Low-rate DDoS attack detection method using data compression and behavior divergence measurement (LDDM)

Jan 2021

Computer and Security

14 citations

حملات منع خدمت توزیع شده به دو دسته high-rate و low-rate تقسیم می‌شوند.حملات منع خدمت با نرخ پایین(مخفی) به دلیل شباهتشان با ترافیک‌های معمولی به سختی قابل شناسایی هستند. این مقاله اسکچ‌های چندبعدی[1] و روشهای اندازه گیری بهینه برای جریانهای شبکه ارایه می‌دهد. متود اندازه‌گیری واگرایی[2] بهبود یافته که بر اساس daub4 wavelet transform می‌باشد، درصد انرژی واگرایی هر اسکچ را اندازه گیری می‌کند. که استفاده از این روش منجر به دستیابی به نتایج خوبی در تمایز ترافیک معمولی و مهاجم می‌شود. علاوه بر این یک روش میانگین متحرک نمایی وزنی اصلاح‌شده[3] که برای ساخت آستانه ترافیک نرمال می‌باشد، طراحی شده است. در همین حال یک مکانیزم فریز ترافیک برای اطمینان از استاندارد بودن آستانه متغیر ارایه شده‌است. درآخر نیز نرخ مثبت/منفی کاذب آن را با متودهای دیگر بررسی می‌کنیم و مشاهده می‌شود که دقت بالایی در شناسایی حملات مخفیانه نرخ پایین دارد.

روشهای بسیاری از انواع مختلف برای شناسایی حملات منع خدمت توزیع شده ارایه شده است: مبتنی بر مدل احتمالاتی، نظریه اطلاعات، اندازه گیری فاصله، یادگیری ماشین، پردازش سیگنال (روش‌های مبتنی بر سیگنال حساسیت بیشتری نسبت به تغییرات دارند) .

LDDOS ها تفاوت کمی در حجم و feature ها با ترافیکهای نرمال و معمولی دارند. Daub4 wavelet transform که یک نوع متداول از discrete wavelet transform می‌باشد نسبت به تغییرات سیگنالی جزیی حساس است. همچنین ما از اسکچهای چند بعدی برای ذخیره اطلاعات جریان که از توابع هش تصادفی استفاده می‌کنند، به جای روش‌های نمونه‌برداری[4] استفاده می‌کنیم. به دلیل یکتابودن مقصد جریان‌ها، جریان‌ها تنها روی آیپی مبدا خلاصه می‌شدند. اما در اینجا جریان‌های دوطرفه را در نظر می‌گیرد. به جای اندازه‌گیری ساختار های اسکچ بازه زمانی واحد، واگرایی‌های اسکچ در بازه‌های زمانی[5] بازبینی و دوباره اندازه گیری شده‌اند. برای نشان دادن واگرایی اسکچ، baseline شبکه مورد نیاز است. بنابرین برای اندازه گیری baseline شبکه به صورت دقیق و بلادرنگ[6]، متود حدآستانه پویا با استفاده از روش میانگین متحرک نمایی استفاده شده است. همچنین برای جلوگیری از اثرگذاری ترافیک مهاجم بر روی baseline، مکانیزم فریز برای استاندارد سازی آن استفاده می‌شود.

---

[1] multi dimensional
[2] divergence
[3] Modified weighted exponential moving average
[4] sampling
[5] Time interval
[6] Real-time

چند تعریف:

اسکچ: به دلیل ماهیت تصادفی بودن توابع هش، توزیع ترافیک نرمال در هر جدول هش تقریباً تصادفی است. و لذا زمانی که ترافیک شبکه به صورت محسوسی تغییر کند، توزیع هش نیز به صورت عظیمی تغییر می‌کند تا آنومالی ها را نشان دهد.

Daub 4 wavelet transform:wavelet ها با توجه به ویژگی‌ای که دارند می‌توانند تغییرات ناخواسته، حتی جزیی ترین‌ها را نیز تشخیص دهند. یک سیگنال S که از K تا المان تشکیل شده است، به یک سیگنال A و یک سیگنال جزییD با استفاده از تبدیل تجزیه می‌شود. و بر اساس این دو سیگنال درصد انرژی سیگنال S اندازه گیری می‌شود(P^d) تا تغییرات سیگنال را نشان دهد.

این متود دو مجموعه ضریب از پیش تعریف شده دارد: ضریب‌های مقیاسی{$\alpha_1, \alpha_2, \alpha_3, \alpha_4$} و ضریبهای موجک {$\beta_1, \beta_2^7, \beta_3, \beta_4$}، که اینها باید در یک رابطه برقرار باشند. سیگنال مقایسی duab 4 یک ماتریس 2/k*K می‌باشد:

$$V=\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_3 & \alpha_4 & 0 & 0 & 0 & 0 & \cdots & \alpha_1 & \alpha_2 \end{pmatrix}.$$

سیگنال موجکی W نیز با همان ابعاد می‌باشد و به همان صورت و تنها با جاگزینی ضرایب موجکی ارایه میشود. و به نحو زیر انرژی سیگنال S محاسبه می‌شود:

$$a_i=\sum_{j=1}^{K} S_j V_{ij} \quad i\in\{1,2,\cdots,\frac{K}{2}\}, \qquad A_j=\sum_{i=1}^{\frac{K}{2}} a_i V_{ij} \quad j\in\{1,2,\cdots,K\},$$

$$d_i=\sum_{j=1}^{K} S_j W_{ij} \quad i\in\{1,2,\cdots,\frac{K}{2}\}. \qquad D_j=\sum_{i=1}^{\frac{K}{2}} d_i W_{ij} \quad j\in\{1,2,\cdots,K\}.$$

$$\Rightarrow \quad P^d(S)=\frac{\sum_{j=1}^{K}(D_j)^2}{(\sum_{j=1}^{K}(A_j)^2+\sum_{j=1}^{K}(D_j)^2)}.$$

P^d زمانی که ترافیک شبکه در حالت غیرعادی باشد به سرعت تغییر می‌کند و مقدارش افزایش پیدا می‌کند اما در حالت عادی مقدار بسیار پایینی خواهد داشت.

[7] interval

معماری LDDM:

از سه تا کامپوننت تشکیل شده است:

Sketch : درابتدا ترافیک شبکه در همه بازه‌ها به صورت جریانی جمع شده و سپس آنها را به پروسه تشخیص ارسال می‌کند. در اسکچ، جریانها در یک ساختار اسکچی با کلیدهای آپی مبدا و مقصد <SIP,DIP> نگاشت شده اند. سپس واگرایی بین اسکچ بازه فعلی و بازه نرمال قبلی حساب شده است (behavior divergence method based on daub 4 wavelet transform) تا p^d را که برای کامپوننت تشخیص می‌باشد، فراهم کند.

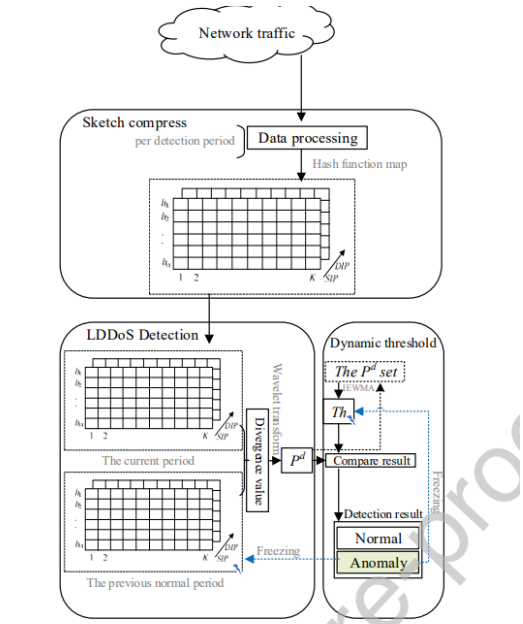

Figure.2 Framework of the proposed low-rate DDoS attacks detection method

Daub4 wavelet transform:

ابتدا چند تعریف ارایه می‌دهیم:

Abnormal hash table: جدول هش ای که انحراف سیگنالی آن در محدوده آستانه نباشد.

Abnormal sketch: اسکچی که بیش از H/2 توابع هش آن abnormal باشند.

Abnormal time: یک بازه زمانی است که در آن یک abnormal sketch در ساختار multi-dimensional sketch باشد. اگر یک بازه زمانی این گونه باشد، مدل مان یک هشدار[8] می‌فرستد.

هر جدول اسکچ به صورت یک سیگنال در نظر گرفته می‌شود و واگرایی بین دو سیگنال متوالی که توزیع خوبی دارند- ترافیک عادی هستند- مقدار واگرایی پایین می‌باشد. برای اندازه‌گیری این واگرایی، این مقاله از daub4 استفاده می‌کند. با اندازه گیری درصد انرژی واگرایی سیگنال، برزگی واگرایی[9] را به دست می‌آورد.

[8] alarm
[9] Divergence magnitude

Algorithm 1. The improved behavior divergence measurement method based on daub 4 wavelet transform

Input: the sketches of the t^{th} time interval, the sketches of the $t+1^{th}$ time interval
Output: the P^d_set
(1) Initialize P^d_set = ø
(2) For each sketch in multidimensional sketch
(3) PD = ø
(4) For each row S_i in a sketch
(5) $S_{dev} = |S_{t+1,i} - S_{t,i}|$
(6) Sort S_{dev} ascendingly
(7) Calculate P^d_i of S_{dev}
(8) Add P^d_i to PD
(9) End for
(10) Add PD to P^d_set
(11) End for

همانگونه که دیده می‌شود این روش بدون نیاز به دیتاست‌های آموزشی روش‌های مبتنی بر یادگیری ماشین، با ترافیک و رفتار متغیر آپدیت می‌شود.

Dynamic threshold: روش ما چون می‌خواهد با ترافیک دایماً در حال تغییر سازگار باشد، باید پویا باشد. به دلیل خاصیت پویایی ذاتی شبکه، درصد انرژی واگرایی سیگنال ثابت نمی‌باشد. و ثابت بودن این مقدار می تواند باعث نرخ مثبت و منفی کاذب زیادی شود. از روش میانگین متحرک متحرک نمایی بهبودیافته (IEWMA) برای محاسبه آستانه پویا استفاده می‌شود.

پارامتهایی که کلاه دارند مقدار تخمینی و بقیه مقادیر واقعی می‌باشند. آلفا بتا و لاندا پارامترهای تغییر پذیر می‌باشند. به دلیل این که در حملات منع خدمت توزیع شده آدرسهای IP مبدا توزیع شده می‌باشند لذا انرژی اسکچ ($p^d(s)$) کم خواهد بود اما در IP های مقصد مقادیر بالا می روند. لذا آستانه‌های پویا این دو باید روش‌های متفاوتی باشد:

$$\hat{P}^d_{t+1} = \alpha P^d_t + (1-\alpha)\hat{P}^d_t,$$
$$d_t = |P^d_t - \hat{P}^d_t|,$$
$$\sigma^2_{t+1} = \beta d^2_t + (1-\beta)\sigma^2_t,$$
$$Th_{t+1} = \begin{cases} \hat{P}^d_{t+1} + \lambda\sigma_{t+1} & sketch.attribute = DIP \\ \hat{P}^d_{t+1} - \lambda\sigma_{t+1} & sketch.attrobute = SIP' \end{cases}$$

Src IP role: ⇨ $\delta_{t+1} = \begin{cases} 1 & Th_{t+1} > P^d_{t+1} \\ 0 & Th_{T+1} < p^d_{t+1} \end{cases}$

Dst IP role: $\delta_{t+1} = \begin{cases} 1 & Th_{t+1} < P^d_{t+1} \\ 0 & Th_{T+1} > p^d_{t+1} \end{cases}$

اگر انرژی از مقادیر آستانه بیشتر شود، یعنی یک abnormal hash table می‌باشد. و علاوه بر این برای جلوگیری از استفاده این مقدار انرژی در بازه بعد (که منجر به نرخ منفی کاذب میشود) از مکانیزم فریز برای آستانه و سیگنال استفاده می‌شود. تا زمانی که حمله برطرف شود، به روزرسانی آستانه ادامه می‌یابد.

a destination IP address as an example to describe the implementation of freezing mechanism.

Algorithm 2. Freezing Mechanism

Input: P_t^d of the t^{th} time interval, Th_t of the t^{th} time interval, σ, β, λ

Output: Th_{t+1}

(1) If $P_t^d > Th_t$

(2) freeze $S_{t,i}$, Th_t

(3) While $P_{t+1}^d < Th_t$

(4) calculate the P^d value of the next time interval $P_{t+1}^d = P^d\left(S_{t+1,i}, S_{t-1,i}\right)$, continue to compare P_{t+1}^d and Th_t

(5) End while

(6) Else

(7) calculate the P_{t+1}^d and Th_{t+1} value of the next time interval, continue to compare Th_{t+1} and P_{t+1}^d

(8) End if

(9) unfreeze Th, calculate the Th_{t+1} value of the next time interval and $P_{t+1}^d = P^d\left(S_{t+1,i}, S_{t,i}\right)$, compare P_{t+1}^d and Th_{t+1}

در کامپوننت آستانه پویا، طبق مجموعه p^d روش میانگین متحرک وزنی نمایی سازگار استفاده می‌شود تا آستانه تشخیص Th را تقریب بزند. ورودی p^d با Th مقایسه می‌شود. سپس p^d در مجموعه p^d ذخیره می‌شود.

اگر تشخیص داده شد که حمله ای رخ داده است مکانیزم فریز صدا زده می‌شود تا اسکچ،آستانه‌ها و متغیرهای مورد استفاده برای تخمین آستانه پویا را فریز کند.

تنظیم پارامترها:

H,K : علاوه برخطا و آزمایش نظریه‌های مختلفی برای اثبات برقراری storage accuracy نیز موجود می‌باشد.

آلفا،بتا و لاندا : ضرایب میرایی هستند که می توانند میزان وابستگی مقدار آستانه به مقادیر بازه‌های قبلی را تعیین کنند. تاثیر لاندا بیشتر می‌باشد و بایستی با دقت بیشتری تعیین شود.

بازه زمانی[10] تشخیص دلتا: ریزدانگی تشخیص و زمان بازخورد را تعیین می:ند. ریزدانگی تشخیص پایین نمی‌تواند مشخصه‌های آماری ترافیک را نشان دهد و می‌تواند به نرخ مثبت کاذب بالا منجر شود. همچنین در زمان پاسخ نیز مساله دارد. ریزدانگی‌های بالا اطلاعات آماری حملات LDDOS را در حجم بزرگی از ترافیک نمی‌توانند بازتاب دهند که منجر به نرخ منفی کاذب بالایی می شود. در این مقاله طول بازه ۱۰ ثانیه تنظیم شده است.

مقادیر اولیه اسکچ و آستانه‌ها بر اساس ترافیک نرمال اولیه شبکه تا زمان m، به دست می‌آیند. این فرض بلااشکال و طبیعی است که در شبکه‌ی ما تا آن زمان، ترافیک‌ها نرمال هستند.در اینجا ما m را ۱۰ گرفتیم.

[10] Time interval

ارزیابی: ترافیک های نرمالی که ضبط شده به همراه ترافیک های حملات منع خدمتی که در آزمایشگاه خودمان اجرا کرده‌ایم با نسبت‌های مختلفی تشکیل انواع دیتاست‌ها را می‌دهند. معیارهای بررسی موثر بودن LDM شامل Accuracy,TPR,FPR,FNR می‌باشند.

پیش‌پردازش داده‌ها:

- ضبط بسته‌ها با استفاده از وایرشارک و به دست‌آوردن مقادیر: timestamp,srcIP,destIP,src port,dest port,protocol and bytes.
- تبدیل آدرسهای آیپی به مقادیر عددی
- تجمیع ها بسته ها در جریانها با مشخصات srcIP,dstIP در مدت زمان بازه زمانی تعیین شده.

نتایج نهایی بدین شرح می‌باشد:

Table 5 Setting values of the related parameters

Items	Parameters	Description	Values of Dataset1,2,3	Values of Dataset4	Values of Dataset5
Sketch	H	Number of hash functions	5	5	5
	K	Size of hash table	100	100	16000
IEWMA	α	Damping coefficient	0.1	0.7	0.7
	β	Variance damping coefficient	0.1	0.1	0.3
	λ	Threshold damping coefficient	3	3	4
Other parameters	ΔT	Detection time interval	20s	20s	20s

Table 6 Overall effects of the proposed LDDM

Dataset	Dataset1	Dataset2	Dataset31	Dataset4	Dataset5
Acc	0.97	0.98	0.98	0.98	0.95
TPR	0.95	1	1	1	1
FPR	0.01	0.02	0.02	0.02	0.05
FNR	0.04	0	0	0	0

C. Availability analysis of multidimensional sketch structure

همچنین در بحث بررسی اسکچها مشاهده می‌کنیم که اسکچهای تک بعدی(مثلا کلید آنها تنها SIP می‌باشد) در مقایسه با اسکچ‌های چندبعدی استفاده شده دقت پایین تری خواهند داشت. به دلیل این است که در زمان وقوع حملات منع خدمت توزیع‌شده، مجموعه آدرس آیپی مبدا و مقصد بهتر می‌تواند بی نظمی را نشان بدهند.

سپس کارایی متود اندازه‌گیری واگرایی بهبود یافته مبتنی بر daub4 (reordered duab4) (میزان بزرگ بودن انرژی p^d) با قبل از بهبود آن مقایسه شده است که نتیجه می‌گیریم بهتر می‌تواند در تشخیص ترافیک حمله کمک کند.(یعنی در صورت وقوع حمله p^d بزرگتر می‌باشد)

برای ارزیابی روش بکاررفته برای آستانه پویا و مکانیزم فریز، مشاهده می شود که این راهکار ها به خوبی در ترافیک دایم در حال تغییر جواب می‌دهند.

در کارهای آینده برای بررسی زمان موردنیاز، به برروی تکنیک نمونه برداری و توزیع یافتگی برای کاهش بیشتر پردازش جریان‌های شبکه در شبکه های با سرعت بالا بررسی می‌کنیم

درآخر راهکارمان را با چندتا روش دیگر که آنها هم از اسکچها و روشهای سیگنالی استفاده می‌کنند بررسی می‌نماییم.نتیجه می‌شود که واگرایی اسکچ در بازه‌های زمانی متوالی بهتر میتواند از اسکچ‌های تنها در یک بازه زمانی واحد حملات را تشخیص دهد. تبدیل

موجک نیز به در مقایسه با دیگر متودها حساستر است. در خلاصه که IDDM به خوبی می‌تواند LDDOS ها را در محیط‌های مختلف شبکه(LAN یا WAN) شناسایی کند.

نتیجه گیری: