علوم و مهندسی کامپیوتر
نشریه علمی پژوهشی انجمن کامپیوتر ایران
مجلد ۱۱، شماره ۳ (الف)، ۱۳۹۲
صفحات ۱-۹
مقاله عادی

تحلیل ترافیک VOIP به‌منظور امنیت IMS

مرتضی عیسی‌پره حسن اصغریان احمد اکبری

دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، ایران

چکیده

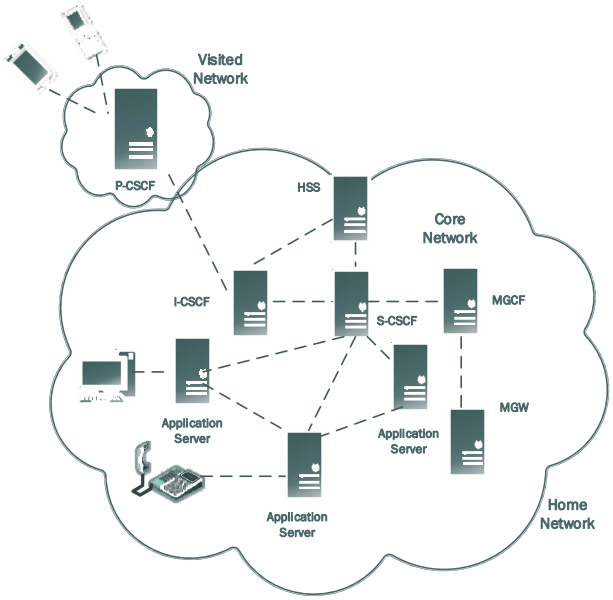
زیر سیستم چندرسانه‌ای مبتنی بر IP (IMS) معماری استاندارد برای شبکه‌های نسل آینده است. این معماری توسط موسسه 3GPP معرفی شده است و به سه قسمت کنترل، چند رسانه‌ای و سرویس تقسیم شده است. در لایه کنترل IMS پروتکل‌های SIP و DIMITER استفاده شده است. مزیت این پروتکل‌ها متنی، مبتنی بر IP و استقلال از نوع داده انتقالی است. عیب این پروتکل‌ها نبود مکانیزم امنیتی مناسب برای مواجه با انواع حملات است. این چالش سبب شده است که طیف وسیع کاربران شبکه نسل آینده با افت شدید کیفیت سرویس در زمان حملات مواجه شوند. ایده اصلی این مقاله بررسی تاثیر حملات انکار سرویس بر روی اجزای اصلی معماری IMS در سطح معماری زیرساخت است. به عبارت دیگر در این مقاله به دنبال تعریف خصیصه‌هایی در زیرساخت هستیم که عملکرد سیستم اعم از حالت عادی یا حمله را در لایه کاربرد نشان می‌دهد. همچنین در صورت وقوع حمله، سیاست‌های مختلفی نظیر تخصیص منابع بیشتر یا قطع دسترسی به برخی از مولفه‌ها می‌تواند در لایه کاربرد یا در لایه‌های پایین‌تر به منظور حفظ کیفیت سرویس اعمال گردد. به همین منظور خصیصه‌هایی برای مدل‌سازی رفتار موجودیت‌های اصلی IMS معرفی شده و این خصیصه‌ها در حالت‌های ترافیک طبیعی و ترافیک حمله مطالعه و مدل‌سازی شدند. برای مطالعه ترافیک IMS در مقابل حملات، از ابزارهای استاندارد مختلف Open IMS Core، SIPp و IMS Bench استفاده شده است. خصیصه‌های تعریف شده صرفا بر اساس سرآیند پروتکل‌های SIP و DIMITER و مطالعه آماری بر روی آنها تعریف شده‌اند. نتایج شبیه‌سازی بر روی بستر آزمایشگاهی پیکربندی شده (test-bed) کارایی مدل پیشنهادی را نشان می‌دهد.

کلمات کلیدی: زیرسیستم چند رسانه‌ای مبتنی بر IP، شبکه‌های نسل آینده، VOIP، Open IMS Core، امنیت SIP.

۱- مقدمه

وجود چارچوب واحد برای همگرایی شبکه‌های صوت، داده و ارتباطات سیار و ثابت دستاورد بزرگی در دنیای مخابرات محسوب می‌شود. اما چالش بزرگ یک چارچوب واحد، برقرار کردن یک سطح امنیتی مناسب برای این ساختار ناهمگون است. همین‌طور که در شکل ۱ مشاهده می‌شود، IMS یک معماری برای همگرایی قالب‌های داده متفاوت است. از آنجایی که شبکه‌های مبتنی بر IMS بر روی شبکه IP پیاده‌سازی می‌شوند، مشابه شبکه‌های داده عمومی در معرض حملات امنیتی متعددی از جمله حملات انکار سرویس قرار دارند. این حملات به عنوان عمده‌ترین حملات موجود در IMS شناخته شده‌اند [۴]. راه‌حل‌هایی از قبیل دیوار آتشدر مواجهه با این تهدیدها شکست خورده‌اند. وجود این چالش‌های امنیتی سبب می‌شود که طیف وسیع کاربران شبکه‌های نسل آینده با افت شدید کیفیت سرویس مواجه شوند. هدف شبکه‌های نسل سوم، ترکیب شبکه‌های سلولی و اینترنت است. عنصر کلیدی در معماری نسل سوم، امکان دسترسی به تمام سرویس‌های موجود در همه مکان‌ها و تمام زمان‌ها است. IMS استاندارد نوینی در ارتباطات است که توسط 3GPP تعریف شده است. IMS به صورت دیدی ترکیبی از دو فن‌آوری، از موفق‌ترین فن‌آوری‌های ارتباطات در شبکه‌های سلولی و اینترنت است. در یکپارچه‌سازی سرویس‌های تعریف شده در IMS، کاربران توسط ابزار سلولی خود قادرند به سرویس‌های داخل شبکه به آسانی، به طور مؤثر، قابل اعتماد و با قیمت منطقی دسترسی یابند. تمامی ارتباطات شبکه بر اساس پروتکل اینترنت است. سرویس VOIP برنامه اصلی در ارتباطات چندرسانه‌ای مبتنی بر پروتکل اینترنت است. تحقیقات زیادی برای کشف حملات سرویس‌های VOIP و زیرساخت آن انجام شده است اما به دلیل عدم وجود معیارها و مشخصه‌های مناسبی از ترافیک طبیعی VOIP در IMS و همچنین عدم وجود پایگاه داده

مناسبی از ترافیک طبیعی و ترافیک ناشی از حملات موجود در آن، امکان مقایسه کارهای مختلف وجود ندارد.



شکل ۱- معماری رایج IMS [۲]

از سوی دیگر از نظر فراهم‌کنندگان سرویس در شبکه‌های نسل آینده، مطالعه پارامترهای زیرساخت و برقراری ارتباط بین این پارامترها با وضعیت ارائه سرویس به کاربران از اهمیت ویژه‌ای برخوردار است. با توجه به اهمیت امنیت سرورهای IMS، در این مقاله مشخصه‌های مؤثر در روال‌های مختلف برای تشخیص امن بودن سرورهای IMS در برابر حملات انکار سرویس شناسایی می‌شوند. رفتار این مشخصه‌ها در حالت ترافیک طبیعی و حملات مدل می‌شوند. هدف از تعریف این مشخصه‌ها تعیین معیار مناسب برای تشخیص میزان طبیعی بودن ترافیک در هر لحظه از زمان است. به دلیل غیر قطعی بودن ترافیک شبکه، استخراج مشخصه‌هایی که در تمام حالات ترافیکی بیانگر مشخصه‌های ترافیک واقعی باشد، تقریبا غیر ممکن است. پس مشخصه‌هایی که تخمین واقع‌گرایانه‌ای از دنباله ترافیک ارائه دهند، باید در نظر گرفته شود. این مشخصه‌ها توصیف مناسبی از ترافیک طبیعی و حمله ارائه می‌دهند.

در ادامه این مقاله در بخش ۲ به مرور کارهای مرتبط در زمینه امنیت IMS پرداخته شده است. در بخش ۳ به معیارهای ارزیابی مورد نظر و روش پیشنهادی بیان می‌شود و در بخش ۴ پیکربندی محیط آزمایش و ارزیابی و تحلیل نتایج آورده شده است. در نهایت در بخش ۵ نیز جمع‌بندی و مرور کارهای آتی بیان می‌گردد.

۲- مرور مقالات مرتبط

در این بخش تلاش شده است که مقالات مرتبط در دو بخش مربوط به امنیت IMS و نیز مدل‌سازی ترافیک در IMS مرور شده است.

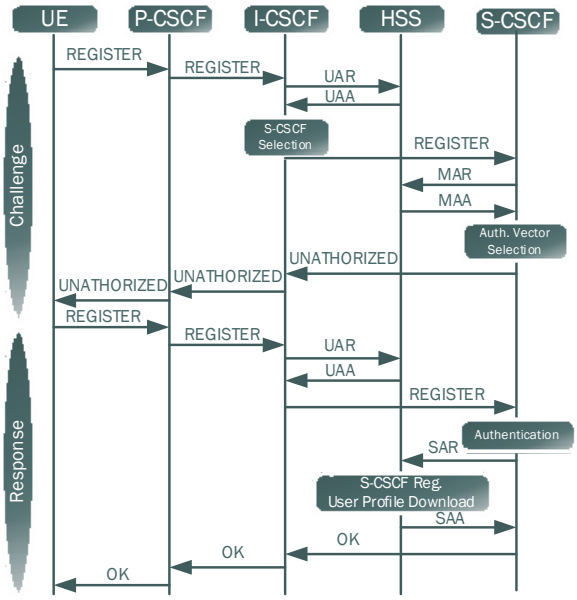
ساختار IMS دارای آسیب‌پذیری‌های متنوعی است زیرا کاربران در این شبکه همیشه به صورت برخط متصل هستند و استفاده از نسخه SIP با ساختار باز آنرا نسبت به حملات انکار سرویس آسیب‌پذیر نموده است [۹]. در مرجع [۵] به‌منظور مدل‌سازی ترافیک شبکه IMS و تخمین رفتار ترافیک صوت، داده و ویدئو در این بستر ارتباطی، از فرایند مارکف MMPP استفاده شده است. صحت و دقت انطباق MMPP بر ترافیک چندرسانه‌ای در شبکه IMS، ارزیابی روش‌هایی به‌منظور بهبود عملکرد تطبیق فرایند MMPP و بدست آوردن نتایج واقع گرایانه‌تر، پیشنهاد شده است. با مقادیر مختلف مشخصه HURST ترافیک تولید شده بررسی و ارزیابی شده است و نشان داده است که ترافیک IMS خود همسان (self-similar) است. در [۳] برای تولید ترافیک با مشخصه HURST مناسب از ۱۴۰ کاربر در محیط OPNET استفاده کرده است و از الگوریتم LAMBDA برای تنظیم کردن MMPP به ترافیک IMS استفاده کرده است. در [۳] به دلیل این‌که از ابزار استانداردی برای شبیه‌سازی IMS استفاده نشده است، ترافیک مناسبی تولید نشده است و دقت ارزیابی قابل دفاع نیست. در این مقاله به‌منظور افزایش دقت، تعداد حالت‌های مدل مارکف افزایش داده شده است اما الزاما با افزایش تعداد حالت‌ها دقت افزایش نمی‌یابد. حالت‌های مارکف باید متناسب با عناصر و اجزای معماری IMS در نظر گرفته شود که در این مقاله این مورد رعایت نشده است. نویسندگان در [۵] از مدل مارکف و الگوریتم LAMBDA برای مدل‌سازی ترافیک IMS استفاده کرده‌اند. در این مقاله از مدل‌سازی ترافیک IMS برای بهبود کیفیت سرویس استفاده شده است. بررسی حملات سیل‌آسا در SIP یا IMS در مقالات زیادی مورد بررسی قرار گرفته شده است. در بسیاری از کارهای پیشین، تمرکز محققین بر روی استفاده از تکنیک‌های بسیار ساده‌ای مانند مشخصه حد آستانه ثابت بر روییک یا چند مشخصه از ترافیک بوده است. روش‌هایی که از مشخصه آستانه ثابت استفاده می‌کنند، دارای دامنه عملکرد بسیار محدود هستند زیرا آستانه ثابتی برای انواع مختلف شبکه‌ها و شرایط مختلف بار ترافیکی نمی‌توان متصور بود.

نویسنده در [۷] با استفاده از الگوریتم KNN حملات UDP در P-CSCF و تأثیر آن حملات بر ترافیک IMS را مورد بررسی قرار داده است. نویسنده در [۹] از الگوریتم CUSUM برای کشف حملات سیل‌آسا بر روی ترافیک IMS استفاده کرده است. الگوریتم CUSUM می‌تواند تغییرات تدریجی را در زمان در نظر گرفته شده آشکار کند. در این مقالات فقط ترافیک P-CSCF بررسی شده است که برای مدل‌سازی ترافیک IMS کافی به نظر نمی‌رسد. علت محدود کردن مطالعات بر روی P-CSCF آن است که این سرور در واقع نقطه ورود به شبکه IMS است ولی با توجه به تعدد سرورهای P-CSCF، مهاجم می‌تواند طرح حمله خود را به صورت توزیع‌شده بر روی شبکه IMS و از طریق سرورهای P-CSCF مختلف اجرا نماید که در آن صورت نیاز به مطالعه تاثیر این حملات بر روی زیرساخت موجود وجود دارد. در [۶] ابتدا روش‌هایی که برای بهبود روش‌های تشخیص حملات سیل‌آسا به سرورهای SIP وجود دارد بررسی شده است و در ادامه یکی از روش‌ها با نام KASP را بهینه کرده و با تغییر اولویت‌بندی در بررسی پیام‌های آمده به سرور، زمان بررسی پیام‌ها را کاهش داده و مقابله با حمله را بهبود بخشیده است.

این مقاله حملات مربوط به پروتکل DIAMETER را در نظر نگرفته است. طبق آنچه در مرجع [۵] گفته شده است، شبکه IMS امکان انتخاب قابلیت اعتبارسنجی همه درخواست‌های کاربران SIP را دارا است. با اعتبارسنجی تمام درخواست‌های SIP ارسال شده به S-CSCF، ترافیک نقطه مرجع به نام Cx که واسط بین S-CSCF و HSS است، افزایش چشم‌گیری می‌یابد. با انتخاب برخی سیگنال‌ها برای احراز هویت، کاهش بار این بخش را خواهیم داشت. در صورتی که شبکه IMS احراز هویت کاربران SIP را الزامی نموده باشد، حملات ناشی از آدرس IP جعلی و یا جعل هویت غیر ممکن می‌شود زیرا کاربر از طریق S-CSCF مجبور است با پروتکل DIAMETER و موجودیت HSS احراز هویت شود (از طریق یکی از الگوریتم‌های AKA و یا MD5) و در این فرایند جعلی بودن آدرس IP محرز می‌شود. در ادامه به معرفی خصیصه‌های پیشنهادی برای ارزیابی امنیتی بستر IMS پرداخته شده است و مطالعه این پارامترها انجام شده است.

۳- روش پیشنهادی برای ارزیابی امنیتی IMS

مطالعه امنیت بستر IMS نیازمند بررسی رفتار اجزای مختلف آن معماری در ترافیک طبیعی و غیرطبیعی است. به همین جهت با هدف بررسی ایجاد تمایز بین حالت طبیعی و غیرطبیعی، وضعیت ترافیک زیرساخت IMS در حالات ترافیکی مختلف با کمک استخراج خصیصه‌هایی از روی ترافیک طبیعی در موجودیت‌های IMS مطالعه می‌شوند. از آنجایی که خصیصه‌های مورد نظر باید معرف رفتار سیستم باشند، مراحل ایجاد یک تماس در سناریوهای مختلف در ادامه بررسی شده و خصیصه‌های پیشنهادی معرفی می‌شوند. رویه برقراری یک تماس در IMS به این صورت است که با ورود یک درخواست از طرف کاربر به P-CSCF با توجه به نوع درخواست، برای بررسی و پاسخ به آن، پیام‌های متفاوتی بین اجزای معماری IMS رد و بدل می‌شود. این درخواست کاربر با استفاده از پروتکل SIP به P-CSCF داده می‌شود و سپس P-CSCF با استفاده از پروتکل SIP درخواست را به I-CSCF ارسال می‌کند و I-CSCF با بررسی درخواست با پروتکل DIAMTER با S-CSCF و HSS ارتباط برقرار می‌کند. با توجه به اطلاعات بدست آمده، پاسخ را به P-CSCF ارسال می‌کند و در نهایتP-CSCF پاسخ را به کاربر ارسال می‌کند. به عنوان مثال اگر درخواست REGISTER از طرف کاربر ارسال شده باشد، رویه شکل ۲ برای پاسخ به آن انجام می‌گیرد.



شکل ۲- حالت طبیعی انجام ثبت‌نام در IMS [۵]

با توجه به مشخص بودن نرخ تماس‌ها که در بخش محیط آزمایش بیان می‌شود، میزان ترافیک بین هر کدام از مولفه‌های معماری IMS روندی منطقی و قابل پیش‌بینی خواهد داشت. ما در این مقاله در مرحله اول ترافیک طبیعی تولید و رفتار هر کدام از اجزای معماری IMS را مدل‌سازی و تحلیل می‌کنیم. در مرحله بعد با ایجاد تعدادی از حملات شناخته شده VoIP به این بستر، رفتار مؤلفه‌های معماری IMS را مجددا مدل‌سازی و مطالعه کرده و بدین ترتیب نشان می‌دهیم که خصیصه‌های انتخابی قادر به ایجاد تمایز بین ترافیک طبیعی و حمله هستند. هدف اصلی طرح پیشنهادی آن است که با بررسی مشخصه‌های ترافیک داخل شبکه IMS بتوانیم بروز ناهنجاری در آنرا که عموما در نقاط ورود (P-CSCFها) رخ می‌دهد را شناسایی کنیم.

برای فراهم کردن ترافیک طبیعی دو روش عمده وجود دارد. اولین روش جمع‌آوری ترافیک یک مکان خاص است. به این صورت که ترافیک یک محل خاص در بازه‌های زمانی متفاوت مثلا به صورت هفتگی یا ماهانه به صورت شبانه‌روز جمع‌آوری شود. معمولا در این روش، رفتار ترافیک در ساعات اوج تماس‌ها مورد بررسی قرار می‌گیرد. این روش زمانی مناسب است که امکان دسترسی به ترافیک زیرساخت یک مجموعه و زمان کافی برای جمع‌آوری ترافیک وجود داشته باشد. به دلیل این که تعداد کاربران به صورت دقیق در این روش قابل تعیین نیست و همچنین تعداد مکالمات کاربران نیز قابل کنترل نیست و نیاز به مجوزهای خاص برای دسترسی به ترافیک زیر ساخت وجود دارد و نتایج آن نیز قابل انتشار نیست، عموما در کارهای تحقیقاتی مورد استفاده قرار نمی‌گیرد. مشخصه زمان نیز در این روش به این دلیل مورد توجه است که هر چقدر بازه زمانی جمع‌آوری ترافیک بیشتر باشد، ترافیک جمع‌آوری شده طبیعی‌تر خواهد بود و رفتار واقعی ترافیک شبکه را در حالت‌های مختلف به خوبی نشان می‌دهد.

روش دوم برای فراهم کردن ترافیک طبیعی، استفاده از ابزارهای استاندارد موجود برای تولید ترافیک به صورت مصنوعی است. مزیت این روش در مقایسه با روش اول، جامع بودن ترافیک تولید شده است. مزیت عمده این روش آن است که به ترافیکیک مکان خاص با تعداد کاربران مشخص و تماس‌های کم، محدود نمی‌شود. به عبارت دیگر در این روش تلاش می‌شود تا با بهره‌گیری از ابزارهایی که برای تست بار در محیط‌های واقعی استفاده می‌شوند، ترافیک معتبر تولید و سیستم مورد نظر ارزیابی گردد. به همین منظور در این مقاله نیز همین روش مورد نظر قرار گرفته است. در این مقاله با بهره‌گیری از ابزارهای استانداردی نظیر Open IMS Core، IMS Bench SIPp و SIPp به همراه سناریوهای مختلف برای تولید ترافیک استفاده شده است که در بخش محیط آزمایش نحوه پیکربندی آن‌ها شرح داده شده است.

برای تولید ترافیک نیاز به مشخصه‌هایی از قبیل نرخ تماس‌های کامل شده، نرخ تماس‌های رد شده و نرخ تماس‌های لغو شده وجود دارد که این مشخصه‌ها را با بهره‌گیری از مراجعی که شرح آن‌ها در ادامه آورده شده است، استخراج و مورد استفاده قرار گرفته است. برای مدل‌سازی و تحلیل ترافیک IMS، باید مشخصه‌هایی در نظر گرفته شوند که رفتار موجودیت‌های معماری IMS را در حالت‌های مختلف نشان دهند. با توجه به این که بیشترین رویه‌هایی که در IMS اجرا می‌شود، رویه برقراری تماس (INVITE) و ثبت‌نام (REGISTER) است و به دلیل این که بیشتر ترافیک SIP و DIAMETER در حالت طبیعی مربوط به درخواست‌های REGISTER و INVITE و پاسخ‌های مرتبط با آنها است، مشخصه‌های زیر برای مدل‌سازی مورد نظر قرار گرفتند که نتایج مربوط به آن‌ها در بخش ارزیابی شرح داده می‌شود:

جدول ۱- خصیصه‌های پیشنهادی برای ارزیابی امنیتی

عنوان	توضیح
تعداد REGISTERها	بین کاربر و P-CSCF
INVITEها	بین کاربر و P-CSCF
نسبت UAR به UAA	بین I-CSCF و HSS
نسبت SAR به SAA	بین S-CSCF و HSS

علت انتخاب هر یک از خصیصه‌های ذکر شده در جدول ۱ آن است که با ایجاد هر تراکنش جدید در بستر IMS مشخصه‌های ذکر شده دچار تغییراتی می‌شوند. به همین منظور مشخصه‌های یاد شده در ترافیک طبیعی مدل و رفتار ترافیک طبیعی با کمک آن‌ها بیان می‌گردد. برای ایجاد تماس ابتدا کاربر باید REGISTER شود، در ترافیک طبیعی یک کاربر در بازه زمانی مشخص (به طور پیش فرض در هر ساعت یک بار)، به تعداد معینی دستور ثبت‌نام ارسال

می‌شود که با بررسی تعداد REGISTERهای بین کاربر و P-CSCF میزان طبیعی بودن ترافیک از نظر تعداد REGISTERها قابل ارزیابی است. بعد از اتمام فرایند ثبت‌نام، کاربر اقدام به برقراری تماس با ارسال فرمان INVITE می‌کند که در تماس معمولی یک INVITE برای برقراری تماس استفاده می‌شود و اگر برای هر تماس تعداد INVITEها زیاد و تکراری باشد ترافیک طبیعی نیست. برای احراز هویت کاربر، با ارسال دستور UAR از I-CSCF به HSS در هنگام ثبت‌نام، نام S-CSCF انتخاب می‌شود و هنگام DEREGISTER با ارسال دستور UAA از HSS به I-CSCF، S-CSCF آزاد می‌شود. در هر تماس معمولی یک بار باید I-CSCF به HSS وصل شود ولی اگر تماس غیرمعمولی باشد، این کار چندین بار تکرار می‌شود. برای به‌روزرسانی نام S-CSCF و دریافت مشخصات کاربران دستورهای SAR و SAA بین HSS و S-CSCF ارسال می‌شود. در هر بازه زمانی بین HSS و S-CSCF، امکان حمله و سرقت مشخصات کاربران و استفاده از IP مجازی وجود دارد. در مرحله بعد به منظور تولید ترافیک ناشی از حملات، مجموعه حملات انکار سرویس توسط ابزارهایی که در بخش محیط آزمایش توضیح داده می‌شود، به P-CSCF اعمال شدند. علت اعمال حملات به پروکسی P آن است که این پروکسی نقطه تماس کاربر با معماری IMS است و نیز به علت آنکه بیشترین ضعف سرورهای IMS نسبت به حملات سیل‌آسا است [۷][۱۲]، در این مقاله به مطالعه تأثیر حملات سیل‌آسا بر ترافیک IMS پرداخته شده است. این حملات منابع سیستم از قبیل حافظه، پهنای باند و پردازنده را مورد تهدید قرار می‌دهند.

۴- پیکربندی محیط آزمایش

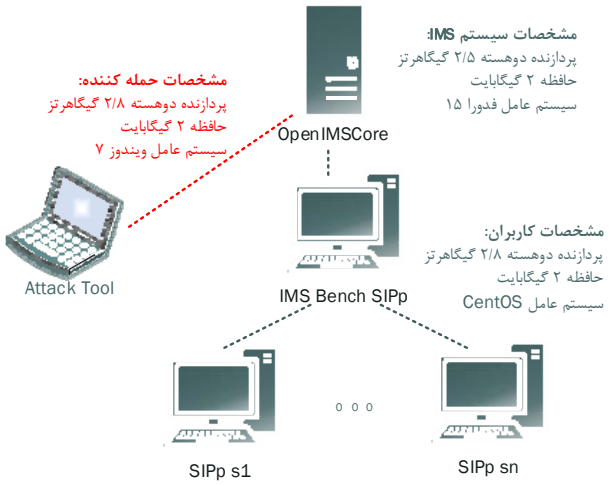
اجزای اصلی محیط آزمایش پیکربندی شده برای انجام آزمایش‌ها از سه بخش بستر IMS، مولد ترافیک طبیعی و مولد ترافیک حمله تشکیل شده است. بستر IMS مورد نیاز با بهره‌گیری از ابزار متن باز Open IMS core [۸] بر روی یک ماشین مجازی پیکربندی و راه‌اندازی شد. برای تولید ترافیک نیز از ابزارهای IMS Bench SIPp استفاده شد و همچنین برای ایجاد و تست سیستم نیز با استفاده از SIPp [۹] عامل‌های کاربری پیاده‌سازی و استفاده شدند (شکل ۳).

تعداد کاربران برابر ۲۰۰ هزار کاربر ثبت‌نام شده در نظر گرفته شده و چهار سناریو برای تولید ترافیک در نظر گرفته شد که عبارتند از: تماس‌های کامل، تماس‌های رد شده، تماس‌های بی‌پاسخ و تماس‌های لغو شده که نرخ هر کدام از این سناریوها با بهره‌گیری از نتایج منتشر شده مراجع دیگر نظیر [۶] استخراج و استفاده شد. مشخصه‌های مربوطه برای تولید ترافیک طبیعی در جدول ۲ زیر آورده شده است:

جدول ۲- مشخصه‌های تولید ترافیک طبیعی

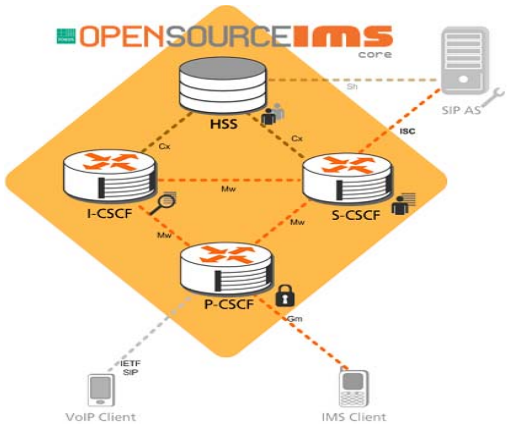
عنوان مشخصه	مقدار
درصد تماس‌های کامل شده	۷۰
درصد تماس‌های لغو شده	۱۵
درصد تماس‌های رد شده	۱۰
درصد تماس‌های REGISTER	۲.۵
درصد تماس‌های REREGISTER	۲.۵

همانطور که عنوان شد برای پیاده‌سازی بستر IMS نیاز به بهره‌گیری از ابزارهای استاندارد وجود دارد. نرم‌افزار Open IMS Core یک ابزار متن باز استاندارد است که به منظور پیاده‌سازی معماری IMS بکار می‌رود. معماری این نرم‌افزار در شکل ۴ نشان داده شده است. این معماری در این مقاله مورد استفاده قرار گرفته است. این بستر بر روی یک ماشین مجازی با سیستم عامل سیستم-عامل لینوکس فدورا ۹ پیکربندی شد. برای اجرای سناریوها و برقراری تماس بین کاربران، از نرم‌افزارهای تولید ترافیک طبیعی IMS Bench SIPp و SIPp که توسط شرکت HP ارائه شده‌اند، استفاده شده است.



شکل ۳- بستر آزمایش

با در نظر گرفتن مشخصه‌های جدول ۲، در گام اول و با هدف استخراج مدل مورد نظر، به مدت ۵ دقیقه ترافیک طبیعی تولید شد.



شکل ۴- معماری نرم‌افزار Open IMS Core [۱۰]

نرم‌افزار IMS Bench SIPp برای مدیریت و راه‌اندازی درخواست‌های SIPp از جمله دریافت تماس از UAC و ارسال آن به پروکسی Open IMS Core و ارسال تماس به UAS استفاده می‌شود. با استفاده از نرم‌افزار SIPp سناریوهای مختلف مورد نیاز اجرا شده و در نرم‌افزار IMS Bench SIPp مشخصه‌های اجرای آن‌ها از قبیل نرخ اجرا تنظیم می‌شود. IMS Bench SIPp قابلیت‌های بیشتری از جمله پشتیبانی از تعداد کاربران زیاد، اجرای چندین سناریو توسط اجرای یک خط فرمان SIPp، مدیریت و کنترل چندین SIPp اجرایی توسط یک سیستم مدیر مرکزی و تولید گزارش، در مقایسه با SIPp دارد. نرم‌افزار IMS Bench و SIPp بر روی یک ماشین مجازی دیگر برای تکمیل محیط آزمایش نصب و پیکربندی شد. پارامترهای زمان اجرای هر یک از موجودیت‌های مورد نیاز بر اساس توضیحات بالا تنظیم و در هر آزمایش به طور مناسب پیکربندی و اجرا شدند. به طور مثال در آزمایش مربوط به ثبت‌نام کاربران، سرور پروکسی Open IMS Core باید طوری

پیکربندی شود که با ارسال پیام ۴۰۱ از هر کاربر شناسه و رمز عبور را تقاضا نماید. بعد از تنظیم مناسب مشخصه‌های آزمایش و در نظر گرفتن ترتیب اجرای سناریوها در بخش مدیریت IMS Bench، عملیات تولید ترافیک آزمایشی شروع می‌شود.

به منظور تولید ترافیک حمله به ابزارهای حمله نیاز داریم که از ابزارهای استانداردی که در آزمایشگاه گروه تحقیقاتی شبکه دانشگاه علم و صنعت آماده شده‌اند استفاده شده است. اطلاعات مربوط به ابزارهای حمله در مرجع [۱۱] موجود است. این ابزارها با تولید ترافیک حمله مربوط به حملات سیل‌آسا امکان بررسی تاثیر این حملات را بر روی بستر IMS ممکن می‌سازند.

۵- ارزیابی و تحلیل نتایج

پس از پیکربندی محیط آزمایش و تولید و جمع‌آوری ترافیک بر اساس پارامترهای یاد شده، خصیصه‌های مورد نظر در ترافیک طبیعی و حملات تحلیل و استخراج شدند. با مقایسه و بررسی رفتار این مشخصه‌ها، وجه تمایز بین ترافیک طبیعی و ناهنجاری استخراج شد. فایل‌های پیکربندی و آزمایش‌های مربوط به تمامی فعالیت‌های بالا بر روی صفحه تحلیل ترافیک IMS در سایت آزمایشگاه تحقیقات شبکه‌های کامپیوتری دانشکده کامپیوتر علم و صنعت به آدرس http://nrg.iust.ac.ir/ims-traffic موجود هستند. نتایج تولید ترافیک در جدول‌های (۳) و (۴) و (۵) نشان داده شده است. این ترافیک‌ها در بازه‌های زمانی مختلف از ۵۰ ثانیه تا ۳۰۰ ثانیه تولید شد.

جدول ۳- خصیصه‌های استخراجی از ترافیک طبیعی

مشخصه		مقدار	مشخصه		مقدار
$\frac{SAR}{Reg}$	P	0.5	$\frac{SAR_{out}\ HSS}{UAR_{in}HSS}$		0.96
	I	0.5	$\frac{resArrival}{NbRes}$		115888
	S	0.5	$\frac{ReqArrival}{NbReq}$		99688
	HSS	0.5	$\frac{Nbsender}{NbReciever}$		0.99
$\frac{4XX}{Register}$	P	0	$\frac{ACK}{Req}$	P	0.12
	I	0		I	0
	S	0		S	0.12
$\frac{180}{INVITE}$	P	0.92	$\frac{Reg}{Req}$	P	0.001
	I	0		I	0.001
	S	0.92		S	0.001
$\frac{100}{INVITE}$	P	0.92	$\frac{BYE}{Req}$	P	0.10
	I	0		I	0
	S	0.92		S	0.11
$\frac{4XX}{INVITE}$	P	0	$\frac{INVITE}{Req}$	P	0.12
	I	0		I	0
	S	0		S	0.12
$\frac{BYE}{INVITE}$	P	1.14	$\frac{BYE}{ACK}$	P	0.84
	I	0		I	0
	S	0.88		S	0.89
$\frac{(4XX_{out}HSS)}{UAR_{in}HSS}$		0.09	تعداد کل بسته‌ها		94159

۵-۱- تحلیل نتایج

برای تحلیل خصیصه‌ها، باید پنجره زمانی مناسبی تعیین شود. انتخاب غیردقیق پنجره زمانی باعث عدم‌تمایز مناسب ترافیک طبیعی و ناهنجاری می‌شود. از قانون لیتل برای تعیین اندازه پنجره زمانی استفاده می‌کنیم که عبارت است از متوسط تعداد کاربران (L) در یک سیستم پایدار برابر است با متوسط نرخ ورود تماس‌ها (λ) ضرب در متوسط زمانی که تماس‌ها در سیستم پردازش (W) می‌شوند:

$$L = \lambda W \quad (۱)$$

برای تولید ترافیک تعداد کل کاربران را برابر ۲۰۰ هزار نفر در نظر گرفتیم. نرخ ورود تماس‌ها را از قانون ارلانگ بدست آوردیم که عبارت است از:

$$M_{max} \times \alpha = \lambda \times T_{call} \quad (۲)$$

جدول ۴- مشخصه‌های استخراج شده از ترافیک حمله حافظه

مشخصه		مقدار	مشخصه		مقدار
$\frac{SAR}{Reg}$	P	0.5	$\frac{SAR_{out}HSS}{UAR_{in}HSS}$		0.84
	I	0.5	$\frac{resArrival}{NbRes}$		148539
	S	0.5	$\frac{ReqArrival}{NbReq}$		101698
	HSS	0.5	$\frac{Nbsender}{NbReciever}$		0.99
$\frac{4XX}{Reg}$	P	0	$\frac{ACK}{Req}$	P	0.06
	I	0		I	0
	S	0		S	0.06
$\frac{180}{INVITE}$	P	0.088	$\frac{Reg}{Req}$	P	0.001
	I	0		I	0.001
	S	0.91		S	0.001
$\frac{100}{INVITE}$	P	0.97	$\frac{BYE}{Req}$	P	0.1
	I	0		I	0
	S	0.93		S	0.1
$\frac{4XX}{INVITE}$	P	0.91	$\frac{INVITE}{Req}$	P	0.59
	I	0.91		I	0
	S	0		S	0.058
$\frac{BYE}{INVITE}$	P	0.10	$\frac{BYE}{ACK}$	P	0.97
	I	0		I	0
	S	0.92		S	0.99
$\frac{4XX_{out}HSS}{UAR_{in}HSS}$		0.19	تعداد کل بسته‌ها		143237

جدول ۵- مشخصه‌های استخراج شده از ترافیک حمله پهنای باند

مشخصه		مقدار	مشخصه		مقدار
$\frac{SAR}{Reg}$	P	0.001	$\frac{SAR_{out}HSS}{UAR_{in}HSS}$		0.27
	I	0.27	$\frac{resArrival}{NbRes}$		123547
	S	0.5	$\frac{ReqArrival}{NbReq}$		126355
	HSS	0.001	$\frac{Nbsender}{NbReciever}$		0.99
$\frac{4XX}{Register}$	P	0.81	$\frac{ACK}{Req}$	P	0.06
	I	0.80		I	0
	S	0.002		S	0.06
$\frac{180}{INVITE}$	P	0.90	$\frac{Reg}{Req}$	P	0.52
	I	0		I	0.001
	S	0.90		S	0.001
$\frac{100}{INVITE}$	P	0.92	$\frac{BYE}{Req}$	P	0.1
	I	0		I	0
	S	0.92		S	0.1
$\frac{4XX}{INVITE}$	P	0	$\frac{INVITE}{Req}$	P	0.062
	I	0		I	0
	S	0		S	0.062
$\frac{BYE}{INVITE}$	P	1.11	$\frac{BYE}{ACK}$	P	0.84
	I	0		I	0
	S	0.85		S	0.89
$\frac{4XX_{out}HSS}{UAR_{in}HSS}$		0.78	تعداد کل بسته‌ها		172448

ضریب فعالیت (α) هر کاربر را مانند شبکه‌های معمولی ۰.۰۵ در نظر گرفتیم [۱۲]. متوسط زمان تماس (T_{call}) ۱۰۰ ثانیه با استفاده از مقالات در نظر گرفته شده است. با استفاده از رابطه (۲) نرخ ورود تماس‌ها، ۱۰۰ تماس در هر ثانیه محاسبه شد و با رابطه (۱) اندازه پنجره مناسب قابل محاسبه است. به طور مثال اگر زمان پردازش هر پیام را برابر ۱۰۰ میلی‌ثانیه در نظر بگیریم، اندازه پنجره برابر ۱۰ خواهد بود. پر واضح است که هر چه اندازه پنجره بزرگتر انتخاب شود، نتایج دقیق‌تر خواهد بود ولی انتخاب پنجره بزرگ علاوه بر ایجاد تاخیر در تشخیص، موجب افزایش حجم پردازش مورد نیاز نیز می‌شود.

در حمله حافظه، حمله‌کننده با ارسال تعداد زیادی درخواست حافظه مرکز ارائه خدمت سیستم را غیر فعال می‌کند و در حمله پهنای باند مهاجم با ارسال تماس‌هایی توسط کاربران شناسایی نشده، پهنای باند شبکه را مصرف می‌کند. با مقایسه جدول‌های ۳، ۴ و ۵ مشخصه‌های متمایز کننده قابل تعیین هستند.

۵-۲- دیدگاه‌های ارزیابی

خصیصه‌های انتخابی در قسمت‌های مختلف معماری IMS مورد بررسی قرار گرفته‌اند که انتخاب این مشخصه‌ها از دو جهت و در دو بخش قابل بررسی برای کشف حمله هستند:

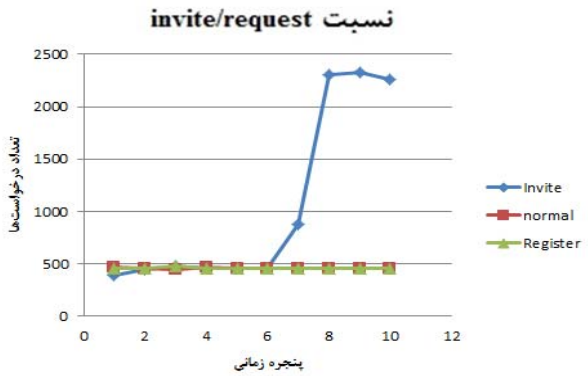
- مقدار این مشخصه‌ها در یک سرور مشخص: مقدار مشخصه‌های در نظر گرفته باید در هر یک از موجودیت‌های IMS (سرورهای P، I، S و HSS) مقدار مشخصی داشته باشد. به طور مثال اگر خصیصه $\frac{\text{INVITE}}{180}$ را در نظر بگیریم، طبق روال استاندارد برقراری تماس در IMS، مقدار این مشخصه باید در سرورهای P در ترافیک طبیعی تقریبا نزدیک به یک باشد چون برای هر درخواست INVITE یک درخواست 180 باید ارسال شود.
- بررسی مقدار این مشخصه‌ها در سرورهای مختلف: برخی از خصیصه‌های ترافیکی مورد نظر اختصاص به یک سرور خاص ندارند و در کل ترافیک زیرساخت باید در نظر گرفته شوند. به طور مثال مشخصه $\frac{\text{SAR}}{\text{Reg}}$ بین سرورهای P، I، S و HSS باید با صرف نظر از خطاها و ازدحام‌های شبکه، یکسان باشد اما در صورتی که مقدار این مشخصه در P خیلی بیشتر از S باشد یعنی به سرور P تعداد زیادی درخواست نامعتبر ثبت‌نامه ارسال شده است که این موضوع می‌تواند به عنوان حمله یا ترافیک ناهنجار در نظر گرفته شود.

علت در نظر گرفتن خصیصه‌های نوع دوم این است که ممکن است حمله‌ای به یک سرور خاص صورت بگیرد که نسبت مشخصه‌ها را مانند روال استاندارد تنظیم کند. به طور مثال ممکن است حمله‌ای به سرور P، پاسخ‌های 180 را ارسال کند و به همان نسبت از سرور P درخواست‌های INVITE ارسال کند که با این شرایط حمله‌ای که در P صورت گرفته شده کشف نمی‌شود، اما استفاده از پارامترهای دیگر که با تحلیل ترافیک بین چند موجودیت در IMS محاسبه می‌شوند، این حمله کشف می‌شود. برای بررسی وجود حمله سیل‌آسا از نوع ثبت‌نام خصیصه‌های $\frac{\text{SAR}}{\text{Reg}}$، $\frac{4\text{XX}}{\text{Reg}}$، $\frac{4\text{XX}_{\text{outHSS}}}{\text{UAR}_{\text{inHSS}}}$، $\frac{\text{SAR}_{\text{outHSS}}}{\text{UAR}_{\text{inHSS}}}$ و $\frac{\text{Reg}}{\text{Req}}$ استفاده می‌شود. از خصیصه‌های $\frac{\text{SAR}}{\text{Reg}}$ و $\frac{\text{SAR}}{\text{Reg}}$ نسبت ثبت‌نام‌های موفق را می‌توان بدست آورد و از مشخصه‌های $\frac{4\text{XX}}{\text{Reg}}$ و $\frac{4\text{XX}_{\text{outHSS}}}{\text{UAR}_{\text{inHSS}}}$ نسبت رجیسترهای ناموفق را می‌توان بدست آورد.

۵-۳- نتایج ارزیابی

برای بررسی وجود حمله INVITE از خصیصه‌های $\frac{180}{INVITE}$، $\frac{100}{INVITE}$، $\frac{4\text{XX}}{\text{INVITE}}$، $\frac{\text{BYE}}{\text{INVITE}}$ و $\frac{\text{INVITE}}{\text{Req}}$ استفاده می‌شود. به طور مثال انتظار داریم برای هر درخواست INVITE یک پاسخ ۱۰۰ دریافت شود. پس نسبت ۱۰۰ها به INVITEها با صرف نظر از ازدحام در شبکه، در بین سرورهای P و S باید نزدیک به یک باشد. همچنین با توجه به این موضوع که هر دیالوگ در SIP با INVITE شروع و با BYE ختم می‌شود، نسبت این دو پارامتر نیز می‌تواند برای شناسایی حملاتی نظیر ایجاد تراکنش‌های ناقص با کمک همکار در SIP مورد استفاده قرار بگیرد. خصیصه‌های تعریف شده دیگر برای کشف حملات مختلفی بکار می‌روند به طور مثال خصیصه $\frac{\text{BYE}}{\text{ACK}}$ برای کشف حملات BYE و ACK می‌تواند بکار رود.

در ادامه با استفاده از پنجره زمانی بدست آمده و نتایج ذکر شده در جدول‌های ۳، ۴ و ۵ خصوصیات ترافیکی مشخصه‌ها را بررسی می‌کنیم. در این مقاله فقط مشخصه‌هایی را در نظر می‌گیریم که در همه تماس‌ها نقش اساسی برای برقراری تماس و احراز هویت کاربران دارند به عبارت دیگر تمرکز خود را بر روی پیام‌های درخواست اصلی شامل INVITE، BYE، REGISTER و ACK قرار می‌دهیم. اولین خصیصه‌ی مورد نظر برای ارزیابی، $\frac{\text{INVITE}}{\text{Req}}$ است. طبق روال استاندارد برقراری تماس در IMS، نسبت این مشخصه در سرورهای P و S مساوی و یا بهم نزدیک هستند. همچنین نسبت کل INVITEها به کل درخواست‌ها نباید از حد آستانه مشخصی بیشتر شود و افزایش این مقدار به معنی رخداد حالت ناهنجاری است که می‌تواند معرف حملاتی نظیر حمله سیل‌آسای INVITE، حملات تراکنش ناقص و نیز حملات Brute Force باشد. همان‌طور که در شکل ۵ ملاحظه می‌شود، خصیصه $\frac{\text{INVITE}}{\text{Request}}$ در ترافیک طبیعی و حمله REGISTER بسیار کمتر از حمله INVITE است. با استخراج مدل ترافیکی خصیصه $\frac{\text{INVITE}}{\text{Request}}$ در هر کدام از حالت‌های ترافیکی، همان‌طور که در جدول ۶ ملاحظه می‌شود، در حالت ترافیک طبیعی دارای توزیع گاوسی است اما در حالات حمله غیر گاوسی است.

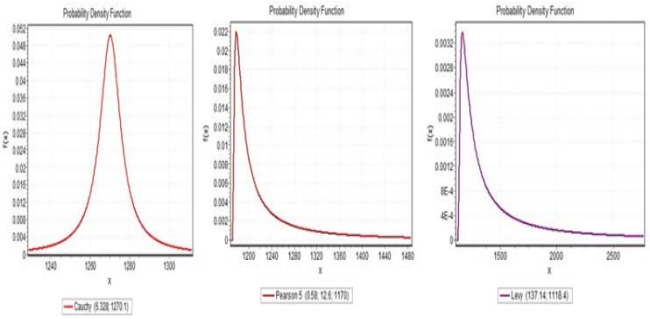


شکل ۵- نسبت درخواست‌های INVITE به کل درخواست‌ها

با استخراج توزیع‌های آماری خصیصه $\frac{\text{INVITE}}{\text{Req}}$ از روی جدول ۶ شکل ۶ را استخراج کردیم.

جدول ۶- توزیع‌های متناسب با خصیصه $\frac{\text{INVITE}}{\text{Req}}$

نوع ترافیک	نوع توزیع	رفتار عادی توزیع
طبیعی	Cauchy σ=6.328 μ=1270.1	S=1 m=0
حمله پهنای باند (REGISTER)	Pearson 5 (3P) σ=0.58 β=12.6 γ=1170	a=2 b=1 g=0
حمله حافظه (INVITE)	Levy (2P) σ=137.14 γ=1118.4	s=1 g=0

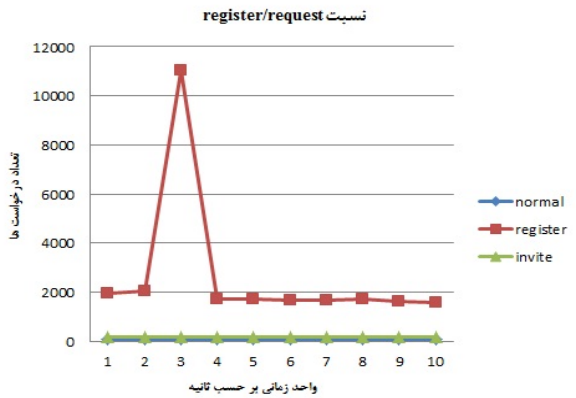


شکل ۶- توزیع درخواست‌های INVITE به کل درخواست‌ها

از جدول ۵ و شکل ۶ نتیجه گرفته می‌شود که نسبت مشخصه $\frac{\text{INVITE}}{\text{Req}}$ در ترافیک طبیعی در تمام ترافیک جمع‌آوری شده، توزیع مشخصی دارد. در نیمه اول ترافیک این نسبت برای برقراری تماس‌ها رو به افزایش است اما با رسیدن به انتهای جمع‌آوری ترافیک که تعداد برقراری تماس‌ها کاهش می‌یابد، این نسبت نیز کاهش می‌یابد. اما این نسبت در ترافیک‌های حمله به طور انفجاری افزایش می‌یابد و سپس کاهش می‌یابد. با بررسی شکل ۷ مشاهده می‌شود که نسبت خصیصه $\frac{\text{Register}}{\text{Request}}$ در ترافیک طبیعی و حمله INVITE بسیار کمتر از حمله REGISTER است. مدل ترافیک این مشخصه در حالت طبیعی طبق جدول ۷ پواسن با نرخ ورود ۱۱.۶ تماس درثانیه است.

جدول ۷- توزیع‌های متناسب با خصیصه $\frac{\text{Register}}{\text{Req}}$

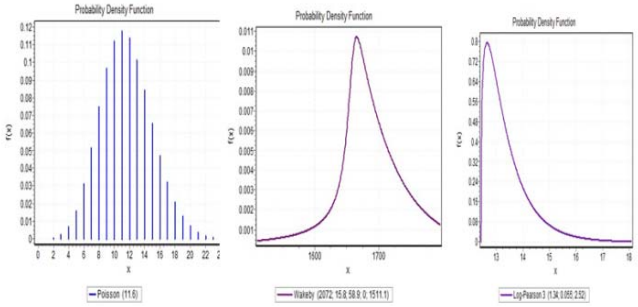
نوع ترافیک	نوع توزیع	رفتار عادی توزیع
طبیعی	Pearson5 (3P) α=273.4 β=23451.0 γ=68.7	a=2 b=1 g=0
حمله پهنای باند (REGISTER)	Lognormal (3P) σ=5.63 μ=4.1 γ=156.2	s=1 m=1 g=0
حمله حافظه (INVITE)	Cauchy σ=7.75 μ=141.33	s=1 m=0



شکل ۷- نسبت درخواست‌های ثبت‌نام به کل درخواست‌ها

با استخراج توزیع‌های آماری مشخصه $\frac{\text{Register}}{\text{Req}}$ از روی جدول ۷ شکل ۸ را استخراج کردیم. با کمک جدول ۷ و شکل ۸ نتیجه گرفته می‌شود که نسبت خصیصه $\frac{\text{Register}}{\text{Req}}$ در ترافیک طبیعی در تمام ترافیک جمع‌آوری شده، به صورت هارمونیک افزایش و کاهش می‌یابد. اما این نسبت در ترافیک‌های حمله به طور انفجاری افزایش می‌یابد و سپس کاهش می‌یابد. با افزایش تعداد درخواست‌های غیرمجاز از طرف کاربران غیرمجاز، سرور پاسخ 4xx را به کاربر ارسال می‌کند. همان‌طورکه شکل ۸ نشان می‌دهد تعداد 4xx به کل پاسخ‌ها درترافیک طبیعی خیلی کمتر از ترافیک حملات است. طبق جدول ۸ توزیع این خصیصه درحالت طبیعی دارای توزیع Pearson است که با حالات حمله متفاوت است.

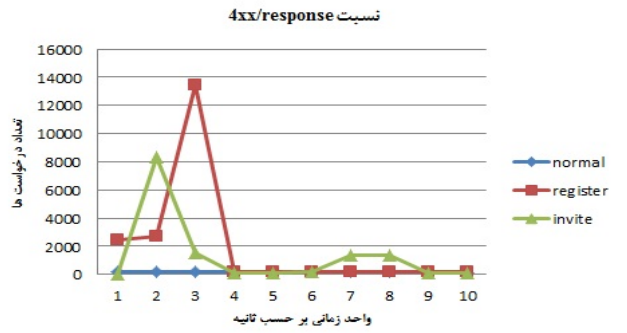
با استخراج توزیع‌های آماری مشخصه $\frac{4xx}{\text{Res}}$ از روی جدول ۸ شکل ۱۰ را استخراج کردیم.



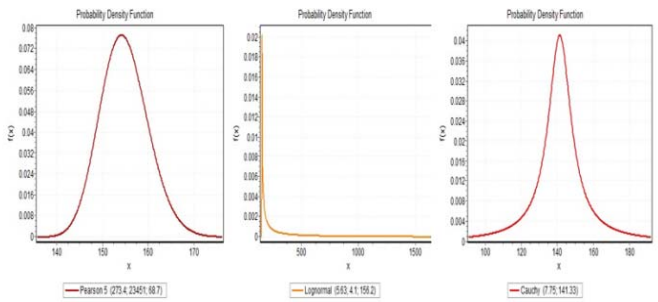
شکل ۸- توزیع درخواست‌های REGISTER به کل درخواست‌ها

جدول ۸- توزیع‌های متناسب با خصیصه $\frac{\text{4xx}}{\text{Res}}$

نوع ترافیک	نوع توزیع	رفتار عادی توزیع
طبیعی	Poisson ε=11.6	l=10
حمله پهنای باند (REGISTER)	Wakeby α=2072,β=15.8 γ=58.9 δ=0.944 ε=1511.1	a=10,b=5,g=1 ,d=0.5,x=0
حمله حافظه (INVITE)	Log-Pearson 3 α=1.34 β=0.055 γ=2.52	a=2 b=1 g=0



شکل ۹- نسبت پاسخ‌های 4xx به کل پاسخ‌ها



شکل ۱۰- توزیع درخواست‌های 4xx به کل درخواست‌ها

۶- نتیجه‌گیری و کارهای آینده

هدف اصلی این مقاله از تحلیل ترافیک IMS، استخراج رفتار مولفه‌ها و موجودیت‌های مختلف اجزای معماری IMS در حالت‌های ترافیک طبیعی و ترافیک حمله بود. به عبارت دیگر سعی در استخراج پارامترهایی از ترافیک زیرساخت IMS داشتیم که به کمک آنها امکان ایجاد تمایز بین حالت حمله و حالت طبیعی امکان‌پذیر باشد. به عبارت دیگر از آنجایی که نقطه ورود کاربران به شبکه‌های IMS از طریق سرورهای P- CSCF انجام می‌شود و این سرورها با توجه به توزیع جغرافیایی کاربران در شبکه توزیع می‌شوند و عملا بررسی وضعیت آنها در یک نقطه ممکن است غیر ممکن باشد، در این مقاله با تعریف خصیصه‌های ترافیکی مناسب و قابل اندازه‌گیری در زیرساخت شبکه IMS، به دنبال کشف حالات ناهنجار و ترافیک حمله در سرویس‌های ارائه شده در این بستر بودیم. هر چند مطالعات و آزمایش‌های طرح شده در این مقاله اختصاص به بستر IMS دارد ولی رهیافت پیشنهادی برای تشخیص حالات ناهنجار در سیستم، می‌تواند در تمامی سرویس‌هایی که در لایه کاربردی در هر نوع شبکه‌ایارائه می‌شوند، در نظر گرفته شود. برای ارزیابی خصیصه‌های پیشنهادی، با توجه به عمومیت حملات انکار سرویس در SIP، تمرکز اصلی را بر روی این نوع حملات قرار داده و با پیکربندی یک بستر آزمایشگاهی عملیاتی مبتنی بر ابزارهای متن- باز، اقدام به مطالعه خصیصه‌های پیشنهادی در این بستر نمودیم. نتایج بدست آمده بیانگر رفتار خصیصه‌ها در حالت ترافیک طبیعی با حالت ترافیک حمله هستند و می‌توان از مدل‌های تولید شده برای تشخیص طبیعی یا ناهنجار بودن ترافیک استفاده کرد. همچنین خصیصه‌های معرفی شده در این مقاله برای استفاده در سیستم‌های تشخیص نفوذ نیز مناسب هستند. نوآوری‌های مقاله حاضر شامل تعریف خصیصه‌های ترافیک طبیعی سرویس‌های مبتنی بر SIP (به طور خاص VoIP) در بستر IMS، مدل‌سازیترافیک VOIP در IMS بر اساس مشخصه‌های آن و نیز تحلیل توزیع خصیصه‌های پیشنهادی برای تشخیص نفوذ و ناهنجاری در بستر IMS است. همچنین پس از پیکربندی محیط آزمایش شرح داده شده در این مقاله، مجموعه دادگانی برای ارزیابی سیستم‌های تشخیص نفوذ SIP در بستر IMS جمع‌آوری شد. این مجموعه دادگان بر روی سایت گروه تحقیقاتی شبکه دانشگاه علم و صنعت ایران، به آدرس http://nrg.iust.ac.ir/ims-traffic قرار داده شده است.

در ادامه فعالیت‌های مربوط به این مقاله، فعالیت‌های اصلی برای توسعه شامل در نظر گرفتن روال‌های دیگر علاوه بر روال برپایی جلسه و ثبت‌نام (نظیر ابطال ثبت‌نام و ثبت‌نام مجدد)، توسعه مجموعه حملات مورد نظر (نظیر حملات BYE، CANCEL) و نیز تعریف و تحلیل خصیصه‌های دیگر (نظیر تأخیر صف، توزیع بسته‌ها در پنجره زمانی، طول بسته‌ها، تعداد بسته‌ها، زمان انتظار بسته‌ها) است.

مراجع

[1] P. Agrawal, and et al., "Ip Multimedia Subsystem in 3gpp & 3gpp2: Overview and Scalability Issues," *IEEE Trans. Communications*, vol. 46, no. 1, pp. 138-145, 2008.

[2] N. Rajagopal, and M. Devetsikiotis, "Modeling and Optimization for the Design of IMS Networks," *Proc, IEEE Int'l Conf. Simulation*, pp. 34-41, 2006.

[3] K. D. Chang, and et al., "Challenges to Next Generation Services in IP Multimedia Subsystem," *Journal of Information Processing Systems*, vol. 6, no. 2, pp. 129-146, 2010.

[4] A. Madani, H. Asgharian, and A. Akbari, "Improving of Ims Sip Server Security with Vulnerability Assessment," *Proc, IEEE Int'l Conf. Science and Engineering*, pp. 45-52, 2011.

[5] S. Ghandali, and S. M. Safavi, "Modeling Multimedia Traffic in IMS Network using Mmpp," *Proc, IEEE Int'l Conf. Electronics Computer Technology*, pp. 281-286, 2011.

[6] V. S. Abhayawardhana, and R. Babbage, "A Traffic Model for the IP Multimedia Subsystem (IMS)," *Proc, IEEE Int'l Conf. Vehicular Technology*, pp. 783-787, 2007.

[7] Y. Bai, *Analysis of Enterprise VOIP Traffic from a wire Line IMS System*, Ph. D. Dissertation, Dalarna University, Falun, Sweden, 2009.

[8] D. Geneiatakis, et al., "Utilizing Bloom Filters for Detecting Flooding Attacks against Sip based Services," *Journal of Computers and Security*, vol. 28, no. 7, pp. 578-591, 2009.

[9] D. Vingarzan, et al., "Design and Implementation of an Open IMS Core," *Proc, Int'l Conf. Mobility aware Technologies and Applications*, *Springer*, pp. 284-293, 2005.

[10] An Open Source Implementation of IMS Call Session Control Functions, www.openimscore.org, 2011.

[11] Network Research Group, http://nrg.iust.ac.ir, 2012.

[12] Z. Asgharian, H. Asgharian, A. Akbari, and B. Raahemi, "Detecting Denial of Service Attacks on Sip Based Services And Proposing Solutions," *Proc, IEEE Int'l Symp. Privacy, Intrusion Detection and Response*, pp. 145-167, 2012.

[13] Z. Asgharian, H. Asgharian, A. Akbari, and B. Raahemi, "A Framework for Sip Intrusion Detection and Response Systems," *Proc, IEEE Int'l Symp. Computer Networks and Distributed Systems*, pp. 100-105, 2011.

[14] D. Simchi-Levi, and M. A. Trick, "Introduction To Little's Law As Viewed on Its 50th Anniversary," *Journal of Operations Research*, vol. 59, no. 3, pp. 535-535, 2011.

[15] D. Sisalem, J. Floroiu, J. Kuthan, U. Abend, and H. Schulzrinn, "Media Security," *Proc, Int'l Conf. Sip Security*, pp. 173-223, 2009.

مرتضی عیسی‌پره متولد ۱۳۶۴ دارای مدرک تحصیلی کارشناسی‌ارشد رشتهٔ کامپیوتر از دانشگاه علم و صنعت ایران است. امنیت شبکه‌های کامپیوتری، شبکه‌های نسل آینده و امنیت شبکه‌های نسل آینده از جمله علایق پژوهشی وی است.

آدرس پست‌الکترونیکی ایشان عبارت است از:

isapareh@comp.iust.ac.ir

حسن اصغریان متولد ۱۳۶۲ دارای مدرک تحصیلی کارشناسی‌ارشد رشتهٔ کامپیوتر از دانشگاه امیرکبیر است. وی هم‌اکنون دانشجوی دکتری در رشتهٔ کامپیوتر از دانشگاه علم و صنعت ایران است. امنیت شبکه‌های کامپیوتری، شبکه‌های چند رسانه‌ای و امنیت سرویس‌های در بستر شبکه از جمله علایق پژوهشی وی است.
آدرس پست‌الکترونیکی ایشان عبارت است از:
asgharian@iust.ac.ir

احمد اکبری متولد ۱۳۴۴ دارای مدرک دکتری در رشتهٔ کامپیوتر از دانشگاه رن فرانسه است. وی هم‌اکنون دانشیار دانشکدهٔ کامپیوتر دانشگاه علم وصنعت ایران است. پردازش سیگنال و گفتار، امنیت شبکه‌های کامپیوتری، سیستم‌های تشخیص و پاسخ به نفوذ و امنیت شبکه‌های چند رسانه‌ای از جمله علایق پژوهشی وی است.
آدرس پست‌الکترونیکی ایشان عبارت است از:
akbari@iust.ac.ir

اطلاعات بررسی مقاله:

تاریخ ارسال: ۹۲/۱/۳۱
تاریخ اصلاح: ۹۲/۵/۲۴
تاریخ قبول شدن: ۹۲/۵/۲۷
نویسنده مرتبط: حسن اصغریان، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، ایران.