فصلنامه علمي- پژوهشي
فنّاوری اطلاعات و ارتباطات ایران

سال اول، شماره‌هاي ۱و ۲، پاییز و زمستان ۱۳۸۷
صص: ٤١- ٥٤

ارزیابی پیکربندی‌های مختلف شبکه سیگنالینگ SIP با استفاده از اندازه‌گیری پارامترهای کیفیت برقراری تماس

مجتبی جهانبخش*[۱] سید وحید ازهری* مریم همایونی* احمد اکبری*

* دانشکده مهندسی کامپیوتر، دانشگاه علم وصنعت ایران

چکیده

گستردگی و تنوع سرویس‌های فراهم شده توسط شبکه‌های IP[۲] باعث شده تا انواع مختلف شبکه‌های دسترسی به سمت استفاده از این پروتکل حرکت کنند که این خود می‌تواند به مجتمع‌سازی شبکه‌های دسترسی مختلف کمک نماید. پروتکل SIP[۳] با توجه به امکاناتی چون متنی بودن، برقراری تماس انتهابه‌انتها، استقلال از نوع داده انتقالی و مهمتر از همه پشتیبانی از انواع جابجایی[٤]، انتخاب مناسبی برای پروتکل سیگنالینگ جهت برقراری ارتباط بین دو کاربر شبکه IP است. این مزایا موجب شده تا SIP به‌عنوان پروتکل سیگنالینگ در IMS[٥]، که بستر سیگنالینگ پیشنهادی برای شبکه‌های نسل آینده است، درنظرگرفته شود. با همه این مزایا، عملکرد دقیق این پروتکل در صورتی که توسط کاربران میلیونی شبکه مورد استفاده گسترده قرارگیرد، مشخص نیست. در این مقاله با استفاده از بستر تست توسعه داده شده، کارایی پروتکل SIP مورد ارزیابی دقیق قرار گرفته شده است و پارامترهایی چون تأخیر برقراری تماس، نرخ تماس‌های ناموفق و بار پردازشی پروکسی[٦] در قالب هشت پیکربندی مختلف مورد بررسی قرار گرفته است. همچنین اثر نوع پروتکل لایه انتقال TCP و UDP روی کارایی SIP تحلیل شده است. نتایج بدست آمده از این بررسی نشان می‌دهد که استفاده از SIP در شبکه‌های بزرگ مستلزم بکارگیری تکنیک‌هایی جهت متعادل نمودن بار پروکسی‌ها و همچنین جلوگیری از اضافه بارهای موقت می‌باشد.

کلید واژگان: SIP، ارزیابی کارایی، پیکره بندی، مدیریت جابجایی

۱- مقدمه

پروتکل SIP به منظور شروع، مدیریت و خاتمه نشست مابین دویا چند برنامه کاربردی مورد استفاده قرار می‌گیرد [۱]. SIP پروتکلی از نوع مشتری- سرویس‌دهنده است. برنامه‌های کاربردی تماس گیرنده یا عامل‌های کاربر در نقش مشتری‌ها و پروکسی‌ها به عنوان عناصری میانی به منظور مسیریابی پیام‌ها در این پروتکل تعبیه شده‌اند.

استفاده از SIP بخصوص برای مکالمات صوتی مبتنی بر VoIP از رشد روزافزونی برخوردار شده، تا آنجا که عملا SIP به‌عنوان پروتکل سیگنالینگ در IMS، که بستر سیگنالینگ پیشنهادی برای شبکه‌های نسل آینده است، درنظر گرفته شده است. دلایل استفاده روز افزون از SIP، قابلیت‌های منحصر به فردی نظیر امکان تفکیک ترافیک سیگنالینگ از ترافیک داده‌ها، مستقل بودن پروتکل از محتوای پیام‌ها و نیز نوع جلسه در حال تشکیل و متنی بودن پیام‌ها می‌باشد. این مزایا SIP را قادر می‌سازد تا از انواع ارتباطات چند رسانه‌ای چون مکالمات

---

۱. نویسنده عهده‌دار مکاتبات (m_jahanbakhsh@comp.iust.ac.ir)
۲.Internet Protocol (IP)
۳.Session Initionation Protocol (SIP)
٤.Mobility
٥.IP Multimedia Subsystem (IMS)
٦.Proxy

صوتی، تصویری، و نیز محاوره متنی در یک قالب واحد پشتیانی کند.

با این حال بارزترین مشخصه پروتکل SIP امکان پشتیبانی از جابجایی کاربر[۱]، ترمینال[۲]، سرویس[۳] و جلسه[۴] است. جابجایی کاربر به این معنی است که یک کاربر مشخص می‌تواند از هر نقطه دلخواه به شبکه وصل شده و از سرویس‌های SIP از جمله دریافت تماس بهره ببرد، همانگونه که می‌توان از هر نقطه به پست الکترونیکی خود دسترسی داشت. همچنین پروتکل SIP دارای مکانیزم‌هایی است که می‌توان از آنها برای دست‌به‌دست‌دهی[۵] ارتباط به هنگام جابجا شدن ترمینال بین دو شبکه استفاده نمود. با توجه به رشد چشمگیر استفاده از SIP، تحقیقات گسترده‌ای روی کارایی این پروتکل انجام شده است.

SIPStone [۲] مجموعه محکی[۶] است که درآن معیارهای متنوعی برای ارزیابی توان سرورهای پروکسی[۷]، راهنما[۸] و ثبت‌کننده[۹] در پاسخگویی به درخواست‌های SIP، پیشنهاد شده است. در [۳] یک محک دیگر برای اندازه‌گیری اثر سیستم-عامل، پیکربندی سخت‌افزاری، پایگاه‌داده و لایه انتقال انتخابی در کارایی SIP ارائه شده است. در [۴] روی چهار نوع پیاده‌سازی پروکسی که از لحاظ مدیریت رگه[۱۰] و روش تخصیص حافظه متفاوتند، آزمایش‌های عملی انجام گرفته است. نتایج این آزمایشات نشان می‌دهد که پارامترهای موثر در کارایی پروکسی را می‌توان به دو دسته تقسیم نمود: پارامترهای مرتبط با پروتکل، از قبیل طول پیام، متغیربودن طول و نامرتب بودن سربارها و پارامترهای مرتبط با نوع پیاده‌سازی سرور، مانند نحوه تخصیص منابع سیستم عامل به تراکنش‌ها. همچنین در [۵] نیز تحقیقات مشابهی در مورد اثر سیستم عامل و نوع پیاده‌سازی پروکسی روی کارایی SIP انجام شده است.

در [۶] کارایی سیگنالینگ SIP در برقراری تماس‌های VoIP با استفاده از JAIN SIP API و با در نظرگرفتن تاثیر مدت زمان مکالمه و نرخ تماس‌ها روی تأخیر برقراری تماس بین دو عامل‌کاربر[۱۱] انتهابه‌انتها مطالعه شده است. در این تحقیق از پروکسی SIP استفاده نشده است و برای سیگنالینگ SIP از پروتکل لایه انتقال UDP استفاده شده است. در [۷] با معرفی ابزاری تحت عنوان SIPPerfromer، تاثیر تأخیر پاسخ کاربر روی کارایی سرور SIP مورد تحلیل قرارگرفته است. در [۸] با قراردادن تنها یک پروکسی بین عامل‌های کاربر، مسائلی چون قابل توجه بودن هزینه امنیت در پیکربندی با تصدیق‌هویت، اثر حالتمند[۱] - بودن یا نبودن پروکسی و نوع پروتکل لایه انتقال روی کارایی پروکسی مورد مطالعه قرار گرفته است.

دسته‌ای از پژوهش‌ها بر ارزیابی کارایی SIP تحت تکنولوژی‌های دسترسی مختلف متمرکز شده‌اند. برای نمونه در [۹] با استفاده از یک پروکسی، اثر تأخیر انتقال و گم‌شدن بسته‌ها روی لینک W-CDMA، بررسی شده است. در [۱۰] تأخیر سیگنالینگ SIP در برقراری جلسات IMS برای کانال های مختلف WiMax با سرعت‌های متفاوت ارزیابی شده است. همچنین برای کاهش حجم بسته‌های SIP و تأخیر ارسال آنها از تکنیکهای فشرده‌سازی روی پیام‌های SIP استفاده شده است.

انتخاب پروتکل لایه انتقال نیز درکارایی سیگنالینگ SIP تاثیرگذار است. در [۱۱] گزینه‌های مختلف در انتخاب پروتکل لایه انتقال برای SIP مورد بررسی کیفی قرار گرفته است. در [۱۲] تاثیر بکارگیری پروتکل‌های لایه انتقال مختلف، بخصوص تاثیر مکانیزم کنترل پنجره در TCP، روی گذردهی[۲] و تأخیر برقراری تماس مورد بررسی قرار گرفته است. در [۱۳] نشان داده شده است که برخلاف تصور عام که علت استفاده متداول از UDP در برابر TCP را سربار پردازشی کم آن قلمداد می‌کنند، ممکن است نامطلوب بودن کارایی در استفاده از TCP ناشی از نحوه پیاده‌سازی پروکسی باشد.

دراین مقاله درنظرداریم به طور عمیق‌تری به تحلیل و بررسی تاثیرپذیری پارامترهای کیفیت تماس از پیکربندی‌های مختلف پروکسی سرور SIP، پروتکل انتقال بکار رفته و فاصله طرفین تماس از یکدیگر بپردازیم. از اینرو با درنظر گرفتن یک سرور به ازای هر دامنه، هزینه فرایندهای امنیتی چون تصدیق-هویت برای تمامی تماس‌های برقرارشده و تاثیر حالتمند یا بدون حالت بودن سرور، در شرایطی که تمام تماس‌ها محلی بوده و در داخل یک دامنه صورت می‌گیرند و نیز در حالتی که تماس‌ها بین دامنه‌ای هستند مورد مطالعه قرارگرفته است. به

۱.Perssonal Mobility
۲.Terminal Mobility
۳.Service Mobility
۴.Session Mobility
۵.Handoff
۶.benchmark
۷.Proxy server
۸.Redirect server
۹.Registrar
۱۰.Thread management
۱۱.User Agent (UA)

۱.stateful
۲.Throughput

علاوه تاثیر انتخاب پروتکل لایه انتقال روی پارامترهای کیفیت تماس در هریک از سناریوهای فوق بررسی شده است. معیارهای کارایی درنظرگرفته شده دراین مقاله عبارتند از: تأخیر ایجاد تماس، گذردهی سرور، منابع پردازشی سرور و نرخ خطا در ایجاد تماس به‌عنوان تابعی از میزان بار اعمال شده روی سرور.

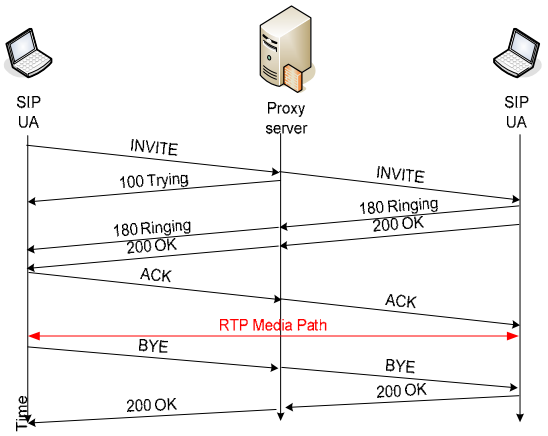
دراین مقاله با آزمایش عملی تماس‌های خارج دامنه‌ای، نقش DNS بعنوان یک گلوگاه در اینگونه تماس‌ها بررسی می‌شود و همچنین نحوه تخصیص حافظه برای پروکسی‌های SIP جهت کمرنگ کردن اثر اضافه بار مطالعه شده است.

در ادامه این مقاله ابتدا به معرفی اجمالی پروتکل SIP پرداخته و به الگوهای متداول استفاده از SIP در قالب چند مثال اشاره شده است. در بخش۳- بستر تست منطبق با الگوهای مذکور معرفی شده است. بخش ۴- شامل نتایج حاصل از انجام آزمایش‌ها به همراه تحلیل آن‌هاست. در پایان، بخش ۵- به جمع بندی و نتیجه گیری می‌پردازد.

۲- مروری بر پروتکل SIP

پروتکل SIP یک پروتکل لایه کاربرد و مبتنی بر متن می‌باشد که برای مدیریت جلسات توسط IETF استاندارد شده است. معماری این پروتکل متشکل از دو نوع نهاد منطقی تحت عنوان عامل کاربر (UA) وسرور می‌باشد. عامل‌های کاربر که خود به دوگروه عامل کاربر مشتری (UAC) وعامل کاربر سرویس‌دهنده (UAS) تقسیم می‌شوند به ترتیب به صدور درخواست و پاسخ می‌پردازند. سرورها نیز خود به چند دسته تقسیم می‌شوند. سرورهای ثبت کننده که وظیفه ثبت کردن کاربر را برعهده دارند و سرورهای راهنما با ارائه مکان‌های متعددی که ممکن است کاربر در آن جا باشد، به مکان یابی عامل کاربر SIP می‌پردازد و سرورهای پروکسی که بر خلاف سرور راهنما، خود به جستجوی کاربر مورد نظر می‌پردازند و عملا مسیر یابی برای رساندن درخواست‌ها به محل و کاربر مورد نظر، را بر عهده دارند. پروکسی‌ها ممکن است بسته به شرایط و نیاز شبکه (که در بخش۲-۱- مفصلا به آن اشاره خواهد شد)، به صورت‌های متفاوتی پیکربندی شوند. به عنوان مثال رفتار پروکسی با تراکنش‌های SIP می‌تواند حالتمند یا بدون-حالت[۱] باشد. منظور از تراکنش SIP، یک درخواست و تمامی پاسخ‌های مرتبط با آن است که بین دو عنصر مجاور SIP ردوبدل می‌شود. پروکسی حالتمند، لازم است اطلاعات حالت[۲]

۱.stateless
۲.state

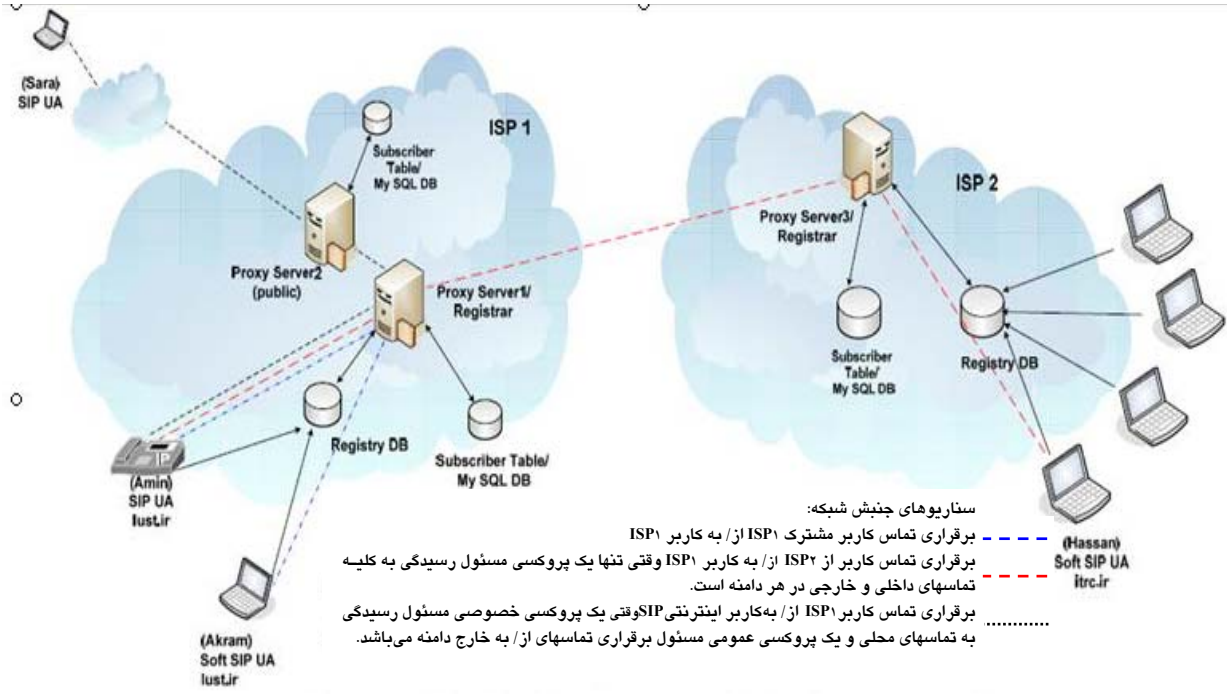


شکل۱: پیام های مبادله شده به منظور برقراری تماس درSIP

هر تراکنش را برای انجام برخی عملیات مانند ارسال مجدد احتمالی بسته‌های سیگنالینگ نگهداری کند. پروکسی‌های SIP طوری طراحی شده‌اند که می‌توانند سابقه عملیات تراکنش به ازای هر درخواست را ثبت نمایند (حالتمند) یا سابقه را ثبت نکنند (بدون حالت) [۱۴].

شکل۱ روند برقراری تماس بین دو عامل کاربر را در حالتی که پروکسی میانی به صورت حالتمند پیکربندی شده است، نشان می‌دهد. همانطور که در این شکل مشاهده می‌شود، اقدام به برقراری تماس با ارسال پیام INVITE از جانب یکی از طرفین تماس صورت می‌گیرد. با رسیدن این پیام به سرور، پاسخ Trying ۱۰۰ به سمت عامل کاربر درخواست دهنده صادر شده و پیام INVITE او به طرف دیگر مکالمه باز ارسال[۱] می‌شود. با رسیدن پیام INVITE به شخص مورد نظر، پاسخ Ringing ۱۸۰ و با برداشتن تلفن پیام پاسخ OK ۲۰۰ از جانب وی ارسال می‌شود. در نهایت پس از ارسال ACK توسط طرف اول مکالمه تماس بین طرفین برقرار می‌شود و از این پس پیام‌های مکالمه بین طرفین، بدون عبور از سرورها مبادله می‌شود. به همین ترتیب خاتمه دادن به تماس نیز با ارسال پیام BYE از سوی یکی از طرفین مکالمه و صدور پاسخ OK ۲۰۰ توسط دیگری انجام می‌گیرد. لازم به ذکر است در صورتی که پروکسی بدون حالت پیکربندی شده باشد، تراکنشی روی پروکسی ساخته نمی‌شود و پروکسی تایمری را برای پیگیری حسن انجام سیگنالینگ کاربر و ارسال‌های مجدد تنظیم نمی‌کند و در نتیجه پیام Trying ۱۰۰ نیز از جانب پروکسی ارسال نمی‌شود.

۱.forward



شکل۲: مسیر عبور سیگنالینگ تماس با توجه به معماری شبکه و مکان قرارگیری طرفین تماس

در شرایطی که لازم باشد کاربر برای دریافت سرویس، احراز هویت شود پروکسی با تصدیق هویت پیکربندی خواهدشد ومطابق شکل۳، پروکسی علاوه بر ایجاد تراکنش برای هر مکالمه، در پاسخ به INVITE اولیه پیام Unauthorized ۴۰۷ را ارسال می‌کند تا مشتری را وادار به ارائه اعتبارنامه کند. سپس مشتری INVITE مجددی ارسال می‌کند که در سربارِ Authorization آن اعتبارنامه‌اش آمده است.

با توجه به استقلال پروتکل SIP از پروتکل‌های لایه انتقال، پیامهایSIP می‌توانند روی انواع پروتکل‌های لایه انتقال اعم از TCP یا UDP منتقل شوند. با توجه به اینکه پروتکل انتقال پیش فرض،UDP است مکانیزم های ارسال مجددی درSIP تعبیه شده است که قادر است در صورت لزوم به جبران گم شدن بسته‌ها بپردازد اما در مواردی که پروتکل انتقال، TCP باشد ارسال مجدد در لایه انتقال انجام می‌شود.

۲-۱- الگوهای متداول در استفاده ازSIP

شکل۲ نحوه بکارگیری سرورهای SIP و سناریوی‌های مختلف برقراری تماس برای دو مرکز خدمات اینترنتی[۱] که سرویس VoIP مبتنی برSIP ارائه می‌دهند را نمایش می‌دهد. در این شکل:

- SIP Proxy Server/Registrar: مجموعاً سرور پروکسی SIP و سرور ثبت کننده می‌باشد که مسئول سرویس دهی به تماس‌های درون مرزی[۱] به درون مرزی و درون‌مرزی به برون مرزی[۲] است.
- Proxy Server (Public): پروکسی سرور SIP است که مسئول تماس‌های برون مرزی به درون مرزی می‌باشد و مسئولیت ثبت کردن کاربران را به عهده ندارد.
- Registery DB: پایگاه داده مربوط به کاربران ثبت شده است که با مرکز مربوطه ارتباط برخط[۳] دارند.
- Subscriber Table/ My SQL DB: حاوی اطلاعات مربوط به مشترکین مرکز مربوطه است که لزوما دارای ارتباط برخط نیستند.

همانطور که در این شکل مشاهده می‌شود وقتی امین می‌خواهد با اکرم با آدرس akram@iust.ir تماس بگیرد، پروکسی۱ با پایگاه داده ثبت خود مشورت کرده و INVITE امین را به تلفن اکرم باز ارسال می‌کند. بطور کلی اگر دو طرف مکالمه در پایگاه داده یک سرور محلی ثبت شده باشند، سیگنالینگ مربوط به مکالمه آن‌ها تنها از طریق پروکسی مربوط به همان دامنه مسیریابی می‌شود. مسیر سینگالینگ در این سناریو با خط چین کوتاه[۴] نشان‌داده شده‌است.

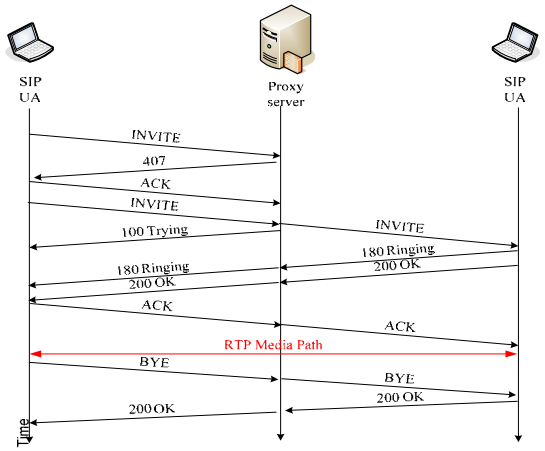
۱.Internet Service Provider (ISP)

۱.Inbound
۲.Outbound
۳.online
۴.Short dotted line

هنگامیکه امین می‌خواهد با حسن که از مشتریان ISP دیگریست تماس بگیرد باید سیگنالینگ SIP از طریق پروکسی محلی امین (پروکسی شماره۱) به پروکسی محلی حسن (پروکسی شماره۳) و از آنجا به تلفن حسن ارسال شود. در این حالت دو پروکسی وظیفه برقراری تماس را بعهده دارند و بسته‌های سیگنالینگ از مسیر نشان داده شده با خط چین طولانی در شکل۲ عبور خواهند کرد. از آنجا که در اینگونه تماس‌های برون مرزی تعداد بیشتری پروکسی دخالت دارند تأخیر ایجاد تماس و همچنین احتمال ناموفق بودن تماس بیشتر از حالت تماس‌های درون مرزی است.

تصدیق‌هویت عامل درخواست دهنده تماس، مسئله مهم دیگریست که باید مورد توجه قرار گیرد. اهمیت این قضیه از آن جهت است که باید هویت کاربر درخواست دهنده سرویس احراز شده، درصورتیکه مجاز به استفاده از آن سرویس می‌باشد به او اجازه شرکت در روند سیگنالینگ داده شود. برای مثال فرض کنید ISP۱ برای مشتریان خودش اجازه تماس با شبکه‌های خارجی از جمله PSTN را فراهم کند. از آنجا که اتصال به شبکه خارجی نیازمند خرید پهنای باند است، این ISP می‌خواهد مطمئن شود تنها مشترکان خود او می‌توانند تماس‌های خارجی برقرار کنند. برای این کار کافیست پروکسی۳ به هنگام گرفتن درخواست تماس از طرف یک مشتری مانند حسن به مقصدی چون سارا یا اکرم، از مشتری خود (حسن) تقاضای تصدیق هویت نماید اما اگر حسن تقاضای برقراری ارتباط با مشتری دیگری ازهمین ISP را داشته باشد دیگر نیازی به تصدیق هویت مجدد نخواهد بود. حتی در شرایطی برخی ISP ها بدلیل جلب مشتری اجازه می‌دهند که همه کاربران خارجی حتی اگر از مشترکان آنها نباشند، بتوانند با مشترکین ISP مذکور ارتباط برقرار نمایند. در چنین شرایطی تماس‌هایی که از خارج به داخل انجام می‌شوند نیازی به تصدیق هویت نخواهند داشت.

گاهی ممکن است تماس‌های بین مشترکین یک ISP که از طریق یک پروکسی مسیریابی می‌شوند نیز نیاز به تصدیق هویت داشته باشند. چنین سیاستی هنگامی اتخاذ می‌شود که شرکت سرویس دهنده تماس تلفنی (مثلا مبتنی بر VoIP) مستقل از ISP فراهم کننده اتصال شبکه است، باشد. از این دسته مثال های متنوعی وجود دارد که یک نمونه از آنها در[۱۵] پیاده‌سازی شده است. در شکل۳ نمونه‌ای از سیگنالینگ مربوط به برقراری تماس با تصدیق هویت نشان داده شده است.

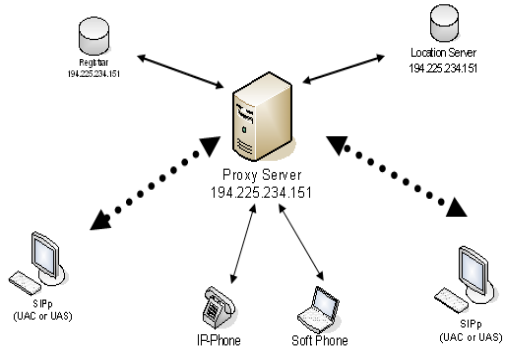


شکل۳: سناریوی یک پروکسی همراه با تصدیق هویت

همانطورکه پیش از این اشاره شد، مسأله مهم دیگر در پیکر بندی پروکسی سرور SIP، بدون‌حالت یا حالتمند بودن آن در رابطه با تراکنش‌های SIP است. پردازش پیام ها در پروکسی حالتمند شامل ایجاد، جستجو، به روز رسانی و حذف حالت تراکنش، و ایجاد و تنظیم چندین تایمر به ازای هر تراکنش می‌باشد. بنابراین هر درخواستی که به صورت حالتمند توسط پروکسی پردازش می‌شود در مقایسه با بدون حالت، نیازمند حافظه بیشتر، زمان پردازش بیشتر در CPU، رسیدگی به تایمر و به طور خلاصه صرف منابع بیشتری می‌باشد.

اگرچه در نگاه اول به نظر می‌رسد استفاده تام از پروکسی‌های بدون‌حالت سبب افزایش گذردهی پروکسی خواهد شد، اما برای مثال وقتیکه نرخ گم شدن بسته روی لینک‌های شبکه ناچیز نباشد، استفاده از پروکسی‌های بدون‌حالت که قادر به ارسال مجدد نیستند، سبب به طول انجامیدن زمان برقراری تماس خواهد شد [۱۴]. معمولا پروکسی‌هایی که مسئولیت‌هایی چون انشعاب[۱]، پیمایش NAT، رسیدگی به ارسال مجدد پیام، یافتن کاربر، و محاسبه صورت حساب را به عهده دارند حالتمند و پروکسی-هایی که تنها مسئول اعمالی چون توزیع بار و ترجمه و باز ارسال کردن پیام‌ها هستند، بدون حالت تنظیم می‌شوند [۱۶]. یکی از بهینه سازی‌های ممکن این است که پروکسی با توجه به نوع درخواست، میزان بار CPU و کیفیت لینک، تنها برای برخی از پیامهای SIP (برای مثال INVITE و BYE) ایجاد تراکنش نموده و حالتمند عمل کند [۱۴] و در مقابل هنگامیکه نرخ گم شدن بسته‌ها ناچیز باشد یا اینکه سیگنالینگ SIP از طریق TCP که یک سرویس انتقال تضمین شده است انجام شود حالت نگهداری نشود.

۱.forking



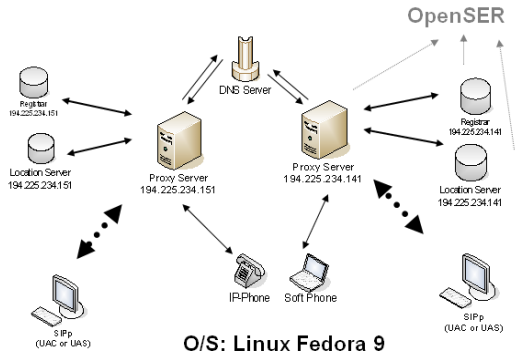
شکل۴: بستر تست برای آزمایش با یک پروکسی

دربخش بعدی بستر تست فراهم شده برای ارزیابی کارایی SIP و بررسی معیارهای ارزیابی این پروتکل از جمله تأخیر برقراری تماس و گذردهی پروکسی معرفی شده و سناریوهایی که تست آن ها به یک ارزیابی فراگیر از پروتکل SIP منجر می‌شود توضیح داده شده است. در ادامه، در بخش ۴- نتایج حاصل از بررسی کارایی SIP تحت پیکربندی های مختلف در حالاتیکه کلیه تماس‌ها داخل دامنه ای و خارج دامنه ای هستند ارائه شده است. همچنین در در بخش ۴- اثر بکارگیری هریک از پروتکل های لایه انتقال در کارایی SIP تحلیل شده است.

۳- معرفی بستر و سناریوهای آزمایش

ساختار کلی بستر تست بکار رفته برای سناریوهایی که تمامی تماس‌ها درون مرزی (یک پروکسی) و یا برون مرزی (دو پروکسی) هستند به ترتیب در شکل۴ و شکل۵ نشان داده شده است. جهت پیاده‌سازی موجودیتهای سرور از نرم افزار openSER [۱۷] استفاده شده است و هر یک از سرورها به‌ترتیب روی یک PC با پردازنده ۲٫۸GHz INTEL Dual Core و ۲٫۰GHz و حافظه ۱٫۵GB و ۲٫۰GB نصب شده اند. همچنین برای عامل‌های کاربر که وظیفه تولید ترافیک SIP را دارند از نرم افزار SIPp [۱۸] روی PC هایی با پردازنده Intel Pentium۴ ۲٫۸GHz و حافظه ۱٫۰GB استفاده شده است.

تمامی کامپیوترهای بستر تست از سیستم عامل لینوکس فدورا نسخه ۹ استفاده می‌کنند. برای بررسی زمان و نوع پیامهای ارسالی و دریافتی توسط کاربرها از گزارشاتی که SIPp تولید می‌کند استفاده شده است. همچنین از گزارشات نرم افزار openSER برای اندازه‌گیری وضعیت پیشرفت تماس‌ها و تراکنش‌های روی پروکسی استفاده شده و نرم‌افزار oProfile نیز جهت اندازه گیری بار پردازشی پروکسی بکار رفته است.



شکل۵: بستر تست برای آزمایش با دو پروکسی

پیکربندی‌های مورد مطالعه در این دو ساختار در جدول۱ نشان داده شده اند. در هر دو سناریوی شامل یک و دو پروکسی کلیه پیکربندی‌های فوق در حالتی که پروتکل لایه انتقال TCP یا UDP باشد تست و مورد مقایسه قرار گرفته‌اند.

جدول۱: سناریو های آزمون و پیکربندی های مربوطه

پیکربندی / نام سناریو	تصدیق هویت	حالتمند
WA-SF[۱]	✓	✓
WA-SL[۲]	✓	×
NA-SF[۳]	×	✓
NA-SL[۴]	×	×

۴- تحلیل نتایج ارزیابی کارایی SIP

معیارهای متعددی برای تعیین کارایی SIP وجود دارد [۱۹] که از این میان، ما در این پژوهش روی تأخیر برقراری تماس (زمان بین ارسال INVITE از طرف UAC تا زمان دریافت OK از پروکسی)، نرخ ارسال مجدد و گذردهی پروکسی (تعداد تماسهای موفق در واحد زمان) متمرکز شده‌ایم. ابتدا در بخش ۴-۱- به بررسی کارایی پروکسی تحت پیکربندی‌های گوناگون در حالتی که کاربرها درون مرزی هستند و برقراری تماس بینشان از طریق یک پروکسی صورت می‌گیرد پرداخته شده است. در بخش ۴-۲- با این فرض که دو پروکسی بین طرفین تماس واقع شده است، به بررسی نتایج در تماس‌های برون مرزی می‌پردازیم و در نهایت این بخش را با بررسی اثر بکارگیری پروتکلهای لایه انتقال TCP و UDP و مقایسه مزایا و معایب هریک به پایان می‌رسانیم.

۱.With Authentication-Stateful
۲.With Authentication-Stateless
۳.No Authentication – Stateful
٤.No Authentication - Stateless

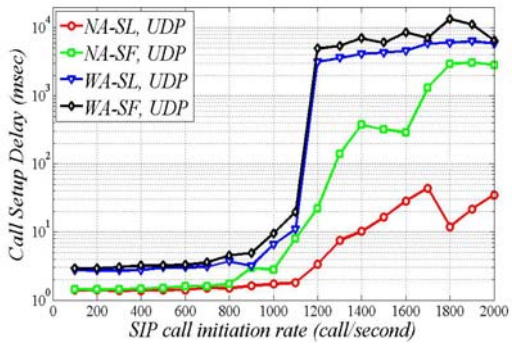
۴-۱- ارزیابی کارایی پروکسی درتماسهای درون مرزی

در این بخش به بررسی عوامل تاثیر گذار بر کارایی یک پروکسی SIP می‌پردازیم. همانطور که قبلا اشاره شد مطابق شکل۴ بار سیگنالینگ توسط دو عامل کاربر UAC و UAS تولید می‌شود. نرخ تولید مکالمه از مقدار کم ۱۰۰ تماس در ثانیه شروع شده و تا نرخ مکالمه سنگین ۲۰۰۰ تماس در ثانیه ادامه می‌یابد. در این حالت تنها یک پروکسی به مسیریابی تماس‌ها رسیدگی می‌کند.

شکل۶ میانگین زمان برقراری تماس برای چهار پیکربندی را نشان می‌دهد. با مقایسه منحنی‌های این شکل می‌توان نتیجه گرفت که هزینه انجام تصدیق هویت در پروکسی نسبتا زیاد است. برای مثال تحت بار میانه‌ای چون ۸۰۰ تماس بر ثانیه، تأخیر برقراری تماس در پیکربندیهای بدون تصدیق هویت حدودا ۲ میلی ثانیه است که کمتر از نصف تأخیر پیکربندی‌های دارای تصدیق هویت با تأخیر بیش از ۴ میلی ثانیه می‌باشد. این تفاوت همانطور که ملاحظه می‌شود در بارهای بالاتر بسیار قابل ملاحظه است تا جاییکه وقتی نرخ تماس ۱۲۰۰ در ثانیه می‌شود تأخیر ایجاد تماس برای پیکربندی WA-SF به بالای ۴ ثانیه می‌رسد.

شکل۶ همچنین اثر بدون حالت و یا حالتمند بودن پروکسی را در تأخیر برقراری تماس نشان می‌دهد. با مقایسه نمودارهای مربوط به پیکربندی NA-SF و NA-SL واضح است که پیکربندی حالتمند سبب افزایش تأخیر ایجاد تماس می‌شود. دلیل این مسئله مصرف حافظه و منابع پردازشی بیشتر توسط پروکسی برای ایجاد تراکنش برای هر مکالمه می‌باشد. البته همانطور که در منحنی‌ها نیز مشهود است، هزینه حالتمند رفتارکردن پروکسی بسیار کمتر از پشتیبانی از تصدیق هویت می‌باشد. این مطلب از روی ناچیز بودن تفاوت میان منحنی‌های تأخیر WA-SF و WA-SL مشهود است. اثر حالتمند رفتار کردن پروکسی تنها در بارهای زیاد قابل توجه است. برای مثال منحنی‌های پیکربندی NA-SF و NA-SL در بارهای میانه و کم تأخیری تقریبا مساوی دارند، در حالیکه برای بارهای بیش از ۱۰۰۰ تماس در ثانیه، تأخیر پیکربندی NA-SF نزدیک به ده برابر NA-SL می‌باشد که دلیل این مسئله در تنگنا قرار گرفتن پروکسی از لحاظ بار پردازشی و حافظه برای ذخیره‌سازی حالت یک تراکنش در پیکربندی حالتمند است.

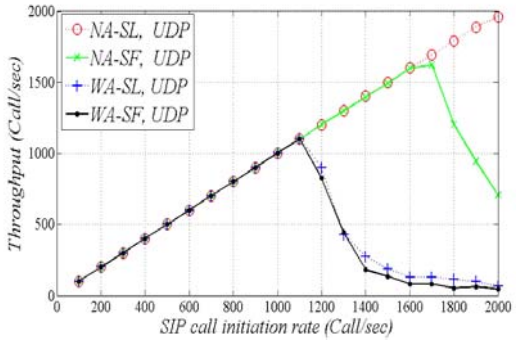
پدیده بارز دیگری که دراین شکل مشاهده می‌شود جهش تأخیر برقراری تماس برای بارهای بیش از یک حد آستانه مشخص است. در پیکربندی‌هایی که پروکسی از تصدیق هویت پشتیبانی می‌کند، مقدار این آستانه کوچکتر و درحدود ۱۱۰۰ تماس برثانیه می‌باشد و مقدار جهش نیز بسیار بزرگ است



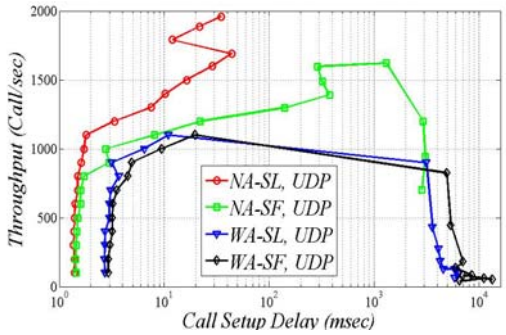
شکل۶: میانگین زمان برقراری تماس برای پیکربندی های مختلف

بطوریکه تأخیر برقراری تماس برای بار ۱۲۰۰ تماس بر ثانیه به بیش از ۳ ثانیه می‌رسد. به طور کلی علت این افزایش تأخیر را می‌توان ناشی از بالارفتن بار پردازشی CPU، کمبود حافظه جهت ایجاد تراکنش و گم شدن بسته‌ها بدلیل کمبود فضا در بافرهای سیستم عامل و بافر پروتکل SIP و در نتیجه افزایش احتمال ارسال مجدد هر پیام دانست. دلیل جهش بسیار فاحش تأخیر در پیکربندی با تصدیق هویت اینست که به ازای هر تماس یکبار دسترسی به پایگاه داده کاربران انجام می‌شود، که در بار زیاد این دسترسی به گلوگاه سیستم تبدیل می‌شود. در ادامه به بررسی موارد مطرح شده خواهیم پرداخت.

شکل۷ گذردهی پروکسی را نشان می‌دهد. در این شکل تعداد تماس‌های برقرار شده در واحد زمان برحسب نرخ درخواست تماس برای چهار پیکربندی مختلف ترسیم شده است. همانگونه که ملاحظه می‌شود در پیکربندی‌های مشتمل بر تصدیق هویت بیشترین گذردهی پروکسی در نرخ تماس ۱۱۰۰ بدست می‌آید که متناظر با پرش قابل ملاحظه تأخیر نشان داده-شده در شکل۸ می‌باشد. از این پس با افزایش بار، گذردهی پروکسی متناسب با بار ورودی افزایش نمی‌یابد که این به معنی عدم موفقیت پروکسی در برقراری برخی تماس‌هاست. همانطور که در این شکل مشهود است، پیکربندی‌های بدون تصدیق هویت از گذردهی بالاتری برخوردار هستند.



شکل۷: گذردهی پروکسی درحالت تک پروکسی

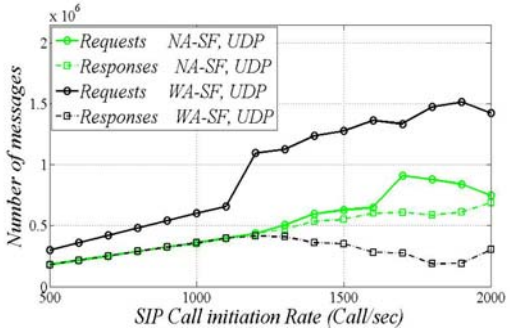


شکل۸: گذردهی پروکسی برحسب تأخیر برقراری تماس برای حالت تک پروکسی

نکته قابل ملاحظه دیگر اینست که با عبور بار از آستانه مشخصی، گذردهی پروکسی نه تنها افزایش نمی‌یابد بلکه کاهش نیز می‌یابد. به عبارت دیگر پروکسی دیگر حتی قادر نیست با همان ظرفیت گذشته خود تماس‌ها را سرویس دهد، بلکه با افزایش بار ظرفیت پروکسی کاهش می یابد.

بررسی‌های بعمل آمده روشن ساخت که این پدیده بدلیل انباشتگی بافرهای پروکسی با بسته‌های SIP می‌باشد که پس از مدتی باعث سرریز شدن آن‌ها و بالا رفتن نرخ گم شدن بسته‌ها و درنتیجه ناموفق بودن تماس‌ها می‌شود. شکل۸ نیز بر این مطلب صحه می‌گذارد زیرا نشان می‌دهد با عبور بار ورودی از یک آستانه مشخص، گذردهی شروع به کاهش می‌کند اما تأخیر همچنان افزایش می‌یابد. این افزایش تأخیر بدلیل گم شدن بسته‌های ارسالی از طرف کاربران است که منجر به ارسال مجدد بسته‌ها پس از انقضای تایمر SIP می‌شود و این خود باعث جهش تأخیر ایجاد تماس است. شاید در وهله اول اینطور به نظر برسد که با افزایش بافر پروکسی می‌توان از این مسأله جلوگیری نمود اما واقعیت آنست که با بیشتر شدن بار ورودی از ظرفیت پروکسی، مقدار بافر هر قدر هم که باشد در مدتی محدود پرخواهد شد. بنابراین باید سعی شود تا اساسا باری بیش از ظرفیت پروکسی به آن تحمیل نشود.

ارسال مجدد پیام‌ها نه تنها باعث عدم موفقیت برخی تماس‌ها می‌شود بلکه حتی اگر تماس هم موفقیت آمیز باشد برقراری آن به اندازه چند دوره انقضای تایمر SIP طول خواهد کشید که سبب افزایش تأخیر ایجاد تماس می‌شود. از طرف دیگر با افزایش تأخیر ایجاد تماس، تایمرهای عامل های کاربر منقضی شده و نرخ ارسال مجدد افزایش می‌یابد که این به نوبه خود باعث افزایش تأخیر، سرریز بیشتر بافر پروکسی و درنتیجه احتمال بیشتر گم شدن بسته‌ها می‌شود. همانطور که ملاحظه می‌کنید فیدبک مثبت ایجاد شده در سیستم باعث افت ناگهانی گذردهی پروکسی و جهش تأخیر ایجاد تماس می‌شود.

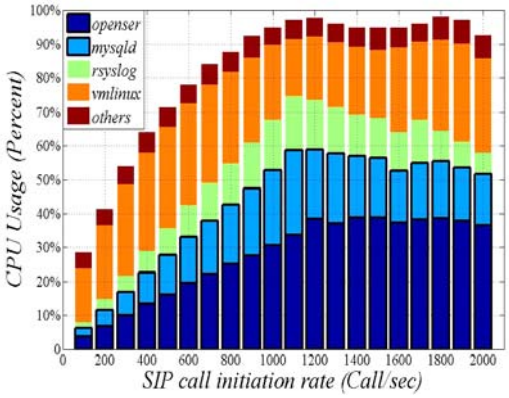


شکل۹: تقاضاها و جوابهای دریافتی در سرور پروکسی

شکل۹ تعداد درخواست‌ها و پاسخهای دریافت شده توسط پروکسی را نشان می‌دهد. دقت در این شکل صحت مطالب فوق در زمینه اثر مخرب ارسال‌های مجدد را روشن می‌کند. با توجه به این شکل، با وجود تصدیق هویت از نرخ ۱۱۰۰ به بعد، منحنی دریافت تقاضاها (که با خط ممتد نشان داده شده است) بدلیل افزایش ناگهانی ارسال‌های مجدد دچار یک جهش می‌شود. این افزایش ناگهانی تعداد تقاضاهای دریافتی، موجب سرریز شدن بافر ورودی پروکسی می‌شود که باعث گم شدن برخی بسته‌ها و درنتیجه سبب عدم پردازش برخی از تماس‌ها و کاهش تعداد پاسخ‌های دریافتی در پروکسی می‌شود (نقطه چین). درحقیقت علت کاهش گذردهی پروکسی در بارهای زیاد (شکل۷) نیز همین کاهش تعداد جلسات موفق است.

هنگامی که سرور تصدیق هویت نمی نماید از نرخ ۱۲۰۰ تا ۱۶۰۰ هر دو منحنی دریافت تقاضا و پاسخ با اندکی افزایش مواجه می‌شوند. در حقیقت در این نرخ‌ها سرور در مرحله پیگیری تماس‌ها دچار مشکل می‌شود (و نه در مرحله تجزیه کردن پیام) و پاسخهای (OK) نیز مجددا ارسال می‌شوند. در نرخ ۱۷۰۰و ۱۸۰۰ بالاترین نرخ ارسال مجدد تقاضا را داریم اما با توجه به درصد بالای ناموفقیت تماس‌ها، پروکسی اغلب اوقات درگیر تجزیه تماس‌ها و اختصاص تراکنش برای پیگیری تماس‌هاست. بنابراین تماس‌های موفق میانگین زمان برقراری تماس بالایی دارند و همچنین تماس‌های زیادی ناموفق تمام می‌شوند. شایان ذکر است که در آزمایشات مربوط به تصدیق هویت، مقدار حافظه اختصاصی بقدر کافی درنظر گرفته شده تا قبل از اینکه پردازنده به اشباع برسد، کمبود حافظه برای ایجاد تراکنش هر تماس رخ ندهد.

در موارد بدون تصدیق هویت، تعداد پیام‌ها به ازای هر تماس کمتر است. از طرف دیگر فرایند MySQL نیز اجرا نشده و بنابراین تماس‌های بیشتری توسط OpenSER پردازش



شکل ۱۰: درصد استفاده از پردازنده در پروکسی
برای پیکربندی WA_SF

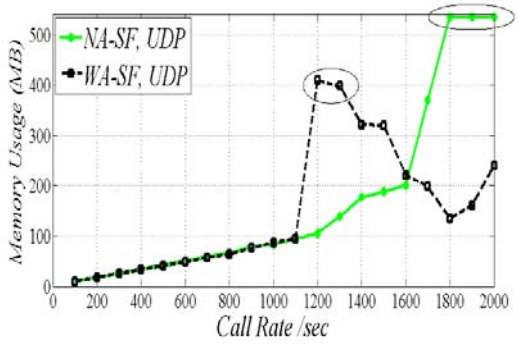
می‌شوند تا آنجا که برای نرخ تماس‌های زیاد مشکل کمبود حافظه پیش می‌آید. در چنین شرایطی سرور با ارسال خطای ۵۰۰، تعدادی از تماس‌ها را ناموفق می‌گذارد.

۴-۱-۱- منابع پردازشی وحافظه‌ای پروکسی

در این بخش اثر محدودیت حافظه و پردازنده را بر کارایی پروکسی بررسی می‌کنیم. در این آزمایشات ۵۱۲ مگابایت حافظه به OpenSER تخصیص داده شده، سپس میزان حافظه استفاده شده در طول زمان تست نیز مانیتور شده است. همچنین تعداد پیام‌های ارسالی، دریافتی و حذف شده از بافر SIP نیز مانیتور شده‌اند.

درشکل ۱۰ منابع پردازشی استفاده شده در پروکسی حالتمند با تصدیق هویت نشان داده شده است. همانطور که مشاهده می‌شود، با افزایش نرخ تماس، درصد استفاده از CPU توسط OpenSER و MySQL که به‌ترتیب عهده‌دار پردازش بسته‌های SIP و مدیریت پایگاه داده کاربران هستند، افزایش می‌یابد تا اینکه در نرخ حدود ۱۱۰۰ (قبل از جهش نمودار میانگین زمان برقراری تماس) کارایی پردازنده تقریبا به ۱۰۰٪ می‌رسد. از این پس با افزایش بار منابع پردازشی بیشتری به این دو فرایند اختصاص نمی یابند که در نتیجه این امر، از این نرخ به بعد، تأخیر برقراری تماس‌ها شدیدا افزایش می‌یابد.

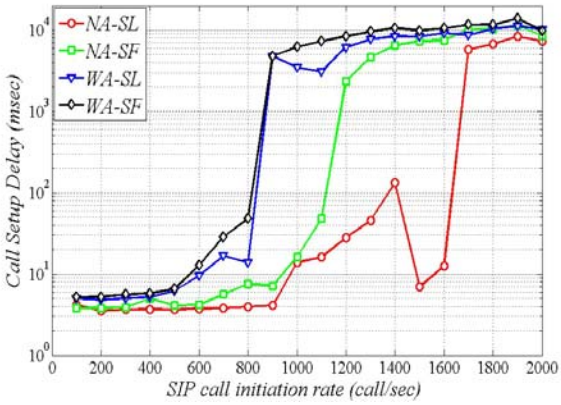
درشکل ۱۱ حداکثر میزان حافظه اشتراکی استفاده شده در پروکسی نشان داده شده است که بطور طبیعی تابعی صعودی از نرخ تماس است. در منحنی نقطه‌چین که پروکسی باتصدیق هویت و حالتمند است، درنرخ ۱۲۰۰ و ۱۳۰۰ تماس در ثانیه استفاده ازحافظه به بالاترین حد خود رسیده است. در این دوحالت سرور تقاضاهای بسیاری را تجزیه می‌کند و برای آنها ایجاد تراکنش می‌نماید، اما بدلیل کمبود



شکل ۱۱: حداکثر میزان حافظه استفاده شده توسط فرایند OpenSER

منابع پردازشی، زمان برقراری تماس بسیار بالاست و تعدادی از تماس‌ها با شکست مواجه می‌شوند. با بالاتر رفتن نرخ ایجاد تماس قسمت اعظم پیام‌ها یا INVITE هستند و یا ارسال مجدد آن. درنتیجه پروکسی بیشتر درگیر تجزیه تماس-ها و انجام عملیات مربوط به تصدیق هویت و ارتباط با پایگاه داده است. بنابراین پیام‌های کمتری به فاز تخصیص تراکنش و ارسال به مقصد می‌رسند که این منجر به کاهش حافظه مورد استفاده توسط پروکسی می‌شود. در منحنی بدون تصدیق هویت و حالتمند حافظه پروکسی در نرخ‌های بالاتر از ۱۸۰۰ تماس بر ثانیه به حد اشباع می‌رسد. در این وضعیت تعداد تراکنش‌های فعال بسیار بالا می‌رود (بالغ بر ۷۰۰۰۰) و چون سرور حافظه کافی برای تماس‌های جدید ندارد با خطای ۵۰۰ که به منزله خطای داخلی سرور است کاربرهای جدید را از اصرار بر تقاضای تماس منصرف می‌کند. همچنین با پرشدن حافظه پروکسی بر تعداد بسته‌های گم شده نیز افزوده می‌شود.

این دو نمودار نشان می‌دهند که کارایی پروکسی متاثر از دو عامل است: مقدار حافظه تخصیص یافته به آن و قدرت پردازشی پردازنده‌ای که پروکسی بر روی آن اجرا می‌شود. همانطور که ملاحظه شد اشباع پردازنده و کمبود حافظه هر دو باعث افت شدید کارایی پروکسی می‌شوند. شایان ذکر است با محدود نمودن حافظه اختصاص داده شده به پروکسی می‌توان آن را از قبول تماس‌های بیش از ظرفیتش بازداشت. در چنین شرایطی پردازنده پروکسی هیچگاه به حد اشباع نخواهد رسید و با ارسال بسته ۵۰۰ از جانب پروکسی تماس‌های اضافی به وجود نمی‌آید. البته ذکر این نکته ضروری است که این سیاست تا حد مشخصی کارایی پروکسی را بهبود می‌دهد و با بالا رفتن نرخ تماس‌ها پردازنده پروکسی که ناگزیر است تمامی بسته‌های دریافتی را جهت اطلاع از محتویات آن‌ها تجزیه



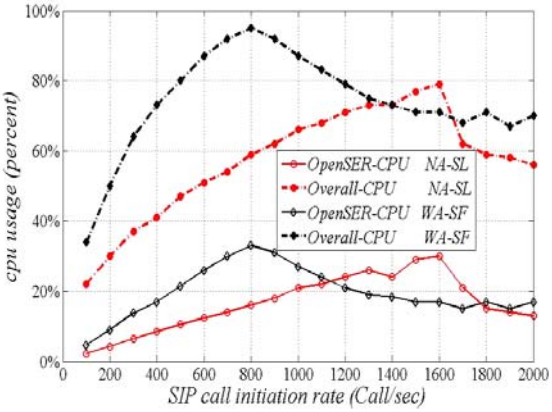
شکل۱۲: بررسی میانگین زمان برقراری تماس با انجام DNS

نماید باز هم به اشباع خواهد رسید، اگرچه این رخداد تحت بارهای بالاتری اتفاق خواهد افتاد.

۴-۲- ارزیابی کارایی در تماس‌های برون مرزی با وجود دو پروکسی

هنگامی که تماس‌ها برون مرزی باشند مسیر سیگنالینگ بین پروکسی های مربوط به هر دامنه خواهد بود. مطابق شکل۵ بار سیگنالینگ توسط دو عامل کاربر UAC و UAS تولید می‌شود. نرخ تولید مکالمه از مقدار کم شروع شده و تا نرخ مکالمه سنگین ادامه می یابد. وقتی که یک تقاضای خارج دامنه‌ای به پروکسی می‌رسد، پروکسی ابتدا با ارسال تقاضای DNS، آدرس IP پروکسی شبکه مقصد را پیدا می کند و در ادامه تقاضا را به آن ارسال می‌کند. تماس با DNS تاخیر زمان برقراری تماس را کمی بیشتر می‌کند. یک راه حل، نگهداری آدرس پروکسی‌های فعال اطراف، در حافظه نهان[1] پروکسی است. البته این روش برای مواقعی که از DNS برای توزیع بار بین پروکسی‌های مختلف استفاده می‌شود مناسب نیست [۲۰].

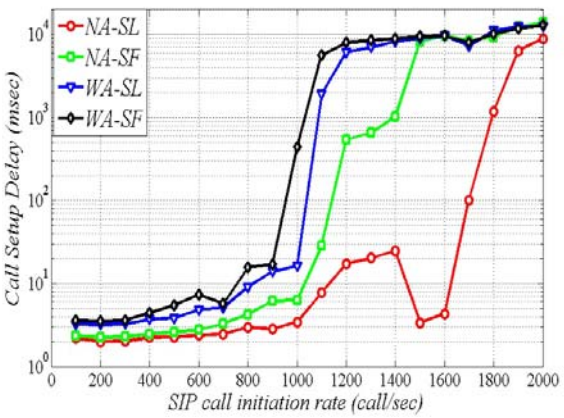
در شکل۱۲ تأخیر زمان برقراری تماس برای چهار حالت تست نشان داده شده است. در اینجا آدرس شبکه پروکسی‌های اطراف در آدرس نهان وجود ندارد و برای هر تقاضا یک پروسه DNS انجام می‌شود. تفاوت این شکل با حالت تک پروکسی، بالاتر بودن تأخیر برقراری تماس در نرخ‌های یکسان و جهش تأخیر برقراری تماس در نرخ‌های کمتر است. این افزایش تأخیر بدلیل اضافه شدن یک پروکسی دیگر در مسیر سیگنالینگ و همچنین تقاضای DNS است. تاثیر پروسه DNS در تأخیر و مقیاس پذیری سرور هنگامی واضحتر می‌شود که بار پردازشی CPU مورد بررسی قرار گیرد. در شکل۱۳ تاثیر پروسه DNS روی



شکل۱۳: بار پردازشی کل پردازنده و بار پردازشی پروسه OpenSER وقتی که پروکسی حالتمند و باتصدیق هویت است و وقتیکه بدون حالت و بدون تصدیق هویت است.

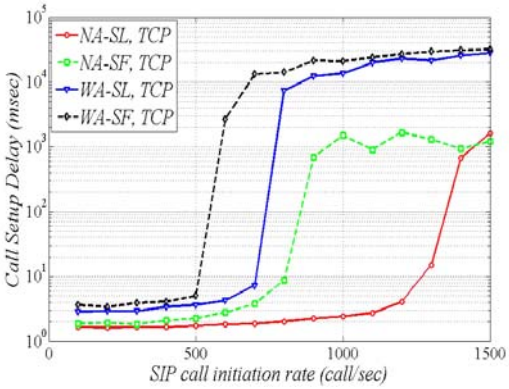
پروکسی حالتمند- با تصدیق هویت و بدون حالت-بدون تصدیق هویت نشان داده شده است. با توجه به این شکل تا قبل از اشباع سرور حالتمند و با تصدیق هویت روند مصرف CPU رو به افزایش است. اما برخلاف تصور در نرخ‌های بالاتر مصرف CPU و بار پردازشی پروسه OpenSER کاهش می‌یابد. این مساله برای سرور بدون حالت و بدون تصدیق هویت (کمترین بار اجرایی) نیز صادق است با این تفاوت که پردازنده هیچگاه اشباع نمی‌شود.

بررسی‌های انجام شده نشان داد که علت بالارفتن تأخیر تماس‌ها با وجود اشباع نبودن بار پردازنده در نرخ‌های بالا تأخیر پروسه DNS می‌باشد در حین ردوبدل شدن تقاضای DNS پردازنده عملا درحال انتظار می‌ماند و بنابراین با وجود اشباع نبودن پردازنده پروکسی، پروکسی عملا از پردازش تماس‌ها باز می‌ماند. با بهینه‌کردن پیاده‌سازی پروکسی می‌توان از این زمان‌های انتظار درجهت پذیرش تماس‌های بیشتر استفاده نمود. همانطور که ذکر شد سیاست قراردادن آدرس ها در حافظه نهان، راه کار مناسبی برای افزایش کارایی پردازنده پروکسی می‌باشد. از همین رو در نمودار شکل۱۴ پروسه DNS را حذف کرده‌ایم و از آدرس‌دهی



شکل۱۴: بررسی میانگین زمان برقراری تماس بدون انجام DNS

۱.cache



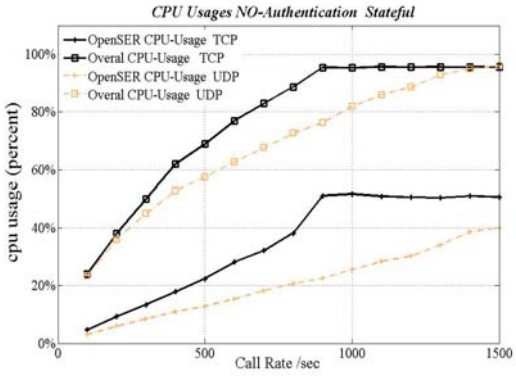
شکل۱۵: میانگین زمان برقراری تماسها برحسب نرخ ایجاد تماس با استفاده از پروتکل TCP

مستقیم برای ارسال بسته‌ها بین پروکسی‌ها استفاده نموده‌ایم. دراین حالت دیگربار پردازنده پروکسی برخلاف شکل۱۳ کاهش نمی‌یابد و همچنین میزان حذف بسته‌ها به کمترین حد خود می‌رسد.

با مقایسه شکل۱۲ و شکل۱۴ متوجه می‌شویم که میانگین زمان برقراری تماس بهبود پیدا کرده است و جهش تأخیر نیز در نرخ تماس بالاتری رخ می‌دهد. البته بدیهی است که تأخیر برقراری تماس از حالت تک پروکسی کمی بیشتر است. به‌علاوه بررسی وضعیت تماس‌ها نشان می‌دهند که با حذف فرایند DNS تعداد تماس‌های ناموفق هم کاهش یافتند.

۴-۳- تاثیر پروتکل لایه انتقال

درشکل۱۵ میانگین زمان برقراری تماس هنگامیکه سیگنالینگ SIP توسط پروتکل انتقال TCP حمل می‌شود نشان داده شده است. در مقایسه با پروتکل UDP این منحنی‌ها از نرخ ۱۰۰ تا ۱۵۰۰ تماس در ثانیه تولید شده‌اند زیرا در نرخ‌های بالاتر فرایند کنترل ازدحام TCP عملا از ارسال هرگونه بسته‌ای به پروکسی جلوگیری می‌کند. رفتار کلی این نمودار مانند نمودارهای پروتکل UDP است با این تفاوت که تأخیر در نرخ‌های پایینتر در حالات مشابه کمی‌بالاتر است و همچنین جهش‌ها در نرخ کمتری اتفاق افتاده‌اند. جهش زودهنگام منحنی‌ها در این حالت (نسبت به استفاده از UDP) ناشی از بار پردازشی بیشتر و نیاز به حافظه بیشتر برای برقراری یک ارتباط TCP درمقایسه با UDP می‌باشد. همچنین فرایند کنترل ازدحام پروتکل TCP نرخ ارسال بسته‌های SIP را به پروکسی کاهش می‌دهد که باعث افزایش تأخیر ایجاد تماس می‌شود. بعلاوه برای ایجاد ارتباط TCP بین پروکسی‌ها و بین عامل‌های کاربر و پروکسی‌ها احتیاج به یک دستدهی سه طرفه[۱] است که خود به تأخیر ایجاد تماس می‌افزاید.



شکل۱۶: مقایسه بار پردازشی پروتکل TCP وUDP در هنگامی که سرور حالتمند و بدون تصدیق هویت است

در شکل۱۶ میزان بار پردازشی برای حالتیکه پروتکل لایه انتقال UDP و TCP است مقایسه شده است. در این شکل میزان استفاده OpenSER از CPU و بار کلی CPU در شرایطی که پروکسی حالتمند و بدون تصدیق هویت است نشان داده شده است. طبق این شکل در نرخ حدود ۹۰۰ که نقطه جهش نمودار تأخیر نیز می‌باشد، میزان استفاده از CPU به بالاترین حد خود رسیده است. این درحالی است که هنگامی که از پروتکل UDP استفاده می‌کنیم در نرخهای بالاتر هم پردازنده اشباع نمی‌شود. بنابراین می‌توان نتیجه گرفت که اگرچه استفاده از TCP بدلیل دارا بودن مکانیزم کنترل ازدحام باعث تخفیف در افت گذردهی پروکسی می‌شود اما هزینه پردازشی و حافظه‌ای فزاینده‌ای را به پروکسی تحمیل می‌کند که باعث افزایش تأخیر برقراری تماس و کاهش ظرفیت پروکسی می‌شود.

۵- مشاهدات و پیشنهادات

نتایج حاصل از تست‌های متنوع انجام شده روی بستر تست که برای انواع شرایط بار کم، میانه و سنگین انجام شده است، نشان می‌دهد که بالا رفتن نرخ درخواست تماس منجر به افزایش ناگهانی تأخیر ایجاد تماس و افت گذردهی پروکسی شده و درنتیجه نرخ تماس‌های ناموفق افزایش می‌یابد. دلیل این مسئله اینست که پروتکل SIP عملا هیچگونه واکنشی نسبت به ازدحام پروکسی نشان نمی‌دهد بلکه با ارسال های مجدد، بافر پروکسی را بیهوده پر نموده و منجر به گم شدن بیشتر بسته‌ها و درنتیجه افزایش مضاعف ارسال‌های مجدد می‌شود تا آنجا که عملا بافر پروکسی بخش بزرگی از ظرفیت خود را صرف بسته‌های تکراری خواهد کرد و از دریافت تماس‌های جدید باز خواهد ماند.

۱.Tree way handshaking

در این راستا دو راه حل بالقوه وجود دارد. اولین و ساده ترین آنها استفاده از پروتکل TCP بعنوان لایه انتقال برای SIP است. از آنجاییکه TCP بطور ذاتی دارای قابلیت کنترل جریان ترافیک و ازدحام است، می‌توان امیدوار بود که در مواردیکه بار پروکسی زیاد است از ارسال‌های بیهوده جلوگیری نماید. اما آزمایشات انجام شده نشان دادند که تأخیر ایجاد تماس در حالت TCP بسیار بالاتر از UDP است. علیرغم نتایج بدست آمده می‌توان از پروتکل TCP برای ارتباط بین دو پروکسی استفاده نمود. در حقیقت در صورتی که ارتباطات TCP بین دو پروکسی بصورت بهینه پیاده‌سازی شده و تمامی تماس‌های بین دو دامنه از طریق یک ارتباط TCP بین دو پروکسی سرویس دهی شوند پروتکل TCP مناسب عمل می‌کند. به هرصورت ارتباط کاربران با پروکسی طبق نتایج بدست آمده نامناسب است.

راه حل دیگر استفاده از UDP و کنترل بار اضافه است. ایده اصلی اینست که بجای قبول بار بیش از حد و ایجاد نشدن درصدی از تماسها بهتر است این تعداد تماس اصلا توسط پروکسی پردازش نشوند تا اینکه بار کمتر شده و تأخیر ایجاد تماس کاهش یابد. برای پیاده‌سازی چنین راه حلی می‌توان از ارسال پیامهای ردهٔ ۵۰۰ به عامل‌های کاربر استفاده نمود. عامل کاربر به محض دریافت این پیام از ادامه سیگنالینگ منصرف می‌شود و در نتیجه بار پروکسی را بیش از آنچه هست افزایش نمی‌دهد.

نظر به اینکه در شرایط اضافه بار، مخربترین پدیده که منجر به افزایش بیش از حد انتظار بار ورودی به سرور و نهایتا از کارافتادن آن می‌شود، ارسال‌های مجدد هستند، یک راه حل متفاوت برای کاهش بار مضاعف پروکسی، تغییر قانون تنظیم تایمر ارسال مجدد درعاملهای کاربر و سایر پروکسی‌هاست. برای این کار باید پس از هر بار انقضای تایمر مقدار آنرا بیش ازحالت استاندارد قرار داد. برای مثال می‌توان تایمر را هربار که منقضی می‌شود بجای دو برابر کردن، سه برابر نمود. بدین صورت طی یک زمان مشخص درخواست‌های کمتری و درنتیجه بار کمتری از طرف عامل کاربر به پروکسی تحمیل می‌شود. البته ایراد این راه حل اینست که اگر درشرایط بار متوسط یا کم، بسته‌ای گم شود و تایمر مربوط به آن منقضی شود، زمان برقراری تماس بسیار طولانی خواهد شد. علیرغم این ایراد لازم است متذکر شویم که در شبکه‌های فعلی که نرخ گم شدن بسته‌ها روی لینک‌ها بسیار پایین است، احتمال وقوع چنین سناریویی بسیار کم است. غالبا گم شدن بسته‌ها بدلیل ازدحام درشبکه اتفاق می افتد که در این شرایط اتفاقا هدف ما افزایش بیش از حد معمول مقدار تایمر است.

پیکربندی پروکسی از نظر تولید تراکنش به ازای هر تماس و پشتیبانی از تصدیق هویت نیز تاثیر بسزایی برکارایی پروتکل سیگنالینگ SIP و درنتیجه تأخیر برقراری تماس و نرخ تماس‌های ناموفق دارد. این مسأله بوضوح با بررسی نتایج آزمایش‌های انجام شده تحت پیکربندی‌های مختلف تایید می‌شود. نتایج نشان می‌دهند که هزینه انجام تصدیق هویت برای هر تماس بسیار زیاد است و هزینه حالتمند رفتار کردن پروکسی نیز قابل توجه می‌باشد. لذا باید سعی نمود تا جاییکه ممکن است از این پیکربندی‌ها اجتناب شود. به عنوان نمونه می‌توان به چند راهکار زیر اشاره نمود.

یک راهکار برای اجتناب از تصدیق هویت تک تک تماس‌ها از جانب موسسه‌ای که سرویس تماس SIP، مانند VoIP، را در اختیار مشترکان قرار می‌دهد این است که، به هنگام اتصال مشترکین به شبکه، آنها را با هر مکانیزم دیگری چون RADIUS تصدیق هویت نموده، سپس اجازه دسترسی به شبکه و جزئی از آن که همان پروکسی SIP است صادر شود. در چنین شرایطی تنها کاربرانی که اشتراک سرویس SIP دارند می‌توانند به شبکه وصل شوند و دیگر احتیاجی به تصدیق هویت نخواهد بود. البته ممکن است مشترکین از طریق یک شبکه دیگر (برای مثال از محل کار خود) بخواهند با پروکسی خود ارتباط برقرار نمایند که در اینصورت استفاده از تصدیق هویت اجتناب ناپذیر خواهد بود. در هر حال با این روش تعداد کاربرانی که نیاز به تصدیق هویت خواهند داشت به طور قابل ملاحظه‌ای کاهش می‌یابد.

استفاده از تکنولوژی VPN نیز می‌تواند به حذف تصدیق هویت در پروکسی SIP کمک کند. در شرایطی که مشترکین سرویس SIP، اتصال شبکه خود را از طریق دیگری بجز شرکتی که به آنها سرویس SIP می‌دهد فراهم می‌کنند، شرکت سرویس دهنده SIP می‌تواند به محض ثبت نمودن کاربر، به او یک اتصال VPN در شبکه خود بدهد. درچنین شرایطی کاربر اگرچه از اتصال شبکه دیگری استفاده می‌کند اما عملا جزو شبکه SIP محسوب می‌شود و دیگر برای برقراری تماس احتیاجی به تصدیق هویت در پروکسی نخواهد بود. البته این راهکار زمانی ناکارامد خواهد بود که تعداد مشترکینی که ثبت شوند اما لزوما درخواست برقراری تماس ندارند بسیار زیاد باشد، که این شرایط منجر به ایجاد گلوگاه روی سرور VPN خواهد شد. بطور کلی باید خاطر نشان نمود که استفاده از VPN

به عنوان یک راه حل برای رفع مشکل تصدیق هویت همواره مطلوب نیست زیرا گلوگاه را از پروکسی SIP به سرور VPN منتقل می‌کند. بلکه این راه حل در شرایطی توصیه می‌شود که بنا به دلایلی کاربران دور، به شبکه سرویس دهنده SIP با استفاده از VPN وصل می‌شوند. بعنوان مثال می‌توان از حالتی نام برد که یک دانشگاه سرویس SIP را روی شبکه داخلی خودش در اختیار کارکنانش قرار می‌دهد و همچنین کارکنان می‌توانند با استفاده از VPN از خارج دانشگاه به شبکه دانشگاه متصل شوند. در چنین حالتی دیگر حتی نیاز به تصدیق هویت کاربران خارج از دانشگاه هم نمی‌باشد.

نکته دیگری که باید به آن توجه داشت شرایطی است که هنگام جابجایی ترمینال بین دو شبکه یا دو زیر شبکه پدید می‌آید. منظور از زیر شبکه‌ها، مجموعه قلمروهای IP متفاوت هستند که زیر نظر یک مدیریت مرکزی اداره می‌شوند، مانند شبکه‌های دانشکده‌های مختلف در دانشگاه یا تمامی قلمروهای IP متفاوتی که توسط یک ISP اداره می‌شوند. در صورتیکه عمل دست‌به‌دست‌دهی بین دو زیرشبکه با مدیریت واحد انجام شود، برای بهنگام سازی مسیر جدید تماس، نیازی به تصدیق هویت با پروکسی نمی‌باشد زیرا کاربر قبلا به هنگام برقراری تماس (یا اتصال به شبکه) یک بار هویتش احراز شده است. در چنین حالتی زمان مورد نیاز برای دست‌به‌دست‌دهی و همچنین احتمال ناموفق بودن آن کم است. اما اگر کاربر درحین تماس به شبکه متفاوتی دست‌به‌دست‌دهی نماید حتما باید عمل تصدیق هویت توسط پروکسی SIP و یا هنگام درخواست اتصال به شبکه توسط سرویسی مانند RADIUS انجام شود که این باعث افزایش تأخیر دست‌به‌دست‌دهی و احتمال بروز قطعی می‌شود. متاسفانه درچنین حالتی راه حل ساده‌ای وجود ندارد مگر اینکه بین مالکین دو شبکه از قبل قراردادهایی منعقد شده باشد. برای مثال اعتبارنامه‌های یکدیگر را قبول نمایند تا مشترک یک شبکه مجبور نباشد از ابتدا احراز هویت شود.

حالتمند رفتار نمودن پروکسی SIP از دیگر عواملی است که باعث افزایش تأخیر ایجاد تماس و احیانا افزایش تأخیر دست‌به‌دست‌دهی می‌شود. لذا به عنوان یک راهکار می‌توان در شرایطی از پروکسی در وضعیت بدون حالت استفاده نمود. البته در این صورت پروکسی قادر به پیگیری فرایند تماس و ازآن جمله انجام اعمالی چون حسابرسی نخواهد بود. بنابراین یک راهکار مناسب آن است که از پروکسی‌های حالتمند برای برقراری تماس استفاده شود اما تعدادی پروکسی بدون حالت نیز در نقش توزیع کننده بار بکار روند و ترافیک عامل‌های کاربر را به یک پروکسی حالتمند با بار متعادل ارسال نمایند. با این کار می‌توان از ایجاد اضافه بار روی پروکسی‌های حالتمند و افزایش بیش ازحد تأخیر برقراری تماس و نرخ تماس‌های ناموفق جلوگیری نمود. درعین حال پروکسی‌های توزیع کننده بار در وضعیت بدون حالت کار می‌کنند و می‌توانند بدون اینکه دچار اضافه بار شوند به تعداد درخواست بیشتری سرویس بدهند.

۶- نتیجه‌گیری

دراین مقاله به تحلیل و بررسی اثر پذیری پارامترهای کیفیت تماس از جمله تأخیر ایجاد تماس، تأخیر پاسخگویی پروکسی، ارسال مجدد و نرخ خطا در ایجاد تماس به عنوان تابعی از میزان بار اعمال شده روی سرور، در پیکربندی‌های مختلف پروکسی سرور SIP پرداختیم. بدین منظور با درنظر گرفتن یک سرور به ازای هر دامنه، هزینه فرایندهای امنیتی چون تصدیق‌هویت برای تمامی تماس‌های برقرارشده و حالتمند یا بدون حالت بودن سرور، در شرایطی که تمام تماس‌ها محلی بوده و در داخل یک دامنه صورت می‌گیرند و درحالتی که تماس‌ها برون مرزی هستند بررسی گردید. به علاوه تاثیر پروتکل لایه انتقال استفاده شده در پیکربندی‌های فوق نیز، مورد مطالعه قرارگرفت.

نتایج حاصل از آزمایشات انجام شده نشان‌دهنده تاثیر پیکربندی پروکسی روی کارایی آن می‌باشد. در این میان مهمترین عامل تاثیر گذار بر کارایی سرور SIP انجام تصدیق هویت و پس از آن حالتمند رفتار کردن پروکسی است که راه حل هایی نیز برای اجتناب از آن‌ها در بخش ۵- ذکر شد.

به منظور کاهش اثر نامطلوب بار پردازشی زیاد بر روی پروکسی، حافظه اختصاص داده شده به پروکسی مورد بررسی قرار گرفت و نشان داده شد که با تعیین مناسب حافظه اختصاصی پروکسی از پذیرش تماس‌های بیش از ظرفیت پردازشگر تا حد زیادی جلوگیری می‌شود.

بررسی‌ها نشان دادند که پروتکل SIP در مواجهه با ازدحام چندان کارامد نمی‌باشد طوری که با بالا رفتن نرخ درخواست تماس، تأخیر ایجاد تماس به طور ناگهانی افزایش یافته، گذردهی پروکسی افت و نهایتا نرخ تماس‌های ناموفق افزایش یابد. بنابراین بهبود این مکانیزم یک زمینه باز تحقیقاتی بوده و مورد توجه می‌باشد.

سپاسگزاری

این کار با پشتیبانی مادی و معنوی مرکـز تحقیقـات مخـابرات ایـران انجام گرفته است. بدینوسیله از این مرکز کمال تشکر به عمل می‌آید.

مراجع

[۱] J. Rosenberg et al. , “SIP: Session Initiation Protocol”, IETF RFC ۳۲۶۱ , June ۲۰۰۲

[۲] Schulzrinne, H., Narayanan, S., LENNOX, J., AND DOYLE, M., “SIPstone – Benchmarking SIP server performance”, Tech. rep., Columbia University, Apr. ۲۰۰۲. Available from http://www.columbia.edu/

[۳] Raatikainen K., et al. "A Control Plane Benchmark for Telecommunications Signalling Applications", Linux Conf Europe, ۵th September ۲۰۰۷

[۴] M. Cortes, J. R. Ensor, and J. O. Esteban, “On SIP Performance”, Bell Labs Technical Journal, Volume ۹, Issue ۳, pp. ۱۵۵-۱۷۲, ۲۰۰۴

[۵] S. Wanke۱, M. Scharf۱, S. Kiesel۱, S. Wahl۲, "Measurement of the SIP Parsing Performance in the SIP Express Router", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Berlin / Heidelberg, Volume ۴۶۰۶ LNCS, pp. ۱۰۳-۱۱۰, ۲۰۰۷

[۶] SS Gokhale., “Signaling performance of SIP based VoIP: A measurement-based approach”, In Proc. of IEEE Globecom ’۰۵, Vol. ۲,pp. ۷۶۱-۷۶۵, Nov. ۲۰۰۵

[۷] Caixia Chi, Dong Wang, Ruibing Hao, Wei Zhou, "Performance Evaluation of SIP Servers", ۲۰۰۸

[۸] Erich M. Nahum, John Tracey, and Charles P. Wright, "Evaluating SIP Proxy Server Performance", ۱۷th International workshop on Network and Operating Systems Support for Digital Audio & Video, ۲۰۰۷

[۹] Vincent Planat, Nadjia Kara, "SIP Signaling Retransmission Analysis over ۳G network', MoMM, ۲۰۰۶

[۱۰] A. Munir, "Analysis of SIP-based IMS Session Establishment Signaling for WiMax-۳G network", Proceedings of the Fourth International Conference on Networking and Services (icns ۲۰۰۸) ,Volume ۰۰, pp.۲۸۲-۲۸۷, ۲۰۰۸

[۱۱] V. K. Gurbani, R. Jain, "Transport Protocol Considerations for Session Initiation Protocol Networks", Bell Labs Technical Journal, Volume ۹, Issue ۱, pp. ۸۳-۹۷, ۲۰۰۴

[۱۲] Masataka Ohta, "Performance Comparisons of Transport Protocols for Session Initiation Protocol Signaling", ۲۰۰۸

[۱۳] Kaushik Kumar Ram, Ian C. Fedeli, Alan L. Cox, and Scott Rixner. "Explaining the Impact of Network Transport Protocols on SIP Proxy Performance", IEEE International Symposium on Performance Analysis of Systems and software, ISPASS,pp. ۷۵-۸۴, ۲۰۰۸

[۱۴] M. Cortes, J.O. Esteban, H. Jun, " Towards Stateless Core: Improving SIP Proxy Scalability", IEEE Global Telecommunications Conference. GLOBECOM '۰۶. , pp. ۱-۶, ۲۰۰۶

[۱۵] Yul Pyun ,"SIP Deployment Notes at University of Hawaii", http://net.its.hawaii.edu/advanced/sip/index.html

[۱۶] Jan Janak, “SIP Server Effectiveness”, Master’s Thesis, Czech Technical University, Faculty Of Electrical Engineering, Department of Computer Science, ۲۰۰۳

[۱۷] www.opensips.org

[۱۸] Richard Gayraud, Olivier Jaques et al.: SIPp - SIP Load Generator., http://sipp.sourceforge.net/index.html

[۱۹] D. Malas," SIP End-to-End Performance Metrics," Internet-Draft, October ۳۱, ۲۰۰۸ (work in progress), http://www.ietf.org/internet-drafts/draft-ietf-pmol-sip-perf-etrics-۰۲.txt

[۲۰] Kundan Singh and Henning Schulzrinne, “Failover, load sharing and server architecture in SIP telephony”, Computer Communications, Volume ۳۰, Issue ۵, pp.۹۲۷-۹۴۲, March ۲۰۰۷.