Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
DOI: 10.22034/jscit.2026.591041.2283
Volume *, Number *, Season 20**, pp. **-**
Received: 07/12/2025, Revised: 09/24/2026, Accepted: 09/27/2026

An Attack-Aware Mathematical Model for the Optimization of Controller Placement and Quality of Service in Software-Defined Networks Under DDoS Attacks

Ahmad Jalili [1*]
1*- Department of Computer Engineering, Faculty of Basic Sciences and Engineering, Gonbad Kavous University, Basirat Blvd., Shahid Fallahi St., Gonbad Kavous 49717-99151, Iran.
[1*] jalili@gonbad.ac.ir

Corresponding author's address: Ahmad Jalili, Faculty of Basic Sciences and Engineering, Gonbad Kavous University, Golestan, Iran.

Abstract— Software-Defined Networks (SDNs) have significantly enhanced network flexibility, programmability, and manageability by decoupling the control plane from the data plane. However, the concentration of control logic in one or more controllers makes the control plane one of the most critical targets for Distributed Denial-of-Service (DDoS) attacks. A review of existing studies indicates that most controller placement models have primarily focused on criteria such as latency minimization, load balancing, or fault tolerance, while failing to simultaneously account for the impact of different DDoS attack intensities on controller placement and backup controller selection. This study proposes an attack-aware Mixed-Integer Linear Programming (MILP) model for the joint determination of the number, location, and type of regular and intelligent backup controllers, switch-to-controller assignment, and control-plane mesh connectivity. In addition to minimizing deployment costs, the proposed model incorporates processing capacity, port capacity, bandwidth, and maximum Quality of Service (QoS) delay constraints. The model was evaluated using AMPL and the IBM ILOG CPLEX solver across 13 operational scenarios. The results show that, as the attack intensity increases from the no-attack condition to combined attack levels 1–7, the number of deployed intelligent controllers increases from 0 to 28 units. Accordingly, the total deployment cost increases from $23,950 under normal conditions to $51,550 under severe triple attacks and ultimately to $117,650 under multi-point attacks. Furthermore, the model solution time ranges from 0.125 to 893.5 seconds for networks with 9 to 100 candidate nodes, while maintaining an optimality gap of 0.00%. These results demonstrate that the proposed model provides a rigorous mathematical baseline for strategic and offline planning of SDN infrastructures at small and medium scales.

Keywords- Software-Defined Networking (SDN), Controller Placement Problem (CPP), Controller Placement and Assignment, Distributed Denial-of-Service (DDoS) Attacks, Mixed-Integer Linear Programming (MILP), Smart Controller, Network Resilience.

مجله علمی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
شناسه دیجیتال: 10.22034/jscit.2026.591041.2283
جلد *، شماره *، فصل **۱۴، صفحه **-**
دریافت: ۱۴۰۵/۰۴/۲۱، بازنگری: ۱۴۰۵/۰۷/۰۲، پذیرش: ۱۴۰۵/۰۷/۰۵

ارائه یک مدل ریاضی آگاه از حمله برای بهینه‌سازی مکان‌یابی کنترلرها و کیفیت سرویس در شبکه‌های مبتنی بر نرم‌افزار تحت حملات DDoS

احمد جلیلی[1*]
۱*- گروه مهندسی کامپیوتر، دانشکده علوم پایه و فنی مهندسی، دانشگاه گنبدکاووس، گنبدکاووس، ایران.
[1*]jalili@gonbad.ac.ir

* نشانی نویسنده مسئول: احمد جلیلی، گنبدکاووس، خیابان شهید فلاحی، دانشگاه گنبدکاووس، دانشکده علوم پایه و فنی مهندسی.

چکیده- شبکه‌های مبتنی بر نرم‌افزار با جداسازی سطح کنترل از سطح داده، انعطاف‌پذیری، برنامه‌پذیری و قابلیت مدیریت شبکه را به‌طور چشمگیری افزایش داده‌اند. با این حال، تمرکز منطق کنترل در یک یا چند کنترلر، لایه کنترل را به یکی از مهم‌ترین نقاط آسیب‌پذیر در برابر حملات محروم‌سازی از سرویس توزیع‌شده (DDoS) تبدیل کرده است. بررسی مطالعات پیشین نشان می‌دهد که بیشتر مدل‌های مکان‌یابی کنترلر، بر معیارهایی مانند کاهش تأخیر، تعادل بار یا تحمل خرابی تمرکز داشته‌اند و اثر شدت‌های مختلف حملات DDoS بر فرآیند مکان‌یابی و انتخاب کنترلرهای پشتیبان را به‌صورت هم‌زمان در نظر نگرفته‌اند. در این پژوهش، یک مدل برنامه‌ریزی خطی عدد صحیح مختلط (MILP) آگاه از حمله برای تعیین همزمان تعداد، مکان و نوع کنترلرهای ساده و هوشمند پشتیبان، تخصیص سوئیچ‌ها و همبندی مش لایه کنترل ارائه شده است. این مدل علاوه بر کمینه‌سازی هزینه‌های استقرار، قیود ظرفیت پردازشی، پورت، پهنای باند و سقف تأخیر کیفیت سرویس را لحاظ می‌کند. ارزیابی مدل با ابزار AMPL و حل‌کننده IBM ILOG CPLEX در ۱۳ سناریوی عملیاتی نشان داد که با افزایش شدت حمله از سطح صفر تا سطوح ترکیبی ۱ تا ۷، تعداد کنترلرهای هوشمند مستقرشده از ۰ به ۲۸ واحد افزایش یافته و هزینه کل استقرار از ۲۳،۹۵۰ دلار در شرایط عادی به ۵۱،۵۵۰ دلار در حملات شدید سه‌گانه و نهایتاً ۱۱۷،۶۵۰ دلار در حملات چندنقطه‌ای تغییر می‌یابد. همچنین زمان حل مدل برای شبکه‌های با ۹ تا ۱۰۰ گره کاندید بین ۰،۱۲۵ تا ۸۹۳،۵ ثانیه با شکاف بهینگی ۰،۰۰٪ متغیر است. این نتایج نشان می‌دهد که مدل پیشنهادی یک خط مبنای ریاضی دقیق برای برنامه‌ریزی استراتژیک و آفلاین زیرساخت‌های SDN در مقیاس‌های کوچک و متوسط فراهم می‌سازد.

واژه‌های کلیدی: شبکه‌های مبتنی بر نرم‌افزار، مسئله مکان‌یابی کنترلر، مکان‌یابی-تخصیص، حملات DDoS، مدل‌سازی خطی عدد صحیح مختلط MILP، کنترلر هوشمند، تاب‌آوری شبکه.

۱- مقدمه

در سال‌های اخیر، با گسترش سریع رایانش ابری و اینترنت اشیاء، نیاز به شبکه‌هایی با قابلیت مدیریت آسان، انعطاف‌پذیری بالا و مقیاس‌پذیری مناسب بیش از گذشته احساس می‌شود. شبکه‌های سنتی به دلیل وابستگی مستقیم سطح کنترل[۱] و سطح داده[۲] به تجهیزات سخت‌افزاری، پیکربندی پیچیده و مدیریت دستی، پاسخگوی این نیازها نیستند. شبکه‌های مبتنی بر نرم‌افزار[۳] به عنوان یکی از مهم‌ترین فناوری‌های نوین شبکه، با جداسازی سطح کنترل از سطح داده و انتقال منطق تصمیم‌گیری به یک کنترلر مرکزی، بسیاری از این محدودیت‌ها را برطرف کرده‌اند [۱] [۲]. این معماری به دلیل برنامه‌پذیری، انعطاف‌پذیری، مدیریت متمرکز و کاهش هزینه‌های بهره‌برداری، به سرعت در مراکز داده و

زیرساخت‌های ارتباطی بزرگ مورد استفاده قرار گرفته است [۳].

با وجود مزایای فراوان، تمرکز عملکرد کنترل شبکه در یک یا چند کنترلر، چالش‌های جدیدی را نیز به همراه دارد. مهم‌ترین این چالش‌ها مربوط به قابلیت اطمینان، مقیاس‌پذیری و امنیت شبکه است. ازآنجاکه تصمیم‌گیری‌های اصلی شبکه در لایه کنترل انجام می‌شود، کنترلرها به یکی از مهم‌ترین اهداف حملات سایبری تبدیل شده‌اند [۳] [۴]. در میان تهدیدهای امنیتی، حملات محروم‌سازی از سرویس توزیع‌شده[۴] از خطرناک‌ترین حملات علیه شبکه‌های SDN به شمار می‌روند. در این حملات، ارسال حجم بالایی از بسته‌های ترافیک نامتعارف موجب تولید پیام‌های متعدد Packet-In، اشباع بافر و مصرف توان پردازشی کنترلر می‌گردد. در نتیجه، کنترلر دیگر قادر به پاسخ‌گویی به درخواست‌های قانونی نیست و ارتباط سوئیچ‌های متصل به آن نیز دچار اختلال می‌شود که این موضوع می‌تواند عملکرد کل شبکه را تحت تأثیر قرار دهد [۵]. این پدیده زمان پاسخ‌دهی را افزایش داده و سرویس‌دهی به کاربران مجاز را مختل می‌سازد.

یکی از راهکارهای مؤثر برای کاهش اثر این حملات، طراحی مناسب محل استقرار کنترلرها در شبکه است. این مسئله که با عنوان مسئله مکان‌یابی کنترلر[۵] (CPP) شناخته می‌شود، نقش مهمی در افزایش قابلیت اطمینان و پایداری شبکه دارد [۶]. بررسی پیشینه پژوهش نشان می‌دهد که بیشتر مدل‌های ارائه‌شده برای CPP، بر معیارهایی نظیر کمینه‌سازی تأخیر انتشار یا تحمل خرابی‌های تصادفی سخت‌افزاری یا قطع لینک ها تمرکز داشته‌اند [۷-۱۲]. در مقابل، تأثیر شدت‌های مختلف حملات DDoS بر عملکرد کنترلرها و ظرفیت پردازشی آن‌ها کمتر مورد توجه قرار گرفته است. همچنین، در اغلب این مدل‌ها، انتخاب هم‌زمان نوع کنترلر، ظرفیت پردازشی و محل استقرار آن‌ها متناسب با میزان تهدید در بخش‌های مختلف شبکه انجام نشده است. در این میان، دو شکاف پژوهشی عمده مشاهده می‌شود: نخست، بیشتر مدل‌های امنیتی موجود، حمله را به صورت یک وضعیت دودویی (حضور یا عدم حضور) فرض کرده و از مدل‌سازی اثر سطوح مختلف شدت حمله بر بار پردازشی لایه کنترل غفلت نموده‌اند. دوم، استقرار کنترلرهای پشتیبان معمولاً به صورت همگن انجام شده و هزینه اثربخشی استفاده از کنترلرهای با ظرفیت‌های پردازشی متفاوت بررسی نشده است.

برای رفع این محدودیت‌ها، در این پژوهش یک مدل برنامه‌ریزی خطی عدد صحیح مختلط[۶] (MILP) آگاه از حمله برای مکان‌یابی کنترلرها ارائه شده است. نوآوری اصلی این پژوهش به شرح زیر خلاصه می‌شود:

- **فرمول‌بندی یکپارچه آگاه از حمله:** ارائه یک مدل ریاضی دقیق برای تعیین همزمان تعداد، مکان و تخصیص سوئیچ‌ها به کنترلرها با در نظر گرفتن اثر سطوح گوناگون شدت حمله DDoS.
- **استقرار دوگانه و ناهمگون کنترلرها:** ترکیب کنترلرهای ساده استاندارد برای شرایط عادی و کنترلرهای هوشمند پشتیبان برای مدیریت بار در شرایط بحرانی.
- **ادغام محدودیت‌های عملیاتی و واقعی شبکه:** درنظر گرفتن همزمان ظرفیت پردازشی کنترلرها، محدودیت پورت‌ها، پهنای باند لینک‌ها و سقف تأخیر مجاز کیفیت سرویس[۷] (شامل تأخیر انتشار و کران بالای تأخیر صف).
- **ارزیابی عملکرد و تحلیل محاسباتی:** پیاده‌سازی و حل مدل با حل‌کننده استاندارد IBM ILOG CPLEX در سناریوهای متعدد، و بررسی دقیق معیارهای زمان حل، تعداد تکرار و موازنه هزینه تاب‌آوری.

ادامه مقاله به صورت زیر سازمان‌دهی شده است. در بخش دوم، پژوهش‌های مرتبط و مطالعات انجام‌شده در زمینه مکان‌یابی کنترلر و امنیت شبکه‌های SDN بررسی می‌شوند. در بخش سوم، مبانی فنی حملات DDoS در شبکه‌های SDN و مفهوم کنترلرهای پشتیبان هوشمند معرفی می‌شود. بخش چهارم به تشریح مدل ریاضی پیشنهادی، تابع هدف و محدودیت‌های مدل اختصاص دارد. در بخش پنجم، نتایج شبیه‌سازی و تحلیل سناریوهای مختلف ارائه می‌شود و در نهایت، در بخش ششم، جمع‌بندی پژوهش و پیشنهادهایی برای تحقیقات آینده بیان می‌شود.

۲- مرور کارهای مرتبط و مطالعات پیشین

مسئله مکان‌یابی کنترلرها، یکی از مهم‌ترین موضوعات پژوهشی در طراحی شبکه‌های مبتنی بر نرم‌افزار است. انتخاب محل مناسب برای استقرار کنترلرها، تأثیر مستقیمی بر عملکرد، پایداری و امنیت شبکه دارد. پژوهش‌های انجام‌شده در این زمینه را می‌توان به چهار دسته اصلی تقسیم کرد: ۱) مکان‌یابی با هدف بهبود کارایی و کیفیت سرویس، ۲) مکان‌یابی مقاوم در برابر خرابی، ۳) مکان‌یابی با رویکرد امنیتی و مقابله با حملات هدفمند و ۴) روش‌های تشخیص و کاهش اثر حملات در لایه کنترل. در ادامه، مهم‌ترین مطالعات هر یک از این حوزه‌ها بررسی و محدودیت‌های آن‌ها بیان می‌شود.

مکان‌یابی با هدف بهبود کارایی و کیفیت سرویس: پژوهش‌های اولیه در مسئله مکان‌یابی کنترلرها، عمدتاً بر شاخص‌های عملکردی نظیر کاهش تأخیر بین سوئیچ و کنترلر، توزیع بار و بهینه‌سازی پهنای باند تمرکز داشته‌اند. برای مثال، کاظمیان و همکاران [۷] با استفاده از یک روش بهینه‌سازی چندهدفه مبتنی بر الگوریتم‌های فراابتکاری، مدلی برای کاهش تأخیر و مدیریت بهتر پهنای باند ارائه کرده‌اند. همچنین، هوک و همکاران [۸] در یک مطالعه جامع، تأثیر توپولوژی شبکه و محدودیت‌های ظرفیتی را بر مکان‌یابی کنترلرها بررسی کرده‌اند. در پژوهش مربوط به جلیلی و همکاران [۹]، یک روش مبتنی بر فازی به منظور بهینه کردن مکان کنترلرها بر اساس تأخیر و ظرفیت کنترلرها ارائه شده است. همچنین توسط این نویسندگان یک روش بهینه سازی مبتنی بر الگوریتم فراابتکاری NS-MF برای تضمین کیفیت سرویس شبکه های مبتنی بر نرم افزار ارائه شده است [۱۰].

این مطالعات صرفاً بر شرایط پایدار و عادی شبکه تمرکز دارند و مکانیزمی برای مدیریت بار پردازشی مازاد در شرایط بحرانی و حملات سایبری پیش‌بینی نکرده‌اند؛ در نتیجه لایه کنترل در مواجهه با ترافیک‌های غیرعادی دچار اشباع سریع می‌شود.

مکان‌یابی مقاوم در برابر خرابی: با افزایش اهمیت قابلیت اطمینان، پژوهشگران به مدل‌سازی اثر خرابی گره‌ها و پیوندهای ارتباطی روی آوردند. در این زمینه، هو و همکاران [۱۱] مدلی ریاضی برای مکان‌یابی کنترلرها ارائه کردند که هدف آن حفظ عملکرد شبکه و کاهش تأخیر در زمان خرابی کنترلرها بود. در این پژوهش، از کنترلرهای پشتیبان غیرفعال[۸] برای بازیابی سرویس استفاده شد. همچنین، لیو و همکاران [۱۲] با پیشنهاد یک روش مبتنی بر تکرارسازی[۹]، تلاش کردند زمان بازیابی شبکه پس از خرابی کنترلرها را کاهش دهند.

با وجود نتایج مناسب این مطالعات، فرض بنیادین این گروه از پژوهش‌ها، وقوع خرابی‌های تصادفی ناشی از نقص سخت‌افزاری یا قطع لینک است. در مقابل، حملات DDoS رفتاری هدفمند و همزمان دارند که طی آن چندین کنترلر یا لینک ارتباطی به صورت همزمان تحت فشار شدید قرار می‌گیرند؛ پدیده‌ای که مدل‌های خرابی تصادفی قادر به دفع آن نیستند.

مکان‌یابی با رویکرد امنیتی و مقابله با حملات هدفمند: در سال‌های اخیر، امنیت لایه کنترل به عنوان یکی از مؤلفه‌های اصلی وارد مدل‌های بهینه‌سازی شده است. طاهریان‌فرد و همکاران [۱۳] مدلی برای مکان‌یابی کنترلرها در برابر حملات محروم‌سازی از سرویس ارائه کرد که احتمال آسیب‌پذیری هر گره را در فرآیند تصمیم‌گیری در نظر می‌گرفت. با این حال، در این مدل تفاوتی میان توان پردازشی کنترلرهای اصلی و پشتیبان وجود نداشت. از سوی دیگر، جیمنز و همکاران [۱۴] در یک مقاله مروری، روش‌های مختلف مکان‌یابی کنترلرها از دیدگاه امنیت را بررسی کرده و بر ضرورت استفاده از معماری‌های توزیع‌شده و قابل بازپیکربندی تأکید کردند. همچنین، سبپلو و همکاران [۱۵] مسئله مکان‌یابی کنترلرها را در شبکه‌های گسترده (WAN) و در شرایط حملات DDoS مطالعه کردند، اما مدل آن‌ها امکان انتخاب کنترلرهای پشتیبان با ظرفیت‌های پردازشی متفاوت را فراهم نمی‌کرد.

در این مدل‌ها، وقوع حمله به صورت یک متغیر دودویی (صفر و یک) فرض شده و از اثر تغییرات پیوسته شدت حمله بر ظرفیت پردازشی غفلت شده است. علاوه بر این، کنترلرهای اصلی و پشتیبان به صورت همگن در نظر گرفته شده‌اند که این امر هزینه استقرار را به شدت افزایش می‌دهد.

تشخیص و مقابله با حملات DDoS در لایه کنترل: دسته چهارم بر توسعه سازوکارهای دفاعی و پایش ترافیک تمرکز دارند. علاوه بر مکان‌یابی کنترلرها، برخی پژوهش‌ها بر توسعه روش‌های تشخیص و مقابله با حملات DDoS تمرکز کرده‌اند. کاله و جاویدان [۱۶] یک روش تطبیقی برای دفاع در برابر حملات DDoS ارائه داده‌اند، که با استفاده از منطق فازی، میزان تهدید را ارزیابی کرده و تصمیم مناسب را اتخاذ می‌کند. همچنین، الاشهاب و همکاران [۱۷] با بررسی روش‌های مبتنی بر یادگیری ماشین نشان دادند که تشخیص حمله به تنهایی برای حفظ عملکرد شبکه کافی نیست و لایه کنترل باید از نظر ساختاری نیز توان مقابله با این شرایط را داشته باشد. یانگ و همکاران [۱۸] نیز مدلی ارائه کردند که به صورت هم‌زمان مکان‌یابی کنترلرها و مسیریابی امن را بهینه می‌کند تا اثر حملات کاهش یابد.

تمرکز این تحقیقات بر الگوریتم‌های نرم‌افزاری تشخیص است، در حالی که پژوهش حاضر بر طراحی بهینه زیرساخت فیزیکی لایه کنترل و استقرار ساختاری کنترلرها تمرکز دارد تا پیش‌نیاز سخت‌افزاری لازم برای اجرای این الگوریتم‌های دفاعی فراهم گردد.

تحلیل شکاف پژوهشی و نوآوری مقاله: بررسی مطالعات پیشین نشان می‌دهد که هنوز دو محدودیت مهم در این حوزه وجود دارد. نخست آنکه بیشتر مدل‌های امنیتی، حملات DDoS را تنها به صورت وجود یا عدم وجود حمله در نظر می‌گیرند و تأثیر

شدت‌های مختلف حمله بر عملکرد لایه کنترل را مدل‌سازی نمی‌کنند. در حالی که شدت حمله می‌تواند تأثیر مستقیمی بر میزان بار پردازشی کنترلرها و عملکرد شبکه داشته باشد. دوم آنکه در اغلب پژوهش‌های پیشین، کنترلرهای اصلی و پشتیبان از نظر ظرفیت پردازشی تفاوتی با یکدیگر ندارند. استفاده از کنترلرهای پشتیبان همسان، علاوه بر افزایش هزینه‌های استقرار، در شرایط حملات شدید نیز کارایی لازم را ندارد.

مدل ارائه‌شده در این پژوهش با استفاده از یک مدل برنامه‌ریزی عدد صحیح[۱۰] (IP)، به صورت هم‌زمان تعداد، محل استقرار و نوع کنترلرهای اصلی و پشتیبان را تعیین می‌کند. همچنین، شدت حملات DDoS در فرآیند تصمیم‌گیری لحاظ شده و هزینه استقرار کنترلرها و لینک‌های ارتباطی نیز به طور هم‌زمان بهینه می‌شود. در نتیجه، مدل پیشنهادی علاوه بر کاهش هزینه‌ها، پایداری و امنیت لایه کنترل را در شرایط مختلف حمله بهبود می‌بخشد.

مقایسه تطبیقی مدل پیشنهادی با مطالعات شاخص: به منظور تبیین دقیق جایگاه علمی و تمایزات فنی پژوهش حاضر، جدول زیر (جدول ۱) مقایسه‌ای ساختاریافته میان مدل پیشنهادی و برجسته‌ترین مدل‌های مکان‌یابی کنترلر در ادبیات موضوع را ارائه می‌دهد. همان‌طور که از مقایسه ویژگی‌ها مشخص است، اکثر مدل‌های پیشین یا صرفاً بر بهبود تأخیر و خرابی‌های تصادفی تمرکز داشته‌اند و یا در مدل‌های امنیتی، استقرار کنترلرها را به صورت همگن و بدون در نظر گرفتن شدت‌های متغیر حمله فرموله کرده‌اند. در مقابل، مدل پیشنهادی این پژوهش با ترکیب ناهمگون کنترلرهای ساده و هوشمند، لحاظ پیوندهای مش بین‌کنترلری و در نظر گرفتن قیود جامع پورت، پهنای باند و تأخیر صف، یک چارچوب بهینه‌سازی یکپارچه برای موازنه هزینه و تاب‌آوری فراهم می‌سازد.

۳- پیش‌زمینه‌ها و مفاهیم اولیه

طراحی و فرمول‌بندی یک مدل ریاضی بهینه‌سازی کارآمد برای مکان‌یابی کنترلرها در شرایط بحرانی، مستلزم ایجاد یک پل مفهومی منسجم بین پدیده‌های فیزیکی شبکه و معادلات ریاضی است. هدف اصلی این بخش، تبیین و کالبدشکافی دقیق سازوکارهای فنی حملات DDoS، نحوه اشباع منابع در لایه‌های مختلف معماری شبکه مبتنی بر نرم‌افزار و همچنین تحلیل رفتار عملیاتی و اقتصادی کنترلرهای دوگانه (ساده و هوشمند) است. برای طراحی یک مدل ریاضی کارآمد، ابتدا باید نحوه عملکرد شبکه در شرایط عادی و همچنین رفتار آن در زمان وقوع حملات DDoS به‌خوبی شناخته شود. مدل ارائه‌شده در این مقاله بر اساس ویژگی‌های واقعی شبکه‌های SDN توسعه یافته است؛ بنابراین، پارامترهایی مانند ظرفیت پردازشی کنترلرها، پهنای باند لینک‌ها، تأخیر ارتباطی و شدت حمله، همگی بر مبنای رفتار واقعی شبکه در نظر گرفته شده‌اند. در این بخش، ابتدا نحوه وقوع حملات DDoS در معماری SDN تشریح می‌شود، سپس مسیر انتشار این حملات در بخش‌های مختلف شبکه بررسی خواهد شد. در پایان نیز تفاوت عملکرد کنترلرهای ساده و هوشمند و نقش هر یک در افزایش پایداری شبکه توضیح داده می‌شود. آشنایی با این مفاهیم، درک بهتری از محدودیت‌ها و روابط ریاضی ارائه‌شده در بخش بعد فراهم می‌کند.

جدول ۱. جدول مقایسه تطبیقی مدل پیشنهادی با مدل‌های شاخص پیشین

مدل / مرجع پژوهشی	نوع مدل بهینه‌سازی	مدل‌سازی چندسطحی شدت حمله DDoS	استقرار دوگانه و ناهمگون کنترلرها	بهینه‌سازی همبندی مش لایه کنترل	لحاظ همزمان قیود پورت، پهنای باند و تأخیر صف	رویکرد اقتصادی- امنیتی (CapEx vs. QoS)
هوک و همکاران [8] (ITC)	چندهدفه پارتو	بدون حمله	کنترلر همگن	فقط تأخیر	فقط ظرفیت ساده	✗
هو و همکاران [11] (China Comm.)	برنامه‌ریزی خطی	خرابی تصادفی	پشتیبان غیرفعال همگن	✗	فقط تأخیر انتشار	✗
طاهریان‌فرد و همکاران (IEEE Access) [13]	عدد صحیح مختلط	آسیب‌پذیری باینری	کنترلر یکسان	✗	بدون تأخیر صف	محدود
کاله و همکاران [16] (IJCP)	برنامه‌ریزی خطی	حملات گسسته هدفمند	پشتیبان همگن	لینک‌های ساده	بدون قید پورت	✗
یانگ و همکاران [18] (IEEE TNSM)	بهینه‌سازی مقاوم	محدود به مسیریابی امن	تک کنترلی	✗	فقط تأخیر انتشار	فقط هزینه کنترلر
مدل پیشنهادی (این پژوهش)	برنامه‌ریزی خطی عدد صحیح مختلط (MILP)	چندسطحی DDoSN : ϵ [0,7]	ترکیب ناهمگون ساده و هوشمند	همبندی مش با لینک‌های چندگانه	قیود جامع پورت، پهنای باند و کران بالای صف	موازنه دقیق هزینه استقرار و تاب‌آوری

شناخت عمیق این مفاهیم، بنیان نظری و توجیه فنی لازم برای درک چرایی و چگونگی تعریف پارامترهای ظرفیتی، پهنای باند و تأخیر صف را در محدودیت‌های مدل ریاضی (رابطه‌های بیان شده در بخش چهارم) فراهم می‌آورد. این مقدمه برای مخاطب روشن می‌سازد که هر یک از قیود ریاضی پیشنهادی، پاسخگوی کدام نیاز فیزیکی و امنیتی در یک شبکه واقعیِ تحت حمله است.

۳-۱- یکپارچه‌سازی و تعریف اصطلاحات کلیدی

به منظور حفظ یکپارچگی مفهومی و جلوگیری از هرگونه ابهام نگارشی و اصطلاحات در بخش‌های مختلف مقاله، تعاریف عملیاتی اصطلاحات تخصصی مورد استفاده در این پژوهش در ادامه زیر خلاصه شده است. در تمام بخش‌های بعدی مقاله، فرمول‌بندی ریاضی و تحلیل سناریوها، این واژگان صرفاً با همین تعاریف ثابت به کار رفته‌اند.

کنترلر ساده[۱۱] **(پیش‌فرض)**: کنترلر اصلی و استاندارد SDN که برای مدیریت ترافیک عادی شبکه با هزینه استقرار پایین (Coc) و توان پردازشی پایه (prp_c) طراحی شده است.

کنترلر هوشمند پشتیبان[۱۲]: کنترلر پشتیبان فعال با ظرفیت پردازشی و پورت بسیار بالا (prp_{sc}, $Port_{sc}$) که به ماژول‌های دفاعی و مدیریت انتقال سوئیچ مجهز بوده و در زمان حمله فعال می‌شود.

پشتیبان فعال[۱۳]: ساختاری که در آن کنترلرهای هوشمند پشتیبان از قبل در حالت روشن و آماده‌به‌کار (Hot-Standby) قرار داشته و بدون تأخیر بوت، آماده جذب بار هستند.

مهاجرت پویا[۱۴] **(انتقال سوئیچ)**: فرآیند استاندارد OpenFlow برای انتقال برخط و بلادرنگ مدیریت سوئیچ‌های تحت حمله از کنترلر ساده به کنترلر هوشمند بدون قطعی سرویس.

پارامتر شدت حمله[۱۵]: پارامتر ریاضی بدون بعد در بازه $[0, 7]$ در مدل بهینه‌سازی که مقیاس ضریب افزایش بار ترافیکی حمله در گره nرا تعیین می‌کند.

سطح و نرخ ترافیک حمله[۱۶]: کمیت فیزیکی ترافیک حمله بر حسب بسته در ثانیه که بار ترافیکی واقعی ناشی از بات‌نت را مشخص می‌کند.

۳-۲- حملات DDoS در شبکه‌های SDN

یکی از مهم‌ترین ویژگی‌های شبکه‌های مبتنی بر نرم‌افزار، متمرکز بودن تصمیم‌گیری در لایه کنترل است. درواقع در این نوع شبکه‌ها، تصمیم‌گیری و مدیریت ترافیک توسط کنترلر انجام می‌شود. این تمرکز مدیریت، اگرچه باعث ساده‌تر شدن کنترل شبکه و افزایش انعطاف‌پذیری آن می‌شود، اما کنترلر را به یکی از مهم‌ترین اهداف حملات سایبری تبدیل می‌کند. به گونه‌ای که از کار افتادن آن می‌تواند عملکرد بخش بزرگی از شبکه را مختل کند. به همین دلیل، امنیت لایه کنترل یکی از مهم‌ترین چالش‌های شبکه‌های SDN به شمار می‌رود [۱۹].

در شبکه‌های سنتی، بخش زیادی از پردازش ترافیک در همان تجهیزات شبکه انجام می‌شود، اما در معماری SDN هرگاه یک سوئیچ با جریانی روبه‌رو شود که قانون متناظر آن در جدول جریان[۱۷] وجود نداشته باشد، اطلاعات مربوط به آن را برای تصمیم‌گیری به کنترلر ارسال می‌کند. همین ویژگی، زمینه را برای سوءاستفاده مهاجمان فراهم می‌کند [۲۰].

در حملات DDoS، مهاجم از تعداد زیادی رایانه یا تجهیزات آلوده که به آن‌ها بوت‌نت[۱۸] گفته می‌شود، برای ارسال حجم بسیار زیادی از بسته‌های داده به سمت شبکه استفاده می‌کند. هدف اصلی این حملات، درگیر نمودن منابع پردازشی و ارتباطی شبکه و جلوگیری از ارائه سرویس به کاربران مجاز است. زمانی که بسته‌های حمله وارد سوئیچ‌های شبکه می‌شوند، سوئیچ ابتدا جدول جریان خود را بررسی می‌کند. اگر برای بسته دریافتی قانونی وجود نداشته باشد، رویدادی به نام عدم تطابق با جدول جریان[۱۹] رخ می‌دهد. در این شرایط، سوئیچ مطابق پروتکل OpenFlow، پیام Packet-In را برای کنترلر ارسال می‌کند تا درباره نحوه پردازش آن تصمیم‌گیری شود [۲۱]. در شرایط عادی، تعداد این پیام‌ها محدود است و کنترلر به‌راحتی آن‌ها را پردازش می‌کند. اما هنگام وقوع حمله DDoS، تعداد بسیار زیادی پیام Packet-In به طور هم‌زمان تولید می‌شود. این موضوع باعث افزایش شدید استفاده از پردازنده، حافظه و پهنای باند کنترلر شده و در نتیجه صف پردازش درخواست‌ها به سرعت طولانی می‌شود. ادامه این وضعیت می‌تواند موجب افزایش زمان پاسخ، کاهش کیفیت سرویس و در نهایت از کار افتادن کنترلر شود.

پردازش هر پیام Packet-In در لایه کنترل مستلزم تخصیص بافر حافظه (RAM) در کنترلر، مصرف چرخه‌های پردازشی پردازنده (CPU) جهت محاسبه مسیر و در نهایت تولید و ارسال پیام‌های متناظر Packet-Out یا Flow-Mod به سوئیچ است. در حین یک حمله شدید، نرخ تولید این پیام‌ها به طور نمایی فراتر از قدرت پردازشی اسمی کنترلر ساده (prp_c) می‌رود. این پدیده منجر به اشباع ناگهانی حافظه موقت کنترلر، طولانی شدن صف‌های

پردازش (که فیزیک حاکم بر محدودیت‌های تاخیر مدل در بخش ۴-۳ است) و در نهایت خفگی کامل لایه کنترل می‌گردد. به همین دلیل، در مدل ریاضی پیشنهادی شدت حمله با پارامتر $DDoS_N$ نمایش داده می‌شود تا تصمیم‌گیری درباره نحوه استقرار کنترلرهای پشتیبان بر اساس شرایط واقعی شبکه انجام گیرد.

۳-۳- مسیر انتشار حملات DDoS در معماری SDN

برای طراحی یک مدل مقاوم در برابر حملات، لازم است مشخص شود که بسته‌های مخرب چگونه در شبکه منتشر می‌شوند و کدام بخش‌های شبکه بیشترین تأثیر را از حمله می‌پذیرند. به طور کلی، انتشار حملات DDoS (موسوم به DAP) در معماری SDN در سه مرحله انجام می‌شود که مبنای فیزیکی محدودیت‌های سخت‌افزاری مدل در بخش ۴ را تشکیل می‌دهند [۲۲].

مرحله اول - لایه داده (لایه زیرساخت): در نخستین مرحله، بسته‌های مخرب وارد سوئیچ‌های شبکه می‌شوند. ازآنجاکه ظرفیت جدول جریان (TCAM) در سوئیچ محدود است، ورود تعداد زیاد جریان‌های جدید باعث پر شدن این جدول و افزایش تعداد پیام‌های Packet-In می‌شود. همچنین افزایش حجم ترافیک می‌تواند موجب اشباع لینک‌های ارتباطی و کاهش عملکرد شبکه شود. به همین دلیل، در مدل پیشنهادی محدودیت‌هایی برای کنترل ظرفیت لینک‌ها و جلوگیری از اشباع آن‌ها در نظر گرفته شده است.

مرحله دوم - واسط ارتباطی جنوبی (ارتباط میان سوئیچ و کنترلر): در مرحله بعد، پیام‌های Packet-In از طریق واسط جنوبی[۲۰] به کنترلر ارسال می‌شوند. با افزایش تعداد این پیام‌ها، حجم ترافیک روی کانال ارتباطی نیز افزایش یافته و تأخیر انتقال بسته‌ها بیشتر می‌شود. این گلوگاه فیزیکی، زمان انتقال بسته‌ها روی لینک را به شدت بالا برده و تأخیر کل شبکه را افزایش می‌دهد. ازآنجاکه کیفیت سرویس در شبکه‌های SDN به زمان پاسخ کنترلر وابسته است، مدل پیشنهادی محدودیت‌هایی برای کنترل مجموع تأخیر انتقال، تأخیر انتشار و زمان پردازش در نظر گرفته است تا زمان پاسخ از مقدار مجاز بیشتر نشود. این پدیده، اساس تعریف محدودیت‌های تأخیر سخت (۸) و (۹) در مدل پیشنهادی است تا همواره تأخیر کل از آستانه مجاز فراتر نرود.

مرحله سوم - لایه کنترل (واسط‌های شرقی–غربی): در شبکه‌هایی که از چند کنترلر استفاده می‌کنند، کنترلرها برای تبادل اطلاعات و هماهنگی وضعیت شبکه با یکدیگر ارتباط برقرار می‌کنند. پس از ورود بسته‌ها به کنترلر هدف، این کنترلر به منظور همگام‌سازی وضعیت شبکه، اطلاعات مربوطه را با سایر کنترلرهای همکار از طریق پروتکل‌های واسط شرقی-غربی تبادل می‌کند. اگر یکی از کنترلرها تحت حمله قرار گیرد، حجم بالای پیام‌های کنترلی می‌تواند از طریق این ارتباطات به سایر کنترلرها نیز منتقل شود و عملکرد کل لایه کنترل را تحت تأثیر قرار دهد. این تبادل اطلاعات نابجا در شرایط حمله، ترافیک مخرب را به سایر کنترلرهای سالم سرایت داده و کل لایه کنترل را فلج می‌کند. این تهدید جدی، ضرورت بهینه‌سازی هم‌زمان هزینه‌های لینک بین-کنترلی ($Cost_L(R)$) و ظرفیت سخت‌افزاری پورت‌ها (محدودیت های تعریف شده در بخش ۴-۲) را به منظور جلوگیری از جداافتادگی و گسستگی لایه کنترل تبیین می‌کند. به همین دلیل، مدل پیشنهادی علاوه بر تعیین محل استقرار کنترلرها، هزینه و ظرفیت لینک‌های بین کنترلرها را نیز در فرآیند بهینه‌سازی در نظر می‌گیرد تا ضمن حفظ ارتباط میان کنترلرها، احتمال انتشار اثر حمله در شبکه کاهش یابد.

۴-۳- کنترلرهای ساده و کنترلرهای هوشمند

برای افزایش پایداری شبکه در برابر حملات DDoS، در این مقاله از یک راهکار استقرار دوگانه (دو نوع کنترلر با قابلیت‌های متفاوت) استفاده شده است که شامل کنترلرهای ساده و کنترلرهای هوشمند است.

کنترلر ساده وظیفه مدیریت عادی شبکه را بر عهده دارد. این واحد به عنوان کنترلر اصلی و پیش‌فرض شبکه عمل می‌کند. ظرفیت پردازشی (prp_c) و تعداد پورت‌های ارتباطی ($Port_c$) این کنترلر بر اساس ترافیک معمول شبکه انتخاب می‌شود تا هزینه استقرار تجهیزات (Co_c) در حد مناسبی باقی بماند. استفاده از این کنترلر باعث می‌شود هزینه پیاده‌سازی شبکه در شرایط عادی تا حد امکان کاهش یابد.

در مقابل، کنترلر هوشمند به عنوان یک واحد پشتیبان فعال و مجهز به قابلیت‌های دفاع خودکار در شبکه مستقر می‌شود [۲۳]. این کنترلر علاوه بر وظایف مسیریابی عادی، مجهز به ماژول‌های امنیتی پیشرفته نظیر موتور تحلیل رفتار ترافیک و پروتکل هدایت پویای سوئیچ‌ها است. کنترلر هوشمند با مانیتورینگ مداوم وضعیت، به محض عبور نرخ پیام‌های ورودی از آستانه مجاز، فرآیند انتقال پویای سوئیچ‌های تحت حمله به سمت خود را مدیریت می‌کند. ازآنجاکه اجرای این الگوریتم‌های هوشمند امنیتی و پردازش همزمان مکانیزم‌های دفاعی، بار محاسباتی سنگینی را ایجاد می‌کند، این کنترلرها الزماً نیازمند توان پردازشی به مراتب بالاتر ($prp_{sc} \gg prp_c$)، پهنای باند ارتباطی بیشتر و تعداد

پورتهای فیزیکی بالاتری هستند تا از ایجاد گلوگاه‌های پردازشی در شرایط بحرانی جلوگیری شود. بنابراین، ویژگی هوشمندی نرم‌افزاری، علت اصلی نیاز به ظرفیت فیزیکی ارتقایافته در این نوع کنترلرها است. اگرچه هزینه استقرار آن بیشتر از کنترلر ساده است، اما در شرایط بحرانی و در زمان وقوع حملات DDoS می‌تواند حجم زیادی از ترافیک کنترلی را مدیریت کرده و از توقف سرویس جلوگیری کند. هزینه استقرار این کنترلر (Co_{sc}) بالاتر است، اما ظرفیت تحمل بار آن در شرایط بحران بی‌نظیر است. البته استفاده از این کنترلرها هزینه بیشتری به شبکه تحمیل می‌کند؛ بنابراین استقرار آن‌ها باید به صورت هدفمند و تنها در محل‌های ضروری انجام شود.

ضرورت استفاده هم‌زمان از دو نوع کنترلر: استفاده از کنترلرهای هوشمند در تمام نقاط شبکه اگرچه سطح امنیت را افزایش می‌دهد، اما هزینه پیاده‌سازی و نگهداری شبکه را به شدت افزایش خواهد داد. از سوی دیگر، استفاده صرف از کنترلرهای ساده نیز باعث می‌شود شبکه در برابر حملات DDoS آسیب‌پذیر باشد. به همین دلیل، مدل پیشنهادی از ترکیب این دو نوع کنترلر استفاده می‌کند. در شرایط عادی، بار اصلی شبکه توسط کنترلرهای ساده مدیریت می‌شود تا هزینه‌ها کاهش یابد. اما هرگاه شدت حمله در یک ناحیه افزایش پیدا کند، مدل با استفاده از پارامتر $DDoS_N$ و با در نظر گرفتن محدودیت‌های ظرفیت پردازشی، به صورت خودکار محل مناسب استقرار کنترلرهای هوشمند را تعیین می‌کند.

مدل ریاضی پیشنهادی با درک عمیق این موازنه[۲۱] اقتصادی-امنیتی و با رصد پارامتر شدت حمله ($DDoS_N$)، از طریق محدودیت‌های ظرفیت پردازشی (تعریف شده در بخش ۴) به طور بهینه تصمیم می‌گیرد که کدام گره‌ها مستحق دریافت کنترلر ساده و کدام مناطق استراتژیک نیازمند کنترلر هوشمند پشتیبان هستند. به طور کلی، در مدل پیشنهادی هنگام تشخیص حمله در هر گره $n\epsilon N$ و با توجه به شدت حمله $DDos_N$، کنترلر هوشمند متناظر به صورت خودکار فعال می‌شود. سپس با استفاده از فرآیند Switch Migration، مدیریت سوئیچ‌های متصل به کنترلر آسیب‌دیده را بر عهده می‌گیرد [۲۴]. به این ترتیب، این رویکرد تضمین می‌کند که فرآیند هدایت ترافیک کاربران قانونی بدون تأخیرهای ناشی از بازپیکربندی دستی، تداوم یابد و بدون نیاز به دخالت دستی، خدمات شبکه برای کاربران قانونی ادامه یافته و از اختلال گسترده در عملکرد شبکه جلوگیری می‌شود.

در مجموع، استفاده هم‌زمان از کنترلرهای ساده و هوشمند این امکان را فراهم می‌کند که میان هزینه استقرار تجهیزات و پایداری شبکه در برابر حملات DDoS تعادل مناسبی برقرار شود؛ موضوعی که یکی از ایده‌های اصلی مدل ریاضی پیشنهادی این پژوهش است.

۳-۵- معماری عملیاتی دو فازی (آفلاین/آنلاین) برای مقابله با پویایی حملات

با توجه به ماهیت پویا و تغییرات سریع حمالت DDoS در مقیاس ثانیه، اعمال مستقیم مدل ریاضی MILP به صورت آنلاین به دلیل زمان محاسباتی حل مدل غیرممکن است. بر این اساس، چارچوب پیشنهادی این مقاله در دو فاز مجزا کار می‌کند:
۱. فاز برنامه ریزی استراتژیک (آفلاین): در این فاز، با استفاده از سناریوهای آماری و پیش‌بینی‌های بلندمدت شدت حمله، مدل MILP حل شده و تعداد، نوع و مکان فیزیکی بهینه کنترلرهای ساده و هوشمند پشتیبان در شبکه مشخص و مستقر می‌شوند. این فاز پیش از وقوع حمله و در مرحله طراحی شبکه انجام می‌گیرد.
۲. فاز واکنش عملیاتی (آنلاین): در این فاز، به محض وقوع حمله و تشخیص آن توسط سیستم‌های IDS، مدل ریاضی مجدداً حل نمی‌شود؛ بلکه پروتکل انتقال پویای سوئیچ فعال شده و در مقیاس میلی‌ثانیه، سوئیچ‌های تحت حمله را به کنترلرهای هوشمند پشتیبانی که قبلاً در فاز آفلاین در بهترین نقاط شبکه نصب شده‌اند، متصل می‌کند.

همچنین برای مقابله با خطاهای احتمالی IDS و نوسانات ناگهانی ترافیک، ظرفیت پردازشی تجهیزات مستقر شده در فاز آفلاین، همواره با یک حاشیه امنیت مازاد در نظر گرفته می‌شود.

۴- مدل ریاضی پیشنهادی

مسئله مکان‌یابی کنترلرها در شبکه‌های مبتنی بر نرم‌افزار یکی از مهم‌ترین مسائل طراحی لایه کنترل است. این مسئله به علت تعداد زیاد حالت‌های ممکن به دلیل تعداد زیاد مکان‌های کاندید برای استقرار کنترلر، تنوع تجهیزات، محدودیت‌های فنی شبکه و وابستگی متقابل تصمیم‌ها، در رده مسائل **NP-hard** قرار می‌گیرد. ازاین‌رو، یافتن پاسخ بهینه برای آن، به‌ویژه در شبکه‌های واقعی، نیازمند استفاده از مدل‌های بهینه‌سازی دقیق است.

در این پژوهش، یک مدل برنامه‌ریزی خطی عدد صحیح مختلط ارائه شده است که مکان‌یابی کنترلرها را با در نظر گرفتن شرایط عادی شبکه و همچنین سناریوهای مختلف حملات DDoS به‌صورت هم‌زمان مدل‌سازی می‌کند. برخلاف بسیاری از مطالعات

پیشین که تنها یکی از اهداف کاهش هزینه یا افزایش تاب‌آوری را دنبال کرده‌اند، مدل پیشنهادی هر دو هدف را به صورت یکپارچه در فرآیند تصمیم‌گیری لحاظ می‌کند. در این مدل، مکان استقرار کنترلرهای ساده و هوشمند، نوع تجهیزات مورد استفاده، نحوه تخصیص سوئیچ‌ها به کنترلرها و همچنین ساختار ارتباطی میان کنترلرها به طور هم‌زمان تعیین می‌شود. علاوه بر این، محدودیت‌های فیزیکی و عملیاتی شبکه مانند ظرفیت پردازشی کنترلرها، ظرفیت پورت‌ها، پهنای باند لینک‌ها، تأخیر انتها به انتها و شدت حملات نیز در فرآیند بهینه‌سازی لحاظ شده‌اند تا راهکار نهایی علاوه بر اقتصادی بودن، از نظر عملکرد نیز قابل اجرا باشد.

به طور کلی، مدل ارائه‌شده سه هدف اصلی را دنبال می‌کند:

- کاهش هزینه استقرار تجهیزات و لینک‌های ارتباطی
- حفظ کیفیت سرویس و جلوگیری از افزایش تأخیر در لایه کنترل
- افزایش تاب‌آوری شبکه در برابر حملات DDoS از طریق استقرار هدفمند کنترلرهای هوشمند

در ادامه، اجزای مختلف مدل شامل مجموعه‌ها، پارامترها، متغیرهای تصمیم، تابع هدف و محدودیت‌های مدل معرفی می‌شوند.

۴-۱- تعاریف نمادها، پارامترها و متغیرهای تصمیم

برای فرمول‌بندی مدل، ابتدا لازم است مجموعه‌های مورد استفاده، پارامترهای ثابت و متغیرهای تصمیم تعریف شوند. این مؤلفه‌ها پایه اصلی روابط ریاضی مدل را تشکیل می‌دهند و نحوه نمایش عناصر مختلف شبکه را مشخص می‌کنند. در این بخش، مجموعه‌ها، پارامترهای ثابت و متغیرهای تصمیم مورد استفاده در مدل معرفی می‌شوند. این تعاریف، مبنای فرمول‌بندی مدل ریاضی و روابط بهینه‌سازی هستند.

الف) مجموعه‌های مدل

مجموعه‌های اصلی مورد استفاده در مدل عبارت‌اند از:

- مجموعه کنترلرهای هوشمند ($SC = \{sc1, sc2, sc3,...\}$): شامل انواع کنترلرهای پشتیبان با توان پردازشی بالا که در شرایط حمله مورد استفاده قرار می‌گیرند.
- مجموعه کنترلرهای ساده ($C = \{c1, c2, c3,...\}$): شامل کنترلرهایی که در شرایط عادی مدیریت شبکه را بر عهده دارند.
- مجموعه سوئیچ‌ها ($S = \{s1, s2, s3,...\}$): مجموعه سوئیچ‌های موجود در لایه داده که باید به یکی از کنترلرها متصل شوند.
- مجموعه لینک‌ها ($L = \{l1, l2, l3,...\}$): انواع لینک‌های ارتباطی با ظرفیت و هزینه‌های مختلف.
- مجموعه گره‌های کاندید ($N = \{1,2,3,4,5,6,7...\}$): مکان‌های قابل انتخاب برای استقرار کنترلرها در زیرساخت شبکه.

این مجموعه‌ها فضای جستجوی مسئله را مشخص کرده و تمامی تصمیم‌های مدل بر اساس آن‌ها انجام می‌شود.

ب) پارامترهای ثابت مدل

پارامترهای ثابت، ویژگی‌های فیزیکی و عملیاتی شبکه را مشخص می‌کنند و در طول فرآیند بهینه‌سازی تغییر نمی‌کنند. مهم‌ترین این پارامترها عبارت‌اند از:

- *Coc*: هزینه استقرار کنترلر ساده نوع c (بر حسب دلار).
- *Cosc*: هزینه استقرار کنترلر هوشمند نوع sc (بر حسب دلار)
- *Col*: هزینه احداث هر متر از لینک ارتباطی نوع l (بر حسب دلار بر متر).
- $Range_{ab}$: فاصله فیزیکی و جغرافیایی بین دو گره a و b (بر حسب متر).
- *PacketSize*: میانگین اندازه بسته‌های کنترلی تبادلی در لایه کنترل (بر حسب بایت Byte).
- *SpeedLight*: سرعت انتشار سیگنال در محیط انتقال (۲۹۹،۷۹۲،۴۵۸ متر بر ثانیه m/s).
- *BW_l*: ظرفیت پهنای باند لینک ارتباط ی نوع l (بر حسب بایت در ثانیه Byte/s).
- Prp_c: توان پردازش اسمی کنترلر ساده نوع c (بر حسب بسته در ثانیه pps).
- prp_{sc}: توان پردازش اسمی کنترلر هوشمند نوع sc (بر حسب بسته در ثانیه pps).
- $Port_c$: تعداد پورت‌های سخت‌افزاری کنترلر ساده نوع c (تعداد پورت).
- $Port_{sc}$: تعداد پورت‌های سخت‌افزاری کنترلر هوشمند نوع sc.
- Avl_s: نرخ تولید بسته‌های کنترلی سوئیچ s در شرایط عادی

(بر حسب بسته در ثانیه pps).

- Avl_c: تعداد موجودی در انبار از کنترلر ساده نوع c بر حسب عدد Unit).
- Avl_{sc}: تعداد موجودی در انبار از کنترلر هوشمند نوع sc.
- $Proc_{TCandSC}$: بیشینه تأخیر پردازش و صف کنترلر در بدترین حالت بارگذاری (بر حسب ثانیه s).
- $MaxLatency$: حداکثر تأخیر مجاز انتها به انتها در مسیر سوئیچ تا کنترلر (بر حسب ثانیه s).
- $DDoS_N$: پارامتر شدت حمله DDoS در گره n (بدون بعد، در بازه $[0, 7]$).
- λ_n^A: نرخ ترافیک فیزیکی حمله DDoS تحمیل‌شده به گره n (بر حسب بسته در ثانیه pps)

همانطور که بیان شد، مقدار پارامتر $DDoS_N$ در بازه $[۰،۷]$ تعریف می‌شود. برای برقراری ارتباط میان این مقیاس ریاضی و کمیت‌های فیزیکی در یک شبکه واقعی، هر سطح از پارامتر DDoSN معادل با گام‌های مشخصی از نرخ تولید پیام‌های مخرب Packet-In در ثانیه (pps) در نظر گرفته می‌شود. بر این اساس، نرخ فیزیکی ترافیک حمله در گره n از رابطه ($\lambda_n^A = DDoSN * \alpha$) محاسبه می‌شود، که در آن $\alpha = 2000\ pps$ به عنوان گام ترافیکی مبنا تعیین شده است. این معادل‌سازی خطی به مدل ریاضی اجازه می‌دهد تا بار پردازشی ناشی از حمله را مستقیماً با ظرفیت پردازشی اسمی کنترلرهای ساده (prp_c) و هوشمند (prp_{sc}) در محدودیت‌های ظرفیت (رابطه‌های ۱۷ و ۱۸) مقایسه نموده و تصمیم بهینه را اتخاذ کند. به عنوان مثال، در شدیدترین حالت ($DDoSN=7$)، ترافیک حمله معادل 14,000 pps خواهد بود که از ظرفیت پردازش قوی‌ترین کنترلر ساده موجود در بازار (۱۳،۰۰۰ بسته در ثانیه طبق جدول (۲)) فراتر رفته و عملاً مدل را ملزم به استقرار کنترلرهای هوشمند پشتیبان با ظرفیت ۱۶،۰۰۰ بسته در ثانیه می‌نماید.

در این پژوهش، برخلاف بسیاری از مدل‌های پیشین که تنها وجود یا عدم وجود حمله را در نظر می‌گیرند، شدت حمله به صورت یک پارامتر چندسطحی مدل‌سازی شده است. این ویژگی باعث می‌شود مدل بتواند متناسب با شرایط واقعی شبکه درباره نوع و تعداد کنترلرهای پشتیبان تصمیم‌گیری کند.

در مدل ریاضی پیشنهادی، پارامتر شدت حمله در هر گره به عنوان یک ورودی پویا در نظر گرفته می‌شود. فرآیند تعیین این پارامتر مبتنی بر یک سیستم مانیتورینگ ترافیک توزیع‌شده و سیستم تشخیص نفوذ (IDS) مستقر در لایه داده است. این سیستم حفاظتی با پایش مداوم نرخ پیام‌های کنترلی Packet-In و تحلیل آماری معیارهایی نظیر آنتروپی آدرس‌های IP مبدأ، شدت حمله را به صورت بلادرنگ تخمین می‌زند. سپس، مدل ریاضی بهینه‌سازی به صورت دوره‌ای یا بر اساس رویدادهای تحریک‌کننده پس از عبور ترافیک از آستانه‌های بحرانی مجدداً اجرا شده و لایه کنترل را به طور پویا بازپیکربندی می‌کند.

ج) متغیرهای تصمیم

مدل پیشنهادی از متغیرهای تصمیم باینری برای تعیین ساختار بهینه شبکه استفاده می‌کند. این متغیرها عبارت‌اند از:

- متغیر استقرار کنترلر ساده

$$T_{cn} \in \{0.\ 1\}$$

اگر کنترلر ساده نوع c در گره n نصب شود مقدار آن برابر ۱ و در غیر این صورت برابر صفر خواهد بود.

- متغیر استقرار کنترلر هوشمند

$$T_{scn} \in \{0.\ 1\}$$

در صورت استقرار کنترلر هوشمند نوع sc در گره n مقدار آن برابر ۱ خواهد بود.

- متغیر تخصیص سوئیچ به کنترلر

$$Z_{lsn} \in \{0.\ 1\}$$

اگر سوئیچ s از طریق لینک نوع l به کنترلر مستقر در گره n متصل شود مقدار آن برابر ۱ خواهد بود.

- متغیر اتصال بین کنترلرها

$$R_{lnm} \in \{0.\ 1\}$$

اگر میان دو کنترلر مستقر در گره‌های n و m لینک ارتباطی نوع l برقرار شود مقدار این متغیر برابر ۱ خواهد بود.

- متغیر کمکی خطی‌سازی

$$Y_{c.sc.n} \in \{0.\ 1\}$$

این متغیر برای خطی‌سازی برخی قیود استفاده می‌شود و بیانگر استقرار هم‌زمان کنترلر ساده و کنترلر هوشمند در یک گره است. استفاده از این متغیر موجب می‌شود مدل همچنان در قالب **MILP** باقی بماند و توسط حل‌کننده‌هایی مانند **CPLEX** با کارایی مناسب حل شود.

ساختار فوق، پایه ریاضی مدل پیشنهادی را تشکیل می‌دهد.

مجموعه‌ها فضای تصمیم را مشخص می‌کنند، پارامترها ویژگی‌های فیزیکی و عملیاتی شبکه را نمایش می‌دهند و متغیرهای تصمیم نیز نحوه استقرار کنترلرها، تخصیص سوئیچ‌ها و ایجاد ارتباط میان اجزای لایه کنترل را تعیین می‌کنند. بر مبنای این تعاریف، در بخش بعد تابع هدف و سپس محدودیت‌های مدل ارائه می‌شوند تا مسئله مکان‌یابی کنترلرها به صورت یک مدل MILP کامل فرمول‌بندی شود.

۴-۲- فرمول‌بندی تابع هزینه و تابع هدف

هدف مدل پیشنهادی، کمینه‌سازی هزینه کل استقرار لایه کنترل شبکه است. این هزینه شامل هزینه خرید و نصب کنترلرها و همچنین هزینه ایجاد لینک‌های ارتباطی میان اجزای مختلف شبکه است. به بیان دیگر، مدل تلاش می‌کند ضمن حفظ عملکرد مناسب شبکه در شرایط عادی و هنگام وقوع حملات DDoS، کم‌هزینه‌ترین ساختار ممکن را برای لایه کنترل انتخاب کند. هزینه کل مدل از چهار بخش اصلی تشکیل شده است:

۱. هزینه استقرار کنترلرهای ساده ($Cost_c$): این بخش، هزینه خرید و نصب کنترلرهای ساده را محاسبه می‌کند. مقدار این هزینه به تعداد کنترلرهای مستقر و نوع آن‌ها بستگی دارد و به صورت زیر (رابطه (۱)) محاسبه می‌شود:

$$Cost_c(T_c) = \sum_{c \in C} Co_c \sum_{n \in N} T_c n \qquad (۱)$$

که در آن، Co_c هزینه استقرار کنترلر ساده از نوع c و $T_c n$ متغیر تصمیم مربوط به استقرار آن در گره n است.

۲. هزینه استقرار کنترلرهای هوشمند ($Cost_{sc}$): این بخش، هزینه مربوط به کنترلرهای هوشمند را محاسبه می‌کند. ازآنجاکه این کنترلرها از توان پردازشی و امکانات سخت‌افزاری بیشتری برخوردار هستند، هزینه استقرار آن‌ها معمولاً بیشتر از کنترلرهای ساده است. (رابطه (۲))

$$Cost_{sc}(T_{sc}) = \sum_{sc \in SC} Co_{sc} \sum_{n \in N} T_{sc} n \qquad (۲)$$

که در آن، Co_{sc} هزینه استقرار کنترلر هوشمند از نوع sc را نشان می‌دهد.

۳. هزینه لینک‌های ارتباطی بین سوئیچ و کنترلر ($Cost_L(Z)$): این بخش، هزینه ایجاد لینک‌های ارتباطی (رابطه (۳)) میان سوئیچ‌ها و کنترلرها را محاسبه می‌کند. این هزینه به نوع لینک انتخاب‌شده و فاصله فیزیکی میان سوئیچ و کنترلر بستگی دارد.

$$Cost_L(Z) = \sum_{l \in L} Co_l \sum_{s \in S} \sum_{n \in N} Range_{sn} Z_l sn \qquad (۳)$$

در این رابطه، Co_l هزینه هر واحد از لینک نوع l و $Range_{sn}$ فاصله بین سوئیچ s و کنترلر مستقر در گره n را نشان می‌دهد.

۴. هزینه لینک‌های ارتباطی بین کنترلرها ($Cost_L(R)$): برای تبادل اطلاعات و هماهنگی میان کنترلرها، لازم است لینک‌های ارتباطی بین آن‌ها نیز ایجاد شود. رابطه (۴) نحوه محاسبه هزینه لینک های ارتباطی را نشان میدهد. هزینه این بخش بر اساس نوع لینک و فاصله میان گره‌های میزبان کنترلرها محاسبه می‌شود.

$$Cost_L(R) = \sum_{l \in L} Co_l \sum_{m \in N} \sum_{\substack{m \in N \\ m<n}} Range_{mn} R_l nm \qquad (۴)$$

که در آن، $R_l nm$ نشان می‌دهد آیا لینک نوع l بین کنترلرهای مستقر در گره‌های m و n برقرار شده است یا خیر.

تابع هدف نهایی:

پس از محاسبه چهار مؤلفه فوق، تابع هدف مدل به صورت مجموع آن‌ها تعریف می‌شود. هدف مدل، یافتن پیکربندی‌ای است که این هزینه کل را حداقل کند. (رابطه (۵))

$$Minimize: Cost_c(T_c) + Cost_{sc}(T_{sc}) + Cost_L(Z) + Cost_L(R) \qquad (۵)$$

در نتیجه، مدل پیشنهادی به صورت هم‌زمان تعداد، نوع و محل استقرار کنترلرها و همچنین ساختار لینک‌های ارتباطی را به گونه‌ای تعیین می‌کند که علاوه بر کاهش هزینه‌های استقرار، پایداری و قابلیت سرویس‌دهی شبکه در شرایط مختلف، به‌ویژه هنگام وقوع حملاتDDoS ، حفظ شود.

شایان ذکر است که تابع هدف (رابطه (۵)) بر بهینه‌سازی هزینه‌های سرمایه‌ای استقرار زیرساخت[۲۲] شامل خرید کنترلرها و ایجاد لینک‌های ارتباطی تمرکز دارد. فرآیند مهاجرت سوئیچ‌ها در زمان حمله، یک پدیده گذرا و کوتاه‌مدت است؛ ازاین‌رو، هزینه‌های سربار پروتکلی آن مستقیماً وارد تابع هدف استاتیک نشده است. با این وجود، زیرساخت ارتباطی لازم برای تبادل پیام‌های هماهنگ‌سازی مهاجرت (نظیر پیام‌های واسط شرقی-غربی OpenFlow)، از طریق تخصیص لینک‌های بین‌کنترلری ($Cost_L(R)$) و قیود ظرفیت پورت‌ها (رابطه (۱۵)) به طور کامل در مدل تضمین و لحاظ گردیده است. همچنین، توان پردازشی مازاد کنترلرهای هوشمند (prp_{sc}) و قیود محدودکننده تأخیر (روابط (۸) و (۹)) مانع از بروز اختلال یا تأخیر غیرمجاز در کیفیت سرویس شبکه حین فرآیند مهاجرت می‌شوند.

۴-۳- محدودیت‌های مدل

تابع هدف به تنهایی برای دستیابی به یک راه‌حل عملی کافی نیست. به همین دلیل، مجموعه‌ای از محدودیت‌ها در مدل در نظر گرفته شده است تا اطمینان حاصل شود که پاسخ نهایی علاوه بر کمینه بودن هزینه، از نظر فنی نیز قابل اجرا بوده و بتواند عملکرد پایدار شبکه را در شرایط عادی و همچنین هنگام وقوع حملات DDoS حفظ کند. این محدودیت‌ها جنبه‌های مختلف طراحی شبکه، از جمله استقرار کنترلرها، تأخیر، ظرفیت تجهیزات و ساختار ارتباطات را پوشش می‌دهند.

الف) محدودیت‌های مرتبط با حملات DDoS:

در مدل پیشنهادی، شدت حمله یکی از عوامل اصلی در فرآیند تصمیم‌گیری است. برخلاف بسیاری از مدل‌های موجود که تنها وجود یا عدم وجود حمله را در نظر می‌گیرند، در این پژوهش شدت حمله نیز در تعیین نوع کنترلرهای مورد استفاده نقش دارد. محدودیت (۶) تضمین می‌کند که به ازای وقوع حمله با شدت DDoSN در گره‌های دارای کنترلر ساده فعال ($T_{cn}=1$)، تعداد کنترلرهای هوشمند پشتیبان مستقرشده در سطح شبکه (در میان گره‌های کاندید ($m \epsilon N$) متناسب با مقیاس تهدید افزایش یابد تا توان مقابله با بار حمله در شبکه فراهم گردد.

$$\sum_{m\in N}\sum_{sc\in SC} T_{sc.m} \geq \sum_{n\in N}\left(DDoSN * \sum_{c\in C} T_{cn}\right) \quad \forall n \in N \qquad (۶)$$

شایان ذکر است که محدودیت (۱۲) همچنان تضمین می‌نماید که در هر گره کاندید مجزا، حداکثر یک کنترلر مستقر شود و کنترلرهای هوشمند در گره‌های مختلف شبکه توزیع گردند.

در مقابل، محدودیت (۷) از استقرار غیرضروری کنترلرهای هوشمند جلوگیری می‌کند. ازآنجاکه این کنترلرها هزینه بیشتری نسبت به کنترلرهای ساده دارند، تنها در گره‌هایی فعال می‌شوند که احتمال وقوع حمله یا شدت تهدید در آن‌ها قابل توجه باشد. این موضوع علاوه بر کاهش هزینه‌ها، باعث استفاده بهینه از منابع سخت‌افزاری نیز می‌شود. محدودیت (۷) به عنوان یک قید مسدودساز صریح عمل کرده و از استقرار کنترلرهای هوشمند در گره‌های فاقد تهدید جلوگیری می‌کند.

$$\sum_{sc\in SC} T_{sc.n} \leq DDoSN \qquad \forall n \in N \qquad (۷)$$

عملکرد این قید به این صورت است که در شرایط عادی ($DDoSN=0$)، رابطه به صورت $\sum T_{sc.n} \leq 0$ تبدیل شده و به طور قطعی نصب هرگونه کنترلر هوشمند را در گره n ناممکن می‌سازد ($T_{sc.n} = 0$). در هنگام بروز حمله ($DDoSN \geq 1$)، این کران بالا آزاد شده و به مدل اجازه می‌دهد تا متناسب با ظرفیت مورد نیاز، کنترلر هوشمند را فعال کند. علاوه بر تابع هدف، وجود این قید خطی صریح، فضای جستجوی شاخه و کران حل‌کننده CPLEX را به شدت محدود کرده و زمان همگرایی را کاهش می‌دهد.

ب) محدودیت‌های تأخیر ارتباطی:

یکی از مهم‌ترین معیارهای کیفیت سرویس در شبکه‌های SDN، تأخیر بین سوئیچ و کنترلر است. در زمان وقوع حملات DDoS، افزایش حجم ترافیک باعث طولانی شدن صف پردازش در کنترلر و افزایش زمان پاسخ می‌شود. بنابراین، لازم است مجموع تأخیرهای موجود در مسیر ارتباطی (شامل تأخیر انتشار فیزیکی، تأخیر انتقال روی لینک و تأخیر صف پردازش کنترلر) از مقدار مجاز بیشتر نشود.

محدودیت‌های (۸) و (۹) این شرط را برای کنترلرهای هوشمند و کنترلرهای ساده اعمال می‌کنند. در این روابط، تأخیر کل از سه بخش تشکیل شده است: تأخیر انتقال بسته روی لینک ارتباطی، تأخیر انتشار سیگنال که به فاصله فیزیکی وابسته است، و تأخیر پردازش و انتظار در کنترلر. مجموع این سه مؤلفه باید همواره کمتر از حداکثر تأخیر مجاز شبکه ($MaxLatency$) باشد.

$$\frac{2Packet_{Size}}{Bw_l} Z_l sn + \sum_{sc\in SC} \frac{2Range_{SN}}{t} T_{sc}n + Avl_S T_{sc}n \leq Max_{Latency} \qquad (۸)$$

$$\frac{2Packet_{Size}}{Bw_l} Z_l sn + \sum_{sc\in SC} \frac{2Range_{SN}}{t} T_{c}n + Avl_S T_{c}n \leq Max_{Latency} \qquad (۹)$$

که در آن $s \in S, sc \in SC, n \in N, l \in L$ میباشد.

توجیه تئوریک تأخیر پردازش و صف: در تئوری صف (نظیر مدل M/M/1)، تأخیر صف‌بندی تابعی غیرخطی از نرخ ورود درخواست‌ها (λ) و نرخ پردازش کنترلر (μ) است ($W_q = \frac{\lambda}{\mu(\mu-\lambda)}$). به منظور حفظ ساختار خطی مدل MILP و اجتناب از پیچیدگی‌های غیرخطی MINLP، در این پژوهش از رویکرد کران بالای بدترین حالت[۲۳] استفاده شده است. با توجه به اینکه قیود ظرفیت پردازشی (روابط ۱۷ و ۱۸) مانع از رسیدن نرخ ترافیک به نقطه اشباع قطعی کنترلر می‌شوند ($\lambda \leq \rho_{max} * prp$)، حداکثر تأخیر صف ممکن در بدترین شرایط بارگذاری از رابطه ($D_{queue}^{max} = \frac{1}{\mu(1-\rho_{max})}$) محاسبه شده و در قالب پارامتر $ProcTCandSC$ لحاظ

گردیده است. ازآنجاکه تأخیر واقعی صف همواره کوچکتر از این کران محافظه‌کارانه است ($D_{actual} \leq D_{queue}^{max}$)، ارضای محدودیت (۸) و (۹) تضمین ریاضی قطعی می‌دهد که تأخیر کل شبکه در هنگام وقوع حملات شدید نیز هرگز از سقف کیفی *MaxLatency* تجاوز نخواهد کرد.

ج) محدودیت‌های استقرار کنترلرها:

به دلیل محدود بودن تجهیزات موجود، تعداد کنترلرهایی که می‌توان در شبکه نصب کرد محدود است. محدودیت‌های (۱۰) و (۱۱) تضمین می‌کنند که تعداد کنترلرهای هوشمند و ساده انتخاب‌شده از تعداد تجهیزات موجود بیشتر نباشد.

$$\sum_{sc \in SC} T_{sc} n \leq Avl_{sc}, \quad sc \in SC \qquad (۱۰)$$

$$\sum_{c \in C} T_c n \leq Avl_c, \quad c \in C \qquad (۱۱)$$

همچنین، محدودیت (۱۲) بیان می‌کند که در هر گره کاندید، حداکثر یک کنترلر نصب شود. این محدودیت از استقرار هم‌زمان چند کنترلر در یک محل جلوگیری کرده و موجب توزیع مناسب منابع در سطح شبکه می‌شود.

$$\sum_{c \in C} T_c n \leq 1, \quad n \in N \qquad (۱۲)$$

د) محدودیت‌های ساختار شبکه و اتصال سوئیچ‌ها:

برای جلوگیری از بروز ناهماهنگی در مدیریت شبکه، هر سوئیچ باید تنها به یک کنترلر متصل باشد. محدودیت (۱۳) این شرط را برقرار می‌کند و از تخصیص هم‌زمان یک سوئیچ به چند کنترلر جلوگیری می‌کند.

$$\sum_{l \in L} \sum_{n \in N} Z_l sn = 1, \quad s \in S \qquad (۱۳)$$

علاوه بر این، کنترلرهای مستقر باید بتوانند با یکدیگر ارتباط برقرار کنند تا اطلاعات مدیریتی و وضعیت شبکه را تبادل کنند. محدودیت (۱۴) اتصال مناسب میان کنترلرهای فعال را تضمین کرده و از ایجاد بخش‌های جداافتاده در لایه کنترل جلوگیری می‌کند.

$$\sum_{c \in C} T_c m \sum_{c \in C} T_s n \leq \sum_{l \in L} R_l nm + 1, \ n \in N, m \in N, m \succ n \qquad (۱۴)$$

محدودیت (۱۴) به همراه متغیرهای ماتریس ارتباطی R_{lnm}، یک همبندی مش مستقیم میان کنترلرهای ساده فعال و کنترلرهای هوشمند پشتیبان ایجاد می‌کنند. در این ساختار، به ازای استقرار K کنترلر فعال در شبکه، یک گراف همبند با درجه اتصال (K-1) تشکیل می‌شود که فاقد نقطه تکی خرابی (SPoF) بوده و مسیرهای ارتباطی چندگانه و با پهنای باند اختصاصی را میان کنترلرها فراهم می‌سازد. این همبندی مش در ترکیب با قیدهای تضمین ظرفیت پشتیبان (قیود ۶ و ۱۸) و قیود تضمین سقف تأخیر (قیود ۸ و ۹)، تاب‌آوری کامل لایه کنترل را در برابر اشباع پردازشی و قطع پیوندهای ارتباطی تضمین می‌نماید.

هـ) محدودیت‌های ظرفیت تجهیزات:

کنترلرها علاوه بر محدودیت پردازشی، از نظر تعداد پورت‌های ارتباطی نیز دارای ظرفیت مشخصی هستند. محدودیت (۱۵) تضمین می‌کند که مجموع ارتباطات ورودی هر کنترلر، شامل اتصال سوئیچ‌ها و لینک‌های بین‌کنترلری، از ظرفیت پورت‌های آن بیشتر نشود.

$$\sum_{m \in M} \sum_{l \in L} (R_l nm + R_l mn) + \sum_{s \in S} \sum_{l \in l} Z_l sn \leq \sum_{c \in C} Avl_c T_c n \qquad (۱۵)$$

محدودیت (۱۶) نیز از اشباع لینک‌های ارتباطی جلوگیری می‌کند. بر اساس این رابطه، حجم کل ترافیک عبوری از هر لینک نباید از ظرفیت پهنای باند آن بیشتر شود.

$$Avl_s Packet_{size} \leq \sum_{c \in C} Function_{byte} Bw_l \, Z_l sn \qquad (۱۶)$$

در نهایت، محدودیت‌های (۱۷) و (۱۸) ظرفیت پردازشی کنترلرهای ساده و هوشمند را کنترل می‌کنند. این روابط تضمین می‌کنند که نرخ ورود بسته‌های کنترلی از مجموع توان پردازشی کنترلر مستقر بیشتر نباشد. رعایت این شرط از ایجاد گلوگاه پردازشی و افزایش شدید تأخیر در لایه کنترل جلوگیری می‌کند.

$$\sum_{l \in L} \sum_{s \in S} Avl_s Z_l sn \leq \sum_{c \in C} prp_c T_c n \qquad (۱۷)$$

$$\sum_{l \in L} \sum_{s \in S} Avl_s Z_l sn \leq \sum_{c \in C} prp_{sc} T_{sc} n \qquad (۱۸)$$

مجموعه محدودیت‌های فوق، چارچوب عملیاتی مدل پیشنهادی را تشکیل می‌دهد. این محدودیت‌ها اطمینان می‌دهند که راه‌حل نهایی علاوه بر کمینه بودن هزینه، از نظر ظرفیت تجهیزات، ساختار ارتباطات، کیفیت سرویس و مقاومت در برابر حملات DDoS نیز قابل اجرا باشد. در نتیجه، مدل قادر است پیکربندی مناسبی برای لایه کنترل شبکه SDN ارائه دهد که ضمن حفظ پایداری شبکه، استفاده بهینه‌ای از منابع سخت‌افزاری و ارتباطی

داشته باشد.

و) قیود خطی‌سازی متغیر کمکی Y:

متغیر باینری $Y_{c,sc,n}$ برای مدل‌سازی خطی عبارت غیرخطی ضرب استقرار همزمان کنترلر ساده و هوشمند در یک گره ($Y_{c,sc,n}=T_{cn}*T_{scn}$) استفاده می‌شود. به منظور حفظ ساختار خطی مدل MILP ، قیود استاندارد زیر در بهینه‌سازی اعمال می‌گردند:

$$Y_{c.sc.n} \leq T_{cn} \qquad \forall c \in C. sc \in SC. n \in N \qquad (۱۹)$$

$$Y_{c.sc.n} \leq T_{scn} \qquad \forall c \in C. sc \in SC. n \in N \qquad (۲۰)$$

$$Y_{c.sc.n} \geq T_{cn} + T_{scn} - 1 \qquad \forall c \in C. sc \in SC. n \in N \qquad (۲۱)$$

به طوری که $Y_{c.sc.n} \in \{0.1\}$. محدودیت های (۱۹) و (۲۰) تضمین می‌کنند که با صفر بودن هر یک از متغیرهای اصلی، مقدار $Y_{c.sc.n}$ صفر شود و محدودیت (۲۱) در صورت یک بودن همزمان هر دو متغیر، مقدار $Y_{c.sc.n}$ را برابر یک قرار می‌دهد.

۵- ارزیابی عملکرد و نتایج تجربی

در این بخش، عملکرد مدل پیشنهادی در شرایط مختلف مورد ارزیابی قرار می‌گیرد تا میزان کارایی آن در طراحی لایه کنترل شبکه‌های SDN بررسی شود. هدف از این ارزیابی، سنجش توانایی مدل در انتخاب محل مناسب کنترلرها، حفظ کیفیت سرویس و ادامه عملکرد شبکه در شرایط عادی و همچنین هنگام وقوع حملات DDoS است. علاوه بر این، نتایج شبیه‌سازی نشان می‌دهد که مدل از نظر زمان حل، هزینه استقرار و رعایت محدودیت‌های فنی نیز عملکرد قابل قبولی دارد.

۵-۱- محیط شبیه‌سازی و تنظیم پارامترها

مدل ریاضی پیشنهادی با استفاده از زبان مدل‌سازی AMPL پیاده‌سازی و توسط حل‌کننده IBM ILOG CPLEX نسخه ۱۲٫۸ حل شده است. این ابزارها از شناخته‌شده‌ترین محیط‌های مدل‌سازی و حل مسائل بهینه‌سازی هستند و در بسیاری از پژوهش‌های حوزه طراحی شبکه و برنامه‌ریزی ریاضی مورد استفاده قرار می‌گیرند.

تمامی آزمایش‌ها روی یک رایانه شخصی با مشخصات زیر انجام شده است: پردازنده Intel® Core™ i5-6500 (CPU) با فرکانس ۳٫۴۰GHz، حافظه اصلی 6GB (RAM)، و سیستم‌عامل Windows 10 Enterprise.

به منظور ارزیابی دقیق و واقعی‌گرایانه مدل ریاضی پیشنهادی، پارامترها و ویژگی‌های فیزیکی تجهیزات شبکه بر اساس مشخصات تجاری و صنعتی موجود در بازار تنظیم شده‌اند. بدین منظور، انواع مختلفی از کنترلرهای ساده، کنترلرهای هوشمند پشتیبان، لینک‌های ارتباطی و سوئیچ‌ها با ظرفیت‌ها و هزینه‌های متنوع تعریف شده‌اند تا توانایی مدل در بهینه‌سازی شبکه‌های ناهمگون[۲۴] سنجیده شود. مشخصات فنی و پارامترهای عددی مورد استفاده در شبیه‌سازی‌ها (شامل مشخصات کنترلرها، سوئیچ‌ها، لینک‌های ارتباطی و سایر پارامترهای عملیاتی شبکه) براساس مقادیر ارائه شده در جداول ۲ تا ۶ تنظیم شده‌اند. این پارامترها به گونه‌ای انتخاب شده‌اند که شرایط واقعی شبکه‌های مبتنی بر نرم‌افزار را تا حد امکان شبیه‌سازی کنند و امکان ارزیابی دقیق مدل را فراهم آورند.

جدول ۲. مشخصات فنی و هزینه‌ای انواع کنترلرهای ساده (C)

نوع کنترلر	تعداد پورت $Port_c$	قدرت پردازش prp_c (بسته در ثانیه)	هزینه استقرار Co_c (دلار)	موجودی انبار Avl_c
C1	۸	۲،۵۰۰	۱،۰۰۰	۲۰
C2	۳۲	۴،۰۰۰	۲،۰۰۰	۱۵
C3	۶۴	۸،۰۰۰	۴،۵۰۰	۱۰
C4	۱۶	۵،۵۰۰	۵،۰۰۰	۲۸
C5	۶۴	۶،۰۰۰	۷،۰۰۰	۱۹
C6	۱۲۸	۱۳،۰۰۰	۹،۵۰۰	۱۲
C7	۱۶	۵،۵۰۰	۵،۰۰۰	۲۸
C8	۶۴	۶،۰۰۰	۷،۰۰۰	۱۹
C9	۱۲۸	۱۳،۰۰۰	۹،۵۰۰	۱۲

جدول ۳. مشخصات فنی و هزینه‌ای انواع کنترلرهای هوشمند پشتیبان (SC)

نوع کنترلر هوشمند	تعداد پورت $Port_{sc}$	قدرت پردازش prp_{sc} (بسته در ثانیه)	هزینه استقرار Co_{sc} (دلار)	موجودی انبار Avl_{sc}
SC1	۸	۳،۵۰۰	۱،۲۰۰	۲۰
SC2	۳۲	۶،۰۰۰	۲،۳۰۰	۲۵
SC3	۶۴	۹،۰۰۰	۵،۵۰۰	۳۰
SC4	۱۶	۴،۵۰۰	۲،۲۰۰	۲۰
SC5	۶۴	۶،۰۰۰	۲،۵۰۰	۲۵
SC6	۱۲۸	۱۶،۰۰۰	۹،۵۰۰	۴۰
SC7	۱۶	۱۶،۰۰۰	۹،۵۰۰	۳۰

جدول ۴. مشخصات و پهنای باند انواع لینک‌های ارتباطی (L)

نوع لینک	پهنای باند BW_l (بایت در ثانیه)	هزینه احداث به ازای هر متر Co_l (دلار)
L1	۱۰،۰۰۰،۰۰۰	۰،۲۵
L2	۲۰۰،۰۰۰،۰۰۰	۰،۶۳
L3	۱۰،۰۰۰،۰۰۰،۰۰۰	۲۹،۰۰

جدول ۵. سایر پارامترهای ثابت و عملیاتی شبکه

نوع پارامتر ثابت	مقدار عددی	واحد سنجش
اندازه بسته کنترلی	۵۰۰	بایت (Byte)
سرعت انتشار سیگنال	۲۹۹،۷۹۲،۴۵۸	متر بر ثانیه (m/s)
فاصله فرضی بین گره‌ها	۱۰۰	متر (m)
تأخیر ذاتی پردازش کنترلر	۰،۰۰۰۰۰۱	میلی‌ثانیه (ms)
حداکثر تأخیر مجاز بیسیم	۱۰،۰۰۰	میلی‌ثانیه (ms)
حداکثر تأخیر مجاز سیمی	۳۰۰،۰۰۰،۰۰۰	میلی‌ثانیه (ms)

جدول ۶. مشخصات ترافیکی انواع سوئیچ‌های شبکه (S)

نوع لینک	نرخ ارسال بسته‌ها Avl_s (بسته در ثانیه)
S1	۱۰۰
S2	۸۰۰
S3	۷۰۰
S4	۶،۰۰۰
S5	۵،۰۰۰
S6	۷۰۰
S7	۶،۰۰۰
S8	۹۰۰
S9	۹،۰۰۰

به منظور بررسی جامع عملکرد مدل، آزمایش‌ها در دو سناریوی اصلی انجام شده‌اند:

۱. شرایط عادی شبکه: در این سناریو هیچ حمله‌ای در شبکه وجود ندارد و مدل تنها با هدف کاهش هزینه استقرار، رعایت محدودیت‌های فنی و بهبود کیفیت سرویس، مکان مناسب کنترلرها و نحوه اتصال سوئیچ‌ها را تعیین می‌کند.

۲. شرایط وقوع حملات DDoS: در این سناریو، شدت‌های مختلف حمله به عنوان ورودی مدل در نظر گرفته می‌شود. مدل با توجه به میزان تهدید هر گره، کنترلرهای هوشمند را در محل‌های مناسب مستقر کرده و نحوه تخصیص سوئیچ‌ها را به گونه‌ای تغییر می‌دهد که ضمن حفظ عملکرد شبکه، از اشباع لایه کنترل و کاهش کیفیت سرویس جلوگیری شود.

مقایسه نتایج این دو سناریو، امکان بررسی تأثیر حملات DDoS بر ساختار لایه کنترل و همچنین ارزیابی میزان اثربخشی مدل پیشنهادی در افزایش پایداری، قابلیت اطمینان و تداوم سرویس شبکه را فراهم می‌کند.

۵-۲- تحلیل نتایج سناریوهای بدون حمله DDoS

در نخستین مرحله از ارزیابی، عملکرد مدل در شرایط عادی شبکه و بدون وجود حملات DDoS بررسی شد. هدف از این آزمایش‌ها، ارزیابی توانایی مدل در انتخاب محل مناسب کنترلرها، تخصیص بهینه منابع و کاهش هزینه استقرار، بدون در نظر گرفتن شرایط بحرانی است. همچنین، نتایج این بخش مبنایی برای مقایسه عملکرد مدل در سناریوهای دارای حمله فراهم می‌کند.

جدول (۷)، نتایج حاصل از اجرای مدل در پنج سناریوی مختلف را نشان می‌دهد. در این سناریوها، تعداد سوئیچ‌ها، لینک‌ها، گره‌های کاندید و حجم ترافیک تغییر کرده است تا رفتار مدل در شرایط مختلف از نظر هزینه، زمان حل و عملکرد حل‌کننده مورد بررسی قرار گیرد.

تحلیل نتایج سناریوهای بدون حمله

نتایج جدول (۷) نشان می‌دهد که مدل پیشنهادی در تمامی

سناریوها توانسته است یک پاسخ بهینه و قابل قبول از نظر هزینه و محدودیت‌های فنی ارائه دهد. با این حال، مقایسه سناریوهای مختلف بیانگر آن است که زمان حل مسئله بیش از آنکه به تعداد سوئیچ‌ها یا حجم ترافیک وابسته باشد، به ابعاد فضای تصمیم و تعداد گره‌های کاندید بستگی دارد.

الف) تحلیل سناریوهای ۱ و ۴؛ تأثیر تعداد گره‌های کاندید بر زمان حل

سناریوهای ۱ و ۴ از نظر بسیاری از پارامترها کاملاً مشابه هستند. در هر دو سناریو، تعداد سوئیچ‌ها (۵)، تعداد لینک‌ها (۶)، تعداد کنترلرهای مورد نیاز (۲)، حجم ترافیک (۱۲،۶۰۰ بایت) و حتی هزینه نهایی استقرار (۹،۳۵۰ دلار) یکسان است. تنها تفاوت این دو سناریو، تعداد گره‌های کاندید برای استقرار کنترلرها است که از ۹ گره در سناریوی اول به ۱۰۰ گره در سناریوی چهارم افزایش یافته است. این تغییر، تأثیر بسیار چشمگیری بر عملکرد حل‌کننده داشته است. زمان حل از ۰٫۱۲۵ ثانیه به ۸۹۳٫۵۴۷ ثانیه (حدود ۱۵ دقیقه) افزایش یافته و تعداد تکرارهای CPLEX نیز از ۳۲۶ به ۶۵۸٫۵۱۱ رسیده است.

دلیل این رفتار، افزایش شدید فضای جستجوی مسئله است. در مسائل برنامه‌ریزی عدد صحیح، هر گره کاندید جدید، تعداد زیادی حالت ممکن برای استقرار کنترلر ایجاد می‌کند. در نتیجه، حل‌کننده برای یافتن پاسخ بهینه باید تعداد بسیار بیشتری از حالت‌های ممکن را بررسی کند. این پدیده که به انفجار ترکیباتی[۲۵] معروف است، یکی از ویژگی‌های اصلی مسائل NP-hard محسوب می‌شود.

این نتایج نشان‌دهنده یک محدودیت محاسباتی ساختاری در مدل‌های دقیق MILP است؛ به طوری که حساسیت مدل به تعداد گره‌های کاندید ($|N|$) بسیار بیشتر از تعداد سوئیچ‌ها یا حجم ترافیک است. زمان حل حدود ۱۵ دقیقه در سناریوی چهارم (۱۰۰ گره کاندید)، اگرچه در فاز برنامه‌ریزی و طراحی آفلاین شبکه کاملاً قابل توجیه و پذیرفته‌شده است، اما نشان می‌دهد که این مدل دقیق ریاضی برای سناریوهای تصمیم‌گیری برخط یا شبکه‌های بسیار بزرگ مقیاس‌پذیر نیست. بنابراین در کاربردهای عملیاتی واقعی، پیشنهاد می‌شود پیش از اجرای مدل، با استفاده از الگوریتم‌های پیش‌پردازش و فیلترینگ توپولوژی (مانند تحلیل مرکزیت گراف یا خوشه‌بندی)، تعداد گره‌های کاندید به مجموعه‌ای منتخب از نقاط استراتژیک محدود گردد تا زمان همگرایی حل‌کننده به حداقل برسد.

بنابراین، نتایج این دو سناریو نشان می‌دهد که افزایش تعداد مکان‌های قابل انتخاب، حتی بدون تغییر در اندازه واقعی شبکه، می‌تواند زمان حل را به طور قابل توجهی افزایش دهد. این موضوع اهمیت استفاده از روش‌های کارآمد بهینه‌سازی و همچنین توسعه الگوریتم‌های فراابتکاری برای شبکه‌های بسیار بزرگ را نشان می‌دهد.

ب) تحلیل سناریوی ۳؛ تأثیر ساختار توپولوژی شبکه

در سناریوی سوم، تعداد سوئیچ‌ها به ۱۲ و تعداد لینک‌ها به ۲۷ افزایش یافته است، اما زمان حل تنها ۲۳٫۱۵ ثانیه گزارش شده است. این مقدار در مقایسه با سناریوی چهارم بسیار کمتر است، با وجود اینکه اندازه شبکه بزرگ‌تر است.

علت این موضوع، محدود بودن تعداد گره‌های کاندید به ۱۲ گره است. در این شرایط، اگرچه مدل باید تعداد بیشتری سوئیچ و لینک را مدیریت کند، اما فضای تصمیم نسبتاً محدود باقی می‌ماند و حل‌کننده می‌تواند سریع‌تر به جواب بهینه برسد. این نتیجه نشان می‌دهد که پیچیدگی محاسباتی مدل بیشتر تحت تأثیر تعداد گزینه‌های مکان‌یابی کنترلرها قرار دارد تا تعداد تجهیزات موجود در شبکه.

ج) تحلیل سناریوهای ۲ و ۵؛ تأثیر هم‌زمان اندازه شبکه و منابع مورد نیاز

سناریوهای دوم و پنجم از نظر تعداد کنترلرها تقریباً مشابه هستند، اما افزایش تعداد سوئیچ‌ها، لینک‌ها و حجم ترافیک در سناریوی پنجم باعث افزایش هزینه نهایی استقرار شده است. با این حال، زمان حل در این سناریو تنها ۰٫۳۴ ثانیه است که نشان می‌دهد کوچک بودن مجموعه گره‌های کاندید، نقش مهمی در کاهش زمان اجرای مدل دارد. این موضوع بار دیگر نشان می‌دهد که اندازه توپولوژی به تنهایی عامل تعیین‌کننده پیچیدگی مسئله نیست، بلکه تعداد مکان‌های قابل انتخاب برای استقرار کنترلرها مهم‌ترین عامل در افزایش زمان حل مدل است.

به طور کلی، نتایج این بخش نشان می‌دهد که مدل پیشنهادی در تمامی سناریوها قادر است پاسخ بهینه را با رعایت تمامی محدودیت‌های فنی ارائه کند. همچنین، تحلیل رفتار حل‌کننده نشان می‌دهد که اگرچه مدل از نظر محاسباتی در دسته مسائل NP-hard قرار می‌گیرد، اما برای شبکه‌های کوچک و متوسط، زمان حل آن مناسب بوده و قابلیت استفاده در طراحی عملی شبکه‌های SDN را دارد. علاوه بر این، نتایج حاصل اهمیت انتخاب مناسب مجموعه گره‌های کاندید را در کاهش زمان حل و افزایش مقیاس‌پذیری مدل به‌خوبی نشان می‌دهد.

جدول ۷. راه‌حل‌های بهینه به‌دست‌آمده توسط CPLEX برای مسئله مکان‌یابی کنترلر در شرایط عادی (بدون حمله DDoS)

سناریو (S#)	تعداد سوئیچ (S)	تعداد لینک (L)	گره‌های کاندید / فعال	تعداد کنترلر (C)	ترافیک پردازشی (بایت)	هزینه کل (دلار)	تعداد تکرار CPLEX	زمان حل (ثانیه)
۱	۵	۶	۲/۹	۲	۱۲،۶۰۰	۹،۳۵۰	۳۲۶	۰،۱۲۵
۲	۵	۱۱	۴/۳۰	۴	۲۷،۰۰۰	۱۸،۸۵۰	۶۸،۰۱۳	۷،۸۱۲۵
۳	۱۲	۲۷	۶/۱۲	۶	۶،۶۰۰	۹،۳۰۰	۳۵۸،۴۴۹	۲۳،۱۵۶۲
۴	۵	۶	۲/۱۰۰	۲	۱۲،۶۰۰	۹،۳۵۰	۶۵۸،۵۱۱	۸۹۳،۵۴۷
۵	۹	۱۲	۴/۷	۴	۲۹،۲۰۰	۲۴،۰۵۰	۳،۳۷۷	۰،۳۴۳۷

جدول ۸. نتایج استقرار کنترلرهای هوشمند در سناریوهای مختلف حملات DDoS

سناریو (S#)	شدت حمله	نرخ ترافیک حمله هر کنترلر (pps)	تعداد کنترلرهای تحت حمله (DAC)	تعداد کنترلرهای هوشمند مستقرشده (SCP)	هزینه کل شبکه (دلار)	تعداد تکرار CPLEX	زمان حل (ثانیه)
۱	بدون حمله (سطح ۰)	۰	۰	۰	۲۳،۹۵۰	۱،۱۸۴	۰،۲۵
۲	حمله ضعیف (سطح ۱)	۲۰۰۰	۱	۱	۲۵،۱۵۰	۹۸۱	۰،۱۹
۳	حمله ضعیف (سطح ۱)	۲۰۰۰	۲	۲	۲۶،۳۵۰	۷۹۸	۰،۱۷
۴	حمله متوسط (سطح ۲)	۴۰۰۰	۱	۲	۲۷،۶۵۰	۱،۴۰۴	۰،۲۹
۵	حمله متوسط (سطح ۲)	۴۰۰۰	۲	۴	۳۱،۳۵۰	۱،۶۰۳	۰،۳۴
۶	حمله متوسط (سطح ۲)	۴۰۰۰	۳	۶	۳۵،۰۵۰	۱،۲۰۷	۰،۲۷
۷	حمله شدید (سطح ۳)	۶۰۰۰	۱	۳	۳۳،۱۵۰	۱،۲۸۵	۰،۳۰
۸	حمله شدید (سطح ۳)	۶۰۰۰	۲	۶	۴۲،۳۵۰	۱،۱۲۴	۰،۲۶
۹	حمله شدید (سطح ۳)	۶۰۰۰	۳	۹	۵۱،۵۵۰	۲،۱۶۵	۰،۵۲
۱۰	حمله بسیار شدید (سطح ۴)	۸۰۰۰	۱	۴	۳۲،۴۵۰	۱۷،۵۹۳	۲،۸۷
۱۱	حمله بسیار شدید (سطح ۵)	۱۰۰۰۰	۲	۱۰	۵۱،۵۸۰	۴۴۲،۱۴۵	۲۴،۶۲
۱۲	حمله بسیار شدید (سطح ۶)	۱۲۰۰۰	۳	۱۸	۹۴،۲۵۰	۵،۲۲۱،۶۶۴	۴۲۸،۶۰
۱۳	حملات ترکیبی (سطوح ۱تا۷)	۲۰۰۰ تا ۱۴۰۰۰	۷	۲۸	۱۱۷،۶۵۰	۷۸۶،۶۲۵،۰۱۵	۱۵۴۲،۳۰

۵-۳- تحلیل نتایج سناریوهای تحت حملات با شدت‌های مختلف DDoS

در این بخش، عملکرد مدل پیشنهادی در شرایط وقوع حملات DDoS مورد بررسی قرار می‌گیرد. برای این منظور، ۱۳ سناریوی مختلف با شدت‌های متفاوت حمله، از وضعیت بدون حمله تا حملات بسیار شدید و ترکیبی، طراحی و اجرا شده است. هدف از این آزمایش‌ها، ارزیابی توانایی مدل در حفظ پایداری لایه کنترل، تعیین تعداد مناسب کنترلرهای هوشمند و بررسی تغییرات هزینه و پیچیدگی محاسباتی در شرایط بحرانی است.

برای برقراری ارتباط دقیق میان پارامتر ریاضی DDoSN، بار ترافیکی تحمیل‌شده به شبکه و سناریوهای مورد بررسی، نگاشت کمی زیر در سناریوها اعمال شده است: سطح صفر (DDoSN=0) نشان‌دهنده شرایط عادی، سطوح ۱ تا ۶ متناظر با نرخ تولید ترافیک مخرب از ۲،۰۰۰ تا ۱۲،۰۰۰ بسته در ثانیه ($\lambda_n^A = DDoSN * 2000\ pps$) برای هر کنترلر هدف، و سناریوی ۱۳ شامل وقوع همزمان هفت حمله با شدت‌های متغیر از ۱ تا ۷ (تا سقف ۱۴،۰۰۰ بسته در ثانیه) در گره‌های مختلف است. جدول (۸) نتایج خروجی حل‌کننده CPLEX را با درج دقیق این مقادیر نمایش می‌دهد.

نتایج جدول (۸) نشان می‌دهد که مدل پیشنهادی با افزایش شدت حملات، به صورت خودکار تعداد کنترلرهای هوشمند مورد نیاز را افزایش می‌دهد. این رفتار بیانگر آن است که مدل تنها به تشخیص وجود حمله اکتفا نمی‌کند، بلکه شدت حمله را نیز در فرآیند تصمیم‌گیری لحاظ کرده و متناسب با آن منابع لازم را در اختیار شبکه قرار می‌دهد. در نتیجه، لایه کنترل حتی در شرایط

بحرانی نیز قادر به ادامه ارائه خدمات خواهد بود.

الف) عملکرد مدل در حملات با شدت پایین

سناریوهای ۲ و ۳ مربوط به حملات سطح ۱ هستند. در این شرایط، حجم ترافیک مخرب هنوز به اندازه‌ای نیست که به ظرفیت پردازشی بالایی نیاز داشته باشد. بنابراین، مدل به ازای هر کنترلر آسیب‌دیده، تنها یک کنترلر هوشمند را فعال می‌کند.

به همین دلیل، تعداد کنترلرهای هوشمند با تعداد کنترلرهای تحت حمله برابر است و هزینه شبکه نیز به صورت تدریجی افزایش می‌یابد. هزینه کل از ۲۳،۹۵۰ دلار در حالت بدون حمله به ۲۵،۱۵۰ دلار و سپس ۲۶،۳۵۰ دلار افزایش پیدا می‌کند. این روند نشان می‌دهد که مدل از استقرار تجهیزات اضافی جلوگیری کرده و تنها منابع مورد نیاز را به شبکه اختصاص می‌دهد.

ب) عملکرد مدل در حملات با شدت متوسط

با افزایش شدت حمله به سطح ۲، رفتار مدل تغییر می‌کند. در این شرایط، تنها جایگزین کردن کنترلر آسیب‌دیده کافی نیست، زیرا حجم بسته‌های مخرب نیز افزایش یافته و بار پردازشی بیشتری به شبکه تحمیل می‌شود.

به همین دلیل، مدل برای هر کنترلر تحت حمله بیش از یک کنترلر هوشمند در نظر می‌گیرد. برای مثال، در سناریوی ۴ با وجود حمله به تنها یک کنترلر، دو کنترلر هوشمند فعال می‌شوند. همچنین در سناریوی ۶، سه کنترلر آسیب‌دیده توسط شش کنترلر هوشمند پشتیبانی می‌شوند.

این رفتار نشان می‌دهد که مدل علاوه بر تعداد نقاط حمله، شدت ترافیک مخرب را نیز در فرآیند تصمیم‌گیری لحاظ می‌کند.

ج) عملکرد مدل در حملات شدید

در سناریوهای ۷ تا ۹، شدت حمله به سطح ۳ افزایش یافته است. در این شرایط، رشد تعداد کنترلرهای هوشمند تقریباً متناسب با شدت حمله ادامه پیدا می‌کند. برای نمونه، در سناریوی ۷ تنها یک کنترلر مورد حمله قرار گرفته است، اما مدل سه کنترلر هوشمند را فعال می‌کند تا بار پردازشی میان آن‌ها توزیع شود و احتمال اشباع کنترلرها کاهش یابد. در سناریوی ۹ نیز با حمله هم‌زمان به سه کنترلر، تعداد کنترلرهای هوشمند به ۹ عدد افزایش یافته و هزینه کل شبکه به ۵۱،۵۵۰ دلار می‌رسد. این افزایش هزینه در واقع بهای حفظ پایداری شبکه در شرایط بحرانی است.

د) عملکرد مدل در حملات بسیار شدید

سناریوهای ۱۰ تا ۱۲ شرایطی را بررسی می‌کنند که شدت حمله بسیار زیاد است و فشار سنگینی بر لایه کنترل وارد می‌شود. در این وضعیت، مدل برای جلوگیری از اشباع کنترلرها، تعداد بیشتری کنترلر هوشمند مستقر می‌کند. به عنوان مثال، در سناریوی ۱۲ تنها سه کنترلر تحت حمله قرار دارند، اما مدل ۱۸ کنترلر هوشمند را برای توزیع بار پردازشی فعال می‌کند. در کنار افزایش تعداد تجهیزات، پیچیدگی محاسبات نیز به طور محسوسی افزایش می‌یابد. تعداد تکرارهای حل‌کننده از چند هزار تکرار در سناریوهای ابتدایی به بیش از ۵،۲ میلیون تکرار در این سناریو می‌رسد. این موضوع نشان می‌دهد که با افزایش شدت حمله، فضای تصمیم مدل بزرگ‌تر شده و فرآیند یافتن جواب بهینه دشوارتر می‌شود.

هـ) تحلیل سناریوی حملات ترکیبی

سناریوی ۱۳ سخت‌ترین شرایط آزمایش را شبیه‌سازی می‌کند. در این سناریو، هفت حمله هم‌زمان با شدت‌های مختلف در نقاط مختلف شبکه رخ می‌دهد. چنین شرایطی از نظر عملی یکی از پیچیده‌ترین حالت‌های ممکن برای مدیریت لایه کنترل محسوب می‌شود. در این وضعیت، مدل با استقرار ۲۸ کنترلر هوشمند توانسته است شرایط لازم برای ادامه عملکرد شبکه را فراهم کند. هزینه نهایی شبکه به ۱۱۷،۶۵۰ دلار افزایش یافته و حل‌کننده برای یافتن پاسخ بهینه بیش از ۷۸۶ میلیون تکرار انجام داده است. اگرچه این سناریو از نظر محاسباتی بسیار پیچیده است، اما مدل همچنان موفق به یافتن یک پاسخ بهینه شده است. این موضوع نشان می‌دهد که مدل پیشنهادی حتی در شرایطی که چندین حمله هم‌زمان با شدت‌های متفاوت رخ می‌دهد، قادر است با تخصیص مناسب منابع، پایداری شبکه را حفظ کند.

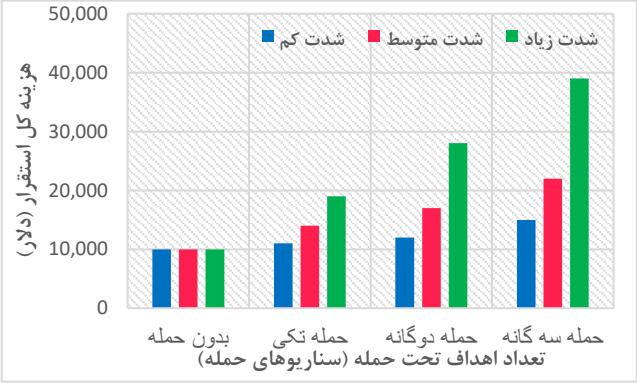
ثبت ۷۸۶،۶۲۵،۰۱۵ تکرار سیمپلکس و زمان حل ۱،۵۴۲،۳ ثانیه (حدود ۲۵ دقیقه) در این سناریو، نشان‌دهنده بیشترین چالش محاسباتی مدل است. مدل در این سناریو با ۱،۴۸۰ متغیر باینری و ۳،۶۲۰ قید خطی روبرو بوده است. وقوع همزمان هفت حمله با شدت‌های مختلف، ماتریس تصمیم‌گیری لینک‌های بین‌کنترلری (R_{lnm}) و تخصیص سوئیچ‌ها (Z_{lsn}) را به شدت مقید ساخته که این امر منجر به ایجاد شکاف اولیه‌ی بزرگ در آرام‌سازی خطی و پیمایش بیش از ۲،۴ میلیون گره در درخت Branch-and-Cut شده است. اگرچه حل‌کننده در نهایت با MIP Gap معادل ٪۰،۰۰ موفق به اثبات بهینگی مطلق گردید، اما این حجم از تکرار سیمپلکس نمایانگر محدودیت ساختاری فرمول‌بندی‌های یکپارچه

دقیق در مواجهه با سناریوهای حملات چندگانه گسترده است.

به طور کلی، نتایج این بخش نشان می‌دهد که مدل پیشنهادی رفتاری کاملاً تطبیقی در برابر حملات DDoS دارد. با افزایش شدت حمله، تعداد کنترلرهای هوشمند، هزینه استقرار و پیچیدگی محاسباتی به صورت منطقی افزایش می‌یابد، اما در مقابل، شبکه توانایی ادامه ارائه خدمات خود را حفظ می‌کند. این ویژگی، مهم‌ترین مزیت مدل پیشنهادی نسبت به روش‌های سنتی است که معمولاً شدت حمله را در فرآیند مکان‌یابی کنترلرها در نظر نمی‌گیرند و تنها بر شرایط عادی یا خرابی‌های ساده تمرکز دارند.

۵-۴- تحلیل تأثیر شدت حمله بر هزینه کل لایه کنترل

یکی از مهم‌ترین معیارهای ارزیابی مدل پیشنهادی، بررسی تغییرات هزینه لایه کنترل در برابر افزایش شدت حملات DDoS است. اگرچه استفاده از کنترلرهای هوشمند موجب افزایش هزینه استقرار می‌شود، اما این افزایش هزینه در واقع سرمایه‌گذاری برای حفظ پایداری شبکه و جلوگیری از قطع سرویس در شرایط بحرانی است. برای بررسی این موضوع، تغییرات هزینه کل شبکه در سناریوهای مختلف حمله تحلیل شده و نتایج آن به صورت شماتیک در شکل ۱ نمایش داده شده است. این شکل روند تغییر هزینه‌ها را از حالت عادی تا سناریوهای دارای حملات تک‌گانه و چندگانه نشان می‌دهد.



شکل ۱. روند تغییر هزینه کل لایه کنترل (برحسب دلار) با افزایش تعداد و شدت حملات DDoS

نتایج نشان می‌دهد که با افزایش شدت حمله، هزینه کل شبکه نیز افزایش پیدا می‌کند. این افزایش ناشی از استقرار کنترلرهای هوشمند، ایجاد لینک‌های ارتباطی جدید و اختصاص منابع پردازشی بیشتر برای حفظ عملکرد شبکه است. با این حال، روند افزایش هزینه کاملاً هدفمند بوده و تنها زمانی اتفاق می‌افتد که شرایط شبکه به آن نیاز داشته باشد.

الف) شرایط بدون حمله

در حالت عادی، هیچ‌گونه حمله‌ای در شبکه وجود ندارد و بنابراین نیازی به استفاده از کنترلرهای هوشمند نیست. در این شرایط، مدل تنها کنترلرهای اصلی مورد نیاز را مستقر کرده و کم‌هزینه‌ترین پیکربندی ممکن را انتخاب می‌کند. به همین دلیل، هزینه کل شبکه در پایین‌ترین مقدار خود قرار دارد و تمامی محدودیت‌های فنی نیز رعایت می‌شوند. این نتیجه نشان می‌دهد که مدل در شرایط عادی از تخصیص منابع اضافی جلوگیری کرده و تنها تجهیزات مورد نیاز را فعال نگه می‌دارد.

ب) حملات تک‌گانه

با وقوع نخستین حمله، مدل به صورت خودکار کنترلرهای هوشمند مورد نیاز را وارد مدار می‌کند. میزان افزایش هزینه به شدت حمله بستگی دارد. در حملات با شدت پایین، تنها تعداد محدودی کنترلر هوشمند فعال می‌شود و افزایش هزینه نسبتاً کم است. اما با افزایش شدت حمله، تعداد کنترلرهای هوشمند، ظرفیت پردازشی مورد نیاز و هزینه استقرار نیز افزایش می‌یابد. این رفتار نشان می‌دهد که مدل به جای استفاده از یک سیاست ثابت، منابع را متناسب با شرایط واقعی شبکه تخصیص می‌دهد.

ج) حملات هم‌زمان به چند کنترلر

زمانی که حملات به طور هم‌زمان چندین کنترلر را هدف قرار می‌دهند، نیاز به منابع پشتیبان نیز افزایش پیدا می‌کند. در این شرایط، مدل علاوه بر استقرار کنترلرهای هوشمند بیشتر، ممکن است لینک‌های ارتباطی جدیدی نیز ایجاد کند تا بار پردازشی میان کنترلرها توزیع شود. به همین دلیل، هزینه کل شبکه نسبت به حالت تک‌حمله با سرعت بیشتری افزایش پیدا می‌کند. برای مثال، در سناریوهای دارای حملات شدید و چندگانه، هزینه استقرار از حدود ۴۰ هزار دلار فراتر رفته و در برخی آزمایش‌ها به ۹۴،۲۵۰ دلار نیز رسیده است. البته این افزایش هزینه، به معنای اتلاف منابع نیست، بلکه هزینه لازم برای جلوگیری از توقف شبکه و حفظ کیفیت سرویس در شرایط بحرانی محسوب می‌شود.

جمع‌بندی تحلیل هزینه

بررسی نتایج نشان می‌دهد که رابطه میان شدت حمله و هزینه کل شبکه، یک رابطه افزایشی و غیرخطی است. هرچه شدت حمله بیشتر شود، مدل منابع بیشتری برای حفاظت از لایه کنترل اختصاص می‌دهد. با این حال، این افزایش تنها در صورت نیاز انجام می‌شود و از استقرار تجهیزات غیرضروری جلوگیری می‌شود.

بنابراین، مدل پیشنهادی توانسته است میان دو هدف مهم، یعنی کاهش هزینه استقرار و افزایش قابلیت اطمینان شبکه، تعادل مناسبی برقرار کند. در نتیجه، شبکه در شرایط عادی با کمترین هزینه ممکن بهره‌برداری می‌شود و در زمان وقوع حملات نیز با اختصاص منابع کافی، تداوم سرویس و پایداری لایه کنترل حفظ خواهد شد.

۶- جمع‌بندی و نتیجه‌گیری

در این پژوهش، یک مدل برنامه‌ریزی خطی عدد صحیح مختلط آگاه از حمله برای مکان‌یابی کنترلرها در شبکه‌های مبتنی بر نرم‌افزار ارائه شد. یافته‌های حاصل از ارزیابی ۱۳ سناریوی عملیاتی نشان داد که استقرار دوگانه و ناهمگون کنترلرهای ساده و هوشمند پشتیبان، پاسخی منعطف و بهینه در برابر تغییرات شدت حملات DDoS فراهم می‌کند. مدل پیشنهادی توانست در شرایط عادی با کمینه‌سازی هزینه استقرار (۲۳،۹۵۰ دلار) بهره‌برداری اقتصادی از شبکه را تضمین نموده و در هنگام وقوع حملات چندگانه و شدید، با فعال‌سازی کنترلرهای هوشمند مناسب، پایداری و سقف تأخیر کیفیت سرویس لایه کنترل را با شکاف بهینگی ٪۰،۰۰ حفظ نماید.

علی‌رغم تضمین بهینگی مطلق سراسری، تحلیل‌های محاسباتی نشان داد که زمان حل مدل دقیق MILP نسبت به تعداد گره‌های کاندید و وقوع همزمان حملات حساسیت نمایی دارد؛ به‌طوری‌که افزایش گره‌های کاندید به ۱۰۰ نقطه، زمان حل را به حدود ۱۵ دقیقه و وقوع حملات ترکیبی ۷ گانه، تکرارهای سیمپلکس را به بیش از ۷۸۶ میلیون افزایش داد. بنابراین، این مدل دقیق ریاضی برای فاز برنامه‌ریزی استراتژیک و آفلاین زیرساخت مناسب است و برای بازپیکربندی‌های برخط یا شبکه‌های مقیاس‌بزرگ با محدودیت مقیاس‌پذیری مواجه است.

با توجه به نتایج و محدودیت‌های شناسایی‌شده، مسیرهای کلیدی زیر برای توسعه پژوهش پیشنهاد می‌شود:

توسعه الگوریتم‌های تجزیه و حل مقیاس‌پذیر: استفاده از روش‌های تجزیه ریاضی نظیر تجزیه بندرز (Benders Decomposition) و الگوریتم‌های فراابتکاری چندهدفه (مانند NSGA-III) جهت کاهش زمان همگرایی در شبکه‌های گسترده.

مدل‌سازی عدم قطعیت با بهینه‌سازی استوار (Robust Optimization): لحاظ نمودن عدم قطعیت‌های آماری در نرخ ترافیک حمله و خطاهای تخمین سیستم‌های تشخیص نفوذ با استفاده از مجموعه‌های عدم قطعیت چندوجهی.

اعتبارسنجی عملیاتی در بسترهای شبیه‌ساز واقعی: پیاده‌سازی سازوکار انتقال پویای سوئیچ و ارزیابی سربار زمانی پروتکل‌های OpenFlowدر بستر Mininet با کنترلرهای تجاری نظیر ONOS و OpenDaylightتحت تزریق ترافیک واقعی حملات DDoS.

مراجع

[1] M. A. Ouamri, T. Alharbi, D. Singh, and Z. Sylia, “A comprehensive survey on software-defined wide area network (SD-WAN): Principles, opportunities and future challenges,” *The Journal of Supercomputing*, vol. 81, no. 1, Art. no. 291, 2025, doi: 10.1007/s11227-024-06718-1.

[2] H. Riggs, A. Khalid, and A. I. Sarwat, “An overview of SDN issues—A case study and performance evaluation of a secure OpenFlow protocol implementation,” *Electronics*, vol. 14, no. 16, Art. no. 3244, 2025, doi: 10.3390/electronics14163244.

[3] A. Hirsi, J. I. Mohamed, A. A. Warsame, A. A. Khalif, L. Audah, A. Salh, *et al*., “A survey of supervised, unsupervised, and ensemble learning approaches for DDoS detection in SDN,” in *Proc. 12th Int. Conf. Inf. Technol. (ICIT)*, Amman, Jordan, 2025, pp. 99–104, doi: 10.1109/ICIT64950.2025.11049252.

[4] J. A. Diaz, R. S. Rodriguez, J. L. Ruiz, and L. C. Rada, “Systematic review on perimeter security in the detection of centralization vulnerabilities in SDN networks,” *IET Conference Proceedings*, vol. 2025, no. 3, pp. 349–357, 2025, doi: 10.1049/icp.2025.1137.

[5] B. Alhijawi, S. Almajali, H. Elgala, H. B. Salameh, and M. Ayyash, “A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets,” *Computers & Electrical Engineering*, vol. 99, Art. no. 107706, 2022, doi: 10.1016/j.compeleceng.2022.107706.

[6] B. Sapkota, A. Ray, M. K. Yadav, B. R. Dawadi, and S. R. Joshi, “Machine learning-based attack detection and mitigation with multi-controller placement optimization over SDN environment,” *Journal of Cybersecurity and Privacy*, vol. 5, no. 1, Art. no. 10, 2025, doi: 10.3390/jcp5010010.

[7] M. M. Kazemian and M. Mirabi, “Controller placement in software defined networks using multi-objective antlion algorithm,” *The Journal of Supercomputing*, vol. 78, no. 4, pp. 5626–5649, 2022, doi: 10.1007/s11227-021-04109-4.

[8] D. Hock, M. Hartmann, S. Gebert, M. Jarschel, T. Zinner, and P.-G. Tran-Gia, “Pareto-optimal resilient controller placement in SDN-based core networks,” in *Proc. 25th Int. Teletraffic Congr. (ITC)*, 2013, pp. 1–9, doi: 10.1109/ITC.2013.6662939.

[9] A. Jalili, “A fuzzy logic-based framework for multi-objective controller placement in software defined networks,” *Fuzzy Optimization and Modeling Journal*, vol. 6, no. 1, 2025, doi: 10.57647/j.fomj.2025.16560.

[10] A. Jalili, “Enhancing quality of service in SDNs through Pareto-optimized controller placement using NS-MF algorithm,” *International Journal of Nonlinear Analysis and Applications*, vol. 16, no. 9, pp. 157–167, 2025, doi: 10.22075/ijnaa.2024.34424.5141.

[11] Y. Hu, W. Wang, X. Gong, X. Que, and S. Cheng, “On reliability-optimized controller placement for software-defined networks,” *China Communications*, vol. 11, no. 2, pp. 38–54, 2014, doi: 10.1109/CC.2014.6821736.

[12] A. Alowa, T. Fevens, and Y. Khamayseh, “Survival backup strategy for controller placement problem in software defined networking,” *Computer Communications*, vol. 185, pp. 104–117, 2022, doi: 10.1016/j.comcom.2021.12.020.

[13] E. Taherian-Fard, T. Niknam, R. Sahebi, M. Javidsharifi, A. Kavousi-Fard, and J. Aghaei, “A software defined networking architecture for DDoS-attack in the storage of multimicrogrids,”

IEEE Access, vol. 10, pp. 83802–83812, 2022, doi: 10.1109/ACCESS.2022.3197283.

[14] M. B. Jiménez, D. Fernández, J. E. Rivadeneira, L. Bellido, and A. Cárdenas, "A survey of the main security issues and solutions for the SDN architecture," *IEEE Access*, vol. 9, pp. 122016–122038, 2021, doi: 10.1109/ACCESS.2021.3109564.

[15] R. Sebopelo and B. Isong, "An integrated framework for controllers placement and security in software-defined networks ecosystem," *Journal of Information Systems and Informatics*, vol. 6, no. 1, pp. 464–494, 2024, doi: 10.51519/journalisi.v6i1.682.

[16] E. Calle, D. Martínez, M. Mycek, and M. Pióro, "Resilient backup controller placement in distributed SDN under critical targeted attacks," *International Journal of Critical Infrastructure Protection*, vol. 33, Art. no. 100422, 2021, doi: 10.1016/j.ijcip.2021.100422.

[17] A. A. Alashhab, M. S. Zahid, B. Isyaku, A. A. Elnour, W. Nagmeldin, A. Abdelmaboud, T. A. A. Abdullah, and U. D. Maiwada, "Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model," *IEEE Access*, vol. 12, pp. 51630–51649, 2024, doi: 10.1109/ACCESS.2024.3384398.

[18] S. Yang, L. Cui, Z. Chen, and W. Xiao, "An efficient approach to robust SDN controller placement for security," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1669–1682, 2020, doi: 10.1109/TNSM.2020.2994837.

[19] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H. N. Lee, "Systematic review of security vulnerabilities in Ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022, doi: 10.1109/ACCESS.2021.3140091.

[20] Z. A. Bhuiyan, S. Islam, M. M. Islam, A. A. Ullah, F. Naz, and M. S. Rahman, "On the (in)security of the control plane of SDN architecture: A survey," *IEEE Access*, vol. 11, pp. 91550–91582, 2023, doi: 10.1109/ACCESS.2023.3307467.

[21] D. Gao, Z. Liu, Y. Liu, C. H. Foh, T. Zhi, and H.-C. Chao, "Defending against Packet-In messages flooding attack under SDN context," *Soft Computing*, vol. 22, no. 20, pp. 6797–6809, 2018, doi: 10.1007/s00500-018-3407-3.

[22] S. Sutradhar, K. Chowdhury, S. Deb, J. L. Sarkar, C. Kumar, and A. K. Sahu, "A comprehensive review of DDoS attack prevention, detection, and mitigation in IoT and SDN-IoT networks," *Discover Internet of Things*, vol. 6, Art. no. 67, 2026, doi: 10.1007/s43926-026-00341-7.

[23] P. K. Thiruvasagam, A. Chakraborty, A. Mathew, and C. S. R. Murthy, "Reliable placement of service function chains and virtual monitoring functions with minimal cost in softwarized 5G networks," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1491–1507, 2021, doi: 10.1109/TNSM.2021.3056917.

[24] R. Kołakowski, S. Kukliński, and L. Tomaszewski, "Evaluating scalability of hierarchical multi-controller SDN: A holistic approach," *Journal of Network and Systems Management*, vol. 34, no. 4, Art. no. 107, 2026, doi: 10.1007/s10922-026-10087-w.

پاورقی‌ها:

۱ Control Plane
۲ Data Plane
۳ Software Defined Networks
۴ Distributed Denial of Service Attack
۵ Controller Placement Problem
۶ Mixed-Integer Linear Programming (MILP)
۷ Quality of Services
۸ Passive Backup
۹ Replication
۱۰ Integer Programming
۱۱ Simple Controller
۱۲ Smart Backup Controller
۱۳ Active Backup
۱۴ Dynamic Switch Migration
۱۵ DDoS Intensity
۱۶ Attack Level
۱۷ Flow Table
۱۸ Botnet
۱۹ Flow Table Miss
۲۰ Southbound Interface
۲۱ Trade-off
۲۲ CapEx
۲۳ Worst-Case Upper Bound
۲۴ Heterogeneous
۲۵ Combinatorial Explosion