یازدهمین کنگره ملی سراسری
فناوریهای نوین در حوزه توسعه پایدار ایران
11th National Congress of
the New Technologies in Sustainable Development of Iran
senaconf.ir

تهدیدها و آسیب پذیریهای موجود در شبکه های SDN

غلامرضا محمدی ده بزرگ[۱]، امین هاشمی پور[۲]، محمد درویشی پادوک[۳]

[۱] مربی گروه کامپیوتر،دانشگاه علمی کاربردی،واحد گچسارا ،ایران، گچساران g.mohamadi1371@gmail.com
[۲] مدیر گروه مهندسی کامپیوتر ، دانشگاه علمی کاربردی، ایران،گچساران amin_hashemipour@yahoo.com
[۳] مربی گروه کامپیوتر ، دانشگاه آزاد، واحد گچساران ، ایران ،گچساران darvishi.mohammad@gmail.com

چکیده

شبکه های نرم‌افزار محور (SDN) الگویی است که همراه با دیگر فن‌آوری‌های شبکه روندی رو به رشد را در پیش گرفته است . جداسازی صفحات کنترل و داده در شبکه های SDN امکان ظهور ویژگی‌های جدید شبکه مانند مدیریت متمرکز جریان داده و همچنین قابلیت برنامه‌ریزی شبکه ها را فراهم می‌کند . این شبکه ها ، بهبود جنبه‌های برجسته گسترش شبکه مانند انعطاف‌پذیری، مقیاس پذیری، قابلیت مشاهده گستردهٔ شبکه و مقرون به‌صرفه بودن آنها را در بر می گیرد. اگرچه SDN تکامل سریعی را نشان می‌دهد بطوریکه این فن‌آوری را به عنوان یک فناوری توانمندساز و کلیدی برای پیاده‌سازی‌های آینده در سناریوهای شبکه ی ناهمگون، یعنی مراکز داده، ISP ها، شرکت‌های بزرگ دانشگاهی و خانه ها ، شکل می‌دهد، اما این فن‌آوری تا به امروز امن و قابل‌اعتماد در نظر گرفته نشده است .لذا ما در این نوشتار ، تهدیدها و آسیب پذیری های موجود در شبکه های SDN و لایه های آن را بررسی می کنیم.

واژه‌های کلیدی

شبکه های SDN ، امنیت در شبکه های SDN

۱. مقدمه

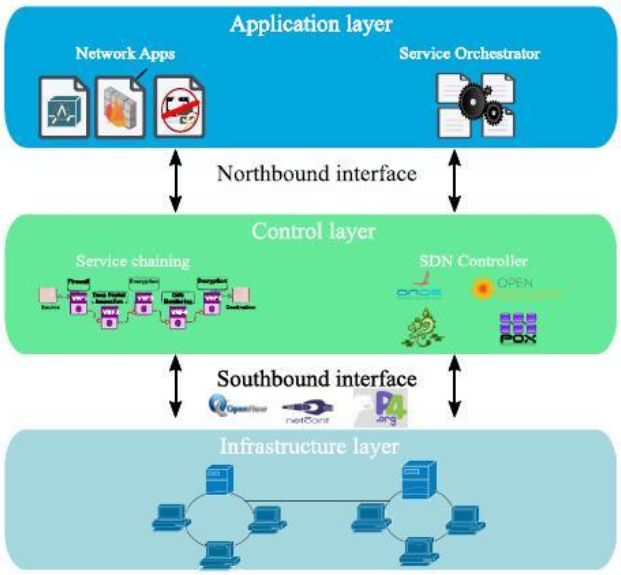
الگوی SDN ، صفحه کنترل و داده را از هم جدا می کند ، بنابراین تمام هوش و منطق کنترل شبکه از دستگاه های شبکه به یک نهاد مبتنی بر نرم افزار متمرکز منطقی معروف به کنترل کننده شبکه منتقل می شود. کنترل کننده شبکه در صفحه کنترل قرار دارد که در آن توابع کنترل متمرکز و مدیریت شبکه ، رفتار انتقال به تمام عناصر توزیع شده در زیرساخت را آموزش می دهند. در صفحه داده ، عناصر شبکه به نام سوئیچ ها برای مطابقت با فراداده ها در بسته های جریان بر خلاف قوانین و دستورالعمل های حمل و نقل صادر شده توسط کنترل کننده شبکه طراحی شده اند. چنین فرآیندی قبل از تصور هرگونه تصمیم ارسال ، پیش می رود. مشخصه متمرکز SDN به این معنی است که کنترل کننده شبکه همیشه از وضعیت شبکه آگاه است و اینکه تمام جریان های ترافیک در طول عمر شبکه برای تعریف رفتار انتقال بسته ها، حداقل یک بار به کنترل کننده منتقل می شوند. علاوه بر مدیریت جریان متمرکز ،SDN مفهوم قابلیت برنامه نویسی شبکه را پرورش می دهد. از این رو ، توابع مختلف شبکه به عنوان برنامه های نرم افزاری تعبیه شده اند که می توانند در بالای کنترل کننده نصب شوند یا به عنوان توابع مصرف کننده داده مستقل استفاده شوند.SDN مفهوم برنامه پذیری شبکه را تجسم می بخشد زیرا کلیه عملیات شبکه باید به عنوان برنامه های نرم افزاری ، الگوریتم های یکپارچه ، ساختار داده ها و مفاهیم برنامه نویسی توصیف شوند که به محیط توسعه نرم افزار تعلق دارند. امنیت که یک جنبه حساس در شبکه های ارتباطی و داده ای می باشد، ممکن است از ویژگی های SDN از جمله برنامه های شبکه خود بهره مند شود. چندین مشکل امنیتی که اغلب شبکه های معمولی را تهدید می کنند می توانند به صورت به موقع و قابل اطمینان در SDN مرتب شوند و برنامه های نرم افزاری امنیت شبکه را اجرا کنند در شبکه های SDN فمقیاس پذیری و انعطاف پذیری راه حل های امنیتی افزایش داده شده است و استقرار چنین راه حل هایی در زیرساخت های گسترده شبکه سهولت می بخشد. با وجود تمام مزایایی که شبکه های SDN دارد ، قابل ذکر است که معماری SDN شامل مشکلات امنیتی ناشناخته و اضافی ، خطرات و تهدیدهایی است که به دلیل معرفی رابط های شبکه جدید و تغییر عناصر شبکه و طرح ارتباطی سنتی آنها ظاهر می شود. بنابراین علاوه بر توسعه استراتژی های امنیتی جدید با استفاده از SDN ، باید تعهدی برای تعبیه امنیت در معماری مرجع SDN وجود داشته باشد. از آن جایی که SDN می تواند اهرمی برای افزایش امنیت شبکه باشد ، اما در عین حال باید از امنیت کافی برخوردار باشد[1] .

۲. معماری SDN

مهمترین و بارزترین ویژگی در مورد شبکه تعریف شده توسط نرم افزار (SDN)، جدا کردن کنترل شبکه و وظایف انتقال بسته است. این اساساً به مهاجرت تمام اطلاعات شبکه اشاره دارد که اصولا در اطلاعات سخت افزاری قرار دارد ، ساختار کلی در این معماری ، به یک نهاد مبتنی بر نرم افزار متمرکز منطقی روی آورده، در حالی که همه دستگاه های انتقال داده به عناصر انتقال بسته ی ساده تبدیل می شوند. جداشدن سطوح کنترل و داده در SDN ، به معنای متمرکز کردن منطقی کنترل و مدیریت کلیه دستگاه های انتقال شبکه است که به نوبه خود مدیریت شبکه را به عنوان یک فعالیت گسترده در شبکه ارتقا می بخشد[2].

شبکه ها از جدا کردن سطوح کنترل و داده و قابلیت برنامه نویسی نرم افزار سود می برد ، زیرا توابع پیچیده شبکه را می توان با استفاده از روال های نرم افزاری ساده و الگوریتم ها پیاده سازی کرد. سپس می توان رفتار یا عملکرد متفاوت شبکه را مورد ارزیابی قرار داد[3].

همانطور که در شکل ۱ مشاهده می شود ، معماری SDN از سه بخش عمده ی لایه برنامه ، لایه کنترل و لایه صفحه داده و دو اینترفیس شمالی و جنوبی تشکیل شده است.



شکل ۱ . معماری SDN[3]

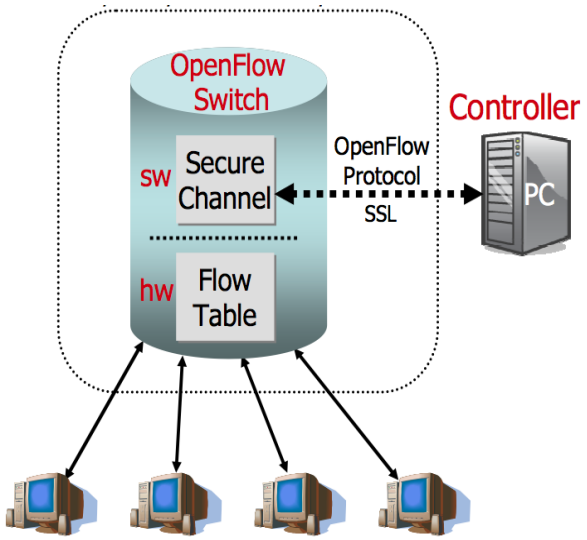
هر یک از این اجزا زیر لایه ها و رابط های عملکردی خاص خود را نشان می دهد. لایه برنامه دارای برنامه هایی است که رفتار شبکه ، خط مشی ها و طرح های انتقال بسته را تعریف می کنند. لایه کنترل نقش شبکه ی عامل را بازی می کند . سیستمی که در آن کنترل کننده های شبکه جزئیات شبکه سطح پایین را برای برنامه های شبکه و مدیریت جمع می کنند و همچنین سیاست های سطح بالا را به قوانین انتقال داده تبدیل می کنند که در کلِ زیرساخت شبکه پخش می شوند[4].

لایه کنترل به مجموعه دستگاه های هدایت کننده متشکل از زیرساخت های شبکه گفته می شود که وظایف اصلی آنها اجرای اقدامات ارسال بر روی بسته های جریان مطابق دستورالعملهای مربوطه ارائه شده توسط کنترل کننده و گزارش اقدامات وضعیت شبکه در صورت درخواست برنامه های شبکه است. رابط های Northbound برنامه ها را در صفحه Application به سیستم عامل های شبکه (NOS) در صفحه کنترل متصل می کنند ، در حالی که رابط های جنوبی به کانال کنترل برای تبادل داده ها بین NOS و دستگاه های صفحه داده می شوند[5].

۳. پروتکل اوپن فلو

به طور قطع می توان گفت که شرط استفاده از شبکه های نرم افزار محور ، پروتکلopenflow می باشد ، چرا که به کمک این پروتکل ،دستگاه های شبکه سخت افزار های روانه سازی هستند که به طور اختصاصی و به کمک قوانینی که از کنترلر مرکزی دریافت می کنند وظیفه هدایت بسته ها را برعهده دارند. از طرفی با افزایش روزافزون ترافیک اینترنت و پیدایش رویکردهای نوین مانند رایانش ابری و خدمات شبکه های مختلف (نرم افزار محور ، اجتماعی و ...) نیاز مبرم به بستری امن، سریع،گسترده و قابل توسعه بیش از پیش مشاهده می شود. لذا محققان نیاز به بستری بزرگ و نزدیک به واقعیت دارند تا بتوانند ایده ها و پروتکل های جدید را در محیطی عملیاتی آزمایش کنند[6,7]. مشتریان IT نیز با خرید حجم زیادی از تجهیزات شبکه، بدنبال کنترل بیشتر و هزینه کمتر در شبکه های خود هستند؛ اما با توجه به معماری متفاوت هر تولیدکننده، جای خالی یک استاندارد که محققان و مشتریان را قادر به برنامه نویسی تجهیزات شبکه بر حسب نیازهای پژوهشی و سازمانی کند حس می شود. از این رو محققان دانشگاه برکلی و استنفورد (نیک مک‌کون و اسکات شنکر) به ابداع پروتکل openflow پرداختند [8]. بطور کلی میتوان پروتکل Openflow را یک استاندارد آزاد جهت ارتباطات دانست که میتواند توسط سازنده ها و تولید کننده های مختلف مورد استفاده قرار گیرد و همچنین امکان ایجاد یک پروتکل جدید را در محیط

های آزمایشگاهی و آموزشی فراهم کند. پروتکل openflow براساس تفکیک بین سطوح داده و کنترل و اجرای کنترل مبتنی بر جریان داده بنا شده است ، که این جریان داده توسط اطلاعات موجود در بسته، از لایه ۱ تا لایه ۴ تعریف می شود. در شکل ۲ نمایی از این معماری را مشاهده می کنیم.



شکل ۲ . پروتکل Openflow [8]

۴. تهدیدها و آسیب پذیری ها ی SDN

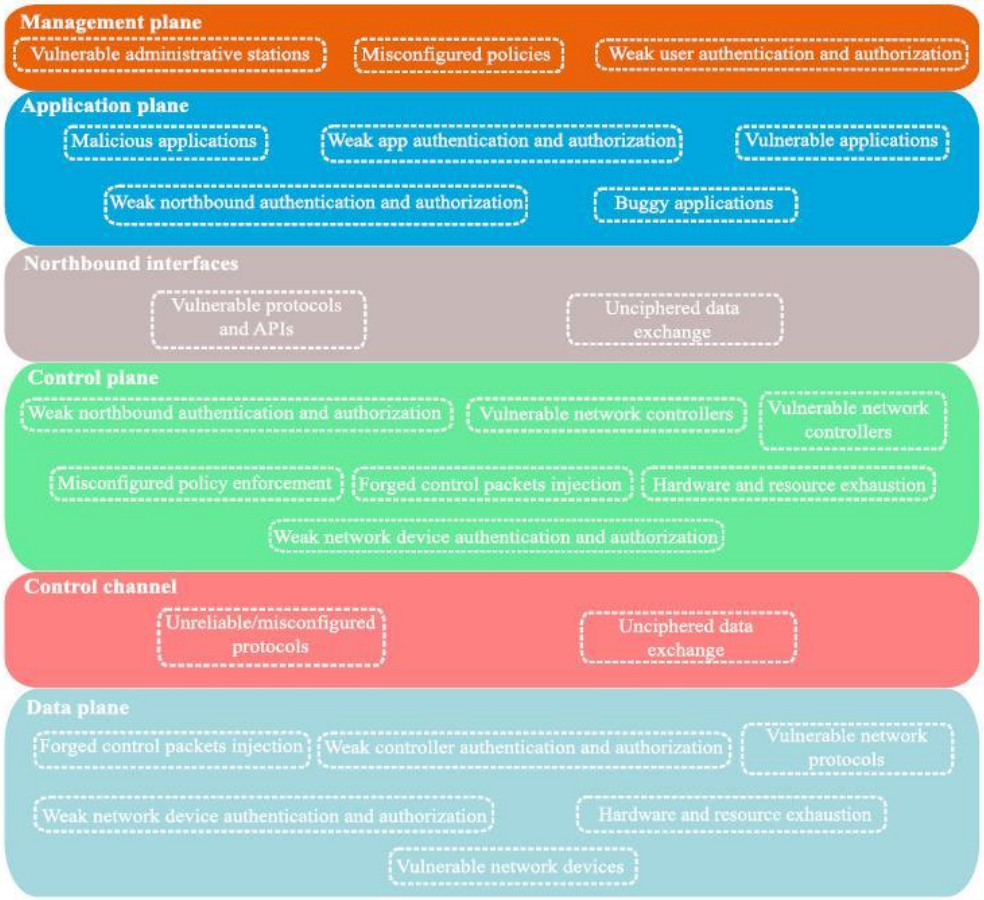
SDN به عنوان هر فناوری جدید دیگری، دارای موافقان و مخالفان خاص خود می باشد . به عنوان مثال در مورد امنیت ، فناوری SDN می تواند برای کاهش برخی از خطرات و آسیب پذیری هایی که معمولاً در شبکه های معمولی مورد سوء استفاده قرار می گیرند استفاده شود. متأسفانه فناوری SDN آسیب پذیری ها و مسیرهای تهدید جدیدی را معرفی می کند که مخصوص ذات معماری این شبکه ها می باشد. در حقیقت ، جداسازی صفحه های کنترل و داده ها و تمرکز منطقی تمام اطلاعات شبکه ، نقطه ای از یک خرابی را نشان می دهد که می تواند برای به خطر انداختن کل یک شبکه SDN مورد سوء استفاده قرار بگیرد. ما در این نوشتار ، یک نمای کلی از مشهودترین سطوح حمله و مسیرهای تهدید را که در صفحه ها و رابط های معماری SDN شناسایی شده اند را ارائه می دهیم و به تشریح این حلات میپردازیم[9].

۵. سطوح حمله و مسیر های تهدید در SDN

درست مثل شبکه های معمولی ، پروتکل ، دستگاه یا لایه مشارکت کننده در SDN می تواند مورد سوء استفاده عمدی یا غیر عمدی قرار گیرند که در برخی موارد برای افشاگری افشای خطاهای سیستم یا رونمایی از رفتار انحرافی ضمنی استفاده می شود. این استدلال کافی است تا این ادعا مطرح شود که هر عنصر یا لایه ،که بخشی از معماری SDN را تشکیل دهد می تواند یک تهدید بالقوه یا یک سطح حمله در نظر گرفته شود ، به این معنی که هرگونه پیکربندی نامناسب یا استقرار نامناسب هر عنصر SDN ، می تواند به عنوان منبع نوظهور آسیب پذیری و پتانسیل خطرات امنیتی پایه گذاری شود.

اگر صفحه کنترل به عنوان یک اتصال از لایه برنامه و لایه سیستم عامل شبکه در نظر گرفته شود ، به دنبال این رویکرد ، آسیب پذیری ها و حملاتی که برنامه های شبکه یا API های منتهی به رابط شمالی ، آسیب پذیری صفحه کنترل یا حملات بدون تمایز را هدف قرار می دهد در نظر گرفته می شوند[10].

در شکل ۳ ، هر صفحه / رابط SDN لیستی را با مرتبط ترین سطوح تهدید که ممکن است توسط کاربران مخرب برای به خطر انداختن یک شبکه که تحت پارادایم SDN استفاده می شود ، ذکر شده است که در ادامه به تشریح آنها می پردازیم:



شکل ۳ . مرتبط ترین سطوح تهدید[10]

۶. حمله به معماری SDN

همه لایه ها و رابط ها به حملات خاصی حساس هستند که ممکن است اجزای شبکه مستقر در لایه را به خطر بیندازد یا عناصر موجود در لایه دیگر را هدف قرار دهد. در ادامه ما تمام لایه های معماری SDN را تشریح می کنیم و علاوه بر آن به حملات خاصی که این لایه ها را تهدید می کند می پردازیم :

۱.۶.سطح کاربردی

در حملات و تهدیدات مربوط به سطح کاربردی ما می توانیم به موارد زیر اشاره کنیم :

۱.۱.۶.خاتمه برنامه به کمک امتیازات و اختیارات ثابت

برنامه های شخص ثالث و کنترل با اختیارات نامحدود در سیستم شبکه را می توان به خطر انداخت که شامل اجرای دستورات سیستم است که بیشتر برای قطع / خاموش کردن برخی از API ها یا برنامه های حساس شبکه استفاده می شود[11].

۲.۱.۶. خنثی سازی سرویس

از موارد مخربی که با موفقیت در بالای کنترل کننده نصب شده است ، می توان برای دستکاری بسته های کنترل کننده استفاده کرد ، سپس یک سرویس را با کمک چهار مورد زیر انجام داد[12] . که این چهار مورد عبارتند از :

۱- دور انداختن بسته های کنترل برای جلوگیری از دستیابی آنها به برنامه های مورد نظر .
۲- براندازی نظمی که در آن دستیار برنامه ها به بسته های کنترل دسترسی دارند.
۳- تداخل در زنجیره های خدمات برای برهم زدن انتقال بسته کنترل.
۴- بازرسی بسته های کنترل برای استشمام اطلاعات حساس شبکه و انجام اقدامات انحرافی خاص.

۳.۱.۶. حملات به API های(برنامه های کاربردی) آسیب پذیر محدوده شمال

پیکربندی های اشتباه و آسیب پذیری در API های شمال را می توان برای خاتمه دادن به برنامه avictim با صدور دستور سیستم یا افشای اطلاعات رد و بدل شده بین کنترل کننده و یک برنامه هدف استفاده کرد[12].

۲.۶. لایه کنترل

در حملات و تهدیدات مربوط به لایه کنترل ما میتوانیم به موارد زیر اشاره کنیم :

۱.۲.۶. تونل زنی قاعده جریان پویا

در صورت اجرای برنامه های مخربی که می توانند قوانین جریان همپوشانی و متناقض را آموزش دهند ، مهاجمان ممکن است از قوانین جریان فایروال مانند (بلوک ، رها کردن) استفاده کنند و از این واقعیت استفاده کنند که کنترل کننده ها نمی توانند تعارضات ضمنی را بین قوانین جدید صادر شده و قوانین موجود تشخیص دهند و به مجموعه های مختلف سیاست های شبکه و کنترل متصل شوید[13].

۲.۲.۶. مسمومیت کنترل کننده

از پروتکل های آسیب پذیر شبکه و برنامه های مخرب می توان برای مسموم کردن اطلاعات کنترل کننده و نمای توپولوژی استفاده کرد که به نوبه خود باعث اجرای حملات به صفحه داده می شود. به عنوان مثال ، در حمله آسیب رساندن بسته LLDP (پروتکل کشف لایه) ، یک دشمن بسته های LLDP دستکاری شده را به کنترل کننده می فرستد تا نمای توپولوژی شبکه خود را مسموم کند زیرا این بسته های دستکاری شده کنترل کننده را وادار می کند تا ورودی های جعلی لینک شبکه را به سوابق توپولوژی خود اضافه کند. . مثال دیگر حمله میزبانی مکان میزبان است ، که در آن می توان با استفاده از بسته های LLDP ساخته شده از یک آسیب پذیری در سرویس نمایه میزبان استفاده کرد ، در نتیجه مخزن مشخصات کنترل کننده میزبان مسموم شده و بسته های در نظر گرفته شده برای یک سوئیچ هدف خاص مهاجم می شوند[14] .

۳.۲.۶. سو استفاده از سیستم عامل شبکه

برنامه های به خطر افتاده و دستگاه های متفرقه صفحه داده می توانند از آسیب پذیری ها و تنظیمات نادرست کنترل کننده برای دستیابی به اهداف مختلف سو ء استفاده کنند[13] ، به عنوان مثال می توان به موارد زیر اشاره کرد :

۱- اجرای یک دستور سیستم که کنترل کننده را مجبور به خاتمه می کند.
۲- نشت اطلاعات حساس که در هر نمونه از ذخیره سازی داده های شبکه داخلی وجود دارد.
۳- تغییر مسیر اطلاعات در نظر گرفته شده برای یک دستگاه قانونی .
۴- سیاست های شبکه ربودن پایگاه داده نصب روت کیت یا اتصالات دسترسی از راه دور برای حفظ کانال دسترسی غیر مجاز به کنترل کننده .
۵- معرفی داده های ورودی نامعتبر است که ممکن است کنترلر را در یک حالت غیرقابل پیش بینی قرار دهد.

۳.۶. کانال کنترل

در حملات و تهدیدات مربوط به کانال کنترل ما میتوانیم به موارد زیر اشاره کنیم :

۱.۳.۶.استراق سمع

دشمن می‌تواند از کانال‌های کنترل رمزگذاری نشده برای انجام حملات اسنیفینگ بسته استفاده کند، سپس مهاجم می‌تواند به تمام اطلاعات کنترل، توپولوژی و مدیریت شبکه که در کانال کنترل مبادله می‌شود گوش دهد[15].

۲.۳.۶. نفوذگر در وسط کانال

کانال‌های کنترل نامشخص همراه با حملات مسمومیت ARP می‌توانند برای وارد کردن یک میزبان نفوذگر در وسط کانال کنترل برای نفوذ در ارتباطات بین کنترل‌کننده و هر دستگاه سطح داده هدف استفاده شوند[15].

۴.۶. لایه زیرساخت

در حملات و تهدیدات مربوط به لایه زیر ساخت ما می توانیم به موارد زیر اشاره کنیم :

۱.۴.۶. انکار سرویس با استفاده از حمله مسمومیت ARP

یک مهاجم می تواند با جعل هویت کنترل کننده، به ایزوله سوئیچ هدف دست یابد. با استفاده از حمله مسمومیت ARP، مهاجم هویت کنترلر را ربوده و یک سوئیچ هدف را مجبور می کند تا اتصال به کنترل کننده اصلی را قطع کند و به جای آن به کنترل کننده جعلی متصل شود. این منجر به قطع سوئیچ به شبکه می شود[12].

۲.۴.۶. اصلاح / فلاشینگ قانون جریان

مهاجمان می‌توانند اطلاعات نصب شده در جدول جریان سوئیچ‌ها را دستکاری کنند، یا قوانین جریان موجود را بازنویسی یا شستشو دهند. مهاجمان می توانند این حمله را از یک برنامه در معرض خطر یا یک کنترلر شبکه در معرض خطر راه اندازی کنند[12].

۳.۴.۶. سیل قانون جریان

با استفاده از تکنیک های حمله کانال جانبی، مهاجم می تواند در مورد دو موقعیت خاص استنباط کند[12] ، که عبارتند از :

۱- اگر یک جدول سوئیچ نزدیک است کاملاً پر شود.

۲- نوع بسته هایی که یک جدول را از دست می دهند، سوئیچ را مجبور می کند تا درخواستی را برای نصب یک قانون جریان جدید به کنترل کننده ارائه دهد. با توجه به موقعیتی که مهاجم در مورد چنین اطلاعاتی استنباط کرده است، سپس می تواند یک حمله سیلابی جدول جریان را راه اندازی کند و سوئیچ را مجبور کند که دائماً قوانین جدید را بخواهد و سپس جدول جریان خود را پر کند، چنین رفتاری می تواند تأثیرات منفی روی سوئیچ داشته باشد.

۴.۴.۶. تزریق بسته کنترلی نادرست

یک سوئیچ هدف می‌تواند به حالت نامطلوب هدایت شود اگر در معرض یک موقعیت حمله فازی قرار گیرد، بسته‌های کنترل دستکاری شده حاوی هدرهای نادرست یا استفاده نادرست را دریافت کند که به طور هوشمندانه برای افشای آسیب‌پذیری‌های موجود یا رفتار نادرست آزمایش شده تحت ورودی نامعتبر ساخته شده‌اند. همه حملات به امنیت شبکه را می توان با توجه به هدف اصلی حمله طبقه بندی کرد ، به عنوان مثال استراق سمع رابط کنترل را می توان به عنوان حمله ای هدف اصلی آن دستکاری در داده های خصوصی و حساس رد و بدل شده بین لوازم شبکه عنوان کرد ، این نشان دهنده یک افشای غیر مجاز اطلاعات به معنای وسیع تر آن. ویژگی‌های SDN مانند دید در سراسر شبکه، هوشمندی متمرکز شبکه و قابلیت برنامه‌ریزی شبکه، نحوه ارسال بسته‌ها و وظایف کنترل اولیه شبکه در شبکه‌های قابل برنامه‌ریزی را تغییر دادند. با این حال، همانطور که در بخش قبل توضیح داده شد، این ویژگی ها و خود معماری SDN امنیت جدیدی را معرفی می کند[12].

نتیجه گیری

معماری شبکه های SDN انقلابی در مدیریت و کنترل شبکه بوجود آورده است و ویژگی های خاصی را به شبکه ها اضافه کرده که به دنبال آن عملکردهای مختلف شبکه ها افزایش یافته و همزمان راه حل هایی برای مسائل دست و پاگیر موجود در شبکه های معمولی ارائه می دهد. کنترل متمرکز و قابلیت برنامه نویسی شبکه در SDN در سرعت بخشیدن به نمونه سازی و توسعه عملکردهای شبکه همکاری می کند . به طور کلی بیشتر توابع شبکه ای که در معماری های معمولی یافت می شوند ، می توانند به صورت پیاده سازی نرم افزار ساده در SDN ارائه شوند. امنیت شبکه همچنین از طریق اجرای ویژگی های SDN در محدوده نوآوری شبکه می باشد. علی رغم معرفی طرح های امنیتی جدید و تقویت برنامه های موجود که به نوبه خود ابزارها و مکانیزم های جدیدی برای امنیت شبکهٔ قوی تر فراهم می کند ، امنیت در SDN به طور کامل تضمین نمی شود. علاوه بر این ، لایه های اضافی و رابط های SDN به راحتی باعث ایجاد آسیب پذیری های جدید و تهدیدات امنیتی می شوند. آسیب پذیری ها و حملات شبکه در SDN بطور فزاینده ای پیچیده و پیچیده است. بنابراین ، امکان ظهور چالش های جدید که تحقیقات امنیتی را مجبور به شکل دادن به معماری SDN می کند، در تعامل مداوم با فن آوری های مختلف می باشد و سعی در ادغام عناصر و ویژگی هایی است که می توانند در ساخت چارچوب های امنیتی نوآورانه و چند رشته ای اعمال شوند. الگوریتم های یادگیری ماشین ، خدمات Cloud ، توابع شبکه مجازی ، نمونه های خوبی از فناوری هایی هستند که می توانند برای ساخت محیط امنیتی SDN نسل بعدی مشترک باشند. اگرچه تقریباً یک دهه از انتشار اولین پیشنهادات مربوط به امنیت SDN می گذرد اما تلاش های گسترده ای در زمینه های خاص لازم است تا ما بتوانیم شبکه های SDN را محیطی امن و قابل اعتماد در نظر بگیریم.

منابع

[1] Egilmez.H.E., Dane.s.t., Bagci.k.t. and Tekalp.a.m.(2012). OpenQoS: An OpenFlow Controller Design for Multimedia Delivery with End-to-End Quality of Service over Software-Defined Networks," Signal & Information Processing Association Annual Summit and Conference (APSIPA ASC) IEEE, pp. 1-8.

[2] Nunes, B.A.A., Mendonca, M., Nguyen, X.N., Obraczka, K., Turletti, T., 2014. A survey of software-defined networking: past, present, and future of programmable networks. IEEE Commun. Surv. Tutor. 16 (3), 1617–1634,

[3] Kim, H., Feamster, N., 2013. Improving network management with software defined networking. IEEE Commun. Mag. 51 (2), 114–119,

[4] Kreutz, D., Ramos, F.M.V., Verssimo, P.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S., 2015. Software-defined networking: a comprehensive survey. Proc. IEEE 103 (1), 14–76,

[5] Li, C.-S., Liao, W., 2013. Software defined networks. IEEE Commun. Mag. 51 (2) 113113.Lin, Z., Tao, D., Wang, Z., 2017. Dynamic construction scheme for virtualization security service in software-defined networks. Sensors 17 (4), 920

[6] H.Farhady., L.HyunYong. and N.Akihiro.(2015).Software-defined networking: A survey, Computer Networks 81, pp.79-95 .

[7] K. Li., W. Guo., W. Zhang., Y. Wen., C. Li. and W. Hu.(2014). QoE-based Bandwidth Allocation with SDN in FTTH Networks," Network Operations and Management Symposium (NOMS), IEEE, Vol. 18, pp. 1-8

[8] Azadolmolki. S. (2013) . Packt Publishing Software Defined Networking with OpenFlow, book onlin. https://www. packtpub. com/networking-and-servers/software-defined-networking-openflow

[9] Kreutz, D., Ramos, F., Verissimo, P., 2013. Towards secure and dependable software-defined networks. In: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. ACM, pp. 55–60.

[10] Juan . C ., Jenny , V., 2020. Security in SDN: A comprehensive survey .Universidad de Antioquia and Instituto Tecnolٰgico Metropolitano de Medellيn, Universidad de Medellيn, Universidad de Antioquia Calle, 67 # 53 – 108,

[11] Yoon, C., Shin, S., Porras, P., Yegneswaran, V., Kang, H., Fong, M., O'Connor, B., Vachuska, T., 2017b. A security-mode for carrier-grade sdn controllers. In: Proceedings of the 33rd Annual Computer Security Applications Conference. ACM, pp. 461–473.

[12] Yoon, C., Lee, S., Kang, H., Park, T., Shin, S., Yegneswaran, V., Porras, P., Gu, G., 2017a. Flow wars: systemizing the attack surface and defenses in software-defined networks.IEEE/ACM Trans. Netw. 25 (6), 3514–3530,

[13] Rpke, C., Holz, T., 2015. Sdn rootkits: subverting network operating systems of software-defined networks. In: International Workshop on Recent Advances in Intrusion Detection. Springer, pp. 339–356

[14] Nguyen, T.-H., Yoo, M., 2017. Analysis of link discovery service attacks in sdn controller. In: 2017 International Conference on Information Networking. ICOIN, pp. 259–261,

[15] Benton, K., Camp, L.J., Small, C., 2013. Openflow vulnerability assessment. In: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. ACM, pp. 151–152.