بررسی اثرات حمله سیل‌آسای بسته‌های درخواست تماس در شبکه VOIP و ارائه راهکاری جدید برای تشخیص حمله

احمدرضا خواجویی نژاد[1]، حمیدرضا دلیلی اسکویی[2]، سید رضا چوگان سنبل[3]

۱دانش‌آموخته کارشناسی ارشد، دانشگاه علوم و فنون هوایی شهید ستاری، ahmadreza.khajoei@yahoo.com

۲استادیار، دانشگاه علوم و فنون هوایی شهید ستاری

۳دانش‌آموخته کارشناسی ارشد، دانشگاه علم و صنعت ایران

تاریخ دریافت: ۹۳/۲/۳ تاریخ پذیرش: ۹۴/۱/۱۷

چکیده

گسترش اینترنت، ارتباط صوتی در شبکه VOIP را امکان‌پذیر ساخته است. پروتکل SIP مهم‌ترین پروتکل علامت‌دهی در این شبکه است. این مقاله در رابطه با حملات ممانعت از سرویس‌دهی و به‌طور خاص حمله سیل‌آسای بسته‌های درخواست تماس روی پروتکل SIP است. در این نوع حملات، مهاجم با ارسال پیاپی بسته‌های درخواست تماس سرویس‌دهی سرور شبکه را مختل می‌کند. در این مقاله نحوه‌ی ایجاد حمله سیل‌آسای درخواست تماس و تأثیرات این حمله روی سرور SIP را بررسی نمودیم. نتایج این آزمایش نشان می‌دهد که با افزایش نرخ حمله، میزان مصرف پردازنده سرور افزایش می‌یابد. افزایش مصرف پردازنده خود منجر به افزایش تعداد بسته‌های تکراری ارسالی و کاهش موفقیت در برقراری نشست می‌گردد. همچنین نشان دادیم که با جایگزینی فاصله جفری به جای فاصله هلینگر تشخیص حمله سریع‌تر انجام می‌گیرد.

کلید واژه

شبکه VOIP، پروتکل SIP،حمله سیل‌آسا، فاصله جفر

مقدمه

امروزه استفاده از فناوری انتقال صدا روی پروتکل اینترنت[1] برای برقراری ارتباط صوتی بسیار متداول شده است. این فناوری هزینه‌های ارتباطی را کاهش داده و امکان برقراری ارتباط هم‌زمان بین چندین کاربر را میسر ساخته است [۱]. گسترش اینترنت، شرکت‌های مخابراتی را وادار به انتقال صدا روی پروتکل اینترنت کرد [۲]. برای برقراری یک تماس اینترنتی، ابتدا علامت‌دهی کانال رسانه صورت می‌گیرد. پس از تبدیل سیگنال‌های صوت آنالوگ به دیجیتال و کدگذاری، سیگنال دیجیتال بسته‌سازی شده و روی شبکه اینترنت منتقل می‌شود. در طرف گیرنده نیز همین مراحل به صورت معکوس روی می‌دهد [۳]. مهمترین پروتکل شبکه VOIP، پروتکل SIP[2] است. SIP یک پروتکل سرویس‌دهنده و سرویس‌گیرنده است [۴]. در این مقاله ما با سرویس‌دهنده پروکسی SIP[3] سروکار داریم.

شبکه VOIP مانند هر سیستمی آسیب‌پذیری‌هایی دارد که این شبکه را تهدید می‌کند [۵]. از این‌روی بایستی این تهدیدات را شناخت و آن‌ها را ارزیابی نمود تا بتوان با تشخیص به موقع، تلفات را به حداقل رساند. حملات ممانعت از سرویس‌دهی[4] و به ویژه حمله‌ی سیل‌آسای درخواست تماس[5] پروتکل SIP از تهدیدات مهمی است که سرویس‌دهی سرور را مختل می‌سازد.

در این مقاله، حمله سیل‌آسای بسته‌های درخواست تماس و اثرات آن روی سرور پروکسی مورد بررسی قرار می‌گیرد و با ارائه روش‌های مبتنی بر خواص آماری بسته‌های عبوری در شبکه به تشخیص حمله می‌پردازیم. در مرجع [۶]روشی پیشنهاد شده که می‌تواند با استفاده از فاصله هلینگر (HD)[6] وقوع حمله را تشخیص دهد. در این مقاله، ما فاصله جفری (JD)[7] را جایگزین هلینگر کرده و به کمک آن حمله را تشخیص می‌دهیم.

در بخش دوم مقاله حملات سیل‌آسا و به طور خاص، نحوه ایجاد و اثرات حمله سیل‌آسای درخواست تماس بررسی می‌شود. سپس به تشریح روش‌های HD و JD و تشخیص حمله با استفاده از این دو روش می‌پردازیم. در بخش سوم یک شبکه آزمایش را راه‌اندازی

1 Voice over Internet Protocol (VOIP)
2 Session Initiation Protocol
3 SIP Proxy Server

4 Denial of Service (DoS)
5 Invite Flooding Attack
6 Hellinger Distance
7 Jeffrey Distance

کرده و حمله سیل‌آسا را روی آن اعمال می‌کنیم. بخش چهارم به نمایش اثرات حمله سیل‌آسای درخواست تماس روی نمودار و تحلیل نتایج حاصل از حمله اختصاص دارد. در این بخش به کمک روش‌های HD و JD حمله را تشخیص داده و این دو روش را با هم مقایسه می‌نماییم. نهایتاً، در بخش پنجم نتیجه‌گیری کرده و پیشنهاداتی برای ادامه کار ارائه خواهد شد.

حملات سیل‌آسای پیام

حملات سیل‌آسای پیام با پیام‌های متفاوت SIP (پیام درخواست تماس[8] ، پیام ثبت‌نام[9] ، پیام انصراف[10] ، پیام اتمام[11]) ایجاد می‌گردند و پروکسی‌های متفاوتی را تهدید می‌کنند [۷]. در این حملات مهاجم با برقراری تعداد بسیار زیادی تماس عمدی، ترافیک سنگینی را ایجاد می‌کند و منجر به بروز مشکل در سه منبع زیر می‌شود [۸].

پهنای باند: با ارسال پیام‌های بسیار زیاد، پهنای باند شبکه اشغال شده و احتمال حذف پیام‌های واقعی وجود دارد [۸].

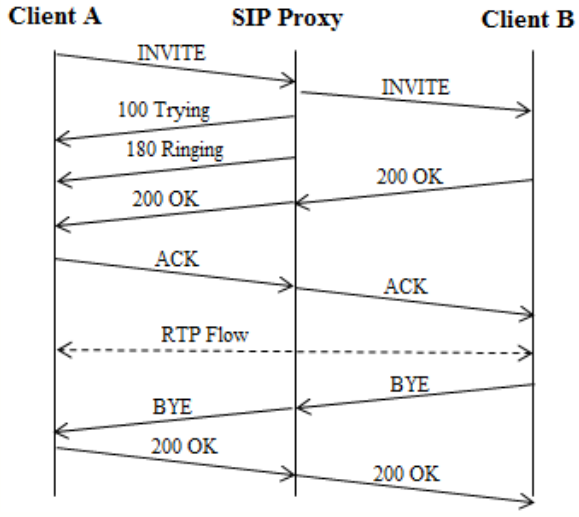
پردازنده: افزایش مصرف پردازنده سرور از مهم‌ترین اثرات مخرب حمله سیل‌آسای پیام روی سرورهای مورد حمله است. در اثر افزایش مصرف پردازنده، سرور در پاسخگویی به کاربران دچار مشکل می‌شود. در بخش‌های آتی افزایش مصرف پردازنده را به عنوان یکی از اثرات حمله بررسی خواهیم نمود [۸].

حافظه: برخی از درخواست‌های ارسالی از طرف کاربر باعث ایجاد حالت نشست[12] می‌شود. برای مثال یک پیام درخواست تماس که به سرور پروکسی ارسال می‌شود، توسط پروکسی به جلو فرستاده شده و در این حالت تا سه دقیقه منتظر جواب می‌ماند. در این فاصله زمانی حافظه خاصی در پروکسی اشغال می‌گردد. هرچه تعداد این پیام‌ها بیشتر شود، حافظه سرور پروکسی نیز بیشتر مشغول می‌شود [۸].

پیام‌های سیل‌آسای درخواست تماس، انصراف و اتمام قادرند به سرور پروکسی آسیب بزنند، چراکه تنها این پیام‌ها در آن قابل قبول هستند و در صورتی‌که پیام‌های دیگری به‌طور سیل‌آسا ارسال شوند، به راحتی توسط سرور شناسایی شده و قبل از آن‌که آسیبی برساند، سرور آن‌ها را حذف خواهد کرد [۸]. در مرجع [۱۰] میزان اثرات حملات سیل‌آسای پیام‌های متفاوت SIP، بر روی مصرف پردازنده سرور پروکسی مورد بررسی قرار گرفت. این ارزیابی نشان داد که میزان مصرف پردازنده سرور پروکسی در زمان حمله با سرعت بالا برای پیام درخواست تماس افزایش می‌یابد. این میزان برای سایر پیام‌های قابل قبول در سرور پروکسی تغییر چندانی نمی‌کند. البته میزان مصرف پردازنده برای پیام ثبت‌نام نیز افزایش می‌یابد، اما این پیام مربوط به سرور ثبت‌نام بوده و سرور پروکسی به راحتی می‌تواند آن را شناسایی و حذف نماید. در این مقاله، ما حمله سیل‌آسای بسته‌های درخواست تماس و سرور پروکسی را برای ادامه کار انتخاب نموده‌ایم.

حمله سیل‌آسای بسته‌های درخواست تماس

برای یک مکالمه مطابق شکل (۱)، ابتدا کاربر A بسته‌ی INVITE را به پروکسی ارسال می‌کند. بنابراین بسته درخواست تماس آغازگر هر مکالمه است. پروکسی بسته دریافتی را به کاربر B فرستاده و با پاسخ 100Trying به کاربر A از او می‌خواهد تا رسیدن جواب از کاربر B صبر کند. کاربر B در صورت تمایل به برقراری نشست، بسته 200ok را به پروکسی فرستاده و پروکسی نیز آن را به کاربر A تحویل می‌دهد. نهایتاً با ارسال بسته ACK نشست آغاز می‌شود. برای اتمام مکالمه هر کاربر با ارسال بسته BYE به پروکسی نشست را خاتمه می‌دهد. بنابراین چهار بسته INVITE، 200ok، ACK و BYE برای برقراری مکالمه یا نشست لازم هستند [۹].



شکل ۱. برقراری مکالمه در SIP [۹]

در حمله سیل‌آسای درخواست تماس، بسته‌های درخواست تماس به صورت طوفانی به سرور پروکسی ارسال می‌شوند، بطوریکه سرور قادر به پاسخ‌گویی به آن‌ها نباشد [۱۰].

8 INVITE
9 REGISTER
10 CANCEL
11 BYE
12 Session

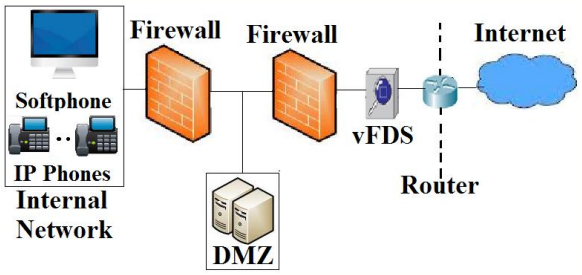
اثرات حمله سیل‌آسای بسته‌های درخواست تماس

پس از آن‌که مهاجم سیل پیام‌های درخواست تماس را به سمت سرور پروکسی روانه کرد، پروکسی SIP با دریافت هر درخواست قسمتی از حافظه خود را تا زمان رسیدن پاسخ از کاربر، به اجزایی از این درخواست اختصاص می‌دهد. وقتی مهاجم با سرعت زیاد اقدام به ارسال پیام‌های درخواست تماس نماید، حافظه سرور پروکسی به شدت مشغول می‌شود و چون تعداد بسته‌های ارسالی متناسب با توان پردازشی پردازنده سرور نبوده، لذا میزان مصرف پردازنده به شدت افزایش می‌یابد. هرچه فاصله میان ارسال دو بسته کمتر باشد و حمله چند مبدأیی باشد، شدت حمله بیشتر بوده و نتیجه آن سریع‌تر نمایان می‌شود [۱۱].

بالا رفتن میزان مصرف پردازنده کاملاً مرتبط با نرخ حمله است. در حمله‌های با نرخ زیاد سرور با افت شدید کارایی مواجه شده و کاربران به ندرت می‌توانند نشست برقرار کنند. کاهش موفقیت کاربران عادی شبکه در برقراری نشست از اثرات بعدی حمله خواهد بود. از دیگر اثرات این حمله، افزایش تعداد پیام‌های اضافی است که از طرف هر کاربر برای برقراری نشست به سرور ارسال می‌شود. با افزایش مصرف پردازنده، سرور قادر به پاسخگویی لحظه‌ای به درخواست‌ها نمی‌باشد. در نتیجه پیام‌ها منقضی شده و دوباره توسط کاربرها ارسال می‌شوند.

تشخیص حمله سیل‌آسای بسته‌های درخواست تماس

روش هلینگر یکی از روش‌های کارا در تشخیص حملات سیل‌آسا است. این روش به علت داشتن قابلیت تشخیص سریع و عدم محاسبات پیچیده مورد توجه قرار گرفته است. از این روش در منابعی نظیر [۶]، [۱۲]و [۱۳]استفاده شده است. نویسندگان در مرجع [۶]برای تشخیص حمله از خواص آماری بسته‌های عبوری در شبکه استفاده کرده‌اند. آن‌ها با در نظر گرفتن حمله به عنوان یک رفتار غیر عادی در شبکه و به کمک یک سیستم تشخیص حمله به نام (vFDS)[13] حمله را تشخیص می‌دهند. این سیستم بین ترافیک شبکه در حالت حمله و حالت نرمال (بدون حمله) تمایز قائل می‌شود. به این ترتیب که تمامی جریانات ترافیک فعلی نسبت به یک الگوی خاص سنجیده می‌شوند تا در صورت مشاهده انحراف نسبت به الگوی خاص، حمله تشخیص داده شود. در مرجع [۶]این حالت انحراف با اندازه‌گیری HD بین دو زمان آموزشی[14] و زمان تست[15] به دست می‌آید. اگر HD بدست آمده از یک حد آستانه بیشتر باشد، vFDS تشخیص حمله می‌دهد. شکل (۲) سیستم ارائه شده در [۶]را نشان می‌دهد.



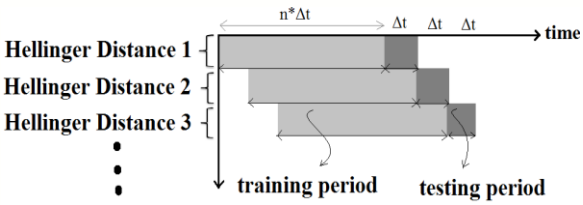
شکل ۲. شبکه VOIP [۶]

در شکل (۲) vFDS در ورودی سرورها قرار گرفته تا در صورت بروز حمله فوراً اقدام کند.

طراحی vFDS

اساس کار vFDS تشخیص حالت غیر عادی در بین مجموعه‌ای از بسته‌های عبوری در شبکه است. این تشخیص شامل دو مرحله بوده که مدام در حال تکرار است. با توجه به شکل (۳)، ابتدا از لحظه شروع تا زمانی معین خواص جریان عبوری شناسایی می‌شود. این دوره زمانی، فاصله زمانی آموزشی ($n\times\Delta t$) نام دارد. حال فاصله زمانی کوتاهی پس از اولین فاصله آموزشی به نام فاصله زمانی تست (Δt) مورد بررسی قرار می‌گیرد.

مطابق شکل (۳)، پارامترهای آموزشی و تست پی‌درپی اندازه‌گیری می‌شوند. ابتدا یک فاصله زمانی ($n\times\Delta t$)، سپس یک زمان Δt محاسبه می‌گردد. در این صورت HD در هر Δt فاصله زمانی نسبت به ($n\times\Delta t$) ثانیه قبل به دست خواهد آمد.



شکل ۳. ارتباط بین فاصله زمانی تست و آموزشی [۶]

فاصله هلینگر

فاصله هلینگر برای محاسبه دو بردار احتمال در فضای متناهی به کار می‌رود. اگر P و Q دو توزیع احتمال در فضای متناهی Ω باشند و هر کدام به ترتیب دارای N احتمال $(p_1,p_2,\ldots,p_N)$ و $(q_1,q_2,\ldots,q_N)$ باشند، با توجه به مثبت بودن مقادیر احتمالات یعنی:

$$p_\alpha \geq 0,\ q_\alpha \geq 0,\ \sum_\alpha p_\alpha = 1, \sum_\alpha q_\alpha = 1 \qquad (۱)$$

در نتیجه HD بین P و Q مطابق رابطه (۱) خواهد بود.

$$HD = d_H^2(P,Q) = \sum_{\alpha=1}^{N}(\sqrt{p_\alpha} - \sqrt{q_\alpha})^2 \qquad (۲)$$

13 VOIP Flooding Detection System
14 Training Period
15 Testing Period

در رابطه (۱)، P مربوط به احتمالات فاصله زمانی آموزشی و Q احتمالات فاصله زمانی تست است. این فاصله همواره بین صفر و یک است و در صورتی صفر می‌شود که P=Q باشد. بالاترین فاصله نیز برابر با یک به معنای بیشترین اختلاف است [۱۴]، [۱۵].

محاسبه HD برای درخواست تماس

برای محاسبه HD بایستی احتمالات وقوع چهار بسته INVITE، 200OK، ACK و BYE در زمان‌های آموزشی و تست جداگانه محاسبه شوند. اگر احتمالات وقوع بسته‌ها در زمان آموزشی با p و در زمان تست با q در نظر گرفته شوند. آن‌گاه HD برای بسته‌های درخواست تماس عبوری بین سرور و کاربر مطابق فرمول (۲) خواهد بود.

$$HD = \left(\sqrt{p_{INVITE}} - \sqrt{q_{INVITE}}\right)^2 + \left(\sqrt{p_{200\,OK}} - \sqrt{q_{200\,OK}}\right)^2 + \left(\sqrt{p_{ACK}} - \sqrt{q_{ACK}}\right)^2 + \left(\sqrt{p_{BYE}} - \sqrt{q_{BYE}}\right)^2 \quad (۳)$$

فاصله جفری و محاسبه آن برای بسته درخواست تماس

فاصله جفری همچون فاصله هلینگر برای محاسبه دو بردار احتمال در فضای متناهی به کار می‌رود. مزیت JD به HD در این است که محدودیتی در اندازه ندارد. همان‌طور که بخش قبل گفته شد، HD همواره بین صفر و یک بوده و این باعث می‌شود که HD در زمان حمله نسبت به HD در زمان نرمال افزایش شدیدی نداشته باشد. اما JD به خاطر اینکه نقاط ماکزیمم و مینیمم آن فاصله بیشتری نسبت به هم دارند، در زمان حمله فاصله بیشتری را نشان خواهد داد. در نتیجه با انتخاب یک حد آستانه مناسب، سیستم تشخیص حمله می‌تواند حمله را سریع‌تر تشخیص دهد. این موضوع در بخش آینده و با رسم نمودارها به وضوح قابل رویت است. رابطه JD مطابق فرمول (۳) است.

$$JD = \sum_{i=1}^{n}(p(i) - q(i))(ln(p(i)) - ln(q(i))) \quad (۴)$$

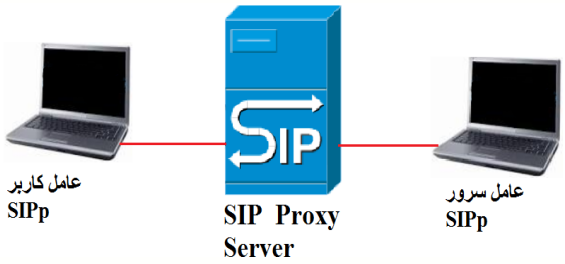
در رابطه (۳) نیز همانند رابطه (۲) احتمالات وقوع بسته‌ها در زمان آموزشی p و در زمان تست q است. از این‌روی رابطه (۳) برای چهار بسته تماس به شکل رابطه (۴) در خواهد آمد.

$$JD = (p_{INVITE} - q_{INVITE})(\ln(p_{INVITE}) - \ln(q_{INVITE})) + (p_{200\,OK} - q_{200\,OK})(\ln(p_{200\,OK}) - \ln(q_{200\,OK})) + (p_{ACK} - q_{ACK})(\ln(p_{ACK}) - \ln(q_{ACK})) + (p_{BYE} - q_{BYE})(\ln(p_{BYE}) - \ln(q_{BYE})) \quad (۵)$$

از مهم‌ترین خواص JD آن است که صفر و یا بزرگتر از صفر است. هرگاه دو توزیع احتمال P و Q برابر باشند، مقدار JD صفر می‌شود. هرچه این دو اختلاف داشته باشند، این مقدار نیز افزایش می‌یابد [۱۶].

راه‌اندازی شبکه آزمایش

شبکه آزمایش مشابه شکل (۴) است. در اینجا به دلیل حجم ناچیز بسته‌های عبوری محدودیتی برای پهنای باند در نظر گرفته نشده است. در این شبکه به کمک نرم‌افزارهایی که بر روی سیستم‌ها نصب می‌شوند، می‌توان هر تعداد کاربر را که نیاز است تعریف و تست نمود. در ادامه به معرفی نرم‌افزارهای کمکی می‌پردازیم.



شکل ۴. شبکه آزمایش اثرات حمله

تجهیزات و نرم‌افزارهای مربوطه

تجهیزات و نرم‌افزارهای مورد نیاز برای راه‌اندازی شبکه شکل (۴) به قرار زیر است. یک سیستم با حافظه 1GB، حجم هارد 20GB و یک پردازنده با فرکانس 2.50GHz را به عنوان سرور پروکسی مهیا می‌کنیم. برای این که سیستم با این مشخصات به عنوان پروکسی سرور عمل کند، می‌بایست دارای سیستم عامل لینوکس سنت‌اوس[۱۶] بوده و بر روی آن نرم‌افزار Opensips نصب گردد. این نرم‌افزار عمدتاً به عنوان یک پراکسی SIP به کار می‌رود. کلیه پیام‌های SIP باید به پراکسی SIP وارد شده و از این طریق عبور نمایند.

دو سیستم دیگر با حافظه 512MB، حجم هارد 8GB، یک پردازنده با فرکانس 2.50GHz و سیستم عامل ویندوز را بعنوان مشترکین کاربر آماده می‌نماییم. روی یکی از سیستم‌ها نسخه کاربری SIPp و روی سیستم دیگر نسخه سروری SIPp را نصب می‌کنیم. برای اینکه ما بتوانیم تعداد کاربر دلخواه برای تست شبکه در هر دو حالت نرمال و حمله داشته باشیم، باید از نرم‌افزار SIPp استفاده کنیم. این نرم‌افزار قادر است حمله‌هایی با نرخ‌های متفاوت ایجاد کند [۱۷]. در این ابزار می‌توان سناریوهای متعددی برای عملکرد عامل کاربر یا عامل سرور تعریف نمود. برای جمع‌آوری بسته‌های عبوری از نرم‌افزار Wireshark استفاده می‌شود. این نرم‌افزار روی سرور نصب شده و دائماً کارت شبکه را رصد کرده و بسته‌های عبوری را ضبط می‌کند.

16 CentOS

آزمایش شبکه در حالت بدون حمله

پس از نصب نرم‌افزارهای کاربر و سرور، شبکه در شرایط بدون حمله آزمایش می‌شود. اگر شبکه در این حالت به درستی به تراکنش‌ها پاسخ داد، می‌توان انتظار داشت که در زمان حمله پاسخ قابل استناد است. برای این کار کاربران عادی باید بتوانند در شبکه نشست برقرار کنند. با استفاده از نرم‌افزار SIPp ترافیک نرمال را ایجاد کرده و نتایج را ثبت می‌کنیم. در این مقاله موقع بررسی اثرات حمله، شرایط نرمال برقراری نشست در مدت زمان ۹۰ ثانیه برای ۳۰ کاربر است. اما در هنگام تشخیص حمله، شرایط نرمال برقراری نشست برای ۲۰ کاربر است.

ایجاد حمله با استفاده از SIPp

پس از برقراری نشست در شبکه، بایستی شبکه را در شرایط حمله آزمایش کرد. این کار توسط SIPp صورت می‌گیرد. مشابه حالت نرمال مدت زمان انجام تست برای بررسی اثرات حمله ۹۰ ثانیه است که در طول این دوره زمانی در فاصله زمانی بین ۳۰ تا ۶۰ ثانیه حملاتی با نرخ‌های ۲۰، ۵۰، ۱۰۰، ۱۵۰، ۲۵۰ و ۵۰۰ بسته در ثانیه به مدت ۳۰ ثانیه روی می‌دهد. اما برای تشخیص حمله یک زمانی ۴۸۰ ثانیه‌ای داریم که در طول این دوره زمانی حملات با نرخ‌های متفاوت روی می‌دهد. این حملات از نرخ پایین شروع شده و به تدریج افزایش می‌یابد.

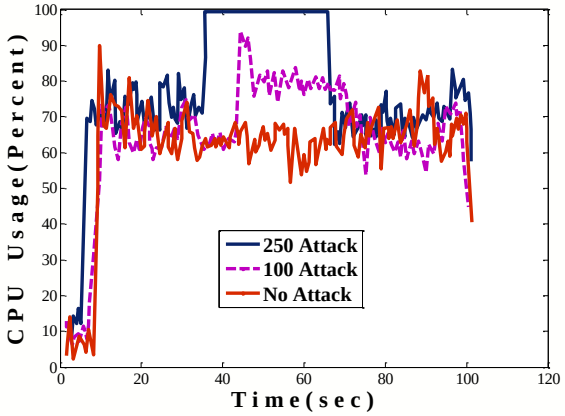
تحلیل و بررسی اثرات حمله

پس از تست شبکه در حالت نرمال و حمله، به بررسی اثرات حمله می‌پردازیم. سپس با استفاده از روش‌های HD و JD به تشخیص حمله پرداخته و این دو روش را با هم مقایسه می‌نماییم. در ادامه اثرات حمله را به‌طور جداگانه توضیح می‌دهیم.

افزایش مصرف پردازنده

افزایش مصرف پردازنده مهمترین عامل پس از وقوع حمله است که باعث افت کارایی سرور می‌شود. در بستر آزمایش ابتدا ۹۰ ثانیه بدون حمله میزان مصرف پردازنده اندازه‌گیری شد. سپس حمله‌های با نرخ‌های ۲۰، ۵۰، ۱۰۰، ۱۵۰، ۲۵۰ و ۵۰۰ به مدت ۳۰ ثانیه و در فاصله زمانی بین ۳۰ تا ۶۰ ثانیه اعمال گردید. نتیجه حاصل از حملات در نمودار شکل (۵) نشان داده شده است. محور افقی نمودار زمان بر حسب ثانیه و محور عمودی درصد مصرف پردازنده را نشان می‌دهد.

این آزمایش نشان می‌دهد که در حملات با نرخ پایین مصرف پردازنده افزایش چشمگیری ندارد. برای مثال در حمله با نرخ ۲۰ بسته بر ثانیه مصرف پردازنده مقدار کمی بیشتر از حالت بدون حمله است. با توجه به شکل (۵) وقتی نرخ حمله ۱۰۰ بسته بر ثانیه است، همچنان مصرف پردازنده افزایش شدیدی ندارد و از ۱۰۰ درصد کمتر است. اما هنگامی که نرخ حمله به بالاتر از ۲۵۰ بسته بر ثانیه می‌رسد، نمودار مصرف پردازنده همواره به ۱۰۰ درصد می‌رسد و این حالت برای حمله با نرخ ۵۰۰ نیز وجود دارد. لذا بایستی به دیگر اثرات حمله مراجعه شود تا بتوان افزایش نرخ حمله را بهتر بررسی نمود.

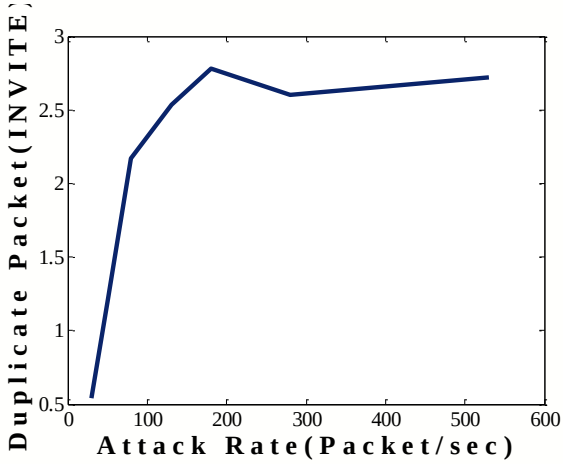


شکل ۵. درصد مصرف پردازنده در زمان‌های بدون حمله و حمله با نرخ‌های ۱۰۰ و ۲۵۰ بسته بر ثانیه

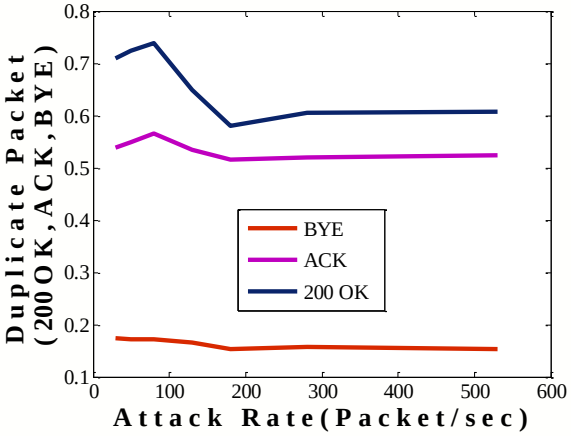
ارسال بسته‌های تکراری

با افزایش مصرف پردازنده سرور، سرور نمی‌تواند به صورت لحظه‌ای پاسخ تمامی درخواست‌ها را بدهد. لذا برخی درخواست‌ها بدون پاسخ مانده، تا این‌که تایمر عامل کاربر دوباره آن‌ها را ارسال کند. این عمل تا زمان دریافت پاسخی از سرور تکرار می‌شود.

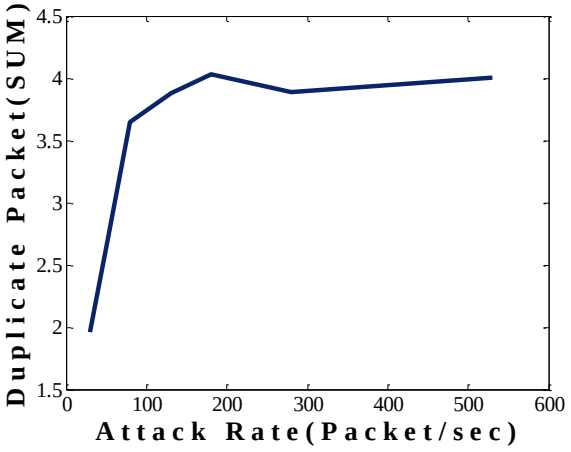
بسته به نرخ حمله، تعداد بسته‌های تکراری نیز زیاد می‌شود. شکل (۶) این موضوع را برای بسته‌ی INVITE نشان می‌دهد. این افزایش برای بسته‌ی INVITE بسیار قابل توجه بوده؛ چراکه این بسته، اولین بسته‌ای است که برای برقراری نشست ارسال می‌شود و اگر سرور نتواند به آن پاسخ دهد، سایر بسته‌ها ارسال نمی‌شوند. در زمانی که نرخ حمله ۵۰۰ بسته بر ثانیه می‌شود، این عدد برای INVITE به ۲,۷۲ می‌رسد. این بدین معناست که اگر در لحظه عادی بعد از ارسال اولین پیام INVITE از عامل کاربر به سرور، سرور پاسخ 200OK را ارسال می‌کرد، در زمان حمله با نرخ ۵۰۰ بسته بر ثانیه، هر کاربر برای دریافت پاسخ از سرور، به طور متوسط ۲,۷۲ بسته INVITE را ارسال می‌کند. شکل (۷) نشان می‌دهد که این مقادیر برای سایر بسته‌ها در زمان حمله تغییر چندانی نمی‌کند. چرا که سرور این بسته‌ها را به سمت عاملین کاربر می‌فرستد و سرور نیز درگیر پاسخ به بسته INVITE است. البته شکل (۸) حاکی از آن است که مجموع بسته‌های تکراری در زمان حمله افزایش یافته و در نرخ ۵۰۰ بسته بر ثانیه، حدوداً ۴ برابر خواهد شد.



شکل ۶. متوسط تعداد بسته‌های تکراری INVITE بر حسب نرخ حمله



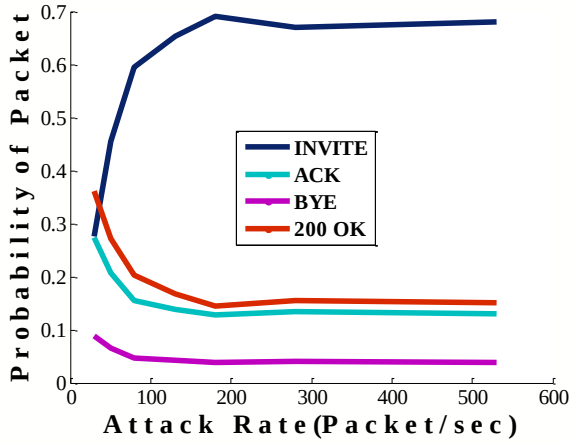
شکل ۷. متوسط تعداد بسته‌های تکراری 200 OK، ACK و BYE بر حسب نرخ حمله



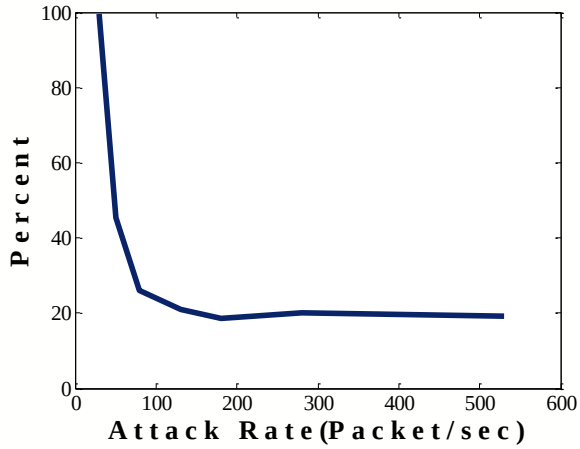
شکل ۸. متوسط مجموع بسته‌های تکراری بر حسب نرخ حمله

درصد موفقیت در برقراری نشست

در زمان حمله احتمالات مربوط به بسته‌های عبوری به شدت تغییر می‌کند. این احتمالات برابر است با: "نسبت تعداد بسته موردنظر به تعداد کل بسته‌های موجود در یک فاصله زمانی معین". این موضوع در شکل (۹) نشان داده شده است. در زمان نرمال احتمال مربوط به بسته‌های INVITE و ACK دقیقاً یکسان است. اما با افزایش نرخ حمله این مقدار بشدت تغییر می‌کند و دو مقدار کاملاً متفاوت می‌شود. برای برقراری یک نشست ابتدا بسته INVITE ارسال شده و با دریافت بسته ACK نشست برقرار می‌شود. در زمان بدون حمله چون احتمال هر دو بسته INVITE و ACK یکسان است، پس تمامی تراکنش‌ها با موفقیت انجام شده و به ازای تمام کاربرها نشست برقرار شده است. ولی موقع حمله احتمالات تغییر کرده است. این مسئله حاکی از کاهش برقراری نشست‌هاست. اگر درصد موفقیت برقراری نشست "نسبت تعداد بسته‌های ACK به تعداد بسته‌های INVITE به درصد" باشد. شکل (۱۰) نشان می‌دهد که در زمان حمله درصد موفقیت برقراری نشست یا برقراری تماس کاهش می‌یابد.



شکل ۹. احتمالات مربوط به هر بسته

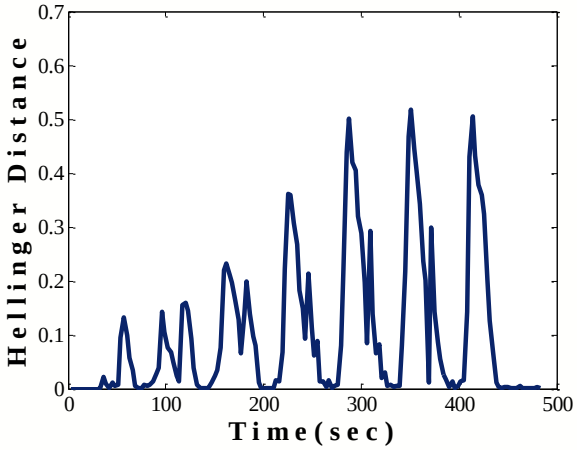


شکل ۱۰. درصد موفقیت در برقراری نشست

تشخیص حمله با استفاده از HD

برای استفاده از الگوریتم HD در تشخیص حمله، در یک فاصله زمانی مشخص (۴۸۰ ثانیه) چندین حمله با نرخ‌های متفاوت روی سرور پروکسی صورت می‌گیرد. فرض بر آن است که نرخ تراکنش شبکه در حالت نرمال ۲۰ بسته باشد، یعنی در هر ثانیه ۲۰ بسته به سمت سرور ارسال می‌شود. سپس حملاتی با نرخ‌های گوناگون بر روی سرور اعمال می‌گردد. پس از ضبط تمامی تراکنش‌ها،

احتمالات مربوط به بسته‌ها تعیین شده و با استفاده از نرم‌افزار متلب محاسبات مربوط به HD به دست خواهد آمد. نتایج در شکل (۱۱) نشان داده شده است. در این آزمایش Δt برابر ۱ ثانیه و n برابر ۳ است.

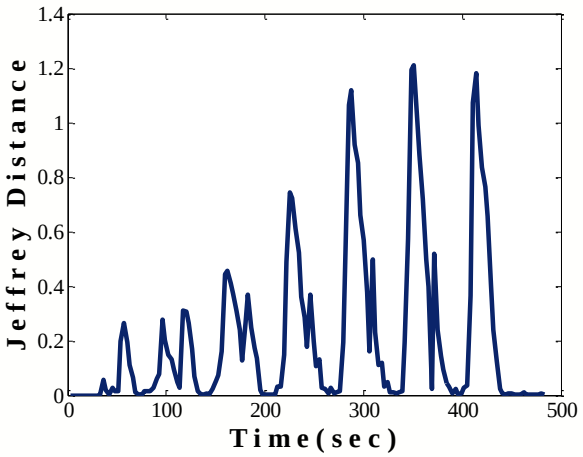


شکل ۱۱. فاصله هلینگر برای حملات با نرخ‌های متفاوت

با توجه به شکل (۱۱)، در زمان‌های مختلف حملات با نرخ‌های متفاوت رخ داده است. کمترین نرخ حمله در ثانیه‌ی ۵۰ رخ داده که این حمله حدود ۲۰ ثانیه طول کشیده است. نرخ این حمله ۲۰ بسته بر ثانیه بوده و فاصله‌ی بدست آمده برای آن ۰,۱۳۳ است. به ترتیب در زمان‌های بعدی حملات با نرخ‌های ۵۰، ۸۰، ۱۰۰، ۲۰۰، ۳۰۰ و ۵۰۰ روی می‌دهد. فاصله هلینگر برای نرخ‌های ۲۰۰، ۳۰۰ و ۵۰۰ به ترتیب ۰,۵۰۰۹، ۰,۵۱۷۵ و ۰,۵۰۴۴ است که در این زمان‌ها فاصله هلینگر افزایش یافته و مقدار تقریباً یکسانی دارند و به‌راحتی می‌توان با قرار دادن مقادیر حد آستانه مناسب حمله را تشخیص داد. همچنین در زمان‌هایی چون ۱۲۰ و ۱۸۳ نیز فاصله هلینگر قابل توجه‌ایی داریم که می‌تواند به دلیل اشکال در سرور باشد که در لحظه‌ای خاص نتوانسته به درخواست‌ها پاسخ دهد.

تشخیص حمله با استفاده از JD

در بخش قبل به چگونگی محاسبه JD اشاره شد. در این قسمت قصد داریم با استفاده از الگوریتم JD حمله سیل‌آسای بسته‌های درخواست تماس را تشخیص دهیم. این موضوع در شکل (۱۲) نشان داده شده است. در این آزمایش نیز هم چون آزمایش HD، Δt برابر ۱ ثانیه و n برابر ۳ در نظر گرفته شده است.

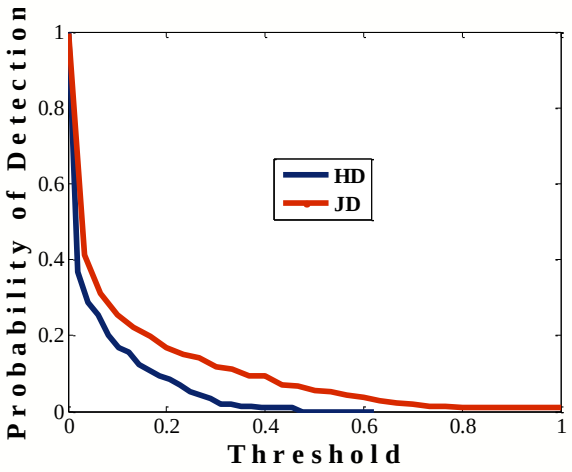


شکل ۱۲. JD برای حملات با نرخ‌های متفاوت

با توجه به شکل (۱۲) نقاط ماکزیمم (حد آستانه) و مینیمم (نقاط بدون حمله) این نمودار دارای اختلاف زیادتری نسبت به نمودار مربوط HD است. می‌توان گفت که با تعیین یک حد آستانه سریع‌تر می‌توان حمله را تشخیص داد. مثلاً برای حمله با نرخ ۲۰۰ فاصله به مقدار ۱,۱۱۸ می‌رسد که می‌تواند حد آستانه مناسبی برای سیستم تشخیص حمله باشد. همچنین به علت افزایش قابل ملاحظه عرض نقاط ماکزیمم و مینیمم، سیستم تشخیص حمله به راحتی و سریع‌تر می‌تواند حمله را شناسایی کند. در نمودار (۱۲) مانند نمودار (۱۱) در زمان‌های ۱۲۰ و ۱۸۳ نقاط ماکزیمم وجود دارد که بخاطر بروز مشکل در پاسخ‌گویی سرور بوده است.

مقایسه روش JD با HD

بخش‌های (۴-۴) و (۴-۵) نشان داد که فاصله پیشنهادی می‌توانست حمله را سریع‌تر تشخیص بدهد. اکنون این سوال مطرح می‌شود که فاصله پیشنهادی در زمینه تشخیص صحیح حمله چگونه عمل می‌کند. برای اثبات این مسئله می‌بایست برای هر دو فاصله نمودارهای مربوط به تشخیص حمله را مطابق شکل (۱۳) رسم کنیم. در این نمودار محور عمودی، احتمال تشخیص صحیح حمله و محور افقی، حدود آستانه است.



شکل ۱۳. نمودار تشخیص صحیح حمله برای HD و JD

در شکل (۱۳)، منحنی که بالاتر قرار گرفته مربوط به احتمال تشخیص صحیح حمله در حدود آستانه متفاوت برای JD و منحنی دیگر مربوط به احتمال تشخیص صحیح حمله در حدود آستانه متفاوت برای HD است. مطابق شکل (۱۳) برای یک حد آستانه مشخص مثلاً ۰/۳ احتمال تشخیص صحیح حمله برای HD و JD به ترتیب مقادیر ۰/۰۱۸ و ۰/۱۱۷ خواهد بود. این مسئله حاکی از آن است که فاصله جفری در تشخیص حمله بهتر از فاصله هلینگر عمل می‌کند.

نتیجه‌گیری

در این مقاله، امنیت شبکه VOIP مورد توجه بود. در این راستا حملات ممانعت از سرویس‌دهی و به‌طور خاص حمله سیل‌آسای بسته‌های درخواست تماس مورد بررسی قرار گرفت. حمله سیل‌آسای درخواست تماس اثرات مخربی روی سرور VOIP ایجاد می‌کند. چنانچه نرخ حمله افزایش یافته و به ۵۰۰ بسته بر ثانیه برسد، سرویس‌دهی سرور با اختلال جدی روبرو می‌شود. ما با راه‌اندازی شبکه VOIP و اعمال حملات با نرخ‌های متفاوت، اثرات حملات را بررسی نمودیم. در مرجع [۱۰]فقط به بررسی میزان مصرف پردازنده در حملات با نرخ‌های متفاوت پرداخته شده بود. اما ما علاوه بر ارزیابی میزان مصرف پردازنده، اثرات دیگر حمله نظیر افزایش تعداد بسته‌های ارسالی تکراری در شبکه و کاهش درصد موفقیت کاربرها در برقراری نشست را نیز ارزیابی کرده و برای روشن‌تر شدن موضوع در نمودارهای جداگانه رسم گردید.

در این مقاله علاوه بر اثرات حمله، سناریوی حمله سیل‌آسا و تشخیص حمله نیز در دستور کار ما بود. در مرجع [۶]از فاصله هلینگر برای تشخیص حمله استفاده شده بود. ما با ارائه یک فاصله جایگزین به نام جفری نشان دادیم که فاصله جایگزین سریع‌تر می‌تواند حمله را تشخیص دهد. همچنین با فرض یک حد آستانه ثابت، احتمال تشخیص صحیح حمله افزایش می‌یابد. آن‌چه را که به عنوان پیشنهاد برای ادامه کار مطرح می‌کنیم، کار روی راه‌های جلوگیری از ادامه حمله و اثرگذاری آن است تا بتوان اثرات مخرب حمله را به حداقل رساند.

مراجع

[1] Drew, "Next-Generation VoIP Network Architecture", MSF Technical Report, Vol. 1, pp. 3-4, 2003.

[2] Schulzrinne and Rosenberg, "A Comparison of SIP and H.323 for Internet Telephony", in Proceedings of The 8th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 98), Cambridge, UK, pp. 83–86, July 1998.

[3] Johnston, "SIP: Understanding the Session Initiation Protocol", Boston, Artech House, 2001.

[4] Davidson, Peters, "Voice over IP Fundamentals", Cisco Press, Vol. 2, pp. 223-311, 2006.

[5] Park, "Voice over IP security", Cisco Systems, Vol. 1, pp. 20-104, 2008.

[6] Hemant, Wijesekera, "Detecting VoIP Floods Using the Hellinger Distance", Ieee Transactions On Parallel And Distributed Systems, Vol. 19, No. 6, pp. 784-795, 2008.

[7] Hemant, Wijesekera, Wang, and Jajodia, "VOIP intrusion detection through interacting protocol state machines", Independable systems and networks. International Conference on IEEE, pp. 393-402, 2006.

[8] Ehlert, Geneiatakis, Magedanz, "Survey of network security systems to counter SIP-based denial-of-service attacks", 29th computers & security, pp. 225–243, 2010.

[9] Jonathan, James, "Voice over IP Fundamentals", Cisco Press, Vol. 2, pp. 223-311, 2006.

[10] Voznak, Safarik, "DoS attacks targeting SIP server and improvements of robustness", International Journal of Mathematics and Computers in Simulation, Vol. 6, Issue 1, pp. 177-184, 2012.

[11] Hemant, Wijesekera, "Detecting VoIP Floods Using the Hellinger Distance", IEEE Transactions On Parallel And Distributed Systems, Vol. 19, No. 6, pp. 794-805, 2008.

[12] Tang, Cheng, and Zhou, "Sketch-based SIP Flooding Detection Using Hellinger Distance" in Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), pp. 1–6, 2009.

[13] Hecht, Christoph, Reichl, Berger, Jung, and Gojmerac "Intrusion Detection in IMS: Experiences with a Hellinger Distance-Based Flooding Detector" In Evolving Internet, INTERNET'09, First International Conference on, IEEE, pp. 65-70, 2009.

[14] Pollard. Asymptopia. (Book in Progress), 1st edition, 2000.

[15] Fannes and Spincemaille. The mutual affinity of random measures. In eprint arXiv:math-ph/0112034, December 2000.
[16] McLachlan, Discriminant analysis and statistical pattern recognition, Wiley-Interscience, March 1992.
[17] M. Voznak, J. Rozhon, "SIP infrastructure performance testing," In Proceedings 9th WSEAS International Conference on Telecommunications and Informatics, Catania, pp. 153-158, 2010.