بسمه‌تعالی

گزارش و تحلیل مقاله

SDN-Enabled IoT- Ensuring Reliability in IoT Networks Through Software Defined Networks

تعریف مسئله و هدف اصلی مقاله

تضمین قابلیت اطمینان برای شبکه‌های اینترنت اشیا (IOT) خصوصا در مواردی مثل اتومبیل‌های خودران، اینترنت لمسی[1]، تجهیزات مراقبت‌های بهداشتی که جهت تسهیل خدمات به اتصال بدون وقفه نیازمند هستند، بسیار مهم است.

شبکه‌های نرم‌افزارمحور (SDN) برنامه‌نویسی شبکه را تسهیل و مدیریت کارا بر شبکه‌های پیچیده مثل اینترنت اشیا را امکان‌پذیر می‌کند. جهت یک پیاده‌سازی کارا و مداوم از SDN در شبکه اینترنت اشیا، باید چالش‌های قابلیت اطمینان در راستای ارائه سناریوهای انتقال اطلاعات با تاخیر کم و بسیار مطمئن حتی در صورت وجود خرابی در شبکه را حل کرد.

برای شبکه‌های اینترنت اشیا مبتنی بر SDN باید تشخیص خطا و بازگردانی سرویس‌ها بسیار سریع رخ دهد در حالی‌که فشاری بر data plane یا کنترلر مرکزی SDN (SDNC) وارد نشود.

تحقیقات مرتبط

تحقیقات زیادی در زمینه مدیریت خرابی وجود دارد. در این قسمت برخی از آن‌ها را بررسی می‌کنیم.

مکانیزم‌های بازیابی شکست[2]

در شبکه‌های CGN با استراتژی‌های ترمیم و محافظت، شکست بازیابی می‌شود. بعد از شناسایی شکست، مسیرهای پشتیبان جهت بازیابی، برقرار می‌شوند. در این شرایط، تخصیص پویای منابع، باعث تاخیر در بازیابی می‌شود. هم‌چنین در استراتژی محافظت، مسیرهای پشتیبان قبل از رخ دادن شکست، تنظیم می‌شوند. این روش از نظر تاخیر، بهینه است.

استراتژی محافظت به دو روش:

- حفاظت از لینک
- حفاظت از مسیر
  - روش ۱:۱ حفاظت از مسیر: بسته‌ها فقط در مسیر اصلی ارسال شده و در صورت شکست از مسیر پشتیبان ارسال می‌شوند.

---

[1] Tactile

[2] Failure recovery mechanism

- روش ۱+۱ حفاظت از مسیر: بسته‌ها همزمان از مسیر اصلی و پشتیبان ارسال شده و در صورت شکست یکی از مسیرها، فقط پهنای باند ارسال کاهش پیدا می کند.

تقسیم می‌شوند.

کشف شکست در CGN با استفاده از Bi-Directional Forwarding Detection (BFD) و Loss of Signal (LOS) انجام می‌پذیرد. در LOS وضعیت پورت از UP به DOWN در صورت شکست سوییچ، تغییر می‌کند. هم‌چنین در پروتکل BFD، پیام "Hello" به صورت دوره‌ای بین سوییچ‌ها رد و بدل می‌شود و زمانی که لینک ارتباطی بین سوییچ‌ها از کار بیافتد، نشست BFD همسایگان بریده شده و اعلان پخش می‌شود.

بازیابی شکست در SDN

محققان زیادی روی شکست در SDN کار می‌کنند. بیشتر کارهای موجود روی تنظیم مسیر پشتیبان برای جریان‌های قطع شده، تمرکز دارند. برخی پیشنهاد دارند که مسیری پشتیبان برای هر جریان تعریف شود. با توجه به وجود هزاران جریان برای هر لینک، در زمان شکست ممکن است فشار زیادی بر سوییچ جهت تعریف مسیرهای پشتیبان وجود داشته باشد.

محدودیت حافظه در سوییچ‌های شبکه، در تعریف مسیرهای پشتیبان محدودیت ایجاد می‌کند. تحقیقات نشان داده که برای ۱۰۰.۰۰۰ گره محاسباتی در یک مرکز داده، میلیون‌ها جریان وجود دارد. در این سناریو، امکان ذخیره مسیرهای پشتیبان به دلیل فشار بر کنترلر مرکزی و ایجاد گلوگاه، وجود ندارد. حافظه Ternary Content-Address Memory (TCAM) که جهت ذخیره جریان‌ها کاربرد دارد، در حال حاضر حداکثر ظرفیت ۶۰۰۰ جریان را دارد که امکان ذخیره میلیون‌ها مسیر اصلی و پشتیبان را به ما نمی‌دهد.

برخی تحقیقات از روش ترمیم برای بازیابی، استفاده می‌کنند. روش‌های ترمیم، زمان بیشتر نسبت به روش‌های محافظت، جهت بازیابی نیاز دارند. روش‌های ارائه بازیابی با ترمیم بیشتر بر ویژگی fast failover group تکیه دارند. این ویژگی خود وابسته به سازنده و نسخه firmware سوییچ است و نمی‌توان روی آن حساب کرد.

محققان این مقاله علاوه بر تمام چالش‌های موجود در این زمینه، در تحقیقات پیشین خود، راه حل‌هایی ارائه کرده‌اند که در ادامه به آن می‌پردازیم.

راه‌حل پیشنهادی مقاله برای مسئله و ارزیابی آن

در یک شبکه اینترنت اشیا مبتنی بر SDN، مکانیسم محافظت را می‌توان به رویکرد پیشگیرانه[1] یا واکنشی[2] تحقق بخشید. در یک رویکرد واکنشی، پس از تشخیص خرابی، ورودی‌های هدایت شده در سوییچ اصلاح مسیر می‌شوند تا جریان‌ها متوقف شده به مسیر پشتیبان از قبل پیکربندی‌شده تغییر مسیر دهند. در مقابل، در رویکرد فعال، گره سوییچینگ، خرابی پورت را تشخیص می‌دهد و جریان‌های قطع شده را به مسیر پشتیبان از پیش تنظیم شده تغییر مسیر می دهد.

---

[1] Proactive

[2] Reactive

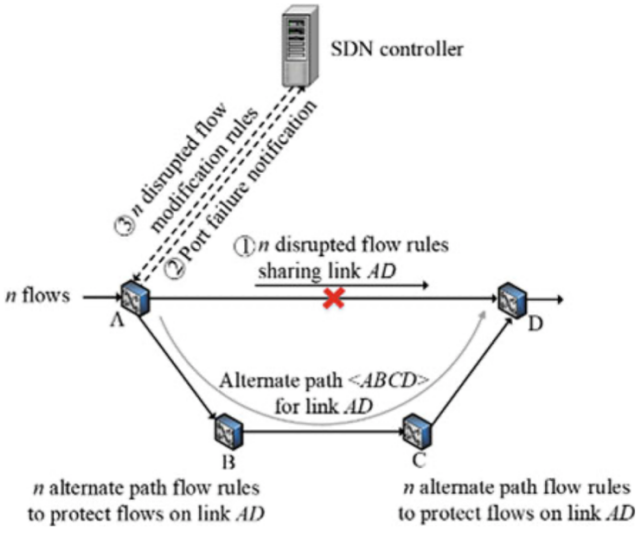
جهت ارزیابی روش پیشنهادی، توپولوژی شبکه AT&T در Mininet در نظر گرفته می‌شود. هم‌چنین جهت عدم تاثیر مسیرهای داده و کنترلی بر هم، یک ارتباط مستقل بین هر سوییچ و کنترلر تعریف شده است. با استفاده از iPerf جریان بسته به سرعت 100Mbps که هر بسته آن ۵۰ بایت حجم دارد، ایجاد می‌شود.

روش بازیابی لینک در اینترنت اشیا مبتنی بر SDN

در ابتدا یک روش سر راست وابسته به کنترلر (CoD) پیاده‌سازی شده است که جهت تغییر مسیر جریان متوقف شده نیاز به درگیری SDNC دارد. برای به حداقل رساندن بار SDNC از روش Local Immediate (LIm) که به قابلیت Fast Failover (FF) پروتکل OpenFlow وابسته است، استفاده شده است. روش Lim با در نظر گرفتن مصرف حافظه جدول جریان، جریان‌های متوقف شده را در یک جریان واحد، جمع می‌کند. قابلیت FF به سازنده و فریمور سوییچ وابسته است و برای غلبه بر این موضوع، روش Intermediate control dependent (ICoD) پیشنهاد شده است. در این روش، بازیابی لینک با حداقل درگیری SDNC و کاهش زمان بازیابی با عدم نیاز به تغییر مسیر جداگانه برای هر جریان، انجام می‌شود.

رویکرد بازیابی CoD

در روش بازیابی CoD، هنگامی که ارتباط بین سوییچ A و D قطع می‌شود همانطور که در تصویر- ۱ نشان داده شده است، سوییچ A خرابی پورت را شناسایی می‌کند و اعلان خرابی پورت را به SDNC منتقل می‌کند. در پاسخ، SDNC با ارسال پیام‌های اصلاح n جریان، تغییر مسیر n جریان متوقف شده از سوییچ A به سوییچ B را با مسیر پشتیبان از پیش پیکربندی‌شده ABCD برای پیوند AD، انجام می‌دهد. سوییچ B و سوییچ C از پیش برای مسیرهای جریان پشتیبان، با قوانین n جریان، تنظیم شده‌اند.



تصویر- ۱

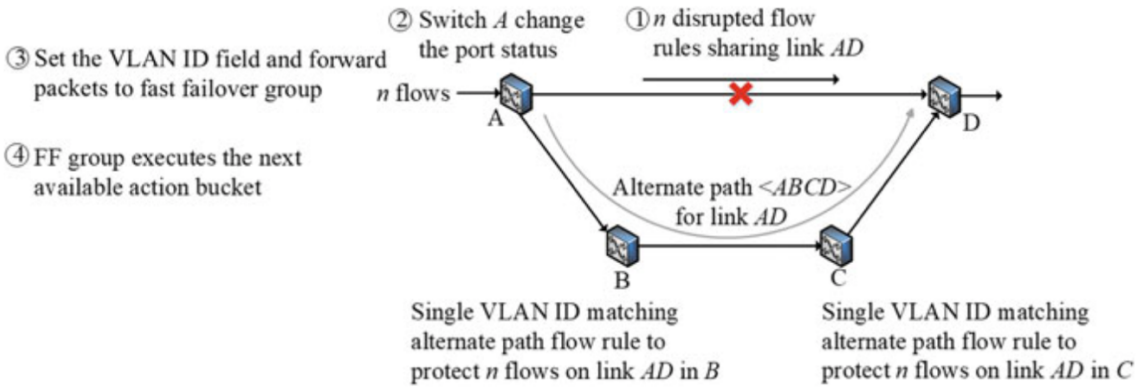
رویکرد بازیابی LIm

این رویکرد از قابلیت group table از OpenFlow 1.1 که جهت گروه‌بندی جریان‌های ورودی با پورت‌های معمول خروجی، استفاده می‌شود، استفاده کرده است.

با استفاده از گروه FF، یک سوییچ به صورت محلی جریان‌های متوقف شده را تغییر مسیر داده و نیاز به درگیری SDNC را برطرف می‌کند.

در روش LIm وقتی جریان‌ها به سوییچ می‌رسند، با شناسه لینک بالادستی، برچسب‌گذاری می‌شوند. شناسه لینک در بخش VLAN Tag از هدر VLAN بسته، کدگذاری می‌شوند. پس از خرابی اتصال بین سوییچ A و D همانطور که در تصویر- ۲ نشان داده شده است، سوییچ A خرابی پورت را شناسایی می‌کند و وضعیت پورت خراب را از UP به DOWN تغییر می‌دهد. واحد عملکرد گروههای FF با درگاه خروجی با وضعیت پایین ، واحد عمل بعدی را که مسیر قطع شده به مسیر پشتیبان اختصاصی ABCD را تغییر می دهد ، اجرا می کند. قوانین جریان متوقف شده در مسیر پشتیبان با استفاده از شناسه VLAN آن در سوئیچ های B و C مطابقت دارد. با استفاده از استراتژی جمع آوری جریان فعال شده توسط VLAN ، یک قاعده جریان واحد در کلیدهای مسیر پشتیبان می تواند اتصال n جریان متوقف شده را بازیابی کند. واحد[1] عملکرد گروه‌های FF با پورت خروجی در وضعیت DOWN، واحد عمل بعدی را که مسیر قطع شده را به مسیر پشتیبان اختصاصی ABCD تغییر می‌دهد ، اجرا می‌کند.

قوانین جریان قطع شده در مسیر پشتیبان با استفاده از شناسه VLAN آن در B و C مطابقت می‌کند. با استفاده از استراتژی تجمیع جریان، فعال شده توسط VLAN، یک قاعده جریان واحد در سوییچ‌های مسیر پشتیبان می‌تواند اتصال n جریان متوقف شده را بازیابی کند.



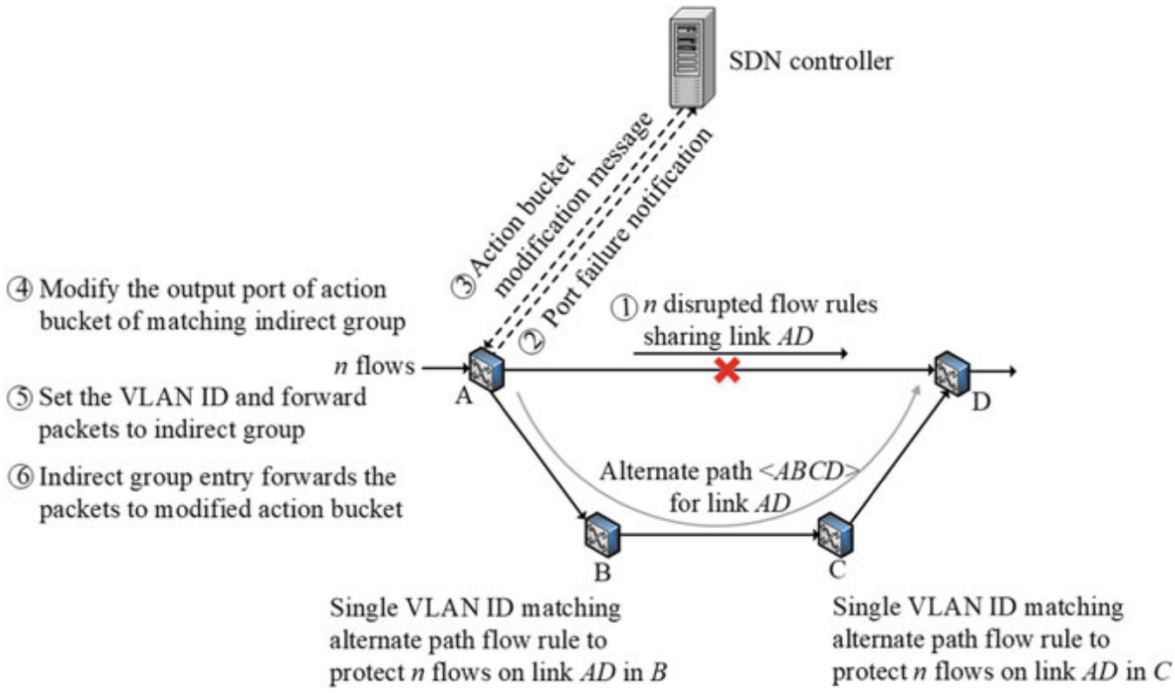
تصویر- ۲

[1] Bucket

مکانیزم ICoD

در این مقاله روش ICoD جهت رفع کاستی روش LIm که به FF group وابسته است ارائه شده است. در این مکانیزم از قابلیت Indirect group پروتکل OpenFlow استفاده شده است.

در رویکرد بازیابی ICoD، هنگامی که ارتباط بین سوییچ A و D قطع می‌شود، همان‌طور که در تصویر- ۳ نشان داده شده است، سوییچ A خرابی پورت را شناسایی می‌کند و یک اعلان به SDNC منتقل می‌کند. پس از دریافت اعلان خرابی، SDNC پیام اصلاح ورودی گروه را برای تغییر درگاه خروجی واحد عمل که تحت تاثیر خرابی قرار دارد، ارسال می‌کند. یک پیام اصلاح گروهی می‌تواند n جریان موجود در پیوند AD را به مسیر پشتیبان خود یعنی ABCD تغییر مسیر دهد. قوانین جریان متوقف شده در مسیر پشتیبان با شناسه VLAN آن در سوییچ‌های B و C مطابقت دارد. با استفاده از استراتژی تجمیع جریان فعال شده توسط VLAN، یک قاعده جریان در هر سوییچ مسیر پشتیبان می‌تواند اتصال n جریان متوقف شده را بازیابی کند.



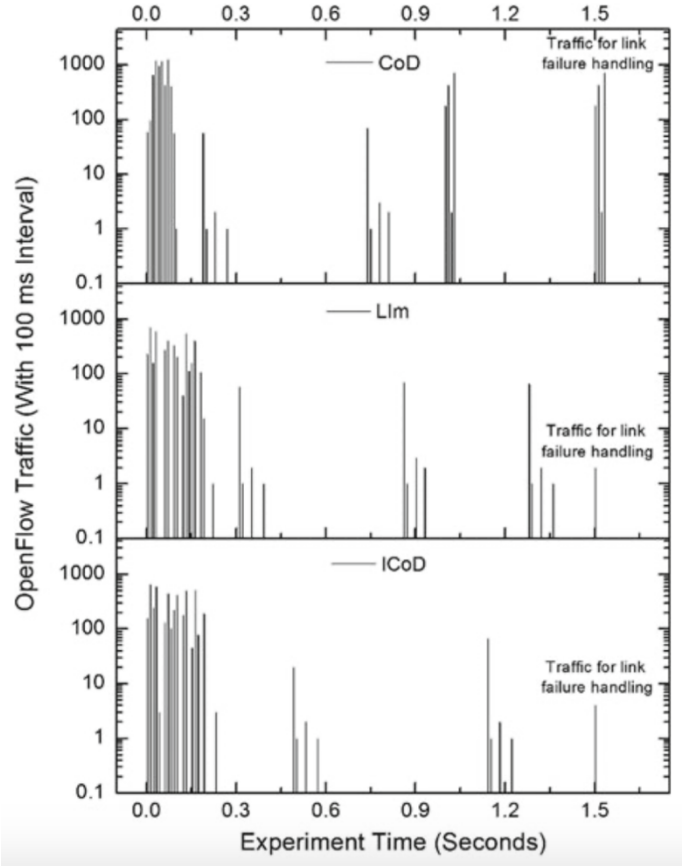
تصویر- ۳

ارزیابی عملکرد

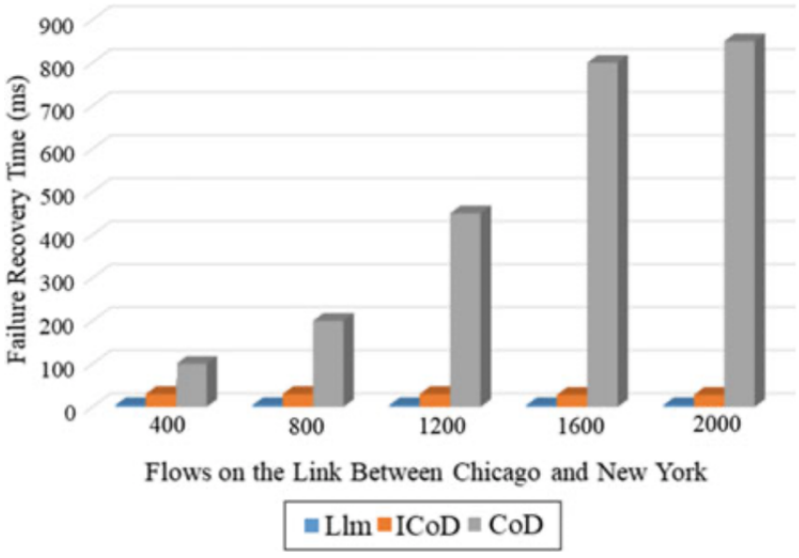
ارزیابی عملکرد بر اساس ساختار شبکه AT&T که پیش‌تر اشاره کردیم انجام شده است. مقایسه عملکرد روش‌های LIm، CoD و ICoD انجام شده است. معیارهای این ارزیابی شامل این موارد هستند:

- ترافیک تجربی در SDNC (تصویر- ۴)
- زمان بازیابی شکست (تصویر- ۵): برای روش LIm ۳-۲ میلی ثانیه، ICoD ۲۰ میلی ثانیه و CoD وابسته به تعداد جریان‌های قطع شده

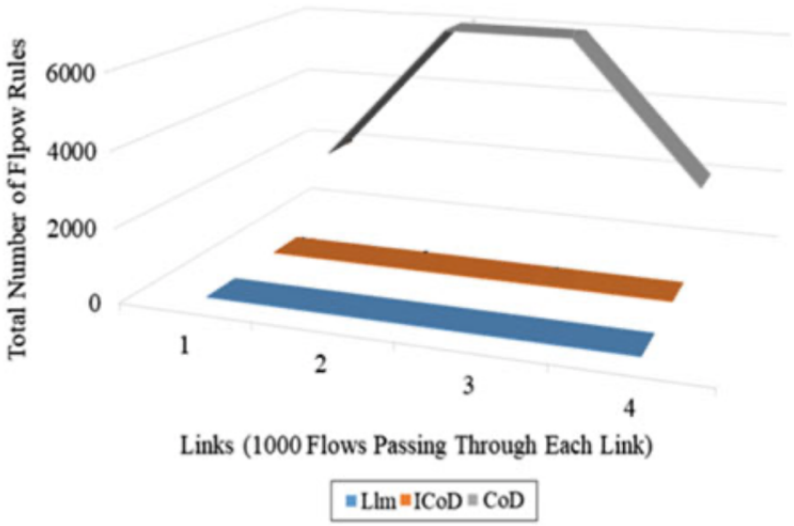
- تعداد قوانین جریان نصب شده برای محافظت لینک (تصویر- ۶): بیش از ۹۹ درصد قوانین جریان در روش LIm و ICoD کاهش یافته



تصویر- ۴



تصویر- ۵

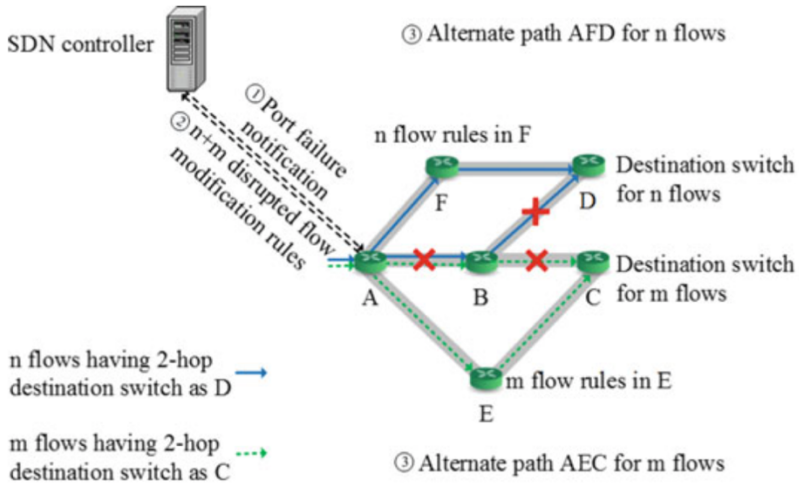


تصویر- ۶

بازیابی سریع و مقاوم گره از ترافیک داده‌ها در شبکه‌های اینترنت اشیا مبتنی بر SDN

رویکرد واکنشی

رویکرد واکنشی ساده‌ترین رویکرد برای درک بازیابی شکست است. پس از رسیدن جریان ورودی، SDNC یک مسیر ارسال را محاسبه می‌کند و قوانین جریان را برای برپایی مسیر، پیکربندی می‌کند. پس از برپایی مسیر اصلی، SDNC باید یک مسیر پشتیبان برای هر یک از پیوندهای اصلی یا پیوند سوییچ و لبه تنظیم کند. وقتی سوییچ یا پیوند خراب می‌شود، سوییچ خرابی را شناسایی می‌کند و SDNC را مطلع می‌کند. در پاسخ، SDNC پورت پشتیبان را برای پورت قطع‌شده پیدا می‌کند و پورت خروجی عملکرد قانون جریان را به روز می‌کند تا جریان قطع شده را به مسیر پشتیبان از قبل پیکربندی شده برای سوییچ یا لینک شکست خورده، تغییر دهد.

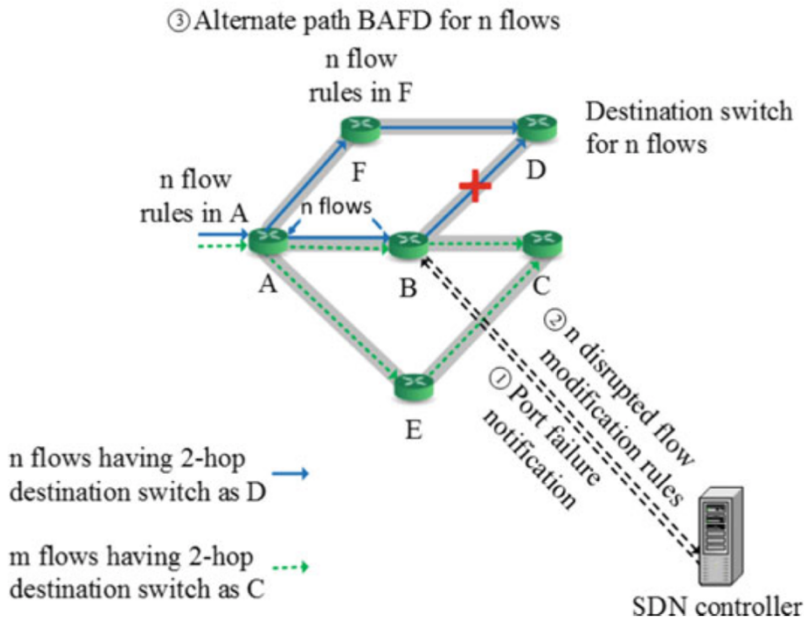


تصویر- ۷

هنگامی که اتصال بین سوییچ A و B یا سوییچ B همانطور که در تصویر- ۷ نشان داده شده مختل می‌شود، سوییچ A خرابی را شناسایی کرده و SDNC را مطلع می‌کند. در پاسخ، SDNC پیام‌های بروزرسانی جریان را

برای هر جریان قطع‌شده در اتصال بین سوییچ A و B به سوییچ ۲-هاپ مورد نظر خود از طریق مسیر پشتیبان از پیش تنظیم شده می‌فرستد. برای محافظت از n جریان که از سوییچ A به D وجود دارند، مسیرهای پشتیبان AFD و AED به ترتیب با پیکربندی قوانین n و m جریان در سوییچ F و E تنظیم می‌شوند.

برای خرابی BD در پیوند لبه، مسیر پشتیبان BAFD از قبل پیکربندی شده است. پس از اطلاع رسانی خرابی، SDNC پیام به‌روزرسانی جریان را به سوییچ B منتقل می‌کند تا جریان‌های قطع شده از اتصال بین سوییچ‌های B و D به مسیر پشتیبان BAFD تغییر مسیر یابند. سوییچ B جریان‌هایی با لینک اصلی BD را به همسایه ۲-هاپ، تغییر مسیر می دهد (تصویر- ۸).



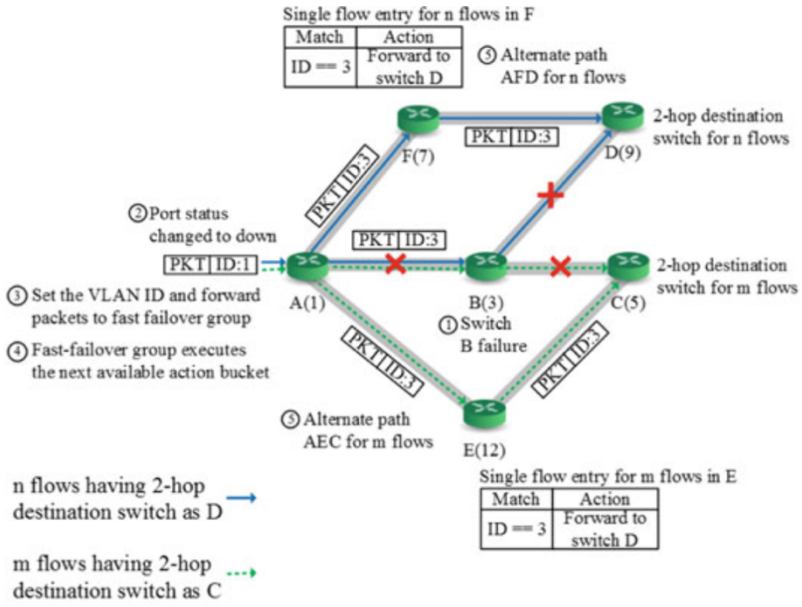
تصویر- ۸

رویکرد پیشگیرانه

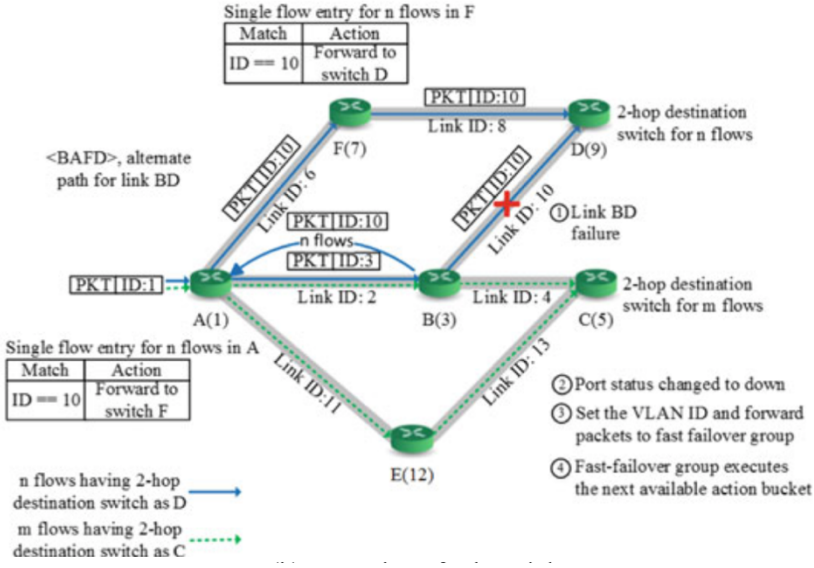
برای از بین بردن نیاز به درگیری SDNC، ویژگی FF OpenFlow استفاده شده است. گروه FF می‌تواند جریان‌ها را به صورت محلی تغییر مسیر دهد و بنابراین در دستیابی به بازیابی سریع و پیشگیرانه کمک کند. با این حال، برای تغییر مسیر محلی، مسیرهای پشتیبان باید از قبل پیکربندی شوند. در این مقاله از استراتژی تجمیع جریان در بازیابی پیشگیرانه استفاده شده که جریان‌هایی با سوییچ مقصد مشترک را با برچسب‌گذاری تجمیع می‌کند تا مصرف حافظه جدول جریان را برای ذخیره قوانین جریان مسیر پشتیبان کاهش دهد. در مسیر پشتیبان، SDNC فقط یک قانون جریان واحد را پیکربندی می‌کند که با برچسب جریان‌های تجمیع‌شده شده مطابقت دارد.

با قطع اتصال AB یا سوییچ B همانطور که در تصویر- ۹ نشان داده شده است، سوییچ A خرابی را شناسایی می‌کند، بسته‌ها را با شناسه سوییچ هسته شکست خورده برچسب‌گذاری می‌کند و جریان‌های قطع شده به سمت همسایه ۲-هاپ را از طریق مسیرهای پشتیبان از پیش تنظیم شده به صورت محلی تغییر مسیر می

دهد. بسته‌های ورودی در مسیر پشتیبان با استفاده از شناسه VLAN در هدر بسته در سوییچ F تطبیق داده می‌شوند و دوباره بسته‌ها را به سوییچ بعدی در مسیر پشتیبان هدایت می‌کند. به طور مشابه، در تصویر- ۱۰، سوییچ B با استفاده از مسیر پشتیبان BAFD بسته را در اطراف لینک، تغییر مسیر می‌دهد. روش پیشنهادی برخلاف بازیابی واکنشی به بهبودی محلی دست می یابد.



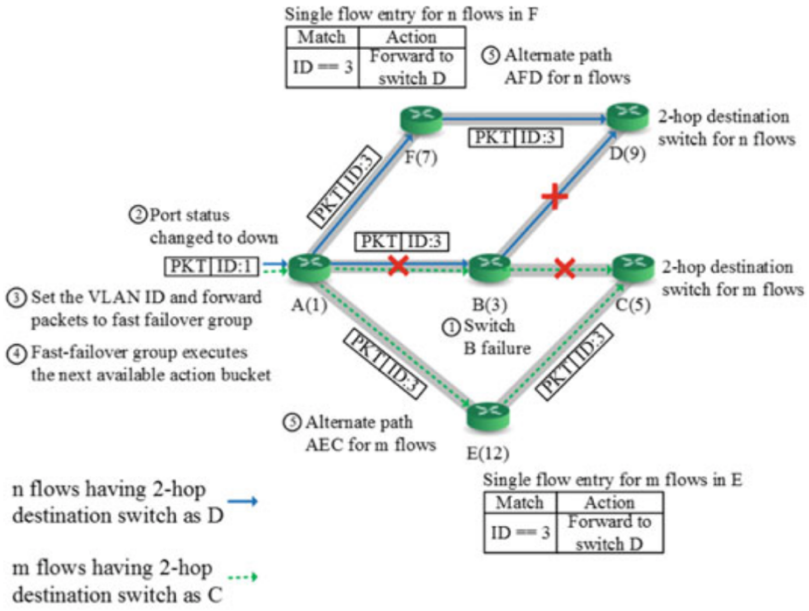
تصویر- ۹



تصویر- ۱۰

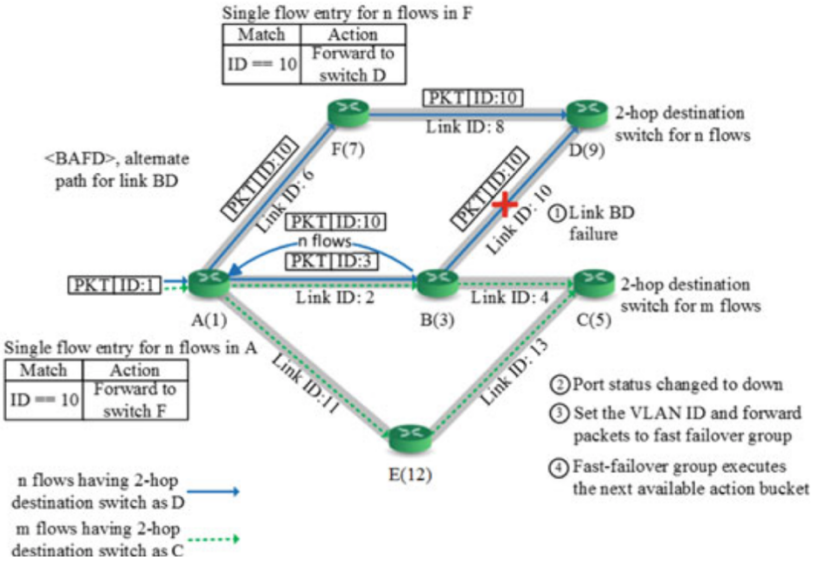
رویکرد ترکیبی[1]

در این مقاله رویکرد ترکیبی به دلیل رفع نقص رویکرد پیشگیرانه در وابستگی به FF ارائه شده است. در این روش از Indirect group در OpenFlow استفاده شده است. همانند روش پیشگیرانه در این روش نیز مسیرهای پشتیبان را جهت امن کردن سیستم در مقابل خرابی لینک و سوییچ، از پیش پیکربندی شده است. برای کاهش مصرف حافظه سوییچ در پیکربندی مسیرهای پشتیبان، با استفاده از مکانیسم برچسب‌گذاری جریان مبتنی بر VLAN، جریان‌ها تجمیع شده‌اند. در رویکرد ترکیبی پیشنهادی، وقتی پیوند لبه BD همانطور که در تصویر- ۱۱ نشان داده شده مختل می‌شود، سوییچ متاثر از خرابی، خرابی پورت را شناسایی می‌کند و پیام اطلاع‌رسانی پورت DOWN شده را به SDNC منتقل می‌کند. در پاسخ، SDNC پیام تغییر Indirect group را برای مسیریابی مجدد جریان‌های موجود در پیوند BD به سوییچ لبه D از طریق مسیر پشتیبان BAFD ارسال می‌کند. پیام اصلاح، پورت خروجی واحد اقدام Indirect group را از یک پورت ناموفق به یک پورت پشتیبان تغییر می دهد، که جریان‌های متوقف شده را به مسیر پشتیبان BAFD تغییر مسیر می‌دهد. بنابراین، طرح بازیابی ترکیبی می‌تواند بازیابی را برای تمام جریان‌های تحت تاثیر خرابی پیوند لبه با یک پیام اصلاحی به گروه انجام دهد. با این حال، برای یک جز از هسته شبکه، جریان‌ها باید بر اساس سوییچ همسایه ۲-هاپ آن تجمیع شوند. در مورد خرابی سوییچ B یا اتصال AB همان‌طور که در تصویر- ۱۲ نشان داده شده است، جریان‌های قطع شده از طریق مسیرهای پشتیبان به سوئیچ همسایه ۲-هاپ منحرف می‌شوند.



تصویر- ۱۱

[1] Hybrid

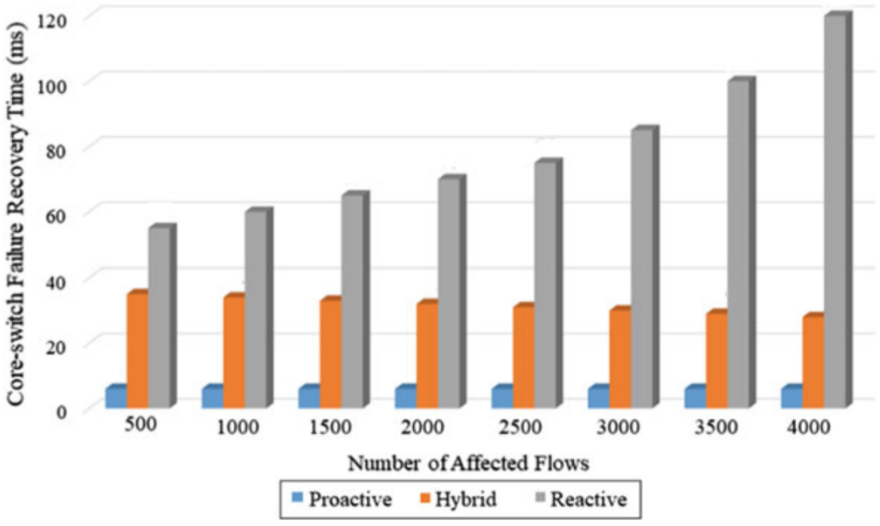


تصویر- ۱۲

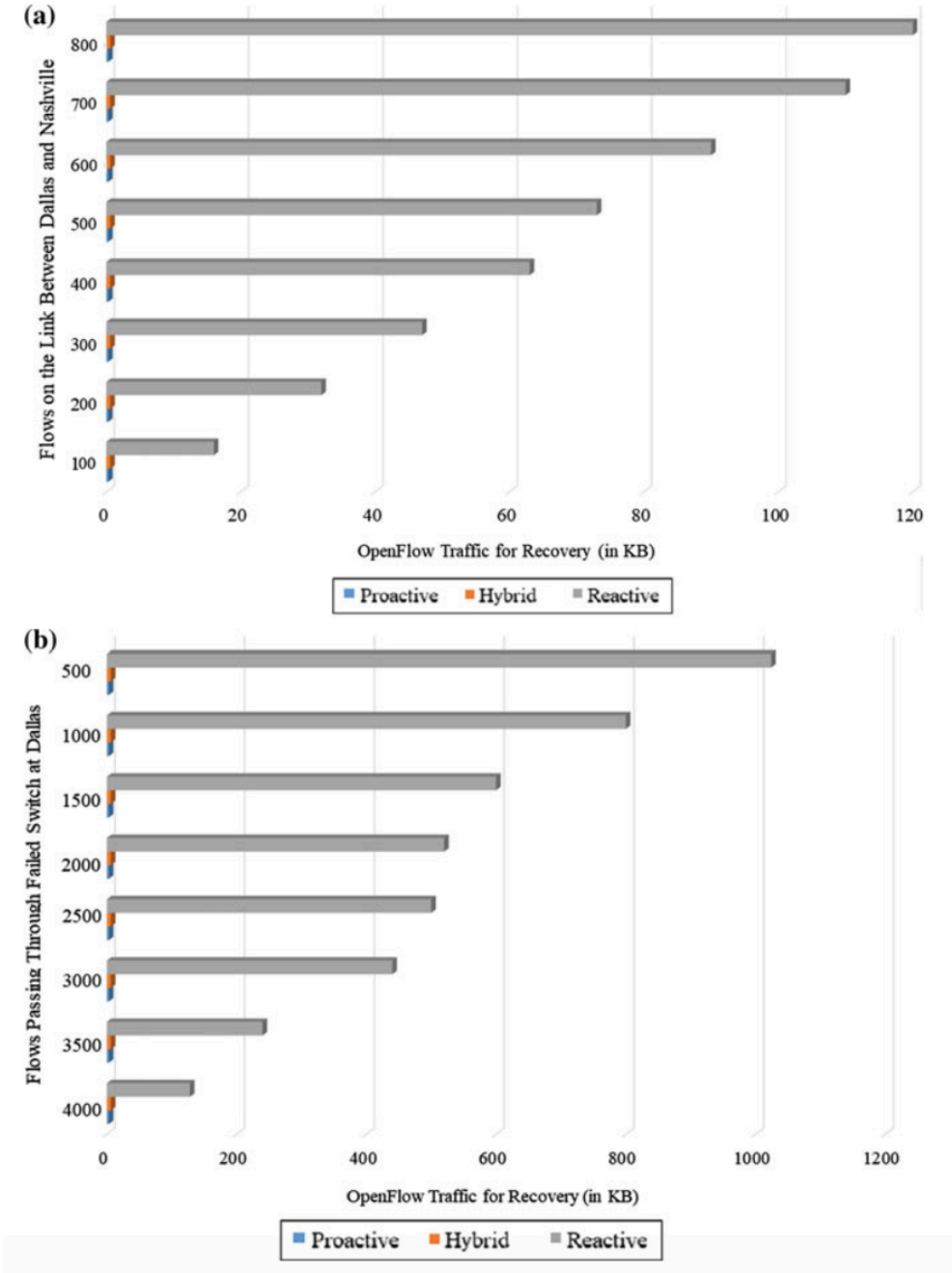
ارزیابی عملکرد

ارزیابی عملکرد بر اساس ساختار شبکه AT&T که پیش‌تر اشاره کردیم انجام شده است. مقایسه عملکرد روش‌های پیشگیرانه، واکنشی و ترکیبی انجام شده است. معیارهای این ارزیابی شامل این موارد هستند:

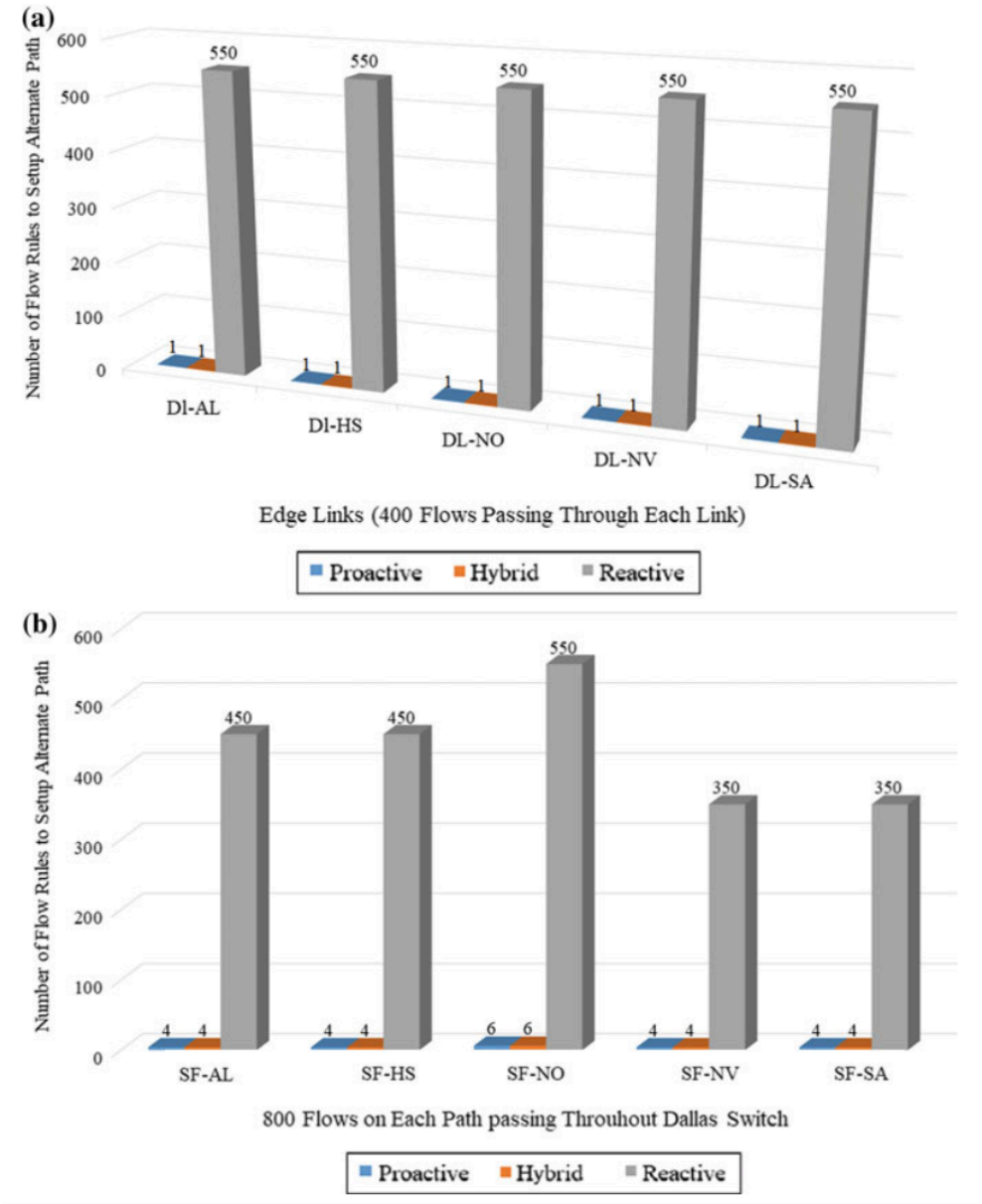
- زمان بازیابی شکست (تصویر- ۱۳): برای روش پیشگیرانه ۲-۳ میلی ثانیه، ترکیبی ۲۰ میلی ثانیه و واکنشی وابسته به تعداد جریان‌های قطع شده
- ترافیک OpenFlow در شبکه (تصویر- ۱۴): بیش از ۹۹ درصد ترافیک در روش پیشگیرانه و ترکیبی کاهش یافته
- تعداد قوانین جریان پشتیبان (تصویر- ۱۵): بیش از ۹۹ درصد قوانین جریان پشتیبان در روش پیشگیرانه و ترکیبی کاهش یافته



تصویر- ۱۳


(a)
Flows on the Link Between Dallas and Nashville
800
700
600
500
400
300
200
100
0
20
40
60
80
100
120
OpenFlow Traffic for Recovery (in KB)
Proactive
Hybrid
Reactive
(b)
Flows Passing Through Failed Switch at Dallas
500
1000
1500
2000
2500
3000
3500
4000
0
200
400
600
800
1000
1200
OpenFlow Traffic for Recovery (in KB)
Proactive
Hybrid
Reactive

تصویر- ۱۴



تصویر- ۱۵

نتیجه‌گیری

بر اساس ارزیابی‌های انجام شده، روش‌های LIm و ICoD (پیشنهادی)، زمان بازیابی‌ای بین ۲ تا ۲۰ میلی ثانیه دارند که به صورت قابل توجهی کمتر از ۵۰ میلی ثانیه سقف زمانی بازیابی در CGN است. هم‌چنین نتایج نشان می‌دهند رویکرد پیشگیرانه و ترکیبی با ۹۹ درصد کاهش حجم ذخیره‌سازی جریان‌ها و ۲۰ میلی ثانیه زمان بازیابی، رویکردهایی مناسب هستند.

نقاط قوت و ضعف مقاله

نقاط قوت این مقاله:

- ارائه مکانیزم و رویکرد عملی قابل پیاده‌سازی

- ارائه شاخص‌های مقایسه کاربردی و نتیجه‌گیری بر اساس شاخص‌ها و کاربرد آن در CGN

نقاط ضعف این مقاله:

- در زمینه خود SDNC بحث SPOF وجود دارد.
- در زمینه لینک‌های کنترلر با سوییچ‌ها، روش بازیابی ویژه‌ای ارایه نشده است.

جمع‌بندی و پیشنهادات برای کارهای آتی

در این مقاله سه روش و مکانیزم جهت روبرو شدن با چالش‌های بازیابی از خرابی مطرح و بررسی شده است:

- CoD
- LIm
- ICoD (پیشنهادی)

هم‌چنین سه رویکرد در این زمینه مطرح شده است:

- واکنشی
- پیشگیرانه
- ترکیبی (پیشنهادی)

در نتیجه رویکرد و روش پیشنهادی با ۲۰ میلی ثانیه زمان بازیابی و ۹۹ درصد کاهش میزان حافظه مورد نیاز ذخیره جریان‌ها، برتری خود را نشان دادند.

در این راه‌کار مواردی در نظر گرفته نشده است و به صورت کار آتی می‌توان در نظر گرفت:

- بالا بردن قابلیت اطمینان با استفاده از چندین SDNC
- شبیه‌سازی در شبکه‌ها با الگوی متفاوت و ترافیک بالاتر

مشخصات دقیق مقاله

Thorat, Pankaj, Sukhdeep Singh, Avinash Bhat, V. Lakshmi Narasimhan, and Gaurav Jain, "SDN-Enabled IoT: Ensuring Reliability in IoT Networks Through Software Defined Networks", In Towards Cognitive IoT Networks, pp. 33-53. Springer, Cham, 2020