یک سیستم مدیریت شبکه برای رسیدگی به جریان های داده های علمی

چکیده

انتقال های اطلاعات علمی حجیم اغلب با سرعت های بالایی انجام می شوند که این خود باعث نوسان افزایش یافته در ترافیک اینترنت می شود. به منظور محدود کردن اثرات مضر این چنین جریان های حجیم با سرعت بالا، که به آنها جریان های α گفته می شود، برروی جریان های ویدیو/صوت حساس به تاخیر، یک سیستم مدیریت شبکه به نام سیستم مهندسی ترافیک جریان آلفا (AFTES) برای مهندسی ترافیک درون قلمرو پیشنهاد شده است. یک روش آفلاین استفاده شده است که در آن AFTES رکورد های نت فلو جمع آوری شده توسط روترها را آنالیز می کند، پیشوندهای آدرس منبع-مقصد را استخراج می کند، و از این پیشوندهای برای پیکربندی فیلترهای فایروال در روترهای ورودی شبکه یک ارائه دهنده استفاده می کند تا جریان های α آینده را به مسیرهای طراحی شده ترافیکی و صف های مجزا را دوباره هدایت می کند. سودمندی این طرح از طریق آنالیز هفت ماه از اطلاعات نت فلو بدست آمده از یک روتر شبکه علوم انرژی (Esnet) ارزیابی شده بود. درمورد این مجموعه اطلاعات، 91٪ از بایت های تولید شده توسط جریان های α در طول بازه های با سرعت بالا ممکن بود هدایت شوند اگر که AFTES بکارگرفته شده بود. همچنین، جنبه منفی استفاده پیشوندهای آدرس در فیلترهای فایروال، یعنی، هدایت دوباره جریان های β به صف ها / مسیرهای جریان α،بصورت کمی درآمده بودند .

کلید واژه ها: آنالیز برافیک نت فلو. جریان های فیلی. محاسبه علمی. شبکه های آموزش و تحقیق (RENs). MPLS.مدارهای مجازی

1. مقدمه

کاربردها محاسبه علمی در رشته های از قبیل فیزیک انرژی بابا، علم اقلیم، ژنومیک، و ...، مجموعه اصلاحات (با اندازه های ترا تا پتا بایت) حجیم تولید می کنند[1]. جهت انتقال این مجموعه های داده با سرعت های بالا، کاربرهای علمی اغلب در خوشه های محاسبه اعلاء با سری های دیسک، سیستم های فایل متقارن، و لینک های دسترسی با سرعت بالا خوشه های محاسبه اعلاء سرمایه گذاری می کنند. گزارش های استفاده که در این سرورهای انتقال داده جمع آوری شده اند، نشان می دهند که برخی از انتقال ها در یک کسر چشمگیر قابلیت لینک، یعنی، 4 Gbps برروی لینک های 10 Gbps اتفاق افتاده اند[2]. گونه های TCP جدید از قبیل H-TCP [3] جهت تولید چنین سرعت های بالایی برای جریان های واحد استفاده شده اند. انتقال های حجیم با سرعت بالا، که به آنها جریان های α گفته می شود، منبع اولیه نوسان در ترافیک IP می باشند[4].

فراهم کننده های شبکه آموزش و تحقیق اصلی، از قبیل شبکه علوم انرژی (ESnet) سازمان انرژی US (DOE) [5]، تشخیص داده است که چنین جریان های α برای جریان های (β) با هدف کلی تاثیرات مضری دارد. از آنجایی که جریان های α باعث نوسان می شوند، برنامه های ویدو/صوت، واریانس تاخیر بسته (اختلال) و یک تحلیل مشابه در عمل تجربه می کنند. چنین زوال های در عمل باعث بلیط های مشکل ساز می شود که بر هزینه های اجرایی فراهم کننده می افزاید. به منظور رسیدگی به این هزینه ها، DOE تحقیقاتی برروی سیستم های مهندسی ترافیک را مورد حمایت قرار داده است. ما پیشنهاد می کنیم یک این چنین سیستمی: 1- جریان های انتقال داده حجیم با سرعت بالا را از ترافیک بسته که به روترهای ورودی شبکه یک فراهم کننده وارد می شوند، مجزا می کند.2- مسیر استفاده شده توسط این جریان ها را بوسیله ایجاد مدارهای مجازی درون حوزه (مهندسی ترافیک) کنترل می کند. 3- بسته ها را از این جریان ها جدا می کند و در صف های مجازی مجزا قرار می دهد تا تاثیرات آنها برروی جریان های هدف کلی را کاهش دهد [6-8].

اولین وظیفه سیستم مهندسی ترافیک که در بالا نام برده شد، یعنی شناسایی جریان های حجیم با سرعت بالا از ترافیک بسته که وارد شبکه فراهم کننده می شود، شرح مسئله است که در این تحقیق به آن پرداخته شده است.

اساس رویکرد راه حل ظاهرا یک راه حل ساده، این است که برنامه های کاربر نهایی از قبیل [9] GridFTP را اصلاح می کند تا به شبکه فراهم کننده با یک پیام صفحه کنترل قبل از شروع هر انتقال حجیم با سرعت بالا علامت دهد. چنین پیامی می تواند نیاز به سیستم های شناسایی جریان α خودکار درون شبکه یک فراهم کننده را خنثی کند. این راه حل در پروژه های Lambdastation [10]، Terapaths [11]، و CHEETAH [12] مورد استفاده قرارگرفته بود، ولی مشکلات کاربردی ارتقاء ها و اقتباس برنامه بوسیله کاربران از بکارگیری آن جلوگیری می کرد. این مسئله باعث شد تا ما یک راه حل مهندسی ترافیک درون حوزه را دنبال کنیم زیرا بکارگیری این چنین سیستمی بطور کامل در کنترل فراهم کننده خواهد بود. چنین راه حلی از تلاش برای اقتباس تکنولوژی همسان رویکرد علامت داده شده برنامه نهایی جلوگیری نمی کند.

برای شبکه های فراهم کننده جهت شناسایی خودکار جریان های α، ما با امتحان کردن ویژگی های دردسترس روترهای IP امروزی شروع می کنیم. متاسفانه، روترها مکانیزم های توکار جهت مشخص کردن اندازه و سرعت یک جریان را ندارند (جایی که یک "جریان" به وسیله توالی 5-tuple شناسایی شده است: آدرس های IP منبع و مقصد، شماره های درگاه لایه انتقال منبع و مقصد). در مرحله بعد، ما یک مکانیزم درگاه انعکاس دهنده را در نظر گرفتیم که در آن روترهای IP قابل پیکربندی بودند تا از بسته ها کپی بگیرد و آنها به یک درگاه که به یک سرور بیرونی متصل است، انتقال دهد، و این عمل آخری سپس می تواند جهت اجرا کردن یک آنالیز اندازه/سرعت براساس جریان برای شناسایی جریان α مورد استفاده قرار گیرد. با این حال، چنین مکانیزمی برای سرعت های لینک بالا (Gbps10-100) شبکه های فراهم کننده غیرقابل مقیاس پذیر تلقی می شود.

بعد از این نتیجه گیری که هیچ مکانیزم توکار برای محاسبه اندازه/سرعت جریان در درون روترها وجود ندارد، و اینکه درگاه منعکس کننده غیرممکن است، ما سعی کردیم مکانیزم های دیگری که قابل استفاده بودند را پیدا کنیم. یافته ما این است که نت فلو ، ویژگی که در روترهای IP مقیاس فراهم کننده حمایت شده است، برای حل مشکل ما قابل استفاده می باشد[13]. این ویژگی نت فلو به روترها چنین اجازه ای را می دهد تا اطلاعات را برای یک مجموعه نمونه گیری شده بسته ها جمع آوری کند، که سپس به شکل رکورد های نت فلو به یک جمع کننده نت فلو بیرونی

انتقال می دهد. در راه اندازی های امروزی، رکوردهای نت فلو برروی یک دانه بندی زمان درشت (coarse time) که به ترتیب دقیقه به ساعت می باشد، انتقال داده می شود. یک آنالیز اطلاعات نت فلو نشان داد که پیش بینی دقیق بازه زمانی و اندازه یک جریان α بوسیله نظارت کردن تعداد کمی از اولین رکوردهای نت فلو مربوطه یک جریان (آنلاین) فعال امکان پذیر نیست. هر اقدام مهندسی ترافیک/ جداسازی جریان براساس این پیش فرض که یک جریان، جریان α می باشد ممکن است بی ثمر باشد. زیرا جریان می تواند حتی قبل از اینکه اقدامات پیکربندی روتر برای مهندسی ترافیک و جداسازی جریان کامل شود، به پایان برسد. بنابراین، مکانیزم آفلاینی ایجاد کردیم که در آن رکورد های نت فلو از جریان های کامل شده مورد آنالیز قرارمی گیرند، و اطلاعات استخراج شده از این آنالیز برای پیکربندی روترها استفاده می شود تا جریان های α آینده برای مهندسی ترافیک و جداسازی جریان را شناسایی کند.

رویکرد راه حل ما یک سیستم مدیریت شبکه با نام سیستم مهندسی ترافیک جریان آلفا (AFTES) را پیشنهاد کردیم که می تواند برروی یک سرور بیرون از روترها هم عمل کند. AFTES می تواند رکورد های نت فلو را از جمع کننده نت فلو جمع آوری کند و پیشوندهای آدرس منبع-مقصد جریان های α که از قبل تکمیل شده اند را ذخیره کند. این پیشوندها برای پیکربندی فیلترهای فایروال در ورودی روترها استفاده می شوند، تا جریان های α آینده بین زیرشبکه های منبع/مقصد مشابه به مسیرهای که براساس QoS کنترل شده و طراحی شده ترافیکی هدایت شوند. یک مقیاس مقاومت جهت حذف ورودی های پیشوند آدرس از فیلترهای فایروال که هیچ یک از جریان های α آنها در یک بازه رشد نظارت نشده اند، استفاده شده است. طرح AFTES درصورتی که فرضیه زیر درست باشد، مفید خواهد بود.

فرضیه اکثر شاخه های انتقال اطلاعات با سرعت بالا دارای آدرس های IP ثابت می باشند، و جریان های α بطور مکرر بین زیرشبکه های منبع-مقصد مشابه تولید می شوند. اساس این فرضیه این است که دانشمندان معمولا شبیه سازی هایشان را برروی مراکز ابرمحاسبه مشابه انجام می دهند، و به همین دلیل ما از آنها انتظار داریم که اطلاعات را بین دو خوشه مشابه انتقال دهند. درصورتی که این فرضیه درست باشد، طرح AFTES مبتنی بر مشخص

کننده پیشوند آفلاین در شناسایی و هدایت کردن جریان های α به مسیرهای که براساس QoS کنترل شده اند و طراحی شده ترافیکی ، موثر خواهد بود. ما آنالیز ترافیک رکورد های نت فلو جمع آوری شده از ESnet را انجام دادیم تا این فرضیه را آزمایش کنیم.

یافته ها آنالیز اطلاعات ما نشان داد که اگر AFTES در ابتدای دوره 7ماه که برای آن رکورد های نت فلو آنالیز شده بودند، استفاده می شدند، 91٪ بایت ها از جریان های α که در بازه های سرعت بالا اتفاق افتادند، می توانستند به مسیرهای که بر اساس QoS کنترل شده اند و طراحی شده ترافیکی فرستاده شوند. این عمل فرضیه را برای دوره زمان و روتر ENset آزموده شده، معتبر ساخت؛ به منظور اینکه محققان دیگر توانایی آزمودن این فرضیه با اطلاعات بدست آمده از فراهم کننده های دیگر را داشته باشند، نرم افزار ما برروی یک وب سایت عمومی دردسترس قرار داده شد [14].

یافته دوم ما مربوط می شود به کمی کردن (به عدد نشان دادن) هزینه هدایت دوباره جریان ها براساس پیشوندهای آدرس منبع-مقصد نه براساس مشخص کننده های توالی 5-tuple که بیشتر محدود بودند(که شامل آدرس های IP منبع و مقصد، شماره های port منبع و مقصد، و نوع پروتکل می شود). تاثیر انتخاب این طرح این است که جریان های β (بدون α) که در پیشوندهای آدرس منبع و مقصد مشابه جریان های α هستند، به صف ها و مسیرهای جریان α هدایت خواهند شد. با این حال، آنالیز اطلاعات ما نشان می دهند که تعداد زیادی از چنین بسته های جریان β نشات گرفته از برنامه های انتقال فایل هستند نه از برنامه های تعاملی حساس به تاخیر. این عمل محتمل می باشد زیرا اکثر شاخه های انتقال اطلاعات و محاسبه علمی در زیرشبکه های جداگانه نسبت به آنهایی که برای متصل کردن میزبان های کاربر با اهداف عمومی استفاده شدند، قرار دارند.

نوآوری سه ایده جدید و بکر اساس AFTES را تشکیل می دهند: (1) بکارگیری کنترل های کیفیت سرویس (QoS) در انتقال های فایل نه در جریان های ویدیو و صوت تعاملی؛ (2) استفاده از مدارهای مجازی درون حوزه نه مقصد به مقصد ؛ و (3) بکار گیری دانش رفتارهای انسان و قابلیت های سیستم end در ایجاد کردن یک الگوریتم طبقه بندی جریان.

زمانی که فناوری های حالت انتقال غیرهمزمان (ATM) و سرویس ادغام شده (IntServ) ایجاد شده بودند، سرویس های مدار مجازی برای جریان های ویدیو و صوت تعاملی مدنظر بودند. با این حال، از آنجایی که تعداد چنین جریان هایی بسیار زیاد است و کنترل های QoS در هر جریان تنها می توانند در تعداد کمی از جریان ها در اکثر روترها کاربرد داشته باشند، این راه حل های مدار مجازی به اندازه ای که در اول پیش بینی شده بود مورد استفاده قرار نگرفتند. درعوض، شبکه هایی که براساس IP هدایت می شوند به راحتی بیش از حد تامین شدند. چنین تامین بیش از حدی معمولا برای پایین نگه داشتن تاخیر و اختلال در جریان های ویدیو و صوت تعاملی کافی می باشد. بااین حال، در بازه های کوتاه، جریان های α می توانند به سرعت محافظ های روتر را پر کنند. سرورهای انتقال داده علمی که جریان های α تولید می کنند معمولا کارت های تعامل شبکه 10 Gbps دارند، و بنابراین می توانند بسته ها را با آن سرعت که همچنین سرعت لینک های شبکه اصلی می باشد، منتشر کنند. چنین شیوع های می توانند باعث کاهش های مشهود کیفیت در جریان های ویدیود و صوت تعاملی شوند (قسمت 2 را مشاهده فرمایید). رویکرد جدید ما این است که کنترل های QoS را در جریان های α بکار بگیریم، که از لحاظ تعداد نسبت به جریان های ویدیو و صوت کمتر می باشند و درنتیجه بوسیله روترهای امروزی کنترل شوند.

ایده جدید دوم استفاده از مدارهای مجازی درون حوزه را پیشنهاد می کند، درحالی که تحقیقات قبلی استفاده از مدارهای مجازی مقصد به مقصد را ضروری می دانستند. درصورتی که QoS معیار از قبیل تاخیر مقصد به مقصد ، به تعهد نیاز داشته باشد، سپس مدارهای مجازی باید مسیرهای مقصد به مقصد را گسترش دهند. بااین حال، تعهد های تاخیر برای جریان های α ضروری نیستند، و فناوری های برای ایجاد مسیرهای مقصد به مقصد پیوندی وجود دارند، که در آن برخی از قسمت های یک مسیر که براساس IP هدایت می شوند، هستند درحالی که قسمت های دیگر مدارهای مجازی می باشند. استفاده از مدارهای مجازی درون حوزه به فراهم کننده واحد اجازه می دهد تا بطور یک طرفه AFTES را برای مهندسی ترافیک بهتر بکار گیرد. این عمل اقتباس AFTES را محتمل تر می کند.

سومین ایده جدید ما استفاده از اطلاعات رفتار انسان و قابلیت های کامپیوتر های مقصد در طرح AFTES می باشد. تحقیقات دیگر برروی الگوریتم های طبقه بندی جریان، همانطور که در قسمت 3.2 نمایش داده شد، استفاده از تکنیک های درگاهی و ظرفیت ترابری یا یادگیری ماشین را پیشنهاد می کنند، درحالی که راه حل AFTES ما براساس مشاهدات عملی است. مشاهداتی درباره اینکه چه کسی جریان های α را تولید کرد، و گونه کامپیوترهای مقصد که برای تولید این چنین جریان های مورد نیاز است.

خدمات ارزیابی و طرح AFTES اصلی ترین خدمات این تحقیق می باشند. طرح AFTES یک راه حل عملی می باشد که یک مشکل فنی را حل می کند (کاهش دادن اثرات مضرر جریان های α برروی جریان های دیگر)، درحالی که محدودیت های روترهای امروزی و دشواری های بکارگیری راه حل های بین حوزه ای را درنظر می گیرد. ارزیابی نشان داد که طرح AFTES یک راه حل مناسب برای گسترش می باشد.

اهمیت برای متخصصان ، به وجود آمدن نمونه اولیه AFTES به منظور بکارگیری باالقوه در ESnet می تواند سودمندی مستقیم داشته باشد. استراتژی طرح که تنها به رکورد های نت فلو نیاز دارد، جمع آوری آن پیش از این بوسیله اکثر فراهم کننده ها حمایت شده است، موانع قبول کردن آن توسط فراهم کننده ها را کاهش می دهد. همانطور که پیش تر اشاره شد، ذات درون حوزه راه حل AFTES همچنین مورد پسند متخصصان می باشد. قسمت 2 عوامل انگیزه دهنده برای چنین کاری را توصیف می کند. قسمت 3 تاریخچه و مرورها مربوط به این تحقیق را فراهم می کند. قسمت های 4 و 5، مکانیزم شناسایی جریان α آفلاین پیشنهاد شده را توصیف می کند. یک ارزیابی از این مکانیزم از طریق آنالیز اطلاعات نت فلو ترافیک ESnet در قسمت 6 به نمایش گذاشته شده است. این مقاله در قسمت 7 نتیجه گیری می کند.

4. بررسی کلی

این قسمت یک بررسی کلی طراحی از اینکه چگونه AFTES می تواند در یک شبکه فراهم کننده بکارگرفته شود، فراهم می کند[6,7]. مثال شبکه فراهم کننده که در شکل 3 نشان داده شد را درنظر بگیرید. مسیرهای پیش فرض

که بر اساس IP هدایت می شوند از روتر A تا روتر C در مثال شبکه فراهم کننده با خطوط تیره و قرمز نشان داده شده اند. AFTES یک سیستم نرم افزاری مدیریت شبکه می باشد که می تواند برروی یک سرور بیرونی همانطور که در شکل 3 نشان داده شد، عمل کند. AFTES با دو سیستم بیرونی، یک جمع کننده نت فلو و یک کنترل کننده بین حوزه ای (IDC) ، تعامل برقرار می کند. نقش یک جمع کننده نت فلو در قسمت 3.1 توضیح داده شده است. IDC یک زمان بند مدار مجازی می باشد و در REN های بعنوان ESnet و Internet2 به منظور حمایت کردن ذخیره های از پیش تعیین شده برای مدارهای مجازی (VCs) استفاده شده است [25]. هر دو فراهم کننده از MPLS به منظور حمایت کردن ارائه های سرویس مدار مجازی متحرک آنها استفاده می کنند. AFTES این سرویس را برای جریان های αبه حداکثر می رساند. مرحله نصب در برقراری شبکه VC، فرصتی برای جریان های α مهندسی ترافیک در کنار مسیرهای متمایز از مسیرهای پیش فرض که بر اساس IP هدایت می شوند در صورت نیاز (برای مثال، به منظور تعادل باگیری)، فراهم می کند.

عملکرد های AFTES در دو مرحله دسته بندی شده اند:

شناسایی پیشوند آدرس جریان α AFTES رکورد های نت فلو را از جمع کننده نت فلو بدست می آورد (همانطور که در شکل 3 نشان داده شد)، و پیشوندهای آدرس IP منبع و مقصد جریان های α را استخراج می کند. جزئیات مربوط به آستانه های استفاده شده برای مشخص کردن اینکه کدام جریان ها، جریان های α هستند را در قسمت بعد فراهم می کنیم.

در ESnet، ما انتظار داریم که AFTES را پایه ای شبانه اجرا کنیم و بنابراین ما یک شاخص در هریک روز i در بوجود آوردن یک مجموعه از Ids Fi پیشوند α استفاده می کنیم، با استفاده از پیشوندهای آدرس منبع-مقصد جریان های α که درطول روز مشاهده شده بودند. به منظور جلوگیری از بیش از حد بزرگ شدن مجموعه Fi (زیرا این مجموعه اصول های فیلتر فایروال که به روترها اضافه خواهند شد را مشخص می کند)، جفت های پیشوند آدرس که برای آنها جریان های α درون بازه رشد (برای مثال، 30 روز) مورد نظارت قرار نگرفته اند، حذف خواهند شد.

شکل 3. نمایش نقش سیستم مهندسی ترافیک جریان آلفا(AFTES)

دلیل داشتن یک بازه رشد این است که در رابطه با اصول فیلتر فایروال ثبات فراهم کند. این فرضیه در رابطه با اجرا کردن AFTES بر پایه ای شبانه یک فرضیه آغازین می باشد. براساس الگوهای تکرار مشاهده شده، AFTES به دفعات بیشتری می تواند اجرا شود. برای مثال، اگر در شبکه یک فراهم کننده مشخص شده، ما شاهد این بودیم که یک جفت منبع-مقصد در یک روز انتقال های حجیم با سرعت بالای چندگانه ای اجرا می کند و هزینه اجرا کردن AFTES و پیکربندی روترها قابل قبول می باشد، سپس تناوبی که در آن AFTES انجام شده است را می توان افزایش داد. همچنین، اگر تغییرات غیرمنتظره چشمگیری درون ترافیک شبکه مشاهده شد، یک مدیر بطور دستی می تواند عملیات های AFTES را انجام دهد.

پیکربندی کردن روترها برای هدایت دوباره جریان α آینده همانطور که در قسمت 1 اشاره شد، وظایف دوم و سوم این است که: (ii) کنترل کردن مسیری که توسط جریان های α پیموده شده اند بوسیله مدارهای مجازی، و (iii) جداسازی جریان های α به صفت های مجازی جداگانه به منظور کاهش تاثیرات آنها بر جریان هایی با اهداف کلی. درحالی که این وظایف خارج از حوزه این مقاله می باشد، همانطور که در قسمت 1 گفته شد، ما یک بررسی کلی مختصر برای راه حل های این وظایف فراهم می کنیم.

به منظور پیکربندی روترها برای هدایت دوباره جریان α آینده، AFTES، اول روتر خروجی E را مشخص می کند مرتبط به یک ID پیشوند α که جدیدا از رکورد های نت فلو بدست آمده از روتر ورودی I، شناخته شده است. سپس بازرسی می کند که آیا یک LSP از پیش از روتر ورودی I در روتر خروجی E وجود دارد یا نه. اگه وجود داشته باشد، سپس AFTES با روتر ورودی I رابطه برقرار می کند تا یک اصل فیلتر فایروال جدید پیکربندی کند، که جریان های α آینده که IDs پیشوند آنها با ID پیشوند α جدیدا شناخته شده با LSP موجود همخوانی دارد. در طرف دیگر، اگر AFTES پی برد که هیچ LSP از روتر ورودی I به روتر خروجی E وجود ندارد، AFTES با IDC ارتباط برقرار می کند تا تامین LSP را شروع کند. IDC شامل عملکرد می شود تا اصول فیلتر فایروال را تنظیم کند، و بنابراین AFTES می تواند به آسانی ID پیشوند α به IDC منتقل کند درحالی که به نصب LSP نیاز دارد. راه حل AFTES آفلاین است به این شیوه که Ids پیشوند α جریان های کامل شده برای پیکربندی

کردن روترها جهت هدایت دوباره جریان α آینده استفاده می شوند. بنابراین، هیچ مسیری در میانه یک جریان تغییر مسیر نمی دهد، و بنابراین بسته های بیرون از توالی (که مخالف توان عملیاتی TCP) بوسیله این راه حل مهندسی ترافیک بوجود نخواهند آمد.

با توجه به انتخاب مسیر برای LSP ها برای جریان های α، یک رویکرد این است که آمار و ارقام ترافیک برروی LSP ها را با استفاده از SNMP جمع آوری کند. اگزیاو و همکاران این رویکرد را بعنوان یک وسیله برای بدست آوردن ماتریس ترافیک برای شبکه یک فراهم کننده پیشنهاد کردند[57]. بوسیله تامین LSP ها با هیچ محدودیت پهنای باند میان همه ورودی ها- جفت های روتر خروجی، آمار و ارقام ترافیک SNMP یک شیوه راحتر برای بدست آوردن ماتریس ترافیک پیشنهاد می کند در مقایسه با شیوه هایی که با رکورد های نت فلو از بسته های نمونه گیری شده شروع می کنند. از آمار و ارقام ترافیک SNMP، IDC می تواند شیوه های محاسبه مسیر را اجرا کند، این چنین شیوه هایی در یک مقاله بررسی توصیف شده اند [58]. همچنین مقالات بررسی و مروری در رابطه با مهندسی ترافیک [34, 35] شیوه هایی برای تعادل بارگیری، برای مثال، به منظور کاهش دادن حداکثر استفاده لینک (MLU) پیشنهاد می کند[59].

در رابطه با جداسازی جریان، ما پیکربندی زمان بند های روتر را پیشنهاد می کنیم تا در حالت محافظت کار عمل کند، این بدین معناست که هیچ قسمت بندی محکم پهنای باند میان LSP های متنوع و جریان های که بر اساس IP هدایت می شود و در تعاملی با هم سهیم هستند، وجود ندارد. در مقاله ای دیگر [8]، ما تاثیرات منفی اداره کردن جریان های α (زیرا اکثر این جریان ها از TCP استفاده می کنند) به نمایش گذاشتیم و یک رویکرد زمان بندی WFQ/PQ و بدون اداره کردن پیشنهاد کردیم. برخلاف تکنیک های تسهیم مدار (مثلا، TDM، WDM)، تکنیک های مدار مجازی (VC) از قبیل MPLS، وظیفه انتخاب مسیر و تامین VC از وظیفه تخصیص منابع (پهنای باند و محافظ) برای کنترل QoS را جدا می کنند[57]. در مقاله ما [8]، ما اهمیت ایجاد صف های مجازی چندگانه برای اینکه بسته های که براساس IP هدایت می شوند حساس به تاخیر پشت شیوع های جریان α نمانند، را نشان دادیم. حالت حفظ کار تسهیم منابع، حذف کردن یک LSP میان یک جفت روتر ورودی-خروجی از

ضرورت آن می کاهد، اگر هیچ اصل فیلتر فایروال که جریان هایی با ID های پیشوند α مشخص شده را به LSP هدایت کند وجود نداشته باشد. بنابراین، یک رویکرد آزاد سازی به تاخیر افتاده می تواند اجرا شود. انتظار می رود که LSP ها داری عمری طولانی باشند زیرا جریان های α مکرر با ID پیشوند مشابه مشاهده شده اند.

جدول 2. مجموعه های ایجاد شده برای بازه تراکم اولین (ith)

6. آنالیز اطلاعات نت فلو

اطلاعات نت فلو ESnet از یک روتر edge فراهم کننده ESnet به مدت هفت ماه جمع آوری شده بودند: از 1 ماه مه تا 30 ماه نومبر سال 2011 (214 روز). در روترهای ESnet، نت فلو با نمونه یک در هزار بسته ها پیکربندی شده بود و بازه timeout فعال در 60 ثانیه تنظیم شده بود. اطلاعات جریان برای جهت ورودی همه تعامل های میان حوزه ها جمع آوری شده بودند. ابزارهای جریان [61]، و برنامه های custom Perl و R [62] برای آنالیز اطلاعات استفاده شده اند. این برنامه ها بعنوان نرم افزار منبع آزاد برروی وب سایت پروژه ما [14] قرار داده شده است تا تکثیر آزمون های ما با استفاده از اطلاعات نت فلو از REN های دیگر را ممکن سازد.

ارزش های عوامل زیر مورد استفاده قرار گرفتند: τ، بازه وقفه فعال نت فلو، یک دقیقه بود، بازه تراکم برای ایجاد جریان های پیشوند یک روز بود، و H، آستانه رکورد های نت فلو α، یک GB بود.

ما دلایلمان برای انتخاب کردن آستانه GB1 توضیح می دهیم. اینکه آیا یک جریان α باعث افزایش اختلال و تاخیر بسته برای جریان های واقعی می شود به ترافیک زمینه، سرعت های لینک، و اندازه محافظ روتر بستگی دارد. تحقیق آزمایشی در یک مقاله دیگر [8] نشان داد که چگونه یک شاخه انتقال اطلاعات با یک کارت تعامل شبکه 10 GB (NIC) می تواند بسته های پی در پی با سرعت بالا و شیوع های حجیم که محافظ های روتر را پرمی کنند زمانی که پنجره ازدحام TCP بزرگ است، را ارسال می کند. دانشمندانی که مکررا مجموعه اطلاعات حجیم را حرکت می دهند، در شاخه های انتقال-اطلاعات با چنین NIC هایی با سرعت بالا سرمایه گذاری می کنند. آستانه 1 GB انتخاب شد البته بعد از اینکه از آزمایش هایمان [8] تعیین کردیم که اندازه محافظ روتر GB125 بود، و

همچنین با استفاده از اطلاعات ترافیک زمینه در ESnet4. درصورتی که اندازه پنجره ازدحام TCP به صدها MB افزایش یابد، بسته ها می توانند به شیوع ها در تعامل های روتر با سرعت های نزدیک به 10 Gbps برسد. در حضور ترافیک زمینه، اگر سرعت لینک خروجی در روتر هم 10 Gbps باشد، محافظ های روتر می توانند پرکند. بنابراین، انتقال های فایل حجیم این توانایی را دارند که باعث اختلال و تاخیر بسته افزایش یافته برای جریان های دیگر شوند و بنابراین بعنوان جریان های α از پا در می آیند. در رابطه با سرعت های لینک ها،سرعت های NIC، و ترافیک زمینه مشاهده شده در ESnet4، ما 1 GB را بعنوان آستانه انتخاب کردیم.

اخیرا، ESnet لینک های اصلی خود را به سرعت های 100 GB ارتقاء داده است. در یک آزمون شبکه گسترده،توان عملیاتی TCP مقصد به مقصد Gbps94 بین خوشه های موجود در منطقه خلیج، CA، و در شیکاگو،IL [63] نشان داده شده است. هر یک از خوشه ها از سه سرور تشکیل شده بودند و هر سرور به چهار Gbps 10 NICs مجهز شده بود. روترها در دو موقعیت با یک مدار وسیع 100 Gbps ادغام شده بودند. این آزمایش امکان پذیری جریان های α واحد تولید کننده اطلاعات با سرعتی نزدیک به 100 Gbps را نشان می دهد. از آنجایی که NIC های 100Gbps در بازار بروز یافتند و مورد استفاده قرار گرفتند، این سناریوی که در بالا توصیف شد در مورد محافظ های روتر که پرکردن دوباره رخ می دهد. بطور سنتی، سرعت های NIC از سرعت های تعامل روتر عقب بوده است، ولی معمولا خیلی زود خودشان را به آنها می رساندند، زیرا آنها در جامعه علمی برای انتقال های فایل با سرعت بالا مورد نیاز هستند و مورد استفاده قرار می گیرند. زمانی که سرعت های NIC با سرعت لینک اصلی سازگار می شوند، به مهندسی ترافیک جریان α نیاز است.

یک نماد جدید (I) برای نشان دادن زمان اطلاعات نت فلو آنالیز شده، که 214 روز بود، استفاده شده است. دو نوع از مشخص کننده پیشوند استفاده شد: (1) 32/ آدرس IP منبع و مقصد، و (2) 24/ ID زیرشبکه منبع و مقصد. عامل رشد که برای حذف ورودی ها از فیلتر فایروال استفاده شد متنوع بود به منظور مطالعه تاثیر آن.

اول، در قسمت 6.1 جریان های α مشاهده شده به شیوه های متفاوت توصیف شده اند. نمونه هایی از سوال هایی که جواب داده شدند عبارتند از: حداکثر میزان کلی روزانه بایت های فرستاده شده در بازه های α بوسیله هر جفت

زیرشبکه و میزبان منبع-مقصد واحد، آیا جفت های منبع- مقصدی که جریان های α تولید می کنند، تولیدشان مکرر (در روزهای متفاوت) می باشد، میزان کلی روزانه جمع شونده بایت ها در تمام جفت های منبع-مقصدی که جریان های α تولید می کنند، میزان کلی زمان جایی که یک یا تعداد بیشتری از جریان های α فعال برروی یک تعامل روتر وجود دارد، و چه درصدی از ترافیک کلی توسط جریان های α به نمایش گذاشته شده است. دوم، قسمت 6.2 میزان سودمندی را ارزیابی می کند، درصد بایت های α که ممکن است به مسیرهای طراحی شده ترافیکی دوباره هدایت شده باشند و از جریان های دیگر جدا شده باشند، آیا AFTES در طول دروه ماه مه تا ماه نوامبر سال 2011 عملیاتی بوده اند. درحالی که تعداد سودمندی زمانی که24/ ID های پیشوند در فیلترهای فایروال برای هدایت دوباره جریان α جداسازی استفاده می شوند، بالاتر می رود نسبت به زمانی که32/ ID های پیشوند استفاده شده اند (91٪ در برابر 82٪)، هزینه ای در استفاده از24/ ID های پیشوند وجود دارد و این است که بسته های جریان β که IDهای پیشوند مشابه جریان های α را به اشتراک می گذارند به صف ها و مسیرهای طراحی شده ترافیکی که برای جریان های α نصب شده اند، هدایت می شوند. در سومین مجموعه آنالیز، قسمت 6.3 این هزینه را به عدد نشان می دهد، با استفاده از یک معیار درصد این بسته ها که به برنامه های انتقال فایل قابل نسبت دادن می باشند (فرضیه این است که شیوع جریان های α در رابطه با جریان های انتقال فایل نسبت به جریان های حساس به تاخیر واقعی کمتر مخالف هستند). سرانجام، یک فرضیه که جریان های انتقال در ابتدا از " درهای اطلاعات" ، شاخه های کاملا مجهز وقف شده برای انتقال اطلاعات حجیم با سرعت بالا نشات می گیرند ، آزموده شده و درست از آب در آمد.

6.2.2 سودمندی

شکل 10 سودمندی AFTES را به نمایش می گذارد؛ بخصوص درصد بایت های α که ممکن است بر پایه ای ماهیانه دوباره هدایت و جدا شده باشد. جدول 5 درصد مجموع بایت های α که ممکن است در تمام زمان 24 روزه نظارت شده هدایت شده باشند، مرتبط به ارزش های متفاوت عامل رشد، A را نشان می دهد. استفاده از ID های

پیشوندی 24/ موثرتر از IDهای پیشوندی 32/ بود (وجه منفی این یافته در قسمت بعد به عدد درآمده است). این انتظار می رود، زیرا شاخه های انتقال اطلاعات اغلب کامپیوتر های خوشه ای با آدرس های IP در زیرشبکه مشابه هستند.

شکل 8. تعداد ID های پیشوند α جدید در هر روز

شکل 9. تعداد IDهای پیشوند α جدید در هر روز با عملکرد spline آرام کننده (df=4)

شکل 10. سودمندی AFTES برای ارزش های متفاوت عامل رشد

با راه اندازی های جدید شاخه های انتقال اطلاعات با سرعت بالا، مشخص کننده های پیشوندی 32/ که قبلا ناپیدا بودند ممکن است به وسیله مشخص کننده های 24/ پوشانده شوند. اگر اصول هرگز از فیلتر فایروال حذف نشوند، در رابطه با مورد 24/، 92% از بایت های α از جریان های β درطول هفت ماه ممکن بود جدا شوند.

شکل 11. رشد فیلتر فایروال برای ارزش های متفاوت عامل رشد [6]

جدول 5. درصد بایت های α که ممکن است در طول تمام دوره 214 روزه دوباره هدایت و جدا شده باشند.

7. خلاصه و نتیجه گیری ها

یک مکانیزم آفلاین برای مشخص کردن مشخص کننده های پیشوند جریان های α که به وسیله انتقال اطلاعات حجیم با سرعت بالا به وجود آمد. این چنین انتقال ها معمولا در شبکه های آموزش و تحقیق بوسیله محققان علمی ایجاد می شوند. چنین طرح آفلاینی برای یک سیستم مدیریت شبکه با نام AFTES برای مهندسی ترافیک درون حوزه طراحی شده است. مشخص کننده های پیشوندی (IDها) (پیشوندهای آدرس منبع و مقصد) جریان های α مقاوم به منظور ایجاد فیلترهای فایروال استفاده شده اند تا جریان های α آینده را به مسیرهای طراحی شده ترافیکی دوباره هدایت کند و بسته هایشان را جدا کند تا صف ها را مجزا کند. این اقدام ها می توانند تاثیرات مضری که جریان های α ممکن است برروی بسته های جریان های واقعی داشته باشند، را کاهش دهند. تاثیراتی از قبیل تاخیر بسته افزایش یافته و واریانس تاخیر. سودمندی و هزینه این مکانیزم آفلاین نسبت به جریان های β از طریق یک

آنالیز هفت ماهه اطلاعات بدست آمده از یک روتر ESnet ارزیابی شد. نتیجه گیری های ما عبارتند از: (1) دانشمندانی که مجموعه های حجیم را با سرعت بالا انتقال می دهند، این انتقال ها را بطور مکرر بین جفت های منبع-مقصد مشابه انجام می دهند، و (2) زیرشبکه هایی با شاخه های انتقال اطلاعات اعلاء معمولا از زیرشبکه های مانیتور کاربر که درصد بسته های جریان β واقعی را محدود می کند. این جریان های β پیشوندهای آدرس جریان α را به اشتراک دارند. این مشاهدات شدنی بود راه حل AFTES برای بکار گرفتن فراهم کننده را حمایت می کنند.

Footnotes

1. برخلاف شبکه های مسکونی جایی که قابلیت لینک تنگنا می باشد، در آزمایشگاه های علمی، تنگنا منابع دیسک و محاسبه کامپیوترهای مقصد می باشد، نه لینک ها.

2. این سیستم در مقالات کنفرانسی ما [6,7] پیشنهاد شده بود و به آن سیستم مهندسی ترافیک شبکه پیوندی گفته می شد (HNTES). این نام سپس به AFTES تغییر یافت تا بطور دقیق تری عملکرد آن را انعکاس دهد.

3. بدست آوردن اطلاعات نت فلو از فراهم کننده ها به دلایل حریم خصوصی دشوار است و بنابراین ما نتوانستیم فرضیه هایمان را با اطلاعات دیگر فراهم کنندگان بیازماییم. ولی ما آنالیز دو ماهه قبلی خود [7] را به یک آنالیز هفت ماهه که در این مقاله به نمایش گذاشته شده، توسعه دادیم.

References

1. USDOE Office of Science ASCR: Terabit Networks for Extreme-Scale Science Workshop Report (2011). http://science.energy.gov/*/media/ascr/pdf/program-documents/docs/Terabit_networks_workshop_report.pdf

2. Liu, Z., Veeraraghavan, M., Yan, Z., Tracy, C., Tie, J., Foster, I., Dennis, J., Hick, J., Li, Y., Yang, W.: On using virtual circuits for GridFTP transfers. In: The International Conference for High Performance Computing, Networking, Storage and Analysis 2012 (SC 2012), pp. 81:1–81:11, Nov 10–16, 2012

3. Leith, D., Shorten, R.: H-TCP: TCP for high-speed and long-distance networks. In: Protocols for Fast Long Distance Networks Workshop (PFLDnet), Feb 16–17, 2004

4. Sarvotham, S., Riedi, R., Baraniuk, R.: Connection-level analysis and modeling of nework traffic. In: ACM SIGCOMM Internet Measurement Workshop 2001, pp. 99–104, Nov 2001

5. ESnet. http://www.es.net/

6. Jin, T., Tracy, C., Veeraraghavan, M., Yan, Z.: Traffic engineering of high-rate large-sized flows. In: 2013 IEEE 14th International Conference on High Performance Switching and Routing (HPSR), pp. 128–135 (2013)

7. Yan, Z., Tracy, C., Veeraraghavan, M.: A hybrid network traffic engineering system, In: Proceedings of the IEEE 13th High Performance Switching and Routing (HPSR), Jun 24–27, 2012

8. Yan, Z., Veeraraghavan, M., Tracy, C., Guok, C.: On how to provision Quality of Service (QoS) for large dataset transfers, In: Proceedings of the Sixth International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ), Apr 21–26, 2013

9. GridFTP. http://globus.org/toolkit/docs/3.2/gridftp/

10. The Lambda Station Project. http://www.lambdastation.org/

11. TeraPaths: Configuring End-to-End Virtual Network Paths with QoS Guarantees. https://www.racf.bnl.gov/terapaths/

12. Circuit Switched High-speed End-to-End Transport Architecture (CHEETAH). http://www.ece.virginia.edu/cheetah/

13. NetFlow. http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html

14. Hybrid Network Traffic Engineering System (HNTES). http://www.ece.virginia.edu/mv/research/DOE09/index.html

15. Spragins, J.: Asynchronous transfer mode: solution for broadband ISDN, third edition [New Books]. IEEE Netw. 10, 7 (1996)

16. Braden, R., Zhang, L., Berson, S., Herzog, S., Jamin, S.: Resource ReSerVation Protocol (RSVP)— Version 1 Functional Specification. RFC 2205 (Proposed Standard), Sept 1997. Updated by RFCs 2750, 3936, 4495, 5946, 6437

17. Vietzke, R.P.: Internet2 Headroom Practice, 15 Aug 2008. https://wiki.internet2.edu/confluence/download/attachments/17383/Internet2?Headroom?Practice?8-14-08.pdf?version=1

18. ESnet Graphite. https://stats.es.net/graphite/

19. nuttcp. http://www.nuttcp.net/

20. Wallerich, J., Dreger, H., Feldmann, A., Krishnamurthy, B., Willinger, W.: A methodology for studying persistency aspects of Internet flows. ACM SIGCOMM Commun. Rev. 35(2), 23–36 (2005)

21. ESnet Backbone Topology Map Summer 2010. http://es.net/introducing-esnet5/network-maps/historical-network-maps/

22. GEANT2. http://www.geant2.net/ 23. Interoperable Ondemand Network (ION). http://www.internet2.edu/products-services/advancednetworking/layer-2-services/

24. Next-generation network testbed JGN-X. http://www.jgn.nict.go.jp/english/

25. On-Demand Secure Circuits and Advance Reservation System (OSCARS). http://www.es.net/OSCARS/docs/index.html

26. Liakopoulos, A., Maglaris, B., Bouras, C., Sevasti, A.: Providing and verifying advanced IP services in hierarchical DiffServ networks-the case of GEANT. Int. J. Commun. Syst. 17(4), 321–336 (2004)

27. Claise, B.: Cisco Systems NetFlow Services Export Version 9. RFC 3954 (Informational), Oct 2004
28. Claise, B.: Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information. RFC 5101 (Proposed Standard), Jan 2008
29. Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W.: An Architecture for Differentiated Service. RFC 2475 (Informational), Dec 1998. Updated by RFC 3260
30. Lan, Kun-chan, Heidemann, John: A measurement study of correlations of Internet flow characteristics. Comput. Netw. 50(1), 46–62 (2006)
31. Crovella, M.E., Taqqu, M.S.: Estimating the heavy tail index from scaling properties. Methodol. Comput. Appl. Probab. 1, 55–79 (1999)
32. Brownlee, N., Claffy, K.: Understanding Internet traffic streams: dragonflies and tortoises. IEEE Commun. Mag. 40, 110–117 (2002)
33. Nguyen, T.T.T., Armitage, G.J.: A survey of techniques for Internet traffic classification using machine learning. IEEE Commun. Surv. Tutor. 10(4), 56–76 (2008)
34. Awduche, D.O., Jabbari, B.: Internet traffic engineering using multi-protocol label switching (MPLS). Comput. Netw. 40(1), 111–129 (2002)
35. Wang, N., Ho, K., Pavlou, G., Howarth, M.: An overview of routing optimization for Internet traffic engineering. IEEE Commun. Surv. Tutor. 10(1), 36–56 (2008)
36. Papagiannaki, K., Taft, N., Bhattacharyya, S., Thiran, P., Salamatian, K., Diot, C.: A pragmatic definition of elephants in Internet backbone traffic, In: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment (IMW '02), pp. 175–176 (2002)
37. Callado, A., Kamienski, C., Szabo, G., Gero, B., Kelner, J., Fernandes, S., Sadok, D.: A survey on Internet traffic identification. IEEE Commun. Surv. Tutor. 11, 37–52 (2009)
38. Kamiyama, N., Mori, T.: Simple and accurate identification of high-rate flows by packet sampling, In: Proceedings of INFOCOM 2006. 25th IEEE International Conference on Computer Communications, pp. 1–13 (2006)
39. Mori, T., Uchida, M., Kawahara, R., Pan, J., Goto, S.: Identifying elephant flows through periodically sampled packets, In: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement (IMC '04) (New York, NY, USA), pp. 115–120, ACM (2004)
40. Zhang, Y., Fang, B., Zhang, Y.: Identifying high-rate flows based on bayesian single sampling, In: 2010 2nd International Conference on Computer Engineering and Technology (ICCET), vol. 1, pp. V1-370–V1-374 (2010)
41. Duffield, N., Lund, C., Thorup, M.: Estimating flow distributions from sampled flow statistics. IEEE/ ACM Trans. Netw. 13(5), 933–946 (2005)
42. Fioreze, T., Pras, A.: Self-management of hybrid optical and packet switching networks. In: 2011 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 946–951 (2011)
43. Caria, M., Jukan, A.: A novel approach to accurately compute an IP traffic matrix using optical bypass. In: 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), pp. 1135–1141 (2013)
44. Lu, Y., Wang, M., Prabhakar, B., Bonomi, F.: ElephantTrap: A low cost device for identifying large flows. In: 15th Annual IEEE Symposium on High-Performance Interconnects, 2007 (HOTI 2007), pp. 99–108 (2007)
45. Kodialam, M., Lakshman, T.V., Mohanty, S.: Runs based traffic estimator (rate): a simple, memory efficient scheme for per-flow rate estimation. In: INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1808–1818 (2004)
46. Hao, F., Kodialam, M., Lakshman, T.V., Zhang, H.: Fast, memory-efficient traffic estimation by coincidence counting, In: Proceedings of IEEE INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 2080–2090 (2005)
47. Zadnik, M., Canini, M., Moore, A., Miller, D., Li, W.: Tracking elephant flows in Internet backbone traffic with an FPGA-based cache. In: International Conference on Field Programmable Logic and Applications, 2009 (FPL 2009), pp. 640–644 (2009)

48. Paisley, J., Sventek, J.: Real-time detection of grid bulk transfer traffic, In: 10th IEEE/IFIP Network Operations and Management Symposium (NOMS), pp. 66–72, Apr 2006
49. Hohn, N., Veitch, D.: Inverting sampled traffic. IEEE/ACM Trans. Netw. 14(1), 68–80 (2006)
50. Chen, K., Singla, A., Singh, A., Ramachandran, K., Xu, L., Zhang, Y., Wen, X., Chen, Y.: Osa: An optical switching architecture for data center networks with unprecedented flexibility, In: Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, pp. 18–18, USENIX Association (2012)
51. Farrington, N., Porter, G., Radhakrishnan, S., Bazzaz, H., Subramanya, V., Fainman, Y., Papen, G., Vahdat, A.: Helios: a hybrid electrical/optical switch architecture for modular data centers, In: ACM SIGCOMM Computer Communication Review, vol. 40, pp. 339–350, ACM (2010)
52. Wang, G., Andersen, D., Kaminsky, M., Papagiannaki, K., Ng, T., Kozuch, M., Ryan, M.: c-through: Part-time optics in data centers. In: ACM SIGCOMM Computer Communication Review, vol. 40, pp. 327–338, ACM (2010)
53. Open Networking Foundation. https://www.opennetworking.org/
54. Software-Defined Networking (SDN). https://www.opennetworking.org/sdn-resources/sdn-definition
55. Qazi, Z.A., Lee, J., Jin, T., Bellala, G., Arndt, M., Noubir, G.: Application-awareness in sdn, In: Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM (SIGCOMM '13) (New York, NY, USA), pp. 487–488, ACM (2013)
56. Wang, G., Ng, T.E., Shaikh, A.: Programming your network at run-time for big data applications, In: Proceedings of the First Workshop on Hot Topics in Software Defined Networks (HotSDN '12) (New York, NY, USA), pp. 103–108, ACM (2012)
57. Xiao, X., Hannan, A., Bailey, B., Ni, L.: Traffic engineering with MPLS in the internet. IEEE Netw. 14(2), 28–33 (2000)
58. Paolucci, F., Cugini, F., Giorgetti, A., Sambo, N., Castoldi, P.: A survey on the path computation element (pce) architecture. IEEE Commun. Surv. Tutor. 15, 1819–1841 (2013)
59. Sharma, A., Mishra, A., Kumar, V., Venkataramani, A.: Beyond MLU: An application-centric comparison of traffic engineering schemes. In: 2011 Proceedings of the IEEE INFOCOM, pp. 721–729, IEEE (2011)
60. Jin, T., Tracy, C., Veeraraghavan, M.: Characterization of high-rate large-sized flows. In: 2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), pp. 73–76 (2014)
61. Flow-tools. http://www.splintered.net/sw/flow-tools/docs/flow-tools.html
62. The R Project for Statistical Computing. http://www.r-project.org/
63. Balman, M., Pouyoul, E., Yao, Y., Bethel, E.W., Loring, B., Prabhat, M., Shalf, J., Sim, A., Tierney, B.L.: Experiences with 100 gbps network applications, In: Proceedings of the Fifth International Workshop on Data-Intensive Distributed Computing Date (DIDC '12) (New York, NY, USA), pp. 33–42, ACM (2012)
64. Thompson, K., Miller, G., Wilder, R.: Wide-area Internet traffic patterns and characteristics. IEEE Netw. 11, 10–23 (1997)