

تشخیص حملات انکار سرویس توزیع شده با استفاده از سیستم خبره

علیرضا سعدآبادی *

بیبا امیرشاهی **

چکیده

حملات انکار سرویس به حملاتی اطلاق می شود که منابع سیستم از قبیل پردازشگر، پهنای باند شبکه، حافظه و ... را طوری مصرف می کنند که سیستم از ارائه سرویس به کاربران مجاز باز می ماند. حملات انکار سرویس توزیع شده حملات انکار سرویسی می باشند که به صورت گسترده و توسط چندین سیستم سازماندهی شده (باتنت ها) برای از کار انداختن سرویس دهنده ها به کار می روند. با اینکه بسیاری از کمپانی ها، سیستم های تشخیص حملات انکار سرویس توزیع شده متعددی را معرفی کرده اند، اما به دلیل اینکه الگوی این حملات روز به روز پیچیده تر شده است، پیش گویی حملات انکار سرویس توزیع شده با یک روشی که هزینه مناسبی داشته باشد همچنان مشکل است.

در این مقاله سعی شده است تا با بهره گیری از سیستم های خبره، روشی برای تشخیص حملات ارائه شود تا با در نظر گرفتن علائم حمله و تاریخچه حملات قبلی به تشخیص حمله بپردازد. مزیت این سیستم، آموزش از روی داده های قبلی و پویایی در مقابله با

* کارشناسی ارشد دانشگاه پیام نور، واحد ری، تهران. (نویسنده مسئول: alireza.sadabady@gmail.com)

** استادیار، گروه مهندسی کامپیوتر و فن آوری اطلاعات، دانشگاه پیام نور، تهران.

۶۴ مطالعات مدیریت فناوری اطلاعات، سال پنجم، شماره ۱۷، پاییز ۹۵

الگوهای حمله جدید است. در پایان به پیاده‌سازی روش توسط ویژوال استودیو پرداخته و مقادیر حاصل از سیستم را با نرم‌افزارهای شبیه‌ساز مقایسه می‌کنیم. **کلیدواژگان:** حملات انکار سرویس توزیع‌شده، باتنت، سیستم خبره، آنتروپی جریان، شبکه‌های بیزین، مقیاس بندی فازی.

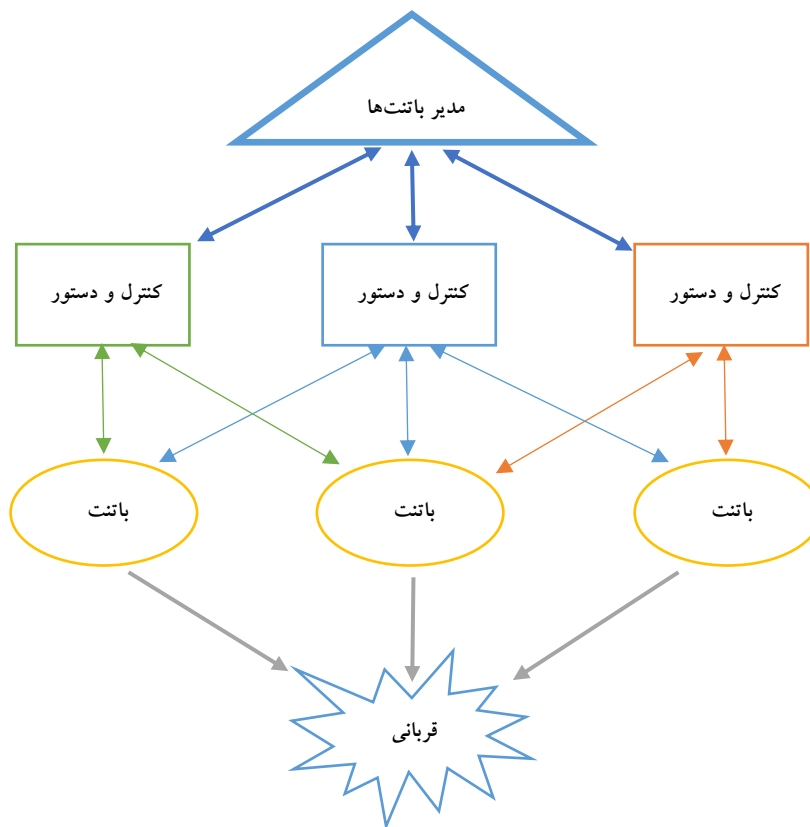
مقدمه

حملات انکار سرویس توزیع شده حملات انکار سرویسی می‌باشند که به صورت گسترده و توسط چندین سیستم سازمان‌دهی شده، برای از کار انداختن سرویس‌دهنده‌ها بکار می‌روند. در این‌گونه حملات، مهاجم به جهت انجام حمله، نیاز به شبکه‌ای از سیستم‌های متصل به اینترنت دارد. به سیستم‌هایی که بدون آگاهی کاربر آن‌ها بتوان از آن‌ها برای مقاصد مختلفی از جمله حملات انکار سرویس توزیع شده استفاده کرد بانت می‌گوییم در حقیقت باتنت‌ها ربات‌های شبکه‌ای هستند که به شکل زامبی گونه‌ای رفتار می‌نمایند. فردی که باتنت را کنترل می‌کند مدیر یا مالک باتنت می‌نامیم. مهاجم برنامه مخرب خود را روی یک یا تعدادی از سیستم‌های داخل شبکه نصب می‌کند و این سیستم‌ها را به سیستم کنترل و دستور تبدیل می‌کند. سپس از طریق این سیستم‌ها دستورات لازم را برای حمله به باتنت‌ها فرستاده و باتنت‌ها شروع به ارسال بسته‌های به صورت یک‌باره و سیل‌آسا به طرف سیستم قربانی می‌کنند. همان‌طور که در شکل (۱) مشخص است هر باتنت می‌تواند با چند سیستم کنترل و دستور در ارتباط باشد.

باتنت‌ها به دلایل متعددی مانند تغییر دائم آی‌پی و دامنه، داشتن سایزهای کاملاً تصادفی، تغییر دائم از حالت یک مهاجم به حالت یک سیستم عادی و بالعکس (آنچه از آن به عنوان زامبی یاد می‌شود) به سادگی قابل شناسایی نیستند. همچنین برنامه‌نویسان باتنت برای جلوگیری از تشخیص سیستم کنترل و دستور تعدادی گره واسط بین باتنت‌ها و سیستم کنترل دستور ایجاد کرده و به تغییر آدرس آی‌پی به صورت دوره‌ای (برای مثال هر هفته) می‌پردازند. علاوه بر این آن‌ها به رمزنگاری پیام‌های ردوبدل شده نیز اقدام می‌کنند.

بر اساس یک گزارش (یو^۱، ۲۰۱۴: ۲) حملات انکار سرویس در سال ۲۰۰۰ میلادی یک گیگابایت بر ثانیه بوده است و این حملات در سال ۲۰۰۷ به هفتاد گیگابایت بر ثانیه رسیده است، این در حالی است که حملات انکار سرویس در سال ۲۰۱۳ به رقم

نگران‌کننده ۳۰۰ گیگابایت بر ثانیه افزایش پیدا کرده است؛ بنابراین نرخ نمایی افزایش این حملات کاملاً نگران‌کننده است. مثال‌هایی از این حملات که اخیراً در سال ۲۰۱۲ نیز برای از کار انداختن پالایشگاه‌های پتروشیمی و انرژی هسته‌ای ایران توسط ایالت متحده و اسرائیل انجام گرفت استاکسنت و فلیم هستند. علاوه بر این، سیستم هدف حتی با داشتن سخت‌افزار قوی نیز می‌تواند تحت تأثیر قرار بگیرد زیرا عملکرد سرور هدف می‌تواند توسط محدود کردن ترافیک بین سرور و کلاینت‌ها و همچنین ایجاد ارتباط ضعیف مختل شود.



شکل ۱. ساختار یک حمله انکار سرویس توزیع شده توسط باتنت‌ها

تشخیص حملات انکار سرویس توزیع ... ۶۷

در این مقاله با استفاده از علائم تشخیص بانته‌ها، سنجش آنتروپی جریان (اندازه‌گیری عددی یک نتیجه غیرقطعی را آنتروپی می‌گویند)، ضریب همبستگی و احتمال حملات مشابه قبلی و با بهره‌گیری از استنتاج سیستم خبره، احتمال حمله را تشخیص می‌دهیم. ابتدا توسط شبکه‌های بیزین (به‌عنوان موتور استنتاج) روابط علت-معلولی بین علائم و حمله را مشخص نموده سپس با استفاده از جدول احتمالات پیشین و جدول احتمالات شرطی به محاسبه احتمالات پسین می‌پردازیم.

پیشینه تحقیق

الگوریتم کلونی مورچگان برای مقابله با حملات انکار سرویس توزیع شده در سال ۲۰۰۸ معرفی شد. حرکت مورچگان از لانه به سمت غذا و برعکس و جاگذاری فرمون باعث راهنمایی مابقی مورچه‌ها شده و در حقیقت مسیر موردنظر را برجسته‌تر می‌کند، این موضوع باعث می‌گردد مورچه‌های دیگری که در اطراف پرسه می‌زنند نیز با پیدا کردن این مسیر از آن استفاده کنند. در اینجا بایت عبوری از هر مسیریاب به‌عنوان فرمون در نظر گرفته می‌شود و مسیرهای برجسته‌تر ردگیری می‌گردد تا در نهایت گره مهاجم ردیابی گردد (لای و همکاران^۱، ۲۰۰۸، ۳۰۷۱). مشکل این روش این است که اگر حمله در گره‌های مجاور رخ دهد، تشخیص حمله دچار اختلال می‌گردد.

حمزه‌کلایی به بهبود الگوریتم کلونی مورچگان هساین لای پرداخته است. در این روش برخلاف روش هساین لای که گره جواب گره‌ای بود که بیشترین مورچه در آخر الگوریتم به آن همگرا شده است، گره جواب گره‌ای است که بیشترین تعداد مورچه‌ها در کل دفعات تکرار الگوریتم آن را به‌عنوان گره هدف معرفی کرده‌اند. این روش اگرچه مشکل روش آقای هساین لای را برطرف کرده است اما به دلیل طولانی‌تر کردن حلقه بیرونی الگوریتم، زمان جستجو را دو برابر کرده است که برای رفع این نقص فضای جستجو را کاهش داده است، به عبارتی تنها گره‌های با سطح جریان نزدیک به ماکزیمم

1. Lai et al.

مورد جستجو قرار می‌گیرند (حمزه‌کلایی و همکاران، ۱۳۹۲: ۷۷). این موضوع سبب می‌شود که الگوریتم از مجموعه‌ای از گره‌ها غافل گشته و این مهم خود می‌تواند آسیب‌پذیری جدی را در بر داشته باشد. چراکه ممکن است باتنت‌ها الگوریتم را دور بزنند.

پینزونا و همکاران یک معماری چند عامله توزیع‌شده را برای مسدود کردن پیام‌های سوپ‌ناهنجار در لایه شبکه ارائه کردند. آن‌ها از یک دسته‌بندی دومارحله‌ای استفاده کردند: ابتدا یک دسته‌بندی سریع با استفاده از درخت تصمیم ایجاد می‌کنند، سپس در مرحله دوم یک شبکه عصبی را پیاده‌سازی کردند که توسط درخواست‌های سالم و درخواست‌های ناهنجار مورد آزمایش قرار می‌گیرد (پینزونا و همکاران، ۲۰۱۱: ۵۴۸۶). این سیستم به دلیل نیاز به به‌روزرسانی دستی و آزمایش مجدد در عمل قابل‌استفاده نیست.

چویی و همکاران روشی را ارائه کردند که در آن با استفاده از پردازش نگاشت-کاهش به تشخیص سریع حملات انکار سرویس توزیع‌شده پروتکل انتقال ابرمتن در محیط ابری می‌پرداختند. چارچوب ارائه‌شده برای تشخیص حملات انکار سرویس توزیع‌شده شامل سه بخش است. اول، ماژول جمع‌آوری لاگ و بسته که به تجزیه کردن بسته‌های عبوری و لاگ وب‌سرورها می‌پردازد. دوم، ماژول تحلیل الگو که الگوهای برای تشخیص حمله تولید می‌کند؛ و در آخر، ماژول تشخیص که توسط مدل رفتاری نرمال به تشخیص حملات می‌پردازد (چویی و همکاران، ۲۰۱۴: ۱۶۹۸). روش آن‌ها برای تشخیص انواع حملات انکار سرویس توزیع‌شده جامعیت نداشته و برای تشخیص الگوهای مدرن‌تر آینده کارایی ندارد. تعیین حد آستانه به‌صورت دستی نیز از دیگر ایرادات وارده به روش آن‌ها است.

زو و همکاران روشی را پیشنهاد کردند که از یک بردار فرکانس بلادرنگ و ویژگی‌های

1. Pinzóna et al.

2. Choi et al.

تشخیص حملات انکار سرویس توزیع ... ۶۹

بلادرنگ ترافیکی به عنوان یک مجموعه مدل استفاده می‌کند. آن‌ها با سنجش آنروپی جریان حملات انکار سرویس توزیع شده به تشخیص حملات می‌پرداختند (زو و همکاران^۱، ۲۰۱۳: ۳۶). عیب روش آن‌ها ناتوانی در تمایز بین حملات و ترافیک‌های ناگهانی مجاز است.

یو روشی را ارائه کرده (یو، ۲۰۱۴: ۴۱) که در آن با استفاده از سنجش آنروپی جریان به شناسایی جریان‌های حمله می‌پردازد. یو همچنین برای برطرف کردن عیب روش زو (زو و همکاران، ۲۰۱۳: ۳۶) پارامتر ضریب همبستگی را ارائه کرده است که توسط آن می‌توان بین جریان حمله و ترافیک ناگهانی مجاز تفاوت قائل شد. روش یو به یک هماهنگی جهانی در زمینه سخت‌افزارهای شبکه نیازمند است، همچنین استفاده از این روش، هزینه بالای محاسباتی دارد که در همه‌جا مقرون به صرفه نیست.

مور و همکاران بر اساس تحلیل نحوه فعالیت به تشخیص این حملات پرداختند (مور و همکاران^۲، ۲۰۰۶: ۱۱۵) اما تشخیص بر پایه ویژگی می‌تواند به راحتی توسط برنامه‌نویسان باتنت دور زده شود.

روش پژوهش

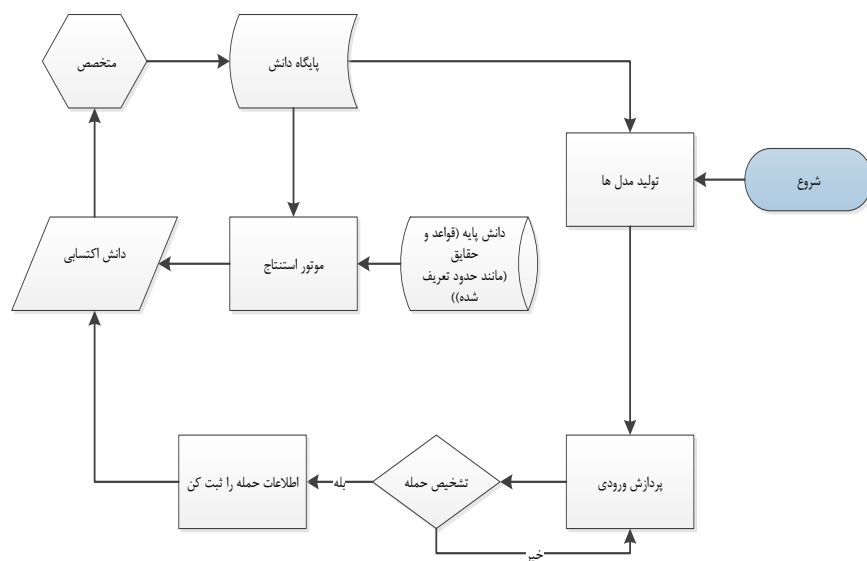
مزیت روش ما استفاده ترکیبی از سنجش آنروپی جریان، ضریب همبستگی، تکنیک‌های تشخیص باتنت‌ها و حملات مشابه قبلی است که این مهم با استفاده از استنتاج سیستم‌های خبره بسیار هوشمندانه و جامع‌تر عمل خواهد کرد. این درست است که سنجش آنروپی جریان و ضریب همبستگی دقیق‌ترین پارامترها برای تشخیص حمله می‌باشند (یو، ۲۰۱۴: ۴۱) اما ممکن است استفاده از آن‌ها در همه‌جا امکان‌پذیر نباشد (هماهنگی جهانی و سربر محاسباتی). از طرف دیگر تکنیک‌های باتنت‌ها ممکن است هر روز تغییر کنند. علاوه بر این، تشخیص باتنت‌ها همیشه دلیل بر حمله نیست، زیرا از

1. Zhou et al.
2. Moore

باتنت‌ها برای مقاصد دیگری نظیر ارسال اسپم نیز استفاده می‌شود؛ بنابراین بهترین راه‌حل استفاده ترکیبی از علائم بالا است. جهت دقیق‌تر کردن استنتاج تشخیص، از احتمال حملات مشابه قبلی نیز استفاده می‌شود. درنهایت با آموزش سیستم خبره و اکتساب دانش می‌توان روزبه‌روز بر دقیق‌تر عمل کردن سیستم افزود.

ساختار سیستم

همان‌طور که در شکل (۲) آمده است، سیستم پس از شروع به کار اقدام به تولید مدل از روی پایگاه دانش سیستم خبره می‌کند، سپس تا زمانی که حمله‌ای تشخیص داده نشود به پردازش ورودی بر اساس مدل تولید شده می‌پردازد. در صورتی که حمله‌ای تشخیص داده شود، اطلاعات حمله در بخش دانش اکتسابی سیستم خبره ثبت می‌شود. متخصص مربوطه پس از بررسی اطلاعات مربوط به حمله می‌تواند این اطلاعات را تأیید و یا رد نماید.



شکل ۲. ساختار کلی سیستم

تشریح عملکرد سیستم خبره

از پنج بخش اساسی تشکیل شده است: دانش پایه، پایگاه دانش، موتور استنتاج، دانش اکتسابی و رابط کاربری.

تجربه تشخیص حمله متخصصان این حوزه، تشکیل دهنده دانش این سیستم خبره است. این تجربه از علائم حملات، تشخیص نوع حمله و راه‌حل‌های مربوطه به دست آمده است.

دانش اکتسابی همیشه گلوگاه یک سیستم خبره در پیاده‌سازی بوده است و معمولاً به دو روش مستقیم و غیرمستقیم پیاده‌سازی می‌گردد. فرآیند روش غیرمستقیم به این شکل است که ابتدا خبرگان، دانش خود را در قالب شفاهی و یا کتبی بیان می‌کنند و سپس مهندسان دانش آن‌ها را تحلیل کرده و با یک قالب‌بندی خاص وارد پایگاه دانش می‌کنند. روش مستقیم به این شکل است که خود ماشین از داده‌ها و تخصص ارائه‌شده توسط خبرگان به یادگیری و کسب دانش می‌پردازد.

در این سیستم از هر دوی این روش‌ها استفاده شده است، روش غیرمستقیم به‌منظور توسعه امکانات کسب دانش و ساخت پایگاه دانش اولیه استفاده شده است که پس از آن متخصصان قادر خواهند بود تا دانش تشخیص حمله را به سیستم وارد کنند. دانش‌های دیگر مانند تاریخچه تشخیص حملات بعد از تصدیق شدن توسط متخصصین به پایگاه دانش اضافه خواهند گردید.

در این سیستم از استنتاج تشخیصی برای محاسبه احتمال بین علامت و نوع حمله استفاده شده است. ابتدا مهندس دانش علائم حمله، نوع حمله، قواعد و حقایق را وارد سیستم می‌کند. علائم حمله و نوع حمله به همراه احتمال رخ دادن علائم در جدولی نگهداری می‌گردد. احتمال رخ دادن هر علامت (علامت‌ها) را به‌عنوان احتمال پیشین از این جدول می‌خوانیم و پس از استنتاج البته با در نظر گرفتن علائم احتمالی دیگر و ارتباط بین علائم و همچنین نتایج قبلی که در جدول کارنامه حملات ثبت شده است، احتمال پسین را به دست آورده و حمله را در جدول دیگری ثبت می‌کنیم. رکوردهای

این جدول با استفاده از رابط کاربری و توسط متخصصان بررسی می‌گردد. در صورتی که تشخیص حمله درست باشد متخصص امر، آن را تصدیق می‌کند و در غیر این صورت آن را تکذیب می‌نماید. رکوردهای این جدول می‌توانند در نتیجه‌گیری‌های بعدی در نظر گرفته شوند. برای مثال تعداد حملات تصدیق شده و همچنین تعداد حملات تکذیب شده را برای تشخیص حملات بعدی که علامت مشابه دارند نیز در استنتاج شرکت دهیم. به عبارت ساده‌تر می‌توان گفت که هر رکورد ثبت شده دارای یک بیت پرچم است که می‌تواند توسط متخصص به مقدار صحیح یا غلط تنظیم شود. این بیت پرچم در صورت صحیح بودن به موتور استنتاج اطمینان از عملکرد صحیح را می‌دهد و در صورت غلط بودن موتور استنتاج را مجاب می‌کند تا در بهره‌برداری‌های بعدی از این اشتباه عبرت بگیرد.

همان‌طور که گفته شد، جدول علامت حمله و نوع حمله دارای احتمالی است. این احتمال می‌تواند در دوره‌های زمانی توسط ماشین استنتاج و از روی جدول کارنامه حملات، به‌روزرسانی گردد؛ بنابراین جدول مربوط به علائم حمله احتمالات پیشین ما را تشکیل می‌دهند و جدول حملات ثبت شده احتمالات پسین ما را تشکیل می‌دهند. جدول احتمال شرطی نیز به احتمال بین علائم و حمله مربوط می‌شود.

مابین علائم نیز می‌تواند روابط پدر-فرزندی وجود داشته باشد. برای مثال آنتروپی جریان پدر ضریب همبستگی است؛ بنابراین در تولید جدول احتمال شرطی اگر علامتی دارای پدر باشد آنگاه داریم:

اگر پدر صحیح باشد آنگاه

اگر فرزند صحیح باشد به احتمال X درصد حمله رخ داده است.

اگر فرزند غلط باشد به احتمال $1-X$ درصد حمله رخ داده است.

در ابتدای کار، احتمال رخ دادن هر علامت حمله را پنجاه درصد در نظر می‌گیریم. لازم به ذکر است که این احتمال می‌تواند توسط متخصصین امر و یا از طریق سیستم خبره به‌روزرسانی گردد.

ساختار شبکه بیزین

ممکن است این سؤال در ذهن خواننده مطرح شود که چرا از شبکه‌های بیزین یا شبکه‌های باور استفاده شده است؟

باید گفت که می‌توان از روش‌هایی نظیر شبکه‌های عصبی و نظریه مجموعه‌های ناهمگون و دارای ابهام بهره برد اما برخی از معایب این روش‌ها به شرح ذیل است: نیاز به حجم زیادی از داده‌های نمونه جهت آموزش. تفسیر بد نتایج تشخیص.

خوب عمل نکردن در مواجهه با روابط علت و معلولی.

این در حالی است که شبکه‌های بیزین توانایی بیان کردن موارد غیرقطعی را در یک ساختار منعطف دارند. در حقیقت این شبکه‌ها یک گراف جهت‌دار بدون دور می‌باشند که رأس‌های آن‌ها موارد غیرقطعی را نشان می‌دهد و لبه‌های آن‌ها احتمال مربوط بودن این موارد به یکدیگر را نشان می‌دهد. از طرف دیگر الگوریتم بیز از سایر الگوریتم‌های دیگر برای یادگیری مناسب‌تر است؛ زیرا برای آموزش دستگاه سریع‌تر عمل می‌کند.

با توجه به اینکه قواعد ما دارای احتمال می‌باشند از شبکه‌های بیزین برای جامه عمل پوشاندن به آن‌ها استفاده شده است. شکل (۳)، ارتباط بین علائم و همچنین ارتباط علائم با حمله انکار سرویس توزیع شده را نشان می‌دهد.

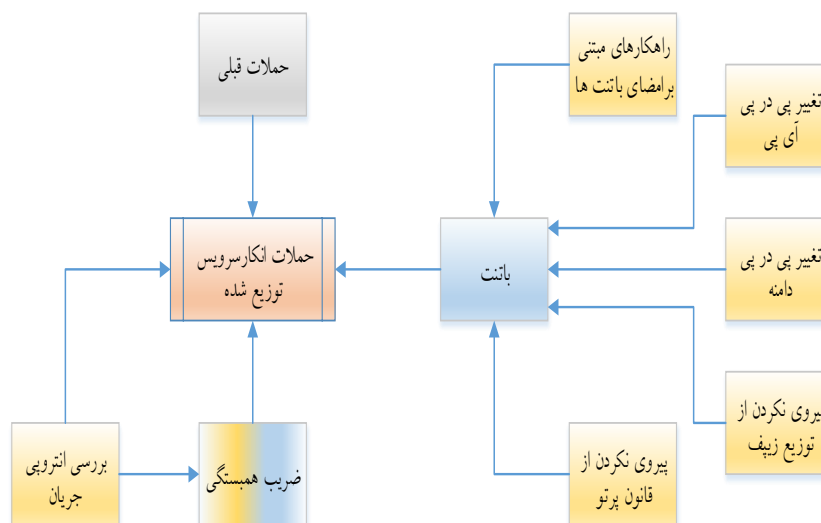
بر اساس تحقیقات صورت گرفته به این نتیجه رسیدیم که بهترین علائم برای تشخیص باتنت‌ها عبارت‌اند از:

راه کارهای مبتنی بر امضا: اگرچه باتنت‌ها هر روز از تکنیک‌های جدیدتری استفاده می‌کنند اما تحقیقات نشان می‌دهد الگوی اکثر حملات تکراری است.

تغییر پی‌درپی آی‌پی: این تکنیک و تکنیک بعدی به دلیل اینکه جدیدترین تکنیک‌های مورد استفاده برنامه‌نویسان باتنت‌ها می‌باشند در تشخیص باتنت‌ها در نظر گرفته می‌شوند (یو، ۲۰۱۴: ۱۶).

تغییر پی‌درپی دامنه.

پیروی نکردن از توزیع زیپف: یکی از راه‌های تشخیص باتنت‌ها پیروی نکردن آن‌ها از توزیع زیپف است (زی و همکاران، ۲۰۰۹: ۵۴).
 پیروی نکردن از قانون پرتو: باتنت‌ها از قانون پرتو پیروی نمی‌کنند (پاکسون و فلوید^۱، ۱۹۹۵: ۲۲۶؛ کروولا و بستاورس^۲، ۱۹۹۷: ۸۳۵).



شکل ۳. شبکه بیزین سیستم

همان‌طور که پیش‌تر نیز اشاره شد بهترین راه‌حل برای تشخیص حملات یک راه‌حل ترکیبی از تشخیص بر پایه ویژگی و تشخیص بر اساس آنتروپی جریان است. ترکیب دانش سیستم خبره با این راه‌حل ترکیبی به استنتاج و هوشمندی سیستم می‌انجامد. همان‌طور که در شکل مشاهده می‌شود علائم اولیه که می‌توانند توسط کاربر مشخص شده و یا از جدول احتمال پیشین استفاده نمایند با رنگ نارنجی، علائم میانی که احتمال آن‌ها با توجه به جدول احتمال شرطی و از روی علائم اولیه به دست می‌آیند با رنگی آبی و

1. Paxson and Floyd
 2. Crovella and Bestavros

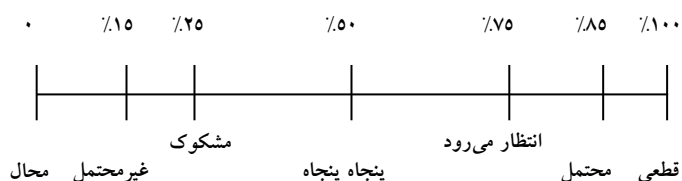
تشخیص حملات انکار سرویس توزیع ... ۷۵

حملات انجام شده قبلی که نیاز به محاسبه از روی جدول کارنامه حملات را دارند با رنگ خاکستری، مشخص شده‌اند. رنگ نارنجی-آبی مربوط به ضریب همبستگی به این معناست که این علامت هم متأثر از علامت آنتروپی جریان است و هم می‌تواند در صورت غیرمجاز بودن آنتروپی جریان توسط کاربر (و یا سنسورهای ورودی) تعیین گردد. با توجه به اینکه رابطه علت و معلولی بین علائم و حملات و دلایل به وجود آمدن آنها و دانش سیستم غیرقطعی است، قواعد تولید شده بایستی دارای احتمال باشند. این قواعد به صورت "اگر...آنگاه...به احتمال..." بیان می‌گردند برای مثال اگر قاعده‌ای به این شکل داشته باشیم: اگر وجود باتنت اثبات گردد آنگاه حمله انکار سرویس توزیع شده رخ داده است. [۰/۱۰]

به این معنی است که اگر وجود باتنت اثبات گردد آنگاه به احتمال ۱۰ درصد حمله انکار سرویس توزیع شده رخ داده است.

مقیاس بندی فازی

ایجاد جدول احتمال شرطی برای دانش تخصصی در کاربردهای واقعی به صورت غیردقیق بسیار مشکل است به عبارت دیگر نمی‌توان صرفاً یک عدد دقیق برای آن تعیین کرد. سخت‌ترین کار در ساختن شبکه‌های بیزین تبدیل این دانش تخصصی غیردقیق به احتمالات عددی است. در این سیستم توسط یک مقیاس بندی منطقی فازی که در شکل (۴) نشان داده شده است این دانش تخصصی غیردقیق را به احتمالات عددی تبدیل می‌کنیم.



شکل ۴. مقیاس بندی منطقی فازی

برای مثال می‌توان گفت زمانی که آنتروپی جریان از حدش تجاوز کرده است و ضریب همبستگی نیز نامعتبر است حتی اگر تشخیص باتنت‌ها نامشخص باشند و حمله‌ای با این علائم از قبل هم رخ نداده باشد آنگاه رخ دادن حمله محتمل است یعنی به احتمال ۸۵ درصد حمله رخ داده است.

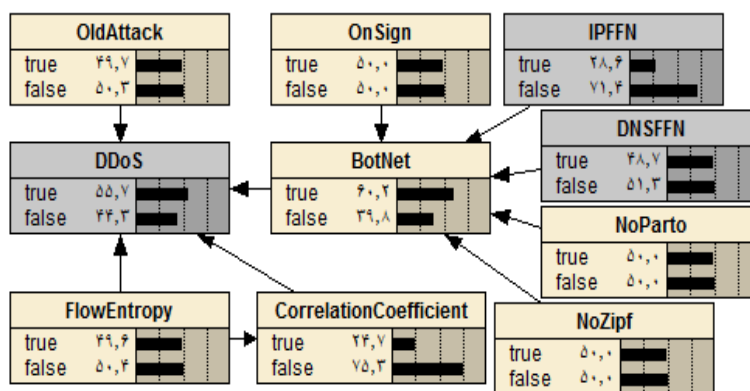
پیاده‌سازی سیستم

در این بخش شبکه بیزین مربوط به مقاله را توسط نرم‌افزار شبیه‌ساز نتیکا پیاده‌سازی نموده و پس از آن به پیاده‌سازی کامل سیستم توسط ویژوال استودیو ۲۰۱۵ و اس‌کیوال سرور ۲۰۱۴ می‌پردازیم.

در انتها خواهیم دید که نتایج به دست آمده از طریق نرم‌افزار نتیکا تقریباً با نتایج حاصل از سیستم تشخیص حملات انکار سرویس توزیع شده ما منطبق است.

پیاده‌سازی توسط نتیکا

در ابتدا گره‌ها و ارتباط‌های لازم را که در شکل (۳) نشان داده شده ایجاد می‌نماییم. شکل (۵) شبکه بیزین حاصل از نتیکا را نشان می‌دهد.



شکل ۵. شبکه بیزین سیستم در نرم‌افزار نتیکا

تشخیص حملات انکار سرویس توزیع ... ۷۷

بدیهی است که تمامی احتمالات از روی مطالعه و استنتاج شخصی در نظر گرفته شده است و با آموزش سیستم و به مرور زمان می‌تواند اصلاح گردد. لازم به ذکر است که این نرم‌افزار نمی‌تواند مانند یک سیستم خبره عمل نماید و تنها برای اثبات نتیجه حاصل از سیستم ما به کار برده شده است. جداول احتمالات را از روی علائم اولیه به طریق زیر مقداردهی می‌نماییم.

فرضیات جدول احتمال باتنت‌ها

تغییر پی‌درپی آی‌پی و تغییر پی‌درپی دامنه نمی‌توانند به صورت هم‌زمان مثبت باشند زیرا برنامه‌نویس باتنت یکی از این تکنیک‌ها را در آن واحد استفاده می‌کند؛ بنابراین احتمال مربوط به این سطرها x (از این طریق به نرم‌افزار نتیکا می‌فهمانیم که چنین چیزی نمی‌تواند اتفاق بیفتد) در نظر گرفته شده است.

تشخیص بر پایه ویژگی باتنت‌ها تأثیر ۴۰ درصدی بر روی تشخیص باتنت دارد؛ یعنی در صورتی که این علامت وجود داشته باشد آنگاه به احتمال ۴۰ درصد باتنت‌ها وارد عمل شده‌اند. تغییر پی‌درپی آی‌پی و تغییر پی‌درپی دامنه هر کدام ۴۰ درصد تأثیر دارند، البته فقط یکی از آن‌ها می‌تواند در آن واحد رخ دهد. پیروی نکردن از قانون پرتو و توزیع زیپف به ترتیب دارای تأثیر احتمالی ۵ و ۱۵ درصدی می‌باشند. بنابراین جدول احتمال شرطی باتنت‌ها به شکل (۶) است.

OnSign	IPFFN	DNSFFN	NoParto	NoZipf	true	false
true	true	true	true	true	x	x
true	true	true	true	false	x	x
true	true	true	false	true	x	x
true	true	true	false	false	x	x
true	true	false	true	true	۱۰۰	۰
true	true	false	true	false	۸۵	۱۵
true	true	false	false	true	۹۵	۵
true	true	false	false	false	۸۰	۲۰
true	false	true	true	true	۱۰۰	۰
true	false	true	true	false	۸۵	۱۵
true	false	true	false	true	۹۰	۱۰
true	false	true	false	false	۸۰	۲۰
true	false	false	true	true	۴۰	۴۰
true	false	false	true	false	۴۵	۵۵
true	false	false	false	true	۵۰	۵۰
true	false	false	false	false	۴۰	۴۰
false	true	true	true	true	x	x
false	true	true	true	false	x	x
false	true	true	false	true	x	x
false	true	true	false	false	x	x
false	true	false	true	true	۴۰	۴۰
false	true	false	true	false	۴۵	۵۵
false	true	false	false	true	۵۰	۵۰
false	true	false	false	false	۴۰	۴۰
false	false	true	true	true	۴۰	۴۰
false	false	true	true	false	۴۵	۵۵
false	false	true	false	true	۵۵	۴۵
false	false	true	false	false	۴۰	۴۰
false	false	false	true	true	۲۰	۸۰
false	false	false	true	false	۵	۹۵
false	false	false	false	true	۱۵	۸۵
false	false	false	false	false	۰	۱۰۰

شکل ۶. جدول احتمال شرطی باتنت‌ها

فرضیات جدول احتمال ضریب همبستگی

در صورتی که آنتروپی جریان از حدش تجاوز نکند آنگاه دیگر لازم نیست که ضریب همبستگی چک گردد. احتمال ۱۰۰ درصدی غلط به همین خاطر گنجانده شده است؛ و

تشخیص حملات انکار سرویس توزیع ... ۷۹

اگر آنتروپی از حدش تجاوز کرد آنگاه بایستی ضریب همبستگی چک گردد. احتمال ۵۰ درصدی هم برای این منظور قرار داده شده است. به دلیل محدودیت در نمایش شکل و همچنین تشابه جداول احتمال شرطی، از آوردن شکل جدول احتمال ضریب همبستگی و احتمال حمله خودداری نمودیم.

فرضیات احتمال حمله انکار سرویس توزیع شده

در صورتی که آنتروپی جریان از حدش تجاوز کند آنگاه به احتمال ۵۰ درصد احتمال دارد که حمله‌ای رخ داده باشد.

در سطرهایی که آنتروپی جریان از حدش تجاوز کرده است و همچنین ضریب همبستگی هم شرایطش برآورده شده است حداقل ۸۵ درصد احتمال حمله داریم. در این شرایط تأثیر احتمالی باتنت و حملات قبلی به ترتیب ۵ و ۱۰ درصد است. در سطرهایی که آنتروپی جریان از حدش تجاوز نکرده است، ضریب همبستگی نمی‌تواند مثبت باشد و بنابراین این سطرها x در نظر گرفته شده‌اند. در سطرهایی که آنتروپی جریان از حدش تجاوز کرده اما ضریب همبستگی منفی است تأثیر احتمالی آنتروپی جریان، حملات قبلی و باتنت به ترتیب ۵۰، ۳۰ و ۱۰ درصد در نظر گرفته شده است.

در نهایت در سطرهایی که آنتروپی جریان از حدش تجاوز نکرده و ضریب همبستگی هم منفی است تأثیر احتمالی حملات قبلی و باتنت به ترتیب ۵۰ و ۱۰ درصد در نظر گرفته شده است.

نکته: تمامی احتمالات مربوط به حمله انکار سرویس بر این اساس شکل گرفته است که "آنتروپی جریان‌های حمله یک روش مستقل از ویژگی حمله‌ها است و بر اساس تحقیقات صورت گرفته بهترین و دقیق‌ترین علامت برای تشخیص حملات سیل‌آسا است" بنابراین در صورت وجود و یا عدم وجود علامت آنتروپی تأثیر احتمالی حملات قبلی و باتنت دست‌خوش تغییرات می‌شوند. از طرف دیگر به دلیل این که در تمام موارد

نمی‌توان آن‌تروپی جریان و ضریب همبستگی را محاسبه نمود (هزینه مصرف منابع بالا نسبت به موارد دیگر و نیاز به سخت‌افزارهای جدید و سازگار برای محاسبه آن‌تروپی جریان و ضریب همبستگی) بر آن شدیم تا راه‌های دیگری نظیر تشخیص باتنت‌ها را در تشخیص حمله دخیل نماییم. بدیهی است که تمامی احتمالات فوق با آموزش سیستم و به‌مرور زمان می‌تواند اصلاح گردد.

پیاده‌سازی سیستم

برای پیاده‌سازی شبکه‌های بیزین در دات‌نت از چارچوبی به نام اینفردانت استفاده کرده‌ایم. اینفردانت الگوریتم‌های نوین انتقال پیام و روال‌های آماری مورد نیاز جهت انجام استنتاج بر روی مجموعه وسیعی از کاربردها را فراهم می‌کند. این چارچوب توسط محققان شرکت مایکروسافت توسعه داده شده است. اینفردانت دارای سه الگوریتم برای استنتاج است:

- Expectation Propagation
- Variational Message Passing
- Gibbs Sampling

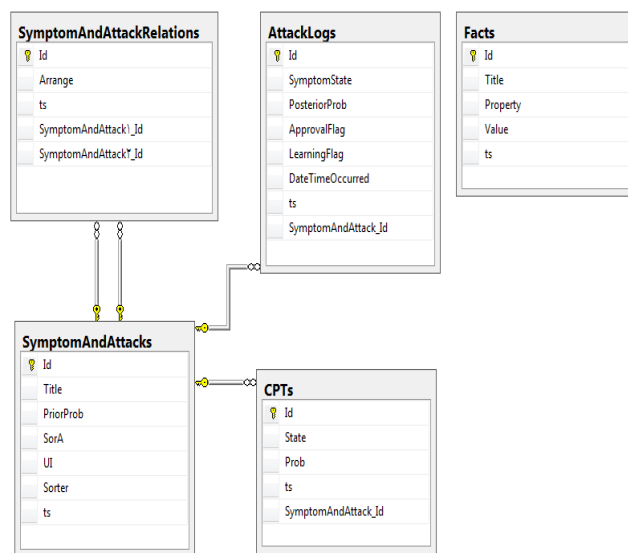
که ما از VMP استفاده کرده‌ایم زیرا توزیع را بر اساس پارامترها آموزش می‌دهد، نزدیک شدن به راه‌حل را تضمین می‌کند، راه‌حل یکسانی را برای زمان‌بندی و قالب‌بندی آغازین یکسان، تولید می‌کند.

پیاده‌سازی سیستم تولید مدل

از آنجاکه از فن‌آوری Entity Code First استفاده شده است تولید مدل می‌تواند به‌صورت کاملاً پویا انجام پذیرد. در واقع در صورتی که در آینده نیاز باشد که علائم دیگری با انواع حملات دیگری به سیستم اضافه شود، به راحتی امکان‌پذیر خواهد بود. تولید مدل فقط در اولین بار اجرا شدن پروژه صورت می‌گیرد و بازتولید مدل فقط زمانی انجام می‌پذیرد که تغییر ساختاری در مدل صورت گیرد.

تشخیص حملات انکار سرویس توزیع ... ۸۱

همان‌طور که در شکل (۷) مشاهده می‌کنید مدل ما از جداول زیر تشکیل شده است: علائم و حملات: علائم حمله و خود حمله در این جدول قرار گرفته (مدیریت بهتر و پویایی بیشتر) و با یک بیت از هم تمایز داده می‌شوند. این جدول حاوی احتمالات پیشین برای علائم اولیه است. علائم میانی و حملات، احتمال پیشین ندارند. ارتباط بین علائم و حملات: توسط این جدول ارتباط بین علائم میانی-علائم اولیه و همچنین ارتباط بین علائم و حملات را مشخص می‌نماییم.



شکل ۷. دیاگرام سیستم

جدول احتمالات شرطی: مقادیر مربوط به احتمالات شرطی حملات و علائم میانی در این جدول نگهداری می‌گردند. جدول کارنامه حملات: این جدول که در حقیقت همان جدول احتمالات پسین نیز است حاوی اطلاعات یک حمله از قبیل تاریخ، زمان، علائم حمله و ... است. جدول حقایق: شامل حقایق موجود در رابطه با باتنت‌ها، علائم حمله، حدود مورد نیاز و ... است.

پیاده‌سازی سیستم خبره

حال نوبت به آن رسیده است که به نحوه پیاده‌سازی سیستم خبره بپردازیم. همان‌طور که قبلاً نیز اشاره شد تولید مدل فقط در اولین بار اجرا شدن پروژه صورت می‌گیرد و بازتولید مدل فقط زمانی انجام می‌پذیرد که تغییر ساختاری در مدل صورت گیرد.

تشخیص حمله

با مشخص شدن علائم ورودی توسط کاربر (البته این علائم می‌توانند از طریق سنسورها مقداردهی شوند که نیاز به پیاده‌سازی سخت‌افزاری دارد) سیستم شروع به بازیابی اطلاعات حملات قبلی می‌کند که دارای علائم مشابه با حمله فعلی هستند. در صورتی که حمله و یا حملاتی با علائم مشابه رخ داده باشند آنگاه تعداد حملات درست تشخیص داده شده (حملات تشخیص داده شده قبلی که توسط متخصصان تأیید شده باشند) را از تعداد حملات تشخیص داده شده اشتباه قبلی کسر می‌کند. حاصل در یک ضریب که از جدول حقایق برداشته می‌شود و قابل به‌روزرسانی است گرفته می‌شود (مقدار پیش‌فرض یک درصد است). حاصل با آخرین احتمال درست تشخیص داده شده تجمیع می‌گردد؛ و اما اگر هیچ حمله‌ای با علائم مشابه در سیستم رخ نداده باشد آنگاه سیستم احتمال رخ دادن حملات قبلی مشابه را پنجاه درصد در نظر می‌گیرد زیرا ممکن است این حمله در دنیای واقعی رخ داده باشد.

نکته: در صورتی که احتمال حملات قبلی این‌قدر تأیید شده باشد که به بیشتر از صد درصد برسد مقدار آن را همان صد درصد در نظر می‌گیریم. همچنین در صورتی که احتمال حملات قبلی این‌قدر تکذیب شده باشد که احتمال آن منفی شده باشد احتمال آن را صفر در نظر می‌گیریم.

احتمال رخ دادن علائم اولیه در صورت مشخص نبودن به‌صورت پیش‌فرض پنجاه درصد در نظر گرفته می‌شود که البته این مقدار از طریق آموزش سیستم (جلوتر به آن خواهیم رسید) قابل به‌روزرسانی است. در صورتی که علامت اولیه‌ای نامعتبر باشد مقدار آن را

تشخیص حملات انکار سرویس توزیع ... ۸۳

صد درصد در نظر گرفته و اگر معتبر باشد مقدار آن را صفر درصد در نظر می‌گیریم. برنامه‌نویس باتنت در آن واحد فقط از یکی از تکنیک‌های تغییر پی‌درپی آی‌پی و یا دامنه استفاده می‌کند (یو، ۲۰۱۴: ۱۶)؛ بنابراین این موضوع را توسط نرم‌افزار واسط کنترل می‌کنیم تا در صورتی که مثبت بودن علامت یکی از دو مورد، علامت دیگری منفی گردد. ضریب همبستگی فقط در صورتی که می‌تواند معتبر و یا نامعتبر باشد که آن‌تروپی جریان از حدش تجاوز کرده باشد (نامعتبر باشد) این موضوع نیز در رابط کاربری گنجانده شده است. جدول احتمال شرطی مربوط به ضریب همبستگی نیز فقط زمانی تشکیل می‌گردد که دارای مقدار نامشخص باشد.

سیستم توسط احتمال پیشین علائم حمله و محاسباتی که بر روی حملات مشابه قبلی انجام داده است به استنتاج در رابطه با حمله پرداخته و نتیجه را در کارنامه حمله (به‌عنوان تاریخچه حمله) ثبت می‌کند. نتیجه ثبت‌شده دارای پرچم تأیید نشده است و بایستی توسط متخصصان تأیید شود.

در انتها سیستم به ارائه اطلاعات آماری از حملات مشابه قبلی نظیر بیشینه و کمینه احتمال حملات درست تشخیص داده شده، تعداد تشخیص صحیح و اشتباه و همچنین تاریخ و زمان حملات می‌پردازد.

شکل (۸) نمایی از رابط کاربری سیستم تشخیص است. آخرین رکورد جدول نشان‌دهنده اولین حمله تشخیص داده شده با علائم نامشخص است که احتمال را ۵۷/۵ درصد محاسبه کرده است. به دلیل تکذیب تشخیص، رکورد بعدی دارای احتمال ۵۷ درصدی است که در حقیقت نیم درصد احتمال حمله را به دلیل تکذیب متخصصان پایین آورده است. رکورد بعدی دارای احتمال ۶۰ درصد است که در حقیقت به دلیل تأیید تشخیص رکورد قبلی ۳ درصد افزایش پیدا کرده است.

سیستم تشخیص حملات انکار سرویس توزیع شده

علامت ها

	نامشخص	راهکارهای مبتنی بر امنیتی بافت ها:
نامشخص	نامشخص	شبکه های تغییر روی آبی آی آی:
نامشخص	نامشخص	پیروی کردن از قانون پارتو:
نامشخص	نامشخص	بررسی آنتروپی جریان:

گزارش حمله

احتمال حمله: 0.607

تاریخچه تشخیص حمله با علائم مشابه

	2	تعداد تشخیص داده شده:
4	2	تعداد تشخیص اشتباه:
0.5712	0.6026	پیشینه احتمال درست تشخیص داده شده:
0.5712	0.6026	کمینه احتمال درست تشخیص داده شده:

تاریخ و زمان	احتمال حمله	پرچم آبی
04/02/2016 04:08:24 پ.ظ	0.6109	<input type="checkbox"/>
04/02/2016 04:07:12 پ.ظ	0.6148	<input type="checkbox"/>
04/02/2016 04:06:42 پ.ظ	0.6187	<input type="checkbox"/>
04/02/2016 04:06:22 پ.ظ	0.6026	<input checked="" type="checkbox"/>
04/02/2016 03:57:25 پ.ظ	0.5712	<input checked="" type="checkbox"/>
04/02/2016 04:17:40 ق.ظ	0.575	<input type="checkbox"/>

شکل ۸. نمایی از رابط کاربری سیستم

هر یک از علائم دارای سه حالت می باشند:

نامشخص: در این صورت احتمال حمله از روی استنتاج اطلاعات قبلی سیستم گرفته می شود.

نامعتبر: به این معنی است که علامت مربوطه رخ داده است.

تشخیص حملات انکار سرویس توزیع ... ۸۵

معتبر: یعنی علامت مربوطه رخ نداده است.

تأیید و تکذیب تشخیص توسط متخصصان

همان‌طور که در شکل (۹) نشان داده شده است در رابط کاربری صفحه‌ای گنجانده شده است تا متخصصان بتوانند از طریق آن حملات تشخیص داده‌شده را تأیید نمایند. متخصصان می‌توانند در این صفحه با مشاهده نوع حمله، وضعیت علائم، تاریخ، زمان و احتمال تشخیص داده‌شده، در رابطه با تأیید تشخیص، تصمیمات لازم را بگیرند. بدیهی است که رکوردهایی که تأیید نشوند به‌صورت پیش‌فرض تکذیب شده در نظر گرفته می‌شوند.

سیستم تشخیص حملات انکار سرویس توزیع شده

تأیید و یا تکذیب تشخیص حملات

شماره حمله	تاریخ و زمان	احتمال	وضعیت علامت	شماره لاگ	برچسب آموزش	برچسب تأیید	وضعیت
9	04-09-25 2016/04/02 ب.ظ	0.607	2222222	9	<input type="checkbox"/>	<input type="checkbox"/>	ویرایش حذف
9	04-08-24 2016/04/02 ب.ظ	0.6109	2222222	8	<input type="checkbox"/>	<input type="checkbox"/>	ویرایش حذف
9	04-07-12 2016/04/02 ب.ظ	0.6148	2222222	7	<input type="checkbox"/>	<input type="checkbox"/>	ویرایش حذف
9	04-07-03 2016/04/02 ب.ظ	0.7337	2222201	6	<input type="checkbox"/>	<input type="checkbox"/>	ویرایش حذف
9	04-06-42 2016/04/02 ب.ظ	0.6187	2222222	5	<input type="checkbox"/>	<input type="checkbox"/>	ویرایش حذف
9	04-06-22 2016/04/02 ب.ظ	0.6026	2222222	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ویرایش حذف
9	03-57:25 2016/04/02 ب.ظ	0.5712	2222222	3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ویرایش حذف
9	03-57:10 2016/04/02 ب.ظ	0.287	2222211	2	<input type="checkbox"/>	<input type="checkbox"/>	ویرایش حذف
9	11:17:40 2016/04/02 ق.ظ	0.575	2222222	1	<input type="checkbox"/>	<input type="checkbox"/>	ویرایش حذف

شکل ۹. بخش تأیید و یا تکذیب تشخیص حملات

آموزش سیستم

به دو بخش تقسیم می‌شود. آموزش جدول احتمالات پیشین که مربوط به علائم اولیه می‌گردد. آموزش جدول احتمالات شرطی.

آموزش جدول احتمالات پیشین

ابتدا رکوردهایی از کارنامه حملات که در آموزش سیستم مشارکتی نداشته‌اند در قالب فهرستی از پایگاه داده گرفته می‌شوند (لیست اول). سپس فهرستی از علائم اولیه که توسط ستون "مرتب کننده" مرتب می‌گردد، تهیه می‌شود (لیست دوم). در مرحله بعد وضعیت علائم در لیست اول را از سمت چپ به راست به ترتیب مورد بررسی قرار می‌دهیم. در صورتی که علامت موردنظر نامشخص باشد (مقدار آن ۲ باشد) آنگاه در آموزش سیستم نقشی نخواهد داشت در غیر این صورت دو حالت وجود دارد. حالت اول نامعتبر بودن علامت است و حالت دوم معتبر بودن آن است. هر یک از حالت‌ها نیز می‌توانند تأیید شده و یا تکذیب شده باشند. هنگامی که علامتی نامعتبر باشد و تشخیص حمله نیز تأیید شده باشد و یا علامتی معتبر بوده و تشخیص حمله نیز تکذیب شده باشد از آن به‌عنوان یک فاکتور مثبت در رابطه با علامت حمله استفاده می‌گردد. برعکس هنگامی که علامتی نامعتبر باشد و تشخیص حمله تکذیب شده باشد و یا علامتی معتبر بوده و تشخیص حمله نیز تأیید شده باشد از آن به‌عنوان یک فاکتور منفی در رابطه با علامت حمله استفاده می‌گردد. فاکتورهای مثبت و منفی تجمیع گردیده و در ضریبی که از جدول حقایق خوانده می‌شود و دارای مقدار پیش‌فرض یک درصد است (که البته قابل به‌روزرسانی است) ضرب می‌شود و با احتمال پیشین قبلی علامت موردنظر تجمیع می‌گردد. منطق این آموزش در این است که اگر علامتی معتبر باشد و حمله هم تکذیب شده باشد و یا اگر علامتی نامعتبر باشد و حمله هم تأیید شود بنابراین می‌توان گفت که این علامت نقش مؤثرتری را باید ایفا کند و در غیر این صورت باید از نقش این علامت در تشخیص حمله کاست.

تشخیص حملات انکار سرویس توزیع ... ۸۷

در پایان، سیستم تمامی رکوردهایی که در آموزش شرکت داده شده‌اند را توسط پرچم آموزش مشخص می‌کند و جدول احتمال پیشین را قبل و بعد از آموزش به کاربر نشان می‌دهد.

آموزش جدول احتمالات شرطی

در ابتدا احتمالات شرطی را در قالب یک لیست ترتیبی از پایگاه داده می‌گیریم سپس برای هر حالت موجود در لیست به جستجو در کارنامه حملات می‌پردازیم، رکوردهایی که با یک حالت تطابق دارند را فیلتر کرده و بر اساس تائید و تکذیب تشخیص جدا می‌نماییم. تائید را به‌عنوان فاکتور مثبت و تکذیب را به‌عنوان فاکتور منفی در نظر گرفته و پس از تجمیع در یک درصد (مقدار پیش‌فرض که قابل به‌روزرسانی است) ضرب می‌نماییم. سپس نتیجه را با احتمال قبلی تجمیع می‌نماییم.

بدیهی است که با این روش دیگر علائمی که دارای مقدار ۲ در پنج رقم اول کد ترنری وضعیت علامت خود می‌باشند دیگر در نظر گرفته نمی‌شوند.

برای مثال همان‌طور که در کارنامه حملات فرضی شکل (۱۰) مشاهده می‌شود:

حمله انکار سرویس توزیع شده دو بار با علائم زیر صورت گرفته است.

راه کارهای مبتنی بر امضا = نامعتبر

تغییر پی‌درپی آی‌پی = نامعتبر

تغییر پی‌درپی دامنه = معتبر

پیروی کردن از قانون پرتو = خیر

پیروی کردن از توزیع زیپف = خیر

آنتروپی جریان = نامشخص

ضریب همبستگی = نامشخص

سیستم تشخیص حملات انکار سرویس توزیع شده

تایید و یا تکذیب تشخیص حملات

شناسه حمله	تاریخ و زمان	احتمال	وضعیت علام	شناسه لاگ	برچسب آموزش	برچسب تایید	برچسب حذف
9	03:43:46 2016/04/03	0.5965	0010022	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	03:43:17 2016/04/03	0.6	0010022	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

شکل ۱۰. یک کارنامه فرضی از حملات

پنج رقم اول مربوط به باتنت‌ها می‌باشند، به دلیل اینکه منطق فهرست‌های کشویی مربوط به رابط کاربری برعکس منطق مربوط به جدول احتمالات شرطی است (برای درک راحت‌تر کاربر در انتخاب مقادیر صحیح) بنابراین پنج رقم اول که ۰۰۱۰۰ است را ابتدا به ۱۱۰۱۱ تبدیل کرده که معادل دسیمال آن برابر عدد ۲۷ می‌گردد. هردوی این حملات تکذیب شده‌اند؛ بنابراین سیستم بایستی در آموزش جدول احتمالات شرطی در حالت ۲۷ مربوط به باتنت‌ها ۲ درصد از احتمال شرطی قبلی کسر نماید.

به‌روزرسانی دستی مقادیر توسط متخصصان

در این سیستم امکانی فراهم شده است تا در صورت لزوم، متخصصان بتوانند به ویرایش رکوردهای موجود در جدول احتمالات شرطی، جدول احتمالات پیشین و جدول حقایق بپردازند.

مقایسه موردی

برای این‌که به صحت و سقم نتیجه سیستم تشخیص حملات انکار سرویس توزیع شده پی ببریم، برآن شدیم تا نتایج حاصل از سیستم را با نرم‌افزار نتیکا و در شرایط یکسان مقایسه کنیم. برای برقراری شرایط یکسان باید سیستم تشخیص را طوری تغییر دهیم تا احتمال حملات قبلی را پیوسته پنجاه درصد در نظر بگیرد و از محاسبه احتمال حملات قبلی و آموزش خود صرف‌نظر کند؛ زیرا نرم‌افزار نتیکا نمی‌تواند مانند یک سیستم خبره عمل کند.

تشخیص حملات انکار سرویس توزیع ... ۸۹

مثال اول: علامت تغییر پی‌درپی آی‌پی نامعتبر بوده و تغییر پی‌درپی دامنه معتبر است. مابقی علائم نامشخص می‌باشند. احتمال تشخیص حمله توسط نرم‌افزار نیتیکا ۵۷/۳ درصد است و احتمال تشخیص حمله توسط سیستم ما برابر ۵۸/۱ درصد است. اختلاف بین دو سیستم کمتر از یک درصد است که به دلیل تفاوت در الگوریتم استنتاج است. مثال دوم: تغییر پی‌درپی آی‌پی نامعتبر، تغییر پی‌درپی دامنه معتبر، راه‌کارهای مبتنی بر امضا نامعتبر و تغییرات آنروپی جریان نامعتبر و مابقی علائم نامشخص می‌باشند. تقریباً هر دو سیستم مقدار ۸۴ درصد را به دست آورده‌اند. مثال سوم: تغییر پی‌درپی آی‌پی معتبر، تغییر پی‌درپی دامنه نامعتبر، توزیع زیپف نامعتبر، قانون پرتو نامعتبر، تغییرات آنروپی جریان نامعتبر، ضریب همبستگی نامعتبر و مابقی علائم نامشخص می‌باشند. هر دو سیستم دقیقاً مقدار ۹۴ درصد را به دست آورده‌اند. بنابراین بر اساس سه مثال تصادفی فوق می‌توان گفت سیستم تشخیص حملات انکار سرویس توزیع شده ما به درستی کار می‌کند.

نتیجه‌گیری

حملات انکار سرویس توزیع شده هنوز هم وجود دارند و در آینده نیز وجود خواهند داشت چراکه این حملات جز جدانشدنی فضای سایبری هستند. به دلیل ماهیت فضای سایبری، حملات انکار سرویس توزیع شده و دفاع در برابر آن‌ها یک نزاع تمام‌نشدنی میان مهاجمان و مدافعان است. هر بار که مدافعان یک روش دفاعی طراحی می‌کنند از آن طرف مهاجمان سعی در اختراع راهبرد یا روش جدید برای نفوذ به سیستم دفاعی جدید می‌کنند و برعکس.

در این مقاله سعی شد تا با الهام گرفتن از روش‌ها و تکنیک‌های جدید و موفق موجود در مقاله‌ها و کتب معتبر دیگر و ترکیب آن‌ها سیستمی ارائه شود که با بهره‌گیری از سیستم خبره به منظور آموزش و استنتاج به تشخیص حملات انکار سرویس توزیع شده بپردازد. از مزایای سیستم ارائه شده می‌توان به موارد زیر اشاره نمود:

آموزش و به‌روزرسانی خودکار سیستم از طریق سیستم خبره. قابلیت نصب سیستم بر روی انواع سیستم‌عامل‌ها و ماشین‌های مجازی. قابلیت تغییر مدل با تغییر تکنیک‌ها و علائم حملات. قابلیت تخمین احتمال حمله برای علائم نامشخص با استفاده از قوه استنتاج. به نظر می‌رسد که تنها عیب سیستم هزینه‌های پردازشی آن است که به‌واسطه مضراتی که حملات انکار سرویس توزیع شده ایجاد می‌کنند قابل اغماض است. توجه به این مهم ضروری است که حتی اگر یک سیستم دفاعی به حدی از بلوغ برسد که نفوذ به آن امکان‌پذیر نباشد بازهم با ظهور فن‌آوری‌های جدید ممکن است از پا در بیاید. برای مثال رایانش ابری با قدرتی که می‌تواند در زمینه محاسبات تولید کند قادر به پیدا کردن کلیدهای بزرگ، الگوریتم‌های رمزنگاری پیچیده در کسری از زمان است. علاوه بر این، با ظهور هر فن‌آوری جدید نمی‌توان تمامی نقاط آسیب‌پذیر آن را به‌سرعت کشف و یا حتی پیشگویی کرد.

مشکل بزرگی که با آن روبرو هستیم عدم شناخت صحیح فضای سایبری است. برای برطرف کردن مشکلات امنیتی فضای سایبری بایستی فهم بهتر و عمیق‌تری نسبت به آن پیدا کنیم. به‌عنوان نشانه‌ای از این مورد می‌توان به مجلس تحقیقات آمریکا اشاره کرد که به‌تازگی تحقیقی را بر روی دانش شبکه آغاز کرده‌اند^۱. علاوه بر این، همان‌طور که اینترنت و وب روزبه‌روز عظیم‌تر و پیچیده‌تر می‌گردند، ما با چالش‌های بیشتری در فهم این شبکه‌های عظیم، مواجه می‌شویم. یکی از مسائل ضروری که با آن مواجه هستیم این است که هنوز هم یک تئوری بنیادین امکان‌پذیر برای شبکه‌ها نداریم. این موضوع به‌طور عادی توسط جامعه شبکه پذیرفته شده است که ما برای شبکه کمبود تئوری داریم. اگرچه ابزارهای تئوری مختلفی برای مسائل خاص ارائه شده است اما این ابزار معمولاً در یک بازه محدود مؤثر واقع می‌شوند. ابزار اصلی برای شبکه، تئوری گراف و تئوری صف است. این تئوری‌ها نیز در سطح وسیعی توسعه داده شده‌اند، اما تمامی این توسعه‌ها

1. <http://www.nap.edu/catalog/11516.html>

از هدف نهایی دور می‌باشند (یو، ۲۰۱۴: ۲۴).

اگر به سرعت به تاریخچه علم نگاهی بیندازیم، خواهیم فهمید که همیشه قبل از این که بشر واقعاً بخواهد شروع به کاری بکند، ابزارهای ریاضی لازم برای او فراهم بوده است. برای مثال، زمانی که آلبرت انیشتین از هندسه دیفرانسیل در کارهایش استفاده می‌کرد هندسه دیفرانسیل کاملاً به بلوغ خود رسیده بود. در نتیجه، بایستی دلگرم باشیم که ابزارهای ریاضی از قبل برای ما وجود دارند تا بتوانیم با استفاده از آنها، وب، اینترنت و شبکه‌های پیچیده را مدل کنیم. وظیفه ما درک عمیق این ابزار ریاضی و به‌کاربردن آنها در مسائل علوم کامپیوتر است. در صورت لزوم می‌توان حتی ابزار ریاضی جدیدی را برای حل مشکل اختراع کرد.

منابع

- حمزه کلایی. م.ح، شامانی. م.ر، شامانی. م.ج، (۱۳۹۲)، بهینه کردن الگوریتم کلونی مورچگان برای ردیابی آی پی حملات انکار سرویس، *مجله عملی - پژوهشی پدافند الکترونیکی و سایبری*، ۴، ۷۷-۸۶.
- Choi.Junho, Choi.Chang, Ko.Byeongkyu, Kim.Pankoo, (2014), A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment, *Soft Computing*, 18, 9, 1697-1703.
- Crovella. M. E, Bestavros. A, (1997), *Self-similarity in world wide web traffic: evidence and possible causes*, *IEEE/ACM Transactions on Networking*, vol. 5, no. 6, pp. 835-846.
- Hsin Lai. G, Chen. C.M, Jeng. B.Ch, Chao. W, (2008), *Ant-based IP traceback*, *Expert Systems with Applications*, 34, 4, 3071-3080.
- Moore. D, Shannon. C, Brown. D. J, Voelker. G. M, Savage. S, (2006), *Inferring internet denialof-service activity*, *ACM Transactions on Computer Systems*, vol. 24, no. 2, pp. 115-139.
- Paxson. V, Floyd. S, (1995), *Wide area traffic: the failure of poisson modeling*, *IEEE/ACM Transactions on Networking*, vol. 3, no. 3, pp. 226-244.
- Pinzóna. Cristian I, Bajob. Javier, Pazb. Juan F. De, Corchadob. Juan M, (2011), S-MAS: An adaptive hierarchical distributed multi-agent architecture for blocking malicious SOAP messages within Web Services environments, *Expert Systems with Applications*, 38, 5, 5486-5499.
- Xie. Y, Yu. S. Z, (2009), *A large-scale hidden semi-markov model for anomaly detection on user browsing behaviors*, *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 54-65.
- Yu. Shui, (2014), *Distributed Denial of Service Attack and Defense*, *SpringerBriefs in Computer Science*.
- Zhou.Wei, Jia.Weijia, Wen.Sheng, Xiang.Yang, Zhou.Waniei, (2013), Detection and defense of application-layer DDoS attacks in backbone web traffic, *Future Generation Computer Systems*, 38, 36-46.