مجله علمی پژوهشی «پدافند الکترونیکی و سایبری»
سال ششم، شماره ۴، زمستان ۱۳۹۷؛ ص ۸۹-۷۹

شناسایی حملات منع سرویس وب با استفاده از آنتروپی و الگوریتم ماشین بردار پشتیبان

وحید یادگاری، احمدرضا متین‌فر*

۱- کارشناس ارشد مهندسی فناوری اطلاعات، دانشگاه تربیت مدرس، ۲- استادیار، دانشگاه جامع امام حسین(ع)

(دریافت: ۱۳۹۶/۱۰/۰۲، پذیرش: ۱۳۹۷/۰۳/۰۶)

چکیده

با گسترش خدمات مبتنی‌بر اینترنت و توسعه وب‌سایت‌ها، تهدیدات سایبری نیز در حال افزایش است.یکی از این تهدیدات، انجام حملات منع سرویس و ایجاد اختلال در خدمات یک وب‌سایت می باشد. حملات منع سرویس لایه وب و یا کاربردی از طریق ایجاد مصنوعی حجم زیاد ترافیک بر روی وب سرور تولید و باعث اخلال در سرویس‌دهی وب می‌گردد. در این تحقیق برای شناسایی این دسته از حملات، لاگ‌های وب سرور با ایجاد پنجره‌های زمانی ۲۰ ثانیه‌ای و محاسبه میزان فعالیت هر آی‌پی دسته‌بندی گردیده و سپس آنتروپی مربوط به هر آی‌پی در پنجره زمانی محاسبه و از طریق واریانس آنتروپی پنجره‌های زمانی دارای پیوستگی تعیین و در مرحله بعد از طریق الگوریتم ماشین بردار پشتیبان، شبکه آموزش داده می‌شود تا پنجره‌های زمانی ناهنجار و درنهایت آی‌پی آدرس‌هایی که منجر به حملات منع سرویس و یا منع سرویس توزیع‌شده‌اند دسته‌بندی و برچسب‌گذاری شوند. مدل پیشنهادی بر روی مجموعه داده استاندارد EPA-HTTP پیاده‌سازی و نتایج آن با سایر روش‌ها مقایسه گردید که بیانگر بهبود نتایج نسبت به نتایج سایر تحقیق‌های قبل هست.

واژه‌های کلیدی: رخدادهای وب، حملات منع سرویس، واریانس، آنتروپی، ماشین بردار ماشین

۱- مقدمه

ازلحاظ تاریخی، یک مجموعه از حملات منع سرویس که در ماه فوریه سال ۲۰۰۰ علیه سایت‌های یاهو، آمازون و ای بی[1] رخداده که منجر به از دست دادن تقریباً ۱,۲ بیلیون دلار شده است. تحلیلگران تخمین زدند در طول سه ساعت که وب‌سایت یاهو مختل شده بود، حدود ۵۰۰۰۰۰ دلار از دست رفته است. براساس گزارش سایت آمازون، حملات منع سرویس علت از دست دادن ۶۰۰۰۰۰ دلار در طول ۱۰ ساعت خرابی بوده است. به همین ترتیب، در طول حملات منع سرویس علیه ای بی، در دسترس بودن سایت ای بی از ۱۰۰٪ به ۹/۴٪ تنزل یافته بود. در ژانویه ۲۰۰۱، مایکروسافت در طول یک دوره چندروزه حمله منع سرویس در سایت خود حدود ۵۰۰ میلیون دلار را از دست داد. در سال ۲۰۱۱، حملات منع سرویس پنج وب‌سایت با رده‌بالا، یعنی ویزا[2]، مستر کارت[3]، سونی[4]، ورد پرس[5] و سازمان سیا را ویران کرد. امروزه، حملات منع سرویس قادر به تخریب قوی یک سایت در یک حمله ساده هستند. بر طبق برآوردها انتظار می‌رود که هزینه‌های قطع ناگهانی ۲۴ ساعته برای یک شرکت تجارت الکترونیک بزرگ ۳۰ میلیون دلار باشد. یکی از راه‌کارهای حفظ امنیت و پایداری وب‌سایت‌ها و کاهش خسارات مالی و فنی، تحلیل مستمر ترافیک وب هست. ترافیک وب مجموعه درخواست‌ها و پاسخ‌های یک وب هست که در وب سرور ثبت و ذخیره می‌گردد. تحلیل ترافیک این لایه که تحت عنوان رخداد یا لاگ در وب سرور ثبت می‌شود می‌تواند منجر به شناسایی حملات صورت گرفته به وب سرور باشد که به‌واسطه نوع ساختار آن در لایه‌های دیگر مثل لایه سه و چهار شناخته‌نشده است. [۱], [۲].

۲- کلیات و مفاهیم

✓ حملات وب:

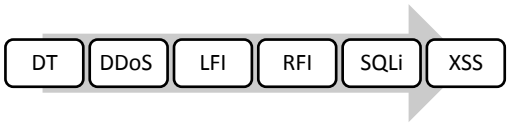
حملات نوع خاصی وجود دارند که به حملات نرم‌افزارهای کاربردی وب[6] و یا لایه هفت شبکه مشهور هستند. لایه هفتم یا لایه کاربردی رابط بین کاربر و سیستم‌عامل محسوب می‌شود و همان‌طور که از اسمش پیداست، می‌توان به‌وسیله این لایه با

*رایانامه نویسنده پاسخگو: a.matinfar@chmail.ir

1- eBay.com
2- Visa
3- MasterCard
4- Sony
5- WordPress

6- Web Application Attacks

نرم‌افزارهای کاربردی ارتباط برقرار کرد. برای مثال وقتی از نرم‌افزار جستجوگر اینترنت[1] برای ارسال درخواست باز کردن صفحه وبی مانند گوگل استفاده می‌شود، در حقیقت از پروتکل HTTP برای ارسال درخواست توسط این نرم‌افزار استفاده می‌شود که همه این‌ها در لایه هفتم از مدل OSI[2] (یک مدل فرضی برای درک مفاهیم شبکه) فعالیت می‌کنند. در شکل (۱) اهم حملات این لایه عنوان‌شده است [۳].



شکل (۱): حملات وب

✓ حملات منع سرویس:

حملات منع سرویس تلاش برای از کار انداختن سامانه کاربر یا یک سازمان است. در حمله منع خدمت، مهاجم تلاش می‌کند تا سامانه‌ها را از حالت پایدار خارج کند و یا سرعت آن را به‌شدت کاهش دهد و کاربران نتوانند از منابع آن استفاده کنند. هدف از این حمله، این نیست که به سامانه یا داده‌های هدف دسترسی پیدا کنند، بلکه هدف این است که اجازه خدمت‌رسانی به کاربران قانونی را بگیرند. حملات منع سرویس توزیع‌شده، نوع پیشرفته حملات منع سرویس ساده است [۴].

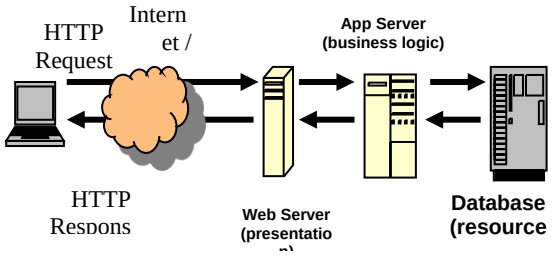
✓ وب سرور[3]:

وب سرور سامانه‌ای است که سایت‌ها بر روی آن قرارگرفته و توانایی پاسخگویی به مرورگر وب و ارسال صفحه درخواستی مرورگر را دارا است. صفحات وب بر پایه‌یک ساختار مشخص و با یک نام یگانه (IP) بر روی وب سرور قرارمی‌گیرند. بر روی یک وب سرور امکان قرار گرفتن صفحات متعدد و با ساختارهای جداگانه وجود دارد. تابع اولیه یک وب سرور ارائه صفحات وب به کاربران است. از انواع وب سرورهای اینترنتی به آپاچی[4] و آی.آی.اس[5] می‌توان اشاره کرد[۱].

✓ لاگ‌های وب‌سایت‌ها:

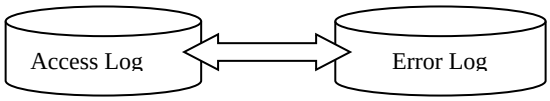
برای بررسی حملات وب می‌توان از لاگ‌های شبکه، لاگ‌های وب سرور و غیره استفاده کرد. ازآنجاکه هدف اصلی این پژوهش در خصوص لاگ‌های وب و به‌طور ویژه وب سرور هست، نیاز است فرآیند مربوط به وب موردتوجه قرار گیرد. شکل (۲) بیانگر فرآیندیک وب هست [۱].

1- Internet Explorer
2- Open System Interconnection
3- Web Server
4- Apache
5- Internet Information Services (IIS)



شکل (۲): فرآیند کاری یک وب

کلیه فعالیت‌های صورت پذیرفته در این فرآیند در فایل‌های همچون Access Log، Error Log (شکل ۳) در سمت سرور و فایل‌های کوکی در سمت کاربر ذخیره و نگهداری می‌گردد.



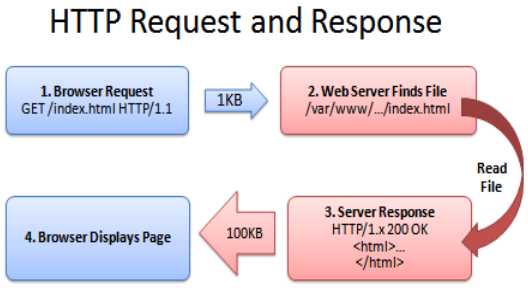
شکل (۳): فایل‌های ثبت لاگ وب

فایل AccessLog در وب سرور آپاچی برای ثبت رخدادهای وب سرور هست (در وب سرور IIS می‌توان اطلاعات فوق را در مسیر مشخص[6] مشاهده نمود). محتوای این فایل به‌صورت متنی ذخیره‌شده و نیاز است برای قالب‌بندی و ایجاد ساختار فیلدها، محتوا در قالب فایل‌هایCSV خوانده‌شده و در مرحله بعد با تفکیک فیلدهای اطلاعاتی، پیش‌پردازش اطلاعات انجام می‌شود. حجم رخدادهای ثبت‌شده با توجه به کارکرد سایت متغیر هست [۲].

✓ داده‌های یک رخداد وب‌سایت:

پیش از آنکه به انواع این‌گونه‌داده‌ها بپردازیم ابتدا تعاریفی از فراداده‌هایی که توسط وب‌سایت تولید و استفاده می‌شوند ارائه می‌کنیم. شکل (۴) یک تراکنش HTTP رابین یک مشتری HTTP و یک سرور HTTP نشان می‌دهد. برای سادگی فرض کنید که مشتری HTTP یک مشتری وب است و یک سرور HTTP نیز یک وب سرورهست. یک مشتری وب که برای کاربران انسانی طراحی‌شده است یک مرورگر وب نامیده می‌شودمانند فایرفاکس[7]، موزیلا[8] و اینترنت اکسپلورر[9]. از وب سرور عبارت‌اند وب سرورهای اینترنتی به آپاچی[10] و آی.آی.اس[11] می‌توان اشاره کرد [۲].

6- LogFiles\W3SVCx
7- Firefox
8- Mozilla
9- Microsoft Internet Explorer.
10- Apache
11- Internet Information Services (IIS)



شکل (۴): تراکنش HTTP

در یک تراکنش HTTP داده‌های کاربرد اساسی با فراداده‌های زیر تعریف می‌شوند:

۱) آدرس IP ماشین مشتری؛
۲) شناسه کاربر درصورتی‌که فرایند تصدیق HTTP را انجام می‌دهد.
۳) زمانی که سرور پردازش درخواست را انجام می‌دهد.
۴) متد HTTP (GET، POST، ...)
۵) URI درخواست
۶) پروتکل و نسخه‌ی پروتکل مانند HTTP1.0، HTTP 1.1 و ...
۷) کد وضعیت HTTP که به مشتری پس‌فرستاده می‌شود.
۸) اندازه‌ی پاسخ برحسب بایت
۹) ارجاع دهنده که URI ای است که گزارش‌ها مشتری از آن ارجاع شده‌اند.
۱۰) عامل کاربر که شامل اطلاعاتی است که مرورگر مشتری در مورد خود گزارش می‌کند. این اطلاعات شامل این موارد است: نام مرورگر، نسخه آن و سیستم‌عاملی که مرورگر بر روی آن در حال اجراست.

✓ داده‌کاوی[1] رخدادهای وب:

داده‌کاوی به مفهوم استخراج اطلاعات نهان یا الگوها و روابط مشخص در حجم زیادی از داده‌ها در یک یا چند بانک اطلاعاتی بزرگ است. با توجه به حجم بالای رخدادهای یک وب سرور، از تکنیک‌های داده‌کاوی برای شناسایی و کشف الگوها استفاده می‌گردد [۵].

✓ آنتروپی:

آنتروپی اطلاعات که به نام آنتروپی شانون هم شناخته می‌شود[2] حاکی از تمایل سیستم‌ها به کهولت و بی‌نظمی است. سیستم‌های بسته به‌مرور زمان ازهم گسیخته می‌شوند، زیرا انرژی یا داده جدید از محیط دریافت نمی‌کنند ولی سیستم‌های باز آنتروپی منفی دارند یعنی می‌توانند خود را ترمیم کرده با حفظ ساختار خود زنده بمانند و حتی با واردکردن انرژی اضافی یعنی ورود انرژی بیش از صدور آن رشد می‌کند [۵].

آنجا که حملات منع سرویس حاکی از ایجاد یک سربار اضافی باهدف ایجاد اختلال و متوقف نمودن فعالیت‌های یک وب هست، به‌نوعی سیستم هدف دچار درهم‌ریختگی، بی‌نظمی و کهولت می‌گردد که میزان این به‌هم‌ریختگی و آشفتگی را می‌توان با محاسبه آنتروپی هر IP محاسبه نمود. برای محاسبه آنتروپی IP از رابطه (۱) استفاده می‌کنیم. نتیجه آنتروپی بیانگر رفتار نرمال، غیرمعمول و بحرانی یک IP در یک وب سرور هست [۶].

$$p(x_i) = s_i / \sum_{i=1}^{n} s_i$$
$$Entropy = -\sum_{x} p(x_i) log p(x_i) = E[log\{\frac{1}{p(x_i)}\}] \quad (۱)$$

✓ واریانس:

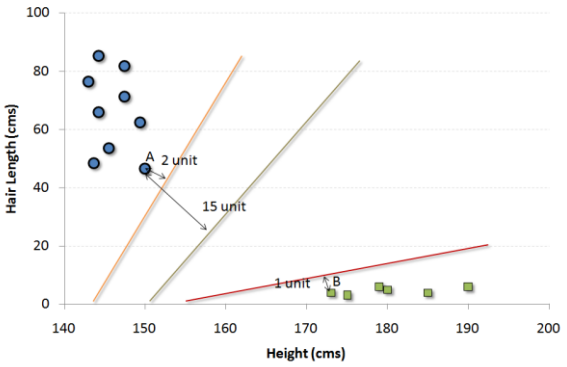
یکی از شاخص‌های پراکندگی هست که برای به‌دست‌آوردن آن باید ابتدا میانگین داده‌ها را به‌دست آوریم، سپس هرکدام از داده‌ها را از میانگین کم نموده سپس حاصل به‌دست‌آمده را به توان ۲ می‌رسانیم و درنهایت همه را باهم جمع نموده تقسیم‌بر تعداد داده‌ها می‌کنیم. رابطه (۲) مربوط به واریانس هست [۷].

$$\sigma^2 = (\sum(Xi - \bar{X})2)/N \quad (۲)$$

✓ ماشین بردار پشتیبان:

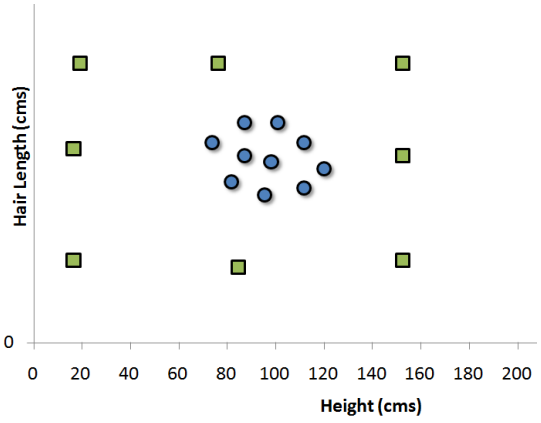
بردارهای پشتیبان به زبان ساده، مجموعه‌ای از نقاط در فضای n بعدی داده‌ها هستند که مرز دسته‌ها را مشخص می‌کنند و مرزبندی و دسته‌بندی داده‌ها بر اساس آن‌ها انجام می‌شود و با جابجایی یکی از آن‌ها، خروجی دسته‌بندی ممکن است تغییر کند. در فضای دوبعدی، بردارهای پشتیبان، یک خط، در فضای سه‌بعدی یک صفحه و در فضای n بعدی یک ابر صفحه را شکل خواهند داد. در ماشین بردار پشتیبان، فقط داده‌های قرارگرفته در بردارهای پشتیبان مبنای یادگیری ماشین و ساخت مدل قرار می‌گیرند و این الگوریتم به سایر نقاط داده حساس نیست و هدف آن‌هم یافتن بهترین مرز در بین داده‌هاست به‌گونه‌ای که بیشترین فاصله ممکن را از تمام دسته‌ها (بردارهای پشتیبان آن‌ها) داشته باشد. برای ایجاد یک ماشین بر مبنای بردارهای پشتیبان، به‌ازای داده‌های موجود در مجموعه داده، تعداد زیادی مرزبندی می‌توانیم داشته باشیم. در شکل (۵) یک مجموعه دارای سه مرزبندی نمایش داده شده است.

1-Data mining
۲- متأثر از نام Claude E. Shannon ریاضی‌دان آمریکایی



شکل (۵): مجموعه دارای سه مرزبندی

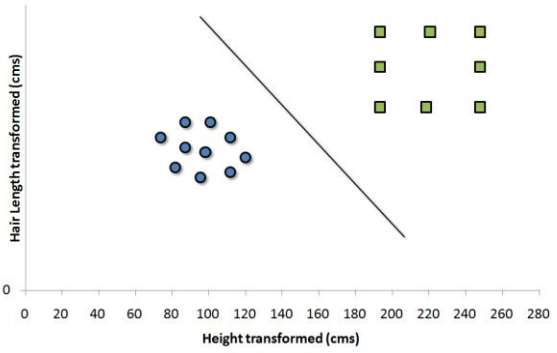
یک‌راه ساده برای انجام این کار و ساخت یک دسته‌بند بهینه، محاسبه فاصله‌ی مرزهای به‌دست‌آمده با بردارهای پشتیبان هر دسته (مرزی‌ترین نقاط هر دسته یا کلاس) و درنهایت انتخاب مرزی است که از دسته‌های موجود، مجموعاً بیشترین فاصله را داشته باشد که در شکل (۵) خط میانی، تقریب خوبی از این مرز است که از هر دودستهفاصله زیادی دارد. این عمل تعیین مرز و انتخاب خط بهینه (در حالت کلی، ابر صفحه مرزی) به‌راحتی با انجام محاسبات ریاضی نه‌چندان پیچیده قابل پیاده‌سازی است. اگرداده‌ها به‌صورت خطی قابل‌تفکیک باشند، الگوریتم فوق می‌تواند بهترین ماشین را برای تفکیک داده‌ها و تعیین دسته یک رکورد داده، ایجاد کند اما اگر داده‌ها به‌صورت خطی توزیع و یا عبارتی غیرخطی مانند شکل (۶) باشد.



شکل (۶): مجموعه داده‌های غیرخطی

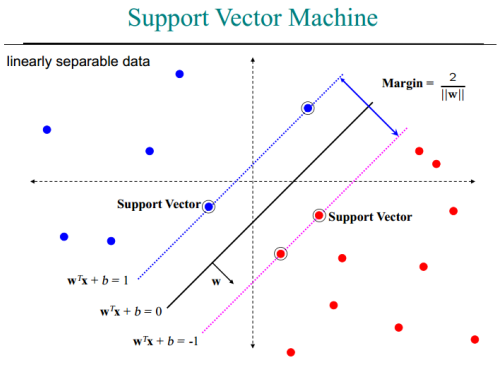
ما نیاز داریم داده‌ها را به کمک یک تابع ریاضی[1]، در یک فضای دیگر نگاشت کنیم که در آن فضا، داده‌ها تفکیک‌پذیر باشند تا بتوان SVM آن‌ها را به‌راحتی تعیین کرد. تعیین درست این تابع نگاشت در عملکرد ماشین بردار پشتیبان مؤثر است. با فرض یافتن تابع تبدیل برای مثال فوق، فضای داده ما برابر شکل (۷) خواهد شد.

1- Kernel functions



شکل (۷): فضای داده با تابع نگاشت

همان‌طور که اشاره شد، ماشین بردار پشتیبان داده‌ها را با توجه به دسته‌های از پیش تعیین‌شده آن‌ها به یک فضای جدید می‌برد به‌گونه‌ای که داده‌ها به‌صورت خطی (ابر صفحه) قابل‌تفکیک و دسته‌بندی باشند و سپس با یافتن خطوط پشتیبان (صفحات پشتیبان در فضای چندبعدی)، سعی دریافتن معادله خطی دارد که بیشترین فاصله رابیندودسته ایجاد می‌کند. در شکل (۸) داده‌ها در دودسته آبی و قرمز نمایش داده‌شده‌اند و خطوط نقطه‌چین، بردارهای پشتیبان متناظر با هر دسته را نمایش می‌دهند که با دایره‌های دو خط مشخص شده‌اند و خط سیاه ممتد نیز همان SVM است. بردارهای پشتیبان هم هرکدام یک رابطه مشخصه دارند که خط مرزی هر دسته را توصیف می‌کند [۷].



شکل (۸): بردارهای پشتیبان متناظر با هر دسته

۳- پیشینه پژوهش

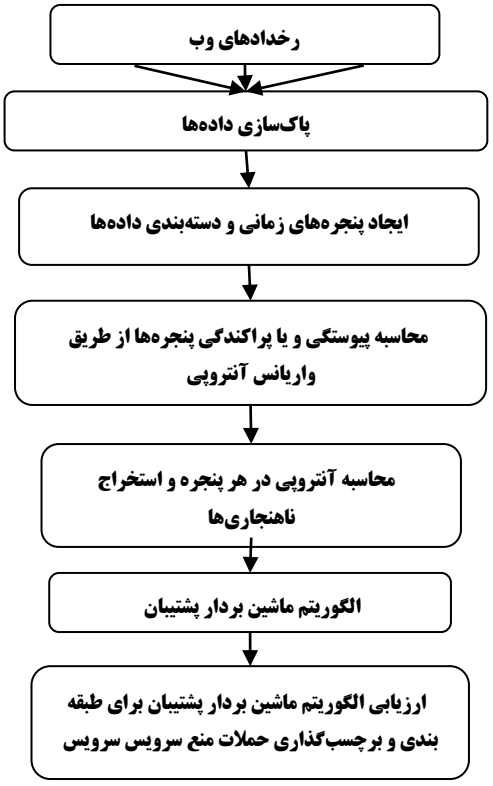
- جانسون [۷] در پژوهش خود ترافیک HTTP را در پنجره‌های زمانی ۲۰ ثانیه‌ای دسته‌بندی کرده و بعد از محاسبه آنتروپی و واریانس آن حملات منع سرویس را شناسایی کرده و از طریق یک الگوریتم ترکیبی دسته‌بندی مبتنی‌بر شبکه‌های عصبی مصنوعی و ژنتیک رفتارهای هنجار و ناهنجار سیستم را تعیین کردند.

- آدبی [۸] در پژوهش خود تجزیه‌وتحلیل ترافیک حملات انجام‌شده با استفاده از سه تکنیک یادگیری ماشین، یعنی، درخت تصمیم و ماشین بردار پشتیبان را پیاده‌سازی کردند.
- در [۶]، یک سازوکار تشخیصی و دفاعی یکپارچه برای ایجاد و شناسایی حملات DDoS با استفاده از الگوریتم‌های یادگیری ماشین‌ها مانند شبکه عصبی عقب[1]، نقشه خودسازمانده[2] و دستگاه بردار پشتیبانی[3] و شناسایی آدرس IP واقعی از منبع حمله تفسیر شده با استفاده از سازوکار دفاعی مبتنی بر آنتروپی ارائه داد.
- اکبری در پژوهش خود [۴]، رصد قربانی با استفاده از انواع حسگرهای سایبری اعم از فنی و بشری را مدل‌سازی و شبیه‌سازی کرده‌اند. در ابتدا حسگرهای فضای سایبری مانند سایت‌های خبری، شبکه‌های اجتماعی و گزارش‌های مردمی و حسگر دیده‌بانی فنی را بررسی و خصیصه‌های احصاء شده و درنهایت اهمیت هر یک را با استفاده ازنظر خبرگان با استفاده از روش فرآیند تحلیل سلسله مراتبی، ارزش‌گذاری کرده‌اند. سپس ترکیبی از خصیصه‌ها را برای هریک از حسگرها تشکیل داده و وضعیت‌های قربانی را نسبت به آن تعیین کرده‌اند. شرایط تلفیق اطلاعات با استفاده از روش دسته‌بندی بر اساس منطق فازی مهیا گردیده است. با اجرای سه سناریو نشان داده شده است که طرح فوق دارای کارایی مطلوب است.
- در پژوهش مهنانی [۹]، یک طرح جدید از دسته‌بندی ترافیک با ترکیب تکنیک‌های یادگیری ماشین با ناظر و بدون ناظر برای چالش یادشده ارائه‌شده است. طرح پیشنهادی قابلیت شناسایی ترافیک حملات با استفاده از تبعیض کلاس‌های از پیش تعریف‌شده را دارد. در طرح پیشنهادی از ترکیب الگوریتم‌های FCM و TWSVM جهت شناسایی و دسته‌بندی حملات استفاده‌شده است.
- در مقاله خیرخواه و دیگران [۱۰] برای مدل‌سازی در مرحله تولید دنباله‌ها برای اولین بار در حوزه سایبری از یک خوشه‌بندی جدید به‌عنوان خوشه‌بندیIMD_DBSCAN که یکی از انواع بهبودیافته خوشه‌بندیDBSCAN افزایشی است، استفاده کرده‌اند. علاوه بر این از یک الگوریتم حریصانه با الهام از القاء گرامر در پردازش زبان طبیعی استفاده‌شده تا با ادغام فعالیت‌های سطح پایین به فعالیت‌های سطح بالا دست‌یابی داشته باشند. در الگوریتم پیشنهادی در بخش ادغام و تشخیص فعالیت‌های سطح بالا، برای اولین بار یک معیار شباهت به معیارهای موجود اضافه شده است. این معیار برگرفته از فاصله ویرایش یا فاصله لون اشتاین است که برای محاسبه میزان تفاوت میان دو رشته در علوم کامپیوتر و نظریه داده‌ها استفاده می‌شود

1- BPNN
2- SOM
3- ESVM

۴- مدل پیشنهادی

مدل پیشنهادی برابر شکل (۹) است. در مرحله اول مدل پیشنهادی ضمن خلاصه‌سازی و تجمیع انبوه رخدادهای ثبت‌شده، نسبت به‌شناسایی ناهنجاری‌ها که بیانگر حملات مشکوک به منع سرویس است اقدام خواهد شد. برای این کار ابتدا با ایجاد پنجره‌های زمانی ۲۰ ثانیه‌ای، میزان فعالیت هر آی‌پی دسته‌بندی و محاسبه گردیده و سپس آنتروپی مربوط به هر آی‌پی در پنجره زمانی محاسبه و از طریق واریانس آنتروپی پنجره‌های زمانی دارای پیوستگی تعیین و در مرحله بعد از طریق الگوریتم ماشین بردار پشتیبان، شبکه آموزش داده می‌شود تا پنجره‌های زمانی ناهنجار و درنهایت آی‌پی آدرس‌هایی که منجر به حملات منع سرویس و یا منع سرویس توزیع شده‌اند شناسایی دسته‌بندی و برچسب‌گذاری شوند.



شکل (۹): چارچوب مدل پیشنهادی

۵- دیتاست استاندارد برای پیاده‌سازی مدل

دیتاست EPA-HTTP مجموعه استاندارد متشکل از ثبت درخواست‌هایHTTP در مدت‌زمانی یک‌روزه است. سرور این مجموعه در پارک تحقیقاتی مثلث[1] مستقراست. این مجموعه داده استاندارد در اکثر مقالات علمی برای آزمودن الگوریتم‌های پیشنهادی مورداستفاده قرار گرفته است [۱۱].

۶- مراحل اجرا و تجزیه‌وتحلیل داده‌ها

برای پیاده‌سازی مدل پیشنهادی (شکل ۹) از نرم‌افزار متلب و ابزارهای مرتبط با ماشین‌بردار پشتیبان در آن استفاده‌شده که ترتیب مراحل و نتایج آن به شرح ذیل است

۶-۱- رخدادهای خام وب و پاک‌سازی داده‌ها:

همان‌طور که قبلاً مطرح شد رخدادهای وب سرور در وب سرور آپاچی در فایل AccessLog ذخیره می‌شود و برای انجام پیش‌پردازش اطلاعات فایل موردنظر را در قالب فایل‌های CSV خوانده می‌شوند و در مرحله بعد با تفکیک فیلدهای اطلاعاتی، پیش‌پردازش اطلاعات انجام می‌شود. حجم رخدادهای ثبت‌شده با توجه به کارکرد سایت متغیراست.

۶-۲- ایجاد پنجره‌های زمانی:

پس از پیش‌پردازش اولیه، تجمیع داده‌ها صورت می‌پذیرد. در این مرحله می‌بایستی با توجه به حجم رخدادها و نوع فیلدهای موجود، خلاصه‌سازی و کاهش ابعاد و ایجاد فیلدهای جدید در یک محدوده زمانی خاص بر اساس رابطه (۳) و الگوریتم شکل (۱۰) (در اکثر مقالات پنجره‌های زمانی به‌صورت ۲۰ ثانیه‌ای تشکیل شده‌اند) صورت پذیرد [۷].

$$\Delta t = (< X1\ S1 >< X2, S2 > \cdots) \qquad (۳)$$

Δt: محدوده زمانی در نظر گرفته‌شده برای دسته‌بندی رخدادهای وب.

X1: اشاره به یک آی‌پی در پنجره زمانی دارد.

S1: اشاره به تعداد رخدادهای وب از آی‌پی X در محدوده زمانی Δt دارد.

1- Research Triangle Park

```
Algorithm 1 HTTP GET Flow Count for the N
    Participating Clients for Every 20 s Time Window
1: Begin
    2: for (Frame.Timei =
    strx;Frame.Timei<Frame.Timei +20;i+ +)
        3: for (IPj = 1;IPj ≤N;j+ +)
            4:Compute I =(IPj&&IPdst)
            5:Compute HGET =
            (http.request.method == GET)
            6: Compute Final = I && HGET
        7: end for
    8: end for
9: end
```

شکل (۱۰): الگوریتم ایجاد پنجره‌های زمانی

پس ازا جرای شبه الگوریتم شکل (۱۰)، جداول ۵ گانه (۵-۱) به‌عنوان خروجی این مرحله استخراج خواهد شد.

جدول (۱): پنجره زمانی ۱

Num	Source Address	Des_ Address	Count
۱	۲۰۲,۱,۱۷۵,۲۵۲	۷۱,۱۲۶,۲۲۲,۶۴	۱۲۱۳
۲	۱۹۲,۱۲۰,۱۴۸,۲۲۷	۷۱,۱۲۶,۲۲۲,۶۴	۱۲۴۲
۳	۵۱,۵۸,۱۶۶,۲۰۱	۷۱,۱۲۶,۲۲۲,۶۴	۲۲۱
۴	۱۹۲,۹۵,۲۷,۱۹۰	۷۱,۱۲۶,۲۲۲,۶۴	۱۸۵۶
۵	۵۱,۱۳۷,۲۹۹,۲۵۵	۷۱,۱۲۶,۲۲۲,۶۴	۷۳۹
۶	۴۰,۷۵,۸۹,۷۲	۷۱,۱۲۶,۲۲۲,۶۴	۱۱۸۲

جدول (۲):پنجره زمانی ۲

Num	Source Address	Des_Address	Count
۱	۲۰۲,۱,۱۷۵,۲۵۲	۷۱,۱۲۶,۲۲۲,۶۴	۶۱۹
۲	۱۹۲,۱۲۰,۱۴۸,۲۲۷	۷۱,۱۲۶,۲۲۲,۶۴	۶۳۷
۳	۵۱,۵۸,۱۶۶,۲۰۱	۷۱,۱۲۶,۲۲۲,۶۴	۷۸
۴	۱۹۲,۹۵,۲۷,۱۹۰	۷۱,۱۲۶,۲۲۲,۶۴	۱۰۲۵
۵	۵۱,۱۳۷,۲۹۹,۲۵۵	۷۱,۱۲۶,۲۲۲,۶۴	۳۲۲
۶	۴۰,۷۵,۸۹,۷۲	۷۱,۱۲۶,۲۲۲,۶۴	۶۰۰

جدول (۳): پنجره زمانی ۳

Num	Source Address	Des_Address	Count
۱	۲۰۲,۱,۱۷۵,۲۵۲	۷۱,۱۲۶,۲۲۲,۶۴	۱۲۲۹
۲	۱۹۲,۱۲۰,۱۴۸,۲۲۷	۷۱,۱۲۶,۲۲۲,۶۴	۱۲۷۸
۳	۵۱,۵۸,۱۶۶,۲۰۱	۷۱,۱۲۶,۲۲۲,۶۴	۳۰۱
۴	۱۹۲,۹۵,۲۷,۱۹۰	۷۱,۱۲۶,۲۲۲,۶۴	۱۸۰۳
۵	۵۱,۱۳۷,۲۹۹,۲۵۵	۷۱,۱۲۶,۲۲۲,۶۴	۲۱۷
۶	۴۰,۷۵,۸۹,۷۲	۷۱,۱۲۶,۲۲۲,۶۴	۱۲۰۱

جدول (۴): پنجره زمانی ۴

Num	Source Address	Des_Address	Count
۱	۲۰۲,۱,۱۷۵,۲۵۲	۷۱,۱۲۶,۲۲۲,۶۴	۱۲۵۳
۲	۱۹۲,۱۲۰,۱۴۸,۲۲۷	۷۱,۱۲۶,۲۲۲,۶۴	۱۲۷۳
۳	۵۱,۵۸,۱۶۶,۲۰۱	۷۱,۱۲۶,۲۲۲,۶۴	۳۳۴
۴	۱۹۲,۹۵,۲۷,۱۹۰	۷۱,۱۲۶,۲۲۲,۶۴	۱۷۳۴
۵	۵۱,۱۳۷,۲۹۹,۲۵۵	۷۱,۱۲۶,۲۲۲,۶۴	۷۷
۶	۴۰,۷۵,۸۹,۷۲	۷۱,۱۲۶,۲۲۲,۶۴	۱۰۹۹

جدول (۵): پنجره زمانی ۵

Num	Source Address	Des_Address	Count
۱	۲۰۲,۱,۱۷۵,۲۵۲	۷۱,۱۲۶,۲۲۲,۶۴	۱۲۳۶
۲	۱۹۲,۱۲۰,۱۴۸,۲۲۷	۷۱,۱۲۶,۲۲۲,۶۴	۱۲۷۷
۳	۵۱,۵۸,۱۶۶,۲۰۱	۷۱,۱۲۶,۲۲۲,۶۴	۳۷۷
۴	۱۹۲,۹۵,۲۷,۱۹۰	۷۱,۱۲۶,۲۲۲,۶۴	۱۷۱۳
۵	۵۱,۱۳۷,۲۹۹,۲۵۵	۷۱,۱۲۶,۲۲۲,۶۴	۱۱۶
۶	۴۰,۷۵,۸۹,۷۲	۷۱,۱۲۶,۲۲۲,۶۴	۱۱۴۸

برای محاسبه آنتروپی هر آی پی در پنجره‌های زمـانی و واریـانس آنتروپی در هر پنجره ازرابطه (۴) استفاده می‌کنیم

نتـایج آنتروپـی هـر آی‌پـی در پنجـره زمـانی و محاسـبه میـانگین و واریانس آنتروپی‌ها در هر پنجره با استفاده از رابطه (۴) برابر جدول‌های شکل (۶ و ۷) است و نمودارهای آن برابر شکل‌های (۱۲-۱۱) می باشد.

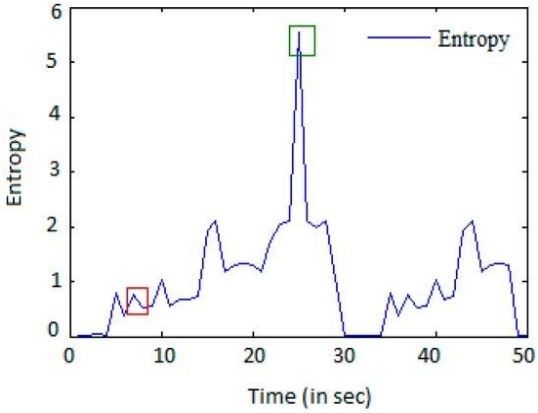
$$E(i.wt) = -\log\frac{C(i.Wt)}{\sum_{i=1}^{n} C(i.Wt)} + \lambda(i.Wt)$$

$$\lambda(i.Wt) = \{\left|\log\frac{C(i.Wt+1)}{C(i.Wt)}\right| . C(i.Wt) \geq C(i.Wt+1) \quad (۴)$$

$$\lambda(i.Wt) = \{\left|\log\frac{C(i.Wt)}{C(i.Wt+1)}\right| . C(i.Wt) \geq C(i.Wt+1)$$

جدول (۶): جدول آنتروپی

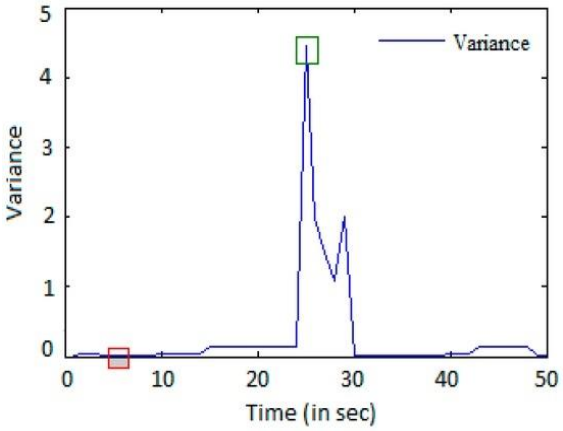
آدرس منبع	آنتروپی				
	پنجره ۱	پنجره ۲	پنجره ۳	پنجره ۴	پنجره ۵
۱. ۱۷۲. ۲۵۲ ۲۰۲.	۰۱۸.۱	۰۲۲.۱	۵۴۴.۰	۶۶۹.۰	۶۷۸.۰
۱۴۸. ۲۲۷ ۱۹۲. ۱۲۰.	۰۰۶.۱	۰۱۴.۱	۵۲۱.۰	۶۵۷.۰	۶۶۳.۰
۵۸. ۱۶۶. ۲۰۱ ۵۱.	۹۱۸.۱	۲۱۱.۲	۱۹۲.۱	۲۹.۱	۳۱۹.۱
۹۵. ۲۷. ۱۹۰ ۱۹۲.	۷۹۹.۰	۷۵۱.۰	۳۸۷.۰	۵۲۷.۰	۵۴۸.۰
۲۹۹. ۲۵۵ ۵۱. ۱۷۳.	۳۰۲.۱	۱۷۹.۱	۷۳۹.۱	۰۵۲.۲	۱۰۶.۲
۷۵. ۸۹. ۱۷۲ ۴۰.	۰۳۲.۱	۰۳۸.۱	۵۸۵.۰	۷۳۸.۰	۷۴۵.۰



شکل (۱۱): خروجی آنتروپی

جدول(۷):جدول واریانس آنتروپی

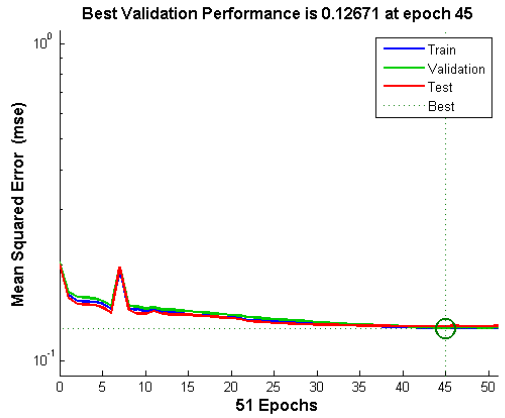
آدرس منبع	متوسط	واریانس	تقریبی
۲۰۲. ۱. ۱۷۲. ۲۵۲	۰/۷۸۶	۰/۰۳۸۶۸۷	۰/۰۳۹
۱۹۲. ۱۲۰. ۱۴۸. ۲۲۷	۰/۷۷۲	۰/۰۴۰۲۸۵	۰/۰۴
۵۱. ۵۸. ۱۶۶. ۲۰۱	۱/۵۸۶	۰/۱۹۲۹۹۸	۰/۱۶۳
۱۹۲. ۹۵. ۲۷. ۱۹۰	۰/۶۰۲	۰/۰۱۳۹۱	۰/۰۱۴
۵۱. ۱۷۳. ۲۹۹. ۲۵۵	۱/۶۷۶	۰/۱۴۳۴۲۶	۰/۱۴۳
۴۰. ۷۵. ۸۹. ۱۷۲	۰/۸۲۸	۰/۰۳۱۹۵۱	۰/۰۳۲



شکل (۱۲): خروجی واریانس آنتروپی و حملات

۴-۶- استفاده از ماشین بردار پشتیبان برای کلاسه‌بندی و برچسب‌گذاری حملات:

همان‌طورکه در شکل (۹) اشاره گردید پس از شناسایی ناهنجاری‌های و تشکیل پنجره‌های زمانی، نیاز است شبکه آموزش داده شود تا بقیه لاگ‌ها مبتنی‌بر نمونه انجام‌شده برچسب‌گذاری شده و رفتارهای عادی و ناهنجار از هم تفکیک شوند. ما برای این کار از ماشین بردار پشتیبان استفاده کرده (خروجی برابر شکل (۱۳) است) و نتایج آن را با سایر کارها مقایسه کرده‌ایم. ماشین بردار پشتیبان یا SVM داده‌ها را با توجه به دسته‌های از پیش تعیین‌شده آن‌ها به یک فضای جدید می‌برد به‌گونه‌ای که داده‌ها به‌صورت خطی (ابر صفحه) قابل‌تفکیک و دسته‌بندی باشند و سپس با یافتن خطوط پشتیبان (صفحات پشتیبان در فضای چندبعدی)، سعی دریافتن معادله خطی دارد که بیشترین فاصله را بین دودسته ایجاد می‌کند

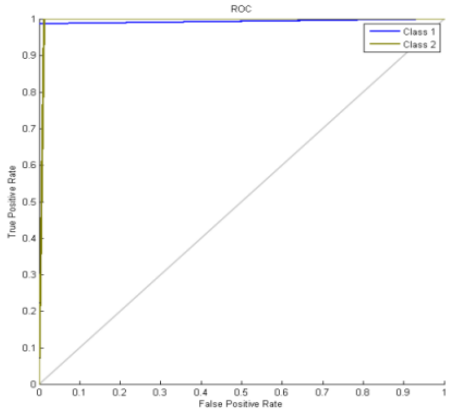


شکل (۱۳): آموزش داده‌های ورودی

در قدم اول نیاز است نمودار تأیید اعتبار برای آموزش داده‌های ورودی را بررسی کنیم. این نمودار در شکل (۱۳)

ارائه‌شده است. تحلیل این نمودار بیانگر این موضوع است که بهترین عملکرد اعتبار سنجی، در زمان مقرر، ۰/۰۱۲۶۷۱ است. در شکل (۱۳)، روند اعتبارسنجی، روند آموزش و خطای آزمودن (به‌ترتیب با خطوط سبز، آبی و قرمز) با افزایش دوره زمان یا حجم آموزش کاهش می‌یابد.

نمودارمشخصه عملیاتی گیرنده[1] (شکل ۱۴) روشی برای بررسی کارایی دسته‌بندها است. درواقع منحنی‌های نمودار مشخصه عملیاتی گیرنده، منحنی‌های دوبعدی هستند که در آن‌ها نرخ تشخیص صحیح دسته مثبت[2] روی محور Y و به‌طور مشابه نرخ تشخیص غلط دسته منفی[3] روی محور X رسم می‌شوند. به‌بیان‌دیگر یک منحنی مشخصه عملیاتی گیرنده مصالحه نسبی میان سودها و هزینه‌ها را نشان می‌دهد. منحنی مشخصه عملیاتی گیرنده اجازه مقایسه تصویری مجموعه‌ای از دسته‌بندی کننده‌ها را می‌دهد، همچنین نقاط متعددی در فضای مشخصه عملیاتی گیرنده قابل‌توجه است. نقطه پایین سمت چپ (۰, ۰) استراتژی را نشان می‌دهد که در یک دسته‌بندی مثبت تولید نمی‌شود. استراتژی مخالف که بدون شرط دسته‌بندهای مثبت تولید می‌کند، با نقطه بالا سمت راست (۱, ۱) مشخص می‌شود. نقطه (۰, ۱) دسته‌بندی کامل و بی‌عیب را نمایش می‌دهد. به‌طورکلی یک نقطه در فضای مشخصه عملیاتی گیرنده بهتر از دیگری است اگر در شمال غربی‌تر این فضا قرارگرفته باشد. همچنین در نظر داشته باشید منحنی‌های مشخصه عملیاتی گیرنده رفتار یک دسته‌بندی کننده را بدون توجه به توزیع دسته‌ها یا هزینه خطا نشان می‌دهند، بنابراین، کارایی دسته‌بندی را از این عوامل جدا می‌کنند. فقط زمانی که یک دسته‌بندی در کل فضای کارایی به‌وضوح بر دسته دیگری تسلط یابد، می‌توان گفت که بهتر از دیگری است [۱۱].



شکل (۱۴):نمودارمشخصه عملیاتی گیرنده

1- Receiver operating characteristic (ROC)
2- True Positive Rate(TPR)
3- False Positive Rate (FPR)

$$
\begin{aligned}
&\text{I:} && CA = \frac{TN+TP}{TN+FN+TP+FP} \\
&\text{II:} && ER = \frac{FN+FP}{TN+FN+TP+FP} = 1 - CA \\
&\text{III:} && DR = \frac{TP}{FN+TP} \\
&\text{IV:} && FAR = \frac{FP}{TN+FP}
\end{aligned}
\qquad (۵)
$$

TN: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها منفی بوده و الگوریتم دسته‌بندی نیز دسته آن‌ها را به‌درستی منفی تشخیص داده است.

TP: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها مثبت بوده و الگوریتم دسته‌بندی نیز دسته آن‌ها را به‌درستی مثبت تشخیص داده است.

FP: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها منفی بوده و الگوریتم دسته‌بندی دسته آن‌ها را به‌اشتباه مثبت تشخیص داده است.

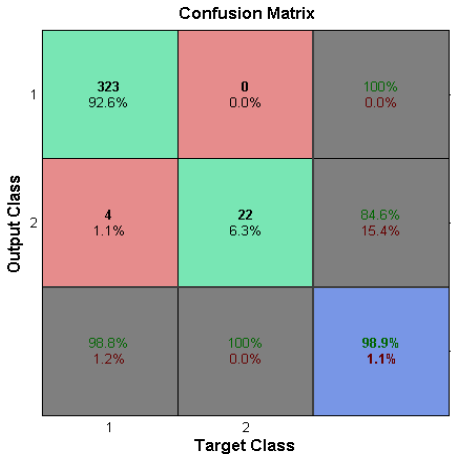
FN: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها مثبت بوده و الگوریتم دسته‌بندی دسته آن‌ها را به‌اشتباه منفی تشخیص داده است.

جدول (۸):ارزیابی دسته‌بندیSVM

CA	ER	DR	FAR
۰/۹۸۸۵۳۸۷	۰/۰۱۱۴۶۱۳۱۸	۱	۰/۱۵۳۸۴۶

همانطور که جدول (۸) در خصوص ارزیابی دسته بندی SVM نشان می دهد، معیار DR بیانگر دقت تشخیص دسته مثبت و معیار FAR نرخ هشدار غلط را با توجه به دسته منفی بیان می‌کند. تحلیل نتایج هر دو پارامتر بیانگر نتیجه مطلوب الگوریتم دسته‌بندی در تشخیص دسته‌ها است [۱۱].

در ادامه ماتریس نتایج ماتریس درهم‌ریختگی[4] بررسی می‌شود.



شکل (۱۵): ماتریس درهم‌ریختگی

4Confusion Matrix

ماتریس درهم‌ریختگی، به ماتریسی گفته می‌شود که در آن عملکرد الگوریتم‌های مربوطه را نشان می‌دهند. معمولاً چنین نمایشی برای الگوریتم‌های یادگیری با ناظر استفاده می‌شود، اگرچه در یادگیری بدون ناظر نیز کاربرد دارد. هر ستون از ماتریس، نمونه‌ای از مقدار پیش‌بینی‌شده را نشان می‌دهد. درصورتی‌که هر سطر نمونه‌ای واقعی (درست) را در بردارد.[۱۲]. در این مرحله ما از ماتریس درهم‌ریختگی برای صحت عملکرد الگوریتم پیاده‌سازی شده تا دقت، صحت و حساسیت دسته‌بندها و کلاسه‌های ایجادشده را مشخص کنیم.

معیارهای ارزیابی در رابطه (۶) دیده می‌شود [۷]

$$\text{صحت} = \frac{TP + \text{TN}}{\text{TP} + \text{TN} + \text{FN} + \text{FP}}$$

$$\text{دقت} = \frac{TP}{\text{TP} + \text{FP}} \qquad (۶)$$

$$\text{حساسیت} = \frac{TN}{\text{T}P + \text{FN}}$$

نتایج مقایسه‌ای مدل پیشنهادی برابر معیارهای رابطه (۶)، برابر جدول (۹) می باشد.

جدول (۹): مقایسه نتایج الگوریتم‌ها

مدل‌های دسته بندی[1]	ماتریس درهم‌ریختگی[2]	صحت[3]	دقت[4]	حساسیت[5]
Random Forest	۲۷۸۶(TP) ۴(TN) ۸۲(FP) ۴(FN)	۹۷/۷۶	۰/۹۸۵۲	۰/۴۶۵
RBF Network	۲۷۸۶(TP) ۷(TN) ۸۲(FP) ۵(FN)	۹۶/۶۳	۰/۹۸۱۳	۰/۰۷۸۷
MLP	۲۷۰۶(TP) ۱۱(TN) ۸۰۷(FP) ۶(FN)	۹۵/۲۳	۰/۹۷۷۳	۰/۱۲۰۸
روش پیشنهادی	۲۷۸۳(TP) ۰(TN) ۲۲(FP) ۴(FN)	۹۸/۹	۱/۰۱	۰

1-Classification Model
2- Confusion Matrix
3- Accuracy
4- Sensitivity
5- Specificity

صحت: درصد اطلاعاتی که به‌درستی توسط مدل پیش‌بینی شده است

دقت: نسبت موارد پیش بینی شده مثبت صحیح به مجموع پیش بینی‌های مثبت (صحیح و کاذب)

حساسیت: نرخ پیش‌بینی مثبت صحیحقدرت طبقه‌بندی مناسب رویدادهای خوب را نشان می‌دهد. هر چقدر میزان حساسیت کمتر باشد، الگوریتم کاراتر می‌باشد.

۷- نتیجه‌گیری

بدون شک حملات منع سرویس و به‌ویژه حملات منع سرویس توزیع‌شده، می‌توانند آسیب‌های جدی برای یک وب‌سایت ایجاد نمایند. در این تحقیق از روش ایجاد پنجره‌های زمانی، محاسبه آنتروپی هر آی‌پی در یک پنجره و سپس محاسبه واریانس آنتروپی‌ها در هر پنجره استفاده گردید و در نهایت با الگوریتم SVM که یکی از الگوریتم‌های یادگیری ماشین است، شبکه آموزش داده شد تا حملات منع سرویس را دسته‌بندی نماید. صحت و دقت این الگوریتم از سه الگوریتم RandomForest، RBFNetwork، MLP که در مقالات سنوات اخیر پیاده‌سازی شده است بالاتر است و به نظر دسته‌بندی بهتری برای این کار است. برای تحقیقات آتی پیشنهاد می‌شود از سایر الگوریتم‌های یادگیری ترکیبی و با دیتاست‌های مختلف دیگر پیاده‌سازی، استفاده شده و موارد ذیل موردبررسی دقیق‌تری قرار گیرد.

با توجه به که مرز بین حملات FC و DDOS, DOS مشخص نیست و عدم قطعیت می‌تواند وجود داشته باشد از روش‌های فازی برای شناسایی حملات استفاده شود.

الگوریتم‌های ترکیبی دسته‌بندی مثل ژنتیک، تئوری بیز و... استفاده شود.

۱) اگر وب‌سایت‌های معتبر از طریق وایر شاک و ابزارهای مشابه جمع‌آوری و الگوریتم‌ها پیاده‌سازی در محیط کاملاً واقعی انجام شود.
۲) محصولات وب فارنزیک شرکت‌های معتبر موردبررسی قرارگرفته و مطالعه تطبیقی صورت پذیرد.
۳) سایر حملات وب که در متن تحقیق عنوان‌شده موردبررسی قرار گیرد.

۹- منابع

[1] S.T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE communications surveys & tutorials, vol. 15, no. 4, pp. 2046-2069, 2013.

[2] V. Kumar and K. Kumar, "Classification of DDoS attack tools and its handling techniques and strategy at application layer. In Advances in Computing, Communication, & Automation (ICACCA) (fall)," International Conference on, IEEE, pp. 1-6, 2016.

[3] "OWASP Top 10 -The Ten Most Critical Web Application Security Risks," 2017. www.OWASP.org.

[4] H. Akbari and Safavi Homami, "Provide a framework for estimating the status of distributed denial-of-service attacks by integrating information about human-technical sensors based on fuzzy logic," Electronic and Cyber Defense Magazine, Number 3, 1396. (In Persian)

[5] S. Chawla, M. Sachdeva, and S. Behal, "Discrimination of DDoS attacks and Flash Events using Pearson's Product Moment Correlation Method," International Journal of Computer Science and Information Security, vol. 14, no. 10, p. 382, 2016.

[6] T. Subbulakshmi, "A learning-based hybrid framework for detection and defence of DDoS attacks," International Journal of Internet Protocol Technology, vol. 10, no. 1, pp. 51-60, 2017.

[7] J. Singh, K. Thongam, and T. De, "Entropy-Based Application Layer DDoS Attack Detection Using Artificial Neural Networks. Entropy," vol. 18, no. 10, p. 350, 2016.

[8] E. Adi, Z. Baig, and P. Hingston, "Stealthy Denial of Service (DoS) attack modelling and detection for HTTP/2 services," Journal of Network and Computer Applications, vol. 91, pp. 1-13, 2017.

[9] M. Mahanani, M. Jalali, and H. Namvar, "Classification and Identification of Day zero Attack Traffic Intrusion Detection Systems using TWSVM, FCM," Third National Conference on Modern Approaches to Computer and Electrical Engineering, Rudsar, Azad University Islamic Unit of Rudsar and Amlash - Youth and Elite Researchers Club of RudsarAmlash, 1396. (In Persian)

[10] K. Dadashtabar Ahmadi and A. Jabbar Rashidi, "Detection of advanced cyber attacks using behavioral modeling, Benevolent, coral," Fourth International Conference on Knowledge Based Research in Computer Engineering and Information Technology, Tehran, University of Abrar, 1396. (In Persian)

[11] M. Kantardzic, "Data Mining: Concepts, Models, Methods, and Algorithms," John Wiley & Sons, 2011.

[12] M. V.Nidhi and K. M. Prasad, "Detection of Anomaly Based Application Layer DDos Attacks Using Machine Learning Approaches," i-Manager's Journal on Computer Science, vol. 4, no. 2, p. 6, 2016.

Journal of Electronical & Cyber Defence
Vol. 6, No. 4, 2019, Serial No. 24

Detect Web Denial of Service Attacks Using Entropy and Support Vector Machine Algorithm

V. Yadegari, A. R. Matinfar*
Tarbiat Modarres University
(Received: 23/12/2017, Accepted: 27/05/2018)

ABSTRACT

By expanding Internet-based services and developing websites, cyber threats are also increasing. One of these threats is to perform denial-of-service attacks and interfere with the services of a website. Web or application-layer service blocking attacks by creation of artificial traffic impose a heavy traffic on the web server and thus disrupt the Web service. In this research, to detect these attacks, Web server logs are classified by applying 20 second time windows and calculating the activity level and the entropy of different IPs in each time window. Using entropy variance, time windows with continuity are determined. In the next stage, through the backup machine algorithm, the network is trained to store abnormal time windows, and ultimately IP addresses that lead to blocked service attacks or service disruptions are classified and labelled. The proposed model was implemented on the EPA-HTTP standard dataset indicating improvement compared to previous studies.

Keywords: Support Vectore machin(SVM),Entropy, DDOS, log,Variance

* Corresponding Author Email: a.matinfar@chmail.ir