نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال دوازدهم، شماره ۳، پاییز ۱۴۰۰؛ ص ۲۸۴- ۲۷۳

علمی- پژوهشی

ارائه یک چارچوب دفاعی جدید در برابر حملات منع سرویس توزیع‌شده با استفاده از شبکه نرم‌افزار محور

مسعود محمدعلی پور[۱]، سعید شکرالهی[۲*]

۱- کارشناس ارشد، ۲- استادیار دانشگاه شهید بهشتی

(دریافت: ۱۳۹۹/۱۱/۱۱، پذیرش: ۱۴۰۰/۰۳/۰۸)

چکیده

اغلب شبکه‌های فاقد زیرساخت ثابت و مدیریت متمرکز مبتنی بر رایانش ابری با چالش‌های امنیتی متعددی مواجه هستند. اخیراً، روش‌های متفاوتی از شبکه نرم‌افزار محور (SDN) توزیع‌شده جهت رویارویی با چالش‌های پیش‌رو بهره برده‌اند. از جمله روش‌های رایج، چارچوب دفاعی پیش‌فعال متکی بر شبکه نرم‌افزار محور توزیع‌شده است که از راه‌حل تشخیص نفوذ آستانه‌ای به‌منظور ایجاد، حفظ و ارتقاء امنیت استفاده می‌کند. شبکه نرم‌افزار محور توزیع‌شده بر مقیاس‌پذیری این چارچوب افزوده و معضل شکست نقطه‌ای را برطرف می‌سازد؛ اگرچه در مقابل تهدیدات منع سرویس توزیع‌شده آسیب‌پذیر است. به‌کارگیری راه‌حل آستانه‌ای تشخیص نفوذ نیز این آسیب‌پذیری را تقویت می‌کند. در این مقاله با الگوبرداری از چارچوب دفاعی فوق، چارچوب پیش‌فعال چندلایه متکی بر شبکه نرم‌افزار محور توزیع‌شده پیشنهاد می‌شود. در چارچوب دفاعی پیشنهادی با انجام عملیات فیلترینگ داده‌ها به‌وسیله یک فیلترکننده ورودی یا امضای دیجیتال متکی بر تابع چکیده‌ساز با الگوی درختی مرکل که هر دو به‌عنوان عوامل پیشگیری‌کننده نفوذ هستند از سیستم تشخیص نفوذ Snort جهت رفع مشکل معیار آستانه‌ای تشخیص نفوذ نیز استفاده شده است. نتایج حاصل از پیاده‌سازی نشانگر این است که چارچوب پیشنهادی ما از سرعت تشخیص نفوذ، کنترل ترافیک و ثبات امنیتی لازم بهره‌مند است.

کلیدواژه‌ها: امنیت، چارچوب دفاعی، شبکه نرم‌افزار محور، حمله منع سرویس توزیع‌شده

The Presentation of a New Defense Framework Against the Distributed Denial of Service Attacks Using the Software Defined Network

M. Mohammadalipour, S. Shokrollahi[*]
Shahid Beheshti University

(Received: 30/01/2020; Accepted: 29/05/2021)

Abstract

The lack of fixed infrastructure and centralized management in most cloud computing networks causes serious security threats. In the past few years, different approaches have been taken based on the distributed software defined network (SDN) to counterbalance these facing challenges. One of these common approaches is the SDN-based Pro Defense framework which uses the threshold intrusion detection to improve security. Although the distributed software defined network is weak in the face of distributed denial of service attacks, it expands the scalability of the above-mentioned framework and resolves the point-breaking problems. On the other hand, utilizing the threshold criterion escalates the network vulnerability. In this research, the author suggests a framework called distributed SDN-based multilayer Pro Defense framework and inspires the input filter or the digital signature, and the hash function based on the Merkle tree is employed as the intrusion prevention agent. This article resolves the threshold intrusion detection criteria by utilizing the Snort intrusion detection system. The results of implementing the suggested framework indicates that it has acceptable traffic control, intrusion detection speed, and stable security.

Keywords: Security, Defense Framework, Software Defined Network, Distributed Denial of Service Attack

[*]Corresponding Author E-mail: s_shokrollahi@sbu.ac.ir

۱- مقدمه

به‌کارگیری رایانش ابری[1] برای از بین بردن محدودیت‌های موجود در شبکه مؤثر است. بر اساس تحقیقات مختلف می‌توان از مزایای آن در شبکه‌های فاقد زیرساخت ثابت و مدیریت متمرکز استفاده نمود [۱]. رایانش ابری ویژگی‌های مهمی مانند چابکی در میزان منابع مورداستفاده، کاهش هزینه، اطمینان‌پذیری، چندمستأجری، امنیت، محاسبه و نگهداری را به این قبیل شبکه‌ها تزریق می‌کند؛ هرچند حفظ و بهبود امنیت و حریم خصوصی در برابر تهدیدات مختلف در این محیط، همواره با چالش‌های مختلفی روبرو است؛ بنابراین در هنگام ارسال اطلاعات به محیط ابری، همواره نگرانی در مورد ایمنی داده‌ها و حفظ حریم خصوصی وجود دارد [۲].

در حال حاضر حفظ و برقراری امنیت از مهم‌ترین چالش‌های شبکه‌های فاقد زیرساخت ثابت محسوب می‌شود. در برخی از تحقیقات جهت بهبود امنیت در شبکه فاقد زیرساخت مبتنی بر رایانش ابری، استفاده از ویژگی‌های شبکه نرم‌افزار محور[2] شامل کنترل متمرکز و تجزیه و تحلیل ترافیک پیشنهاد شده است [۳].

این فناوری قابلیت‌هایی مانند برنامه‌ریزی، کنترل متمرکز و تجزیه و تحلیل ترافیک را برای شبکه به‌همراه دارد که می‌تواند در راستای بهبود امنیت مورد استفاده قرار گرفته و مجازی‌سازی، هوشمندی و دیدگاه‌های جدیدی را به شبکه اضافه نماید.

هر شبکه نرم‌افزار محور شامل سطوح داده، کنترل و برنامه کاربردی است. از اصول اساسی این قبیل شبکه‌ها، جداسازی سطوح کنترل و داده از هم و صدور مجوز کنترل داده توسط کنترل‌کننده متمرکز منطقی با استفاده از پروتکلی امن و استاندارد مانند OpenFlow است. این پروتکل، ارتباط امن بین سوئیچ و کنترل‌کننده نرم‌افزار محور را برقرار می‌کند. سطح کنترل به‌عنوان کنترل‌کننده سوئیچ OpenFlow عمل می‌کند. این سوئیچ شامل پروتکل OpenFlow، جداول جریان و کانال ارتباطی امن است. کنترل‌کننده می‌تواند به‌روزرسانی، افزودن یا حذف ورودی‌های جریان را در پاسخ به بسته‌های ورودی با کمک قوانین معین اعمال نماید.

محققان ادعا می‌کنند که شبکه‌های فاقد زیرساخت ثابت مبتنی بر رایانش ابری می‌توانند به‌منظور برطرف‌نمودن مشکلاتی شامل فقدان مدیریت متمرکز و زیرساخت ثابت از شبکه نرم‌افزار محور با قابلیت‌هایی مانند کنترل و مدیریت متمرکز و تجزیه و تحلیل ترافیک استفاده نمایند [۴]. با راه‌اندازی کنترل‌کننده متمرکز در این قبیل شبکه‌ها، ضمن اجرای مدیریت کیفیت سرویس و مدیریت ترافیک، امنیت در ارسال داده نیز بهبود می‌یابد. انواع ساختارهای مورداستفاده کنترل‌کننده نرم‌افزار محور در شبکه‌های ارتباطی شامل کنترل‌کننده متمرکز واحد، کنترل‌کننده سلسله‌مراتبی و کنترل‌کننده توزیع‌شده تخت[3] با دید جهانی یا محلی است [۵]. هر یک از ساختارهای بیان‌شده دارای نقاط ضعف و قوّتی هستند. در جدول (۱) ساختارهای مختلف کنترل‌کننده نرم‌افزار محور از لحاظ پارامترهای مهم مقیاس‌پذیری، شکست، ثبات و حریم خصوصی مقایسه شده است.

جدول ۱. مقایسه ساختارهای مختلف کنترل‌کننده SDN [۵]

نوع پارامتر	اولویت اول	اولویت دوم	اولویت سوم	اولویت چهارم
مقیاس‌پذیری	توزیع‌شده تخت با دید محلی	سلسله مراتبی	توزیع‌شده تخت با دید جهانی	متمرکز واحد
شکست	توزیع‌شده تخت با دید محلی و جهانی	------	سلسله مراتبی	متمرکز واحد
ثبات	توزیع‌شده تخت با دید جهانی	سلسله مراتبی	توزیع‌شده تخت با دید محلی	متمرکز واحد
حریم خصوصی	سلسله مراتبی	متمرکز واحد	توزیع‌شده تخت با دید محلی	توزیع‌شده تخت با دید جهانی

برقراری امنیت به‌وسیله شبکه نرم‌افزار محور در شبکه‌های بدون زیرساخت ثابت با چالش‌ها و مشکلاتی روبرو است. هرچند که برخی از قابلیت‌های این فناوری از قبیل تجزیه و تحلیل ترافیک، اعمال کنترل به‌صورت متمرکز و به‌روزرسانی بدون وقفه قوانین موجب تسهیل در تشخیص نفوذ و مقابله با تهدیدات می‌شود، اما دو خصیصه اعمال کنترل به روش نرم‌افزاری و به‌صورت تمرکزی در شبکه نرم‌افزار محور خود زمینه را جهت تهدیداتی از قبیل منع سرویس[4] و منع سرویس توزیع‌شده[5] فراهم می‌سازد. با توجه به این‌که در میان الزامات رایانش ابری دسترسی به خدمات بسیار مهم است، در شبکه‌های فاقد زیرساخت ثابت مبتنی بر رایانش ابری به حملات منع سرویس و منع سرویس توزیع‌شده بیشتر توجه شده است [۶]. حملات منع سرویس توزیع‌شده توسط بات‌های[6] (عامل) مختلف به‌منظور جلوگیری از دسترسی مشتری به سرویس ابری اجرا می‌شود.

تنویر آلام [۷] با ادغام شبکه موردی سیار[7] (نوعی شبکه فاقد زیرساخت ثابت و مدیریت متمرکز) و رایانش ابری یک مدل متحرک و جدید شبکه موردی سیار - ابر را طراحی نمود. نتایج نشان داد که میان‌افزار مورداستفاده در مدل متحرک فوق جهت ارتباط بین دستگاه‌های هوشمند بدون سیستم متمرکز مناسب است.

[1] Cloud Computing
[2] Software Defined Network (SDN)
[3] Flat
[4] DoS (Denial of Service)
[5] DDoS (Distributed Denial of Service)
[6] Bot
[7] Mobile Ad hoc Network (MANET)

پولاراکیس [۸] طرح استفاده از بستر شبکه نرم‌افزار محور در شبکه‌های موردی سیار را ارائه کرد. این طرح نشان می‌دهد که به‌کارگیری شبکه نرم‌افزار محور در شبکه‌های موردی سیار تاکتیکی (نظامی) که اغلب شامل تیم‌های یکپارچه و مختلف است، باعث تمرکز مدیریت در شبکه موردی سیار می‌شود.

هانگ و همکارانش [۹] از سیستم تشخیص نفوذ مبتنی بر روش آستانه‌ای و هانی‌پات (تله‌عسل) به‌عنوان روش کاهش‌دهنده حمله جهت محافظت از کنترل‌کننده نرم‌افزار محور و رویارویی با تهدیدات منع سرویس توزیع‌شده استفاده کرده‌اند. استفاده از این روش درصد ریسک‌پذیری در تشخیص درست تهدیدات را افزایش می‌دهد. یان و همکارانش [۱۰] الگوریتم برنامه‌ریزی کنترل‌کننده نرم‌افزار محور چند صفی را مبتنی بر راه‌حل اختصاص‌دهنده برش زمانی پیشنهاد نمودند. نتایج حاصله از شبیه‌سازی‌ها اثربخشی طرح فوق را نشان داده است.

محمودی و همکارانش [۱۱] به‌کارگیری سیستم تشخیص ناهنجاری مبتنی بر هشدار که از روش‌های کنترل کیفیت آماری برای تعیین حدود کنترلی و تشخیص با معیار آستانه‌ای در مقابله با تهدیدهای عملیاتی استفاده می‌کند، پیشنهاد نموده است. روش فوق ضمن اینکه قادر است ناهنجاری‌ها را بی‌درنگ به روش آستانه‌ای تشخیص و به‌طور تفکیک‌شده برای هر پست و شبکه محاسبه و شناسایی نماید، در برابر شرایط ناهنجار ناشی از سیل هشدار (جاری شدن هشدارهای سیل‌آسای تکراری و زنجیره‌ای) که با نرخ ۱۰ هشدار در دقیقه و بالاتر ایجاد می‌شوند، قادر به برطرف‌نمودن هشدارها نبوده و نیازمند پردازشگر هوشمند است.

جواهری و همکارانش [۱۲] به‌منظور تشخیص زودهنگام حمله تزریق کد/ کتابخانه قبل از کامل‌شدن و محروم‌شدن از کنترل جریان اجرایی برنامه قربانی، به‌کارگیری روش یادگیری مبتنی بر قواعد انجمنی بر اساس الگوریتم Apriori را پیشنهاد نموده است. روش فوق با داده‌کاوی در حجم انبوه بدافزار، زنجیره فراخوانی‌های رفتار مخرب تزریق کد/ کتابخانه را به‌وسیله نصب قلاب‌های شنودگر در فضای هسته سیستم‌عامل استخراج و بر اساس تابع رگرسیون خطی مدل‌سازی می‌کند. همچنین این روش می‌تواند از وقوع حمله با انسداد فراخوانی ایجاد نخ راه دور جلوگیری نماید.

قسمی و همکارانش [۱۳] با درنظرگرفتن قابلیت‌ها و معماری شبکه نرم‌افزار محور از راه‌حل آنتروپی سریع[1] جهت برقراری امنیت ابر در مواجهه با تهدیدات منع سرویس توزیع‌شده بهره برده‌اند. این روش نیز مبتنی بر معیار آستانه‌ای برای تشخیص‌دادن نفوذ است.

بشیر [۱۴] به‌منظور کشف اثربخشی روش SPRT[2] در تشخیص حملات انکار سرویس توزیع‌شده در مواجهه با کنترل‌کننده شبکه نرم‌افزار محور و شناسایی رابط‌های سوئیچ به‌خطرافتاده، جریان‌ها را به دو صورت نرمال و کم ترافیک طبقه‌بندی نمود. نتایج طبقه‌بندی به‌عنوان ورودی روش SPRT تعیین گردید. در این روش جهت ارزیابی از مجموعه داده‌های DARPA استفاده شد. نتایج حاصل‌شده از این تحقیق، ۹۹٪ دقت در تشخیص نفوذ را نشان می‌دهد.

دهکردی و همکارانش [۱۵] روش ترکیبی مبتنی بر مدل‌های آماری و یادگیری ماشین را جهت تشخیص حملات انکار سرویس توزیع‌شده پیشنهاد نمودند. روش فوق شامل سه بخش جمع‌کننده، آنتروپی و طبقه‌بندی است. آزمایش‌های انجام‌شده نشان داد که روش‌های مبتنی بر آنتروپی با آستانه ایستا نتایج مطلوبی را به‌همراه نداشته و از روش آستانه پویا با میزان FPR[3] بالا نتایج بهتری به‌دست می‌آید. روش پیشنهادی فوق به علت داشتن دقت بالا در تشخیص حملات انکار سرویس توزیع‌شده بر روی شبکه نرم‌افزار محور نسبت به سایر روش‌ها از اهمیت ویژه‌ای برخوردار است.

سین و همکارانش [۱۶] طی تحقیقاتی به این نتیجه رسیدند که اگرچه SDN در مقایسه با شبکه‌های معمولی مبتنی بر IP یک شبکه امن به نظر می‌رسد، هنوز خود آسیب‌پذیر هست. در تحقیق انجام‌شده به‌طور نظام‌مند ۷۰ مکانیسم برجسته تشخیص و کاهش حملات انکار سرویس توزیع‌شده در شبکه‌های نرم‌افزار محور بررسی شده است. این مکانیسم‌ها به چهار دسته روش‌های مبتنی بر تئوری اطلاعات، روش مبتنی بر یادگیری ماشین، روش‌های مبنی بر شبکه‌های عصبی مصنوعی (ANN) و سایر روش‌های متفرقه دسته‌بندی شدند.

گادز و همکارانش [۱۷] مدل‌های مبتنی بر یادگیری عمیق، حافظه کوتاه‌مدت و بلندمدت (LSTM) و شبکه‌های عصبی کانولوشن (CNN) را بررسی نمودند. تحقیق فوق بر روی حملات سیل UDP، TCP و TCMP که کنترل‌کننده را هدف قرار می‌دهند، متمرکز شده است. عملکرد مدل‌ها بر اساس دقت، فراخوان و نرخ منفی - درست ارزیابی می‌شود و جزئیات بیشتری در مورد زمان لازم جهت تشخیص و کاهش حمله ارائه می‌کنند. نتایج نشان داد که RNN LSTM یک الگوریتم یادگیری عمیق بادوام و دقیق است که می‌تواند به‌منظور تشخیص و کاهش حملات DDOS در کنترل‌کننده SDN استفاده شود.

بختیاری و همکارانش [۱۸] چارچوب جدیدی مبتنی بر یک مدل آماری تشخیص ناهنجاری ترافیک شبکه را برای مقابله با حملات منع سرویس توزیع‌شده در شبکه

[1] Fast Entropy

[2] Sequential Probability Ratio Test

[3] False Positive Rate

نرم‌افزار محور پیشنهاد نمودند. چارچوب فوق شامل چهار مرحله نتایج آزمایش‌های قبلی جهت تجزیه و تحلیل رفتار عادی و ترافیک حمله، پیشنهاد یک مدل ذوزنقه آماری برای تخمین تعداد خطاهای جدول در کنترل‌کننده، تخمین میزان آستانه خطاهای جدول با استفاده از تابع رگرسیون خطی همراه با برآورد EWMA[1] و در آخرین مرحله مدل مشتق‌شده را به‌عنوان مرجعی جهت تشخیص حمله و ناهنجاری‌ها به‌کار می‌گیرد. نتایج حاصل‌شده از تحقیق فوق نشان داد که استفاده از این روش با چند خطای مثبت - غلط و صرف‌نظر از مشخصات حمله می‌تواند حملات منع سرویس توزیع‌شده را در مراحل اولیه خود تشخیص دهد.

بوانی و همکارانش [۱۹] چارچوبی قابل تنظیم جهت برنامه‌های کاربردی مختلف در مواجهه با حملات منع سرویس توزیع‌شده تحت عنوان چارچوب دفاعی پیش‌فعال[2] مطرح نمودند. چارچوب بیان‌شده علاوه بر استفاده از کنترل‌کننده در یک شبکه نرم‌افزار محور توزیع‌شده، جهت تشخیص تهدیدات منع سرویس توزیع‌شده و آسانی تنظیم برای تعیین فیلترهای مختلف از روش تشخیص نفوذ آستانه‌ای بهره می‌گیرد. در چارچوب ارائه‌شده، راه‌حل‌های مختلف تشخیص نفوذ با روش‌های شناسایی ناهنجاری و سوءاستفاده در راستای جلوگیری از گسترش تهدیدات منع سرویس توزیع‌شده به قربانی کمک می‌کند.

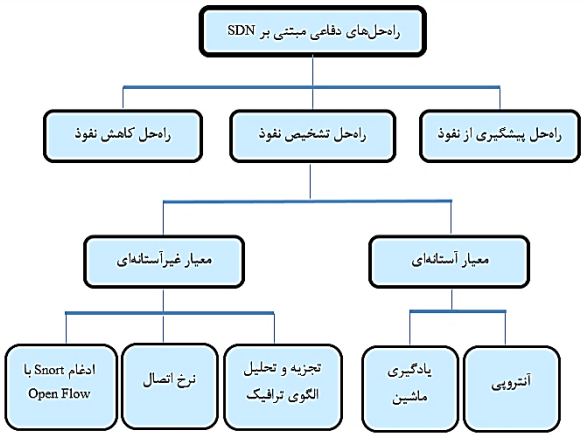
همچنین حملات منع سرویس توزیع‌شده به شیوه‌های مختلفی بر اساس تخلیه پهنای باند (حمله سیلاب و تقویت) یا حملات تخلیه منبع (حمله بسته ناقص و حمله سوءاستفاده) طبقه‌بندی شده‌اند [۲۰]. راه‌حل‌های دفاعی این قبیل حملات در محیط ابری به ترتیب بر اساس روش‌های مبتنی بر پیشگیری از نفوذ، تشخیص نفوذ و پاسخ به تشخیص نفوذ (کاهش) طبقه‌بندی می‌شوند.

بهترین راهبرد در رویارویی با تهدیدات، ممانعت از واقع‌شدن حملات است. یکی از این راهکارها استفاده از انواع فیلترها است. در این راستا از فیلترهای ورودی، خروجی و توزیع‌شده مبتنی بر مسیر مختلفی استفاده می‌شود. فیلتر توزیع‌شده مبتنی بر مسیر برای مسدودکردن یا فیلترنمودن آدرس IP بسته‌های جعلی از اطلاعات مسیر بهره می‌گیرد. سایر فنون پیشگیری از قبیل کاربرد امضاء جهت تعیین هویت، از کار انداختن سرویس‌های فاقد استفاده، بهره‌برداری از بسته‌های امنیتی، اعمال تغییراتی در آدرس IP، از کار انداختن قابلیت پخش IP به‌صورت همگانی، ایجاد تعادل بار و استفاده از تله عسل است.

در ضمن برخی از مهم‌ترین فنون تشخیص این حملات مبتنی بر شبکه نرم‌افزار محور شامل تشخیص با روش آنتروپی، تشخیص حملات با روش یادگیری ماشین و تشخیص حملات با ادغام Snort و OpenFlow است که هرکدام جهت تشخیص نفوذ از معیارهای آستانه‌ای یا غیر آستانه‌ای استفاده می‌کنند.

همچنین از روش‌های کاهش‌دهنده حمله به‌منظور ترمیم، بازیابی و جلوگیری از اجرای حملات مجدد استفاده می‌شود. برخی از روش‌های کاهش‌دهنده تهدیدات شناخته‌شده شامل مسدودکردن پورت، تغییر آدرس IP، تغییر مسیر و جداسازی ترافیک است [۱۹].

اغلب مهاجمان همسو با روند صعودی تهدیدات منع سرویس توزیع‌شده سعی می‌کنند تا به سیستم قربانی دسترسی داشته باشند. قربانی با بهره‌گیری راه‌حل‌ها یا چارچوب‌های دفاعی کارا و مؤثر قادر است از نفوذ مهاجمان جلوگیری نموده و ضمن تشخیص سریع نفوذ، تأثیر آن‌ها را به طرز چشمگیری بکاهد [۲۳-۲۲-۲۱]. شکل (۱) دسته‌بندی انواع راه‌حل‌های دفاعی را نشان می‌دهد که شامل راه‌حل‌های پیشگیری، تشخیص و کاهش نفوذ است. در ضمن انواع راه‌حل‌های تشخیص نفوذ مبتنی بر شبکه نرم‌افزار محور را بر اساس روش آشکارسازی تهدیدات به دو دسته کلی راه‌حل‌های تشخیص نفوذ آستانه‌ای و غیر آستانه‌ای طبقه‌بندی نموده و تکنیک‌های شناخته‌شده مربوط به هر یک را مشخص می‌کند.



شکل ۱. دسته‌بندی راه‌حل‌های دفاعی مبتنی بر شبکه نرم‌افزار محور [۱۹].

در این مقاله با الهام‌گرفتن از چارچوب دفاعی پیش‌فعال، راه‌کارهایی را ارائه کردیم که با استفاده از قابلیت‌های شبکه نرم‌افزار محور توزیع‌شده بتوانند ضمن رفع نقاط ضعف آن در برابر حملات منع سرویس توزیع‌شده، مشکل معیار آستانه‌ای تشخیص نفوذ را نیز برطرف نمایند. ما این مشکل را با به‌کارگیری عوامل پیشگیری از قبیل فیلتر ورودی یا امضای دیجیتال و سیستم تشخیص نفوذ Snort در چارچوب پیشنهادی (چارچوب دفاعی پیش‌فعال چندلایه) برطرف نمودیم. این چارچوب، کنترل ترافیک و پایداری امنیت بهتری را در برابر حملات منع سرویس توزیع‌شده

[1] Exponentially Weighted Moving Average
[2] (Pro Defense) Proactive Defense

برای شبکه‌های فاقد زیرساخت ثابت مبتنی بر رایانش ابری ارائه می‌کند.

ادامه مقاله به‌ترتیب زیر سازمان‌دهی شده است: در بخش ۲ با مطرح‌کردن دو ایده، بخش‌های مختلف چارچوب دفاعی پیش‌فعال چندلایه (ML – ProDefense[1]) مبتنی بر شبکه نرم‌افزار محور توزیع‌شده را بررسی می‌کنیم. در بخش ۳ ضمن ارزیابی چارچوب پیشنهادی، نتایج به‌دست‌آمده را با کارهای مشابه مقایسه می‌کنیم. در بخش ۴ این مقاله را جمع‌بندی می‌کنیم.

۲- چارچوب ML–Pro Defense بر پایه شبکه نرم‌افزار محور توزیع‌شده

امروزه تهدیدات منع سرویس توزیع‌شده همانند سلاحی در دستان هکرها است که جهت اخّاذی در محیط سایبری کاربرد دارد. این قبیل تهدیدات به‌سرعت قربانی را ناتوان ساخته و خسارت و هزینه هنگفتی به او تحمیل می‌کند. بنابراین چارچوب دفاعی پیش‌فعال بر پایه شبکه نرم‌افزار محور توزیع‌شده به‌منظور رفع نیازمندی‌های یک راه‌حل دفاعی مؤثر طراحی و ارائه شده است [۱۹]. این چارچوب، قابل تنظیم (سفارشی) بوده و روشی جدید در جهت برقراری امنیت شبکه در محیطی با برنامه‌های متنوع است.

در چارچوب ارائه‌شده، ضمن به‌کارگیری سیستم تشخیص نفوذ آستانه‌ای از انواع فیلترهای تطبیقی با توجه به میزان الزامات امنیت سایبری برنامه‌های مختلف استفاده می‌شود. مطابق نیازمندی امنیت سایبری، انواع برنامه‌ها مانند شبکه هوشمند، سیستم کنترل‌کننده ترافیک، مراقبت هوشمند بهداشتی، خدمت‌رسانی الکترونیکی، سامانه هوشمند حمل‌ونقل، شبکه هوشمند نظامی و غیره به سه دسته بحرانی، بسیار بحرانی و متوسط تقسیم می‌گردند. در چارچوب فوق جهت برنامه‌هایی با میزان حساسیت متفاوت به‌ترتیب از فیلتر متوسط، فیلتر بسیار واکنش‌پذیر و فیلتر با کمترین واکنش‌پذیری استفاده می‌شود. برای تعیین نوع فیلتر در برنامه‌های کاربردی مختلف از معادله فیلتر (۱) استفاده می‌شود [۱۹].

$$PT_t = \alpha PT_{t-1} + (1-\alpha)CT_t + c \qquad (۱)$$

در رابطه فوق PT_t: میزان ترافیک پیش‌بینی‌شده، CT_t: میزان ترافیک موجود (فعلی)، α: میزان بهره و c: یک مقدار ثابت و وابسته به خصوصیات ترافیک است. معمولاً این فیلترها قادرند در صورت تشخیص تهدید، خیلی سریع یا به‌آرامی عکس‌العمل نشان دهند. چنانچه مقدار عددی α زیاد باشد، تهدید تشخیص داده نشده و جهت α با مقادیر کمتر، اعلام فوری هشدار حمله را به‌همراه دارد.

در معادله فیلتر عنوان‌شده، چنانچه اندازه $\alpha = 0.1$ باشد، باعث غالب‌شدن اثر نرخ ترافیک موجود (فعلی) شده و فیلتر موردنظر جهت برنامه‌های کاربردی در دسته بسیار بحرانی مناسب است. این فیلتر به‌عنوان فیلتر بسیار واکنش‌پذیر (HR) معرفی شده و فوراً هشدارهای امنیتی لازم را صادر می‌کند.

در معادله فیلتر فوق اگر اندازه $\alpha = 0.5$ باشد، باعث می‌گردد نرخ‌های موجود (فعلی) و قبلی ترافیک به‌طور یکسان در نظر گرفته شود. این فیلتر به‌عنوان فیلتر با واکنش‌پذیری متوسط (IR) معرفی شده و علاوه بر استفاده جهت برنامه‌های کاربردی در دسته بحرانی، برای بیشتر شبکه‌ها قابل استفاده است.

در معادله این فیلتر اگر مقدار $\alpha = 0.9$ باشد، در برابر تهدیدات بسیار آهسته واکنش نشان داده و در برنامه‌های کاربردی مربوط به دسته متوسط که نیازمند چالاکی امنیتی کمتری هستند، استفاده می‌گردد. در این قبیل فیلترها که به‌عنوان فیلتر با کمترین میزان واکنش‌پذیری (LR) خوانده می‌شوند، هر وقت هزینه ناشی از خطای مثبت - غلط بیشتر باشد، مفیدتر و مؤثرتر هستند.

ضمن این‌که چارچوب دفاعی پیش‌فعال از ویژگی‌ها و قابلیت‌های شبکه نرم‌افزار محور با معماری کنترل‌کننده توزیع‌شده بهره می‌گیرد از معیار آستانه‌ای برای تشخیص نفوذ استفاده می‌نماید.

استفاده از معیار آستانه‌ای تشخیص نفوذ، درصد ریسک‌پذیری را می‌افزاید و آسیب‌پذیری در برابر این تهدیدات را تشدید می‌کند. همچنین حملات پیچیده‌ای که شبیه به الگوهای ترافیک مجاز هستند، تشخیص آن بسیار دشوار است و چنانچه ترافیک غیرمجاز زیر سطح آستانه باشد، ناشناخته می‌ماند؛ بنابراین به‌کارگیری الگوهای تشخیص نفوذ آستانه‌ای، قابلیت اعتماد و اطمینان‌پذیری راه‌حل را بسیار می‌کاهد [۱۹].

به همین دلیل در ادامه تلاش می‌کنیم با طرح دو ایده، چارچوب دفاعی جدیدتری که عنوانش چارچوب دفاعی پیش‌فعال چندلایه (ML - Pro Defense) مبتنی بر شبکه نرم‌افزار محور توزیع‌شده هست، امنیت چارچوب دفاعی پیش‌فعال را بهبود ببخشیم. در معماری چارچوب دفاعی پیش‌فعال چندلایه، برخلاف چارچوب پیش‌فعال که از لایه‌های پیشگیری‌کننده استفاده نشده از چندین لایه دفاعی شامل تجزیه‌وتحلیل غیر آستانه‌ای اولیه، فیلتر یا امضای دیجیتال و سیستم تشخیص نفوذ با معیار غیر آستانه‌ای Snort بهره می‌گیریم.

۲-۱- ایده اول

به‌عنوان ایده اول در چارچوب پیشنهادی از یک فیلتر ورودی پیشگیری از نفوذ با قابلیت مسدودنمودن بسته‌های غیرمجاز استفاده کردیم. این فیلتر قبل از ورود داده‌ها به سیستم تشخیص نفوذ، استفاده شده است. به‌کارگیری فیلتر قبل از سیستم

[1] Multi Layer Proactive Defense

تشخیص نفوذ، حجم ترافیک روی این سیستم را می‌کاهد و از اجرای حمله اشباع بر روی سیستم تشخیص نفوذ جلوگیری می‌کند. در ادامه به‌جای استفاده از الگوهای تشخیص نفوذ آستانه‌ای از سیستمی با عنوان سیستم تشخیص نفوذ Snort بهره گرفتیم. سیستم تشخیص نفوذ Snort قابلیت تحلیل بلادرنگ داده را (با معیار غیر آستانه‌ای) بر پایه قوانین نوشته‌شده اولیه و ثبت رویداد بسته‌های مختلف بر روی IP شبکه دارد.

۲-۱-۱- معماری چارچوب ML - Pro Defense مبتنی بر شبکه نرم‌افزار محور توزیع‌شده

راه‌حل تشخیص نفوذ مبتنی بر معماری شبکه نرم‌افزار محور به‌منظور برقراری امنیت رایانش ابری در برابر حملات منع سرویس توزیع‌شده طی تحقیقاتی به‌عنوان روش SecCloudDD معرفی شده است [۱۳]. در واقع ویژگی‌های کنترل و برنامه‌ریزی متمرکز شبکه نرم‌افزار محور، نظارت بر ترافیک ابر را مؤثرتر و امن‌تر می‌سازد.

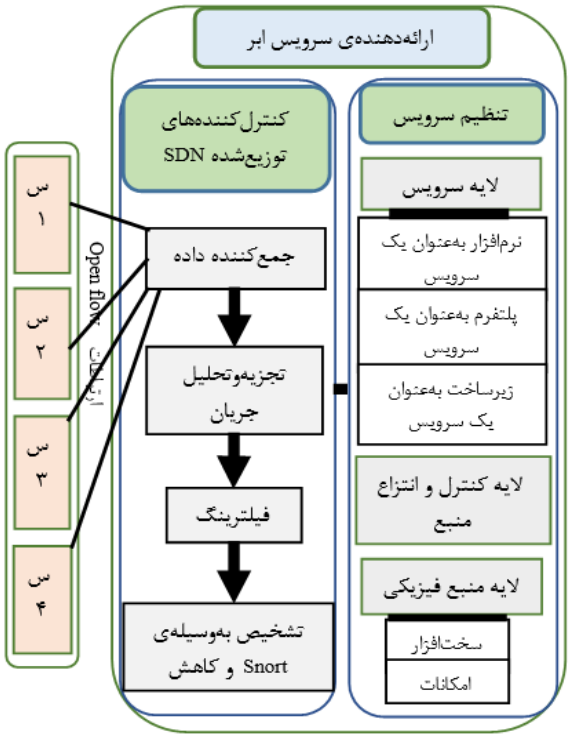
در چارچوب دفاعی پیش‌فعال چندلایه که بر اساس روش SecCloudDD طراحی شده، درخواست هر گره (نود) از طریق سوئیچ‌های OpenFlow جمع‌آوری و در جداول جریان ثبت می‌شود. سپس ویژگی‌های هر جریان ترافیکی به‌وسیله کانال ارتباطی امن (مبتنی بر پروتکل OpenFlow) و مطابق قوانین به‌روزشده ارسالی از طرف کنترل‌کننده و جداول جریان مربوط به سوئیچ‌ها به سمت جمع‌کننده جریان ارسال می‌شود. در ضمن برای هر درخواست گره جدید، سوئیچ‌های SDN ویژگی‌های درخواست از قبیل آدرس IP منبع، آدرس IP ابر و شمارنده را در جداول جریان به‌روزرسانی نموده و سپس این ویژگی‌ها را به کنترل‌کننده ارسال می‌کنند.

همچنین به‌منظور محافظت از ابر در برابر حملات منع سرویس توزیع‌شده به‌ترتیب عملیات جمع‌آوری داده، تجزیه و تحلیل اولیه، فیلترینگ، تشخیص و کاهش نفوذ به‌وسیله سیستم تشخیص نفوذ غیر آستانه‌ای (Snort) انجام می‌شود که در ادامه آن را تشریح می‌کنیم.

شکل (۲) معماری چارچوب ML–Pro Defense مبتنی بر شبکه نرم‌افزار محور را نشان می‌دهد. در این معماری درخواست‌های هر نود از طریق سوئیچ‌های شماره ۱، شماره ۲، شماره ۳ و شماره ۴ به کنترل‌کننده ارسال می‌شود (در شکل س ۱، س ۲، س ۳ و س ۴ معرف سوئیچ‌های OpenFlow شبکه نرم‌افزار محور می‌باشند).

۲-۱-۲- عملکرد کنترل‌کننده شبکه نرم‌افزار محور در معماری ML - Pro Defense

کنترل‌کننده شبکه نرم‌افزار محور پس از وصول جریان‌های ترافیکی از طریق سوئیچ‌های OpenFlow و جمع‌آوری آن‌ها در جمع‌کننده جریان، با استفاده از راه‌حل‌های غیر آستانه‌ای (مشخصات جریان از قبیل پهنای باند اشغالی، طول، نوع پروتکل، محتوا و سرآیند و غیره) جریان‌ها (بسته) را تجزیه و تحلیل کرده و چنانچه جریان ترافیکی مخرب (تهدید) تشخیص داده نشوند، آن را از فیلتر پیشگیری‌کننده عبور می‌دهد.

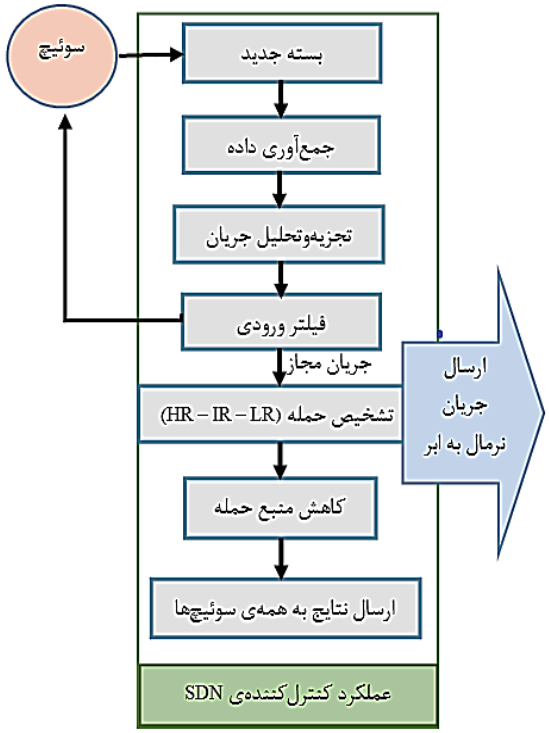


شکل ۲. معماری چارچوب ML – Pro Defense مبتنی بر SDN [۱۳]

در مرحله تجزیه و تحلیل جریان، ترافیک مجاز از فیلتر عبور کرده و ترافیک مشکوک مسدود شده و طبق قوانین به سوئیچ متناظر آن اعاده می‌شود. پس از عبور جریان ترافیکی از فیلتر، وارد سیستم Snort شده و بر اساس میزان اهمیت برنامه‌های مختلف شبکه مبتنی بر رایانش ابری، بعد از تشخیص ناهنجاری مرتبط با تهدید منع سرویس توزیع‌شده، هشدارهای امنیتی مناسب را می‌فرستد. در ادامه موتور خط‌مشی برابر نوع برنامه (طبق نیازمندی امنیت سایبری) نوع فیلتر هشداردهنده را تعیین می‌کند؛ بنابراین با توجه به این‌که روش تشخیص نفوذ Snort بر پایه قوانینی هست که در ابتدا نوشته شده، چنانچه در بخش موتور تشخیص، داده‌ای با یکی از قوانین تطبیق یابد، این بخش به‌منظور اعلام هشدار فراخوانده می‌شود.

موتور خط‌مشی به‌منظور کاهش تأثیر بسته مخرب و حملات ناشی از آن، یکی از راه‌حل‌های کاهش‌دهنده تهدیدات فوق را تعیین کرده و علاوه بر ردیابی‌نمودن و تشخیص‌دادن هویت مهاجم، ضعف احتمالی در آن را ترمیم و بازیابی نموده و از تهدیدات مجدد ممانعت می‌کند. در گام آخر نتایج به‌دست‌آمده از تشخیص نفوذ در کنترل‌کننده‌های توزیع‌شده را جهت ثبت و ذخیره در جداول جهانی، به کلیه سوئیچ‌ها می‌فرستد.

شکل (۳) نحوه عملکرد کنترل‌کننده نرم‌افزار محور در چارچوب ML – Pro Defense در راستای رویارویی با تهدیدات منع سرویس توزیع‌شده را نشان می‌دهد.



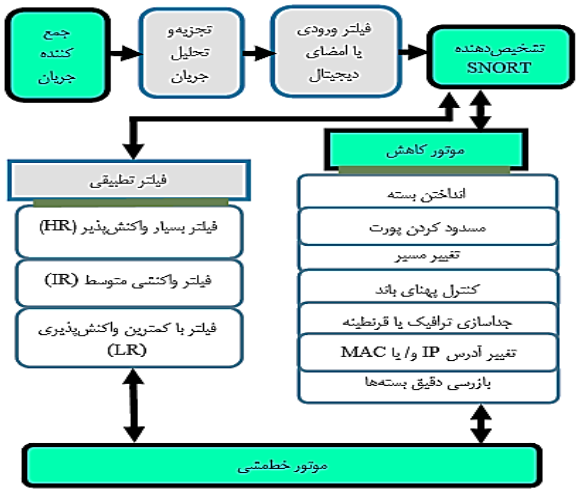
شکل ۳. نحوه عملکرد کنترل‌کننده SDN در ML - Pro Defense

۲-۱-۳- عملکرد عناصر اصلی چارچوب ML – Pro Defense

عناصر اصلی چارچوب ML – Pro Defense مشتمل بر جمع‌کننده جریان، موتور خط‌مشی، سیستم تشخیص‌دهنده نفوذ و موتور کاهش‌دهنده است. موتور کاهش‌دهنده، سیستم تشخیص‌دهنده نفوذ Snort و فیلترهای تطبیقی از هم مجزا هستند. در مرحله کاهش حملات منع سرویس توزیع‌شده، موتور خط‌مشی پس از اعلام هشدار توسط Snort با توجه به معیارهایی مانند محیط و نوع برنامه‌های کاربردی مورداستفاده و میزان الزامات امنیت سایبری آن‌ها، یکی از روش‌های کاهش‌دهنده را انتخاب می‌کند. شکل (۴) نشان‌دهنده نحوه عملکرد عناصر اصلی راه‌حل پیشنهاد شده در راستای پیشگیری و تشخیص تهدیدات منع سرویس توزیع شده و به دنبال آن پاسخ به تشخیص تهدیدات (اقدامات کاهش‌دهنده) است.

۲-۲- ایده دوم

در ایده دوم این مقاله، مدلی از امضای دیجیتال مبتنی بر تابع چکیده‌ساز (Hash Function) با عنوان امضای درختی مرکل به‌جای فیلتر ورودی در ایده اول معماری ML – Pro Defense استفاده می‌کنیم. با توجه به ایمنی بسیار خوب امضاهای مبتنی بر توابع چکیده‌ساز، استفاده از آن‌ها می‌تواند امنیت شبکه موردی سیار مبتنی بر ابر را با استفاده از شبکه نرم‌افزار محور در برابر تهدیدات منع سرویس توزیع‌شده بهبود ببخشد.



شکل ۴. عملکرد مؤلفه‌های (عناصر) اصلی چارچوب ML – Pro Defense

چارچوب ML – Pro Defense مبتنی بر امضای دیجیتال

امضای دیجیتال مبتنی بر تابع چکیده‌ساز، علاوه بر این‌که دارای امنیت بسیار بالایی هست، سرعت مناسبی نسبت به الگوهای مشابه خود دارد. در ساختار فوق، پس از ارسال بسته‌ها (داده) توسط سوئیچ به جمع‌کننده جریان ترافیک، داده‌ها جمع‌آوری شده و در ادامه بر اساس روش‌های غیر آستانه‌ای تجزیه و تحلیل می‌گردند. در گام بعدی ترافیک ارسال‌شده باید از امضای دیجیتال پیشنهادی یعنی امضای درختی مرکل عبور کرده تا به سیستم تشخیص نفوذ Snortوارد شود. عبور بسته‌های غیرمجاز و مخرب از الگوی مبتنی بر توابع چکیده‌ساز تنها در حالتی امکان‌پذیر است که کلید خصوصی را داشته باشند. چنانچه بسته‌های ارسالی فاقد کلید خصوصی باشند، به‌عنوان بسته مخرب ضمن مسدود شده و مجوز عبور به بسته‌های فوق داده نمی‌شود؛ بنابراین بسته‌های ورودی دارای کلید خصوصی از امضای دیجیتال متکی بر تابع چکیده‌ساز عبور می‌کنند. سپس جهت اطمینان بیشتر از تشخیص صحیح، بسته‌های عبوری از امضای درختی مرکل به سمت سیستم تشخیص‌دهنده نفوذ Snort هدایت می‌شوند. در ادامه کلیه اقداماتی که انجام می‌شود، دقیقاً مشابه بخش ۲- ۱ است که در تشریح نحوه عملکرد کنترل‌کننده شبکه نرم‌افزار محور بیان شده است.

نحوه عملکرد امضای مرکل در چارچوب پیشنهادی

درصورتی‌که پیام سه بیتی باشد (مانند ۱۱۱، ۱۰۱ و ۰۰۱)، برای هرکدام از آن‌ها یک کلید خصوصی تولید می‌نماییم؛ بنابراین کلید خصوصی موردنظر مشتمل بر هشت مقدار بوده که کاملاً به‌شکل تصادفی تولید شده‌اند.

مقدار اصلی کلید عمومی، مقدار نهایی حاصل‌شده از ترکیب توابع چکیده‌ساز با معماری درختی، در مسیر تعیین‌شده و برابر مقادیر میانی مشخص است (چنانچه هدف‌گذاری در الگوی فوق n بیت باشد، این ساختار می‌تواند ساختار مناسبی باشد).

بنابراین نکته حائز اهمیت در امضای درختی مرکل این است که مقادیر میانی و کلید خصوصی به کاربر واگذار نمی‌شوند، بلکه واگذاری مقدار اولیه و مقادیر لازم جهت هر مسیر ضروری است. به‌منظور تأیید صحت امضاء با داشتن مقادیر چکیده ترکیبی می‌توانیم مقدار کلید عمومی را به‌دست آوریم. همچنین با تأیید صحت کلید عمومی، صحت امضای دیجیتال نیز تأیید می‌شود. جعل‌کردن ساختار فوق نشان می‌دهد که یک پیش تصویر دوم (Second – Preimage) برای تابع چکیده‌ساز وجود دارد. همچنین در امضای درختی فوق علاوه بر کمترشدن تعداد توابع چکیده‌ساز، کلید خصوصی افشاء نمی‌شود؛ بنابراین استفاده از امضای فوق به‌منظور یک راه‌حل، میزان ایمنی بالایی را به همراه دارد. در امضای ذکرشده قادریم از توابع چکیده‌ساز SHA3 جهت ارتقاء و بهبود امنیت چارچوب پیشنهادی، استفاده نماییم.

۳- ارزیابی کارایی و مقایسه نتایج

با عنایت به این‌که چارچوب دفاعی پیش‌فعال چندلایه به‌صورت ماژولار طراحی شده است، ما با بخش‌بندی مختلف آن را اجرا و پیاده‌سازی کردیم.

در این مقاله با فرض پیاده‌سازی سایر بخش‌ها از قبیل کنترل‌کننده شبکه نرم‌افزار محور، نتایج حاصل از پیاده‌سازی نرم‌افزار تشخیص نفوذ Snort و پیاده‌سازی امضای درختی مرکل را ارزیابی کردیم. در ادامه نتایج حاصل از چارچوب پیشنهادی ما را با سایر مدل‌های ارائه‌شده مقایسه نمودیم.

۳-۱- ارزیابی کارایی

مطابق چارچوب پیشنهادی در بخش ۲، ابتدا توسط زبان برنامه‌نویسی Python کد امضاء درختی مرکل را پیاده‌سازی نمودیم. نتایج نشان‌دهنده این است که الگوریتم امضای فوق فقط بسته‌های مجاز را عبور داده و بسته‌های غیرمجاز (مخرب) پیش از واردشدن به سیستم تشخیص‌دهنده نفوذ، مسدود می‌گردد. الگوریتم امضای مرکل به‌جهت به‌کارگیری توابع چکیده‌ساز کمتر در معماری درختی خود، دارای سرعت پردازش بالاتری نسبت به سایر امضاها هست. همچنین بهره‌گیری از این امضاء در کاهش حجم ترافیک مخرب بر روی سیستم تشخیص‌دهنده نفوذ نیز بسیار تأثیرگذار است و از سنگینی بار ترافیک مخرب بر روی سیستم فوق به طرز چشمگیری می‌کاهد. در چارچوب پیشنهادی، الگوریتم امضای مرکل داده‌های مجاز را عبور داده و به سمت سیستم تشخیص نفوذ Snort هدایت می‌کند.

همچنین به‌منظور تشخیص و کاهش نفوذ از سیستم تشخیص نفوذ Snort و برنامه Win Pcap استفاده نمودیم. سپس حمله منع سرویس توزیع‌شده مبتنی بر بسته UDP را با دستور Hping3 اجرا کردیم. پیاده‌سازی نشان داد وقتی‌که حمله منع سرویس توزیع‌شده بر پایه بسته UDP انجام شود، این سیستم مطابق قوانین غیر آستانه‌ای تعریف‌شده و با وجود تعداد بسته‌های ترافیکی خیلی زیاد (مثلاً ۲۵۰۰۰ بسته در ثانیه، ۴۰۰۰۰ بسته در ثانیه یا ۵۰۰۰۰ بسته در ثانیه) قادر است بلادرنگ حمله منع سرویس توزیع‌شده را تشخیص داده و اعلام هشدار نماید.

چنانچه از قوانین آستانه‌ای Snort جهت تشخیص‌دادن نفوذ بر پایه سیل UDP استفاده کنیم، این سیستم این قابلیت را دارد که با وجود تعداد بسته‌های خیلی زیاد مثلاً ۲۵۰۰۰ بسته در ثانیه، ۴۰۰۰۰ بسته در ثانیه یا ۵۰۰۰۰ بسته در ثانیه به‌ترتیب در مدت ۱۰ ثانیه، ۱۶ ثانیه و ۲۰ ثانیه ضمن تشخیص حمله (نفوذ) سیل UDP، اعلام هشدار کند (هدف اصلی این مقاله بهره‌گیری از روش‌های غیر آستانه‌ای جهت بهبود و ارتقاء امنیت هست و اختلاف در تعداد بسته‌های ارسال‌شده در نتایج کلی تأثیری ندارد).

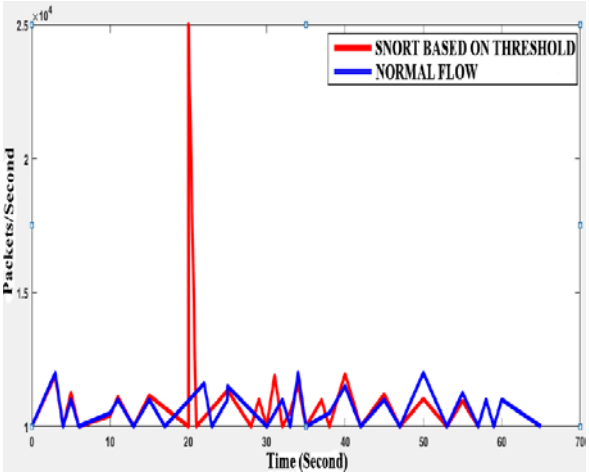
با توجه به این‌که سرعت در تشخیص نفوذ رابطه مستقیم با کارایی سیستم دارد از عوامل اصلی اجرای به‌موقع اقدامات کاهش‌دهنده تهدیدات منع سرویس توزیع‌شده به‌منظور برقراری، حفظ و بهبود امنیت است.

بررسی نتایج به‌دست‌آمده از پیاده‌سازی چارچوب دفاعی پیش‌فعال چندلایه بر پایه سیستم تشخیص نفوذ Snort آستانه‌ای و غیر آستانه‌ای و راه‌حل‌های به‌کارگرفته‌شده در تحقیقات دیگر نشان می‌دهد که چارچوب پیشنهادی ما در زمان بسیار کمتری نفوذ را تشخیص داده و روش‌های کاهش را جهت برقراری امنیت پایدار استفاده می‌نماید [۲۵-۲۴-۱۹-۱۳]؛ بنابراین چارچوب پیشنهادی ما از سرعت در تشخیص نفوذ، کنترل ترافیک و ثبات (پایداری) امنیتی قابل قبولی بهره‌مند هست.

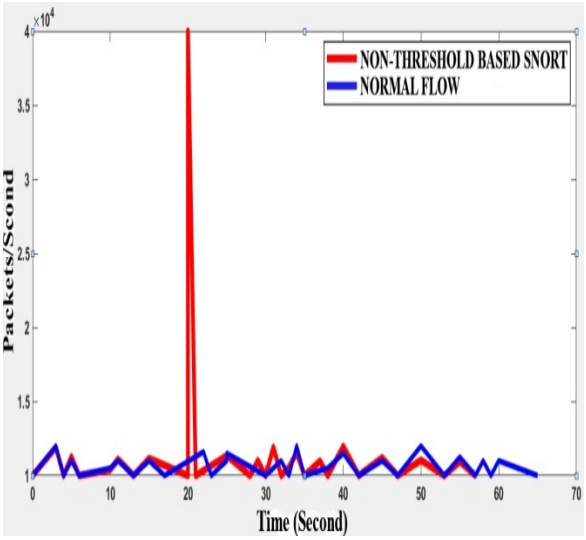
شکل‌های (۵)، (۶) و (۷) عملکرد سیستم Snort غیر آستانه‌ای را در تشخیص‌دادن نفوذ و انجام اقدامات کاهش‌دهنده در برابر حمله منع سرویس توزیع‌شده بر پایه بسته UDP به‌ترتیب با درنظرگرفتن تعداد ۴۰۰۰۰، ۲۵۰۰۰ و ۵۰۰۰۰ بسته در ثانیه نشان می‌دهند.

پیاده‌سازی نشان داد که سیستم تشخیص نفوذ Snort با معیارهای غیر آستانه‌ای مطابق قوانینی با مشخصات بسته مشتمل بر مقدار پهنای باند اشغالی، طول بسته، نوع پروتکل مورداستفاده، محتوا و سرآیند قادر است تهدیدات ذکرشده مبتنی بر بسته UDP را بلادرنگ تشخیص دهد. در این روش تعداد بسته‌های ورودی تأثیری در سرعت تشخیص نفوذ به‌وسیله سیستم فوق ندارد.

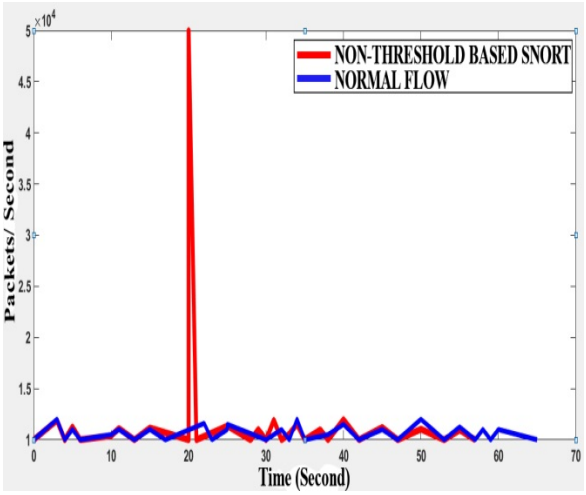
همچنین پارامترهای استفاده‌شده عبارتند از: تعداد نودها مشتمل بر ۳۰۰-۱۰۰ نود، کل سوئیچ‌ها شامل ۵٪ تعداد نودها، اندازه پنجره زمانی ۱ ثانیه، پروتکل مورداستفاده OpenFlow، تعداد بسته ورودی ۲۵۰۰۰، ۴۰۰۰۰ یا ۵۰۰۰۰ بسته در ثانیه، مدت‌زمان شبیه‌سازی ۷۰ ثانیه، فاصله میان نودها ۲۰۰ متر و نرخ حمله ۲۵٪، ۵۰٪، ۷۵٪.



شکل ۵. تشخیص حمله DDOS با ورود تعداد ۲۵۰۰۰ بسته UDP در ثانیه به‌وسیله Snort با روش غیر آستانه‌ای



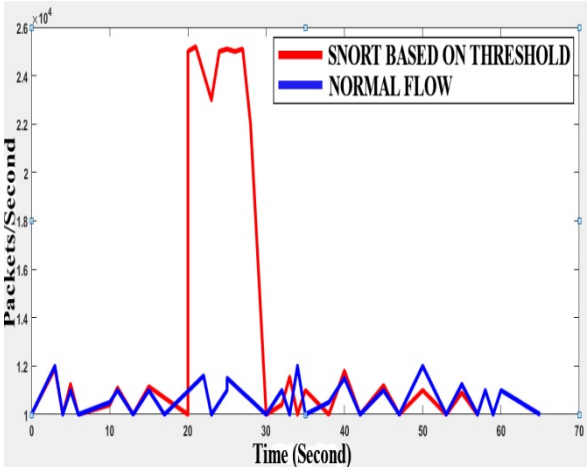
شکل ۶. تشخیص حمله DDOS با ورود تعداد ۴۰۰۰۰ بسته UDP در ثانیه به‌وسیله Snort با روش غیر آستانه‌ای



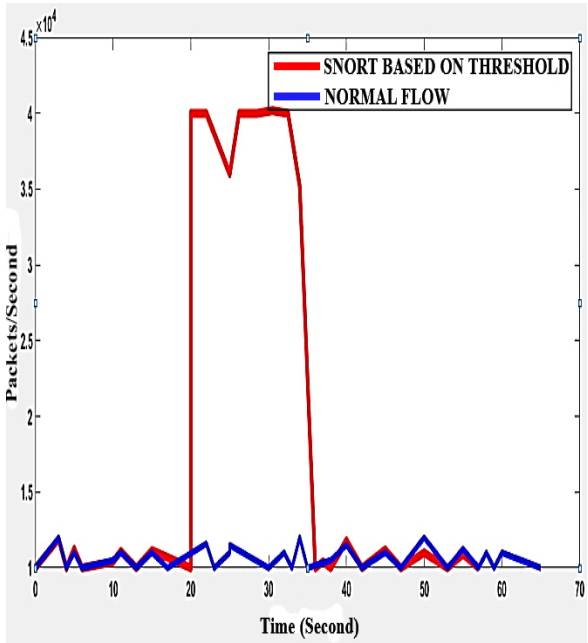
شکل ۷. تشخیص حمله DDOS با ورود تعداد ۵۰۰۰۰ بسته UDP در ثانیه به‌وسیله Snort با روش غیر آستانه‌ای

شکل‌های (۱۰- ۸) عملکرد سیستم Snort آستانه‌ای را در تشخیص‌دادن و کاهش‌دادن حمله منع سرویس توزیع‌شده بر پایه سیل بسته‌های UDP به‌ترتیب با ورود تعداد ۲۵۰۰۰، ۴۰۰۰۰ و ۵۰۰۰۰ بسته در ثانیه نشان می‌دهد. در روش فوق، سیستم Snort با تعیین سطح آستانه می‌تواند حجم ترافیک بالاتر از آن میزان را به‌عنوان ترافیک غیرمجاز و حمله مبتنی بر سیل UDP معرفی نماید. پیاده‌سازی سیستم تشخیص نفوذ Snort با روش آستانه‌ای نشان می‌دهد که مدت‌زمان لازم جهت تشخیص نفوذ به‌وسیله سیستم فوق، رابطه مستقیم با تعداد بسته‌های ورودی دارد.

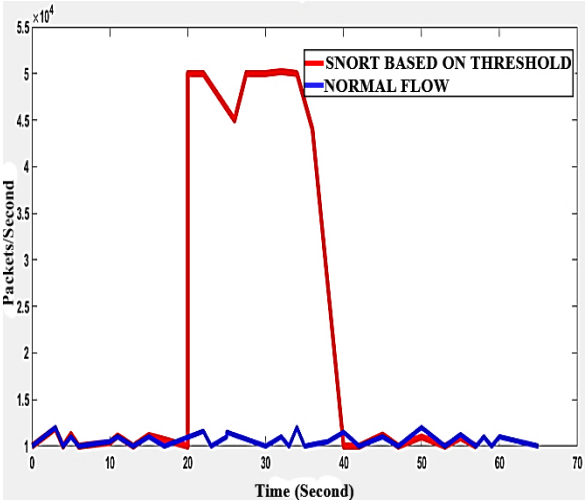
در این حالت Snort قادر است با ورود تعداد ۲۵۰۰۰، ۴۰۰۰۰ و ۵۰۰۰۰ بسته سیل UDP در ثانیه با استفاده از قوانین آستانه‌ای به‌ترتیب در مدت ۱۰ ثانیه، ۱۶ ثانیه و ۲۰ ثانیه حمله سیل UDP را تشخیص داده و هشدارهای لازم را ارسال نماید.



شکل ۸. تشخیص DDOS مبتنی بر سیل UDP با ورود ۲۵۰۰۰ بسته ترافیکی در ثانیه به‌وسیله Snort با روش آستانه‌ای



شکل ۹. تشخیص DDOS مبتنی بر سیل UDP با ورود ۴۰۰۰۰ بسته ترافیکی در ثانیه به‌وسیله Snort با روش آستانه‌ای



شکل ۱۰. تشخیص DDOS مبتنی بر سیل UDP با ورود ۵۰۰۰۰ بسته ترافیکی در ثانیه به‌وسیله Snort با روش آستانه‌ای

جدول (۲) نتایج حاصل از آزمایش‌های مختلف انجام‌شده را نشان می‌دهد. در جدول زیر مدت‌زمان لازم جهت تشخیص نفوذ به‌وسیله سیستم تشخیص نفوذ Snort با ورود تعداد ۲۰۰۰۰، ۴۰۰۰۰ و ۵۰۰۰۰ بسته در ثانیه به تفکیک روش‌های تشخیص آستانه‌ای و غیر آستانه‌ای گزارش شده است.

جدول ۲. نتایج کلی آزمایش‌های انجام‌شده

ردیف	روش تشخیص نفوذ	تعداد بسته ورودی در ثانیه	زمان تشخیص
۱	سیستم Snort با روش آستانه‌ای	۲۵۰۰۰ بسته ۴۰۰۰۰ بسته ۵۰۰۰۰ بسته	۱۰ ثانیه ۱۶ ثانیه ۲۰ ثانیه
۲	سیستم Snort با روش آستانه‌ای	۲۵۰۰۰ بسته ۴۰۰۰۰ بسته ۵۰۰۰۰ بسته	بلادرنگ بلادرنگ بلادرنگ

در ادامه، آزمایش‌های انجام‌شده را به‌منظور تعیین میزان صحت و دقت نتایج اولیه توسط برخی پارامترهای آماری از قبیل میانگین و میزان انحراف معیار ۳۰ بار تکرار نمودیم.

با استفاده از رابطه‌های (۲ و ۳) که به‌ترتیب نشان‌دهنده میانگین (مقدار متوسط داده‌ها) و انحراف معیار (به‌عنوان یکی از شاخص‌های پراکندگی) هستند، نتایج حاصل را از لحاظ متوسط مدت‌زمان لازم جهت تشخیص نفوذ و میزان پراکندگی (میانگین فاصله بین داده‌ها تا مقدار متوسط به‌دست‌آمده) محاسبه نمودیم.

$$\mu = \frac{\sum_{i=1}^{n}(x_i)}{n} \quad (۲)$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(x_i - \mu)^2}{N}} \quad (۳)$$

در رابطه (۲)، μ میانگین و n تعداد نمونه‌ها و x_i مقدار هر نمونه است. همچنین در رابطه (۳)، σ نشان‌دهنده انحراف معیار است و N تعداد داده‌ها (در جامعه آماری یا نمونه آماری) و x_i مقدار هر نمونه و μ مقدار متوسط (میانگین) نمونه‌ها است.

بیان این نکته حائز اهمیت است که در تحلیل داده‌های آماری میزان انحراف معیار کمتر، پراکندگی داده‌های کمتر و میزان انحراف معیار بیشتر، پراکندگی داده‌های قابل توجهی را به‌همراه دارد.

بررسی نتایج به‌دست‌آمده از تعداد ۳۰ بار تکرار آزمایش تحت جمعیت آماری ۵= N (جامعه آماری ۵ فرض شده است) و ورود تعداد ۲۵۰۰۰، ۴۰۰۰۰، ۵۰۰۰۰، ۷۵۰۰۰ و ۱۰۰۰۰۰ بسته UDP در ثانیه، نشان‌دهنده این است که سیستم تشخیص نفوذ Snort با معیار آستانه‌ای در حالت‌های مختلف تکرار آزمایش مطابق جدول (۳) می‌تواند به‌موقع نفوذ را تشخیص داده و اعلام هشدار نماید.

در جدول (۳) میانگین زمان تشخیص نفوذ به‌وسیله Snort و انحراف معیار در حالت‌های مختلف تکرار آزمایش (شامل ۱۰، ۲۰ و ۳۰ بار آزمایش) نشان داده شده است. نتایج به‌دست‌آمده صحت و دقت انجام آمایش‌های اولیه ما را تائید می‌کنند.

۳-۲- مقایسه نتایج

استفاده از عوامل پیشگیری‌کننده، بار ترافیک را در سیستم تشخیص نفوذ Snort به طرز چشمگیری کاهش داده و سبب کنترل جریان ترافیک توسط سیستم تشخیص نفوذ Snort شده است.

آزمایش‌های انجام‌شده نشان داد که سیستم تشخیص نفوذ Snort با معیار آستانه‌ای به‌علت داشتن سرعت عمل بالا در تشخیص تهدیدات منع سرویس توزیع‌شده دارای میزان ریسک‌پذیری امنیتی خیلی کمتری در قیاس با سایر الگوهای آستانه‌ای است. همچنین سیستم فوق با معیار غیر آستانه‌ای مطابق قوانینی در زمینه مشخصات بسته شامل میزان پهنای باند اشغالی، طول بسته، نوع پروتکل استفاده‌شده، محتوای بسته و سرآیند قادر است تهدیدات ذکرشده مبتنی بر بسته UDP، ICMP، TCP را به‌صورت بلادرنگ تشخیص دهد. با توجه به مطالب بیان‌شده در بخش ۳-۱، سرعت عمل در تشخیص نفوذ رابطه مستقیم با کارایی سیستم دارد. در ضمن هنگامی یک سیستم تشخیص نفوذ دارای کارایی لازم هست که به‌موقع تهدید را تشخیص دهد [۱۱]؛ بنابراین سرعت از عوامل اصلی اجرای به‌موقع اقدامات کاهش‌دهنده نفوذ به‌منظور برقراری، حفظ و بهبود امنیت است. با توجه به موارد عنوان‌شده با کاهش مدت‌زمان لازم جهت تشخیص و کاهش نفوذ، امکان اشباع‌شدن سیستم که در برخی تحقیقات [۱۱] به‌عنوان شرایط ناهنجار در سیستم معرفی شده کاهش می‌یابد.

جدول ۳. نتایج حاصل‌شده از ۳۰ بار تکرار آزمایش به‌وسیله سیستم تشخیص نفوذ Snort با معیار آستانه‌ای

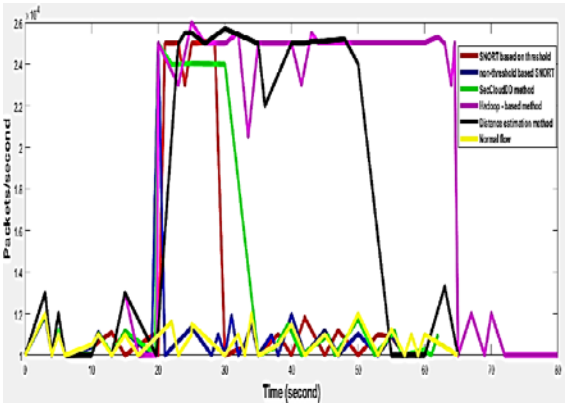
تعداد بسته ورودی / انواع حالت‌ها	۲۵۰۰۰ بسته در ثانیه	۴۰۰۰۰ بسته در ثانیه	۵۰۰۰۰ بسته در ثانیه	۷۵۰۰۰ بسته در ثانیه	۱۰۰۰۰۰ بسته در ثانیه
میانگین مدت‌زمان تشخیص در ۱۰ بار تکرار آزمایش	۱۰/۱۵ ثانیه	۱۶/۱۳ ثانیه	۲۰/۱۰ ثانیه	۳۰/۱۴ ثانیه	۴۰/۱۳ ثانیه
میانگین مدت‌زمان تشخیص در ۲۰ بار تکرار آزمایش	۱۰/۱۰ ثانیه	۱۶/۲۸ ثانیه	۲۰/۲۱ ثانیه	۳۰/۱۸ ثانیه	۴۰/۲۴ ثانیه
میانگین مدت‌زمان تشخیص در ۳۰ بار تکرار آزمایش	۱۰/۱۸ ثانیه	۱۶/۲۰ ثانیه	۲۰/۱۶ ثانیه	۳۰/۱۲ ثانیه	۴۰/۱۷ ثانیه
انحراف معیار در ۱۰ بار تکرار آزمایش	۰/۰۳۰۹	۰ /۰۳۱۶	۰/۰۷۰۷	۰/۰۵۶۵	۰/۰۶۷۸
انحراف معیار در ۲۰ بار تکرار آزمایش	۰/۰۱۲۶	۰/۰۸۸۵	۰/۰۶۳۵	۰/۰۵۲۱	۰/۰۳۰۳
انحراف معیار در ۳۰ بار تکرار آزمایش	۰/۰۵۰۵	۰/۰۳۱۶	۰/۰۲۶۰	۰/۰۳۸۹	۰/۰۳۰۰

بنابراین ما در این مقاله با استفاده از کنترل‌کننده شبکه نرم‌افزار محور توزیع‌شده، ضمن بهبود مقیاس‌پذیری و کاهش بار ترافیک، سرعت تشخیص نفوذ را توسط Snort افزایش دادیم.

پیاده‌سازی نشانگر این هست که چارچوب دفاعی پیشنهادی ما (دفاعی پیش‌فعال چندلایه) با بالارفتن سرعت در تشخیص نفوذ و کنترل جریان ترافیک از ثبات امنیتی قابل قبولی بهره‌مند است.

شکل (۱۱) عملکرد سیستم تشخیص نفوذ Snort را با معیارهای آستانه‌ای و غیر آستانه‌ای استفاده‌شده در چارچوب دفاعی پیشنهادی ما در قیاس با سایر روش‌های تحقیقاتی، هنگامی‌که تعداد بسته‌های ورودی ۲۵۰۰۰ بسته در ثانیه هست، نشان می‌دهد. در شکل خط زرد نشان‌دهنده رفتار ترافیکی نرمال و هریک از خطوط قرمز و آبی به ترتیب نشانگر رفتار ترافیکی مخرب (حمله منع سرویس توزیع‌شده) در چارچوب متکی بر سیستم Snort با معیار تشخیص نفوذ آستانه‌ای و غیر آستانه‌ای هستند.

همچنین خطوط صورتی، مشکی و سبز نشان‌دهنده رفتار ترافیکی مخربی هستند که جهت تشخیص حملات ذکرشده به ترتیب از روش‌های هادوپ (روش کاهش حجم ترافیک داده با استفاده از فن FIFO[1])، تخمین فاصله (بر اساس طول عمر بسته) و روش مبتنی بر Sec Cloud DD (آنتروپی با معیار آستانه‌ای) که توسط شبیه‌ساز Cloud Sim حاصل‌شده، استفاده می‌کنند [۱۳]. هر سه روش فوق در قیاس با راه‌حل (چارچوب) پیشنهادی ما (دفاعی پیش‌فعال چندلایه)، نیازمند زمان بیشتری جهت تشخیص‌دادن، کاهش تهدیدات منع سرویس توزیع‌شده و تثبیت سیستم هستند.



شکل ۱۱. عملکرد دفاعی چارچوب ML – Pro Defense مبتنی بر سیستم Snort، مقابل تهدیدات DDOS، در مقایسه با سایر روش‌ها

همچنین جدول (۴) عملکرد Snort در چارچوب پیشنهادی ما را با سایر روش‌های تشخیص نفوذ استفاده‌شده در مقالات مختلف، وقتی‌که تعداد بسته‌های ورودی ۲۵۰۰۰ بسته هستند یا در برابر حجم انبوهی از ترافیک مخرب از حیث سرعت، کنترل ترافیک و پایداری (ثبات) امنیتی قیاس کرده است.

جدول ۴. مقایسه عملکرد سیستم تشخیص نفوذ در مقالات مختلف

روش تشخیص نفوذ	مراجع	تعداد بسته ترافیکی	زمان تشخیص
آنتروپی سریع مبتنی بر آستانه	[۱۳-۱۹]	۲۵۰۰۰ بسته در ثانیه	۱۵ ثانیه
تخمین فاصله (عمر بسته)	[۲۴]	۲۵۰۰۰ بسته در ثانیه	۳۵ ثانیه
مبتنی بر هادوپ (FIFO)	[۲۵]	۲۵۰۰۰ بسته در ثانیه	۴۵ ثانیه
یادگیری مبتنی بر قواعد انجمنی با استفاده از الگوریتم Apriori	[۱۲]	حجم انبوهی از رفتارهای مخرب تزریق کد/ کتابخانه	قبل محروم‌شدن از کنترل اجرای برنامه (به‌موقع)
پردازش ناهنجاری‌ها به‌وسیله کنترل کیفیت آماری	[۱۱]	حالت اول: نرخ ۱۰ هشدار در دقیقه و بالاتر (جاری‌شدن سیل هشدار) حالت دوم: در برابر تهدیدهای عملیاتی	عدم تشخیص و برطرف نکردن هشدارها در شرایط ناهنجار ناشی از سیل هشدار (بدون پردازشگر هوشمند) – تشخیص بی‌درنگ مبتنی بر تعیین سطح آستانه
Snort با روش آستانه‌ای	این مقاله	۲۵۰۰۰ بسته در ثانیه	۱۰ ثانیه
Snort با روش غیر آستانه‌ای	این مقاله	۲۵۰۰۰ بسته در ثانیه	بلادرنگ

[1] First In First Out

۴- نتیجه‌گیری

در این مقاله با توجه به پیشرفت فزاینده تهدیدات منع سرویس توزیع‌شده در شبکه‌های فاقد زیرساخت ثابت و مدیریت متمرکز مبتنی بر ابر، یک راه‌حل دفاعی جدید جهت بهبود و ارتقاء امنیت این قبیل شبکه‌ها ارائه نمودیم. به‌همین‌منظور از چارچوب پیش‌فعال بر پایه شبکه نرم‌افزار محور توزیع‌شده الگوبرداری نموده و راه‌حل (چارچوب) دفاعی پیش‌فعال چندلایه (ML – Pro Defense) بر پایه شبکه نرم‌افزار محور توزیع‌شده پیشنهاد شده است. چارچوب پیشنهادی با بهره‌گیری فیلتر ورودی یا امضای دیجیتال مبتنی بر تابع چکیده‌ساز به‌عنوان عوامل پیشگیری‌کننده، باعث کاهش بار ترافیک و تشخیص سریع‌تر نفوذ به‌وسیله Snort می‌شود. پیاده‌سازی نشان می‌دهد Snort قادر است نفوذ را بلادرنگ در حالت غیر آستانه‌ای و بر اساس قوانین از پیش نوشته‌شده تشخیص دهد. سرعت در تشخیص نفوذ ضمن این‌که رابطه مستقیم با کارایی سیستم داشته از عوامل اصلی برای اجرای به‌موقع اقدامات کاهش‌دهنده تهدیدات منع سرویس توزیع‌شده جهت برقراری، حفظ و بهبود (ارتقاء) امنیت پایدار در چارچوب ارائه‌شده و سایر روش‌های تشخیص نفوذ در تحقیقات مختلف هست. بررسی نتایج حاصل از پیاده‌سازی نشان‌دهنده این است که چارچوب پیشنهادی ما ضمن این‌که مشکلات تشخیص نفوذ آستانه‌ای در راه‌حل‌های ارائه‌شده قبلی را برطرف می‌سازد از سرعت در تشخیص نفوذ، کنترل جریان ترافیک و ثبات (پایداری) امنیتی لازم برخوردار هست.

۵- مرجع‌ها

[1] Zhou, L.; Haas, Z. J. “ Securing Ad hoc Networks”; IEEE Network. 1399, 13, 6, 24-30.

[2] Allam, H.; Nasser, N.; Rajan, A.; Ahmad, J. “A Critical Overview of Latest Challenges and Solutions of Mobile Cloud Computing ”; IEEE Trans. Second Int. Conf. Fog and Mobile Edge Computing 2017, 225-229.

[3] Yan, Q.; Yu, F. R.; Gong, Q.; Li, J. “Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges”; IEEE Commun. Surveys & Tutorials 2015, 18, 602-622.

[4] Bellavista, P.; Dolci, A.; Giannelli, C. “MANET-Oriented SDN: Motivations, Challenges, and a Solution Prototype”; IEEE 19th Int. Symp. A World of Wireless, Mobile and Multimedia Networks 2018, 14-22.

[5] Oktian, Y. E.; Lee, S.; Lee, H.; Lam, J. “ Distributed SDN Controller System: A Survey on Design Choice”; Comput Networks 121, 2017, 100-111.

[6] Ghosekar, P.; Katkar, G.; Ghorpade, P. “Mobile Ad hoc Networking: Imperatives and Challenges”; IJCA Special Issue on MANETs 2010, 3, 153-158.

[7] Alam, T. “Middleware Implementation in Cloud MANET Mobility Model for Internet of Smart Devices”; Int. J. Comput. Sci. Network Secur. 2017, 17, 86-94.

[8] Poularakis, K.; Iosifidis, G.; Tassiulas, L. “SDN-Enabled Tactical Ad hoc Networks: Extending Programmable Control to the Edge”; IEEE Commun. Mag. 2018, 56, 132-138.

[9] Huang, X.; Du, X.; Song, B. “An Effective DDoS Defense Scheme for SDN”; IEEE Int. Conf. Commun. 2017, 1-6.

[10] Yan, Q.; Gong, Q.; Yu, F. R. “Effective Software-Defined Networking Controller Scheduling Method to Mitigate DDoS Attacks”; Electron. Lett. 2017, 53, 469-471.

[11] Mahmoudi, N. P.; Yazdian, V. A. “An Anomaly Detection System for Operational Threats in SCADA System”; J. Adv. Defence Sci. & Technol. 2016, 10, 209-218.

[12] Javaheri, D.; Hosseinzadeh, M. “A Solution for Early Detection and Negation of Code and DLL Injection Attacks of Malwares”; J. Adv. Defence Sci & Technol. 2020, 1, 393-406.

[13] Guesmi, H.; Saidane, L. A. “Using SDN Approach to Secure Cloud Servers Against Flooding Based DDoS Attacks”; IEEE 25th Int. Conf. Systems Eng. 2017, 309-315.

[14] Ali, B. H. “ Study the Effectiveness of Sequential Probability Ratio Test in Detection DDoS Attacks Against SDN”; Al-Iraqia J. Sci. Eng. Res. Jan. 2021, 46-53.

[15] Dehkordi, A. B.; Soltanaghaei, M.; Boroujeni, F. Z. “The DDoS Attacks Detection Through Machine Learning and Statistical Methods in SDN”; J. Supercomput. 2021, 77, 2383-2415.

[16] Singh, J.; Behal, S. “Detection and Mitigation of DDoS Attacks in SDN: A Comprehensive Review Research Challenges and Future Directions ”; Comput. Sci. Surv. 2020, 37, 100279.

[17] Gadze, J. D.; Bamfo-Asante, A. A.; Agyemang, J. O.; Nunoo-Mensah, H.; Opare, K. A. B. “An Investigation Into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers”; Technologies 2021, 9, 14.

[18] Shohani, R. B.; Mostafavi, S.; Hakami, V. “A Statistical Model for Early Detection of DDoS Attacks on Random Targets in SDN”; Wireless Personal Communications 2021, 1-22.

[19] Bawany, N. Z.; Shamsi, J. A.; Salah, K. “DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions”; Arabian J. Sci. Eng. 2017, 42 , 425-441.

[20] Deshmukh, R. V.; Devadkar, K. K. “Understanding DDoS Attack & its Effect in Cloud Environment”; Proc. Compu. Sci. 2015, 49, 202-210.

[21] Bhushan, K.; Gupta, B. B. “Distributed Denial of Service (DDoS) Attack Mitigation in Software Defined Network (SDN) - Based Cloud Computing Environment”; J. Ambient Intell. Hum. Comput. 2019, 10, 1985-1997.

[22] Li, C.; Wu, Y.; Yuan, X.; Sun, Z.; Wang, W.; Li, X.; Gong, L. “Detection and Deep Learning in Based on Defense of DDoS Attack OpenFlow□Based SDN”; Int. J. Commun. Syst. 2018, 31, 3497.

[23] Swami, R.; Dave, M.; Ranga, V. “ Software - Defined Networking - Based DDoS Defense Mechanisms ”; ACM Comput. Surveys 2019, 52, 1-36.

[24] Chapade, S. S.; Pandey, K. U.; Bhade, D. S. “ Securing Cloud Servers Against Flooding Based DDoS Attacks ”; IEEE. Int. Conf. Commun. Syst. Network Technol. 2013, 524-528.

[25] Tripathi, S.; Gupta, Almomani, A.; Mishra, A.; Veluru, S. “Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attack”; J. Inf. Security 2013, 4, 150.