اولین کنفرانس بین المللی مطالعات بین رشته ای در مدیریت و مهندسی
۲۳ اسفند ۱۳۹۷ - دانشگاه تهران
1st International Conference Interdisciplinary Studies in Management and Engineering
14 March 2019 - University Of Tehran
ISC
کد اختصاصی 97181-23104
با مجوز شماره ۱۶/۷۶۰۷۷
وزارت علوم تحقیقات و فناوری

نظارت هوشمند مبتنی بر چارچوب مشترک SDN/NFV برای شهرهای هوشمند

مهناز عباسی

دانشجوی کارشناسی ارشد شبکه های کامپیوتری (موسسه آموزش عالی جهاد دانشگاهی اصفهان)

Abbasi.200730@gmail.com

محمدرضا مصلحی

عضو هیئت علمی موسسه آموزش عالی جهاد دانشگاهی اصفهان

Mr.moslehi@gmail.com

سیداحمد موسوی پور

دانشجوی کارشناسی ارشد شبکه های کامپیوتری (موسسه آموزش عالی جهاد دانشگاهی اصفهان)

Mr.musavipur@gmail.com

هاجر پناهنده

دانشجوی کارشناسی ارشد شبکه های کامپیوتری (موسسه آموزش عالی جهاد دانشگاهی اصفهان)

hajarpnd@gmail.com

چکیده

در چند سال اخیر، شبکه‌های نرم‌افزار محور (Software Defined Networking) و مجازی‌سازی توابع شبکه (Network Function Virtualization) به عنوان راهی جدید برای طراحی، گسترش و مدیریت خدمات شبکه-ای به اینترنت افزوده شده است. وقتی این روش‌ها باهم عمل می‌کنند می‌توانند اجزای شبکه بندی را با استفاده از فناوری‌های مجازی سازی استاندارد IT در سرورهای با حجم بالا و هم چنین در محیط‌های کاربر انتهایی و گره‌های دسترسی یکپارچه کرده و تحویل دهند، در نتیجه امکان پدید آمدن خدمات جدیدی را فراهم می‌کنند؛ بر این اساس، این مقاله پلتفرم هوشمند نظارت ویدیویی را ارائه می‌دهد که برای بهره‌گیری از تسهیلات ارائه شده بوسیله شبکه‌های SDN-NFV طراحی شده است. این پلتفرم براساس نرم‌افزار منبع آزاد و باز است که در تجهیزات ارائه دهنده (PE) اجرا می‌شود، بنابراین امکان ساده کردن عملکرد و کاهش هزینه را فراهم می‌کند.

کلمات کلیدی– شبکه‌های نرم‌افزار محور، مجازی‌سازی توابع شبکه، رایانش مه / لبه، پخش ویدیویی زنده، اینترنت اشیا

۱- مقدمه

الگوهای جدید شبکه‌های نرم‌افزار محور (SDN) و مجازی سازی توابع شبکه (NFV) اخیراً چشم‌انداز اینترنت را از نو تعریف کرده‌اند : توان SDN براساس مشخصه جداسازی کنترل و صفحات داده است که هوش شبکه را به سمت کنترل کننده متمرکز می‌برد. از سوی دیگر، فناوری جدیدNFV تغییر مهمی در رویکرد ارائه خدمات شبکه برای یکپارچه‌سازی امکانات تجهیزات شبکه و خدمات کاربری در سرورهای استانداردی که در مراکز داده، گره‌های شبکه و حتی در محیط طرف کاربر که بر فناوری NFV متکی است ایجاد می‌کند.

بنابراین بکارگیری مشترک چارچوب SDN/NFV امکان اجرای کارهای شبکه و کاربری را درون ماشین مجازی با استفاده از NFV، و کنترل پویای جریان‌های ترافیک از طریق توابع شبکه مجازی درخواست شده (VNF) با شبکه SDN فراهم می‌کند. با این کار، شبکه‌ها خود را از پلتفرم سخت‌افزاری که از میان افزارها یا مسیریاب های نرم‌افزاری ساخته شده‌اند به شبکه نرم افزاری انعطاف پذیرتری کهVNFها طبق سیاست‌های خاصی با هدف بهینه سازی راندمان انرژی، هزینه‌ها و عملکرد، با در نظر گرفتن ازدحام بخش‌های شبکه، منتقل می‌کنند.

بر اساس این زمینه فنی، این مقاله پلتفرم نظارت ویدیویی مبتنی بر SDN/NFV را پیشنهاد می‌کند که امکان بکارگیری راحت تعداد بسیار زیادی دوربین مبتنی بر IP را در قلمرو شهر هوشمند فراهم می‌کند، و جریان‌های ویدیویی مربوطه را به کاربران ارتباط می‌دهد که ممکن است پلیس محلی، نیروهای امنیتی، نهادهای اجرایی و حتی شهروندان ساده باشند.

برخلاف روش کلاسیکی که در سیستم‌های نظارت ویدیویی گذشته بکار می‌رفت، به خاطر وجود شبکه ارتباطی SDN/NFV، در اینجا جریان ویدیویی که بوسیله هر IP ایجاد می‌شود به صورت خودکار مستقیما به "گیرنده‌های مربوطه" به صورت چند نقطه‌ای هدایت می‌شود. با این ویژگی، نصب دوربین‌های جدید کار پیش افتاده‌ای است زیرا نیازی نیست که دوربین‌های جدید پیکربندی شوند زیرا شبکه به صورت خودکار تصمیم می‌گیرد که جریان ویدیویی را کجا ارسال کند. بعلاوه، به خاطر کمک SDN، جریان ویدیویی ایجاد شده از دوربین برای مقصد دوباره تکرار نمی‌شود، در حالیکه به خاطر کمک NFV، می‌توان به راحتی افزونه‌های جدیدی را به شکل زنجیره‌های خدمات توابع مجازی (VF) بین منبع و مقصد جریان داده افزود. برای مثال، ماشین‌های مجازی بیشتری را می‌توان در شبکه اجرا کرد تا خدمات لایه شبکه و کاربری فراهم شود، مثل کنترل نسبت ویدیویی، رمزگشایی جریان، یا کنترل جریان TCP. توجه داشته باشید که ارتباط یک نقطه با چند نقطه با روش‌هایی که بتوان مطلق در نظر گرفت، صورت نمی‌گیرد، مثل ارتباط (P2P)، که ممکن است برخی مسائل ناپایداری به همراه داشته باشد. از سوی دیگر، ارتباط یک نقطه با چند نقطه در سیستم پیشنهادی در این مقاله درون شبکه برقرار می‌شود، بنابراین ترافیک به حداقل می‌رسد و به خاطر هماهنگی منابع همزمان در سطح شبکه و در سطح کاربری، عملکرد به حداکثر می‌رسد.

۲- رابطه SDN و NFV چیست؟

معماری SDN (Software Defined Networking) رویکردی است که در آن بخش کنترلی شبکه از بخش دیتا جدا شده است و دستگاه‌های موجود در شبکه (مانند مسیریاب و سوئیچ) صرفا تبدیل به دستگاه‌هایی ناتوان در تصمیم‌گیری می‌شوند و فقط براساس جداول جریانی که کنترل کننده به آن‌ها ابلاغ می‌کنند انجام وظیفه می‌نماید.

مجازی سازی عملکردهای شبکه (Network Function Virtualization) یا به اختصار NFV اپراتورهای شبکه را قادر به پیاده‌سازی المان‌های شبکه به صورت مولفه‌های نرم افزاری مجازی می‌کند. هریک از این مولفه‌ها در حالت سنتی به صورت یک دستگاه سخت‌افزاری مجزا پیاده‌سازی می‌شدند. مثلا در یک شبکه وجود دستگاه‌های دیوارآتش(Firewall)، مسیریاب(Router)، متوازن کننده بار و ... به طور مجزا امری طبیعی بوده است. بدیهی است که وجود دستگاه‌های مجزا برای هر کاربرد بسیار هزینه‌بر است و پیچیدگی‌های مدیریتی بسیاری نیز در پی دارد.

با استفاده از SDN می‌توان به راحتی عمکردهای شبکه را مجازی نمود به طوری که می‌توان هریک از المان‌های شبکه را به عنوان برنامه کاربردی(Application) از کنترل کننده SDN تعریف نمود. مجازی‌سازی عملکردهای شبکه مکمل شبکه نرم افزاری تعریف شده است ولی بدان وابسته نیست و بالعکس NFV می‌تواند بدون استفاده از SDN نیز پیاده‌سازی شود، اگرچه با ادغام دو تکنولوژی SDN و NFV نتایج بهتری حاصل خواهد شد. در حال حاضر پروتکل استانداردی برای NFV تعریف نشده است و گروه ETSIدر حال انجام بررسی‌های تکمیلی به منظور استانداردسازی برای این تکنولوژی می‌باشد.

۳- مزایای فناوری SDN/NFV

NFV با استفاده از نرم افزارSDN سرویس های شبکه را مجازی سازی می کند تا بتوانند عملیات ذیل را انجام دهد:

کاهش CaPEX : کاهش نیاز به خرید سخت افزار های سفارشی و پشتیبانی از مدل های "دریافت به اندازه پرداخت" برای از بین بردن هزینه های زیاد ذخیره تجهیزات سخت افزاری

کاهش OpEX :کاهش فضا، مصرف برق و تجهیزات برودتی و تسهیل و ساده سازی مدیریت سرویس های شبکه و کاهش هزینه های تعمیرات

افزایش سرعت خرید: کاهش زمان مورد نیاز برای راه اندازی سرویس های شبکه ای جدید، پشتیبانی از تغییر نیاز های کسب و کار، ربودن فرصت های جدید در بازار و بهبود بازگشت سرمایه در سرویس های جدید، کاهش ریسک های راه اندازی سرویس های جدید، فراهم کردن امکان تست سرویسها برای مشتریان بطوری که بتوانند مشخص کنند کدام سرویس مناسب است.

افزایش سرعت و انعطاف پذیری: افزایش یا کاهش سریع امکانات سرویس ها به منظور برآورده کردن تغییرات در نیاز ها، پشتیبانی از نوآوری و فراهم کردن سرویس هایی که قابل راه اندازی بر روی هرگونه سرور سخت افزاری استاندارد باشد.

برنامه ریزی انتقال جریان: اولین شرط ایجاد شبکه SDN ایجاد قابلیت برنامه ریزی شبکه با استفاده از یک استاندارد متن باز است که بتواند در شبکه هایی که از سخت افزارهای تولید شده توسط چند شرکت سازنده استفاده می شود، هزینه های مدیریتی را کاهش دهد. استاندارد Open Flow و بعضی استاندارد های اختصاصی مثل CISCO onePK در همین راستا ایجاد شده اند. زیر ساخت شبکه باید قادر باشد که لایه ارتباطی را با استفاده از این استانداردها برنامه ریزی کند و با پشتیبانی از این استانداردها برای برنامه ریزی جریان به صورت فعال و غیرفعال بپردازد.

عملکرد پویا و در لحظه: به علت استفاده روزافزون از محیط های دینامیک و مجازی در مراکزداده(Data Center)، ترافیک اطلاعات بیش از پیش غیرقابل پیش بینی شده است. بنابراین کنترل دستی این سیستم ها عملا غیر ممکن است. این سیستم ها از ضعف در

پاسخگویی به نیازهای پویای شبکه رنج می برند. SDN معماری نوینی را برای این سیستم های پویا طراحی کرده است که می تواند در لحظه تغییرات مورد نیاز شبکه را اعمال کند.

پایداری بالا: پایداری بالا یکی از عوامل اصلی در اطمینان از عملکرد مناسب و مداوم شبکه است، زیرساخت شبکه باید قادر به تشخیص سریع هر گونه ناهماهنگی در مسیر باشد و بتواند به سرعت در هنگام بروز خطا مسیر جایگزین را انتخاب کند و به سرعت مسیر معیوب را رفع عیب و راه اندازی مجدد کند. زیرساخت SDN با پایداری بالا، به صورت لحظه ای تمامی اجزای شبکه را بررسی می کند و در صورت تشخیص عیب در هر نقطه از شبکه مانند مسیر داده، افت کیفیت اتصالات، عدم تعادل در ترافیک و ... تمامی تغییرات را به صورت از پیش برنامه ریزی شده و در همان لحظه انجام می دهد تا همواره پایداری و کیفیت شبکه تضمین شده باشد.

تعیین مسیر هوشمند : محاسبه مسیر یکی از مهمترین عوامل برای مهندسی ترافیک شبکه است. با استفاده از SDN مسیر صحیح به سرعت شناسایی می شود و ترافیک از بهینه ترین مسیر عبور داده می شود. با استفاده از این معماری امکان استفاده از الگوریتم های جدید Routing و سوییچ به صورت لحظه ای در شبکه وجود دارد.

۴- نمونه پیاده سازی شده SDN/NFV

این قسمت از مقاله نمونه پیاده سازی شده توسط نویسندگان Corrado Rametta, Gabriele Baldoni, Alfio Lombardo می باشد که در دوازدهمین کنفرانس بین المللی FNC 2017 ارائه کرده اند.

۴-۱- توضیح پلتفرم

هدف از پلتفرم پیشنهادی ایجاد پلتفرم نظارت ویدیویی است که ویژگی‌های زیر را داشته باشد: هوشمند، اتصال و اجرا (plug & play)، انعطاف پذیر، مقیاس پذیر از نظر تعداد دستگاه‌های فرستنده و گیرنده.

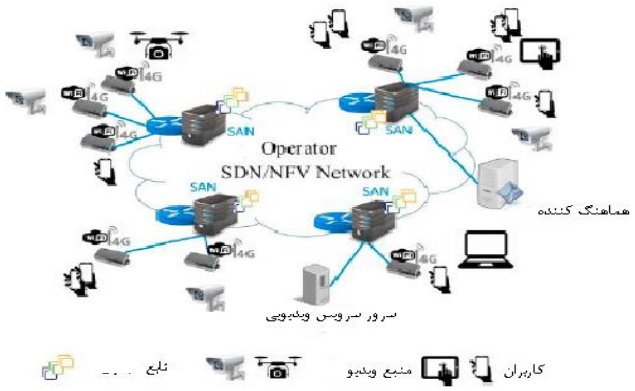
بویژه، دسترسی به پلتفرم با قرار دادن دستگاه‌های گره دسترسی هوشمند (SAN) همراه SDN/NFV حاصل می‌شود که با استفاده از سخت افزار عمومی صورت می‌گیرد که اتصال Wi-Fi یا 4G را فراهم می‌کند، و هر یک منطقه کوچک یا متوسطی را پوشش می‌دهند (مثل پارکینگ خودرو، میدان، مدرسه و مانند آن)، و امکان اتصال فرستنده‌ها و گیرنده‌های ویدیویی را فراهم می‌کنند. هر کاربر متصل به پلتفرم از طریق اپلیکیشن وب یا اپلیکیشن موبایل، نقشه‌ای از منطقه تحت پوشش پلتفرم دارد (یعنی شهر هوشمند). اتصال یک یا چند دوربین به کاربران مجاز با کلیک روی نقشه‌ای که در صفحه دیده می‌شود یا از طریق کد QR موجود در محیط دوربین به راحتی صورت می‌گیرد. بنابراین کاربر می‌تواند ویدیویی دریافتی و وقایع مربوط به هر دوربین را هماهنگ کند، مثلا با درخواست از سیستم برای ارسال هشدار در صورت شناسایی حرکت از دوربینی خاص. ابزارهای دیگری نیز وجود دارند مثل تصویر موزائیکی که جریان چند دوربین را انتقال می‌دهد. البته ممکن است بیش از یک کاربر به یک دوربین نصب شده در منطقه معیّنی که با سرویس پوشش داده شده است، مرتبط باشد. به خاطر وجود شبکه SDN/NFV، جریان ویدیویی ایجاد شده بوسیله هر دوربین مبتنی بر IP به صورت خودکار مستقیما به "گیرنده‌های مربوطه" به صورت یک نقطه به چند نقطه هدایت می‌شود. با این ویژگی، نصب دوربین جدید کار پیش پا افتاده‌ای است زیرا پیکربندی دیگری لازم نیست: هماهنگ کننده پلتفرم به صورت خودکار مقصد جریان ویدیویی را تعیین می‌کند. بعلاوه، به خاطر کمک SDN، جریان ویدیویی که از دوربین ایجاد می‌شود برای هر مقصد تکرار نمی‌شود، در عین حال که به خاطر کمک NFV، پلتفرم می‌تواند از تعداد زیادی خدمات شخصی براساس نیازهای کاربران

پشتیبانی کند: به عبارت دقیق‌تر، هر جریان داده در طول مسیر از منبع تا مقصد مجموعه‌ای از VFها را (زنجیره خدمات) طبق نوع سرویسی که کاربر نهایی درخواست کرده است، عبور خواهد داد. بعلاوه، این پلتفرم می‌تواند به راحتی پلاگین‌های جدیدی را ادغام کند تا از توانمندی‌های جدید پشتیبانی کند و کارکردهای جدیدی را فراهم کند.

پلتفرم نظارت ویدیویی پیشنهادی (VSP)، که در شکل ۱ نشان داده شده است، متشکل از پنج بلوک اصلی است: منابع ویدیو، کاربران یا گیرنده‌های ویدیو، شبکه SDN/NFV، توابع مجازی یا پلاگین‌های سرویس و مدیر سرویس ویدیویی.

فرستنده ویدیو دستگاهی متصل به شبکه است که قادر است ویدیو را به آدرس IP انتقال دهد، مثل وب‌کم، دوربین‌های IP، تلفن‌های هوشمند و تبلت‌ها و کامپیوترهای شخصی.

مدیر سرویس (Service Manager) پلتفرم نهایی را نشان می‌دهد، و کاربران پلتفرم را براساس پروفایل آنها و نیازهای آنها، و فرستنده‌های ویدیویی مجاز (دارای مجوز) مدیریت می‌کند. بعلاوه، با اتصال به فرستنده از طریق رابط وب یا اپلیکیشن موبایل، کاربران می‌توانند خدمات دریافتی را هماهنگ کنند، که در زیر توضیح داده شده است. یکی از مشخصات اصلی پلتفرم قابلیت گسترش آن است. این قابلیت از طریق نصب عناصر اختیاری اضافی فراهم می‌شود که پلاگین نامیده می‌شوند. پلاگین‌ها ابزارهای نرم افزاری هستند که با رابط خاصی به شبکه وصل می‌شوند. این پلاگین‌ها را همراه با خدمات اساسی که بوسیله پلتفرم در شروع راه اندازی سرویس فراهم می‌شوند، می‌توان به راحتی پشت سرهم (زنجیروار) وصل کرد تا خدمات پیچیده‌تری فراهم شود.



شکل ۱. سناریوی کاربری

۴-۲- نمونه‌هایی از پلاگین‌ها عبارتند از:

- **رمزگذاری ویدیو:** این پلاگین از دو قطعه نرم افزار تشکیل شده است، یکی برای درج در شروع زنجیره برای رمزگذاری ویدیوی منتقل شده، و دیگری در انتهای زنجیره برای رمزگشایی ویدیوی دریافتی.

- **نظارت منطقه‌ای:** این پلاگین به کاربر اجازه می‌دهد بخشی از منطقه تحت نظارت را برای دریافت و هشدار در صورت آشکار شدن حرکتی در آن تعریف کند.
- **پنهان کردن منطقه‌ای:** این پلاگین امکان پنهان سازی بخشی از منطقه را به دلایل محرمانگی فراهم می‌کند.
- **دنبال کننده هدف:** این پلاگین امکان اشاره به هدفی معین (مثلا شخصی که در دوربین دیده می‌شود)، و دنبال کردن آن را فراهم می‌کند حتی اگر هدف به مناطقی دیگر حرکت کند که تحت پوشش دوربین نیست، برای سناریوهای امنیتی مفید است.
- **موزائیک:** این پلاگین به کاربر امکان می‌دهد بیش از یک جریان ویدیویی را، که هر یک از دوربین متفاوتی می‌آیند، در یک جریان ویدیویی ترکیب کند تا امکان تماشای همزمان بیش از یک جریان فراهم شود.

در نهایت، شبکه SDN/NFV زیرساختار ارتباطی است که با شبکه نرم‌افزار محور (SDN) و الگوهای مجازی تابع شبکه (NFV) تکمیل می‌شود. با این الگوها می‌توان کارهای شبکه و کاربری را در گره‌های شبکه "نرم افزاری" کرد و هوش را در مرکز قرار داد تا منابع در واحد مرکزی که هماهنگ کننده (Orchestrator) نامیده می‌شود هماهنگ، مدیریت و تخصیص داده شوند.

با استفاده از SDN/NFV می‌توان به راحتی فرستنده‌ها و گیرنده‌های ویدیویی را به صورت "Plug & Play" و بوسیله گره‌های دسترسی هوشمند به پلتفرم وصل کرد. در واقع با الگوها NFV، می‌توان زنجیره سرویس برای مدیریت جریان‌های ویدیویی ایجاد کرد، و با الگو SDN جریان‌های ویدیویی ایجاد شده بوسیله فرستنده‌های ویدیویی در ورودی شبکه جدا کرد و به صورت خودکار به زنجیره سرویس لازم هدایت کرد و در نهایت به گیرنده‌های مربوطه فرستاد.

بکارگیری الگوهای SDN/NFV پلتفرمی را با ویژگی مقیاس پذیری فراهم می‌کند و تفاوت مهمی در آن نسبت به آخرین دستاوردهای فعلی در این حوزه پدید می‌آورد. در واقع، درپیشرفته ترین سیستم‌های نظارت ویدیویی، پردازش ویدیو در سرور مرکزی سطح بالا (OTT) نسبت به شبکه دربرگیرنده صورت می‌گیرد. بنابراین در این سیستم‌ها، شبکه دربرگیرنده باید بتواند جریان‌های ورودی را به تعداد دوربین‌های ورودی به سرور مرکزی انتقال دهد و به تعداد کاربر گیرنده از سرور مرکزی جریان‌ها را به کاربران انتقال دهد. برعکس، در این مورد، جریان‌های ویدیویی تولید شده بوسیله دوربین‌ها مستقیماً در گره‌های لبه، در نزدیک‌ترین فاصله ممکن به منبع ویدیویی طبق روش رایانش مه قابل پردازش هستند. بعلاوه، کاربران علاقه مند به یک جریان ویدیویی (یکسان) و دسترسی به شبکه از طریق یک گره دسترسی مشترک به لبه فقط یک جریان بزرگ را موجب می‌شوند، جریانی که به سمت گره خروجی هدایت می‌شود. ارتباطات نقطه با چند نقطه با گره خروجی برقرار می‌شود، بنابراین از اتلاف پهنای باند در شبکه اصلی اجتناب می‌شود. به همین دلیل، افزایش تعداد فرستنده‌ها و گیرنده‌های ویدیویی موجب افزایش بار و پیچیدگی شبکه دربرگیرنده نمی‌شود.

۵- مزایای حاصل با این فناوری

با توجه به آخرین سیستم‌های نظارت ویدیویی که امروزه در بازار وجود دارند، پلتفرم پیشنهادی ویژگی‌های زیر را دارد که می‌تواند توجه سهامداران اصلی سیستم را به خود جلب کند، یعنی اپراتور ارائه دهنده، کاربران و دریافت کنندگان خدمات نظارت ویدیویی.

در واقع به خاطر وجود فناوری SDN/NFV که برای تحقق SANها و NANها بکار رفته است، این پلتفرم مزایای عمده زیر را فراهم می‌کند:

۱) **کاهش ترافیک شبکه با بهبودهایی در عملکرد:** در واقع جریان داده‌ای که بوسیله هر فرستنده جریان داده تولید می‌شود به صورت خودکار و مستقیم فقط به "گیرنده‌های مربوطه" به صورت یک نقطه به چند نقطه، درون شبکه هدایت می‌شود و از نیاز به سرورهای سطح بالا (OTT) اجتناب می‌شود، که موجب تکرار جریان حتی برای کاربرانی می‌شود که از یک گره ورودی مشترک به شبکه دسترسی دارند.

۲) **مقیاس پذیری:** وقتی کاربری که جریان داده معینی را درخواست می‌کند و از طریق گره دسترسی به شبکه دسترسی پیدا می‌کند که حداقل یک کاربر در آن همان جریان را دریافت می‌کند، ترافیک شبکه افزایش نمی‌یابد. بعلاوه، افزایش ترافیک شبکه با تعداد فرستنده‌های جریان داده خطی است.

۳) **تاخیر سرتاسر پایین:** این مزیت از بکارگیری الگوی رایانش مه حاصل می‌شود، زیرا VFهای زیادی بوسیله گره‌های دسترسی برای کاربر فراهم می‌شود.

۴) **کاهش OpEX و CapEX:** چون بوسیله ابزارهای نرم‌افزاری صورت می‌گیرد که در سخت افزار عمومی اجرا می‌شوند.

۵) **Plug & Play:** نصب دوربین‌های جدید یا منابع دیگر جریان داده آسان است زیرا نیازی به پیکربندی ندارند: مقصد جریان ویدیویی آنها به صورت اتوماتیک بوسیله هماهنگ کننده مرکزی SDN/NFV تعیین می‌شود.

۶) **افزوده‌های پلتفرم:** پلتفرم می‌تواند از تعداد زیادی سرویس‌های تخصصی پشتیبانی کند (مثل رمزگذاری ویدیو، نظارت منطقه‌ای، پنهان سازی منطقه، دنبال کننده هدف، موزائیک) که به صورت پلاگین در برخی SANها یا گره‌های هسته طبق نیازهای کاربران نصب می‌شوند. به بیان دقیق‌تر، طبق نوع سرویسی که از سوی کاربران نهایی درخواست می‌شود، هر جریان داده از طریق مجموعه‌ای از VFهای لازم که در زنجیره‌های سرویس سازماندهی شده‌اند، مسیریابی و هدایت می‌شود؛ بعلاوه، پلتفرم به راحتی می‌تواند پلاگین‌های جدیدی ادغام کند تا توانمندی‌های جدیدی ادغام شود و کارهای جدید فراهم کند.

۶- اثبات مفهوم

۶-۱- مراحل شبیه سازی

شبیه سازی با اتصال شبیه ساز Mininet به دستگاه‌های واقعی فراهم شده است، مثل نقاط دسترسی بی‌سیم، 4G femtocell، کامپیوترهای شخصی و تلفن‌های هوشمند. کنترل کننده SDN بکار رفته در توپولوژی شبکه پیشنهادی نسخه تنظیم شده OpenDaylight است. همه اجزای مختلف پلتفرم نیز توضیح داده خواهد شد.

۶-۱-۱- Mininet (محیط مجازی رایانش و شبکه بندی)

Mininet شبیه ساز شبکه منبع باز است که به کاربران امکان ایجاد شبکه‌های مجازی نرم‌افزار محور را فراهم می‌کند که شامل کنترل کننده Open Flow، شبکه Ethernet با چند کلید مجهز به Open Flow، و چندین میزبان متصل به این کلیدهاست.

برپایی پلتفرم ، بوسیله ساختارهای پیکربندی زبان پایتون، پورت‌های کلید Open Flow با رابط‌های دستگاه-های فیزیکی شبکه که نتیجه مستقیما به چارچوب شبیه سازی وصل می‌شود، ویژگی اتصال را دارد. این راه حل امکان اتصال نقاط دسترسی فیزیکی بی سیم (AP) و شبکه‌های دسترسی رادیویی 4G (RAN) را فراهم می‌کند تا شبکه مورد آزمایش، و در نتیجه هر دستگاه فیزیکی (مثل تلفن هوشمند، کامپیوتر شخصی یا هر وسیله دیگری که با اینترنت کار می‌کند) به عنوان بخشی از شبکه شبیه سازی به نتایج APها / RANها وصل شود.

۶-۱-۲- OpenDaylight (کنترل کننده SDN)

کنترل کننده SDN در پلتفرم تقلیدی OpenDaylight منبع باز است. این کنترل کننده سیستم کار شبکه برای SDN-NFV است که با رهنمودهای بنیاد لینوکس و به زبان جاوا ایجاد شده است.

این کنترل کننده به عنوان کنترل کنندهی در زیرساختار مبتنی بر SDN-NFV عمل می‌کند، و امکان مدیریت شبکه‌هایی را نیز که به بخش‌هایی تقسیم شده‌اند، فراهم می‌کند. در نسخه فعلی، این کنترل کننده از نسخه Hydrogen، OpenDaylight استفاده می‌کند که از مشخصات Open Flow 1.0 پشتیبانی می‌کند. OSGi، چارچوب جاوا که امکان داشتن سیستمی چندبخشی را فراهم می‌کند، بکار رفته است. بنابراین می‌توان کارکردهای ODL را با استفاده از Bundleهای معروف گسترش داد. Bundle جزئی است که به زبان جاوا با استفاده از چارچوب OSGi و OpenDaylight Java API نوشته شده است، و امکان ایجاد قسمتی برای کنترل کننده را فراهم می‌کند؛ Bundle درون کنترل کننده اجرا می‌شود و می‌تواند با کلیدهای در شبکه هم کنشی کند.

OpenDaylight با کلیدهای L2 و اپلیکیشن‌ها با استفاده از رابط Southbound و Northbound هم-کنشی می‌کند. Northbound سرویس REST API را ارائه می‌دهد که امکان مدیریت شبکه را فراهم می‌کند. برای برقراری هم کنشی بین Southbound و کلیدهای L2، ODL از پروتکل‌های مختلفی پشتیبانی می‌کند؛ در چارچوب پیشنهادی از Open Flow 1.0 برای تضمین سازگاری و هماهنگی با Open VSwitches تقلید شده بوسیله Mininet استفاده می‌کند.

۶-۱-۳- 4G femtocell + Accuver XCore (شبکه دسترسی LTE + مقلد EPC)

برای فراهم کردن پلتفرم تقلیدی با شبکه دسترسی موبایل، "4G femtocell در باکس" به پلتفرم متصل شده است. femtocell ضمیمه، که اتصال LTE به دستگاه‌های موبایل در حال حرکت در منطقه تحت پوشش آن

را ممکن می‌سازد، به EPC Emulator Accuver XCORE متصل شده است که از طریق روتر وای-فای در لپ تاپ اجرا می‌شود. اتصال بین این دو عنصر بوسیله VPN صورت می‌گیرد که از قبل در چارچوب femtocell و در لپ تاپ پیکربندی شده است. مقلد XCORE EPC کار کل زیرساختار EPC را در یک کامپیوتر شخصی پیاده می‌کند، و به این ترتیب امکان تست و ایجاد راه‌حل‌هایی را برای سیستم‌های LTE بدون نیاز به زیرساختار شبکه واقعی فراهم می‌کند. ما از تلفن‌های هوشمند سامسونگ گالاکسی S4 استفاده کردیم که برای کار با femtocell با نصب سیم کارت ویژه‌ای از قبل پیکربندی شده بود.

۶-۱-۴- KVM (هایپروایزر توابع مجازی)

ماشین مجازی مبتنی بر کرنل (KVM) به عنوان هایپروایزر توابع مجازی انتخاب شده است. اپلیکیشن سرور-مشتری با هدف ایجاد رابط بین هماهنگ کننده شبکه و هایپروایزر ایجاد شده است. مشتریان در گره‌های پردازشی اجرا می‌کنند، یعنی گره دسترسی هوشمند ساختار پیشنهادی، و با سروری ارتباط برقرار می‌کنند که از آن دستورات ایجاد، تخریب، تعلیق یا جابجایی توابع مجازی را دریافت می‌کنند.

۶-۱-۵- توپولوژی

توپولوژی بستر تست که در شکل ۳ نشان داده شده است، بوسیله دو Intel NUC MiniPCs DC53427HYE (Ubuntu 14.04 به عنوان سیستم کار)، به نام MiniNet PC و PC B فراهم شده است، که به ترتیب مقلد شبکه MiniNet و کنترل کننده OpenDayLight را اجرا می‌کنند.

MiniNet PC مجهز به سه آداپتور است تا رابط‌های لازم شبکه برای داده‌های و برنامه مدیریت فراهم شود؛ سه نقطه دسترسی وای-فای به عنوان CPE برای دستگاه‌های مکمل 802.11 مثل کامپیوترهای شخصی و مانند آن عمل می‌کنند؛ و در نهایت، 4G femocell متصل به مقلد EPC دسترسی به تلفن‌های هوشمند 4G متصل به پلتفرم را فراهم می‌کند.

ماشین میزبان کنترل کننده OpenDayLight برای میزبانی هماهنگ کننده (Orchestrator) نیز بکار می‌رود، بنابراین به عنوان کنترل کننده شبکه SDN و سرور جلویی برای سرویس ما عمل می‌کند. این کنترل کننده برای مدیریت شبکه با رابط‌های اترنت به NUC دیگری متصل شد و با آداپتور اترنت-USB به نقطه دسترسی متصل شد (به این ترتیب می‌توان برای گره‌های درون شبکه تقلیدی آن را آدرس دهی کرد).

ساختار تنظیم شده راه اندازی و پیکربندی برای MiniNet، که به زبان پایتون نوشته شده است، امکان اتصال میان سه پورت فیزیکی اترنت MiniNet PC و Open vSwitches که بوسیله مقلد شبکه تقلید می‌شوند، را فراهم می‌کند.

بنابراین به طور کل زیرساختار تقلید شده متشکل از بخش کاملا مجازی شده (بوسیله ابزار MiniNet) و بخش شبکه حقیقی است که بوسیله الگوی پیکربندی به قسمت قبلی متصل می‌شود، و دستگاه‌های فیزیکی از طریق آن به کلیدهای مجازی وصل می‌شوند.

شبکه مجازی متشکل از ۸ کلید SDN است که به ۴ گره هسته متصل به هم به صورت شبکه کامل و ۴ گره لبه تقسیم می‌شوند، یکی برای هر گره، که به عنوان گره دسترسی هوشمند (SAN) عمل می‌کنند.

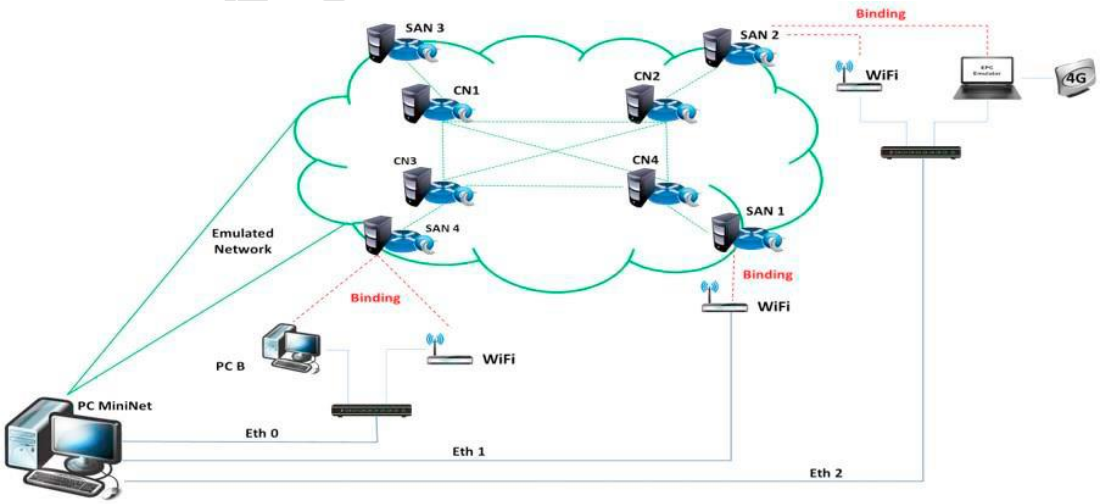
دستگاه‌های فیزیکی در پلتفرم سه نقطه دسترسی وای-فای است که به گره‌های دسترسی هوشمند SAN1, SAN2 و SAN4 متصل می‌شوند و هر یک اتصال بی سیم به دستگاه های وای فای را فراهم می‌کنند؛ Accuver Femtocell دسترسی رادیویی LTE را فراهم می‌کند و به SAN2 شبکه مجازی متصل شده است. به این ترتیب می‌توان سرویس SDN-NFV راکه فناوری دسترسی 4G را دربرمی‌گیرد، تست کرد.

۶-۲- بستر تست

اثبات ساده مفهوم در توپولوژی (شکل ۳) آغاز شده است. به عبارتی دقیق‌تر، دوربین مبتنی بر IP به گره دسترسی ۱ متصل می‌شود و تلفن هوشمند اندروید که اپلیکیشن موبایل را اجرا می‌کند به گره دسترسی هوشمند ۲ وصل شده است. SANها میزبان Open vSwitches و NFV Manager Clients است: بعد از شروع، اولی به کنترل کننده Open Daylight وصل می‌شود و دومی به سرور مدیر NFV وصل می‌شود، هر دو PC B میزبانی می‌شوند.

اپلیکیشن موبایل کاربر برای اندروید ایجاد کردیم تا کارکرد پلتفرم تست شود. اپلیکیشن موبایل در Android Studio v2.3 ایجاد شده است، و سازگاری با اندروید 5.0 (Lollipop) را تضمین می‌کند. با اپلیکیشن موبایل می‌توان:

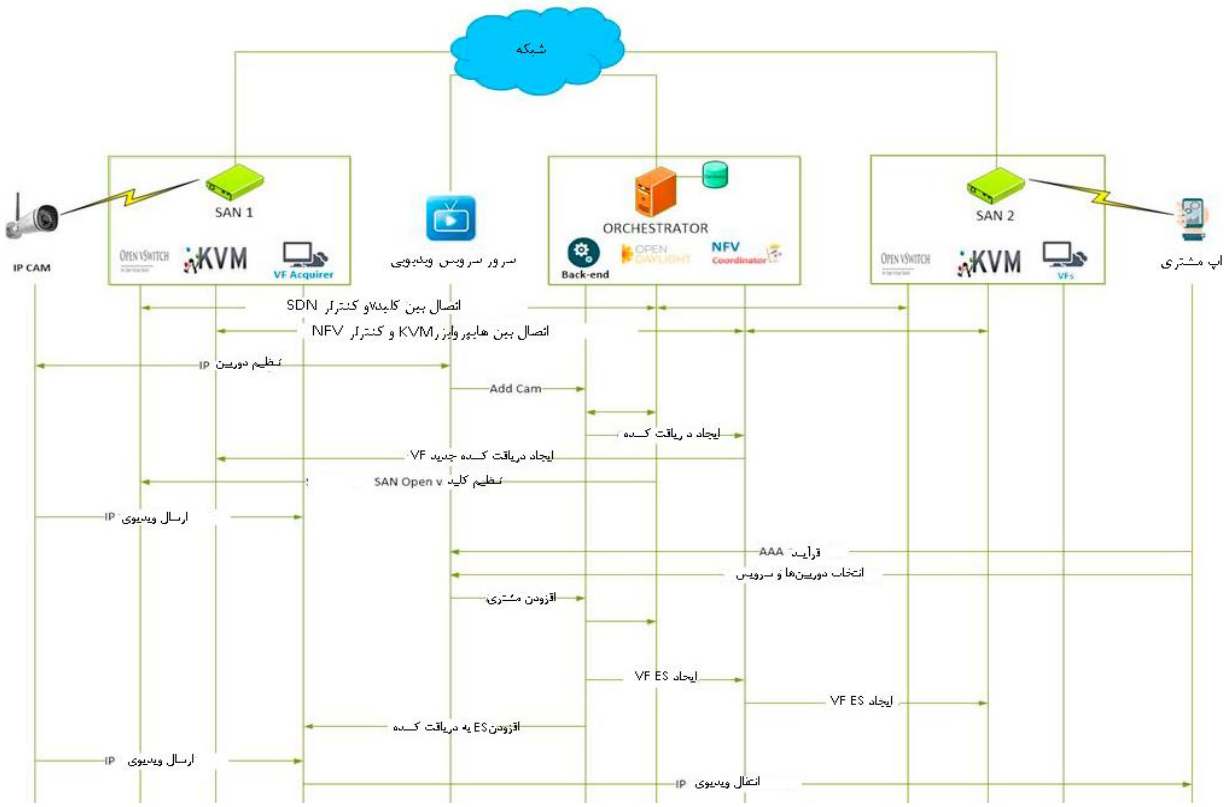
- دوربین مبتنی بر IP را برای سیستم نظارت ویدیویی ثبت کرد؛
- به سرویس ملحق شد.



شکل ۳. توپولوژی بستر تست

دوربین مبتنی بر IP با درج آدرس MAC، نام محل (یعنی ارجاع به جایی که دوربین قرار گرفته است)، مختصات جغرافیایی (برای مکان یابی جغرافیایی بوسیله نقشه‌های گوگل)، کد QR (کاربر بتواند دوربین‌هایی را که می‌خواهد با خواندن کد QR درون برنامه کاربردی موبایل انتخاب کند)، سرویس‌های موجود (تشخیص حرکت، ضبط، پخش زنده، شناسایی چهره و غیره)، و محدودیت ها (کاربران یا گروهی از کاربران مجاز به استفاده از خدمات هستند) را دریافت می کند.

بعد از ثبت دوربین مبتنی بر IP، سرور سرویس ویدیویی آدرس IP خود را به سرور بعدی منتقل می‌کند، که از طریق کنترل کننده SDN، از SAN که دوربین مبتنی بر IP به آن متصل شده است، مطلع می‌شود. در مثال ما، دریافت کننده تابع مجازی، که امکان جریان ویدیویی زنده را فراهم می‌کند، در SAN 1 راه اندازی شده است، و به عنوان ریشه درخت تحویل محتوای محلی عمل می‌کند و کارهای اصلی آن عبارتند از شناسایی جریان‌های رسانه (که از یک یا چند دوربین می‌آیند)، دریافت دستورات ارسال از هماهنگ کننده (Orchestrator) (به شکل فهرستی از آدرس‌های IP که جریان رسانه‌ای باید به آنها ارسال شود) و ارسال جریان‌های رسانه‌ای به مقصد.



شکل ۴. نمودار ترتیب اثبات مفهوم پیشنهادی

در مرحله دوم بستر تست یک کاربر از طریق اپ موبایل خود به سرویس ملحق می‌شود، و از SAN2 به شبکه دسترسی پیدا می‌کند. اپ موبایل به سرور سرویس ویدیویی متصل می‌شود و کاربر می‌تواند: دوربین مبتنی بر IP را از روی کد QR آن، نام محل آن یا با انتخاب آن با استفاده از نقشه انتخاب کند؛ و سرویس‌هایی را از میان سرویس‌های مربوط به دوربینی که انتخاب کرده است، انتخاب کند. پس از انتخاب دوربین و سرویس، سرور سرویس ویدیویی سه‌تایی (کاربر IP، دوربین ID، سرویس درخواستی ID) را به هماهنگ کننده (Orchestrator) می‌فرستد؛ هماهنگ کننده با ارسال پرسش به کنترل کننده SDN می‌داند کاربر به کدام SAN متصل است و با هماهنگ کننده NFV (Coordinator) ارتباط برقرار می‌کند تا تابع مجازی Edge Streamer را درون SAN2 شروع کند. در واقع، هدایت کننده لبه (Edge Streamer) فراکدگذاری جریان ویدیوی را با اجرای پخش کننده ویدیو در تلفن موبایل و براساس کتابخانه Vitamio انجام می‌دهد. Edge Streamer با استفاده از نسخه تنظیم شده نرم افزار منبع باز Multicat صورت می‌گیرد.

بعد از نمونه‌سازی Edge Streamer، هماهنگ کننده (Orchestrator) آدرس IP مقصد جدید را به دریافت کننده تابع مجازی ارسال می‌کند تا فهرست گیرنده‌های جریان ویدیویی را به روز سازد. از این پس ارسال جریان ویدیویی از دوربین مبتنی بر IP به کاربرانی که آن را درخواست کرده‌اند، شروع می‌شود. روند کار بستر تست که در بالا توضیح داده شد در شکل ۴ نشان داده شده است.

۷- فراگیر نشدن شبکه نرم افزاری

SDN امروزه برای شرکت های بسیاربزرگ کم کم در حال تبدیل شدن به یک واقعیت است اما این مساله برای شرکت های کوچک و متوسط کاملا متفاوت است. شرکت های سازنده تجهیزات سخت افزاری در حال کار بر روی تجاری‌سازی این فناوری هستند اما هنوز مسائل و سوالاتی درباره این مفهوم وجود دارد که باید آنها را با دقت بیشتر بررسی کرد.

۷-۱- مساله اول: امنیت

یکی از مسائل اصلی موجب نگرانی متخصصان فناوری اطلاعات در زمینه امنیت SDN است. به گفته یکی از متخصصان این زمینه در موسسه بیوتکنولوژی شهر اسلو، پیش از استفاده از این سیستم در کاربردهای حساس باید از نحوه کار و رابط کاربری این سیستم در رابطه با انتقال اطلاعات درون شبکه کاملا مطمئن باشیم. مثلا امروزه وقتی اطلاعات با استفاده از شبکه Juniper منتقل میشوند، چندین محل چک کردن اطلاعات و امنیت به صورت Static وجود دارد که کار را برای نفوذ به شبکه و اجرای بدافزار در شبکه دشوار می کند، اما چنین مکانیزمی در مورد SDN باید بیشتر مورد مطالعه قرار گیرد. طبق بررسی های انجام شده به صورت پایلوت برای یک کنترل کننده SDN در یک شبکه سیسکو و اچ پی، در هنگام مهاجرت از حدود ۶۰ عدد VLAN به کنترل کننده OpenDaylight در یک سیستم ابری با OpenStack مشکلاتی روی داد. این مشکل در زمینه بررسی شبکه برای ورودی و خروجی ها IDS/IPS بود. سیستم IDS/IPS توسط یک یا چندین پورت مشخص اجرا می‌شود تا کل ترافیک یک VLAN را برای Sniffing جایگزین کند. در سیستم‌های سنتی ترافیک به صورت سخت افزاری منتقل می شود و آنرا به IDS/IPS انتقال میدهد. اما برخلاف این روند، در SDN سیستم از دستورات یک سیستم عامل پیروی میکند تا اطلاعات را جایگزین کند.در نتیجه بررسی روی چندین IDS/IPS مشخص شد که SDN حدود ۲۵ تا ۳۰ درصد از Event های هدف را از دست میدهد. نتیجه‌گیری اولیه این است که

SDN در زمینه جایگزینی ترافیک روی پورت‌ها و از دست دادن ترافیک اترنت ضعیف‌تر عمل میکند. همچنین مشکلاتی در زمینه ثبت MAC Address نیز وجود داشت که بسیاری از این آدرس‌ها به علت مشکل در سیستم نرم‌افزاری SDN به درستی ثبت و منتقل نشده بودند. در بررسی دیگری نیز مشخص شد که در شرایط خاصی حمله‌کننده توانست به دسترسی کامل شبکه متصل شود و به دسترسی‌های اصلی شبکه که برای یک کاربر ثالث مجاز نیست دسترسی کامل پیدا کند، که این موضوع کاملا برای امنیت شبکه مخرب است.

طبق گفته کارشناسIT، شرکت VMware و دیگر شرکتهای تکنولوژی در حال کار روی حل این مشکلات امنیتی هستند. استفاده از این مفهوم در نهایت باعث کاربری ساده تر و ارزان تر شبکه ها خواهد شد اما برای استفاده در شبکه های مهم هنوز باید مشکلات امنیتی موجود در این روش، با دقت بیشتری بررسی و مرتفع شود.

۷-۲- مساله دوم: اتوماسیون

یکی از مزایای اصلی SDN، توانایی آن در تصمیم‌گیری بر اساس سیاست های شبکه به صورت نرم‌افزاری است. اما علاوه بر این SDN در مورد اتوماسیون نیز مورد استفاده قرار میگیرد. این مساله برای متخصصانی که قصد استفاده از SDN برای تحقیق و توسعه را دارند بسیار مهم خواهد بود. آنها میخواهند با ساخت یک چارچوب، موتور سخت‌افزارهای سازندگان مختلف را به هم متصل کنند و به صورت اتوماتیک سرویس‌ها را برای مشتریان خود اجرا کنند. تا به امروز شرکت‌های زیادی در این زمینه سرمایه‌گذاری نکرده‌اند زیرا مطمئن نیستند که آیا این امکان در سیستم های SDN وجود دارد یا خیر .

۷-۳- مساله سوم: آشنایی ناکافی

متخصصان IT در مورد SDN مطالعات زیادی کرده‌اند اما در عمل کمتر با این سیستمها کارکرده‌اند یا آنها را مدیریت کرده‌اند و این در حالی است که زیر ساخت فعلی شبکه ها دارای منابع اطلاعاتی کامل برای انجام همه کارهای شبکه است و روش های مختلفی که گاها زمان بر نیز هستند، برای اجرای هر دستور در شبکه وجود دارد.

متخصصان شبکه نیازمند درک بهتری از SDN هستند و اینکه چگونه این سیستم نیازهای جاری آنها را برآورده می‌کند. علاوه‌براین SDN وعده بهره وری بالاتر، اتوماسیون و هماهنگی کل شبکه را میدهد اما تا زمانی که متخصصان در عمل این ویژگی‌ها را بررسی نکنند این سیستم نمی‌تواند به‌قدرکافی گسترده شود.

۷-۴- مساله چهارم: استاندارد

برای اینکه متخصصان از SDN استفاده کنند نیاز به مهارتهای جدیدی دارند اما استانداردی وجود ندارد که دقیقا چه مهارتهایی مورد نیاز است و اینکه از کجا باید شروع کرد. متخصصان نیازمند این هستند که بدانند SDN چطور مهارت‌های فعلی آنها را تحت تاثیر قرار می دهد. متخصصان باید بدانند که چطور به صورت استاندارد این تکنولوژی به کار برده

می‌شود، تا حدود ۲ سال قبل تصور عمومی این بود که OpenFlow به صورت استاندارد جهانی خواهد بود اما امروزه بسیاری از سازندگان از این سیستم روی‌گردان شده‌اند و هم اکنون گزینه‌های دیگری نیز وجود دارند.

۵-۷- مساله پنجم: فروش

حتی اگر متخصصان آی‌تی در زمینه استفاده از این تکنولوژی قانع شوند و علاقه مند به استفاده از آن باشند باز هم باید مدیران ارشد و سرمایه‌گذاران را مجاب به مفید بودن استفاده از این سیستم کنند. SDN نیازمند سرمایه‌گذاری جدی در زمینه تجهیزات سازگار با این سیستم و همچنین سرمایه‌گذاری بیشتر در زمینه توسعه این تکنولوژی است. بسیاری از مدیران ارشد هنوز وقت و منابع مالی لازم برای این کار را ندارند. اما با این حال اگر بتوان راه‌های استفاده و کاربردهای بیشتری برای این تکنولوژی پیدا کرد مسلما فروش و گسترش آن هم آسان‌تر خواهد شد.

۸- نتیجه‌گیری

طراحی و گسترش پلتفرم پیشنهادی کاری بین رشته‌ای را در آینده می‌طلبد و در برمی‌گیرد، چون به کارشناسی در حوزه‌های شبکه ارتباطات راه دور، علوم کامپیوتر، برنامه نویسی کامپیوتر، مدیریت مرکز داده، شبکه‌های موبایل 4G و 5G، کدگذاری ویدیو، جرم یابی کامپیوتر، امنیت، وب و طراحی اپ موبایل نیاز دارد. به همین دلیل، گسترش این پلتفرم را می‌توان بذری اولیه برای ایجاد زیرساختار توانمندی‌هایی در توسعه آتی پلتفرم به منظور ارائه سرویس‌های پیچیده تر با عملکرد بهتر محسوب کرد.

منابع

1. White paper on “Software-Defined Networking: The New Norm for Networks”, available at https://www.opennetworking.org/.
2. White paper on “Network Functions Virtualisation”, available at http://portal.etsi.org/NFV/NFV_White_Paper.pdf.
3. A. Manzalini *et al.*, “Software-Defined Networks for Future Networks and Services,” White Paper based on the IEEE Workshop SDN4FNS, 2014.
4. A. Manzalini and R. Saracco, "Software Networks at the Edge: A Shift of Paradigm," *2013 IEEE SDN for Future Networks and Services (SDN4FNS)*, Trento, 2013.
5. V. Sekar, S. Ratnasamy, M. K. Reiter, N. Egi, G. Shi, "The middlebox manifesto: Enabling innovation in middlebox deployment", Proc. ACM HotNets-X, pp. 1-6, 2011.
6. G. Calarco, C. Raffaelli, G. Schembra, G. Tusa, “Comparative Analysis of SMP Click Scheduling Techniques,” Proc. of QoSIP 2005, Catania (Italy), February 2-4, 2005, pp. 379-389.
7. R. Morris, E. Kohler, J. Jannotti, and M. F. Kaashoek, “The Click modular router,” Proc. of the 17th ACM Symposium on Operating Systems Principles (SOSP '99), pages 217--231, Kiawah Island, South Carolina, December 1999.
8. A. Lombardo, C. Panarello, D. Reforgiato, G. Schembra, “Measuring and modeling Energy Consumption to design a Green NetFPGA Giga-Router,” in Proc. of IEEE Globecom 2012, Anaheim, California, USA, 3-7 December 2012.
9. P. Sharma, S. Banerjee, D. Demir, S. Natarajan and S. Mandavilli, "NEEM: Network energy efficiency manager," *2012 IEEE Network Operations and Management Symposium*, Maui, HI, 2012.

10. A. Lombardo, *et al.*, "Multipath Routing and Rate-Controlled Video Encoding in Wireless Video Surveillance Networks," Multimedia Systems, Volume 14, Number 3, pp. 155-165.
11. X. Fu and B. l. Guo, "Framework for Distributed Video Surveillance in Heterogeneous Environment," *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Harbin, 2008.
12. L. Galluccio, *et al.*, "An analytical framework for the design of intelligent algorithms for adaptive-rate MPEG video encoding in next generation time-varying wireless networks," *IEEE Journal on Selected Areas in Communications*, Vol. 23 No. 2, February 2005.
13. Thung-Hiung Tsai and Jin-Jang Leou, "A rate control scheme for H.264 video transmission," *2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No.04TH8763)*, Taipei, 2004.
14. A. Lombardo, G. Schembra, "Performance evaluation of an Adaptive-Rate MPEG encoder matching IntServ Traffic Constraints," *IEEE Transactions on Networking*, vol. 11, no. 1, pp. 47-65, February 2003.
15. D. M. Dumbere and N. J. Janwe, "Video encryption using AES algorithm," *Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014*, Coimbatore, 2014.
16. M. Li, C. Yang and J. Tian, "Video Selective Encryption Based on Hadoop Platform," *2015 IEEE International Conference on Computational Intelligence & Communication Technology*, Ghaziabad, 2015, pp. 208-212.
17. A. Lombardo, M. Barbera, C. Panarello, G. Schembra, "Active Window Management: an efficient gateway mechanism for TCP traffic control", Proc. IEEE ICC 2007, GLASGOW, Scotland (UK), 24-28 June 2007.
18. M. Barbera, A. Lombardo, G. Schembra, M. Tribastone, "A Markov Model of a Freerider in a BitTorrent P2P Network," Proc. IEEE Globecom 2005, St. Louis, MO, USA, 28 Nov. – 2 Dec. 2005, pp. 985-989.
19. N. Magharei, Y. Guo and R. Rejaie, "Issues in Offering Live P2P Streaming Service to Residential Users," 2007 4th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 2007.
20. A. G. Busà, A. Lombardo, M. Barbera, G. Schembra, "CLAPS: A Cross-Layer Analysis Platform for P2P video Streaming," *Proc. IEEE ICC 2007*, GLASGOW, Scotland (UK), 24-28 June 2007.
21. Mininet, Available online at http://mininet.org/
22. Openflow, Available online at http://www.opennetworking.org/sdn-resources/openflow
23. OpenDaylight, Available online at http://www.opendaylight.org
24. Xcore LTE EPC Net. Emulator, http://www.accuver.com
25. Kernel Virtual Machine, https://www.linux-kvm.org/page/Main_Page
26. Vitamio SDK, https://www.vitamio.org/en/
27. Multicat, http://www.videolan.org/projects/multicat.html