KNO-1002-4006

ارزیابی امنیت شبکه نرم افزار محور SDN

شهرام محمدی

Shahram_mohamadi1@yahoo.com

مربی گروه مهندسی کامپیوتر، دانشگاه فنی و حرفه ای دختران اصفهان، اصفهان ، ایران

چکیده

کشش شبکه نرم افزار محور (SDN)، مغناطیسی است. تعداد کمی در جامعه شبکه وجود دارد که از تاثیر رها شده اند. از آنجایی که مزایای قابلیت دید شبکه و قابلیت برنامه نویسی دستگاه شبکه، مورد بحث قرار می گیرد، ممکن است این سوال راجع به این مساله مطرح شود که چه کسی دقیقا بهره خواهد برد؟ آیا آن اپراتور شبکه خواهد بود یا در واقع مخل شبکه خواهد بود؟ همانطور که دستگاه های شبکه نرم افزار محور SDN و سیستم ها به بازار ضربه وارد میکنند، امنیت در شبکه نرم افزار محور SDN باید در این دستور جلسه، بالا رود. این مقاله یک بررسی جامع از تحقیقات مربوط به امنیت را در شبکه نرم افزار محور SDN ارائه میدهد که تا این تاریخ صورت گرفته است. هر دو ارتقاء امنیتی مشتق شده از استفاده از شبکه نرم افزار محور SDN و چالشهای امنیتی مطرح شده توسط شبکه مورد بحث قرار میگیرد. با دسته بندی کار موجود، یک مجموعه از نتیجه گیری ها و پروپوزالها برای رهنمود های تحقیقاتی آینده ارائه میشوند.

واژگان کلیدی : ارزیابی، امنیت شبکه، نرم افزار ، SDN

1. مقدمه

شبکه نرم افزار محور SDN با دستگاه های فعال شده با SDN در توسعه و تولید، به سرعت از دیداری به واقعیت سوق می یابد. ترکیب کنترل تفکیک شده و قابلیت عملکرد سطح داده و قابلیت برنامه نویسی در شبکه که از دیرباز در دنیای تحقیقات مورد بحث قرار داشته است، در فناوری های رایانش ابری و مجازی سازی، کاربرد تجاری خود را یافته است.

مزایای شبکه نرم افزار محور SDN در سناریوهای مختلف (مثلا، سرمایه گذاری، دیتاسنتر و غیره) و در سرتاسر شبکه های اصلی مختلف از قبل اثبات شده اند مثلا Google B4 [1]. با این حال، چالشهایی برای اجرای شبکه حامل مقیاس کامل شبکه نرم افزار محور SDN وجود دارد. شماری از این چالشها در [2] ارائه شده اند. یک حوزه اصلی که به تازگی جلب توجه که سزاوارش است را آغاز کرده است، حوزه امنیت در شبکه نرم افزار محور SDN است.

معماری شبکه نرم افزار محور SDN، می تواند ارتقاء امنیت شبکه را با تامین نظارت امنیت به شدت انفعالی، تحلیل و سیستم پاسخ بکار ببرد. تحلیل ترافیک یا روش های کشف نابهنجاری گسترش یافته در شبکه، داده های مربوط به امنیت را گسترش داد که می تواند به طور منظم به کنترل کننده مرکزی منتقل گردد. برنامه های کاربردی میتوانند در کنترل کننده برای تحلیل و همبستگی این بازخورد از شبکه کامل اجرا شوند. بر مبنای این تحلیل، سیاست امنیتی بروز می تواند در کل شبکه به شکل قواعد جریان انتشار یابد. این رویکرد یکپارچه می تواند به طرز کارآمدی کنترل و محدودیت تهدیدهای امنیتی شبکه را تسریع کند.

در عین حال، صفات مشابه کنترل متمرکز و قابلیت برنامه نویسی وابسته به پایگاه شبکه نرم افزار محور SDN، چالشهای امنیتی شبکه را مطرح میکند. یک پتانسیل مضاعف برای حملات منع سرویس (DoS) به خاطر کنترل کننده متمرکز و محدودیت flow-table در دستگاه های شبکه، یک نمونه اولیه است. مساله نگران کننده دیگر بر مبنای قابلیت برنامه نویسی آزاد شبکه، اعتماد است؛ هم بین برنامه های کاربردی و کنترل کننده ها و هم بین کنترل کننده ها و دستگاه های شبکه.

شماری از راه حلها برای این چالشهای امنیتی شبکه نرم افزار محور SDN، در آثار ارائه شده اند. این راه حل ها در طیف طرح های تکرار کنترل کننده از طریق حل تعارض سیاست گرفته تا مکانیسم های تایید سندیت را در بر میگیرد. به طور مشابه، شماری از پروپوزالها برای بکارگیری چارچوب شبکه نرم افزار محور SDN برای امنیت شبکه ی ارتقا یافته صورت گرفته اند.

تحلیلی از چالش های امنیتی، در این مقاله ارائه شده اند. مسائل امنیت فردی طبق لایه SDN تحت تاثیر یا هدف گیری شده، دسته بندی میشوند. راه حل های ارائه شده و پدید آمده برای این چالشها بعد مورد بحث قرار میگیرند و دسته بندی میشوند. شرایط لازم برای کار بیشتر برای ایجاد یک شبکه نرم افزار محور SDN امن و قوی، به طور واضح از شکاف بین مسائل و تحقیقات موجود، شناسایی شده است. بدون افزایش عمده در تمرکز بر امنیت برای شبکه نرم افزار محور SDN حمایت از قابلیت در حال تکامل وابسته به عنوان مثال مجازی سازی عملکرد شبکه (NFV)، ممکن نخواهد بود.

2. تحلیل امنیت شبکه نرم افزار محور SDN

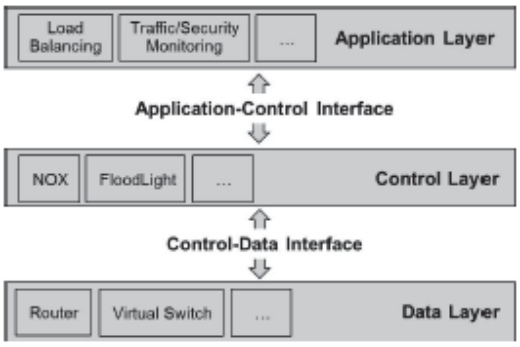
ویژگی های اصلی یک شبکه ارتباطات امن، عبارتند از: قابلیت اعتماد، بی نقصی، دسترسی اطلاعات، تایید سندیت و عدم رد. به منظور ارائه یک شبکه حفاظت شده از حمله بد اندیشانه یا آسیب غیر عمدی، کارشناسان امنیتی باید داده ها، دارایی های شبکه (مثلا دستگاه ها) و تراکنشهای ارتباطات سرتاسر شبکه را حفظ کنند. تغییرات در معماری شبکه که توسط شبکه نرم افزار محور SDN مطرح شده اند، باید برای تضمین حفظ امنیت شبکه، ارزیابی شوند.

در یک تکرار زود هنگام آنچه امروز به عنوان شبکه نرم افزار محور شبکه نرم افزار محور SDN شناخته شده است، کاسادو و همکارانش، به طور ویژه ابعاد امنیتی کنترل مجزا و شبکه ارسال را بررسی کردند. معماری SANE آنها که در سال 2006 ارائه شده است بر یک کنترل کننده متمرکز منطقی مسئول تایید هویت هاست ها و اجرای سیاست، متمرکز است. در زمان ارائه آن، این مساله به عنوان یک رویکرد افراطی قلمداد میشد که به تغییر ریشه ای در زیر ساخت شبکه سازی و هاست های نهایی نیاز دارد که می تواند برای برخی سرمایه گذاری ها محدود کننده باشد.

اتان [6] اثر SANE را توسعه داده اما از یک رویکرد استفاده کرد که به تغییر کمتری برای شبکه اصلی نیاز داشت. این رویکرد شبکه را از طریق استفاده از دو مولفه کنترل می کرد؛ یک کنترل کننده متمرکز مسئول اعمال سیاست جهانی و راه گزینی های اتان

که به سادگی بسته های مبتنی بر قوانین در یک جدول جریان را ارسال کرد. این کنترل شبکه ساده شده، به داده ها اجازه داد و سطحی را کنترل کرد که برای بررسی قابلیت برنامه نویسی، تفکیک شد. گرچه معماری اتان، به ما یک دیدگاه دقیق تر از آنچه شبکه نرم افزار محور SDN و OpenFlow به آن تبدیل خواهد شد، ارائه داد، اما دچار شماری از کمبودها است. یکی از اینها، این واقعیت است که ترافیک برنامه کاربردی میتواند به شناخت سیاست شبکه برسد. در معماری شبکه نرم افزار محور شبکه نرم افزار محور SDN امروز برنامه های کاربردی برای تامین خدمات گوناگون بکار می روند، برای نمونه با مجازی سازی عملکرد شبکه (NFV) شناخت برنامه های کاربردی احتمالا می تواند در شبکه کلی شکاف ایجاد کند.

با بررسی مسائل ویژه با امنیت در شبکه نرم افزار محور SDN از چشم انداز چارچوب شبکه نرم افزار محور SDN (شکل 1)، ما چالشهای وابسته به هر لایه از شبکه را شناسایی میکنیم: برنامه کاربردی، کنترل و سطوح داده و در فواصل زمانی بین این لایه ها.



شکل 1. معماری کارکردی SDN، لایه های داده، کنترل و برنامه کاربردی و واسط ها را نشان میدهد.

شماری از تحلیلهای امنیتی اخیرا صورت گرفته اند که پی برده اند عناصر تغییر یافته یا رابطه بین عناصر در چارچوب شبکه نرم افزار محور SDN، آسیب پذیری های جدیدی را مطرح میکنند که قبل از

شبکه نرم افزار محور SDN وجود نداشتند. چنین مقاله ای، تحلیل پروتکل OpenFlow را با استفاده از متدولوژی تحلیل تهدید STRIDE تکمیل میکند. این مقاله بر اجرای افشای اطلاعات و حملات منع سرویس DoS تمرکز دارد که نویسنده مشخص کرده است برای اجرای موفق امکان پذیر بوده اند. گرچه شماری از روش های کاهش، ارائه میشوند اما این تکنیک ها در این اثر، اثبات شده اند.

مشخصات راه گزینی OpenFlow، استفاده از امنیت لایه انتقال (TLS) با تایید هویت بین کنترل کننده ها و راه گزینی های آنها را توصیف میکند. در عین حال ویژگی امنیت، اختیاری است و استاندارد امنیت لایه انتقال (TLS) مشخص نیست. عدم پذیرش TLS توسط فروشندگان بزرگ و امکان حملات منع سرویس DoS مورد تمرکز یک ارزیابی آسیب پذیری OpenFlow قرار دارد. مولفین پی برده اند کمبود استفاده از TLS میتواند منجر به اثبات قانون کلاهبرداری شود.

در [11] کروتز و همکارانش یک تحلیل سطح بالا را از امنیت کلی شبکه نرم افزار محور SDN ارائه می دهند. آنها نتیجه گیری میکنند به خاطر ماهیت کنترل کننده متمرکز و قابلیت برنامه نویسی شبکه، تهدیدهای جدیدی مطرح میشوند که به پاسخهای سریع نیاز دارند. آنها شماری از روش ها را برای بررسی تهدیدهای مختلف از جمله تکرار، تنوع و مولفه های امن ارائه می کنند.

نهایتا، شبکه تحقیقاتی و بستر آزمون، ProtoGENI، مورد تحلیل قرار گرفته است. مولفین کشف کرده اند، حملات بیشماری بین کاربران بستر آزمون، در طول انتشار بد اندیشانه و حملات طوفانی به اینترنت وسیعتر، در زمان استفاده از شبکه ProtoGENI ممکن بود.

نتایج این تحلیلها بیانگر طیف مسائل امنیتی وابسته به چارچوب شبکه نرم افزار محور SDN بود. در جدول 1، یک دسته بندی از مسائل امنیتی شبکه نرم افزار محور SDN ارائه میگردد. بین نوع مساله/ حمله، یک اتصال رسم میشود (مثلا دستیابی غیر مجاز) و لایه / واسط شبکه نرم افزار محور SDN که تحت تاثیر مساله/ حمله قرار دارد.

3. ارتقاء امنیت با استفاده از شبکه نرم افزار محور SDN

معماری شبکه نرم افزار محور SDN ، پتانسیل نوآوری در استفاده از شبکه را مطرح میکند. ترکیبی از دیدگاه جهانی یا در سطح شبکه و قابلیت برنامه نویسی شبکه، از فرایند برداشت هوش از سیستم های تشخیص نفوذ (IDS) و سیستم های جلوگیری از نفوذ (IPS) حمایت میکند، برای نمونه با تحلیل و برنامه نویسی متمرکز شبکه، دنبال میشود. این رویکرد می تواند شبکه نرم افزار محور SDN را برای حمله مخرب نسبت به شبکه های سنتی، قویتر نماید.

لایه های کنترل و داده، در جدول 1 به صورت اهداف واضح حمله شناسایی میشوند. این مساله، تمایز های اصلی بین شبکه سنتی و شبکه نرم افزار محور SDN را بازتاب میکند؛ تمایزهای عنصر کنترل متمرکز و عناصر مسیر داده تغییر یافته برای حمایت از قابلیت برنامه نویسی.

گرچه این تحلیل، به مسائل امنیتی مربوط به لایه های داده و کنترل اشاره دارد، تحقیقات محدودی در حوزه بررسی این چالشها وجود داشته است. در واقع، همانطور که در بخش بعدی جزئیات این مساله شرح داده شده است، توجه بیشتری به بررسی بهبود های احتمالی در امنیت شبکه شده است که از چارچوب شبکه نرم افزار محور SDN استنتاج شده است.

جدول 1. دسته بندی مسائل امنیتی وابسته با چارچوب SDN که از طریق لایه/ واسط تحت تاثیر قرار میگیرد.

دستیابی غیر مجاز به عنوان مثال	تحت تاثیر یا مورد هدف SDN لایه				
	لایه برنامه کاربردی	واسط Ctl- App	لایه کنترل	واسط داده Ctl	لایه داده
دستیابی کنترل کننده غیر مجاز					
برنامه کاربردی تایید نشده			✓	✓	✓
جابجایی غیر قانونی داده از امکانات کامپیوتری	✓	✓	✓		
کشف قاعده جریان (حمله کانال جانبی روی بافر ورودی)					
کشف سیاست ارسال (تحلیل زمانبندی پردازش بسته)					✓
اصلاح داده مثلا					✓
اصلاح قاعده جریان برای اصلاح بسته ها					
برنامه های کاربردی بد اندیشانه مثلا			✓	✓	✓
درج قاعده کلاهبرداری					
تسخیر کنترل کننده	✓	✓	✓		
رد سرویس مثلا			✓	✓	✓
طغیان ارتباطات راه گزین- کنترل کننده					
طغیان جدول جریان راه گزینی			✓	✓	✓
مسائل پیکربندی مثلا					✓
(یا تکنیک تایید سندیت TLS پذیرش کمبود دیگر)					
(یا تکنیک تایید سندیت TLS پذیرش کمبود اعمال سیاست			✓	✓	✓
	✓	✓	✓		

الف. کادر میانی شبکه نرم افزار محور SDN

شبکه های سنتی از کادرهای میانی برای ارائه کارکردهای امنیت شبکه استفاده می کنند. اخیرا، در مورد تلفیق کادرهای میانی امنیتی در شبکه نرم افزار محور SDN برای بکارگیری مزیت قابلیت برنامه نویسی برای هدایت مجدد ترافیک شبکه انتخاب

شده از طریق کادر میانی، بحث صورت گرفته است. به عنوان مثال، معماری Slick، یک کنترل کننده متمرکز را ارائه میدهد، که مسئول نصب و مهاجرت کارکردهای روی کادرهای میانی بر حسب عادت است. برنامه های کاربردی آنگاه می توانند کنترل کننده Slick را برای نصب کارکردهای ضروری برای مسیریابی جریان های خاص بر مبنای شرایط لازم امنیتی، هدایت کنند.

معماری FlowTags، استفاده از کادرهای میانی اصلاح شده حداقل را ارائه میدهد که با یک کنترل کننده شبکه نرم افزار محور SDN از طریق یک واسط برنامه نویسی برنامه کاربردی FlowTags تعامل برقرار میکند. FlowTags از اطلاعات جریان ترافیکی تشکیل میشود که در عناوین بسته برای ارائه پیگیری جریان درج شده است و مسیریابی کنترل شده بسته های برچسب دار را میسر می سازد. یک نقص آشکار این معماری، این واقعیت است که فقط با سیاستهای از قبل تعریف شده کار میکند و در حال حاضر اقدامات دینامیکی را ساماندهی نمیکند.

لایه اعمال سیاست SIMPLE یک رویکرد برای استفاده از شبکه نرم افزار محور SDN برای مدیریت گسترشهای کادر میانی است. در مقایسه با [13]، [14]، به هیچ اصلاحی در قابلیتهای شبکه نرم افزار محور SDN یا عاملیت کادر- میانی نیاز نیست، که آن را برای سیستم های موروثی، مناسب میسازد.

بر مبنای این ارائه ها، به نظر میرسد یک رویکرد ساده برای تامین امنیت شبکه، معرفی یک کادر میانی مناسب و برنامه نویسی شبکه برای هدایت ترافیک انتخاب شده از طریق کادر میانی است. در عین حال، این مساله کاملا به آن اندازه، صریح نیست. گمارش و یکپارچگی مناسب کادرهای میانی شبکه نرم افزار محور SDN باید در طول جریمه عملکردی تعیین گردد که میتوان زمانیکه ترافیک از طریق یک لینک مکمل منتقل میشود، تحمل شود. چنین سوالاتی هنوز حل نشده اند.

در عین حال، همانطور که در جدول1 نشان داده شده است، طیف حملاتی که برای شبکه تهدید ایجاد میکنند، کاملا شناخته شده است. به این ترتیب، فراتر از کادرهای میانی، یک سری از راه حل ها مطرح

شده اند که به طور ویژه ای چارچوب شبکه نرم افزار محور SDN را برای تامین راه حلهای امنیت شبکه، به کار میگیرند.

ب. SDN = "شبکه سازی امنیت محور"؟

حمله کنندگان از روش های اسکن گوناگونی برای کشف اهداف آسیب پذیر در شبکه استفاده میکنند. یک دفاع ارائه شده برای بی اثر کردن این حملات، استفاده از آدرسهای پروتکل اینترنتی مجازی تصادفی با استفاده از SDN است. این تکنیک از کنترل کننده OpenFlow برای مدیریت یک مخزن از آدرس های IP مجازی استفاده میکند که به هاست ها در شبکه تخصیص می یابند، IP آدرسهای حقیقی را از دنیای خارجی پنهان میکنند. این کار دفاع هدف متحرک را ارائه میدهد که شکلی از امنیت مجازی سازگار است.

سیستم های نظارتی در حفاظت شبکه از حمله، ضروری هستند. در [17]، مولفین یک روش تشخیص حمله منع سرویس توزیع شده (DDoS) را بر مبنای مشخصات جریان ترافیکی متعدد، ارائه میدهد. این سیستم NOX را تحت نظارت قرار میدهد (C++ مبتنی بر کنترل کننده OpenFlow) در فواصل زمانی منظم راه گزینی میکند و از نقشه های خود سازمان دهنده برای شناسایی جریانهای نابهنجار استفاده میکند. در رویکرد دیگری، OpenSAFE از زبان سیاست ALARMS برای مدیریت مسیریابی ترافیک از طریق دستگاه های نظارت شبکه استفاده میکنند. یک ایده مشابه بر SDN در ابر تمرکز دارد که جریان های شبکه را برای تضمین این مساله کنترل می کند که کل بسته های شبکه ضروری با برخی دستگاه های امنیتی بازرسی می شوند. این چارچوب، از نظر خودکار بودن خط سیر بسته های شبکه که باید از طریق دستگاه های امنیت شبکه ی از قبل نصب شده وارسی شوند، منحرف می کند.

این راه حل ها بر مبنای طرح مدیریت شبکه متمرکز است؛ با این حال، سایر مشوق های کاری، نمایندگی برخی کنترلها را به دستگاه ها و هاست های شبکه بر میگردانند. به عنوان مثال رزوناس، کنترل دستیابی دینامیکی اعمال شده توسط خود دستگاه ها را بر مبنای سیاست های امنیت در سطح بالاتر،

ارائه میدهد. نائوس و همکارانش، پروتکل ident++ را برای پرس و جوی هاست های نهایی و کاربران برای اطلاعات بیشتر مطرح می کنند تا تصمیم ارسال بگیرند؛ بحث آنها این است که کنترل کننده مرکزی میتواند به یک تنگنا تبدیل شود. در حالیکه با حفظ ویژگی های قابلیت برنامه نویسی SDN، این روشها، شامل بودن دستگاه های شبکه تحت کنترل شبکه را مطرح می کنند تا تکیه به یک کنترل کننده متمرکز واحد.

شکل خاص سیستم نظارت، IDS، مورد تمرکز شماری از راه حلهای SDN قرار داشته است. اسکورا و همکارانش، یک IDS یادگیری را ارائه میدهند، از معماری SDN هم برای کشف و هم پاسخ دهی به حملات شبکه در دستگاه های موبایل تعبیه شده، استفاده میکند. یک NIDS تسریع شده سخت افزاری (IDS شبکه) یا طرح NIPS (IPS شبکه)، در [23] توصیف شده است، که اجازه میدهد مدیر شبکه، الگوهای رشته ای را برای استفاده از طریق یک ماژول بازرسی بسته عمیق (DPI) پیکربندی نماید. نهایتا، ارزش استفاده از SDN، تامین کشف نفوذ در یک محیط Office/Small Home Office در [24] را ارائه می دهد.

امکان تقویت و ساده سازی امنیت شبکه از طریق معماری SDN، از این ساختار تحقیقات مشهود است. این پتانسیل هم چنین از نظر بازرگانی با طیفی از محصولات امنیت SDN در مراحل مختلف توسعه، به رسمیت شناخته شده است.

4. چالشهای امنیتی با SDN

در حالیکه امنیت به عنوان مزیت چارچوب SDN به رسمیت شناخته شده است، راه حل ها برای حل تامین چالش های شبکه SDN، از نظر تعداد معدودتر هستند.

SDN ها، به ما توانایی برنامه نویسی راحت شبکه و بررسی خلاقیت سیاستها جریان دینامیکی را ارائه میدهند. در واقع، این مزیت است که از این گذشته منجر به آسیب پذیری های امنیتی میشود. در این محیط، حیاتی است سیاست امنیت شبکه، اعمال شود. بررسی مدل به یک مرحله مهم در کشف ناسازگاری ها در سیاستهای حاصل از برنامه های کاربردی یا نصب شده در کل دستگاه های متعدد

تبدیل می شود. بررسی مدل ترکیب شده با اجرای نمادین ممکن است برای محک زدن برنامه های کاربردی OpenFlow برای صحت بکار رود. نمودارهای تصمیم دودوئی هم چنین میتواند برای محک زدن برای سوء پیکربندی راه گزینی-داخلی در یک جدول جریان واحد، بکار رود. FlowChecker، FlowVisor را بکار میگیرد، که جداسازی را با پارتیشن بندی منابع شبکه به صورت بخشها، میسر میسازد. سان و همکارانش، فلاور [28] را مطرح میکنند، که از مجموعه اثباتها و نظریه ها برای اثبات سیاستهای جریان استفاده می کند در حالیکه VeriFlow [29] اثبات نامتغیرها را در زمان حقیقی، مطالعه میکند. یک لایه اضافی، که بین کنترل کننده SDN و دستگاه های شبکه قرار دارد، مانع قواعد جریان میشود، قبل از اینکه به شبکه برسند. گرچه VeriFlow، تاخیر کم فرایند بررسی را بهتر می کند اما نمیتواند کنترل کننده های متعدد را ساماندهی نماید. در [30]، مولفین استفاده از امنیت مبتنی بر زبان را مطرح میکنند که اعمال سیاست مبتنی بر جریان را در کنار جداسازی شبکه، میسر میسازد. این راه حل، به صورت یک برنامه کاربردی NOX اجرا میشود و اجازه یکپارچه سازی منابع تایید هویت خارجی برای تامین کنترل دستیابی را می دهد. اخیرا، جداسازی عالی (Splendid Isolation) [31] به عنوان وسیله ای برای اثبات جداسازی ترافیک برنامه، مطرح شده است. این مدل برنامه ریزی از ایده بخش های شبکه برای تامین مفاهیم اساسی امنیت محرمانه بودن و بی نقصی، حمایت میکند. تاکید آشکاری از سوی جامعه تحقیقاتی در مساله حل تعارض سیاست، وجود دارد.

در عین حال، مطالب ارائه شده برای کمک به طراحی SDN امن، محدود هستند. فرسکو [32]، یک نقش برجسته دارد که یک چارچوب توسعه برنامه کاربردی امنیت OpenFlow را ارائه میدهند که FortNox را به همراه دارد [33]؛ یک هسته اعمال امنیت. ایده پشت FRESCO، اجازه دادن طراحی سریع و توسعه ماژولهای ویژه امنیتی است که میتواند به عنوان یک برنامه کاربردی OpenFlow همراه گردد. پوراس و همکارانش یک کتابخانه از ماژولهای قابل استفاده

مجدد را ارائه میدهد که میتواند برای کشف و کاهش تهدیدهای شبکه به کار رود. این سیستم، موتور اعمال FortNox را به همراه دارد که تعارض های ممکن را با درج قاعده، ساماندهی میکند. اگر یک تعارض قاعده به عنوان نتیجه یک قاعده OpenFlow جدید پدید آید که یک قاعده موجود ممنوع/ مجاز را فعال یا غیر فعال میکند، آنگاه قاعده جدید، بسته به میزان تایید هویت امنیت مولف، برای ارائه قاعده متعارض موجود، پذیرفته یا رد میشود. گرچه FortNox، مولفه های بی شماری را ارائه میدهد، که برای اعمال امنیت ضروری هستند، مولفین احساس میکنند باز هم کار زیادی برای ارائه یک مجموعه جامع از برنامه های کاربردی نیاز است. با حرکت از فضای طراحی به سوی اجرا، یکی از دغدغه های مهم صنعت با امنیت در SDN، تامین فرایند حسابرسی است. برای اجابت و عملیات شبکه، یک موجودی کنترل شده از دستگاه های شبکه، لازم است. این موجودی، دانش اینکه چه دستگاه هایی کار میکنند.

جدول 2. دسته بندی تحقیقات در زمینه امنیت در SDN.

SDNلایه /واسط				OpenFlow	امنیت			کار تحقیقاتی
داده	داده Ctl	Ctl	Ctl-App	App		راه حل	ارتقاء	تحلیل	

[7], [10], [12]	✓			✓			✓	✓	✓
[11]	✓				✓		✓	✓	✓
[5]							✓	✓	✓
[13], [14], [21]		✓		✓	✓	✓	✓	✓	✓
[15]		✓			✓		✓		✓
[16]		✓		✓			✓	✓	✓
[17], [24]		✓		✓	✓		✓	✓	
[18], [19]		✓		✓	✓	✓	✓	✓	
[20], [22]		✓		✓	✓		✓	✓	✓
[23]		✓			✓				✓
[25]			✓	✓	✓	✓		✓	
[26], [28]–[30], [32]			✓	✓	✓	✓	✓	✓	
[31]			✓			✓	✓		
[33], [34]			✓	✓		✓	✓	✓	
[35]			✓	✓	✓			✓	

چطور به شبکه و غیره، محدود میشوند را در بر می گیرد، این مساله به طور مستقیم به پتانسیل مجازی سازی عناصر شبکه و کارکردهایی که از طریق شبکه SDN حمایت میشود، مربوط است. گرچه یک چالش حل نشده پیرامون عملی بودن وضعیت شبکه نگاشت در کل کارکردهای موبایل و مجازی وجود دارد، اما برخی از آثار مرتبط در زمینه اثبات شبکه، ارزش ذکر کردن را دارند. در [34]، مولفین مساله مقیاس پذیری و امنیت شبکه های OpenFlow و استفاده آنها در فضای فیزیکی- سایبری را بررسی می کنند. Verificare مدلسازی مشخصات و اثبات صحت شبکه، همگرایی و خواص مربوط به پویایی را بررسی میکنند. هادیگل و همکارانش، استفاده از اشکال یابی شبکه نمونه اولیه را مطرح می کنند [35] که می تواند به توسعه دهندگان SDN اجازه دهد، زنجیره رویدادهایی را بازسازی کنند که منجر به یک باگ (خطا) و شناسایی دلیل ریشه ای آن میشود.

همانطور که در بخش 2 شناسایی شده است، معماری SDN میتواند به عنوان مجموعه ای از لایه ها و رابط ها، قلمداد شود. لایه/ رابط، تحت تاثیر برخی مسائل امنیتی ویژه SDN است که در جدول 1 شناسایی شدند. در یک شیوه مشابه، اثر تحقیقاتی امنیتی SDN، در جدول 2 توسط لایه/ رابط، دسته بندی می شود که تحلیل، ارتقاء یا اهداف راه حل میباشند.

نتایج این دسته بندی، در بخش بعدی مورد بحث قرار می گیرند. لازم به ذکر است، SANE جزو جدول 2 برای دسته بندی با توجه به لایه ها/رابط ها، محسوب می شود. در عین حال، به عنوان یک معماری مجزا، راحلی برای ارتقاء امنیت SDN شناسایی نمی شود.

5. بحث

با بررسی دسته بندی اثر تحقیقاتی در جدول 2 میتوان دید تمرکز بیشتری بر به کارگیری SDN برای امنیت شبکه ارتقا یافته وجود دارد تا بر ایجاد راه حل هایی برای مسائل شناسایی شده امنیت. اثر ارتقاء، بر استفاده از کادرهای میانی و سیستم های نظارت برای درج خدمت امنیتی برای کشف پویا و یا جلوگیری از ترافیک مشکوک در طول عملیات شبکه زنده، تمرکز کرده است.

پتانسیل بیشتری در این حوزه برای بهره برداری از قابلیتهای دینامیکی و سازگار چارچوب SDN با استفاده از روشهای دفاع هدف متحرک وجود دارد. کار ارائه شده در [16]، نمونه ای است که در آن تصادفی کردن آدرسهای IP مجازی کار را برای حمله کننده برای نفوذ در شبکه دشوارتر میکنند. بدون یک سیستم ثابت برای مشاهده و آماده حمله شدن، قدرت حمله کننده کاهش می یابد.

روش ها و تکنیک های جدید باید برای گسترش روی قابلیت برنامه ریزی شبکه بررسی شوند که تنظیمات دینامیکی در قابلیت های نظارت امنیتی، کشف و پیشگیری را میسر میسازند.

مشاهده جزئی از محتوای جدول 2، اکثریت مراجع کاری یا اجراهای OpenFlow برای رابطه داده-کنترل است. گرچه هر جایگزینی برای OpenFlow، دارای صفات مشابهی خواهد بود که لازم به ذکر است OpenFlow ممکن است تنها پروتکل رابط داده-کنترل منحصر به فرد/ قطعی در SDNها نباشد. به عنوان مثال، چندین گروه کار گروه مهندسی اینترنت (IETF)، پروتکلهای پیرامون تفکیک سطوح ارسال و کنترل، پیکربندی شبکه و مسیریابی را تعریف کرده اند. این موارد شامل

IETF ForCES (تفکیک عنصر کنترل و ارسال)، PCE (عنصر محاسبه مسیر)، Netconf (پیکربندی شبکه)، LISP (موجز/ پروتکل تفکیک ID) و I2RS (واسط برای سیستم مسیریابی) است. به علاوه، پروتکلهای اختصاصی، توسط شرکتهای انفرادی توسعه می یابند. کار شناسایی و اصلاح محدودیت های مربوط به شبکه پروتکل OpenFlow باید در طراحی و توسعه پروتکلهای دیگر بررسی شود. این مساله میتواند هم برای واسط سطح داده-کنترل و هم برای تجرید های سطح بالاتر در واسط کنترل-برنامه ی کاربردی به کار رود که ممکن است دغدغه های مشابهی را ارائه دهد.

مهم ترین عنصر برای تاکید از دسته بندی تحقیقات SDN مربوط به امنیت این است که یک عدم اتصال قابل شناسایی بین تحلیل های امنیتی ارائه شده تاکنون وجود دارد که بر مسائل سطح داده-کنترل و راه حل ها برای مسائل امنیتی، تمرکز دارد، که اکثر آنها بر یک مساله سطح کنترل-برنامه تمرکز دارد؛ که از راه حل تعارض سیاست محسوب می شود.

با بررسی وسعت مسائل امنیتی احتمالی خلاصه شده در جدول 1، مشخص می شود یک افزایش معنادار مورد تلاش برای شناسایی راه حلها برای این چالش ها لازم است.

این شرایط لازم در سال گذشته در برخی نواحی جامعه شبکه سازی به رسمیت شناخته شده است. از زمان شروع سال 2013، کارگروه های مختلفی هم در صنعت استاندارد سازی و هم گروه های تحقیقات صنعتی، ایجاد شده اند. در بنیاد شبکه سازی آزاد (ONF) و موسسه استاندارد های مخابرات اروپا (ETSI)، گروه ها به ترتیب به طور ویژه بر امنیت در SDN و NFV تمرکز کردند، که راه اندازی شده اند. در کار گروه تحقیقات اینترنت (IRTF) و اتحادیه مخابرات بین الملل- بخش استاندارد سازی مخابرات (ITU-T)، گروه های مطالعه SDN کلی راه اندازی شده اند که در آنها امنیت در SDN، یک مساله شناسایی شده است.

یکی از موضوعات مکرر حاصل از این کارگروه های صنعتی، اهمیت طراحی امنیت از ابتدا مطرح است. منظور این است در حالیکه SDN در مراحل اولیه

توسعه قرار دارد، مسائل امنیتی مربوطه باید شناسایی و حل شوند. در عین حال، سخت افزار سازگار با SDN، نرم افزار و سرویسها، هم اکنون در حال تولید و خدمت هستند. در حالیکه برخی از این راه حلها، در واقع، محصولات امنیت SDN هستند، بسیاری دیگر، با بررسی جزئی یا بدون بررسی مضامین امنیتی برای یک گسترش شبکه ناحیه وسیع، توسعه یافته اند.

لذا، ضروری است، تکنیکها، روشها و سیاست ها برای غلبه بر چالشهای امنیت SDN، مورد بررسی قرار گیرند و برای فعال سازی گسترش های SDN وسیع قابل اطمینان و قوی، بررسی و تعریف می شوند. یک تاکید بیشتر بر این مساله اکنون میتواند از کاهش در عملکرد و قابلیت SDN های آینده در نتیجه ی راه حلهای امنیتی بهسازی خودداری نماید.

6. نتیجه گیری

دو مکتب فکری در مورد امنیت در شبکه سازی تعریف شده نرم افزاری وجود دارد. اولی پیشرفت های مهم در امنیت شبکه است که میتواند به طور همزمان، قابلیت برنامه ریزی را بکار گیرد و دیدگاه شبکه متمرکز که توسط SDN مطرح می شود. دومی این است که این دو ویژگی مشابه SDN، با شبکه در طیفی از حملات جدید مواجه می شوند. در این مقاله، ما چالش های امنیتی SDN را دسته بندی کرده ایم و یک مرور جامع از اثر تحقیقاتی را پیرامون امنیت در SDN تاکنون ارائه داده ایم. تحلیل ما بدون توجه به مکتب فکری شما شناسایی می کند که باز هم کار بیشتری برای انجام وجود دارد؛ پتانسیل بهره برداری نشده و چالش های حل نشده بیشتر. تلاش هماهنگ در هر دو جهت می تواند یک شبکه نرم افزار محور قابل اطمینان و امن را به دست آورد.

REFERENCES

[1] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, and M. Zhu, "B4: Experience with a globally-deployed software defined wan," in *Proceedings of the ACM SIGCOMM 2013 conference*. ACM, 2013, pp. 3–14.

[2] S. Sezer, S. Scott-Hayward, P. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? Implementation challenges for software-defined networks," *Communications Magazine, IEEE*, vol. 51, no. 7, 2013.

[3] "Network Functions Virtualization - Introductory White Paper," October, 2012. [Online]. Available: http://portal.etsi.org/NFV/NFV White Paper.pdf

[4] C. Douligeris and D. N. Serpanos, *Network security: current status and future directions*. Wiley. com, 2007.

[5] M. Casado, T. Garfinkel, A. Akella, M. J. Freedman, D. Boneh, N. McKeown, and S. Shenker, "Sane: A protection architecture for enterprise networks," in *USENIX Security Symposium*, 2006.

[6] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, "Ethane: Taking control of the enterprise," in *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4. ACM, 2007, pp. 1–12.

[7] R. Kloeti, "OpenFlow: A Security Analysis," April 2013. [Online]. Available: ftp://yosemite.ee.ethz.ch/pub/students/ 2012-HS/MA-2012-20 signed.pdf

[8] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, "Threat modeling-uncover security design flaws using the stride ap- proach," *MSDN Magazine-Louisville*, pp. 68–75, 2006.

[9] "OpenFlow Switch Specification Version 1.3.2," Open Networking Foundation. [Online]. Available: https://www. opennetworking.org

[10] K. Benton, L. J. Camp, and C. Small, "OpenFlow Vulnerability Assessment," in *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*. ACM, 2013, pp. 151–152.

[11] D. Kreutz, F. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," in *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*. ACM, 2013, pp. 55–60.

[12] D. Li, X. Hong, and J. Bowman, "Evaluation of Security Vul- nerabilities by Using ProtoGENI as a Launchpad," in *Global Telecommunications Conference (GLOBECOM 2011)*. IEEE, 2011, pp. 1–6.

[13] B. Anwer, T. Benson, N. Feamster, D. Levin, and J. Rexford, "A Slick Control Plane for Network Middleboxes," *Open Networking Summit*, 2013. [On- line]. Available: http://nextstep-esolutions.com/Clients/ONS2.0/ pdf/2013/research track/poster papers/final/ons2013-final51.pdf.

[14] S. Fayazbakhsh, V. Sekar, M. Yu, and J. Mogul, "FlowTags: Enforcing Network-Wide Policies in the Presence of Dynamic Middlebox Actions," in *Proceedings of the second workshop on Hot topics in software defined networks*. ACM, 2013.

[15] Z. A. Qazi, C.-C. Tu, L. Chiang, R. Miao, V. Sekar, and M. Yu, "SIMPLE-fying Middlebox Policy Enforcement Using SDN." ACM SIGCOMM, August 2013..

[16] J. R. Ballard, I. Rae, and A. Akella, "Extensible and scalable network monitoring using opensafe," *Proc.INM/WREN*, 2010.