شـــــرکت ارتبـاطات زیرساخت وزارت ارتباطات و فناوری اطلاعات	**مقاله عنوان: بررسی احیای مسیر با استفاده از پروتکل مسیریابی BGP و شبکه های مبتنی بر نرم افزار** **تهیه کننده/گان: رشته تحصیلی رشته شغلی اداره کل/دفتر** **تاتینا صدیفی کارشناس مهندسی کامپیوتر نرم افزار فناوری اطلاعات اداره کل طرح و توسعه/ کارشناس طراحی شبکه** **علی زعیم کهن کارشناسی ارشد شبکه مدیر فناوری اطلاعات اداره کل طرح و توسعه/ معاون طراحی شبکه**
این قسمت توسط دبیرخانه کمیته علمی تکمیل می-گردد.	**شماره مقاله: ۶۹ حوزه کاربردی: شناسایی و معرفی چالش های شبکه موجود و لزوم حرکت به سمت شبکه های مبتنی بر نرم افزار (SDN)**

چکیده

اتصال اینترنتی پایان ناپذیر برای سبک جدید زندگی انسان کاملا ضروری است. از سوی دیگر، افزایش شدید میزان ترافیک شبکه باعث تشدید چالش‌ها برای تثبیت شبکه ای بدون اتلاف وقت شده است . پیچیدگی‌های پروتکل‌های مسیریابی و سازوکارهای مبنایی باید به درستی مورد بررسی قرار بگیرند. در این مقاله، ابعاد مختلف پروتکل مسیریابی ورودی مرزی [۱] (BGP) بررسی می‌شود، یعنی پروتکل مسیریابی مرتبط با سیستم‌های میاری خودمختار. امکان دارد که ناهنجاری‌های متعددی از طریق BGP به وجود آید که باید از طریق شبکه سازی مبتنی بر نرم افزار[۲] (SDN) بررسی شوند. در این مقاله، یک شبیه‌سازی نیز از طریق کنترل گر SDN- Ryu در Mininet برای BGP انجام گرفته و مشخص شده است که ادغام SDN با BGP باعث بهبود کارایی شبکه‌ها می‌شود.

I. مقدمه

توسعه مصارف جدید شبکه های کامپیوتری باعث بهبود زندگی انسان ها شده است. با این وجود، با افزایش طراحی اپلیکیشن های مختلف در اینترنت، برای نمونه اسکایپ، بانک داری الکترونیکی و باقی موارد، سازماندهی ترافیک به سرعت توسعه یافته است . این ترافیک شدید در سیستم ، سازماندهی انسدادها و یا قطع ارتباط را ضروری می سازد. در این روند انسداد یا قطع ارتباط، امکان از دست دادن بسته یا وقوع بی‌نظمی‌ها وجود دارد. این حالت سیستم تاثیری قابل توجه بر فعالیت ویدئوکنفرانس و تبادل وب محور دارد. برای مثال، تنوع، امنیت و سرعت سیستم باعث بروز مشکل برای فعالیت ابزارهای شبکه‌ای می‌شوند. دلیل این امر توسعه مستمر ترافیک سیستم است. بنابراین به منظور هدایت ترافیک سیستم، به چارچوب‌بندی و مهندسی دقیق سیستم نیاز است چون احتمال دارد ابزارهای فعلی شبکه با درخواست های تغییر ترافیک سیستم همخوانی نداشته باشند. درعوض تفکیک چارچوب سیستم، امکان مسیربندی مولفه های پروتکل وجود دارد. پروتکل مسیریابی ورودی

---

[۱] Border Gateway Routing Protocol

[۲] Software Defined Networking

مرزی نوعی پروتکل است که مسئولیت اینترنت را برعهده دارد. این پروتکل راه زیادی را پشت سر گذاشته و پیوسته باید به روزرسانی شود. به روزرسانی‌های مورد نیاز در هر شبکه متفاوت است . این امر به نیاز برای سفارشی سازی BGP منتهی شده است. شبکه‌یابی مبتنی بر نرم افزار (SDN) پلتفورمی را برای پرداختن به این چالش BGP فراهم می‌کند. کنترل‌گر Ryu در SDN دارای کتابخانه‌هایی برای BGP است.

ابعاد مختلف BGP را می‌توان مطابق با الزامات شبکه برنامه‌ریزی کرد. درضمن، در مسیر کاهش احیای مسیر شبکه۳ (NPR) بین سیستم‌های خودمختار، اجرای فناوری‌های نوظهوری مثل شبکه یابی مبتنی بر نرم افزار و پرو تکل مسیریابی به کار زیادی نیاز دارد . بنابراین نباید به این مسئله به روشی خودمختار نگاه کرد و در صورت استفاده BGP و SDN با یکدیگر کارایی بیشتری خواهد داشت . پروتکل ورودی مرزی (نسخه ۴)، پروتکل اصلی برای پیوند سیستم های خودمختار است. در واقع BGP پروتکل مسیریابی بردار مسیر (Path Vector) بوده و از متریک‌های ارائه شده در جدول ۱ برای انتخاب بهترین مسیر به سمت مقصد استفاده می‌کند.

جدول ۱: اولویت انتخاب مسیر BGP

اولویت	ویژگی سیاستگذاری
۱	بالاترین مقدار LOCAL-PREF
۲	پایین‌ترین مسیر AS
۳	پایین‌ترین Origin type
۴	پایین‌ترین ارزش MED
۵	یادگیری EBGP بر روی یادگیری IBGP
۶	پایین‌ترین هزینه IBGP
۷	پایین‌ترین مشخصه مسیریاب (Router ID)

بسیاری از ناهنجاری‌ها در BGP در نتیجه سیاست نادرست مسیریابی، رشد ترافیک شبکه، ویژگی های ذاتی و باقی موارد پدیدار می شوند. این ناهنجاری‌ها باعث شده تا بسیاری از محققان به سمت بررسی مسائل مرتبط با پروتکل BGP روی بیاورند. شبکه‌یابی مبتنی بر نرم افزار نوعی فرآیند مهندسی است که هدفش هماهن گ‌سازی و سازگاری شبکه هاست. هدف SDN بهبود کنترل سازماندهی از طریق ارتقای توانایی تامین‌کنندگان خدمات اینترنتی برای واکنش سریع به ضروریات متغیر دنیای کسب وکار است. این برنامه به ابزارهای شبکه امکان می دهد تا فعالیتی مجزا و خودمختار داشته باشند. به این طریق، ابزارها مطابق با خواسته مشتریان فعالیت داشته و تحت هدایت کنترلر SDN قرار دارند.

---

[۳] Network Path Restoration

II. پیشینه

دسترسی به وب اهمیت فزاینده ای برای سبک فعلی زندگی انسان ها دارد. افزایش شدید میزان ترافیک شبکه باعث تشدید مشکلاتی برای تثبیت شبکه‌ای بدون اتلاف شده است. در این بین، مسیریابی پروتکل و همچنین برنامه‌ریزی سازوکار احیای مسیر شبکه اهمیت زیادی دارد.

مسیر ارسال ترافیک شبکه از یک سیستم به سیستم بعدی توسط مسیریاب با عنوان فرآیند «مسیریابی» شناخته می شود. انواع مختلف مسیریابی در شکل زیر نشان داده شده است:

شکل ۱: انواع مسیریابی

پروتکل‌های ویژه‌ای برای گسترش این مسیریابی ها وجود دارد. برای مثال، برای اجرای مسیریابی پویا، سه نوع پروتکل ویژه برای موقعیت های مختلف وجود دارد (شکل ۲).

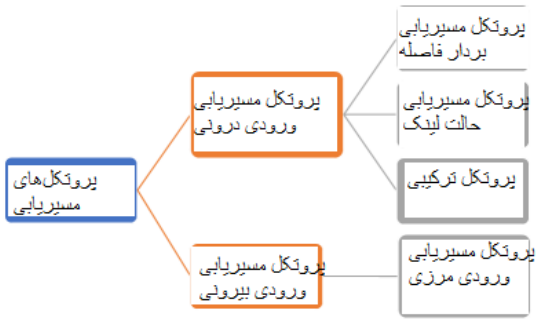
شکل ۲: انواع پروتکل‌های مسیریابی پویا

در بالاترین بعد، اینترنت در بین هزاران سیستم خودمختار [۴] (ASes) فعالیت دارد . پروتکل ورودی مرزی (BGP) ساختار استاندارد اشتراک‌گذاری میان سیستم های خودمختار است. مسیریاب BGP می‌تواند به صورت درونی یا بیرونی باشد.

---

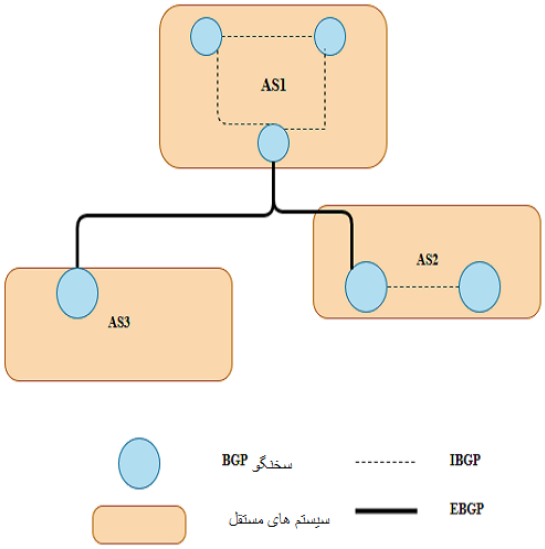
[۴] Autonomous System

شکل ۳: انواع پروتکل‌های مسیریابی



در سناریوهای واقعی، سیستم خودمختار از چندین مسیریاب متفاوت BGP تشکیل می‌شود (شکل ۴). مسیریاب‌های سخنگوی BGP برای رسیدن به ثبات لازم، به روزرسانی ها را با یکدیگر به تبادل می گذارند. این سخنگوهای BGP در صورت ادغام با دیگر سخنگوهای BGP حاضر در سیستم خودمختاری مشابه، به عنوان IBGP شناخته می‌شوند. اگر سخنگوهای حاضر در سیستم های خودمختار متفاوتی با هم ترکیب شوند، در این صورت EBGP شکل می‌گیرد. در ساده‌ترین حالت ممکن، هر مسیریابی دارای یک جلسه IBGP با هر مسیریاب بیرونی است، درنتیجه آرایش «شبکه کل» به وجود می‌آید. این طراحی همزمان با افزایش معیار سیستم خودمختار، مقیاس‌بندی را کنار می‌گذارد.

شکل ۴: سیستم‌های بین AS که از طریق مسیریاب‌های BGP متصلند



پروتکل ورودی مرزی (BGP) همان پروتکل قراردادی برای مسیریابی سیستم بین AS است. مراجعه‌کنندگان با تامین‌کننده خدمات اینترنتی[۵] (ISP) تعامل دارند. این تامین کنندگان از BGP به عنوان ابزاری قراردادی برای آغاز کار با یک ISP و سپس رفتن به ISP دیگر استفاده می‌کنند. این ابزار یک پروتکل مسیریابی بردار مسیر بوده و مکانیسم ضد Loop را در اختیار دارد . سخنگوهای BGP قادر به تبادل به روزرسانی‌های مسیریابی با یکدیگر هستند. این روند با تکیه بر سیاست مسیریابی انجام می‌شود. زمانیکه سخنگوی BGP به روزرسانی‌ها را به

[۵] Internet Service Provider

جفت BGP خودش ارسال می کند، ارسال کننده باید منتظر حداقل بازه انتشار مسیر۶ (MRAI) باشد تا انتشار دیگری را در ارتباط با شبکه‌های مقصد ارسال کند. رویکرد هدایت مسیر شبکه شاید از اولویت های محلی، تعداد سیستم های خودمختار و تفکیک گر چند خروجی تشکیل شود.

پروتکل مسیریابی BGP تعمیم‌های زیادی در اختیار دارد. مشکلات در BGP، مثل تاخیر بیشتر به دلیل بی ثباتی سیستم، باید توسط مولفه‌ای بررسی شود که قادر به بهبود سرعت شبکه پروتکل اینترنت است.

گستره مسائل در BGP ابعاد مختلفی دارد، از جمله تاخیر همگرا یی، مقیاس پذیری هدایت چندگانه، عدم تطابق سیاست مسیریابی، طرح مسیریابی چند مسیره، امنیت و مقیاس‌پذیری، فقدان عملکرد مناسب در پارامترهای کیفیت خدمات و اعلان‌های چندتایی.

فارغ از روند سازگارسازی ظرفیت های BGP که باعث تطابق آنها در احیای مسیر شبکه می شود، مسئله سفارشی سازی پروتکل‌ها به آینده اینترنت ارتباط دارد. اخیرا، شبکه‌یابی مبتنی بر نرم افزار (SDN) علائق متفاوتی را برای مدیریت طراحی شبکه در ارتباط با سفارشی سازی پروتکل‌های مسیریابی شکل داده است. این فرآیند به سازمان‌های خلاق اجازه می‌دهد تا علاقه به اینترنت را در درون سازمان شکل دهند . در این بین، توجهات تنها به سمت تاثیر BGP و SDN بر سرعت و سازگاری در ترافیکی عظیم سوق یافته اند. پیوند این دو ممکن است باعث بهبود سرعت، امنیت و سازگاری شود . در این مقاله، توپول وژی سیستم از BGP به عنوان ابزار ارسال بسته و SDN به عنوان نمایش کنترل‌کننده استفاده کرده است. شبکه‌یابی مبتنی بر نرم افزار امکان تشخیص BGP را به وجود آورده و باعث ترکیب BGP و SDN می‌شود. حاصل این ترکیب، رسیدن به NPR و حداقل مقدار ضرر بسته است . گستره مسائل در BGP ابعاد مختلفی دارد، از جمله تاخیر همگرایی، مقیاس‌پذیری هدایت چندگانه، عدم تطابق سیاست مسیریابی، طرح مسیریابی چند مسیره، امنیت و مقیاس پذیری، فقدان عملکرد مناسب در پارامترهای کیفیت خدمات و اعلان‌های چندتایی.

III. مسائل و چالش‌ها: BGP

اعلان‌های چندتایی: اندازه رو به رشد جدول مسیریابی

پروتکل BGP موردی از محاسبه مسیریابی بردار فاصله بلمان- فورد[۷] است. این محاسبه امکان جمع آوری سخنگوهای BGP را به منظور آشنایی با توپولوژی کلی سیستم واسط به وجود می آورد. روش مورد نیاز برای این محاسبه بسیار شفاف و صریح است: هر سخنگوی BGP به تمامی همسایه‌ها اطلاعاتی را در مورد تغییر یا عدم تغییر چشم انداز سیستم توسط داده‌های جدید ارائه می‌دهد.

این خصوصیت به افزایش اندازه جدول مسیریابی منتهی شده و تاخیرهای طولانی را در جستجوی ورودی مسیر از جدول مسیریابی BGP به وجود می‌آورد.

---

[۶] Minimum Route Advertisement Interval

[۷] Bellman-Ford

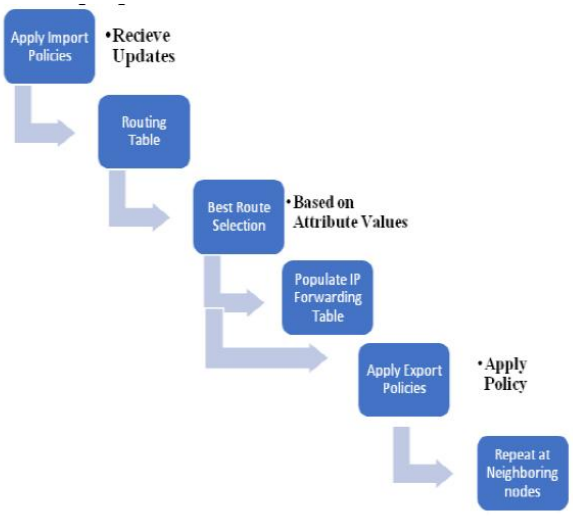
Ghost Entries

هیچ تایمر به روزرسانی در BGP وجود ندارد، درنتیجه مسیریاب فاقد آخرین ورودی های به روزشده خواهد بود . این وضعیت به شکل گیری ورودی‌های روح[۸] منتهی می‌شود چون این پسوندهای مقصد هرگز در دسترس نخواهند بود.

عدم تطابق سیاست مسیریابی

سخنگوهای BGP داده‌های خود را در تطابق با سیاست های مسیریابی به اشتراک می گذارند. این وضعیت ممکن است حتی با انتخاب بهترین مسیر با مخالفت روبرو شود.

شکل ۵: پویایی انتخاب مسیر BGP



علاوه براین، BGP از ابتدای طراحی اش با چالش ها و احتمالات جدید تکامل یافته است . یکی از چالش ها این حقیقت است که BGP تنها پروتکل بیرونی پیونددهنده سیستم های بین AS است. هر سیستم بین AS توسط چندین اپراتور با نیاز به سازگاری انتقال های چند مسیره کنترل می‌شود. این احتمال همکاری بسیار شدید بوده و باعث پیدایش فرصت‌های جدید می‌شود.

MRAI: کاهش به روزرسانی‌ها و افزایش تاخیر

زمانی‌که سخنگوی BGP به روزرسانی‌ها را به نظیر یا همسایه خودش ارسال می کند، فرستنده باید منتظر حداقل بازه اعلان مسیر (MRAI) باشد تا اینکه اعلان دیگری را در مورد شبکه‌های مقصد مشابه ارسال کند. احتمال دارد که MRAI در نهایت تعداد به روزرسانی‌ها را به بهای تاخیر اضافی کاهش دهد.

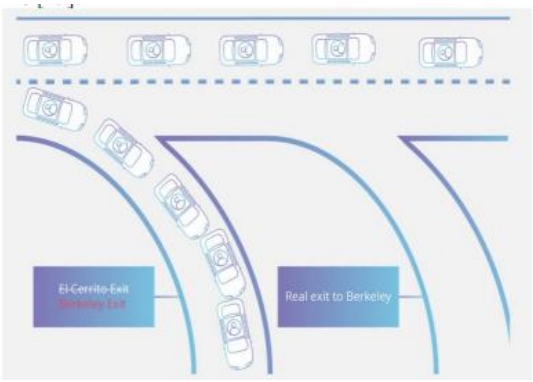
---

[۸] Ghost entry

سرقت BGP

سرقت BGP زمانی رخ می‌دهد که مهاجمان به شکلی خرابکارانه مسیر ترافیک اینترنت را تغییر می‌دهند. مهاجمان این کار را با اعلان دروغین مالکیت گروه‌های آدرس IP، به نام پیشوندهای IP، کنترل برآنها و سپس مسیریابی جدید انجام می دهند. سرقت BGP مشابه با تغییر تمامی علائم در یک شاهراه و مسیربندی مجدد رفت‌وآمد ماشین‌ها به سمت خروجی‌های نادرست است.

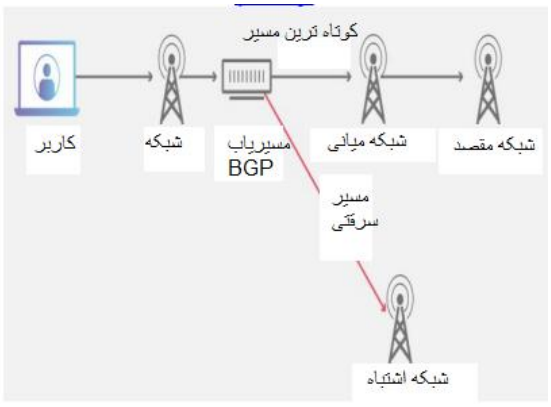
شکل ۶: مسیریابی مجدد ترافیک به سمت خروجی اشتباه



امنیت: مسیریابی سیاه چاله

درنتیجه سرقت پیشوند، ترافیک مخرب و قانونی به مسیر یا گره ای سوق داده می شود که به نام مسیریابی سیاه چاله شناخته می شود. اگر پروتکل از UDP فاقد اتصال استفاده کند، فرستنده پاسخ یا هشدار در مورد بسته گم شده را دریافت نخواهد کرد . هرچند، BGP از TCP استفاده می‌کند چون اتصال محور بوده و به اتصال سه مسیره برای دریافت هشدار در مورد بسته‌های گم شده نیاز دارد.

شکل ۷: مسیریابی سیاه چاله



IV. شبکه مبتنی بر نرم افزار

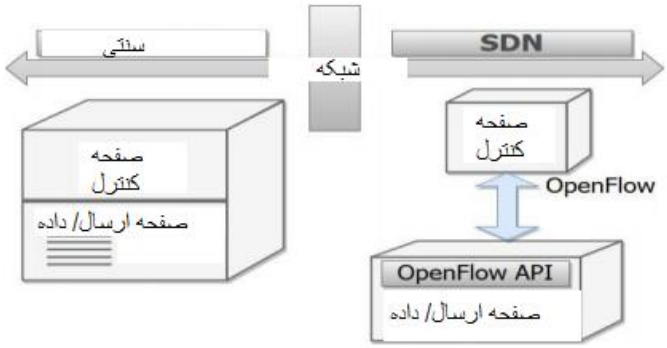
شبکه‌های مبتنی بر نرم افزار را می توان از طریق دیدگاه چشم اندازهای مبادلاتی به تصویر کشید. این شبکه‌ها از طریق کنترلر ها، قراردادها و واسطها اجرا می‌شود. ایده SDN از این مسئله نشات گرفته که افراد از چارچوب محاسبه توزیعی برای تفکیک چارچوب کاری از ابزارها استفاده

می‌کردند. شکل ۹ چشم انداز زیرساخت ابری را نشان داده که در آن ابزارها با سوئیچی ویژه محدود شده و سوئیچ موجود در مرز بعدی با جمع آوری ابزارها و تکمیل دسترسی و کارایی شبکه ارتباط دارد.

شکل ۹: زیرساخت ابری

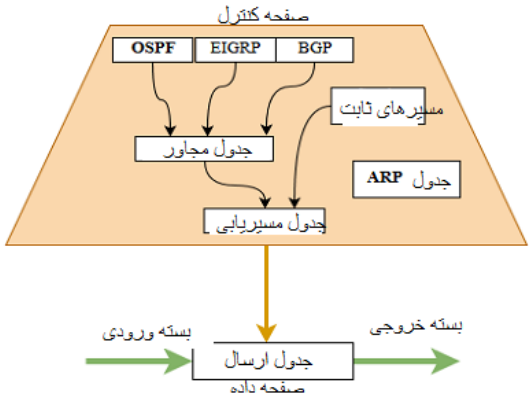
طراحی SDN به کنترلر اجازه می‌دهد تا ابزارهای مخصوص مسیریاب ها و سوئیچ‌ها را سازماندهی کند. به دلیل نزدیکی یک کنترلر ، ابزارهای مختلف بر همین مورد برای به روزرسانی سیستم تکیه دارند . در چارچوب‌های استاندارد و مرسوم، ابزارهای اجرای سیستم در حکم جهشی کامل از صفحه ارسال (مولفه‌های سخت افزار) و صفحه کنترل (سیستم عامل) است. کار SDN جداسازی صفحه ارسال و کنترل است. شکل ۹ بررسی چارچوب‌های سنتی و SDN را نشان می‌دهد.

شکل ۹: شبکه سنتی در برابر شبکه‌های SDN



در SDN، صفحه جداسازی ، بعدی باورنکردنی از سازگاری را شکل می دهد که تاثیر چارچ وب را برجسته ساخته و درنتیجه فضا را برای پروتکل‌ها و اپلیکیشن‌های جدید آماده می‌سازد. شکل ۱۰ دیدگاه تفکیکی طراحی SDN را نشان می‌دهد.

شکل ۱۰: معماری جداشده SDN



همانطوری که در بنیاد شبکه سازی آزاد (ONF) گفته شده، غیرمرسوم بودن کاربرد های موجود باید توسط خصوصیات SDN مورد توجه قرار گیرند، برای نمونه پویایی، مزیت مالی و معقول بودن. آرایش SDN از سه لایه تشکیل می‌شود:

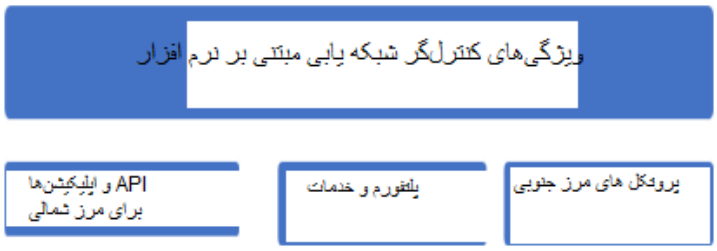
(۱) لایه زیرساخت

(۲) لایه کنترل

(۳) لایه کاربرد

لایه زیرساخت توانایی توصیف صفحه ارسال یا د اده را در اختیار دارد . لایه کنترل با کنترل گرهای مختلف به تصویر کشیده می شود، مثل NOX، POX، Ryu و باقی موارد. لایه اپلیکیشن با اپلیکیشن هایی مثل فایروال، متعادل کننده بار و باقی موارد نشان داده می شود. ابزارهای متفاوتی مثل POX، Ryu و OLD برای ایجاد صفحه کنترل وجود دارد . این ابزارها زمینه را برای متخصصان و محققان برای ساختاربندی سیستم‌ها فراهم می‌کنند. شکل ۱۱ ویژگی‌های کنترل‌گر SDN را نشان می‌دهد.

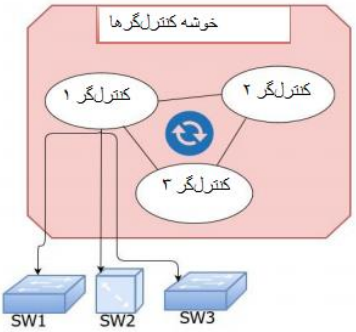
شکل ۱۱: ویژگی‌های کنترلر SDN



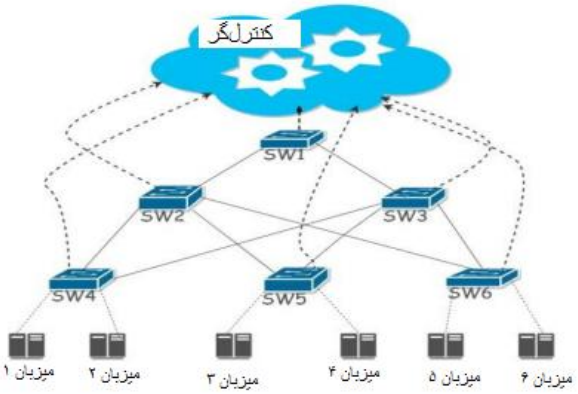
به دلیل اینکه هدف این بررسی پرداختن به احیای مسیر شبکه با حداقل تاخیر است، SDN مولفه تحمل خطا را ارائه می کند. این پروتکل که صفحه کنترل و ارسال / داده را به هم پیوند می زند، OpenFlow (نسخه ۱.۵.۱) است. این پروتکل رابطه چندین کنترلر به یک سوئیچ را امکان‌پذیر می‌سازد به طوریکه اگر یک کنترلر با مشکل روبرو شود، کنترلر بعدی در دسترس خواهد بود. شکل ۱۲، SDN را به شکل مهندسی تحمل خطا نشان می‌دهد.

علاوه براین، به دلیل نزدیکی کنترل‌گر، به تعویق افتادگی رخ داده در شناسایی خطای شبکه کمتر از سیستم های عادی خواهد بود. شکل ۱۳، SDN را با دیدگاه کنترل‌گر مرکزی نشان می‌دهد.

شکل ۱۲: SDN به عنوان معماری تحمل خطا



شکل ۱۳: کنترلر مرکزی SDN



در یک تحقیق روشی خاص پیشنهاد شده که برای متقارن سازی زمان و تازه سازی سیستم استفاده می شود. به روزرسانی همیشگی مسیر سیستم باعث بروز ناهنجاری های مختصری می شود، برای نمونه حلقه های ترافیکی، فشردگی و باقی موارد . این به روزرسانی ها باید برای محدودسازی مشکلات مطرح شده اجرا شوند. سیستم مورد نظر TIME4 است که به متقارن‌سازی ساعتی در میان سوئیچ‌ها و کنترل‌گرها نیاز دارد. مدل ارائه شده باعث بهبود عملکرد شبکه و رویکرد امنیتی می شود. علاوه براین، SDN باید از طریق مهندسی ترافیک بررسی شود. برای رسیدن به این هدف، مدیریت جریان، متعادل‌سازی بار، تحمل خطا و پیوستگی باید به دقت تحت کنترل باشند.

V. چالش‌ها و مسائل: SDN

این بخش به بررسی ویژگی‌ها، مزایا، معایب، مسائل و چالش‌های مکانیسم‌های فوق می‌پردازد.

A. SDN- سرعت و امنیت

مزایای SDN عبارتند از تنوع، ظرفیت انتقال بهتر، ظرفیت سفارشی سازی پروتکل ها و اپلیکیشن های مسیریابی، کاهش فشردگی شبکه و انعطاف پذیری. شبکه‌یابی مبتنی بر نرم افزار فرآیند رمزگذاری را انجام نمی دهد بلکه یک سیستم خصوصی مجازی بوده و از اینترنت همگانی

مجزاست. به این شکل، SDN به عنوان حالت انتقال محافظت شده درنظر گرفته می شود. هرچند، این شبکه به ح ملات DDOS آسیب‌پذیر است، امری که بر شبکه‌ها تاثیر می‌گذارد.

B. SDN- هزینه

در بخش مثبت، SDN اجازه استفاده از چندین پیوند اینترنتی ارزان و با پهنای باند زیاد را صادر می کند. هرچند، هزینه سوئیچ ها و کنترل‌گرهای SDN بیشتر از سوئیچ‌های سنتی است. علاوه سوئیچ‌ها و کنترل‌گرهای SDN، پهنای باند هم نقشی مهم ایفا کرده و هزینه شبکه SDN را تحلیل می‌کند. این معادله هزینه را می‌توان به این صورت نشان داد: هزینه = α (S) + β (C) + Y (B)

S = هزینه سوئیچ‌های SDN

C = هزینه کنترلر

B = شارژهای کاربرد پهنای باند

α, β, Y ناهمگنی فاکتورهای هزینه را نشان می‌دهند. علاوه براین، SDN به کاربرد جریانی کارکنان نیز اشاره دارد.

C. SDN- عملکرد

از سوی دیگر، SDN از اینترنت عمومی استفاده می کند. اینترنت عمومی آسیب‌پذیری بیشتری به اتلاف بسته، Jitter و تاخیر دارد، بنابراین عملکرد SDN تضمین نخواهد شد. برای همین، SDN عملکرد بهتر از نظر مقیاس پذیری و دسترسی در طول کارایی منبع را تضمین می کند ولی هیچ تضمینی برای کیفیت خدمات وجود ندارد.

D. BGP-SDN- سرعت همگرایی

علاوه براین، BGP مزایای زیادی در ارتباط با مسائلی خاص در اختیار دارد، برای نمو نه رشد جدول مسیریابی، بی ثباتی، همگرایی کندتر و امنیت. این مشکلات با پیوند معماری شبکه با SDN حل می‌شوند. به دلیل وجود کنترلر مرکزی در SDN، فرآیند توزیع حالت تسریع یافته و به دلیل وجود دیدگاهی جامع در کنترل، تصمیم برای مسیر جایگزین برمبنای به روزرسانی‌ها خواهد بود.

جدول ۲: مقایسه شبکه‌های مبتنی بر نرم افزار و سنتی

Metrics	Existing Network	SDN
Network Perspective	Hardware Dominated	Software Dominated
Configuration Control	Hardware Vendor	User
Technology Openness	Closed Structure	Open Structure
Interlock Compatibility	Independent Protocol	Standardized Protocol
Managerial efficiency	Low-efficiency/ high cost operation	High-efficiency / Logical Operation
New Technological Adoption	Acc to the vendor needs	Acc to users' needs
Market Fairness	Monopoly	Fair Competition

SDN- تشخیص سریع

زمان شناسایی مشکل و هماهنگ سازی منابع برای حل مسئله در SDN حالتی حداقلی دارد.

A. مقایسه SDN/ شبکه موجود

مزیت SDN این است که معماری ترافیک شبکه در نقطه مرکزی قرار م ی‌گیرد و به راحتی سیاست‌ها را در تمامی ابزارهای WAN به کار می‌برد. جدول ۲ مقایسه بین شبکه‌یابی سنتی و مبتنی بر نرم افزار را نشان می‌دهد.

علاوه براین، SDN دارای کنترلرهای مختلفی است. جدول ۴ مقایسه سه کنترلر بر Mininet را نشان می دهد. این ابزار، مقلد شبکه SDN بوده و نشان می‌دهد که عملکرد شبکه با ابزار Iperf صورت می‌گیرد. این ابزار نشان می‌دهد که BGP تنها از طریق کنترل RYU اجرا می‌شود.

جدول ۳: خلاصه مقایسه کنترل‌گرهای SDN

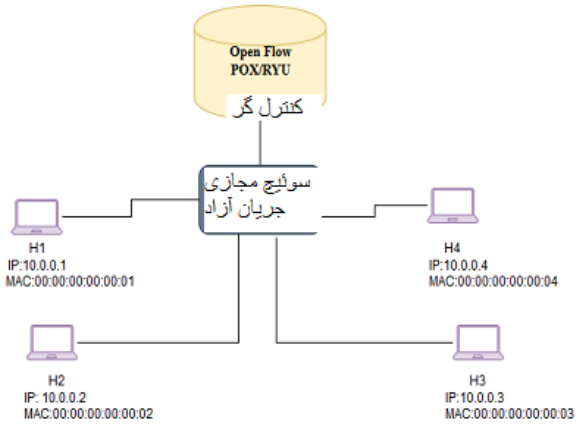
	NOX	POX	Ryu
Language	C++	Python	Python
Performance	Fast	Slow	Slow
OpenFlow	1.0/1.3	1.0	1.0 - 1.4
BGP Library	No	No	Yes
MPLS Library	No	Yes	Yes

VI. بستر تست پایلوت

توپولوژی موجود در شکل ۱۴ نشاندهنده ۴ میزبان با آدرس‌های پروتکل اینترنت و MAC است. تمامی میزبان‌ها به سوئیچ مجازی جریان آزاد (نسخه ۲.۰.۲) اتصال دارند. کنترل‌ها بر روی بسترهای Ubuntu 14.04.0 LTS VM، با ۸TM)Core(R) Intel(RAM GB) i7-7500 CPU @ 2.70GHZ فعالیت دارند. سوئیچ با POX (نسخه ۰.۲.۴) و سپس Ryu (نسخه ۴.۱۰) اجرا می شود. هر دوی این کنترل‌ها بر python استوار بوده و در پورت ۶۶۳۳ فعالیت دارند.

توپولوژی اجراشده با کنترلر POX و Ryu بر روی Mininet فعالیت دارد، یعنی مقلد شبکه SDN. عملکرد شبکه هم با ابزار Iperf ثبت می‌شود (جدول ۵). نتایج اجرا در جدول ۶ ارائه شده‌اند.

شکل ۱۴: توپولوژی ۴ میزبان سوئیچ مجزا



جدول ۴: جدول مورد استفاده از انجام آزمایش

ابزارهای مورد استفاده
Mininet- مقلد شبکه برای **SDN**
Iperf- ابزار اندازه گیری عملکرد شبکه

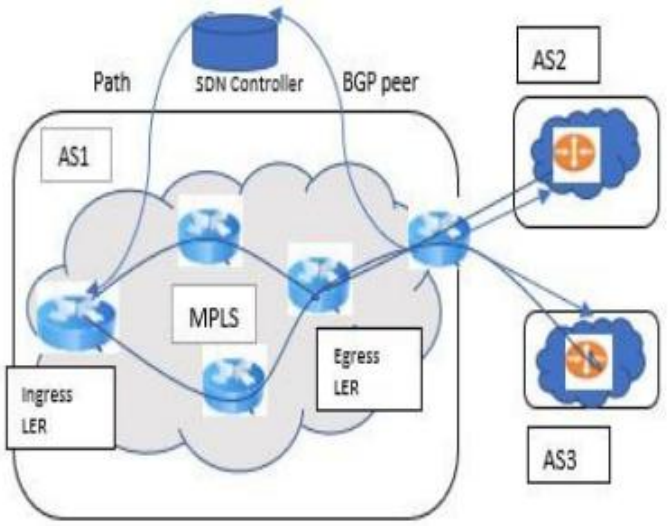
جدول ۵: عملکرد شبکه POX و Ryu

Parameters	POX	Ryu
Round Trip Time	3.0129(ms)	0.036(ms)
Throughput	5.01Gbit/sec	5.81 Gbit/sec
Web Server Latency	4.6(ms)	3.5 (ms)
BGP Library	No	Yes
MPLS Library	Yes	Yes

بررسی فوق نشان داد که برای طراحی و توسعه مکانیسم ارت قایافته احیای مسیر شبکه، کنترل Ryu دارای پتانسیل کتابخانه های BGP و MPLS است. این کنترل دارای مقدار تاخیر سرور وب و RTT کمتری است. کنترل Ryu راه ساده‌ای را برای اجرای SDN/ OpenFlow در بستر آزمایش و همچنین در توپولوژی‌های واقعی فراهم می‌سازد.

بحث فوق تضمینی بر رویکردی یکپارچه از BGP و SDN است. شکل ۱۵ معماری پیشنهادی برای رسیدن به نتایج ارتقای کیفیت خدمات در BGP را نشان می‌دهد.

شکل ۱۵: معماری پیشنهادی



توپولوژی فوق از طریق Minimet، Quagga، کنترل SDN اجرا شده است. معماری Mininet شبکه مجازی OpenFlow را با کنترل، میزبان‌های سوئیچ و لینک‌ها ایجاد کرده و امکان طراحی توپولوژی‌های ویژه با استفاده از متن های Python را به وجود می‌آورد. این معماری به یکی از ابزارهای برجسته تقلید در این زمینه تبدیل شده چون چندین عنصر از شبکه‌یابی مبتنی بر نرم افزار را به کار می‌برد. این ابزار که در دانشگاه استنفورد طراحی شده، یک مقلد منبع باز است که واسط قابل برنامه ریزی را برای تعریف و ساخت آرایش شبکه با عناصر مجازی ارائه می‌دهد. در این جا، Mininet بر روی Vmware 12.5.1 نصب شده است. سیستم‌های مرتبط با AS2 و AS3 بر روی Quagga اجرا شده‌اند. Quagga مجموعه نرم افزار مسیریابی شبکه است که اجرای پروتکل های مسیریابی را امکان پذیر می کند، برای نمونه ارسال کوتاه‌ترین مسیر باز[۹] (OSPF)، پروتکل اطلاعات مسیریابی[۱۰] (RIP)، BGP.

---

[۹] Open Shortest Path Forwarding

[۱۰] Routing Information Protocol

شکل ۱۶: اسکرین شات از سیستم VMware در حال اجرای Mininet

در تحقیق حاضر، پروتکل ورودی مرزی (BGP) بر روی Quagga اجرا شده است. برای تامین هدف کنترل، SDN-Ryu از کتابخانه BGP در Python پشتیبانی می‌کند. برای این منظور، فایل‌هایی با عناوین «bgpspeaker.py, bgpapplication.py» استفاده شده است.

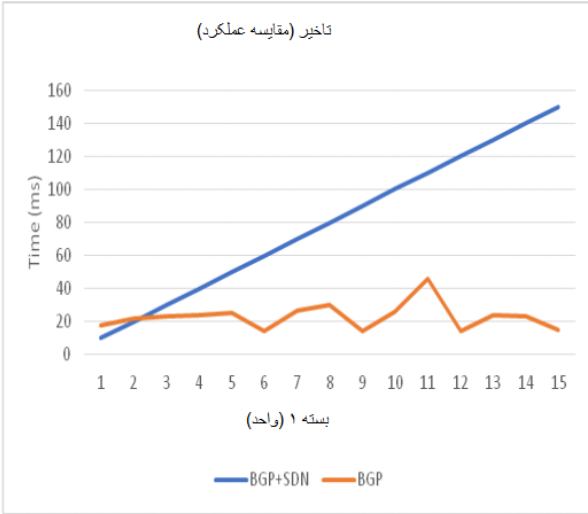
جدول ۶: اجزای کلیدی طراحی شبکه آزمایش شده

مولفه‌ها	ابزار / واسط	شمارش	آرایش	توصیف
ابزار شبکه	مسیریاب	۴ (Inter-AS) + ۲ (Intra-AS)	۷۲۰۰ سری مسیریاب سیسکو	این مسیریاب ها برای آرایش‌های MPLS و BGP، برای Inter-AS و EIGER برای ارتباط Intra-AS شکل می‌گیرند.
پهنای باند	لینک‌های سریالی	۵	64000 Kbps	پهنای باند لینک شبکه که برابر است با مقدار بیت های داده انتقالی در یک زمان مشخص
	اترنت سریع	۳	100 Mbps	
اندازه پنجره	اندازه درخواست Ping	۵	۵۶ بایت	تعداد بیت های داده قابل انتقال بدون انتظار برای تائید

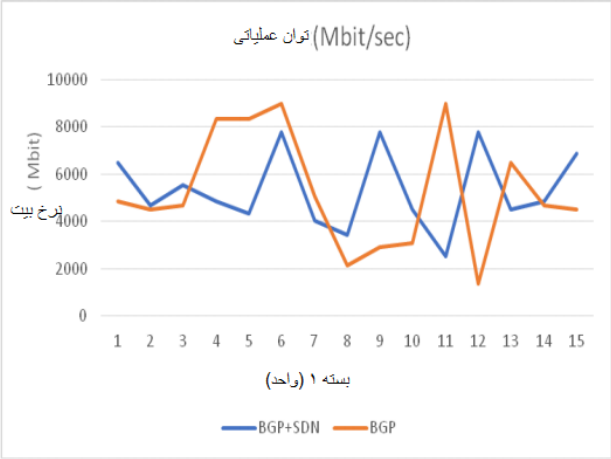
VII. نتایج و بحث

نمودارهای ارائه شده در شکل ۱۷ و شکل ۱۸ برای تاخیر و توان عملیاتی هستند . این مسئله نشان می دهد که رویکرد تلفیقی سازوکارهای مختلف عملکرد چندان بهتری در مقایسه با BGP ندارد. دلیل این امر این است که کنترلر SDN شاید باعث افزایش تاخیر ارتباط بین گره مشتری و کن ترل شود . همین مسئله بر توان عملیاتی نهایی ت اثیر خواهد گذاشت . هرچند، کنترلر SDN باعث انعطاف پذیری روند سفارشی‌سازی سازوکارهای مسیریابی از میان کتابخانه‌های سیستم شود.

شکل ۱۷: مقایسه عملکرد BGP و BGP + SSN با توجه به تاخیر

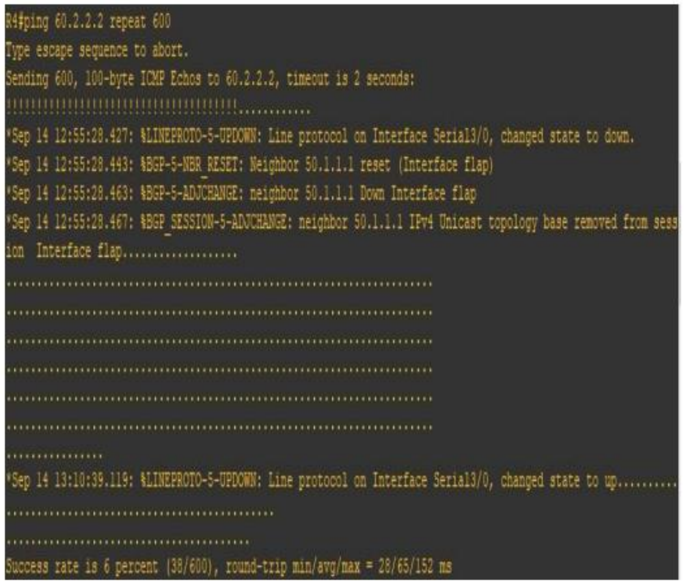


شکل ۱۸: توان عملیاتی (مقایسه عملکرد)

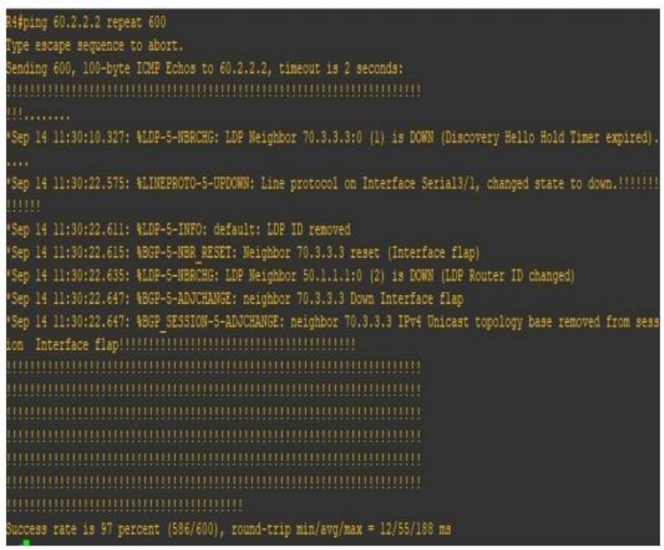


شکل ۱۹ و شکل ۲۰ نشاندهنده زمان مورد استفاده توسط مسیریاب ها برای احیای مسیر شبکه هستند، البته اگر یک گره یا واسط در مسیر مقصد عملکرد ناقصی داشته باشد. هرچند، تصاویر ارائه شده در شکل ۱۹ و ۲۰ به این اشاره دارند که مسیریابی که از BGP استفاده کرده به زمان بسیار بیشتری برای احیای مسیر نیاز داشته و بسته های بیشتری هدر رفته‌اند. این امر بیانگر این است که کنترلر SDN نتایج بهتری در ارتباط با حداقل اتلاف بسته در زمان احیای بسته شبکه دارد . با این وجود، در مورد تاخیر و توان عملیاتی، سیاست مسیریابی باید به منظ ور رسیدن به نتایج مثبت‌تر اصلاح شود.

شکل ۱۹: احیای مسیر شبکه با BGP



شکل ۲۰: احیای مسیر شبکه با MPLS + BGP + SDN



VIII. نتیجه گیری

پروتکل مسیریابی BGP باید مطابق با شرایط حاکم به روزرسانی شود . کنترل SDN-Ryu پتانسیل سفارشی سازی رفتار BGP را در اختیار دارد. این مقاله در ابتدا کنترل POX و RYu در SDN را از طریق شبیه سازی در Mininet مورد بررسی قرار دادیم. در این بین، SDN-Ryu از کتابخانه‌های BGP پشتیبانی کرده است. نتایج به دست آمده از شبیه سازی دیگر در Quagga و SDN-Ryu نشان داد که رویکرد تلفیقی BGP و SDN پتانسیل بالایی برای احیای مسیر شبکه و حداقل سازی اتلاف بسته دارد . هرچند برای رسیدن به تاخیر کمتر و توان عملیاتی بالاتر، سیاست‌های مسیریابی BGP باید تغییر داده شوند، در غیراین صورت، کنترل SDN ممکن است باعث افزایش تاخیر در ارتباط بین گره مشتری و کنترل‌گر SDN شود. همین امر بر توان عملیاتی تاثیر خواهد گذاشت.

مراجع

1. F. Hu, Q. Hao, and K. Bao, "A survey on software-defined network and OpenFlow: From concept to implementation," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 4, pp. 2181–2206, 2014.
2. K. Bakshi, "Considerations for Software Defined Networking (SDN): Approaches and use cases," *IEEE Aerosp. Conf. Proc.*, pp. 1–9, 2013.
3. S. U. Masruroh, A. Fiade, M. F. Iman, and Amelia, "Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP," *Proc. - 2017 Int. Conf. Innov. Creat. Inf. Technol. Comput. Intell. IoT, ICITech 2017*, vol. 2018–Janua, pp. 1–7, 2018.
4. B. Al-Musawi, P. Branch, and G. Armitage, "BGP Anomaly Detection Techniques: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 1, pp. 377–396, 2017.
5. Y. Rekhter, "A Border Gateway Protocol 4 (BGP-4)," 1995.
6. L. Todd, *CCNA Routing and Switching Study Guide: Exams 100-101, 200-101, and 200-120*. 2013.
7. Jeff Doyle, *CCIE Professional Development Routing TCP/IP, Volume I, Second Edition*, vol. I, no. 1919. 2005.
8. R. Musunuri and J. A. Cobb, "An overview of solutions to avoid persistent BGP divergence," *IEEE Netw.*, vol. 19, no. 6, pp. 28–34, 2005.
9. R. B. Da Silva and E. S. Mota, "A Survey on Approaches to Reduce BGP Interdomain Routing Convergence Delay on the Internet," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2949–2984, 2017.