رویکرد ترکیبی هوشمند برای تشخیص حملات DDoS قابل استفاده در شبکه پلیس

سارا آزادمنش[۱]، رضا عزمی[۲]، علیرضا نوروزی[۳]

۱- دانشجوی دکترای کامپیوتر، مجمتع دانشگاهی فناوی اطلاعات و ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران، ایران

azadmanesh@mut.ac.ir

۲- دانشیار دانشکده مهندسی کامپیوتر، دانشگاه الزهرا، تهران، ایران

azmi@alzahra.ac.ir

۳- استادیار دانشکده مهندسی رسانه، دانشگاه صدا و سیما، تهران، ایران

alirezanowroozi@iribu.ac.ir

چکیده: حمله انکار سرویس توزیع شده (**DDoS**)[۱] تلاشی است که باعث می شود منابع شبکه برای کاربران قانونی در دسترس نباشد. امروزه، تعداد حملات **DDoS** به سرعت افزایش یافته‌اند و این تهدیدی برای کاربران اینترنت است، شبکه‌های پلیس نیز از این تهدید مستثنا نیستند و با توجه به نیاز دائمی پاسخگو بودن این شبکه‌ها در برابر درخواستهای قانونی از حساسیت بیشتری برخوردارند . اگرچه هدف حملات **DDoS** ممکن است متفاوت باشد، اما به طور کلی سعی می شود خدمات یک سرور قربانی متصل به اینترنت را به طور موقت یا دائم از دسترس خارج کند. در این مقاله، یک روش مبتنی بر لایه شبکه و مستقل از پروتکل‌های ارتباطی ارائه شده است که قادر است رفتارهای حمله را بدون نیاز به دانستن رفتارهای عادی شبکه تشخیص دهد. علاوه بر این، در این روش نیازی به ذخیره حجم بالای پروفایل‌ها، لیست‌های متعدد و امضاهای حمله نیست. این روش در سه مرحله صورت می‌گیرد: استخراج ویژگی از طریق موجک دو بعدی که نمودار توزیع انرژی را فراهم می کند، تشخیص نقطه تغییر با کمک قوانین منطق فازی و تجزیه و تحلیل شبکه عصبی عمیق به عنوان مرحله نهایی تشخیص. روش پیشنهادی در مجموعه داده‌های **VAST** و **ISCX** اجرا شد که در آن قادر به شناسایی حملات **DDoS** طی ۱۰ ثانیه با دقت ۹۹,۹۹ برای دادگان**VAST** و دقت ۹۹,۰۸ برای **ISCX** بود.

واژه‌های کلیدی: تشخیص **DDoS**، نقطه تغییر انرژی، شبکه عصبی، قوانین فازی.

تاریخ دریافت مقاله: ۱۴۰۰/۰۴/۲۷	**تاریخ پذیرش مقاله: ۱۴۰۰/۰۶/۱۳**
از صفحه ۴۳ تا ۵۵	**نوع مقاله : پژوهشی**
نویسنده مسئول: رضا عزمی	**نشریه علمی فناوری اطلاعات و ارتباطات انتظامی- دوره دوم- شماره ۶ - تابستان ۱۴۰۰**

[1] Distributed denial of service

۱- مقدمه

توسعه‌ی روزافزون زیرساخت‌های فناوری اطلاعات و ارتباطات در کشور و افزایش کاربران و استفاده کنندگان از اینترنت و سایر فنّاوری‌های اطلاعاتی، ارتباطی و مخابراتی نظیر خطوط تلفن‌های ثابت و همراه، شبکه‌های دیتای کشوری و محلّی، ارتباطات ماهواره‌ای از جمله‌ی دلایلی است که لزوم ایجاد و توسعه‌ی سازوکاری برای برقراری امنیت در فضای تولید و تبادل اطلاعات کشور را توجیه می‌کند.

از سوی دیگر، رشد قارچ‌گونه‌ی جرایم در حوزه‌ی فضای تولید و تبادل اطلاعات کشور (فتا) مثل کلاهبرداری‌های اینترنتی، جعل داده‌ها و عناوین، سرقت اطلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، هرزه‌نگاری و جرایم اخلاقی و برخی جرایم سازمان‌یافته‌ی اقتصادی، اجتماعی و فرهنگی ایجاب می‌کند که پلیس تخصصی که توان پی‌جویی و رسیدگی به جرایم سطح بالای فناورانه داشته باشد، به وجود آید و از این رو اهمیت پاسخگو بودن و فعالیت همیشگی این شبکه‌ها از اهمیت بالایی برخوردار است.

با تولید ترافیک بالای داده، حملات انکار سرویس توزیع شده [۲] باعث می‌شوند منابع در دسترس سیستم‌های هدف به سرعت مصرف شوند و متعاقباً خدمات شبکه را مختل کنند [۶] و [۱]. طبق گزارشات منتشر شده توسط شرکت کسپرسکی، در مقایسه با سه ماهه چهارم سال ۲۰۱۸ تعداد حملات DDoS در سه ماهه اول سال ۲۰۱۹، ۸۴ درصد افزایش یافته است و این پدیده طوفان DDoS نامیده می شود [۷]. مکانیسم‌های دفاعی متداول معرفی شده در برابر DDoS به اندازه کافی کارآمد نیستند، زیرا اشکالات عمومی خدمات شبکه به جای مشکلات پیکربندی، هنگام حمله استفاده می‌شوند [۸]. در این حمله، ازشبکه بات-شبکه ای از رایانه‌های آلوده- برای ارسال حجم زیادی از ترافیک از طریق چندین میزبان مختلف در اینترنت، توسط bot master استفاده می‌شود. در حقیقت، مدیر منابع محدود اهداف بالقوه را که برای دستیابی و دسترسی به مشتریان قانونی قربانی است، مصرف می‌کند [۹] و [۲] و [۱].

از آنجا که تشخیص ترافیک حمله از ترافیک عادی دشوار است، حملات DDoS تهدیدهای جدی برای ارائه‌دهندگان خدمات هستند [۱۰]. شبکه‌های پلیس نیز از این تهدید مستثنا نیستند علاوه بر اینکه درخواست‌های زیاد از سوی شهروندان (اطلاع از خلافی، درخواست گواهینامه و...) دارند، نیروهای پلیس نیز (در فرودگاهها، کلانتری‌ها و...) نیاز به پاسخگویی دارند به دلایل قانونی نیز بایستی شبکه مطمئن و همواره پاسخگویی داشته باشند که روش‌های هوشمند تشخیص این حملات کمک شایانی در این زمینه می‌کند. روش‌های مختلفی برای شناسایی حملات DDoS معرفی شده است. با این وجود باتنت‌های زیادی وجود دارد که از قربانیان بهره برداری می کنند. علاوه بر این، امروزه باتنت‌ها از ترکیبی از بردارهای حمله مختلف مانند سیلاب، فرسودگی منابع و لایه کاربرد استفاده می کنند[۱۱]. به طور کلی، روش‌های تشخیص را می‌توان در دو دسته طبقه‌بندی کرد: تشخیص ناهنجاری و تشخیص مبتنی بر امضا [۱۲]. بیشتر روش‌های تشخیص ناهنجاری پیشنهادی، براساس مدل‌سازی رفتار شبکه در شرایط عادی و تشخیص تغییرات غیرعادی است [۱۳] و [۱]. یادگیری عمیق[۳] در سیستم‌های تشخیص نفوذ استفاده می‌شود و رویکردهای مبتنی بر DL راه‌های جدید، دقیق و سریعی را در تشخیص DDoS باز می‌کنند. علاوه بر این، از نمودارهای توزیع انرژی برای تشخیص وضعیت سیستم‌ها استفاده می‌شود. این روش مفید و کاربردی است و فواید ارزشمندی را نشان می‌دهد به طوری که می‌توان برای تشخیص DDoS به‌کار گرفته شود. با این حال، ترکیبی از روش‌های ذکر شده ممکن است عملکرد موثرتری را ارائه دهد.

در این مقاله، یک روش ترکیبی ساده معرفی شده است، که در سه مرحله امکان تشخیص سریع حملات DDoS را دارد. روش پیشنهادی با مرحله استخراج بر اساس موجک دو بعدی شروع می‌شود. پس از آن، نمودارهای کنترل به‌دست آمده با استفاده از قوانین فازی برای تعیین نقاط تغییر ارزیابی می‌شوند. در مرحله آخر، با استفاده از یک شبکه عصبی عمیق[۴] جریان‌های ترافیکی مشکوک برای شناسایی حملات مورد تجزیه و تحلیل بیشتر قرار می‌گیرند. در این روش برای اولین بار از ویژگی‌های رفتاری فرستنده و گیرنده در زمان واحد و نیز مفهوم نقطه تغییر انرژی با استفاده از نمودارهای کنترل استفاده می‌شود. در واقع، نمودارهای توزیع انرژی توسط موجک دو بعدی بدست می‌آیند و براساس قوانین فازی برای آشکار کردن موارد مشکوک مورد تجزیه و تحلیل قرار می‌گیرند. پس از آن، DNN برای شناسایی سریع و دقیق حملات DDoS استفاده می‌شود. استفاده از این روش دارای مزایایی مانند اینکه نیازی به ذخیره تعداد زیادی از پروفایل‌ها، لیست‌های متعدد و امضاهای حمله نیست. بعلاوه، در این روش دانش قبلی زیادی در مورد ساختار شبکه نیز مورد نیاز نیست و این روش سریع، ساده، دقیق و عملی با توجه به خصوصیات ذکر شده است، این روش می‌تواند

[2] Distributed denial of service(DDoS)

[3] Deep learning (DL)
[4] Deep Neural Network (DNN)

به عنوان تجزیه و تحلیل سریع داده‌ها مورد استفاده قرار گیرد. بنابراین، روش پیشنهادی می‌تواند چابکی سیستم‌های امنیتی را افزایش دهد.

ادامه مقاله به صورت زیر سازماندهی می‌شود: در بخش بعدی، مختصری از کارهای مرتبط ارائه می‌شود. سپس، روش پیشنهادی شرح داده شده است. در مرحله بعد، نتایج و بحث ارائه شده است. سرانجام، نتیجه گیری انجام می‌شود.

۲- بررسی منابع

۲-۱- پیشینه

تحقیقات زیادی در مورد شناسایی حمله DDoS انجام شده است. با این حال، استفاده از تشخیص نقطه تغییر انرژی با نمودارهای کنترل در این زمینه مطالعه جدید است. در اینجا، برخی از تحقیقات مرتبط ارائه شده است:

در [۱۱]، با استفاده از موجک مبتنی بر توزیع انرژی سری زمانی از ترافیک شبکه در نظر گرفته شده است و یک روش تشخیص برای حملات DDoS سیل‌آسا ارائه شده است. در این تحقیق از توزیع انرژی برای شناسایی تغییرات ترافیکی استفاده شده است. علاوه بر این، نوسانات ترافیکی کوچک، که از رفتار طبیعی ناشی می‌شود، هموارتر می‌شوند تا مثبت کاذب کاهش یابد. با این حال، مشخصاً انتخاب آستانه برای آشکار کردن نقطه تغییر مورد بحث قرار نگرفته است. از ویژگی تشابه به خود برای ترافیک عادی در [۱۴] و از روش واریانس موجک برای تخمین پارامتر H برای تشابه به خود استفاده شده است. زمانی که مقدار آن زیر آستانه باشد ترافیک به عنوان حمله شناخته می‌شود. در [۱۵]، از ماشین بردار پشتیبان (SVM) برای ارائه ماشین بردار پشتیبان موجک (WSVM) برای شناسایی دقیق حملات DDoS استفاده می‌کند. WSVM اتصالات شبکه را طبقه‌بندی می‌کند و داده‌های عادی را از حالت غیر عادی متمایز می‌نماید. متعاقبا، مسئله تشخیص حمله با شناسایی الگو جایگزین می‌شود که منجر به کاهش مثبت کاذب در مقایسه با SVM می‌شود.

برای دسته‌بندی ویژگی‌های مبتنی بر موجک استخراج شده، خانواده‌های daubechies، symlets و coiflets در [۱۶] استفاده می‌شوند. پس از آن، یادگیری نیمه نظارت شده برای تشخیص ترافیک حمله استفاده می‌شود. د [۱۷]، یک روش در زمان واقعی که از تجزیه و تحلیل مبتنی بر موجک استفاده می‌کند، برای یافتن ناهنجاری‌ها معرفی شده است. درصد انحراف و آنتروپی به عنوان معیارهای ارزیابی انتخاب می‌شوند و نتایج موجک‌های coiflets و پاول کارایی بیشتری را در تشخیص نشان می‌دهند. برای شناسایی حملات سیل‌آسا و محافظت از روترها، در [۱۸] از تجزیه و تحلیل موجک استفاده شده است. این روش ترافیک حمله را از ترافیک قانونی تشخیص می‌دهد. در این تحقیق، حمله در زیر ساخت با استفاده از روش موجک استخراج می‌شود و نتایج امکان پذیر بودن این روش را تأیید می‌کند. در [۱۹]، از موجک برای استخراج ویژگی‌های موج از سیگنال استفاده می‌شود، سپس از ماشین بردار پشتیبانی (SVM) برای طبقه‌بندی استفاده شده است. برای شناسایی حملات مبتنی بر امضا، در [۲۰] از موجک برای تجزیه و تحلیل ترافیک شبکه و محاسبه شباهت به خود استفاده کرده‌اندو نتایجشان دقت بالایی را نشان می‌دهد. با این حال، این روش قادر به شناسایی انواع حمله نیست.

در [۲۱]، با استفاده از تبدیل موجک دیجیتال، از نقطه تغییر سری زمانی برای تشخیص حمله استفاده می‌شود. با استفاده از پارامترهای مختلف ترافیک، این روش می‌تواند ترافیک شبکه را از دیدگاه‌های مختلف بررسی کند. نتایج این تحقیق توانایی تشخیص در لایه کاربرد[5] را پیشنهاد می‌کند. [۲۲] از طیف انرژی موجک برای شناسایی ویژگی‌های ترافیک عادی استفاده کرد. متعاقباً، ضرایب طیف چند مقیاس ترافیک حمله توسط یک شبکه عصبی به دست آمد.

در [۲۳] فرض بر این است که میزان ترافیک به آرامی تغییر می‌یابد و در هنگام حمله، تغییرات ناگهانی در سری زمانی نرخ ورود بسته مشاهده می‌شود. و سپس از آمار جمع تجمعی[6] برای تشخیص نقطه تغییر استفاده شد. این روش شامل دو مرحله است:۱) افزایش نرخ انتقال شبکه با استفاده از مطالعه آماری بدست می‌آید، ۲) رشد ناگهانی نرخ ورود بسته- به عنوان ویژگی اصلی تشخیص حمله- به سرعت با تجزیه و تحلیل موجک آشکار می‌شود. در [۲۴]، از تغییرات خروجی و ورودی نرخ روتر به عنوان معیارهای احتمالی ترافیک حمله استفاده کردند و برای تشخیص زود هنگام حملات DDoS درختان تجمع تغییر (CAT) برای ارائه یک ساختار تشخیص توزیع شده نقطه تغییر (DCD) استفاده می شود. این روش از مدلهای تصادفی مشروط (CRF) استفاده می کند و مبتنی بر ترکیبی از ویژگیهای آنتروپی با ویژگی‌های نرمال است.

در [۲۵] از محاسبه اختلاف بازسازی تجزیه موجک واقعی ترافیک و بازسازی پیش بینی شده توسط LSTM به شناسایی ریسک (حملات) موجود در ترافیک استفاده شده است.

[5] Application layer

[6] cumulative sum statistics

در [۲۶]، یک سیستم تشخیص نفوذ هوش مصنوعی (AI) با استفاده از DNN در پاسخ به حمله شبکه در حال تحول مورد بررسی قرار گرفت. در مرحله اول، تبدیل و نرمال سازی داده‌ها انجام شده، سپس الگوریتم DNN برای ایجاد یک مدل یادگیری از داده‌های ارائه شده با پیش پردازش استفاده شده است. در نهایت، برای تعیین اثربخشی و دقت تشخیص مدل DNN، نرخ مثبت کاذب محاسبه شده است، که ۱۰ درصد از مجموعه داده‌ها برای تولید مجموعه آموزشی استفاده شد و دقت ۹۹ درصد به دست آمده است. در [۲۷]، ویژگیهای مبتنی بر آنتروپی جریان شبکه به همراه نسخه پیشرفته ای از تکنیکهای RNN و DL برای یادگیری مدلهای معمولی استفاده شد. این ترکیب امکان استفاده از روش‌های تشخیصی اختیاری برای طیف وسیعی از داده‌ها و شبکه‌های بزرگ را فراهم کرد. علاوه بر این، این رویکرد بدون نظارت است و نیازی به داده‌های دارای برچسب ندارد و داده‌های آموزشی نیز به طور کامل و بدون حمله مورد نیاز نیست. روش ارائه شده کارآمد بود زیرا RNN می تواند یک مدل معمولی را در چند ثانیه یاد بگیرد.

در [۲۸]، یک الگوریتم یادگیری مداوم برای یادگیری الگوی ترافیک رفتار عادی شبکه مورد استفاده قرار گرفت که می تواند به مدیران شبکه کمک کند تا اقدامات فوری را برای کاهش تأثیر حملات DDoS انجام دهند. در این رویکرد، ویژگی‌های جریان محور ترافیک برای تجزیه و تحلیل تفاوت الگو بین بسته‌های عادی و ناهنجاری با دقت ۹۵ استفاده شد. در [۲۹]، یک روش تشخیص DL برای شناسایی رفتار مخرب تهدیدهای سایبری DDoS علیه کسب و کارهای متوسط پیشنهاد شد. این رویکرد در زمان واقعی عمل می کند و ترافیک مخرب را از ترافیک معمولی متمایز می کند. نتایج این سیستم تشخیص نفوذ نشان داد که مدل پیشنهادی می تواند به دقت ۹۹,۷۹ دست یابد.

تحقیقات بررسی شده اکثرا مبتنی بر پروفایل‌سازی بلند مدت و یا استفاده از متغییرهای مشابه پایه گذاری شده‌اند.

۲-۲- متغیرهای استفاده شده

برای شناسایی حملات DDoS، در مقالات قبلی متغییرهای مختلفی به کار رفته است و در جدول (۱) برخی از متغیرهای پرتکرار ذکر شده‌اند. حملات DDoS از منابع مختلفی تولید می‌شوند و نگهداری و نظارت بر ویژگی‌هایی مانند IP مبدا / مقصد و پورت‌ها برای ذخیره‌سازی به حافظه زیادی احتیاج دارد. علاوه بر این، هنگامی که مهاجمان زیادی وجود دارد، جستجو در آدرس‌ها یک پروسه زمانبر است. بنابراین، معیارهای ذکر شده مفید نیستند. روش‌هایی که از مسیر حمله به مقصد و بسته‌های زمان رسیدن به بسته استفاده می-کنند حداقل به یک دانش منطقی از پیکربندی شبکه نیاز دارند که به دست آوردن این دانش دشوار است. مطالعه آنتروپی ترافیک و ویژگی‌های شباهت ترافیکی عادی به فواصل طولانی مشاهده ترافیک نیاز دارد و باید تضمین شود که هیچ حمله ای در این دوره‌های مشاهده وجود ندارد، این متغیرها نیز در تشخیص DDoS ناکارآمد هستند. در حقیقت، کمبودهای ذکر شده از روش تشخیص سرچشمه می گیرد و در این مقاله رویکردی برای جلوگیری از این موارد معرفی شده است.

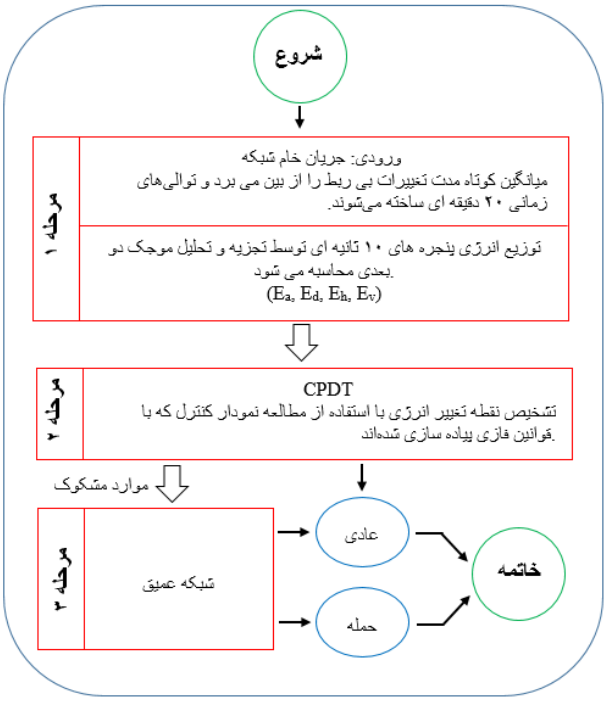
جدول (۱): متغییرهای به کار رفته برای تشخیص حمله DDoS

	مراجع
The number of received packets per time interval	[۳۱],[۱۱]
Mean packet inter arrival times	[۳۱]
Ratio of incoming to out-going packets	[۱۱]
The number of flows per minute	[۱۶]
The average number of packets per flow over one minute	[۱۶]
The average number of bytes per flow over one minute	[۱۶]
Ratio of number of flows to bytes per packet over one minute	[۱۶]
Arrival rate of packets	[۳۲]–[۳۴]
Rate of packet type	[۳۴][۳۵]
Flow inter-arrival time	[۳۵]
Traffic entropy	[۳۵]
Source IP address	[۳۶]
Source IPs and destination IPs,	[۳۳]
The number of SYN errors	[۳۷]
The number of connections to the same host during the specified time	[۳۷]

۳- رویکرد پیشنهادی

شکل ۱ خلاصه گرافیکی روش تشخیص پیشنهادی را نمایش می‌دهد، در آن مراحل مختلف روش پیشنهادی تشخیص حمله DDoS به طور خلاصه ذکر شده است. در مرحله اول، به عنوان یک مرحله متوسط گیری و هموار سازی، ویژگی‌های ترافیک شبکه طی بازه‌های زمانی ۱ ثانیه‌ای متوسطشان گرفته می شوند. سپس،

توالی‌های متوسط در پنجره‌های ۱۰ ثانیه‌ای (پنجره‌های کشویی[7] با ۱۰٪ همپوشانی) کپسوله می‌شوند. متعاقباً، در مرحله نمودار کنترل، از منطق فازی برای شناسایی نقطه تغییر انرژی در ترافیک استفاده می‌شود. اگر شرایط قوانین اتفاق بیفتد، یک نقطه تغییر انرژی وجود دارد و یک رفتار مشکوک شناسایی می‌شود. اگر شرایط قوانین رخ ندهد، حمله‌ای صورت نمی‌گیرد و ترافیک عادی است. در نتیجه، ویژگی‌های به دست آمده از ترافیک مشکوک به مرحله شناسایی نهایی به DNN منتقل می‌شود. در این روش، نیازی به ذخیره اطلاعات زیاد یا دانستن رفتار طبیعی شبکه نیست و روش کار آن ساده، عملی و موثر است.



شکل (۱): چکیده گرافیکی و نمودار جریان روش تشخیص پیشنهادی

الگوریتم ۱ روند تشخیص ترکیبی DDoS را نشان می دهد. این روش با میانگین گیری ساده، استخراج توالی داده‌ها و ریختن آنها در پنجره‌های کشویی آغاز می‌شود. سپس، از موجک دو بعدی برای تجزیه و تحلیل داده‌ها و به دست آوردن نمودار توزیع انرژی استفاده می‌شود. پس از آن، قوانین فازی برای ارزیابی نمودار انرژی و یافتن نقاط احتمالی تغییر انرژی به کار گرفته می‌شوند. سرانجام از DNN برای کشف حملات استفاده می‌شود.

الگوریتم ۱ برای مدل سازی و تجزیه و تحلیل داده‌های پنجره دار

BEGIN

Input: raw traffic

Capsulated traffic = average raw traffic in 1 second

Flow = every n seconds with d percent overlap

Procedure

Select streams of flows which there is a change in them (e.g. 20 minutes with start of attack from 19 minutes before the attack to 1 minute before attack)

Calculate 2D wavelet analysis for each flow

Create 2DWT sequences

Calculate borders (high, mrdian, low values for each sequence)

Detect if there is a change (**suspicious**) or nothing changed (benign)

DNN(input: suspicious traffic,out put:attack or normal)

END

۳-۱- سری زمانی

جریان F در زمان T را می توان به صورت زیر نشان داد:

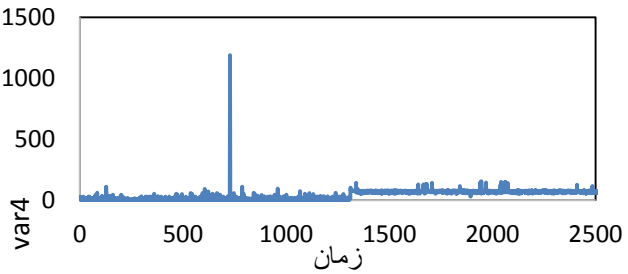
$$\left\langle t_1,s_1,d_1,dp_1 \ , \ t_2,s_2,d_2,dp_2 \ ,\ldots, \ t_n,s_n,d_n,dp_n \right\rangle \quad (1)$$

که t_i ، s_i، d_i، وdp_iبه ترتیب نشانگر زمان بسته، IP مبدا، IP مقصد و شماره پورت مقصد است. بسته‌ها را در یک بازه زمانی T می-توان بر اساس برابریIP مبدا یا IP مقصد در یک جریان IPFIX طبقه بندی کرد. در روش پیشنهادی ابتدا میانگین متغیرها از ترافیک خالص در طی بازه زمانی ۱ ثانیه‌ای استخراج شده و سری زمانی ترافیک ایجاد می‌شود. در حقیقت، میانگین گیری کوتاه مدت تغییرات بی‌ربط را از بین می برد و باعث می شود که سری‌های زمانی ترافیک هموار باشند. به عنوان مثال، همانطور که در شکل (۲) نشان داده شده است، در حالیکه ترافیک عادی است، ترافیک بین بازه زمانی ۵۰۰-۱۰۰۰ تغییر ناگهانی دارد. با این حال، پس از زمان ۱۳۰۰ یک تغییر مداوم قابل توجه در مقدار متغیر firstSeenSrcTotalBytes و در جایی که حمله شروع شده، مشاهده می‌شود. بنابراین، داده‌های کپسوله شده سری زمانی به صورت زیر تشکیل می‌شود.

$$Time\ sery_{IPF} = Avg_{\Delta t=1}\ IPFIX_t \quad (2)$$

همانطور که در فرمول (۲) نشان داده شده است، توالی سری زمانی با میانگین‌گیری داده‌های جریان خالص بر روی هر متغیر در بازه‌های زمانی ۱ ثانیه ساخته می شود.

[7] Sliding window



شکل (۲): یک تغییر ناگهانی بی ربط در ترافیک قبل از میانگین گیری (در جایی که حمله ای وجود ندارد)

۳-۲- متغیرهای بکار رفته

از آنجا که داده مربوط به ترافیک شبکه پلیس در دسترس نبود و روش پیشنهادی نیز روشی کلی و قابل استفاده برای تمامی شبکه‌ها است، از دادگان استاندارد برای ارزیابی روش و ارائه نتایج استفاده شده است.

از مجموعه داده VAST [38]برای ارزیابی روش پیشنهادی استفاده می شود و ویژگی‌های جریان خالص استفاده شده در جدول (۲) نشان داده شده است. از میانگین Var1-6 به عنوان مولفه‌های ترافیک استفاده می شود.

جدول (۲): اندازه گیری مجموعه داده VAST

Variable	Label
firstSeenSrcPayloadBytes	Var1
firstSeenDestPayloadBytes	Var2
firstSeenSrcTotalBytes	Var3
firstSeenDestTotalBytes	Var4
firstSeenSrcPacketCount	Var5
firstSeenDestPacketCount	Var6

معیارهای دو بعدی قادر به نشان دادن رفتار مبدا و مقصد به طور همزمان هستند، علاوه بر این، از نوع حمله و پروتکل استفاده شده مستقل هستند.

۳-۳- تجزیه و تحلیل موجک دو بعدی ترافیک

پس از به دست آوردن سری‌های زمانی با میانگین‌گیری از معیارهای دو بعدی ذکر شده، تجزیه و تحلیل موجک دوبعدی همبستگی‌های پیچیده زمان را به دست می‌آورد و توزیع انرژی با استفاده از تجزیه و تحلیل موجک دو بعدی برای هر دنباله در پنجره‌های ۱۰ ثانیه ای با ۱۰٪ همپوشانی (پنجره‌های کشویی) محاسبه می‌شود. در ترافیک عادی، توزیع انرژی در طول زمان و شرایط غیر حمله‌ای تغییرات کمی را نشان می‌دهد. با این حال، ترافیک حمله باعث تغییرات قابل توجهی در سطح انرژی ترافیک شبکه در طی زمان می‌شود. تشخیص این تغییر، با استفاده از قوانین فازی، منجر به تشخیص شروع حمله و تغییر وضعیت ترافیک می‌شود.

سری فوریه فقط برای تجزیه و تحلیل سیگنالهای ثابت مناسب است، زیرا همه فرکانس‌ها در هر لحظه در دسترس هستند. علاوه بر این، تجزیه و تحلیل کوتاه مدت فوریه، پیشنهاد شده توسط گابور، تجزیه و تحلیل فوریه را با استفاده از یک پنجره زمانی محلی انجام می‌دهد. با این حال، قادر به ارائه وضوح مناسب فرکانس و زمان نیست (بسته به پنجره زمانی). تبدیل موجک پیشنهادی توسط مورلت می‌تواند فرکانس و وضوح زمانی مناسب را بدست آورد[17] و این تغییر منجر به دستیابی به انسجام متناسب با پنجره زمانی می‌شود. در این مقاله، سیگنال شبکه به عنوان یک سیگنال فرکانس شکسته در نظر گرفته شده است. بنابراین، می‌توان از تجزیه موجک گسسته (DWT) استفاده کرد [31]. برای سیگنال X (t)، DWT به صورت ضرب سیگنال و موجک تعریف می شود:

$$DWT_x\ \ j,1 = d_{j,1}\ k\ = X\ \ k\ \ , \Psi_{j,1}\ k \qquad (3)$$

که در آن مقادیر $d_{j,1}(k)$ ضرایب گسسته X (k) در موقعیت زمانی l با مقیاس $1 = 0،\ldots، 2^{j-1}$ و حضور انرژی محلی در پهنای باند طول موج در نظر گرفته شده است. اگر ضرایب انرژی کافی باشد، فرض می‌شود سیگنالی که این فرکانس را تولید کرده است. در واقع، در فضای یک بعدی سیگنال بر اساس یک تقریب و یک جزئیات در هر فاز بررسی می‌شود. با این حال، در فضای دو بعدی سیگنال به عنوان یک تقریب و سه جزئیات (افقی، عمودی و مورب) بررسی می‌شود و سیگنال اصلی از مجموع آنها به دست می‌آید.

برای استفاده از تبدیل، باید اطمینان حاصل شود که پدیده‌ها پس از تبدیل حذف نمی‌شوند. بنابراین، خطای بازسازی هر خانواده موجک محاسبه می‌شود تا تضمین کند که تبدیل به درستی انجام شده است. در این تحقیق، ترافیک با استفاده از ضرایب انرژی بر اساس تجزیه و تحلیل اجزای جفت متغییرها مانند دوتایی var 1، var 2، به E_a (انرژی تقریبی)، E_d (جزئیات انرژی مورب)، E_v (جزئیات انرژی عمودی) و E_h (جزئیات انرژی افقی) مورد مطالعه قرار می گیرد. در ادامه، خانواده‌های Haar، Daubechies، Symlets، Coiflets، BiorSplines و ReverseBior مورد بررسی قرار گرفتند. که موجک-های Haar کمترین خطای بازسازی را دارد. بنابراین از این موجک استفاده می‌شود.

۳-۴- تشخیص نقطه تغییر انرژی

طبق بحث‌های قبل، تجزیه و تحلیل موجک دو بعدی، توزیع انرژی ترافیک شبکه را فراهم می‌کند. نمودارهای توزیع انرژی محاسبه شده به عنوان نمودارهای کنترل استفاده می‌شوند. نمودارهای کنترل به طور گسترده‌ای برای نظارت بر ثبات و فعالیت فرآیند استفاده می‌شوند و بر اساس داده‌هایی هستند که یک یا چند ویژگی مربوط به کیفیت خدمات را نشان می‌دهند. از نمودارهای کنترل عددی در مواردی استفاده می‌شود که ویژگی‌ها با مقیاس عددی قابل اندازه‌گیری باشند. محدودیت‌های کنترل با استفاده از قوانین احتمال محاسبه می‌شوند.پ. با این حال، حتی اگر همه نقاط در محدوده کنترل قرار بگیرند، ممکن است روند کنترل نشده باشد(اگر الگوی تغییرات عادی را نشان ندهد). در حقیقت، فرایند زمانی کنترل می‌شود که نقاط تقریباً حول میانگین فرآیند متمرکز شده باشند و تغییراتی را در یک الگوی طبیعی نشان دهند. الگوی طبیعی به معنی همسو شدن فرآیند بر اساس احتمال توزیع طبیعی است. از سوی دیگر، فرض می‌شود که تغییرات و الگوهای غیرعادی به عنوان حالت‌های کنترل شده در نظر گرفته شوند و شرایط کنترل نشده معمولاً دلایل خاصی دارند که باید برطرف شوند.

ایده اصلی در تعریف یک قاعده برای یک الگوی غیر طبیعی، احتمال وقوع آن است. این قوانین بر این فرض استوار است که یک داده خاص احتمالاً در یک جریان داده کاملاً تصادفی اتفاق می‌افتد. به طور کلی، احتمال بروز یک الگوی غیر طبیعی کمتر از ۱٪ است. اگرچه برخی از الگوهای غیر طبیعی وجود دارد که برای موارد صریح شناسایی شده‌اند، اما قانون قطعی در مورد الگوهای غیر طبیعی وجود ندارد. انتخاب مجموعه‌ای از قوانین به ترجیحات کاربر بستگی دارد و الگوهای غیر عادی برای دوره‌های کوتاه مدت تعریف می‌شوند. در این تحقیق از ۲۰ نقطه متوالی در نمودار کنترل تجزیه و تحلیل می شود.

علاوه بر این، برای شناسایی الگوهای غیر عادی در نمودار کنترل، مجموعه ای از قوانین تصمیم‌گیری مانند وسترن الکتریک وجود دارد . [۳۹] و [۴۰] درصورتی که در صورت بروز هر یک از شرایط معرفی شده فرایند، کنترل نشده فرض می‌شود.

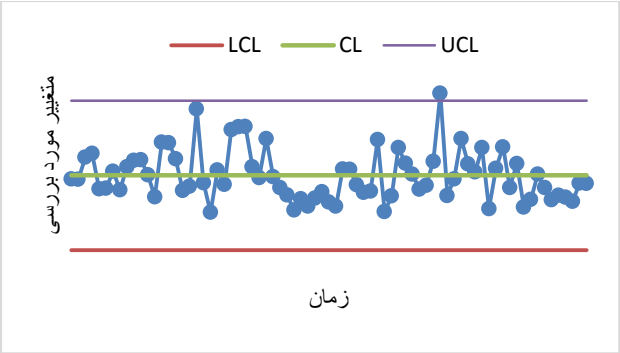
برای شناسایی حمله DDoS در وهله اول سری زمانی، میانگین متغیرهای ترافیک خالص netflow در بازه‌های زمانی ۱ ثانیه تولید می‌شود. سپس، مجموعه‌های بدست آمده به توالی‌های زمانی ۲۰ دقیقه‌ای تقسیم می‌شوند تا با استفاده از آنالیز موجک دو بعدی مورد مطالعه قرار گیرند. برای اطمینان از صحت روش، در هر توالی تغییری وجود دارد(دوره زمانی تجزیه و تحلیل از ۱۹ دقیقه قبل تا ۱۹ دقیقه پس از حمله متغیر است در نتیجه در توالی ۲۰ دقیقه حتما یک تغییر وجود خواهد داشت). بنابراین، روش پیشنهادی باید تغییر در همه نمونه‌ها را تشخیص دهد و اگر تغییر مشاهده نشود، تشخیص نادرست رخ می‌دهد. سپس، برای تولید نمودارهای توزیع انرژی، تجزیه موجک دو بعدی روی متغیرها برای هر بازه زمانی ۱۰ ثانیه ای پیاده سازی می‌شود. برای شناسایی نقطه تغییر انرژی، نمودار بر اساس قوانین وسترن الکتریک ارزیابی می شود. در این تحقیق، استفاده از سه قانون فازی برای تجزیه و تحلیل نمودارها (نمودارهای کنترل) کافی است :

قانون ۱: قرار گرفتن نقاط خارج از محدوده نمودار کنترل.(شکل ۴ نمونه وقوع این قانون است)

قانون ۲: قرار گرفتن هشت نقطه متوالی در یک طرف خط وسط.

قانون ۳: دو یا سه نقطه متوالی در انتهای یک سوم هر طرف خط وسط قرار گیرند.

احتمال وقوع قوانین ذکر شده به ترتیب ۰/۰۰۱۳۵، ۰/۰۰۳۹ و ۰/۰۰۱۵ محاسبه شده‌است. معمولاً الگوهای غیرطبیعی متغیر هستند و نمی توانند در اطراف خط مرکزی[8] پایدار باشد. با استفاده از نمودارهای کنترلی، می‌توان تغییرات فرآیند را برای تشخیص نقطه تغییر سازمان داد.



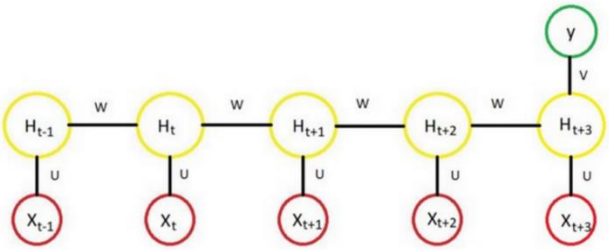
شکل (۴): نمونه ای از نمودار کنترلی

۳-۵- یادگیری عمیق

شبکه‌های عصبی بازگشتی[9] به ابزار اصلی برای مدل‌سازی توالی تبدیل شده‌اند. واحد حافظه کوتاه مدت (LSTM) یک نوع محبوب RNN است که توانایی خود را در ایجاد توالی در برنامه‌های مختلف، به ویژه پردازش متن ثابت کرده است. مدل‌های LSTM به دلیل یادگیری ذاتی مراحل قبلی و ویژگی‌های مهم آنها، رفتارهای مهم گذشته را می‌آموزند. به طور خلاصه، RNNهای LSTM قادرند روابط

[8] Control line (CL)
9 Recurrent neural network (RNN)

بسیار پیچیده و غیرخطی را در داده‌های سری زمانی بیاموزند و آنها را به یک روش پیش بینی مناسب برای پیش بینی نوع ترافیک در یک بازه زمانی بسیار کوتاه تبدیل می‌کند. در اینجا، ما از معماری RNN استفاده کردیم که با دادن یک دنباله از ۱۰ عدد متغیر به شبکه، یک خروجی (نرمال / حمله) بدست می‌آید. ورودی RNN یک توالی از نظر زمانی است و برخلاف شبکه‌های عصبی feed forward، مقادیر لایه پنهان هم از مقادیر ورودی و هم از مقادیر مرحله قبل، با وزن لایه پنهان بدست می آیند (حافظه‌ای از رویدادهای گذشته و قبلی دارد).



شکل (۵): محاسبه مقادیر لایه پنهان

در شکل (۵)، مقادیر مرحله زمان لایه مخفی (t) به صورت زیر محاسبه می شود:

$$H_t = Activatefunction\ \ Input \times H_{weights} + W \times H_t - 1 \quad (4)$$

$$y_t = softmax\ \ H_{weights} \times H_t \quad (5)$$

$H_{(t-1)}$ مرحله زمانی قبلی است و ضرایب W برای تمام مراحل زمانی برابر است. توابع فعال‌سازی می توانند Tanh، Relu، Sigmoid و غیره باشند. بعلاوه، H_t برای سایر مراحل زمانی دیگر قابل محاسبه است:

۱. $H_{(t-1)}$ را با U و X محاسبه کنید
۲. $y_{(t-1)}$ را از $H_{(t-1)}$ و V محاسبه کنید
۳. H_t را از U، X، W و $H_{(t-1)}$ محاسبه کنید
۴. y_t را از V و H_t و غیره محاسبه کنید.

توجه داشته باشید که:

۱. U و V بردارهای وزنی هستندو برای هر مرحله متفاوتند
۲. همچنین، ابتدا یک لایه پنهان (تمام مراحل زمانی) را محاسبه میکند سپس مقادیر y را محاسبه می‌شود.
۳. بردارهای وزن در ابتدا تصادفی هستند.

از آنجا که خروجی نهایی در قالب ۲ حالت است، برای محاسبه خروجی از آنتروپی متقابل باینری[10] استفاده کردیم. تابع از بین رفتن آنتروپی باینری با محاسبه میانگین زیر، از دست دادن یک مثال را محاسبه می کند:

$$Loss = \frac{1}{output\ size} \sum_{i=1}^{output\ size} y_i'.\log y_i' + 1 - y_i'\ .\log\ 1 - y_i' \quad (6)$$

جایی که $\dot{y}_i$ مقدار عددی i-th خروجی مدل است، $\dot{y}_i$ مقدار هدف مربوطه است و اندازه خروجی تعداد مقیاس‌های عددی موجود در خروجی مدل است. این معادل میانگین نتیجه تابع از دست دادن آنتروپی طبقه ای است که برای بسیاری از مشکلات طبقه بندی مستقل اعمال می شود، هر مسئله فقط دارای دو کلاس ممکن با احتمال هدف $\dot{y}_i$ و $(\dot{y}_{i-1})$ است.

در روش تشخیص DL، از سه نوع معیار برای ارزیابی مدلهای تشخیص استفاده شده است:دقت ریال صحت و بازخوانی که دقت معیار رایج ارزیابی در یادگیری ماشین است و در معادله (۲) تعریف شده اس:

$$Accuracy = \frac{TP_{Attack} + TN_{BENING}}{TP_{Attack} + FN_{Attack} + TN_{BENING} + FP_{Attack}} \quad (2)$$

منظور از TP ، TN، FPو FN به ترتیب، مثبت واقعی، منفی واقعی، مثبت کاذب و منفی کاذب هستند.

۴- بحث و نتایج

همانطور که گفته شد، با وقوع هر قانون، ترافیک به عنوان کنترل نشده شناسایی می‌شود. در ادامه، نتایج اجرای قوانین پیشنهادی در جدول (۳) ارائه شده است. برای هر پارامتر ۶۰ تکرار انجام می‌شود و هر تکرار حتما شامل یک حمله است. به عنوان مثال برای نمونه DDoS1 و پارامتر E_a ، ۵۴ بار حمله شناسایی و ۶ مثبت کاذب شناسایی شده است پس درصد مثبت کاذب ۱۰٪ (۱۰۰/۶۰/۶) بدست می آید. نتایج، مثبت کاذب کم برای اکثر پارامترها و نمونه‌ها را نشان می‌دهد. بنابراین، روش پیشنهادی در تشخیص حمله DDoS موفقیت آمیز است. DDoS1-5 انواع مختلفی از حملات را نشان می‌دهد که تعداد متفاوتی از حمله دارد. DDoS1 با ۱۰ مهاجم ۳ ساعت طول می کشد. در DDoS2، 15 مهاجم وجود دارد و سیستم برای ۲ ساعت مورد حمله قرار می‌گیرد. هر یک از حملات DDoS 1 و ۲ دارای ۱۱ میلیون داده ترافیکی است. DDoS3 با ۵ مهاجم در طی ۱ ساعت یک

[10] Binary cross entropy

تلاش ناموفق است. DDoS 4 و DDoS5 دارای ۸ مهاجم هستند و در یک دوره ۱۲ ساعته به دنبال یکدیگر اتفاق می افتند. نتایج بدست آمده از روش پیشنهادی تشخیص DDoS در ویندوز ۱۰ با ۶۴ بیت برای محیط توسعه، شبیه سازی شده است. داده‌های جریان از طریق پایتون ۳,۵ استخراج و تشخیص با استفاده از MATLAB شبیه سازی شده است.

جدول (۳): نتایج تشخیص تغییر در پنج نمونه حمله DDoS روی مجموعه داده VAST

نمونه	مثبت کاذب (%)				تغییر تشخیص داده شده				تکرار
	Ea	Ed	Eh	Ev	Ea	Ed	Eh	Ev	
DDoS1	10	3.3	0	16.7	54	58	60	50	240
DDoS2	23.3	1.7	10	16.7	46	59	54	50	240
DDoS3	1.7	0	0	6.7	59	60	60	56	240
DDoS4	1.7	3.3	3.3	1.7	59	58	59	59	240
DDoS5	0	0	0	0	60	60	60	60	240

دول ۵ نتایج روش تشخیص پیشنهادی برای جفت متغیرهای استفاده شده از مجموعه داده VAST را ارائه می دهد. برای هر پارامتر ۲۰ تکرار انجام می شود و همانطور که مشاهده می شود Var5 و Var6 حداقل مثبت کاذب را نشان می دهند. بنابراین، با استفاده از این متغیرها می توان برای تشخیص قابل اعتماد حمله DDoS پیشنهاد کرد. با این حال، Var1 و Var2 مثبت کاذب بالاتری را نشان می دهند و ممکن است برای روش تشخیص پیشنهادی مناسب نباشد.

جدول (۴): متغیرهای مرتبط در تشخیص نقطه تغییر در مجموعه داده VAST

نمونه	متغییرها	مثبت کاذب (%)				تغییر تشخیص داده شده				تکرار
		Ea	Ed	Eh	Ev	Ea	Ed	Eh	Ev	
	Var1,2	30	10	0	40	14	18	20	12	80
DDoS1	Var3,4	0	0	0	10	20	20	20	18	80
	Var5,6	0	0	0	0	20	20	20	20	80
	Var1,2	40	5	30	30	12	19	14	14	80
DDoS2	Var3,4	20	0	0	15	16	20	20	17	80
	Var5,6	10	0	0	0	18	20	20	20	80
	Var1,2	5	0	0	10	19	20	20	18	80
DDoS3	Var3,4	0	0	0	10	20	20	20	18	80
	Var5,6	0	0	0	0	20	20	20	20	80
	Var1,2	5	5	0	5	19	19	20	19	80
DDoS4	Var3,4	0	5	5	0	20	19	19	20	80
	Var5,6	0	0	0	0	20	20	20	20	80
	Var1,2	0	0	0	0	20	20	20	20	80
DDoS5	Var3,4	0	0	0	0	20	20	20	20	80
	Var5,6	0	0	0	0	20	20	20	20	80

طبق ارزیابی‌ها، روش پیشنهادی در مواردی که تغییری رخ می دهد دقیق است (شروع حمله در بازه بررسی باشد). با این حال، اگر تغییری ایجاد نشود (حالت بلوغ حمله) ناکارآمد است. برای تشخیص وضعیت بلوغ حمله، می توان انرژی متوسط جریان را برای مدت طولانی، به عنوان مثال داده‌های روزانه، مطالعه کرد. علاوه بر این، آزمایش دیگری از رویکرد در برابر حملات DDoS در بخش بعدی با استفاده از مجموعه داده ISCX ارائه شده است [۴۱].

۴-۱- شناسایی حمله با استفاده از مجموعه داده ISCX

مجموعه داده‌های ISCX نیز دادگان شناخته شده و واجد شرایطی برای ارزیابی روش پیشنهادی هستند. در ۱۴ و ۱۵ ژوئن در

این مجموعه داده دو حمله انجام شده است. با استفاده از ترافیک دارای برچسب این روزها، از جمله دقایقی قبل از حمله، ترافیک ارزیابی استخراج می‌شود و متغیرهای به کار رفته مجموعه داده به ترتیب شامل totalSourceBytes (Var1)، totalDestinationBytes (Var2)، totalDestinationPackets (Var3) و totalSourcePackets (Var4) هستند. در ادامه، نتایج روش تشخیص پیشنهادی با استفاده از مجموعه داده ISCX در جدول (۶) ارائه شده است، برای هر پارامتر با ۴۰ تکرار آزمایش می‌شود. همانطور که نشان داده شده است، حداقل مثبت کاذب برای پارامترهای Ea و Eh بدست می آید. بعلاوه، تأثیر جفت متغییرهای جریان بر روی مجموعه داده ISCX در جدول (۶) آورده شده است که ۲۰ تکرار برای هر پارامتر انجام شده است. در اینجا Var3 و Var4 حداقل مثبت کاذب را ارائه می دهند.

جدول (۵): نتایج تشخیص نقطه تغییر در مجموعه داده‌های ISCX

نمونه	مثبت کاذب (%)				تغییر تشخیص داده شده				تکرار
	Ea	Ed	Eh	Ev	Ea	Ed	Eh	Ev	
ISCX-14	2.5	65	22.5	55	39	14	31	18	160
ISCX-15	0	2	0	0	40	38	40	40	160

جدول (۶): متغیرهای مرتبط در تشخیص نقطه تغییر با استفاده از مجموعه داده ISCX

نمونه	متغییرها	مثبت کاذب (%)				تغییر تشخیص داده شده				تکرار
		Ea	Ed	Eh	Ev	Ea	Ed	Eh	Ev	
ISCX-14	Var1,2	5	100	45	75	19	0	11	5	80
	Var3,4	0	30	0	35	20	14	20	13	80
ISCX-15	Var1,2	0	0	0	0	20	20	20	20	80
	Var3,4	0	10	0	0	20	18	20	20	80
Return sequences	False			تجربی						

بعد از تشخیص ترافیک مشکوک در مرحله قبل، پارامترهای آنها به DNN ارسال می‌شود. در جدول (۷)، مقادیر ابرپارامترهای استفاده شده برای RNN و مقدار و روش استفاده شده برای انتخاب آنها را نشان داده است. ابر پارامترهای ذکر شده برای آموزش مدل مورد استفاده قرار گرفتند و برای دستیابی به نتایج بهینه تنظیم شده‌اند و ما با مقایسه عملکرد و سایر تکنیک‌های استفاده در ادبیات، نتایج خود را ارزیابی خواهیم کرد.

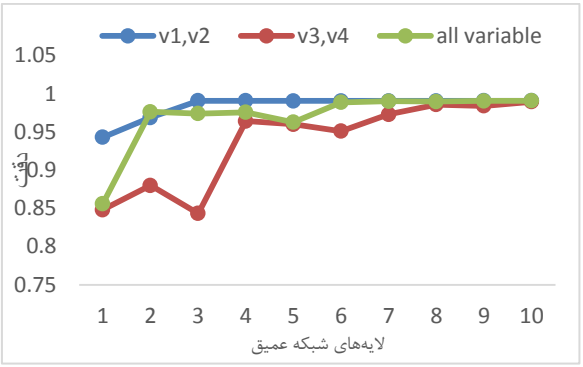
جدول (۷): ابر پارامترهایی که برای آموزش مدل استفاده شدند

ابرپارامتر	مقدار	روش
نرخ یادگیری	1×10^{-3}	Adam
بهینه ساز	Adam	بهترین روش
Epochs	50	تجربی
Batch size	10	تجربی
LSTM layers	1-10	تجربی
هزینه	Binary cross-entropy	تجربی
معیار ارزیابی	Accuracy	تجربی

هنگامی که از خروجی تجزیه و تحلیل دو بعدی سه جفت متغیر در DNN استفاده می شود، دقت بالای قابل توجهی در تشخیص حمله بدست می‌آید. همانطور که در جدول (۸) نشان داده شده است به بیش از ۱۰ لایه نیازی نیست، زیرا دقت مناسبی به دست آمد. همانطور که در جدول مشاهده می شود، جفت متغیرهای ۱ و ۲ دارای دقت شناسایی قابل قبول هستند که با ترکیب دو متغیر ۵ و ۶، این دقت با ۷ لایه تا ۰,۹۹۹۴ افزایش می‌یابد و همچنین ترکیب همه متغیرها در ۱۰ لایه دقت ۰,۹۹۹۹ را ارائه می‌دهد. بسته به زمان قابل قبول برای تشخیص، می توان از هر سه حالت بالا استفاده کرد (هر جه تعداد متغیرهای بیشتری شود، مدت یادگیری نیز طولانی تر است در نتیجه تشخیص دیرتر اتفاق می افتد) .

جدول (۸)نتایج DNN با استفاده از خروجی ویژگی‌های تجزیه موجک دوبعدی از مجموعه داده VAST

متغییرها / لایه ها	V1,v2	V3,v4	V5,v6	V1,v2,v3,v4	V1,2,5,6	V3,4,5,6	همه متغییرها
1	0.9573	0.8581	0.8654	0.7906	0.877	0.8670	0.8462
2	0.9902	0.8900	0.8673	0.9985	0.9644	0.855	0.9712
3	0.9908	0.8333	0.8817	0.9576	0.9763	0.9297	0.9840
4	0.9906	0.9741	0.8901	0.9078	0.9869	0.8992	0.9856
5	0.9908	0.9700	0.8861	0.9927	0.9759	0.9461	0.9527
6	0.9908	0.9409	0.8796	0.9708	0.9992	0.9692	0.9986
7	0.9908	0.9728	0.8692	0.9816	0.9994	0.9536	0.9950
8	0.9908	0.9958	0.8840	0.9985	0.9994	0.9638	0.9997
9	0.9907	0.9840	0.8916	0.9995	0.9995	0.9835	0.9996
10	0.9907	0.9894	0.8713	0.9999	0.9989	0.9858	0.9999



شکل (۶) نتایج دقت DNN با استفاده از خروجی ویژگی‌های تجزیه موجک دوبعدی از مجموعه دادهISCX

همه نتایج به دست آمده در بخش یادگیری عمیق، به k fold cross validationبا k=5 به دست آمده اند و نتایج گزارش شده در جدول (۸) و شکل (۶) میانگین ۵ تکرار مربوطه است.

در جدول (۹) نتیجه مقایسه روش پیشنهادی با تحقیقات قبلی آمده است که دقت روش پیشنهادی نتیجه بهتری نسبت به روشهای قبلی دارد. نقطه ضعف روش پیشنهادی، باتهایی که رفتار انسان را تقلید می‌کنند، است.

جدول (۹): مقایسه نتایج روش پیشنهادی با روش‌های قبلی

	دقت (%)
روش پیشنهادی (ترکیبی)	99.99
DNN[26]	99
Adaptive DL[28]	95
Multiple DNN[29]	99.79
Cloud Computing + SDN [42]	80.29
Digital Wavelet [43]	80
Stacked AutoeEcoder [44]	98.99
SVM and DNN [45]	92.30
DL in SDN [46]	75.75
Hybrid DL [47]	96.30

۵- نتیجه

حملات DDoS می‌تواند از تجهیزات مقصد یا مسیر سواستفاده کنند. علاوه بر این، این حملات می توانند مسیرها و امکاناتی را که توسط کاربران قانونی استفاده می‌شود، به طور غیرقانونی به کار گیرد و کاربران قانونی را از دسترسی به خدمات محروم سازند که این امر خصوصا در شبکه‌هایی مانند شبکه پلیس که نیاز به در دسترس بودن آن همیشگی است از اهمیت بیشتری برخوردار است. بنابراین، شناسایی حملات DDoS براساس رفتار کاربران یک مسئله مهم است و روش‌های تشخیص با زمان محاسباتی کم و سادگی بالا از سایر روش‌ها موثرترند. در این مقاله یک روش برای شناسایی اولیه حمله DDoS با استفاده از ویژگی‌های ترافیک بدون نیاز به دانستن رفتار عادی شبکه یا ذخیره مشخصات ارائه شد. تجزیه و تحلیل موجک دو بعدیبرای بدست آوردن نمودارهای توزیع انرژی، به عنوان نمودارهای کنترل استفاده می‌شود. سپس، از نقطه تغییر انرژی برای شناسایی حملات توسط قوانین منطق فازی استفاده می‌شود و ترافیک مشکوک به عنوان ورودی به شبکه عمیق برای تشخیص دقیق ارسال می‌شود. این روش در مجموعه دادههای VAST و ISCX اجرا شد و زمان تشخیص ۱۰ ثانیه و دقت ۹۹,۹۹ درصد برای دادگان VAST و ۹۹,۰۸ درصد برای دادگانISCX بدست می‌آید. برای تحقیقات بیشتر، استفاده از روش پیشنهادی در سایر مجموعه‌های داده و انواع حمله دیگر پیشنهاد می شود.

مراجع

[1] N. Dayal, P. Maity, S. Srivastava, and R. Khondoker, "Research Trends in Security and DDoS in SDN," *Secur. Commun. Networks*, vol. 9, no. 18, pp. 6386–6411, Dec. 2016.

[2] H.-T. Wu and C.-W. Tsai, "An intelligent agriculture network security system based on private blockchains," *J. Commun. Networks*, vol. 21, no. 5, pp. 503–508, Oct. 2019.

[3] K. J. Singh and T. De, "MLP-GA based algorithm to detect application layer DDoS attack," *J. Inf. Secur. Appl.*, vol. 36, pp. 145–153, Oct. 2017.

[4] Y. Wang, J. Ma, L. Zhang, W. Ji, D. Lu, and X. Hei, "Dynamic game model of botnet DDoS attack and defense," *Secur. Commun. Networks*, vol. 9, no. 16, pp. 3127–3140, Nov. 2016.

[5] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis," in *2016 8th International Conference on Communication Systems and Networks*

"Detection of collusive interest flooding attacks in named data networking using wavelet analysis," in *Proceedings - IEEE Military Communications Conference MILCOM*, 2017, vol. 2017-October, pp. 557–562.

[19] Z. Du, L. Ma, H. Li, Q. Li, G. Sun, and Z. Liu, "Network Traffic Anomaly Detection Based on Wavelet Analysis," in *2018 IEEE 16th International Conference on Software Engineering Research, Management and Applications (SERA)*, 2018, pp. 94–101.

[20] G. Kaur, A. Bansal, and A. Agarwal, "Wavelets Based Anomaly-Based Detection System or J48 and Naïve Bayes Based Signature-Based Detection System: A Comparison," in *Advances in Intelligent Systems and Computing*, vol. 696, Springer Verlag, 2018, pp. 213–224.

[21] D. Lavrova, P. Semyanov, A. Shtyrkina, and P. Zegzhda, "Wavelet-analysis of network traffic time-series for detection of attacks on digital production infrastructure," *SHS Web Conf.*, vol. 44, no. 14, p. 00052, Jun. 2018.

[22] M. Yue, L. Liu, Z. Wu, and M. Wang, "Identifying LDoS attack traffic based on wavelet energy spectrum and combined neural network," *Int. J. Commun. Syst.*, vol. 31, no. 2, p. e3449, Jan. 2018.

[23] G. Carl, R. R. Brooks, and S. Rai, "Wavelet based Denial-of-Service detection," *Comput. Secur.*, vol. 25, no. 8, pp. 600–615, Nov. 2006.

[24] Y. Chen, K. Hwang, and W.-S. Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 12, pp. 1649–1662, Dec. 2007.

[25] Y. Lv, H. Ren, X. Gao, T. Sun, H. Zhang, and X. Guo, "Multi-scale Risk Assessment Model of Network Security Based on LSTM," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12519 LNCS, pp. 257–267, 2020.

[26] J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, "Method of intrusion detection using deep neural network," *2017 IEEE Int. Conf. Big Data Smart Comput. BigComp 2017*, pp. 313–316, 2017.

[27] C. G. Cordero, S. Hauke, M. Muhlhauser, and M. Fischer, "Analyzing flow-based anomaly intrusion detection using Replicator Neural Networks," in *2016 14th Annual Conference on Privacy, Security and Trust, PST 2016*, 2016, pp. 317–324.

[28] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, "Towards sFlow and adaptive polling sampling for deep *(COMSNETS)*, 2016, no. 1, pp. 1–2.

[6] Q. Liao, H. Li, S. Kang, and C. Liu, "Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching," *Secur. Commun. Networks*, vol. 8, no. 17, pp. 3111–3120, Nov. 2015.

[7] M. Arman, "Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 7, no. 1, pp. 56–70, Apr. 2020.

[8] H. Rahmani, N. Sahli, and F. Kammoun, "Joint entropy analysis model for DDoS attack detection," in *5th International Conference on Information Assurance and Security, IAS 2009*, 2009, vol. 2, pp. 267–271.

[9] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

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

[11] P. Shinde and S. Guntupalli, "Early DoS Attack Detection using Smoothened Time-Series andWavelet Analysis," in *Third International Symposium on Information Assurance and Security*, 2007, pp. 215–220.

[12] J. Cheng, C. Zhang, X. Tang, V. S. Sheng, Z. Dong, and J. Li, "Adaptive DDoS Attack Detection Method Based on Multiple-Kernel Learning," *Secur. Commun. Networks*, vol. 2018, pp. 1–19, Oct. 2018.

[13] A. Aborujilah and S. Musa, "Cloud-Based DDoS HTTP Attack Detection Using Covariance Matrix Approach," *J. Comput. Networks Commun.*, vol. 2017, 2017.

[14] X. Ren, R. Wang, and H. Wang, "Wavelet analysis method for detection of DDoS attack on the basis of self-similarity," *Front. Electr. Electron. Eng. China*, vol. 2, no. 1, pp. 73–77, Mar. 2007.

[15] M. hui YANG and R. chuan WANG, "DDoS detection based on wavelet kernel support vector machine," *J. China Univ. Posts Telecommun.*, vol. 15, no. 3, pp. 59–63, 2008.

[16] V. Srihari and R. Anitha, "DDoS detection system using wavelet features and semi-supervised learning," in *Communications in Computer and Information Science*, 2014, vol. 467, pp. 291–303.

[17] C.-T. Huang, S. Thareja, and Y.-J. Shin, "Wavelet-based Real Time Detection of Network Traffic Anomalies," in *2006 Securecomm and Workshops*, 2006, pp. 1–7.

[18] Y. Xin, Y. Li, W. Wang, W. Li, and X. Chen,

learning based DDoS detection in SDN," *Futur. Gener. Comput. Syst.*, vol. 111, pp. 763–779, 2020.

[29] D. Chamou *et al.*, "Intrusion detection system based on network traffic using deep neural networks," *IEEE Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD*, vol. 2019-Septe, pp. 1–6, 2019.

[30] S. Katti, B. Krishnamurthy, and D. Katabi, "Collaborating against common enemies," *Proc. 5th ACM SIGCOMM Conf. Internet Meas. - IMC '05*, p. 1, 2005.

[31] M. Hamdi and N. Boudriga, "Detecting Denial-of-Service attacks using the wavelet transform," *Comput. Commun.*, vol. 30, no. 16, pp. 3203–3213, Nov. 2007.

[32] S. N. Shiaeles, V. Katos, A. S. Karakos, and B. K. Papadopoulos, "Real time DDoS detection using fuzzy estimators," *Comput. Secur.*, vol. 31, no. 6, pp. 782–790, Sep. 2012.

[33] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," *2015 Int. Conf. Comput. Netw. Commun. ICNC 2015*, pp. 77–81, 2015.

[34] X. Ma and Y. Chen, "DDoS detection method based on chaos analysis of network traffic entropy," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 114–117, Jan. 2014.

[35] X. Ma and Y. Chen, "DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 114–117, Jan. 2014.

[36] S. Jin and D. S. Yeung, "A covariance analysis model for DDoS attack detection," in *IEEE International Conference on Communications*, 2004, vol. 4, pp. 1882–1886.

[37] V. Gulisano, M. Callau-Zori, Z. Fu, R. Jiménez-Peris, M. Papatriantafilou, and M. Patiño-Martínez, "STONE: A streaming DDoS defense framework," *Expert Syst. Appl.*, vol. 42, no. 24, pp. 9620–9633, Dec. 2015.

[38] "Vast dataset." [Online]. Available: https://vacommunity.org/VAST+Challenge+2013%3A+Mini-Challenge+3.

[39] M. Gülbay and C. Kahraman, "Development of fuzzy process control charts and fuzzy unnatural pattern analyses," *Comput. Stat. Data Anal.*, vol. 51, no. 1, pp. 434–451, 2006.

[40] "Western E. Statistical quality control handbook. Western Electric Co."

[41] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Comput. Secur.*, vol. 31, no. 3, pp. 357–374, 2012.