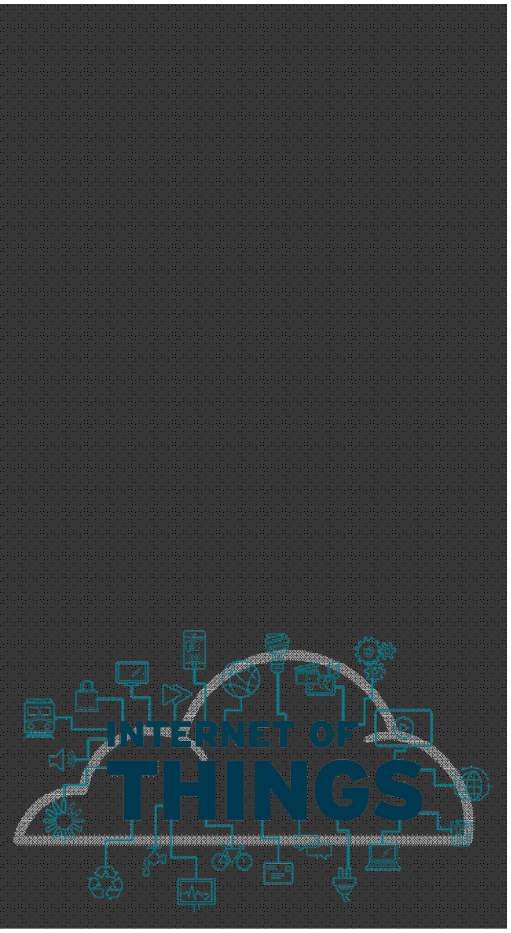


Near real-time security system applied to SDN environments in IoT networks using convolutional neural network

محمد سعید انصاری

دانشجوی دکتری معماری کامپیوتر

استاد گرامی: خانم دکتر جاسبی

تعریف مسئله

- اینترنت اشیا یک فناوری در حال تکامل است که در آن هر دستگاهی از طریق شبکه می‌تواند متصل شود و از طریق یک ایستگاه از راه دور کنترل شود.
- اصلی‌ترین مشکل در اینترنت اشیا، ویژگی ناهمگنی آن است، چون هر سامانه‌ای برای کاربرد بهینه نیازمندی‌های متفاوتی در شبکه دارد.
- بنابراین شبکه‌های سنتی برای تامین نیازهای جدید اینترنت اشیا، نا کارآمد هستند.
- الگوی جدیدی که هدف آن مقیاس‌پذیری و انعطاف‌پذیری در مدیریت شبکه است، شبکه‌های نرم‌افزارمحور (SDN) است.

تعریف مسئله

- SDN با تبدیل اجزای شبکه سنتی "Black-box" به مولفه‌های کنترل شده نرم افزاری "White-box" ، امکان مدیریت متمرکز شبکه و پیکربندی و بهینه‌سازی کارآمد را فراهم می‌کند.
- این انتزاع با جدا کردن صفحه کنترل (control plane) و داده (data plane) امکان پذیر است.
- کمبود امنیت در اینترنت اشیا، باعث حملات بزرگ DDoS از طریق botnetها شده است.
- روش‌های سنتی مقابله با این حملات به دلیل حجم بالای حملات، امروز کاربرد خود را از دست داده‌اند.
- این حملات محیط SDN را به دلیل یک کنترلر مرکزی می‌توانند مختل کنند.

تعریف مسئله

- در این مقاله، یک سیستم امنیتی تقریبا بلادرنگ در محیط‌های SDN برای کاهش حملات DDoS ناشی از تجهیزات داخلی مانند botnetها، ارائه شده است.
- سیستم پیشنهادی کنترلر مرکزی SDN را در مقابل flooding محافظت کرده و از خروج حملات از شبکه مبدا جلوگیری می‌کند که باعث محافظت غیر مستقیم سرور قربانی می‌شود. این سیستم به دو بخش تقسیم می‌شود:
  - ماژول تشخیص: مسئول تشخیص و شناسایی حملاتی که رخ می‌دهند، است. در این ماژول از یک روش یادگیری عمیق با استفاده از تجزیه و تحلیل جریان IP چند بعدی، به نام Convolutional Neural Network (CNN) استفاده شده است.
  - ماژول کاهش: مسئول انتخاب سیاست‌های drop برای ایمن‌سازی کنترلر SDN، است.

مطالعات پیشین

- حمله DDoS از مسائل مهم در امنیت شبکه است که برای سازمان‌ها و افراد هزینه‌های زیاد زمانی، اعتباری و مالی، دارد. در مطالعات پیشین جهت کاهش این حملات، راه‌حل‌های متفاوتی ارائه شده است:
  - از Artificial Neural Network (ANN)، برای شناسایی حملات DDoS
  - از طریق الگوریتم دسته‌بندی Multi-layered Perceptron (MLP) برای حملات DDoS لایه Application

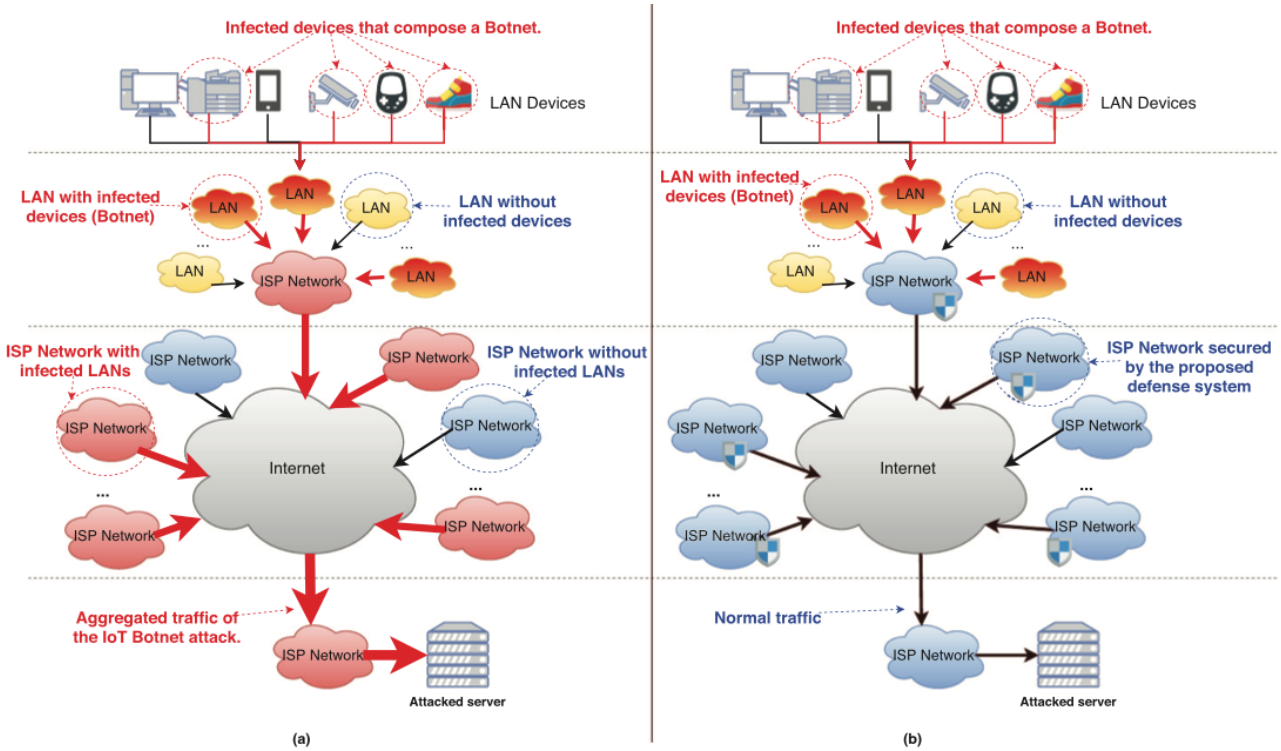
مطالعات پیشین

- داده‌های خام جریان IP، به صورت تصویر نشان داده شده و با استفاده از Convolutional Neural Network (CNN)، ترافیک مخرب دسته‌بندی و شناسایی می‌شود.
- دو رویکرد دسته‌بندی Payload بر اساس
  - Convolutional Neural Network (CNN)
  - و Recurrent Neural Network (RNN)

راه‌کار پیشنهادی

- روش پیشنهادی این مقاله با استفاده از کنترلر مرکزی SDN، حملات DDoS را کاهش می‌دهد. در این روش با جلوگیری از حملات به اهداف خارجی، حملات DDoS روی اینترنت کاهش پیدا می‌کند. رویکرد این روش، تقسیم و غلبه است که با جلوگیری از حملات از مبدا در ISPها، شکل می‌گیرد.

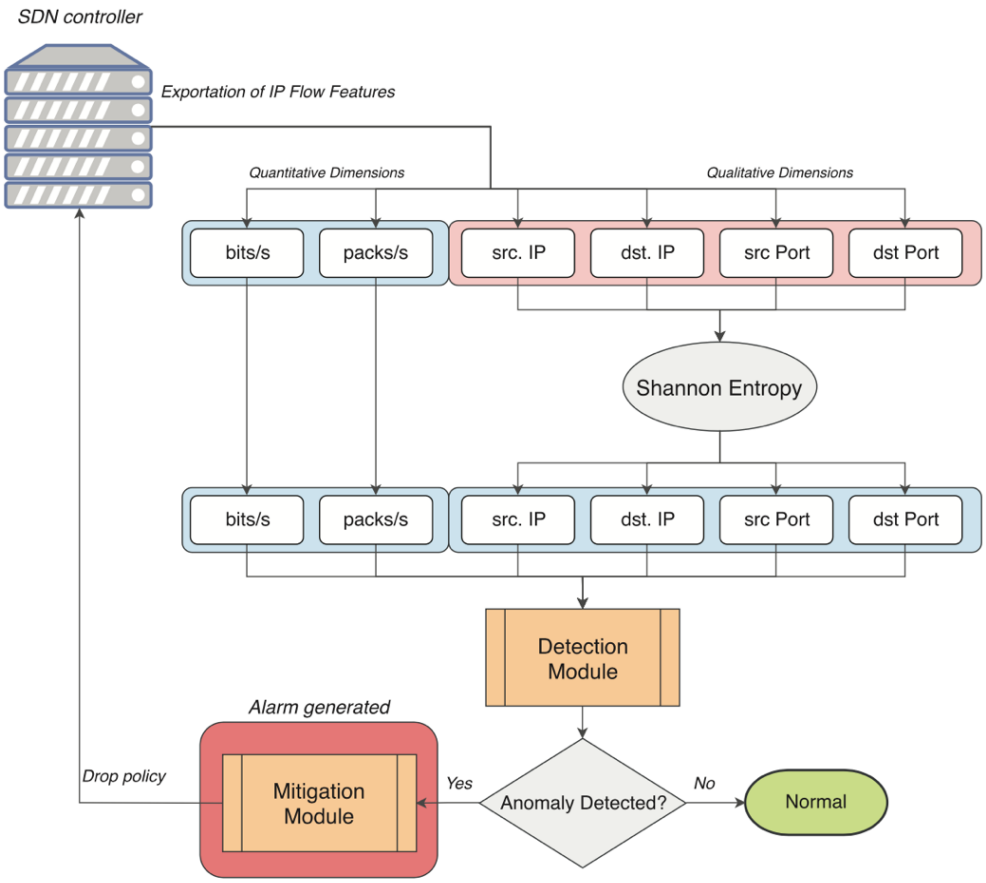
راه‌کار پیشنهادی



راه‌کار پیشنهادی

- سیستم پیشنهادی مبتنی بر تجزیه و تحلیل ابعاد جریان IP، با استفاده از ویژگی‌های مجزا برای شناسایی الگویی مربوط به عملکرد طبیعی شبکه و تشخیص وجود حملات DDoS است.
- برای کاهش تاثیر حملات DDoS بر روی کاربران قانونی، سیستم پیشنهادی با استخراج و تحلیل داده‌های جریان IP در فواصل یک ثانیه به صورت تقریبا بلادرنگ کار می‌کند. این تجزیه و تحلیل در فاصله زمانی، شناسایی و کاهش سریع حملات، کاهش آسیب به کنترل کننده SDN (و در نتیجه کاربران آن) و سرور مورد حمله خارجی را ممکن می‌کند.
- جهت تشخیص و کاهش سریع حملات، سیستم به صورت خودکار عمل می‌کند. حتی اگر به مدیر سیستم اعلانی هم داشته باشد ولی برای ادامه کار به تعامل انسانی نیاز ندارد.

راه‌کار پیشنهادی



راه‌کار پیشنهادی

- ماژول Detection Module در بخش Training با استفاده از CNN و داده‌های پیشین کالیبره شده و حملات توسط Anomaly Detection کشف می‌شوند.
- ماژول Mitigation Module پس از کشف حمله، با تصمیم‌سازی، باعث کاهش حملات می‌شود که روش ابتکاری آن خارج از محدوده این مقاله است.
- Mitigation Module دارای دو زیر ماژول است.
  - زیر ماژول اول با رویکرد Game Theory و به صورت بهینه، قوانین لازم را محاسبه می‌کند که روی مسیریاب مرزی SDN اعمال می‌شوند. ممکن است حملات مستقیما عملکرد SDN را مورد هدف قرار ندهند ولی ترافیک عبوری از کنترلر مرکزی می‌تواند آن را مختل کند. خروجی این زیر ماژول، نرخ بهینه افتادن بسته است.
  - نهایتا، زیر ماژول دوم، سیاست‌های ایجاد شده توسط زیر ماژول اول را به کنترلر مرکزی SDN برای اجرا، ارسال می‌کند.

ارزیابی راه‌کار پیشنهادی

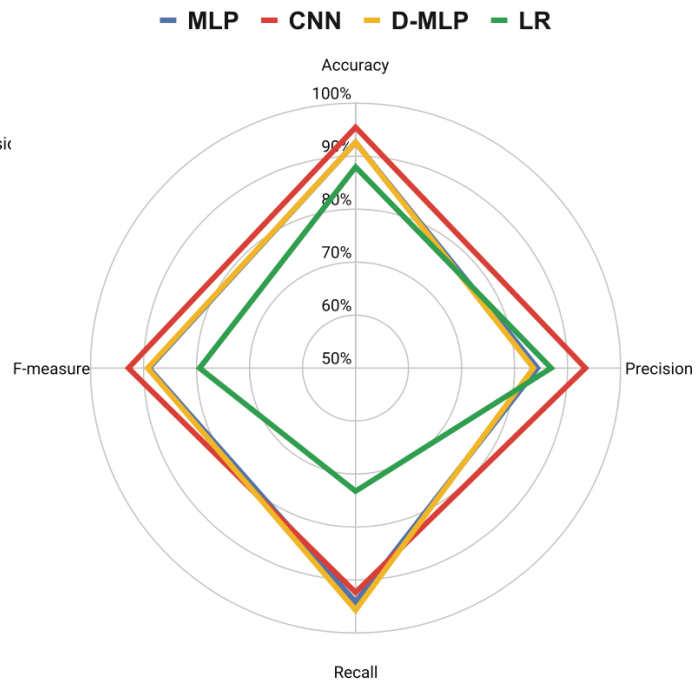
- سناریو اول، داده شبیه‌سازی شده SDN
  - با استفاده از Mininet، جریان‌های IP ایجاد شده، مورد آزمایش قرار گرفتند.
- سناریو دوم، مجموعه داده CICDDoS 2019

Summary of training (Day 1) and test days (Days 2 to 7) on the first scenario.

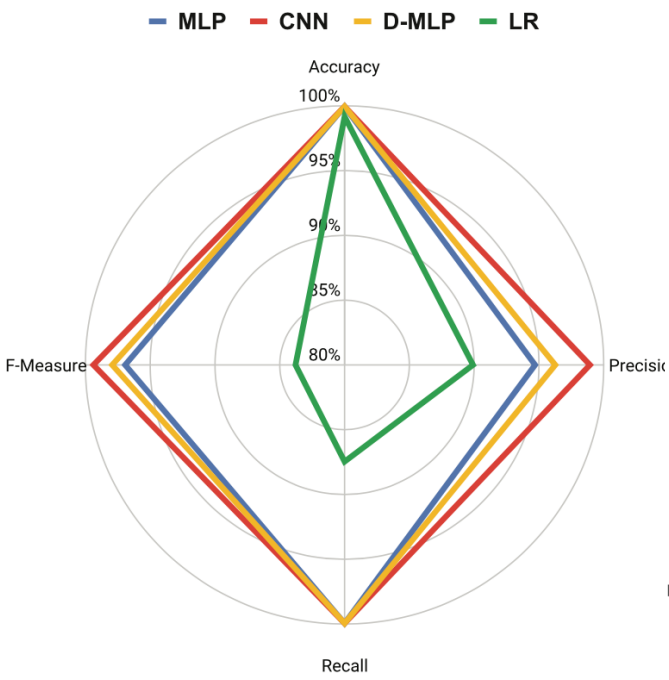
Day 4	Day 5	Day 6	Day 7			
Switches	6	6	6	6	6	6	6
Hosts	120	200	200	150	150	150	150
# of DDoS attacks	2	1	1	1	1	1	1 (short)
# of attacking hosts	15	20	20	15	20	10	10

ارزیابی راه‌کار پیشنهادی

- سناریو دوم



- سناریو اول



جمع‌بندی و کارهای آتی

- در این مقاله
  - روشی جهت تشخیص و کاهش حملات DDoS در SDN پیشنهاد شد.
  - این روش رفتار ترافیکی SDN را در فواصل زمانی یک ثانیه بررسی می‌کند و به طور موثر وقوع حملات به کنترلر SDN و در نتیجه حملات به سرور خارجی را شناسایی و کاهش می‌دهد.
  - طی دو سناریو در مقایسه با دیگر روش‌ها (MPL، D-MLP و LR)، برتری و کارایی این روش به نمایش درآمد.
  - هم‌چنین کارایی ماژول Mitigation بر اساس GT، نمایان شد.
- کارهای آتی:
  - افزایش تعداد میزبان‌ها جهت افزایش حجم حملات خصوصا حملات داخلی پنهانکارانه DDoS
  - بررسی دیگر روش‌های Deep learning و مقایسه با روش پیشنهادی
  - افزایش ویژگی‌ها به لیست ویژگی‌های مورد بررسی در شبکه

مرجع

- de Assis, Marcos VO, Luiz F. Carvalho, Joel JPC Rodrigues, Jaime Lloret, and Mario L. Proença Jr, "Near real-time security system applied to SDN environments in IoT networks using convolutional neural network", Computers & Electrical Engineering 86, pp.106738, 2020

با تشکر از توجه شما