ۲۴..... ۲-۱۲-۱-۲: حملات از راه دور
- ۲۵..... ۲-۱۲-۲-۲: حملات محلی
- ۲۶..... ۲-۱۲-۳: دسته‌بندی حملات DDoS بر اساس نقاط آسیب‌پذیری
- ۲۶..... ۲-۱۲-۳-۱: حملات سیلابی
- ۲۷..... ۲-۱۲-۳-۲: حملات تقویتی
- ۲۸..... ۲-۱۲-۳-۳: حملات استعمار پروتکل‌ها
- ۲۹..... ۲-۱۲-۳-۴: حملات بسته‌های ناهنجار
- ۲۹..... ۲-۱۲-۴: دسته‌بندی حملات DDoS بر اساس درجه خودکارسازی حمله

۲۹.....	۱-۴-۱۲-۲ : حملات دستی
۳۰.....	۲-۴-۱۲-۲ : حملات نیمه خود کار
۳۰.....	۳-۴-۱۲-۲ : حملات خود کار
۳۱.....	۵-۱۲-۲ : دسته بندی حملات DDoS بر اساس میزان پویایی نرخ حمله
۳۱.....	۱-۵-۱۲-۲ : حملات با نرخ ثابت
۳۱.....	۲-۵-۱۲-۲ : حملات با نرخ متغیر
۳۲.....	۶-۱۲-۲ : دسته بندی حملات DDoS بر اساس شدت اثر حمله
۳۲.....	۱-۶-۱۲-۲ : حملات مخرب
۳۲.....	۲-۶-۱۲-۲ : حملات پست کننده
۳۲.....	۷-۱۲-۲ : دسته بندی حملات DDoS بر اساس عامل ها
۳۳.....	۱-۷-۱۲-۲ : حملات با مجموعه عامل ثابت
۳۳.....	۲-۷-۱۲-۲ : حملات با مجموعه عامل متغیر
۳۳.....	۱۳-۲ : ابزارهای مورد استفاده در راه اندازی حمله DDoS
۳۳.....	۱-۱۳-۲ : ابزار مبتنی بر عامل
۳۵.....	۲-۱۳-۲ : ابزار مبتنی بر IRC
۳۷.....	۱۴-۲ : خلاصه
فصل سوم: پیشنهادهاى تحقیق (سیستم‌های عصبی فازی تطبیقی و الگوریتم هوش جمعی	
۳۸.....	بهینه سازی ازدحام ذرات)
۳۹.....	۱-۳ : مقدمه
۳۹.....	۲-۳ : محاسبات نرم
۴۱.....	۳-۳ : تاریخچه نظریه مجموعه‌های فازی
۴۱.....	۴-۳ : مفاهیم نظریه مجموعه‌های فازی
۴۱.....	۱-۴-۳ : مجموعه‌های فازی
۴۲.....	۲-۴-۳ : تابع عضویت و درجه عضویت
۴۳.....	۳-۴-۳ : قواعد اگر- آنگاه فازی
۴۳.....	۵-۳ : عملیات اساسی بر روی مجموعه‌های فازی

- ۴۴..... عملگر مکمل ۱-۵-۳
- ۴۴..... عملگر اجتماع ۲-۵-۳
- ۴۵..... عملگر اشتراک ۳-۵-۳
- ۴۵..... سیستم استنتاج فازی ۶-۳
- ۴۶..... فازی سازی ۱-۶-۳
- ۴۶..... پایگاه قواعد ۲-۶-۳
- ۴۶..... موتور استنتاج فازی ۳-۶-۳
- ۴۷..... اعمال ورودی به مقدم‌ها و بدست آوردن درجه عضویت آنها ۱-۳-۶-۳
- ۴۷..... اعمال عملگرهای فازی ۲-۳-۶-۳
- ۴۷..... تجميع خروجی‌ها ۴-۳-۶-۳
- ۴۸..... انواع سیستم های استنتاج فازی ۷-۳
- ۴۸..... سیستم استنتاج ممدانی ۱-۷-۳
- ۴۸..... سیستم استنتاج سوگنو ۲-۷-۳
- ۴۹..... شبکه‌های عصبی مصنوعی (ANN) ۸-۳
- ۵۱..... توابع محرک ۹-۳
- ۵۱..... مجموعه داده آموزشی، آزمایشی و اعتبارسنجی ۱۰-۳
- ۵۲..... تقسیم بندی شبکه‌های عصبی ۱۱-۳
- ۵۲..... شبکه‌های عصبی با یادگیری باناظر ۱-۱۱-۳
- ۵۳..... شبکه‌های عصبی با یادگیری بدون ناظر ۲-۱۱-۳
- ۵۳..... سیستم استنتاج عصبی فازی تطبیقی ۱۲-۳
- ۵۴..... ساختار و الگوریتم ANFIS ۱۳-۳
- ۵۷..... مقدمه‌ای بر الگوریتم بهینه‌سازی ازدحام ذرات ۱۴-۳
- ۵۸..... مفاهیم اولیه ۱-۱۴-۳
- ۵۹..... الگوریتم بهینه‌سازی ازدحام ذرات ۲-۱۴-۳
- ۶۰..... نحوه بروزرسانی مقادیر ۱-۲-۱۴-۳
- ۶۰..... پارامترهای الگوریتم بهینه‌سازی ذرات ۳-۱۴-۳

۶۱.....	۱۵-۳ : مزایای الگوریتم بهینه‌سازی ذرات
۶۱.....	۱۶-۳ : کاربردهای الگوریتم بهینه‌سازی ازدحام ذرات
۶۲.....	۱۷-۳ : معایب الگوریتم بهینه‌سازی ازدحام ذرات
۶۲.....	۱۸-۳ : خلاصه

فصل چهارم: مروری بر کارهای انجام شده در زمینه محاسبات نرم برای تشخیص حمله DDoS

۶۴.....	
۶۵.....	۱-۴ : مقدمه
۶۵.....	۲-۴ : Bagging
۶۶.....	۳-۴ : Boosting
۶۶.....	۴-۴ : AdaBoost
۶۷.....	۵-۴ : RBPBoost
۶۸.....	۶-۴ : سیستم مبتنی بر گروه NFBBoost
۶۹.....	۱-۶-۴ : پیش‌پردازش
۶۹.....	۲-۶-۴ : طبقه‌بندی‌کننده NFBBoost
۷۲.....	۷-۴ : الگوریتم NFBBoost+CM
۷۳.....	۸-۴ : خلاصه

فصل پنجم: ارائه روش پیشنهادی

۷۵.....	۱-۵ : مقدمه
۷۵.....	۲-۵ : بررسی برخی از مکانیزم‌های تشخیص حمله DDoS
۷۶.....	۱-۲-۵ : روش‌های آماری
۷۶.....	۱-۲-۵ : روش‌های مبتنی بر دانش
۷۷.....	۳-۲-۵ : روش‌های محاسبات نرم
۷۷.....	۳-۵ : ارائه روش پیشنهادی NFPBoost
۷۸.....	۱-۳-۵ : استخراج ویژگی‌ها
۷۹.....	۲-۳-۵ : نرمال‌سازی
۸۰.....	۳-۳-۵ : آموزش

۸۱.....	۱-۳-۳-۵: آموزش طبقه‌بندی‌کننده‌ها با PSO
۸۲.....	۴-۳-۵: انتخاب بهترین طبقه‌بندی‌کننده
۸۲.....	۵-۳-۵: آزمایش
۸۵.....	۴-۵: خلاصه
۸۶.....	فصل ششم: پیاده‌سازی مدل پیشنهادی و ارزیابی کارایی آن
۸۷.....	۱-۶: مقدمه
۸۷.....	۲-۶: مراحل کلی روش پیشنهادی NFPBoost
۸۸.....	۳-۶: آماده‌سازی الگوریتم
۸۹.....	۴-۶: آغاز فرآیند پیش‌پردازش
۹۰.....	۵-۶: مقداردهی اولیه پارامترها
۹۱.....	۶-۶: آموزش طبقه‌بندی‌کننده‌ها
۹۲.....	۷-۶: آزمایش الگوریتم
۹۲.....	۸-۶: معیارهای ارزیابی کارایی برای تشخیص حمله
۹۳.....	۹-۶: مقایسه کارایی روش پیشنهادی با سایر روش‌ها
۹۶.....	۱۰-۶: خلاصه
۹۷.....	نتیجه‌گیری
۹۸.....	پیشنهاد برای کارهای آتی
۹۹.....	مراجع
۱۰۵.....	واژه‌نامه انگلیسی به فارسی
۱۱۱.....	واژه‌نامه فارسی به انگلیسی

فهرست شکل‌ها

- شکل ۱-۲ : دسته‌بندی حملات انکار سرویس توزیع شده ۲۲
- شکل ۲-۲ : معماری راه‌انداز-عامل برای حمله DDoS ۲۳
- شکل ۳-۲ : معماری مبتنی بر کانال ارتباطی IRC ۲۴
- شکل ۴-۲ : حملات DDoS بر اساس توپولوژی حمله ۲۵
- شکل ۱-۳ : مراحل سیستم استنتاج فازی ۴۶
- شکل ۲-۳ : سیستم استنتاج فازی سوگنو ۵۵
- شکل ۳-۳ : معادل ANFIS ۵۵
- شکل ۴-۳ : شبه کد الگوریتم PSO ۵۹
- شکل ۵-۳ : فلوجارت الگوریتم PSO ۶۳
- شکل ۱-۴ : شمای روش RBPBoost ۶۹
- شکل ۲-۴ : مراحل پیش پردازش ۷۰
- شکل ۳-۴ : شمای روش NFBoost ۷۱
- شکل ۱-۵ : شمای کلی روش پیشنهادی ۸۴
- شکل ۱-۶ : مراحل کلی روش پیشنهادی ۸۷
- شکل ۲-۶ : ماتریس پراکنندگی ۹۳

فهرست جدول‌ها

- جدول ۱-۱: مزایا و معایب روش‌های ذکر شده ۶
- جدول ۱-۲: مراحل راه‌اندازی حمله انکار سرویس توزیع شده ۱۹
- جدول ۲-۲: خلاصه‌ای از دسته‌بندی حملات انکار سرویس توزیع شده ۳۴
- جدول ۳-۲: خلاصه‌ای از ابزارهای راه‌اندازی حملات انکار سرویس توزیع شده ۳۶
- جدول ۱-۴: مقایسه روش‌های مبتنی بر گروه در تشخیص حمله DDoS ۷۳
- جدول ۱-۵: لیست ویژگی‌ها ۷۹
- جدول ۲-۵: مقایسه روش‌های مبتنی بر گروه و روش پیشنهادی NFPBoost در تشخیص حمله DDoS ۸۳
- جدول ۱-۶: توزیع ترافیک در ۱۰٪ مجموعه داده KDD99 ۸۸
- جدول ۲-۶: توزیع ترافیک در داده‌های آموزشی و آزمایشی ۸۹
- جدول ۳-۶: مقداردهی اولیه پارامترهای الگوریتم بهینه‌سازی ذرات ۹۰
- جدول ۴-۶: مقداردهی اولیه پارامترهای روش پیشنهادی ۹۱
- جدول ۵-۶: نتایج مقایسه روش پیشنهادی با روش‌های پیشین ۹۴

فهرست نمودارها

نمودار ۶-۱: درصد دقت تشخیص حمله DDoS..... ۹۴

نمودار ۶-۲: هزینه طبقه‌بندی هر نمونه..... ۹۵

فصل اول:

کلیات

۱- مقدمه

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 مجاز خود 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 بکار گرفته 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 بار آوردند. آنها به سایت‌های شناخته شده‌ای همچون Amazon، yahoo، eBay، Buy، CNN و Date ... 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^۱ 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. از آنجائیکه حمله DDoS باعث کارکرد نامناسب یک سیستم اطلاعاتی می‌شود و کاربران را از دسترسی به خدماتی که سرویس‌دهنده مورد نظر ارائه می‌دهد محروم می‌کند، از شایع‌ترین انواع حمله‌هاست؛ بنابراین تشخیص این حملات امری ضروری است که روش‌های محاسبات نرم همچون شبکه‌های عصبی^۲، سیستم‌های استنتاج فازی (FIS)^۳ 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^۴ 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^۵ و همکارانش [۴] با استفاده از سیستم‌های استنتاج عصبی فازی تطبیقی و الگوریتم Bagging یک گروه از طبقه‌بندی‌کننده^۶ها 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 گرادینان 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]. اسپرر 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 Backpropagation algorithm

نسبت به روش‌های دیگر با توجه به قابلیت تنظیم خودکار وزن‌هایش بدون فرضیات قبلی، بهتر عمل 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 وزندار شده^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 جمع‌آوری داده، مرحله پیش‌پردازش، مرحله طبقه‌بندی و مرحله پاسخ می‌باشد [۱۳].

جلیلی و همکارانش [۱۴] روش جدیدی برای تشخیص حملات DDoS، بر اساس یک پیش‌پردازش گر آماری و شبکه‌های عصبی مصنوعی بدون ناظر^۳ معرفی کرده‌اند. در این روش ابتدا با در نظر گرفتن مجموعه بسته‌های موجود در یک بازه زمانی، ویژگی‌های آماری نشان‌دهنده رفتار این گونه حملات توسط پیش‌پردازش گر 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 برآورد گر 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