اثرات حمله طوفان بسته‌های ثبت نام در سیستم تلفن اینترنتی و تشخیص آن با استفاده از فاصله Kullback-Leibler

سیدرضا چوگان سنبل، محمود فتحی و محمود رمضانی میمی

چکیده: ارتباطات صوتی در بستر اینترنت و با استفاده از سیستمی به نام VoIP که شامل مجموعه‌ای از پروتکل‌ها است صورت پذیرفته و موضوع امنیت آن به شدت مورد توجه واقع گردیده است. SIP مهم‌ترین پروتکل علامت‌دهی در VoIP است که شناسایی حملات و اثرات آنها بر روی SIP می‌تواند در جهت امن‌سازی این سیستم مؤثر باشد و این مقاله به حملات طوفان ثبت نام پروتکل SIP اختصاص دارد. مهاجمین می‌توانند با ارسال پیام‌های ثبت نام به صورت طوفانی، خطرات زیادی برای کارگزار ثبت نام در بر داشته باشند. در این مقاله با بررسی حملات طوفان، حملات طوفان ثبت نام به طور جزئی‌تر تحلیل شده و اثرات این حمله بر روی کارگزار ثبت نام ذکر گردیده و در نهایت با آزمایش در یک شبکه واقعی، اثرات حمله با توجه به نرخ آن در مقابل شرایط عادی مورد ارزیابی قرار گرفته است. همچنین این مقاله به ارائه روشی برای تشخیص حملات طوفان ثبت نام پروتکل SIP اختصاص داشته و با جایگزینی فاصله Kullback-Leibler به جای فاصله Hellinger برای تشخیص حملات طوفان ثبت نام، با بهره‌گیری از نمودار ROC نشان داده شده که این روش می‌تواند در تشخیص این نوع حملات با دقت بهتر و خطای کمتری عمل نماید.

کلید واژه: **اثرات طوفان ثبت نام، امنیت VoIP، تشخیص طوفان ثبت نام، فاصله Kullback-Leibler.**

۱- مقدمه

تلفن اینترنتی (VoIP)[1] امکان استفاده از اینترنت به منظور مکالمات تلفنی را فراهم می‌نماید. در مقابل استفاده از خطوط تلفن سنتی، تلفن اینترنتی از فناوری دیجیتال استفاده می‌نماید و نیازمند یک اتصال پهن باند نظیر DSL[2] است. در واقع با استفاده از فناوری تلفن اینترنتی صدای انسان توسط بسته‌های اطلاعاتی IP و از طریق اینترنت ارسال می‌گردد. تلفن اینترنتی می‌تواند به منظور تأمین خواسته فوق از سخت‌افزارهای مختلف استفاده نماید و در یک محیط مبتنی بر کامپیوترهای شخصی استفاده شود [۱] و [۲].

سیستم تلفن اینترنتی مانند هر تکنولوژی جدیدی با جوانب مثبت و منفی همراه است. این سیستم‌ها آسیب‌پذیری‌هایی دارند که قابلیت تهدید از طرف مهاجمین به سیستم می‌باشد و در حقیقت تهدیدات بالقوه‌ای هستند که معمولاً در هر سیستمی با توجه به ساختار آن وجود داشته و مدیران امنیتی بایستی به درستی آنها را شناسایی کنند، چرا که در صورت غفلت از آنها می‌تواند به تهدید بالفعل تبدیل شده و این کار توسط مهاجمین صورت می‌پذیرد [۳]. در نتیجه بایستی تهدیداتی که از طرف آنها ایجاد می‌شود بررسی شده، اثرات و نتایج آن ارزیابی گردد تا بتوان با استفاده از ابزارهای مختلفی که در دست است جلوی سوء استفاده مهاجمین از آسیب‌پذیری‌های موجود در سیستم گرفته شود و اثرات حملات آنها کاهش یابد. از آنجا که تهدیدات طوفان ثبت نام پروتکل SIP[3]، سرویس‌دهی را با خطر جدی مواجه می‌سازد، از جمله حملات ممانعت از سرویس‌دهی[4] شناخته می‌شود لذا در این مقاله این نوع حملات بررسی شده و اثرات آن بر روی کارگزار[5] ثبت نام[6] مورد ارزیابی قرار می‌گیرد. همچنین برای تشخیص این نوع حمله در [۴] روشی پیشنهاد شده که با استفاده از فاصله Hellinger (HD)[7] می‌توان لحظه وقوع حمله را تشخیص داد. با جایگزینی فاصله Kullback-Leibler (KLD)[8] با HD در این مقاله و با استفاده از نمودارهای ROC[9] نشان داده شده که این فاصله می‌تواند حملات طوفان بسته‌های ثبت نام را با دقت بیشتر و خطای کمتری تشخیص دهد. به این معنا که با فرض یک احتمال هشدار غلط (P_{FA})[10] ثابت، احتمال تشخیص (P_D)[11] حمله با KLD بیشتر از HD است.

در بخش دوم مقاله حملات طوفان مورد بررسی قرار می‌گیرد و طوفان ثبت نام و نحوه ایجاد آن و نیز اثرات حمله به طور دقیق ذکر خواهد شد. در بخش سوم نحوه تشخیص حمله طوفان ثبت نام با استفاده از الگوریتم HD مورد بررسی قرار گرفته و پس از آن روش KLD و طریقه جایگزینی آن بیان می‌گردد. بخش چهارم به ذکر اثرات حمله طوفان ثبت نام در شبکه آزمون و نتایج و تحلیل آنها و نیز نمودارهای مختلف تشخیص حمله و در نهایت نمودار ROC مربوط به مقایسه دو روش تشخیصی اختصاص دارد. در نهایت در بخش پنجم با ارائه جمع‌بندی نهایی، پیشنهادهایی برای ادامه مقاله مطرح خواهد شد.

۲- طوفان پیام

هنگامی که در رابطه با حملات ممانعت از سرویس‌دهی بحث می‌شود، یکی از مواردی که خطرات شدیدی بر روی قربانی ایجاد می‌کند طوفان

این مقاله در تاریخ ۷ دی ماه ۱۳۹۱ دریافت و در تاریخ ۲۲ شهریور ماه ۱۳۹۲ بازنگری شد.

سیدرضا چوگان سنبل، دانشکده کامپیوتر، دانشگاه علم و صنعت ایران، تهران، (email: chogan@csri.ac.ir).

محمود فتحی، دانشکده کامپیوتر، دانشگاه علم و صنعت ایران، تهران، (email: mahfathy@iust.ac.ir).

محمود رمضانی میمی، دانشکده برق، دانشگاه شاهد، تهران (email: ma.ramezani@shahed.ac.ir).

1. Voice over IP
2. Digital Subscriber Line
3. SIP Register Flood
4. Denial of Service (DoS) Attack
5. Server
6. Registrar
7. Hellinger Distance
8. Kullback-Leibler Distance
9. Receiver Operating Characteristic (ROC) Curve
10. Probability of False Alarm
11. Probability of Detection

جدول ۱: میزان اثرات انواع حملات طوفان [۷].

نوع پیام طوفان	تأثیر بر روی پردازنده کارگزار	میزان اثر حمله
REGISTER	افزایش شدید مصرف پردازنده حتی در زمان حمله با سرعت کم	بسیار زیاد
INVITE	افزایش مصرف پردازنده بسته به سرعت حمله	زیاد
CANCEL ،BYE ،ACK	افزایش کم مصرف پردازنده	کم
OPTIONS	افزایش بسیار کم مصرف پردازنده	خیلی کم

پیام است. مهاجمین از این حمله در برابر سه منبع مهم شبکه تلفنی بهره می‌برند. این سه منبع عبارتند از پهنای باند[1]، پردازنده[2] و حافظه[3]. مهاجم مهاجم با ارسال طوفانی از پیام‌ها برای این سه منبع ایجاد خطر کرده و آنها را اشغال می‌نماید.

پهنای باند: هنگامی که پیام‌های زیادی از طرف مهاجم در شبکه ارسال گردد، پهنای باند زیادی توسط آنها مصرف می‌شود و در نتیجه احتمال حذف پیام‌های واقعی افزایش می‌یابد. البته ذکر این نکته مهم به نظر می‌رسد که این حمله مختص SIP نبوده و برای کل شبکه اینترنت به حساب می‌آید [۵].

پردازنده: یکی از مهم‌ترین اثرات مخرب طوفان پیام‌ها، افزایش مصرف پردازنده[4] بوده که بر روی کارگزارهای مورد حمله صورت می‌گیرد. با افزایش میزان مصرف پردازنده، کارگزار در پاسخگویی به کاربران مجاز و واقعی دچار اخلال شده و در مواقع حمله با تأخیر به آنها جواب می‌دهد و در نتیجه برخی از کاربران نمی‌توانند از سرویس مورد نظر بهره ببرند. همچنین اگر میزان افزایش مصرف پردازنده بیش از اندازه بالا رود ممکن است کارگزار را از کار انداخته و لازم باشد دوباره راه‌اندازی شود و در این مدت تمامی کاربران از سرویس محروم می‌شوند. در مواقعی که لازم است کارگزار عملیات تشخیص هویت را انجام دهد، اگر طوفان پیامی صورت پذیرد دچار افزایش مصرف پردازنده می‌گردد. در بخش‌های بعدی یکی از موارد مهمی که به عنوان اثرات حمله مورد بررسی قرار می‌گیرد، افزایش مصرف پردازنده می‌باشد [۵].

حافظه: برخی از درخواست‌ها که از طرف کاربر ارسال می‌گردد باعث ایجاد حالت نشست می‌شود. برای مثال یک پیام INVITE که از طرف کاربر به کارگزار پروکسی ارسال می‌شود، توسط کارگزار پروکسی SIP به جلو فرستاده می‌شود و در این حالت تا سه دقیقه منتظر جواب می‌شود. در این فاصله زمانی حافظه خاصی در پروکسی اشغال می‌گردد. در صورتی که تعداد این پیام‌ها بیش از حد شود، حافظه کارگزار پروکسی بیش از اندازه مشغول می‌شود [۵].

طوفان پیام با پیام‌های متفاوت SIP (مانند INVITE، REGISTER، OPTIONS و ...) می‌تواند این حالت را ایجاد نماید و پروکسی‌های متفاوت و یا عاملین کاربر[5] را تهدید نماید [۶].

۲-۱ انواع طوفان پیام در SIP

کارگزار پروکسی و کارگزار ثبت نام از مهم‌ترین سرویس‌دهنده‌های SIP می‌باشند که در صورت حمله به آنها ممکن است سرویس‌دهی به صورت جدی مورد آسیب قرار گیرد. مهاجم با ارسال طوفان‌های پیام مختص به هر یک از این کارگزارها می‌تواند برای آنها ایجاد خطر کند.

1. Bandwidth
2. CPU
3. Memory
4. CPU Usage
5. User Agent

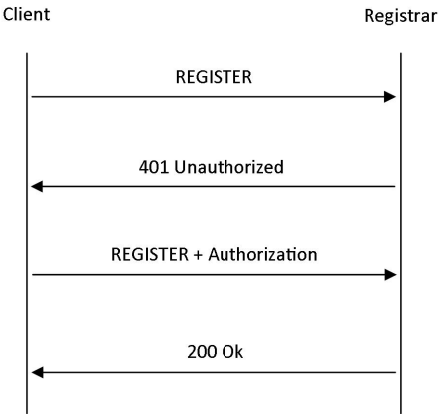
مثلاً اگر بخواهد کارگزار پروکسی را دچار آسیب نماید بایستی از طوفان پیام‌های INVITE، CANCEL، BYE و OPTION استفاده کند چرا که تنها این پیام‌ها در آن قابل قبول است و در صورتی که پیام‌های دیگری به عنوان طوفان انتخاب نماید به راحتی توسط کارگزار شناسایی شده و قبل از آن که آسیبی به آن برساند آنها را حذف خواهد کرد. همچنین اگر مهاجم طوفان پیام‌های REGISTER را به سمت کارگزار ثبت نام ارسال نماید می‌تواند آن را با خطر جدی مواجه سازد. در جدول ۱ با مقایسه مصرف پردازنده‌ها در زمان حمله نشان داده شده که طوفان ثبت نام می‌تواند بیشترین خطر را برای کارگزار در بر داشته باشد [۷]. در ادامه توضیحات بیشتری در رابطه با طوفان ثبت نام مطرح می‌شود.

۲-۲ حملات طوفان ثبت نام

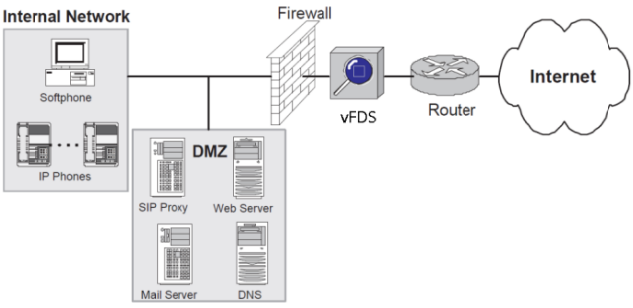
اگر مهاجم تعداد زیادی پیام ثبت نام را که حاوی کلمه عبور نادرست است به سمت کارگزار روانه کند، کارگزار دچار حمله خواهد شد. مهاجم بایستی از IPهایی مشابه با IP سایر کاربران در شبکه بهره ببرد چرا که در غیر این صورت با محدودکردن آدرس‌های IP با استفاده از لیست دسترسی به راحتی جلوی حمله او گرفته خواهد شد. همچنین برای به خطر انداختن بیشتر کارگزار، مهاجم می‌تواند از نام‌های کاربری موجود استفاده نموده و تنها با واردکردن رمز عبورهای تصادفی کارگزار را مشغول سازد.

عامل کاربر برای ثبت نام در کارگزار بسته‌ای با عنوان REGISTER ارسال می‌کند و کارگزار پس از دریافت آن بسته ۴۰۱ را به عامل کاربر می‌فرستد که در آن به کاربر می‌گوید برای تکمیل ثبت نام شناسه و رمز عبور خود را ارسال نماید. سپس کاربر در بسته‌ای با عنوان REGISTER شناسه و رمز عبور خود را می‌فرستد و در نهایت کارگزار پس از اطمینان از صحت شناسه و رمز عبور بسته ۲۰۰ OK را به کاربر ارسال می‌کند [۸]. در این مقاله بسته اول کاربر REG۱، بسته ۴۰۱ AUTH و بسته دوم کاربر REG۲ نامیده می‌شود. در اینجا ذکر چند نکته ضروری به نظر می‌رسد:

- رمزنگاری کلمه‌های عبور اگرچه می‌تواند سبب امنیت آنها شود اما کار را برای کارگزار دشوار می‌سازد چرا که برای تک‌تک کاربران لازم است این عملیات بازگشایی رمز صورت گرفته و پس از تطبیق آنها با کلمه عبور موجود در پایگاه داده کارگزار که مختص آن کاربر است، اجازه ثبت نام را صادر نماید. در صورتی که تعداد درخواست‌ها به سمت کارگزار زیاد گردد، کارگزار از پاسخگویی به آنها عاجز خواهد بود و مهاجمین از این آسیب‌پذیری نهایت استفاده را می‌برند.
- برای آن که حضور کاربران در سیستم مشخص شود، لازم است که به صورت دوره‌ای و در زمان‌های معینی عملیات ثبت نام صورت پذیرد. حتی کاربرانی که همواره برخط هستند نیز این عملیات را انجام می‌دهند. این خود یک آسیب‌پذیری است که مهاجمین می‌توانند از آن بهره برده و هر موقع طوفان پیام را به اجرا درآورند.



شکل ۱: ثبت نام در شرایط عادی [۸].



شکل ۳: شبکه VoIP [۴].

- در صورتی که بعد از رسیدن پیام اول از کاربر به کارگزار، کارگزار نتواند در مدت زمان معینی پاسخ کاربر را بدهد، پیام منقضی شده و کاربر دوباره پیام را ارسال می‌کند. این موضوع برای پیام‌های دیگر نیز مطرح است.

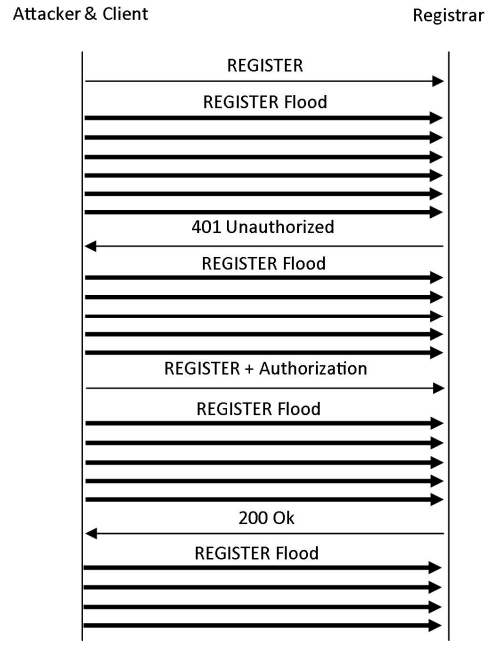
شکل ۱ ثبت نام در شرایط عادی و شکل ۲ ثبت نام در زمان وقوع حمله را نشان می‌دهد.

۲-۳ اثرات حمله طوفان ثبت نام

پس از آن که مهاجم سیل پیام‌ها را به سمت کارگزار ثبت نام ارسال کند، کارگزار دچار افت کارایی شده و مصرف پردازنده آن به شدت بالا می‌رود. بالارفتن میزان مصرف پردازنده کاملاً مرتبط با میزان حمله خواهد بود. در حمله‌های با سرعت خیلی بالا (به این معنا که تعداد بسته‌های پیام ثبت نام از طرف مهاجم در ثانیه بسیار بیشتر از کاربران عادی باشد) کارگزار با افت شدید کارایی مواجه شده و کاربران عادی به ندرت ثبت نام می‌شوند. کاهش تعداد ثبت نام‌های عادی نیز از عوامل و اثرات حمله خواهد بود. فاصله زمانی اولین پیام ارسالی از کاربر تا آخرین پیام دریافتی (۲۰۰ Ok) نیز می‌تواند مورد بررسی واقع شود. در صورتی که در شرایط عادی این فواصل زمانی تقریباً ثابت است، در زمان حمله و با افزایش سرعت آن این فاصله به مراتب بیشتر خواهد شد. از دیگر اثرات حمله افزایش تعداد پیام‌های اضافی است که لازم است از طرف هر کاربر برای ثبت نام به طرف کارگزار فرستاده شود، یعنی با بالارفتن مصرف پردازنده کارگزار قادر به پاسخگویی نبوده و پیام‌ها منقضی می‌گردد، لذا بایستی پیام‌ها دوباره به سمت مقصد ارسال گردند.

۳- تشخیص حملات طوفان ثبت نام

پس از شناسایی اثرات حمله طوفان برای کاهش این اثرات بایستی ابتدا لحظه وقوع این حمله در سیستم شناسایی شود. یکی از روش‌های



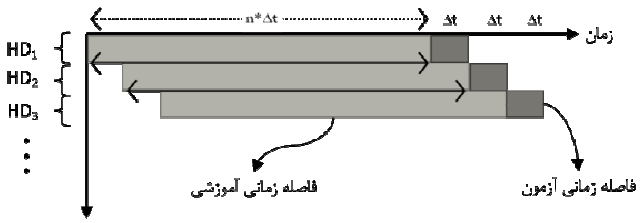
شکل ۲: طوفان ثبت نام و ثبت نام در شرایط حمله [۹].

تشخیص حملات طوفان استفاده از فاصله Hellinger می‌باشد که این روش تشخیص، کارا و مفید بوده و در منابع زیادی از آن بهره گرفته شده [۴] و [۱۰] تا [۱۲] و همچنین محاسبات زیادی نداشته و قابلیت تشخیص سریع را فراهم می‌آورد. نویسندگان در [۴] برای تشخیص حملات طوفان که رفتار غیر عادی تلقی می‌شود، از یک سیستم تشخیص حملات VoIP (که در اینجا vFDS[1] نامیده شده است) بهره برده‌اند که تمایزی بین ترافیک عادی و حمله قایل می‌شوند. اساس کار این سیستم آن است که بسته‌هایی که در لایه کاربرد و یا بالاتر از IP هستند مورد بررسی قرار می‌گیرند. به نحوی تمامی جریانات ترافیکی فعلی نسبت به یک الگوی خاصی که در شرایط عادی ایجاد شده سنجیده شوند تا در صورت انحراف نسبت به حالت عادی، تشخیص حمله داده شود. در [۴] این حالت انحراف را با استفاده از اندازه‌گیری HD بین دو زمان گذشته (که احتمالاً حالت عادی سیستم است) و زمان حال به دست می‌آورد. در نتیجه اگر HD بین این دو زمان بیش از حد آستانه باشد، vFDS تشخیص حمله می‌دهد. از آنجا که محاسبات مربوط به HD زیاد نبوده و نیز بر اساس ویژگی‌های پروتکل می‌باشد (می‌توان ویژگی‌های پروتکل را به نحوی با HD مرتبط نمود)، لذا در [۴] از آن به عنوان پایه تشخیص حملات استفاده شده است. نویسندگان اعتقاد دارند این روش به دلیل آن که می‌تواند انواع حملات بر روی سیستم VoIP را تشخیص دهد کارایی بالایی دارد. مثلاً حملات در لایه TCP، RTP و SIP از جمله حملاتی است که در صورت طوفان بسته‌های توسط vFDS شناسایی می‌گردد در نتیجه با استفاده از یک سیستم به صورت مجتمع می‌توان انواع حملات طوفان را تشخیص داد.

شکل ۳ سیستم ارائه‌شده در [۴] و محل قرارگیری vFDS در یک شبکه VoIP را نشان می‌دهد.

در صورتی که vFDS در ورودی کارگزارها و پس از آخرین مسیریاب قرار گیرد، می‌توان اطمینان داشت که تمامی ترافیک ورودی به کارگزارها از طرف شبکه اینترنت از آن خواهد گذشت. لذا در صورتی که بتوان حمله‌ای را تشخیص داد، بلافاصله می‌توان برای جلوگیری از ادامه آن اقدام کرد.

1. VoIP Flooding Detection System



شکل ۴: ارتباط بین فاصله زمانی آزمون و آموزشی [۴].

۳-۱ طراحی vFDS

به صورت کلی vFDS حالت غیر نرمال را در بین مجموعه‌ای از بسته‌های جریان تشخیص می‌دهد. این شناسایی شامل دو مرحله می‌شود که همواره در حال تکرار است. همان طور که در شکل ۴ نشان داده می‌شود، ابتدا بایستی از لحظه شروع تا زمانی معین خواص جریان عبوری شناسایی گردد که به این فاصله زمانی آموزشی[1] گفته می‌شود. حال فاصله زمانی کوتاهی پس از اولین فاصله آموزشی به عنوان فاصله آزمون مورد بررسی قرار گرفته و HD این دو اندازه‌گیری می‌شود. فاصله زمانی آزمون Δt بوده و فاصله زمانی آموزشی برابر با $n\times\Delta t$ خواهد بود.

نکته بسیار مهم آن است که بایستی پارامترهای آزمون و آموزشی بدون وقفه و در کوتاه‌ترین زمان ممکن اندازه‌گیری شوند. همان‌طور که در شکل ۴ مشاهده می‌شود بایستی در فاصله زمانی Δt بعدی نیز پارامترها محاسبه گردند و در $n\times\Delta t$ قبل از آن هم پارامترها برای قسمت آموزشی محاسبه گردند و پس از آن HD اندازه‌گیری شود. واضح است در این صورت در هر Δt فاصله زمانی، HD نسبت به $n\times\Delta t$ ثانیه قبل به دست خواهد آمد.

۳-۲ فاصله Hellinger

HD برای محاسبه دو بردار احتمال به کار گرفته می‌شود. اگر فرض کنیم P و Q دو توزیع احتمال در فضای متناهی Ω و هر کدام دارای N احتمال $(p_1,p_2,\ldots,p_N)$ و $(q_1,q_2,\ldots,q_N)$ باشند و همچنین با توجه به این که این مقادیر احتمالات بوده و همگی مثبت هستند و جمع آنها کمتر از صفر نیست، داریم: $\sum_\alpha q_\alpha = 1$، $\sum_\alpha p_\alpha = 1$، $q_\alpha \geq 0$ و $p_\alpha \geq 0$. در نتیجه HD بین P و Q از رابطه زیر به دست می‌آید

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

برخی از مواقع ضریب ۱/۲ از (۱) حذف می‌گردد. در این صورت از خواص این فاصله آن است که همواره بین صفر و یک بوده و در صورتی برابر با صفر است که $P=Q$ باشد. همچنین بالاترین فاصله برابر با یک به معنای بیشترین اختلاف موجود بین این دو می‌باشد. در اینجا فرض شده است P مرتبط با احتمالات فاصله زمانی آموزشی و Q مرتبط با احتمالات فاصله زمانی آزمون می‌باشد.

۳-۳ محاسبه HD برای ثبت نام

برای محاسبه HD بایستی احتمالات وقوع چهار بسته REG۱، AUTH، REG۲ و OK ۲۰۰ در زمان آزمون و آموزشی جداگانه محاسبه شود. در نتیجه HD به روش زیر برای بسته‌های بین کارگزار ثبت نام و کاربر محاسبه می‌شود. احتمالات وقوع در زمان آموزشی با p و در زمان آزمون با q نشان داده شده است

$$HD = (\sqrt{p_{REG1}}-\sqrt{q_{REG1}})^2 + (\sqrt{p_{AUTH}}-\sqrt{q_{AUTH}})^2 + (\sqrt{p_{REG2}}-\sqrt{q_{REG2}})^2 + (\sqrt{p_{200\,OK}}-\sqrt{q_{200\,OK}})^2 \qquad (2)$$

۳-۴ فاصله Kullback-Leibler

فاصله دیگری که بررسی خواهد شد KLD است که در حملات با نرخ پایین بسیار مؤثرتر است چرا که نقاط ماکسیمم و مینیمم آن فاصله بیشتری نسبت به هم دارند. مزیت KLD بر HD آن است که محدودیتی در اندازه KLD وجود ندارد. همان طور که در قبل ذکر شد HD حتماً بین صفر و یک است و این باعث می‌شود که HD در زمان حمله نسبت به HD در زمان عادی افزایش شدیدی نداشته باشد، مخصوصاً این که نرخ حمله پایین باشد. در KLD زمانی که حمله رخ دهد، فاصله بیشتری نشان داده می‌شود در نتیجه نمودار ROC آن در یک احتمال هشدار غلط ثابت، دارای احتمال تشخیص حمله بهتری خواهد بود. این موضوع در بخش آینده که نمودارها رسم شده‌اند به وضوح قابل رؤیت است. در نتیجه می‌توان این گونه بیان کرد که KLD بهتر از HD در تشخیص حمله عمل خواهد کرد. لازم به ذکر است که p و q دقیقاً مشابه احتمالات در محاسبه HD است یعنی p مرتبط با احتمالات بسته‌ها در زمان آموزشی و q مرتبط با احتمالات بسته‌ها در زمان آزمون خواهد بود

$$KLD(P,Q) = \sum_i \ln(\frac{p(i)}{q(i)})p(i) \qquad (3)$$

از مهم‌ترین خواص KLD آن است که صفر و یا بزرگ‌تر از صفر است. زمانی KLD برابر صفر خواهد بود که دو توزیع احتمال P و Q برابر هم باشند و همچنین هر چه اختلاف این دو زیادتر باشد این عدد افزایش می‌یابد [۱۳]. برای محاسبه KLD برای بسته‌های ثبت نام از رابطه زیر بهره می‌گیریم

$$KLD = \ln(\frac{p_{REG1}}{q_{REG1}})p_{REG1} + \ln(\frac{p_{AUTH}}{q_{AUTH}})p_{AUTH} + \ln(\frac{p_{REG2}}{q_{REG2}})p_{REG2} + \ln(\frac{p_{200\,OK}}{q_{200\,OK}})p_{200\,OK} \qquad (4)$$

نکته بسیار مهم آن است که محل قرارگیری این سیستم تشخیص طوفان ثبت نام شبیه به محل vFDS در [۴] است.

بخش بعدی به ارائه نتایج به دست آمده از آزمایش‌ها در شبکه واقعی اختصاص دارد.

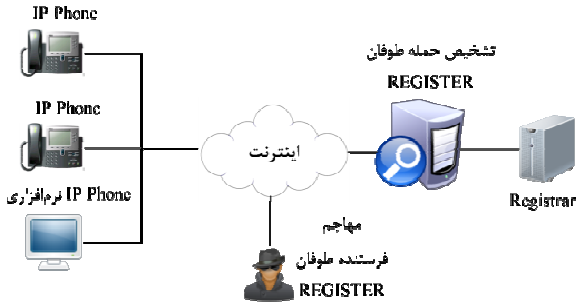
۴- نتایج و مقایسه‌ها

در این بخش نتایج آزمایشات در قالب نمودارها رسم خواهد شد. در ابتدا توضیحاتی در رابطه با شبکه آزمون ارائه خواهد شد.

۴-۱ ایجاد و راه‌اندازی شبکه آزمون

شبکه‌ای که آزمایش بر روی آن قرار گرفته است به صورت منطقی شبیه به شکل ۵ است. کاربران از طریق اینترنت می‌توانند به کارگزارها دسترسی داشته باشند و پس از ثبت نام در کارگزار ثبت نام می‌توانند با یکدیگر تماس برقرار نمایند. محدودیتی برای پهنای باند شبکه در نظر گرفته نشده است چرا که اساساً موضوع مورد بررسی بحث ثبت نام و طوفان این بسته‌هاست و به دلیل آن که تمامی بسته‌های عبوری در این قسمت از این نوع می‌باشد و حجم بسته‌ها ناچیز است، لذا پهنای باند محدودیتی ایجاد نخواهد کرد.

1. Training



شکل ۵: شبکه VoIP برای تشخیص طوفان ثبت نام.

کارگزار مورد بررسی در این قسمت کارگزار ثبت نام خواهد بود که نرم‌افزار آن از مجموعه نرم‌افزارهای آزاد 3CX انتخاب شده است [۱۴] و محدودیتی برای پاسخگویی به کاربران ندارد و تنها محدودیت‌های سخت‌افزاری هستند که ممکن است ایجاد گردند. کاربران عادی این سیستم هم از نرم‌افزار مجموعه 3CX بهره برده‌اند. با استفاده از این نرم‌افزار می‌توان عامل کاربر را بر روی ویندوز هر کاربر نصب نمود تا با آن بتوانند در کارگزار ثبت نام نموده و تماس‌های صوتی و تصویری برقرار سازند. در بستر آزمایش به دلیل محدودیت سخت‌افزاری می‌توان از نرم‌افزار متن باز SIPp بهره برد [۱۵].

این نرم‌افزار که یک تولیدکننده بسته SIP است، قابلیت به کار رفتن به جای مشتری عامل کاربر[1] و کارگزار عامل کاربر[2] را دارد و همچنین قابلیت ارسال بسته‌های RTP را نیز دارا بوده و می‌تواند الگوریتم‌های مختلفی برای ایجاد انواع بسته‌های مرتبط با SIP به وجود آورد. در بستر آزمایش، این نرم‌افزار بر روی لینوکس CentOS نسخه ۵/۳ نصب شده و جایگزین چندین عامل کاربر واقعی شده است به این معنا که با استفاده از SIPp می‌توان هم‌زمان چندین بسته به سمت کارگزار ارسال نمود به طوری که این گونه به نظر می‌رسد که چندین کاربر واقعی در حال ارتباط با کارگزار هستند. نسخه SIPp استفاده‌شده در این مقاله ۳/۱ می‌باشد که هم برای کاربران واقعی و هم برای مهاجمین از آن بهره گرفته شده است. همچنین لازم به ذکر است برای کارگزار، سیستم عامل ویندوز XP با حافظه یک گیگابایت و حجم دیسک ۱۲ گیگابایت و یک پردازنده با فرکانس ۲/۵ گیگاهرتز انتخاب شده است.

۴-۲ آزمون شبکه در حالت عادی

پس از آن که نرم‌افزارهای کاربر و کارگزار نصب گردید لازم است که آن را در شرایط عادی بیازماییم. اگر شبکه در حالت عادی به درستی به تمامی تراکنش‌ها پاسخ مناسب داد، می‌توان انتظار داشت که در زمان حمله پاسخ آن قابل استناد باشد و برای این کار باید شبکه با وجود کاربران عادی به صورت درست کار نماید. کاربران بتوانند در کارگزار ثبت نام نموده و در صورت نیاز بتوانند با یکدیگر تماس حاصل کنند. بسته‌های جابه‌جا شده بین کارگزارها و کاربران با استفاده از نرم‌افزار Wireshark که مختص ضبط بسته‌هاست، می‌تواند رصد گردد. حال می‌توان با استفاده از نرم‌افزار SIPp ترافیک عادی برای کاربران ایجاد کرده و نتایج شرایط عادی را ثبت نمود. آدرس IP کارگزار ثبت نام برابر با ۱۰.۱.۵۱.۱ می‌باشد در نتیجه در خط دستور در نرم‌افزار SIPp باید نوشته شود:

./sipp 10.1.51.1 –sf REGISTER_Client.xml - inf REGISTER_Client.csv -r 50

1. User Agent Client
2. User Agent Server

sipp نام نرم‌افزار و عبارت بعدی آدرس IP کارگزار ثبت نام است. در این دستور sf به این معناست که الگوریتم ارتباط کارگزار و کاربر توسط این فایل xml صورت می‌گیرد که در زیر جزئیات آن آمده است. در این فایل مراحل چهارگانه از درخواست اولیه تا نحوه دریافت OK ۲۰۰ توسط عامل کاربر مشخص شده است. همچنین زمان‌بندی‌هایی برای ارسال بسته در صورتی که بسته‌ها در مدت مشخصی به کارگزار نرسد و یا پاسخی از آن دریافت نکند، وجود دارد. فایل csv برای آن است که این نرم‌افزار شناسه و رمز عبور کاربران مختلف را به کار برده و به جای آنها در کارگزار ثبت نام نماید. عبارت ۵۰ r- در متن دستور برای آن است که نرخ کاربران را که در هر ثانیه ثبت نام می‌کنند، مشخص کند و این عدد ۵۰ در نظر گرفته شده است. همچنین نرم‌افزار این قابلیت را می‌دهد که محدود به یک دوره زمانی و یا تعداد عملیات ثبت نام باشد.

۴-۳ ایجاد حمله با استفاده از SIPp

پس از برقراری ارتباط بین کاربران و کارگزار بایستی شبکه در حالت حمله آزموده شود که این کار نیز با استفاده از نرم‌افزار SIPp صورت می‌گیرد و تنها تفاوت حالت حمله با حالت عادی در شناسه و رمز عبور کاربران است. البته در تمامی آزمایش‌ها از شناسه کاربران مجاز بهره گرفته شده و تنها کلمات عبور مهاجمین عبارتی نادرست خواهد بود. حمله با نرخ کاربران متفاوت صورت می‌گیرد. ابتدا آزمون‌هایی با مهاجمین خیلی کم (۱۰ حمله بر ثانیه) انجام می‌شود و سپس نرخ حمله به تدریج افزایش می‌یابد تا به ۵۰۰ حمله بر ثانیه برسد. در بیشتر آزمون‌ها دوره زمانی وقوع حمله ۳۰ ثانیه و همچنین تعداد کاربرانی که به صورت عادی در حال ثبت نام هستند ۵۰ کاربر بر ثانیه در نظر گرفته شده است [۴]. عبارت حمله در نرم‌افزار SIPp به صورت زیر است:

./sipp 10.1.51.1 –sf REGISTER_Client.xml - inf Attacker.csv -r 50

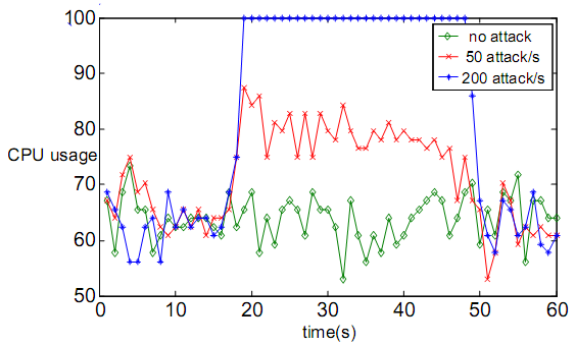
مهاجمین برای حمله به کارگزار ثبت نام بایستی از الگوی ثبت نام عادی پیروی نمایند و همان طور که گفته شد تنها کلمه عبور اشتباه دارند. دلیل آن هم این است که معمولاً دیواره آتش داخلی در سیستم عامل مانع از رسیدن بسته‌های غیر لازم به کارگزارها می‌شوند یعنی اگر بسته‌ای خارج از پورت ۵۰۶۰ وارد کارگزار شد ممکن است حذف گردد. بنابراین مهاجمین نیز باید از همان راه به کارگزارها حمله نمایند.

۴-۴ بررسی اثرات حمله

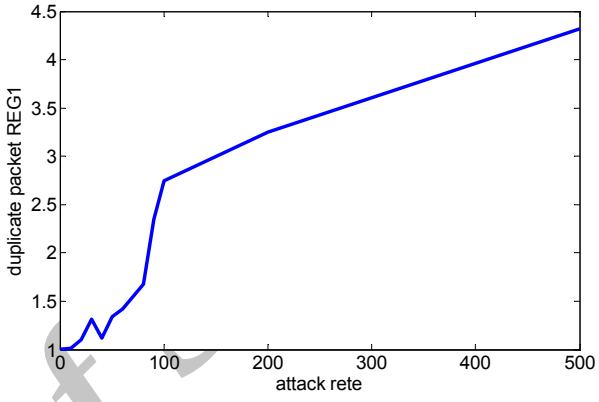
پس از آزمون شبکه در حالت عادی و حمله باید اثرات حمله در مقابل شرایط عادی سنجیده شود. این اثرات می‌تواند شامل موارد زیر باشد که به طور مجزا بررسی خواهد شد.

۴-۴-۱ افزایش مصرف پردازنده

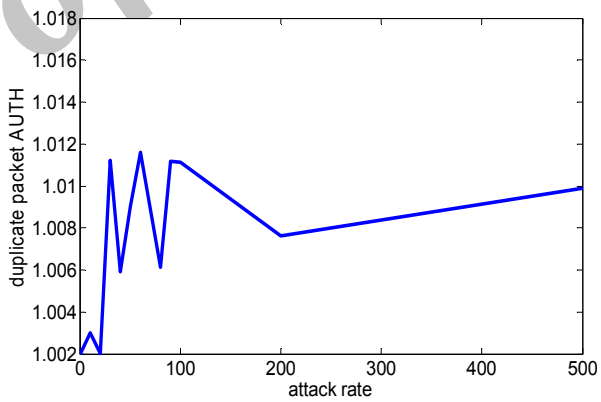
مهم‌ترین عامل پس از وقوع حمله که باعث افت کارایی کارگزار می‌شود، افزایش مصرف پردازنده آن است. این مشکل به آن دلیل ایجاد می‌شود که تعداد درخواست‌ها به طرف کارگزار بیش از آن است که بتواند آن را پاسخ دهد و لذا به شدت مشغول می‌گردد. در بستر آزمایش ابتدا ۶۰ ثانیه کامل بدون حمله این میزان اندازه‌گیری شد، سپس با ایجاد حمله و با افزایش نرخ آن این موضوع بررسی شد که در شکل ۶ رسم گردیده است. حمله به مدت ۳۰ ثانیه و در فاصله زمانی بین ۲۰ تا ۵۰ ثانیه ایجاد گردیده و محور افقی نمودار زمان بر حسب ثانیه و محور عمودی درصد مصرف پردازنده را نشان می‌دهد. از نمودار این موضوع کاملاً مشخص است که در حمله با نرخ پایین در مدت حمله مصرف پردازنده افزایش



شکل ۶: درصد مصرف پردازنده در زمان عادی و حمله با نرخ ۵۰ بسته بر ثانیه و ۲۰۰ بسته بر ثانیه.



شکل ۷: متوسط تعداد بسته‌های تکراری REG۱ در زمان حمله.



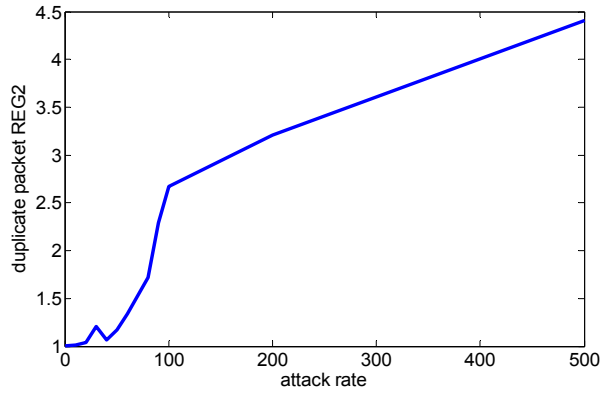
شکل ۸: متوسط تعداد بسته‌های تکراری AUTH در زمان حمله.

چشمگیری نخواهد داشت. حملات با نرخ بالاتر (۲۰۰ بسته بر ثانیه) می‌تواند مصرف پردازنده را به ۱۰۰ درصد برساند که این موضوع سبب اختلال در سرویس‌دهی خواهد شد.

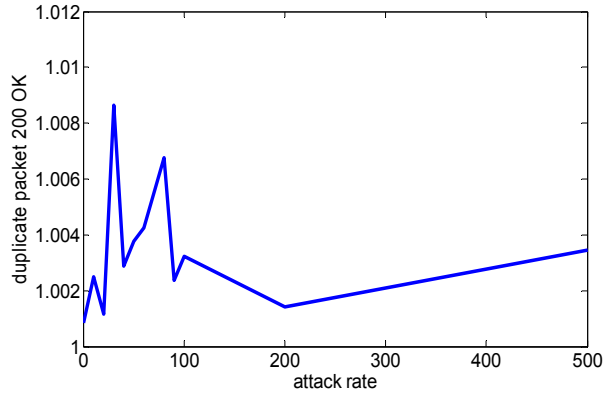
٤-٤-٢ ارسال بسته‌های تکراری

زمانی که مصرف پردازنده کارگزار بالا می‌رود، کارگزار نمی‌تواند به صورت لحظه‌ای پاسخ تمامی درخواست‌هایی را که به سمتش می‌آید بدهد، لذا برخی درخواست‌ها بدون پاسخ مانده تا این که شمارنده عامل کاربر باعث ارسال دوباره بسته می‌شود. این عمل تا زمانی که پاسخی از طرف کارگزار به عامل کاربر بیاید تکرار می‌شود و بسته به نرخ حمله، تعداد بسته‌های تکراری نیز زیاد می‌شود. شکل‌های ۷ تا ۱۱ این موضوع را برای چهار بسته‌ای که در زمان ثبت نام جابه‌جا می‌شوند نشان می‌دهد.

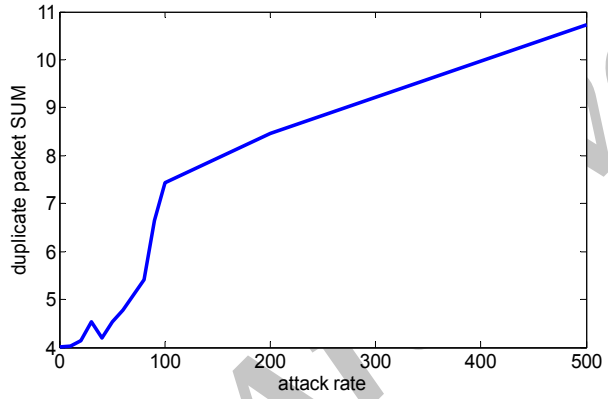
همان طور که در شکل‌ها مشاهده می‌شود در بسته‌هایی که از طرف عامل کاربر به کارگزار ارسال می‌شود، هر چه نرخ حمله افزایش پیدا کند تعداد بسته‌هایی که توسط کارگزار بی‌پاسخ مانده زیاد شده و در نتیجه



شکل ۹: متوسط تعداد بسته‌های تکراری REG۲ در زمان حمله.

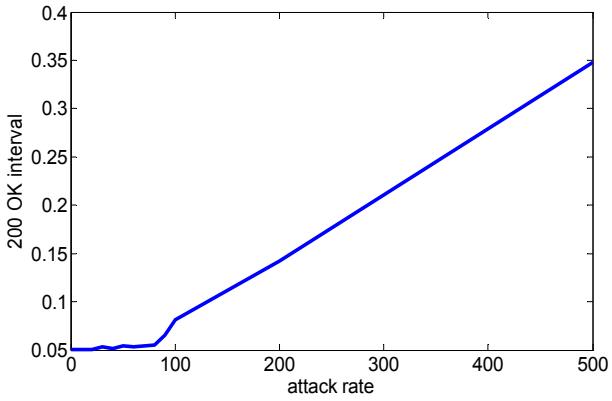


شکل ۱۰: متوسط تعداد بسته‌های تکراری ۲۰۰ OK در زمان حمله.

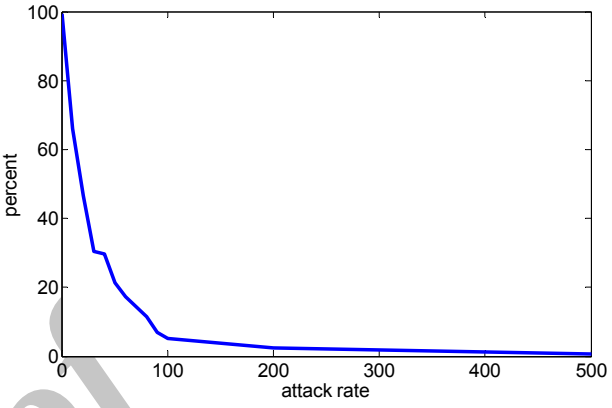


شکل ۱۱: متوسط مجموع تعداد بسته‌های تکراری در زمان حمله.

بایستی دوباره از طرف عامل کاربر ارسال شوند. این افزایش بسیار قابل توجه بوده و در زمانی که نرخ حمله به ۵۰۰ بسته ثبت نام بر ثانیه می‌رسد، این عدد برای REG۱ به ۴٫۳ افزایش می‌یابد. این بدین معناست که اگر در لحظه عادی بعد از ارسال اولین پیام REG۱ از عامل کاربر به کارگزار، کارگزار پاسخ AUTH را ارسال می‌کرد، در زمان حمله با نرخ ۵۰۰ بسته بر ثانیه بایستی هر عامل کاربر (چه مهاجم و چه عادی) برای این که به پاسخی از طرف کارگزار برسند، به طور متوسط ۴٫۳ بسته REG۱ را ارسال نمایند. البته همان طور که از نمودارهای AUTH و ۲۰۰ OK مشخص است این مقادیر برای آنها در زمان‌های حمله تغییرات بسیار اندکی خواهد داشت چرا که کارگزار این بسته‌ها را ارسال می‌کند و به سمت عاملین کاربر می‌فرستد. با توجه به آن که عاملین کاربر مشکلی در ارسال سریع پاسخ ندارند، لذا افزایش خاصی مطرح نخواهد بود. با توجه به شکل ۱۱ می‌توان فهمید که مجموع تعداد بسته‌های اضافی در زمان حمله با نرخ ۵۰۰ بسته بر ثانیه تقریباً ۱۱ خواهد بود.



شکل ۱۲: متوسط فاصله زمانی OK ۲۰۰ در زمان حمله.



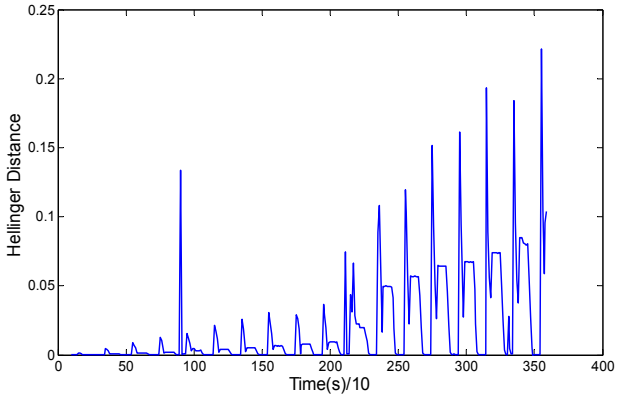
شکل ۱۳: درصد موفقیت ثبت نام.

٤-٤-٣ متوسط فاصله ثبت نام‌ها

از دیگر اثرات حمله می‌توان به افزایش فاصله زمانی بین ثبت نام کاربران اشاره نمود. با فرض این که تعداد بسته‌های ارسالی از طرف کاربران در شرایط عادی ۲۰ عدد بر ثانیه و حملات در حال افزایش باشد می‌توان نمودار شکل ۱۲ را به دست آورد. در زمانی که ۵۰۰ بسته بر ثانیه حمله از طرف مهاجمین به سمت کارگزار ارسال می‌شود، فاصله بین دو ثبت نام کاربران عادی به ۰٫۳۵ ثانیه افزایش می‌یابد، در صورتی که این میزان در شرایط عادی برابر با ۰٫۰۵ ثانیه است. این افزایش زمان به این معناست که تعداد کاربران عادی کمتری توانسته‌اند ثبت نام نمایند و عملاً سرویس‌دهی کارگزار ثبت نام با اختلال جدی مواجه شده است.

٤-٤-٤ درصد موفقیت

یکی از اثرات حمله بر روی کارگزار ثبت نام کاهش درصد موفقیت ثبت نام‌ها ست. درصد موفقیت این گونه تعریف می‌شود: "نسبت تعداد بسته‌های OK ۲۰۰ به تعداد بسته‌های REG۱ به درصد". در زمان حمله، درصد موفقیت ثبت نام از دو جهت کاهش می‌یابد، اول آن که بسته‌های ثبت نام هم از طرف کاربران عادی و هم از طرف مهاجمین به سمت کارگزار ارسال می‌شود. تنها کاربران عادی هستند که مجاز به ثبت نام می‌باشند، لذا بقیه بسته‌های ثبت نامی، اضافی تلقی شده و باعث کاهش درصد موفقیت می‌گردد. همچنین افزایش نرخ حملات، افزایش مصرف پردازنده کارگزار را در بر داشته و در نتیجه بسته‌های تکراری زیادی ارسال خواهند شد و این موضوع باعث کاهش درصد موفقیت می‌شود. شکل ۱۳ این مطلب را نشان می‌دهد. زمانی که نرخ حملات به ۵۰۰ می‌رسد، درصد موفقیت نیز کمتر از یک خواهد بود.



شکل ۱۴: محاسبه HD برای حملات با نرخ متفاوت.

٤-٥ تشخیص حمله با استفاده از HD

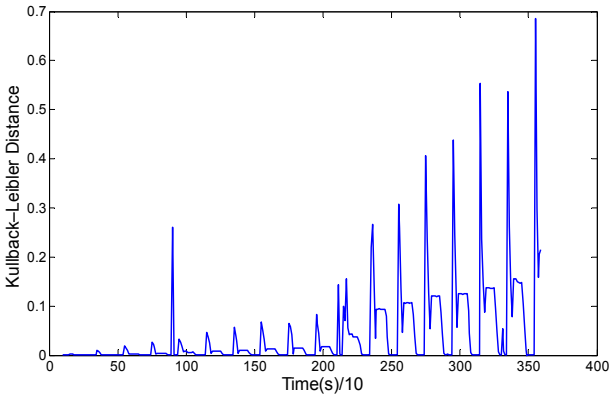
برای استفاده از الگوریتم HD در آزمایشات، در یک فاصله زمانی مشخص چندین حمله بر روی کارگزار ثبت نام صورت می‌پذیرد. فرض بر آن است که نرخ تراکنش کاربران عادی ۵۰ عدد است، یعنی در هر ثانیه ۵۰ بسته ثبت نام از طرف کاربران عادی به سمت کارگزار ارسال شده و سپس حملات با نرخ‌های مختلف به سمت کارگزار روانه می‌گردد. پس از ضبط تمامی تراکنش‌ها، احتمالات آنها تعیین شده و در نرم‌افزار Matlab محاسبات مربوط به HD به دست خواهد آمد. شکل ۱۴ این موضوع را نشان می‌دهد. لازم به ذکر است در تمامی آزمایشات Δt برابر ۱۰ ثانیه و n برابر ۱۰ در نظر گرفته شده است.

در شکل ۱۴ نشان داده شده که در زمان‌های مختلف حملات با نرخ‌های متفاوتی رخ داده است. مثلاً کمترین نرخ حمله در ثانیه ۱۵۵ رخ داده که این حمله ۳۰ ثانیه به طول انجامیده و نرخ این حمله برابر با ۱۰ بسته بر ثانیه می‌باشد. این نرخ بسیار پایین بوده و فاصله به دست آمده ۰٫۰۰۱۳۱۶ است. به ترتیب در زمان‌های بعدی حملات با نرخ‌های ۲۰، ۳۰، ۴۰، ... و ۱۰۰ رخ داده که حمله با نرخ ۱۰۰ در ثانیه ۱۹۵۰ بوده که در نمودار زمان ۱۹۵ نشان داده شده است. در دو مقطع زمانی حمله‌ای رخ نداده ولی ماکسیمم نسبی رخ داده است. این زمان‌ها به ترتیب ۹۰۰ و ۲۱۱۰ می‌باشد که در نمودار ۹۰ و ۲۱۱ است. این اتفاق می‌تواند به دلیل اشکال در کارگزار رخ داده باشد که در لحظه‌ای خاص نتوانسته به درخواست‌ها پاسخ دهد. بالاترین حمله نیز ۳۰۰ بسته بر ثانیه است که در ثانیه ۳۵۵۰ یا زمان ۳۵۵ نمودار رخ داده است. در این زمان HD به شدت زیاد است به طوری که به راحتی و با قراردادن مقادیر حد آستانه مناسب می‌توان آن را تشخیص داد.

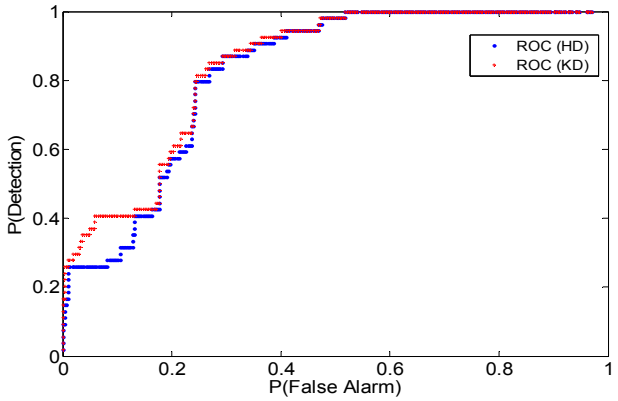
٤-٦ تشخیص حمله با KLD

در بخش قبل به نحوه محاسبه این فاصله اشاره شد و در این قسمت تمامی حملات با استفاده از این فاصله تشخیص داده شده و این موضوع در شکل ۱۵ آمده است.

با توجه به این که فاصله نقاط ماکسیمم و مینیمم این نمودار دارای اختلاف زیادتری نسبت به نمودار قبلی است، می‌توان گفت در این نمودار با تعیین یک حد آستانه راحت‌تر و با خطای کمتری می‌توان حمله را تشخیص داد. نکته قابل توجهی که از این دو نمودار به دست آمده، نقطه ۹۰ یا ثانیه ۹۰۰ نمودار است که خطای کارگزار به حساب می‌آید. اگر به نمودارهای HD مراجعه شود واضح است که عرض نمودار در این لحظه از عرض نقاط ۲۳۵ و ۲۵۵ بیشتر ولی در KLD عرض نمودار در ۹۰ از



شکل ۱۵: محاسبه KLD برای حملات با نرخ متفاوت.



شکل ۱۶: نمودارهای ROC مربوط به تشخیص با HD و KLD.

عرض نمودار در ۲۳۵ و ۲۵۵ کمتر است که این خود دلیلی بر تفاوت نمودارها خواهد بود. البته برای اثبات این موضوع که فاصله KLD با خطای کمتری حمله را تشخیص می‌دهد نیاز است نمودار ROC رسم گردد و این موضوع در ادامه مطرح خواهد شد. البته همان طور که در شکل‌های ۱۴ و ۱۵ دیده می‌شود پس از تشخیص حمله توسط هر دو روش، دوباره در زمان اتمام حمله نمودارهای فواصل افزایش نسبی دارند. این موضوع در ایجاد خطا در سیستم اثرگذار بوده و دقت تشخیص را پایین می‌آورد و به عبارت دیگر پس از حمله به علت افزایش فاصله، دوباره حمله مجدد تشخیص داده می‌شود. این موضوع به دلیل نحوه محاسبه و زمان‌بندی فاصله زمانی آزمون و آموزشی ایجاد شده که با محاسبه دقیق‌تر بایستی از این خطا جلوگیری کرد که به آینده موکول می‌گردد.

۴-۷ مقایسه نمودارهای ROC

برای اثبات آن که روش تشخیص با KLD بهتر از روش تشخیص با HD است از نمودار ROC بهره گرفته‌ایم و در این نمودار محور افقی احتمال هشدار غلط و محور عمودی احتمال تشخیص را نشان می‌دهد [۱۶]. حال هر چه نمودار به صورت قائم باشد و از نیمساز ربع اول بالاتر باشد و زودتر به ارتفاع یک برسد، می‌توان گفت که با خطای کمتری توانسته حملات را تشخیص دهد و هر چه نمودار به نیمساز ربع اول نزدیک‌تر باشد به این معناست که احتمال تشخیص با هشدار غلط پیش رفته و تشخیص مناسبی نداشته‌ایم. شکل ۱۶ این موضوع را نشان می‌دهد.

همان طور که مشخص است در روش پیشنهادی برای جایگزینی KLD به جای HD، خطای تشخیص کاهش یافته و در نتیجه تشخیص حمله طوفان ثبت نام بهتر و با دقت بیشتری صورت می‌گیرد.

۵- نتیجه‌گیری و کارهای آینده

حملات طوفان ثبت نام می‌تواند بر روی کارگزار ثبت نام اثرات بسیار شدید و مخربی ایجاد نماید و چنانچه نرخ حملات افزایش داشته باشد (۵۰۰ بسته بر ثانیه) می‌تواند سرویس‌دهی را با اختلال جدی روبه‌رو سازد. اگر عاملین کاربر نتوانند در کارگزار ثبت نام نمایند بقیه فعالیت آنها در شبکه مختل خواهد شد. در این مقاله با اشاره به اثرات این حملات در بستر یک شبکه واقعی آزمایشاتی صورت پذیرفت و این اثرات در نمودارهای جداگانه ترسیم شد که از جمله این اثرات می‌توان به افزایش مصرف پردازنده در کارگزار ثبت نام اشاره کرد. این اثر باعث ایجاد اثرات دیگری نظیر افزایش زمان ثبت نام کاربران عادی، کاهش تعداد کاربران مجاز برای ثبت نام در یک ثانیه، افزایش بسته‌های تکراری و در نتیجه کاهش درصد موفقیت ثبت نام خواهد شد. همچنین با بررسی سناریوی حمله طوفان ثبت نام به بررسی روش تشخیص حمله با استفاده از HD پرداخته شد و با ارائه یک فاصله جایگزین به نام Kullback - Leibler نشان داده شد که این جایگزینی می‌تواند در جهت تشخیص حمله با خطای کمتر مؤثر واقع شده و با فرض یک احتمال ثابت برای هشدار غلط، احتمال تشخیص حمله افزایش پیدا می‌کند. پس از تشخیص حمله طوفان ثبت نام پیشنهاد می‌شود به عنوان کار آتی بر روی روش‌های جلوگیری از ادامه حمله و اثرگذاری آن فعالیت شود. این موضوع می‌تواند در جهت کاهش اثرات حمله در زمان وقوع آن مؤثر باشد. همچنین تشخیص دیگر حملات ممانعت از سرویس‌دهی مانند ارسال BYE و CANCEL نیز می‌تواند مورد توجه قرار گیرد. محاسبه دقیق‌تر زمان‌بندی‌های آزمون و آموزشی می‌تواند از بروز خطای تشخیص به میزان قابل توجهی بکاهد و این خود می‌تواند در مقاله‌ای جداگانه در آینده بررسی گردد.

مراجع

[1] P. Drew, "Next-generation VoIP network architecture," *MSF Technical Report*, vol. 1, pp. 3-4, 2003.

[2] Nacico, *VoIP and IP Telephony: Planning for Cconvergence in State Government*, Representing Chief Information Officers of the States, vol. 1, pp. 1-18, 2005.

[3] P. Park, "Voice over IP security," *Cisco Systems*, vol. 1, Ver. 6.0, pp. 20-104, 2008.

[4] H. Sengar and D. Wijesekera, "Detecting VoIP floods using the hellinger distance," *IEEE Trans. on Parallel and Distributed Systems*, vol. 19, no. 6, pp. 794-805, Jun. 2008.

[5] S. Ehlert, D. Geneiatakis, and T. Magedanz, "Survey of network security systems to counter SIP-based denia-of-service attacks," *Computers & Security*, vol. 29, no. 2, pp. 225-243, 2010.

[6] H. Sengar, D. Wijesekera, H. Wang, and S. Jajodia, "VoIP intrusion detection through interacting protocol state machines," in *Proc. Int. IEEE Conf. on Dependable Systems and Networks*, pp. 393-402, 25-28 Jun. 2006.

[7] M. Voznak and J. Safarik, "DoS attacks targeting SIP server and improvements of robustness," *Int. J. of Mathematics and Computers in Simulation*, vol. 6, no. 1, pp. 177-184, 2012.

[8] J. Davidson and J. Peters, "Voice over IP fundamentals," *Cisco Press*, 2nd Ed., pp. 223-311, 2006.

[9] A. Kumar, "A novel approach for evaluating and detecting low rate SIP flooding attack," *Int. J. of Computer Applications*, vol. 26, no. 1, pp. 31-36, Jul. 2011.

[10] J. Tang, Y. Cheng, and C. Zhou, "Sketch-based SIP flooding detection using hellinger distance," in *Proc. of the IEEE Global Telecommunications Conf., GLOBECOM'09*, 6 pp., 30 Nov.- 4 Dec. 2009.

[11] M. A. Akbar, Z. Tariq, and M. Farooq, "A comparative study of anomaly detection algorithms for detection of sip flooding in IMS," in *Proc. 2nd Int. Conf. on Internet Multimedia Services Architecture and Applications,* 6 pp., Dec. 2008.

[12] C. Hecht, P. Reichl, A. Berger, O. Jung, and I. Gojmerac, "Intrusion detection in IMS: experiences with a hellinger distance-based flooding detector," in *Proc. IEEE 1st Int. Conf. on Evolving Internet Conf., INTERNET'09,* pp. 65-70, 2009.
[13] M. N. Do and M. Vetterli, "Wavelet-based texture retrieval using generalized Gaussian density and Kullback-Leibler distance," *IEEE Trans. on Image Processing,* vol. 11, no. 2, pp. 146-158, Feb. 2002.
[14] 3CX: http://www.3cx.com/
[15] M. Voznak and J. Rozhon, "SIP infrastructure performance testing," in *Proc. 9th WSEAS Int. Conf. on Telecommunications and Informatics*pp. 153-158, *Catania*, 2010.
[16] J. A. Hanley, "Characteristic (ROC) Curvel," Radiology 743, pp. 29-36, 1982.

سید رضا چوگان در سال ۱۳۸۸ مدرک کارشناسی مهندسی برق خود را از دانشگاه شاهد و در سال ۱۳۹۱ مدرک کارشناسی ارشد مهندسی فناوری اطلاعات خود را از دانشگاه علم و صنعت ایران در یافت نمود. از سال ۱۳۸۹ الی ۱۳۹۳ نامبرده به عنوان کارشناس در مرکز تحقیقات مخابرات ایران به کار مشغول بود. از سال ۱۳۹۳ نیز به عنوان هیأت علمی در دانشگاه جامع علمی کاربردی تهران وارد این دانشگاه شد. زمینه‌های علمی مورد علاقه نام‌برده متنوع بوده و شامل موضوعاتی مانند امنیت سیستم‌های کامپیوتری، تلفن‌های اینترنتی و شبکه‌های کامپیوتری و همچنین شبکه‌های اجتماعی می‌باشد.

محمود فتحی مدرک کارشناسی خود را در رشته‌ی مهندسی برق – الکترونیک در سال ۱۳۶۳ از دانشگاه علم و صنعت ایران گرفته است، و سپس در سال ۱۳۶۶ مدرک کارشناسی ارشد را در گرایش معماری سیستم-های کامپیوتری از دانشگاه برادفورد انگلستان، برادفورد غربی و دکتری را از دانشگاه منچستر انگلستان – موسسه‌ی علوم و فن‌آوری در سال ۱۳۷۰ در حوزه‌ی معماری کامپیوتر سیستم‌های پردازش تصویر گرفته است. از سال ۱۳۷۰ تا کنون وی به عنوان هیأت علمی در دانشگاه علم و صنعت ایران مشغول است و در حال حاضر مرتبه علمی استاد در دانشکده‌ی مهندسی کامپیوتر را دارد. علاقمندی‌های تحقیقاتی وی شامل کیفیت سرویس در شبکه‌های کامپیوتری، شامل انتقال ویدیو و تصویر در اینترنت، کاربردهای شبکه‌های تک منظوره بین خودرویی در سیستم‌های حمل و نقل هوشمند، پردازش تصویر بلادرنگ بخصوص در کاربردهای ترافیکی و سیستم های نظارت بر سلامت از راه دور است.

محمود رمضانی میمی در سال ۱۳۸۷ و ۱۳۹۰ مدارک کارشناسی مهندسی پزشکی-بیوالکتریک و کارشناسی ارشد مهندسی برق-مخابرات خود را از دانشگاه شاهد دریافت نمود. از سال ۱۳۹۰ تا ۱۳۹۲ نام‌برده به عنوان دستیار تحقیقاتی در مرکز تحقیقات مخابرات ایران به کار مشغول بود و پس از آن به دوره دکترای مهندسی برق و کامپیوتر در دانشگاه راتگرز در نیوجرزی آمریکا وارد گردید. زمینه‌های علمی مورد علاقه او شامل امنیت در تبادل اطلاعات، حسگری فشرده و کاربرد آن در آشکارسازی سیگنال، و پردازش دیجیتال سیگنال است.