نخستین همایش ملی واکاوی تهدیدهای نوپدید دفاعی - نظامی
دافوس آجا - آبان ماه ۱۳۹۷
دانشگاه فرماندهی و ستاد آجا

ارائه راهکاری جدید برای کاهش حملات DDOS در ابر با استفاده از روش های محاسباتی نرم

هادی روح پرور*

* کاشناسی ارشد نرم افزار ، Hadyroohparvar@gmail.com

چکیده

امروزه محیط ابر و رایانش ابر از موضوعات تحقیقاتی مهم به شمار می رود ماهیتاً. هدف آن تحکیم کاربری تجاری از طریق توسعه تکاملی ، بسیاری از رویکردهای موجود و فناوری های محاسباتی است۰سیستم دفاعی پیشنهادی دارای پنج واحد است که با هدف فیلتر حملات DDOS کاربرد دارد۰

مقدمه

حمله DDOS مخفف (denial of service attack) به زبان ساده یعنی سرازیر کردن تقاضاهای زیاد به یک سرور و استفاده بیش از حد از منابع (پردازنده، پایگاه داده، پهنای باند، حافظه و...) به طوری که سرویس دهی عادی آن به کاربرانش دچار اختلال شده یا از دسترس خارج شود (به دلیل حجم بالای پردازش یا به اصطلاح overload شدن عملیات های سرور)، عاملین حملاتDDOS به طور معمول سایتهای مختلفی را مورد حمله قرار میدهد که تاثیر آنها در هر حمله متفاوت است و ناراحتی جزئی را در کاربران به همراه دارد و یا در برخی موارد ممکن است زیانهای مالی جدی را برای شرکت هایی که به صورت بر خط به کسب و کار می پردازد به بار آورد.

مبانی نظری و تجربی

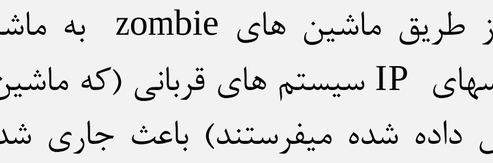
دسته بندی سیل حملات DDOS

حملات مستقیم و حملات بازتابنده در حملات مستقیم مهاجم به طور مستقیم سیل بسته ای جعلی را از طریق ماشین های zombie به سمت قربانی میفرستد. حملات DDOSمستقیم به دو دسته از حملات طبقه بندی می شوند. حملات DDOS علیه شبکه و حملات DDOS علیه کاربرد. حملات DDOS علیه شبکه شامل TCP flood، UDP flood، Icmp flood، syn flood میشود. حملات DDOS علیه کاربرد شامل سیل http، سیل https، سیل FTP و. . . اشاره کرد.

در حملات بازتابنده مهاجم از طریق ماشین های zombie به ماشینها پیام درخواست نیز میفرستد و از طریق جعل آدرسهای IP سیستم های قربانی (که ماشین های بازتابنده به عنوان نتیجه ،پاسخ خود را به آدرس داده شده میفرستند) باعث جاری شدن سیل بسته در سرور قربانی میشود. حملات بازتابنده شناخته شده، شامل حملات پاسخ به سیل ICMP ECHO، سیل syn acknowledge سیل DNS و حملاتspoof نیز می شود

روش پیشنهادی ما مبتنی بر شناخت رفتار کاربر مجاز نسبت به سرور است. به عبارت دیگر یک کاربر معمولی در یک دوره زمانی رفتار تقریبا مشخصی از لحاظ تعداد تقریبی درخواست ها به سرور و مقدار پهنای باند مصرفی در بازه زمانی هنگام دسترسی به سرویس دهنده وب را از خود نشان می دهد. برای پیش گیری از انجام این نوع از حملات، استفاده از دیوار آتش در اکثر این شبکه ها است .

بزرگترین مشکلی که در ابتدای کار وجود دارد، دسته بندی داده های ورودی به دو بخش کاربران مجاز و غیر مجاز (مشکوک به حمله کردن) است. درخواست هایی که مشکوک باشند می بایست شناسایی شوند و از طریق دیوار آتش بلاک شوند. طرح ارائه شده بر اساس روالی که در شکل۱ نشان داده شده عمل می کند.



شکل ۱: طرح دفاعی پیشنهادی

در هر مرحله از این طرح ترافیک ها بررسی می شوند به این معنا که خروجی هر یک از ماژول ها که ترافیکی را غیر نرمال و مشکوک شناسایی کرد آن را به دیوار آتش می فرستد و برای بازه زمانی آن ترافیک را بلاک می کند و در نتیجه این فیلتر ها حجم درخواست های رسیده به ماژول متعادل کننده بار که انتظار می‌رود از نوع ترافیک نرمال باشند کاهش می یابد۰

زمان انتظار برای درخواست جاری با توجه به سرعت پردازنده و بارکاری روی ماشین مجازی به دست می‌آید (رابطه شماره ۱) در نهایت، درخواست به ماشینی اختصاص داده می شود که مجموع زمان پردازش و انتظار آن، کمترین مقدار را داشته باشد

$$\text{زمان انتظار} = \frac{\text{بار روی ماشین مجازی}}{\text{سرعت پردازنده ماشین مجازی (MIPS)}} \quad (۱)$$

ماژول متوازن کننده بار، قدرت پردازش ماشین های مجازی را بدست می آورد. هر چه قدرت پردازش ماشین مجازی بالاتر باشد زمان اجرا کمتر و هر چه قدرت ماشین مجازی پایین تر باشد، زمان اجرا طولانی تر می شود (رابطه شماره ۲۰)

$$\text{زمان اجرا} = \frac{\text{تعداد دستورالعمل های درخواست جاری}}{\text{سرعت پردازنده ماشین مجازی (MIPS)}} \quad (۲)$$

متوازن کننده بار همچنین زمان پاسخ درخواست جاری را که مجموعی از زمان انتظار و اجرا است، روی تمام ماشین های مجازی (رابطه شماره ۳) محاسبه می‌کند.

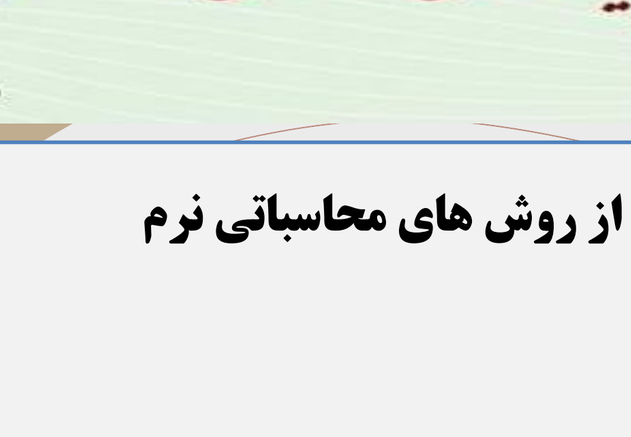
$$\text{زمان پاسخ} = \text{زمان اجرا} + \text{زمان انتظار} \quad (۳)$$

یافته های پژوهشی

سیستم پیش بینی کننده صحت درخواست دارای یک تابعی است که نوع درخواست رسیده را مشخص می کند. درخواست ها بر اساس نوع آنها به مسیر خود در طرح پیشنهادی ادامه می دهند. اگر درخواست به عنوان درخواست جدید شناسایی شود، به ماژول مدیریت نگهداری درخواست ها ارسال می شود باقی درخواست های تصدیق شده، برای گرفتن سرویس به بخش توازن بار ارسال می شوند. در مرحله احراز هویت درخواست ها را در مخزنی نگهداری و شماره شناسایی کاربر را با استفاده از الگوریتم رمزنگاری ، و به مشتری ارسال می کند

و مشتری می بایست با کلید خود آن را رمز گشایی کند و در صورتی که رمزگشایی صحیح باشد، به مسیر خود ادامه می‌دهد.

فعالیت توازن بار درست بعد از رسیدن درخواست ها از ماژول مدیریت نگهداری درخواست ها آغاز می شود. شکل ۲ الگوریتم متعادل سازی مرکزی بار شبکه را نمایش می دهد،

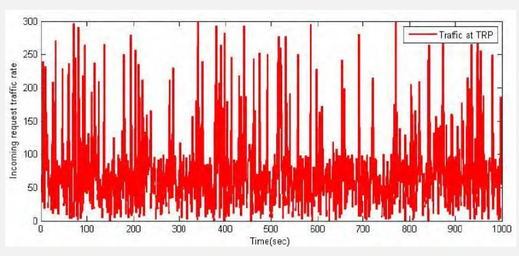


شکل ۲: نحوه انجام طرح کنترل کننده مرکزی بار شبکه

متعادل کننده مرکزی بار شبکه به تمام کاربران متصل است و اولویت های ماشین مجازی را بر اساس سرعت پردازشگر مرکزی ماشین ها و حافظه در دسترس آن ها انجام می دهد. نحوه محاسبه این روش اولویت بندی به صورت رابطه (۴) می باشد.

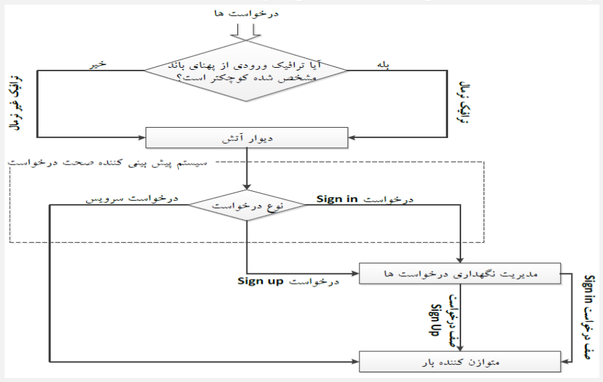
$$\Pr(i) = t * Tc(i) + s^* Tm(i) \quad (۴$$

شکل ۴ نشان دهنده کل ترافیک ورودی به سیستم ارائه دهنده سرویس می باشد و شامل ترافیک خام است؛ نوسانات شکل به دلیل وجود حملات انکار سرویس توزیعی است که هنوز توسط دیوار آتش بلاک نشده اند



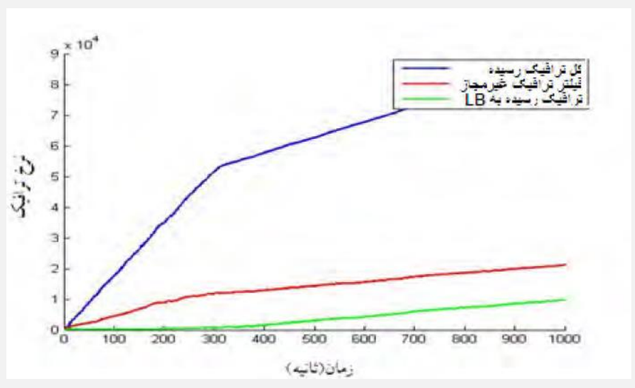
شکل۴: دریافت کننده محدوده ترافیک

در شکل ۵مشاهده می شود، این سیستم در واقع توسعه یافته سیستم پیش بینی کننده صحت درخواست بوده با این تفاوت که فقط برای ثبت درخواست های جدید فعالیت می کند.



شکل۵:دسته بندی درخواست ها

اثر بخشی طرح پیشنهادی را می توان در شکل۶ مشاهده نمود. همانگونه که در شکل مشخص است نرخ جریان ترافیک به سمت وب سرویس با عبور از چند لایه دفاعی در معماری پیشنهادی کاهش یافته است.



شکل ۶: : اثربخشی طرح پیشنهادی

نتیجه گیری

الگوریتم تشخیص پیشنهادی به اندازهٔ کافی برای اجرای استنتاج بست آنلاین سریع بوده و به نرخ تشخیص بالایی دست پیدا کرده است. طرح پیشنهادی این پژوهش درخواست های ورودی را بر حسب تقاضا دسته بندی می کند که این دسته بندی ها موجب بهینه سازی سرویس دهی می شود، همچنین درخواست کاربرانی که از قبل در سیستم ثبت نام نموده اند را سریع تر از باقی درخواست ها فراهم می کند.

طرح پیشنهادی با ثبت و نگهداری ترافیک های درخواستی می تواند نرخ ترافیک برای هر شناسه کاربری را محاسبه نماید . یکی دیگر از مزایایی که می‌توان برای طرح پیشنهادی این مقاله مطرح نمود، شناسایی اضافه بار ترافیک جاری شبکه و تشخیص درخواست کننده‌هایی است که قصد تحمیل این اضافه بار را بروی وب سرویس ها دارند. درخواست های مشکوک به حمله در لیستی توسط دیوار آتش نگهداری می شوند، از این رو کاربرانی که اطلاعات آن ها از قبل در این لیست وجود داشته باشد با ارسال درخواست مشکوک بعدی در یک بازه زمانی کوتاه مشخص می‌شوند که این سرعت بالای شناسایی خود مزیتی دیگر از طرح پیشنهادی است . شبیه سازی های صورت گرفته این مقاله به این مهم دست یافت که به مرور و با گذشت زمان درخواست هایی که در هر دوره توسط دیوار آتش بلاک می‌شوند به صورت چشمگیری کاهش می یابد. همین امر باعث کاهش ترافیک رسیده به متعادل کننده بار و در نتیجه کاهش سربار اضافی و خطر حملات انکار سرویس توزیعی به وب سرویس ها می باشد.

منابع

1. Xiao, L., Wei, W., Yang, W. et al. Soft Comput (2017) 21: 3713. https://doi.org/10.1007/s00500-015-2025-6.
2. Nitesh Bharot, Priyanka Verma ,Sangeeta Sharma,Veenadhari Suraparaju,2018." Distributed Denial-of-Service Attack Detection and Mitigation Using Feature Selection and Intensive Care Request Processing Unit",Arab J Sci Eng ,43:959–967.
3. Zhuo Chen , Fu Jiang ,Yijun Cheng ,Xin Gu ,Weirong Liu ,Jun Peng,2018." XGBoost Classifier for DDoS Attack Detection and Analysis in SDN-Based Cloud".IEEE International Conference on Big Data and Smart Computing (