«علوم و فناوری‌های پدافند نوین»
سال چهاردهم، شماره ۱، بهار ۱۴۰۲؛ ص ۶۸- ۵۱

علمی - پژوهشی

تشخیص حملات انکار سرویس با روش یادگیری جمعی

مهدی اسدی[۱*]، باقر زارعی[۲]

۱- استادیار، دانشگاه آزاد اسلامی واحد خامنه ۲- استادیار، دانشگاه آزاد اسلامی واحد شبستر

(دریافت: ۱۴۰۱/۱۲/۲۲، بازنگری: ۱۴۰۲/۰۲/۰۱، پذیرش: ۱۴۰۲/۰۲/۲۲، انتشار: ۱۴۰۲/۰۳/۰۱)
DOR:https://dor.isc.ac/dor/20.1001.1.26762935.1402.14.1.5.5

چکیده

در سال‌های اخیر، فضای مجازی مملو از حملات اینترنتی ازجمله حملات انکار سرویس، فیشینگ اطلاعات، کلاهبرداری مالی، ارسال هرزنامه ایمیل و غیره شده است. از رایج‌ترین حملات اینترنتی که سبب زیان‌های اقتصادی قابل‌توجهی به زیرساخت مالی کشورهای مختلف شده است، حملات انکار سرویس است. به‌عنوان یک اقدام پیشگیرانه، سامانه‌های تشخیص نفوذ مجهز به الگوریتم‌های طبقه‌بندی یادگیری ماشین برای تشخیص ناهنجاری‌ها در ترافیک شبکه توسعه داده شده است. این الگوریتم‌های طبقه‌بندی در ارتباط با نوع حمله انکار سرویس، میزان موفقیت متفاوتی در شناسایی این حملات داشته و به کاربران اجازه می‌دهند تا به طور مؤثر بین ترافیک عادی و ترافیک مخرب انکار سرویس بادقت خوبی تمایز قائل شوند. در روش پیشنهادی، سه مرحله برای شناسایی و طبقه‌بندی متداول‌ترین حملات انکار سرویس به‌کارگرفته‌شده است. در مرحله اول، پیش‌پردازش داده‌های مجموعه داده واقعی **SNMP-MIB** برای حذف داده‌های ناقص و مقیاس‌بندی داده‌ها انجام می‌شود. در مرحله دوم با کاهش تعداد متغیرهای مجموعه داده، صرفاً از متغیرهای گروه واسط مجموعه داده استفاده‌شده که منجر به کاهش زمان تشخیص حملات می‌شود و در مرحله آخر روش یادگیری جمعی نظارتی رأی‌گیری برای تفکیک ترافیک عادی از ترافیک حمله به کار گرفته می‌شود. نتایج نشان می‌دهد که می‌توان ترافیک عادی و ۵ حمله انکار سرویس از مجموعه داده استفاده‌شده را با نرخ دقت ۱۰۰ درصدی تشخیص داد و تنها دقت تشخیص دو حمله **UDP Flood** و **Slowloris** به ترتیب با ۹۹/۸۷ و ۹۹/۹۴ درصد، با استفاده از روش پیشنهادی دارای خطای بسیار ناچیزی بوده است.

کلیدواژه‌ها: حمله انکار سرویس، یادگیری ماشین جمعی، تشخیص ناهنجاری شبکه، مجموعه داده **SNMP-MIB**، ترافیک شبکه، امنیت شبکه

Detection of Denial of Service Attacks by Ensemble Learning Method

M. Asadi*, B. Zarei
Islamic Azad University, Khameneh Branch, Khameneh, Iran
(Received: 2023/03/11 ; revised: 2023/04/13 ; Accepted: 2023/05/11 ; published: 2023/05/22)

Abstract

In recent years, cyberspace has been filled with cyber-attacks such as denial of service (DoS) attacks, information phishing, financial fraud, spam and so on. One of the most common cyber-attacks that have caused significant economic damage to the financial infrastructure of different countries is denial of service attacks. As a preventive measure, intrusion detection systems equipped with machine learning classification algorithms have been developed to detect anomalies in network traffic. These classification algorithms, depending on the type of DoS attack, have varying degree of success in detecting these attacks and allow users to effectively identify between normal traffic and malicious DoS traffic. In the proposed approach, three steps are used to identify and classify the most common denial of service attacks. The first step is to pre-process the actual SNMP-MIB dataset to scale the data and delete the defective data. In the second stage, by reducing the number of data set features, only the features of the interface group are used, which leads to a reduction in attack detection time. The results show that using the proposed approach, normal traffic and five DoS attacks can be detected from the SNMP-MIB dataset with 100% accuracy rate. Only the detection accuracy of two attacks, UDP Flood and Slowloris, with 99.87 and 99.94% respectively, had a very small error of detection rate.

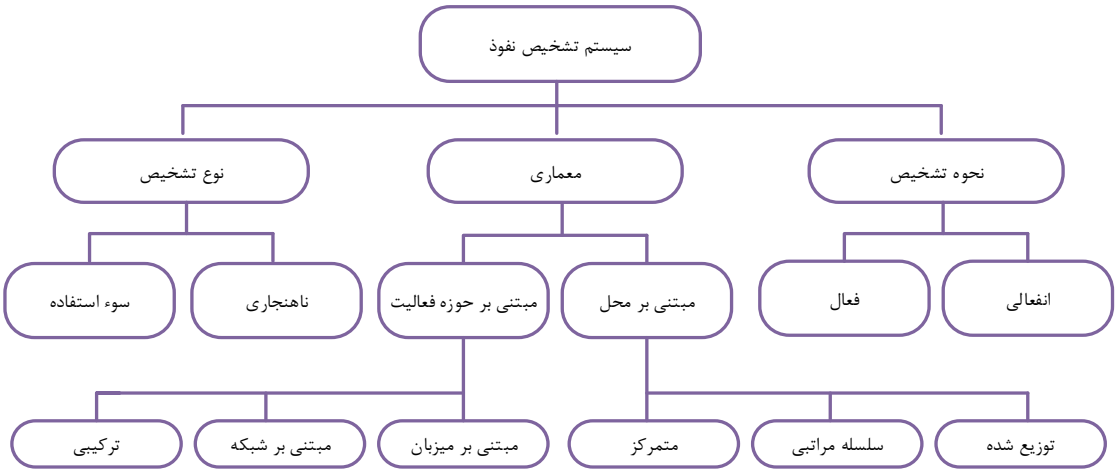
Keywords: Denial of Service Attack, Ensemble Machine Learning, Network Anomaly Detection, SNMP-MIB Dataset, Network Traffic, Network Security

*Corresponding Author E-mail :mehdi.asadi@iau.ac.ir

۱. مقدمه

با گسترش اینترنت و جذب بیشتر جنبه‌های زندگی روزمره از هر زمان دیگری، از ارتباطات اجتماعی گرفته تا پرداختی‌های الکترونیکی، تعداد حملات اینترنتی مخرب هم ازنظر نوع و هم ازنظر تعداد افزایش‌یافته است؛ بنابراین، نیاز به شناسایی انواع مختلف این حملات و جلوگیری از استفاده آن‌ها از فن‌های مختلف امنیت شبکه بسیار مهم است [۱]. هدف برخی از حملات دسترسی غیرمجاز به دستگاه‌ها و اطلاعات مانند سرریز بافر و حملات بروت فورث[1] است همچنین در حملات دیگر از قبیل کرم اینترنتی و حملات انکار سرویس[2]، هدف آن است که سامانه‌ها از دسترس خارج شوند [۴-۲]. در بین تمام انواع حملات ذکرشده، حملات انکار سرویس به‌عنوان خطرناک‌ترین و پرکاربردترین حملات مورداستفاده قرار می‌گیرند و سبب ضررهای مالی هنگفتی می‌شوند [۵]. برای مقابله با این حملات، سیستم تشخیص نفوذ به یکی از اجزای اصلی هر سامانه در شبکه تبدیل‌شده است. هدف سیستم تشخیص نفوذ، شناسایی درخواست‌های مخرب ورودی به شبکه است [۸-۶].

شکل (۱)، نمای کلی یک سیستم تشخیص نفوذ را نشان می‌دهد. دو روش اصلی برای تشخیص این درخواست‌ها وجود دارد؛ اولین روش که تشخیص ناهنجاری نفوذ[3] نامیده می‌شود درخواست‌های جدید ورودی به سامانه را با درخواست‌های عادی قبلی مقایسه کرده و ناهنجاری در ترافیک شبکه را تعیین می‌کند، دومین روش که موسوم به تشخیص سوءاستفاده از نفوذ[4] [۹] است درخواست‌های جدید را با امضاهای حملات شناخته‌شده مقایسه کرده و تعیین می‌کند که آیا الگوی حملات با امضاهای موجود مطابقت دارد یا نه؟

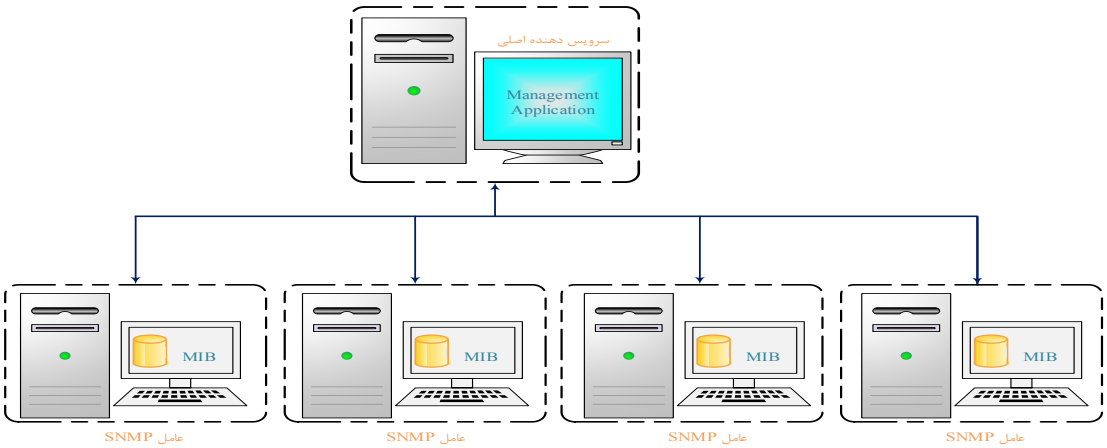


شکل ۱. نمای یک سیستم تشخیص نفوذ [۱۰]

هر دو روش اشاره‌شده، برای تشخیص نفوذ، متکی به مجموعه داده‌ای هستند که برای مقایسه با درخواست‌های جدید استفاده می‌کنند. به‌عنوان‌مثال، هنگام استفاده از داده‌های بسته خام، بار پردازش قابل توجه بوده و منجر به کند شدن زمان تشخیص می‌شود، این امر منجر به توسعه پروتکل‌های مختلف برای نظارت و مدیریت بسته‌های داده ازجمله پروتکل اطلاعات مدیریت مشترک[1]، مانیتورینگ از راه دور شبکه[2] و پروتکل ساده مدیریت شبکه[3] شده است. پروتکل ساده مدیریت شبکه، اطلاعات دستگاه‌ها و تجهیزات مختلف متصل به یک شبکه، اطلاعات مرتبط با لایه‌های مختلف شبکه و همچنین اطلاعات پروتکل‌های مختلف ازجمله پروتکل کنترل انتقال[4]، پروتکل دیتاگرام کاربر[5]، پروتکل اینترنت[6]، پروتکل پیام کنترلی اینترنت[7] را نیز جمع‌آوری می‌کند [۱۱]. شکل (۲) چگونگی ترکیب پروتکل ساده مدیریت شبکه با پایگاه اطلاعات مدیریت[8] را به‌عنوان یک اصل اساسی در هر مدل مدیریت اینترنت نشان می‌دهد. برای استفاده از این حجم زیاد داده، یک سیستم پایگاه داده معروف به پایگاه اطلاعات مدیریت از چندین متغیر مدیریتی برای ذخیره این داده‌ها در قالب آماری استفاده می‌کند. در زمان اتصال پایگاه اطلاعات مدیریت به پروتکل ساده مدیریت شبکه، سیستم مناسبی برای شناسایی و تشخیص انواع حملات مختلف با استفاده از نظارت غیرفعال و جمع‌آوری و ذخیره‌سازی سازمان‌یافته داده‌ها فراهم می‌شود [۹].

[1] Brute Force Attacks
[2] Denial of Service (DoS)
[3] Anomaly Intrusion Detection (AID)
[4] Misuse Intrusion Detection (MID)
[5] Common Management Information Protocol (CMIP)
[6] Remote Network Monitoring (RNM)
[7] Simple Network Management Protocol (SNMP)

[4] Transmision Control Protocol (TCP)
[5] User Datagram Protocol
[6] Internet Protocol (IP)
[7] Internet Control Message Protocol (ICPM)
[8] Management Information Base (MIB)



شکل۲. معماری مدیریت شبکه [۱۳]

النایمت و همکاران [۹]، ثابت کردند که ناهنجاری‌های شبکه را می توان با استفاده از SNMP-MIB و دسته‌بندی کننده‌های مناسب تشخیص داد. آن‌ها از مجموعه داده‌ای با ۳۴ متغیر استفاده کردند که در پنج گروه طبقه‌بندی‌شده بودند. نتایج به‌دست‌آمده موفقیت در تشخیص حملات با درصد بالایی را ارائه داده است.

در روش ارائه‌شده، با کاهش فرآیندها و عملیات انجام‌شده توسط سیستم تشخیص نفوذ برای یادگیری الگوهای ترافیکی و طبقه‌بندی ترافیک شبکه، سرعت تشخیص حملات افزایش‌یافته است. هدف، افزایش کار آیی سیستم تشخیص نفوذ با کاهش منابع موردنیاز است. هدف از این مقاله تجزیه‌وتحلیل پرکاربردترین حملات انکار سرویس به‌صورت جداگانه و مقایسه آن‌ها ازنظر میزان تشخیص با استفاده از مجموعه داده SNMP-MIB ارائه شده توسط الکساب و همکاران [۱۲] است. در روش پیشنهادی، ابتدا عملیات پیش‌پردازش داده‌ها بر روی مجموعه داده، برای حذف داده‌های پرت انجام می‌شود. در مرحله انتخاب ویژگی‌های تأثیرگذار، با بررسی‌ها و آزمایش‌های مختلف صرفاً از هشت متغیر گروه واسط مجموعه داده به‌جای استفاده از تمامی ۳۴ متغیر مجموعه داده، استفاده می‌شود و درنهایت روش یادگیری رأی‌گیری برای تفکیک ترافیک عادی از ترافیک حمله، مورداستفاده قرار می‌گیرد.

ساختار مقاله در ادامه به شرح زیر است: بخش ۲ مروری بر پژوهش‌های مرتبط را که از یادگیری ماشین در سامانه‌های تشخیص نفوذ استفاده کرده‌اند ارائه می‌دهد. در بخش ۳، مفاهیم پایه همچون حملات انکار سرویس، پروتکل شبکه ساده، یادگیری ماشین و حملات انکار سرویس ارائه شده است. روش پیشنهادی، تشریح مجموعه داده SNMP-MIB، به‌کارگیری یادگیری ماشین و جزئیات پیاده‌سازی در بخش ۴ و نتایج حاصل از آزمایش‌ها و مقایسه با طبقه‌بندی‌کننده‌های یادگیری ماشین و روش‌های ارائه‌شده در مطالعات پیشین در بخش ۵ نمایش‌داده‌شده است. درنهایت، نتیجه‌گیری این مقاله در بخش ۶ ارائه‌شده است.

۲. پیشینه تحقیق

ازآنجاکه شناسایی ناهنجاری‌ها و تشخیص نفوذ در شبکه بسیار حائز اهمیت است، مطالعات و تحقیقات زیادی درگذشته انجام‌یافته و مورد ارزیابی قرارگرفته است. اکثر این روش‌ها بر تجزیه‌وتحلیل داده‌های ترافیک خام بر اساس جریان شبکه، آدرس‌های آی پی، تعداد بسته‌های ردوبدل شده در شبکه، پورت-ها و سایر ویژگی‌های کلیدی متمرکز بوده‌اند. نوع دیگری از روش برای تشخیص ناهنجاری‌ها استفاده از پایگاه اطلاعات مدیریت پروتکل مدیریت شبکه ساده[1] به‌عنوان منبع داده است. در این بخش به بررسی تحقیقات پیشین با محوریت تشخیص نفوذ با استفاده از روش پایگاه اطلاعات مدیریت پروتکل مدیریت شبکه ساده می‌پردازیم.

یکی از مطالعات اولیه در این زمینه توسط کابرا و همکاران [۱۴] انجام‌شده است که از آزمون‌های آماری حاصل از متغیرهای مختلف پایگاه اطلاعات مدیریت برای تشخیص زودهنگام حملات انکار سرویس توزیع‌شده[2] استفاده کردند. برای استخراج متغیرها، سه نوع مختلف از حملات انکار سرویس توزیع‌شده اعمال‌شده و ۹۱ متغیر پایگاه اطلاعات مدیریت از پنج گروه مختلف (TCP، UDP، IP، ICMP و SNMP) در سمت سیستم مهاجم و نیز در سمت سیستم قربانی موردبررسی قرارگرفته است. ارزیابی این روش نشان داده است که پیش‌بینی و تشخیص حمله انکار

[1] SNMP-MIB
[2] Distributed Denial of Service (DDoS)

سرویس توزیع‌شده قبل از خاموش شدن سیستم قربانی با نرخ مثبت کاذب[1] تقریبی تنها ۱٪ امکان‌پذیر بوده است.

در تحقیق ارائه‌شده توسط رحمانی و همکاران [۱۵]، روش پیشنهادی دیگری با استفاده از آزمایش‌های آماری برای تشخیص حملات پیشنهادشده است. متغیرهای پایگاه اطلاعات مدیریت با نمونه‌برداری از ترافیک شبکه از چهار گروه TCP، UDP، IP و ICMP جمع‌آوری‌شده است. در هر ۵ ثانیه نمونه‌گیری انجام‌شده و این روش برای پنج نوع حمله انکار سرویس توزیع‌شده مورد آزمایش قرارگرفته و میزان دقت بالایی در تشخیص را نشان داده است. سیائو و همکاران [۱۶] نیز از پارامترهای SNMP-MIB برای تشخیص یک نوع خاص از حمله بنام حمله جعلی ARP استفاده کرده‌اند. آن‌ها سه روش متفاوت شامل یک الگوریتم ساده بیزی، یک الگوریتم ماشین بردار پشتیبانی و درنهایت یک الگوریتم C4.5 را آزمایش کرده و نتایج این روش‌ها را با همدیگر مقایسه کرده‌اند. آن‌ها از معیارهایی نظیر نرخ مثبت کاذب، میزان دقت[2] و نرخ ازدست‌رفته برای شناسایی نقاط قوت و ضعف هر روش استفاده کرده‌اند. بر اساس نتایج به‌دست‌آمده الگوریتم درخت تصمیم C4.5 دارای بالاترین نرخ دقت بوده، درحالی‌که کمترین میزان دقت مربوط به الگوریتم بیزی ساده بود و الگوریتم ماشین بردار پشتیبان دارای کمترین تعداد هشدارهای کاذب بوده است.

یو و همکاران [۱۷] موفق شده‌اند تا با روش پیشنهادی خود حملات سیل‌آسا را با استفاده از پارامترهای SNMP-MIB و الگوریتم درخت تصمیم C4.5 به میزان ۹۳٪ تشخیص دهند. این پارامترها بر اساس عملکرد حمله سیل‌آسا در محیط شبیه‌سازی به‌دست‌آمده و از یک الگوریتم بهبودیافته C4.5 برای طبقه‌بندی انواع مختلف ترافیک و تشخیص حملات سیل‌آسا بر روی پارامترهای تولیدشده استفاده می‌کرد.

سرونی و همکاران [۱۸] در تحقیق دیگری از داده‌کاوی توزیع‌شده جدیدی برای تشخیص نوع خاصی از حمله انکار سرویس توزیع‌شده استفاده کردند که این روش در یک محیط شبکه شبیه‌سازی‌شده و بر روی ۱۴ پارامتر مجموعه داده (مرتبط با آی پی و تی سی پی) برای تشخیص حمله انجام‌شده است. این روش برای محیط‌های آزمایشگاهی غیرمتمرکز ارزیابی‌شده و میزان تشخیص مطلوبی را ارائه داده است.

در مقاله ارائه‌شده توسط النایمت و همکاران [۱۹] مجموعه پارامترهای مجموعه داده و روش یادگیری ماشین برای ساخت یک سیستم تشخیص نفوذ دارای سه مدل استفاده‌شده است. ماژول اول از الگوریتم‌های C4.5 ، الگوریتم انتخاب ویژگی و الگوریتم RIPPERبرای انتخاب متغیرهای برتر پایگاه اطلاعات مدیریت استفاده کرده و این متغیرها نیز توسط مدل دوم برای ایجاد یک سیستم تشخیص نفوذ استفاده‌شده است. همچنین مدل سوم از خروجی مدل دوم آن برای تشخیص بلادرنگ حملات انکار سرویس استفاده کرده است. این سیستم از چهار گروه پایگاه اطلاعات مدیریت مرتبط با حملاتICMP ، UDP و TCP–SYN برای آزمایش استفاده کرده و نرخ تشخیص بالای ۹۹/۰۳ را به دست آورده است.

از سوی دیگر، سرونی و همکاران [۲۰] از یک مکانیسم تشخیص غیرمتمرکز دومرحله‌ای بر اساس الگوریتم خوشه‌بندی استفاده کردند. مرحله اول شامل یک مرحله پایش بوده که در این مرحله چندین منبع برای جمع‌آوری پارامترهای SNMP-MIB موردبررسی قرارگرفته است. مرحله دوم مرحله تشخیص ترافیک بود که از پارامترهای مجموعه داده برای طبقه‌بندی ترافیک در ترافیک غیرعادی و ترافیک معمولی استفاده‌شده است. برای آزمایش مکانیسم تشخیص غیرمتمرکز، سرونی و همکارانش از زیرمجموعه‌ای از مجموعه داده مذکور که مربوط به مکانیسم‌های تشخیص غیرمتمرکز است، استفاده کردند و پس از انجام آزمایش-ها مشخص شد که الگوریتم دومرحله‌ای پیشنهادی آن‌ها قابلیت شناسایی با موفقیت نفوذهای محتمل را در زیرمجموعه‌ای از مجموعه داده داشته است.

النایمت و همکاران [۹] از فن‌های طبقه‌بندی یادگیری ماشینی همچون جنگل تصادفی، آدابوست و شبکه عصبی چندلایه برای ساخت مدل تشخیص حملات انکار سرویس و حملات بروت فورث بر روی داده‌های پایگاه اطلاعات مدیریت مرتبط با پروتکل مدیریت شبکه ساده استفاده کرده و متغیرهای پایگاه اطلاعات مدیریت را در پنج گروه (ICMP، Interface، IP، TCP و UDP) دسته‌بندی کرده‌اند. از نتایج کار آن‌ها این‌گونه استنباط شده است که گروه‌های واسط و آی‌پی تنها گروه‌هایی هستند که در بین پنج گروه، بیشترین تأثیر و سایر گروه‌ها کمترین تأثیر را از انواع حملات داشته‌اند. همچنین با استفاده از طبقه‌بندی کننده جنگل تصادفی بالاترین میزان دقت برای گروه آی‌پی به میزان ۱۰۰٪ و برای گروه آی‌پی به میزان ۹۹/۹۳% به‌دست‌آمده است.

همچنین النایمت و همکاران [۲۱] در مقاله دیگری برای تشخیص ناهنجاری‌های شبکه از طبقه بند یادگیری ماشین Lazay.IBk، روش همبستگی[3] و الگوریتم ReliefF برای انتخاب ویژگی‌های تأثیرگذار از پارامترهای مجموعه داده استفاده کرده‌اند. آن‌ها علاوه بر کاهش استفاده از منابع سخت‌افزاری همچون پردازنده و حافظه میزان دقت تشخیص بالایی نیز ارائه داده‌اند.

در تحقیق ارائه‌شده توسط مانا و همکاران [۲۲]، داده‌های مجموعه داده برای شناسایی ناهنجاری‌های حملات انکار سرویس

[1] False Positive Rate
[2] Accuracy Rate
[3] Correlation

در شبکه استفاده‌شده است. در روش ارائه‌شده توسط آن‌ها سه الگوریتم یادگیری ماشین جنگل تصادفی[1]، درخت تصمیم J48 و درخت REP برای طبقه‌بندی داده‌ها و دو الگوریتم ارزیابی ویژگی InfoGain و ReliefF برای انتخاب ویژگی‌های تأثیرگذار استفاده‌شده است. طبقه‌بندی کننده‌ها و انتخاب ویژگی‌ها بر روی داده‌ها و پارامترهای گروه آی‌پی اعمال‌شده و نتایج به‌دست‌آمده نشان داده که بیشترین دقت در تمام گروه‌های آی‌پی، زمانی است که از طبقه‌بندی کننده درخت REP استفاده‌شده است.

راجاسکار و ماگودیسواران [۲۳] با استفاده از روش‌های یادگیری ماشین بر روی مجموعه داده SNMP-MIB، مکانیسم مؤثری برای شناسایی و طبقه‌بندی حملات انکار سرویس توزیع‌شده ارائه داده‌اند. بدین منظور، پایگاه اطلاعات مدیریت برای طبقه‌بندی حملات مرتبط با پروتکل مدیریت شبکه ساده در نظر گرفته‌شده است. آن‌ها از شبکه عصبی بازگشتی دروازه‌ای[2] مبتنی بر طبقه‌بندی کننده میانگین وزنی ویژگی دو جهتِ[3] (GRU-BWFA)به‌عنوان طبقه‌بندی کننده پیشنهادی برای نرخ تشخیص بالا و دقت در تشخیص حملات انکار سرویس توزیع‌شده استفاده کرده‌اند. برای انتخاب ویژگی‌های بهینه برای شناسایی حملات، آن‌ها از الگوریتم بهینه‌سازی ازدحام سالپ پیشرفته استفاده کرده و با استفاده از طبقه‌بندی کننده‌های مختلف، مطالعه دقیقی در مورد اثربخشی مجموعه داده در تشخیص حملات انکار سرویس توزیع‌شده ارائه داده‌اند. یافته‌های تجربی آن‌ها نشان می‌دهد که روش‌های یادگیری ماشینی در شناسایی و طبقه‌بندی حملات با نرخ دقت بالاتر بسیار مؤثر بوده است.

با توجه به اینکه سرعت تشخیص حملات انکار سرویس بسیار حائز اهمیت است و نیز دقت بالا برای تشخیص این حملات در محیط‌هایی همچون مراکز مالی و نظامی بسیار مهم است با انتخاب ۸ ویژگی گروه واسط بجای استفاده از ۳۴ ویژگی مجموعه داده SNMP-MIB، علاوه بر بالابردن سرعت، دقت بالایی نیز با به‌کارگیری تعداد ویژگی‌های کمتر و استفاده از روش جمعی حاصل‌شده است که با پیاده‌سازی آن نسبت به روش‌های پیشین و مطرح‌شده عملکرد بهتر و بالاتری ارائه کرده است.

۳. مفاهیم پایه

در ادامه به مباحثی همچون حملات انکار سرویس و انواع آن، پروتکل مدیریت شبکه ساده و الگوریتم‌های یادگیری ماشین پرداخته می‌شود.

۳-۱. حملات انکار سرویس

روش‌های زیادی ازجمله از شنود، فیشینگ[4] و تزریق اس‌کیوال[5] برای به خطر انداختن شبکه وجود دارد. بااین‌حال، یکی از روش‌های مورداستفاده مهاجمان، حمله انکار سرویس است. در مواردی که هدف حملات دیگر ممکن است برای دستیابی به دسترسی غیرمجاز یا داده‌های محافظت‌شده باشد، حملات انکار سرویس قصد دارند عملکرد شبکه یا خدماتی را که ارائه می‌دهد را مختل کنند. حمله انکار سرویس مجموعه اقداماتی است که مانع از انجام وظایف شبکه‌ها، منابع شبکه و کاربران مجاز آن شبکه‌ها می‌شود. برای دستیابی به این هدف، حمله انکار سرویس، منابع متعددی از شبکه را مورد هدف قرار داده و به خطر می‌اندازد. اولین منبع مورد حمله، پهنای باند شبکه است به‌طوری‌که حمله، اتصال بین یک سرور وب و تجهیزاتی که به آن متصل می‌شوند را هدف قرار داده و یا اتصال بین سرور وب و اینترنت جهانی را هدف قرار می‌دهد. دومین منبعی که حمله انکار سرویس می‌تواند هدف قرار دهد منابع سامانه کامپیوتری است، به‌طوری‌که درخواست‌های بسیار زیادی را به‌صورت مستمر به سامانه ارسال کرده و مانع از پاسخگویی به کاربران مجاز واقعی می‌شود. آخرین هدف برای حمله انکار سرویس منابع کاربردی و برنامه است که حمله با کل سامانه کاری ندارد و فقط یک برنامه خاص از آن سیستم را از دسترس خارج می‌کند.

در این بخش، انواع مختلف حملات انکار سرویس که اغلب توسط هکرها و مهاجمان مورداستفاده قرار می‌گیرند بررسی و ارائه می‌شود [۲۴]:

- حمله جعلی SYN: این حمله، اصلی‌ترین حمله سیل‌آسا است که جداول سرویس‌دهنده‌هایی را که ارتباطات را با مشتریان مدیریت می‌کنند، مورد هدف قرار می‌دهد. در این حمله از پروتکل دستکانی[6] سه‌طرفه در درخواست‌های اتصال پروتکل کنترل انتقال استفاده می‌شود. روش دستکانی عادی سه‌طرفه با ارسال درخواست TCP-SYN توسط مشتری آغازشده، سرویس‌دهنده با پیام SYN-ACK پاسخ می‌دهد و درنهایت مشتری یک بسته پاسخ را برای تأیید اتصال ارسال می‌کند. فعالیتی که در حمله جعلی SYN انجام می‌شود بدین‌گونه است که با آدرس آی پی مبدأ جعلی درخواست‌های TCP-SYN زیادی به سمت سرور ارسال می‌شود که سرویس‌دهنده درخواست SYN-ACK را به آن‌ها ارسال می‌کند. این کار سبب دو واکنش می‌شود؛ اولین مورد این است که تعداد زیادی درخواست TCP-SYN بدون دریافت بسته‌های پاسخ مناسب در جدول ذخیره می‌شوند؛ زیرا آدرس‌های آی پی جعلی به

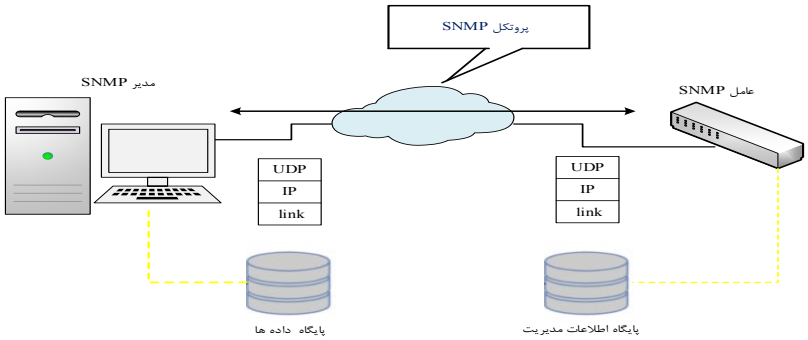
[1] Random Forest
[2] Gated Recurrent Unit Neural Network
[3] Bidirectional Weighted Feature Averaging
[4] Phishing
[5] SQL Injections
[6] Handshake Protocol

درخواست‌های SYN-ACK که سرویس‌دهنده ارسال می‌کند نمی‌تواند پاسخ دهد. دومین مورد اینکه برای هر درخواستی (SYN-ACK) که سرویس‌دهنده ارسال می‌کند، مکانی برای تأیید پاسخ در نظر گرفته‌شده و سبب ایجاد سربار می‌شود. این موارد سبب می‌شود تا جدول سرویس‌دهنده با درخواست‌های ناقص TCP-SYN و SYN-ACK پر شود و نتواند سایر درخواست‌های اتصال مشتری را برآورده کند.

- حمله ارسال سیل‌آسای پروتکل دیتاگرام کاربر[1]: این حمله یک درگاه خاص در سیستم یا سرویس‌دهنده قربانی را هدف قرار می‌دهد، سپس درگاه موردنظر را با بسته‌های پروتکل دیتاگرام کاربر غرق می‌کند تا بیشتر از ظرفیت درگاه بسته‌ها بارگذاری شود و سرویس ارائه‌شده را خاموش کند.
- حمله ارسال سیل‌آسای پروتکل انتقال ابر متن[2]: حمله‌ای مبتنی بر پروتکل انتقال ابر متن است که با به‌کارگیری بات‌های متعددی که به وب سرویس‌دهنده نفوذ می‌کنند تا وظایف پروتکل انتقال ابر متن را انجام دهند منابع سرویس‌دهنده من‌جمله اطلاعات موجود در حافظه را تخلیه می‌کند.
- حمله Slowloris: یکی دیگر از حملات مبتنی بر پروتکل انتقال ابر متن است که در این حمله، مهاجم چندین اتصال به سرویس‌دهنده را بر اساس درخواست‌های ناقص پروتکل انتقال ابر متن ایجاد می‌کند، برای جلوگیری از قطع‌شدن این اتصالات، پیام‌های پی‌درپی برای زنده نگه‌داشتن اتصال ارسال می‌شود، این مداومت در به‌کارگیری تمامی اتصالات، یک سرویس‌دهنده را مشغول کرده و سبب رد سرویس به سایز اتصالات می‌شود.
- حمله Slowpost: حمله‌ای تقریباً مشابه به حمله Slowloris است. Slowpost یکی دیگر از حملات مبتنی بر پروتکل انتقال ابر متن است که درخواست‌های پروتکل انتقال ابر متن را به سرویس‌دهنده قربانی ارسال می‌کند، تفاوت این روش حمله با روش Slowloris در اینجا است که در این حمله درخواست‌های پروتکل انتقال ابر متن کامل است؛ یعنی دارای فیلد طول محتواست که پیام ارسال‌شده به درخواست را نشان می‌دهد؛ بااین‌حال، محتوا بسیار آهسته با نرخ یک بایت در هر دو دقیقه تحویل داده می‌شود و درنهایت بار بسیار زیادی بر روی سرویس‌دهنده اعمال می‌شود تا فعالیت سرویس‌دهنده توسط درخواست‌های پروتکل ناتمام مختل شود.
- حمله ICMP Echo: در شبکه‌های TCP/IP درخواست‌های Echo به طور مرتب برای تشخیص درگاه‌ها استفاده می‌شوند. مهاجمان و هکرها، درخواست‌های Echo و بسته‌های ICMP رو به سمت سرویس‌دهنده ارسال می‌کنند و دسترسی مؤثر هر سرویس‌گیرنده به سرویس‌دهنده را دشوار می‌کند. مدیران سامانه‌ها معمولاً این پروتکل را با دیواره آتش یا سامانه‌های تشخیص نفوذ محدود می‌کنند. حمله بروت فورث: این حمله به‌عنوان یک روش ساده برای دورزدن گذرواژه مورداستفاده قرار می‌گیرد، اما از آن به‌عنوان یک حمله انکار سرویس نیز استفاده می‌شود با این حمله درخواست‌های احراز هویت گذرواژه به‌صورت سیل‌آسا به سمت سرویس‌دهنده ارسال می‌شود تا منابع آن به پایان برسد.

۳-۲. پروتکل مدیریت شبکه ساده (SNMP)

این پروتکل در لایه کاربرد شبکه برای کنترل بهتر و نظارت و تجزیه‌وتحلیل ترافیک یک شبکه خاص توسعه داده شده است که شامل دو زیرسیستم (۱) عامل پروتکل مدیریت شبکه ساده و (۲) مدیر پروتکل مدیریت شبکه ساده است که در شکل (۳) نشان‌داده‌شده است. عامل پروتکل مدیریت شبکه ساده بر روی دستگاه‌هایی که قصد نظارت بر روی آن‌ها را دارد تعبیه می‌شود و داده‌ها را از شبکه آن دستگاه جمع‌آوری کرده و در پایگاه اطلاعات مدیریت ذخیره می‌کند.



شکل ۳. پروتکل SNMP و زیرسیستم‌های آن [۱۳]

[1] User Datagram Protocol (UDP)
[2] Hyper Text Transfer Protocol (HTTP)

مدیر پروتکل مدیریت شبکه ساده این اطلاعات را از عامل پروتکل مدیریت شبکه ساده درخواست کرده و از آن برای ارائه تعدادی از وظایف مدیریت شبکه ازجمله پیکربندی، اقدامات امنیتی و نظارت بر عملکرد و خطاها استفاده می‌کند. سه نسخه از پروتکل مدیریت شبکه ساده وجود دارد که هرکدام ویژگی‌های متفاوتی دارند که نسخه سوم آن با ویژگی‌های امنیتی بیشتری طراحی‌شده است و امن‌ترین نسخه این پروتکل محسوب می‌شود.

۳-۳. یادگیری ماشین

یادگیری ماشین، فنی برای تجزیه‌وتحلیل داده‌ها است که شامل ساخت و تطبیق مدل‌هایی است که به برنامه‌ها اجازه می‌دهند از طریق تجربه آموزش داده شوند. یادگیری ماشین شامل تولید الگوریتم‌هایی است که مدل‌های خود را برای بهبود توانایی آن‌ها در پیش‌بینی تطبیق می‌دهند [۲۵].

زمانی که یک فن یادگیری ماشین از مجموعه داده برچسب-گذاری شده برای آموزش الگوریتم استفاده می‌کند، یادگیری ماشین نظارتی نامیده می‌شود. دسته‌بندی، نوعی فن یادگیری ماشین نظارتی است که میزان دقت بالای آن سبب می‌شود تا در تعدادی از سامانه های تشخیص نفوذ برای دسته‌بندی ترافیک عادی از ترافیک غیرعادی با میزان موفقیت بالا مورداستفاده قرار گیرد. یادگیری جمعی[1] حوزه‌ای در یادگیری ماشین است که در آن فن‌هایی مطرح‌شده است که به کمک آن‌ها از چندین مدل به‌صورت ترکیبی و هم‌زمان جهت تصمیم‌گیری استفاده می‌شود تا توان مدل در تخمین خروجی داده بالا برده شود.

در مدل‌های یادگیری ماشین ترکیبی یا مدل‌های جمعی، چندین مدل یادگیری‌های ضعیف[2] یا مدل‌های پایه[3] در حل یک مسئله برای دستیابی به نتایج مطلوب باهم ترکیب و آموزش‌داده‌شده می‌شوند. زمانی که مدل‌های ضعیف به‌صورت مناسب با یکدیگر ترکیب شوند مدل‌های دقیق‌تری می‌تواند تولید شود. در مدل‌های یادگیری ماشین جمعی، انتخاب مدل‌های پایه در دستیابی به نتایج مناسب بسیار حائز اهمیت است. انتخاب این مدل‌ها به متغیرهای زیادی ازجمله مقادیر داده‌ها، فرضیه توزیع داده‌ها و ابعاد داده‌ها وابسته است. بایاس[4] کم و واریانس[5] کم، دو ویژگی اساسی و بااهمیت برای داشتن مدلی مناسب هستند.

در روش‌های یادگیری ماشین جمعی، اجزای سازنده (مدل-های پایه) با یکدیگر ترکیب می‌شوند تا مدل‌های پیچیده‌تری ایجاد کنند. در اغلب اوقات مدل‌های پایه به‌تنهایی عملکرد خوبی ندارند؛ زیرا بایاس یا واریانس بالا دارند.

در روش یادگیری ماشین جمعی، برای ایجاد یک مدل، ابتدا مدل‌های پایه انتخاب می‌شود. در بسیاری از موارد از یک مدل یادگیری پایه یکتا استفاده می‌شود، بنابراین تعدادی مدل پایه یکسان وجود دارد و با روش‌های مختلف آموزش داده می‌شوند که به آن مدل‌های جمعی همگون[6] [۲۶] می‌گویند. در روش دیگر، انواع مختلفی از مدل‌های یادگیری پایه استفاده می‌شود که به مدل‌های جمعی ناهمگون[7] موسوم هستند. نکته مهم در انتخاب مدل‌های پایه، ترکیب منطقی و منسجم[8] با یکدیگر است؛ یعنی اگر مدل پایه‌ای با بایاس کم و واریانس بالا انتخاب شود، باید از یک روش جمعی که تمایل به کاهش واریانس دارد استفاده شود، درحالی‌که اگر مدل‌های پایه با واریانس کم و بایاس بالا انتخاب شود، باید از روشی که تمایل به کاهش بایاس دارد، استفاده شود. سه روش کلی برای ترکیب مدل‌های پایه وجود دارد:

- روش بسته‌بندی[9]: در این روش از مدل‌های پایه همگون استفاده می‌شود، آموزش مدل‌ها به‌صورت مستقل از یکدیگر و به حالت موازی است و برای ترکیب مدل‌ها با یکدیگر از فرآیند میانگین‌گیری قطعی[10] استفاده می‌شود. الگوریتم جنگل تصادفی[11] نمونه‌ای از این دسته است.
- روش تقویتی[12]: در این روش نیز همانند روش بسته‌بندی مدل‌های پایه همگون مورداستفاده قرار می‌گیرد و به‌صورت دنباله‌ای و با یک روش تطبیقی[13] آموزش داده می‌شوند (یک مدل پایه وابسته به مدل قبل از خود است) و با یک استراتژی قطعی ترکیب می‌شوند. الگوریتم آدابوست[14] نمونه‌ای از این دسته است.
- روش پشته‌سازی[15]: این روش از مدل‌های پایه ناهمگون استفاده می‌کند که آموزش به‌صورت موازی بوده و با آموزش یک متامدل[16] بر روی خروجی‌های پیش‌بینی‌شده مدل‌های

[1] Ensemble learning
[2] Weak learner
[3] Base models
[4] Bias
[5] Variance

[6] Homogenous
[7] Heterogeneous
[8] Coherent
[9] Bagging
[10] Deterministic averaging process
[11] Random Forest
[12] Boosting
[13] Adaptive
[14] AdaBoost
[15] Stacking
[16] Meta-Model

پایه، ترکیب می‌شوند. برای نمونه، در یک مسئله دسته‌بندی می‌توان از یک دسته‌بند کای نزدیک‌ترین همسایه[1]، یک درخت تصمیم[2] و یک شبکه عصبی[3] به‌عنوان مدل‌های پایه استفاده کرده و یک شبکه عصبی را به‌عنوان متامدل به کار گرفت. ورودی شبکه عصبی، خروجی سه مدل پایه بوده و پیش‌بینی نهایی بر اساس نتایج شبکه عصبی انجام می‌شود.

روش‌های بسته‌بندی برای ایجاد مدل‌های جمعی با واریانس کمتر نسبت به مدل‌های پایه خود، تمرکز دارند. ولی روش‌های تقویتی و پشته‌سازی تلاش می‌کنند تا مدلی قوی‌تر با میزان بایاس کمتر نسبت به مدل‌های پایه خود ایجاد کنند که امکان کاهش میزان واریانس نیز وجود دارد.

۴. روش پیشنهادی

روش پیشنهادی از روش یادگیری جمعی رأی‌گیری برای بهبود دقت و صحت در تشخیص حملات انکار سرویس استفاده می‌کند. روش پیشنهادی در سه مرحله کار می‌کند. همان‌طور که در مقدمه نیز اشاره شد، مدل پیشنهادی شامل مرحله پیش‌پردازش داده‌ها، مرحله انتخاب و کاهش ویژگی و درنهایت مرحله پیش-بینی و تشخیص حملات است. چارچوب مدل پیشنهادی در زیر بخش‌های بعدی موردبحث قرار می‌گیرد. مدل پیشنهادی در شکل (۴) نشان‌داده‌شده است.

روش‌های پیش‌پردازش داده که در ادامه معرفی می‌شوند، جهت تولید داده برای الگوریتم‌های یادگیری ماشین، می‌توانند روی مجموعه داده اعمال شوند. این روش‌ها عبارت‌اند از:

- مقیاس‌بندی[4]: مجموعه داده استفاده‌شده از ویژگی‌هایی با مقیاس متغیر تشکیل‌شده است، اما نمی‌توان چنین داده‌ای به الگوریتم یادگیری ماشین داد، چون به مقیاس‌بندی مجدد نیاز خواهد داشت. مقیاس‌بندی مجدد داده، این تضمین را به وجود می‌آورد که ویژگی‌ها در مقیاس مشابه قرار گیرند و ویژگی‌ها در بازه بین صفر و یک مجدداً مقیاس‌بندی می‌شوند. مقیاس‌بندی بر اساس سه روش زیر انجام می‌پذیرد:

  ۱- مقیاس‌بندی مینیمم - ماکزیمم[5]

  ۲- مقیاس‌بندی استاندارد[6]

  ۳- مقیاس‌بندی منسجم[7]

- عادی‌سازی[8]: از عادی‌سازی برای مقیاس‌بندی هر سطر از داده، برای اینکه دارای طول یک باشد، استفاده می‌شود. این روش اساساً برای مجموعه داده‌های پراکنده[9] که در آن تعداد صفر زیادی داریم مفید است.
- استانداردسازی[10]: برای تبدیل ویژگی‌های داده توسط یک توزیع گوسی[11] استفاده می‌شود. این روش میانگین و انحراف از معیار[12] را به یک توزیع گوسی استاندارد با میانگین صفر و یک تبدیل می‌کند.

در مدل پیشنهادی یادگیری جمعی رأی‌گیری، در مرحله پیش‌پردازش، داده‌های ناقص در مجموعه داده MIP-SNMP بررسی و حذف‌شده و همچنین با روش مقیاس‌بندی مینیمم - ماکزیمم با کمک کلاس MinMaxScaler از کتابخانه پایتون scikit-learn، داده‌ها مقیاس‌بندی مجدد می‌شود. در این روش مقیاس‌بندی ویژگی، مقیاس ویژگی‌ها بین صفر تا یک تنظیم می‌شود که با رابطه (۱) قابل‌محاسبه است [۲۵]:

$$x' = \frac{x - min(x)}{max(x) - min(x)} \qquad (۰)$$

با این روش، همه داده‌های یک ویژگی در مجموعه داده، بین صفر و یک تنظیم می‌شوند. در مرحله انتخاب و کاهش ویژگی از زیرمجموعه داده واسط و متغیرهای این گروه بجای استفاده از تمامی ویژگی‌ها و متغیرهای مجموعه داده استفاده می‌شود؛ چون این ویژگی‌ها میزان همبستگی[13] بالایی نسبت به سایر ویژگی‌ها در مرحله انتخاب ویژگی از خود نشان داده‌اند. ویژگی‌هایی که بر اساس ماتریس همبستگی به‌عنوان ویژگی‌های برتر انتخاب می‌شوند، بسته به مقدار ضریب همبستگی و معیاری که برای بررسی همبستگی استفاده می‌شود، متفاوت است [۲۸]. در ادامه به برخی از معیارهای معمول برای بررسی همبستگی ویژگی‌ها در راستای انتخاب ویژگی‌های برتر، اشاره می‌شود.

- ضریب همبستگی پیرسون[14]: در این معیار، ضریب همبستگی پیرسون بین هر دو ویژگی محاسبه می‌شود که مقدار آن بین ۱- تا ۱ است. ویژگی‌هایی که ضریب همبستگی پایین دارند (نزدیک به صفر)، باهم هیچ همبستگی معناداری ندارند. ویژگی‌هایی که ضریب همبستگی بالا دارند (مثبت یا منفی)،

[1] K-Nearest neighbor (KNN)
[2] Decision Tree (DT)
[3] Neural Network (NN)
[4] Scaling
[5] Min Max Scaling
[6] Standard Scaling
[7] Robust Scaling
[8] Normalization
[9] Sparse
[10] Standardization
[11] Gaussian distribution
[12] Standard Deviation
[13] Correlation
[14] Pearson Correlation Coefficient

باهم همبستگی معنادار دارند. ویژگی هایی که ضریب همبستگی با مقدار بیشتر از ۱ یا کمتر از ۱- دارند، وجود خطا در داده ها را نشان می‌دهند [۲۸].

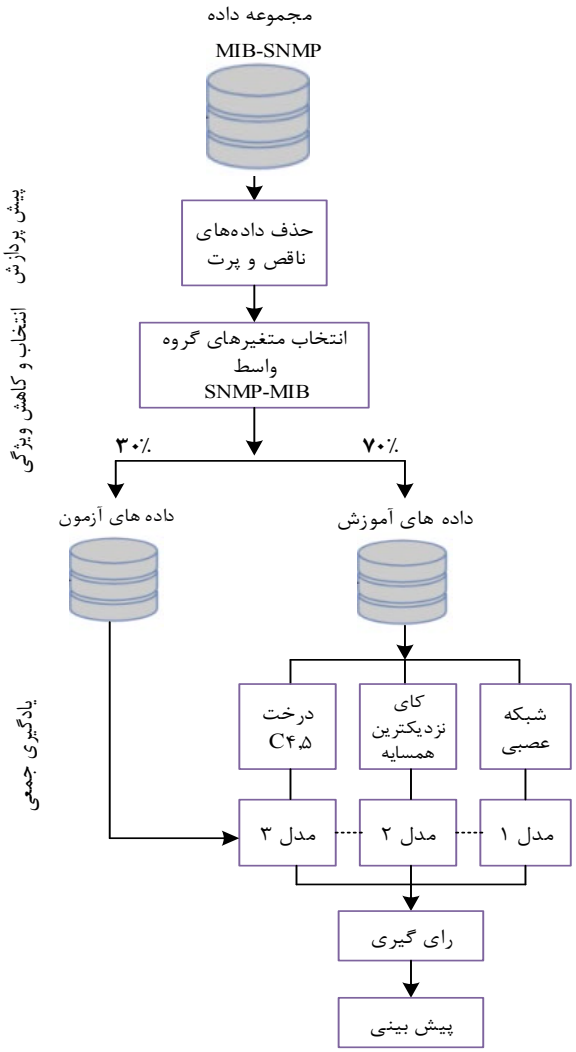
- ضریب همبستگی رتبه اسپیرمن[1]: در این معیار، ضریب همبستگی بین هر دو ویژگی محاسبه می شود. این معیار برای داده‌هایی با توزیع نامنظم استفاده می‌شود. ویژگی‌هایی که ضریب همبستگی رتبه اسپیرمن بالا دارند، باهم همبستگی معنادار دارند [۲۸].
- اندازهٔ همبستگی: در این معیار، برای هر ویژگی، مجموع مقادیر مطلق ضرایب همبستگی آن با دیگر ویژگی‌ها محاسبه شده و ویژگی‌هایی که بیشترین مجموع را دارند، به‌عنوان ویژگی‌های برتر شناخته می‌شوند؛ چراکه با دیگر ویژگی‌ها بیشترین همبستگی را دارند [۲۸].

در کل، انتخاب ویژگی های برتر بر اساس ماتریس همبستگی بسته به نوع داده، معیارهای بررسی همبستگی و هدف موردنظر ممکن است متفاوت باشد. در این مقاله از روش همبستگی پیرسون به دلیل سادگی پیاده‌سازی استفاده‌شده است. در بخش ۵-۲ ضرایب همبستگی تمامی ویژگی‌ها با ویژگی کلاس و برچسب مجموعه داده محاسبه و ارائه‌شده است.

تقسیم‌بندی داده‌ها برای مرحله آموزش به میزان ۷۰ درصد از داده‌ها و ۳۰ درصد باقی‌مانده برای مرحله آزمایش انجام می‌شود. استفاده از روش‌های یادگیری جمعی ازجمله روش رأی‌گیری با توجه به استفاده از چندین روش یادگیری ماشین تکی، می‌توانند بر مسائلی ازجمله بایاس و واریانس بالا فائق آیند و دقت بالایی نسبت به استفاده تک ماشین یادگیری ارائه دهند. ترکیب‌های متفاوتی با تعداد متنوع از الگوریتم‌ها و روش‌ها برای ایجاد یک روش جمعی رأی‌گیری می‌توان انتخاب کرد. در این مقاله، با توجه به انجام آزمایش‌های متعدد و انتخاب الگوریتم‌های مختلف یادگیری، به دلیل به‌دست‌آمدن میزان دقت بالا توسط سه الگوریتم یادگیری شبکه عصبی (تعداد هشت گره ورودی برابر با تعداد ویژگی‌های واسط و استفاده از یک‌لایه مخفی[2]، نرخ یادگیری ۰/۳ و تابع فعال‌سازی سیگمید[3] با تعداد ۵۰۰ تکرار)، کای نزدیک‌ترین همسایه و درخت تصمیم C4.5 که در شکل (۴) نشان‌داده‌شده است از این الگوریتم‌ها در مرحله یادگیری استفاده می‌شود و سه مدل تولیدشده و داده‌های آزمایش به‌عنوان ورودی به این مدل‌ها واردشده و نهایتاً با استفاده از روش یادگیری جمعی رأی‌گیری نتایج سه مدل، بررسی و با روش حداکثر رأی‌گیری[4] یا همان انتخاب رأی بیش از دو ماشین یادگیر، پیش‌بینی ترافیک حمله یا عادی بادقت بالا انجام می‌شود.

۵. نتایج و اعتبارسنجی

آزمایش‌های پیاده‌سازی شده در این مقاله باهدف آزمایش تعدادی از حملات رایج سیل‌آسای انکار سرویس توسط روش پیشنهادی و تعدادی از طبقه‌بندی‌کننده‌های یادگیری ماشین مطرح بکار گرفته‌شده در سامانه‌های تشخیص نفوذ انجام‌شده است.



شکل ۴. مدل پیشنهادی

۵-۱. جزئیات پیاده‌سازی

دستگاهی با پردازنده اینتل Core i7-2670QM با سرعت ۲/۲ گیگاهرتز، حافظه اصلی ۸ گیگابایت، کارت گرافیکی انویدیا جیفورس ۵۴۰ با ۲ گیگابایت حافظه و سیستم‌عامل ویندوز ۷ (۶۴

[1] Spearman Rank Correlation Coefficient
[2] Hidden Layer
[3] Sigmoid
[4] Max-Voting

بیتی) برای انجام آزمایش‌ها مورداستفاده قرارگرفته است. الگوریتم شبکه عصبی و طبقه‌بندی‌کننده‌های یادگیری ماشین با استفاده از زبان برنامه‌نویسی پایتون نسخه ۳/۸ در محیط ژوپیتر نوت بوک [۲۶] پیاده‌سازی و آموزش‌داده‌شده است. آزمایش‌های مختلفی برای تعیین پارامترهای تنظیم مطلوب برای این طبقه‌بندی‌کننده‌ها انجام‌شده است.

۵-۲. مجموعه داده

در این مقاله از مجموعه داده SNMP-MIB [۱۲] استفاده‌شده است که این مجموعه داده دارای ۳۴ ویژگی و ۴۹۹۸ رکورد ترافیکی شبکه است و که پنج گروه در جدول (۱) و در ۸ دسته ترافیک عادی و حمله در جدول (۲) ارائه‌شده، تقسیم‌بندی شده است.

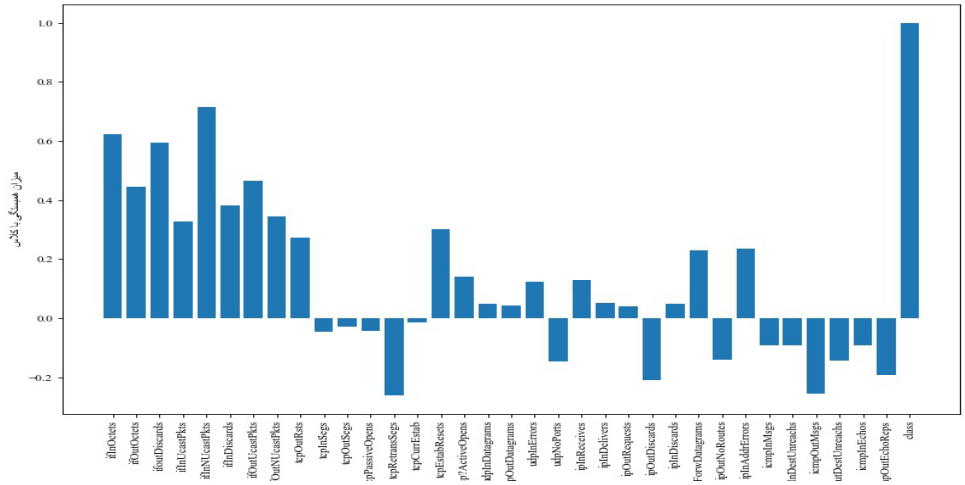
در این مقاله با توجه به‌سهولت پیاده‌سازی، روش همبستگی پیرسون برای محاسبه ضرایب همبستگی تمامی ویژگی‌ها با ویژگی برچسب و کلاس مجموعه داده استفاده‌شده است که میزان ضرایب در شکل (۵) ارائه‌شده است. با توجه به بالابودن میزان همبستگی تمامی ویژگی‌های واسط مجموعه داده، این گروه از ویژگی‌ها که از خصوصیات مرتبط با بسته‌های ردوبدل شده در شبکه استخراج‌شده‌اند انتخاب‌شده‌اند. شایان‌ذکر است که برخی دیگر از ویژگی‌های همچون tcpEstabResets یا tcpRetransSegs نیز میزان همبستگی خوبی با ویژگی کلاس دارند؛ ولی در این مقاله با توجه به انتخاب ویژگی‌ها و پیاده‌سازی روش پیشنهادی بر روی ویژگی‌های واسط مشخص شد این داده‌ها می‌توانند در شناسایی حملات ترافیکی شبکه نسبت به سایر ویژگی‌ها و ترکیب‌های مختلف عملکرد بهتری داشته باشند.

جدول ۱. رکوردهای ترافیک شبکه در مجموعه داده SNMP-MIB

ردیف	نوع ترافیک	زیر نوع	تعداد رکوردها
۱	عادی	Normal	۶۰۰
۲	حمله انکار سرویس	TCP-SYN	۹۶۰
۳		UDP-flood	۷۷۳
۴		ICMP-ECHO	۶۳۲
۵		HTTP-flood	۵۷۳
۶		Slowloris	۷۸۰
۷		Slowpost	۴۸۰
۸	حمله	Brute Force	۲۰۰
مجموع			۴۹۹۸

جدول ۲. مجموعه داده SNMP-MIB

گروه واسط (Interface)	گروه UDP	گروه ICMP	گروه TCP	گروهIP
ifInOctets	udpInDatagrams	icmpInMsgs	tcpOutRsts	ipInReceives
ifOutOctets	udpOutDatagrams	icmpInDestUnreachs	tcpInSeg	ipInDelivers
ifoutDiscards	udpInErrors	icmpOutMsgs	tcpOutSegs	ipOutRequests
ifInUcastPkts	udpNoPorts	icmpOutDestUnreachs	tcpPassiveOpens	ipOutDiscards
ifInNUcastPkts	–	icmpInEchos	tcpRetransSegs	ipInDiscards
ifInDiscards	–	icmpOutEchoReps	tcpCurrEstab	ipForwDatagrams
ifOutUcastPkts	–	–	tcpEstabResets	ipOutNoRoutes
ifOutNUcastPkts	–	–	tcpActiveOpens	ipInAddrErrors



شکل ۵. ضریب همبستگی ویژگی‌ها با ویژگی کلاس مجموعه داده

۵-۳. ارزیابی عملکرد و نتایج

برای ارزیابی روش رأی‌گیری پیشنهادی و طبقه‌بندی‌کننده‌های دیگر از روش اعتبارسنجی متقابل[1] با K-fold=۵ استفاده شد. با این روش میزان عملکرد روش ارائه‌شده به‌صورت دقیق‌تر مورد ارزیابی قرار گرفت. میانگین نتایج، با ۲۰ بار آزمایش بر روی مجموعه داده محاسبه‌شده و برای روش پیشنهادی و طبقه‌بندی‌کننده‌های دیگر ارائه‌شده است.

۵-۳-۱. سنجه‌های ارزیابی

ارزیابی کارایی[2] از مهم‌ترین مراحل پس از ساخت مدل است. در طبقه‌بندی‌کننده‌های یادگیری ماشین برای ارزیابی عملکرد هر یک از آن‌ها، سنجه‌هایی ازجمله نرخ صحت[3]، نرخ تشخیص[4] یا نرخ بازخوانی[5]، نرخ هشدار نادرست[6] استفاده می‌شود. این سنجه‌ها توسط عناصر ماتریس آشفتگی[7] تعیین می‌شوند که در جدول (۳) نمایش‌داده‌شده و در ادامه نحوه محاسبه هریک از آن‌ها بررسی‌شده است [۲۵].

جدول ۳. ماتریس آشفتگی با دو کلاس

	کلاس پیش‌بینی‌شده[8]		
		مثبت	کاذب
کلاس واقعی[9]	مثبت	مثبت درست (TP)	مثبت کاذب (FP)
	کاذب	منفی کاذب (FN)	منفی درست (TN)

- مثبت درست (TP): تعداد نمونه‌های حمله که به‌درستی به‌عنوان نمونه‌های حمله و مخرب تشخیص داده می‌شوند.
- مثبت کاذب (FP): تعداد نمونه‌های عادی که به‌اشتباه به‌عنوان نمونه‌های حمله تشخیص داده می‌شوند.
- منفی درست (TN): تعداد نمونه‌های عادی که به‌درستی به‌عنوان نمونه‌های عادی تشخیص داده می‌شوند.
- منفی کاذب (FN): تعداد نمونه‌های حمله که به‌اشتباه به‌عنوان نمونه‌های عادی تشخیص داده می‌شوند.

✓ **صحت:** میزان پیش‌بینی‌های صحیح تمام نمونه‌ها را نشان می‌دهد [۲۵]

$$Accuracy\left(ACC\right)=\frac{TP+TN}{TP+TN+FP+FN} \quad (۰)$$

✓ **دقت:** میزان نمونه‌های عادی که به‌درستی به‌عنوان نمونه عادی طبقه‌بندی‌شده‌اند را نشان می‌دهد [۲۵].

$$Precision=\frac{TP}{TP+FP} \quad (۰)$$

✓ **نرخ تشخیص یا نرخ بازخوانی:** میزان نمونه‌های حمله‌ای است که به‌درستی به‌عنوان یک نمونه حمله پیش‌بینی‌شده است [۲۵].

$$Recall\ or\ True\ Posetive\ Rate\left(TPR\right)=\frac{TP}{TP+FN} \quad (۰)$$

✓ **میانگین هارمونی:** سنجه‌ای برای اندازه‌گیری دقت آزمون انجام‌شده است. برای محاسبه این سنجه از دو سنجه بازخوانی و دقت آزمون استفاده می‌شود [۲۵].

$$F\text{-}Measure\ or\ F1=\frac{2*\left(Precision*Recall\right)}{Precision+Recall} \quad (۰)$$

✓ **نرخ هشدار نادرست:** میزان نمونه‌های عادی که به‌اشتباه به‌عنوان نمونه حمله طبقه‌بندی‌شده‌اند را نشان می‌دهد [۲۵].

[1] Cross Validation (CV)
[2] Performance Evaluation
[3] Accuracy
[4] True Positive Rate (TPR) or Detection Rate
[5] Recall
[6] False Alarm Rate (FAR)
[7] Confusion Matrix
[8] Predicted Class
[9] Actual Class

$$FAR = \frac{FP}{FP + TN} \quad (۰)$$

۵-۳-۲. نتایج

برای بررسی دلیل به‌کارگیری روش رأی‌گیری استفاده‌شده، ترکیب روش پیشنهادی رأی‌گیری با برخی از ترکیبات دیگر مقایسه شده است که در جدول (۴) ازنظر صحت مورد ارزیابی قرارگرفته است. نتایج نشان می‌دهد که ترکیب طبقه‌بندی درخت تصمیم C4.5، کای نزدیک‌ترین همسایه و شبکه عصبی، میزان صحت بالاتری را نسبت به سایر ترکیب‌ها نشان می‌دهد. برای شبکه عصبی از تعداد ۸ گره ورودی که بیانگر تعداد ویژگی‌های واسط از مجموعه داده است استفاده‌شده و یک‌لایه مخفی مابین لایه ورودی و لایه خروجی در نظر گرفته‌شده است. نرخ یادگیری شبکه عصبی برابر با ۰/۳ و تابع فعال‌سازی سیگمید برای لایه آخر با دو گره (عادی بودن ترافیک یا حمله) در نظر گرفته‌شده است. همچنین تعداد تکرار ۵۰۰ برای آموزش شبکه عصبی استفاده‌شده است.

در جدول (۵) معیارهای ارزیابی با استفاده از روش پیشنهادی و روش‌های ارائه‌شده در مقالات الحیدری و همکاران [۱۱] و راجاسکار و همکاران [۲۳] نشان‌داده‌شده است. در آزمایش‌های انجام‌شده ابتدا بدون درنظرگرفتن مرحله کاهش ویژگی‌ها، تمامی ۳۴ ویژگی مجموعه داده، انتخاب‌شده و نتایج بر اساس آن‌ها در جداول (۶) تا (۸) ارائه‌شده است.

جدول ۴. مقایسه روش‌های مختلف رأی‌گیری برای انتخاب مدل پیشنهادی بر اساس میزان صحت

روش / معیارهای ارزیابی	صحت
روش رأی‌گیری ۱ (درخت تصمیم، کای نزدیک‌ترین همسایه و ماشین بردار پشتیبان)	۹۹/۸۷ ± ۰/۰۴۹
روش رأی‌گیری ۲ (درخت تصمیم، کای نزدیک‌ترین همسایه و جنگل تصادفی)	۹۹/۹۱ ±۰/۰۱۷
روش رأی‌گیری ۳ (جنگل تصادفی، کای نزدیک‌ترین همسایه و شبکه بیزی)	۹۸/۹۲ ±۰/۱۳۶
روش رأی‌گیری ۴ (جنگل تصادفی، شبکه عصبی و شبکه بیزی)	۹۹/۰۲ ±۰/۳۷۱
روش رأی‌گیری ۵ (جنگل تصادفی، ماشین بردار پشتیبان و شبکه عصبی)	۹۹/۹۰ ±۰/۰۲۲
روش رأی‌گیری ۶ (جنگل تصادفی، ماشین بردار پشتیبان و شبکه بیزی)	۹۹/۶۷ ±۰/۰۹۳
روش رأی‌گیری پیشنهادی (درخت تصمیم، کای نزدیک‌ترین همسایه و شبکه عصبی)	۹۹/۹۴ ±۰/۰۱۴

جدول ۵. مقایسه معیارهای ارزیابی روش‌های مختلف با روش رأی‌گیری پیشنهادی

روش / معیارهای ارزیابی	مرجع [۱۱]			مرجع [۲۳]	
	آدابوست	جنگل تصادفی	پرسپترون چندلایه	GRU-BWFA	روش رأی‌گیری
صحت	۹۹/۵۷	۹۹/۹۱	۹۸/۸۱	۹۹/۹۷	۹۹/۹۴ ±۰/۰۲
دقت	۹۹/۶۴	۹۹/۹۸	۹۷/۸۵	۹۹/۹۶	۹۹/۹۹ ±۰/۰۱
بازخوانی	۹۹/۷۵	۹۹/۹۵	۹۸/۷۹	۹۹/۹۹	۹۹/۹۹ ±۰/۰۱
معیار هارمونی	۹۹/۶۹	۹۹/۹۶	۹۸/۳۲	۹۹/۹۷	۹۹/۹۹ ±۰/۰۱
نرخ هشدار نادرست	۰/۵۱ ±۰/۰۹	۰/۳۲ ±۰/۲۳	۰/۹۳ ±۰/۱۴	--	۰/۱۲ ±۰/۰۳

جدول ۶. مقایسه میزان دقت روش‌های مختلف بر اساس ترافیک موجود در مجموعه داده با تمامی ویژگی‌ها

مرجع	ترافیک / روش	Noraml	TCP-SYN	UDP Flood	ICMP ECHO	HTTP Flood	Slowloris	Slowpost	Bruteforce
[۱۱]	آدابوست	۹۹/۸۲	۱۰۰	۹۷.۸۵	۹۹/۹۲	۱۰۰	۹۹/۸	۹۹/۹	۱۰۰
	جنگل تصادفی	۹۹/۸	۹۹/۹	۹۹/۹	۱۰۰	۱۰۰	۹۹/۷	۱۰۰	۱۰۰
	پرسپترون چندلایه	۹۹/۷۶	۹۹/۵۶	۹۹/۴۶	۹۹/۵۶	۱۰۰	۹۹/۲۱	۹۹/۷۹	۸۸/۰۰
[۲۳]	GRU-BWFA	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰
	روش رأی‌گیری	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰

جدول ۷. مقایسه میزان بازخوانی روش‌های مختلف بر اساس ترافیک موجود در مجموعه داده با تمامی ویژگی‌ها

مرجع	ترافیک / روش	Noraml	TCP-SYN	UDP Flood	ICMP ECHO	HTTP Flood	Slowloris	Slowpost	Bruteforce
[۱۱]	آدابوست	۹۹/۹۸	۹۸/۰۰	۹۷/۸۵	۹۹/۹	۹۹/۴۸	۹۸/۸۴	۹۹/۸۶	۱۰۰
	جنگل تصادفی	۹۹/۹	۹۹/۸۸	۹۹/۸۸	۹۹/۷	۹۹/۷	۹۹/۹۴	۱۰۰	۱۰۰
	پرسپترون چندلایه	۹۹/۸۶	۹۹/۵۶	۹۹/۴۶	۹۹/۵۶	۹۹/۵۶	۹۸/۸۵	۹۹/۷۹	۹۸/۰۰
[۲۳]	GRU-BWFA	۹۹/۹۶	۹۹/۹۶	۹۹/۹۶	۹۹/۷	۹۹/۷	۱۰۰	۱۰۰	۱۰۰
	روش رأی‌گیری	۱۰۰	۹۹/۹۶	۱۰۰	۹۹/۷۸	۹۹/۷۸	۱۰۰	۹۹/۹۲	۱۰۰

با درنظرگرفتن تمامی ۳۴ ویژگی مجموعه داده، نتایج به‌دست‌آمده از جدول (۶) نشان می‌دهد که دقت روش پیشنهادی در تشخیص تمامی حملات و همچنین تشخیص ترافیک عادی، ۱۰۰ درصد موفق عمل کرده است و همچنین روش GRU-BWFA [۲۳] نیز عملکرد ۱۰۰ درصدی در دقت تشخیص از خود نشان داده است.

با درنظرگرفتن تمامی ویژگی‌های مجموعه داده، با توجه به نتایج جدول (۷)، میزان سنجه بازخوانی روش پیشنهادی در تشخیص حملات UDP Flood، Slowloris، Bruteforce و همچنین تشخیص ترافیک عادی، برابر با ۱۰۰ درصد بوده است و میزان بازخوانی نسبت به روش GRU-BWFA [۲۳] درمجموع بهتر عمل کرده و تنها در تشخیص حمله Slowpos به میزان ۰/۰۸ درصد عملکرد ضعیفت تری داشته است. با درنظرگرفتن موارد و اینکه سنجه میانگین هارمونی از سنجه‌های دقت و بازخوانی محاسبه می‌شود میزان میانگین هارمونی ارائه‌شده در جدول (۸) نیز بیانگر بالا بودن میزان تشخیص حملات انکار سرویس و همچنین میزان تشخیص ترافیک عادی نسبت به سایر روش‌های مطرح‌شده در مقاله است.

جدول ۸. مقایسه میزان میانگین هارمونی روش‌های مختلف بر اساس ترافیک موجود در مجموعه داده با تمامی ویژگی‌ها

مرجع	ترافیک / روش	Noraml	TCP-SYN	UDP Flood	ICMP ECHO	HTTP Flood	Slowloris	Slowpost	Bruteforce
[۱۱]	آدابوست	۹۹/۹۰	۹۹/۰۰	۹۷/۸۵	۹۹/۹۱	۹۹/۷۴	۹۹/۳۲	۹۹/۸۸	۱۰۰
	جنگل تصادفی	۹۹/۸۵	۹۹/۸۹	۹۹/۸۹	۹۹/۸۹	۹۹/۸۵	۹۹/۸۵	۱۰۰	۱۰۰
	پرسپترون چندلایه	۹۹/۸۱	۹۹/۵۶	۹۹/۴۶	۹۹/۵۶	۹۹/۷۸	۹۹/۰۳	۹۹/۷۹	۹۲/۷۴
[۲۳]	GRU-BWFA	۹۹/۹۸	۹۹/۹۸	۹۹/۹۸	۹۹/۹۸	۹۹/۸۵	۱۰۰	۱۰۰	۱۰۰
	روش رأی‌گیری	۱۰۰	۹۹/۹۸	۱۰۰	۱۰۰	۹۹/۸۹	۱۰۰	۹۹/۹۶	۱۰۰

در ادامه نتایج آزمایش‌ها بر اساس ویژگی‌های انتخاب‌شده (ویژگی‌های واسط SNMP-MIB) از مجموعه داده بر اساس روش‌های مختلف ارائه می‌شود. جداول (۹) تا (۱۱) و همچنین شکل‌های (۶) تا (۹)، نتایج حاصل از عملکرد روش پیشنهادی و روش‌های ارائه‌شده در مراجع [۱۱] و [۲۳] را در سه سنجه دقت، بازخوانی و میانگین هارمونی نشان می‌دهند.

جدول ۹. مقایسه میزان دقت روش‌های مختلف بر اساس ترافیک موجود در مجموعه داده با ویژگی‌های واسط

مرجع	ترافیک / روش	Noraml	TCP-SYN	UDP Flood	ICMP ECHO	HTTP Flood	Slowloris	Slowpost	Bruteforce
[۱۱]	آدابوست	۱۰۰	۱۰۰	۹۷/۳۴	۹۹/۸۷	۱۰۰	۱۰۰	۹۹/۹۳	۱۰۰
	جنگل تصادفی	۱۰۰	۱۰۰	۹۹/۸۶	۱۰۰	۱۰۰	۱۰۰	۹۹/۹۴	۱۰۰
	پرسپترون چندلایه	۱۰۰	۹۸/۱۳	۹۸/۶۷	۹۸/۱۷	۱۰۰	۹۸/۷۲	۹۹/۳۲	۸۹/۷۶
[۲۳]	GRU-BWFA	۱۰۰	۹۹/۸۷	۹۹/۹۱	۹۹/۸۹	۱۰۰	۱۰۰	۱۰۰	۱۰۰
	روش رأی‌گیری	۱۰۰	۱۰۰	۹۹/۹۴	۱۰۰	۱۰۰	۱۰۰	۹۹/۹۷	۱۰۰

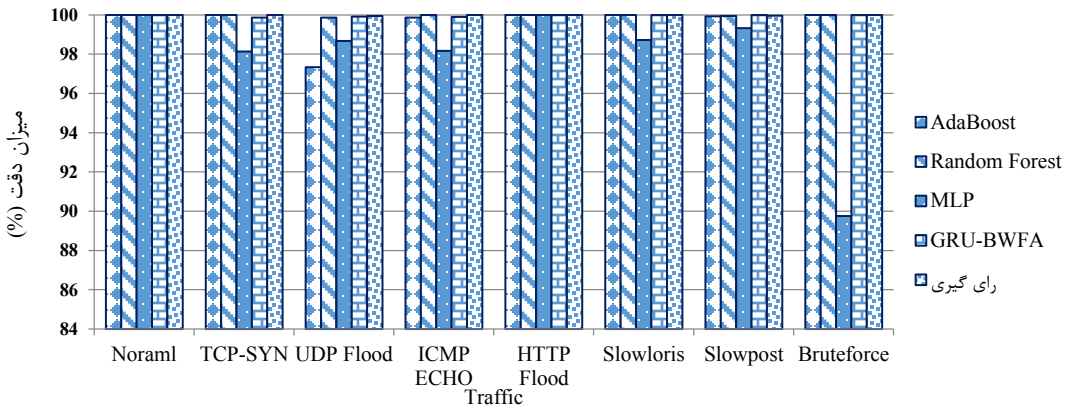
جدول ۱۰. مقایسه میزان بازخوانی روش‌های مختلف بر اساس ترافیک موجود در مجموعه داده با ویژگی‌های واسط

مرجع	ترافیک / روش	Noraml	TCP-SYN	UDP Flood	ICMP ECHO	HTTP Flood	Slowloris	Slowpost	Bruteforce
[۱۱]	آدابوست	۱۰۰	۹۸/۴۱	۱۰۰	۹۹/۵۷	۱۰۰	۱۰۰	۱۰۰	۱۰۰
	جنگل تصادفی	۱۰۰	۱۰۰	۱۰۰	۹۹/۵۹	۱۰۰	۱۰۰	۱۰۰	۱۰۰
	پرسپترون چندلایه	۱۰۰	۹۹/۹۸	۹۹/۴۹	۹۵/۶۰	۹۸/۰۱	۹۹/۹۹	۱۰۰	۹۷/۲۷
[۲۳]	GRU-BWFA	۱۰۰	۱۰۰	۱۰۰	۹۹/۸۹	۱۰۰	۱۰۰	۱۰۰	۱۰۰
	روش رأی‌گیری	۱۰۰	۱۰۰	۱۰۰	۹۹/۹۱	۱۰۰	۱۰۰	۹۹/۹۸	۱۰۰

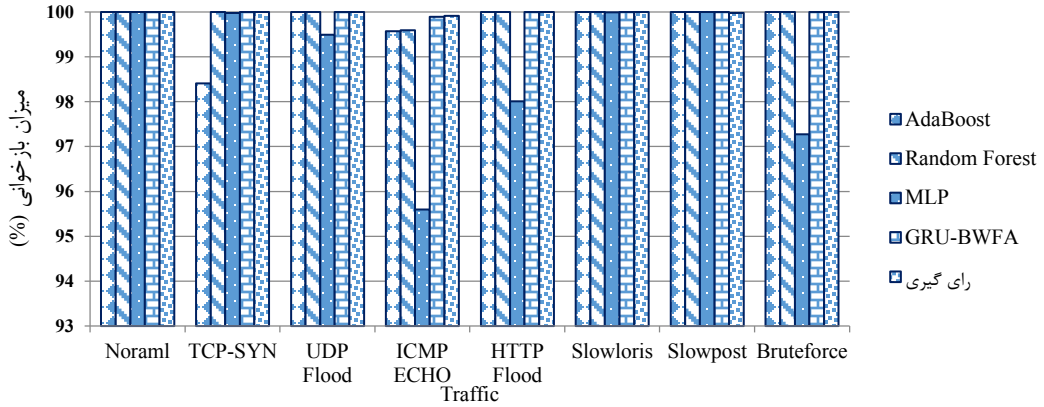
جدول ۱۱. مقایسه میزان میانگین هارمونی روش‌های مختلف بر اساس ترافیک موجود در مجموعه داده با ویژگی‌های واسط

مرجع	ترافیک / روش	Noraml	TCP-SYN	UDP Flood	ICMP ECHO	HTTP Flood	Slowloris	Slowpost	Bruteforce
[۱۱]	آدابوست	۱۰۰	۹۹/۲۰	۹۸/۶۵	۹۹/۷۲	۱۰۰	۱۰۰	۹۹/۹۶	۱۰۰
	جنگل تصادفی	۱۰۰	۱۰۰	۹۹/۹۳	۹۹/۷۹	۱۰۰	۱۰۰	۹۹/۹۷	۱۰۰
	پرسپترون چندلایه	۱۰۰	۹۹/۰۵	۹۹/۰۸	۹۶/۸۷	۹۹/۰۰	۹۹/۳۵	۹۹/۶۶	۹۳/۳۶
[۲۳]	GRU-BWFA	۱۰۰	۹۹/۹۳	۹۹/۹۵	۹۹/۸۹	۱۰۰	۱۰۰	۱۰۰	۱۰۰
	روش رأی‌گیری	۱۰۰	۱۰۰	۹۹/۹۷	۹۹/۹۵	۱۰۰	۱۰۰	۹۹/۹۷	۱۰۰

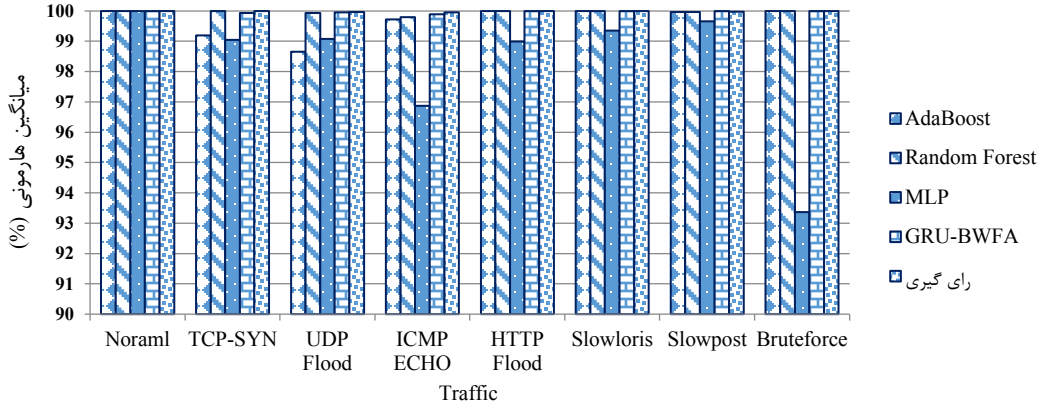
همان‌گونه که در جدول (۹) مشاهده می‌شود میزان دقت به‌دست‌آمده از روش پیشنهادی در تشخیص ترافیک عادی و ترافیک حملات، عملکرد بسیار خوبی نشان داده و به‌جز حملات ارسال انبوه UDP و Slowpost در سایر ترافیک‌ها دقت ۱۰۰ درصدی نشان داده است و تنها در حمله Slowpost میزان دقت کمتری به میزان ۰/۰۳ درصد نسبت به روش GRU-BWFA ارائه داده است. در جدول (۱۰) میزان بازخوانی به‌دست‌آمده از روش پیشنهادی در تشخیص ترافیک عادی و ترافیک حملات نشان داده‌شده است در این سنجه نیز روش پیشنهادی عملکرد خوبی نشان داده و به‌جز حملات Slowpost و ICMP-ECHO در سایر ترافیک‌ها میزان ۱۰۰ درصدی نشان داده است و تنها در حمله Slowpost ۰/۰۲ درصد نسبت به روش GRU-BWFA میزان بازخوانی کمتری داشته است. سنجه میانگین هارمونی، سنجه مناسبی برای ارزیابی مدل‌ها و روش‌های یادگیری ماشین است و در این مقاله نیز میزان این سنجه برای روش پیشنهادی و روش‌های ارائه‌شده در مقالات [۱۱] و [۲۳] محاسبه و در جدول (۱۱) نمایش‌داده‌شده است. در این سنجه روش پیشنهادی در ترافیک عادی و حملات TCP-SYN، HTTP Flood، Slowloris و Bruteforce میزان ۱۰۰ درصدی ارائه داده و در حمله Slowpost ۰/۰۳ درصد نسبت به روش GRU-BWFA مقدار کمتری داشته و در حملات UDP Flood و ICMP ECHO نیز به ترتیب مقادیر ۹۹/۹۷ درصد و ۹۹/۹۵ درصد را ارائه داده است که این مقادیر نیز بیانگر میزان تشخیص بالای این حملات توسط روش پیشنهادی است.



شکل ۶. میزان دقت برای ترافیک عادی و ترافیک حملات در روش پیشنهادی و روش‌های مختلف بر اساس ویژگی‌های واسط



شکل ۷. میزان بازخوانی برای ترافیک عادی و ترافیک حملات در روش پیشنهادی و روش‌های مختلف بر اساس ویژگی‌های واسط



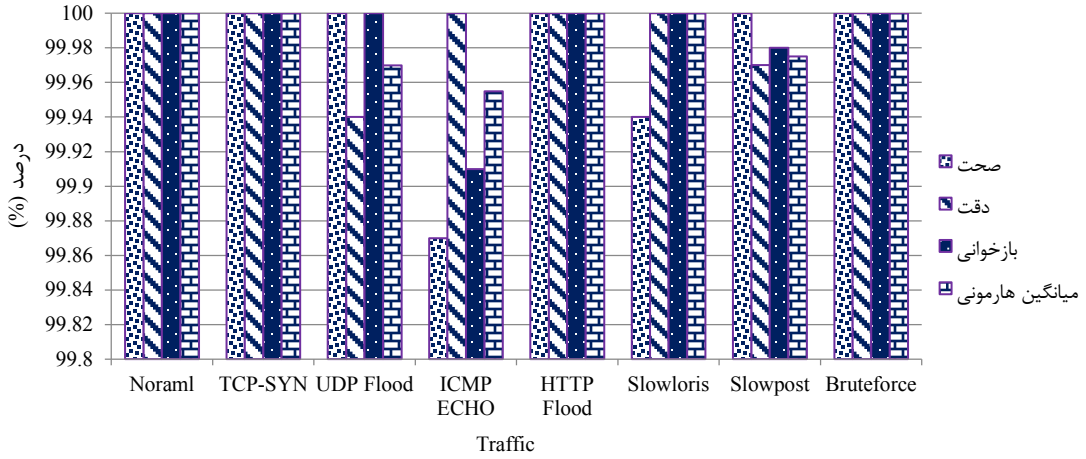
شکل ۸. میزان میانگین هارمونی برای ترافیک عادی و ترافیک حملات در روش پیشنهادی و روش‌های مختلف بر اساس ویژگی‌های واسط

برای مشخص شدن معیارهای ارزیابی بر اساس ترافیک عادی و ترافیک حملات انکار سرویس جدول (۱۲) و شکل (۹) ارائه‌شده است. نتایج نشان می‌دهند که با روش پیشنهادی می‌توان به میزان دقت، بازخوانی و میانگین هارمونی بسیار بالایی نسبت به روش‌های ارائه‌شده توسط الحیدری و همکاران [۱۱] با زمان کمی بیشتر از آن‌ها و میزان دقت، بازخوانی و میانگین هارمونی بالاتری در زمان نسبتاً کمتری نسبت به روش ارائه‌شده توسط راجاسکار و همکاران [۲۳] دست‌یافت که این نتایج بیانگر تأثیرگذار بودن استفاده از روش پیشنهادی در تشخیص ترافیک حمله از ترافیک عادی است.

جدول ۱۲. مقایسه کلی معیارهای ارزیابی روش پیشنهادی بر اساس ترافیک موجود (عادی و حملات) در مجموعه داده با ویژگی‌های واسط

ترافیک / معیارهای ارزیابی	Noraml	TCP-SYN	UDP Flood	ICMP ECHO	HTTP Flood	Slowloris	Slowpost	Bruteforce
صحت	۱۰۰	۱۰۰	۱۰۰	۹۹/۸۷	۱۰۰	۹۹/۹۴	۱۰۰	۱۰۰
دقت	۱۰۰	۱۰۰	۹۹/۹۴	۱۰۰	۱۰۰	۱۰۰	۹۹/۹۷	۱۰۰
بازخوانی	۱۰۰	۱۰۰	۱۰۰	۹۹/۹۱	۱۰۰	۱۰۰	۹۹/۹۸	۱۰۰
میانگین هارمونی	۱۰۰	۱۰۰	۹۹/۹۷	۹۹/۹۵	۱۰۰	۱۰۰	۹۹/۹۷	۱۰۰

درنهایت جدول (۱۳) زمان آموزش و زمان آزمایش روش‌های بررسی‌شده بر روی مجموعه داده SNMP-MIB را در مقایسه با روش پیشنهادی ارائه می‌دهد. در اینجا زمان آموزش و زمان آزمایش روش‌های بررسی‌شده و روش پیشنهادی بر روی مجموعه داده با تمامی ویژگی‌ها و مجموعه داده تنها دارای ویژگی‌های واسط انتخاب‌شده در این مقاله مورد بررسی قرارگرفته است. با توجه به زمان‌های به‌دست‌آمده می‌توان به این نتیجه رسید که علی‌رغم اختلاف کم در زمان آموزش و زمان آزمایش روش‌های بررسی‌شده بر روی مجموعه داده آموزش (۷۰ درصد داده انتخاب‌شده از مجموعه داده) و مجموعه داده آزمایش (۳۰ درصد داده انتخاب‌شده از مجموعه داده)، روش پیشنهادی می‌تواند با میزان صحت و دقت بالاتری در زمان مناسب حملات انکار سرویس را در شبکه با انتخاب ویژگی‌های واسط مجموعه داده شناسایی کند.



شکل ۹. معیارهای صحت، دقت، بازخوانی و میانگین هارمونی برای ترافیک عادی و ترافیک حملات در روش پیشنهادی بر اساس ویژگی‌های واسط

همان گونه که در جدول (۱۳) مشاهده می‌شود بهترین زمان آموزش و آزمایش توسط الگوریتم شبکه عصبی پرسپترون چندلایه ارائه‌شده است؛ ولی با توجه به میزان صحت و دقت به‌دست‌آمده از روش پیشنهادی با اختلاف زمانی بسیار کم نسبت به الگوریتم شبکه عصبی پرسپترون چندلایه، روش پیشنهادی می‌تواند راهکار مناسبی برای استفاده در سامانه‌های شناسایی حملات انکار سرویس انتخاب شود. همچنین در روش پیشنهادی با توجه به اینکه هشت ویژگی از ۳۴ ویژگی موجود در مجموعه داده انتخاب‌شده است می‌توان مشاهده کرد که میزان استفاده از حافظه اصلی سامانه کمتر شده و ازنظر استفاده از حافظه نیز کارایی سامانه بهبود داده شده است.

جدول ۱۳. مقایسه زمان آموزش و زمان آزمایش روش‌های مختلف

روش	با تمامی ویژگی‌ها		با ویژگی‌های واسط (۸ ویژگی)	
	زمان آموزش	زمان آزمایش	زمان آموزش	زمان آزمایش
آدابوست	۴/۰۱۶۱	۰/۲۹۹۲	۰/۹۶۵۰	۰/۰۶۲۲
جنگل تصادفی	۳/۹۳۰۹	۰/۲۹۴۳	۰/۸۷۹۰	۰/۰۵۷۶
پرسپترون چندلایه	۳/۱۹۳۶	۰/۱۷۲۷	۰/۶۳۷۱	۰/۰۳۶۰۱
روش رأی‌گیری پیشنهادی	۳/۲۲۶۷	۰/۱۷۷۹	۰/۶۵۸۳	۰/۰۳۶۲۴

۵-۳-۳. تحلیل نتایج

با بررسی کلی نتایج می‌توان توانایی روش پیشنهادی بر پایه یادگیری ماشین رأی‌گیری را نسبت به سایر روش‌ها و الگوریتم-های طبقه‌بندی مشاهده کرد. این روش عملکرد مناسبی را نسبت به سایر الگوریتم‌های یادگیری ماشین بررسی‌شده در تفکیک ترافیک عادی از ترافیک حملات (مخرب) ارائه داد. زمان آموزش و آزمایش روش پیشنهادی نیز درمجموع با توجه به میزان دقت بالای آن قابل‌قبول بود. در طبقه‌بند جنگل تصادفی و روش GRU-BWFA علی‌رغم دستیابی به نتایج خوب در نرخ دقت، نرخ بازخوانی و میانگین هارمونی، مدت‌زمان آموزش و آزمایش بسیار بالا بوده و عملکرد زمانی بسیار ضعیف‌تری نسبت به سایر الگوریتم‌ها ارائه داد؛ بنابراین، با توجه به این نقطه‌ضعف، کاربرد این طبقه‌بندها بر روی مجموعه داده SNMP-MIB برای تشخیص حملات انکار سرویس مناسب نخواهد بود.

مدت‌زمان آزمایش روش پیشنهادی در مقایسه با طبقه‌بندهای دیگر بکار گرفته‌شده در مقاله ارائه‌شده توسط الحیدری و همکاران [۱۱] بسیار نزدیک و اختلاف‌زمانی آن‌ها قابل‌چشم‌پوشی است ولی نتایج ارائه‌شده توسط روش پیشنهادی برای تشخیص حملات انکار سرویس نسبت سایر الگوریتم‌ها بهتر بود. الگوریتم شبکه عصبی چندلایه نیز سرعت مناسبی در مراحل آموزش و آزمایش داشت ولی به نتایج ضعیف‌تری نسبت به سایر روش‌ها دست‌یافت.

۶. نتیجه‌گیری

کارهای متعددی در تشخیص حملات انکار سرویس در شبکه‌های کامپیوتری انجام‌یافته است، بااین‌حال، با توجه به استفاده از این حملات در سامانه‌های مالی، تنوع و تعداد این نوع از حملات روزبه‌روز افزایش چشمگیری داشته است. دقت تشخیص بالای حملات و نیز مدت‌زمان تشخیص آن‌ها ازجمله چالش‌هایی است

که منجر به ارائه روش‌های متعددی شده است. در این مقاله سعی شده است با استفاده از پیش‌پردازش داده‌های مجموعه داده SNMP-MIB و انتخاب ویژگی‌های تأثیرگذار به همراه به‌کارگیری روش یادگیری جمعی رأی‌گیری حملات انکار سرویس را شناسایی کرد. عملکرد روش تشخیص پیشنهادشده با مقالات ارائه‌شده توسط الحیدری و همکاران [۱۱] و راجاسکار و همکاران [۲۳] مقایسه شده است و نتایج نشان می‌دهد که روش پیشنهادی، میزان دقت، صحت، بازخوانی و میانگین هارمونی بالایی را نسبت به روش‌های مذکور ارائه می‌دهد. با توجه به اینکه در بیشتر معیارهای ارزیابی روش پیشنهادی مقادیر بهتری ارائه داده است این امیدواری را می‌دهد تا بتوان با این روش انواع حملات انکار سرویس ناشناخته و جدید را نیز شناسایی کرد. مطالعات آتی در راستای گسترش و به‌کارگیری روش‌های انتخاب ویژگی‌های تأثیرگذار برای بالابردن نرخ دقت و صحت تشخیص حملات انکار سرویس در مجموعه‌داده‌های دیگر و همچنین کاهش خطای تشخیص در روش پیشنهادی خواهد بود.

۷. مرجع‌ها

[1] Husák, M.; Komárková, J.; Bou-Harb E.; Čeleda, P. “Survey of Attack Projection, Prediction, and Forecasting in Cyber Security”; IEEE Commun. Surv. Tutorials., 2018, 21, 1, 640–660. http://doi.org/10.1109/COMST.2018.2871866.

[2] J. Yu, H. Lee, M.-S. Kim, and D. Park, “Traffic Flooding Attack Detection with SNMP MIB using SVM”; Comput. Commun., 2008, 31, 17, 4212–4219. http://doi.org/10.1016/ j.comcom.2008.09.018.

[3] Asadi, M.; Parsa, S.; Jabreil Jamali, M. A.; Majidnezhad, V. “P2P Botnet Detection Using Deep Learning Method”; Electronic and Cyber Defense 2020, 8, 1–14. (In Persian). https://dor.isc.ac/dor/20.1001.1.23224347.1399.8.2.1.3

[4] Alipour, M. M.; Shokrollahi, S. “The Presentation of a New Defense Framework Against the Distributed Denial of Service Attacks Using the Software Defined Network”; Adv. Defence Sci. & Technol. 2021, 12, 273–284. (In Persian)

[5] Alkasassbeh, M.; Al-Naymat, G.; Hassanat, A.; Almseidin, M. “Detecting Distributed Denial of Service Attacks using Data Mining Techniques”; Int. J. Adv. Comput. Sci. Appl. 2016, 7, 436–445. http://doi.org/10.14569/IJACSA.2016. 070159.

[6] Thakkar, A.; Lohiya, R. “A Survey on Intrusion Detection System: Feature Selection, Model, Performance Measures, Application Perspective, Challenges, and Future Research Directions”; Artif. Intell. Rev. 2022, 55, 453–563. http:// doi.org/10.1007/s10462-021-10037-9.

[7] Asadi, M. “Detecting IoT Botnets Based on the Combination of Cooperative Game Theory with Deep and Machine Learning Approaches”; J. Ambient Intell. Hum. Comput. 2021, 13, 5547-5561. http://doi.org/10.1007/ s12652-021-03185-x.

[8] Asadi, M.; Parsa, S.; Jabreil Jamali, M. A.; Majidnezhad, V. “Detecting Botnet by using Particle Swarm Optimization Algorithm Based on Voting System”; Future Gener. Comput. Syst. 2020, 107, 95–111. http://doi.org/10.1016/ j.future.2020.01. 055.

[9] Al-Naymat, G.; Al-Kasassbeh, M.; Al-Hawari, E. “Exploiting SNMP-MIB Data to Detect Network Anomalies using Machine Learning Techniques”; SAI Intelligent Systems Conference, 2018, 991–1004.

[10] Pathan, A.-S. K. “The State of the Art in Intrusion Prevention and Detection”; Auerbach Publications, 2014. http://doi.org/10.1201/ b16390.

[11] Alhaidari, S.; Alharbi, A.; Alshaikhsaleh, M.; Zohdy, M.; Debnath, D. “Network Traffic Anomaly Detection Based on Viterbi Algorithm using SNMP-MIB Data”; Third Int. Conf. Information System and Data Mining, 2019, 92–97. http://doi.org/10.1145/3325917.3325928.

[12] Al-Kasassbeh, M.; Al-Naymat, G.; Al-Hawari, E. “Towards Generating Realistic SNMP-MIB Dataset for Network Anomaly Detection”; Int. J. Comput. Sci. Inform. Secur. 2016, 14, 1162-1185.

[13] Abushwereb, M.; Mustafa, M.; Al-Kasassbeh, M.; Qasaimeh, M. “Attack Based DoS Attack Detection using Multiple Classifier” arXiv Prepr. arXiv2001.05707, 2020.

[14] Cabrera, J. B. D.; Lewis, L.; Qin, X.; Lee, W.; Mehra, R. K. “Proactive Intrusion Detection and Distributed Denial of Service Attacks: A Case Study in Security Management”; J. Network Syst. Manage. 2002, 10, 225–254. http://doi.org/ 10.1023/ A:1015910917349.

[15] Rahmani, C.; Sharifi, M.; Tafazzoli, T. “An Exprimental Analysis of Proactive Detection of Distributed Denial of Service Attacks”; IIT Kanpur Hackers Workshop (IITKHACK04) 2004, 37–44.

[16] Hsiao, H.-W.; Lin, C. S.; Chang, S.-Y. “Constructing an ARP Attack Detection System with SNMP Traffic Data Mining”; 11th Int. Conf. Electronic Commerce 2009, 341–345. http://doi.org/10.1145/1593254.1593309.

[17] Yu, J.; Kang, H.; Park, D.; Bang, H.-C.; Kang, D. W. “An In-Depth Analysis on Traffic Flooding Attacks Detection and System using Data Mining Techniques”; Journal of Systems Architecture, 2013, 59, 1005–1012. http://doi.org/ 10.1016/ j.sysarc.2013.08.008.

[18] Cerroni, W.; Moro, G.; Pirini, T.; Ramilli, M. “Peer-to-Peer Data Mining Classifiers for Decentralized Detection of Network Attacks”; Twenty-Fourth Australasian Database Conference, 2013, 101–107.

[19] Namvarasl S.; Ahmadzadeh, M. “A Dynamic Flooding Attack Detection System Based on Different Classification Techniques and using SNMP-MIB Data”; Int. J. Comput. Netw. Commun. Secur. 2014, 2, 9, 279–284.

[20] Cerroni, W.; Moro, G.; Pasolini, R.; Ramilli, M. “Decentralized Detection of Network Attacks Through P2P Data Clustering of SNMP Data”; Comput. Secur. 2015, 52, 1–16. http://doi.org/10.1016/ j.cose.2015.03.006.

[21] Al-Naymat, G.; Hambouz, A.; Alkasassbeh, M. “Evaluating the Impact of Feature Selection Methods on SNMP-MIB Interface Parameters to Accurately Detect Network Anomalies”; IEEE International Symposium on Signal Processing and Information Technology, 2019, 1–6. http://doi.org/10.1109/ ISSPIT47144. 2019.9001882.

[22] Manna A.; Alkasassbeh, M. “Detecting Network Anomalies using Machine Learning and SNMP-MIB Dataset with IP Group”; 2nd International Conference on New Trends in Computing Sciences (ICTCS), 2019, 1–5. http://doi.org/ 10.1109/ ICTCS. 2019.8923043.

[23] Rajasekar P.; Magudeeswaran, V. “GRU-BWFA Classifier for Detecting DDoS Attack within SNMP-MIB Dataset”; Wireless Pers. Commun., 2021. http://doi.org/10.21203/ rs.3.rs-848205/v1.

[24] Shiravi, A.; Shiravi, H.; Tavallaee, M.; Ghorbani, A. A. "Toward Developing a Systematic Approach to Generate Benchmark Datasets for Intrusion Detection"; Comput. Secur., 2012, 31, 357–374. http://doi.org/10.1016/J.COSE.2011.12.012.

[25] Alpaydin E. "Machine Learning: The New AI"; MIT press, 2016. http://doi.org/10.7551/mitpress/13811.001.0001.

[26] Ding, S.; Hu, S.; Pan, J.; Li, X.; Li, G.; Liu, X. "A Homogeneous Ensemble Method for Predicting Gastric Cancer Based on Gastroscopy Reports"; Expert Syst. 2020, 37, 3, e12499. http://doi.org/10.1111/exsy.12499.

[27] Petrakova, A.; Affenzeller, M.; Merkurjeva, G. "Heterogeneous versus Homogeneous Machine Learning Ensembles"; Inf. Technol. Manage. Sci. 2015, 18, 135–140. http://doi.org/10.1515/itms-2015-0021.

[28] Asuero, A. G.; Sayago, A.; González, A. G. "The Correlation Coefficient: An Overview"; Crit. Rev. Anal. Chem. 2006, 36, 41-59. http://doi.org/10.1080/10408340500526766.