RT-SAD: Real-Time Sketch-Based Adaptive DDoS Detection for ISP Network

Jul 2021

Security and Communication Networks(Wiely & Hindawi) (rank 11)

آرتی- سد: روشی تطبیق‌پذیر مبتنی بر انگاره برای شناسایی حملات منع‌خدمت توزیع‌شده به صورت درلحظه (بلادرنگ) برای شبکه‌های ارائه‌دهنده خدمات اینترنتی

با گسترش شبکه‌های کامپیوتری و پیچیده‌تر شدن این شبکه‌ها شناسایی حملات منع‌خدمت نیز پیچیده‌تر شده است. از طرفی افزایش دستگاه‌های مبتنی بر اینترنت اشیا و آسیب‌پذیرتر بودن و امکان استفاده از این دستگاه ها در حملات منع‌خدمت توزیع‌شده نیز باعث افزایش چشمگیر حملات در سالیان اخیر شده‌است. برای تشخیص حملات منع‌خدمت حجیم و بزرگ امروزی، تشخیص حملات و ضبط ترافیک در قسمت پشتی (backbone) شبکه از انجام این کارها در نزدیک سمت کاربر موثرتر هست. روشهای قبلی که بیشتر مبتنی بر یادگیری ماشین و یادگیری عمیق بودند به دلیل این‌که از ویژگی‌های آماری استفاده می‌کردند با بروز حملات جدید به مشکل برمی‌خوردند. موضوع یاددادن مجدد آن‌ها با ترافیک جدیدتر و حتی به دست آوردن آن ترافیک‌های جدید جهت آموزش و زمان انجام یاددهی مجدد نیز دشوارهایی به همراه داشت. علاوه براینها روشهای قبلی اکثراً تنها دقت تشخیص و میزان‌خطا را درنظر می‌گرفتند. اما در این مقاله میزان مصرف منابع و کارایی لحظه‌ای نیز مورد آزمایش قرار گرفته است.

بدین منظور این مقاله قصد دارد الگوریتمی سازگارپذیر (که به‌صورت خودکار پارامترهای تشخیص مدل را بر اساس وضعیت فعلی شبکه تغییر می دهد) با عملکردی بهینه و همچنین مصرف بهینه منابع برای شبکه‌های ارائه دهنده خدمات اینترنتی، که از مصادیق شبکه‌های بلادرنگ با سرعت بالا و همچین دسته‌ای از شبکه‌های میانی هستند که تشخیص حملات در آنها به دلیل وجود ترافیک عبوری بیشتر دقیق‌تر هست (که البته این مزیت نیز مشکلات حافظه‌ای و بار پردازشی نیز ایجاد می کند)، معرفی نماید .

طریقه کار: ایده اصلی بخش شناسایی این روش عدم‌تقارن در ترافیک هست. هر جریان مستقل را بر اساس جفت (آی‌پی مبدا، آی‌پی مقصد) می‌شناسد. ترافیک را شامل پنجره‌هایی با اندازه مشخص در نظر می‌گیرد که هر کدام شامل جریان‌های عبوری هستند. هر جریان از یکسری ماژولها عبور می‌کند.

از سه مازول تشکیل شده است:

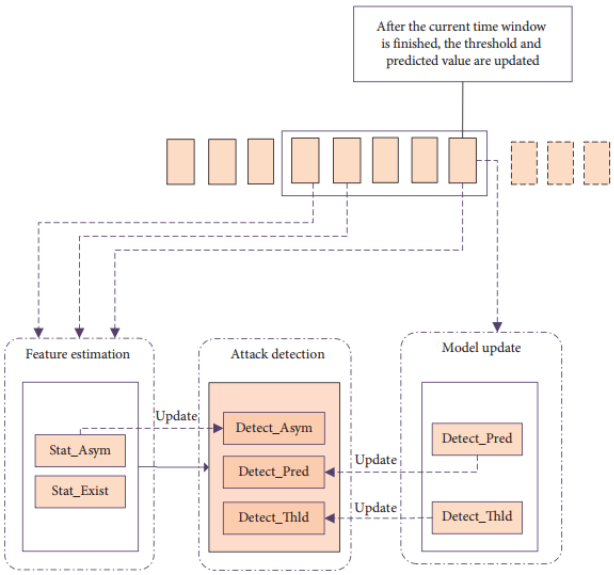

FIGURE 1: Overall architecture.

- Feature extraction: از دو جدول انگاره (یکی برای ذخیره این که این جفت آی‌پی در این پنجره وجود دارد و دیگری برای ذخیره مقدار نامتقارن هر آی‌پی استفاده میشود) برای استخراج و ذخیره ویژگی‌های جریان نامتقارن استفاده می‌کند. و اگر ویژگی نامتقارن مشاهده کرد، برای آدرس آی‌پی مقصد جریان، مقدار ویژگی نامتقارن را افزایش می‌دهد.
- Attack detection: شامل سه جدول انگاره هست. یکی برای ذخیره آستانه هست که بر اساس پس‌مانده‌های پنجره‌های قبلی هست (منظور از پس‌مانده یک آی‌پی در یک پنجره، اختلاف میان مقدار ویژگی و مقدار پیش‌بینی‌شده آن ویژگی هست) :

مقدار آستانه برای هر آی‌پی در پنجره فعلی = میانگین (پس مانده های پیشین) + ۳ x انحراف معیار (پس مانده ای پیشین)

(برای این که منابع را برای ذخیره اطلاعات قبلی هدر ندهد از یک روش جایگزین و همچنین الگوریتم ارائه شده در یک از مراجع استفاده می کند)

جدول دیگر برای ذخیره مقدار موردانتظار است:

مقدار مورد انتظار ویژگی نامتقارن یک آی‌پی = مقدار قبلی نامتقارن مورد انتظار برای آن آی‌آپی (1-a)x + (a) تعداد جریانات فعلی نامتقارن آی‌پی در پنجره فعلی

این دو جدولمدام در حال بروزرسانی هستند و از آن‌ها (شامل مقادیر نامتقارن ویژگی ، مقدار موردانتظار و مقدار آستانه) برای شناسایی استفاده می‌کند و اعلام می‌کند که آیا آدرس آی‌پی مقصد جریان فعلی تحت حمله هست یا خیر.

- Model update : پس از بررسی تمام جریانهای یک پنجره، این ماژول آغاز به کار می‌کند و بر اساس پنجره گذشته، مقدار قابل انتظار و آستانه را به عنوان مقادیر متناظر ویژگیهای متناظر با جریانات را تنها

برای آدرس‌های معمولی که مورد حمله قرار نگرفته‌اند، بروز می‌کند و ویژگی آدرس حمله شده نیز تا زمانی که به حالت عادی بازنگردد، بروز نمی‌شود.

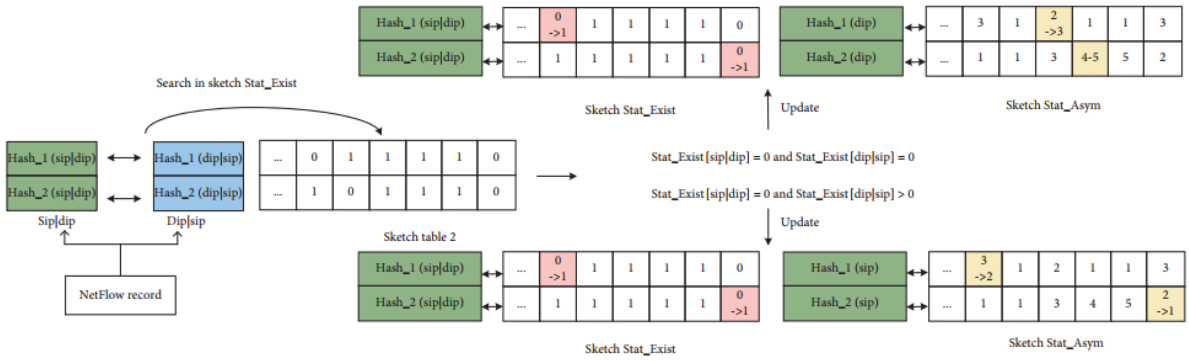

FIGURE 5: Estimation of asymmetric flows.

Input: Sketch Stat_Exist, Stat_Asym
Output: Sketch Stat_Exist, Stat_Asym
(1) **if** Stat_Exist[SIP|DIP] = 0 **then**
(2) Stat_Exist[SIP|DIP] = Stat_Exist[SIP|DIP] + 1
(3) **if** Stat_Exist[DIP|SIP] = 0 **then**
(4) Stat_Asym[SIP] = Stat_Asym[SIP] + 1
(5) **end if**
(6) **if** Stat_Exist[DIP|SIP] > 0 **then**
(7) Stat_Asym[SIP] = Stat_Asym[SIP] − 1
(8) **end if**
(9) **end if**

ALGORITHM 2: Feature updating algorithm.

Input: NetFlow Record, Sketch Detect_Asym, Detect_Pred, Detect_Thld
Output: DDoS attack detection results
(1) **while** Current window not end do
(2) Get a NetFlow record (SIP, DIP)
(3) Update the Detect_Asym [DIP] by using (SIP, DIP)
(4) Residual = abs (Detect_Pred [DIP] − Detect_Asym [DIP])
(5) **if** Residual > Detect_Thld[DIP] **then**
(6) Alert of DDoS
(7) **else**
(8) Put the DIP into Update_Set
(9) **end if**
(10) **end while**
(11) **for** each DIP in Update_Set **do**
(12) Update Detect_Pred [DIP]
(13) Update Detect_Thld[DIP]
(14) **end for**

ALGORITHM 1: DDoS attack detection algorithm.

ارزیابی: از ترافیک ضبط شده واقعی ستون‌فقرات و ترافیک تولید شده به کمک ابزارstrees به منظور ایجاد بسته‌های مرتبط با حملات مختلف منع خدمت توزیع شده استفاده شده‌است. برای معیار ارزیابی، چون روش پیشنهادی‌مان از پنجره استفاده می کند، بنابراین از پنجره زمانی به عنوان واحدی برای ارزیابی نتیجه آزمایش خود استفاده می‌کنیم. برای بهبود هزینه منابع حافظه‌ای و پردازشی نیز نرخ‌های نمونه‌برداری متفاوت و جداول انگاره‌ای مختلف با اندازه‌های متفاوت بررسی شده‌است.به منظور بررسی میزان موفقیت در تشخیص حملات منع خدمت در لحظه، میزان تأخیر در تشخیص حمله و هشداردادن توسط الگوریتم را از زمانی که حمله رخ‌داده هست را درنظر می‌گیریم. از نتایج آزمایش، می‌توان دریافت که الگوریتم عملکرد تشخیص خوبی در لحظه برای نرخ‌های مختلف نمونه برداری از ترافیک شبکه دارد. علاوه بر این، با افزایش نرخ نمونه برداری، تعداد جریان در واحد زمان کاهش می‌یابد، بنابراین میزان بار پردازش الگوریتم افزایش و زمان تشخیص کاهش می‌یابد.

نتیجه گیری: برای شبکه‌های میانی یک الگوریتم سازگار پذیر ارائه شد که از جدوال انگاره برای ضبط و تغییر خصوصیاتی که برای شناسایی حملات استفاده می‌شوند، استفاده می‌کند و آستانه خصوصیت نیز با ترافیک‌های پیشین شبکه مطابقت می‌یابد. از نتایج آزمایش معلوم شد که روش پیشنهادی کارایی خوبی در تشخیص، مصرف منابع و در لحظه‌بودن دارد. اما همزمان می‌توان در مورد نرخ نمونه گیری و تنظیم اندازه ساختارهای انگاره به صورت تطبیقی نیز بهبودهایی را انجام داد.

ارتباط با موضوع پروژه :

- استفاده از ISP ها به دلیل که ترافیکها عبوری از آنها می گذرند
- استفاده از ویژگی نامتقارن (آیا هرنوع حمله منع‌خدمتی را میتوان با آنها تشخیص داد؟)
- استفاده از ابزار stress برای تولید ترافیکهای مهاجم از نوع هر حمله منع‌خدمتی و استفاده از ترافیک موجود CERNET (حجم ۱ ترابایت)
- معیارهای FPR,FNR
- Sketch ها ؟