ارائه یک روش جدید به‌منظور مقابله با حملات منع خدمت توزیع شده در شبکه‌های نامدار

احسان کشوری پور [۱]، محمود دی پیر [۲]، میثم بیات [۳]

۱- کارشناسی ارشد-دانشکده مهندسی برق- دانشگاه علوم وفنون هوایی شهید ستاری- تهران- ایران

ehsan.keshvari1375@gmail.com

۲- دانشیار- دانشکده مهندسی برق- دانشگاه علوم وفنون هوایی شهید ستاری- تهران- ایران

mdeypir@ssau.ac.ir

۳- استادیار- دانشکده مهندسی برق- دانشگاه علوم وفنون هوایی شهید ستاری- تهران- ایران

m_bayat@ssau.ac.ir

چکیده: شبکه‌های نامدار یک معماری بالقوه اینترنت است که به‌صورت یک شبکه توزیع‌شده طراحی می‌شود. شبکه‌های نامدار برای سازمان‌هایی که به‌دنبال اشتراک داده‌ها در شبکه‌های عمومی بوده و حفظ امنیت داده برای آن‌ها مهم است، کاربردی است. از این رو این نوع شبکه‌ها در صورت رفع ایرادات و معایب، در هوشمند سازی شبکه یکپارچه پلیس نیز قابل اجرا می‌باشد. از آن‌جا که انتقال داده با استفاده از شبکه نامدار به آدرسIP نیاز ندارد، بسته‌های معمولی در حین فرآیند انتقال قابل شناسایی نیستند. در این روش انتقال داده فقط فرستنده و گیرنده می‌دانند کدام داده‌ها باید بازسازی شوند. به این ترتیب، لایه امنیتی جدیدی نظیر رمزگذاری فراهم خواهد شد. در این مقاله به بررسی شبکه‌های نامدار و تأثیر حملات منع خدمت توزیع شده بر آن پرداخته شده تا نقطه ضعف اصلی این شبکه در برابر این حملات شناسایی گردد. بعد از شناسایی نقطه ضعف، به ارائه یک روش به منظور کاهش اثر این نقطه ضعف پرداخته شده است. در روش پیشنهادی تغییراتی در تصدیق منفی بسته درخواست (Nack) ایجاد کرده و پروتکل تشخیص ازدحام لایه پیوند به راهبرد بهترین مسیر شبکه‌های نامدار افزوده می‌شود. این تغییرات به منظور استفاده مؤثرتر از پهنای باند شبکه و با هدف بهره‌وری بیشتر از این شبکه‌ها در صورت بروز ازدحام و حمله منع خدمت، صورت پذیرفته است. آزمایش‌های انجام شده پس از شبیه‌سازی روش پیشنهادی، باعث حداقل بهبود ۷۰ درصدی دسترسی شبکه و بهبود ۴۰ درصدی بازیابی داده شبکه و بهبود ۲۷ درصدی نیاز به ارسال مجدد شبکه در ازدحام نسبت به راهکارهای پیشین شده است.

واژه‌های کلیدی: شبکه‌های نامدار - حمله منع خدمت توزیع شده - یافتن بهترین مسیر - تصدیق منفی بسته درخواست

تاریخ دریافت مقاله: ۱۴۰۰/۰۲/۰۷	**تاریخ پذیرش مقاله: ۱۴۰۰/۰۴/۳۰**
از صفحه ۱ تا ۱۱	**نوع مقاله : پژوهشی**
نویسنده مسئول: محمود دی پیر	**نشریه علمی فناوری اطلاعات و ارتباطات انتظامی- دوره دوم- شماره ۶- تابستان ۱۴۰۰**

۱- مقدمه

شبکه‌های نامدار یا Named Data Networks (NDN) یک معماری بالقوه اینترنت است که به‌صورت یک شبکه توزیع‌شده طراحی می‌شود[۱]. این مجموعه به‌عنوان یک مسیریاب نرم‌افزاری عمل می‌کند که با استفاده از یک مؤلفه به‌عنوان هسته شبکه[1] کار می‌کند تا امکان برقراری ارتباط بدون نیاز به آدرس‌های IP یا سرورهای سخت‌افزاری را فراهم سازد. این ساختار موفق شده‌است بسیاری از پیشتازان صنعت شبکه نظیر آلکاتل، سیسکو، هواوی و... را به جمع خود اضافه کند[۱]. این اعضا شامل هشت دانشگاه امریکایی و شش دانشگاه بین‌المللی نظیر UCLA هستند که مسئولیت تولید بدنه برای شبکه‌های نامدار به‌عنوان استاندارد آینده شبکه را به‌عهده دارند. شبکه‌های نامدار برای سازمان‌هایی که به‌دنبال اشتراک داده‌ها در شبکه‌های عمومی بوده و حفظ امنیت انتقال و محتوا برای آن‌ها مهم است، کاربردی است. از آن‌جا که انتقال داده با استفاده از شبکه‌های نامدار به آدرس IP نیاز ندارد، بسته‌های معمولی در حین فرآیند انتقال قابل شناسایی نیستند و فقط فرستنده و گیرنده می‌دانند کدام داده‌ها باید بازسازی شوند. به این ترتیب، لایه امنیتی جدیدی نظیر رمزگذاری فراهم خواهد شد. شبکه نامدار همچنین معماری مناسبی برای پیاده‌سازی روش‌هایی نظیر کدگذاری شبکه محسوب می‌شود. در این روش می‌توان با استفاده از معادلات ریاضی به‌جای ارسال بسته‌ها به نرخ انتقالی معادل ۵ الی ۱۰ برابر سریع‌تر از سایر روش‌ها دست یافت[۱].

بسته‌های محتوا در این شبکه به دو نوع بسته درخواست و بسته داده تقسیم می‌شوند. در این شبکه اجزا اصلی مسیریاب‌هایی هستند که به مسیریاب‌های محتوا معروفند که شامل هدایت بر اساس اطلاعات[2]، ذخیره محتوا[3] و جدول درخواست‌های منتظر[4] می‌شوند[۱].

یک مهاجم می‌تواند با به‌کارگیری چندین ماشین در سطح شبکه و تولید درخواست‌هایی با نام پیشوندهایی که داده‌ای برای آن وجود ندارد، منجر به پر شدن حافظه PIT شده و از سرویس دادن به کاربران قانونی جلوگیری کند[۲]. از این رو تشخیص و کاهش حملات منع خدمت توزیع شده در شبکه‌های نامدار مورد مطالعه و بررسی محققان بسیاری بوده است. در این مقاله با مطالعه و بررسی شبکه‌های نامدار، نقطه ضعف اصلی این شبکه که شامل تأثیر حملات منع خدمت توزیع شده بر آن می‌باشد، شناسایی شده است. سپس به ارائه یک روش جدید پرداخته شده است. با استفاده از روش پیشنهادی بهبود کارایی و بهره‌وری راهبرد بهترین مسیر هدایت[5] (NBR) در شبکه‌های نامدار که از سال ۲۰۱۳ قابل استفاده می‌باشد [۳] ، نشان داده شده است. در روش پیشنهادی، با ایجاد تغییراتی در ساختار بسته‌های درخواست موجود در راهبرد بهترین مسیر هدایت و تغییراتی در تصدیق منفی بسته درخواست (Nack) [۴] از پهنای باند موجود در صورت ازدحام بیشترین بهره برده شده است. همچنین از هدایتی هوشمند برای دریافت و ارسال بسته‌ها استفاده شده است.

تغییرات اساسی معماری NDN نسبت به معماری کنونی و دیگر شبکه‌های ارتباطی، منجر به تعریف طراحی‌های جدید برای ارزیابی این شبکه شده است. بدین منظور شبیه‌سازهایی که به صورت گسترده مورد استفاده قرار گرفته‌اند ndnSIM و ns-3 هستند. برای ارزیابی روش پیشنهادی از شبیه ساز ndnSIM استفاده شده است. شبیه‌ساز ndnSIM در یک فاز ماژولی با استفاده از کلاس‌ها و اینترفیس‌های c++ برای مدل و انتزاع رفتاری هر یک از مشخصه‌های لایه شبکه (FIB،CS و PIT) در NDN پیاده‌سازی شده است[۵].

در ادامه و دربخش ۲ روش تحقیق آورده شده است و رویکرد NBR را معرفی می‌کند، در بخش ۳ به طراحی و معرفی روش پیشنهادی به صورت کلی پرداخته شده است. در بخش ۴ با شبیه‌سازی مناسب در شرایط مختلف با استفاده از مدل‌های ریاضی، شبکه مورد آزمایش قرار داده شده است و در بخش آخر نیز نتیجه‌گیری از روش پیشنهادی ارائه شده است.

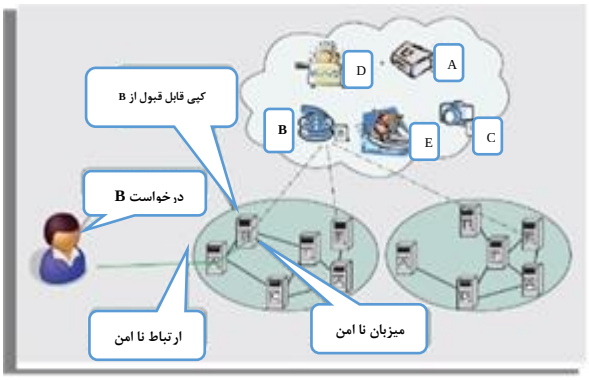
۲- روش تحقیق

چارچوب فعلی اینترنت از اوایل دهه ۹۰ برای استفاده عموم قرار گرفته است[۱]. اینترنت در حال حاضر تمام جنبه‌های زندگی مدرن را در بر می‌گیرد. اگر چه اینترنت رشد زیادی پیدا کرده اما این رشد منجر به شکل‌گرفتن مسائل مختلفی همچون کمبود ذاتی امنیت با فرض قابل اعتماد بودن تمام موجودیت‌ها، کنترل ارتباط تنها از طریق فرستنده، انحصار لایه‌های اصلی اینترنت شده است. رونق رسانه‌های اجتماعی منجر به ایجاد محتوای بیشتر و افزایش تکرار در انتقال شده است. اینترنت امروزی از ضعف‌های امنیتی و حمله‌های همچون حملات منع خدمت رنج می‌برد[۱].

شبکه‌های اطلاعات محور[6]، شبکه‌های میزبان محور هستند که از سال ۲۰۰۶ توسط V.Jacobson پایه‌گذاری شد[۶]. در این شبکه ها

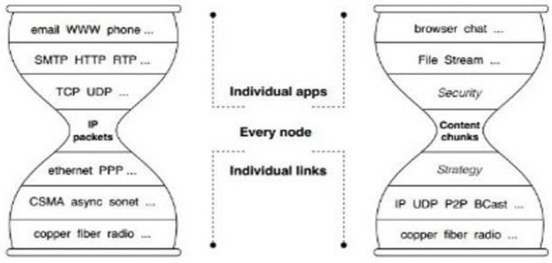
[1] NDN Forwarding Daemon
[2] Information Base Forwarding یا FIB
[3] Content save یا CS
[4] Pending Interest Table یا PIT
[5] NDN Best Rout
[6] Information-centric networking

ارتباطات بر پایه نام میزبان‌ها می‌باشد. برای نمونه می‌توان به وب سرویس‌ها، کامپیوترهای شخصی و دیگر دستگاه‌ها اشاره کرد. (شکل۱) قدرت معماری ICN در ذخیره کردن، ایجاد ارتباطات چندگانه از طریق تکرار محتوا است که ارسال کنندگان و دریافت کنندگان را از یکدیگر جدا می‌کند. هدف نهایی به دست آوردن کارایی و اعتماد پذیری توزیع محتواهایی است که با فراهم سازی یک زیرساخت برای سرویس‌های ارتباطی به دست می‌آید[۶].



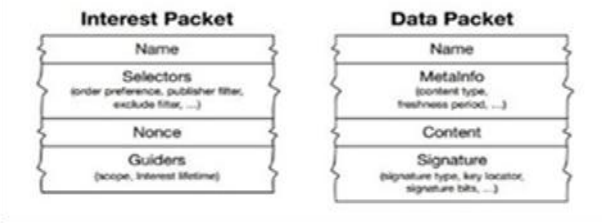
شکل (۱): مدل ارتباطی ICN، سمت کاربر[۶]

مدل ساعت شنی معماری اینترنت امروزی بر روی لایه‌ی شبکه‌ی IP متمرکز است که حداقل عملکردهای لازم را برای اتصال کلی پیاده سازی می‌کند(شکل۲). این مدل میانه‌ای با گذردهی محدود دارد که با رشد سریع اینترنت، فشار بار زیادی بر لایه‌های بالایی و پایینی ایجاد می‌کند. شبکه‌های توزیع محتوا، عمومی‌تر از شبکه‌های ارتباطی هستند و حل کردن مشکلات توزیع با پروتکل ارتباطی نقطه به نقطه، پیچیده و مستعد خطا می‌باشد [۷].



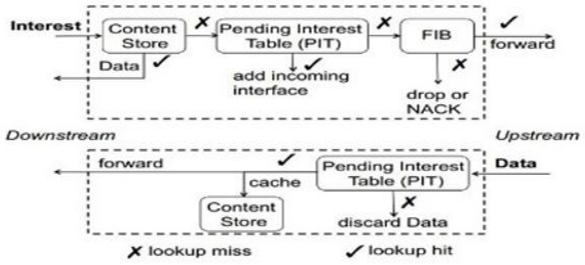
شکل (۲): ساختارهای اصلی تشکیل دهنده معماری NDN در مقایسه با معماری IP [۷]

ارتباطات NDN از طرف درخواست‌کننده داده آغاز می‌گردد. مطابق شکل (۳) دو نوع بسته NDN شامل درخواست (interest) و داده (Data) وجود دارد. درخواست‌کننده برای به دست آوردن محتوا، بسته درخواست را بر روی شبکه ارسال می‌کند. هر گره‌ای که این بسته را دریافت کند، در صورتی که داده‌ای در جواب این درخواست داشته باشد، به درخواست‌کننده برمی‌گرداند.



شکل (۳): انواع بسته‌های NDN [۷]

در واقع نام، شناسه‌ای است که یک داده و درخواست بر اساس آن مبادله می‌شود. یعنی در صورتی که نام درخواست پیشوندی از نام داده باشد، داده در جواب یک درخواست ارسال می‌شود[۷].



شکل (۴): مدل موتور ارسال NDN [۷]

هر مسیریاب NDN جهت انجام کارکردهای حمل بسته‌ی داده و درخواست، سه ساختار داده را نگه می‌دارد: جدول درخواست‌های منتظر یا PIT، هدایت بر ارسال اطلاعات یا FIB و ذخیره‌ی محتوا یا CS. به همراه ماژول راهبرد ارسال که تعیین می کند آیا / کی/ کجا بسته‌ی درخواست ارسال شود (شکل ۴). PIT تمام درخواست‌هایی را که مسیریاب ارسال کرده است ولی هنوز برآورده نشده‌اند را نگهداری می‌کند. هر ورودی از PIT، نام داده‌ی حمل شده در اینترنت را به همراه واسط‌های ورودی و خروجی اش ثبت می‌کند. زمانی که بسته درخواست وارد می‌شود، مسیریابNDN، CS خود را جهت یافتن داده، جستجو می‌کند. اگر آن داده موجود بود مسیریاب بسته‌ی داده را از طریق همان واسطی که درخواست از طرف آن آمده بود، ارسال می‌کند. در غیر این صورت مسیریاب آن نام را در PIT خودش جستجو می‌کند و در صورتی که انطباق یافت شد، به راحتی واسط ورودی این بسته‌ی درخواست را در آن ورودی از PIT ثبت می‌کند. در صورتی که انطباقی از PIT برای آن نام یافت نشد، مسیریاب بسته‌ی درخواست را بر اساس اطلاعات موجود در FIB به سمت تولیدکنندگان داده ارسال

می‌کند. زمانی که مسیریاب چندین درخواست را برای یک نام از طرف چندین گره پایینی دریافت کرد، فقط برای اولین گره به سمت تولید کننده ارسال می‌کند. FIB با پیشوندی از نام‌ها بر اساس پروتکل مسیریابی پر شده است و می‌تواند دارای چندین واسط خروجی برای هر پیشوند باشد ممکن است راهبرد ارسال، تصمیم به دور انداختن یک درخواست در موقعیت خاصی بگیرد [۷].

بسته درخواست در شبکه NDN در قالب زیر تعریف می‌شود[۷]:

NDN Interest packet:
- Name
- Selectors
- Nonce
- Scope
- Intersest Life time

بسته داده در شبکه NDN در قالب زیر تعریف می‌شود[۷]:

NDN Data packet:
- Name
- Meta Information
- Content
- Signature

۲-۱- مزایا و معایب NDN نسبت به IP در زمینه ارسال و دریافت بسته

تمام شدن فضای آدرس، پیمایش NAT[1] و مدیریت آدرس مشکلاتی از IP در زمینه ارسال و دریافت بسته است که درNDN حل شده است. چون NDN هیچ وابستگی به آدرس فرستنده و گیرنده ندارد[۸].

مزیت NDN نسبت به IP در زمینه ارسال و دریافت بسته، ثبت داده در CS و ارسال مجدد سریع در صورت نیاز از طریق بازیابی CSهای موجود در پیمایش درختی می‌باشد. عیب NDN نسبت به IP در زمینه ارسال و دریافت بسته، به خطر افتادن محرمانگی است. چون نامگذاری و ذخیره داده‌ها در NDN مشاهده‌ی این را امکان‌پذیر می‌سازد که چه داده‌ای درخواست شده است ولی بدون آدرس مقصد آن، شناسایی این که چه کسی آن را درخواست کرده دشوارتر است[۸].

شرط اصلی توزیع محتوای امن اعتبار محتوای توزیع‌شده، منشأ محتوا توزیع شده و ارتباط بین پاسخ و درخواست است که در جواب سوالاتی مانند: آیا محتوا کامل است؟ آیا داده فاسد نشده است؟، آیا این محتوا یک پاسخ برای سوالی که دریافت‌کننده پرسیده می‌باشد؟ می‌باشند.

اکثر حملات شناخته شده امروزی از این سه پرسش نشأت می‌گیرند[۶-۷].

۲-۲- حملات منع خدمت (منع سرویس)

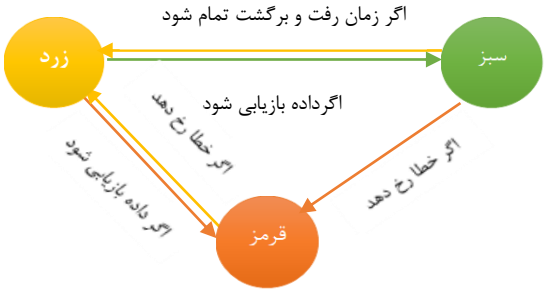
یکی از رایج‌ترین مسائل امنیتی در شبکه‌های کامپیوتری حمله منع خدمت (منع سرویس) است که در آن مهاجمین شبکه سعی می‌کنند تا سرویس‌ها و داده‌های یک سیستم را غیرقابل دسترس کنند[۲].اگر مهاجم برای حمله از یک میزبان استفاده کند به این نوع حمله DoS[2] گفته می‌شود ولی حمله DDoS[3] زمانی اتفاق می‌افتد که چندین سیستم به‌طور هم‌زمان پهنای باند یا منابع سیستم مورد هدف را با بسته‌های سیل‌آسا مورد حمله قرار دهند. وقتی سروری با اتصالات زیادی دچار سربار شود، دیگر نمی‌تواند اتصالات جدیدی را بپذیرد[۲]. انواع حملات DDoS به دودسته اصلی حمله بر اساس هدف و حمله بر اساس درجه خودکارسازی تقسیم می‌شود. حمله بر اساس هدف به دو بخش حمله بر لایه کاربرد و حمله بر لایه پیوند تقسیم می‌شود. حمله بر اساس درجه خودکارسازی شامل سه دسته دستی، نیمه خودکار و خودکار است[۲]. در NDN برای مقابله با این حملات از راه‌های هدایت بسته‌ها بر اساس پهنای باند، تشخیص پهنای باند گام به گام، استفاده از چند مسیر برای ارسال و دریافت و استفاده از حافظه نهان (CS) قابل اجراست[۹].

۲-۳- راهبرد انتخاب بهترین مسیر هدایت در NDN یا NBR[4]

محققان با تجمیع چهار راه جلوگیری از حمله در NDN توانسته‌اند روشی تحت عنوان راهبرد بهترین مسیر هدایت در NDN پیشنهاد دهند که به طور چشمگیری از ازدحام و خارج شدن سیستم از ارائه خدمت جلوگیری می‌کند[۹]. این روش همان‌طور که از نام آن مشخص است با قرار دادن راهبرد مناسب و کارآمد در یافتن و انتخاب مسیر مناسب و به دور از ازدحام برای ارسال و دریافت محتوا، می‌تواند نواقص احتمالی شبکه NDN در مقابل حمله DDoS را پوشش دهد[۹].

[1] Network Address Translation

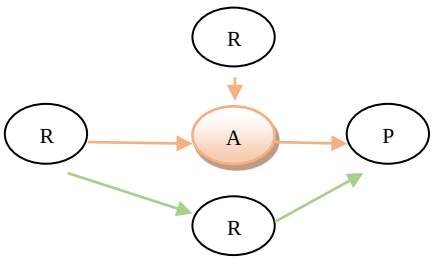
[2] Denial of Service attacks
[3] Distributed DoS
[4] NDN Best Route



شکل(۵): رنگ واسط انتقال در طرح هدایتیNDN

رنگ واسط انتقال در طرح هدایتی NDN مانند شکل(۵) به سه دسته تقسیم می‌شود که رنگ سبز هر واسط به این معناست که واسط می‌تواند داده را به عقب بازگرداند. در رنگ زرد وضعیت مشخص نیست؛ واسط ممکن است بتواند داده را به عقب بازگرداند و رنگ قرمز نشان می‌دهد واسط نمی تواند داده را به عقب بازگرداند[۹].

انواع بسته درخواست در NBR به دو نوع بسته درخواست جدید و بسته درخواست دنباله‌رو تقسیم می‌شود. تفاوت این دو در نحوه‌ی عملکرد آن‌ها می‌باشد. به گونه‌ای که بسته درخواست جدید پس از اتمام RTT (Round Trip Time) حذف می‌شود. اما بسته درخواست دنباله رو، با RTT محدودتر نسبت به بسته درخواست اولیه از درخواست‌کننده یکسان ارسال می‌شود[۹].



شکل (۶): عملکرد NBR در NDN در حمله ربودن پیشوند

در شکل (۶) نماد A به عنوان Attacker (حمله کننده) و R به عنوان Router (مسیریاب) و P به عنوان Producer (تولیدکننده محتوا) استفاده شده‌اند که مهاجم (A) سعی می‌کند یک مسیر نادرست جهت ایجاد حمله از طریق واسط (R3 - A) با مسیریاب (R3) ایجاد کند. ازآنجایی که مسیریاب (R3) بسته های درخواستی خود را از مسیر دیگری هدایت می‌کند، بنابراین بسته های داده بازگشتی خود را از مسیری جز مسیر ارسال، دریافت نمی کند و از سوی دیگر در صورت ارسال بسته‌های درخواست از طریق این واسط هیچ بسته داده بازگشتی از تولیدکننده دریافت نمی کند. درنتیجه این واسط در وضعیت زرد قرار خواهد گرفت. در مسیریاب‌های NDN برخلاف IP، ترافیک‌های غیرمستقیم دارای رتبه بالایی در مسیریابی هستند تا زمانی که هر مسیریاب عملکرد مفید و بهتری از خود نشان دهند [۵]. در راهبرد هدایتی، واسط ها در FIB بر اساس انتخاب بهترین واسط برای استفاده مرتب می شوند. هنگامی که مسیریاب یک نام جدید را دریافت می کند، ازآنجایی که هنوز هیچ عملکرد هدایتی از آن مشاهده نشده است، رتبه‌بندی هر واسط بر اساس اولویت‌های مسیریابی به ازای هر پیشوند اسمی صورت می گیرد. هنگامی که اطلاعات لازم در مورد عملکرد هدایتی واسط موجود باشد، راهبرد هدایتی مربوط به رتبه هر واسط با توجه به نوع اطلاعات به دست آمده، تعیین می‌شود. طیف گسترده‌ای از راهبردهای هدایتی می‌توانند توسط NDN پشتیبانی شود[۹].

۲-۳-۱- تصدیق منفی بسته‌های درخواست[1] یا Nack

در طراحی اصلیNDN، هر مسیریاب می‌تواند خرابی درون شبکه را از طریق وقفه به وجود آمده کشف کند. به طورکلی هنگامی که مسیریاب، N بسته درخواستی خود را ارسال می‌کند، یک زمان‌سنج بر اساس RTT برآورد شده توسط تولیدکننده داده درخواستی، شروع به کار می‌کند. اگر بسته‌های داده قبل از انقضای مهلت زمان‌سنج دریافت شوند، RTT بسته‌ها به‌روزرسانی می‌شود. در غیر این صورت مسیریاب N در صورت وجود یک مسیر جایگزین مجدداً درخواست خود را ارسال می‌کند و یا از ارسال درخواست خود منصرف می شود. یک راه‌حل سریع برای مسئله عنوان شده، استفاده از بسته‌های درخواستی Nack است. شکل (۷) شبه کد(۳)، فرآیند پردازش بسته های Nack را توسط مسیریاب های NDN نشان می‌دهد. اگر یک بسته درخواستی برای درخواست داده‌ای با نام M از طریق Nack برگشت داده شود و زمان‌سنج ارسال مجدد آن هنوز در حال اجرا باشد، مسیریاب بسته را با نامی یکسان و با هدف قبلی به طرف واسط‌های در دسترس با حداکثر اولویت هدایت می‌کند. [۴].

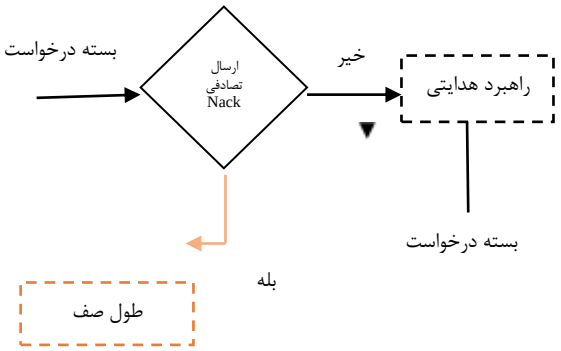
Pseudo-code 3 NDN Best Route Interest Nack Processing

```
1: function Process (Nack)
2:     Pit Entry ← PIT.Find (Nack.Name)
3:      if Pit Entry ≡ ∅ or
4:        PitEntry.RetryTimer expired or
5:          Nack.Nonce ƒ∈ PitEntry.NonceList
6:     then
7:         Return
8:     end if
9:     Forward (Nack. Interest, PitEntry)
10: end function
```

شکل (۷): شبه کد (۳) فرآیند پردازش بسته‌های Nack در روش بهترین مسیر

[1] Negative Acknowledge

بازگشت Nack دو منفعت اساسی را برای سیستم به همراه خواهد داشت. نخست آنکه سیستم بسیار سریع از بسته‌های درخواستی در حال انتظار پاک خواهد شد و دیگر نیازی به انتظار برای به پایان رسیدن طول عمر بسته‌ها نیست. دوم آنکه می توان به راحتی گره‌های پایینی را از طریق بسته Nack آگاه ساخت و این اقدام یک بهبود آگاهانه تلقی می‌شود[۴].

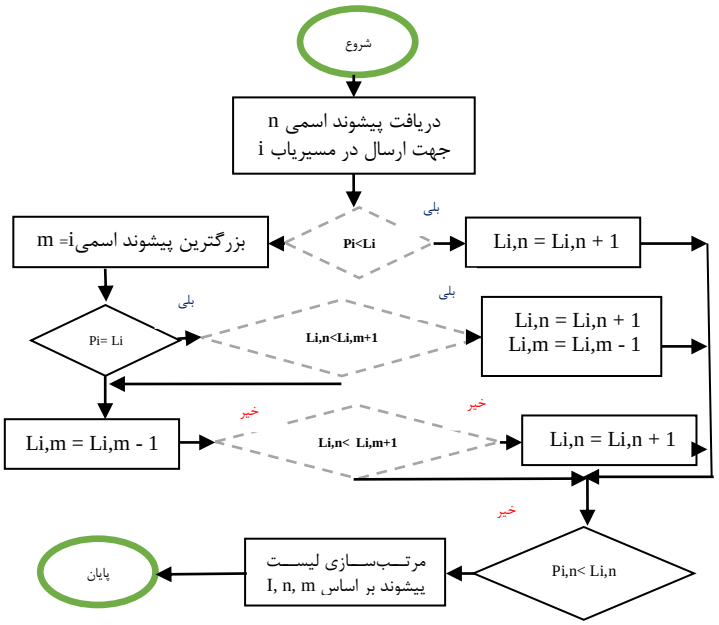


شکل(۸): طرح ارسال تصادفی Nackدر مسیریاب با ازدحام

همان‌طور که در شکل (۸) دیده می‌شود، ارسال تصادفی Nack در شبکه‌های محلی که در آن مسیریاب‌های بعدی بر طول صف نظارت می‌کنند و به صورت فعال اگر صف در حال رشد باشد از طریق یک Nack آن را به مسیریاب قبلی اطلاع می‌دهد.

۳- روش پیشنهادی

با الهام گرفتن از راهبرد انتخاب بهترین مسیر (NBR) و تصدیق منفی بسته‌های درخواست (Nack) می‌توان روشی ارائه کرد که کارایی و امنیت شبکه NDN را بالا ببرد. در این سناریو فرض شده است که راهبرد هدایتی NBR بر روی کلیه مسیریاب‌ها مستقر شود. روش پیشنهادی دارای دو فاز مجزاست. فاز اول، استفاده از یک عامل به منظور افزایش "نرخ محدودیت تعداد بسته‌های درخواست در شرایط عدم وجود ازدحام" است که منجر به گذردهی بیشتر و کاهش تأخیر در ارسال و استفاده بهتر از منابع موجود در شبکه می‌شود. فاز دوم، استفاده از یک عامل دیگر به منظور کاهش نرخ محدودیت تعداد بسته‌های درخواست در شرایط تشخیص ازدحام و یا حمله‌هایی همانند ربودن پیشوند می‌باشد که منجر به افزایش امنیت و کاهش ترافیک و میزان از دست رفتن بسته‌ها می‌گردد.

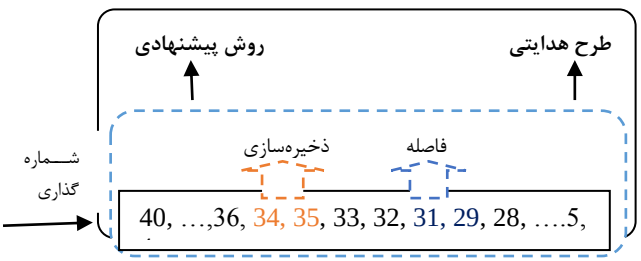


شکل (۹): فلوچارت مکانیزم اعتدال در ازدحام یا حمله

جدول (۱): خلاصه نمادهای استفاده شده در طرح اعتدال

نماد	کاربرد هر نماد
Li	نرخ محدودیت تعداد بسته‌های درخواست در واسط i
Li,n	نرخ محدودیت تعداد پیشوندهای اسمی n در واسط i
Pi	نرخ محدودیت تعداد بسته‌های درخواست در حال انتظار در واسط i
Pi,n	نرخ محدودیت تعداد پیشوندهای اسمی در حال انتظار n در واسط i
Lmin	حداقل نرخ محدودیت تعداد بسته‌های درخواست در هر واسط
Lmax	حداکثر نرخ محدودیت تعداد بسته‌های درخواست در هر واسط

در فلوچارت شکل (۹)، اگر Pi کوچکتر از Li باشد هنوز به حد ارسال بالای بسته‌های درخواست نرسیده‌ایم که می‌توان نرخ محدودیت را افزایش داد و اگر Pi برابر با Li باشد حد بالای ارسال بسته درخواست لمس شده و نرخ محدودیت شروع به کاهش می‌کند. اگر Pi از Li بزرگتر باشد با ازدحام مواجه باشد، در این صورت باید نرخ ارسال کاهش پیدا کند.

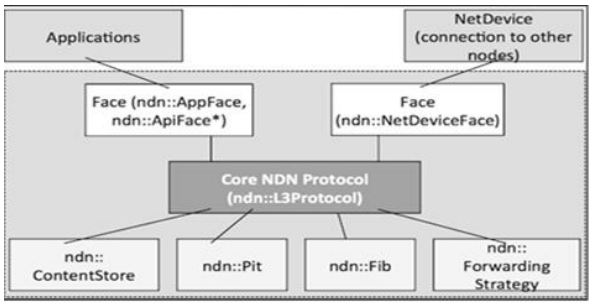


شکل (۱۰): پروتکل تشخیص ازدحام لایه پیوند در NBR بدون نیاز به RTT

تشخیص ازدحام لایه پیوند (LCC[1]) استفاده شده برای NDN همان طرح ارائه شده آن در IP در شبکه‌های محلی است و در آن هر مسیریاب یک شماره ترتیب به بسته درخواست اضافه می‌کند تا به جلو هدایت شود و در انتهای دیگر پیوند، مسیریاب بسته‌های از دست رفته را تشخیص می‌دهد و از آن به عنوان عاملی جهت تشخیص ازدحام استفاده می‌کند که این کار از طریق فاصله ایجادشده در شماره ترتیب بسته‌های دریافتی مانند شکل (۱۰) صورت می‌گیرد.

۴- شبیه‌ساز ndnSIM

در NDN، به جای فرستادن داده‌ها به سمت مکانی مشخص می‌توان داده‌ها را با استفاده از نام هر داده بازیابی کرد. این تغییر کوچک به شبکه NDN اجازه می‌دهد تا از تمام ویژگی‌های آزمایش شده در مهندسی اینترنت، استفاده نماید و نه تنها مشکلات ارتباطات مبتنی بر IP را حل کند، بلکه مشکلات توزیع دیجیتالی و کنترل آن را رفع نماید. از شبیه‌سازی می‌توان به عنوان ابزاری انعطاف‌پذیر برای آزمایش و ارزیابی جنبه‌های مختلفی از این معماری استفاده نمود. شبیه سازی مبتنی بر NS-3 که به صورت متن باز است، برای جامعه بزرگ تحقیقاتی به عنوان زیربنای شبیه‌سازی ارائه شده است. ndnSIM یک شبیه‌ساز است که در آن قسمت‌های پایه شبکه NDN با استفاده از مجموعه کلاس‌های c++ به صورت پیمانه‌ای پیاده‌سازی شده است تا جدول بسته‌های درخواست منتظر یا جدول هدایت براساس اطلاعات هر موجودیت از لایه شبکه در NDN را مدل‌سازی نماید که شامل مخزن محتوا، واسط‌های شبکه و همچنین راهبردهای هدایتی هر درخواست باشد [۵].



شکل (۱۱): شمای کلی از اجزای اصلی ndnSIM [5]

خلاصه‌ای از انتزاع مهم‌ترین اجزا به کار گرفته شده در شبیه‌سازی ndnSIM (شکل ۱۱) به صورت زیر است:

NDN L3Protocol: عملیات و تعاملات هسته پروتکل NDN جهت دریافت بسته‌های درخواست و داده از لایه‌های بالایی و پایینی را به وسیله هر واسط پیاده‌سازی می‌کند.

NDN Face: انتزاعی که برای ارتباط یک گره با گره‌های دیگر شبیه‌سازی شده است.

NDN Content Store: این انتزاع جهت ذخیره‌سازی بسته داده استفاده می‌شود.

NDN PIT: انتزاعی برای جدول بسته‌های درخواست در حال انتظار است و نشانگرهای آن در هر واسط به هنگام دریافت هر درخواست ایجاد می‌شود.

NDN FIB: انتزاعی برای جدول FIB در جهت هدایت درخواست‌های رسیده است.

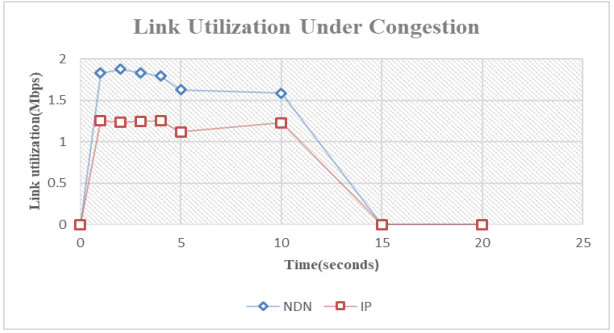
NDN Forwarding Strategy: انتزاعی برای هدایت بسته‌های درخواست و داده است[۵].

۴-۱- سناریوهای طراحی

سه سناریو طراحی در اینجا بررسی می‌شوند. سناریو تحت ازدحام که در آن شبکه‌ای با تعدادی گره که در بعضی از لینک‌های شبکه ازدحام ایجاد خواهد شد.دومین سناریو، سناریوی تحت خرابی لینک است که در آن بعد از اجرای شبیه‌سازی، لینک‌های شبکه خراب و ارسال بسته موقتا قطع خواهد شد و پس از مدتی دوباره ارسال از سر گرفته می‌شود. سومین سناریو، سناریوی تحت گره مهاجم است که در آن گره مهاجم پیشوند نام بسته‌ها را حذف می‌کند.

توپولوژی تعریف شده برای این سناریوها شامل ۴ گره خطی در شبکه NDN است که در آن تأخیر هر پیوند برابر ۵۰ میلی ثانیه و پهنای باند بین دو گره وسط ۱ مگابیت بر ثانیه و پهنای باند بین دیگر گره‌ها ۱۰ مگابیت بر ثانیه و نرخ ارسال بسته‌ها ۲۰۰ بسته بر ثانیه می‌باشد که اندازه‌های بسته‌ها متفاوت با RTT متغییر تعیین شده است.

۴-۲- خروجی‌های شبیه‌سازی



شکل (۱۲): بهره‌وری کانال پس از ازدحام

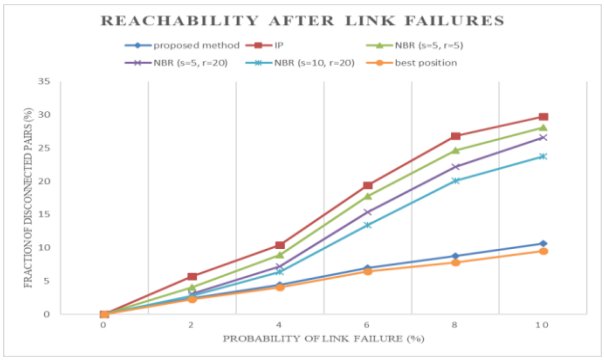
[1] Link layer congestion control

شکل (۱۲) بهره‌وری کانال را پس از ازدحام در شبکه‌های NDN و IP را نشان می‌دهد که در آن محور عمودی استفاده از شبکه و محور افقی زمان را نمایش می‌دهد. در این شکل بهره‌وری IP و NDN مورد مقایسه قرار گرفته‌اند و در پایان هر دو شبکه از دسترس کاربران خارج می‌شوند.

جدول (۲): کمیت‌های IP و NDN در زمان مشخص

Time(sec)	NDN	TCP
0	0	0
1	1.826	1.257
2	1.875	1.231
3	1.831	1.249
4	1.793	1.25
5	1.627	1.117
10	1.584	1.228

برابر جدول (۲)، اگر زمان در هر دو شبکه ۱۰ ثانیه در نظر گرفته شود آنگاه NDN نسبت به IP، ۲۲/۴۸٪ بهره‌وری کانال را در ازدحام بهبود می‌بخشد.



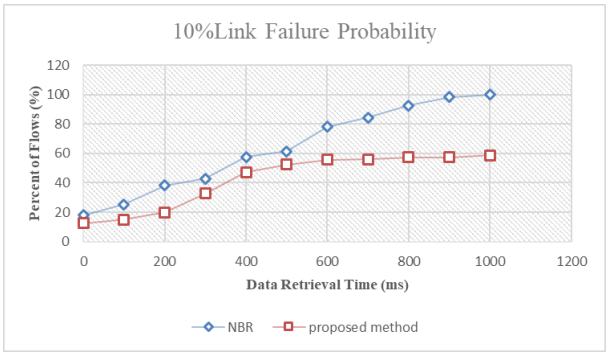
شکل (۱۳): قابل دسترس بودن شبکه در حمله ربودن جلسه

شکل (۱۳) قابل دسترس بودن شبکه در حالت‌های مختلف را نشان می‌دهد که محور عمودی درصد قطع دسترسی و محور افقی درصد احتمال خرابی شبکه است. همان‌طور که در شکل مشخص می‌باشد با افزایش احتمال خرابی لینک شبکه مبتنی بر IP نسبت به proposed method و NBR ضعیف‌تر عمل می‌کند و احتمال از بین رفتن اتصال بین گره‌ها افزایش می‌یابد. در این شکل، NBR با زمان (s) و تعداد دفعات ارسال متغییر (r) مورد بررسی قرار گرفته است.

جدول (۳): کمیت‌های هر شبکه با درصد قطع دسترسی مشخص

Fraction of Disconnected Pairs (%)	proposed method	IP	NBR (s=5, r=5)	best position
2	2.4	5.73	4.081	2.24
6	7	19.39	17.74	6.47
10	10.65	29.77	28.08	9.55

همانگونه که از جدول (۳) استخراج می‌شود، با درصد قطع دسترسی ۱۰ درصد، proposed method توانسته است با ۷٪ خطا نسبت به بهترین موقعیت، بهبودی ۱۳۸/۷۵٪ ی نسبت به IP و ۷۰٪ ی نسبت به روش NBR ارائه کند.



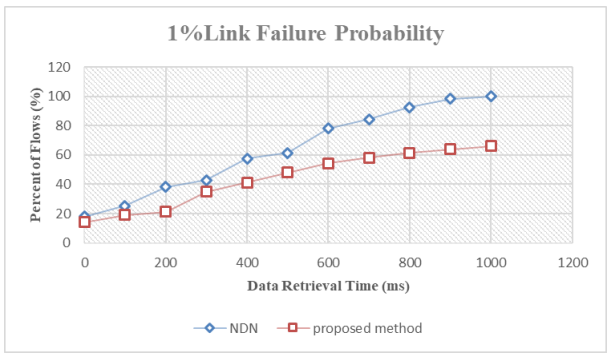
شکل (۱۴): میزان بازیابی داده با احتمال خرابی ۱۰٪ لینک در ازدحام

شکل (۱۴) میزان بازیابی داده با احتمال خرابی ۱۰٪ لینک را نشان می‌دهد که در آن محور عمودی درصد جریانات و محور افقی زمان بازیابی اطلاعات را نمایش می‌دهد. در این شکل تنها روش NBR و proposed method مورد مقایسه قرار گرفته‌اند.

جدول (۴): کمیت‌های شبکه در دو حالت NDN و proposed method

Data Retrieval Time (ms)	NBR	proposed method
300	42.75	32.7
600	78.08	55.66
900	98.38	57.42
1000	100	58.71

نتایج حاصل از جدول (۴)، نشان از بهبود راهکار proposed method نسبت به NBR می‌باشد که توانسته است حداقل ۴۱/۳٪ از بسته‌ها را در زمان بازیابی ۱۰۰۰ میلی ثانیه با موفقیت ارسال کند.



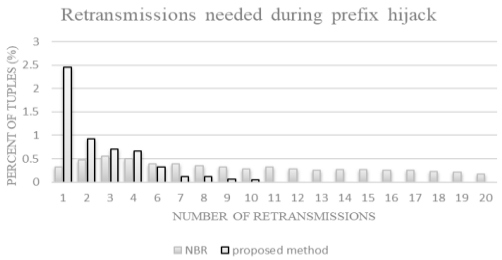
شکل (۱۵): میزان بازیابی داده با احتمال خرابی ۱٪ لینک در ازدحام

شکل (۱۵) میزان بازیابی داده را با احتمال خرابی ۱٪ لینک نشان می‌دهد که در آن محور عمودی درصد جریانات و محور افقی زمان بازیابی اطلاعات را نمایش می‌دهد. در این شکل نیز تنها روش NBR و proposed method مورد مقایسه قرار گرفته‌اند. نتایج حاصل، نشان از بهبود روش پیشنهادی نسبت به NBR می‌باشد که توانسته است حداقل ۴۰٪ از بسته‌ها را با موفقیت ارسال کند.

جدول (۵): کمیت‌های شبکه در دو حالت NDN و proposed method

Data Retrieval Time (ms)	NDN	proposed method
300	42.75	35.05
600	78.08	54.28
900	98.38	63.83
1000	100	65.95
Data Retrieval Time (ms)	NDN	proposed method

نتایج حاصله از جدول (۵)، نشان از بهبود راهکار proposed method نسبت به NBR می‌باشد که توانسته است حداقل ۳۴/۰۵٪ از بسته‌ها را در زمان بازیابی ۱۰۰۰ میلی ثانیه با موفقیت ارسال کند.



شکل (۱۶): میزان نیاز به ارسال مجدد در ازدحام با دو حالت روش proposed method و NBR

در شکل (۱۶) میزان نیاز به ارسال مجدد در دو حالت proposed method و NBR را مشاهده می‌کنید که در آن محور عمودی درصد خطا شبکه و محور افقی تعداد دفعات ارسال مجدد است. در زمانی که شبکه توسط مهاجم مورد حمله قرار گیرد و بسته از بین برود، نیاز به ارسال مجدد آن بسته می‌باشد. همانطور که در شکل می‌بینیم در ابتدا درصد خطای proposed method از NBR بیشتر است. اما با گذشت زمان و تعداد دفعات ارسال مجدد درصد خطا در روش پیشنهادی به صفر می‌رسد و بازدهی بهتری نسبت به NBR دارد.

جدول (۶): کمیت‌های شبکه در دو حالت NDN و proposed method

proposed method	NBR	Number of Retransmissions
0.93	0.47	2
0.66	0.5	4
0.05	0.28	10
0	0.27	15
0	0.17	20

نتایج حاصله از جدول (۶)، نشان از برتری روش پیشنهادی نسبت به NBR می‌باشد که توانسته است میزان نیاز به ارسال مجدد را حداقل ۲۷٪ کاهش دهد.

۴-۳- مقایسه روش پیشنهادی با الگوریتم های موجود در کارایی

مکانیزم NBR نشان داد می تواند ازدحام را در مسیرهای چندگانه گام به گام کنترل کند و از طریق اعمال محدودیت در بسته‌های درخواستی، امنیت شبکه را در برخورد با حملات ناشی از حملات منع خدمت و حمله ربودن پیشوند تضمین کند[۹]. اما این روش محدودیت‌های بسیاری دارد. اول آن‌که قادر به بررسی ترافیک داده برگشتی به صورت پویا نیست. یعنی پس از هدایت بسته درخواستی، مسیریاب هیچ کاری را انجام نمی‌دهد تا زمانی که بسته داده خواسته شده بازیابی شود و پس از بازیابی مسیریاب قادر خواهد بود تا محتوای داده را بازگشت دهد و یا آن را به طور موقت در حافظه نهان مسیریاب، ذخیره سازی کند. مسیریاب حتی دانشی نسبت به اندازه بسته داده دریافتی نخواهد داشت؛ بنابراین حتی با اعمال محدودیت در بسته‌های درخواستی ممکن است ترافیکی شدیدی از داده‌ها ایجاد شود. دوم آن‌که مسیریاب قادر به بررسی مسائل در ارتباط با پر شدن بافر نمی باشد[۹]. یک گزینه پیشنهادی اعمال مکانیزم AQM[۱] در پیوند بر روی مسیریاب‌های بعدی است، اما پس از پر شدن بافر توسط بسته‌های درخواست، بدون اطلاع رسانی بسیاری از بسته‌ها دور ریخته خواهند شد؛ بطوریکه درخواست کنندگان می توانند از طریق ارسال مجدد بسته درخواست، هریک از اطلاعات درخواستی خود را بازیابی کنند. در چنین شرایطی بسته‌ها از تمام توانایی‌های هدایت هوشمند در شبکه NDN بهره‌مند نمی‌شوند[۱۰]. سوم آن‌که در میان ارسال و دریافت‌های همزمان، تعادل کافی برقرار نمی‌شود، بنابراین منابع موجود در شبکه به صورت عادلانه برای استفاده درخواست‌کنندگان تخصیص داده نمی‌شود[۱۱]. محاسبه محدودیت موجود در بسته‌های درخواست مهم‌ترین عامل به کار گرفته شده در عملکرد NBR می‌باشد. بر اساس روش پیشنهادی در این مقاله از دو عامل ویژه جدید برای بهینه‌سازی این محدودیت استفاده شده است. روش پیشنهادی به صورت بهینه قادر است محدودیت استفاده از بسته‌های درخواست را بر اساس استفاده از پیوند مرتبط با آن، تنظیم کند. میزان این محدودیت، در زمان دریافت داده معتبر، افزایش و در زمان تشخیص ازدحام، کاهش

[۱] Active queue management؛ تکنیکی است که شامل دور انداختن یا علامت‌گذاری بسته‌ها بر اساس روش ECN قبل از اینکه مسیریاب پرشود.

می‌یابد. در روش تشخیص ازدحام دو روش بررسی گردید که به برآورد RTT در شبکه وابستگی ندارد، اما تخمین درستی از میزان محدودیت در بسته های درخواست می تواند به همراه داشته باشد:

۱ - ارسال تصادفی Nack (REN) در شبکه‌های که در آن مسیریاب‌های بعدی بر طول صف نظارت می‌کنند و به صورت فعال اگر صف در حال رشد باشد از طریق یک Nack آن را به مسیریاب قبلی اطلاع می‌دهند.

۲ - تشخیص ازدحام لایه پیوند (LCC) در شبکه‌های نامدار که از طرح ارائه شده آن در IP، برای NDN استفاده شده است که در آن هر مسیریاب شامل یک شماره ترتیب به بسته درخواست اضافه می کند تا به جلو هدایت شود. در انتهای دیگر پیوند، مسیریاب بسته‌های از دست رفته را تشخیص می دهد و از آن به‌عنوان عاملی جهت تشخیص ازدحام استفاده می‌کند و این کار از طریق فاصله ایجادشده در شماره ترتیب بسته‌های دریافتی صورت می‌گیرد.

روش پیشنهادی باعث حداقل بهبود ۷۰ درصدی دسترسی شبکه و بهبود ۴۰ درصدی بازیابی داده شبکه و بهبود ۲۷ درصدی نیاز به ارسال مجدد شبکه در حالت ازدحام نسبت به راهکارهای پیشین می‌شود، بدون آن‌که از یک پیوند به صورت انحصاری در ارسال یک جریان داده استفاده شود. برای به اشتراک‌گذاری پهنای باند در مسیرهای چندگانه، از مکانیزم ایجاد تعادل محدودیت بسته‌های درخواست استفاده می‌شود که در آن مجموعه محدودیت بسته‌های درخواست به صورت عادلانه بر روی هریک از واسط های موجود در جریان‌های فعال تقسیم می‌گردد و بدین ترتیب می توان از کنترل عادلانه NBR در روش پیشنهادی بهره‌مند شد.

۵- نتیجه‌گیری

شبکه‌های نامدار یک معماری اینترنت است که به‌صورت شبکه توزیع طراحی شده است. برای دسترسی به این شبکه‌ها کاربر باید برنامه‌های نرم‌افزاری نظیر ndnSIM را نصب کند. این شبکه‌ها به‌عنوان یک مسیریاب نرم‌افزاری عمل می‌کند تا امکان برقراری ارتباط بدون نیاز به آدرس‌های IP یا سرورهای سخت‌افزاری را فراهم سازد. شبکه‌های نامدار برای سازمان‌هایی که به‌دنبال اشتراک داده‌ها در شبکه‌های عمومی هستند و حفظ امنیت انتقال و محتوا برای آن‌ها مهم است، جذاب است. از آن‌جا که انتقال داده با استفاده از شبکه نامدار به آدرسIP نیاز ندارد، بسته‌های معمولی در حین فرآیند انتقال قابل شناسایی نیستند. در این روش انتقال داده، فقط فرستنده و گیرنده می‌دانند کدام داده‌ها باید بازسازی شوند. به این ترتیب، لایه امنیتی جدیدی نظیر رمزگذاری فراهم خواهد شد. در این مقاله به بررسی شبکه‌های نامدار و تأثیر حملات منع خدمت توزیع شده بر آن پرداخته شده تا نقطه ضعف اصلی این شبکه در برابر این حملات شناسایی گردد. بعد از شناسایی نقطه ضعف، به ارائه یک روش به منظور کاهش اثر این نقطه ضعف پرداخته شده است. در روش پیشنهادی تغییراتی در Nack ایجاد شده و پروتکل تشخیص ازدحام لایه پیوند به راهبرد بهترین مسیر شبکه‌های نامدار (NBR) افزوده می‌شود. این تغییرات به منظور استفاده مؤثرتر از پهنای باند شبکه و با هدف بهره‌وری بیشتر از این شبکه‌ها در صورت بروز ازدحام و حمله منع خدمت، صورت پذیرفته است.

شبیه‌سازی روش پیشنهادی، در شبیه‌ساز ndnSIM پیاده سازی گردید و عملکردهای آن تحت سناریوهای مختلف ازدحام در جهت افزایش امنیت مسیریابی، مورد ارزیابی قرار گرفت. روش پیشنهادی در حالت ازدحام، باعث حداقل بهبود ۷۰ درصدی دسترسی شبکه و بهبود ۴۰ درصدی بازیابی داده شبکه و ۲۷ درصدی نیاز به ارسال مجدد شبکه نسبت به راهکارهای پیشین شده است. به طور کلی قادر است در میان جریان‌های متعدد موجود در شبکه، تعادل را برقرار کند و در ترکیب آن با هدایت هوشمند موجود در شبکه، قادر به استفاده از منابع شبکه با بهره‌وری و گذردهی بیشتر و تأخیر کمتر در شروع برنامه، نسبت به NBR خواهد بود. این موضوع می‌تواند تضمینی برای امنیت بیشتر در برخورد با منع خدمت و حملات سیاه چاله و ربودن پیشوند باشد.

به عنوان کارهای آینده می‌توان با استفاده از حافظه نهان (CS) در الگوریتم هدایت هوشمند کنترل بهتری بر جریان بسته‌های درخواست داشته باشد یا می‌توان با ایجاد یک تعادل بار برنامه‌ریزی شده در شبکه از بوجود آمدن ازدحام جلوگیری کند علاوه بر این می‌توان با استفاده از یک عامل متغییر به عنوان ضریب اطمینان در هر مسیر با توجه به داده‌های بازگشتی، سرعت افزایش و کاهش محدودیت در مسیر را بهبود ببخشد.

۶- مراجع

[1] C.Yi, A. Afanasyev, L. Wang, B. Zhang and L. Zhang, Adaptive forwarding in named data networking, ACM SIGCOMM Comput. Commun. Rev., Jun.2012.

[2] C. Science, "Scrutiny of DDoS Attacks Defense Mechanisms," Int. J. Adv. Res. Comput. Sci. Technol, vol.2, no. 1, pp.154–157, 2014.V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs and R. L. Braynard. Networking Named Content. In Proceedings of ACM CoNEXT, 2009.

[3] C.Yi, Adaptive forwarding in named data networking, A Dissertation Submitted to the Faculty of the Department

of Computer Science in Partial Fulfillment of the Requirements, Graduate College the University of Arizona, Jun. 2014.

[4] B. Adamson, c. bormann, M. Handley and j. macker, multicast negative – Acknowledgement (Nack) Building blocks, IETF, November2010.

[5] S. Mastorakis, A. Afanasyev, I. Moiseenko, and L. Zhang, ndnSIM2.0: A new version of the NDN simulator for NS-3, NDN, Technical Report NDN0028, 2015.

[6] C.Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang and L. zhang. A case for stateful forwarding plane, computer communications: ICN special Issue,36(7):779{791, april.2013.

[7] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs and R. L. Braynard. Networking Named Content. In Proceedings of ACM CoNEXT, 2009.

[8] C.Yi, A. Afanasyev, L. Wang, B. Zhang, and L. Zhang, Adaptive forwarding in named data networking, ACM SIGCOMM Comput. Commun. Rev., Jun. 2012.

[9] C.Yi, Adaptive forwarding in named data networking, A Dissertation Submitted to the Faculty of the Department of Computer Science in Partial Fulfillment of the Requirements, Graduate College the University of Arizona, Jun. 2014.

[10] S. Mastorakis, A. Afanasyev, I. Moiseenko, and L. Zhang, ndnSIM2.0: A new version of the NDN simulator for NS-3, NDN, Technical Report NDN0028, 2015.

[۱۱] آباده, ص. (۱۳۹۶). داده کاوی کـاربردی. تهـران: نیـاز دانـش.