نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال دهم، شماره ۱، بهار ۱۳۹۸؛ ص ۳۱-۱۹

ارائه روشی نوین جهت بهبود تحمل‌پذیری خطا در شبکه‌های فرماندهی و کنترل با استفاده از شبکه‌های مبتنی بر نرم‌افزار

محمدرضا پارسائی[1*]، رضا جاویدان[2]، رضا سپه‌وند[3]

۱و۳- دانشجوی دکتری، ۲- دانشیار، دانشگاه صنعتی شیراز

(دریافت: ۹۶/۱۰/۲۶، پذیرش: ۹۶/۱۲/۲۶)

چکیده

مراقبت از فضای کشور و کنترل ترددهای هوایی آن یک ضرورت اجتناب‌ناپذیر است و کنترل توسط رادارهای نصب‌شده در آن منطقه صورت می‌گیرد. اطلاعات دریافتی از رادارهای یک منطقه بایستی به صورت برخط برای رده‌های بالاتر فرماندهی و کنترل ارسال شود تا در مورد آن تصمیم‌گیری شده و فرمان‌ها مقتضی به رده‌های پایین‌تر ارسال شود. این تبادل اطلاعات نیاز به یک بستر ارتباطی مطمئن دارد. ارسال برخط و مطمئن این اطلاعات از چالش‌های شبکه ارتباطی فعلی است و در صورت رخ دادن خطا، درصد فقدان بسته و تأخیر شبکه بالا می‌رود. در این مقاله به منظور کاهش این مشکلات و نیز افزایش تحمل‌پذیری خطا در شبکه‌های فرماندهی و کنترل، از یک مسیر پشتیبان علاوه بر مسیر اصلی استفاده شده است که در صورت بروز خطا در مسیر اصلی، از مسیر پشتیبان استفاده شود. همچنین از شبکه‌های مبتنی بر نرم‌افزار به عنوان یک معماری جدید در حوزه شبکه‌های رایانه‌ای و با هدف فراهم نمودن کیفیت خدمات مطلوب استفاده شده است. در روش پیشنهادی مسئله تحمل‌پذیری خطا به عنوان یک مسئله برنامه‌ریزی خطی، مدل شده است که برای حل آن از الگوریتم ژنتیک در ترکیب با سامانه فازی استفاده کرده‌ایم. این کار نسبت به تغییرات پویا در شبکه واکنش بهینه‌ای ایجاد کرده و عدم قطعیت را در نظر می‌گیرد. ارزیابی‌های انجام‌شده کارایی روش پیشنهادی در افزایش تحمل‌پذیری خطا را نسبت به سایر روش‌های موجود نشان می‌دهند.

کلیدواژه‌ها: فرماندهی و کنترل، تحمل‌پذیری خطا، شبکه‌های مبتنی بر نرم‌افزار، کیفیت خدمات.

Providing a New Method for Improving Fault Tolerance in Command and Control Networks Using Software Defined Networks

M.R. Parsaei[*], R. Javidan, R. Sepahvand

Shiraz University of Technology

(Received: 16/01/2018; Accepted: 17/03/2018)

Abstract

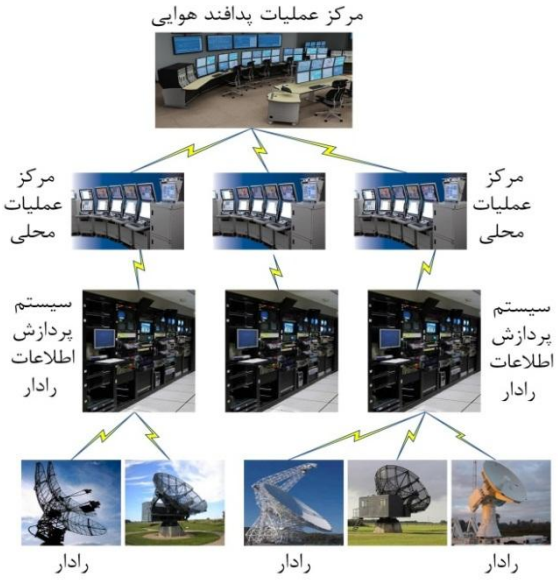
It is an imperative necessity to take care of the country's space and air traffic. Usually radar systems will be used to control and discover possible targets. The received information from a radar system in a specific region must be sent online to the higher levels of command and control centers in order to detect possible threats and make appropriate decisions. This exchange of information requires a reliable communication backbone. However, having an online and secure transceiver communication backbone is still a demanding process. Moreover, errors in the current communication networks will cause an increasing percentage of packet loss and delay which affect the Quality of Service (QoS). In this paper, in order to handle these problems and increase the fault tolerance in command and control networks, a backup path is provided that uses the backup path in case of occurring faults in the main path. In addition, Software Defined networks (SDN) as a new architecture have been used in communication networks to provide desirable QoS. In the proposed method, the fault tolerance problem is modeled as a linear programming problem, which is solved through a combinational method of Genetic Algorithm and Fuzzy System. This solution creates an optimal response to dynamic changes and uncertainty accomplished in the communication network. The results of the performance evaluation showed that the proposed method achieves better fault tolerance compared to existing methods.

Keywords: Commands and Control, Fault Tolerance, Software Defined Networks, Quality of Service

[*] Corresponding Author E-mail: mr.parsaei@sutech.ac.ir

۱. مقدمه

به فرآیند بهره‌گیری از امکانات و اختیارات توسط یک فرمانده در جهت هدایت، رهبری و کنترل نیروهای تحت امر وی، به منظور اجرای مأموریت ابلاغ‌شده، فرماندهی و کنترل گفته می‌شود. شبکه فرماندهی و کنترل پدافند هوایی یک سامانه جامع برای مراقبت از فضای کشور، نظارت و کنترل ترددهای هوایی و مقابله با تهدیدات احتمالی است. در این سامانه، یک شبکه سلسله مراتبی متشکل از مراکز فرماندهی و کنترل منطقه‌ای، پایگاه‌های هوایی، سامانه‌های راداری مرکز فرماندهی و اطلاعات شناسایی است. شکل (۱) ساختار کلی این شبکه را نشان می‌دهد.



شکل ۱. ساختار کلی شبکه فرماندهی و کنترل

در پایین‌ترین سطح از سلسله مراتب سامانه، سنسورهای راداری قرار دارند که شامل رادارهای مختلف، مانند رادارهای جستجو و هشدار اولیه، رادارهای کنترل شکاری و رادارهای هواشناسی هستند. اطلاعات اهداف شناسایی‌شده توسط رادارهای مختلف، در مراکز فرماندهی و کنترل محلی جمع‌آوری شده و از طریق شبکه به مراکز پردازش اطلاعات رادارها[1] که سطح دوم شبکه فرماندهی و کنترل است، منتقل می‌شوند.

از آنجایی که اطلاعات ارسالی توسط رادارها با هم، همپوشانی دارند، قبل از ارسال به مراکز عملیات محلی[2] در مراکز پردازش اطلاعات رادارها، تجمیع و تلفیق می‌شوند. این مراکز داده‌های خام را از رادارهای مختلف دریافت کرده و عملیات پردازش ثانویه مانند کلاسه بندی، تلفیق داده و اولویت‌بندی را روی داده‌های تجمیع شده انجام داده و برای مراکز عملیات محلی ارسال می‌کند. اطلاعات رادارهای هواشناسی و رادارهای فرودگاهی، نیز در این مرکز دریافت می‌شود.

در لایه سوم این ساختار، مراکز عملیات محلی قرار دارند. این مرکز مسئولیت فرماندهی و کنترل یک منطقه را به عهده دارد. در این مرکز اطلاعات شناسایی از مراکز مختلف پردازش اطلاعات رادار دریافت می‌شود. سپس توسط سامانه‌های تصمیم یار هوشمند و فرماندهان تحلیل‌شده و تهدیدها شناسایی و اولویت‌بندی می‌شوند و مسئولیت مقابله با این تهدیدات، به مراکز مقابله با تهدیدها و یا پایگاه‌های هوایی واگذار می‌شود.

در بالاترین سطح از این شبکه، مرکز عملیات پدافند هوایی[3] قرار دارد. این سطح، عملیات پدافند هوایی سامانه فرماندهی و کنترل یکپارچه کل کشور است که مدیریت فضای کل کشور را از نظر نمایش یکپارچه اطلاعات دریافتی از کلیه مراکز عملیات منطقه‌ای و هماهنگی رزمی کلیه نیروهای نظامی را به عهده دارد. این مرکز، اطلاعات دریافتی از مراکز عملیات محلی را دریافت کرده و پس از بررسی، تصمیمات لازم را به آن‌ها ابلاغ می‌نماید.

برای انجام مأموریت در شبکه فرماندهی و کنترل، حفظ ویژگی ارتباطات امن دوطرفه با قابلیت اطمینان بالا و بر خط حیاتی است. مثلاً اگر پرنده ناشناسی وارد فضای کشور شود، این پرنده توسط یک یا چند رادار شناسایی می‌شود، مراکز پردازش اطلاعات رادار، این اطلاعات را دریافت کرده و نتیجه پردازش را بایستی با سرعت بالا و بدون اتلاف وقت به لایه‌های بالاتر ارسال کرده تا فرماندهان در مورد آن تصمیم‌گیری کرده و در صورت لزوم به پایگاه هوایی و یا مرکز درگیری واگذار شود. برای اثربخشی فرماندهی و کنترل بایستی ارتباطات دوطرفه و مطمئن، بین نودهای مختلف شبکه برقرار باشد. نودهای شبکه فرماندهی و کنترل بایستی به نودهای بالاتر، پایین تر و نیز در برخی موارد به نودهای هم رده متصل باشند. اطلاعات مبادله شده شامل گزارش‌های دریافتی از سنسورها (بسته حاوی اطلاعات اهداف کشف‌شده از رادارها) و نودهای پایین تر(اطلاعات پردازش‌شده در مراکز پردازش رادار به مراکز عملیات محلی ارسال می‌شود) و یا فرمان‌های دریافتی از نودهای بالاتر است [۱].

نودهای شبکه فرماندهی و کنترل سامانه‌ها از طریق شبکه فیبر نوری، تجهیزات بی‌سیم مایکروویو به هم متصل می‌شوند. قابلیت اطمینان و عملکرد بدون نقص و تداوم کاری در شرایط حساس عملیاتی از ویژگی‌های مهمی است که بایستی در طراحی شبکه‌های کنترل و فرماندهی در نظر گرفته شود. طراحی باید به گونه‌ای انجام شود که با خرابی قسمتی از تجهیزات رایانه‌ای و مخابراتی، عملکرد کل شبکه مختل نشود. در صورت قطع ارتباط

[1] Radar Information Processing System
[2] Sector Operation Center
[3] Air Defense Operations Center

بین نودهای این شبکه، شبکه ارتباطات خود را جابجا کرده و به صورت خودکار مسیر ارتباط دیگری جایگزین شود. ارسال برخط و با قابلیت اطمینان بالا برای برخی از بسته‌های اطلاعاتی(مثلاً بسته‌های زنجیره آتش) بسیار حیاتی بوده و به همین دلیل فراهم نمودن شبکه‌های ارتباطی با در نظر گرفتن نکات فنی مناسب لازم است. شبکه باید قابلیت پیگیری انتقال اطلاعات را دارا بوده و توانایی اتصال به شبکه‌های دیگر را نیز داشته باشد [۲].

پیچیدگی و پویایی شبکه‌های رایانه‌ای، پیکربندی و مدیریت آن‌ها را امری چالش‌برانگیز ساخته است. اپراتورهای شبکه مسئول پیکربندی شبکه به منظور اعمال سیاست‌های متنوع سطح بالا هستند. از آنجا که پیاده‌سازی این سیاست‌های سطح بالا تنها در قالب یک پیکربندی توزیع‌شده و سطح پایین انجام می‌پذیرد، پیکربندی شبکه به کاری طاقت‌فرسا بدل گشته است [۳]. شبکه‌های مبتنی بر نرم‌افزار امید دستیابی به روش‌های مطلوب تری جهت انجام پیکربندی و مدیریت شبکه به وجود آورده‌اند. در این الگوی جدید از شبکه، سطح کنترلی (که وظیفه محاسبه مسیر داده‌ها را بر عهده دارد) از سطح داده (که مسئول انتقال داده است) جدا شده و در یک لایه جداگانه مجازی به نام کنترل‌کننده قرار می‌گیرد. این جداسازی منطق کنترل از مسیریاب‌ها و سوئیچ‌ها و تعبیه آن در یک کنترل‌کننده متمرکز، که در واقع مغز متفکر شبکه محسوب می‌شود، امکان اعمال سیاست‌های مدیریتی، پیکربندی، پیکربندی مجدد شبکه و نیز روند تکامل شبکه‌های رایانه‌ای را آسان‌تر می‌نماید [۷-۴].

در این مقاله از شبکه‌های مبتنی بر نرم‌افزار به عنوان یک مفهوم جدید در شبکه‌های رایانه‌ای استفاده شده است. برای مقابله با خطاهایی که منجر به حذف لینک‌ها می‌گردد، قبل از رخداد خطا دو مسیر مجزای اصلی و پشتیبان در نظر گرفته می‌شود. در صورت بروز خطا در مسیر اصلی، به سرعت گره‌های میانی از مسیر پشتیبان از پیش تعیین‌شده، اقدام به ارسال ترافیک می‌کنند، تا وقفه‌ای در ارسال اطلاعات به وجود نیاید. با توجه به اینکه در یک شبکه رایانه‌ای تعداد زیادی فرستنده و گیرنده با الگوهای ترافیکی متفاوتی وجود دارند، تأخیر و پهنای باند موجود در هر لینک ممکن است به طور پویا تغییر کند و اختصاص دادن هزینه مناسب به هر لینک سخت باشد و در نتیجه عدم قطعیت را بالا می‌برد. جهت رفع عدم قطعیت، از سامانه فازی برای اختصاص دادن هزینه مناسب به هر لینک بر اساس تأخیر و پهنای باند موجود، استفاده شده است. سپس مسئله به عنوان یک مسئله برنامه‌ریزی خطی مدل شده است که تابع هدف در این مدل، کمینه کردن هزینه مسیر از مبدأ تا مقصد است. همان طور که می‌دانیم مسئله یافتن کوتاه‌ترین مسیر، یک مسئله بهینه‌سازی است که حل آن در فضای بزرگ بسیار دشوار و زمان‌بر است. در این مقاله جهت محاسبه بهینه‌ترین مسیر از الگوریتم ژنتیک استفاده شده است. مسیرهای پشتیبان به گونه‌ای انتخاب شده‌اند که به سرعت جایگزین مسیر اصلی شوند و امکان وقوع خطا در آن‌ها نزدیک به صفر باشد.

سایر بخش‌های این مقاله به این شرح است: در بخش ۲، تحمل‌پذیری خطا و روش‌های آن مطرح می‌شود. در بخش ۳، کارهای ارائه‌شده قبلی مرتبط با مقاله ارائه می‌گردد. در بخش ۴، روش پیشنهادی برای مقابله با خطاهای پیش‌آمده و تضمین کیفیت خدمات، تشریح خواهد شد. شبیه‌سازی و ارزیابی کارایی در بخش ۵ مورد بحث قرار خواهد گرفت. بخش ۶ نیز به نتیجه‌گیری در رابطه با روش پیشنهادی اختصاص خواهد یافت.

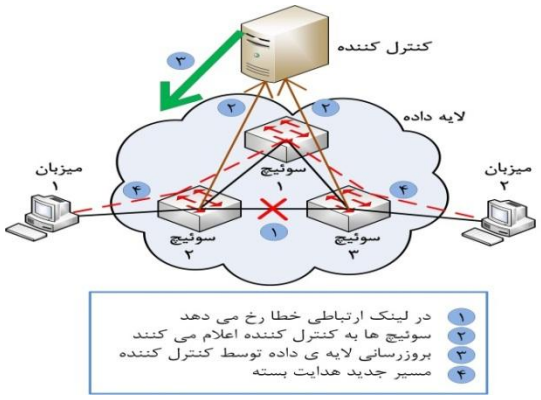
۲. تحمل‌پذیری خطا

تحمل‌پذیری خطا توانایی یک سامانه ارتباطی در مواجهه با خطاهای حاصل از رخدادها است به گونه‌ای که سایر خدمات‌های استفاده‌کننده از سامانه دچار خطا نشوند [۸]. فرایند مدیریت خطا شامل دو مرحله تشخیص و ترمیم خطا است. در شبکه‌های سنتی عموماً مدیریت خطا وابسته به پروتکل‌های توزیع‌شده مسیریابی مانند OSPF[1] است که خود مشکلات متفاوتی را به دنبال دارد [۹]. در مدیریت خطا فاکتورهای متفاوتی از جمله مدت زمان تشخیص خطا و ترمیم خطا (زمانی است که طول می‌کشد تا شبکه بتواند مسیر جایگزین را محاسبه و آن را به گره‌های درگیر اعلام نماید) می‌توانند اثربخشی را تحت تأثیر قرار داده و باعث از بین رفتن بسته‌های داده شوند. در نتیجه مجموع این دو زمان به شدت بر کارایی شبکه تأثیرگذار است. همان طور که گفته شد در شبکه‌های سنتی به دلیل عدم وجود دید متمرکز برای تشخیص خطا بایستی از پروتکل‌های توزیع‌شده مانند OSPF استفاده کرد که این امر چالش‌هایی مانند رخ دادن چندین اعلام خطا برای یک خرابی که در صورت عدم مدیریت می‌تواند منجر به محاسبه چند باره راه‌کار برای یک خطا شود یا تشخیص دیرهنگام دستگاه‌های میانی، در پی دارد [۱۰] و برای رفع این مشکلات از شبکه‌های مبتنی بر نرم‌افزار که دید کلی نسبت به شبکه دارد استفاده شده است. در ادامه سازوکارهای محافظت و بازیابی در شبکه‌های سنتی و شبکه‌های مبتنی بر نرم‌افزار تشریح می‌شود:

رویکرد بازیابی (مقابله با خطا پس از بروز آن): در این رویکرد در شبکه‌های سنتی هیچ مسیر پشتیبانی از قبل مشخص نمی‌شود و پس از تشخیص خطا در مسیرهای ارتباطی اقدام به

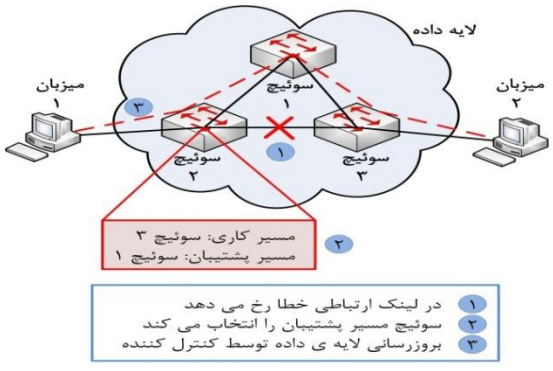
[1] Open Shortest Path First

محاسبه مسیر جایگزین و اعلام آن به گره‌های درگیر می‌کند. همچنین در شبکه‌های مبتنی بر نرم‌افزار سوئیچ پس از تشخیص خطا ابتدا به کنترل‌کننده خطا را اعلام می‌کند. کنترل‌کننده به دلیل دید جامع نسبت به کل شبکه، مسیرهای ارتباطی که دچار خطا شده‌اند را تشخیص می‌دهد. سپس مسیرهایی که این خطا بر آن‌ها اثرگذار بوده است را شناسایی و مسیر جایگزین را محاسبه می‌کند. پس از این مرحله، کنترل‌کننده سوئیچ‌های شبکه را به‌روزرسانی می‌کند [۸]. در شکل (۲) مراحل این روش نمایش داده شده است:



شکل ۲. سازوکار بازیابی در SDN

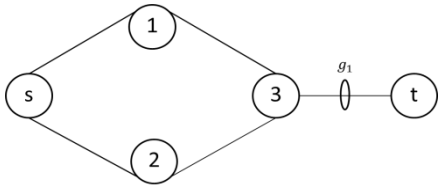
رویکرد محافظت (مقابله با خطا قبل از بروز آن): در شبکه‌هایی مانند کنترل و فرماندهی که ارائه خدمات نباید مختل شود، رویکردی مناسب است. در این رویکرد در شبکه‌های سنتی دو مسیر مجزای اصلی و پشتیبان قبل از بروز خطا محاسبه می‌شوند. در صورت بروز خطا در مسیر اصلی، به سرعت گره‌های میانی از مسیر از پیش تعیین‌شده، اقدام به ارسال ترافیک می‌کنند، تا وقفه‌ای در ارسال اطلاعات به وجود نیاید. در شبکه‌های مبتنی بر نرم‌افزار کنترل‌کننده ابتدا دو مسیر کاری و پشتیبان را محاسبه می‌کند و در اختیار سوئیچ‌ها قرار می‌دهد. سوئیچ پس از تشخیص خطا بدون اعلام به کنترل‌کننده خودکار از مسیر پشتیبان برای ارسال بسته‌ها استفاده می‌کند [۸]. در شکل (۳) مراحل این روش نمایش داده شده است:



شکل ۳. سازوکار محافظت در SDN

SRLG[1] گروهی از لینک‌های شبکه هستند که در منابع فیزیکی با یکدیگر مشترک هستند. بروز خطا در هر یک از اعضای این مجموعه به معنای بروز خطا در همه لینک‌های ارتباطی یک SRLG است. ایجاد ساختارهای شبکه که قابلیت تعامل با خطا را داشته باشد و شفافیت ارائه خدمات به گونه‌ای باشد که کاربران نهایی متوجه این خطا نشوند و بر پارامترهای کیفیت خدمات مانند تأخیر و فقدان بسته نیز کمترین اثر را داشته باشد، همواره یکی از دغدغه‌های ارائه‌دهندگان سرویس است [۱۱].

در این مقاله از مفهوم SRLG و تغییر ماهوی و استفاده از آن در شبکه‌های مبتنی بر نرم‌افزار سعی در بهبود تحمل‌پذیری خطا در شبکه‌های مبتنی بر نرم‌افزار داشته‌ایم. در انتخاب مسیرهای اصلی و پشتیبانی در صورتی که دو مسیر هیچ SRLG مشترکی نداشته باشند، دو مسیر نسبت به هم SRLG مجزای کامل هستند. محاسبه مسیر پشتیبان درحالی‌که SRLG مجزا کامل باشد، همیشه امکان‌پذیر نیست. در این شرایط مسیرهایی محاسبه می‌شوند که کمترین SRLG مشترک را با مسیر اصلی داشته باشند و به آن SRLG مجزای بیشینه گفته می‌شود. به عنوان مثال همان طور که در شکل (۴) مشاهده می‌شود یال g1 یک یال بحرانی است و در همه مسیرهای وارده و خارجه به راس t بایستی حضور داشته باشد. در این شکل امکان یافتن جفت مسیر اصلی و پشتیبان کاملاً مجزا فراهم نیست.



شکل ۴. عدم امکان یافتن مسیرهای اصلی و پشتیبان مجزا

۳. پیشینه تحقیق

با توجه به اینکه تا کنون هیچ مقاله‌ای در زمینه تحمل‌پذیری خطای فرماندهی و کنترل در شبکه‌های مبتنی بر نرم‌افزار ارائه نشده است و از طرفی روش پیشنهادی جهت تحمل‌پذیری خطای فرماندهی و کنترل در شبکه‌های مبتنی بر نرم‌افزار اولین روش در این حوزه است، لذا تنها تعدادی مقاله که مربوط به برقراری کیفیت سرویس در شبکه‌های سنتی (شبکه‌های کنونی) و مدیریت شبکه‌های مبتنی بر نرم‌افزار ارائه‌شده، در این بخش مرور شده است.

بیادی و همکاران[۱۲]، طرحی را برای بقاپذیری و عملکرد بدون نقص شبکه فرماندهی و کنترل، در لحظات حساس عملیات ارائه کرده‌اند. در این طرح علاوه بر ارتباطات معمولی بین نودها،

[1] Shared Risk Link Group

یک لینک رادیوئی برای پشتیبانی از ارتباطات بین هر دو نود، برقرار می‌شود. در طرح پیشنهادی آن‌ها، هر نود به تمامی نودهای لایه بالاتر، پایین‌تر و هم رده متصل می‌شود. با استفاده از نظریه گراف با قطع یک لینک ارتباطی، لینک دیگر جایگزین شده و کارایی شبکه حفظ می‌گردد.

فدائیان و همکاران [۱۳]، برای استفاده از قابلیت خودمختاری یک زیرساخت ارتباطی مبتنی بر تور ارائه کردند. با توجه به اینکه یکی از انتظارات از سامانه‌های فرماندهی و کنترل، ایجاد ساختار برای تبادل داده در محیطی پویا، امن و با قابلیت اطمینان بالا است، زیرساخت گرید را دارای انطباق بالا با انتظارات مطرح‌شده دانسته و آن را به عنوان زیرساخت فرماندهی و کنترل ارائه کرده‌اند. مهم‌ترین چالش مطرح‌شده توسط آن‌ها این است که با توجه به اینکه یک کار به قسمت‌های مختلف شکسته شده و هر ریز کار در یک قسمت از گرید اجرا می‌شود، اطمینان از اجرای صحیح ریزکارها به چه صورت انجام شود. برای این کار یک مدل گرید دانش خودمختار ارائه شده است که دانش مشترک راجع به کل وضعیت سامانه را فراهم می‌کند.

کاشفی و همکاران [۱۴] با توجه به اهمیت قابلیت بقا پذیری، مداومت کاری و عملکرد بدون نقص در شرایط حساس عملیاتی برای شبکه‌های فرماندهی و کنترل، طرحی را ارائه کردند که گره‌های شبکه از وضعیت دیگر گره‌ها مطلع شده و در هنگام خرابی گره‌ها، به صورت خودکار ارتباط دیگری جایگزین می‌شود و باعث تحمل‌پذیری بالاتر شبکه در برابر خطا می‌شود. در این طرح، تعداد اجزاء آتشبار، فاصله مجاز آن‌ها از یکدیگر در ساختار شبکه و نحوه چیدمان آن در حالت عادی و بحرانی با توجه به معیارهای حداکثر کارایی، عدم ایجاد شکاف عملیاتی و از لحاظ هزینه‌های ساخت اجزاء مشخص می‌گردد.

کیم و همکاران [۱۵] یک چارچوبی به نام پروسرا[1] برای مدیریت و کنترل شبکه ارائه دادند که با تعریف یک واسط شمالی، امکان مشخص نمودن و پیاده‌سازی سیاست‌های واکنشی (واکنش به رویدادهای شبکه) را فراهم می‌آورد. این سیاست‌ها با زبان برنامه‌نویسی تابعی[2]، واکنشی[3]، توسط اپراتورها نوشته می‌شوند و سپس به یک مجموعه قوانین هدایت بسته‌ها، که قابل‌استفاده بر روی زیرساخت شبکه مبتنی بر نرم‌افزار است، ترجمه می‌شوند. به عبارت دیگر پروسرا، یک پل ارتباطی میان سیاست‌های سطح بالا و مبتنی بر رویداد[4] با پیکربندی سطح پایین شبکه خواهد بود.

ونگ [۱۶] با استفاده از خصوصیات پروتکل اترنت در لایه فیزیکی روشی برای بررسی سلامت لینک در شبکه‌های سنتی معرفی می‌کند. در روش معرفی‌شده، دستگاه برای بررسی برقراری لینک در صورتی که هیچ ارتباطی برقرار نباشد در بازه ۸±۱۶ میلی‌ثانیه بسته‌های heartbeats را ارسال می‌کند، در صورتی که در بازه ۵۰-۱۵۰ میلی‌ثانیه پاسخی دریافت نکند، قطعی ارتباط را تشخیص می‌دهد.

شارما [۱۷] از سازوکار BFD[5] برای تشخیص خطا استفاده کرده است. در این روش بین هر جفت گره انتهایی یک نشست برقرار می‌شود. گره‌ها در بازه‌های زمانی اقدام به ارسال بسته‌های کنترلی می‌کنند. در صورت عدم دریافت بسته‌ها، خطا در مسیر تشخیص داده می‌شود. این روش در صورتی که برای یک مسیر با چندین لینک استفاده شود توانایی تشخیص مکان یک یا چندین خطا را ندارد و تنها می‌تواند اعلام نماید که مسیر دچار خطا شده است. به‌ازاء هر سوئیچ در بین مسیر در هر بازه زمانی یک پیام کنترلی BFD ارسال می‌شود. برای تشخیص خطا از کانال ارسال داده‌ها استفاده می‌نماید. هرچه طول مسیر نظارت بیشتر باشد مدت زمان تشخیص خطا نیز بیشتر خواهد بود.

ون [۱۸] از سازوکار BFD برای هر لینک استفاده کرده است. در صورتی که تعداد گره‌ها از مرتبه O(n) باشد تعداد نشست‌ها در هر گره برای همه مسیرها از مرتبه $O(n^2)$ خواهد بود و سرباز محاسباتی و ارتباطی زیادی را به همراه خواهد داشت. در روش پیشنهادی وقتی نشستی برای لینک‌ها بر قرار شود، در این صورت هر گره نیاز به نگه‌داری O(n) نشست خواهد داشت. با توجه به محدود شدن طول مسیر نظارت، زمان RTT[6] نیز کاهش پیدا خواهد کرد و با ترکیب با روش LOS[7]، زمان تشخیص خطا به زیر ۵۰ میلی‌ثانیه می‌رسد. یک بسته کنترلی BFD، حداکثر ۲۴ بایت برای احراز هویت، ۸ بایت سرایند بسته‌های UDP، 20 بایت IPv4 و ۳۸ بایت سرایند اترنت خواهد داشت. که مجموعاً ۹۰ بایت که در هر ۱ میلی ثانیه منتقل می شوند. این میزان داده سرباری معادل ۰/۰۶۷ و ۰/۰۰۶۷ درصد به ترتیب در لینک های ۱ و ۱۰ Gbps ایجاد می‌کند.

شبکه‌های کنونی دارای پیچیدگی زیادی هستند و مدیریت آن‌ها در کشور ایران برای فرماندهی و کنترل کار دشواری است. یکی از دلایل این امر در هم تنیدگی سطوح کنترل و داده با یکدیگر است. یک دلیل عمده دیگر، آن است که هر تولیدکننده دستگاه‌های شبکه، واسط‌های مدیریتی و پیکربندی انحصاری خودش را ارائه می‌دهد، که منجر به چرخه طولانی در

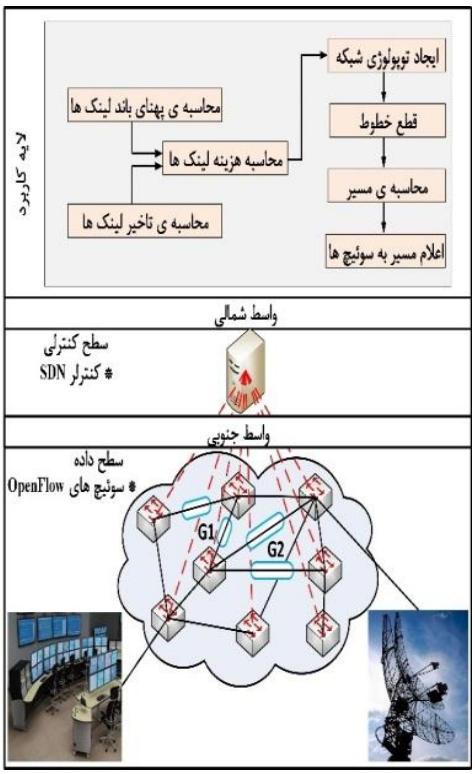
[1] Procera
[2] Functional
[3] Reactive
[4] Event-Driven

[5] Bidirectional Forwarding Detection
[6] Round Trip Time
[7] Loss Of Signal

به‌روزرسانی این دستگاه‌ها می‌شود. این مالکیت انحصاری زیرساخت‌های شبکه، محدودیت‌های سنگینی بر هر گونه تغییر و نوآوری اعمال نموده است. شبکه‌های مبتنی بر نرم‌افزار فرصتی برای حل این مشکلات به وجود آورده‌اند. در شبکه‌های مبتنی بر نرم‌افزار، تمام اجزای سطح کنترلی شبکه در یک موجودیت به نام کنترل‌کننده یا همان سیستم‌عامل شبکه، عرضه می‌شوند، درحالی‌که اجزای سطح داده به دستگاه‌های فاقد اختیار، اما قابل برنامه‌نویسی و با کارایی فوق‌العاده در پیشبرد داده تبدیل شده‌اند و در این مقاله نیز برای پیاده‌سازی یک زیرساخت موفق جهت فرماندهی و کنترل از شبکه‌های مبتنی بر نرم‌افزار استفاده گردیده است.

۴. معماری روش پیشنهادی

همان‌گونه که در بخش‌های قبلی اشاره شد، پیاده‌سازی یک شبکه فرماندهی کنترل که مبتنی بر زیرساخت شبکه کنونی باشد، نمی‌تواند تضمین‌کننده پارامترهایی چون میزان تأخیر و فقدان بسته باشد [۲]. در مقابل، می‌توان از شبکه‌های مبتنی بر نرم‌افزار به دلیل متمرکز شدن کنترل شبکه، به عنوان یک شبکه بستر در این ساختار استفاده نمود. طرح پیشنهادی شبکه فرماندهی کنترل با بهره‌گیری از شبکه‌های مبتنی بر نرم‌افزار به عنوان یک شبکه بستر در شکل (۵) نمایش داده شده است:



شکل ۵. طرح کلی سامانه پیشنهادی

در این شکل کاربران مختلف اقدام به تبادل داده می‌کنند و شبکه زیرساخت مبتنی بر نرم‌افزار بایستی بتواند کمترین میزان تأخیر و از دست دادن بسته‌ها را فراهم نماید. در این شبکه خطوط ارتباطی به صورت ایستا دارای ریسک‌های مشترک هستند. که در صورت بروز خطا در یک گروه دارای ریسک مشترک SRLG، همه لینک‌های آن گروه با خطا مواجه می‌شوند. در تحمل‌پذیری خطا با استفاده از تعاریف SRLG، در مسیرهای اصلی و پشتیبان، خطوط ارتباطی که دارای یک ریسک مشترک هستند، نباید انتخاب شوند. در شکل (۵) دو گروه SRLG با نام‌های G1 و G2 وجود دارند. روش انتخابی برای مدیریت خطا، به این صورت است که در آن مسیرهای اصلی و پشتیبان توسط کنترل‌کننده و با استفاده از الگوریتم ژنتیک قبل از وقوع خطا محاسبه می‌شوند. در روش پیشنهادی از ۷ ماژول برای پیاده‌سازی مدیریت خطا و تعامل سوئیچ‌ها با کنترل‌کننده استفاده شده است. این ماژول‌ها عبارت‌اند از:

ماژول محاسبه پهنای باند مصرفی لینک‌ها: این ماژول به صورت پویا پهنای باند موجود هر لینک را در شبکه محاسبه می‌کند و آن‌ها را در ماتریسی با نام پهنای باند موجود ذخیره می‌کند.

ماژول محاسبه تأخیر لینک‌ها: این ماژول به طور پویا تأخیر هر لینک را در شبکه محاسبه می‌کند و آن‌ها را در ماتریسی به نام تأخیر لینک‌ها ذخیره می‌کند.

ماژول محاسبه هزینه لینک‌ها: ، این ماژول هزینه را برای تمامی لینک‌ها با توجه به ماتریس پهنای باند موجود و ماتریس تأخیر لینک‌ها، با استفاده از سامانه فازی پیشنهادی در این مقاله (که توضیحات آن در بخش ۱-۴ آمده است) محاسبه می‌کند و این هزینه‌ها را در ماتریسی به نام هزینه لینک‌ها ذخیره می‌کند.

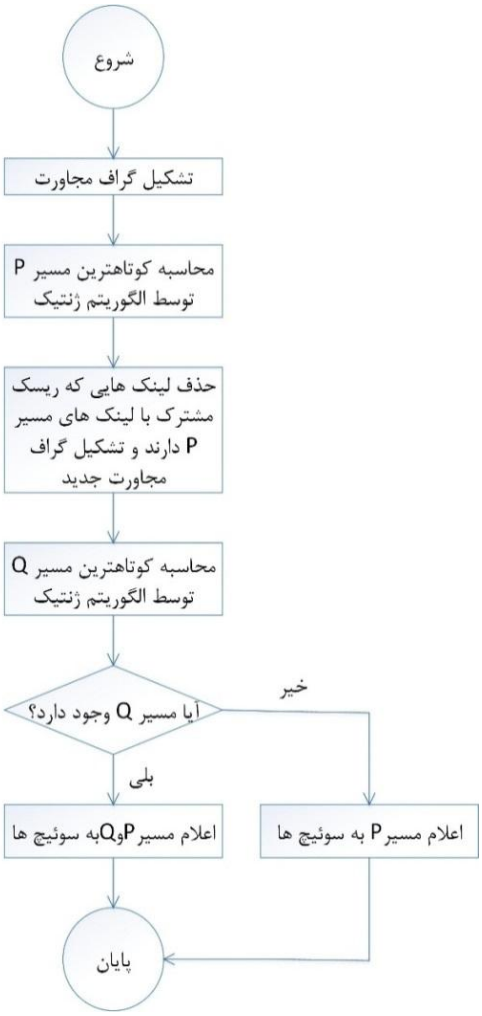
ماژول ایجاد توپولوژی شبکه: این ماژول پس از محاسبه هزینه همه لینک‌ها، وظیفه ایجاد ماتریس مجاورت برای ارائه به ماژول محاسبه مسیر را بر عهده دارد.

ماژول قطع لینک تصادفی: این ماژول وظیفه قطع کردن تصادفی یک لینک از گروه لینک‌ها با ریسک مشترک را بر عهده دارد.

ماژول محاسبه مسیر (مسیرهای اصلی و پشتیبان): با استفاده از ماتریس هزینه لینک‌ها (که در ماژول محاسبه هزینه لینک‌ها توسط سامانه فازی محاسبه گردید) و الگوریتم ژنتیک (که توضیحات آن در بخش ۲-۴ آمده است)، سعی می‌کند جفت مسیر بهینه اصلی و پشتیبان را پیدا کند.

ماژول اعلام مسیر: مسیر حاصل از اجرای الگوریتم را به سوئیچ‌های مربوطه اعلام می‌کند.

همه این ماژول‌ها به صورت پویا و به ترتیب پشت سر هم اجرا شده و باعث می‌شوند که بسته‌های ویدئوی ارسال‌شده تا حد امکان از بهینه‌ترین مسیر انتقال داده شوند. در روش پیشنهادی، از ایده الگوریتم سوربال برای محاسبه مسیرهای SRLG مجزا استفاده شده است. همان طور که گفته شد، محاسبه دو مسیر کاملاً مجزا همیشه امکان‌پذیر نیست و بنابراین باید مسیرهایی را انتخاب کرد که کمترین SRLG مشترک را با هم داشته باشند. جزئیات الگوریتم پیشنهادی در شکل (۶) آمده است.



شکل ۶. فلوچارت الگوریتم سوربال پیشنهادی

همان‌طور که در شکل (۶) نشان داده شده است، ایده روش پیشنهادی استفاده از الگوریتم ژنتیک برای محاسبه هر دو مسیر اصلی P و پشتیبان Q است. برای محاسبه مسیر پشتیبان لینک‌هایی که دارای ریسک مشترک با یکی از لینک‌های مسیر P باشند در گراف مجاورت جدید حذف می‌شوند و سپس مسیر جدید محاسبه می‌گردد. در صورتی که نتواند مسیر دوم را محاسبه کند، تنها یک مسیر محاسبه می‌شود و الگوریتم از روش محافظت خارج می‌شود.

۱-۴. فرموله کردن مسئله

در این روش با مدل‌سازی مسئله به عنوان یک مسئله برنامه‌ریزی خطی، مسیرهای پشتیبان به گونه‌ای انتخاب شده‌اند که به سرعت جایگزین مسیر اصلی شوند و امکان وقوع خطا در آن‌ها نزدیک به صفر باشد. همچنین تابع هدف در این مدل، کمینه کردن هزینه مسیر از مبدا تا مقصد است. مدل ریاضی برنامه‌ریزی خطی استفاده‌شده در این مقاله برای یافتن جفت مسیرهای اصلی و پشتیبان که SRLG مجزا باشند در ادامه آمده است:

$$\text{Min} \quad \sum_k \sum_{ij} d_{ij} x_{ij}^k \qquad (۱)$$

$$\sum_{j:(i.j)\in E} x_{ij}^k - \sum_{j:(i.j)\in E} x_{ij}^k = 1.$$

$$\forall K \in M.\ \text{if}\ i = p \qquad (۲)$$

$$\sum_{j:(i.j)\in E} x_{ij}^k - \sum_{j:(j.i)\in E} x_{ji}^k = 0.$$

$$\forall K \in M.\ i(\neq p.q) \in V \qquad (۳)$$

$$x_{ij}^k + x_{ij}^{k'} \leq 1.\ \forall k.k' \in M.(i.j)\ \in E \qquad (۴)$$

$$x_{ij}^k + x_{i'j'}^{k'} + S(i.j.g) + S(i'.j'.g) \leq 3 \qquad (۵)$$

$$\forall k.k'.(k \neq k') \in M.(i.j).(i'.j').$$

$$\big((i.j) \neq (i'.j')\big) \in E \qquad (۶)$$

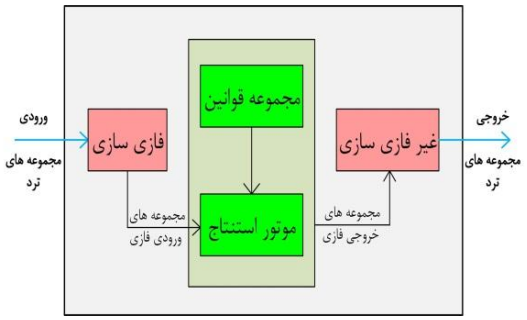
$$x_{ij}^k = \{0.1\}.\ \forall k \in M.(i.j) \in E \qquad (۷)$$

همان‌طور که در فرمول (۱) نشان داده شده است، هدف این مسئله یافتن کم هزینه‌ترین k مسیر است. در این معادله d هزینه یال از راس i به j و x متغیر تصمیم وجود یا عدم وجود یال است. در سایر فرمول‌ها محدودیت‌های حل مسئله بیان شده‌اند. فرمول (۲) بیانگر عدم وجود دور در مسیر انتخابی است. فرمول (۳) مشخص‌کننده مبدأ p و مقصد q است به طوری که این دو متمایز باشند. در فرمول (۴) عدم انتخاب یک یال در دو مسیر بیان شده است. برای آن‌که مسیرهای انتخابی SRLG مجزا باشند بایستی یال‌هایی با یک ریسک مشترک در دو مسیر انتخاب نشوند و این محدودیت در فرمول (۵) بیان شده است. فرمول (۶) مقادیر متغیر تصمیم مدل را نمایش می‌دهد. یک بودن مقدار برای x_{ij}^k بیانگر وجود یال از راس i به j در مسیر شماره k است و مقدار صفر بیانگر عدم وجود یال در مسیر یاد شده است. این نوع متغیر تصمیم مسئله را به یک مدل برنامه‌ریزی خطی صحیح تبدیل می‌نماید. همچنین محدودیت دوم این فرمول بیان می‌کند که یال‌های انتخابی حتماً بایستی وجود داشته باشند. محاسبه هزینه هر لینک توسط سامانه فازی انجام می‌شود که در بخش بعد توضیحات آن آمده است.

۲-۴. سامانه فازی

با توجه به اینکه در یک شبکه رایانه‌ای تعداد زیادی فرستنده و گیرنده با الگوهای ترافیکی متفاوتی وجود دارند، تأخیر و پهنای باند موجود هر لینک ممکن است به طور پویا تغییر کند و اختصاص دادن هزینه مناسب به هر لینک سخت باشد و در نتیجه عدم قطعیت را بالا می‌برد. جهت رفع عدم قطعیت، برای اختصاص دادن هزینه مناسب به هر لینک بر اساس تأخیر و پهنای باند موجود، از سامانه فازی استفاده شده است.

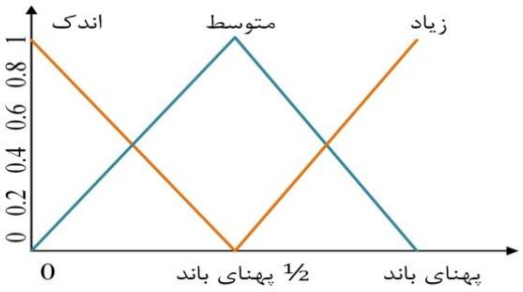
منطق فازی برای اولین بار توسط زاده [۱۹-۲۳] معرفی گردید و شامل سه مرحله است: ۱- فازی ساز[1] (ورودی غیر فازی را به متغیر زبانی تبدیل می‌کند). ۲- موتور استنتاج[2] (با استفاده از قوانین فازی اگر-آنگاه، ورودی فازی را به خروجی فازی تبدیل می‌کند). ۳- غیر فازی ساز[3] (مقادیر فازی خروجی از موتور استنتاج را به مقادیر غیر فازی تبدیل می‌کند). شکل کلی سامانه فازی در شکل (۷) آمده است.



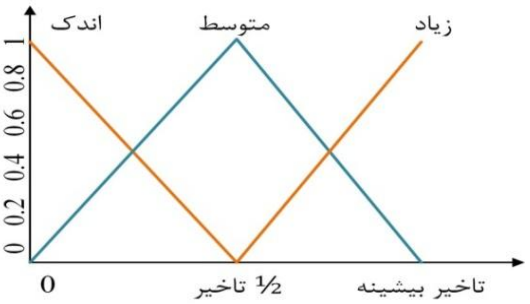
شکل ۷. معماری سامانه فازی [۱۹]

بدین منظور، ورودی‌های سامانه فازی مقادیر تأخیر و پهنای باند موجود، مربوط به یک لینک است و خروجی آن میزان هزینه لینک است. محدوده متغیرهای ورودی بین صفر تا مقدار بیشینه آن متغیر است که در آن "پهنای باند بیشینه" حداکثر مقدار ظرفیت لینک‌ها در شبکه و نیز "تأخیر بیشینه" حداکثر مقدار تأخیر در لینک‌های شبکه است. جهت کاهش پیچیدگی هر دو ورودی به سه سطح اندک، متوسط و زیاد تقسیم شده‌اند. توابع عضویت مربوط به متغیرهای میزان پهنای باند موجود و تأخیر به ترتیب در شکل‌های (۸) و (۹) آمده است. همچنین محدوده متغیر خروجی (هزینه لینک) بین صفر تا صد است و به پنج سطح ضعیف، بد، متوسط، خوب و عالی تقسیم شده است. تابع عضویت مربوط به متغیر خروجی در شکل (۱۰) آمده است.

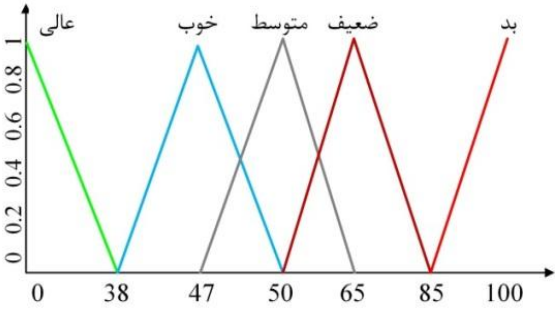
قوانین در نظر گرفته‌شده برای دو ورودی به صورت ماتریس ۳*۳ در شکل (۱۱) آمده است که ستون‌های ماتریس سه سطح مربوط به تأخیر لینک و ردیف‌های ماتریس سه سطح مربوط به پهنای باند موجود را نشان می‌دهد.



شکل ۸. تابع عضویت ورودی برای متغیر پهنای باند موجود



شکل ۹. تابع عضویت ورودی برای متغیر تأخیر



شکل ۱۰. تابع عضویت خروجی برای وزن هر لینک

تاخیر / پهنای باند	اندک	متوسط	زیاد
اندک	ضعیف	ضعیف	بد
متوسط	خوب	متوسط	ضعیف
زیاد	عالی	خوب	ضعیف

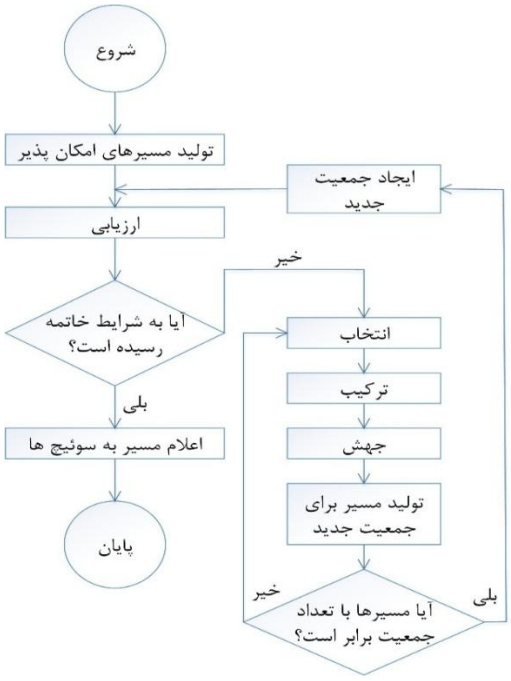
شکل ۱۱. قوانین در نظر گرفته‌شده

در این سامانه فازی، هر چقدر هزینه محاسبه‌شده یال پایین تر باشد، آن یال، یال مناسبی برای انتخاب است. پس از محاسبه هزینه تمامی یال‌ها، کنترل‌کننده، الگوریتم مسیریابی را اجرا می‌کند و بهترین مسیر بین مبدأ و مقصد را پیدا می‌کند. جهت یافتن مسیر بهینه از الگوریتم ژنتیک استفاده شده است. در بخش بعد پیاده‌سازی این الگوریتم شرح داده می‌شود.

[1] Fuzzification
[2] Inference
[3] Defuzzification

۳-۴. الگوریتم ژنتیک

به طور کلی این مسئله به دنبال یافتن یک جفت مسیر (اصلی و پشتیبان) بین مبدأ و مقصد است، به شرطی که دارای کمترین هزینه باشد. به منظور کاهش فقدان بسته، بهتر است بسته‌های مبادله شده از لینک‌هایی مسیریابی شوند که خلوت‌ترند. در شبکه‌های مبتنی بر نرم‌افزار، کنترل‌کننده مرکزی دارای یک دید سراسری از کل شبکه است و از وضعیت تمامی لینک‌ها و منابع شبکه ارتباطی آگاهی دارد. در روش پیشنهادی با توجه به مسیریابی و محاسبه SRLG مجزا بودن برای سناریوهای بزرگ در زمان کم و محدود، تقریباً غیرممکن است [۲۴] .بنابراین باید از الگوریتم‌های فرا ابتکاری برای حل این مدل استفاده کرد. الگوریتم مورد استفاده در این مقاله، الگوریتم ژنتیک [۲۵] است. از جمله مزایای الگوریتم ژنتیک عبارت‌اند از: ۱) نوعی جستجوی تصادفی هدفمند محسوب شده و از مسیرهای مختلف به جواب‌های متفاوتی خواهد رسید. علاوه بر آن، با هیچ محدودیتی در مسیر جستجو و انتخاب پاسخ‌های تصادفی روبرو نیست. ۲) پیاده‌سازی آن ساده بوده و نیازی به روال‌های پیچیده حل مسئله ندارد. ۳) این روش برای بهینه‌سازی مسایلی که با کمیت‌های گسسته سر و کار دارد بسیار مناسب است. فلوچارت الگوریتم ژنتیک مورد استفاده در این مقاله در شکل (۱۲) آمده است.



شکل ۱۲. فلوچارت الگوریتم ژنتیک پیشنهادی

در ادامه مراحلی که در این الگوریتم مورد استفاده قرار می‌گیرد، به طور مختصر شرح داده می‌شود: ورودی الگوریتم، گراف نودهای موجود در شبکه است. داده‌های این گراف با استفاده از ماتریس مجاورت آن به الگوریتم ژنتیک داده می‌شود. با توجه به نوع مسئله در این مقاله ماتریس هزینه حاصله از سامانه فازی، ورودی الگوریتم است. مقدار جمعیت اولیه برابر با ۲۵ در نظر گرفته شده است. هر عضو تولیدشده، یک مسیر از نود مبدأ تا نود مقصد را نشان می‌دهد. بعد از آنکه یک جمعیت تولید می‌شود نیاز است تا این جمعیت تولیدشده مورد ارزیابی قرار گیرد. در مرحله ارزیابی عضوی که کمترین هزینه را داشته باشد، انتخاب می‌شود. برای تولید نسل جدید از دو روش ترکیب و جهش استفاده می‌شود که نرخ ترکیب (ترکیب دو نقطه‌ای) ۰/۷۵ و نرخ جهش ۰/۲۵ و همچنین تعداد تکرار نیز ۱۰۰۰ در نظر گرفته شده است. برای انتخاب نسل جدید با توجه به هزینه هر عضو، یک احتمال به آن عضو نسبت داده می‌شود و در نهایت با استفاده از چرخ رولت اعضای جمعیت نسل بعد انتخاب می‌گردند.

تاکنون تلاشی برای افزودن فراداده‌ها در تصمیم‌گیری الگوریتم‌های مسیریابی برای افزایش تحمل‌پذیری خطا در شبکه‌های مبتنی بر نرم‌افزار صورت نگرفته است. افزودن اطلاعات ریسک‌های فیزیکی یک لینک برای تصمیم‌گیری می‌تواند میزان اطمینان انتخاب مسیرهای جایگزین را ارتقا دهد. به دلیل بزرگ بودن فضای مسئله مسیریابی و افزودن قید و شرط‌ها روش‌های عادی بسیار زمان‌بر هستند. همچنین با بزرگ‌تر شدن مسئله ممکن است یافتن راه حل در زمان مورد نظر امکان‌پذیر نباشد و استفاده از الگوریتم‌های فرا ابتکاری این امکان را فراهم می‌کند تا مسئله بتواند در زمان کوتاهی به جواب بهینه یا نزدیک به بهینه برسد. در روش‌های موجود اولویت با کوتاه‌ترین یا بهینه‌ترین مسیر از لحاظ سرعت و هزینه است، درحالی‌که انتخاب مسیری که از قبل دچار خطا شده باشد، می‌تواند بر خروجی شبکه تأثیر منفی بگذارد. در روش‌های پیشین برای ورودی الگوریتم مسیریابی از گرافی استفاده شده بود که وزن تمامی یال‌ها یکسان بود. در واقع کوتاه‌ترین مسیر فقط بر اساس درصد به‌کارگیری لینک‌ها انتخاب می‌شدند که در حقیقت ممکن بود بهینه‌ترین نباشند. اما روش پیشنهادی از گراف وزن داری استفاده می‌کند که وزن هر یال، ترکیبی از تأخیر و پهنای باند موجود آن یال است. بنابراین در لحظه تعویض مسیر، با انتخاب مسیر جایگزین از لیست کوتاه‌ترین مسیرهای واقعی، بهینه‌تر عمل می‌کند.

۵. شبیه‌سازی و ارزیابی نتایج

در این بخش نتایج پیاده‌سازی روش پیشنهادی و مقایسه آن با سایر روش‌ها ذکر شده است. کارایی روش پیشنهادی با روش‌های زیر مقایسه و ارزیابی می‌گردد.

*الگوریتم پیش‌فرض سوربال [۲۶] که تاکنون در شبکه‌های سنتی استفاده شده است و تغییر این الگوریتم جهت استفاده در

شبکه‌های مبتنی بر نرم‌افزار که در بخش قبلی توضیح داده شد، ولی در نسخه پیش‌فرض (نسخه‌ای که تاکنون مورد استفاده قرار گرفته است) برای وزن یال‌ها تنها از درصد به‌کارگیری لینک‌ها به این صورت استفاده کرده است.

$$d_{ij} = \frac{T_{ij}}{BW_{ij}} \qquad (۷)$$

که در آن Tij نرخ استفاده جاری لینک (i,j) و BWij کل پهنای باند و dij هزینه آن لینک است. از رابطه فوق واضح است هرچه میزان استفاده یا به‌کارگیری از یک لینک کمتر باشد، مقدار هزینه dij به صفر نزدیک‌تر خواهد بود. همچنین در این نسخه برای مسیریابی از الگوریتم دایجسترا استفاده شده است.

*روش OSPF که یک پروتکل مشهور مسیریابی در شبکه‌های رایانه‌ای است و این پروتکل به طور گسترده در ارزیابی کارایی روش‌های جدید ارائه‌شده در شبکه‌های سنتی و شبکه‌های مبتنی بر نرم‌افزار استفاده شده است [۲۷-۲۹]. در این پروتکل هزینه هر لینک، رابطه معکوسی با پهنای باند آن لینک دارد و جهت یافتن مسیر بهینه از الگوریتم دایجسترا استفاده می‌کند. در این روش سازوکاری جهت تحمل‌پذیری خطا وجود ندارد.

با توجه به اینکه برخی پارامترها به صورت تصادفی هستند، برای اطمینان بیشتر و عادلانه بودن مقایسه‌ها، روش پیشنهادی با سایر روش‌ها ۱۰ بار اجرا شده و میانگین این اجراها در نظر گرفته شده است. همچنین این روش‌ها در دو سناریوی زیر با توپولوژی‌های مختلف مورد ارزیابی قرار گرفتند.

*در سناریوی اول، از توپولوژی معروف و مشهور NTT[1] استفاده شده است. این توپولوژی دارای ۱۴۴ لینک با تأخیر و پهنای باند متفاوت و ۵۵ سوئیچ OpenFlow هستند.

*در سناریوی دوم، از توپولوژی معروف و مشهور NSF[2] استفاده شده است. این توپولوژی دارای ۴۲ لینک با تأخیر و پهنای باند متفاوت و ۱۴ سوئیچ OpenFlow هستند.

در پیاده‌سازی روش پیشنهادی و سایر روش‌ها پارامترهایی مانند پهنای باند و تأخیر به صورت پویا اندازه‌گیری شده‌اند. برای شبیه‌سازی خطاهای رخ داده، باید به صورت تصادفی یک لینک از گروه لینک‌ها با ریسک مشترک را انتخاب و آن را برای مدت زمان تصادفی قطع کرد. پس از این مدت زمان، مجدداً، لینک قطع‌شده در مرحله قبل، وصل می‌شود. به این ترتیب، لینک‌هایی که ریسک مشترکی دارند به طور متناوب قطع و وصل می‌شوند تا کارایی روش‌ها در مقابله با این خرابی‌ها بررسی گردند. همچنین مسیرهای اصلی و پشتیبان در جدول‌های جریان سوئیچ‌ها با اولویت متفاوت نگهداری می‌شوند. مسیر اصلی دارای اولویت بالاتر و مسیر پشتیبان اولویت کمتری خواهد داشت. به محض بروز خطا در مسیر اصلی، مسیر با اولویت کمتر برای انتقال بسته‌های داده استفاده می‌شود. زمان محاسبه مسیرها در ابتدا و سپس پس از اعلام هر خرابی به کنترل‌کننده محاسبه می‌شوند.

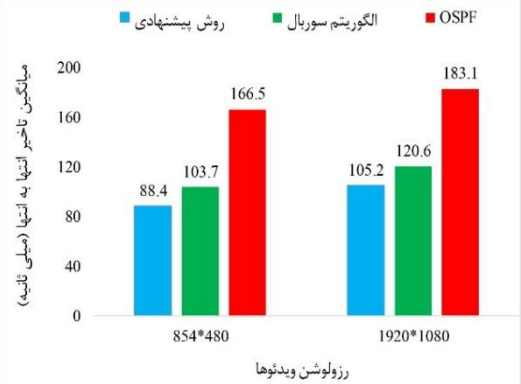
همان طور که قبلاً بیان شد، در این مقاله برای حل مسئله یافتن مسیر اصلی و پشتیبان از الگوریتم ژنتیک استفاده شده است. این الگوریتم با استفاده از زبان برنامه‌نویسی جاوا و در قالب یک باندل[3] به کنترل‌کننده Opendaylight اضافه شده است. Opendaylight کنترل‌کننده مشهور، قدرتمند و به صورت متن باز است که زبان برنامه‌نویسی جاوا را پشتیبانی می‌کند و می‌توان توسط آن شبکه را برنامه‌ریزی و مدیریت کرد. برای مسیریابی پویا، این الگوریتم هر ۱ ثانیه یک بار اجرا می‌شود و با توجه به وضعیت لینک‌ها و منابع شبکه کوتاه‌ترین مسیر را با در نظر گرفتن محدودیت تأخیر محاسبه می‌کند و مسیر بهینه بین مبدأ و مقصد را به سوئیچ‌های مرتبط اعلام می‌کند. در پیاده‌سازی روش پیشنهادی از نرم‌افزار VLC به عنوان سرویس‌دهنده ویدئویی اتاق عمل با استفاده از پروتکل RTSP و همچنین به عنوان گیرنده ویدئو ارسال‌شده در سمت پزشک راه دور، نرم‌افزار Hping3 برای تولید ترافیک میانی در مقلد Mininet استفاده شده است. Mininet شبیه‌سازی میزبان‌ها، سوئیچ‌ها و لینک‌ها را روی یک سامانه با هستهٔ لینوکس فراهم می‌آورد. میزبان‌ها، لینک‌ها و سوئیچ‌های موجود در این مقلد قادر به انجام عملیات مشابه با دنیای واقعی هستند. از جمله ویژگی‌های این مقلد می‌توان به سریع بودن، تولید توپولوژی‌های دلخواه، اجرای برنامه‌های بلادرنگ و سادگی آن اشاره کرد. تمامی سوئیچ‌های موجود در این شبیه‌سازی به کنترل‌کننده وصل شده‌اند. برای ایجاد دو توپولوژی در نظر گرفته‌شده، از کدنویسی زبان پایتون استفاده شده است. جهت ارزیابی کارایی از دو ویدئو با رزولوشن‌های ۴۸۰*۸۵۴ و ۱۰۸۰*۱۹۲۰ با کدک H.264 و ۳۰ فریم بر ثانیه به مدت زمان ۲۵۶ ثانیه استفاده شده است.

در این مقاله طرح پیشنهادی از نظر تأخیر (مدت زمان بین ارسال یک بسته در مبدأ تا زمان دریافت بسته در مقصد)، فقدان بسته (میزان درصد بسته‌هایی که در مبدأ ارسال شده‌اند و در مقصد دریافت نشده‌اند) و PSNR (یک پارامتر کیفیتی از دید کاربر است که فریم‌های ویدئو را قبل و بعد از فشرده‌سازی مقایسه کرده و میزان شباهت آن‌ها را اندازه می‌گیرد) بررسی شده است. شبکه مورد نظر قسمتی از شبکه فرماندهی و کنترل است که داده‌های یک رادار را از پایین‌ترین لایه شبکه فرماندهی و کنترل به یک ADOC در بالاترین سطح از شبکه فرماندهی و

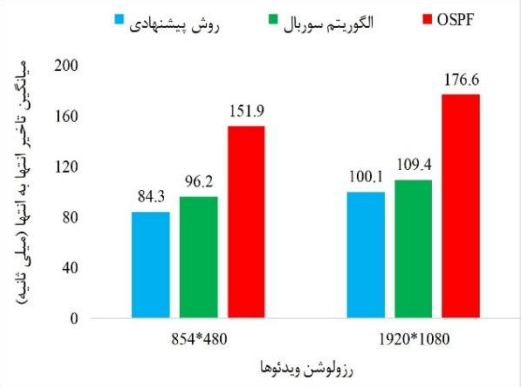
[1] Nippon Telegraph And Telephone
[2] National Science Foundation
[3] Bundle

کنترل ارسال می‌کند. برای بالا بردن قابلیت بقاپذیری و همچنین کنترل ترافیک، مسیرهای مختلف بین SOC های مجاور در نظر گرفته شده است. رادارهای مختلف داده اطلاعات پروازی را تولید کرده و در سلسله مراتب فرماندهی و کنترل به سمت مراتب بالای فرماندهی و کنترل ارسال می‌کنند. شبیه‌سازی برای ارسال اطلاعات یک رادار به ADOC انجام شده است. در فرآیند شبیه‌سازی کلیه رادارها عملیاتی بوده و ارسال اطلاعات در سلسله مراتب شبکه فرماندهی و کنترل در حال انجام فرض شده است. فرض شده است که یک رادار در حال ارسال اطلاعات ویدئوهای چندرسانه‌ای با رزولوشن ۱۰۸۰*۱۹۲۰ بوده و سایر رادارها در حال ارسال داده‌های حاصل از پردازش داده با حجم ۱ مگابیت در ثانیه هستند. نتایج حاصل از شبیه‌سازی برای دو پارامتر میانگین تأخیر انتها به انتها و درصد فقدان بسته در دو سناریوی در نظر گرفته‌شده به ترتیب در شکل‌های (۱۳) تا (۱۶) آمده است.

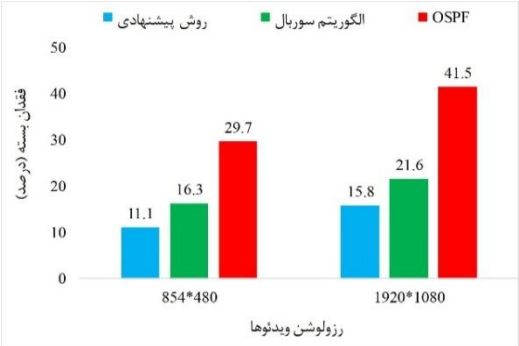
همان‌گونه که از شکل‌های بالا مشخص است وجود سازوکار مقابله با خطا تأثیر بسیار مهمی در پارامترهای میانگین تأخیر انتها به انتها و فقدان بسته داشته است. با توجه به اینکه در پروتکل OSPF هیچ سازوکار تحمل‌پذیری خطا وجود نداشته است، عملکرد آن نسبت به الگوریتم سوربال و روش پیشنهادی خیلی بد بوده است. استفاده از دو مسیر اصلی و پشتیبان در مواجهه با خطا در نتایج بسیار تأثیرگذار بوده است و همچنین روش پیشنهادی بهترین عملکرد را داشته است و این به این دلیل است که در روش سوربال جهت وزن‌دهی لینک‌ها تنها از درصد به‌کارگیری لینک‌ها استفاده شده است و جهت مسیریابی نیز از الگوریتم دایجسترا استفاده کرده است ولی در روش پیشنهادی وزن لینک‌های شبکه، ترکیبی از تأخیر و پهنای باند لینک‌ها و استفاده از سامانه فازی در تعیین وزن لینک‌ها و همچنین برای مسیریابی از الگوریتم ژنتیک استفاده شده است و این بهبود به این دلیل است که ذات الگوریتم ژنتیک گسسته بوده و روی گراف خیلی خوب جواب می‌دهد و به همین دلیل است که در پیدا کردن مسیر بهینه سریع و موفق بوده است. با توجه به اینکه دو پارامتر میانگین تأخیر و میزان فقدان بسته، بیش‌ترین تأثیر را روی PSNR دارند، از این رو با توجه به اینکه هر دو پارامتر میانگین تأخیر و میزان فقدان بسته عملکرد بهتری نسبت به دو روش دیگر داشتند، این عملکرد نیز برای پارامتر PSNR قابل انتظار است که نتایج این پارامتر در شکل‌های (۱۷) تا (۲۰) آمده است



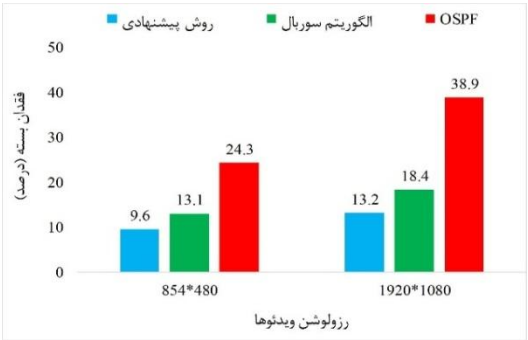
شکل ۱۳. نتایج ارزیابی کارایی میانگین تأخیر در سناریوی اول



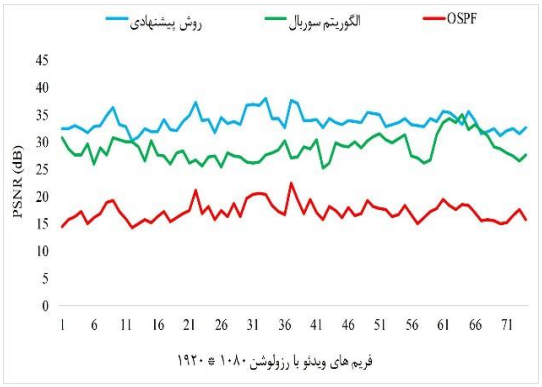
شکل ۱۴. نتایج ارزیابی کارایی میانگین تأخیر در سناریوی دوم



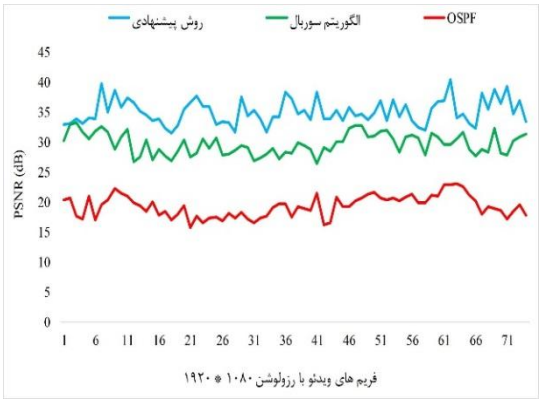
شکل ۱۵. نتایج ارزیابی کارایی فقدان بسته در سناریوی اول



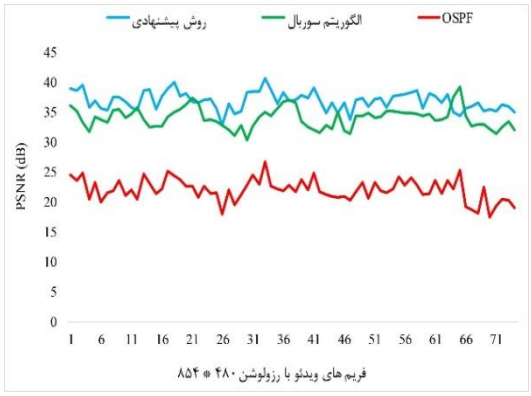
شکل ۱۶. نتایج ارزیابی کارایی فقدان بسته در سناریوی دوم



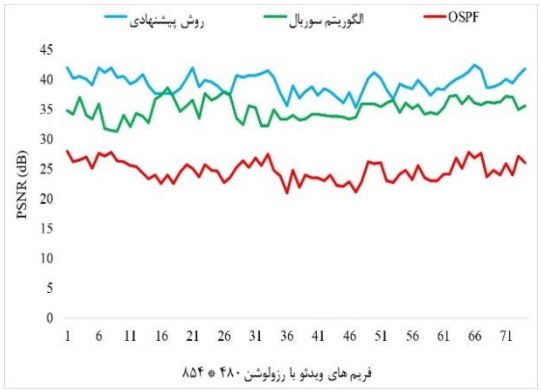
شکل ۱۷. نتایج ارزیابی کارایی PSNR در سناریوی اول



شکل ۱۸. نتایج ارزیابی کارایی PSNR در سناریوی دوم



شکل ۱۹. نتایج ارزیابی کارایی PSNR در سناریوی اول



شکل ۲۰. نتایج ارزیابی کارایی PSNR در سناریوی دوم

۶. نتیجه‌گیری

مراکز کنترل فرماندهی قدرتمند و توانا، علاوه بر بهره‌گیری از آخرین توانمندی‌های علمی، زیرساخت ارتباطی آن‌ها بایستی به گونه‌ای طراحی و ساخته شود که در صورت بروز مشکل در یک لینک یا یک مسیر، شبکه دچار مشکل نشود و کیفیت سرویس ارائه خدمات تضمین شود. سرویس مهمی که بایستی در این شبکه‌ها در نظر گرفته شود، ارسال مطمئن و بدون از دست رفتن بسته‌ها است. مشکل عمده‌ای که در زیرساخت ارتباطی برای مدیریت فرماندهی و کنترل مطرح است، تبادل اطلاعات و ارتباطات است که با توجه به فاصله دور، محدودیت تجهیزات و منابع و هزینه‌های بالا به یک امر حیاتی تبدیل گشته و نیازمند ارتباط مطمئن بین رادارها و مرکز است. شبکه‌های سنتی همیشه دارای پیچیدگی زیاد بوده‌اند و مدیریت آن‌ها نیز کار دشواری است. یکی از دلایل این امر در هم تنیدگی سطوح کنترل و داده با یکدیگر است؛ یک دلیل عمده دیگر، آن است که هر تولیدکننده دستگاه‌های شبکه، واسط‌های مدیریتی و پیکربندی انحصاری خودش را ارائه می‌دهد که منجر به چرخه طولانی در بروز رسانی این دستگاه‌ها می‌شود. این مالکیت انحصاری زیرساخت‌های شبکه، محدودیت‌های سنگینی بر هر گونه تغییر و نوآوری اعمال نموده است. در این مقاله شبکه‌های مبتنی بر نرم‌افزار به عنوان معماری جدیدی برای فراهم نمودن قابلیت اطمینان ارتباطات شبکه‌ای بین اجزای مختلف این سامانه معرفی شده است. جداسازی سطح داده از سطح کنترلی در شبکه‌های مبتنی بر نرم‌افزار به مدیریت، بر مبنای نیاز و شرایطی که برای ارتباطات این سامانه جهت تضمین کیفیت سرویس در راستای توسعه سامانه فرماندهی و کنترل تعریف‌شده، کمک می‌کند. نتایج ارزیابی کارایی نشان می‌دهد که روش پیشنهادی عملکرد بهتری نسبت به روش پایه داشته است. از آنجایی که توابع عضویت در نظرگرفته شده در سیستم فازی و همچنین توابع جهش و ترکیب در الگوریتم ژنتیک، ممکن است بهینه ترین حالت برای این مسئله نباشند و در کارهای آینده می توان برای این مسئله توابع مختلف را بررسی کرد تا به بهینه ترین حالت ممکن رسید.

۷. مرجع‌ها

[1] Weber, M. E.; Cho, J. Y.; Thomas, H. G. “Command and Control for Multifunction Phased Array Radar”; IEEE Transactions on Geoscience and Remote Sensing 2017, 55, 5899-5912.

[2] Parsaei, M. R.; Mohammadi, R.; Javidan, R. “A New Adaptive Traffic Engineering Method for Telesurgery Using ACO Algorithm Over Software Defined Networks”; European Research in Telemedicine 2017, 6, 173-180.

[3] Rowshanrad, S.; Parsaei, M. R.; Keshtgari, M. "Implementing NDN using SDN: A Review on Methods and Applications"; IIUM Engineering Journal 2016, 17, 11-20.

[4] Mohammadi, R.; Parsaei, M. R.; Javidan, R.; Akbari, R. "An Effective Countermeasure Method against Freeloading Attack in Software Defined Networks"; Adv. Defence Sci. & Technol. 2018, 9, 211-219. (In Persian)

[5] Parsaei, M. R.; Sobouti, M. J.; Khayami, S. R.; Javidan, R. "Network traffic classification using machine learning techniques over software defined networks"; International Journal of Advanced Computer Science and Applications 2017, 8, 220-225.

[6] Parsaei, M. R.; Naderi, M.; Javidan, Reza. "A New Architecture to Improve Multimedia QoS over Software Defined Networks"; International Journal of Computer Applications 2018, 179, 14-19.

[7] Parsaei, M. R.; Javidan, R.; Fatemifar, A.; Einavipour, S. "Providing Multimedia QoS Methods over Software Defined Networks: A Comprehensive Review"; International Journal of Computer Applications 2017, 168, 1-4.

[8] Parsaei, M. R.; Khalilian, S. H.; Javidan, R. "A Comparative Study on Fault Tolerance Methods in IP Networks *Versus* Software Defined Networks"; Int. Academic J. Sci. Eng. 2016, 3, 146-154.

[9] Basu, A.; Riecke, J. "Stability Issues in OSPF Routing"; Computer Communication Review 2001, 31, 225-236.

[10] Mohammadi, R.; Javidan, R. "An Adaptive Type-2 Fuzzy Traffic Engineering Method for Video Surveillance Systems over Software Defined Networks"; Multimedia Tools and Applications 2017, 76, 23627-23642.

[11] Sterbenz, J. P.; Çetinkaya, E. K.; Hameed, M. A.; Jabbar, A.; Qian, S.; Rohrer, J. P. "Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation"; Telecommunication systems 2013, 52, 705-736.

[12] Bayadi, F.; Azebr, A. "Optimization of Command and Control Network in an Air Defense System"; 3rd National Conference of Scientific Society Command and Control of Iran 2009, 169-174. (In Persian)

[13] Fadahiyan, M.; Fesharaki, N.; Mehmari, M. "Autonomous GRID Architecture Based on the State-of-the-Art Knowledge Process for Nodes Suitable for C4I Infrastructure"; 3rd National Conference of Scientific Society Command and Control of Iran 2009, 185-190. (In Persian)

[14] Kashefi, S.; Azebar, A. "Provide an Optimal Command and Control Structure in the C4I Defensive Network"; 8th National Conference of Scientific Society Command and Control of Iran 2014, 269-273. (In Persian)

[15] Kim, H.; Feamster, N. "Improving Network Management with Software Defined Networking"; IEEE Communications Magazine 2013, 51, 114-119.

[16] Wang, L.; Chang, R.; Lin, E.; Yik, J. "Apparatus for Link Failure Detection on High Availability Ethernet Backplane"; US Patents 7,260,066, 2007.

[17] Sharma, S.; Staessens, D.; Colle, D.; Pickavet, M.; Demeester, P. "OpenFlow: Meeting Carrier-Grade Recovery Requirements"; Computer Communications 2013, 36, 656-665.

[18] Van Adrichem, N. L.; Van Asten, B. J.; Kuipers, F. "Fast Recovery in Software-Defined Networks"; Third European Workshop on Software Defined Networks 2014, 61-66.

[19] Zadeh, L. A. "The Concept of a Linguistic Variable and Its Application to Approximate Reasoning"; Information Science 1975, 8, 199-249.

[20] Parsa, S. S.; Sourizaei, M.; Dehshibi, M. M.; Shateri, R. E.; Parsaei, M. R. "Coarse-grained correspondence-based ancient Sasanian coin classification by fusion of local features and sparse representation-based classifier"; Multimedia Tools and Applications 2017, 76, 15535-15560.

[21] Gao, W.; Sarlak, V.; Parsaei, M. R.; Ferdosi, M. "Combination of fuzzy based on a meta-heuristic algorithm to predict electricity price in an electricity markets"; Chemical Engineering Research and Design 2018, 131, 333-345.

[22] Parsaei, M. R.; Mollashahi, H.; Darvishan, A.; Mir, M.; Simoes, R. "A new prediction model of solar radiation based on the neuro-fuzzy model"; International Journal of Ambient Energy 2018, 1-9.

[23] Komijani, H.; Parsaei, M. R.; Khajeh, E.; Golkar, M. J.; Zarrabi, H. "EEG classification using recurrent adaptive neuro-fuzzy network based on time-series prediction"; Neural Computing and Applications 2017, 1-12.

[24] Xu, D.; Chen, Y.; Xiong, Y.; Qiao, C.; He, X. "On Finding Disjoint Paths in Single and Dual Link Cost Networks"; Twenty-third Annual Joint Conference on Computer and Communications Societies 2004, 705-715.

[25] Nabaei, A.; Hamian, M.; Parsaei, M. R.; Safdari, R.; Samad-Soltani, T.; Zarrabi, H.; Ghassemi, A. "Topologies and Performance of Intelligent Algorithms: A Comprehensive Review"; Artificial Intelligence Review 2018, 49, 1-25.

[26] Rostami, M. J.; Khorsandi, S.; Khodaparast, A. A. "CoSE: A SRLG-Disjoint Routing Algorithm"; Fourth European Conference on Universal Multiservice Networks 2007, 86-92.

[27] Rakheja, P.; Kaur, P.; Gupta, A.; Sharma, A. "Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network"; Int. J. Comput. Appl. 2012, 48, 18, 6-11.

[28] Mirzahossein, K.; Nguyen, M.; Elmasry, S. "Analysis of RIP, OSPF, and EIGRP Routing Protocols using Opnet"; Simon Fraser University, 2013.

[29] Karl, M.; Gruen, J.; Herfet, T. "December. Multimedia Optimized Routing in OpenFlow Networks"; Proc. 19th IEEE Int. Conf. Networks, Singapore, 2013, 1-6.