An Efficient IDS Framework for DDoS Attacks in SDN Environment

IEEE Access(May 2021)

8 citations

طراحی یک سیستم تشخیص‌نفوذ مقرون‌به‌صرفه برای شناسایی حملات منع‌خدمت توزیع‌شده در شبکه‌های نرم‌افزار محور

سرعت ایجاد و انتقال اطلاعات در شبکه‌های کامپیوتری روزبه‌روز افزایش می‌یابد. یکی از معماری‌هایی که در شبکه‌های بزرگ (سرعت تولید و انتقال اطلاعات در آنها زیاد هست) به کار می‌رود، چارچوب شبکه‌های نرم‌افزار محور است. قابلیت سازگاری و مقیاس‌پذیر بودن و این‌که به صورت پویا میتوان تنظیمات و قوانین فوروارد بسته‌ها را تغییر داد، باعث محبوبیت شبکه‌های نرم‌افزارمحور و استفاده از آنها در شبکه‌های گسترده و بزرگ شده‌است. اما این طراحی با وجود خوبی‌ها، چندین مشکل اساسی در طراحی خود دارد که می‌تواند مورد سوء استفاده مهاجمین برای اجرای حملات منع خدمت قرار بگیرد:

- منطق شبکه بر روی یک بخش به نام کنترلر هست که به معنای متمرکز بودن است.
- استفاده از سوییچ‌های لایه داده که هیچ گونه هوشمندی ندارند.

هدف این مقاله ارائه فریمورکی برای شبکه‌های نرم‌افزارمحور هست که به کمک DPDK و بدون استفاده از سخت‌افزار ویژه‌ای، مشکلات موجود را برطرف کند؛ همچنین این راهکار به صورت موثرتری نسبت به دیگر راه‌حل‌های موجود می‌تواند جلوی حملات منع خدمت را بگیرد. به کمک ابزار DPDK یک الگوریتم تشخیص ناهنجاری آماری به صورت VNF (در این رویکرد از سرورهای مجازی برای ارائه خدمات مبتنی‌برشبکه به جای پیاده سازی آنها برروی قطعات فیزیکی مجزا استفاده می شود.درواقع تمرکزما از سمت سخت‌افزار به نرم‌افزار می‌رود) را فراهم می‌کنیم.

راهکارهای که در شبکه‌های نرم‌افزارمحور مورد استفاده مهاجمین هست به سه دسته اصلی زیر تقسیم می‌شوند:

- سرریزبافر که به‌دلیل محدودیت حافظه برای نگه‌داری اطلاعات هست.
- سرریز کنترلر که به‌دلیل ماهیت متمرکز شبکه‌های نرم‌افزارمحور هست.
- سرریز جداول جریان در سوییچ‌های لایه داده که برای مسیریابی استفاده می‌کنند.
- سرریز ظرفیت لینکی که برای ارتباط بین کنترل و دستگاه‌های لایه داده استفاده می‌شود.

عامل‌اصلی که باعث می‌شود شبکه‌های نرم‌افزارمحوردر برابر حملات‌منع‌خدمت آسیب‌پذیر باشند، متمرکز بودن برروی لایه کنترلر هست و درنهایت مهاجمین با انجام حملات منجر به آسیب به این بخش خواهندشد.

مشکل روشهای فعلی شناسایی حملات، استفاده و تحمیل بیش از حد برروی اجزای شبکه به خصوص کنترلر هست. حملاتی که صورت می گیرد در آخر منجر به آسیب به کنترلر می‌شود و باعث تحمیل بار زیادی برروی این نقطه می‌شود. لذا در شبکه‌های با نرخ‌انتقال بالا نمی توان از این روشها استفاده کرد. راه حل استفاده از یک الگوریتم سبک آماری تشخیص ناهنجاری هست که بخشی از پردازش خود را به لایه داده واگذار و برروی آن پیاده سازی می‌کند. الگوریتمهای آماری به کمک تعدادکمی از خصوصیتها و با حجم‌کم خود امکان شناسایی حملات

جدید همراه با نرخ پاسخ بالاتر و سربار کمتر نسبت به به روشهای دیگر را دارا می باشند.

معماری: سوییچ‌های مجازی که استفاده می‌شود از نوع OVS هستند اما به منظور افزایش کارایی از ابزار دیگر در کنار سوییچها به نام تکنولوژی DPDK استفاده می‌کنیم که می‌تواند فرایند ضبط و مانیتور بسته‌ها را با سرعت چشمگیری بهبود ببخشد، و نام سوییچ را OVS-DPDK می‌گذاریم. علت اصلی بهبود سرعت پردازش ها توسط DPDK به دلیل نرفتن به فضای کرنل برای انجام عملیات دریافت بسته‌هاست و این امر را در همان سطح کاربر انجام می‌دهد. به همین دلیل روش ارائه شده به DPDK based DdoS Detection یا همان D3 نامگذاری شده‌است. به‌دلیل اینکه از NFV استفاده می‌کند هیچ‌گونه وابستگی به دستگاه و سخت‌افزار جانبی ندارد و مقرون‌به‌صرفه است.

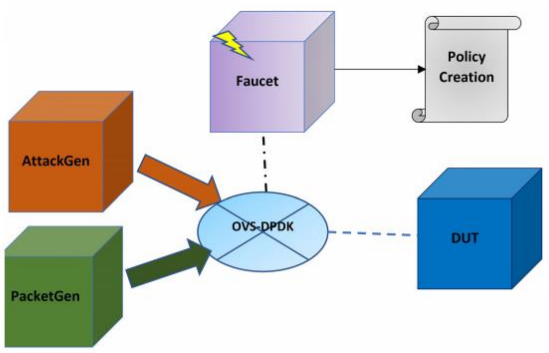

FIGURE 4. Network model of the proposed system.

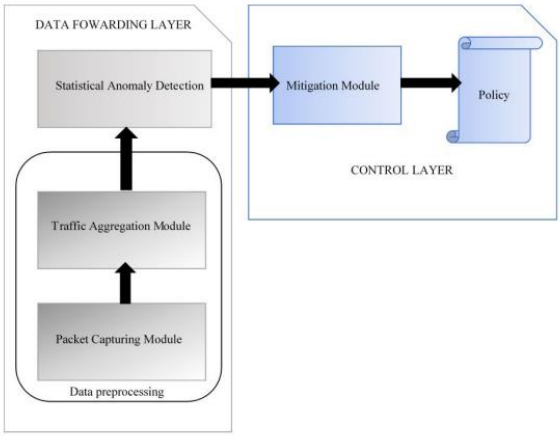

FIGURE 6. Modules in the D3 framework.

DUT: دیتاسروری که مورد حمله قرار می‌گیرد، و همچنین DPDK بر روی آن پیاده‌سازی شده‌است. مسئولیت شناسایی حملات را نیز برعهده دارد.

Faucet: کنترلری که مسئولیت مانیتور و کانفیگ خط‌مشی‌ها را بر اساس اطلاعات به‌دست‌آمده از شناسایی حملات دارد.

طریقه کار الگوریتم تشخیص: یک ویژگی آماری (میانگین نرخ‌گذر) را برای تمامی پورتهای سرور (هر کدام به یک مقصد متفاوت هستند و بسته‌هایی که مقصدشان یکی هست را یک جریان درنظر می‌گیرد) در یک بازه زمانی ثابت به دست می‌آورد. سپس برای هر پنجره میانگین وزن‌دار را محاسبه می‌کند، و به‌عنوان معیار برای شناسایی ناهنجاری و پیش‌بینی حملات برای اسلات بعدی استفاده می‌کند؛ با درنظرگرفتن این نکته که اگر حمله‌ای رخ دهد، نرخ بالایی از تغییرات را مشاهده خواهیم کرد.چون از یک معیار برای شناسایی استفاده می‌کند، سرعت تشخیص بالایی دارد.علاوه براین ترافیک نرمال فعلی را به پنجره بعدی اضافه می‌کند که منجربه کاهش نرخ مثبت کاذب خواهد شد.

ماژول رفع تهدید :

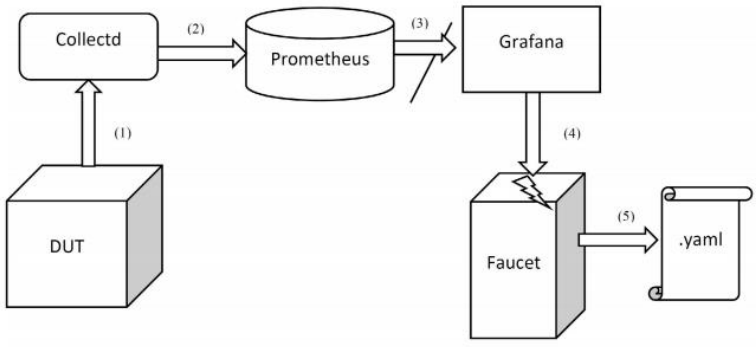

FIGURE 7. Block diagram of mitigation module.

پرومتئوس: پایگاه داده سری زمانی و سیستم مانیتور مبتنی بر pull.

گرافانا: پنل مانیتور و آنالیز تصویری متن‌باز برای پایگاه‌داده پرومتئوس با قابلیت ارسال نوتیفیکیشن به کنترلر SDN

اگر بی نظمی تشخیص داده شد (پیغامی ارسال شد)، کنترلر SDN (faucet) فایل کانفیگ را تغییر می‌دهد. برای رفع مخاطره می‌توان بسته مشکوک را دورانداخت، جریانات را به سمت مقصد خاصی را محدود کرد، پورتی را مسدود کرد یا ترافیک را برای بررسی‌های بیشتر به مراکز scrub ارسال کرد.

پیاده سازی:

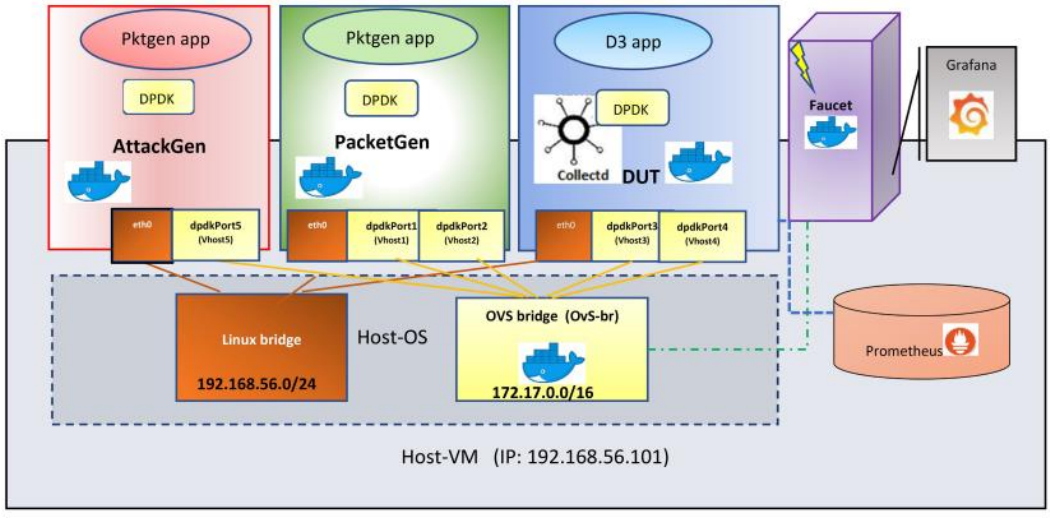

FIGURE 9. Test environment.

ارزیابی:

ارزیابی چارچوب برای آزمایش کارایی IDS انجام می‌شود در حالی که ارزیابی الگوریتم برای بررسی اثرتشخیص اجرا می‌شود.

ارزیابی چارچوب: بررسی کارایی در سه مرحله انجام می‌شود:

- مقایسه کارایی (پهنای باند) و میزان تاخیر OVS و OVS-DPDK
- مقایسه مکانیزم‌های ضبط بسته‌ها با سامانه‌های تشخیص نفوذ دیگر با معیارهای میزان پردازشگر و حافظه مصرفی و میزان دوراندازی بسته‌ها
- مقایسه میزان استفاده بهینه از پردازشگر در d3 با روش‌های دیگر تشخیص‌نفوذ مبتنی بر SDN

ارزیابی الگوریتم تشخیص: در دوقسمت به مقایسه D3 و Overwatch (الگوریتم دیگری که در لایه داده عمل می‌کند) با معیارهای زمان تشخیص، میزان استفاده از حافظه، دقت، معیار f1 و α1 پرداخته است، که اولی با استفاده از چارچوب D3 اجرا شده‌است و در دومی برای تصدیق الگوریتم تشخیص از مجموعه داده CIC dos استفاده کرده است.

نتایج آزمایشات بالا را می‌توان به صورت زیر خلاصه کرد:

چارچوب D3 در مقایسه با سیستم‌های موجود در محیط SDN بسیار کارآمد است، زیرا مکانیزم ایده‌آلی برای گرفتن بسته (DPDK) را در مقایسه با سایر IDS ها ارائه می‌دهد، عملکرد را نسبت به چارچوب OVS افزایش می‌دهد و سربار پایینی بر کنترل‌کننده در یک شبکه پرسرعت تحمیل می‌کند. علاوه بر این، توانایی تشخیص الگوریتم D3 در یک شبکه پرسرعت با معیارهای زمان تشخیص، استفاده از حافظه، دقت، معیار F1 و خطای α برتر از سایرین است. همچنین ارزیابی الگوریتم استفاده‌شده در رقابت با سه راهکار دیگر تشخیص حملات منع‌خدمت در SDN با استفاده از مجموعه داده‌های CIC DoS که در دسترس عموم هست، تایید می‌شود.

کارهای آتی: کارهایی که در آینده برای بهبود سیستم می‌تواند صورت گیرد:

- توسعه مقیاس و اندازه فریمورک با استفاده از پورتهای مقصد بیشتر برای حملات بزرگتر
- معرفی یک الگوریتم تشخیص سازگارپذیر مبتنی بر آستانه
- توسعه ماژول رفع مخاطره
- مدیریت پویای منابع به کمک تکنیک load balancing

ارتباط با موضوع انتخابی:

- معیارهای معرفی شده F1,α
- استفاده از دیتاست معرفی شده.