مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال نهم، شماره ۲، تابستان ۱۳۹۷؛ ص ۲۱۹-۲۱۱

یک روش کارآمد جهت مقابله با حمله بارکشی رایگان در شبکه‌های مبتنی بر نرم‌افزار

رضا محمدی[۱]، محمد رضا پارسائی[۲*]، رضا جاویدان[۳]، رضا اکبری[۴]
۱و۲- دانشجوی دکتری، ۳- دانشیار، ۴- استادیار، دانشگاه صنعتی شیراز
(دریافت: ۹۶/۰۱/۱۹، پذیرش: ۹۶/۰۷/۱۶)

چکیده

ظهور شبکه‌های مبتنی بر نرم‌افزار در طی سالیان اخیر، بسیاری از مباحث مرتبط با مسائل مدیریتی و پیکربندی شبکه را برای مدیران شبکه تسهیل کرده است. در شبکه‌های مبتنی بر نرم‌افزار سطح داده‌ای و سطح کنترلی شبکه به منظور مدیریت متمرکز و پویا از یکدیگر منفک شده‌اند. تمامی امور مرتبط با اعمال سیاست‌های مدیریتی و راهبری شبکه در شبکه‌های مبتنی بر نرم‌افزار در سطح کنترلی انجام می‌شود. با وجود این که این سازوکار امکان مدیریت متمرکز و کارآمد را فراهم می‌کند، برخی نقاط ضعف امنیتی جدیدی را مطرح می‌کند که می‌توانند تأثیر مخربی بر روی عملکرد و کارایی شبکه داشته باشند. یکی از مهم‌ترین حمله‌های موجود در شبکه‌های مبتنی بر نرم‌افزار، حمله بارکشی رایگان می‌باشد که در آن یک کاربر بدخواه می‌تواند از منابع تخصیص داده شده به یک کاربر دیگر به نحوی استفاده کند که سطح کنترلی شبکه متوجه این موضوع نشود. این مقاله، ابتدا به تشریح و معرفی کامل حمله بارکشی رایگان می‌پردازد و در ادامه یک روش مقابله کارآمد جهت پیشگیری از این حمله ارائه می‌دهد. به علت این که بخشی از روش پیشنهادی در سطح داده‌ای شبکه پیاده‌سازی می‌شود، دارای سرعت تشخیص بالا بوده و سربار کمی دارد. نتایج حاصل از شبیه‌سازی نشان می‌دهد که روش پیشنهادی بدون اثرگذاری منفی بر کارایی شبکه، به طور مؤثری می‌تواند حملات بارکشی رایگان را شناسایی و متوقف نماید.

کلید واژه‌ها: شبکه‌های مبتنی بر نرم‌افزار، حمله بارکشی رایگان، امنیت شبکه

An Effective Countermeasure Method against Freeloading Attack in Software Defined Networks

R. Mohammadi, M. R. Parsaei*, R. Javidan, R. Akbari
Shiraz University of Technology
(Received: 08/04/2017; Accepted: 08/10/2017)

Abstract

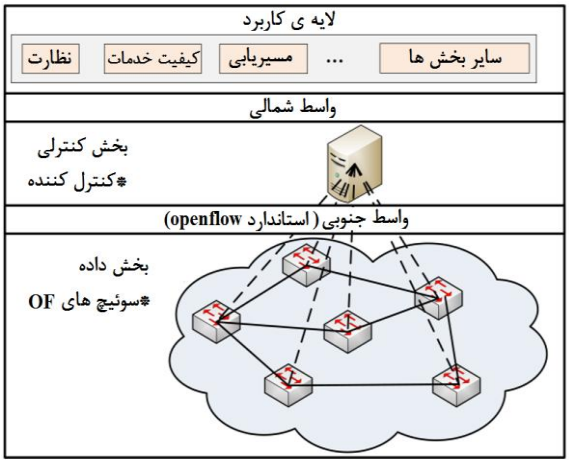
In recent years, Software Defined Networking (SDN) facilitates the most of management and configuration issues for network administrators. In SDN, data plane and control plane are separated from each other and the control plane is responsible for all management functionality issues. Although, this mechanism provides effective and centralized management, it introduces some security problems which might have adversary effect on the performance of network. Freeloading is one of the most important attacks in SDN, in which a malicious user can hiddenly use the network resources. This paper explains the freeloading attack in detail and proposes an effective countermeasure for mitigating the attack. Due to the some components of the proposed method is implemented in data plane; it has low overhead and high accuracy. Simulation results confirm that the proposed method can detect and prevent the freeloading attack effectively without adverse effects on the network performance.

Keywords: Software Defined Networks, Freeloading Attack, Network Security

*Corresponding Author E-mail: mr.parsaei@sutech.ac.ir

۱. مقدمه

شبکه‌های مبتنی بر نرم‌افزار[1] به عنوان پدیده‌ای نوظهور در حوزه شبکه‌های مخابراتی و رایانه‌ای به شمار می‌روند. هدف اصلی ارائه این نوع شبکه‌ها غلبه و رفع مشکلاتی نظیر مدیریت دشوار و پیچیده در شبکه‌های مبتنی بر پروتکل IP که شبکه رایج در ارتباطات امروزی است، می‌باشد [۱]. در شبکه‌های فعلی، مدیران شبکه جهت پیکربندی، تغییر سیاست‌های مدیریتی شبکه‌ها، بررسی و آزمایش پروتکل‌ها و ایده‌های جدید و مدیریت پویای شبکه ناگزیر به اعمال تغییرات و پیکربندی بر روی تجهیزات فعال شبکه هستند. در بسیاری از موارد، این تجهیزات محصول شرکت‌های مختلفی هستند که دستورات پیکربندی خاص خود را دارند. شبکه مبتنی بر نرم‌افزار به عنوان یک مفهوم بسیار جامع و کلی با تفکیک سطح داده‌ای[2] و سطح کنترلی[3] شبکه بسیاری از محدودیت‌ها و مشکلات شبکه‌های فعلی را مرتفع می‌سازد [۲]. در ادبیات شبکه‌های مبتنی بر نرم‌افزار، سطح داده‌ای شبکه به تجهیزاتی اطلاق می‌شود که عملیات هدایت بسته‌های اطلاعاتی را انجام می‌دهند. همچنین سطح کنترلی شبکه که عملیات مدیریتی نظیر مسیریابی، مهندسی ترافیک و اعمال سیاست‌های مدیریتی است را شامل می‌شود [۳ و ۴]. معمولاً در شبکه‌های مبتنی بر نرم‌افزار عملیات سطح کنترلی بر عهده کنترل کننده می‌باشد. در واقع، کنترل کننده شبکه بر اساس پیکربندی مدیر شبکه، به تجهیزات سطح داده‌ای فرمان می‌دهد که با بسته‌های اطلاعاتی چگونه برخورد نمایند و آن‌ها را چگونه هدایت کنند [۵]. در شکل (۱) معماری شبکه‌های مبتنی بر نرم‌افزار نشان داده شده است.



شکل ۱. معماری شبکه‌های مبتنی بر نرم‌افزار

بر اساس شکل (۱)، سطح داده‌ای شبکه شامل سوییچ‌هایی است که صرفاً عملیات هدایت بسته‌ها را انجام می‌دهند و فاقد هرگونه سازوکار کنترلی هستند. این سوییچ‌ها به کمک پروتکل‌های رابط جنوبی[4] با کنترل کننده در ارتباط هستند و قوانین مرتبط با هدایت بسته‌ها را از کنترل کننده دریافت می‌کنند.

پروتکل جریان باز[5] یکی از مهم‌ترین و کاربردی‌ترین پروتکل‌های رابط جنوبی است که امروزه استاندارد قالب اغلب شبکه‌های مبتنی بر نرم‌افزار است [۶ و ۷]. سوییچ‌های جریان باز دارای جدول‌هایی به نام جدول جریان[6] هستند که هر جدول دارای تعدادی مدخل[7] است که هر مدخل شامل قانون[8] و عمل[9] است. مقادیر این جدول‌ها توسط کنترل کننده پر می‌شود. هر قانون شامل تعدادی فیلد می‌باشد که مرتبط با سرآیند بسته‌های ورودی نظیر آدرس فیزیکی[10] مبدأ و مقصد، آدرس IP مبدأ و مقصد، شماره پورت و سایر فیلدهای ضروری است [۶]. هر عمل نیز تعیین می‌کند، با بسته‌ای که منطبق با فیلدهای بخش قانون است چه عملی انجام شود. این عملیات می‌تواند عملیاتی نظیر هدایت به یک پورت خاص از سوییچ، حذف بسته، هدایت بسته به تمام پورت‌ها و ... است. در صورتی که بسته ورودی به سوییچ دارای فیلدهای سرآیندی باشد که مقدار آن‌ها مطابق با مقدار تعیین شده در بخش قانون باشد، عمل در نظر گرفته شده برای آن بسته انجام می‌شود. در غیر این صورت، بسته مورد نظر به کنترل کننده ارسال می‌شود تا کسب تکلیف شده و کنترل کننده قانون و عمل مرتبط با بسته را به سوییچ‌های مرتبط ارسال نماید [۸].

منفک بودن سطح داده‌ای از سطح کنترلی سبب می‌شود تا یک مدیر شبکه بتواند به راحتی سیاست‌های مورد نظر خود را در قالب یک برنامه به کنترل کننده اعلام نموده و کنترل کننده نیز آن را به سطح داده‌ای اعلام کند. همچنین پیکربندی مجدد، خطایابی و آزمایش پروتکل‌ها و ایده‌های جدید نیز به کمک شبکه‌های مبتنی بر نرم‌افزار به راحتی قابل انجام است [۳]. علی‌رغم مزایای متعددی که شبکه‌های مبتنی بر نرم‌افزار دارند، این نوع معماری شبکه دارای برخی محدودیت‌ها و مشکلات از جمله مسائل امنیتی می‌باشند [۹]. یکی از مهم‌ترین حملات امنیتی در شبکه‌های مبتنی بر نرم‌افزار حمله بارکشی رایگان

[1] Software Defined Network
[2] Data Plane
[3] Control Plane

[4] SouthBand
[5] OpenFlow
[6] Flow Table
[7] Entry
[8] Rule
[9] Action
[10] MAC Address

می‌باشد که در آن یک کاربر بدخواه[1] می‌تواند به صورت پنهان از منابع شبکه اختصاص یافته به سایر کاربران استفاده کند و کنترل کننده شبکه متوجه این موضوع نشود [۱۰ و ۱۱]. در این مقاله تشریح کاملی از حمله بارکشی رایگان بیان خواهد شد و در ادامه یک روش مقابله کارآمد جهت تشخیص به موقع و جلوگیری از حمله ارائه می‌شود.

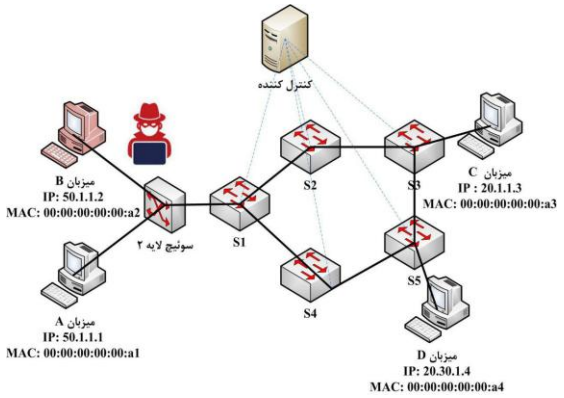
سایر بخش‌های این مقاله به این شرح می‌باشد: در بخش ۲، حمله بارکشی رایگان و کارهای ارائه شده قبلی مرتبط با آن ارائه می‌شود. در بخش ۳، روش پیشنهادی جهت مقابله با حمله تشریح خواهد شد. شبیه‌سازی و ارزیابی روش پیشنهادی در بخش ۴ مورد بحث قرار خواهند گرفت. بخش ۵ نیز به نتیجه‌گیری در رابطه با روش پیشنهادی اختصاص خواهد یافت.

۲. حمله بارکشی رایگان

در شبکه‌های مبتنی بر نرم‌افزار در صورتی که سوئیچ بسته‌ای را دریافت کند که هیچ قانونی برای آن بسته در جدول مدخل‌ها وجود نداشته باشد، سوئیچ آن بسته را به کنترل کننده ارسال می‌کند تا نحوه برخورد با آن بسته و بسته‌های مشابه آن را از کنترل کننده دریافت کند. این سازوکار باعث می‌شود تا کنترل کننده از بسته‌های جدید در شبکه که قانونی برای آن بر روی سوئیچ‌ها وجود ندارد باخبر شود. اما اگر یک کاربر بدخواه، بتواند از قوانین موجود بر روی سوئیچ‌ها با خبر شود و آدرس دیگر کاربران موجود در شبکه را جعل کند و بسته‌هایی با آدرس دیگر کاربران تولید کند، می‌تواند به صورت پنهان از شبکه استفاده کند.

حمله بارکشی رایگان حمله ایست که در آن یک کاربر بدخواه بدون آگاه شدن کنترل کننده می‌تواند به عنوان یک کاربر مجاز در شبکه وانمود کرده و از منابع شبکه استفاده کند. این حمله به تازگی توسط پارک و همکارانش [۱۰] به صورت خلاصه و بسیار جزئی مطرح شده است. در این مقاله حمله بارکشی رایگان به صورت مشروح معرفی شده و راه حل مناسبی جهت مقابله با آن ارائه می‌شود. لازمه انجام این حمله، دسترسی فیزیکی کاربر بدخواه به شبکه مبدأ است. این حمله می‌تواند در سطح لایه ۲ یا لایه ۳ شبکه انجام شود. از آنجا که جعل آدرس‌های IP مرسوم‌تر و راحت‌تر از جعل آدرس لایه کنترل دسترسی رسانه می‌باشد [۱۲]، در این مقاله نحوه عملکرد این حمله و روش مقابله با آن در سطح لایه ۳ بررسی می‌شود. به منظور بررسی دقیق‌تر جزئیات حمله بارکشی رایگان، این حمله در همبندی شکل (۲) تشریح می‌گردد.

[1] Malicious User



شکل ۲. همبندی نمونه جهت تشریح حمله بارکشی رایگان

در شکل (۲)، میزبان A کاربر مجاز شبکه و میزبان B یک کاربر بدخواه و میزبان‌های C و D نیز مقصد می‌باشند. کاربران A وB به یک سوئیچ معمولی لایه ۲ متصلند و در واقع در یک حوزه همه پخشی لایه ۲ قرار دارند. شبکه بستر نیز متشکل از سوئیچ‌های جریان بازی می‌باشد که تحت کنترل و مدیریت یک کنترل کننده قرار دارند و ترافیک موجود در شبکه را بر اساس قوانین ارسال شده توسط کنترل کننده هدایت می‌کنند. کنترل کننده مسیرهای مناسب بین میزبان‌ها را بر اساس سیاست‌های مدیر شبکه بر روی سوئیچ‌های موجود در طول مسیر نصب می‌کند. فرض کنید قوانین نصب شده بر روی سوئیچ S1 به صورت جدول (۱) باشد.

جدول ۱. قوانین هدایت بسته‌ها که روی سوئیچ S1 نصب شده‌اند

IN_PORT	SRC_MAC	DST_MAC	SRC_IP	DSP_IP	SRC_TCP	DST_TCP	ACTIONS
2	*	*	50.1.1.1	20.30.1.4	*	*	Output port 4
2	*	*	50.1.1.2	20.1.1.3	*	*	Output port 8
. . .							

در جدول (۱)، قانون اول مشخص می‌کند که کلیه بسته‌های دریافتی با آدرس ۵۰.۱.۱.۱ که از پورت فیزیکی شماره ۲ می‌آیند و به آدرس مقصد ۲۰.۳۰.۱.۴ می‌روند، باید به پورت فیزیکی شماره ۴ از سوئیچ S1 هدایت شوند. همچنین به طور مشابه، کلیه بسته‌هایی که از پورت فیزیکی شماره ۲ دریافت

می‌شوند و دارای آدرس مبدأ ۵۰.۱.۱.۲ و آدرس مقصد ۲۰.۱.۱.۳ هستند، باید به پورت فیزیکی شماره ۸ هدایت شوند.

در این شبکه، در صورتی که کاربر بدخواه B بخواهد ترافیکی را به سمت میزبان D ارسال کند، به علت این‌که قانونی برای این ارتباط در سوئیچ S1 وجود ندارد، اولین بسته ارسالی آن به محض رسیدن به S1، به کنترل کننده ارسال خواهد شد تا کسب تکلیف گردد. در این حالت کنترل کننده متوجه این درخواست خواهد شد و اقدامات تعیین شده توسط مدیر شبکه از قبیل بلاک نمودن کاربر B توسط کنترل کننده انجام خواهد شد. از آنجایی که کاربر A و B به یک سوئیچ لایه ۲ متصل هستند و در یک حوزه پخشی قرار دارند، کاربر B می‌تواند توسط ابزارها و دستوراتی مانند ping و traceroute از آدرس IP کاربر A و نیز با پایش ترافیک موجود در شبکه از قوانین نصب شده بر روی سوئیچ لبه با خبر شود. حال اگر کاربر B آدرس IP کاربر A را جعل کند و بسته‌هایی با آن آدرس تولید کند، می‌تواند با کاربر D ارتباط برقرار کند و اطلاعات خود را به سمت آن ارسال نماید. در این حالت بدیهی است که کنترل کننده از این ارتباط با خبر نخواهد شد.

یکی از عوارض انجام این حمله، این است که کاربر B می‌تواند با ارسال ترافیک حجیم و زائد باعث هدر رفت منابع شبکه و ایجاد ازدحام در شبکه بستر شود. حالت خطرناک‌تر این حمله، وضعیتی است که ارتباط بین کاربر B و کاربر D در این شبکه غیر مجاز باشد و کاربر B مجوز ارسال اطلاعات و برقراری ارتباط با کاربر D را نداشته باشد. در این وضعیت، در صورتی که مدیر شبکه، کنترل کننده را به نحوی پیکربندی نکرده باشد تا قوانینی برای منع این ارتباط بر روی سوئیچ‌ها نصب کند، کاربر B با انجام این حمله به راحتی می‌تواند ارتباط خود را با کاربر D برقرار کرده و عملیات تخریبی خود را انجام دهد.

لازم به ذکر است که علاوه بر همبندی شکل (۲)، این نوع حمله می‌تواند در شبکه‌های بی‌سیم که در آن دستگاه‌های بی‌سیم تحت پوشش یک access point قرار دارند و شبکه بستر نیز SDN است اتفاق بیفتد. به علت اشتراکی بودن کانال ارتباطی در شبکه‌های بی‌سیم، آگاهی از آدرس IP سایر کاربران و نیز جعل آن به مراتب از شبکه‌های سیمی راحت‌تر است.

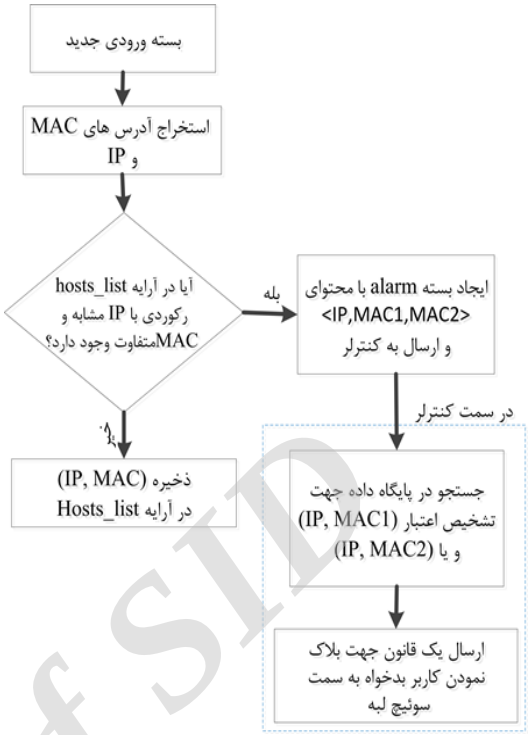
همان‌طور که مطرح شد، این حمله توسط پارک و همکارانش [۱۰] در سال ۲۰۱۶ مطرح شده است و حمله جدیدی است که در حوزه شبکه‌های مبتنی بر نرم‌افزار معرفی شده است. روش پیشنهادی آن‌ها جهت مقابله با این حمله روش مبتنی بر روش واترمارک است. این روش به این ترتیب است که کلیه بسته‌های ارسالی در ماشین فرستنده باید بر اساس یک کلید از قبل به توافق رسیده، یک رشته بیتی به نام واترمارک درون بسته‌ها قرار دهند و در واقع به این ترتیب بسته را امضاء کنند. در سمت گیرنده نیز کلیه بسته‌های دریافتی بررسی می‌شوند تا امضای مربوط به فرستنده اعتبارسنجی شود و در صورت معتبر بودن، بسته‌ها تحویل برنامه کاربردی شوند. علی‌رغم این که این روش یک راه حل برای مقابله با حمله بارکشی رایگان است، دارای نقاط ضعف زیر می‌باشد:

- قرار دادن واترمارک درون هر بسته باعث طولانی‌تر شدن بسته ارسالی می‌شود و در صورت ارسال ترافیک زیاد در شبکه، سربار ارتباطی به وجود می‌آید.
- نیاز به پردازش اضافی در ماشین مبدأ جهت قرار دادن واترمارک و در ماشین مقصد جهت استخراج و بررسی اعتبار واترمارک وجود دارد.
- نیاز به تغییر برنامه سمت فرستنده و گیرنده جهت پشتیبانی از سازوکار واترمارک دارد.
- مدیر شبکه باید برای هر میزبان یک کلید اختصاص دهد و نیاز به مدیریت کلیدها می‌باشد.
- روش واترمارک در سطح لایه ۷ یا لایه کاربرد پیاده‌سازی می‌شود و در صورتی که حمله بارکشی رایگان در لایه‌های پایین‌تر انجام شود، این روش نمی‌تواند با حمله مقابله کند. به عنوان مثال در صورتی که داده‌ها در لایه سوم تولید شوند و در سطح لایه سوم ارسال شوند (مانند پیام‌های مبادله شده برای مسیریابی)، به دلیل عدم وجود واترمارک در بسته‌ها، کاربر بدخواه می‌تواند ترافیک خود را در شبکه ارسال نماید و این روش قادر به تشخیص و پیشگیری از آن نیست.

در بخش ۳، روش پیشنهادی مناسبی جهت مقابله با حمله بارکشی رایگان ارائه می‌شود که نقاط ضعف فوق را تا حد بسیار زیادی کاهش می‌دهد و به طور مؤثری حملات بارکشی رایگان را شناسایی و متوقف می‌کند.

۳. روش پیشنهادی

همان‌طور که در بخش ۲ اشاره شد، به علت مرسوم‌تر و راحت‌تر بودن جعل آدرس IP نسبت به آدرس فیزیکی، در این مقاله روش پیشنهادی جهت مقابله با حمله بارکشی رایگان در لایه ۳ شبکه ارائه می‌شود. در روش پیشنهادی، دو مؤلفه متفاوت جهت کشف و جلوگیری از حمله وجود دارد که یکی از آن‌ها برای تشخیص بر روی سوییچ‌های لبه شبکه بستر پیاده‌سازی می‌شود و مؤلفه دیگر که جهت مقابله است، بر روی کنترل کننده پیاده‌سازی می‌شود. در شکل (۳)، روش پیشنهادی در قالب یک روندنما نشان داده شده است.



شکل ۳. روندنمای روش پیشنهادی (موارد موجود در کادر خط چین، در کنترل کننده اجرا می‌شوند)

مطابق شکل (۳)، یک سوئیچ لبه به محض دریافت یک بسته ورودی قبل از جستجو در جدول مدخل‌ها جهت یافتن قانون و عمل متناظر با بسته ورودی، ابتدا آدرس مبدأ IP و فیزیکی بسته را استخراج می‌کند. مؤلفه پیشنهادی یک آرایه موسوم به hosts_list برای ذخیره جفت آدرس (IP, MAC) میزبان‌ها دارد که در صورت دریافت و استخراج این دو فیلد از بسته ورودی، آن‌ها را درون این آرایه جستجو می‌کند. جفت آدرس (IP, MAC) در صورتی درون این آرایه ذخیره می‌شوند که تکراری نباشند. حال اگر مؤلفه موجود در سوئیچ بسته‌ای را دریافت کند که آدرس IP آن با آدرس IP ذخیره شده در آرایه یکی باشد و آدرس فیزیکی آن متفاوت باشد، مشخص می‌شود که در شبکه ماشینی وجود دارد که دارای آدرس IP جعلی است. در این صورت، مؤلفه موجود بر روی سوئیچ، یک بسته alarm تولید و مقادیر (IP, MAC2, MAC1) را برای کنترل کننده ارسال می‌کند. آدرس MAC1 و MAC2 همان دو آدرس متفاوت هستند.

در کنترل کننده نیز مؤلفه دیگری پیاده‌سازی می‌شود که به محض دریافت بسته alarm، محتوای آن را استخراج می‌کند. آدرس MAC و IP تمامی میزبان‌های شبکه در هنگام اتصال میزبان‌ها به شبکه در این پایگاه داده قرار می‌گیرد. حال، کنترل کننده مقادیر موجود در بسته alarm را در این پایگاه داده جستجو می‌کند تا مشخص شود که میزبانی با آدرس (MAC1, IP) نامعتبر است یا میزبانی با آدرس (MAC2, IP). در صورت تشخیص نامعتبر بودن هر میزبان، بلافاصله کنترل کننده یک قانون برای بلاک نمودن میزبانی که از آدرس IP جعلی استفاده کرده است به سمت سوئیچ لبه می‌فرستد تا از این پس ترافیک مربوط به کاربر بدخواه بلاک شود.

جهت روشن‌تر شدن موضوع، مثالی از حمله بارکشی رایگان و سازوکار کشف و مقابله آن بر روی همبندی شکل (۲)، ارائه می‌شود. فرض کنید در همبندی شکل (۲)، میزبان A بسته‌ای را به سمت میزبان D ارسال می‌کند. این بسته هنگام رسیدن به سوئیچ S1، ابتدا آدرس IP, MAC مبدأ آن استخراج می‌شود و به علت این که آرایه hosts_list تهی است، در این آرایه ذخیره می‌شود. بسته‌هایی که از میزبان B به سمت میزبان C می‌روند نیز توسط مؤلفه پیشنهادی بررسی شده و آدرس‌های IP, MAC مبدأ آن‌ها استخراج و در آرایه ذخیره می‌شود. در این لحظه مقدار آرایه به صورت جدول (۲) خواهد بود.

جدول ۲. محتوای آرایه hosts_list در یک مثال فرضی

IP	MAC
50.1.1.1	00:00:00:00:00:a1
50.1.1.2	00:00:00:00:00:a2

حال فرض کنید کاربر B قصد انجام حمله را دارد. بنابراین، آدرس IP میزبان A را جعل کرده و به جای استفاده از آدرس واقعی خود، از آدرس میزبان A برای ارسال اطلاعات به سمت میزبان D استفاده می‌کند. اولین بسته ارسالی به سوئیچ S1 می‌رسد و مؤلفه پیشنهادی، آدرس IP, MAC مبدأ یعنی فیلدهای 50.1.1.1 و 00:00:00:00:00:a2 را استخراج می‌کند و آن‌ها را در آرایه جستجو می‌کند. هنگام جستجو در آرایه، مشخص می‌شود که قبلاً آدرس IP=50.1.1.1 در آرایه با آدرس فیزیکی متفاوتی ثبت شده است و بنابراین یک تناقض وجود دارد. لازم به ذکر است که در این مرحله، خود سوئیچ نمی‌تواند تشخیص دهد کدام یک از کاربران دارند از آدرس جعلی استفاده می‌کنند. بنابراین نیاز است تا سوئیچ، یک بسته alarm را به کنترل کننده بفرستد تا کنترل کننده بتواند کاربر بدخواه را شناسایی کرده و آن را مسدود کند. بر همین اساس، بلافاصله سوئیچ S1، یک بسته alarm ایجاد نموده و مقادیر (50.1.1.1, 00:00:00:00:00:a1, 00:00:00:00:00:a2) را در آن قرار می‌دهد و به سمت کنترل کننده ارسال می‌کند. در روش پیشنهادی، در کنترل کننده مؤلفه دیگری پیاده‌سازی شده است که با دریافت alarm درون پایگاه داده جستجو می‌کند که تا میزان اعتبار (50.1.1.1, 00:00:00:00:00:a1) یا (50.1.1.1, 000:00:00:00:00:a2) بسنجد. از آنجا که آدرس فیزیکی با آدرس IP=50.1.1.1 در

ابتدای کار مربوط به میزبان A بوده است، بنابراین، میزبان B به عنوان میزبان بدخواه شناخته می‌شود. در این حالت، مؤلفه پیشنهادی در کنترل کننده، یک قانون برای سوئیچ S1 ارسال می‌کند تا کلیه بسته‌های ورودی از سمت میزبان B که دارای آدرس MAC=000:00:00:00:00:a2 هستند بلاک شوند.

روش پیشنهادی در این مقاله بر خلاف روش واترمارک نیازی به تغییر برنامه کاربر انتهایی ندارد. همچنین به علت اینکه در سطح لایه ۳ عملیات تشخیص حمله را انجام می‌دهد، محدود به لایه کاربرد نبوده و حملات بارکشی رایگان مرتبط با لایه‌های شبکه و انتقال را نیز تشخیص می‌دهد. از آنجا که در یک شبکه بستر، معمولاً کاربران شبکه به سوئیچ‌های لبه متصل هستند، تنها کافی است تا مؤلفه پیشنهادی را در سوئیچ‌های لبه فعال نمود تا کارآیی شبکه تحت تأثیر قرار نگیرد.

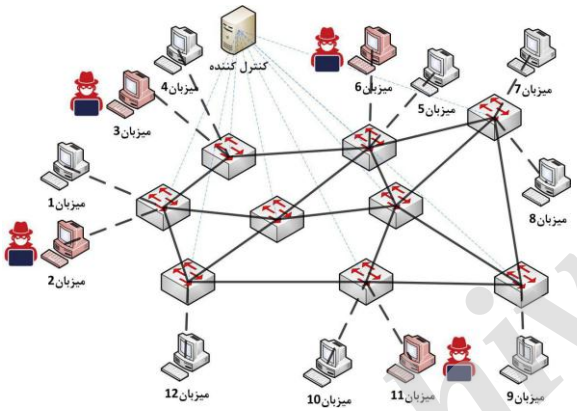
در مواردی که در شبکه حمله بارکشی رایگان وجود ندارد، بسته‌های دریافتی به محض ورود به سوئیچ لبه توسط مؤلفه تشخیص حمله بررسی می‌گردند و به علت عدم وجود حمله، به پروتکل جریان باز تعبیه شده در سوئیچ تحویل داده می‌شوند، تا پردازش بسته‌ها بر اساس این پروتکل انجام پذیرد. در این حالت در صورت وجود مسیر، بسته‌ها از طریق مسیر هدایت می‌شوند. همچنین، در صورتی که مسیری برای بسته‌ها وجود نداشته باشد، سوئیچ برای دریافت مسیر برای بسته‌ها از کنترل کننده کسب تکلیف می‌کند.

۴. شبیه‌سازی و ارزیابی کارایی

در این بخش، جزئیات شبیه‌سازی و پیاده‌سازی و معیارهای مناسب جهت ارزیابی کارایی روش پیشنهادی ارائه می‌شود. همان‌طور که در بخش ۲ اشاره شد، روش پیشنهادی شامل دو مؤلفه مجزا از هم می‌باشد که یکی از آن‌ها در کنترل کننده و دیگری بر روی سوئیچ جریان باز پیاده‌سازی می‌شود. در این مقاله، از کنترل کننده OpenDayLight به منظور کنترل شبکه استفاده می‌شود. این کنترل کننده به عنوان یک کنترل کننده متن باز و محبوب شناخته می‌شود و دارای قابلیت‌ها و امکانات متعددی است که برای پیاده‌سازی اغلب شبکه‌های مبتنی بر نرم‌افزار کفایت می‌کند [۱۳].

در روش پیشنهادی، مؤلفه‌ای که قرار است بر روی کنترل کننده OpenDayLight پیاده‌سازی شود، در قالب یک برنامه جاوا نوشته می‌شود و به عنوان یک باندل، به کنترل کننده اضافه می‌شود. این کنترل کننده پس از دریافت بسته alarm (که توسط مؤلفه پیاده‌سازی شده بر روی سوئیچ ارسال می‌شود)، باندل مربوط به مؤلفه را فراخوانی و اجرا می‌کند. همچنین، مؤلفه مربوط به سوئیچ نیز با استفاده از زبان سی پلاس پلاس بر روی کد مرجع مربوط به سوئیچ جریان باز پیاده‌سازی می‌شود. لازم به ذکر است که این مؤلفه فقط بر روی سوئیچ‌های لبه در شبکه بستر فعال می‌شود تا کارایی شبکه کاهش پیدا نکند.

به منظور ایجاد و شبیه‌سازی همبندی شبکه نیز از شبیه‌ساز مینی نِت استفاده می‌شود. این شبیه‌ساز، می‌تواند همبندی‌هایی با تعداد سوئیچ و میزبان دلخواه ایجاد نماید. سوئیچ‌های ایجاد شده توسط مینی نِت می‌توانند با کنترل کننده در ارتباط باشند و قوانین هدایت بسته‌ها را دریافت نمایند. جهت ایجاد همبندی دلخواه در مینی نِت، همبندی مورد نظر در قالب دستورات زبان پایتون به این شبیه‌ساز داده می‌شود و این شبیه‌ساز همبندی مورد نظر را ایجاد و سوئیچ‌ها را به کنترل کننده متصل می‌کند. همبندی در نظر گرفته شده برای ارزیابی روش پیشنهادی در شکل (۴) نشان داده شده است.

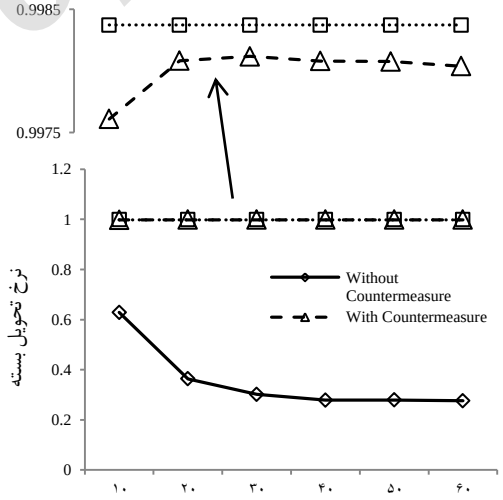


شکل ۴. همبندی مورد شبیه‌سازی

مطابق شکل (۴)، شبکه بستر شامل ۹ سوئیچ جریان باز می‌باشد که مؤلفه تشخیص حمله در سوئیچ‌های لبه فعال شده‌اند. پهنای باند تمامی پیوندها برابر ۱۰۰ مگابیت در ثانیه است و میزان تأخیر انتشار هر پیوند ۵ میلی ثانیه در نظر گرفته شده است. به منظور بررسی دقیق‌تر حمله بارکشی رایگان و همچنین روش پیشنهادی، کاربران بدخواه و مجاز در همبندی شکل (۴) به صورت توزیع شده قرار گرفته‌اند. در این همبندی میزبانی‌های ۱، ۴، ۵ و ۱۰ به ترتیب به میزبان‌های ۷، ۸، ۹ و ۱۲ ترافیک UDP با نرخ ۴ مگابیت در ثانیه ارسال می‌کنند. همچنین میزبان‌های ۲، ۳، ۶ و ۱۱ میزبان‌های بدخواهی هستند که به ترتیب بعد از ثانیه ۲۰،۴۰، ۶۰ و ۸۰ شروع به جعل آدرس میزبان‌های همسایه خود کرده و ترافیک UDP اضافی و زائدی را به شبکه بستر ارسال می‌کنند. ترافیک UDP ارسالی توسط میزبان‌های بدخواه بسته‌های ۱۰۰۰ بایتی با نرخ‌های متفاوت است. در این مقاله از ابزار hping جهت جعل آدرس و ارسال ترافیک کاربران بدخواه استفاده شده است. کل زمان شبیه‌سازی

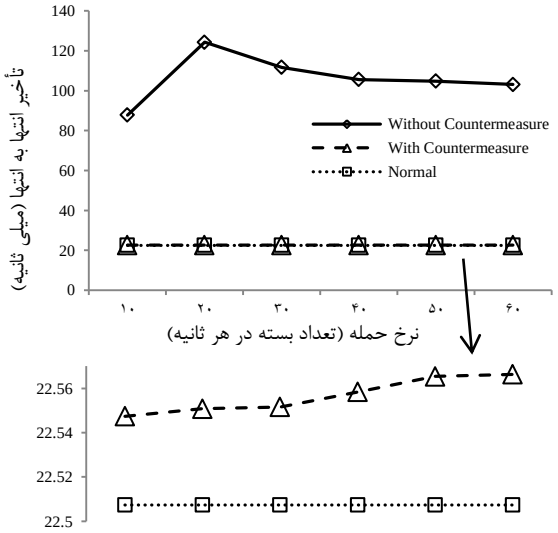
۳۰۰ ثانیه است و نتایج شبیه‌سازی برای سه حالت عادی یا بدون حمله، حالت وجود حمله بدون استفاده از روش پیشنهادی و حالت وجود حمله با استفاده از روش پیشنهادی مورد ارزیابی قرار خواهند گرفت.

شکل (۵) نمودار نرخ تحویل بسته را به ازای نرخ‌های متفاوت حمله نشان می‌دهد. همان‌طور که در این شکل ملاحظه می‌شود، با افزایش نرخ حملات توسط کاربران بدخواه، میزان نرخ تحویل بسته به شدت کاهش می‌یابد. دلیل این امر نیز، ایجاد ازدحام در شبکه به علت ترافیک زائد است که باعث سرریز شدن بافر سوئیچ‌ها و درنهایت افزایش نرخ اتلاف بسته خواهد شد. به علت نزدیک بودن نتایج در حالت عادی و نیز حالتی که از روش پیشنهادی استفاده می‌شود، مقایسه نتایج مربوط به این دو مورد در حالت بزرگ‌تر نمایش داده شده است. همان‌طور که ملاحظه می‌شود، استفاده از روش پیشنهادی تأثیر بسیار جزئی و کمی بر روی نرخ تحویل بسته دارد و اختلاف نتایج در حالتی که از روش پیشنهادی استفاده می‌شود با حالت عادی در حدود ۰/۰۰۱ می‌باشد که این مقدار ناچیز، میزان اتلاف بسته‌ای است که از زمان شروع حمله تا تشخیص آن در شبکه اتفاق می‌افتد.



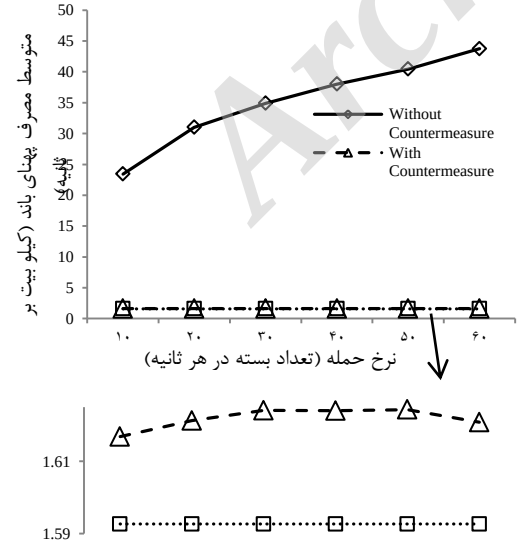
شکل ۵. میزان نرخ تحویل بسته در مقابل نرخ حمله

شکل (۶)، میزان تأخیر انتها به انتهای بسته‌های اطلاعاتی مربوط به کاربران مجاز را نشان می‌دهد. مطابق این شکل، واضح است که ارسال ترافیک زائد توسط کاربران بدخواه سبب افزایش میزان تأخیر برای ترافیک مجاز است. دلیل این امر نیز بروز ازدحام در پیوندهای شبکه و در نتیجه تأخیر طولانی است. همچنین قسمت دوم شکل (۶) نشان می‌دهد که به کارگیری روش پیشنهادی، میزان تأخیر انتها به انتها را چندان تحت تأثیر قرار نمی‌دهد و میزان اختلاف در تأخیر انتها به انتها در روش پیشنهادی و حالت عادی در حدود ۰/۰۵ میلی ثانیه است.



شکل ۶. میانگین تأخیر انتها به انتها در مقابل نرخ‌های متفاوت حمله

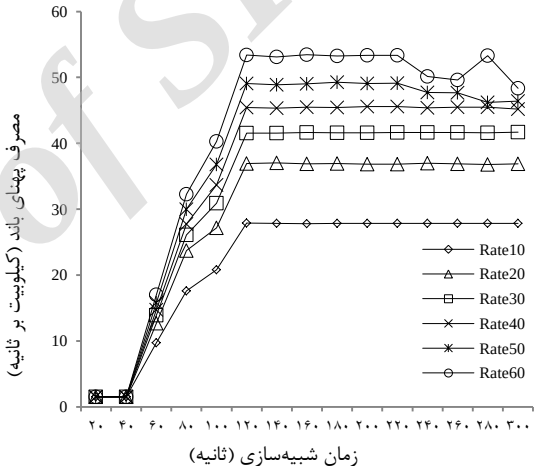
شکل (۷) نمودار مربوط به میانگین پهنای باند استفاده شده به ازای نرخ‌های مختلف حمله را نشان می‌دهد. جعل آدرس و ارسال ترافیک زائد بدون آگاه شدن کنترل کننده باعث شده است تا میانگین پهنای باند استفاده شده در نمودار مربوط به حمله در شکل (۷) افزایش بسیار زیادی در مقایسه با حالت بدون حمله داشته باشد. همچنین شکل (۷) نشان می‌دهد که استفاده از روش پیشنهادی تأثیر بسیار زیادی در کنترل حمله دارد و مانع از اشغال شدن پیوندهای شبکه توسط ترافیک زائد ارسالی توسط کاربران بدخواه می‌شود.



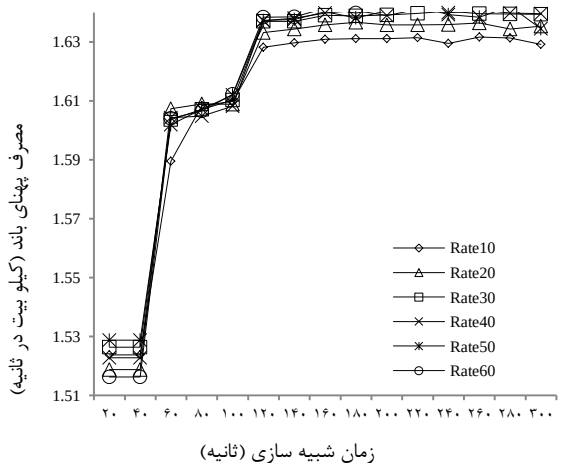
شکل ۷. میانگین پهنای باند مصرفی در مقابل نرخ‌های متفاوت حمله

شکل‌های (۸) و (۹) جهت بررسی دقیق‌تر تأثیر حمله بارکشی

رایگان بر روی پهنای باند مصرفی شبکه و کارایی روش مقابله پیشنهادی ارائه شده‌اند. این دو شکل به خوبی اثر استفاده از روش پیشنهادی را نشان می‌دهد. در شکل (۸)، واضح است که به دلیل عدم استفاده از سازوکار مقابله، میزان پهنای باند استفاده شده در شبکه به ازای نرخ‌های متفاوت حمله افزایش چشمگیری دارد و به مقدار ۴۵ کیلو بیت بر ثانیه نیز می‌رسد. بر خلاف شکل (۸)، همان‌طور که در شکل (۹) مشاهده می‌شود، استفاده از روش مقابله پیشنهادی باعث شده است تا میزان پهنای باند استفاده شده در شبکه تفاوت بسیار جزئی با حالت عادی و بدون حمله داشته باشد. شکل (۹) نشان می‌دهد که روش پیشنهادی به خوبی از حمله بارکشی رایگان جلوگیری می‌کند و اختلاف پهنای باند مصرفی با حالت عادی و بدون حمله در حدود ۰/۱۲ کیلو بیت است.



شکل ۸. پهنای باند مصرفی در حالت بدون استفاده از روش مقابله پیشنهادی



شکل ۹. پهنای باند مصرفی در حالت استفاده از روش مقابله پیشنهادی

۵. نتیجه‌گیری

در این مقاله یکی از حمله‌های مهم و تأثیرگذار در شبکه‌های مبتنی بر نرم‌افزار موسوم به حمله بارکشی رایگان مورد بررسی و ارزیابی قرار گرفت. همچنین یک روش پیشنهادی مؤثر به منظور تشخیص و جلوگیری از حمله بارکشی رایگان ارائه شد. روش پیشنهادی دارای دو مؤلفه تشخیص و جلوگیری است که به ترتیب بر روی سوئیچ‌های جریان باز و کنترل کننده پیاده‌سازی می‌شوند. پیاده‌سازی روش پیشنهادی بر روی سوئیچ‌ها و کنترل کننده امکان تشخیص زود هنگام حمله و نیز مقابله به موقع و کارآمد با کاربران بدخواه را فراهم می‌آورد. در این مقاله، شبیه‌سازی جامعی جهت ارزیابی روش پیشنهادی انجام شده است. نتایج حاصل از شبیه‌سازی نشان می‌دهد که استفاده از روش پیشنهادی به طور مؤثری از حمله بارکشی رایگان جلوگیری می‌کند و تأثیر منفی در کاهش کارایی شبکه نخواهد داشت. علی‌رغم مزیت طرح پیشنهادی بر روش‌های پیشین، کماکان این روش قادر به تشخیص حمله بارکشی رایگان در مواردی که کاربر مهاجم به طور هم‌زمان از آدرس MAC و IP جعلی استفاده کند، نمی‌باشد. از آنجا که در حمله بارکشی رایگان، کاربر مهاجم ترافیک خود را با استفاده از مسیری که به کاربر مجاز متعلق است می‌فرستد، به‌کارگیری روش‌های مبتنی یادگیری ماشین جهت پایش و تحلیل الگوی ترافیک در سوئیچ‌های لبه می‌تواند به تشخیص این نوع حمله منجر شود. بر همین اساس، این ایده به عنوان راه کار آتی می‌تواند در جهت تشخیص این نوع حمله به کار گرفته شود.

۶. مراجع

[1] Benson, T.; Akella, A.; Maltz, D. A. "Unraveling the Complexity of Network Management"; NSDI 2009, 335-348.

[2] Parsaei, M. R.; Mohammadi, R.; Javidan, R. "A New Adaptive Traffic Engineering Method for Telesurgery using ACO Algorithm over Software Defined Networks"; European Research in Telemedicine 2017, 6, 3-4, 173-180.

[3] Parsaei, M. R.; Khalilian, S. H.; Javidan, R. "A Comparative Study on Fault Tolerance Methods in IP Networks versus Software Defined Networks"; International Academic Journal of Science and Engineering 2016, 3, 4, 146-154.

[4] McKeown, N. "Software-Defined Networking"; INFOCOM Keynote Talk 2009, 17, 2, 30-32.

[5] Rowshanrad, S.; Parsaei, M. R.; Keshtgari, M. "Implementing NDN using SDN: A Review on Methods and Applications"; IIUM Engineering Journal 2016, 17, 2, 11-20.

[6] McKeown, N.; Anderson, T.; Balakrishnan, H.; Parulkar, G.; Peterson, L.; Rexford, J.; Turner, J. "Openflow: Enabling Innovation in Campus Networks"; ACM SIGCOMM Computer Communication Review 2008, 38, 2, 69-74.

[7] Openflow Switch Specification. Avaible https://www.opennetworking.org/images/stories/downloads/specification/openflow-spec-v1, 3. 2012.

[8] Naous, J.; Erickson, D.; Covington, G. A.; Appenzeller, G.; McKeown, N. "Implementing an Openflow switch on the NetFPGA platform"; Proc. of the 4th ACM/IEEE Symposium on Architectures for Networking and Communications Systems 2008, 1-9.

[9] Kreutz, D.; Ramos, F.; Verissimo, P. "Towards Secure and Dependable Software-Defined Networks"; Proc. of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking 2013, 55-60.

[10] Park, Y.; Chang, S. Y.; Krishnamurthy, L. M. "Watermarking for Detecting Freeloader Misbehavior in Software-Defined Networks"; Int. Conf. on Computing, Networking and Communications 2016, 1-6.

[11] Shirazi, H.; Jamalyfard, A.; Farshchi, S. M. R. "Detection of Attacks against Web Applications Using Combination of One-Class Classifiers"; Advanced Defence Sci. & Tech. 2014, 5, 107-119 (In Persian).

[12] Fichera, S.; Galluccio, L.; Grancagnolo, S. C.; Morabito, G.; Palazzo, S. "OPERETTA: An Openflow-Based Remedy to Mitigate TCP SYNFLOOD Attacks against Web Servers"; Computer Networks 2015, 92, 89-100.

[13] Medved, J.; Varga, R.; Tkacik, A.; Gray, K. "Opendaylight: Towards a Model-Driven sdn Controller Architecture"; Proc. of IEEE Int. Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, 1-6.