بسمه‌تعالی

گزارش و تحلیل مقاله

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

تعریف مسئله و هدف اصلی مقاله

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. به طور مثال در:

- برنامه وسایل نقلیه هوشمند: تبادل اطلاعات با تاخیر نزدیک به صفر
- شبکه‌های صنعتی: هم تاخیر و هم صفر بودن داده از دست رفته
- سیستم نظارت تصویری: تاخیر و از دست رفتن داده مهم نیست ولی پهنای باند بیشتر می‌خواهند

این نیازهای خاص شبکه با مدل شبکه‌های سنتی که دارای محدودیت‌هایی در زمینه:

- مقیاس‌پذیری
- جابه‌جایی
- میزان ترافیک

هستند، سازگار نیست. 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.

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. تمام عملکردهای کنترلی در یک کنترل‌کننده مرکزی قابل برنامه‌ریزی، اجرا می‌شوند. این کنترل‌کننده، به نوبه خود، سیاست‌های انتقال و مدیریت بسته را به سوییچ‌ها و مسیریاب‌های کنترل‌شده توسط SDN می فرستد و به طور پویا عملکرد آن‌ها و در نتیجه، رفتار شبکه را هماهنگ می‌کند. این ویژگی‌ها SDN را به مکانی امیدوار کننده برای توسعه و بهره برداری از راه‌کارهای اینترنت اشیا تبدیل می‌کند.

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. البته ISPها با استقرار سیستم‌های جلوگیری از DDOS و حمله به کنترلر SDN، شبکه را از این نوع حملات حفظ می‌کنند.

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. این روش به طور گسترده‌ای روی مشکلات شناسایی/طبقه‌بندی تصویر اعمال می‌شود و توانایی یادگیری الگوهای محلی را در مجموعه داده به سیستم می‌دهد.
- ماژول کاهش[1]: 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:

- با استفاده از Artificial Neural Network (ANN)، برای شناسایی حملات DDoS، ترافیک به دو دسته غیرعادی و واقعی تقسیم می‌شود. این الگوریتم با داده‌ها قدیمی و به روز آموزش دیده و با درصد بالایی موفق به شناخت حملات شناخته‌شده و ناشناخته می‌شود. این روش برپایه الگوی خاصی از پورت و آدرس مبدا و مقصد است. این روش در صورت رمزگذاری شدن هدر بسته‌ها، ناکارآمد است.
- از طریق الگوریتم دسته‌بندی Multi-layered Perceptron (MLP) حملات DDoS لایه Application کشف می‌شوند. الگوریتم معرفی شده از الگوریتم ژنتیک (Genetic Algorithm)، به عنوان الگوریتم یادگیری استفاده می‌کند. یافته‌ها در این روش نشان می‌دهد که ویژگی‌های مهم برای شناسایی حملات شامل درخواست‌های HTTP GET برای یک آدرس در فرجه زمانی ۲۰ ثانیه‌ای، آنتروپی درخواست‌ها و واریانس آنتروپی است. نتایج آزمایش این روش حاکی از دقت و حساسیت بالا MLP است.
- داده‌های خام جریان IP، به صورت تصویر نشان داده شده و با استفاده از Convolutional Neural Network (CNN)، ترافیک مخرب دسته‌بندی و شناسایی می‌شود. این روش به نتایج خوبی در کشف وقایع مخرب دست پیدا کرده است. با یادگیری بر اساس جریان‌های خام داده، این روش ممکن است آدرس‌های IP مربوط به رفتار مخرب را کشف کند.

[1] Mitigation

- دو رویکرد دسته‌بندی Payload بر اساس Convolutional Neural Network (CNN) و Recurrent Neural Network (RNN) پیشنهاد شده است. این رویکردها برای تشخیص حمله استفاده می‌شوند و توانایی یادگیری نمایش ویژگی بدون مهندسی ویژگی از داده‌های اصلی را دارند. این روش در مقایسه با دیگر روش‌ها، به دقت بیشتر از ۹۹ درصد در آزمایشات بر مجموعه داده‌های DARPA1998 دست می‌یابد.
- سامانه‌ای بر پایه SDN برای کشف و کاهش حملات DDoS در محیط رایانش ابری به نام DaMask ارائه شده است. این سامانه به دو ماژول تقسیم می‌شود. ماژول اول وظیفه تشخیص حمله و تجزیه و تحلیل آماری و ماژول دوم وظیفه هدف قرار دادن محیط پویای شبکه، انجام اقدامات متقابل و تولید گزارش‌های مربوط به حملات را بر عهده دارند.
- یک دفاع سه لایه برای توپولوژی SDN، ارائه شده است. این روش دو ایراد دارد. اولا، فرض بر این است که شبکه باید عاری از ناهجاری‌های داخلی باشد و اگر حملات داخلی باشند کنترلر تحت فشار قرار می‌گیرد. دوما، تقسیم ترافیک بین پردازنده‌های مختلف می‌تواند منجر به تقسیم حمله بین آن‌ها شود و مانع جست‌وجوی ناهنجاری شود زیرا که این تقسیم‌بندی ممکن است به طور تصادفی حمله را مخفی کند.
- در چند مطالعه بر پایه روش push-back از حملات جلوگیری می‌شود. پس از شناسایی حمله، استراتژی push-back ترافیک حمله را از بین می‌برد و به دیگر تجهیزات انتقال، اطلاع می‌دهد.
- فقدان منابع محاسباتی کافی در سمت قربانیان حمله و حجم زیاد ترافیک شبکه ایجاد شده توسط حمله DDoS راه‌حل‌های امنیتی را آسیب‌پذیر می‌کند. برای غلبه بر این موضوع یک سیستم دفاعی توزیع‌شده در سطح ISP، برای تقسیم پیچیدگی محاسبات بین مسیریاب‌های نزدیک (PoP) ارائه شده است. ترافیک در تمام نقاط ورودی ISP کنترل شده و برای هماهنگ کننده مرکزی در شبکه قربانی ارسال می‌شود.

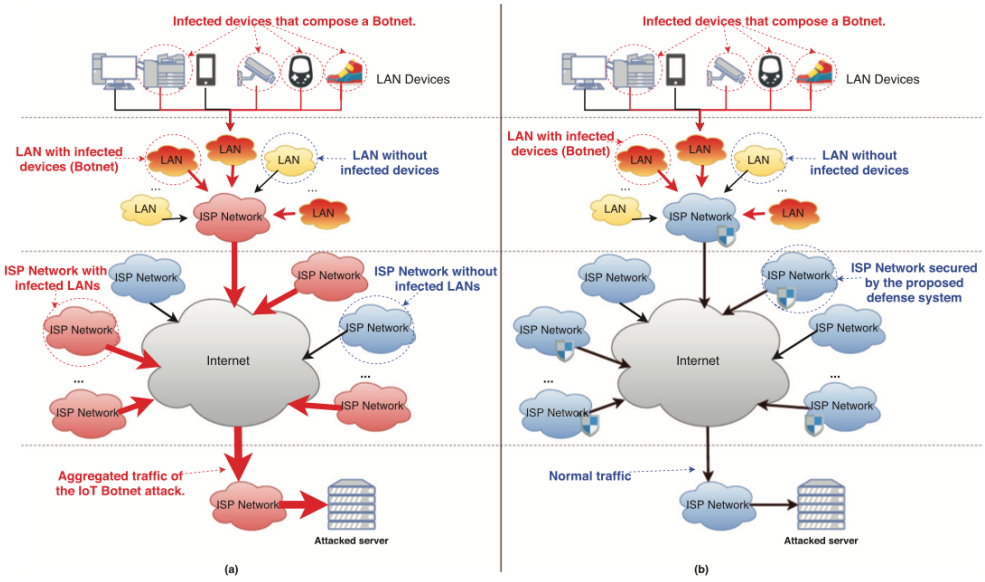
راه‌حل پیشنهادی مقاله برای مسئله

سامانه امنیتی 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 (تصویر- ۱).

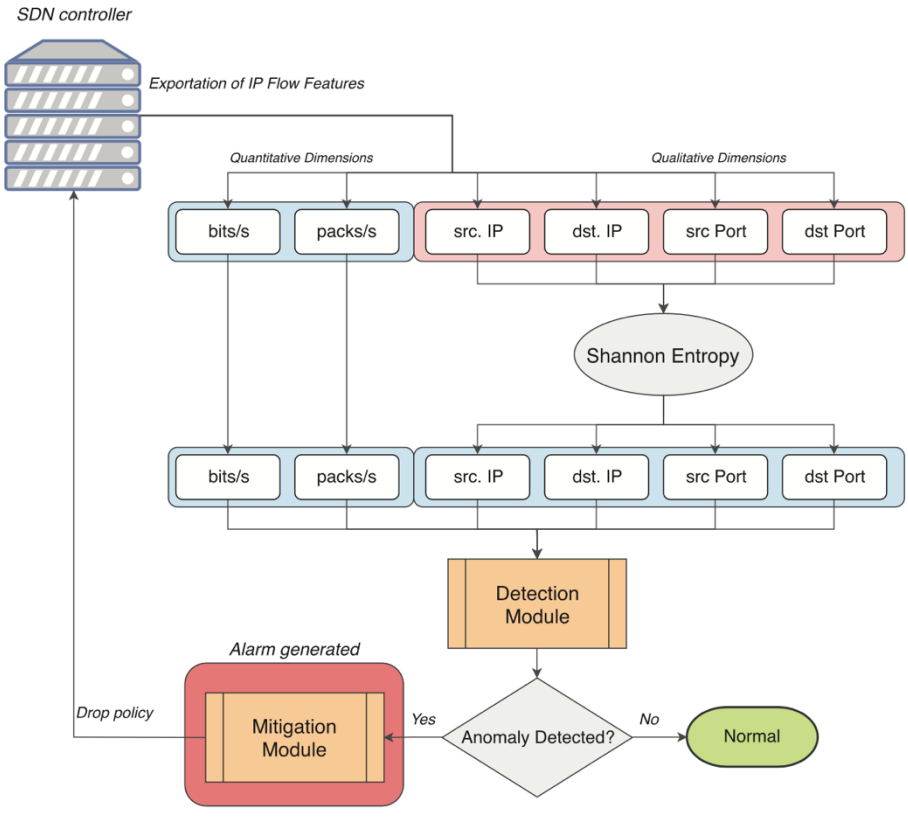
سیستم پیشنهادی مبتنی بر تجزیه و تحلیل ابعاد جریان IP، با استفاده از ویژگی‌های مجزا برای شناسایی الگوی مربوط به عملکرد طبیعی شبکه و تشخیص وجود حملات DDoS است. برای کاهش تاثیر حملات DDoS بر روی کاربران قانونی، سیستم پیشنهادی با استخراج و تحلیل داده‌های جریان IP در فواصل یک ثانیه

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.



تصویر- ۱

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. نمودار جریان عملکرد سیستم پیشنهادی در تصویر- ۲ شرح داده شده است.



تصویر- ۲

بر اساس تصویر- ۲، هر ثانیه ابعاد یا ویژگی‌های جریان IP از کنترلر SDN با پروتکل OpenFlow صادر می‌شود. این ابعاد داده‌های ناهمگنی هستند که می‌توانند به صورت کمی (مانند نرخ بسته‌ها و بیت در ثانیه) و کیفی (مانند پورت‌های مبدا/مقصد و آدرس‌های IP) طبقه‌بندی شوند. جهت ارسال ابعاد به Detection Module، ابعاد کیفی با استفاده از آنتروپی شانون، به صورت کمی تبدیل می‌شوند. برای بعد مورد نظر X={x1,x2,...,xn} که xi فرکانس وقوع نمونه i در بازه زمانی مشخص است، آنتروپی شانون H به این صورت محاسبه می‌شود:

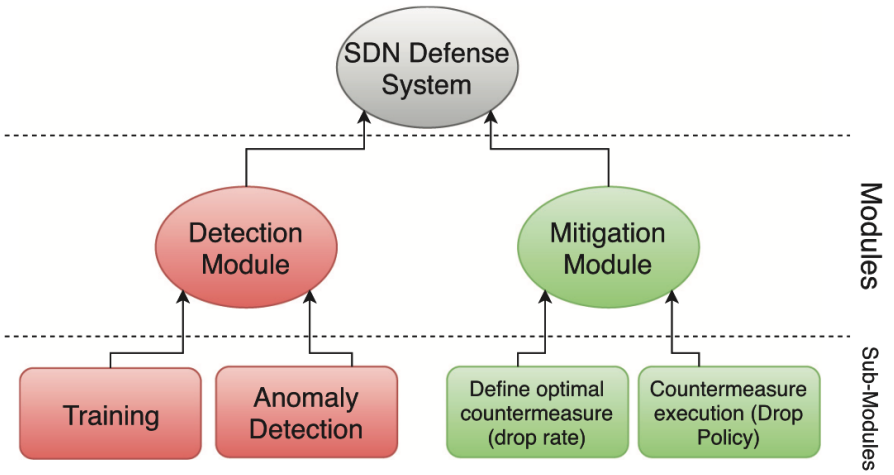
$$H(X) = -\sum_{i=1}^{N} (\frac{x_i}{S}) \log_2 (\frac{x_i}{S})$$

که در آن S جمع وقوع تمام فرکانس‌های المان در بازه زمانی آنالیز است:

$$S = \sum_{i=1}^{N} x_i$$

بنابراین، اگر غلظت زیادی از آدرس IP خاص مقصد وجود داشته باشد، این بعد با مقدار آنتروپی پایین نشان داده می‌شود. از طرف دیگر، اگر پراکندگی زیادی در داده‌های مربوط به همان بعد وجود داشته باشد، مقدار آنتروپی بالاتری بازیابی می‌شود.

ابعاد آنالیزشده به Detection Module ارسال شده تا وقوع حمله DDoS آنالیز و کشف شود. اگر حمله کشف شد، Mitigation Module فعال شده و یک سیاست مقابله ایجاد کرده که باید توسط کنترلر SDN، وارد شود. در تصویر- ۳، ارتباط بین ماژول‌های سامانه، نشان داده شده است.



تصویر- ۳

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[1] بسته است. نهایتا، زیر ماژول دوم، سیاست‌های ایجاد شده توسط زیر ماژول اول را به کنترلر مرکزی SDN برای اجرا، ارسال می‌کند.

رویکرد کشف ناهنجاری

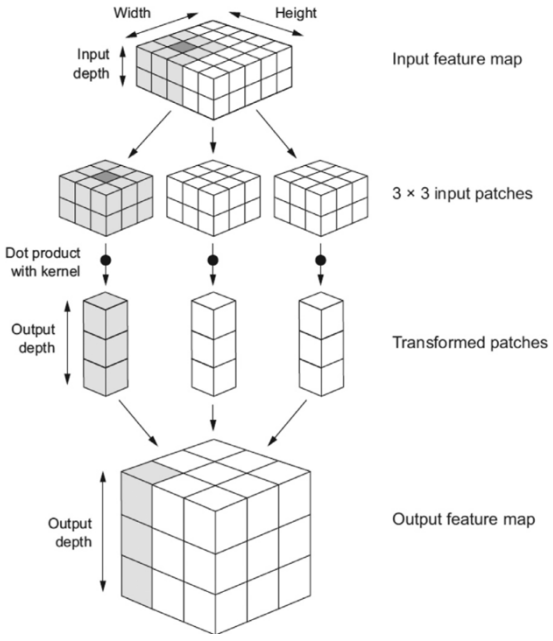
در این بخش به رویکرد کشف ناهنجاری در Detection Module مقاله، می‌پردازیم.

Convolutional Neural Network (CNN)

رویکردهای Deep learning به عنوان یک زیر شاخه از Machine learning، در شناسایی حملات و ناهجاری‌های شبکه‌های کامپیوتری، محبوبیت ویژه‌ای دارند. این رویکردها در مقابله با روش‌های Shallow مثل MLP، دارای لایه‌ها و عمق بیشتری هستند.

همانطور که در مقاله هم ذکر شده، مزیت اصلی روش‌های Deep learning، عدم وجود مهندسی ویژگی‌ها به صورت دستی است. به عبارتی دیگر، این تکنیک‌ها قادر به پیدا کردن الگو در حجم زیادی از داده‌ها، طی فرآیند یادگیری و اهمیت دادن به ویژگی‌های مربوط به طبقه‌بندی، هستند. این ویژگی باعث کشف الگوهایی پیچیده از مجموعه داده‌ها که خارج از دید انسان هستند، می‌شود.

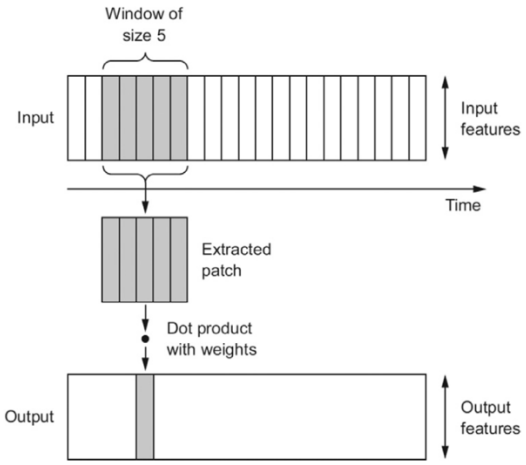
در این مقاله از تکنیک Deep learning به نام CNN استفاده شده است. تصویر- ۴ فرآیند Convolution در این روش را نشان می‌دهد.



تصویر- ۴

[1] Drop

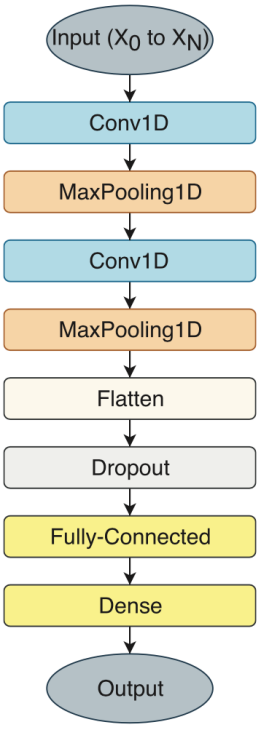
در این مقاله، جریان IP ترافیک داده، به صورت سری زمانی و نه تصویر، نمایش داده می‌شود. بنابراین در این مقاله از Convolution دو بعدی و روش 1D-CNN، استفاده شده است که ساختار و عملکردی مشابه دارد با این تفاوت که داده‌ها یک بعدی یا سری زمانی، هستند (تصویر- ۵).



تصویر- ۵

لایه‌های تک بعدی Convolutional به عنوان ورودی Tensorهای سه بعدی می‌گیرند:

- تعداد نمونه‌ها
- زمان
- ویژگی



تصویر- ۶

در این مقاله، سامانه با یک ثانیه داده عمل می‌کند و ورودی Tensor به صورت

- نمونه‌ها
- ویژگی‌ها
- کانال‌ها

تنظیم می‌شود (تصویر- ۶). همانطور که ... مشاهده شد، معماری CNN از دو لایه Conv1D و MaxPooling1D تشکیل شده است. در ادامه یک لایه Flatten، مسئول تبدیل خروجی سه بعدی لایه‌های قبلی به ورودی‌های دو بعدی برای لایه‌های دیگر، یک لایه Dropout، با هدف جلوگیری از پوشش بیش از حد به دلیل تمایل CNN به هم‌گرایی سریع به یک راه‌حل و یک لایه Dense یا Fully-connected، برای انجام طبقه‌بندی مدل جامع است که در نهایت داده‌ها به عنوان عادی یا DDoS طبقه‌بندی می‌شوند.

ارزیابی راه‌حل پیشنهادی

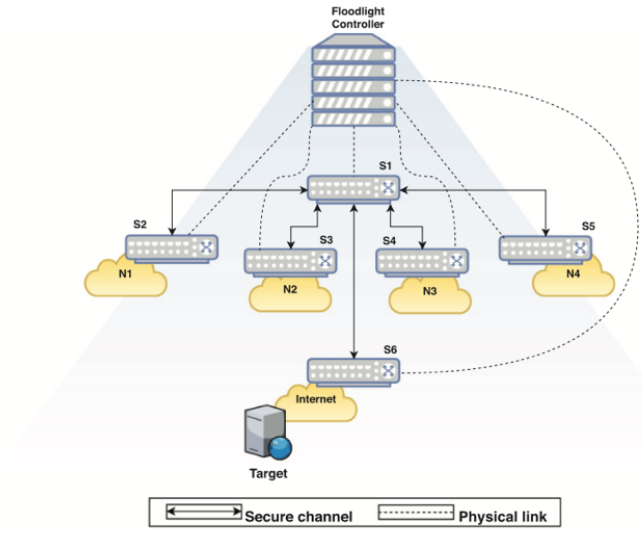
در این ارزیابی Detection Module را بررسی می‌کنیم. برای مقایسه، روش CNN این مقاله با روش‌های:

- Multi-Layered Perception (MLP): یک روش یادگیری ماشین با یک لایه پنهان و ۱۰ نورون درون آن
- Deep Neural Network (DNN) یا Dense MLP (D-MLP): نسخه Deep learning از MLP که سه لایه پنهان دارد و هر لایه ۱۰ نورون درون خود
- Logistic Regression: یک مدل آماری برای پیش‌بینی مقادیر گرفته شده قطعی از یک سری مقادیر پیوسته یا دودویی توصیفی

مقایسه می‌شود.

تمام روش‌های شناسایی با استفاده از Python و Keras در یک رایانه Corei7 2.8Ghz با 8GB حافظه RAM، پیاده شده‌اند.

سناریو اول، داده شبیه‌سازی شده SDN



تصویر- ۷

در این سناریو با استفاده از Mininet، جریان‌های IP ایجاد شده، مورد آزمایش قرار گرفتند. محیط آزمایش SDN با Open vSwitch و Floodlight و جمع‌آوری اطلاعات از طریق پروتکل OpenFlow راه اندازی شد (تصویر- ۷). هفت روز ترافیک که روز اول جهت آموزش و ۶ روز بعد جهت تشخیص ناهنجاری ایجاد شد (تصویر- ۸).

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

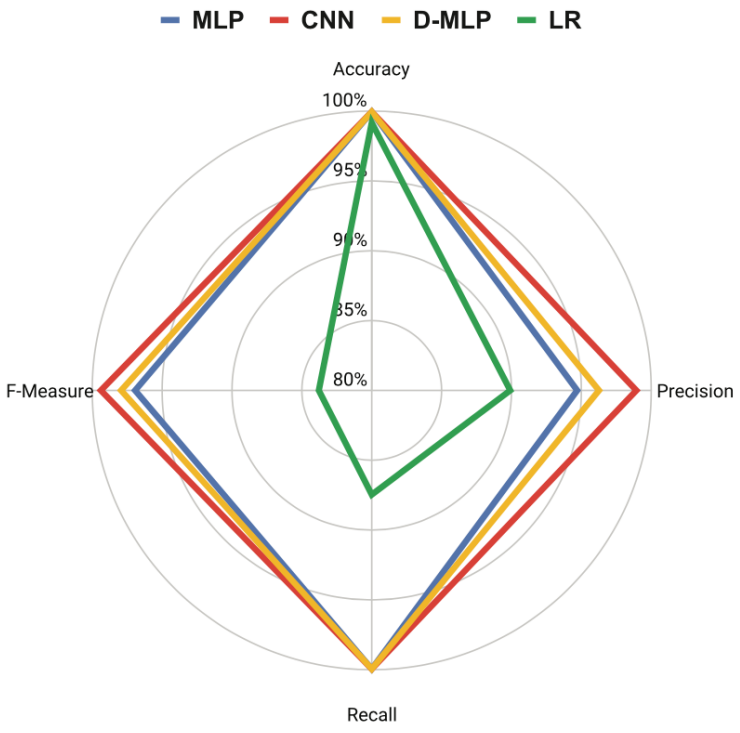
تصویر- ۸

در تصویر- ۹ خلاصه تمام نتایج آزمایش مشاهده می‌شود. در این نمودار مقایسه از نظر معیارهای کلاسیک

- Accuracy: درصد فواصل زمانی که به درستی طبقه‌بندی شده است.
- Precision: نسبت فواصل زمانی است که به درستی به عنوان DDoS در میان تمام نمونه‌هایی که به عنوان DDoS طبقه‌بندی شده‌اند.
- Recall: درصد صحت فواصل زمانی برای DDoS
- F-measure: میانگین هارمونیک بین Recall و Precision

انجام شده است.

برتری روش CNN در مقایسه با سه روش دیگر مشهود است.

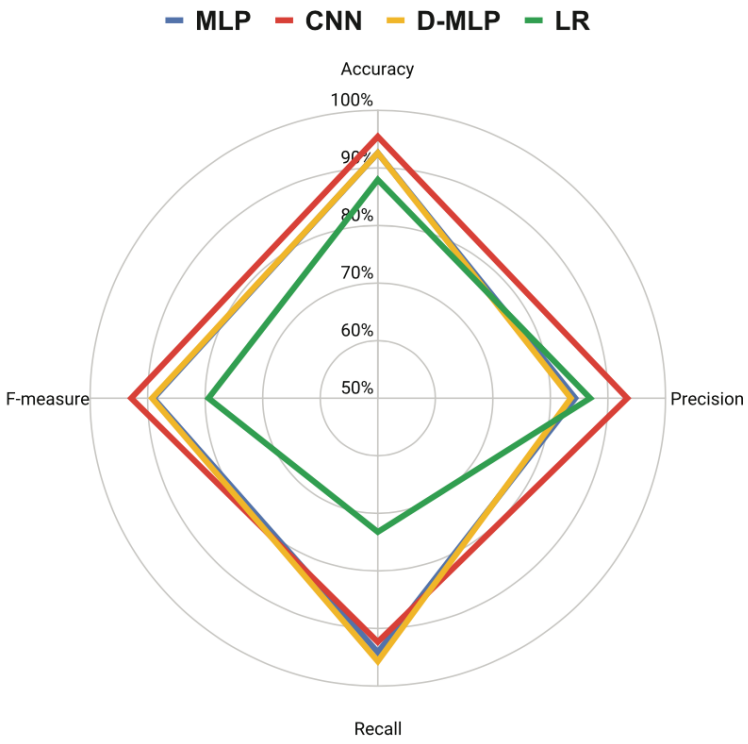


تصویر- ۹

سناریو دوم، مجموعه داده CICDDoS 2019

در این سناریو، جریان‌های IP شبیه‌سازی شده و جمع‌آوری شده از مجموعه داده‌های عمومی به نام CICDDoS 2019 را اعمال شده است. در این مجموعه داده، رفتار ۲۵ کاربر را بر اساس پروتکل‌های مختلف مانند HTTP، FTP و SSH انتزاع می‌کنند.

مجموعه داده‌های CICDDoS 2019 به دو روز تقسیم شد. یک روز آموزشی که شامل ۱۲ نوع حمله مختلف DDoS، از جمله NTP، DNS، MSSQL، LDAP، NetBIOS، SNMP، UDP، UDP-Lag، SSDP، Syn، WebDDoS و TFTP است. یک روز هم آزمایش که شامل ۶ حمله مختلف DDoS که عبارتند از NetBIOS، LDAP، MSSQL، UDP، UDP-Lag و Syn است.



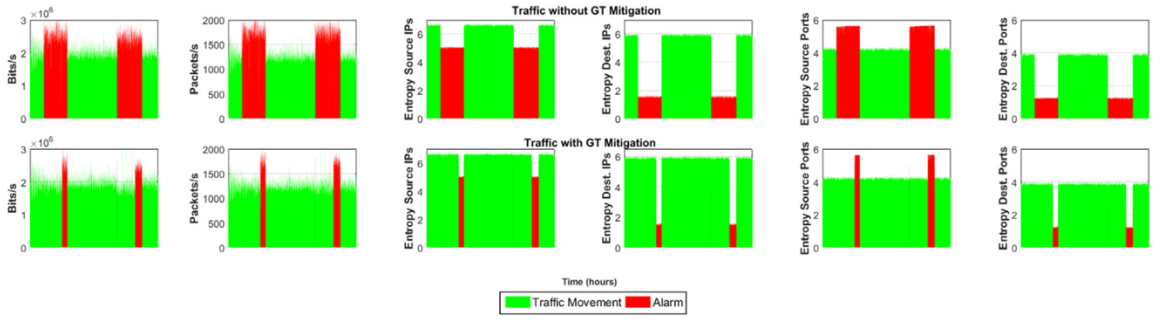
تصویر- ۱۰

همانند سناریوی، روش CNN به طور متوسط نسبت به سایر رویکردها در محیط آزمایش دوم بهتر عمل کرد و به نتایج آزمون امیدوار کننده‌ای دست یافت که آن را به عنوان یک روش کارآمد در تشخیص DDoS تبدیل می‌کند (تصویر- ۱۰).

Mitigation

همان‌طور که قبلا اشاره شد، رویکرد بهینه Mitigation Module در محدوده این مقاله نیست و روش GT برای آن انتخاب شده است. بر اساس خروجی Detection Module که یا برچسب عادی دارد و یا DDoS، این ماژول فعال شده و به صورت خودکار نرخ بهینه افتادن بسته را به عنوان اقدام مقابل DDoS، به دست می‌آورد.

در تصویر- ۱۱، ترافیک SDN آنالیز شده قبل و بعد از عمل Mitigation نشان داده شده است. به طور دقیق‌تر این شکل ترافیک را در بازه ساعتی ۱۲:۳۰ تا ۱۹:۳۰ در روز اول آزمایش که در آن حملات DDoS رخ داده است را نشان می‌دهد.



تصویر- ۱۱

نتایج نشانگر موفقیت رویکرد GT در کاهش حملات DDoS است.

نقاط قوت و ضعف مقاله

نقاط قوت این مقاله:

- امکان پیاده‌سازی روش پیشنهادی در محیط واقعی بدون تغییرات در ساختار شبکه

نقاط ضعف این مقاله:

- میزان کم بهبود نسبت به روش‌هایی مانند MLP که ساده‌تر هم هستند.

جمع‌بندی و پیشنهادات برای 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)، کارایی این روش به نمایش درآمد. هم‌چنین کارایی ماژول Mitigation بر اساس GT، بررسی شد.

به صورت کار آتی می‌توان این موارد را در نظر گرفت:

- 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

مشخصات دقیق مقاله

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