

## ارائه یک مدل تحلیل رفتار مرورگری برای تشخیص روبات‌های وب مخرب در حملات منع خدمت توزیعی

محمد فتحیان<sup>۱\*</sup>، محمد عبدالهی ازگمی<sup>۲</sup>، حسن دهقانی<sup>۳</sup>

۱- استاد، دانشکده مهندسی صنایع، دانشگاه علم و صنعت ایران، ۲- دانشیار، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران

۳- دانشجوی کارشناسی ارشد، دانشکده مهندسی صنایع، دانشگاه علم و صنعت ایران

(دریافت: ۹۴/۰۲/۱۷، پذیرش: ۹۵/۰۲/۱۴)

### چکیده

حملات منع خدمت توزیعی، یکی از مهم‌ترین تهدیدات دنیای تجارت الکترونیکی بوده و هدف اصلی آن جلوگیری از دسترسی کاربران به سایت‌ها و منابع اینترنتی از طریق مصرف بیش از حد منابع است. در این حملات، مؤلفه امنیتی دسترس پذیری، هدف تهاجم قرار می‌گیرد. یکی از روش‌های نیل به این هدف، به‌کارگیری روبات‌های وب است که حمله‌گران با استفاده از این روبات‌های مخرب، حملات منع خدمت در لایه کاربرد را طراحی و اجرا می‌نمایند. برای تشخیص این‌گونه روبات‌های مخرب از سایر روبات‌های غیرمخرب، از روش‌های گوناگونی استفاده شده است. یکی از روش‌هایی که در سال‌های اخیر مورد توجه قرار گرفته، یادگیری ماشین و داده‌کاوی است. محور اصلی این روش‌ها، استخراج و انتخاب خصیصه‌های مناسب جلسات وب از داده‌های ثبت رویداد و به‌کارگیری الگوریتم‌های داده‌کاوی است. این تحقیق سعی دارد تا با توجه به پویایی و سفارشی بودن طراحی و اجرای حملات منع خدمت توزیعی برای هر سایت، یک ساز و کار دفاعی پویا با قابلیت سفارشی‌سازی برای تشخیص روبات‌های وب مخرب مشارکت‌کننده در حملات، با استفاده از تحلیل رفتار مرورگری آن‌ها ارائه دهد. در این مطالعه، ضمن بهینه‌سازی روش‌های قبلی تعیین جلسات وب، استخراج مجموعه خصیصه‌ها براساس ویژگی‌های حملات دی‌داس انجام گرفت. همچنین پالایش خصیصه‌های استخراجی و انتخاب مجموعه خصیصه‌های کارا، باعث کاهش زمان ساخت مدل گردید و در نتیجه، دو درصد افزایش کارایی در مقایسه با بهترین تحقیق مشابه به‌دست آمد.

**واژه‌های کلیدی:** حمله منع خدمت توزیعی، امنیت تجارت الکترونیکی، تشخیص روبات‌های وب مخرب، داده‌کاوی

### ۱- مقدمه

حملات توزیعی باشد و از صدها تا ده‌ها هزار منبع تحت تسلط<sup>۳</sup> نشأت بگیرد، با چالش پیچیده‌تری مواجه خواهیم بود؛ چرا که برخلاف سناریوی حمله منع خدمت از یک منبع، در اینجا مسئله تشخیص<sup>۴</sup> محل منابع مخرب به دلیل تعداد بیشمار منابع شرکت‌کننده در حمله، بسیار سخت می‌شود. در این حالت حجم بسیار سنگینی از ترافیک ایجاد شده توسط تعداد انبوه منابع، به سمت سیستم قربانی<sup>۵</sup> گسیل می‌گردد که نتیجه آن ضرر مالی قابل ملاحظه برای کسب و کار و تجارت الکترونیکی تحت حمله به دلیل مسدود شدن ارائه خدمات می‌باشد. بر طبق گزارش سال ۲۰۰۸ وزارت دفاع آمریکا، حملات سایبری طراحی و اجرا شده از سوی افراد و کشورها به سازمان‌های اقتصادی، سیاسی و نظامی در آینده افزایش یافته و مخارج چند میلیارد دلاری در پی خواهد داشت [۱].

حملات منع خدمت توزیعی یا دی‌داس<sup>۱</sup> یکی از این انواع حملات امنیتی است که هدف اصلی آن از بین بردن قابلیت دسترس پذیری<sup>۲</sup> برنامه‌ها و خدمات تحت اینترنت برای کاربران است. در این نوع حمله، حجم زیادی پیام و داده به ماشین یا سایت مقصد با هدف ایجاد تداخل در عملیات آن ارسال می‌شود که نتیجه آن معلق کردن ماشین یا سایت مقصد به دلیل استفاده بیش از حد از منابع آن مثل پردازنده، حافظه، پهنای باند و غیره است. این امر قطع کامل یا کاهش شدید سرعت ارائه خدمات را به همراه خواهد داشت. در عمل حملات منع خدمت انجام شده از یک محل، به راحتی با شناسایی محل و مسدودسازی ترافیک ارسالی مخرب از سوی آن قابل دفع می‌باشد ولی موقعی که

3 -Compromised Zombie

4- Detection

5 -Victim

\* رایانامه نویسنده مسئول: fathian@iust.ac.ir

1 -Distributed Denial of Service (DDoS)

2- Availability

دسته‌های مختلف مرورگر<sup>۱۵</sup>، تقسیم کنند. هانتینگتون و همکارانش [۴]، یک روش تحلیل رویداد چندمرحله‌ای پیشنهاد دادند که در مرحله اول کلیه آدرس‌های اینترنتی درخواست‌کننده فایل متنی روبات<sup>۱۶</sup> روبات شناسایی می‌شدند. در مرحله بعد از طریق جستجوی معکوس کارگزار نام دامنه، جستجو بر روی کلیه آدرس‌های آی‌پی، انجام شده و نام‌های محتوی کلمات روبات<sup>۱۷</sup>، بات<sup>۱۸</sup>، سرچ<sup>۱۹</sup>، اسپایدر<sup>۲۰</sup> و کراولر<sup>۲۱</sup> با نظارت خبرگان انسانی و به‌صورت دستی به‌عنوان روبات وب دسته‌بندی می‌شدند.

روش تحلیل الگوی ترافیکی به دنبال آن دسته از ویژگی‌های معمول ترافیکی روبات وب می‌گردد که در تقابل با خصیصه‌های ترافیک عامل انسانی قرار دارد. گینز و همکارانش [۵]، یک روش تشخیص روبات پیشنهاد دادند که تحلیل نحوی را با تحلیل الگوی ترافیکی ترکیب می‌کرد. آن‌ها در تحقیقات خود به این نتیجه رسیدند که استفاده از هر یک از روش‌های درخواست فایل متنی روبات، مقایسه آدرس‌های آی‌پی با لیست آدرس‌های روبات‌های شناخته شده و مقایسه فیلد عامل کاربری در برابر پایگاه داده‌ای از عبارات شناخته شده، به تنهایی برای تشخیص روبات کافی نبوده و قابل اعتماد نیست. به همین دلیل از سه الگوی ساده در ترافیک، برای بالابردن درصد تشخیص روبات‌ها استفاده نمودند. این الگوها عبارت بودند از تعیین تعداد درخواست هد<sup>۲۲</sup> که بیشتر مورد استفاده روبات‌ها می‌باشد، فیلد ارجاع<sup>۲۳</sup> که معمولاً در مراجعه روبات‌ها تخصیص نیافته<sup>۲۴</sup> (خالی) است و میزان فایل‌های تصویری که بیشتر درخواست این‌گونه فایل‌ها توسط عامل انسانی و مرورگر است. گیو و همکارانش [۶] از این فرض استفاده کردند که روبات‌های وب، هنگام پیمایش یک سایت فقط منابع خاصی را درخواست می‌کنند. با این فرض آن‌ها سعی در تشخیص روبات براساس الگوهای درخواست منبع نمودند. بر این پایه، آن‌ها دو الگوریتم جدید تشخیص ارائه دادند. در تحقیق آن‌ها منابع به هشت نوع صفحه وب، سند<sup>۲۵</sup>، اسکریپت، تصویر، موزیک، ویدئو، فایل و سایر تقسیم‌بندی شده بودند. اولین الگوریتم براساس حجم و میزان منابع درخواستی و دومی بر پایه نرخ درخواست‌ها به تشخیص روبات می‌پرداخت.

داسکین و همکارانش [۷] از طریق تحلیل نرخ درخواست

در سال‌های اخیر، حملات لایه ۷ مورد توجه حمله‌گران قرار گرفته است و به دلیل شباهت خیلی زیاد رفتار حمله‌گر با رفتار کاربران عادی در این لایه، عملاً تفکیک و تشخیص حمله بسیار سخت می‌باشد و به همین دلیل روش‌های داده‌کاوی<sup>۱</sup> مورد توجه قرار گرفته است. یکی از انواع مهم این‌گونه حملات، حملات مبتنی بر روبات وب<sup>۲</sup> مانند یک خزشگر وب<sup>۳</sup> است که حجم زیادی ترافیک غیرواقعی از طریق عملیات پیمایش روی سایت‌های وب ایجاد نموده و باعث اختلال در عملکرد سایت و به هدر دادن منابع قربانی می‌گردد. موضوع این مقاله، ارائه مدلی برای تحلیل رفتار مرورگری<sup>۴</sup> به‌منظور تشخیص روبات‌های وب مخرب<sup>۵</sup> مشارکت‌کننده در حملات منع خدمت توزیعی می‌باشد.

در بخش دوم این مقاله به مرور ادبیات مشتمل بر معرفی و دسته‌بندی انواع روش‌های تشخیص روبات‌های وب خوش‌رفتار<sup>۶</sup> و بدرفتار<sup>۷</sup> (مخرب) مخرب پرداخته می‌شود. در بخش سوم مدل پیشنهادی برای تشخیص روبات‌های مخرب مشارکت‌کننده در حملات منع خدمت توضیح داده می‌شود. بخش چهارم به تشریح آزمایشات و نتایج حاصله با استفاده از داده‌های آزمایشی و ارزیابی مدل می‌پردازد. در بخش پنجم پس از بحث و بررسی، جمع‌بندی و نتیجه‌گیری ارائه می‌گردد.

## ۲- مرور ادبیات

مطالعات پیشین در حوزه تشخیص روبات وب و تفکیک آن از مرورگران انسانی، روش‌های تشخیص را به چهار دسته تحلیل نحوی ثبت رویداد<sup>۸</sup>، تحلیل الگوی ترافیکی<sup>۹</sup>، روش‌های یادگیری تحلیلی<sup>۱۰</sup> و سیستم‌های تست تورینگ<sup>۱۱</sup> تقسیم کرده‌اند [۲]. سه دسته اول به روش‌های حل مسئله تشخیص غیربرخط<sup>۱۲</sup> و دسته چهارم به روش‌های حل مسئله بی‌درنگ<sup>۱۳</sup> می‌پردازند. در روش تحلیل نحوی داده‌های ثبت رویداد سعی می‌شود روبات‌ها از طریق پردازش داده‌های ثبت رویداد دسترسی به سایت، مورد شناسایی قرار گیرند. کیب و میازاکی [۳] در مطالعه خود، بر اساس توصیف فیلد عامل کاربری<sup>۱۴</sup> توانستند کاربران را به

- 1- Data Mining
- 2- Web Robot
- 3- Web Crawler
- 4- Browsing Behavior
- 5- Malicious
- 6- Well-Behaved
- 7- Ill-Behaved
- 8- Syntactical Log Analysis
- 9- Traffic Pattern Analysis
- 10- Analytical Learning Technique
- 11- Turing Test System
- 12- Off-Line
- 13- Real Time
- 14- User-Agent

- 15- Browser
- 16- Robots.txt
- 17- Robot
- 18- Bot
- 19- Search
- 20- Spider
- 21- Crawler
- 22- Head
- 23- Referrer
- 24- Unassigned
- 25- Document

فایلی که معمولاً روبات ها را برای صفحات قابل دسترسی هدایت می کند؛ ۲- درصد صفحات درخواستی از طریق دستور هد، ۳- درصد درخواست های با فیلد ارجاع خالی، در برچسب دهی اولیه، جلسات کاربری به چهار گروه روبات های شناخته شده، مرورگرهای شناخته شده، روبات های محتمل، و مرورگرهای محتمل تقسیم بندی گردیدند. در نهایت با به کارگیری الگوریتم سی ۴/۵<sup>۱۱</sup> که یک الگوریتم داده کاوی درخت تصمیم<sup>۱۱</sup> است، مدل رده بندی<sup>۱۲</sup> ساخته شد. پس از اعمال این مدل بر روی مجموعه داده ها، روبات ها با صحت بیش از ۹۰ درصد و بعد از تنها چهار درخواست، تشخیص داده شدند. فراخوان و دقت روش آن ها بعد از بیش از سه درخواست ۰/۸۲ و ۰/۹۵ بود.

بومهارت و همکارانش [۱۰] برای تشخیص روبات های وب از شبکه عصبی استفاده کرده و به مقایسه نتایج حاصل با روش درخت تصمیم (شبیه تحقیق تن و کومار) پرداختند. استاسوپولو و دیکاپاکوس [۱۱] یک رویکرد مبتنی بر بیزین<sup>۱۳</sup> برای تشخیص خزشگرها ارائه دادند. لو و یو [۱۲] از مدل مخفی مارکوو<sup>۱۴</sup> برای تشخیص کاربران انسانی از روبات براساس الگوهای ورودی استفاده کردند. بنابه ادعای آن ها یک کاربر انسانی مراجعه کننده به یک صفحه وب را می توان از طریق ارسال درخواست های پی در پی اچ تی تی پی توسط مرورگر برای منابع داخل صفحه و سپس طی مدت زمانی برای بازدید صفحه، توصیف نمود. در مقابل یک روبات درخواست برای منابع را در نرخ آهسته تر و در دوره زمانی یکنواخت تری بین درخواست ها، ارسال می کند. بر این اساس پژوهشگران زمان را در فواصل مجزایی با طول یکسان تقسیم نمودند و یک یا چند درخواست وارد شده توسط یک کاربر در همان فاصله زمانی را یک دسته ورودی<sup>۱۵</sup> نامیدند. هر فاصله زمانی با یک دسته ورودی به صورت یک مشاهده برای مدل مخفی مارکوو در نظر گرفته شد. پژوهشگران از دنباله روبات های قبلاً مشاهده شده برای آموزش مدل خود استفاده کردند. این مجموعه آموزشی از طریق آزمایش فیلد عامل کاربری و استخراج عامل درخواست هایی که به طور واضح از ناحیه روبات بودند، انتخاب شد.

تنها مطالعه ای که با توجه به نقش مشارکت خزشگرهای وب مخرب در اجرای حملات منع خدمت توزیعی، بر روی تشخیص روبات وب مخرب از روبات وب خوش رفتار تمرکز داشت، تحقیقات استوانوویچ و همکارانش [۱۳] بود. آن ها به مطالعه

پرس و جوهای<sup>۱</sup> ارسالی در داده های ثبت رویداد موتور جستجوی وب، روشی برای تفکیک روبات از انسان ارائه دادند. پیشنهاد آن ها این بود که الگوی فعالیت کاربران جستجوگر با استفاده از چندین معیار مورد مطالعه قرار گیرد. این معیارها عبارت بودند از: نرخ ارسال درخواست پرس و جو، فاصله زمانی بین پرس و جوها، نرخ تاپ کردن کاربران، طول جلسه فعالیت های مداوم، همبستگی<sup>۲</sup> با زمان در روز، و نظم و قاعده پرس و جوهای ارسالی. لین و همکارانش [۸]، طرحی را معرفی کردند که ترافیک وب را به سه دسته عوامل انسانی، روبات های وب و سایر پروتکل های اینترنتی مثل اشتراک فایل نظیر به نظیر<sup>۳</sup> تقسیم می کرد. آن ها از سه معیار برای تعیین سه دسته ترافیک پیشنهادی خود استفاده کردند. اولین معیار به نام تشابه انسانی<sup>۴</sup> برای تخمین میزان تشابه هر جلسه خاص با جلسات انسانی در انواع فایل های درخواستی و نتایج درخواست تعریف گردید. معیار دیگری به نام ضریب تنوع<sup>۵</sup> تعریف شد که به میزان تنوع انواع منابع درخواستی در هر جلسه توجه داشت. معیار سوم آن ها به نام وابستگی به صفحات وب<sup>۶</sup> (اچ تی ام ال<sup>۷</sup>)، انعکاس دهنده این فرض است که جلسات انسانی حاوی ترکیبی از انواع منابع بوده و در مقابل در جلسات روباتی درخواست های فایل های محتوی پیوند به منابع تفوق دارد. پژوهشگران با ترکیب این معیارها، یک رده بندی<sup>۸</sup> خودکار برای تشخیص ترافیک روبات وب ایجاد نمودند.

روش های یادگیری تحلیلی به مشاهده و بررسی ویژگی های جلسات ثبت شده پرداخته و احتمال این که هر جلسه توسط یک روبات ایجاد شده باشد را تخمین می زنند. برای این منظور از روش های یادگیری ماشین و مدل های مبتنی بر تئوری احتمالات استفاده می شود. یکی از اولین و مهم ترین مطالعات بر روی رده بندی<sup>۹</sup> روبات های وب با استفاده از الگوریتم های داده کاوی توسط تن و کومار [۹] در سال ۲۰۰۲ انجام گرفت. در اولین مرحله، پژوهشگران یک رویکرد جدید برای استخراج جلسات وب از داده های ثبت رویداد پیشنهاد دادند. در مرحله بعد، ۲۶ خصیصه مختلف را برای هر جلسه وب استخراج نمودند. از میان آن ها، سه خصیصه انتخاب شد که بیشتر احتمال تعلق جلسه به روبات را می داد و از این سه خصیصه برای برچسب دهی استفاده شد. آن ها عبارت بودند: ۱- کنترل دسترسی به فایل متنی روباتز

- 1- Query
- 2- Correlation
- 3- Peer-to-Peer (P2P)
- 4- Human Similarity (HS)
- 5- Diversity Factor (DF)
- 6- Html Affinity (HA)
- 7- HyperText Markup Language (HTML)
- 8- Classifier
- 9- Classification

- 10- C4.5
- 11- Decision Tree
- 12- Classification Model
- 13- Bayesian
- 14- Hidden Markov Model (HMM)
- 15- Batch Arrival

جدول (۱). اهم کارهای انجام شده در حوزه تشخیص روبات وب

مطالعه	روش تشخیص	تشخیص روبات از انسان	تشخیص روبات مخرب	استخراج خصیصه	ساخت مدل تشخیص
[۳-۴]	تحلیل نحوی ثبت رویداد	✓			
[۵-۸]	تحلیل الگوی ترافیکی	✓		✓	
[۹-۱۲]	روش‌های یادگیری تحلیلی	✓		✓	✓
[۱۳-۱۴] و [۱۷]	روش‌های یادگیری تحلیلی	✓	✓	✓	✓
[۱۵-۱۶]	سیستم‌های تست تورینگ	✓			

### ۳- روش تحقیق

هدف این تحقیق، تشخیص روبات‌های وب مخرب حمله‌گر از طریق ساخت یک مدل رده‌بندی (کلاس‌بندی) است که توانایی تفکیک خودکار روبات‌های وب مخرب از سایر مراجعه‌کنندگان به سایت اعم از مرورگران عادی و روبات‌های خوش‌رفتار را براساس ویژگی‌های رفتار مرورگری مراجعه‌کننده داشته باشد. برای این منظور از داده‌های ثبت رویداد (لاگ) هر سایت وب به‌عنوان منبعی ارزشمند استفاده می‌شود. اطلاعات مرتبط با ترافیک ورودی به هر سایت، در فایل‌های ثبت رویداد کارگزار (سرور) وب ذخیره می‌گردد. هر فایل ثبت رویداد محتوی هزاران رکورد است که در یک قالب<sup>۱</sup> مشخص و استاندارد ذخیره می‌شوند. طبیعت پروتکل اچ‌تی‌تی‌پی طوری است که رکوردها هیچ‌گونه وابستگی به یکدیگر ندارند. بنابراین داده‌های ثبت رویداد محتوی هیچ اطلاعاتی نیستند که بتواند درخواست‌های صادره در طول یک مراجعه را به هم مرتبط نماید. به‌همین دلیل برای استخراج خصیصه‌های رفتاری مراجعات به سایت مدنظر، قبل از هر اقدامی نیاز است تا داده‌های ثبت رویداد، مورد پردازش قرار گرفته و جلسات وب از آن‌ها استخراج گردد. در صورت برچسب‌دهی مناسب به جلسات، امکان استفاده از الگوریتم‌های داده‌کاوی برای ساخت مدل رده‌بندی با کارایی بالا فراهم می‌گردد.

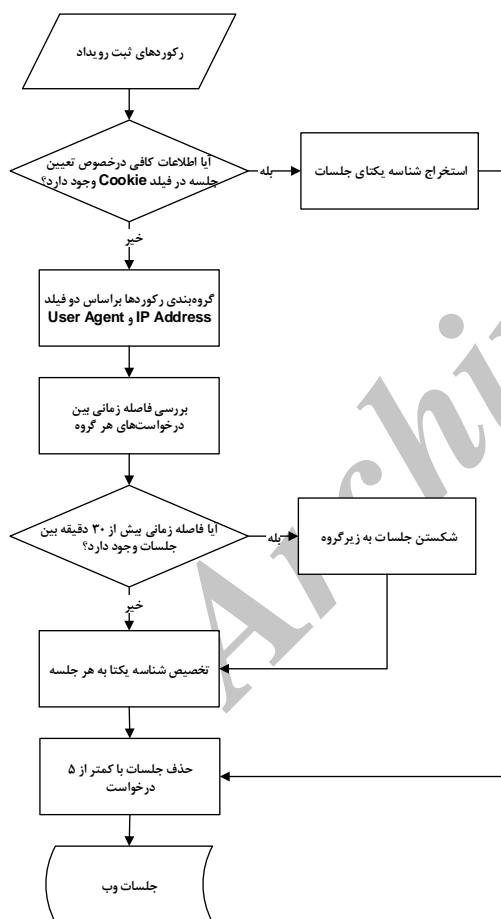
شکل (۱) چارچوب کلی روش تحقیق را نشان می‌دهد. در این تحقیق برای انجام مراحل پیش‌پردازش و آماده‌سازی داده‌های ثبت رویداد و نیز تعیین جلسات، استخراج و انتخاب بهترین خصیصه‌ها (مناسب برای حملات منع خدمت توزیعی) و

تشخیص رفتار کاربران و روبات‌های عادی از روبات‌های مخرب با استفاده از الگوریتم‌های داده‌کاوی موجود پرداختند. در این راستا از هفت الگوریتم مطرح رده‌بند (سی/۴/۵، ریپر<sup>۱</sup>، نزدیک‌ترین همسایه، نایو بی‌زین، شبکه بی‌زین، ماشین بردار پشتیبان<sup>۲</sup> و شبکه عصبی<sup>۳</sup>) برای رده‌بندی جلسات وب روبات‌ها از کاربران انسانی و سپس تعیین جلسات روبات‌های مخرب شرکت‌کننده در حمله از میان آن‌ها استفاده گردید. همچنین دو خصیصه جدید به هفت خصیصه از مطالعات قبلی برای رده‌بندی جلسات روبات‌های وب، اضافه شد و ظرفیت آن‌ها در خصوص بهبود صحت رده‌بندی داده‌کاوی در تعیین جلسات روبات‌های وب مخرب مورد ارزیابی قرار گرفت. بهره‌گیری از دو خصیصه جدید مقدار کمی بر صحت رده‌بندی افزود. همین تیم [۱۴] در ادامه تحقیقات خود در این حوزه، برای افزایش کارایی تشخیص از دو الگوریتم نظارت نشده یادگیری شبکه عصبی برای تحلیل داده‌های ثبت رویداد استفاده نمودند.

مسئله تشخیص روبات در سیستم‌های تست تورینگ سعی در تعیین روبات یا انسان بودن منشأ تولید جلسات دارد. یک مثال متداول از سیستم تست تورینگ، تست کپچا می‌باشد که توسط آن و همکارانش [۱۵] ارائه گردید و در واقع یک تست چالش/پاسخ قرار گرفته در داخل یک صفحه وب است. در این حالت کارگزار وب یک تست ساده استخراج می‌کند که کاربر باید جهت دسترسی به برخی منابع، در آن موفق عمل نماید. تست‌های کپچا که کاربر باید در آن قبول شود می‌تواند کپی متن از یک تصویر یا تایپ یک کلمه یا عبارت از یک فایل صوتی باشد. استخراج کاراکترها از تصویر یا تحلیل فایل صوتی برای تعیین کلمه یا عبارت مربوطه، توسط روبات قابل تشخیص نمی‌باشد. پارک و همکارانش [۱۶] روشی را ارائه دادند که در آن براساس رفتار مرورگری انسان، از تست تورینگ به‌صورت ضمنی<sup>۴</sup> برای تفکیک ترافیک انسان از روبات استفاده می‌شود. در این مطالعه، فعالیت‌های کاربر انسانی از طریق ظهور برخی رویدادهای خاص توسط یک مرورگر وب تشخیص داده می‌شود. یک اسکریپت جاوا<sup>۵</sup> قرار گرفته در صفحه وب که محتوی یک هندلر رویداد<sup>۶</sup> برای حرکت ماوس یا فشردن یک کلید است، می‌تواند تعیین کند که جلسه متعلق به یک انسان است یا یک روبات. جدول (۱) مهمترین کارهای انجام شده در حوزه تشخیص روبات در سنوات اخیر را نشان می‌دهد.

- 1- RIPPER
- 2- Support Vector Machine (SVM)
- 3- Neural Network
- 4- Implicit
- 5- Javascript
- 6- Event Handler

نباشد. اول آن که، این امکان وجود دارد که هر جفت فیلد آدرس آی پی/عامل کاربری، محتوی بیش از یک جلسه باشد؛ به عنوان مثال این حالت می تواند در جلساتی رخ دهد که کاربران وب از طریق یک کارگزار نماینده<sup>۲</sup> مشترک و با یک نوع مرورگر وب، آن ها را ایجاد کرده باشند. دلیل دوم، احتمال وجود چندگانه آدرس آی پی یا عامل کاربری در یک جلسه است که باعث تقسیم یک جلسه به چند جلسه مجزا می شود [۹]. اگر فاصله زمانی بین دو درخواست متوالی در یک جلسه، بیشتر از ۳۰ دقیقه باشد، درخواست جدید آغازگر جلسه جدیدی است. شکل (۲) فرایند استخراج و تعیین جلسات وب از رکوردهای ثبت رویداد را نشان می دهد. همچنین ما جلسات با تعداد کمتر از پنج درخواست را حذف می نماییم، چرا که عملاً امکان بررسی و ارزیابی این قبیل جلسات برای تخصیص برچسب حتی توسط عامل انسانی و به صورت دستی وجود ندارد.

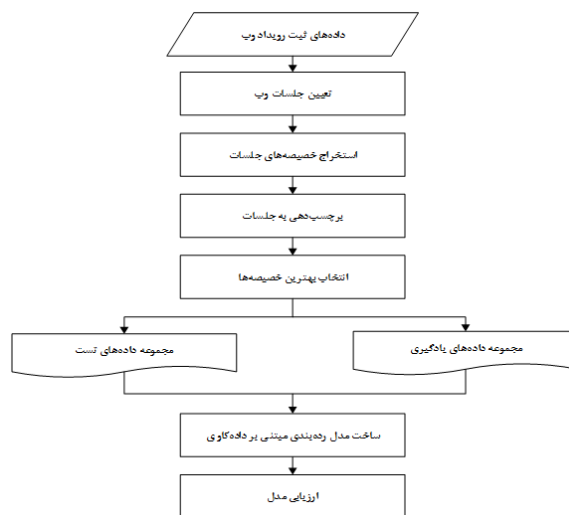


شکل (۲). فرایند تعیین جلسات وب

### ۲-۳- استخراج خصیصه

مرحله بعد از تعیین جلسات وب، استخراج خصیصه های هر

برچسب دهی به جلسات، یک تحلیلگر داده های ثبت رویداد<sup>۱</sup> طراحی شد. برای رتبه بندی خصیصه ها و انتخاب زیرمجموعه مناسبی از آنها و نیز ساخت مدل رده بندی و ارزیابی آن از نرم افزار داده کاوی و کا<sup>۲</sup> استفاده گردید.



شکل (۱). چارچوب کلی روش تحقیق

### ۱-۳- تعیین جلسه

یک جلسه وب عبارت است از کلیه فعالیت هایی که یک کاربر از لحظه ورود به یک سایت تا لحظه ترک آن انجام می دهد [۱۸]. به عبارت دیگر یک جلسه وب دنباله ای از درخواست های اچ تی تی پی است که از یک مبدأ نشأت گرفته و در یک بازه زمانی مشخص و محدود، به کارگزار وب وارد گردند. تعیین جلسه عبارت از فرایند تبدیل رکوردهای ثبت رویداد هر کاربر به جلسات وب مربوطه می باشد. هر رکورد، متناظر با یک درخواست اچ تی تی پی است. به طور کلی تعیین جلسه به این صورت انجام می گیرد: ۱- در صورت امکان استفاده از روش های ابتکاری برای استخراج شناسه یکتا، ۲- گروه بندی درخواست های اچ تی تی پی براساس آدرس آی پی و فیلد عامل کاربری، ۳- شکستن گروه ها به زیرگروه هایی با فاصله زمانی بیش از یک آستانه از قبل تعریف شده.

چالش کلیدی این روش، تعیین صحیح مقدار آستانه با توجه به رفتارهای مرورگری مختلف کاربران وب است. در اکثر تحقیقات مرتبط، این مقدار معادل ۳۰ دقیقه به عنوان حداکثر طول زمانی یک جلسه مدنظر قرار گرفته است [۱۳].

به هر حال این رویکرد، ممکن است به دو دلیل روش کاملی

- رفتار آن‌ها بسیار شبیه روبات‌های معمولی به‌ویژه خزشگرهای جستجوی وب می‌باشد.
  - نرخ درخواست‌های آن‌ها متناوب و احتمالاً ضربانی است.
  - درخواست‌های آن‌ها از ساختار خاصی تبعیت نمی‌کند.
- با مدنظر قرار دادن ویژگی‌های حملات منع خدمت توزیعی و نیز بررسی رفتار مرورگری روبات‌های مخرب، می‌توان به مجموعه‌ای از بهترین خصیصه‌ها برای جداسازی روبات‌های وب مخرب حمله‌گر از سایر مرورگران انسانی و روباتی دست یافت. در این مطالعه، ملاک عمل ابتدا بررسی خصیصه‌های مطالعات قبلی در خصوص جلسات روبات‌های وب مخرب بوده است و سپس براساس نتایج بررسی، مجموعه مناسب‌تری که هم‌راستا با ویژگی‌های حملات منع خدمت باشد، با توجه به گزاره‌های زیر استخراج شده است:

- عمده مرورگرهای انسانی و روبات‌های خوش‌رفتار وب مثل خزشگرهای جستجو، به دنبال صفحات با محبوبیت بیشتر هستند، اما کارکرد اصلی روبات‌های وب مخرب حمله‌گر، صرفاً ارسال حجم زیادی درخواست بدون هدف صفحه، برای ایجاد ترافیک مزاحم می‌باشد.
  - روبات‌های مخرب وب برای رسیدن به هدف اصلی خود که همانا مصرف بی‌رویه منابع قربانی از جمله پهنای باند است، زمان زیادی را برای حضور در سایت صرف می‌کنند و به همین دلیل جلسات وب طولانی‌تری را سپری می‌نمایند.
  - اندازه و حجم داده‌های مبادله شده در جلسات روبات‌های وب مخرب زیادتر از جلسات معمولی است که دلیل آن درگیر بودن کارگزار وب در پاسخ‌گویی به درخواست‌های پیمایشی روبات حمله‌گر است.
- متناظر با نتایج فوق چهار خصیصه به شرح زیر انتخاب گردید:

- شاخص محبوبیت صفحه: این شاخص میزان محبوبیت یک صفحه وب را نشان می‌دهد. مقدار این شاخص برای روبات‌های مخرب کمتر از سایر مراجعه‌کنندگان (روبات‌های خوش‌رفتار و مرورگران انسانی) است.
- نرخ ترافیک: عبارت از نسبت حجم داده‌های مبادله شده در یک جلسه به زمان آن جلسه است. این مقدار برای روبات‌های مخرب بیشتر از سایرین است.
- نرخ درخواست: عبارت از نسبت تعداد درخواست‌ها در یک جلسه به زمان آن جلسه است. این فرکانس برای روبات‌های مخرب بیشتر از سایرین است.
- زمان پردازش: عبارت از مدت زمانی است که در یک جلسه صرف پردازش درخواست‌ها می‌گردد. این زمان برای روبات‌های مخرب طولانی‌تر از سایرین است.

جلسه در رابطه با تفکیک الگوهای مرورگری کاربران انسانی و روبات‌های وب است. با تعمیم این خصیصه‌ها و با توجه به ویژگی‌های روبات‌های وب مشارکت‌کننده در حملات منع خدمت، می‌توان به دسته‌ای از خصیصه‌ها رسید که از طریق آن‌ها می‌توان روبات‌های مخرب را از سایر گروه‌های کاربری اعم از کاربران انسانی و روبات‌های خوش‌رفتار تشخیص داد. رکوردهای ثبت رویداد، محتوی اطلاعاتی از قبیل آدرس آی‌پی، نام میزبان مراجعه‌کننده به سایت، آدرس صفحه درخواستی، تاریخ و ساعت درخواست، اندازه داده‌های درخواستی، روش درخواست و غیره است. علاوه بر این در هر رکورد ثبت رویداد، فیلد رشته حرفی عامل کاربری قرار دارد که در واقع توصیف‌کننده سخت‌افزار و نرم‌افزار کاربر مراجعه‌کننده به سایت می‌باشد. همچنین فیلد ارجاع که مشخص‌کننده صفحه‌ای است که کاربر از طریق آن به صفحه جاری ارجاع داده شده است، از دیگر فیلدهای موجود در رکورد ثبت رویداد است. از این فیلدها می‌توان برای توصیف خصیصه‌های خاص یک جلسه وب کاربر استفاده کرد.

هدف این تحقیق صرفاً تشخیص روبات‌های وب در دو گروه خوش‌رفتار و مخرب نبوده و بلکه در یک نوآوری، این مطالعه بنا دارد مدلی برای تشخیص روبات‌های وب مخرب مشارکت‌کننده در حملات منع خدمت توزیعی از سایر مرورگران اعم از کاربران انسانی عادی و روبات‌های وب خوش‌رفتار ارائه نماید. برای این منظور قبل از هر چیز باید ویژگی‌های یک حمله منع خدمت توزیعی را شناخت تا بتوان براساس آن، خصیصه‌های مناسب برای تشخیص این‌گونه روبات‌های وب مخرب حمله‌گر را تعریف نمود. به‌طورکلی ویژگی‌های خاص یک حمله منع خدمت توزیعی در لایه کاربرد به این شرح است:

- از تعداد زیادی منبع (روبات وب) برای حمله و ارسال درخواست به سایت قربانی استفاده می‌شود.
- حجم داده‌های مبادله شده بین منابع و قربانی نسبتاً زیاد است تا پهنای باند سایت قربانی پر شود.
- نوع و نرخ درخواست‌های ارسالی طوری است که سایت قربانی را به شدت درگیر پاسخ‌گویی می‌کند.
- از آدرس‌های آی‌پی مبدأ متناوب و احتمالاً جعلی برای درخواست‌ها استفاده می‌شود.
- قواعد متداول بین روبات‌های خوش‌رفتار مثل ضوابط مندرج در فایل روباتز رعایت نمی‌شود.
- از فیلد عامل کاربری ناشناخته و احیاناً جعلی استفاده می‌گردد.
- شبیه روبات‌های خوش‌رفتار معمولاً فیلد ارجاع (آدرس صفحه قبلی) خالی است.

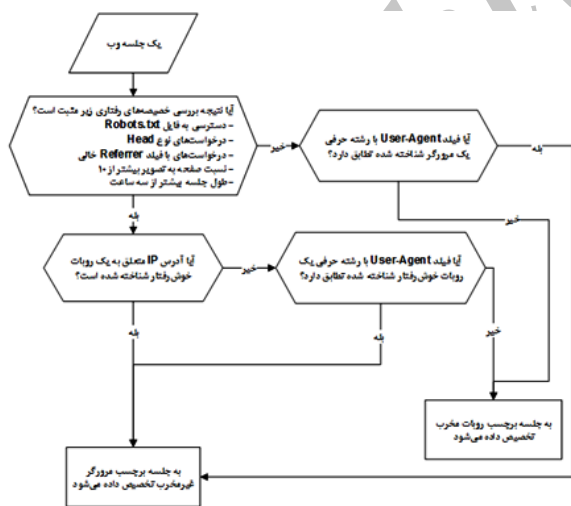
ما در این کار، خصیصه‌ها را به دو دسته تقسیم می‌کنیم: دسته اول خصیصه‌هایی که برای تشخیص هر نوع روباتی قابل استفاده هستند و دسته دوم خصیصه‌هایی که کارایی بالاتری را در تشخیص روبات‌های دی‌داس در لایه کاربرد ارائه می‌دهند. جدول (۲) لیست خصیصه‌های استخراج شده برای این تحقیق را نشان می‌دهد.

جدول (۲). خصیصه‌های استخراج شده برای تحقیق

ردیف	نام خصیصه	شرح	نوع روبات
۱	Request Number	تعداد درخواست اچ‌تی‌تی‌بی	خاص دی‌داس
۲	Click Number	تعداد درخواست صفحه وب	عمومی
۳	HTML-to-Image Ratio	نسبت درخواست صفحه وب به درخواست فایل تصویری	عمومی
۴	%PDF/PS	درصد درخواست فایل پی‌دی‌اف/پی‌اس	عمومی
۵	%4xx Error	درصد پاسخ خطا با کد 4XX	عمومی
۶	%Head	درصد درخواست نوع هد	عمومی
۷	%Unassigned Referrer	درصد درخواست با فیلد ارجاع خالی یا تخصیص نیافته	عمومی
۸	Robots.txt	مشخص کننده دسترسی به فایل روباتز	عمومی
۹	Client Size	حجم داده‌های ارسال از سوی کاربر به سمت کارگزار	خاص دی‌داس
۱۰	Server Size	حجم داده‌های ارسال از سوی کارگزار به سمت کاربر	خاص دی‌داس
۱۱	Total Size	مجموع داده‌های تبادل شده	خاص دی‌داس
۱۲	Time Taken	کل زمان صرف شده برای پردازش درخواست‌ها	خاص دی‌داس
۱۳	Duration	کل زمان سپری شده در یک جلسه	خاص دی‌داس
۱۴	Page Popularity Index	شاخص محبوبیت یک صفحه	عمومی
۱۵	Request Rate	نرخ درخواست‌های ارسالی	خاص دی‌داس
۱۶	Traffic Rate	نرخ ترافیک مبادله شده	خاص دی‌داس

مشکل از بردار خصیصه‌ها، باید به هر بردار یک برچسب توسط برنامه تحلیلگر داده‌های ثبت رویداد داده شود. به‌طور کلی هر بردار خصیصه متعلق به یکی از چهار گروه مرورگران انسانی، روبات‌های وب خوش‌رفتار، روبات‌های وب مخرب و مراجعه‌کنندگان ناشناس می‌باشد. ما جلسات وب را به دو گروه (۱) روبات‌های وب مخرب و (۲) مرورگران غیرمخرب شامل کاربران انسانی و روبات‌های خوش‌رفتار تقسیم می‌کنیم. برای انجام فرایند برچسب‌دهی، برنامه تحلیلگر ما یک جدول از فیلدهای عامل کاربری انواع مرورگران و روبات‌های وب شناخته شده را در خود نگهداری می‌کند. این اطلاعات از طریق سه سایت [۲۱-۱۹] به دست می‌آید. شکل (۳) فرایند برچسب‌دهی به جلسات وب را به شرح زیر نشان می‌دهد:

- همه بردارهای خصیصه دارای ویژگی‌های خاص به‌عنوان روبات وب خوش‌رفتار برچسب می‌گیرند (برچسب صفر).
- همه بردارهای خصیصه با فیلد عامل کاربری با رشته حرفی مربوط به یک مرورگر شناخته شده، به‌عنوان یک مراجعه‌کننده انسانی برچسب می‌گیرند (برچسب صفر).
- همه بردارهای خصیصه با فیلد عامل کاربری با رشته حرفی مربوط به یک روبات وب ناشناخته، به‌عنوان یک روبات وب مخرب برچسب می‌گیرند (برچسب یک).
- سایر بردارهای خصیصه به‌عنوان مراجعه‌کنندگان ناشناس برچسب می‌گیرند (برچسب یک).



شکل (۳). فرایند برچسب‌دهی به جلسات وب

### ۳-۳- برچسب‌دهی

پس از استخراج مجموعه داده آموزش، نیاز است به هر بردار خصیصه متناظر با یک جلسه وب، یک برچسب تخصیص یابد تا بتوان عملیات رده‌بندی و ساخت مدل را انجام داد. برچسب‌دهی به هر جلسه وب عبارت است از عمل تخصیص یک جلسه به یک روبات مخرب یا سایر مرورگران. پس از استخراج جلسات وب

### ۴-۳- انتخاب خصیصه‌ها

مرحله انتخاب خصیصه یکی از مهمترین مراحل پیش‌پردازش در داده‌کاوی است که با استفاده از الگوریتم‌های مربوطه، به جستجوی بهترین ترکیب ممکن از خصیصه‌هایی

## ۳-۵- رده‌بندی

بعد از تعیین جلسات وب، استخراج و انتخاب خصیصه‌ها و برچسب‌دهی به جلسات، ساختن مدل‌های رده‌بندی (کلاس‌بندی) براساس الگوریتم‌های داده‌کاوی شروع می‌گردد. در این تحقیق، الگوریتم‌های مختلف با هدف تشخیص روبات‌های مخرب از سایر مرورگران غیرمخرب با کارایی و صحت بالا مورد آزمایش و ارزیابی قرار می‌گیرند. الگوریتم‌های مدنظر در این تحقیق که با استفاده از نرم‌افزار وکا مورد ارزیابی قرار می‌گیرند، به شرح زیر می‌باشند [۲۵]:

- J48: یادگیرنده مبتنی بر درخت تصمیم، پیاده‌سازی شده براساس الگوریتم C4.5
- NaiveBayes: رده‌بند مبتنی بر مدل احتمالات نایو بیزین
- IBK<sup>۸</sup>: رده‌بند مبتنی بر الگوریتم نزدیکترین همسایه
- SMO<sup>۹</sup>: الگوریتم حداقل بهینه‌سازی ترتیبی برای رده‌بندی بردار پشتیبان
- MLP<sup>۱۰</sup>: مدل مبتنی بر شبکه عصبی انتشار به عقب<sup>۱۱</sup> (پس انتشار)

برای ارزیابی کارایی یک رده‌بند از معیارهای بخصوصی استفاده می‌گردد. دو معیار مهم برای ارزیابی کارایی رده‌بندها، معیارهای فراخوان و دقت است که در روابط (۲ و ۱) آمده است [۲۶ و ۹]:

$$Recall, r = \frac{\text{Number of robot sessions found correctly}}{\text{Total number of actual robot sessions}} \quad (1)$$

$$Precision, p = \frac{\text{Number of robot sessions found correctly}}{\text{Total number of predicted robot sessions}} \quad (2)$$

در رابطه (۱) فراخوان نسبت تعداد جلسات حمله رده‌بندی شده به صورت صحیح به تعداد کل جلسات واقعی حمله است. در واقع، فراخوان معیاری برای تحلیل سبک و سنگین نمودن بین خطاهای مثبت درست (ترو پوزتیو)<sup>۱۲</sup> و منفی غلط (فالس نگاتیو)<sup>۱۳</sup> است. در رابطه (۲) دقت نسبت تعداد جلسات حمله رده‌بندی شده به صورت صحیح به تعداد کل جلسات پیش‌بینی شده به‌عنوان حمله است. در حقیقت، دقت معیاری برای تحلیل سبک و سنگین نمودن بین خطاهای مثبت درست (ترو پوزتیو) و مثبت غلط (فالس پوزتیو)<sup>۱۴</sup> است. این دو معیار می‌توانند در قالب

پرداخته می‌شود که باعث صرفه‌جویی در مصرف حافظه و کاهش زمان پردازش گردد. این عمل با کاهش تعداد خصیصه‌ها و حذف خصیصه‌های نامرتبط<sup>۱</sup> و افزونه<sup>۲</sup> انجام می‌پذیرد. افزایش خصیصه‌ها از یک طرف مشکلاتی از قبیل اشغال حجم بیشتر حافظه مصرفی و افزایش زمان پردازش را در رابطه با محاسبات در پی دارد و از طرف دیگر تعداد زیاد خصیصه‌ها فاکتورهای همبستگی خاصی را سبب می‌شود که نتیجه آن تکرار و به هدر دادن اطلاعات است. به همین دلیل نیاز به استفاده از معیارهایی برای کاهش ابعاد خصیصه‌ها بدون کاهش اثر تشخیص است که به مسئله انتخاب بهینه خصیصه‌ها<sup>۳</sup> معروف می‌باشد [۲۲]. چگونگی ارزیابی خوب بودن خصیصه‌ها برای رده‌بندی، مسئله مهمی است. به‌طور کلی، هر خصیصه‌ای که مرتبط به مفهوم کلاس بوده و نسبت به خصیصه‌های دیگر دارای افزونگی نباشد، به‌عنوان خصیصه خوب<sup>۴</sup> ارزیابی می‌گردد. اگر همبستگی بین دو متغیر<sup>۵</sup> به‌عنوان معیار خوب بودن مدنظر قرار گیرد، تعریف بالا به این صورت در می‌آید که یک خصیصه در صورتی خوب است که به‌طور شدیدی همبسته با کلاس بوده، اما با هیچ خصیصه دیگری همبستگی زیاد نداشته باشد. بنابراین مسئله انتخاب خصیصه تبدیل به جستجو برای یافتن معیاری مناسب برای اندازه‌گیری میزان همبستگی بین خصیصه‌ها می‌شود [۲۳].

در این تحقیق، ما از قابلیت‌های وکا، برای انتخاب خصیصه استفاده می‌کنیم. ابزار نرم‌افزار وکا برای انتخاب خصیصه از دو بخش تشکیل شده است. ارزیابی‌کننده خصیصه<sup>۶</sup> روشی را برای ارزیابی زیرمجموعه‌ای از خصیصه‌ها ارائه می‌دهد و روش جستجو<sup>۷</sup> روشی ساخت یافته را بیان می‌کند که به‌وسیله آن فضای جستجوی زیرمجموعه‌های خصیصه‌ها، براساس نوع ارزیابی‌کننده تحت پیمایش قرار می‌گیرد. برخی از ارزیابی‌کننده‌های خصیصه‌ها و روش‌های جستجو در نرم‌افزار وکا که در این تحقیق مورد استفاده قرار گرفته به شرح زیر است [۲۴].

- ارزیابی‌کننده‌های خصیصه: CfsSubsetEval, GainRatioAttributeEval, ChiSquaredAttributeEval, InfoGainAttributeEval
- روش‌های جستجو: GeneticSearch, BestFirst, Ranker, GreedyStepwise

8- Instance based K-Nearest Neighbors (KNN)

9- Sequential Minimal Optimization

10- Multilayer Perceptron

11- Backpropagation Neural Network

12- True Positive

13- False Negative

14- False Positive

1- Irrelevant

2- Redundant

3- Feature Optimum Selection

4- Good

5- Variable

6- Attribute Evaluator

7- Search Method



در این تحقیق از نرم افزار وکا که یک ابزار یادگیری ماشین است برای ساخت مدل، ارزیابی آن و تحلیل مقایسه‌ای استفاده گردید و ابتدا با ترکیب روش‌های مختلف انتخاب خصیصه، مجموعه‌ای از بهترین خصیصه‌ها انتخاب شده و سپس با اجرای چند الگوریتم داده‌کاوی روی داده‌های آموزش، کارایی آن‌ها مورد ارزیابی و مقایسه قرار گرفت. عملیات انتخاب خصیصه، از طریق سازوکارهای انتخاب خصیصه در نرم‌افزار وکا انجام شده و نتایج در جدول (۵) منعکس گردیده است. در ستون اول این جدول، روش انتخاب خصیصه آورده شده و در ستون دوم تعداد خصیصه‌های انتخاب شده از بین ۱۶ خصیصه جدول (۲)، توسط روش مربوطه بیان شده است. ستون سوم اشاره به شماره خصیصه‌های انتخابی دارد. به منظور انتخاب بهترین زیرمجموعه از خصیصه‌ها، کارایی آن‌ها با استفاده از چندین رده‌بند مبتنی بر الگوریتم‌های داده‌کاوی مورد ارزیابی قرار گرفت. برای انجام آزمایشات در نرم‌افزار وکا، ۷۰ درصد مجموعه داده برای آموزش مدل و ۳۰ درصد باقیمانده جهت تست مدل تخصیص داده شد.

جدول (۵). خصیصه‌های انتخابی توسط روش‌های مختلف انتخاب خصیصه

شماره	روش انتخاب خصیصه	تعداد	شماره خصیصه‌های انتخابی
۱	BestFirst+CfsSubsetEval	۶	۱،۹،۱۳،۱۴،۱۵،۱۶
۲	GeneticSearch+CfsSubsetEval	۴	۷،۹،۱۴،۱۵
۳	GreedyStepwise+CfsSubsetEval	۷	۱،۱۱،۱۲،۱۳،۱۴،۱۵،۱۶
۴	Ranker+InfoGainAttributeEval	۱۱	۷،۹،۱۵،۱۶،۱۰،۱۱،۱۴،۱۳،۱۰،۱۱،۲،۱۲
۵	Ranker+GainRatioAttributeEval	۱۱	۷،۱۵،۹،۸،۱۶،۱۴،۱۳،۱۰،۲،۱۰،۱۱
۶	Ranker+ChiSquaredAttributeEval	۹	۹،۱۵،۱۶،۷،۱۰،۱۱،۱۴،۱

جدول (۵) نتایج آزمایشات را نشان می‌دهد. با استفاده از الگوریتم‌های رده‌بندی اشاره شده در ستون دوم جدول، مدل‌های مختلف برای مجموعه خصیصه‌های مختلف ساخته شده است. در این بخش پس از انجام آزمایشات مربوطه، از دو الگوریتم ماشین بردار پشتیبان و شبکه عصبی به دلیل پایین بودن کارایی آن‌ها در تشخیص حملات صرف‌نظر گردید. برای ارزیابی مدل‌ها و مقایسه آن‌ها نسبت به هم از معیارهای دقت، فراخوان و افیک

یک معیار به نام معیار افیک<sup>۱</sup> مطابق رابطه (۳) خلاصه گردند:

$$F_1 = \frac{2 * Recall * Precision}{Recall + Precision} \quad (3)$$

#### ۴- آزمایشات و ارزیابی

آزمایشات ما در این تحقیق بر روی داده‌های ثبت رویداد کارگزار وب یکی از سازمان‌های دولتی در طول شش ماه اول سال ۲۰۱۴ انجام گرفت. در یک کارگزار (سرور) وب، داده‌های ثبت رویداد در قالب فایل‌های متنی و معمولاً به صورت روزانه سازماندهی می‌شود. منبع داده ما، متشکل از ۱۶۹ فایل ثبت رویداد وب است که در یک بازه شش ماهه تولید شده است. با توجه به حجم بالای داده‌ها و نیاز به تجمیع و یکپارچه نمودن آن‌ها، می‌بایست داده‌ها را به یک پایگاه داده قوی مثل اس‌کیوال سرور منتقل نمود. خوشبختانه نرم‌افزار لاگ‌پارزر شرکت مایکروسافت این عملیات تبدیل و انتقال داده را به خوبی انجام می‌دهد. این نرم‌افزار از زبان اس‌کیوال بر روی فایل‌های داده‌های ثبت رویداد پشتیبانی کرده و به راحتی می‌توان پرس‌وجوهای مختلف را بر روی داده‌ها انجام داد. پس از انجام اقدامات لازم، منبع داده انتخابی ما با تعداد ۱۱۴۳۶۵۶۷ رکورد بر روی پایگاه داده، ایجاد گردید. سپس تفکیک فایل‌ها و منابع (صفحات وب، تصاویر، پی‌دی‌اف و فایل متنی روباتز) انجام شده و منبع داده برای ادامه کار براساس اطلاعات آماری جدول (۳) آماده بهره‌برداری گردید. پس از استخراج خصیصه‌های جلسات، کار تخصیص برچسب کلاس به هر بردار خصیصه متناظر با جلسه وب مربوطه انجام پذیرفت. جدول (۴) توزیع برچسب کلاس در مجموعه داده و آمار فراوانی جلسات را در دو برچسب کلاس صفر (۰) و یک (۱) نمایش می‌دهد.

جدول (۳). توزیع آماری رکوردهای منبع داده

تعداد	نوع درخواست
۱۱۴۳۶۵۶۷	کل درخواست‌ها
۶۶۲۲۴۸	صفحات وب
۴۲۹۲۳۰۷	تصویر
۰	فایل پی‌دی‌اف
۲۰۸۵۳	فایل متنی روباتز (robots.txt)

جدول (۴). توزیع برچسب کلاس در مجموعه داده

تعداد	جلسات وب
۱۲۸۸۰۵	کل جلسات
۱۲۵۷۶۷	جلسات با برچسب کلاس ۰ (مرورگر انسانی + روبات وب خوش‌رفتار)
۳۰۲۸	جلسات با برچسب کلاس ۱ (روبات وب مخرب + مراجعه‌کنندگان ناشناس)

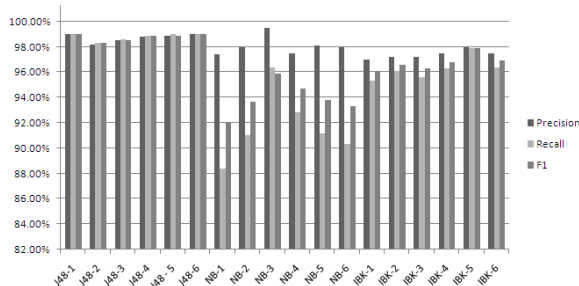
استفاده شده است. همچنین با توجه به اهمیت زمان ساخت هر مدل در ارزیابی و انتخاب آن، اطلاعات مدت زمان ساخت هر

جدول (۶). مقایسه ترکیب‌های مختلف رده‌بند و روش‌های انتخاب خصیصه

ردیف	رده‌بند (Classifier)	شماره روش انتخاب خصیصه	دقت (Precision)	فراخوان (Recall)	معیار افیک (F1_Measure)	زمان ساخت مدل (ثانیه)
۱	J48	۱	۰/۹۹۰	۰/۹۹۰	۰/۹۹۰	۱۹۵/۱۱
۲	J48	۲	۰/۹۸۲	۰/۹۸۲	۰/۹۸۳	۱۱۱/۳۴
۳	J48	۳	۰/۹۸۵	۰/۹۸۶	۰/۹۸۵	۴۱۳/۸۴
۴	J48	۴	۰/۹۸۸	۰/۹۸۹	۰/۹۸۹	۶۴۱/۷۳
۵	J48	۵	۰/۹۸۹	۰/۹۹۰	۰/۹۸۹	۶۰۴/۴۲
۶	J48	۶	۰/۹۹۰	۰/۹۹۰	۰/۹۹۰	۲۵۷/۱۱
۷	NaiveBayes	۱	۰/۹۷۴	۰/۸۸۴	۰/۹۲۱	۶۸/۱۳
۸	NaiveBayes	۲	۰/۹۸۰	۰/۹۱۰	۰/۹۳۷	۴۶/۹۳
۹	NaiveBayes	۳	۰/۹۹۵	۰/۹۶۴	۰/۹۵۹	۷۹/۶۲
۱۰	NaiveBayes	۴	۰/۹۷۵	۰/۹۲۸	۰/۹۴۷	۱۲۸/۵۴
۱۱	NaiveBayes	۵	۰/۹۸۱	۰/۹۱۲	۰/۹۳۸	۱۲۰/۵۹
۱۲	NaiveBayes	۶	۰/۹۸۰	۰/۹۰۳	۰/۹۳۳	۱۱۰/۹۲
۱۳	IBK	۱	۰/۹۷۰	۰/۹۵۳	۰/۹۶۰	۰/۰۵
۱۴	IBK	۲	۰/۹۷۲	۰/۹۶۱	۰/۹۶۶	۰/۰۵
۱۵	IBK	۳	۰/۹۷۲	۰/۹۵۶	۰/۹۶۳	۰/۰۵
۱۶	IBK	۴	۰/۹۷۵	۰/۹۶۳	۰/۹۶۸	۰/۰۶
۱۷	IBK	۵	۰/۹۸۰	۰/۹۷۹	۰/۹۷۹	۰/۰۵
۱۸	IBK	۶	۰/۹۷۵	۰/۹۶۴	۰/۹۶۹	۰/۰۵

برای ساخت مدل ارزیابی انتخاب نمود.

به منظور مقایسه نتایج آزمایش این تحقیق با مطالعه استوانوویچ و همکارانش [۱۳]، آزمایش آن‌ها بر روی مجموعه داده ما و با اجرای الگوریتم درخت تصمیم بر روی مجموعه خصیصه‌های انتخابی توسط آن‌ها انجام پذیرفت. مقایسه کارایی دو آزمایش در جدول (۷) ارائه شده است. همان‌طور که مشاهده می‌شود، در مجموع مقایسه دو عامل کارایی و زمان نشان می‌دهد که چارچوب ارائه شده در تحقیق جاری برای تشخیص روبات‌های وب مخرب (روبات‌های مشارکت‌کننده در حملات منع خدمت توزیعی)، با ۲ درصد افزایش در کارایی و ۲۷ درصد کاهش در زمان ساخت مدل موفق‌تر می‌باشد.



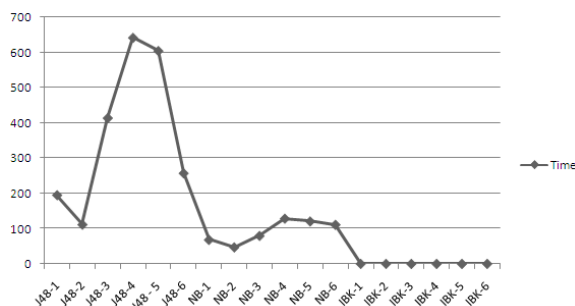
شکل (۴). نمودار مقایسه کارایی ترکیب‌های مختلف رده‌بند و مجموعه خصیصه

شکل‌های (۴ و ۵) نمودار نمایشی گویاتری جهت مقایسه بهتر بین رده‌بندها و مجموعه خصیصه‌های انتخابی هر مدل، ارائه می‌دهند. براساس نمودار شکل (۴)، رده‌بند جی ۴۸ (درخت تصمیم) نسبت به دو رده‌بند نایو بی‌زین و آی‌بی‌کی (نزدیکترین همسایه)، بهترین دقت، فراخوان و افیک را ارائه می‌دهد. کارایی و صحت رده‌بند درخت تصمیم بیش از ۹۸ درصد است. در این آزمایش، الگوریتم درخت تصمیم با شش دسته مجموعه خصیصه انتخابی مورد بررسی قرار گرفته است (ردیف‌های ۱ تا ۶ جدول (۶)). همان‌طور که مشاهده می‌گردد، نتیجه ارزیابی هر شش آزمایش، کارایی بالاتر از ۹۸ درصد را برای این الگوریتم نشان می‌دهد. نقطه ضعف این الگوریتم نسبت به سایر الگوریتم‌ها، براساس نمودار شکل (۵) زمانبر بودن زیاد آن است. الگوریتم نزدیکترین همسایه (ردیف‌های ۱۳ تا ۱۸ جدول (۶))، کارایی کمتری نسبت به درخت تصمیم ارائه می‌دهد ولی در مقابل زمان ساخت مدل در آن بسیار کوتاه است. این نکته حائز اهمیت است که اگرچه زمان ساخت مدل در آن بسیار کوتاه است ولی آزمایشات نشان داد که زمان تست مدل بسیار طولانی می‌باشد. در مجموع، با توجه به مدنظر قرار دادن دو عامل میزان کارایی و زمان‌بری ساخت و تست مدل، می‌توان ردیف ۱ جدول (۶) را با الگوریتم درخت تصمیم و خصیصه‌های شماره ۱، ۹، ۱۳، ۱۴، ۱۵ و ۱۶ به‌عنوان بهترین گزینه با صحت (کارایی) ۹۹ درصد

تشخیص روبات های وب مخرب که مشارکت کننده در حملات دی داس هستند از سایر مرورگران اعم از کاربران انسانی عادی و روبات های وب خوش رفتار ارائه گردید. برای این منظور قبل از هر چیز براساس ویژگی های یک حمله دی داس، خصیصه های مناسب برای تشخیص این گونه روبات های وب مخرب حمله گر تعریف شد. از طریق توجه به ویژگی های حملات دی داس و نیز بررسی رفتار مرورگری روبات های مخرب، می توان به مجموعه ای از بهترین خصیصه ها برای جداسازی روبات های وب مخرب حمله گر از سایر مرورگران انسانی و روباتی دست یافت. به همین دلیل ما خصیصه ها را به دو دسته تقسیم کردیم: دسته اول خصیصه هایی که برای تشخیص هر نوع روباتی قابل استفاده هستند و دسته دوم خصیصه هایی که در تشخیص روبات های دی داس در لایه کاربرد کارایی بهتری را ارائه می دهند. براساس این مطالعه، به طور کلی هر بردار خصیصه متعلق به یکی از چهار گروه مرورگران انسانی، روبات های وب خوش رفتار، روبات های وب مخرب و مراجعه کنندگان ناشناس می باشد.

به دلیل حجم بالای داده های ثبت رویداد، ساخت مدل تشخیص روبات های وب مخرب بسیار پیچیده و نیازمند زمان زیادی برای پردازش است. کاهش تعداد خصیصه ها یعنی انتخاب چند خصیصه از میان خصیصه های استخراج شده، می تواند باعث کاهش زمان پردازش و جلوگیری از پیچیدگی مدل گردد. ما از قابلیت های وکا برای انتخاب مجموعه ای کارآمد از خصیصه ها، استفاده نمودیم. این کار باعث حذف خصیصه های نامرتبط و افزونه شده و نتیجه آن ساخت یک مدل یادگیری اثربخش و کارآمد خواهد بود. در واقع از طریق این بخش از چارچوب پیشنهادی، برای هر سایتی می توان براساس ویژگی های آن، مجموعه مناسبی از خصیصه ها جهت بکارگیری در الگوریتم های داده کاوی، سفارشی سازی نمود. در اینجا، ۶ زیرمجموعه خصیصه مختلف به کمک وکا و توسط الگوریتم های گوناگون استخراج گردید.

پس از آماده شدن مجموعه داده متشکل از بردارهای خصیصه جلسات وب که به هرکدام برچسب تخصیص داده شده است، کار ساخت مدل های مختلف رده بندی انجام پذیرفت. در این مرحله، از نرم افزار وکا استفاده شده و ۵ رده بند روی ۶ مجموعه خصیصه مورد آزمایش قرار گرفت. سپس آزمایشات از لحاظ کارایی و زمان مورد ارزیابی واقع شده و بهترین نتیجه مربوط به الگوریتم درخت تصمیم با مجموعه خصیصه های ویژه حملات دی داس و صحت ۹۹ درصد بود. برای مقایسه نتیجه این تحقیق با کارهای قبلی، مجموعه خصیصه های انتخابی یکی از مهمترین مطالعات در این حوزه، بر روی مجموعه داده موردنظر



شکل (۵). نمودار مقایسه زمان ساخت مدل با ترکیب های مختلف رده بند و مجموعه خصیصه

جدول (۷). مقایسه دو مدل در تحقیق استوانه‌ویچ و تحقیق جاری

تحقیق	رده بند	مجموعه خصیصه های انتخابی	زمان ساخت مدل (ثانیه)	درصد صحت (کارایی)
استوانه‌ویچ	درخت تصمیم (J48)	Click Number HTML-to-Image Ratio %PDF/PS %4xx Error % Head % Unassigned Referrer Robots.txt	۲۶۶/۲۵	۹۷
جاری	درخت تصمیم (J48)	Request Number Client Size Duration Page Popularity Index Request Rate Traffic Rate	۱۹۵/۱۱	۹۹

## ۵- نتیجه گیری

هدف این تحقیق طراحی یک سازوکار دفاعی پویا با قابلیت سفارشی سازی برای تشخیص این نوع روبات های مخرب از طریق تحلیل رفتار آنها و به کارگیری الگوریتم های داده کاوی می باشد. در این روش، استفاده از بردارهای خصیصه های جلسات وب که از منبع داده های ثبت رویداد یک کارگزار وب استخراج می شود، در این الگوریتم های مختلف داده کاوی مدنظر قرار می گیرد. در این تحقیق سعی شد تا با بهینه سازی روش های قبلی تعیین جلسات که در کارهای قبلی ارائه شده بود، بهترین روش تعیین جلسه معرفی گردد. ما برای انجام مراحل پیش پردازش و آماده سازی داده های ثبت رویداد، یک تحلیلگر داده های ثبت رویداد طراحی کردیم و برای تعیین جلسات، استخراج و انتخاب بهترین زیرمجموعه از خصیصه ها و برچسب دهی به جلسات، از آن استفاده شد. برای ساخت مدل های رده بندی و ارزیابی آنها، نرم افزار داده کاوی وکا مورد استفاده قرار گرفت.

در این مطالعه، صرفاً تشخیص روبات های وب از سایر مراجعه کنندگان مدنظر نبوده و بلکه در یک نوآوری، مدلی برای

- [17] D. Stevanovic and N. Vljajic, "An Integrated Approach to Defence Against Degrading Application-Layer DDoS Attacks," Toronto, Canada, 2013.
- [18] H. Liu and V. Keselj, "Combined mining of Web server logs and web contents or classifying user navigation patterns and predicting users' future requests," *Data & Knowledge Engineering*, vol. 61, no. 2, pp. 304-330, 2007.
- [19] 2015. [Online]. Available: <http://www.botsvsbrowsers.com/>.
- [20] 2015. [Online]. Available: <http://www.user-agents.org/>.
- [21] 2015. [Online]. Available: <http://www.useragentstring.com/>.
- [22] K. Selvakuberan, M. Indradevi, and R. Rajaram, "Combined Feature Selection and classification - A novel approach for the categorization of web pages," *Journal of Information and Computing Science*, vol. 3, no. 2, pp. 83-89, 2008.
- [23] L. Yu and H. Liu, "Feature Selection for High-Dimensional Data: A Fast Correlation-Based Filter Solution," in *Proceedings of the Twentieth International Conference on Machine Learning (ICML)*, Washington DC, 2003.
- [24] M. Aggarwal and Amrita, "Performance Analysis of Different Feature Selection Methods In Intrusion Detection," *International Journal of Scientific & Technology Research*, vol. 2, no. 6, pp. 255-231, June 2013.
- [25] I. H. Witten, E. Frank, and M. A. Hall, "Data Mining: Practical Machine Learning Tools and Techniques," Burlington: Morgan Kaufmann - Elsevier, 2011.
- [26] P. N. Tan, M. Steinbach, and V. Kumar, "Introduction to Data Mining," Pearson Education, Inc., 2006.
- [27] "Denial of Service Attacks," [Online]. Available: [http://www.cert.org/tech\\_tips/denial\\_of\\_service.html](http://www.cert.org/tech_tips/denial_of_service.html).
- [28] C. M. Patel, "Survey On Taxonomy of DDoS Attacks With Impact And Mitigation Techniques," *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 9, pp. 1-8, 2012.
- [29] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, pp. 643-666, 2004.
- [30] "Trends in Denial of Service Technology," [Online]. Available: [http://www.cert.org/archive/pdf/DoS\\_trends.pdf](http://www.cert.org/archive/pdf/DoS_trends.pdf).
- [31] H.-V. Nguyen and Y. Choi, "Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDoS Framework," *International Journal of Electrical and Electronics Engineering*, vol. 4, no. 4, pp. 247-252, 2010.
- [32] K. Lee and et al., "DDoS Attack Detection Method Using Cluster Analysis," *Expert Systems with Applications*, vol. 34, no. 3, pp. 1659-1665, 2008.
- [33] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39-53, 2004.
- [34] P. Zaroo, "A Survey of DDoS attacks and some DDoS defense mechanisms," *Advanced Information Assurance (CS 626)*, 2002.
- [35] C. Wilson, "Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress," Washington, DC, 2008.
- [36] J. Mirkovic, J. Martin, and P. Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," Los Angeles, 2002.
- [37] T. Peng, L. Christopher, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Computing Survey*, vol. 39, no. 1, pp. 1-42, 2007.
- آزمایش گردید که نتیجه آن صحت ۹۷ درصد بود و این حکایت از برتری مدل پیشنهادی این تحقیق است.

## ۶- مراجع

- [1] C. Wilson, "Botnets, cyber crime, and cyber terrorism: Vulnerabilities and policy issues for congress," Washington, DC, 2008.
- [2] D. Doran and S. S. Gokhale, "Web robot detection techniques: overview and limitations," *Data Min. Knowl. Disc.*, vol. 22, no. 1-2, pp. 183-210, 2011.
- [3] T. Kabe and M. Miyazaki, "Determining WWW user-agents from server access log," in *Proceedings of seventh international conference on parallel and distributed systems*, 2000.
- [4] P. Huntington, D. Nicholas, and H. R. Jamali, "Web robot detection in the scholarly information environment," *Journal of Information Science*, vol. 34, no. 5, pp. 726-741, 2008.
- [5] N. Geens, J. Huysmans, and J. Vanthienen, "Evaluation of Web robot discovery techniques: a benchmarking study," *Lecture notes in computer science*, vol. 4065, no. 1, pp. 121-130, 2006.
- [6] W. Guo, S. Ju, and Y. Gu, "Web robot detection techniques based on statistics of their requested URL resources," in *Proceedings of ninth international conference on computer supported cooperative work in design*, 2005.
- [7] O. M. Duskin and D. G. Feitelson, "Distinguishing humans from robots in web search logs: preliminary results using query rates and intervals," in *Proceedings of 2009 workshop on Web Search Click Data*, 2009.
- [8] X. Lin, L. Quan, and H. Wu, "An Automatic Scheme to Categorize User Sessions in Modern HTTP Traffic," in *Proceedings of IEEE global telecommunications conference*, 2008.
- [9] P. N. Tan and V. Kumar, "Discovery of Web Robot Sessions Based on their Navigational Patterns," *Data Mining and Knowledge Discovery*, vol. 6, no. 1, pp. 9-35, 2002.
- [10] C. Bomhardt, W. Gaul, and L. Schmidt-Thieme, "Web Robot Detection - Preprocessing Web Log Files for Robot Detection," *New Developments in Classification and Data Analysis*, vol. 1, no. 1, pp. 113-124, 2006.
- [11] A. Stassopoulou and M. D. Dikaiakos, "Web robot detection - A probabilistic reasoning approach," *Computer Networks*, vol. 53, no. 3, pp. 265-278, 2009.
- [12] W.-Z. Lu and S.-Z. Yu, "Web Robot Detection Based on Hidden Markov Model," in *Proceedings of international conference on communications, circuits and systems*, 2006.
- [13] D. Stevanovic, A. An, and N. Vljajic, "Feature evaluation for web crawler detection with data mining techniques," *Expert Systems with Applications*, vol. 39, no. 10, pp. 8707-8717, 2012.
- [14] D. Stevanovic, N. Vljajic, and A. An, "Detection of malicious and non-malicious website visitors using unsupervised neural network learning," *Applied Soft Computing*, vol. 13, no. 1, pp. 698-708, 2013.
- [15] L. V. Ahn and et al., "CAPTCHA: Using Hard AIP Problems for Security," in *Proceedings of Eurocrypt*, 2003.
- [16] K. Park and et al., "Securing Web Service by Automatic Robot Detection," in *Proceedings of the annual conference on USENIX '06 annual technical conference*, 2006.

- [41] P. M. HallamBaker and B. Behlendorf, 2015. [Online]. Available: <http://www.w3.org/TR/WDlogfile.html>.
- [42] J. Lee and et al., "Classification of web robots: An empirical study based on over one billion requests," *computers & security*, vol. 28, pp. 795–802, 2009.
- [43] Z. Chen and W. Feng, "Detecting Impolite Crawler by using Time Series Analysis," in *IEEE 25th International Conference on Tools with Artificial Intelligence (ICTAI)*, pp. 123-126, 2013.
- [44] X. Sun and et al., "Feature selection using dynamic weights for classification," *Knowledge-Based Systems*, vol. 37, no.1, pp. 541–549, 2013.
- [38] K. Arora, K. Kumar, and M. Sachdeva, "Impact Analysis of Recent DDoS Attacks," *International Journal on Computer Science and Engineering (IJCSSE)*, vol. 3, no. 2, pp. 877-884, 2011.
- [39] M. H. Bhuyan and et al., "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions," *The Computer Journal*, 2012.
- [40] S. Noel, D. Wijesekera, and C. Youman, "Modern Intrusion Detection, Data Mining, and Degrees of Attack Guilt," in *Applications of Data Mining in Computer Security*, George Mason, Kluwer Academic Publishers, pp. 1-31, 2003.

Archive of SID

---

## Modeling Browsing Behavior Analysis for Malicious Robot Detection in Distributed Denial of Service Attacks

M. Fathian\*, M. Abdollahi Azgomi, H. Dehghani

\*Iran University of Science and Technology

(Received: 07/05/2015, Accepted: 03/05/2016)

### ABSTRACT

*Distributed denial of service (DDoS) attacks are one of the most important threats for E-commerce. Their main goal is to prevent the users from accessing to web sites and internet resources through excessive use of the resources. In these attacks, availability which is one of the elements of security is targeted. One of the ways to achieve this goal is to apply web robots by which the attackers design and carry out the DDoS attacks at application layer. Various methods have been used to distinguish between malicious and non-malicious web robots. One of the most popular methods in the recent years is data mining and machine learning. This method is based on extracting and selecting those features which are fit for web sessions via web server access log files and applying data mining algorithms. Considering the fact that the DDoS attacks are dynamic and customizable, in this research, an attempt is made to present a customizable dynamic defensive mechanism for detecting malicious web robots through the analysis of behaviors of their browsing. At the present study, features extraction was carried out based on the characteristics of DDoS attacks together with optimization of the previous methods to determine web sessions. Furthermore refining the extracted features and selecting a set of efficient features reduced the time required for building a model. As a consequence, the efficiency enhanced by two percent compared to the best similar study.*

**Keywords:** DDoS Attack, E-Commerce Security, Malicious Web Robot Detection, Data Mining

---

\* Corresponding Author Email: fathian@iust.ac.ir