تشخیص و کاهش حملات DoS و DDoS در SDN حالت مبتنی بر IoT: یک رویکرد تجربی

مقدمه

ظهور مورد انتظار اینترنت اشیا IoTباعث ایجاد تقاضای زیادی از دستگاه‌های تعبیه‌شده شده‌است، که تعامل مستقل حسگرها و فعال‌کننده‌ها را در حالی که همه نوع خدمات هوشمند را ارائه می‌دهند، پیش‌بینی می‌کند . با این حال، این دستگاه‌های IoT در محاسبه، ذخیره‌سازی، و ظرفیت شبکه محدود هستند، که هک و مصالحه را آسان می‌کند . برای دستیابی به توسعه امنIoT ، مهندسی راه‌حل‌های امنیتی مقیاس پذیر بهینه شده‌برای اکوسیستم IoT ضروری است .

تعریف مسئله و هدف اصلی مقاله

در سال‌های اخیر، ما شاهد محبوبیت شبکه‌های ارتباطی بوده‌ایم، که به کاربران اجازه اتصال در هر زمان و تقریبا در هر جایی را داده‌است، در نتیجه باعث افزایش تقاضای ترافیک شده‌است .گسترش دستگاه‌ها و کاربردهای هوشمند مختلف، و همچنین توسعه طیف وسیعی از فن‌آوری‌های شبکه، حجم بی‌سابقه‌ای از ترافیک داده‌ها را ایجاد می‌کند. علاوه بر این، افزایش تعداد اشیا متصل به اینترنت، اینترنت اشیا) (IoTرا به موضوعی رو به رشد در سال‌های

اخیر تبدیل کرده‌است و انتظار می‌رود که در سال‌های آینده به صورت نمایی افزایش یابد .

ضرورت تحقیق

برای دستیابی به توسعه امنIoT ، مهندسی راه‌حل‌های امنیتی مقیاس پذیر بهینه شده‌برای اکوسیستم IoT ضروری است .برای این منظور، شبکه سازی تعریف‌شده نرم‌افزار SDNیک الگوی امیدوار کننده است که به عنوان یک ستون در نسل پنجم سیستم‌های تلفن همراه5G عمل می‌کند که می‌تواند به شناسایی و کاهش انکار خدمات DoSو DDoSکمک کند. در این کار، ما یک راه‌حل مبتنی بر آنتروپی را به صورت تجربی برای شناسایی و کاهش حملات DoSو DDoS در سناریوهای IoT با استفاده از یک صفحه داده SDN وضعیت دار ارائه می‌دهیم. نتایج به‌دست‌آمده برای اولین بار اثربخشی این تکنیک را نشان می‌دهد که ترافیک داده‌های IoT واقعی را هدف قرار می‌دهد . برای دستیابی به موفقیتIoT ، توسعه مکانیزم‌های پیشرفته‌ای که قادر به تضمین سطوح امنیتی مناسب برای شناسایی حملات سایبری و کاهش تهدیدات سایبری در صورت رخداد در شبکه IoT مدیریت‌شده باشند، ضروری است.

این یک چالش بزرگ است زیرا دستگاه‌های IoT ممکن است اطلاعات حساس را مدیریت کنند و بسیاری از دستگاه‌های IoT تجاری کم‌هزینه معمولا از مکانیزم‌های امنیتی قوی پشتیبانی نمی‌کنند، و آن‌ها را به اهداف آسانی برای مطابقت با شبکه مخرب دستگاه‌ها برای حملات مختلف مانند DoSو DDoS تبدیل می‌کنند

شاخه حل جاری

NFVیک رویکرد شبکه در حال تحول است که امکان جایگزینی سخت‌افزار گران‌قیمت، اختصاصی و اختصاصی (مانند روترها، فایروال ها و غیره)با دستگاه‌های شبکه مبتنی بر نرم‌افزار، با جداسازی توابع شبکه از سخت‌افزار اصلی را فراهم می‌کند . NFVهمچنین اجازه می‌دهد که نمونه‌های توابع مجازی توسط چندین مشتری به اشتراک گذاشته شوند . NFV پیشنهاد می‌کند که توابع اجرا شده توسط گره‌های شبکه در یک مدل مجازی تعریف می‌شوند، به طوری که توابع خدمات شبکه را می توان در بلوک‌هایی که می‌توانند زنجیر شوند، طبقه‌بندی کرد NFV .پیشنهاد می‌کند که توابع اجرا شده توسط گره‌های شبکه در یک مدل مجازی تعریف می‌شوند، به طوری که توابع خدمات شبکه را می توان در بلوک‌هایی که می‌توانند زنجیر شوند، طبقه‌بندی کرد . هر یک از این بلوک‌ها نشان‌دهنده یک تابع شبکه مجازی vnfمی‌باشند. این توابع ویژگی‌های شبکه خاص، مانند رمزگذاری / رمزگشایی، VPN، تعادل بار، فایروال و غیره را فراهم می‌کنند. مجازی سازی خدمات توسعه‌های سریع‌تر، کاهش اپکس را فراهم می‌کند .(هزینه اختیاری)، مصرف انرژی و بهبود سازگاری با مدل‌های تجاری جدید. اگرچه SDN و NFV به موفقیت بزرگی دست یافته‌اند، تحقیقات اخیر در این تکنولوژی‌ها چالش‌های امنیتی بالقوه ای را آشکار می‌کند که باید برای اطمینان از امنیت مورد نیاز خدمات و زیرساخت‌های ۵ G جدید مورد توجه قرار گیرند. اگرچه SDN و NFV به موفقیت بزرگی دست یافته‌اند، تحقیقات اخیر در این تکنولوژی‌ها چالش‌های امنیتی بالقوه ای را آشکار می‌کند که باید برای اطمینان از امنیت مورد نیاز خدمات و زیرساخت‌های 5Gجدید مورد توجه قرار گیرند. به طور کلی، هدف اکثریت قریب به اتفاق حملات محدود کردن یا انکار خدمات از طریق افزایش تنوع حملات DoS و DDoS است. این مقاله یک راه‌حل امنیتی حالت دار

SDNبرای ترافیک IoT واقعی ارائه می‌دهد که می‌تواند حملات DoS و DDoS را براساس مفهوم آنتروپی به عنوان روش تشخیص شناسایی و کاهش دهد، که مزایای آن حساسیت بالا، نرخ مثبت نادرست کم برای تنظیم صحیح پارامترهای الگوریتم، محاسبه ساده آنتروپی و عدم نیاز به دستگاه شبکه اضافی است . ما سه سناریوی آزمایشی مختلف را طراحی کرده‌ایم که در آن حملات DoS و DDoS با استفاده از ترافیک داده واقعی از دو مجموعه داده به نام "بیگ فی" و "Bot - IoT" انجام می‌شوند . در سناریوی اول، ما ترافیک واقعی را از مسیر "بیگ فیو" گرفته‌ایم. دو سناریوی آزمایشی دیگر با استفاده از مجموعه داده Bot - IoT انجام شده‌اند Bot - IoT .به این دلیل انتخاب شده‌است که به تازگی طراحی شده‌است و ایجاد آن مبتنی بر یک مجموعه داده ساختار یافته برای تحلیل فارنزیک شبکه در IoT بود .

داشتن ظرفیت تشخیص و کاهش و همچنین آوردن پیچیدگی محاسباتی منطقی در معماری شبکه SDN برای یک راه‌حل آماری) (DoS Dحیاتی است .در این زمینه، مشارکت‌های کلیدی در کار ما را می توان به صورت زیر خلاصه کرد:

ما یک راه‌حل مبتنی بر آنتروپی را توسعه داده‌ایم که به درستی در معماری SDN وضعیت دار کار می‌کند . بهره‌برداری مشترک از راه‌حل آماری و الگوی SDN وضعیت دار امکان ارائه یک طرح جامع را فراهم می‌کند که حملات DoS و DDoS را شناسایی و کاهش می‌دهد .

استفاده از ترافیک IoT واقعی در سناریوهای آزمایشی .اکثر کاره‌ای موجود در ادبیات موضوع با ترافیک مصنوعی سر و کار دارند یا ترافیک شبکه IoT نیستند .همانطور که در مرجع [۲۰] گفته شد، یک مساله مهم برای هر طرح دفاعی مبتنی بر روش‌های

آماری، نیاز به کار با پروفایل های ترافیک خاص است .در این کار، ما آزمایش‌ها خود را با ترافیک IoT واقعی انجام داده‌ایم .

طراحی توپولوژی‌های پیچیده‌تر برای سناریوهای تجربی .کاره‌ای قبلی که با حملات DoSیا DDoS در شبکه‌های بدون حالت SDN سر و کار دارند، نتایج را با استفاده از سناریوهای ساده به دست می‌آورند .به منظور دستیابی به نتایج موثرتر، ما توپولوژی‌ها را با چندین کلید در معماری SDN طراحی کرده‌ایم .

State of the Art

در این بخش، ما شروع به توصیف معماریSDN ، و همچنین تهدیدهای امنیتی مختلفی که در این نوع معماری یافت می‌شوند، می‌کنیم و مشخص می‌کنیم که چه بخش‌هایی از معماری SDN ممکن است وجود داشته باشد . آسیب‌پذیر .سپس، کار مرتبط در مورد شناسایی حملات DoS و DDoS در شبکه‌های SDN نشان‌داده شده‌است .در نهایت، مفهوم آنتروپی برای نشان دادن چگونگی استفاده از این مکانیزم برای تشخیص تهدید امنیت شبکه توضیح داده می‌شود.

SDN

همانطور که در شکل ۱ نشان‌داده شده‌است، کنترلر SDN جز کلیدی صفحه کنترل است، به عنوان "مغز" شبکه و واسط‌ها را به دیگر صفحات ارائه می‌دهد .تعامل با صفحه برنامه از طریق رابط شمالی ایجاد می‌شود، مجموعه‌ای از API های باز (رابط برنامه‌نویسی برنامه)که فرآیند ایجاد برنامه‌های شبکه را ساده می‌کند .تعامل با صفحه داده از طریق رابط از طریق جنوب است که ارتباط بین کنترلر SDN و سوییچ‌ها را ممکن می‌سازد .رایج‌ترین پروتکل مورد استفاده در رابط از طریق جنوب، OpenFlowاست، یک پروتکل مهم در دامنهSDN ، که توسط بنیاد شبکه باز نگهداری می‌شود و توسط تمام فروشندگان تجهیزات شبکه بزرگ پشتیبانی می‌شود .

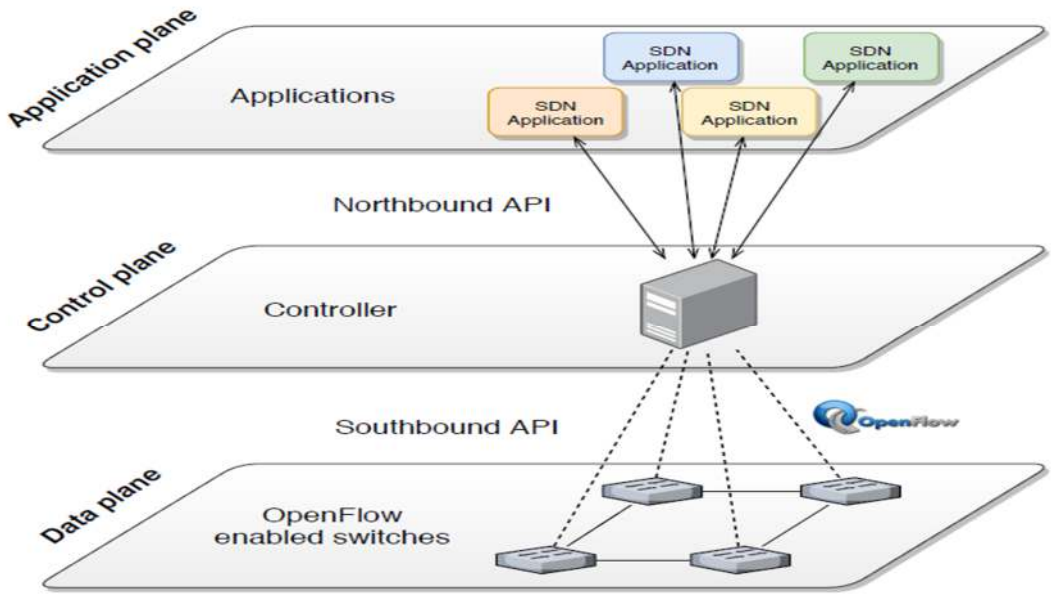


Figure 1. Software Defined Network (SDN) architecture.

اخیرا، یک رویکرد جدید به نام SDN حالت دار، عملکردهای اصلی OpenFlow را گسترش داده و شامل قابلیت‌هایی برای اعمال قوانین مختلف عملیات تطابق براساس حالت‌های مختلف یافت‌شده در جداول جریان SDN سوئیچ می‌باشد .با این عملکرد، سوئیچ توانایی واکنش به رویداده‌ای سطح بسته را پیاده‌سازی می‌کند و کنترلر و صفحه

کنترل را آزاد می‌کند تا توابعی را ایجاد کند که در حال حاضر توسط آن ساخته شده‌اند .اگر نتیجه تحلیل با قوانینی که سوئیچ در جداول جریان دارد مطابقت داشته باشد، می‌تواند مطابق با قانون عمل کند .

SDNهمچنین گسترش خدمات مبتنی بر فن‌آوری‌های جدید مانند IoT را به دلیل جدایی مدیریت و سطح ارسال تسهیل کرده‌است .توسعه کاربردها و خدمات جدید به این دلیل بهینه‌سازی شده‌است که کنترل شبکه به طور کامل توزیع شده‌است و اضافه کردن یک ویژگی جدید با استفاده از برنامه‌های جدید در کنترلر ساده‌سازی شده‌است.

Security Attacks in SDN Networks

معماری SDN توسط بسیاری از انواع اجزا شبکه کنترل‌کننده‌هایSDN ، برنامه‌های SDN، رابط‌های شمالی و جنوبی(ترکیب شده‌است، در حالی که شبکه‌های موروثی تنها توسط یک (دستگاه‌های شبکه)ترکیب شده‌اند .در حال حاضر، نه تنها باید از دستگاه‌های شبکه محافظت شود، بلکه باید از آن‌ها محافظت شود .

جدول ۱ حملات اصلی که در آن SDN آسیب‌پذیر در نظر گرفته می‌شود و ویژگی امنیتی مربوطه را شامل می‌شود را خلاصه می‌کند .

Attack Type	Security Property	SDN NE	SDN Controller	SDN Application
Spoofing	Authentication	vulnerable	vulnerable	vulnerable
Tampering	Integrity	vulnerable	vulnerable	vulnerable
Repudiation	Non-repudiation	-	vulnerable	-
Information disclosure	Confidentiality	vulnerable	vulnerable	vulnerable
Denial of service (DoS)	Availability	vulnerable	vulnerable	vulnerable
Distributed DoS (DDoS)	Availability	vulnerable	vulnerable	vulnerable
Elevation of privileges	Authorization	vulnerable	vulnerable	-

DoS and DDoS Detection Background

داس و DDoS دو مورد از سخت‌ترین حملاتی هستند که به دلیل درخواست اتصالات چندگانه برای یک دوره زمانی که هدف را وادار به کاهش، سقوط یا توقف می‌کند، باید کاهش داده شوند .در محیط‌هایIoT ، ممکن است حتی باعث کاهش حافظه بلند مدت گره‌های رله به دلیل منابع محدود آن‌ها شود. با ظهور SDN و توانایی آن برای توسعه برنامه‌های کاربردی که می‌تواند برای شناسایی و کاهش DoS به راحتی نسبت به استفاده از سخت‌افزار سنتی استفاده شود، مکانیزم‌های مختلفی برای بهبود امنیت شبکه‌ها توسعه داده شده‌اند. نوع اول مکانیسم‌ها مبتنی بر دفاع آماری / سیاسی هستند .این دفاع شامل جمع‌آوری و تحلیل نمونه‌های داده شبکه برای شناسایی ترافیک مخرب است .الگوریتم‌های آماری مختلفی با استفاده از اندازه‌گیری‌های مختلف مانند انحراف معیار، تحلیل همبستگی تطبیقی، آنتروپی یا محاسبه آمار مربع کای نمونه به منظور طبقه‌بندی جریان به عنوان یک حمله یا یک حمله قانونی توسعه داده شده‌اند .دفاع براساس سیاست نصب‌شده در سوئیچ است، که جریان‌های مجاز به ارسال را تعریف می‌کند و جریان‌های دیگر به عنوان مخرب تعریف می‌شوند.

Entropy-Based Detection

همانطور که قبلا گفته شد، تشخیص DoS می‌تواند بر مکانیزم‌های آماری تکیه کند . برخی از معیارهای مبتنی بر نظریه اطلاعات به طور خاص در تشخیص حملات داس

)(Dمحبوب هستند .در نظریه اطلاعات، آنتروپی شانون معیاری از عدم قطعیت مرتبط با یک متغیر تصادفی است و به عنوان یکی از موثرترین روش‌ها برای تشخیص ترافیک غیر عادی در نظر گرفته می‌شود. با توجه به اینکه) (Dحملات DoS باعث تغییرات قابل‌توجهی در توزیع ترافیک شبکه می‌شوند، پارامتر آنتروپی می‌تواند چنین تغییراتی را ثبت کند و یک هشدار در مورد رفتار ترافیک ایجاد کند . به عبارت دیگر، تجزیه و تحلیل الگوی یک حمله) DoS (D، زمانی که بیرون می‌آید، بسته‌های داده جعلی که یک هدف را تهدید می‌کنند، معمولا با آدرس‌های IP منبع مختلف ایجاد و به طور تصادفی توزیع می‌شوند .بنابراین، پس از محاسبه آنتروپی یک پارامتر مانند آدرس IP منبع در یک سری از بسته‌های پیوسته، مقدار بالای آنتروپی به این معنی است که پارامتر تصادفی است .در مقابل، مقدار کوچک‌تر آنتروپی نشان‌دهنده وقوع بالای آماری برای ظهور IP منبع است . بنابراین، پس از محاسبه آنتروپی یک پارامتر مانند آدرس IPمنبع در یک سری از بسته‌های پیوسته، مقدار بالای آنتروپی به این معنی است که پارامتر تصادفی است .در مقابل، مقدار کوچک‌تر آنتروپی نشان‌دهنده وقوع بالای آماری برای ظهور IP منبع است .اگرچه آنتروپی مقداری است که بین یک فاصله نسبتا کوتاه نوسان می‌کند، تغییر قابل‌توجه در تصادفی بودن پارامترهای ترافیک متوالی باعث تغییر زیاد در مقادیر آنتروپی می‌شود، که این مقدار آماری را به یک پارامتر مرتبط برای تشخیص برخی از حملات تبدیل می‌کند . با توجه به تعریف رسمی آن، آنتروپی به صورت زیر فرمول‌بندی می‌شود .اجازه دهید یک منبع اطلاعاتی n نماد مستقل داشته باشد که هر کدام با احتمال انتخاب pi مشخص شده‌اند .سپس، آنتروپی H به صورت زیر تعریف می‌شود:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i.$$

بخش بعدی به تفصیل راه‌حل ایجاد شده در یک شبکه SDN برای شناسایی حملات داس‌از طریق یک مکانیزم مبتنی بر مفهوم آنتروپی را توصیف می‌کند .

Entropy-Based (D)DoS Attacks Detection and Mitigation in Stateful SDNs

کشف و کاهش حملات داس مبتنی بر آنتروپی در SDNs های حالت دار. در این بخش یک رویکرد جدید برای شناسایی و کاهش حملات DoS و DDoS براساس محاسبه آنتروپی توصیف می‌شود .برای توسعه مدلی که از شبکه در برابر حملات Dos محافظت می‌کند، سه مرحله وجود دارد که باید اجرا شود - نظارت ترافیک / جریان؛ تشخیص ناهنجاری

اکثر تحقیقات این مراحل را به روشی سنتی اجرا می‌کنند که در آن کلیدهای شبکه تنها بسته‌های رو به جلو را ارسال می‌کنند و تمام منطق کنترل در کنترلر اجرا می‌شود .این نشان می‌دهد که برای هر مهاجم، سوئیچ باید یک بسته به کنترلر ارسال کند تا بفهمد با اضافه کردن یک قانون جریان جدید چه اقدامی باید انجام دهد .علاوه بر این، اگر مکانیسم تشخیص مربوط به یک الگوریتم مبتنی بر آنتروپی باشد، همه بسته‌ها باید نظارت شوند . بنابراین راه‌حل‌های بدون وضعیت کارآمد یا مقیاس پذیر نیستند .

اخیرا، با ظهور OpenState ذکر شده، شبکه‌های SDN قادر به فراهم کردن سوییچ‌ها با قابلیت‌های پردازش بسته‌های مستقل هستند .یعنی، زمانی که یک بسته می‌رسد، تنها براساس مقادیر موجود در هدرهای آن پردازش نخواهد شد، بلکه در عوض سوئیچ بسته‌هایی را که قبلا دریافت کرده بودند نیز در نظر خواهد گرفت .بنابراین، این رویکرد اجازه می‌دهد تا نظارت و تشخیص جریان‌های مخرب به سوییچ‌ها محول شود .در این

کار، از پیاده‌سازیOpenstate ، با انجام یک نیمه نظارت با کنترل‌کننده استفاده شده‌است .با این رویکرد، سوییچ‌ها بر جریان‌ها نظارت می‌کنند اما تشخیص جریان‌های مخرب در کنترلر انجام می‌شود .

Monitoring

همان طور که قبلا ذکر شد، مرحله اول نظارت بر شبکه برای به دست آوردن اطلاعات در مورد شبکه و تغذیه الگوریتم تشخیص براساس الگوریتم محاسبه آنتروپی است .در این کار، اطلاعات تحلیل‌شده IP منبع / مقصد، پورت منبع / مقصد و اطلاعات در مورد پروتکل مورد استفاده) TCP، UDP، (ICMPهستند .درSDN ، روش‌های متعددی برای توسعه الگوریتم برای نظارت بر ترافیک شبکه وجود دارد OpenFlow .نظارت محلی را با استفاده از پیام‌های پیاده‌سازی شده که پیام‌های مورد استفاده در ارتباط بین کنترل‌کننده‌ها و ... را تعریف می‌کنند، ادغام می‌کند .این پایش تنها توسط سوئیچ انجام می‌شود، و اطلاعات را به صورت مستقل از کنترلر تحلیل می‌کند .برای انجام این کار، سوئیچ از جداول جریان و حالت خود استفاده می‌کند .این رویکرد به دست آوردن اطلاعات مورد نیاز برای شناسایی یک حمله داس را ممکن می‌سازد، زیرا سوئیچ می‌تواند تعداد دقیق رویدادها را برای یک مشخصه ترافیک تحت نظارت بشمارد، و دقت الگوریتم را افزایش دهد .

Detection

مرحله تشخیص با اجرای الگوریتم آنتروپی انجام می‌شود، که داده‌های به‌دست‌آمده در مرحله نظارت را تجزیه و تحلیل می‌کند و می‌تواند جریان‌های

مخرب را شناسایی کند .در مقایسه با سایر ابزارهای مبتنی بر الگوها . الگوریتم های آماری مانند محاسبه آنتروپی به مقدار زیادی حافظه یا ذخیره‌سازی نیاز ندارند .این امر این رویکردها را در یک راه‌حل مناسب برای گنجاندن آن‌ها در عناصر شبکه SDN تبدیل می‌کند .

در معادله (۲)، محاسبه آنتروپی برای سیستم تشخیص نشان‌داده شده‌است، که براساس معادله (۱)است، که در آن p(XI) احتمال رخداد xi را نشان می‌دهد، و n تعداد رویدادها را نشان می‌دهد .

یک توزیع متمرکز بالا نشان‌دهنده مقدار آنتروپی پایین است .در مقابل، یک توزیع متمرکز پایین نشان‌دهنده مقدار آنتروپی بالاتر است، که رفتاری است که انتظار می‌رود حملات در شبکه‌ها را شناسایی کند [۳۳، ۳۴] .برای تجزیه و تحلیل ترافیک، یک فاز یادگیری اولیه برای تغذیه الگوریتم، محاسبه آنتروپی و محدودیت‌های توزیع، تعریف‌شده توسط معادله (۳)مورد نیاز است . برای تشخیص حملات، این فرآیند در فواصل منظم تکرار می‌شود و آنتروپی هر مشخصه را تحلیل می‌کند IPمنبع / مقصد، پورت منبع / مقص(.اگر محاسبه آنتروپی بیش از حد یا تحت محدودیت‌های تعریف‌شده باشد، حمله تشخیص داده می‌شود .این محدودیت‌ها به صورت زیر محاسبه می‌شوند:

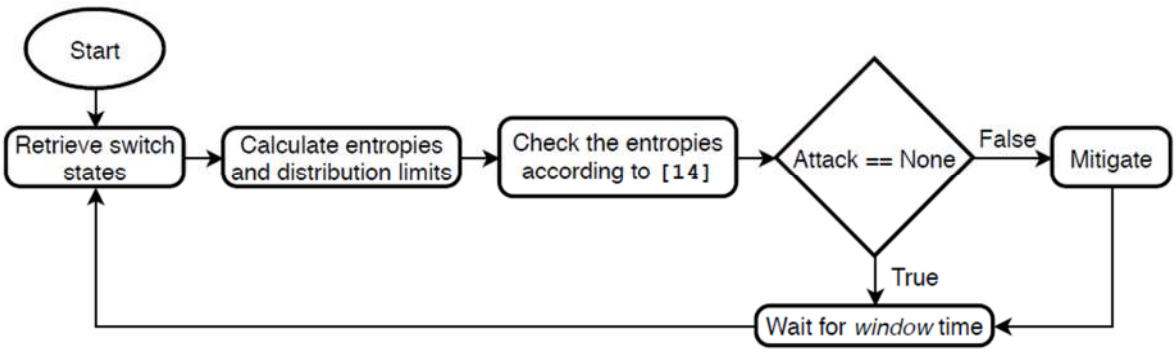
$$limits = \mu \pm \theta\sigma,$$

که m میانگین معیارهای آنتروپی قبلی، qدسته و s انحراف معیار است .این محدودیت‌ها به ما این اطمینان را می‌دهد که یک تهدید مطابق با جدول ۲ در حال وقوع است .

θ	Certainty
1	68%
2	95%
3	99.7%

Mitigation

در نهایت، زمانی که یک حمله مخرب شناسایی می‌شود، مکانیزم کاهش از کاربران نهایی محافظت می‌کند .برای کاهش حمله، قوانین جریان جدیدی به سوییچ‌های با اولویت بالا اضافه می‌شوند تا این قانون را با بسته مشکوک مطابقت دهند .دقت قوانین کاهش بستگی به میزان اطلاعات حمله دارد . کنترلر قوانین موجود در سوییچ‌ها را با استفاده از پیام‌های استاندارد OpenFlowو ارسال پیغام‌های FlowMod پیکربندی می‌کند .مکانیزم‌های مختلفی برای کاهش حمله وجود دارد مانند سیاه‌چاله‌ها، سیستم تشخیص نفوذ ، حتی تکنیک‌های پیشرفته مانند بازرسی بسته عمیق در این کار، الگوریتم کاهش اجرا می‌شود، قوانین مختلف را در سوئیچ پیکربندی می‌کند، که بسته‌های مشکوک را رها می‌کند . در شکل ۲، نمودار جریان الگوریتم مبتنی بر آنتروپی نشان‌داده شده‌است .

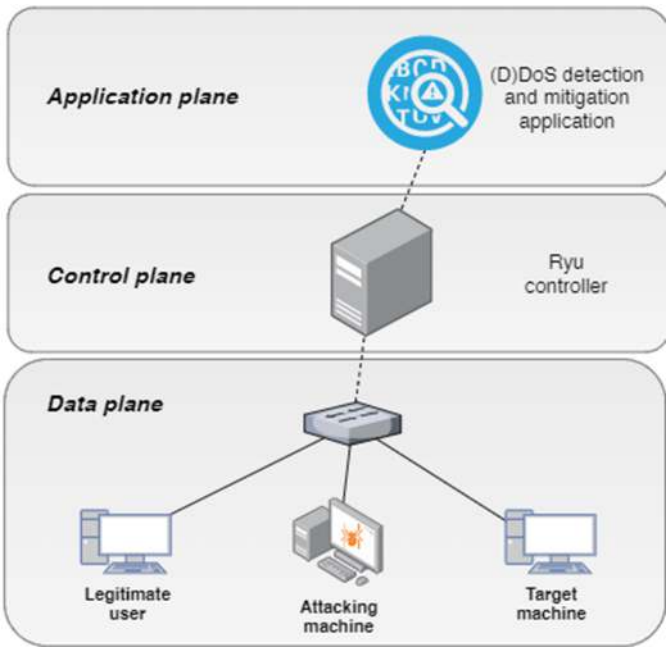


Experimental Evaluation in the Detection and Mitigation of (D)DoS Attacks

ارزیابی تجربی در تشخیص و کاهش حملات داس. در این بخش، سناریوی تجربی مورد استفاده برای استخراج نتایج به‌دست‌آمده را شرح می‌دهیم . بس‌تر آزمایشی براساس شبیه‌ساز مشهور SDN مبتنی بر مینت است.

DoS Attacks Base Scenario

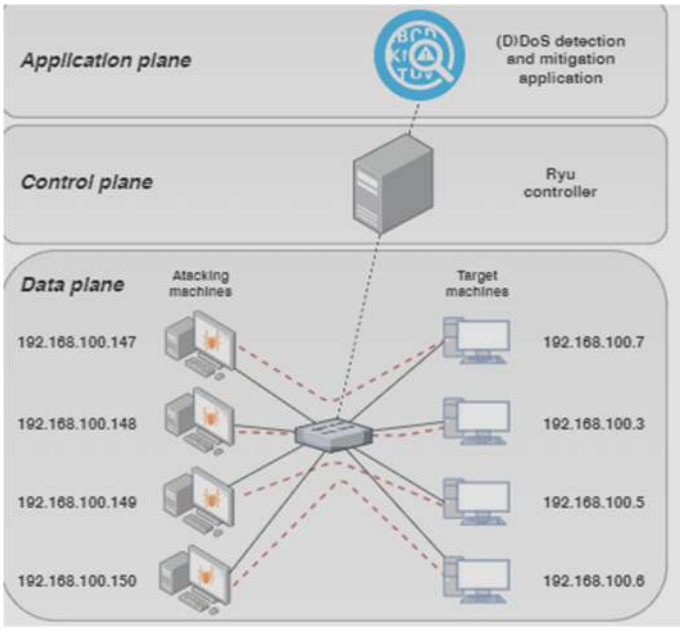
در این راه‌اندازی آزمایشی، ما یک توپولوژی شبکه مانند توپولوژی ارائه‌شده در شکل ۳ را در نظر گرفته‌ایم. میزبان‌ها به صورت Host۱تا ۳ Hostبرچسب گذاری می‌شوند و سوئیچ شبکه به صورت ۱ Sبرچسب گذاری می‌شود .در این شبکه، دو میزبان) ۱ Hو ۳Hگره‌های منظمی هستند که ترافیک نرمال را ارسال و دریافت می‌کنند در حالی که ۲ Hمهاجمی است که حمله DoS را در برابر میزبان ۳ Hانجام خواهد داد .در این محیط، تست‌های زیر انجام می‌شوند .



DoS Attack in an IoT Scenario

توپولوژی مورد استفاده در این مورد در شکل ۶ نشان‌داده شده‌است و از توپولوژی Bot - IoT مورد استفاده برای به دست آوردن مجموعه داده ترافیک اقتباس شده‌است .

در این مجموعه داده، هر دو ترافیک قانونی و مخرب ترکیب می‌شوند، که این مجموعه داده را برای هدف این کار مناسب می‌سازد، زیرا نتایج ممکن است برای دیگر سناریوهای IoT مفید باشند . در شکل ۶، دستگاه‌های شبیه‌سازی شده IoT در ماشین‌های هدف واقع شده‌اند، در حالی که میزبان‌های حمله، انجام حملات DoS VM های کالی هستند.



ارزیابی و بررسی

در این مقاله ما تشخیص و کاهش حملات DoS و DDoS مبتنی بر تکنیک SDN را مورد بحث بررسی قرار دادیم همچنین مکانیزم های پیشرفته ای را برای شناسایی حملات سایبری مورد بحث و بررسی قرار دادیم.

جمع بندی

در این مقاله، ما یک راه‌حل SDN وضعیت دار را توصیف می‌کنیم که قادر به شناسایی و کاهش حملات DoS و DDoS در شبکه‌های IoT است .براساس این تحقیق، ما یک برنامه اثبات مفهوم را در بالای کنترلر ریو SDN توسعه داده‌ایم که حملات DoS و DDoS را با توجه به مقادیر آنتروپی شناسایی می‌کند .مورد اول یک بس‌تر آزمون عمومی است که در آن مقادیر پهنای باند

و آنتروپی در طول حمله اندازه‌گیری می‌شوند، در حالی که مورد دوم و سوم بر یک سناریوی IoT تمرکز می‌کنند .در آینده، این کار برای تعمیم انواع دیگر حملات داس و همچنین برای در نظر گرفتن معیارهای آماری مختلف که می‌توانند در فرآیند تشخیص کمک کنند، گسترش خواهد یافت.

به همین دلیل است که یک مطالعه جامع انجام خواهد شد تا بررسی شود که آیا مشکل مربوط به ساختار سوئیچ یا برنامه SDN است یا خیر .این امر به فرآیند تشخیص انعطاف‌پذیری می‌دهد و در راستای دیگر ستون‌های فن‌آوری 5G مانند NFV خواهد بود .

کارهار آینده