Smart Defense: A distributed deep defense against DDoS attacks with edge computing

Arizona State University

2022

Computer Networks

ظهور دستگاه‌های IOT منجر به بروز حملات منع خدمت با ترافیک حجیم (تا ۲.۳ ترابایت بر ثانیه) شده‌است. روشهای پیشگیری شناسایی حملات منع خدمت به دو دسته تقسیم می‌شوند:

- نزدیک مقصد: استفاده از همان روش‌های سنتی یادگیری ماشین و پکت فیلترینگ و کنترل نرخ‌گذر و.... این روش‌ها به دلیل شبیه بودن ترافیک کاذب با ترافیک‌های نرمال مثبت کاذب زیادی دارند.و در مقابل حملات حجیم امروزی تنها راه‌حلی که باقی می‌گذارند، قطع سیستم قربانی و یا هدایت ترافیک به مراکز دیگری است.
- نزدیک مبدا: در ترافیک‌های حجیم و توزیع شده امروزی کافی نیستند به دلیل این که اطلاعات کافی از استریم‌ها ندارند و نمی‌توانند حملات توزیع‌شده را به درستی تشخیص دهند.

روشهای شناسایی از جهتی دیگر به دو دسته تقسیم می‌شوند اما در حجم‌های حملات امروزی با مشکل روبرو خواهند شد:

- آماری
- یادگیری ماشین

شبکه‌های نرم‌افزارمحور برای مدیریت شبکه‌هایی شامل اینترنت اشیا استفاده می‌شوند و مدیریت شبکه‌های با گستردگی بالا را آسان‌تر می‌کنند. همچنین راهکارهای ایمن نگه‌داشتن مبتنی بر این شبکه‌ها ارایه شده‌است.

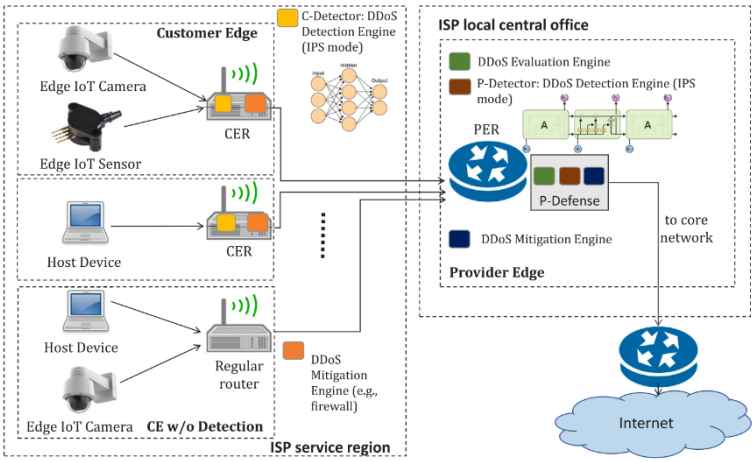
روشهای مبتنی بر یادگیری عمیق با وجود موثر واقع‌شدن در مقابله با حجیم بودن ترافیک یا از روشهای مبتنی بر یادگیری ماشین استفاده می‌کنند مانند Self organizing Map که در بحث یادگیری با کندی یا نرخ مثبت کاذب بالا در ترافیک‌های بلادرنگ مواجه هستند یا منجر به خطای مثبت کاذب در real-time می‌شوند. روشهای مبتنی بر یادگیری تقویتی عمیق با وجود عملکرد خوب در شناسایی و ذخیره‌کردن الگوهای ترافیک،یافتن راه حل بهینه (الگوی حمله) ناکارآمد بوده و می توانند یکنواختی را نقض و تاخیر ایجاد کنند. روشی که ارایه می‌دهیم به ISP ها این امکان کنترل را می‌دهد که مدل آموزش داده‌شده با حملات در حال تغییر سازگار باشد. همچنین این دسته از روش‌های یادگیری ماشین امکان پیاده سازی روی سخت‌افزارهای محدود را دارا می‌باشند.

این مقاله قصد دارد یک روش توزیع‌شده مبتنی بر تشخیص بی‌نظمی یادگیری ماشین برای شناسایی و مقابله با حملات منع خدمت توزیع‌شده با کمک محاسبات لبه ارایه دهد. این روش به دلیل شناسایی مقدار زیادی از حملات در مبدا (معیار کارآمدی بسیاری از روش‌های تشخیص حملات) ، از هدررفت پهنای‌باند جلوگیری می‌کند و همچنین یکنواختی[1] را در زمانهای پیک به دلیل ماهیت

[1] consistency

توزیع‌شده آن (PE,CE) را دارا می‌باشد. همچنین از اطلاعات به دست آمده توسط موتورهای تشخیص مستقر در قسمت فراهم‌کننده و ارسال اطلاعات موردنظر آنها از سمت مشتری، ISP ها می‌توانند دستگاه‌های بات نت مستقر در قسمت مشتری‌ها و ترافیک‌آنها را شناسایی کنند و از پردازش مجدد این ترافیک‌ها جلوگیری کنند. این روش در مقابله با حملات اسپم نیز می‌تواند مفید واقع شود. در این روش دو شبکه یادگیری عمیق استفاده و بررسی شده‌است.

در نتیجه ارزیابی نیز مشاهده می کنیم که می‌تواند ۹۰ درصد ترافیک را در مبدا (لبه مشتری) و ۹۷ درصد از حجم باقی مانده را در سمت فراهم کننده شناسایی و کنترل نماید.



مدل و معماری: از یادگیری عمیق برای شناسایی حملات به دلیل مصرف کم‌تر حافظه نسبت به روش‌های دیگر یادگیری ماشین و همچنین دقت بالاتر استفاده می‌کنیم. دستگاه‌های مبدا با استفاده از SDN مدیریت می‌شوند. برروی دو بخش لبه مشتری(CE) و لبه فراهم کننده(PE) اجرا می‌شود. اجزای اصلی این دو بخش به ترتیب Customer Edge Router و Provider Edge Router که روترهای برنامه پذیر و مدل پیشرفته‌تر مودم‌های کابلی هستند.

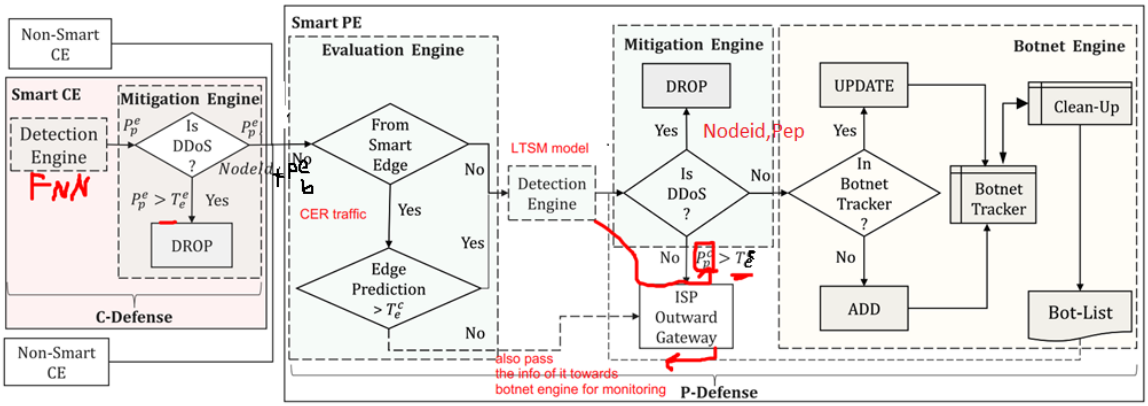
CER ها یک کامپوننت C-Defense دارند که از یک شبکه عصبی عمیق برای شناسایی استفاده می‌کند و مدام توسط ISP آموزش داده می‌شود. PER ها به CER متصل بوده و ترافیک از این طریق عبور خواهدکرد. در CE یک ماژول تشخیص حمله سبک برای پیش اسکن ترافیک مهاجم اجرا می شود تا از بار روی PE بکاهد. CER از دو بخش تشکیل شده است: تشخیص (الگوریتم یادگیری ماشین که یک احتمالی برای ترافیک می دهسد) و مقابله[۲] : در اینجا مقدار آستانه تعریف شده (برای هر CE می تواند متغیر باشد و توسط ISP تعیین می‌شود) تعیین می‌کند که ترافیک در همان منبع دور ریخته شود یا به لایه‌های بالایی برود.P-Defense که در PE هست ترافیک‌های جمع‌آوری‌شده توسط کامپوننت C-Defense را بیشتر می تواند بررسی کند (براساس احتمال به دست آمده). از سه بخش تشکیل شده است: ماژول ارزیابی: بر اساس دو مقدار آستانه برای ترافیک ورودی از CEو خروجی از ISP تصمیم می‌گیرد. اگر ترافیک ورودی از مقدارآستانه پایین‌تر بود به ماژول بعدی P-Detector می رود که درآنجا ترافیک‌های ارسالی از منابع متفاوت را به هم وصل می‌کند و بر اساس آن برای شناسایی تصمیم می‌گیرد و سپس برای مقابله به بخش mitigation می‌فرستد.

مدل مهاجم: فرض می‌کنیم CER و PER دیوایسهای کاملاً محافظت‌شده باشند. P-defense به خاطر botnet engine ای که دارد می‌تواند از مورد قربانی قرارگرفتن خودش جلوگیری نماید.

[۲] mitigate

دیتاست مورد استفاده CICDOS2019 می‌باشد که شامل حملات حجیم(روی ۱۲ تا پروتکل مختلف باشد) و متداول منع خدمت امروزی باشد.از برخی برای یاددهی وبقیه برای آزمایش استفاده می‌کنیم.

جزییات:



Algorithm 1 C-Defense Implementation Algorithm

1: Input: Outgoing Traffic(R)
2: Output: Action To Take(A)
3: **procedure** AT-THE-SOURCE(R)
4: F ← Extract-Features(R) src ip,dst ip,protocol,packet inter-arrival time,
5: P_p^e ← DETECTION-ENGINE(Model, F) threshold
6: **if** MITIGATION-ENGINE(P_p^e, T_e^c) is *FORWARD* **then**
7: FORWARD tuple(R, NodeId, P_p^e)
8: **else**
9: DROP R
10: **end if**
11: **end procedure**

I. C-Defense : مدل FNN (مبتنی بر DNN) توسط یک دیتاست از انواع مختلف حملات منع خدمت برچسب گذاری‌شده، توسط ISP مرتباً آموزش داده می‌شود.

II. P-Defense : مدل LTSM نیز توسط ترافیک‌های حمله برچسب‌گذاری‌شده،آموزش داده شده‌است.

III. Botnet engine: یک جدول ترافیک دارد که شامل NodeId,DestIP,SrcIP,DestPort,SrcPort,FwdPacket (number of forwarded packets),BwdPackets(number of backward packets),P_b^c می‌باشد. هر entry بعد از یک مدت t پلک خواهد شد. هنگام حذف یک entry اگر FwdPckt از MinFwdPckts باشد، NodeIdمربوطه به لیست مشکوک‌ها اضافه می‌شود و وقوع‌های دوباره آن شمارش می‌شود. اگر تعداد دفعات حاضر شدن آن nodeId بیش از مقدار تعیین شده توسط ISP باشد، به لیست سیاه اضافه می‌شود و به این روش تشخیص بر مبنای رفتار پایه‌ای یک سیستم بات هست که در آن درخواستی فرستاده شود، اما فرستنده تمایلی آن درخواست را ادامه نمی‌دهد. که درنتیجه تعداد بسته‌های سشن کمتر از مقدار آستانه تعیین‌شده خواهد بود.

به دلایل زیر دولایه تشخیص باید داشته‌باشیم:

- ترافیک های ناهمگون (همشون از CEها نمی‌آیند) که به ISP PE وارد می‌شوند.

- ترافیک های وابسته به زمان-مکان : با استفاده از LTSM می‌توان آنها را کنترل کرد
- یکنواختی : مقداری از کار را به روی لبه مشتری تقسیم می‌کنیم

ارزیابی کارایی: دیتاست را نرمال سازی کرده و همچنین ویژگی[3]های بی‌اهمیت و رکوردهای تکراری را حذف کرده‌ایم. با دو مد ترافیک تست کرده ایم، مد اول که برخی از CE ها ترافیک بات دارند و در مد دوم همه CE ها دیوایس بات دارند. اینکه چرا از مدل‌های موجود، دو مدل LTSM و FNN انتخاب شده‌است، در مقاله ذکر شده است. سپس دقت این دو مدل را در تشخیص انواع حملات مقایسه کرده است.از آزمایش‌ها نتیجه می‌گیرد که شبکه‌های عصبی ساده مثل FNN به تنهایی برای شناسایی حملات توزیع شده کافی نیستند و مدلهای مبتنی بر time-series می‌توانند موثر واقع شوند.

[3] feature