دانشگاه صنعتی شریف

دانشکده مهندسی کامپیوتر

پایان‌نامه کارشناسی ارشد

رشته فناوری اطلاعات

تشخیص حملات منع سرویس توزیع‌شده از هجوم ناگهانی کاربران

نگارش:

هادی رنجبر

استاد راهنما:

دکتر امیرحسین جهانگیر

تابستان ۱۳۹۴


بسم الله الرحمن الرحيم

به نام خدا

دانشگاه صنعتی شریف

دانشکده مهندسی کامپیوتر

پایان‌نامه کارشناسی ارشد

تشخیص حملات منع سرویس توزیع‌شده از هجوم ناگهانی کاربران

نگارش: هادی رنجبر

استاد راهنما: دکتر امیرحسین جهانگیر **امضاء:**

استاد ممتحن داخلی: دکتر مهدی خرازی **امضاء:**

استاد ممتحن خارجی: دکتر مهدی شجری **امضاء:**

تاریخ:

تقدیم به پدر و مادر عزیز و مهربانم که در تمام مراحل زندگی، پشتیبانی مطمئن برایم بودند.

با تشکر از استاد بزرگوارم، دکتر امیرحسین جهانگیر که بدون کمک‌ها و راهنمایی‌های ایشان، تامین این پایان نامه بسیار دشوار می‌نمود.

از خانم دکتر لاله ارشدی که در طول این پژوهش ،اینجانب را راهنمایی کردند، نهایت تشکر را دارم.

همچنین از آقای دکتر خرازی و آقای دکتر شجری بابت تمام زحماتی که کشیدند، سپاسگزاری می‌کنم.

چکیده

حملات منع سرویس توزیع‌شده، نوعی از تهدیدهای امنیتی مرتبط با شبکه‌های کامپیوتری می‌باشند که دسترس‌پذیری منابع شبکه را هدف قرار می‌دهند. یکی از ویژگی‌های این نوع حملات حجم ترافیک بالا و یا درخواست سرویس توسط تعداد زیادی مهاجم غیرمجاز که با هم شبکه‌ای از ربات‌ها را تشکیل می‌دهند، می‌باشد که باعث کاهش کارایی شبکه می‌شوند. مسئله تشخیص تعداد زیاد کاربران مجاز در هجوم ناگهانی از درخواست‌های غیرمجاز حمله، امروزه یکی از بزرگ‌ترین چالش‌های پیش رو متخصصان امنیت شبکه می‌باشد. روش‌هایی که تاکنون ارائه شده‌اند، عمدتاً یا کارایی لازم را نداشته‌اند و یا با بالا رفتن دانش مهاجمین در تقلید رفتار کاربران مجاز، در کوتاه‌مدت پاسخگو بوده‌اند. روش‌هایی که عملکرد بهتری نسبت به سایر روش‌ها داشته‌اند اکثراً بر اساس استخراج ویژگی‌های آماری عمل می‌کنند که البته بیشتر آن‌ها ویژگی‌های آماری یک جریان ترافیکی را مورد بررسی قرار می‌دهند و درصورتی‌که دو جریان مختلف با هم ترکیب شده باشند، این روش‌ها چندان پاسخگو نمی‌باشند. هدف از این پژوهش ارائه‌ی روشی است که علاوه بر اینکه مزایای روش‌های قبلی در تشخیص نوع مختلف ترافیک (حمله منع سرویس و هجوم ناگهانی کاربران) را داشته باشد، بتواند در هنگام ترکیب دو جریان از ترافیک‌های یادشده با یکدیگر ترافیک حمله را تشخیص داده و نسبت به تفکیک آن از ترافیک سالم کاربران سیستم، به‌درستی عمل نماید. این کار مستلزم این است که روش مذکور بتواند ویژگی‌های جریان مربوط به یک کاربر منحصربه‌فرد را مورد بررسی قرار دهد. این پژوهش ابتدا به بررسی ویژگی‌های ترافیک‌های حمله و هجوم ناگهانی کاربران می‌پردازد. سپس رفتار کاربران مختلف را با جریان رسیده از ربات‌های حمله منع سرویس مقایسه می‌کند. این مقایسه شامل بررسی ویژگی‌های مختلف آماری زمان بین بسته‌های پشت سر هم رسیده از یک مشتری (یک کاربر در هجوم ناگهانی و یا یک ربات در حمله منع سرویس) می‌باشد.

درنهایت با استفاده از این ویژگی‌های استخراج‌شده، بـا اسـتفاده از روش‌هـای خوشـه‌بنـدی، مـی‌تـوان جریان‌های حمله را از جریان‌های کاربران مجاز تشخیص داد و در انتها روش مذکور از نظر میـزان دقـت تشخیص، بازخوانی و سایر معیارهای ارزیابی موجود مورد بررسی قرار می‌گیرد.

واژه‌های کلیدی:

حملات منع سرویس، هجوم ناگهانی کاربران، خوشه‌بندی، خودهمانندی، الگوی رفتاری، آنتروپی

فهرست مطالب

فهرست جدول‌ها

فهرست شکل‌ها

فصل ۱:

مقدمه

۱-۱- تعریف مساله

حملات منع سرویس[1] امروزه یکی از بزرگ‌ترین تهدیدهای امنیتی شبکه‌های کامپیوتری، به‌ویژه اینترنت، محسوب می‌شوند. هدف از این حملات جلوگیری از دسترسی کاربران مجاز به منابع شبکه و اختلال در سرویس‌دهی شبکه است. انگیزه مهاجم از این حملات می‌تواند سیاسی، اقتصادی، انتقام شخصی و یا خرابکاری باشد [۱,۲]. به همین دلیل، سایت‌های بانکی و بورس، درگاه‌های فروش محصولات و شبکه‌های اجتماعی بیشتر در معرض این نوع حملات قرار دارند. البته این حملات مختص سرویس‌دهنده‌ها نمی‌باشند و حتی ممکن است حمله متوجه یک مسیریاب[2] گذرگاه اصلی[3] شبکه اینترنت نیز باشد و کل شبکه را دچار مشکل نماید. انواع مختلفی از این حمله در لایه‌های مختلف شبکه، قابل پیاده‌سازی هستند که نوع حمله و نحوه تأثیرگذاری آن با توجه به ویژگی‌های هر لایه متفاوت است. یکی از مشکلات مطرح در تشخیص این نوع حملات، توانایی تمایز آن‌ها از هجوم ناگهانی کاربران[4] است. هجوم ناگهانی وقتی اتفاق می‌افتد که تعداد زیادی از کاربران در یک‌لحظه اقدام به دسترسی به منابع یک شبکه کنند. در این حالت سرویس‌دهنده ممکن است توان پاسخگویی به حجم عظیم درخواست دهندگان را نداشته باشد و با مشکل مواجه شود و حتی در برخی موارد به‌طور کامل از کار بیافتد. برای مثال، ورود تعداد زیادی کاربر به یک سایت خبری، در هنگام وقوع رویدادی خاص، می‌تواند نمونه‌ای از هجوم ناگهانی باشد. ازآنجایی‌که افزایش ترافیک رسیده به سرویس‌دهنده[5] در حملات منع سرویس تا حد زیادی مشابه هجوم ناگهانی کاربران می‌باشد، تشخیص حملاتی که این هجوم را

---

[1] Denial of Service Attacks

[2] Router

[3] Backbone

[4] Flash Crowd

[5] Server

شبیه‌سازی و تقلید می‌کنند و یا هم‌زمان با وقوع این رویداد اعمال می‌شوند بسیار دشوار است و نیازمند تحلیل و بررسی دقیق ترافیک شبکه و شناخت ویژگی‌های مختلف هر یک از موارد فوق برای تفکیک آن-ها از یکدیگر می‌باشد. تا آنجایی که در سال‌های اخیر نوع جدیدی از حملات منع سرویس معرفی شده‌اند که به آن‌ها حمله هجوم ناگهانی کاربران[1] گفته می‌شود. این حملات به‌صورت توزیع‌شده انجام می‌شود و حجم ترافیک به‌صورت ناگهانی افزایش می‌یابد به‌طوری‌که سیستم‌های تشخیص حمله موجود نمی‌توانند تشخیص دهند که تعداد زیادی از کاربران که با آدرس‌های مختلف در حال درخواست سرویس هستند، کاربران مجاز سیستم هستند و یا با هدف خرابکارانه بخشی از یک حمله منع سرویس می‌باشند [۳]. همان‌طور که گفته شد ممکن است که این حملات هم‌زمان با هجوم ناگهانی کاربران نیز اتفاق بیفتد. برای مثال، یک رقیب اقتصادی که از هجوم خریداران به سایت رقیب خود در ساعات مشخصی آگاه است، می‌تواند اقدام به یک حمله منع سرویس در آن زمان نموده که ترافیک حاصل از ترکیب این حمله با هجوم کاربران می‌تواند بسیار بزرگ و غیر قابل روانه سازی باشد و پیش‌بینی‌های و تمهیدات در نظر گرفته‌شده در مورد میزان سرویس‌دهی و پهنای باند را با خطا و اختلال مواجه کند. بسیاری از روش‌های ارائه‌شده تاکنون، فقط قادر به تشخیص حملاتی هستند که به‌صورت ساده و توسط تعداد محدودی حمله‌کننده انجام می‌شود و تشخیص حملات با گستردگی بالا و تعداد حمله‌کننده زیاد و یا حملاتی که در حین هجوم ناگهانی کاربران اتفاق می‌افتند، یکی از چالش‌های پیش روی متخصصان و محققین امنیت شبکه می‌باشد.

یک روش و سیستم تشخیص حملات منع سرویس باید ویژگی‌های زیر را دارا باشد [۴]:

[1] Flash Crowd attack

۱- تشخیص سریع[1]

ازآنجایی‌که حملات منع سرویس بسیار سریع عمل کرده و در زمان بسیار کمی حجم ترافیک بسیار بالا می‌رود، اگر عمل تشخیص به‌موقع انجام نشود، ممکن است بعد از تشخیص، توانایی مقابله با حمله وجود نداشته باشد، به عبارتی، سیستم وقتی متوجه حمله منع سرویس شود که حمله تأثیر موردنظر خود را گذاشته و برای مقابله با آن دیر شده است. بنابراین باید دقت کرد که لایه‌های دفاعی را قبل‌تر از سرویس‌دهنده موردنظر قرار داد. برای مثال اگر بتوان حمله را در یک مسیریاب تشخیص داد، می‌توان عمل مقابله با آن را در آن مسیریاب و یا حتی قبل‌تر از آن انجام داد و سرویس‌دهنده با استفاده از مسیریاب‌های دیگر تعبیه‌شده به کار خود ادامه دهد. این مسئله اهمیت تشخیص حمله منع سرویس در لایه‌های پایین‌تر شبکه به‌خصوص لایه شبکه[2] و لایه پیوند داده[3] را بیش‌ازپیش روشن می‌شود. تشخیص حمله در لایه‌های بالاتر مانند لایه کاربرد نیازمند بررسی محتویات بسته‌ها در یک سرویس‌گیرنده است که نیازمند صرف منابع مختلف و زمان است.

۲- قابلیت اطمینان[4]

روش پیاده‌سازی شده باید به‌درستی میان ترافیک رسیده از کاربران مجاز (هجوم ناگهانی کاربران) با ترافیک حمله تمایز[5] قائل شود. هرچند ممکن است در عمل این مساله امکان‌پذیر نباشد، اما در روش مورد استفاده، باید تعداد تشخیص‌های منفی نادرست[6] و مثبت نادرست[1]، صفر باشد. در عمل می‌توان به

---

[1] Fast Detection

[2] Network Layer

[3] Data Link Layer

[4] Reliability

[5] Discriminate

[6] False Negative

این شرط بسنده کرد که این موارد حداقل باشند. علاوه بر این، روش موجود باید از نظر مواردی چـون دقت[۲]، بازخوانی[۳] و درستی، دقیق عمل کند.

۳- امکان‌پذیری (عملی بودن)[۴]

روش مورد نظر باید قابلیت پیاده‌سازی در دنیای واقعی را با توجه به زیرساخت‌ها و همبنـدی‌هـای[۵] موجود در شبکه‌ها، داشته باشد. برای مثال، روش‌هایی که نیازمند نگهداری حجم عظیم اطلاعات هستند و یا نیاز به انجام پردازش‌های سنگین روی داده دارند، ممکـن اسـت کـارایی لازم را نداشـته باشـند و پیاده‌سازی آن‌ها از لحاظ عملی امکان‌پذیر نباشد.

۴- تشخیص بی‌درنگ[۶]

روش مورد نظر باید به گونه‌ای باشد که به‌صورت بی‌درنگ و به‌محض دریافت ترافیک‌های غیرطبیعی عملیات تشخیص خود را آغاز کند. ازآنجایی‌که ویژگی حمله منع سرویس، بالا بردن حجم ترافیک است، در صورت گذر زمان و عدم تشخیص بی‌درنگ، حجم ترافیک بالا رفته و حمله به میزان زیادی اثرگـذار خواهد بود. بنابراین هرگونه تأمل اضافی در تشخیص ترافیک حمله ممکن است حتی در صورت تشخیص، مقابله با حمله را غیرممکن سازد.

۵- انعطاف‌پذیری[۷]

---

[1] False Positive

[2] Precision

[3] Recall

[4] Feasibility

[5] Topology

[6] Real Time Detection

[7] Flexibility

روش مورد نظر باید توانایی تشخیص حملات مختلف را داشته باشد و مختص به یک حمله خاص نباشد. مهاجم ممکن است پروتکل مورد استفاده یا روش خود را تغییر دهد. این تغییر روش نباید بر روی سیستم تشخیص تأثیر خاصی داشته باشد و یا بتوان با حداقل تغییرات در سیستم آن را با تغییرات انجام‌شده توسط مهاجم، سازگار کرد.

تاکنون روش‌های بسیاری برای تشخیص حملات منع سرویس و ترافیک‌های مجاز کاربران ارائه‌شده است. اما همچنان این مسئله با توجه به افزایش دانش مهاجمان و استفاده از روش‌های جدیدتر که عملیات کشف توسط سیستم‌های تشخیص را با مشکل مواجه می‌کنند، همچنان مورد توجه محققین قرار دارد. روش‌های قدیمی که بر اساس نوع پروتکل و یا ویژگی‌های پروتکل‌های خاص مانند TCP/IP عمل می‌کردند، با توجه به توانایی مهاجمان به تولید ترافیک‌های دلخواه با ویژگی‌های مختلف قابل استفاده نیستند. روش‌هایی که بر اساس نرخ افزایش ترافیک و آستانه[1] حجم درخواست‌ها عمل می‌کردند، با ظهور پدیده هجوم ناگهانی کاربران و شباهت ترافیک آن با ترافیک مذکور، عملاً کارایی خود را از دست داده‌اند. البته روش‌های جدید که بر اساس ویژگی‌های آماری ترافیک مانند میزان ضریب شباهت و همبستگی دو ترافیک عمل می‌کنند [۵, ۶]، اکثراً توانایی تشخیص جریان‌های ترافیکی از یکدیگر، آن‌هم با ضریب اطمینان پایین را دارند و در حالتی که دو پدیده مذکور (هجوم ناگهانی کاربران و حمله منع سرویس) به‌طور هم‌زمان اتفاق بیفتند، با توجه به ترکیب جریان‌های مختلف رسیده به یک مسیریاب یا سرویس‌دهنده، پاسخگو نمی‌باشند. بنابراین آنچه مشخص است، برای اینکه روش موردنظر کارایی لازم را برای تشخیص در حالتی که هر دو پدیده هم‌زمان اتفاق میافتند داشته باشد، باید به‌جای سطح جریان[2]،

---

[1] Threshold

[2] Collective Level

در سطح تک‌تک درخواست دهندگان[1]، توانایی تشخیص را داشته باشد. یعنی بتواند با توجه به ویژگی‌هایی که بسته‌های رسیده از سمت یک کاربر و مقایسه آن با ویژگی‌های بسته‌های رسیده از سمت یک ربات حمله منع سرویس، دو جریان مختلف را از یکدیگر تشخیص دهد. اساس کارهایی که تاکنون در این مورد انجام گرفته‌اند، چه روش‌هایی که در سطح جریان و چه روش‌هایی که مقایسه‌ها در سطح کاربران انجام می‌دهند، بر پایه ویژگی‌های آماری جریان قرار دارد. طبق تحقیقی که انجام گرفته است، مهاجم در بهترین حالت تنها می‌تواند از ۳۰ درصد سیستم‌هایی که به ربات حمله آلوده شده‌اند و تحت کنترل درآمده‌اند، برای تولید ترافیک حمله استفاده کند [۷]. دلیل این امر نیز این است تمامی این سیستم‌ها درآن‌واحد روشن و در دسترس نیستند و بعلاوه هماهنگی و بکار گرفتن همه این ربات‌ها با توجه به اینکه روی شبکه‌های گوناگون با پهنای باندهای مختلف و زیرساخت‌های مختلف قرار دارند دشوار می‌باشد. لذا ویژگی‌های آماری ترافیکی که توسط یک کاربر مجاز در هجوم ناگهانی کاربران تولید می‌شود، با ترافیکی که توسط یک برنامه خودکار یا نیمه‌خودکار که با دریافت دستور حمله، چه به‌صورت زمان‌بندی‌شده و چه به‌صورت دریافت دستور حمله، اقدام به تولید ترافیک می‌کند تفاوت‌هایی دارد. این پژوهش این ویژگی‌ها را بررسی و استخراج می‌کند و با استفاده از آن‌ها میان ترافیک حمله منع سرویس و هجوم ناگهانی کاربران تمییز[2] قائل می‌شود. با استفاده از این ویژگی‌ها در یک روش خوشه‌بندی، می‌توان این دو پدیده را حتی درصورتی‌که هر دو هم‌زمان با هم رخ دهند، از یکدیگر تفکیک کرد.

---

[1] Individual Level

[2] Discriminate

با استفاده از تفکیک کاربران مجاز و غیرمجاز سیستم درنهایت می‌توان جلوی حمله‌ای را که در حین یک هجوم ناگهانی اتفاق می‌افتد را گرفت. این کار را می‌توان با اطلاع‌رسانی آدرس کاربران غیرمجاز به مسیریاب‌های بالادستی[1] و مسدود کردن[2] آن‌ها انجام داد.

در انتها، بررسی‌های انجام‌گرفته بر روی روش ارائه‌شده، نشان می‌دهد که نسبت به سایر روش‌های پیشین، کارایی و عملکرد بهتری دارد.

بنابراین، در ادامه این پژوهش، در فصل ۲، به بررسی مفاهیم اولیه و روش‌هایی که تاکنون برای تشخیص حملات منع سرویس از هجوم ناگهانی کاربران پیشنهاد شده‌اند، می‌پردازیم و مزایا و معایب هر یک را بررسی خواهیم کرد. سپس در فصل ۳، روش پیشنهادی خود را ارائه می‌کنیم. در فصل ۴، نتایج حاصل از این روش را با توجه به معیارهایی که معرفی خواهیم نمود، ارزیابی کرده و درنهایت در فصل ۵، نتیجه‌ی کلی از این پژوهش و کارهایی را که در آینده، در راستای این پژوهش انجام خواهد شد را بیان خواهیم کرد.

---

[1] Upstream Router

[2] Block

فصل ۲:

مفاهیم اولیه و کارهای پیشین

۲-۱- حملات منع سرویس

همان‌طور که ذکر شد، این حملات برای جلوگیری از دسترسی کاربران مجاز به سرویس‌های شبکه انجام می‌شوند. این حملات انواع مختلفی دارند و در لایه‌های مختلف شبکه مانند لایه انتقال، لایه شبکه و لایه کاربرد قابل انجام هستند که هر یک ویژگی‌های خاص خود را دارند.

امروزه نوع توزیع‌شده این حملات که توسط تعداد زیادی گره آلوده‌شده توسط مهاجم که در سرتاسر دنیا پراکنده شده‌اند و به آن‌ها روبات[1] گفته می‌شود، انجام می‌گیرد. مهاجم با کنترل و فرماندهی شبکه‌ای از روبات‌ها[2]، می‌تواند حملات گسترده و کارایی علیه شبکه‌های مختلف و کارگزاران وب انجام دهد.

فرماندهی این روبات‌ها می‌تواند به‌صورت خودکار و نیمه‌خودکار انجام شود. با رسیدن دستور حمله به روبات‌ها، آن‌ها اقدام به ارسال حجم عظیمی از ترافیک به سمت قربانی می‌کنند. این کار باعث می‌شود که منابع قربانی صرف ترافیک حمله شود و آن‌ها را از دسترس کاربران مجاز سیستم خارج کند. هدف این حملات امروزه از یک سرگرمی ساده برای حمله‌کنندگان خارج شده و به دلایلی چون رقابت‌های اقتصادی و سیاسی و خرابکاری، تبدیل شده است [۱, ۲, ۸]. به‌طوری‌که امروزه مهاجمان شبکه روبات‌های خود را جهت انجام حمله منع سرویس به‌صورت اجاره‌ای در اختیار دیگران قرار می‌دهند. مطالعات رفتارشناسی روبات‌ها و الگوی عملکرد آن‌ها و همچنین کشف و از بین بردن آن‌ها یکی از موضوعات مهم و پر چالش در زمینه‌ی امنیت شبکه می‌باشد[۹] .

---

[1] Bot

[2] Botnet

۲-۱-۱- انواع حملات منع سرویس

حملات منع سرویس با توجه به نحوه عملکرد و لایه‌ای از شبکه که در آن پیاده‌سازی شده‌اند، به دسته‌های گوناگونی تقسیم می‌شوند [۱۰]. در این پژوهش، حملاتی مد نظر ما هستند که با استفاده از حجم بالای ترافیک، منابع سیستم‌ها و شبکه را اشغال می‌کنند و مانع سرویس‌دهی آن‌ها می‌شوند. بنابراین حملاتی که در ادامه معرفی می‌شوند، شامل مواردی که از نقص یک سیستم و پروتکل خاص، مانند حمله پینگ مرگ[1]، استفاده می‌کنند، نمی‌شوند.

۲-۱-۱-۱- جریان سیل‌آسای ICMP[2]

این حمله که نوع خاصی از آن با نام اسمورف[3] نیز شناخته می‌شود، بر اساس ضعف پیکربندی شبکه که اجازه ارسال هر نوع بسته همه پخشی را به کاربران مختلف می‌دهد، عمل می‌کند. در این حمله، مهاجم با یک آدرس جعلی، بسته‌های پینگ را به یک یا چند سرور که قابلیت همه پخشی را دارند، ارسال می‌کند. آدرس جعلی، آدرس سیستم یا شبکه قربانی می‌باشد. سرور همه پخشی این تقاضا را برای تمام شبکه ارسال می‌کند. تمام ماشین‌های شبکه پاسخ را به سرور، ارسال همه پخشی می‌کنند. سرور همه پخشی پاسخ‌های دریافتی را به سمت سیستم هدف هدایت می‌کند. بدین‌صورت زمانی که ماشین حمله‌کننده تقاضایی را به چندین سرور روی شبکه‌های متفاوت همه پخشی می‌نماید، مجموعه پاسخ‌های تمامی کامپیوترهای شبکه‌های گوناگون به سیستم هدف ارسال می‌گردند و آن را از کار می‌اندازند. بنابراین پهنای باند شبکه به‌سرعت استفاده می‌شود و از انتقال بسته‌های مجاز به مقصدشان جلوگیری به عمل خواهد آمد.

---

[1] Ping of Death

[2] Internet Control Message Protocol

[3] Smurf

۲-۱-۱-۲- جریان سیل‌آسای SYN

این حمله زمانی اتفاق می‌افتد که میزبانی از بسته‌های سیل‌آسایTCP/SYN استفاده کند که آدرس فرستنده آن‌ها جعلی است. هرکدام از این بسته‌ها همانند یک درخواست اتصال بوده و باعث می‌شود سرور درگیر اتصالات متعدد نیمه‌باز بماند، با فرستادن یا برگرداندن بسته‌های تصدیق ACK TCP/SYN و منتظر بسته‌های پاسخ از آدرس فرستنده می‌ماند ولی چون آدرس فرستنده جعلی است هیچ پاسخی برگردانده نمی‌شود. این اتصالات نیمه‌باز تعداد اتصالات در دسترس سرور را اشباع می‌کنند و آن را از پاسخگویی به درخواست‌های مجاز تا پایان حمله باز می‌گذارند. بنابراین منابع سرور به اتصال‌های نیمه‌باز اختصاص خواهد یافت و امکان پاسخ‌گویی به درخواست‌ها از سرور منع می‌شود.

۲-۱-۱-۳- جریان سیل‌آسای UDP[1]

در این حمله جریان سیل‌آسایی از بسته‌های UDP به سمت قربانی ارسال می‌شود. ازآنجایی‌که UDP پروتکلی بدون نشست می‌باشد، بدون هیچ تصدیق و شروع ارتباطی، این جریان سیل‌آسا، درگاه‌های مختلف سیستم قربانی را اشغال کرده و مانع از سرویس‌دهی آن می‌شود.

۲-۱-۱-۴- حمله‌ی بازتابی[2]

در این حمله مهاجم بسته‌هایی مخدوش و آدرس جعل‌شده به سمت سیستم‌های مختلف می‌فرستد. این سیستم‌ها در پاسخ، بسته‌هایی به سمت آدرس مبدأ ارسال می‌کنند. اما ازآنجایی‌که این آدرس با آدرس قربانی جعل شده است، سیل عظیمی از بسته‌ها به سمت قربانی سرازیر می‌شوند.

---

[1] Unit Datagram Protocol

[2] Reflection Attack

۲-۱-۱-۵- حملات لایه کاربرد

این نوع حملات که از ویژگی‌های لایه کاربرد سو استفاده می‌کنند، نسبت به بقیه جدیدتر می‌باشند و عمل کشف و مقابله با آن‌ها بسیار سخت‌تر می‌باشد. برای مثال، حملاتی که از ویژگی اتصال موجـود در پروتکل HTTP برای اتصالات نیمه‌باز و هدر دادن منابع سرویس‌دهنده استفاده می‌کنند، از ایـن نـوع حملات هستند. این حملات معمولاً سرویس‌دهنده‌های وب، ایمیل و مواردی از این قبیل را هدف قـرار می‌دهند [۱۱, ۱۲].

۲-۱-۱-۶- حملاتی که برای اولین بار و با روشی جدید، اتفاق می‌افتند[1]

خطرناک‌ترین و تأثیرگذارترین حملات منع سرویس، آن دسته از حملات هستند که با روشی جدید و برای اولین بار اتفاق می‌افتند و ازآنجایی‌که سیستم‌های دفاعی موجود از عملکرد آن‌ها آگاه نیستند و برای آن‌ها برنامه‌ریزی نشده‌اند، بیشترین خسارات را بر جای می‌گذارند. امروزه مهم‌ترین هدف متخصصان امنیت شبکه ارائه روشی است که بتواند این حملات را شناسایی کند که البتـه بـا توجـه بـه افـزایش روزافزون دانش مهاجمان کار دشواری به نظر می‌رسد.

۲-۱-۲- کشف حملات منع سرویس و روش‌های دفاعی در برابر آن‌ها

برای تشخیص حملات منع سرویس بخصوص نوع توزیع‌شده‌ی آن، کارهای بسیاری صـورت گرفتـه است. از روش‌های مبتنی بر محاسبات آماری مانند محاسبه نرخ زمانی بـین بسـته‌هـای جریـان [۱۳]، بررسی ویژگی‌های آماری بسته‌های حمله[۱۴, ۱۵, ۱۶] ، تحلیل خوشه‌های[2] آدرس مبدأ [۱۷]، بررسی

[1] Zero Day Attack

[2] Cluster

اطلاعات بسته‌های جریان [۱۸] گرفته تا روش‌های مبتنی بر آنتروپی[1] [۱۹, ۲۰, ۲۱] و نظریه آشوب[2] [۲۲, ۲۳] و روش‌های مبتنی بر تکنیک‌های هوش مصنوعی و شبکه‌های عصبی[3] [۲۴, ۲۵] و روش‌هایی که بر پایه تحلیل طیف سیگنال[4]های دریافتی ترافیک کار می‌کنند [۲۶]. شاید در ابتدای امر این مسئله بدین گونه تصور شود که این روش‌ها که برای تشخیص حمله منع سرویس از ترافیک سالم به کار می‌روند، می‌توانند پاسخگوی نیاز ما در تشخیص حملات از هجوم ناگهانی کاربران باشد، اما باید این نکته را در نظر گرفت که اولاً هجوم ناگهانی کاربران از نظر ویژگی‌های ترافیکی شباهت بسیار زیادی به حمله منع سرویس و تفاوت نسبت به ترافیک سالم و عادی دارد. ثانیاً هجوم ناگهانی کاربران، همان‌طور که گفته شد، نوعی ناهنجاری در شبکه به شمار می‌رود [۲۷]. ازآن‌جهت که الگوی رفتاری کاربران تا حد بسیاری تغییر می‌کند و همچنین با افزایش تعداد کاربران و عدم توانایی سیستم در پاسخگویی به حجم عظیم درخواست‌ها، کاربران رفتارهای متفاوتی از خود نشان می‌دهند. برای مثال، عده‌ای از کاربران از سرویس‌دهی دلسرد شده و دست از تلاش برای دست‌یابی به سرویس مورد نظر خود برمی‌دارند. عده‌ای دیگر سعی می‌کنند تعداد درخواست‌ها و فاصله بین آن‌ها را افزایش دهند تا شاید درنهایت به هدف موردنظر خود برسند. بنابراین واضح است که هجوم ناگهانی کاربران را باید به‌عنوان پدیده متفاوتی نسبت به دسترسی‌های عادی و معمول به یک سرویس دسته‌بندی کرد که بسیاری از ویژگی‌های آن مشابه رفتارهای مهاجم در حمله منع سرویس است. اما باوجود همه شباهت‌های ذکرشده می‌توان از تفاوت‌های موجود بین این دو نهایت استفاده را در تشخیص آن‌ها از یکدیگر کرد. روش‌های موجود برای تشخیص این دو پدیده نیز بر پایه این تفاوت‌ها عمل می‌کنند [۲۷]. در ابتدای امر باید در نظر داشت که در ترافیک

---

[1] Entropy

[2] Chaos Theory

[3] Neural Networks

[4] Signal Spectrum

حمله منع سرویس، هرچقدر که مهاجم سعی در تقلید رفتار کاربران مجاز را داشته باشد، درنهایت حمله توسط نرم‌افزارهای خودکار تولید می‌شود. از طرفی، بالا بودن تعداد سیستم‌های آلوده‌ی حمله‌کننده (ربات‌ها) و پراکندگی آن‌ها، کار هماهنگی و مدیریت آن‌ها را توسط حمله‌کننده بسیار مشکل کرده است. طبق یک تحقیق انجام‌گرفته، مهاجم در بهترین حالت، تنها می‌تواند از ۳۰ درصد ربات‌های تحت کنترل خود، جهت انجام حمله استفاده کند [۷]. این مسئله بدین دلیل است که درآن‌واحد تمام سیستم‌های آلوده روشن و آماده نیستند.

۲-۲- هجوم ناگهانی کاربران

منظور از هجوم ناگهانی کاربران درخواست تعداد زیادی کاربر به یک سرویس‌دهنده وب در یک بازه زمانی کوچک است به‌طوری‌که تعداد درخواست‌های کاربران به سرویس‌دهنده، به‌صورت نمایی افزایش می‌یابد. این در حالی است که سرویس‌دهنده موردنظر در حالت عادی، این تعداد سرویس‌گیرنده نداشته و ممکن است برای آن برنامه‌ریزی نشده باشد که این باعث اختلال در عملکرد سخت‌افزاری و نرم‌افزاری آن خواهد شد [۸]. به همین دلیل است که این پدیده را جز ناهنجاری‌ها ترافیک شبکه دسته‌بندی می‌کنند. رویدادهایی همچون رقابت‌های ورزشی جهانی و بازی‌های المپیک، منتشر شدن نسخه جدید از یک نرم‌افزار محبوب مانند نسخه‌های جدید یک سیستم‌عامل یا وقوع حوادث سیاسی و اجتماعی مانند حملات تروریستی و... نمونه‌هایی از وقایعی هستند که می‌توانند هجوم ناگهانی کاربران را به سایت‌های مرتبط با آن‌ها در پی داشته باشند [۸].

در [۲۸] بیان شده که اگر تعداد درخواست‌های رسیده از کاربران در دقیقه، به‌صورت نمایی رشد کند، هجوم ناگهانی اتفاق افتاده است. این مسئله در رابطه ۱ نشان داده شده است.

$$r_{ti} > 2^i . r_{t0} \qquad (۱)$$

r_{ti} بیانگر میانگین بر دقیقه نرخ درخواست‌ها در بازه زمانی t_i می‌باشد. طبق این رابطه اگر تعداد درخواست‌ها از مقداری مشخص که با توجه به درخواست‌های قبلی هر کارگزار منحصربه‌فرد، متفاوت می‌باشد، بیشتر شود، هجوم ناگهانی کاربران اتفاق افتاده است. البته به‌طورکلی، رشد تعداد درخواست‌های کاربران در یک بازه‌ی زمانی تا حدی که سرویس‌دهنده مجبور باشد برای ادامه سرویس‌دهی خود، عملیات خود را مدیریت و تنظیم کند، هجوم ناگهانی نامیده می‌شود.

۲-۲-۱- تاریخچه‌ی هجوم ناگهانی کاربران

اصطلاح رویداد هجوم ناگهانی کاربران در سال ۱۹۷۰، سال‌ها قبل از ابداع شبکه اینترنت، توسط نویسنده‌ای به نام لاری نیون[1]، در یک رمان داستانی علمی تخیلی به نام پرواز اسب[2]، مورد استفاده قرار گرفت. در داستان این کتاب، دانشمندی ماشین زمانی اختراع می‌کند که افراد به‌وسیله آن می‌توانند به گذشته، زمانی که رویداد خاصی اتفاق افتاده است، سفر کنند. اوج داستان زمانی اتفاق می‌افتد که جمعیت انبوهی برای سفر به زمان رویداد خاصی هجوم می‌آورند و این هجوم ناگهانی باعث می‌شود که تغییراتی در آن رویداد، رخ داده و گذشته تغییر کند که این موضوع باعث بروز ناهنجاری و آشوب‌هایی می‌شود.

سال‌ها بعد و با ظهور شبکه اینترنت این اصطلاح، به دلیل مشابهت فراوان این داستان با هجوم کاربران به یک کارگزار وب که باعث افزایش درخواست‌های رسیده به آن، به‌صورت نمایی می‌شود، وارد دنیای فناوری اطلاعات شد [۸].

---

[1] Larry Niven

[2] The Flight of the Horse

۲-۲-۲- اثر SlashDot

در مورد دلایل وقوع پدیده هجوم ناگهانی کاربران در قسمت‌های قبل صحبت شد. اما یکی دیگـر از دلایلی که ممکن است باعث وقوع این پدیده شود. وجود پیوندی از یک سایت کم بازدید، در یک سایت پربازدید دیگر است. کاربران زیادی که به‌طورمعمول در یک سایت پربازدید حضور دارنـد، ممکـن اسـت متوجه این پیوند شده و یک‌باره برای مشاهده آن، به سایت کم بازدید و گمنام که ممکن است انتظار این تعداد بازدیدکننده را نداشته باشد، هجوم آورند. در این حالت پدیده هجوم ناگهانی کاربران برای سـایت مذکور اتفاق می‌افتد. سایت SlashDot یک سایت خبری در مورد آخرین اخبار تکنولوژی و نرم‌افزار است که بسیاری از لینک‌های خبری آن، به سایت کوچک دیگر ارجاع داده می‌شود. به همین دلیل این پدیده که برای اولین بار در این سایت اتفاق افتاده است، به اثر SlashDot معروف است [۸].

تاکنون دسته‌بندی‌های مختلفی در مـورد انـواع هجـوم ناگهـانی انجـام شـده اسـت. بـرای مثـال، تقسیم‌بندی هجوم ناگهانی به دو نوع قابل پیش‌بینی و غیر قابل پیش‌بینی، عادی و بحرانی، دو نوع از این دسته‌بندی‌ها هستند [۸].

برای مثال، هجوم کاربران در مواقعی مانند وقتی‌که زمان معینی برای انتشار محصولی جدید، مانند نسخه جدید یک سیستم‌عامل، گوشی هوشمند، وصله نرم‌افزاری و ... تعیین شده است، از پیش محتمل است. اما در مواقعی که یک حادثه غیرمنتظره مانند وقوع یک حمله تروریستی و یا حوادثی مانند طوفان و سیل و ... اتفاق می‌افتد، هجوم ناگهانی کاربران قابل پیش‌بینی نیست.

در مواقع قابل پیش‌بینی، با اندیشیدن تمهیداتی می‌توان جلوی از کار افتادن سرویس‌دهنده را گرفت و یا تا حد زیادی از کاهش کارایی آن جلوگیری کرد[۲۹,۳۰] . اما در برخی مواقع، به‌خصوص وقتی‌که این پدیده غیر قابل پیش‌بینی است، هجوم ناگهانی کاربران باعث از کار افتادن سـرویس‌دهنـده مـی‌شـود و هزینه‌های زیادی را در بر دارد، این نوع از هجوم ناگهانی کاربران، بحرانی نامیده می‌شود.

۲-۲-۳- نمونه‌هایی از هجوم ناگهانی کاربران در سال‌های اخیر

در ۲۹ جولای ۲۰۱۵ که تاریخ عرضه سیستم‌عامل ویندوز ۱۰، از سوی شرکت مایکروسافت اعلام شده بود، شماری زیادی از کاربران برای به‌روزرسانی سیستم‌عامل‌های خود به این نسخه، به کارگزارهای این شرکت هجوم آوردند. باوجوداینکه این شرکت این هجوم را پیش‌بینی کرده بود و شبکه‌های توزیع محتوایی[1] با پهنای باند ۴۰ ترابایت در ثانیه برای آن در نظر گرفته بود، اما بازهم تعداد زیادی از کاربران، در ساعات اولیه موفق به به‌روزرسانی سیستم‌عامل خود نشدند. البته این هجوم از قبل پیش‌بینی‌شده بود و بسیاری از سایت‌های خبری دنیا با تیتر "امروز پرترافیک‌ترین روز تاریخ اینترنت خواهد بود" به استقبال آن رفته بودند.

در سال ۲۰۱۲، طوفان "سندی" بخش وسیعی از سواحل شرقی ایالات‌متحده را درنوردید. در پی این حادثه طبیعی، در عرض تنها چند ساعت، استفاده از اینترنت در جهان ۱۱۳درصد افزایش یافت. سایت نتفلیکس[2] با افزایش ناگهانی ۱۵۰ درصدی ترافیک مواجه شد. همچنین استفاده از سرویس‌های اسکایپ[3] ۱۱۲ درصد افزایش یافت. این مورد که در مواجهه با یک رویداد طبیعی رخ داد، یکی از بزرگ‌ترین موارد هجوم ناگهانی کاربران در سال‌های اخیر محسوب می‌شود [۸].

در سال ۲۰۱۰ و در طی برگزاری جام جهانی در آفریقای جنوبی، حجم عظیمی از کاربران به سایت توییتر[4] هجوم آوردند، به‌طوری‌که حجم توییت‌های کاربران در طول یک بازی به ۷۵۰ توییت در ثانیه رسید. البته ماجرا به همین‌جا ختم نشد و با به ثمر رسیدن گل در یک مسابقه، این سایت با ۲۹۴۰

---

[1] Content Distribution Network

[2] Netflix

[3] Skype

[4] Twitter

توییت در ثانیه مواجه شد که باعث از سرویس خارج شدن کل سایت به مدت چندین دقیقه شد که خسارت‌های فراوانی به آن وارد کرد. البته این اتفاق در طول بازی‌های المپیک و بازی‌های زمستانی نیز، بسیار اتفاق می‌افتد. یکی از بزرگ‌ترین و اولین موارد هجوم ناگهانی کاربران، در سال ۱۹۹۸ و در طول بازی‌های نیمه‌نهایی جام جهانی فرانسه اتفاق افتاد که باعث شد سایت اصلی رقابت‌ها برای مدتی ترافیک بسیار سنگینی را شاهد باشد. ترافیک حاصل از این هجوم ناگهانی در دسترس محققین قرار دارد و در این پژوهش نیز از آن استفاده خواهد شد.

در سال ۲۰۱۴ سایت فروش مایکروسافت آفیس، به دلیل هجوم کاربران برای خرید، از سرویس خارج شد، این اتفاق برای سایت اپل که نسخه جدید سیستم‌عامل iOS خود را برای دانلود در اختیار کاربرانش قرار داده بود، در سال ۲۰۱۳ نیز رخ داد [۸].

سایت‌های خبری بزرگ دنیا در حوادثی مانند یازده سپتامبر و همچنین حوادث بمب‌گذاری در لندن در سال ۲۰۰۸ با حجم عظیمی از ترافیک از سوی بازدیدکنندگان خود مواجه شدند [۸].

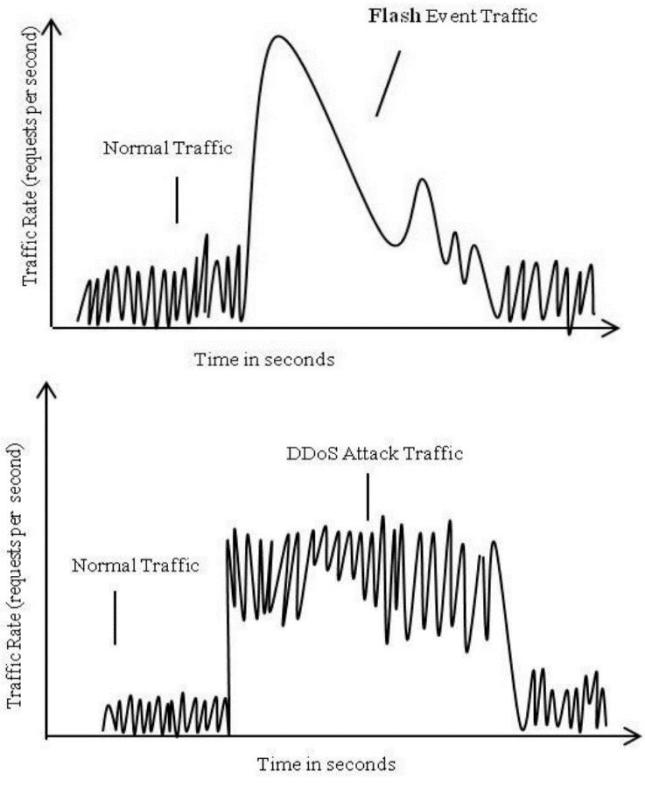
موارد دیگری ازجمله رویدادهایی در سایت‌های خبری که خبر از درگذشت یک شخصیت معروف، یک خبر اقتصادی سیاسی مهم و ... می‌دهند، نمونه‌هایی از هجوم ناگهانی کاربران در سال‌های اخیر بوده‌اند.

از سرویس خارج شدن سرویس‌دهنده‌ی شرکت‌های بزرگ اینترنتی جهان در هنگام هجوم ناگهانی کاربران در سال‌های اخیر نشان می‌دهد که باوجود قابل پیش‌بینی بودن در برخی موارد و اتخاذ تمهیدات مختلف برای مقابله و گذر از این پدیده، هنوز هم این مسئله نیازمند تحقیقات بیشتر و ارائه راهکارهای کارآمدتری برای فائق آمدن بر آن است.

۲-۳- شباهت‌ها و تفاوت‌های هجوم ناگهانی کاربران و حملات منع سرویس

مواردی چون بالا رفتن تعداد درخواست‌ها و افزایش حجم ترافیک به‌صورت ناگهانی، بالا رفتن زمان پاسخ‌دهی و ناپایداری سیستم و درنهایت از دسترس خارج شدن سیستم، ویژگی‌های مشترک بین حمله منع سرویس و هجوم ناگهانی کاربران هستند. اما باید در نظر داشت که حمله منع سرویس توسط منبع مهاجم و با اهداف خرابکارانه صورت می‌گیرد. همچنین باوجود افزایش توانایی‌ها و دانش مهاجمین برای تقلید عملکرد کاربران مجاز، هنوز ازنظر پراکندگی آدرس‌های اینترنتی، تعداد کاربران منحصربه‌فرد، الگوی درخواست‌ها و بسیاری از موارد دیگر، تفاوت‌هایی بین این دو پدیده وجود دارد که از آن‌ها می‌توان برای تشخیص حملات و پیشگیری از آن‌ها استفاده کرد.

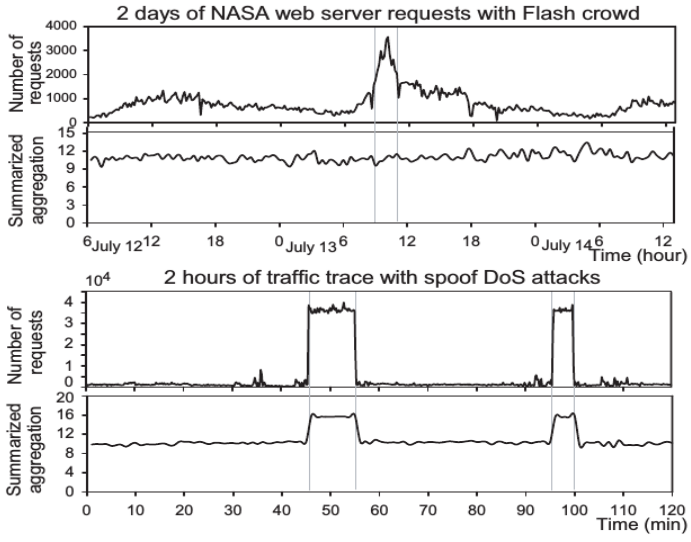
اولین تفاوتی که ازنظر ترافیکی بین این دو پدیده وجود دارد نحوه افزایش و ثبات حجم ترافیک است. در هجوم ناگهانی کاربران، نرخ ترافیک در واحد زمان به‌صورت نوسانی می‌باشد که نمودار آن به‌صورت امواج زیگزاگی مشاهده می‌شوند. درحالی‌که ترافیک حمله منع سرویس پس از رسیدن به میزان مشخصی، معمولاً نرخ ثابتی را در پیش می‌گیرد. دو نمودار شکل ۱ بیانگر این تفاوت هستند [۸, ۲۷].



شکل ۱- نرخ ترافیک در واحد ثانیه برای هجوم ناگهانی کاربران (بالا) و حمله منع سرویس (پایین) [۸]

دلیل این تفاوت، ماهیت دو ترافیک می‌باشد. در هجوم ناگهانی کاربران، پس از اینکه کاربران متوجه افت کیفیت سرویس‌دهی شوند و یا با از کار افتادن‌های متوالی سرویس‌دهنده مواجه شوند، به دو دسته تقسیم می‌شوند، دسته‌ای بر ارسال درخواست‌های خود اصرار می‌ورزند و دسته‌ای نیز دلسرد شده و سعی می‌کنند زمان دیگری را برای دسترسی به خواسته‌های موردنظر خود انتخاب کنند. با خروج این دسته از کاربران، کاربران دیگر وضع بهتری در سرویس‌دهی پیدا می‌کنند و به خواسته‌های خود می‌رسند. البته همان‌طور که گفته شد دلیل هجوم ناگهانی کاربران، رویداد خاصی است که طبیعتاً با گذشت زمان و اطلاع کاربران در مورد آن، حجم درخواست‌ها به‌تدریج کاهش می‌یابد. اما همان‌طور که گفته شد، حمله منع سرویس توسط ربات‌ها حمله و به‌صورت برنامه‌ریزی‌شده و زمان‌بندی‌شده انجام می‌شود. بنابراین حمله در لحظه‌ای خاص آغاز شده و با توجه به هدف آن و مکانیزم‌های دفاعی در مقابل آن، مدت زمان مشخصی به طول می‌انجامد. البته در حملات جدیدتر مهاجمان سعی می‌کنند افزایش نرخ ترافیک به‌صورت ناگهانی نباشد، اما کنترل افت ترافیک در پایان حمله با توجه به مکانیزم‌های دفاعی و همچنین نیاز به هماهنگی و در دسترس بودن ربات‌ها، هنوز مساله ای دشوار برای مهاجمان است.

شکل ۲ نمودار مربوط به تعداد درخواست‌ها و همچنین تعداد آدرس‌های اینترنتی خلاصه‌شده منحصربه‌فرد را برای دو مورد، هجوم ناگهانی کاربران و حمله منع سرویس نشان می‌دهد [۳۱].



شکل ۲- تعداد درخواست‌ها و تعداد آدرس‌های اینترنتی خلاصه‌سازی شده در هجوم ناگهانی کاربران (بالا) و حمله منع سرویس (پایین) [۳۱]

همان‌طور که مشاهده می‌شود در هر دو مورد تعداد درخواست‌ها به‌طور ناگهانی افزایش یافته است، اما آنچه در این بین متفاوت است، تعداد خوشه‌های آدرس خلاصه‌شده می‌باشد. در هجوم ناگهانی کاربران، تعداد خوشه‌های منحصربه‌فرد بعد از خلاصه‌سازی[1]، با روزها و ساعات قبل تفاوتی ندارد و حتی نسبت به بعضی روزها مقدار کمتری نشان می‌دهد. این مطلب نشان‌دهنده این است که فقط تعداد درخواست‌ها نسبت به روزهای مشابه افزایش یافته است. نه تعداد آدرس و خوشه‌های منحصربه‌فرد. اما در مورد حمله منع سرویس، مشخص است که مهاجم از آدرس‌های اینترنتی جعلی[2] استفاده کرده است که به‌صورت یکنواخت و تصادفی تولید شده‌اند. به همین علت هنگام خلاصه‌سازی تعداد خوشه‌های منحصربه‌فرد تقریباً برابر تعداد آدرس‌های موجود است. منظور از خلاصه‌سازی، پیدا کردن بزرگ‌ترین زیر شبکه‌ای[3] است که چند آدرس مختلف روی آن قرار دارند.

مهم‌ترین تفاوت این دو پدیده از منظر سرویس‌دهنده، نحوه مواجهه با آن‌هاست. در هنگام وقوع هجوم ناگهانی، باید تمهیداتی اندیشیده شود تا باوجود افزایش حجم ترافیک و مشکلات ناشی از آن، رضایت کاربران تأمین شود و درخواست‌های آنان پاسخ داده شود. این کار را می‌توان با افزایش قابلیت‌های سخت‌افزاری، استفاده از شبکه‌های محتوا توزیع‌شده و ... انجام داد. اما در مورد حمله منع سرویس، آنچه اهمیت دارد جلوگیری از رسیدن درخواست‌های غیرمجاز و عدم پاسخ به آن‌ها از جانب سرویس‌دهنده است. این کار می‌تواند با استفاده از پازل‌های گرافیکی[۳۲] ، بلوکه کردن آدرس‌های مهاجمین و ربات‌ها در مسیریاب‌های بالادستی، استفاده از تله عسل [۳۳] و ... انجام داد.

---

[1] Summarization

[2] Spoofed

[3] Subnet

در جدول ۱، مقایسه میان حمله منع سرویس و هجوم ناگهانی کاربران به‌صورت تجمیعی آورده شده است:

جدول ۱- مقایسه کلی ویژگی‌های حمله منع سرویس و هجوم ناگهانی کاربران

هجوم ناگهانی کاربران	حمله منع سرویس
سرویس‌دهنده و شبکه با حجم زیادی از ترافیک دریافتی اشباع می‌شوند.	سرویس‌دهنده و شبکه با حجم زیادی از ترافیک دریافتی اشباع می‌شوند.
ترافیک به‌وسیله کاربران مجاز ارسال می‌شود و پاسخ‌دهی به آن ضروری است.	ترافیک به‌وسیله کاربران غیرمجاز ارسال می‌شود و نیازی نیست به آن پاسخ داده شود.
به دو دسته قابل پیش‌بینی و غیرقابل پیش‌بینی تقسیم می‌شود و در پی علاقه کاربران در مورد رویدادی خاص رخ می‌دهد.	غیر قابل پیش‌بینی است و به‌واسطه استفاده مهاجم از سیستم‌های آلوده (زامبی) به ربات تولید حمله رخ می‌دهد.
نرخ ترافیک با توجه به رفتار کاربران نسبت به حجم ترافیک و توانایی سرویس‌دهنده در پاسخ‌دهی به کاربران مختلف ممکن است کاهش یا افزایش یابد.	نرخ ترافیک متأثر از میزان ترافیکی که به سرویس‌دهنده ارسال می‌شود نیست و این نرخ با توجه به برنامه‌ریزی حمله اتفاق می‌افتد.

۲-۴- خودهمانندی[1]

یکی از پارامترهایی که رفتار کاربران مختلف در آن نمو پیدا می‌کند، خودهمانندی یک ترافیک شبکه می‌باشد. به‌طوری کلی خودهمانندی عبارت است از اینکه هر قسمت کوچک، می‌تواند بیانگر مقیاس کوچک‌شده از کل باشد. این اصطلاح برای اولین بار توسط آقای ماندلبورت[2] در سال ۱۹۶۷ استفاده شد.

در گذشته برای مدل کردن ترافیک شبکه از مدل پواسون[3] استفاده می‌شد. اما حدود دو دهه پیش در[۳۴] آقای للاند[4] و همکاران، نشان دادند که ترافیک شبکه از یک فرآیند با وابستگی دوربرد[5] و غیر پواسون پیروی می‌کند. که زمان رسیدن بسته‌های متوالی در آن، یک توزیع دنباله سنگین[6] است.

۳ دلیل برای خودهمانند بودن ترافیک شبکه ذکر شده‌اند که عبارت‌اند از:

۱- زیرساخت‌های شبکه و پروتکل‌ها

در سطوح پایین، تعامل بین پروتکل لایه انتقال و زیرساخت‌های شبکه که باعث بروز رخدادهایی مانند تأخیر، از دست رفتن بسته‌ها، پراکندگی تأخیر و ... می‌شود، باعث می‌شود که ترافیک شبکه در مقیاس‌های زمانی کوچک، شبه خودهمانند شود. منظور از شبه خودهمانندی این است که خودهمانندی فقط در مقیاس‌های زمانی مرتبه پایین وجود دارد[۳۵] .

۲- ماهیت اطلاعات انتقالی در شبکه

---

[1] Self Similarity

[2] Mandelbrot

[3] Poisson

[4] Leland

[5] Long Range Dependence

[6] Heavy Tail

در [۳۶]، آقای کروولا[1] و همکاران نشان داده‌اند که توزیع آماری حجم فایل‌ها در شبکه جهانی وب، مانند تعداد صفحات کتاب‌های موجود در قفسه یک کتابخانه، دنباله سنگین است که این باعث رفتار خودهمانند شبکه اینترنت می‌شود. منظور از دنباله سنگین بودن حجم فایل‌ها این است که باوجود تعداد بسیار زیاد فایل‌های حجم کم، تعدادی فایل با حجم‌های بزرگ هم وجود دارند.

۳- رفتار کاربران و برنامه‌های کاربردی

اگر رفتار کاربران را توالی کارهایی مانند بارگیری[2] و خواندن اطلاعات در نظر بگیریم، این رفتار یک فرآیند دنباله سنگین است که باعث بروز رفتار خود همانند در کل ترافیک شبکه می‌شود. کاربران معمولاً بسته‌های پشت سر هم را به‌طور متوالی ارسال می‌کنند و در توزیع زمانی، زمان‌های غالب، زمان‌های بسیار کوچک هستند، اما در این بین زمان‌های بزرگ نیز نقش بسزایی دارند و باعث دنباله بلند شدن توزیع زمانی می‌شوند.

با توجه به مواردی که ذکر شد، نمی‌توان یکی از سه دلیل فوق را دلیل غالب برای خودهمانندی ترافیک شبکه ذکر کرد، بلکه هریک از آن‌ها در مقیاس‌های زمانی مختلف تأثیر خود را نشان می‌دهند و درمجموع باعث خود همانندی ترافیک شبکه می‌شوند. ویژگی پروتکل‌ها و زیرساخت شبکه تأثیر خود را اغلب در مقیاس بازه‌های زمانی بالای ۱۰۰ میلی‌ثانیه، حجم فایل‌های انتقالی در مقیاس بازه‌های بین ۱۰ میلی‌ثانیه و ۱۰۰ میلی‌ثانیه و رفتار کاربران در مقیاس‌های زیر ۱۰ ثانیه بر خود همانندی ترافیک تأثیرگذار هستند.

---

[1] Crovella

[2] Download

به بیان صوری، اگر نمودار $F(X)$ در مقیاس‌ها مختلف، تحت تبدیل‌های $x_1=bx$ و $y_1=ay$ خودهمانند باشد، آنگاه:

$$F(bx)=aF(x)=b^{H}F(x)$$

به‌طوری‌که در آن $H=\log(a)/\log(b)$، پارامتر Hurst یا ضریب خودهمانندی نامیده می‌شود.

برای مقادیر $0.5<H<1$ نمودار $F(x)$ دارای پیوستگی دوربرد یا خودهمانند نامیده می‌شود.

۲-۴-۱- فاصله اطلاعاتی[1]

فاصله اطلاعاتی که توسعه‌یافته میزان پیچیدگی کولموگروف[2] می‌باشد، نشان‌دهنده فاصله میان دو شی[3] محدود است به‌طوری‌که این فاصله کمترین میزان اطلاعات مورد نیاز برای رسیدن از یک شی به شی ای دیگر را نشان می‌دهد. این دو شی می‌توان دو فایل مختلف، دو نمونه داده و ... باشند.

$$ID(x,y) = \min\{|p|: p(x) = y \,\&\, p(y) = x\} \qquad (۲)$$

در نظریه آماری و نظریه اطلاعات، فاصله اطلاعاتی، میزان شباهت دو شی آماری را نشان می‌دهد. این اشیا می‌توانند دو متغیر تصادفی، دو توزیع مختلف و یا دو نمونه آماری باشند. چند نمونه از فاصله‌های آماری که معمولاً نسبت به بقیه دقیق‌تر عمل کرده و بیشتر مورد استفاده قرار می‌گیرند، عبارت‌اند از:

---

[1] Information Distance

[2] Kolmogorov Complexity

[3] Object

۱- فاصله‌ی Kullback-Leibler

این فاصله اطلاعاتی که واگرایی اطلاعات[1] و آنتروپی نسبی[2] نیز نامیده می‌شود، میزان شباهت و تفاوت دو متغیر تصادفی را نشان می‌دهد. این فاصله نامتقارن می‌باشد و مقادیر D(p,q) و D(q,p) در آن با یکدیگر برابر نمی‌باشند.

$$D_{KL}(p,\mathrm{q}) = \sum_{x \in X} p(x) log \frac{p(x)}{q(x)} \qquad (۳)$$

۲- فاصله‌ی Jeffrey

برای متقارن کردن فاصله Kullback-Leibler، فاصله اطلاعاتی Jeffrey معرفی شده است. البته ازآنجایی‌که میانگین دو مقدار در آن محاسبه‌شده است این فاصله اطلاعاتی، دقیق عمل نمی‌کند.

$$D_J = (p,q) = \frac{1}{2}[D_{KL}(p,q) + D_{KL}(q,p)] \qquad (۴)$$

۳- فاصله‌ی Simpson

[1] Information Divergence

[2] Relative Entropy

یک روش دیگر برای متقارن کردن فاصله Kullback-Leibler، فاصله اطلاعاتی Simpson می‌باشد که به‌نوعی توسعه‌یافته روش Jeffrey می‌باشد. در این روش سعی شده است دقت این فاصله اطلاعاتی افزایش یابد.

$$D_s(p,q) = \frac{1}{2}\{D_{KL}\left[p, \frac{1}{2}(p+q)\right] + D_{KL}\left[q, \frac{1}{2}(p+q)\right]\} \qquad (۵)$$

۴- فاصله‌ی Battacharyya

این فاصله اطلاعاتی میزان شباهت دو متغیر تصادفی را محاسبه می‌کند و به دلیل دقت زیاد، کاربرد زیادی در علم آمار و اطلاعات دارد. این فاصله برگرفته از ضریب Battacharyya (۶) می‌باشد.

$$\mathrm{BC(p,q)} = \sum_{x \in X} \sqrt{p(x).q(x)}, \qquad 0 < \mathrm{BC} < 1 \qquad (۶)$$

ضریب Bhattacharya بیشتر میزان هم‌پوشانی بین دو متغیر تصادفی را نشان می‌دهد، اما معیار فاصله Bhattacharya (۷) که به‌نوعی با استفاده از همین ضریب قابل محاسبه است، برای اندازه‌گیری میزان شباهت و یا فاصله دو متغیر تصادفی به کار می‌رود، به همین دلیل می‌تواند دید دقیق‌تری نسبت به ضریب Bhattacharya در مورد شباهت دو متغیر تصادفی بدهد.

$$d = -\ln BC(p,q), \qquad 0 < d < \infty \qquad (۷)$$

مقدار به‌دست‌آمده برای ضریب شباهت Bhattacharya بین صفر و یک می‌باشد که یک نشان‌دهنده شباهت کامل و صفر نشان‌دهنده عدم شباهت می‌باشد. اما در مورد فاصله Bhattacharya، مقدار به‌دست‌آمده بین صفر و بی‌نهایت می‌باشد. که فاصله زیاد نشان‌دهنده عدم شباهت و فاصله صفر نشان‌دهنده شباهت کامل دو متغیر تصادفی می‌باشد.

۵- فاصله Hellinger

این فاصله برگرفته از فاصله Battacharyya می‌باشد و به‌نوعی شکل تغییریافته آن به‌حساب می‌آید.

$$D_H(p,q) = [\sum_{x\in X}(\sqrt{p(x)} - \sqrt{q(x)})^2]^{\frac{1}{2}} \qquad (۸)$$

۶- فاصله Total Variation

این فاصله که از نوع فواصل مرتبه اول می‌باشد، میزان تفاوت دو متغیر تصادفی را نشان می‌دهد. به‌طوری‌که هرچه عدد به‌دست‌آمده توسط این رابطه بیشتر باشد، نشان‌دهنده تفاوت بیشتر دو متغیر تصادفی می‌باشد.

$$T(P,Q) = \sum_{i=1}^{n} |p_i - q_i| \qquad (۹)$$

۲-۴-۲- معیار احتمال[1]

یک فاصله اطلاعاتی (d)، معیار احتمال نامیده می‌شود اگر سه شرط زیر برای آن برقرار باشد:

فضای نمونه: Ω $\quad d: \Omega \longrightarrow R_+$

همانی $\quad 1)\ d(X,Y) \geq 0\ and\ d(X,Y) = 0 \Leftrightarrow P(X,Y) = 1 \quad \forall X, Y \in \Omega$

تقارن $\quad 2)\ d(X,Y) = d(X,Y)\ \ \forall X, Y\ \in \Omega$

نامساوی مثلث $\quad 3)\ d(X,Y) \leq d(X,Z) + d(Z,Y) \quad \forall X, Y, Z \in \Omega$

در بین فاصله‌های ذکرشده، تنها فاصله‌های Battacharyya و Total Variation ویژگی‌های معیار احتمال را دارند.

۲-۵- کارهای پیشین انجام‌شده

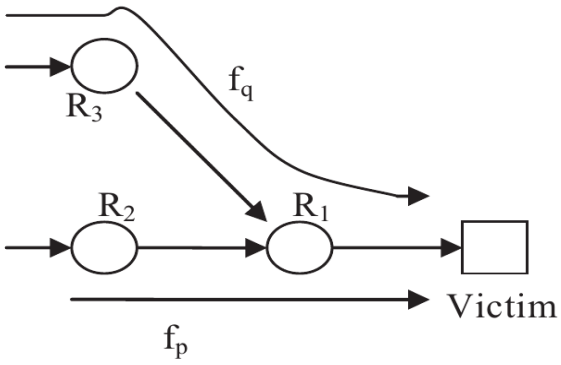
برای تشخیص حملات منع سرویس، روش‌های بسیاری ارائه شده که در فصل قبل به آن‌ها اشاره شد. اما مسئله مورد اهمیت این است که این روش‌ها برای تشخیص حملات منع سرویس از ترافیک عادی معرفی شده‌اند و با توجه به ویژگی‌هایی که برای ترافیک هجوم ناگهانی کاربران و شباهت آن با ترافیک حمله منع سرویس بیان شد، ممکن است این روش‌ها برای تشخیص این دو از هم مناسب نباشند. البته خود ارائه‌دهندگان این راهکارها نیز هدفی برای تشخیص و تمایز ترافیک حمله منع سرویس و هجوم ناگهانی کاربران نداشته‌اند. در ادامه به بررسی روش‌هایی می‌پردازیم که منحصراً برای تشخیص ترافیک

[1] Probability Metric

حمله منع سرویس از هجوم ناگهانی کاربران ارائه شده‌اند و مزایا و معایب هرکدام از آن‌ها را بیان خواهیم نمود.

از میان روش‌های موجود، چند روش وجود دارند که توسط آقای وانلی[1] و همکاران ارائه شده‌اند. این تیم فعالیت گسترده‌ای در زمینه حملات منع سرویس داشته‌اند.

۲-۵-۱- تشخیص حملات منع سرویسی که رفتار کاربران در هجوم ناگهانی را تقلید می‌کنند با استفاده از نظریه اطلاعات



شکل ۳ - نمای یک شبکه ساده، متشکل از ۳ مسیریاب و یک سرویس‌دهنده [۳۷]

این روش [۳۷] برای تفکیک دو ترافیک از محاسبه فاصله آماری (بی‌نظمی نسبی) دو جریان استفاده می‌کند. در این روش فرض شده که دو جریان ترافیکی مختلف مطابق با شکل ۳ از طریق مسیریاب‌های R3 و R2، وارد مسیریاب R1 می‌شوند.

[1] Waneli

در مسیریاب R_1، هنگامی‌که حجم ترافیک شروع به افزایش می‌کند و یا رفتار مشکوکی مشاهده می‌شود، نمونه‌برداری از دو جریان آغاز می‌شود و توزیع تعداد بسته‌های موجود در هر جریان در یک بازه زمانی مشخص محاسبه می‌شود. توزیع جریان f_q با $Q(x)$ و جریان f_p با $P(x)$ نشان داده شده است (روابط ۱۰ و ۱۱). متغیر تصادفی X را چنانکه گفته شد، برابر تعداد بسته‌های رسیده در بازه زمانی مشخص در نظر گرفته شده است. مقدار n (اندازه نمونه‌ها) باید به‌گونه‌ای انتخاب شود که این روش حداکثر کارایی را داشته باشد. یعنی نه آن‌قدر کوچک که هشدارهای منفی نادرست[1] (اعلان عدم حمله درحالی‌که حمله صورت گرفته است) و هشدارهای مثبت نادرست[2] سیستم (اعلان حمله درحالی‌که حمله‌ای صورت نگرفته است) افزایش یابد و نه آن‌قدر بزرگ که تشخیص حمله موقعی رخ دهد که برای مقابله با آن زمانی باقی نمانده باشد.

$$P(X) = p(x_1, x_2, x_3, \dots, x_n) \qquad (۱۰)$$

$$p(x^i) = x_k^i . (\sum_{k=1}^{n} x_k^i)^{-1} \qquad (۱۱)$$

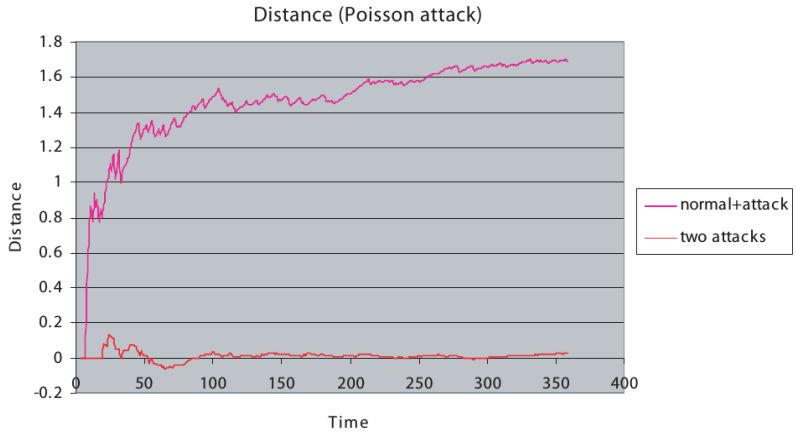
سپس فاصله بین توزیع دو جریان، با استفاده از فرمول فاصله Kullback-Leibler (۳) محاسبه شده است.

هرچقدر دو جریان مشابه یکدیگر باشند، مقدار فاصله بین آن‌ها کمتر خواهد بود. برای مقادیر کمتر از یک مقدار آستانه مشخص‌شده، دو جریان کاملاً مشابه در نظر گرفته می‌شوند. این مطلب بیانگر این

[1] False Negative Alarm

[2] False Positive Alam

است که هر دو جریان توسط یک روبات و به‌صورت خودکار تولید شده‌اند. البته برای تشخیص از نتایج چندین نمونه و مقایسه آن‌ها استفاده شده است. هر دو ترافیکی که این روش بر روی آن‌ها بررسی شده، توسط نرم‌افزار تولید شده‌اند. برای ترافیک حمله از ترافیکی که با توزیع پواسون[1] تولید شده، استفاده شده است. شکل ۴ نمودار حاصل از اعمال این روش بر ترافیک‌های یادشده نشان می‌دهد.



شکل ۴ - فاصله Kullback-Leibler بین دو ترافیک حمله و دو ترافیک حمله و عادی [۳۷]

ازآنجایی‌که این روش، از دو ترافیک ساختگی استفاده کرده است، مطابق شکل ۴، فاصله بین ترافیک حمله بسیار کم و فاصله بین دو ترافیک حمله و ترافیک عادی، بسیار زیاد می‌باشد. بعلاوه فرض این روش بر این بوده که دو ترافیک به‌صورت دو جریان مجزا به مسیریاب‌ها می‌رسند و قابل تفکیک می‌باشند. درصورتی‌که در واقعیت ممکن است چنین اتفاقی نیفتد. همچنین میزان آستانه فاصله‌ای که برای تشخیص در نظر گرفته شده است، به‌صورت تجربی و با توجه به ترافیک‌های مذکور به دست آمده است

[1] Poisson

که قابل اتکا نمی‌باشد و فقط می‌توان به‌صورت نسبی به این نتیجه رسید که میزان فاصله بین دو ترافیک حمله کمتر از فاصله دو ترافیک حمله و هجوم ناگهانی کاربران می‌باشد.

۲-۵-۲- تشخیص حملات منع سرویس توزیع‌شده از هجوم ناگهانی کاربران با استفاده از فاصله اطلاعاتی

در این روش، به‌نوعی از ترکیب ایده قبلی با یک روش جدیدتر استفاده شده است. ایده مطرح‌شده در [۵] مقایسه یکی از دو روش زیر و استفاده از بهترین آن‌ها می‌باشد:

۱- اندازه‌گیری بر اساس نظریه اطلاعات[1]

۲- اندازه‌گیری بر اساس میزان وابستگی[2]

تفاوتی که در این روش وجود دارد این است که پژوهشگران به این نتیجه رسیده‌اند که محاسبه فاصله دو جریان در مسیریاب R_1 شکل ۳ منطقی نمی‌باشد. بنابراین باید این فواصل در مسیریاب‌های بالادستی محاسبه شوند و در صورت تشخیص حمله، بتوان لایه‌های دفاعی را دورتر از کارگزار هدف مهاجم تشکیل داد. به همین منظور در این روش تصمیم گرفته شده که مسیریاب‌های R_3 و R_2 خود کار نمونه‌برداری و محاسبه توزیع جریان را انجام دهند. سپس مقادیر به‌دست‌آمده توسط یک مسیر جداگانه بین دو مسیریاب جابجا می‌شود و با محاسبه فاصله بین دو جریان در هر یک از مسیریاب‌ها، در مورد آن جریان تصمیم‌گیری می‌شود. مشکلی که بر سر راه این روش وجود دارد این است که فرمول Kullback-Leibler متقارن نمی‌باشد. یعنی مقدار $D(P,Q)$ با مقدار $D(Q,P)$ برابر نیست. بنابراین مقادیر

[1] Information Theory

[2] Affinity

به‌دست‌آمده در دو مسیریاب با یکدیگر برابر نخواهند بود. برای حل این مشکل از معیارهای فاصله متقارن Simpson، Jeffrey و Hellinger که در فصل قبل معرفی شدند، استفاده شده است.

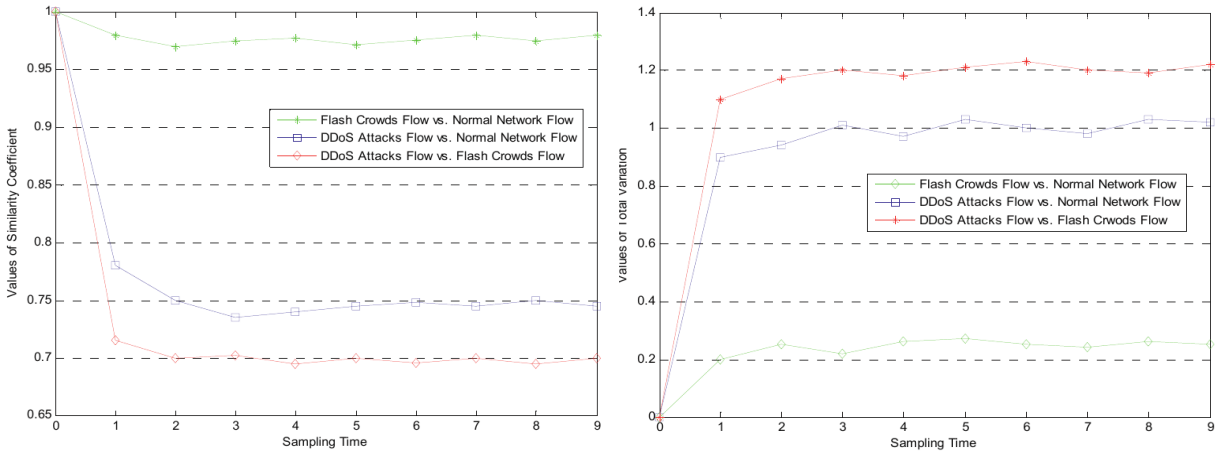
بر اساس بررسی‌های انجام‌شده در [۵] مشخص می‌شود که فرمول فاصله Sibson در بین ۳ مورد ذکرشده، دقیق‌تر می‌باشد. در ادامه با اعمال این فرمول بر روی داده‌های ترافیکی واقعی حمله منع سرویس توزیع‌شده و هجوم ناگهانی کاربران، روش ذکرشده قادر بوده است تا این دو مورد را با دقت ۶۵٪ از یکدیگر تشخیص دهد. البته این مقدار دقت با توجه به اینکه ترافیک مورد استفاده نوعی ساده از حمله منع سرویس می‌باشد، بسیار کم به نظر می‌رسد.

۲-۵-۳- تشخیص حملات منع سرویس توزیع‌شده از هجوم ناگهانی کاربران با استفاده از معیارهای احتمال

این روش [۶] نیز بر اساس معیارهای احتمالی کار می‌کند و بر اساس همان روش‌های پیشین می‌باشد، طبق ادعای ارائه‌دهندگان این روش علاوه بر اینکه می‌تواند حملات منع سرویس را از هجوم ناگهانی کاربران تشخیص دهد، بلکه در حالت کلی می‌تواند هر نوع ناهنجاری را از ترافیک عادی تشخیص دهد. این روش ترکیبی از فرمول میزان وابستگی Battacharyya (۶) و هم‌چنین رابطه میزان تفاوت (۹) می‌باشد.

سیستم تشخیص طراحی‌شده در این روش شامل ۵ بخش می‌باشد که عبارت‌اند از: ۱- کشف ناهنجاری ۲- تخمین زننده توزیع جریان ۳- محاسبه معیار احتمال ترکیبی ۵- بخش تصمیم‌گیری

برای ارزیابی دو معیار ارائه‌شده از سه ترافیک واقعی موجود که شامل ۱- ترافیک حمله منع سرویس ۲- ترافیک هجوم ناگهانی کاربران و ۳- ترافیک عادی استفاده شده است. نمودار حاصل از فرمول‌های فوق بر روی داده‌های موردنظر در شکل ۵ آورده شده است.



شکل ۵- میزان تفاوت کل بین ترافیک‌های مختلف (سمت راست) و میزان شباهت Bhattacharya بین ترافیک‌های مختلف (سمت چپ) [۶]

با توجه به این نمودارها مشخص می‌شود که ادعای قابلیت این روش در تشخیص انواع ترافیک از هم، درست به نظر می‌آید.

۲-۵-۴- تشخیص حملات منع سرویس توزیع‌شده از هجوم ناگهانی کاربران با استفاده از الگوی زمان بین رسیدن بسته‌های متوالی

این روش ترافیک شبکه را به دو دسته قابل پیش‌بینی و غیر قابل پیش‌بینی تقسیم می‌کند [۴]. همان‌طور که قبلاً اشاره شد، ترافیکی که توسط مهاجمین تولید می‌شود، به‌وسیله نرم‌افزارهای خودکار و نیمه‌خودکار تولید می‌شود. بنابراین این ترافیک یا به‌طورکلی قابل پیش‌بینی و طبق اصول و نظم خاصی تولید می‌شود و یا به‌طورکلی تصادفی و بی‌قاعده می‌باشد. در هر دو صورت این ترافیک با ترافیک تولیدشده توسط انبوه کاربران که بر اساس رفتاری انسانی تولید شده‌اند، متفاوت می‌باشد. بر این اساس، روش زیر ارائه شده است تا بتواند ترافیک تولیدشده توسط مهاجم در حملات منع سرویس را از ترافیک سالم کاربران مجاز شبکه تشخیص دهد.

در این روش ترافیک قابل پیش‌بینی به ۳ دسته تقسیم شده است:

۱- ترافیک با نرخ ثابت

۲- ترافیک با نرخ افزایشی

۳- ترافیک با نرخ متناوب

میزان قابل پیش‌بینی بودن یک ترافیک در این روش با استفاده از محاسبه ضریب همبستگی پیرسون[1] به دست می‌آید.

در این مقاله مقدار ضریب همبستگی در دو حالت محاسبه شده است:

۱- همبستگی بین نرخ جریان دریافتی با زمان

۲- همبستگی بین جریان دریافتی و خود آن جریان

مقدار ضریب همبستگی پیرسون برای دو متغیر تصادفی X,Y ، مطابق رابطه (۱۲) محاسبه می‌شود:

$$r = \frac{\sum_i (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_i (x_i - \bar{x})^2}\sqrt{\sum_i (y_i - \bar{y})^2}} \qquad (۱۲)$$

مقدار به‌دست‌آمده توسط این رابطه عددی بین ۱ و ۱- می‌باشد. مقادیر مرزی به معنای همبستگی قوی بین دو متغیر می‌باشند که به آن همبستگی خطی نیز گفته می‌شود. پس مقادیری که در این روش برای کشف ترافیک قابل پیش‌بینی مورد نیاز هستند، این دو عدد هستند. البته همان‌طور که گفته شد، ترافیک تولید شده توسط نرم‌افزار خودکار یا به‌شدت قابل پیش‌بینی هستند و یا به حد زیادی تصادفی

[1] Pearson Correlation Coefficient

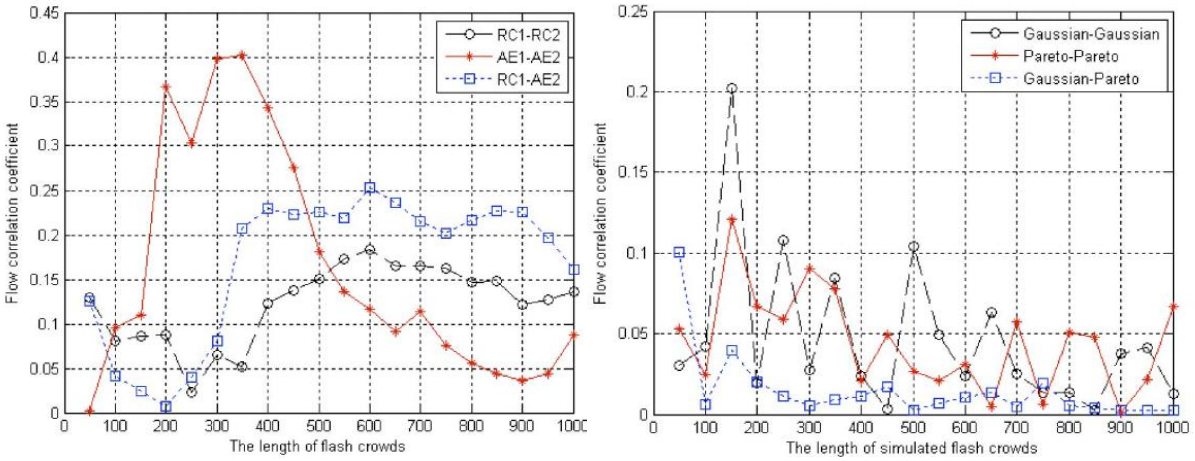
تولید می‌شوند. در این صورت مقدار ضریب همبستگی پیرسون عددی بسیار نزدیک به صفر بـه دسـت خواهد آمد. بنابراین اگر قدر مطلق مقدار به‌دست‌آمده را در نظر بگیریم، مقادیر نزدیک به یک و مقـادیر نزدیک به صفر، بیانگر ترافیک تولیدشده توسط نرم‌افزار خودکار و یا به عبارتی، ترافیک حمله می‌باشند. البته اینکه میزان فاصله آستانه از این دو عدد چه مقدار باشد تا بتوان در مورد آن تصمیم‌گیری کرد نیز در مقاله مورد بررسی قرار گرفته و مقادیر تجربی برای آن محاسبه شده است. در رابطه بـا حالـت‌هـای محاسبه ضریب همبستگی نیز باید گفت که در حالت اول که این مقدار بـین جریـان ترافیـک و زمـان محاسبه می‌شود، در حقیقت مقدار به‌دست‌آمده بیانگر این است که با گذر زمان، نرخ ترافیک چه تغییری می‌کند. در مورد حالت دوم نیز همبستگی بین جریان دریافتی با خود آن جریان محاسبه می‌شود. برای مثال، اگر نرخ‌ها را در بازه‌های زمانی مختلف شماره‌گذاری کنیم، می‌توان همبستگی بین نرخ‌های با نمایه فرد و نرخ‌های با نمایه زوج را به دست آورد. البته همان‌طور که انتظار می‌رود حالت اول کارایی بهتـری نسبت به حالت دوم دارد و طبق بررسی‌های انجام‌شده، با استفاده از حالت اول، می‌توان حمله را در زمان کمتری (۱.۷ثانیه) نسبت به حالت دوم (۲.۴ ثانیه) تشخیص داد. این روش برای اولین بار در سطح کاربران عمل کرده و ویژگی‌های کلی یک ترافیک را مورد بررسی قرار داده است. ترافیک حمله استفاده شده در این روش، تعداد بسیار محدودی حمله‌کننده دارد و بنابراین فرض قابل پیش‌بینی بودن در مـورد آن بـا توجه با ساختار ساده حمله درست به نظر می‌رسد. اما در حملات گسترده، مهاجم مـی‌توانـد بـا ایجـاد بسته‌های تصادفی، قابل پیش‌بینی بودن ترافیک را از بین ببرد که این باعث خطا در تشخیص خواهد شد.

۲-۵-۵- تشخیص حملات منع سرویس توزیع‌شده از هجوم ناگهانی کاربران با استفاده از ضریب همبستگی جریان

در این روش فرض بر این گرفته شده که جریان‌های مختلف از مسیریاب‌هـای مختلـف بـه قربـانی می‌رسند و جریان‌های حمله همبستگی بیشتری با یکدیگر دارند [۳۸]. بر همین اساس مانند روش‌هـای قبل، نمونه‌برداری از تعداد بسته‌های رسیده جریان‌های مختلف در بازه‌های زمانی متفاوت انجام می‌شود و

بر اساس آن، میزان ضریب همبستگی دو جریان با یکدیگر، با استفاده از ضریب همبستگی پیرسون (رابطه ۱۲) محاسبه می‌شود.

شکل ۶ تفاوت میزان همبستگی چند جریان هجوم ناگهانی با چند جریان حمله منع سرویس را نشان می‌دهد. همان‌طور که مشخص است این میزان در ترافیک‌های ساختگی که به‌عنوان ترافیک حمله در نظر گرفته شده‌اند، بالا می‌باشد.



شکل ۶- ضریب همبستگی (پیرسون) بین ۳ ترافیک شبیه سازی شده (سمت چپ) و ضریب همبستگی (پیرسون) بین ۳ ترافیک هجوم ناگهانی (سمت راست) [۳۸]

بااین‌وجود، در این روش هم فرضیاتی در نظر گرفته شده که ممکن است در دنیای واقعی درست نباشند. برای مثال جریان‌های مختلف در دنیای واقعی، مجزا از یکدیگر نیستند. بعلاوه این روش توانایی تشخیص حمله در حین هجوم ناگهانی کاربران را ندارد و بر اساس یک مقدار آستانه که به‌صورت تجربی به‌دست آمده است، عمل می‌کند.

۲-۵-۶- تشخیص حملات سیل‌آسا از هجوم ناگهانی کاربران، بر اساس الگوهای ترافیکی و با استفاده از روش‌های کشف آنتروپی

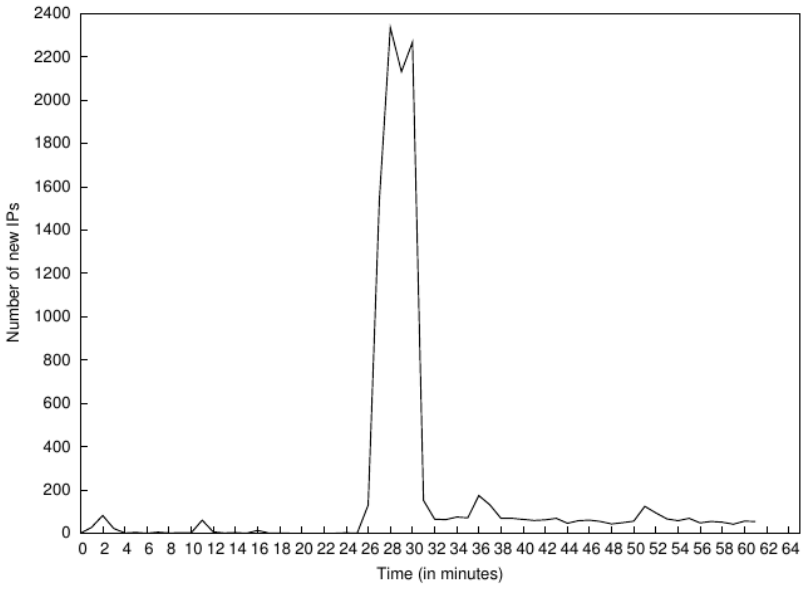
در این روش [۳۹] که از ایده‌ی بررسی تغییرات میزان آنتروپی، ارائه‌شده در [۴۰] استفاده کرده است، ابتدا بر اساس داده‌ی ترافیکی، همبندی شبکه ساخته می‌شود. سپس با استفاده از الگوریتم کوتاه‌ترین مسیر، مسیری که گره‌های مختلف با استفاده از آن بسته‌های خود را به سرویس‌دهنده ارسال می‌کنند، انتخاب می‌شود. ابتدا برای هر کاربر میزان آنتروپی اولیه با استفاده از رابطه ۱۳ محاسبه می‌شود.

$$E = -[\left(\frac{n}{N}\right)\ln(\frac{n}{N})] \qquad (۱۳)$$

در این رابطه، N نشان‌دهنده میزان ترافیک یک گره و n بیانگر مجموع ترافیک دریافتی از کل گره‌های موجود در شبکه می‌باشد. سپس، به تعدادی از گره‌ها، امکان حمله منع سرویس افزوده می‌شود و این گره‌ها شروع به ارسال ترافیک حمله می‌کنند. در این مرحله مقدار آنتروپی ثانویه گره‌ها محاسبه می‌شود و گره‌هایی که میزان آنتروپی در آن‌ها، بیشتر از مقدار آستانه‌ی مشخص‌شده (۰.۱)، تغییر کرده باشد، به‌عنوان گره مشکوک در نظر گرفته می‌شوند. سپس برای هر جفت گره مشکوک، میزان ضریب همبستگی پیرسون با استفاده از رابطه ۱۸ محاسبه‌شده و گره‌هایی که میزان همبستگی آن‌ها با یکدیگر بیشتر از یک مقدار آستانه (۰.۶ در نظر گرفته شده است) باشد، به‌عنوان حمله‌کننده در نظر گرفته می‌شوند. این روش از یک ترافیک عادی برای تشکیل همبندی شبکه استفاده کرده و سپس ترافیک حمله ساختگی به برخی از گره‌های آن افزوده شده است. همچنین، فرض کلی این روش مبنی بر اینکه ابتدا گره‌ها ترافیک سالمی ارسال می‌کنند و سپس برخی از همین گره‌ها به حمله‌کننده تبدیل می‌شوند، منطقی به نظر نمی‌رسد.

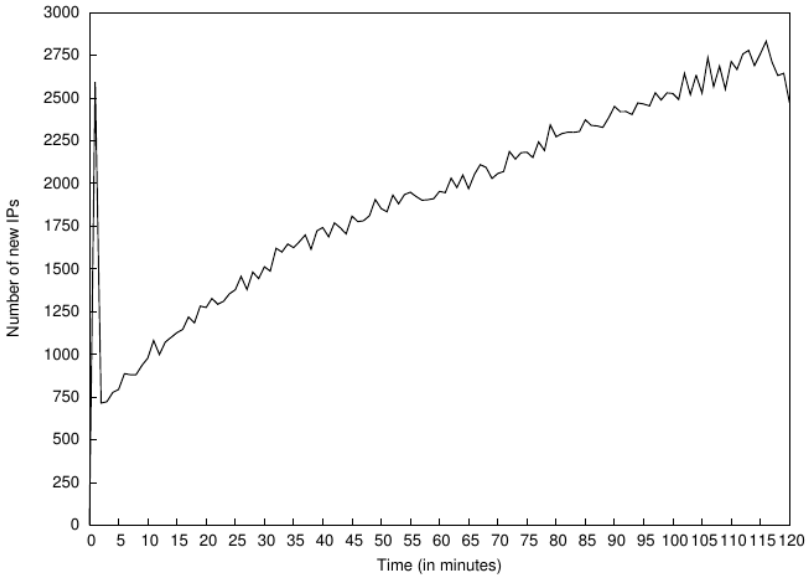
۲-۵-۷- بررسی نرخ ظهور آدرس‌های جدید در ترافیک حمله و هجوم ناگهانی کاربران

در [۲۷] ظهور آدرس‌های جدید در دو ترافیک هجوم ناگهانی و حمله منع سرویس، مورد بررسی قرار گرفته است. همان‌طور که در شکل ۷ مشخص است، تا دقیقه ۲۶ حمله منع سرویس، نرخ ظهور آدرس‌های جدید، بسیار پایین بود و در این مدت، تنها حدود ۱۸۰ کاربر منحصربه‌فرد به سرویس‌دهنده درخواست ارسال می‌کند. اما از دقیقه ۲۶ ام به بعد نرخ ظهور آدرس‌های جدید به‌شدت افزایش می‌یابد و این نشان‌دهنده‌ی این است که حمله اصلی از دقیقه ۲۶ ام به بعد آغاز شده است.



شکل ۷- نرخ ظهور آدرس‌های جدید در حمله منع سرویس CAIDA [۲۷]

شکل ۸، ظهور کاربران نرخ ظهور کاربران جدید در ترافیک هجوم ناگهانی کاربران را نشان می‌دهد. در دقایق ابتدایی هجوم ناگهانی، نرخ ظهور کاربران جدید به‌طور ناگهانی بالا می‌رود، اما پس از آن این نرخ به‌صورت تدریجی افزایش می‌یابد. این مسئله نشان‌دهنده‌ی این است که ابتدا تعداد زیادی کاربر قصد دسترسی در همان ابتدا را دارند.



شکل ۸- نرخ ظهور آدرس‌های جدید در هجوم ناگهانی کاربران به سایت جام جهانی ۹۸ فرانسه [۲۷]

مقایسه شکل‌های ۷ و ۸ نشان می‌دهد که نرخ ظهور یک آدرس جدید در یک رویداد حمله یا منع سرویس نیز می‌تواند معیاری برای تشخیص دو ترافیک مختلف باشد. البته در [۲۷] فقط این تفاوت بیان شده است و روشی مدون برای تشخیص ارائه نشده است.

جدول ۲- مقایسه کلی روش‌های موجود برای تشخیص حملات منع سرویس از هجوم ناگهانی کاربران

ردیف	عنوان روش	شرح	مزایا و معایب	مرجع
۱	تشخیص حملاتی که رفتار کاربران در هجوم ناگهانی را تقلید می‌کنند، با استفاده از نظریه اطلاعات	در این روش با استفاده از فاصله اطلاعاتی Kullback-Leibler، فاصله بین نمونه‌های دو جریان از یکدیگر محاسبه می‌شود. اگر دو جریان حمله باشند، فاصله آن‌ها از یکدیگر بسیار کم خواهد بود و اگر دو جریان مختلف حمله و هجوم ناگهانی باشند، فاصله آن‌ها از یکدیگر زیاد خواهد بود.	جزو اولین روش‌هایی است که بر اساس اندازه‌گیری فاصله جریان‌ها عمل می‌کند. بر روی دو ترافیک ساختگی به‌خوبی عمل می‌کند و می‌تواند آن‌ها را از هم تشخیص دهد. فقط می‌تواند دو ترافیک را درصورتی‌که جدا از هم باشند، تشخیص دهد. از یک فاصله اطلاعاتی نامتقارن استفاده می‌کند. روش فقط بر روی دو ترافیک ساختگی آزمایش‌شده و نتایج آن قابل استناد نمی‌باشد.	[۳۷]
۲	تشخیص حملات منع سرویس توزیع‌شده از هجوم ناگهانی کاربران با استفاده از فاصله اطلاعاتی	در این روش ۳ روش اطلاعاتی مختلف مورد بررسی قرار گرفته است و درنهایت فاصله‌ی نمونه‌های دو جریان با استفاده از معیار فاصله Simpson، محاسبه شده است. اگر فاصله‌های دو جریان از یکدیگر زیاد باشد، دو جریان مختلف و اگر فاصله‌ها از هم کم باشد، دو جریان مشابه و حمله هستند.	از فاصله اطلاعاتی متقارن استفاده می‌کند. فقط می‌تواند دو ترافیک را درصورتی‌که جدا از هم باشند، تشخیص دهد. از شکل متقارن شده یک فاصله اطلاعاتی نامتقارن استفاده می‌کند. دقت روش پایین می‌باشد.	[۵]
۳	تشخیص حملات منع سرویس توزیع‌شده از هجوم ناگهانی کاربران با استفاده از معیارهای احتمال	در این روش از ترکیب دو معیار فاصله Bhattacharya و Total Variation استفاده شده است. مقادیر آستانه برای هریک از فواصل تعریف شده مشخص شده است که به توجه به آن‌ها، نوع دو ترافیک را مشخص می‌کند. این مقادیر آستانه حتی توانایی تشخیص ترافیک حالت عادی و هجوم ناگهانی کاربران را نیز دارند.	از ترکیب دو فاصله اطلاعاتی مختلف استفاده می‌کند. توانایی تشخیص ترافیک‌های مختلف از یکدیگر را دارد (حتی ترافیک عادی از هجوم ناگهانی کاربران) از فواصل اطلاعاتی متغیر و معیار استفاده می‌کند. فقط می‌تواند دو ترافیک را درصورتی‌که جدا از هم باشند، تشخیص دهد. از یک فاصله اطلاعاتی مرتبه اول استفاده می کند.	[۶]

			مقادیر آستانه بسیار به هم نزدیک و به صورت تجربی محاسبه شده-اند. حمله منع سرویس استفاده شده بسیار ابتدایی می باشد.	
۴	تشخیص حملات منع سرویس توزیع شده از هجوم ناگهانی کاربران با استفاده از الگوی زمان رسیدن بین بسته‌های متوالی	در این روش ترافیک حمله به ۳ نوع نرخ افزایشی، نرخ ثابت و نرخ متناوب تقسیم شده است و با تشخیص نوع ترافیک با استفاده از محاسبه همبستگی ترافیک با زمان، حمله یا سالم بودن آن مشخص می‌شود. اگر ترافیک قابل پیش‌بینی نباشد، سالم در نظر گرفته می‌شود.	توانایی تشخیص جریان کاربران مختلف از یکدیگر را دارد. زمان تشخیص آن سریع می‌باشد. بر روی ترافیک حمله ساده آزمایش شده است. مقادیر آستانه به‌صورت تجربی به‌دست‌آمده‌اند.	[۴]
۵	تشخیص حملات منع سرویس توزیع شده از هجوم ناگهانی کاربران با استفاده از ضریب همبستگی جریان	در این روش میزان همبستگی دو جریان مختلف با یکدیگر محاسبه می‌شود. درصورتی‌که همبستگی میان دو جریان زیاد باشد، دو جریان مشابه یکدیگر و توسط مهاجم تولید شده‌اند، در غیر این صورت دو جریان متفاوت و سالم هستند.	فقط می‌تواند دو ترافیک را درصورتی‌که جدا از هم باشند، تشخیص دهد. قابلیت تشخیص لحظه‌ای را ندارد و بر اساس کل ترافیک تصمیم‌گیری می‌کند.	[۳۸]
۶	تشخیص حملات سیل آسا از هجوم ناگهانی کاربران، بر اساس الگوهای ترافیکی و با استفاده از روش های کشف آنتروپی	در این روش میزان آنتروپی اولیه ترافیک یک گره در شبکه، محاسبه و با میزان آنتروپی ثانویه بعد از رخداد حمله مقایسه می شود. در صورت وجود تفاوت بیش از آستانه در میزان آنتروپی اولیه و ثانویه، گره مشکوک در نظر گرفته می شود. سپس میزان همبستگی بین گره های مشکوک محاسبه شده و گره هایی که میزان همبستگی در آنها بیش از حد آستانه باشد، حمله کننده در نظر گرفته می شوند.	در این روش ابتدا همبندی شبکه با استفاده از داده ترافیکی بدست آمده و مسیر رسیدن بسته ها به سرویس دهنده با استفاده از الگوریتم کوتاهترین مسیر، محاسبه می شود. البته در مورد مزیت این کار دقیق توضیح داده نشده است. فرض این روش بر این است که گره ها ابتدا در حال ارسال ترافیک سالم هستند و سپس تعدادی از آن ها شروع به ارسال ترافیک حمله می کنند که این فرض ممکن است چندان درست نباشد.	[۳۹]

فصل ۳: روش پیشنهادی

۳-۱- روش ارائه‌شده

روش‌هایی که در بخش قبل مورد بررسی قرار گرفتند، به‌جز روشی که بر اساس قابل پیش‌بینی نبودن ترافیک یک کاربر و قابل پیش‌بینی بودن ترافیک حمله منع سرویس عمل می‌کرد، همگی بر اساس ویژگی‌های کلی یک ترافیک در سطح جریان، عمل می‌کردند. در این حالت می‌توان دو جریان حمله و سالم ترافیکی را از هم تشخیص داد ولی در دنیای واقعی وقتی‌که ترافیک‌های مختلف با هم ترکیب می‌شوند و یا حتی وقتی‌که یک حمله منع سرویس هم‌زمان با هجوم ناگهانی کاربران اتفاق می‌افتد، این روش‌ها کارایی لازم را ندارند. در این حالت، روشی موردنیاز است که با توجه به ویژگی‌های رفتاری جریان تک‌تک کاربران، بتواند عمل تشخیص را انجام دهد. مزیت این روش این است که می‌توان کاربران مجاز را از ربات‌های حمله تشخیص داد و با مسدود کردن آدرس‌های متخاصم، با حمله مقابله کرد. در ادامه این بخش در مورد تفاوت‌های رفتاری یک کاربر مجاز و یک ماشین خودکار که ترافیک حمله را تولید می‌کند، بحث خواهیم کرد و سپس با توجه به این تفاوت‌ها، روش پیشنهادی خود را ارائه خواهیم نمود.

۳-۲- داده‌های ترافیکی مورد استفاده

۱- ترافیک هجوم ناگهانی کاربران، سرویس‌دهنده انتخاب واحد دانشگاه صنعتی شریف

شروع ضبط ترافیک: سه‌شنبه، ۳۰ دی‌ماه ۱۳۹۳ ساعت ۱۲:۵۰ بعدازظهر

پایان ضبط ترافیک: ۵ بهمن‌ماه ۱۳۹۳، ساعت ۸:۵۰ قبل از ظهر

آدرس اینترنتی سرویس‌دهنده: ۲۱۳.۲۳۳.۱۶۱.۱۱۰

این ترافیک به مدت ۵ روز، شامل درخواست‌های رسیده به سرویس‌دهنده انتخاب واحد دانشگاه صنعتی شریف در سال تحصیلی ۹۴-۹۳ می‌باشد که توسط دستگاه ضبط کننده‌ی ترافیک موجود در آزمایشگاه

تست و ارزیابی تجهیزات شبکه که بین خط ارتباطی سرویس‌دهنده‌ی انتخاب واحد و شبکه اینترنتی، قرار داده شده بود، ضبط شده است. در طول این ۵ روز، ۳ روز، به‌عنوان روزهای انتخاب واحد تعیین شده‌اند که شامل روزهای دوم، چهارم و پنجم می‌باشند. در طول این ۳ روز و در ساعات معینی، حجم ترافیک رسیده به سرویس‌دهنده، بسیار افزایش یافته است. این افزایش به دلیل هجوم کاربران به سرویس‌دهنده، جهت انتخاب واحد می‌باشد. بسیاری از کاربران از شبکه دانشگاه صنعتی شریف برای دسترسی به اینترنت و درنهایت این سرویس‌دهنده استفاده کرده‌اند و به دلیل اینکه در این شبکه از برگردان آدرس شبکه[1] برای دسترسی به شبکه اینترنت استفاده می‌شود، همه‌ی آدرس‌های شبکه داخلی به آدرس خاصی برگردانده شده‌اند. بنابراین نمی‌توان تعداد دقیق کاربران را تعیین کرد.

۲- ترافیک هجوم ناگهانی کاربران، سرویس‌دهنده رقابت‌های جام جهانی ۱۹۹۸ فرانسه

این ترافیک [۴۱] شامل درخواست‌های رسیده به سایت بازی‌های جام جهانی ۹۸ فرانسه، بین ۳۰ آوریل ۱۹۹۸ تا ۲۶ جولای ۱۹۹۸، به مدت ۸۸ روز می‌باشد. تعداد سرویس‌دهنده‌های این سایت ۳۳ عدد می‌باشند که در ۴ منطقه جغرافیایی مختلف قرار دارند. در طول مدت ۸۸ روز، ۱.۳۵۲.۸۰۴.۱۰۷ درخواست توسط سرویس‌دهنده دریافت شده است.

۳- ترافیک حمله منع سرویس، CAIDA

این ترافیک [۴۲] شامل ۶۶ دقیقه، حمله منع سرویس توزیع شده، در تاریخ ۴ آگوست ۲۰۰۷، به سرویس‌دهنده‌ای با آدرس ۷۱.۱۲۶.۲۲۲.۶۴ می‌باشد. این حمله که از نوع جریان سیل‌آسای ICMP می‌باشد، در مدت ۶۶ دقیقه، ۳۵۹.۶۵۵.۸۲۶ درخواست را به سرویس‌دهنده مذکور ارسال کرده است.

[1] Network Address Translation

۳-۳- تخمین خودهمانندی

روش‌های مختلفی برای تخمین پارامتر Hurst وجـود دارنـد کـه روش واریـانس تجمیعـی[1]، روش تخمین ویتل[2]، روش آماره‌ی قابل مقیاس بندی مجدد[3] (R/S) و ... از آن جمله می‌باشند. روش R/S که اولین بار توسط خود آقای Hurst معرفی شد، به‌طور معمول برای محاسبه ضریب خودهمانندی بکـار می‌رود. اما بررسی‌ای که در [۴۳] بر روی خودهمانندی ترافیک‌های مختلف انجـام شـده اسـت، نشـان می‌دهد که این روش ضریب خودهمانندی را کم‌تر از مقدار واقعی خود تخمین می‌زند و بر اساس نتایج به‌دست‌آمده، روش واریانس تجمیعی، برای اندازه‌گیری ترافیک شبکه مناسب‌تر است و مـا نیـز در ایـن پژوهش از این روش استفاده خواهیم کرد.

ما برای محاسبه ضریب خودهمانندی از نرم‌افزار Selfies استفاده کردیم [۴۴, ۴۵]. این نرم‌افزار که در بسیاری از پژوهش‌ها که به بررسی خودهمانندی ترافیک شبکه‌های مختلف پرداخته‌اند، مورد استفاده قرار گرفته است [۴۶, ۴۷, ۴۸]، عملکرد دقیقی دارد و می‌تواند ضریب خودهمانندی را بـه شـش روش مختلف محاسبه کند که نتایج مورد نظر ما با استفاده از روش واریانس به دست خواهند آمد. داده ورودی این نرم‌افزار در روش واریانس تعداد درخواست‌های رسیده به سرویس‌دهنده در واحد زمان می‌باشند.

در این پژوهش، ما خودهمانندی در ترافیک‌های مختلف را مورد بررسی قرار داده ایم:

---

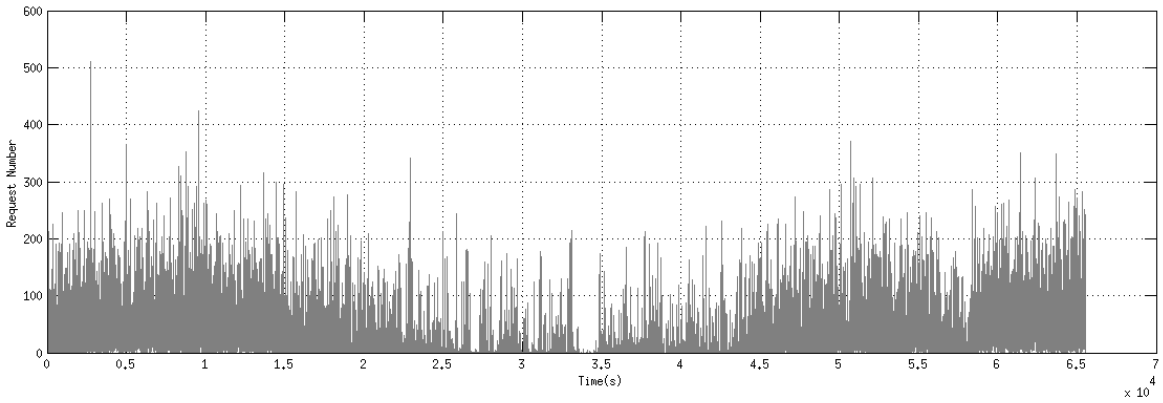
[1] Aggregate Variance

[2] Whittle

[3] Rescaled Range Statistics

۳-۳-۱- خودهمانندی در ترافیک سایت انتخاب واحد دانشگاه شریف

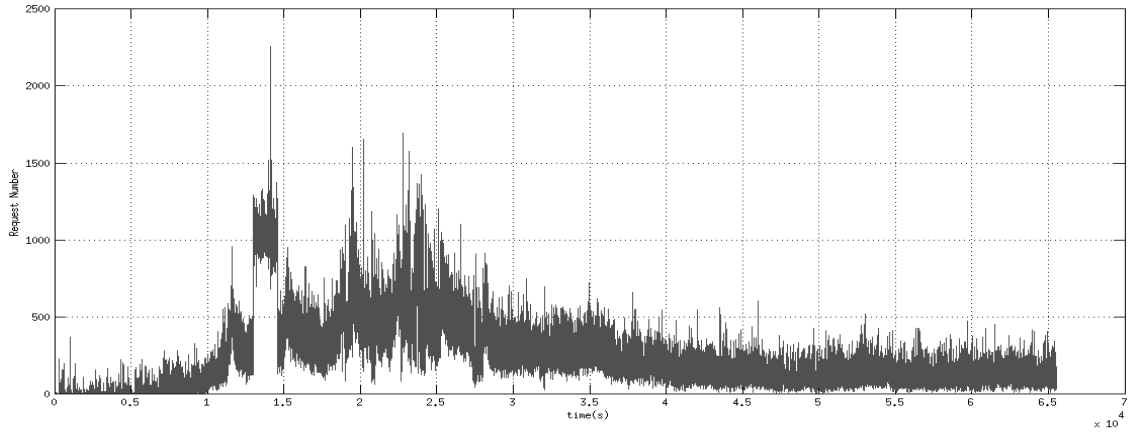
برای این منظور دو نوع ترافیک مختلف مورد بررسی قرار گرفته‌اند، ۱- قسمتی از ترافیک که در روزی غیر از روزهای اعلام شده برای انتخاب (پنج‌شنبه ۲ دی‌ماه ۹۳) واحد ضبط شده و به عبارتی ترافیک سالم و عادی محسوب می‌شود (شکل ۹) و همچنین ترافیکی که در طول مدت انتخاب واحد و هجوم کاربران (دانشجویان) برای اخذ واحدهای درسی، ضبط شده است (شنبه ۴ بهمن‌ماه ۹۳). مدت زمان هر دو ترافیک حدود ۶۵۰۰۰ ثانیه (حدود ۱۸ ساعت می‌باشد). البته تمام این زمان را نمی‌توان مدت زمان هجوم ناگهانی در نظر گرفت، اما همان‌طور که در شکل ۱۰ مشاهده می‌شود، تعداد درخواست‌های کاربران در ساعات بعدی نیز، هنوز متأثر از رویداد انتخاب واحد است و نسبت به روزهای عادی بیشتر می‌باشد.



شکل ۹- تعداد درخواست رسیده در واحد زمان به سرویس‌دهنده انتخاب واحد دانشگاه صنعتی شریف در مدت ۱۸ ساعت در یک روز عادی (۹۳/۱۰/۲)

مقدار پارامتر Hurst برای ترافیک فوق و با استفاده از روش واریانس، ۰.۷۳ به‌دست‌آمده است.

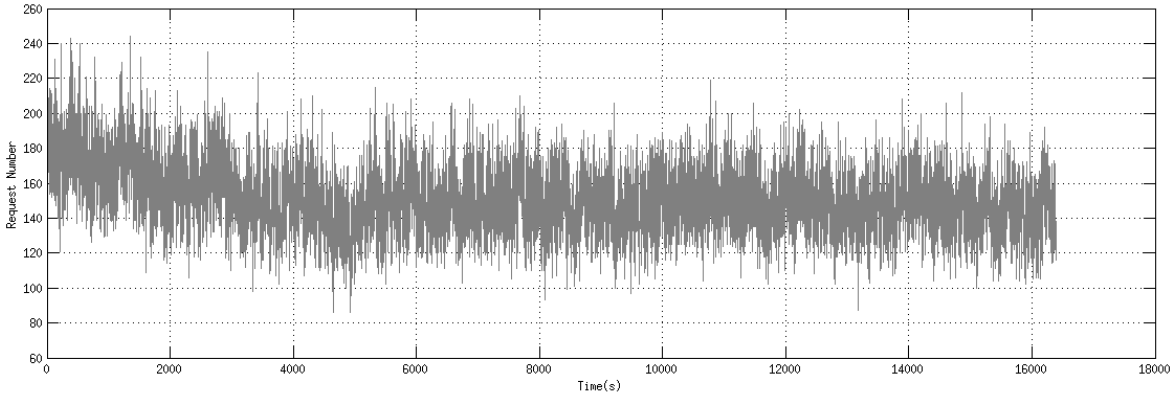
شکل ۱۰، تعداد درخواست‌های رسیده به سرور انتخاب واحد که بخش بزرگی از آن شامل هجوم کاربران می‌باشد را نشان می‌دهد. مقدار پارامتر Hurst محاسبه‌شده برای این ترافیک که مدتی مشابه ترافیک قبلی دارد، با استفاده از روش واریانس، ۰.۹۵ می‌باشد که نشان‌دهنده افزایش حدود ۰.۲ آن نسبت به حالت ترافیک عادی می‌باشد.



شکل ۱۰- تعداد درخواست رسیده در واحد زمان به سرویس‌دهنده انتخاب واحد دانشگاه صنعتی شریف در مدت ۱۸ ساعت در روز انتخاب واحد (۹۳/۱۱/۴)

۳-۳-۲- خودهمانندی در ترافیک سایت جام جهانی ۹۸ فرانسه

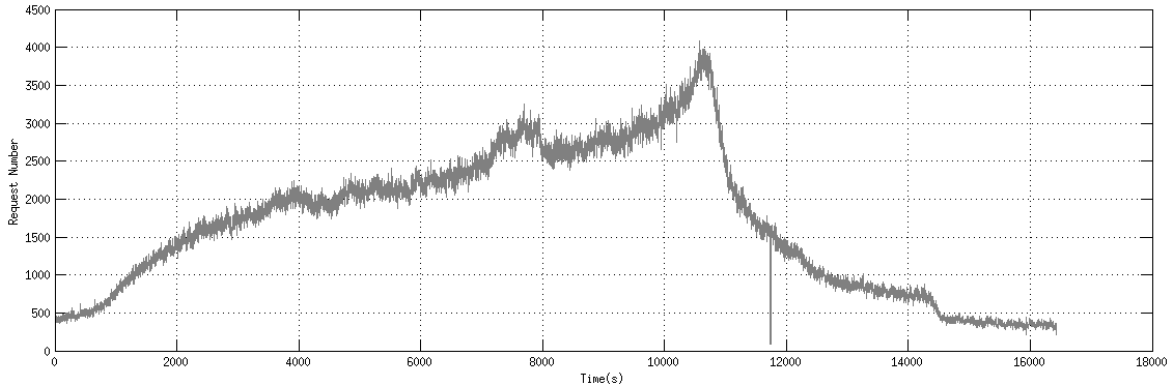
مشابه حالت قبل دو بازه مختلف برای ترافیک عادی یکی در روزی که بازی رقابت‌های جام جهانی در آن برگزار نمی‌شود (روز ۷۶ام- ۶ جولای ۱۹۹۸) و همچنین روزی که در آن یک بازی مهم نیمه‌نهایی برگزار می‌شود (روز ۷۷ ام- ۷ جولای ۱۹۹۸) و کاربران در طول ۹۰ دقیقه بازی، برای دانستن نتیجه بازی، به سایت بازی‌ها هجوم آورده‌اند، انتخاب شده‌اند. مدت زمان هر دو ترافیک ۱۶۰۰۰ ثانیه (حدود ۵ ساعت) می‌باشد. شکل ۱۱ نمودار تعداد درخواست‌های رسیده به سرویس دهنده در واحد زمان، در یک روز عادی را نشان می دهد.



شکل ۱۱- تعداد درخواست رسیده در واحد زمان به سرویس‌دهنده سایت جام جهانی ۹۸ فرانسه در مدت ۵ ساعت یک روز عادی (۶ جولای ۱۹۹۸)

مقدار ضریب خودهمانندی (Hurst) برای ترافیک فوق با استفاده از روش واریانس، ۰.۸۸ می‌باشد.

شکل ۱۲ نیز تعداد درخواست‌ها در واحد زمان در موقع هجوم ناگهانی کاربران به سایت بازی‌ها را نشان می‌دهد. مقدار ضریب خودهمانندی با استفاده از روش واریانس در این ترافیک، ۰.۹۴ محاسبه شده است. البته برخلاف ترافیک قبلی، میزان افزایش ضریب خود همانندی زیاد نمی‌باشد. اما بازهم این مقدار با افزایشی به میزان ۰.۰۶ مواجه شده است.

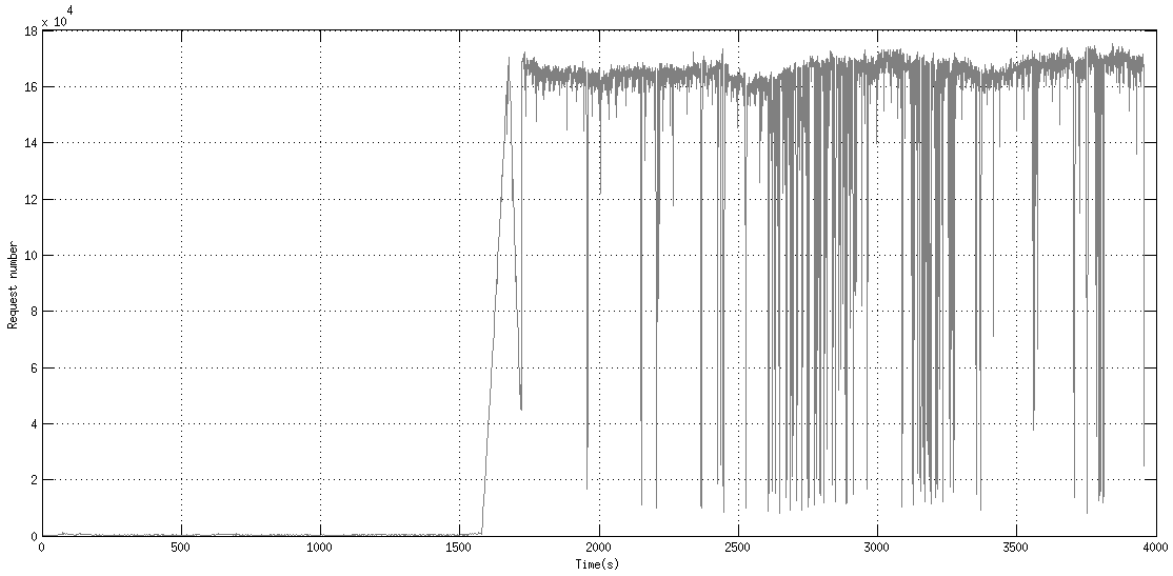


شکل ۱۲- تعداد درخواست رسیده در واحد زمان به سرویس‌دهنده سایت جام جهانی ۹۸ فرانسه در مدت ۵ ساعت هجوم ناگهانی کاربران (۷ جولای ۱۹۹۸)

در [۴۹] که بررسی رفتار کاربران از نظر میزان آنتروپی در رویداد هجوم ناگهانی کاربران پرداخته است، نشان داده شده که بی‌نظمی رفتاری (آنتروپی) کاربران در طول هجوم ناگهانی کاربران به میزان زیادی کاهش می‌یابد و این باعث کاهش بی‌نظمی در سطح کل ترافیک می‌شود و باعث افزایش میزان خودهمانندی ترافیک می‌شود. علت این امر نیز چنین بیان شده است که تعداد زیادی از کاربران به‌طور هم‌زمان به دنبال هدف واحدی هستند. نتایج به‌دست‌آمده توسط ما نیز بر این مسئله که میزان خود همانندی در طول هجوم ناگهانی کاربران افزایش می‌یابد، صحه می‌گذارد.

۳-۳-۳- خودهمانندی در ترافیک حمله منع سرویس CAIDA

شکل ۱۳ نمودار تعداد درخواست‌های رسیده در واحد زمان به قربانی را در یک حمله منع سرویس نشان می‌دهد. با استفاده از روش واریانس مقدار ضریب خودهمانندی برای این ترافیک، مقدار ۰.۶ به‌دست‌آمده است. همان‌طور که ملاحظه می‌شود، مقدار خود همانندی در ترافیک حمله تا حد زیادی کاهش یافته است. علت این امر را می‌توان در دلایلی که برای خودهمانند بودن ترافیک ذکر شد، جستجو کرد. ساختار شبکه معمولاً در حمله و ترافیک سالم یکسان می‌باشد. نوع پروتکل نیز می‌تواند به انتخاب مهاجم انتخاب شود. بنابراین تفاوتی که وجود دارد در رفتار کاربر و رفتار مهاجم در دسترسی به یک منبع است. مهاجم در حمله، هدف خصمانه ای از دسترسی به یک فایل یا یک سرویس‌دهنده وب را دارد. بنابراین رفتارش در ارسال درخواست‌های متوالی به سرویس دهنده، کاملاً متفاوت خواهد بود. یک کاربر پس از دسترسی به یک خبر، مدت زمانی را صرف خواندن آن می‌کند. این رفتار با توجه به کاربران مختلف می‌تواند متفاوت باشد. به همین علت میزان تفاوت رفتار دو کاربر مختلف در هجوم ناگهانی کاربران، هرچند که هدف واحدی در رسیدن به یک مطلب خاص را داشته باشند، متفاوت است. این مورد در حمله منع سرویس قدری متفاوت خواهد بود. در حمله مهاجم با استفاده از یک برنامه خودکار که سیستم زامبی به آن آلوده شده است، اقدام به ارسال ترافیک مشخصی به یک قربانی می‌کند. به همین دلیل پیش‌بینی می‌شود در یک ترافیک حمله الگوی مشخصی وجود داشته باشد. بنابراین با کشف شباهت‌ها میان رفتار کاربران در ترافیک‌های مختلف، می‌توان آن‌ها را دسته‌بندی کرد.



شکل ۱۳- تعداد درخواست رسیده در واحد زمان به یک سرویس‌دهنده قربانی حمله منع سرویس در مدت ۶۶ دقیقه

۳-۴- بررسی رفتار کاربران در ارسال بسته‌های متوالی در ترافیک‌های مختلف

بر اساس ویژگی‌هایی که در بخش اول ذکر شد، یک سیستم تشخیص کارا باید بتواند با تکیه بر کمترین امکانات سخت‌افزاری و در کمترین زمان ممکن، عمل تشخیص حمله منع سرویس را از هجوم ناگهانی کاربران انجام دهد. ازاین‌رو در این پژوهش ما به آن قسمت از رفتار کاربران که در ارسال بسته‌های متوالی یک کاربر نمایان است، پرداخته‌ایم. در حقیقت منظور ما از رفتار، زمان ارسال درخواست‌های متوالی از سوی یک کاربر یا ربات حمله منع سرویس می‌باشد. ویژگی این روش این است که نیاز به بکارگیری تجهیزات پیچیده سخت‌افزاری با توانایی‌های بالا را ندارد و تنها با ذخیره‌سازی زمان رسیدن بسته‌های یک کاربر می‌تواند تحلیل لازم را انجام دهد که بر این اساس نیازی به تحلیل رفتار در لایه‌های بالاتر، به‌خصوص تحلیل ویژگی‌های لایه انتقال و شبکه نیست. این ویژگی باعث می‌شود که بتوان روش فوق را نه تنها در سرویس‌دهنده، بلکه در مسیریاب‌های بالادستی نیز پیاده‌سازی کرد که این

خود باعث دور شدن لایه‌های دفاعی از سرویس‌دهنده شده و باعث سرعت بخشیدن به عمل تشخیص و مقابله با حمله می‌شود. به‌علاوه، تغییر پروتکل‌های مختلف تأثیری در این فرایند تشخیص نخواهد داشت.

شکل‌های ۱۴ تا ۲۵ نمودارهای مختلف مربوط به زمان رسیدن بسته‌های ۱۰۰۰ درخواست متوالی و جدول توزیع‌های متناسب با آن‌ها برای دو کاربر مختلف در هنگام هجوم ناگهانی کاربران، در ترافیک شماره ۱ (هجوم ناگهانی کاربران به سایت جام جهانی ۹۸ فرانسه) و دو حمله‌کننده مختلف، در حمله منع سرویس (CAIDA) را نشان می‌دهند.

شکل های ۱۶، ۱۹، ۲۲ و ۲۵ نشان دهنده توزیعی هستند که بیشترین مقدار شباهت را با توزیع زمانی بسته های متوالی یک کاربر یا مهاجم را دارند. جداول ۳،۴،۵ و ۶ نیز بیانگر توزیع هایی هستند که به ترتیب بیشترین میزان شباهت را با این توزیع زمانی دارند. این برازش نموداری[1] با استفاده از تابع fitmethis نرم افزار متلب[2] انجام شده است که زمان بین ۱۰۰۰ درخواست متوالی یک کاربر به عنوان ورودی به آن داده شده است. این تابع می تواند حدود ۳۰ توزیع مختلف پیوسته و گسسته را بر روی داده مختلف بررسی کرده و آن ها را به ترتیب میزان شباهت مرتب کند. سپس نمودار توزیع احتمال حاصل از شبیه ترین برازش و همچنین توزیع احتمال داده ورودی را رسم کند. در جداول، ۳ ستون اول نشان دهنده پارمترهای توزیع مختلف هر توزیع می باشد. البته تابع بعضی از توزیع ها پارامترهای دوم و یا سوم را ندارند. ستون ششم نشان دهنده‌ی معیار اطلاعاتی آکائیکه[3] می باشد که با AIC مشخص شده است. این معیار برای سنجش میزان خوبی یک برازش[4] به کار می رود. این معیار بر اساس مفهوم آنتروپی بنا

---

[1] Curve Fitting

[2] Matlab

[3] Akaike information criterion

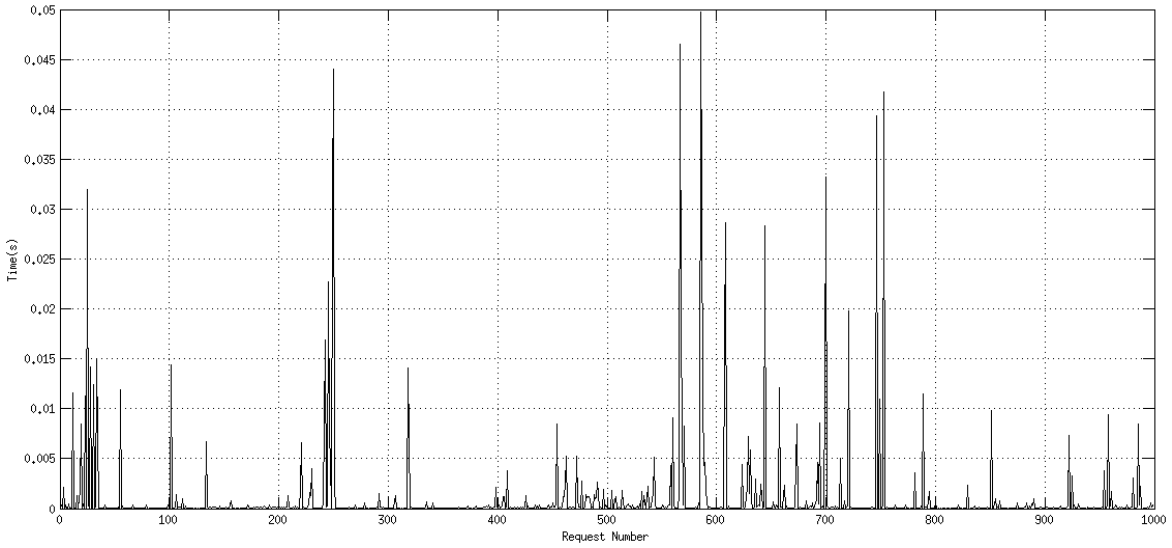
[4] Goodness of fit

شده‌است و نشان می‌دهد که استفاده از یک مدل آماری به چه میزان باعث از دست رفتن اطلاعات می‌شود. به عبارت دیگر، این معیار تعادلی میان دقت توزیع و پیچیدگی آن برقرار می‌کند. این معیار توسط هیروتسوگو آکائیکه برای مقایسه چند توزیع مختلف و انتخاب بهترین توزیع آماری پیشنهاد شده است [۵۰]. با توجه به داده‌ها، چندین توزیع مختلف بر اساس مقدار AIC به ترتیب از کمتر به بیشتر، رتبه بندی می شوند. میزان AIC برای یک توزیع آماری، طبق رابطه‌ی ۱۴ محاسبه می شود.

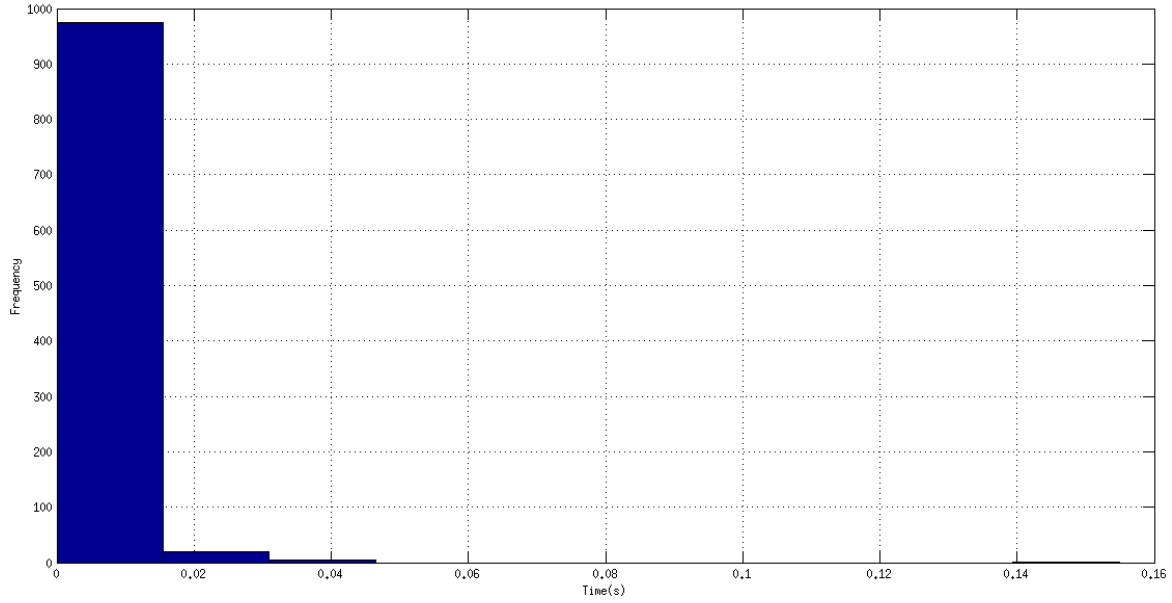
$$AIC = 2k - 2\ln(L) \qquad (۱۴)$$

در این رابطه، k نشان دهنده تعداد پارامترهای یک توزیع و L بیانگر مقدار بیشینه‌ی تابع درست نمایی[1] است. ستون پنجم جدول نیز بیانگر لگاریتم L می باشد.

[1] Likelihood Function

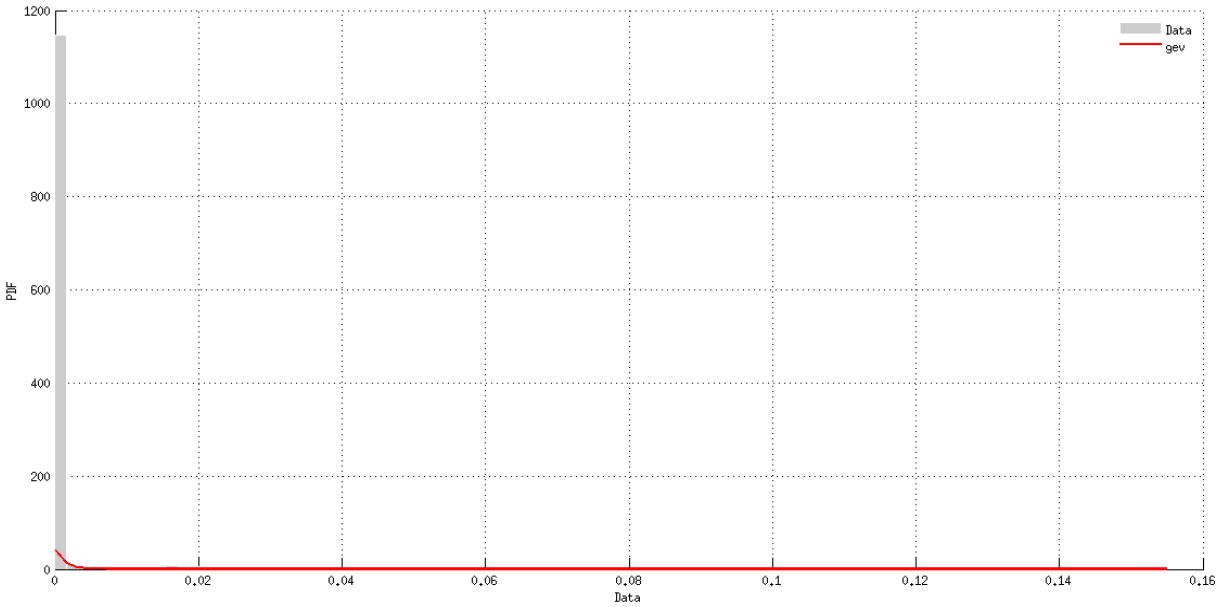


شکل ۱۴ - نمودار فاصله زمانی ۱۰۰۰ درخواست متوالی یک کاربر نمونه در هجوم ناگهانی کاربران



شکل ۱۵- نمودار بافت نگار [1] فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک کاربر نمونه هجوم ناگهانی کاربران

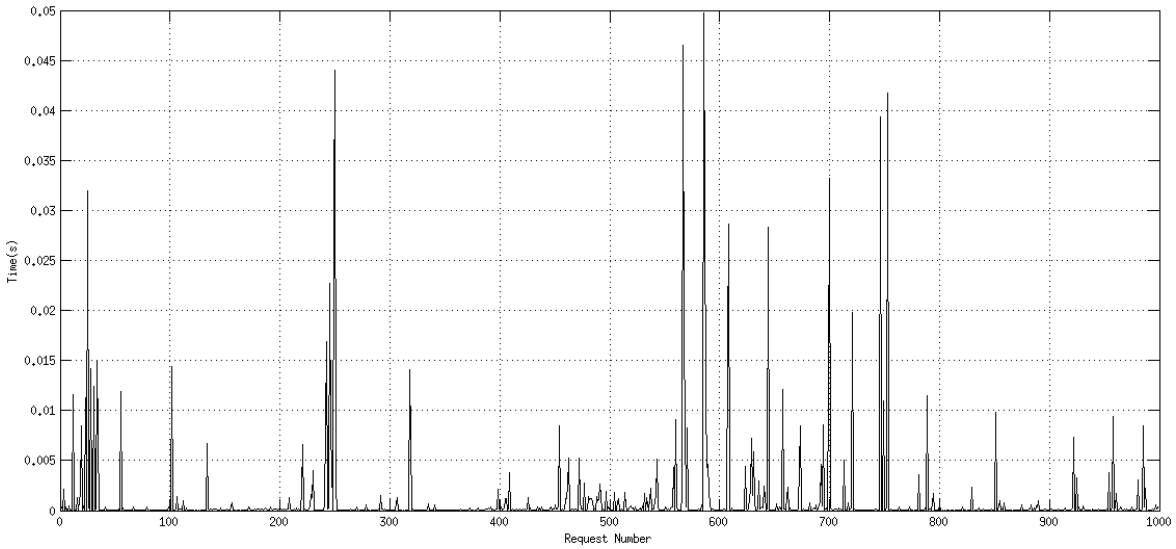
[1] Histogram



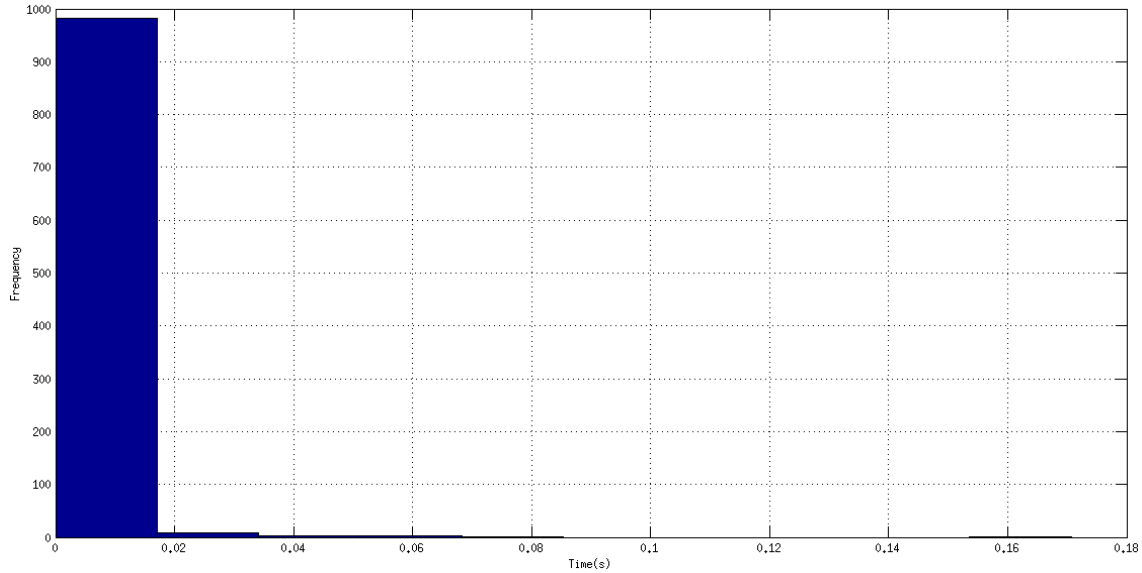
شکل ۱۶- نمودار توزیع فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک کاربر نمونه هجوم ناگهانی کاربران

جدول ۳- توزیع‌های برازش شده بر روی نمودار فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک کاربر نمونه هجوم ناگهانی کاربران، به ترتیب میزان تطابق

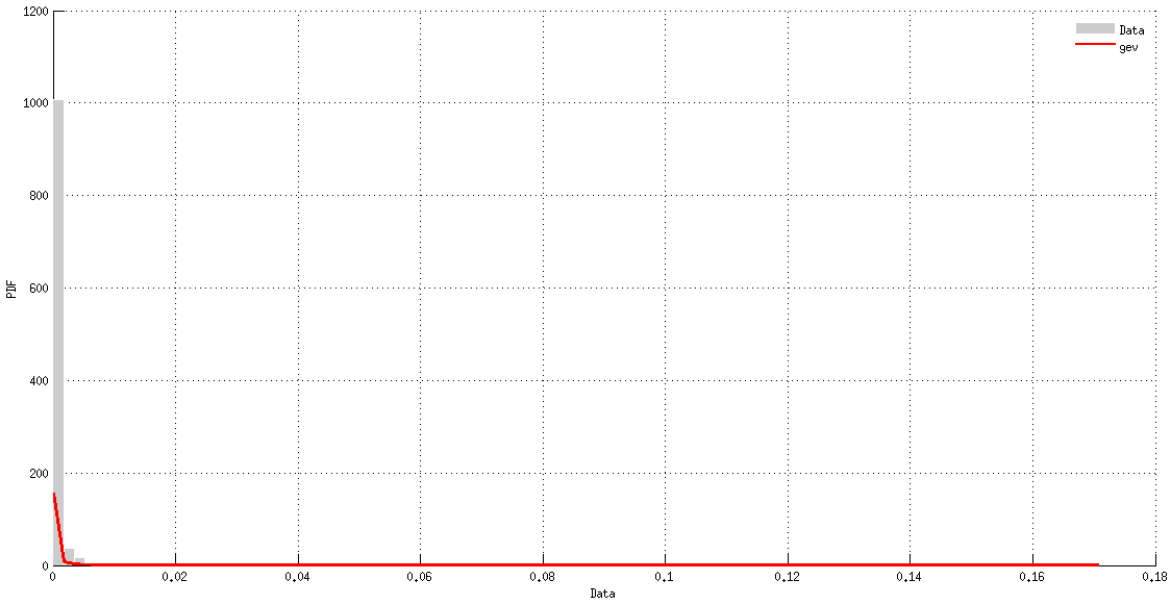
Dist. Name	Par1	Par2	Par3	LogL	AIC
gev	1.496	0.00001412	0.00001454	8666	-17330
inversegaussian	1.00E-003	0.00001769	-	8477	-16950
loglogistic	-10.53	0.8204	-	8379	-16750
gp	1.183	0.00002613	-	8361	-16720
lognormal	-10.25	1.774	-	8250	-16500
tlocationscale	0.00002103	0.00001452	0.7188	8154	-16300
birnbaumsaunders	0.0002584	4.092	-	8082	-16160
weibull	0.0000996	0.395	-	7905	-15810
gamma	0.2172	0.004608	-	7531	-15060



شکل ۱۷- نمودار فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک کاربر نمونه هجوم ناگهانی کاربران



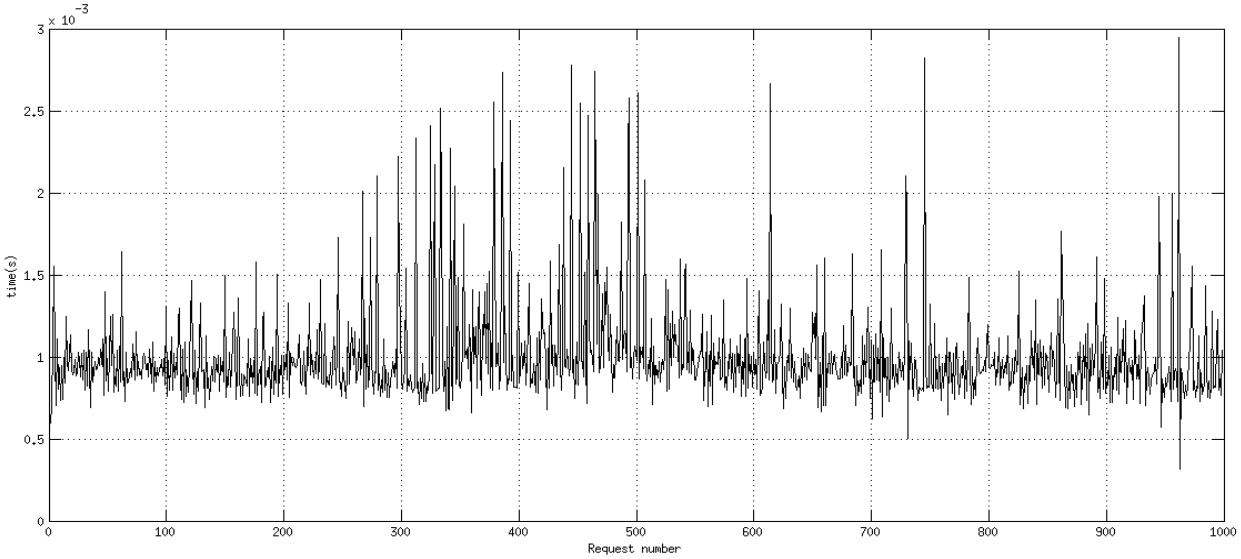
شکل ۱۸- نمودار بافت نگار فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک کاربر نمونه هجوم ناگهانی کاربران



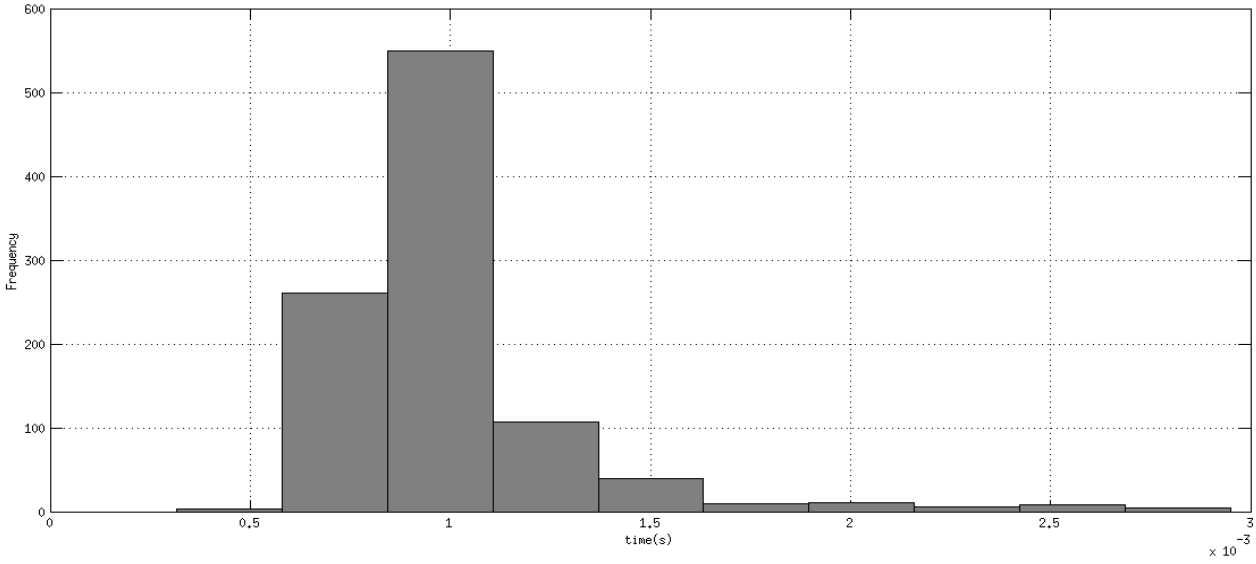
شکل ۱۹- نمودار توزیع فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک کاربر نمونه هجوم ناگهانی کاربران

جدول ۴- توزیع‌های برازش شده بر روی نمودار فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک کاربر نمونه هجوم ناگهانی کاربران، به ترتیب میزان تطابق

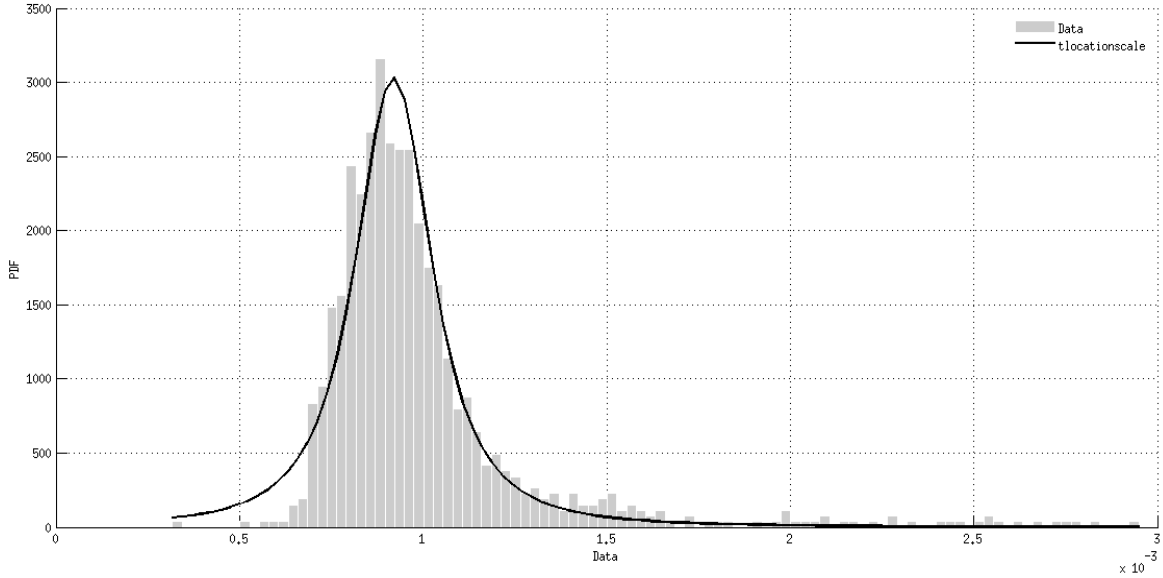
Dist. Name	Par1	Par2	Par3	LogL	AIC
gev	4.669	0.00004262	0.000009128	8192	-16380
beta	0.05754	57.37	-	7551	-15100
gamma	0.05302	0.01888	-	7501	-15000
tlocationscale	0.00005101	0.00004604	0.6763	6902	-13800
exponential	0.001001	-	-	5901	-11800
logistic	0.0002836	0.0008852	-	4760	-9515
normal	0.001001	0.004345	-	4016	-8028
ev	0.00415	0.01101	-	3220	-6436
uniform	0	0.04978	-	2997	-5990



شکل ۲۰ - نمودار فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک مهاجم نمونه در حمله منع سرویس



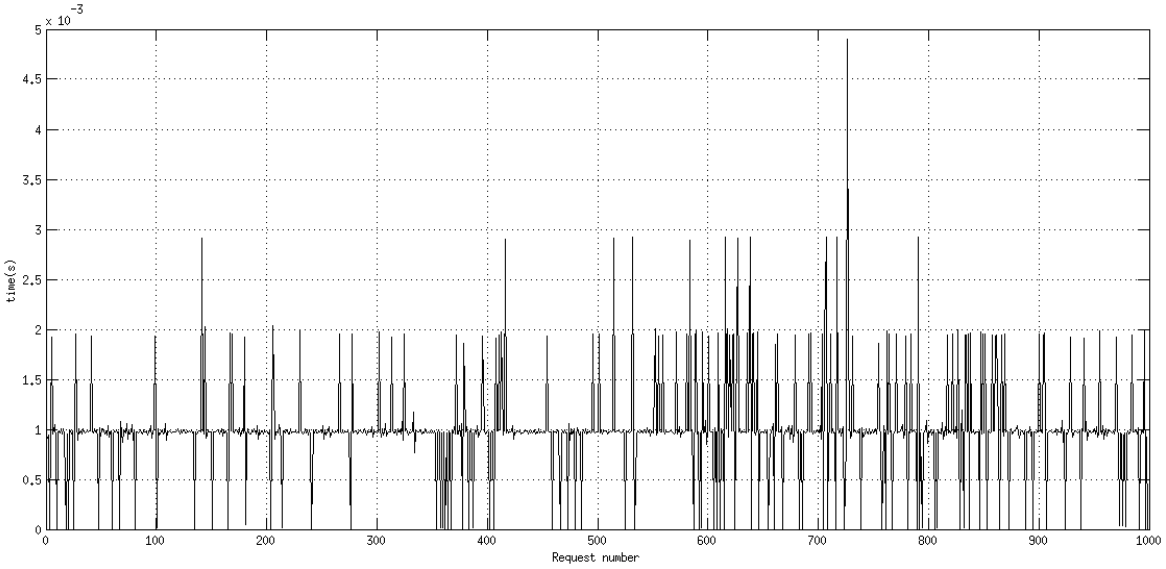
شکل ۲۱ - نمودار بافت نگار فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک مهاجم نمونه در حمله منع سرویس



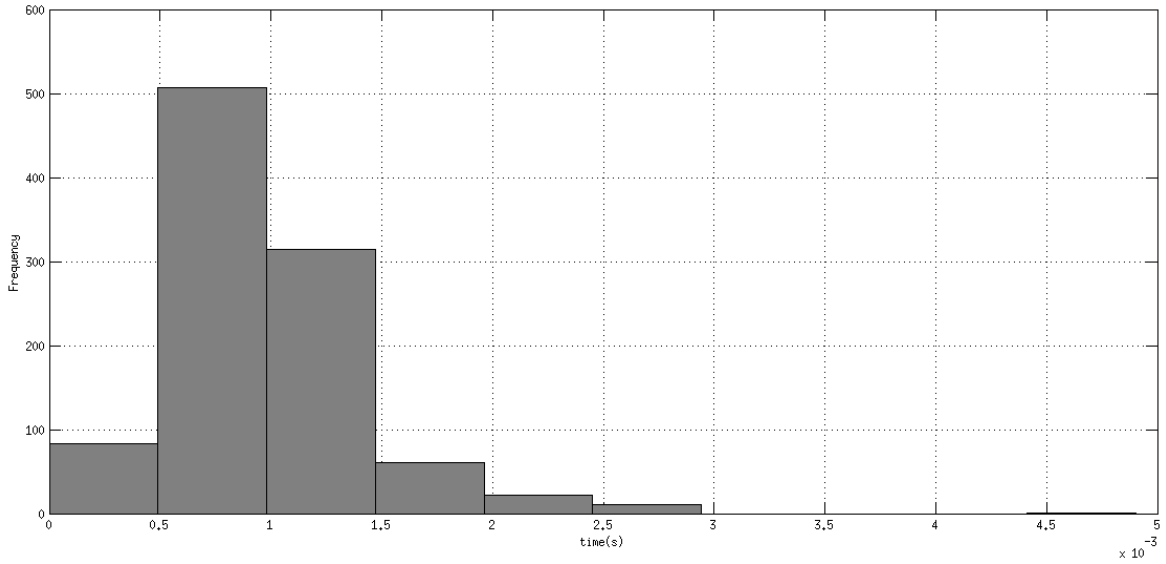
شکل ۲۲- نمودار توزیع فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک مهاجم نمونه در حمله منع سرویس

جدول ۵- توزیع‌های برازش شده بر روی نمودار فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک مهاجم نمونه در حمله منع سرویس، به ترتیب میزان تطابق

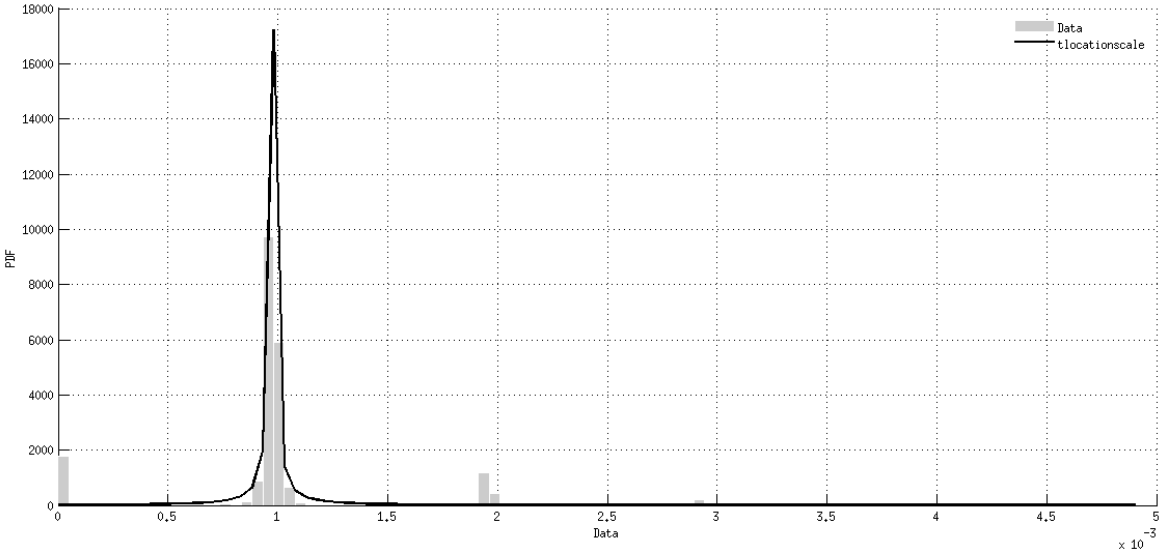
Dist. Name	Par1	Par2	Par3	LogL	AIC
tlocationscale	0.0009195	0.0001149	1.778	7034	-14060
gev	0.0776	0.0001749	0.0008827	7030	-14050
loglogistic	-6.968	0.1191	-	7024	-14040
lognormal	-6.94	0.2421	-	6933	-13860
inversegaussian	0.001001	0.01621	-	6924	-13840
birnbaumsaunders	0.0009715	0.2466	-	6922	-13840
logistic	0.0009511	0.000129	-	6869	-13730
gamma	15	0.00006675	-	6857	-13710
beta	14.98	14950	-	6857	-13710
nakagami	3.317	0.000001097	-	6757	-13510



شکل ۲۳ - نمودار فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک کاربر نمونه هجوم ناگهانی کاربران



شکل ۲۴ - نمودار بافت نگار فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک مهاجم نمونه در حمله منع سرویس



شکل ۲۵- نمودار توزیع فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک مهاجم نمونه در حمله منع سرویس

جدول ۶- توزیع‌های برازش شده بر روی نمودار فاصله زمانی ۱۰۰۰ درخواست متوالی برای یک مهاجم نمونه در حمله منع سرویس، به ترتیب میزان تطابق

Dist. Name	Par1	Par2	Par3	LogL	AIC
tlocationscale	0.0009754	0.00001296	0.5576	7812	-15620
logistic	0.0009809	0.0001874	-	6431	-12860
normal	0.001001	0.000463		6253	-12500
gev	-0.09322	0.0004489	0.0008063	6242	-12480
nakagami	0.4882	0.000001216	-	6078	-12150
gp	-0.2303	0.001162	-	5982	-11960
weibull	0.001043	1.371	-	5954	-11900
beta	1.034	1032	-	5902	-11800
gamma	1.034	0.000968	-	5901	-11800
exponential	0.001001	-	-	5901	-11800

۳-۴-۱- بررسی آنتروپی رفتار کاربران در ارسال بسته‌های متوالی در ترافیک‌های مختلف

در[۴۹] ، میزان بی‌نظمی ترافیک در ترافیک‌های مختلف بررسی شده و به این نتیجه رسیده‌اند که در ترافیک هجوم ناگهانی کاربران، با روش محاسبه بی‌نظمی نمونه، میزان بی‌نظمی نسبت به ترافیک حالت عادی کاهش می‌یابد و دلیل این امر نیز، همان‌گونه که قبلاً ذکر شد این است که تعداد زیادی در کاربران به طور همزمان هدف واحدی را تعقیب می کنند. در مورد تأثیرات این کاهش بر روی میزان خودهمانندی ترافیک نیز پیش‌تر بحث شد.

در این پژوهش ما به بررسی مقدار بی‌نظمی رفتار تک‌تک کاربران (چه کاربر مجاز و چه ربات حمله منع سرویس) در ترافیک‌های مختلف خواهیم پرداخت. تأکید می‌کنیم که در این پژوهش، منظور ما از رفتار، مربوط به بخشی می شود که در ارسال بسته‌های متوالی از سمت کاربر، جلوه پیدا می‌کند.

در ادامه ما با استفاده از محاسبه آنتروپی[۱] اطلاعات، میزان بی‌نظمی را در درخواست‌های کاربران مختلف کشف خواهیم کرد. مفهوم اساسی آنتروپی اطلاعات در نظریه اطلاعات به این منظور تعریف شده است که یک سیگنال یا یک رخداد اتفاقی تا چه حد تصادفی است. آنتروپی اطلاعات که به نام آنتروپی شانون هم شناخته می‌شود، (متأثر از نام کلود شانون[۲] ریاضی‌دان آمریکایی) درواقع میزان تصادفی بودن را به‌صورت یک سنجه‌ی[۳] ریاضی نشان می‌دهد.

$$H(X) = -\sum_{i} P(x_i) log_b P(X_i) \qquad (۱۵)$$

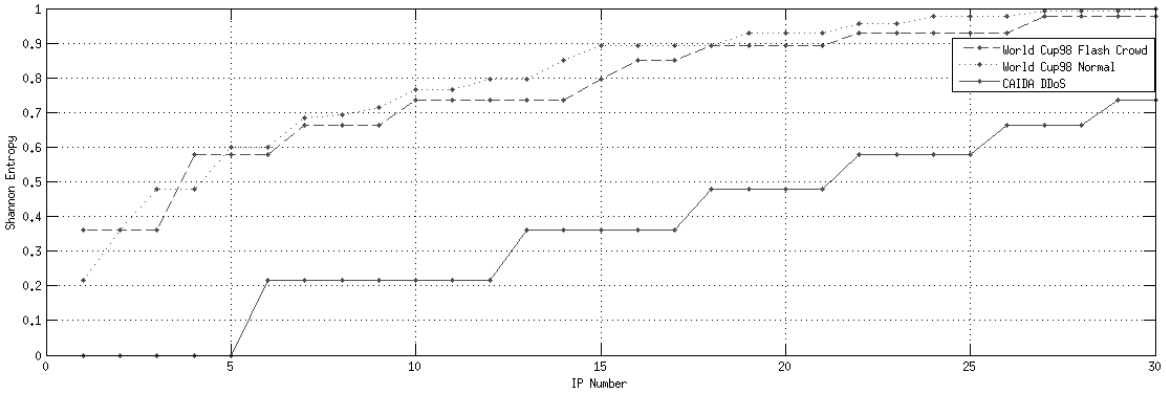
[1] Entrpoy

[2] Claude Shannon

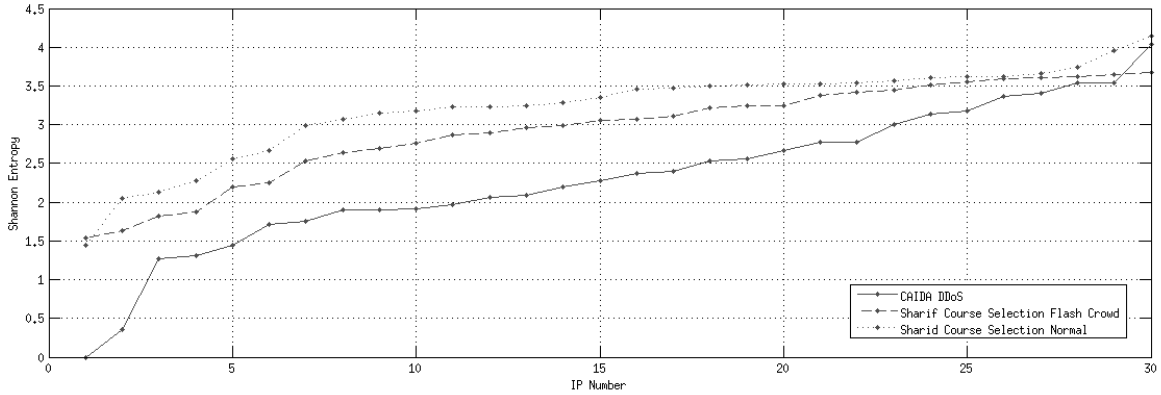
[3] Metric

زمان رسیدن بین بسته‌های متوالی یک کاربر به‌عنوان ورودی به تابع فوق داده می‌شود. خروجی این تابع عددی بدون واحد می‌باشد که نشانگر میزان بی‌نظمی و تصادفی بودن است.

نمودار شکل ۲۶، مقادیر محاسبه این عدد برای ۳۰ آدرس اینترنتی که به‌صورت تصادفی انتخاب شده‌اند را در دو ترافیک مختلف حمله و هجوم ناگهانی، نشان می‌دهد. شکل ۲۷ نیز همین محاسبه را برای دو ترافیک دیگر نشان می‌دهد. ترافیک سالم به دو بخش ترافیک حالت عادی و ترافیک هجوم ناگهانی کاربران تقسیم شده است.



شکل ۲۶- مقایسه مقدار آنتروپی درخواست‌های متوالی ۳۰ کاربر در ۳ ترافیک مختلف



شکل ۲۷- مقایسه مقدار آنتروپی درخواست‌های متوالی ۳۰ کاربر در ۳ ترافیک مختلف

با مقایسه دو نمودار قبل می‌توان به این نتیجه رسید که میزان بی‌نظمی در رفتار ربات‌های انتخاب شده در حمله منع سرویس، به‌طورکلی، کمتر از ترافیک‌های سالم می‌باشد. همچنین همان‌طور که

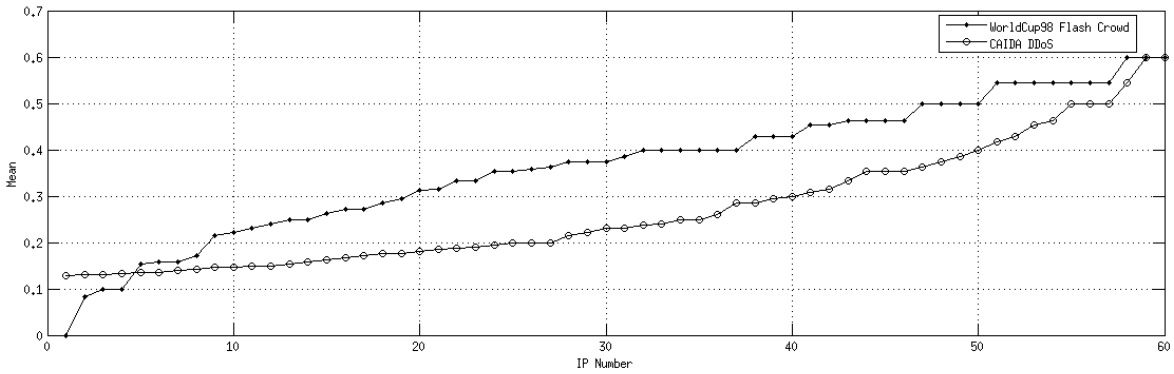
مشخص است، کاربران در هنگام هجوم ناگهانی، بی‌نظمی کمتری، در رفتار خود نشـان مـی‌دهنـد. ایـن نتیجه می‌تواند تأییدی باشد بر [۴۹] که در آن نتیجه به‌دست‌آمده حاکی از کاهش بی‌نظمی ترافیک کلی نسبت در هنگام هجوم ناگهانی کاربران نسبت به حالت عادی بود.

این مسئله که میزان بی‌نظمی در ترافیک حمله منع سرویس، کم می‌باشد را می‌توان ناشی از تولید ترافیک حمله با آهنگ منظم و هدف مشترک تمام حمله‌کنندگان، یعنی تلاش بـرای از کـار انـداختن سرویس‌دهنده با استفاده از حجم بالای ترافیک دانست.

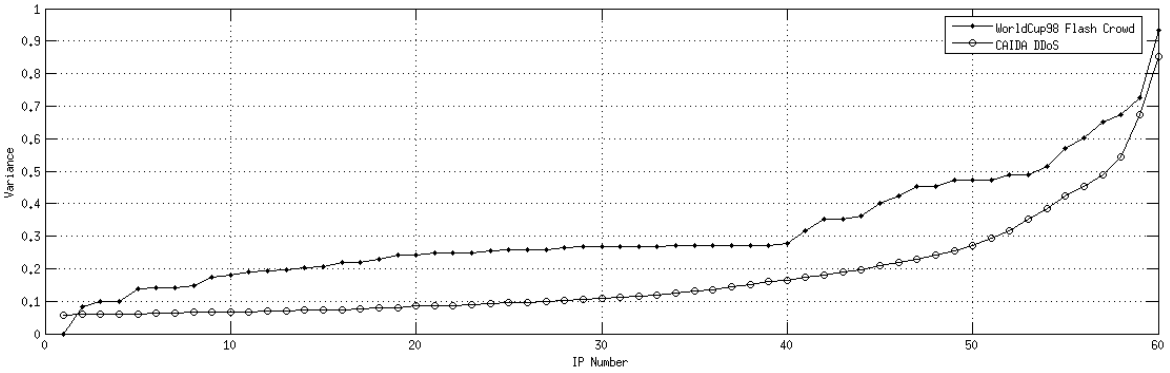
دو شکل ۲۸ و ۲۹، نمودار میانگین و واریانس زمان بین درخواست‌های متوالی چند کاربر در هجوم ناگهانی و چند حمله‌کننده در حمله منع سرویس با یکدیگر مقایسه شده‌اند.

$$\overline{\boldsymbol{x}} = \frac{\boldsymbol{x_1 + x_2 + x_3 + \cdots + x_n}}{\boldsymbol{n}} \qquad (۱۶)$$

$$\boldsymbol{Var(X) = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{x})^2} \qquad (۱۷)$$



شکل ۲۸- مقدار میانگین زمان بین درخواست‌های متوالی حمله‌کنندگان در ترافیک حمله و هجوم ناگهانی کاربران



شکل ۲۹ – مقدار واریانس زمان بین درخواست‌های متوالی کاربران در ترافیک حمله و هجوم ناگهانی کاربران

شکل های ۲۸ و ۲۹ بیانگر این مطلب هستند که میانگین زمان بین بسته های رسیده حمله کننده در حمله منع سرویس به طور کلی، کمتر از یک کاربر در هجوم ناگهانی می باشد. یعنی حمله کننده نرخ ارسال درخواست بسیار بالایی دارد و در بازه زمانی بسیار کوتاهی تعداد زیادی درخواست به سرویس دهنده ارسال کرده است. همچنین مقدار کم واریانس زمان بین بسته های ارسالی حمله کننده نشان دهنده این است که این زمان ها بسیار به هم نزدیک بوده و بنابراین به مقدار میانگین نزدیک می باشند. این مساله می تواند بر کارامد بودن روش مبتنی بر الگوی رفتاری در ارسال بسته های متوالی صحه بگذارد.

به‌طورکلی، دو نمودار نشان‌دهنده این مطلب هستند که فاصله بین درخواست‌های متوالی در حمله منع سرویس، بسیارکمتر از هجوم ناگهانی کاربران بوده و این فواصل به مقدار میانگین بسیار نزدیک هستند.

۳-۵- تشخیص ترافیک حمله منع سرویس از هجوم ناگهانی کاربران با استفاده از میزان شباهت توزیع زمان بین بسته‌های متوالی کاربران

در [۶] آقای وانلی و همکارانشان با استفاده از میزان شباهت موجود بین نمونه‌های دو ترافیک مختلف، توانسته‌اند آن‌ها را از یکدیگر تشخیص دهند. آن‌ها برای اندازه‌گیری میزان شباهت از محاسبه ضریب شباهت Bhattacharya استفاده کرده‌اند و با توجه به مقادیر آستانه‌ای که با آزمایش‌های تجربی به دست آورده‌اند، در صورت داشتن دو ترافیک مختلف، توانسته‌اند نوع آن‌ها را تشخیص دهند. نحوه پیاده‌سازی این روش در بخش قبل بررسی شد. اما بحثی که در این فصل مطرح می شود، بررسی میزان شباهت رفتار دو کاربر مختلف در ارسال بسته‌های متوالی است. از آنجا که ترافیک حمله توسط ماشین‌های خودکار و برنامه‌ای از قبل طراحی‌شده، ارسال می‌شود، پیش‌بینی می‌شود شباهت بین رفتارهای کاربران در آن بیشتر از ترافیک‌های سالم و هجوم ناگهانی کاربران باشد.

برای تعیین معیار فاصله مورد استفاده برای روش ارائه‌شده، ابتدا باید به این نکته توجه کرد که فواصل مرتبه اول، ازآنجایی‌که مهاجم می‌تواند این فواصل را به‌سادگی در ترافیک تولیدی خود تقلید کند، مناسب نمی‌باشند [۵۱]. همچنین باید به این نکته توجه کرد که روش‌هایی که فواصل نامتقارن را به فواصل متقارن تبدیل می‌کنند، دقت پایین‌تری نسبت به روش‌هایی که خود متقارن هستند، دارند. ازاین‌رو ما در این پژوهش از فاصله اطلاعاتی Bhattacharya استفاده خواهیم نمود. این فاصله اطلاعاتی علاوه بر اینکه معیار و متقارن و مرتبه‌ی دو می‌باشد، دقت بالایی نیز دارد و در بسیاری از پژوهش‌ها استفاده شده است.

با استفاده از رابطه زیر، توزیعی از داده‌ها را با توجه به کل زمان، برای ۲۰ درخواست متوالی ۳۰ آدرس مختلف در ۴ ترافیک مختلف به دست می‌آوریم.

$$p(x^i) = x_k^i . (\sum_{k=1}^{n} x_k^i)^{-1} \qquad (۱۸)$$

این ۴ ترافیک عبارت‌اند از:

۱- ترافیک حمله DDoS CAIDA

۲- ترافیک هجوم ناگهانی کاربران جام جهانی ۹۸ فرانسه

۳- ترافیک هجوم ناگهانی کاربران سایت انتخاب واحد دانشگاه صنعتی شریف

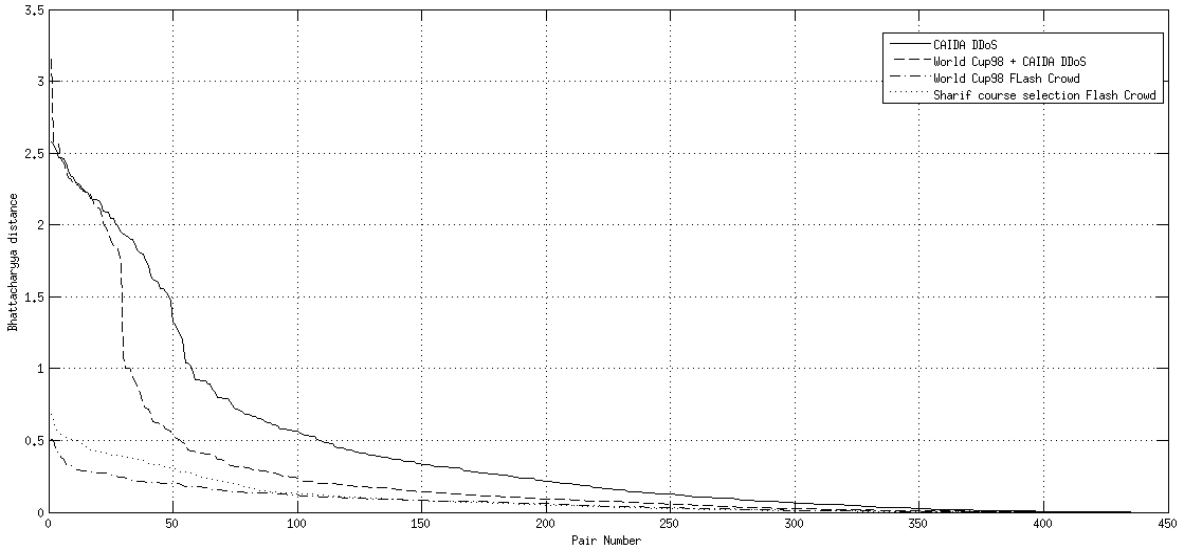
۴- ترکیبی از ترافیک نوع ۱ و نوع ۲

برای ۳۰ آدرس مختلف از هر ترافیک، فاصله Bhattacharya را برای هر جفت آدرس مختلف محاسبه می‌کنیم.

با توجه به رابطه زیر، ۴۳۵ مقایسه مختلف برای هر ترافیک خواهیم داشت.

$$\binom{n}{2} = \frac{n!}{2! \times (n-2)!} \qquad (۱۹)$$

پس از مرتب‌سازی، نتایج به‌دست‌آمده به‌صورت نزولی، نمودار حاصله از اعداد به‌دست‌آمده در شکل ۳۰ آمده است.



شکل ۳۰- مقایسه فاصله Bhattacharya بین کاربران ۴ ترافیک مختلف

جدول ۷- مقایسه مقادیر میانگین، بیشینه و کمینه‌ی فاصله Bhattacharya بین کاربران ۴ ترافیک مختلف

Traffic name	Min	Max	Mean
CAIDA-DDoS	2.2234e-06	2.5803	0.4389
WorldCup98-Flash Cowd	5.5200e-08	0.5091	0.0767
WorldCup98-Flash Cowd+ CAIDA-DDoS	5.5199e-08	3.1819	0.2738
Sharif Uni-Course selection-Flash Crowd	5.2587e-07	0.6821	0.0980

با توجه به نتایج به‌دست‌آمده، در جدول ۷ مشاهده می‌شود که میانگین فاصله Bhattacharya بین توزیع زمان بین درخواست‌های متوالی در حمله منع سرویس، حدود ۶ برابر هجوم ناگهانی کاربران می‌باشد. این مقدار در ترکیبی از ترافیک‌های حمله و ترافیک منع سرویس، حدود ۴ برابر می‌باشد. شیب تند ترافیک ترکیبی نشان‌دهنده این است که رفتار برخی کاربران بسیار شبیه هم می‌باشد و رفتار برخی دیگر با هم فاصله زیادی دارد. بنابراین این معیار فاصله می‌تواند روش مناسبی برای تشخیص انواع ترافیک با یکدیگر باشد که علاوه بر دقت بالا، بر اساس رفتار تک‌تک کاربران نیز عمل می‌کند. در مورد مزیت‌های تشخیص بر اساس رفتار کاربران به‌تفصیل سخن گفته‌ایم.

۳-۵-۱- استفاده از تفاوت‌های موجود در رفتار کاربران برای کشف حملات منع سرویسی که در حین هجوم ناگهانی کاربران اتفاق می‌افتند

در فصل گذشته ذکر کردیم که مزیت بررسی رفتار کاربران، این است که می‌توان یک حمله را در حین هجوم ناگهانی کاربران نیز شناسایی و خنثی کرد. اتفاق افتادن یک حمله در حین هجوم ناگهانی کاربران، با توجه به اهداف اقتصادی و سیاسی و ... که برای تدارک یک حمله ذکر شد، بسیار محتمل می‌باشد.

بنابراین ما به روشی نیاز داریم که با توجه به تفاوت‌های ذکرشده، بتواند آدرس‌های مهاجم را که به‌موازات یک هجوم ناگهانی، اقدام به ارسال ترافیک حمله به‌سوی قربانی می‌کنند، کشف و آن‌ها را مسدود نماید.

در این پژوهش ما از روش‌های خوشه‌بندی برای این کار استفاده خواهیم کرد. ویژگی‌های مورد خوشه‌بندی برای یک کاربر، همان تفاوت‌هایی هستند که در قسمت قبل مورد بررسی قرار گرفتند که عبارت‌اند از مقدار **میانگین**، **واریانس** و **آنتروپی**. همه این موارد با توجه به زمان بین درخواست‌های متوالی یک کاربر یا ربات حمله، محاسبه می‌شوند. در ادامه روش مورد استفاده برای خوشه‌بندی، نتایج و نقد این نتایج ارائه خواهد شد.

پس از استخراج ویژگی‌های ذکرشده، ماتریسی مشابه زیر برای آدرس‌های اینترنتی موجود در یک ترافیک در یک بازه زمانی مشخص، به دست خواهد آمد که هر سطر آن نشان‌دهنده یک آدرس و ستون‌های آن نشان‌دهنده ویژگی‌های مشخص شده می‌باشند که به آن بردار ویژگی می‌گویند. لازم به ذکر است که هر چه تعداد ویژگی‌های متمایز کننده بیشتر باشد، خوشه‌بندی دقیق‌تر انجام خواهد شد.

جدول ۸ - مقادیر ویژگی‌های استخراج‌شده از رفتار چند کاربر مختلف در ارسال بسته‌های متوالی

	Mean	Var	Entropy
IP1	0.1154	0.1062	0.5159
IP2	0.1579	0.1404	0.6292
IP3	0.1818	0.1558	0.684
IP4	0.1304	0.1186	0.5586
IP5	0.0968	0.0903	0.4587
.....	.....	.....	.....

در ادامه، ما ویژگی‌های فوق را برای ترافیکی را که شامل ۲۵ کاربر در حال ارسال درخواست‌های مجاز در حین هجوم ناگهانی کاربران و ترافیکی که ۵ ربات حمله در حال ارسال ترافیک حمله می‌باشند، استخراج نموده‌ایم.

برای نشان دادن میزان شباهت ویژگی‌های رفتارهای این آدرس‌ها به یکدیگر و خوشه‌بندی آن‌ها به دو گروه، کاربران مجاز و همچنین، مهاجمین حمله، در ابتدا فاصله اقلیدسی[1] هر جفت از آدرس‌ها با یکدیگر را به دست می‌آوریم.

برای محاسبه فاصله اقلیدسی بین دو بردار ویژگی، می‌توان از رابطه زیر استفاده کرد:

$$d(X,Y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2} \qquad (۲۰)$$

تعداد مقایسه‌های مورد نیاز برای به دست آوردن فاصله اقلیدسی همه جفت آدرس‌ها از رابطه ۱۶ قابل محاسبه است.

جدول زیر مقدار فاصله‌های به‌دست‌آمده برای ۵ جفت آدرس که به‌طور تصادفی از بین ۳۰ آدرس مختلفی انتخاب شده‌اند، نشان می‌دهد.

[1] Euclidean Distance

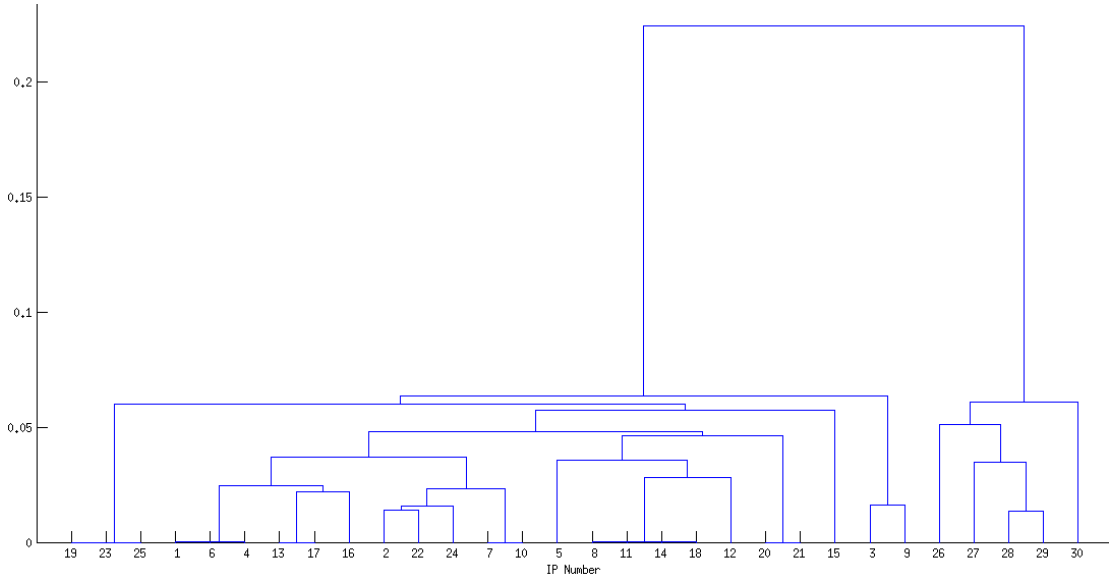
جدول ۹- مقدار فاصله اقلیدسی ویژگی‌های استخراج‌شده از رفتار ۵ کاربر مختلف

Feature / IP Number	IP1	IP2	IP3	IP4	IP5
IP1	0	0.3367	0.2554	0.0011	0.6678
IP2	0.3367	0	0.9187	0.3357	0.0044
IP3	0.2554	0.9187	0	0.2544	0.923
IP4	0.0011	0.3357	0.2544	0	0.6689
IP5	0.6678	0.0044	0.923	0.6689	0

با استفاده از الگوریتم پیوند[1]، می‌توان نزدیک‌ترین جفت‌ها[2] را به هم پیدا کرد، این الگوریتم به این صورت عمل می‌کند که ابتدا دو جفت را که کمترین فاصله اقلیدسی را با هم دارند، به هم متصل می‌کند. جفت بعدی می‌تواند بر اساس میانه فاصله این دو جفت با یک نمونه دیگر و یا اینکه دو جفت نمونه مجزای دیگر باشند. این کار تا جایی که تمام پیوندها با هم متصل شوند، ادامه پیدا می‌کند. شکل ۳۱ عملکرد حاصل از این الگوریتم را بر روی ۳۰ آدرس مختلف که ۵ عدد از آن‌ها مربوط به حمله منع سرویس می‌باشند، نشان می‌دهد.

[1] Linkage Algorithm

[2] Pairs



شکل ۳۱ - نمودار میزان شباهت دودویی ۳۰ کاربر مختلف به‌صورت سلسله مراتبی

همان‌طور که مشاهده می‌شود، در ابتدا بردار ویژگی‌های کاربران (شماره‌های ۱ تا ۲۵) در هجوم ناگهانی کاربران با یکدیگر پیوند می‌خورند. در سمت دیگر، بردار ویژگی در آدرس‌های مربوط به حملات منع سرویس به هم پیوند خورده و درنهایت یک پیوند نهایی این دو را به هم متصل می‌کند. اگر اتصال نهایی قطع شود، کل نمونه‌ها به دو خوشه مجزا تقسیم می‌شوند که یکی از خوشه‌ها شامل ۲۵ نمونه مربوط به هجوم ناگهانی و خوشه دوم مربوط به حمله منع سرویس می‌باشد. الگوریتمی که بر این اساس خوشه‌بندی را انجام می‌دهد، خوشه‌بندی سلسله مراتبی[1] نام دارد. این الگوریتم می‌تواند علاوه بر اینکه بر اساس تعداد خوشه‌های تصمیم‌گیری کند، خوشه‌بندی را بر اساس حداکثر فاصله تعیین‌شده انجام دهد. در این صورت لینک‌هایی که بالاتر از اندازه معینی باشند حذف خواهند شد و تعداد خوشه‌ها بعد از اجرای کامل الگوریتم مشخص خواهد شد.

[1] Hierarchical Clustering

اگرچه به نظر می‌رسد این الگوریتم پاسخ گوی نیاز ما خواهد بود، اما همان‌طور که گفته شد، سرعت تشخیص مساله‌ی بسیار مهمی است و نقش اساسی را در مقابله با یک حمله منع سرویس ایفا می‌کند. بررسی‌های انجام‌شده نشان می‌دهد الگوریتم خوشه‌بندی سلسله مراتبی کارایی و سرعت کمتری نسبت به سایر روش‌های موجود دارد. یکی از این الگوریتم‌ها که امروزه، در زمینه خوشه‌بندی بسیار مورد استفاده قرار می‌گیرد، K-Means نام دارد.

۳-۵-۲- الگوریتم خوشه‌بندی K-Means

K-Means یکی از الگوریتم‌های یادگیری بدون نظارت[1] است که در یادگیری ماشین کاربرد بسیار زیادی دارد. این الگوریتم از یک شیوه ساده برای خوشه‌بندی یک مجموعه داده در یک تعداد از پیش مشخص‌شده (k) خوشه، استفاده می‌کند. در مورد داده‌های ما که قرار است به دو دسته سالم و مشکوک به حمله تقسیم شوند، مقدار k=2 می‌باشد. ایده اصلی تعریف k مرکز برای هر یک از خوشه‌ها می‌باشد. این مراکز باید با دقت زیاد انتخاب شوند، زیرا مراکز مختلف، نتایج مختلف را به وجود می‌آورند .

بنابراین بهترین انتخاب قرار دادن آن‌ها (مراکز) در فاصله هر چه بیشتر از یکدیگر می‌باشد. قدم بعدی تخصیص هر الگو به نزدیک‌ترین مرکز می‌باشد. وقتی همه‌ی نقاط به مراکز موجود تخصیص داده شدند، مرحله اول تکمیل و یک گروه‌بندی اولیه انجام شده است .در مرحله بعد، k مرکز جدید برای خوشه‌های مرحله قبل پیدا می‌شود. بعد از تعیین k مرکز جدید، مجدداً داده‌ها را به مراکز مناسب تخصیص داده می‌شوند. این مراحل آن‌قدر تکرار خواهند شد که دیگر مراکز جابجا نشوند.

[1] Unsupervised Learning Algorithm

این الگوریتم نیز همانند روش قبل بر اساس معیار فاصله اقلیدسی d عمل می‌کند به‌این‌ترتیب کـه تخصیص هر داده به یک خوشه به ترتیبی انجام می‌شود که تابع هدف[1] زیر که به تابع خطای مربعـی[2] معروف است مقدار حداقل داشته باشد.

$$E = \sum_{k=1}^{K} \sum_{x \in C_k} d^2 (X, m_k) \quad (۲۱)$$

در رابطه فوق m ها مراکز خوشه‌ها و Xها نقاطی هستند که به باید به خوشه‌ها تخصیص داده شوند.

مزیت‌های الگوریتم K-Means که باعث شد در این پژوهش از آن استفاده کنیم، عبارت‌اند از:

- سرعت و دقت بسیار بالای الگوریتم نسبت به الگوریتم‌های مشابه
- امکان مشخص کردن تعداد خوشه‌هایی که داده‌ها به آن‌ها تقسیم‌بندی خواهند شد
- مقاومت بالای الگوریتم در برابر اختلال[3] و داده‌های پرت[4]

در این الگوریتم، نقاط شروع در ابتدا به‌صورت تصادفی انتخاب می‌شوند. به همین دلیل، ممکن است در اجراهای متفاوت، الگوریتم جواب‌های متفاوتی داشته باشد. این مسئله یکی از معایب ایـن الگـوریتم می‌باشد [۵۲, ۵۳].

[1] Objective Function

[2] Square Error Function

[3] Noise

[4] Outlier

۳-۶- جمع‌بندی روش ارائه‌شده

بر اساس مواردی که مطرح شد، به‌طورکلی می‌توان گفت که روش ارائه‌شده ما به این صورت عمل می‌کند که ابتدا بر اساس تغییرات حجم ترافیک دریافتی و کاهش یا افزایش میزان خودهمانندی، در مورد وقوع حمله و نوع آن تصمیم‌گیری می‌شود. سپس با خوشه‌بندی ترافیک بر اساس بردار ویژگی شامل میانگین، واریانس و آنتروپی زمان بین درخواست‌های رسیده از گره‌های شبکه (مشتری‌ها)، عمل تفکیک کاربران هجوم ناگهانی را از ربات‌های حمله منع سرویس، انجام می‌دهد. سپس با استفاده از معیار فاصله باتاچاریا در مورد نوع ترافیک هر خوشه تصمیم می‌گیرد و آدرس‌هایی که در چندین مرحله در خوشه‌ی حمله منع سرویس قرار می‌گیرند را مسدود می‌کند.

در فصل آینده، نتایج حاصل از اعمال روش تشخیصی که در این فصل بیان شد، بر روی یک ترافیک هجوم ناگهانی کاربران که در حین آن یک حمله منع سرویس نیز در حال رخ دادن است بررسی و ارزیابی خواهند شد.

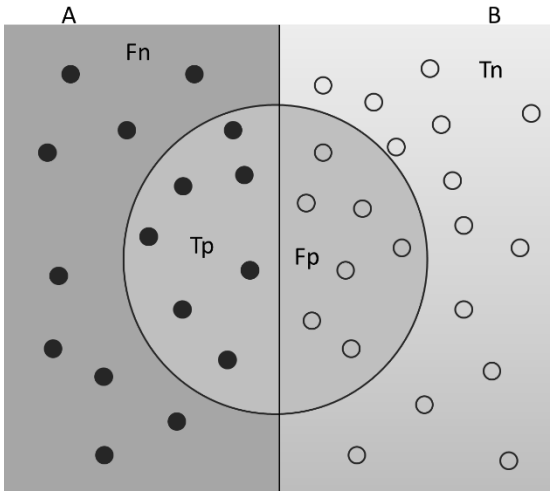
فصل ۴:

ارزیابی نتایج

در این فصل روش معرفی‌شده را با توجه به معیارهای مختلفی که در ادامه معرفی خواهیم کرد، ارزیابی خواهیم نمود. برای ارزیابی، روش فوق بر روی ترکیب ۳۰ دقیقه از ترافیک حمله منع سرویس با ترافیک هجوم ناگهانی کاربران اعمال شده و نتایج به‌دست‌آمده بررسی خواهند شد. فرض بر این است که با شروع هجوم ناگهانی، مهاجم با اهداف خرابکارانه سعی در از کار انداختن سرویس‌دهنده با ارسال ترافیک سنگین به آن را دارد.

۴-۱- معیارهای ارزیابی:

فرض می‌کنیم کل ناحیه شکل ۳۲، فضای نمونه‌ای است شامل آدرس‌هایی که در حمله منع سرویس شرکت دارند و با دایره‌های سیاه‌رنگ مشخص شده‌اند و آدرس‌های مربوط به کاربران مجاز سیستم که با دایره‌های توخالی مشخص هستند. واضح است کل ناحیه‌ای که باید به‌عنوان حمله کشف شود و اعلان، ناحیه A می‌باشد. حال فرض می‌کنیم که روش و سیستم تشخیص ما توانسته است فقط ناحیه‌ای را که با دایره بزرگ مشخص شده، به‌عنوان حمله شناسایی و اعلان کند. با توجه به این مساله، معیارهای ارزیابی در ادامه آورده شده‌اند.



شکل ۳۲- فضای نمونه شامل مهاجمین در حمله (دایره‌های سیاه) و کاربران مجاز سیستم (دایره‌های سفید) و قسمتی که کشف و اعلان شده است (دایره بزرگ)

۴-۱-۱- میزان منفی نادرست[1] و مثبت نادرست[2]

نیم‌دایره سمت راست که با Fp مشخص شده است نشان‌دهنده آدرس‌هایی است که جز حمله منع سرویس نیستند، اما به اشتباه حمله تشخیص داده شده‌اند. به این ناحیه مثبت نادرست گفته می‌شود.

ناحیه سمت چپ، قسمت خارج از دایره که با Fn مشخص شده است، نشان‌دهنده آدرس‌هایی است که جز حمله منع سرویس بوده‌اند ولی به اشتباه جزو ترافیک سالم (هجوم ناگهانی کاربران) تشخیص داده شده‌اند.

در محاسبه میزان ارزیابی، معمولاً از مقادیر Tp و Tn که نشان‌دهنده تشخیص‌های صحیح می‌باشد استفاده نمی‌کنند و بر اساس دو معیار قبلی که گفته شد عمل می‌کنند و یا از معیارهای نسبی استفاده می‌کنند که در ادامه معرفی می‌شوند.

۴-۱-۲- دقت تشخیص[3]

ناحیه‌ای که با دایره مشخص شده است به‌عنوان حمله اعلان شده است. اما نیم‌دایره سمت چپ آن جز تشخیص درست محسوب می‌شود و ناحیه سمت راست به‌اشتباه حمله تشخیص داده شده است. با توجه به این مسئله، دقت تشخیص عبارت است از نسبت تشخیص‌های درست به‌کل ناحیه تشخیص و به عبارت بهتر:

$$Precision = \frac{Tp}{Tp + Fp} \qquad (۲۲)$$

[1] False Negative

[2] False Positive

[3] Precision

۴-۱-۳- بازخوانی[1]

ناحیه سمت چپ که با A مشخص شده است، کل ناحیه‌ای است که باید به‌عنوان حمله تشخیص داده شود. ولی فقط قسمتی از آن که داخل دایره قرار گرفته و با Tp مشخص شده است، به عنوان حمله تشخیص داده شده است. بازخوانی عبارت است از نسبت تشخیص‌های درست در ناحیه تشخیص به کل ناحیه‌ای که باید به‌عنوان حمله تشخیص داده می‌شد و یا به عبارت بهتر:

$$Recall = \frac{Tp}{Tp + Fn} \qquad (۲۳)$$

۴-۱-۴- نرخ مثبت نادرست و نرخ مثبت درست

علاوه بر معیارهای ارزیابی ذکرشده، معیارهای دیگری نیز وجود دارند که در برخی موارد برای ارزیابی کارایی یک روش دسته‌بندی استفاده می‌شوند. نرخ مثبت نادرست عبارت است از نسبت موارد اشتباه تشخیص داده شده در ناحیه تشخیص (دایره بزرگ) به کل ناحیه‌ای که موارد سالم در آن وجود دارند. رابطه‌ی ۲۴ بیانگر این نرخ است. به نرخ مثبت نادرست، رخداد[2] نیز گفته می‌شود.

$$FPR = \frac{Fp}{Tn + Fp} \qquad (۲۴)$$

---

[1] Recall

[2] Fall-Out

نرخ مثبت درست برابر است با نسبت موارد درست تشخیص داده شده به کل ناحیه‌ای که موارد حمله در آن وجود دارند. مقدار این نرخ که به آن میزان حساسیت[1] هم گفته می‌شود، با مقدار بازخوانی برابر است. بنابراین این مقدار از رابطه ۲۵ قابل محاسبه می‌باشد.

$$TPR = \frac{Tp}{Tp + Fn} \qquad (۲۵)$$

۴-۲- نتایج ارزیابی روش ارائه‌شده

سیستم تشخیص و تفکیک حمله ما به این صورت عمل می‌کند که:

۱- با بالا رفتن نرخ ترافیک، سیستم تشخیص فعال می‌شود.

۲- ترافیک دریافتی ازنظر میزان ضریب خودهمانندی (Hurst) بررسی می‌شود و اگر ضریب خودهمانندی پایین‌تر از میزان حالت عادی و نرخ رشد ترافیک بسیار بالا باشد، احتمال حمله منع سرویس وجود دارد.

۳- سیستم شروع به ذخیره زمان رسیدن بسته‌های متوالی کاربران می‌کند. هر کاربر در مدت زمان n، m درخواست متوالی ارسال می‌کند. ازآنجایی‌که برای مقایسه، باید تعداد یکسانی از درخواست‌های متوالی کاربران مختلف را در نظر گرفت، بنابراین، مقدار $k<m$ به شکلی انتخاب می‌شود که بتوان تعداد کافی مقایسه با دقت بالا انجام داد. برای مثال برای همه کاربران، ۲۰ درخواست اول مدنظر قرار می‌گیرد. طبیعی است که اگر تعداد درخواست‌های کاربری کمتر از

[1] Sensitivity

۲۰ باشد، در محاسبات شرکت داده نمی‌شود. بعد از گذشت زمان مشخص n برای هر کاربر مقادیر $(t_1,t_2,t_3,\ldots,t_{k-1})$ وجود دارند که نشان‌دهنده زمان بین رسیدن K بسته متوالی او را نشان می‌دهند. برای هر کاربر، مقادیر $P(X)=(X_1,X_2,..,X_{k-1})$ محاسبه می‌شوند. متغیر تصادفی X نشان‌دهنده توزیع زمان K درخواست است، به‌طوری‌که:

$$X_i = \frac{t_i}{\sum_1^{k-1} t_j}$$

۴- سپس با استفاده از معیار فاصله Bhattacharya و محاسبه آن برای توزیع زمان رسیدن بسته‌های متوالی کاربران مختلف با یکدیگر و مقایسه آن با حالت عادی شبکه، می‌توان نوع ترافیک را مشخص کرد. اگر میانگین فاصله‌های به‌دست‌آمده در حالت عادی شبکه برابر d_n و میانگین فاصله‌های به‌دست‌آمده در حالت نرخ بالای ترافیک، d_a باشد. برای یک مقدار مشخص‌شده p، اگر:

$$d_a > d_n \times p$$

احتمال وقوع یک حمله منع سرویس در حین هجوم ناگهانی کاربران وجود دارد.

۵- اگر ضریب خودهمانندی، افت کمی داشته باشد و نرخ ترافیک به‌صورت تدریجی رشد کند، ولی نمودار میزان فاصله Bhattacharya شیب تندی به پایین داشته باشد، نشان‌دهنده این است که در ترافیک هجوم ناگهانی، تعدادی از سرویس‌گیرنده‌ها، رفتار مشکوکی از خود نشان می‌دهند.

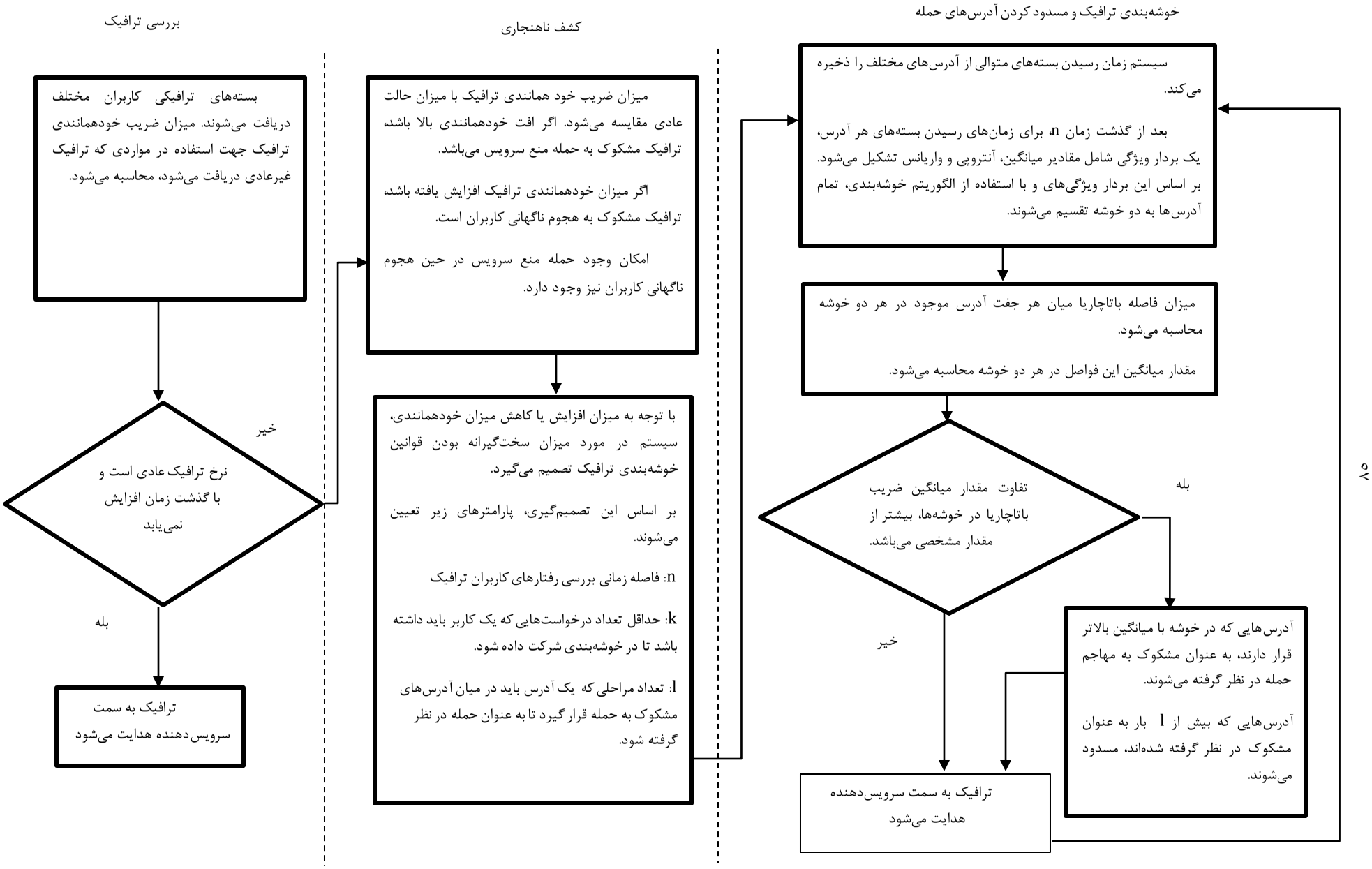
۶- با رسیدن به احتمال وجود حمله در هنگام هجوم ناگهانی کاربران، سیستم ویژگی‌های رفتاری کاربران در ارسال بسته‌های متوالی در مدت زمان n را استخراج کرده و با استفاده از آن، خوشه‌بندی میان آن‌ها را انجام می‌دهد. برای هر کاربر یک بردار ویژگی شامل میانگین، واریانس و آنتروپی زمان بین درخواست‌های متوالی او محاسبه می‌شود.

۷- بردارهای ویژگی هنجارسازی شده و بر اساس آن کاربران موجود در سیستم با استفاده از یک الگوریتم خوشه‌بندی به دو خوشه که نمایانگر دو جریان با ویژگی‌های متفاوت می‌باشند، تقسیم می‌شوند.

مشابه مرحله ۴، سیستم کاربران دو ترافیک را از نظر فاصله Bhattacharya میان آن‌ها بررسی کرده و اگر تفاوت‌های میان میانگین فاصله‌های دو ترافیک زیاد باشد، ترافیکی که میزان شباهت‌ها در آن بیشتر می‌باشد مشکوک و به عنوان حمله در نظر گرفته می‌شود. در این مرحله می‌توان ترافیک را از نظر سایر روش‌هایی که در فصل دوم معرفی شدند نیز بررسی کرد تا فرآیند تشخیص دقیق‌تر باشد. بعلاوه به دلیل محدود بودن تعداد آدرس‌های حمله، نسبت به هجوم ناگهانی [۷]، در مراحل اولیه می‌توان خوشه‌ای را که اندازه بسیار کوچک‌تری نسبت به دیگری دارد، به‌عنوان جریان حمله در نظر گرفت.

۸- مراحل ۶ و ۷ با فاصله‌ی زمانی n از دور قبل تکرار می‌شوند و پس از طی چند دور مشخص (برای مثال ۳ دور)، آدرس‌هایی که برای چندین دور جزو آدرس‌های مشکوک به حمله دسته‌بندی شده‌اند، به‌عنوان حمله تلقی شده و تمهیدات لازم برای مسدود کردن آن‌ها جهت خنثی کردن حمله، در نظر گرفته می‌شود. می‌توان تعدادی از نمونه‌هایی را که به‌عنوان حمله تشخیص داده شده‌اند را برای کمک به تشخیص‌های آتی، تا مدتی در دسته‌بندی‌ها دخیل کرد. این کار باعث می‌شود تا دقت تشخیص افزایش یابد. این بهبود در ابتدای فرآیند تشخیص که ممکن است تعداد آدرس‌های حمله بسیار محدود باشند، بیشتر جلوه می‌کند.

شکل ۳۳، نمودار جریان سیستمی که بر اساس روش ارائه شده کار می‌کند را نشان می‌دهد.



شکل ۳۳- نمودار جریان سیستمی که بر اساس روش ارائه شده کار می کند

فرآیند فوق روی ترافیکی که ترکیبی از حمله منع سرویس CAIDA و هجوم ناگهانی کاربران در ترافیک جام جهانی ۹۸ اعمال شده است. ازآنجایی‌که همه مهاجمین در حمله منع سرویس، به‌طور هم‌زمان ارسال ترافیک حمله را آغاز نمی‌کنند، این فرآیند به‌صورت مداوم و در لحظه، محاسبات موردنظر را انجام داده و به‌صورت تدریجی، حملات را کشف می‌کند. مدت زمان ترافیک، حدود ۳۰ دقیقه می‌باشد.

جدول ۱۰، عملکرد این روش و ارزیابی‌های موردنظر را نشان می‌دهد.

جدول ۱۰-ارزیابی نتایج حاصل از روش ارائه‌شده بر روی ترافیکی که شامل حملات منع سرویس و هجوم ناگهانی کاربران می‌باشد

زمان سپری‌شده از شروع حمله و هجوم ناگهانی برحسب ثانیه	تعداد آدرس‌های منحصربه‌فرد حمله	تعداد آدرس‌های منحصربه‌فرد هجوم ناگهانی کاربران	تعداد آدرس‌های حمله که درست تشخیص داده شده‌اند	تعداد آدرس‌های سالم که حمله تشخیص داده شده‌اند	دقت تشخیص (درصد)	بازخوانی (درصد)
100	76	214	21	0	100%	13%
200	129	321	24	0	100%	14%
400	131	465	35	0	100%	14%
600	134	641	35	6	85%	26%
800	177	3172	35	25	58%	19%
1000	182	3963	67	33	67%	36%
1200	182	4721	78	43	64%	42%
1400	183	4907	94	60	61%	51%
1600	1105	6876	252	169	59%	22%
1700	3704	7451	2319	220	91%	62%
1800	7708	8074	5166	294	95%	67%
1900	8122	8746	5413	302	95%	66%
2000	8666	9321	6257	311	95%	72%

با توجه به نتایج به‌دست‌آمده، روش ما در ۱۶۰۰ ثانیه ابتدایی، درصد بازخوانی کمی دارد و رفته‌رفته، دقت تشخیص آن کمتر می‌شود. اما بعد از ثانیه ۱۶۰۰ دقت تشخیص و بازخوانی تا حد زیادی بالا می‌رود. دلیل این امر را می‌توان با توجه به شکل‌های ۷ و ۸ توجیه کرد. تعداد آدرس‌های منحصربه‌فرد حمله در ۲۶ دقیقه اول (۱۶۰۰ ثانیه) بسیار کم می‌باشد. درحالی‌که تعداد آدرس‌های منحصربه‌فرد هجوم ناگهانی کاربران با نرخ زیادتری در حال افزایش است. به همین دلیل روش ما در ابتدا ضعیف عمل می‌کند و تعداد تشخیص‌های منفی نادرست و مثبت نادرست آن بالا می‌باشد. به عبارتی می‌توان گفت که حمله منع سرویس از دقیقه ۲۶ام به بعد آغاز می‌شود. بنابراین می‌توان گفت که روش ما با شروع حمله اصلی، عملکرد خوبی دارد و می‌تواند با دقت بالایی که نتایج آن در جدول ۱۰ موجود است، حملات منع سرویس و هجوم ناگهانی کاربران را از هم تشخیص دهد.

۴-۲-۱- معایب روش ارائه‌شده:

- با وجود اینکه دقت بازخوانی و تشخیص، با شروع حمله اصلی تا حد بسیار زیادی بهبود می‌یابند، اما بازهم این مقادیر با مقدار مطلوب فاصله دارند. همچنین، ازآنجایی‌که از الگوریتم خوشه‌بندی K-Means در این روش استفاده شده است، با هر بار اجرای الگوریتم ممکن است به جواب‌های مختلفی برسیم. درحالی‌که در تشخیص بی‌درنگ، فرصتی برای اجرای چندباره‌ی این روش وجود ندارد.

- در مراحل ابتدایی که تعداد آدرس‌های منحصربه‌فرد حمله بسیار کمتر از آدرس‌های هجوم ناگهانی کاربران باشند، محاسبه میزان فاصله Bhattacharya ممکن است باعث خطا در تشخیص دو جریان شود. ازاین‌رو در این مواقع ما خوشه بسیار کوچک‌تر را به‌عنوان حمله در نظر گرفته‌ایم. این فرض به این دلیل می‌باشد که در حمله منع سرویس توزیع‌شده، مهاجم معمولاً تعداد کمی سیستم آلوده به ربات در اختیار دارد [۷]. بنابراین با افزایش توانایی مهاجم در استفاده از آدرس‌های متنوع، ممکن است این روش کارایی لازم را نداشته باشد.

- این روش در صورتی قابل پیاده‌سازی است که کاربران منحصربه‌فرد، آدرس‌های منحصربه‌فردی داشته باشند. بنابراین اگر تعداد زیادی از کاربران از یک آدرس با استفاده از روش برگردان آدرس شبکه (NAT) استفاده کنند، ممکن است روش ارائه‌شده در تشخیص خود دچار اشتباه شود. به همین دلیل است که در بخش ارزیابی، روش مذکور بر روی ترافیک انتخاب واحد دانشگاه شریف که در آن تعداد زیادی از کاربران با استفاده از تنها یک آدرس اینترنتی، اقدام به دسترسی به سرویس‌دهنده کرده‌اند و تعداد آدرس‌های منحصربه‌فرد، بسیار محدود می‌باشد، آزمایش نشده است.

فصل ۵:

نتیجه‌گیری و کارهای آینده

۵-۱- نتیجه‌گیری و کارهای آینده

همان‌طور که در فصل قبل بررسی شد، روش ارائه‌شده ما توانایی تشخیص دو ترافیک مختلف حمله و منع سرویس را از یکدیگر، با استفاده از میزان فاصله توزیع زمانی بسته‌های متوالی در سطح کاربران را دارد. ایده این پژوهش این بود که بتوان با بررسی ویژگی‌های کاربران، دو جریان مختلف را حتی اگر با یکدیگر ترکیب شده باشند، تشخیص داد. برای این منظور، ابتدا ما ترافیک‌های مختلف را که ویژگی‌های متمایزی داشتند، از یکدیگر تفکیک کردیم. پس از تفکیک، با استفاده از روش‌هایی که در سطح جریان عمل می‌کنند، دو جریان را از یکدیگر تشخیص دادیم. نتایج ارزیابی‌ها نشان می‌دهد که روش ارائه‌شده ما تا حد زیادی می‌تواند دقیق عمل کند و ایده کلی این روش قابل اجرا می‌باشد. آنچه مهم است، نحوه پیاده‌سازی و فرآیند تشخیص است تا خطاهای موجود تا حد زیادی کاهش یابند و دقت و سرعت روش افزایش یابد.

آنچه در آینده مدنظر ماست، افزایش تعداد ویژگی‌های منحصربه‌فرد است. هرچه تعداد این ویژگی‌ها بیشتر باشد، الگوریتم خوشه‌بندی می‌تواند با دقت بیشتری خوشه‌بندی را انجام دهد که در این صورت خطای روش نیز تا حد زیادی کاهش خواهد یافت. مسئله بعدی تعیین پارامترهایی مانند زمان نمونه‌برداری از جریان، مدت زمان حفظ نتایج قبلی برای کمک به افزایش دقت نتایج آتی است. هرچه زمان نمونه‌برداری کاهش پیدا کند، سرعت کشف حملات افزایش می‌یابد. اما هم‌زمان ممکن است میزان خطا در تشخیص نیز افزایش یابد. بعلاوه همان‌طور که ذکر کردیم، می‌توان تعدادی از نمونه‌های حمله کشف‌شده را تا مدتی نگهداری کرد تا در مراحل بعد، دقت تشخیص افزایش یابد. البته باید در نظر داشت که زیاد بودن این مدت می‌تواند باعث افزایش خطا در تشخیص نیز بشود.

در این پژوهش سعی شده است تا از یکی از بهترین روش‌های خوشه‌بندی که کارایی آن نسبت به سایر روش‌های موجود بهتر می‌باشد، استفاده شود. اما باید این نکته را در نظر گرفت که در این الگوریتم،

نقاط مرکزی ابتدایی به‌صورت تصادفی انتخاب می‌شوند. ازاین‌رو در هر بار اجرای این الگوریتم، ممکن است نتایج به‌دست‌آمده با یکدیگر متفاوت باشند. ازاین‌رو روش‌هایی وجود دارند که این نقاط شروع ابتدایی را به بهترین شکل ممکن انتخاب می‌کنند. می‌توان با ترکیب این روش‌ها با الگوریتم خوشه‌بندی K-Means، خوشه‌بندی را به نحو بهتری انجام داد و به جواب دقیق‌تری رسید. ازاین‌رو یکی دیگر از کارهای آتی، می‌تواند بهینه‌سازی روش خوشه‌بندی باشد و افزایش دقت نتایج باشد.

به نظر می‌رسد می‌توان با رسیدن به این ویژگی‌ها، بتوان روشی ارائه کرد تا در برابر تغییرات روش‌های حمله، تا حد زیادی مطلوب عمل کند و پاسخگوی نیاز ما در تشخیص دقیق و کارای حملات منع سرویس توزیع‌شده از هجوم ناگهانی کاربران باشد.

مراجع

[1] J. Nazario, "Politically Motivated Denial of Service Attacks," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, IOSPress, 2009, pp. 163 - 181.

[2] L. Pau, "Business and social evaluation of denial of service attacks in view of scaling economic counter-measures," in *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP*, Osaka, Japan, April 2010.

[3] Oikonomou, G and Mirkovic, J, "Modeling Human Behavior for Defense Against Flash-Crowd Attacks," in *Communications, 2009. ICC '09. IEEE International Conference on*, Dresden, Germany, June 2009.

[4] T. Thapngam, Y. Shui, Z. Wanlei and B. Gleb, "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns," in *2011 IEEE Conference on*, Shanghai, China, April 2011.

[5] S. Yu, T. Theerasak, L. Jianwen, W. Su and Z. Wanlei, "Discriminating DDoS flows from flash crowds using information distance," in *Third International Conference on*, Gold Coast, Australia, October 2009.

[6] K. Li, Z. Wanlei, L. Ping, H. Jing and L. Jianwen, "Distinguishing DDoS attacks from flash crowds using probability metrics," in *Third International Conference on*, Gold Coast, Australia, October 2009.

[7] R. Abu, Moheeb, Z. Jay, M. Fabian and T. Andreas, "A multifaceted approach to understanding the botnet phenomenon," in *6th ACM SIGCOMM conference on Internet measurement*, Rio de Janeiro, Brazil, October 2007.

[8] A. Dhingra and M. Sachdeva, "Recent Flash Events: A Study," in *International Conference on Communication, Computing & Systems*, Firozpur, Punjab, India, August 2014.

[9] L. Zhen, Q. Liao and A. Striegel, "Botnet Economics: Uncertainty Matters," in *Managing Information Risk and the Economics of Security*, Springer US, 2009, pp. 245-267.

[10] J. Mirkovic and P. Reiher, "a taxonomy of DDoS attacks and defense mechanisms,"

ACM SIGCOMM Computer Communication Review, vol. 34, no. 2, pp. 39-53 , 2004.

[11] Y. Jie, L. Zhoujun, C. Huowang and C. Xiaoming, "A Detection and Offense Mechanism to Defend Against Application Layer DDoS Attacks," in *Networking and Services, 2007. ICNS. Third International Conference on*, Athens, Greece, June 2007.

[12] X. Yi and Y. Shun-zheng, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," *Networking, IEEE/ACM Transactions on,* vol. 17, no. 1, pp. 15 - 25, 2008.

[13] L. Arshadi and A. H. Jahangir, "On the TCP Flow Inter-arrival Times Dsitribution," in *Computer Modeling and Simulation (EMS), 2011 Fifth UKSim European Symposium on*, Madrid, Spain, November 2011.

[14] L. Khan, M. Awad and B. Thuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering," *The VLDB Journal,* vol. 16, no. 4, pp. 507-521, 2006.

[15] F. Y. S. Z. W. H. J. a. B. Yi, "Source-based filtering scheme against DDOS attacks," *International journal of database theory and application,* vol. 1, no. 1, pp. 9-20, 2008.

[16] L. Feinstein, D. Schnackenberg, R. Balupari and D. Kindred, "statistical approach to ddos attack detection and response," *DARPA Information Survivability Conference and Exposition,* vol. 1, pp. 303-314, 2003.

[17] L. Keunsoo, K. Juhyun, K. Ki Hoon, H. Younggoo and K. Sehun, "DDoS attack detection method using cluster analysis," *Expert Systems with Applications,* vol. 34, no. 3, p. 1659–1665, February 2007.

[18] "Distributed Denial of Service Attack and Defense," SpringerBriefs in Computer Science, 2014, pp. 31-53.

[19] L. Arshadi and A. H. Jahangir, "Entropy based SYN flooding detection," in *38th Annual IEEE Conference on Local Computer Networks*, Bonn, Germany, October 2011.

[20] Y. Tao and S. Yu, "DDoS Attack Detection at Local Area Networks Using Information Theoretical Metrics," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on* , Melbourne, Australia, 2013.

[21] Y. Hu, D.-M. Chiu and J. Lui, "Entropy Based Adaptive Flow Aggregation," *Networking, IEEE/ACM Transactions on*, vol. 17, no. 3, pp. 698 - 711 , 2009.

[22] A. Chonka, S. Jaipal and W. Zhou, "Chaos theory based detection against network mimicking DDoS attacks," *Communications Letters, IEEE*, vol. 13, no. 9, pp. 717 - 719, Sept 2009.

[23] Chen, Yonghong, M. Xinlei and W. Xinya, "DDoS detection algorithm based on preprocessing network traffic predicted method and chaos theory," *Communications Letters, IEEE,* vol. 17, no. 5, pp. 1052 - 1054, March 2013.

[24] A. Chonka, Z. Wanlei, S. Jaipal and X. Yang, "Detecting and tracing DDoS attacks by intelligent decision prototype," in *Pervasive Computing and Communications. Sixth Annual IEEE International Conference on*, Hong Kong, March 2008.

[25] L. Jin, L. Yong and G. Lin, "DDoS attack detection based on neural network," in *Aware Computing (ISAC), 2010 2nd International Symposium on*, Tainan, Taiwan, November 2010.

[26] L. Wei and A. A. Ghorbani , "Network anomaly detection based on wavelet analysis," *EURASIP Journal on Advances in Signal Processing - Special issue on signal processing applications in network intrusion detection systems,* vol. 2009, no. 4, Jan 2009.

[27] S. Bhatia, G. Mohay, A. Tickle and E. Ahmed, "Parametric Differences between a Real-world Distributed Denial-of-Service Attack and a Flash Event," in *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, Vienna, Austria, August 2011.

[28] P. Wendell and M. J. Freedman, "Going Viral: Flash Crowds in an open CDN," in

IMC '11 Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conferenc, Berlin, Germany, November 2011.

[29] I. Ari, B. Hong, E. Miller, S. Brandt and D. Long, "Managing flash crowds on the Internet," *Modeling, Analysis and Simulation of Computer Telecommunications Systems, 2003. MASCOTS 2003. 11th IEEE/ACM International Symposium on* , pp. 246 - 249 , 2003.

[30] N. Yoshida, "Dynamic CDN Against Flash Crowds," in *Content Delivery Networks*, Springer Berlin Heidelberg, 2008, pp. 275-296 .

[31] J. Jaeyeon, B. Krishnamurthy and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites," in *11th international conference on World Wide Web*, Hawaii, USA, May 2002.

[32] Isaac and Elizabeth, "Defending DDoS Attack using Stochastic Model based Puzzle Controller," *IJCSNS*, vol. 13, no. 4, pp. 100-105, 2003.

[33] A. Sardana, K. Kumar and R. Joshi, "Detection and Honeypot Based Redirection to Counter DDoS Attacks in ISP Domain," in *Information Assurance and Security, 2007. IAS 2007. Third International Symposium on*, Manchester, England, August 2007.

[34] W. E. Leland, M. S. Taqqu, W. Willinger and D. V. Wilson, "On the self-similar nature of Ethernet traffi," *IEEE/ACM Transactions on Networking (TON)*, vol. 2, no. 1, pp. 1-15, 1994.

[35] A. Erramilli, M. Roughan, D. Veitch and W. Willinger, "Self-similar traffic and network dynamics," *Proceedings of the IEEE*, vol. 90, no. 5, pp. 800 - 819, 2002.

[36] M. Crovella and A. Bestavros, "Self-similarity in World Wide Web traffic: evidence and possible causes," *Networking, IEEE/ACM Transactions on*, vol. 5, no. 6, pp. 835 - 846, 1997.

[37] Y. Shui, W. Zhou and R. Doss, "Information theory based detection against network behavior mimicking DDoS attacks," *Communications Letters*, vol. 12, no. 4, pp. 318-321, April 2008.

[38] Y. Shui, Z. Wanlei, J. Weijia, G. Song, X. Yong and T. Feilong, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 6, pp. 1073 - 1080, 2011.

[39] T. Swaroopa Rani, V. Sindhura, G. RamaKoteswara Rao and K. Pranathi, " Discerning Flooding Attack from Flash Crowd based on traffic patterns using entropy detection method," in *Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on* , Coimbatore, India , 2015.

[40] N. Jeyanthi and N. C. S. N. Iyengar, "An Entropy Based Approach to Detect and Distinguish DDoS Attacks from Flash Crowds in VoIP Networks," *International Journal of Network Security*, vol. 14, no. 5, pp. 257-269, 2012.

[41] I. t. archive, ACM SIGCOMM, [Online]. Available: http://ita.ee.lbl.gov/html/contrib/WorldCup.html. [Accessed 17 10 2014].

[42] CAIDA, "The CAIDA UCSD "DDoS Attack 2007" Dataset," [Online]. Available: http://www.caida.org/data/passive/ddos-20070804_dataset.xml. [Accessed 18 3 2015].

[43] R. G. Clegg, "A practical guide to measuring the Hurst parameter," *International Journal of Simulation: Systems, Science & Technology*, vol. 7, no. 2, pp. 3-14, 2006.

[44] T. Karagiannis and M. Faloutsos, "SELFIS: a tool for self-similarity and long-range dependence analysis," in *1st Workshop on Fractals and Self-Similarity in Data Mining: Issues and Approaches (in KDD)*, Edmonton, Canada, July 2002.

[45] T. Karagiannis, M. Faloutsos and M. Molle, "A user-friendly self-similarity analysis tool," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 3, pp. 81-93, 2003.

[46] M. Yun, Y. Rong, Y. Zhou, H.-A. Choi, J.-H. Kim, J. Sohn and H.-I. Choi, "Analysis of Uplink Traffic Characteristics and Impact on Performance in Mobile Data Networks," in *Communications, 2008. ICC '08. IEEE International Conference on*, Beijing, China, May 2008.

[47] C. Stolojescu, S. Moga, P. Lenca and A. Isar, "Long-range dependence in WiMAX

downlink traffic," in *Signals, Circuits and Systems (ISSCS), 2011 10th International Symposium on*, lasi, Romania , July 2011.

[48] Q. Meng and H. Khoo, "Self-Similar Characteristics of Vehicle Arrival Pattern on Highways," *Journal of Transportation Engineering*, vol. 135, no. 11, p. 864–872, 2009.

[49] J. Pan, H. Hu and Y. Liu, "Human behavior during Flash Crowd in web surfing," *Physica A: Statistical Mechanics and its Applications*, vol. 413, p. 212–219, 2014.

[50] H. Akaike, "A new look at the statistical model identification," *IEEE Transactions on Automatic Control* , vol. 19, no. 6, p. 716–723, 1974.

[51] M. Geva, A. Herzberg and Y. Gev, "Bandwidth Distributed Denial of Service: Attacks and Defenses," *Security & Privacy, IEEE*, vol. 12, no. 1, pp. 54 - 61, 2013.

[52] A. K. Jain and M. N. Murty, "Data clustering: a review," *ACM Computing Surveys (CSUR)*, vol. 31, no. 3, pp. 264-323 , 1999.

[53] A. Nagpal, A. Jatain and D. Gaur, "Review based on data clustering algorithms," in *Information & Communication Technologies (ICT), 2013 IEEE Conference on*, JeJu Island, South Korea, April 2013.

[54] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861-874, 2006.

Abstarct:

Distributed Denial of Service attacks are threats that target availability of network resources. One feature of this type of attacks is high volume of traffic or service request from huge number of illegitimate attackers that organize botnets together, which cause performance decrease of network. Nowadays, distinguishing huge number of legitimate users during Flash Crowd is one of the most challenging issues for network security experts. Most of proposed methods so far, did not have enough performance or were only applicable in short term, due to increasing attackers' knowledge in mimicking legitimate users behavior.

Methods based on extracting statistic features usually, have better performance, but mostly study statistical features of traffic flow on correlative level which is not effective when two different flows are combined together. In this thesis we propose a method that not only has all advantages of past methods in distinguishing different types of traffic (DDoS attack and flash crowd), but also discriminates them when they are combined together.

To achieve this goal our method studies features of flows at individual level. This thesis firstly discusses different features of attack traffic and Flash Crowd. It then compares users' behavior with DDoS attack bots. This comparison is about statistical features of packet inter arrival time of clients i.e. users in Flash Crowd and Bots in DDoS attack.

Finally, based on extracted features, and by using clustering methods, we distinguish attack flows from legitimate users. At last, the proposed method is evaluated and the recall, precision and other related metrics are measured.

Keywords:

DDoS Attacks, Flash Crowd, Clustering, Self similarity, Entropy

Sharif University of Technology

Department of Computer Engineering

M. Sc. Thesis

Distinguishing DDoS attacks from Flash Crowds

By:

Hadi Ranjbar

Supervisor:

Dr. Amir Hossein Jahangir

September 2015