Scientific Journal of Electronic & Cyber Defense
Vol. 11, No. 3, Autumn 2023, Serial No. 43
ISSN: 2322-4347 , E-ISSN: 2980-8979

Evaluation and proof of routing algorithm in Tor anonymity network

Hosseinian Barzi, S. H. [1*] , **Anarfarhad, M.** [2]

Master's degree, , Shahid Beheshti University, Tehran,Iran.

((Received: 2023/02/22, Revised: 2023/07/02, Accepted: 2023/08/26, Published: 2023/09/28)

DOR: https://dorl.net/dor/20.1001.1.23224347.1402.11.3.2.7

Abstract

Tor is one of the most popular networks providing anonymity and privacy on the Internet that works using volunteer systems from around the world. Low latency operation makes it suitable for things like web browsing. The way to select a path in tor network is one of the influential factors in the efficiency and security of this network. The path selection algorithm in the tor network has undergone many changes over its original design. These changes have been made for reasons such as increased efficiency, reliability, and load balancing, sometimes even in response to introduced attacks, they have to change the path selection algorithm. So far, many papers have looked at how to choose relays in the creation of circuits, but none of them, despite the open-source of the tor code, did not analyze the routing algorithm and the weighting method of the relays. And they have not proved logically and mathematically the relations used in this algorithm. In this paper, we attempt after fully analyzing the tor routing algorithm, for the first time, the exact logical and mathematical proofs of the relationships used in this algorithm are discussed. In this paper, we tried to investigate the anonymous network routing algorithm as the largest current anonymous network in the world.

Keywords: Tor Network؛ Anonymity؛ Routing

Corresponding Author Email: hatefbarz @gmail.com

نشریه علمی "پدافند الکترونیکی و سایبری"
سال یازدهم، شماره ۳، پاییز ۱۴۰۲، ص ۲۴-۱۵

علمی – پژوهشی

ارزیابی و اثبات الگوریتم مسیریابی شبکه گمنامی تُر

سید هاتف حسینیان برزی[1*]، میلاد انارفرهاد[2]

۱- کارشناسی ارشد، دانشگاه شهید بهشتی، ۲- کارشناسی‌ارشد ، دانشگاه علم و صنعت،تهران ، ایران

(دریافت: ۱۴۰۱/۱۲/۰۳، بازنگری: ۱۴۰۲/۰۴/۱۱، پذیرش: ۱۴۰۲/۰۶/۰۴، انتشار: ۱۴۰۲/۰۷/۰۶)
DOR: https://dorl.net/dor/20.1001.1.23224347.1402.11.3.2.7

چکیده

تُر یکی از محبوب‌ترین شبکه‌های فراهم‌کننده گمنامی و حفظ حریم خصوصی در سطح اینترنت است که با استفاده از سیستم‌های داوطلبانه در سرتاسر جهان کار می‌کند. کارکرد تُر با تأخیر کم، آن را برای اموری هم چون گردش در وب مناسب می‌سازد. نحوه‌ی انتخاب مسیر در شبکه‌ی تُر از عوامل تأثیرگذار در کارایی و امنیت این شبکه است. الگوریتم انتخاب مسیر در شبکه‌ی تُر نسبت به طراحی اولیه آن، تاکنون دستخوش تغییرات زیادی شده است. این تغییرات به دلایلی چون افزایش کارایی، قابلیت اطمینان و توازن بار صورت گرفته‌اند و یا حتی برخی اوقات در پاسخ به حملات معرفی‌شده، مجبور به تغییر الگوریتم انتخاب مسیر شده‌اند. مقالات زیادی تاکنون به بررسی شیوه‌ی انتخاب رله‌ها در تشکیل مدار پرداخته‌اند ولی هیچ‌کدام باوجود منبع باز بودن کد تُر، الگوریتم مسیریابی و نحوه وزن‌دهی رله‌ها را مورد تجزیه و تحلیل قرار نداده‌اند و روابط مورد استفاده در این الگوریتم را از لحاظ منطقی و ریاضی اثبات نکرده‌اند. در این مقاله سعی شده است بعد از تجزیه و تحلیل کامل الگوریتم مسیریابی تُر، برای اولین بار به اثبات دقیق منطقی و ریاضی روابط مورد استفاده در این الگوریتم پرداخته شود.

کلیدواژه‌ها: شبکه تُر، گمنامی، مسیریابی

۱. مقدمه

امروزه، محافظت از حریم شخصی کاربران تبدیل به یکی از مهم‌ترین نیازمندی‌های حفظ امنیت شده است. اگرچه با استفاده از رمز کردن انتها به انتها، می‌توان جلوی دسترسی غیرمجاز به محتوای پیغام‌های رد و بدل شده را گرفت، ولی با این‌حال همچنان اطلاعات زیادی با استفاده از تحلیل ترافیک به دست می‌آید که می‌تواند موجب نقض امنیت کاربران شود. در برخی شرایط، دانستن زمان‌بندی، آدرس‌دهی و یا حجم ارسال داده، می‌تواند به‌اندازه‌ی محتوای پیغام، نشت اطلاعات داشته باشد، خصوصاً در شرایط بی‌درنگ مثل یک محیط نظامی که ارسال یک پیغام و یا برقراری یک تماس خاص می‌تواند نشانه‌ی یک طرح و یا تصمیم قریب الوقوع باشد. برای اینکه بتوان از حریم شخصی عامل‌های برقراری یک ارتباط حفاظت نمود می‌بایست علاوه بر اینکه از دسترسی غیرمجاز به داده جلوگیری کرد، تدابیری اندیشید که با استفاده از آن‌ها وابستگی طرفین یک ارتباط باهم را پنهان نمود.

ارتباط مبتنی بر گمنامی یکی از فناوری‌های مورد استفاده جهت حفظ حریم شخصی است به‌نحوی‌که به کاربر این امکان را می‌دهد تا بتواند با دیگران ارتباط برقرار نماید، بدون نیاز به اینکه هویت خود و یا شخصی که می‌خواهد با او ارتباط برقرار کند را آشکار سازد. در چنین ارتباطی هیچ‌کس نباید متوجه هرگونه وابستگی عامل برقراری ارتباط به عمل و یا جریان خاصی شود. کاربرانی که از ارتباط گمنام استفاده می‌کنند، سعی می‌کنند که از حریم شخصی خود در برابر آن دسته‌ای که قصد آشکار کردن این ارتباط را دارند، حفاظت نمایند. اطلاعاتی که از این طریق فاش می‌شود ممکن است، خسارات سنگین و غیرقابل بازگشتی را به ثمر برسانند.

در حال حاضر، فقط سیستم‌های معدودی وجود دارند که در زمینه ارائه‌ی یک ارتباط گمنام عملی و کم تأخیر فعالیت می‌کنند. یکی از مشهورترین این سیستم‌ها، تُر نام دارد که بر پایه‌ی مسیریابی پیازی پیاده‌سازی شده است.

عموم این سیستم‌ها با عبور ترافیک از مجموعه‌ای از رله‌ها با پروتکل‌های متفاوت سعی در گمنام ماندن ارتباط می‌کنند. کاربران هر یک از این شبکه‌ها گاهی حین استفاده، با تأخیرهای زمانی طولانی روبه‌رو می‌شوند که این تأخیرها توسط بسیاری از کاربران قابل تحمل نیست. در نتیجه با ترک از آن شبکه، تعداد اعضای مجموعه‌ی گمنامی کاهش می‌یابد و در یک مجموعه‌ی گمنامی کوچک نقض امنیت راحت‌تر می‌شود.

شبکه‌ی تُر به‌منظور برقراری یک ارتباط گمنام کم تأخیر

* رایانامه نویسنده مسئول: *Corresponding Author E-mail: hatefbarz*

طراحی‌شده ولی کاربران این شبکه به دلیل سرعت مناسب از عملکرد این شبکه راضی هستند و روزبه‌روز به کاربران این شبکه افزوده می‌شود. مهم‌ترین عامل تأثیرگذار در کارایی و امنیت این شبکه، نحوه‌ی انتخاب مسیر از میان هزاران رله موجود در شبکه است که عموماً طولی برابر سه دارد. به همین منظور ما در این مقاله، جوانب مختلف روش انتخاب مسیر در شبکه تُر را مورد بررسی قرار می‌دهیم. همچنین الگوریتم مسیریابی مبتنی بر پهنای باند را تشریح و برای اولین بار روابط موجود در آن را به‌طور دقیق از لحاظ منطقی و ریاضی اثبات می‌کنیم.

سازمان‌دهی مقاله به این صورت است که در قسمت دوم به‌صورت مختصر شبکه گمنامی تُر معرفی می‌شود. در قسمت سوم نحوه انتخاب مسیر و جزئیات آن مورد بررسی و ارزیابی قرار می‌گیرد. در قسمت چهارم به الگوریتم وزن‌دهی رله‌ها و اثبات دقیق منطقی و ریاضی روابط مورداستفاده در آن می‌پردازیم. در قسمت پنجم نیز الگوریتم مسیریابی در شبکه تُر را با توجه به ضرایب پهنای باند هر یک از رله‌ها شرح داده و سپس بخش‌های ششم و هفتم در انتهای کار دربردارنده نتیجه‌گیری کلی و مراجع خواهند بود.

۲. معرفی تُر

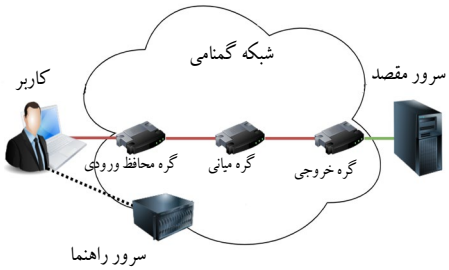
تُر آخرین پروتکل تکامل‌یافته‌ی مسیریابی پیازی است که در سال ۲۰۰۴ توسط راجر دینگلدین و همکارانش در [۱] معرفی گردید. طراحان شبکه‌ی تُر، تغییراتی را در شبکه‌ی گمنامی پیاز اعمال‌کردند تا امنیت، کارایی و گسترش‌پذیری آن را بهبود بخشند. پس از گذشت چند سال، طبق مرجع [۲] این شبکه در سال ۲۰۱۰ بزرگ‌ترین شبکه‌ی گمنامی پیاده‌سازی شده لقب گرفت که شامل بیش از ۲۰۰۰ رله است و روزانه صدها هزار کاربر از آن استفاده می‌کنند.

عملکرد این شبکه به این صورت است که کاربر تُر ابتدا لیست کامل رله‌ها (راهنمای شبکه[1]) و سپس اطلاعات دقیق‌تر هرکدام از آن‌ها (توصیف‌کننده رله[2]) را از تصدیق‌کننده[3]های شبکه بارگیری می‌نماید. راهنمای شبکه توسط تصدیق‌کننده‌ها امضا می‌شود تا از دست‌کاری محتویات آن جلوگیری شود. در شبکه‌ی تُر هر کاربر مسیری شامل سه رله را انتخاب می‌نماید که پس از تبادل کلید با اولین آن‌ها، از طریق آن ارتباط رمز شده یک تونل می‌زند و با رله دوم کلیدی را به اشتراک می‌گذارد و همین‌طور الی آخر. تمام ارتباطات در شبکه‌ی تُر رمز می‌باشند به‌جز مسیر بین رله آخر و مقصدی که کاربر می‌خواهد با او ارتباط برقرار کند.

برای مقاومت در برابر حملات طولانی‌مدت در شبکه‌های گمنامی، هر کاربر وقتی نرم‌افزار تُر خود را برای اولین بار اجرا می‌کند، سه رله محافظ[4] از مجموعه رله‌های سریع و پایدار انتخاب می‌کند. تا زمانی که این محافظ‌ها در دسترس هستند، محافظ جدیدی انتخاب نمی‌شود. اولین رله در هر مدار که توسط کاربر انتخاب می‌شود، یکی از این سه رله محافظ است. همچنین کاربر رله آخر را از زیرمجموعه رله‌های تُر به نحوی انتخاب می‌کند که اجازه دهد ترافیک به شبکه اینترنت منتقل شود (لزوماً ترافیک به شبکه اینترنت نمی‌رود). به این رله، رله خروجی[5] می‌گویند. هر رله خروجی یک سیاست خروج دارد که پورت‌هایی را که آن رله می‌تواند ترافیک را به آن‌ها ارسال کند، مشخص می‌کند. بنابراین انتخاب رله خروجی باید به نحوی باشد که اطلاعات ارسالی توسط کاربر، با سیاست خروجی آن رله هماهنگی داشته باشد. هر رله دیگری می‌تواند به‌جای رله میانی[6] استفاده شود.

یکی از مهم‌ترین دلایل تأثیرگذار روی امنیت و کارایی چنین شبکه‌هایی، نحوه انتخاب مسیر است. نحوه‌ی نامناسب انتخاب مسیر باعث می‌شود که بسته‌ها از مسیرهای با کارایی پایین عبور کنند. علاوه بر این، استفاده‌ی بیش از حد از رله‌های دارای شرایط خوب تا حدی انتخاب مسیر را در شبکه‌های گمنام ساز قابل پیش‌بینی می‌کند. این باعث می‌گردد که برخی رله‌های دارای پهنای باند بالا زیاد انتخاب شوند تا جایی که سایر رله‌ها اصلاً مورد استفاده قرار نمی‌گیرند. از این طریق نقض گمنامی کاربران و حمله به این شبکه به‌راحتی امکان‌پذیر می‌شود.

شکل (۱)، معماری کلی شبکه گمنامی تُر را نشان می‌دهد.



شکل (۱). اجزای شبکه گمنامی تُر

۳. انتخاب مسیر در شبکه تُر

الگوریتم انتخاب مسیر در شبکه‌ی تُر نسبت به طراحی اولیه آن، تاکنون دست‌خوش تغییرات زیادی شده است. این تغییرات به دلایلی چون افزایش کارایی، قابلیت اطمینان و توازن بار صورت گرفته‌اند و یا حتی برخی اوقات در پاسخ به حملات معرفی‌شده[۳]-[۴]، مجبور به تغییر الگوریتم انتخاب مسیر

[1] Network Consensus
[2] Relay Descriptor
[3] Directory Authority
[4] Guard Relay
[5] Exite Node
[6] Milddel Node

شده‌اند.

کلیات انتخاب مسیر به این صورت است که ابتدا آخرین رله مسیر و سپس سایر رله‌ها انتخاب می‌شوند. در تمام مسیرهای انتخاب شده یک رله اجازه ندارد بیشتر از یک بار انتخاب شود و به‌منظور جلوگیری از حمله‌ی سیبل[1] [۵] تمام رله‌های انتخاب شده می‌بایست دارای آدرس‌های پروتکل اینترنت از زیر شبکه‌های مختلف باشند. (این حمله به این صورت است که حمله‌کننده چند رله را روی یک سیستم یا یک شبکه‌ی محلی راه‌اندازی می‌کند تا کاربر به طور اتفاقی مسیری را انتخاب کند که رله ابتدا و انتهای آن زیر مجموعه‌ی این رله‌ها باشد. سپس با مرتبط کردن این دو جریان به یکدیگر گمنامی کاربر را نقض نماید) از موارد بسیار مهم و تأثیرگذار در امنیت شبکه‌ی تُر نحوه‌ی انتخاب مسیر در این شبکه است. اینکه ترافیک ما از چه رله‌هایی عبور کند و به چه کشورهایی ارسال شود، از چه مسیری عبور نماید و یا اینکه چه سیستم‌های خودمختاری[2] امکان مانیتور کردن ترافیک ما را داشته باشند همه و همه تحت تأثیر روش انتخاب مسیر می‌باشند.

اگر فرض را بر ایده‌آل بودن گمنامی در انتخاب مسیر شبکه تُر در نظر بگیریم، همه کاربران تُر، باید رله‌ها را به‌صورت یکنواخت از میان مجموعه همه رله‌های فعال انتخاب کنند. در این صورت مهاجمان نمی‌توانند در فرآیند انتخاب مسیر هیچ اختلالی ایجاد کنند مگر اینکه تعداد روترهای بیشتری را به خدمت بگیرند. اتخاذ این روش منجر به یک عملکرد ضعیف در شبکه گمنامی می‌شود، چراکه روترهای با عملکرد ضعیف با همان احتمالی انتخاب شده‌اند که روترهایی با منابع و عملکرد قوی‌تر در شبکه حضور دارند [۳]. بنابراین برای بالا بردن عملکرد، در تُر انتخاب هر رله بر اساس تمایل به انتخاب رله‌های با پهنای باند بیشتر، وزن‌دهی و وزن هر رله بر اساس پرچم‌های آن و مکان قرارگیری آن در مسیر، تعیین می‌گردد.

مقالات زیادی تاکنون به بررسی شیوه‌ی انتخاب رله‌ها در شبکه تُر پرداخته‌اند و روش‌های متنوعی ارائه شده است که ازجمله این روش‌ها می‌توان به انتخاب مسیر با استفاده از مفهوم اعتماد [[۶]-[۸]] ، انتخاب مسیر با توجه به عبور از سیستم‌های خودمختار[[۹]-[۱۰]] و انتخاب مسیر با در نظر گرفتن زمان رفت‌وبرگشت بسته‌ها [[۱۱]-[۱۲]] اشاره کرد. همان‌طور که ذکر شد در حال حاضر انتخاب مسیر در تُر براساس پهنای باند رله‌ها وزن‌دهی می‌شود که در ادامه مورد بررسی قرار می‌گیرد و روابط موجود در آن مورد ارزیابی و اثبات قرار می‌گیرند.

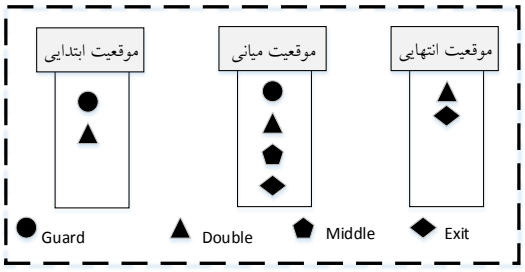
۴. الگوریتم وزن‌دهی پهنای باند رله‌ها

در حالت کلی در شبکه گمنامی تُر یکسری رله داریم که فرض می‌کنیم هرکدام از این رله‌ها دارای دو مشخصه پهنای باند و برچسب هستند که توسط تصدیق‌کننده به هر یک از رله‌ها منتصب شده است.

شبکه تُر، احتمال انتخاب هرکدام از رله‌ها را در سه موقعیت ابتدایی، میانی و انتهایی مسیر مشخص می‌کند. عملکرد قابل قبول تُر همراه با حفظ امنیت است. یعنی همواره به دنبال مصالحه‌ای بین عملکرد و امنیت است. این مفهوم و هدف در شکل (۲) نشان داده‌شده است.

همان‌طور که از شکل (۲) مشخص است هر یک از رله‌ها مطابق با برچسب خود می‌تواند در هر یک از موقعیت‌های مسیر قرار بگیرد، همچنین مطابق با مقدار پهنای باند، ضریبی برای حضور در هر یک موقعیت‌های مسیر اتخاذ می‌کند.

قابل توجه است که این وزن‌دهی به رله‌ها درنهایت برای انتخاب یک مسیر مناسب برای عبور داده البته با حفظ امنیت است. همان‌طور که اشاره شد، تُر برای متعادل کردن و جلوگیری از سرریز ترافیک و کمبود پهنای باند در بین رله‌های مختلف از الگوریتم وزن‌دهی براساس پهنای باند استفاده می‌کند[۱۳].



شکل (۲). هدف کلی از وزن‌دهی رله‌ها

این الگوریتم برپایه چند اصل بنیان‌گذاری شده است. این اصول به قرار زیر است:

۱. مجموع پهنای باند رله‌ها در موقعیت میانی برابر مجموع پهنای باند رله‌ها در موقعیت ابتدایی است.

۲. مجموع پهنای باند رله‌ها در موقعیت انتهایی برابر مجموع پهنای باند رله‌ها در موقعیت ابتدایی است.

۳. رله‌ها با برچسب Double در هر سه موقعیت (ابتدایی، میانی و انتهایی) می‌توانند قرار بگیرند.

۴. رله‌ها با برچسب Guard تنها در موقعیت‌های ابتدایی و میانی می‌توانند قرار بگیرند.

۵. رله‌ها با برچسب Exit تنها در موقعیت‌های انتهایی و میانی می‌توانند قرار بگیرند.

با توجه به هر یک از اصول مطرح‌شده، ۵ معادله به شرح زیر به دست می‌آید.

[1] Sybil attack
[2] Autonomous Systems (AS)

$$W_{gg}G + W_{gd}D = M + W_{md}D + W_{me}E + W_{mg}G \quad (۱)$$

$$W_{gg}G + W_{gd}D = W_{ed}D + W_{ee}E \quad (۲)$$

$$W_{ed}D + W_{md}D + W_{gd}D = D \quad (۳)$$

$$W_{mg}G + W_{gg}G = G \quad (۴)$$

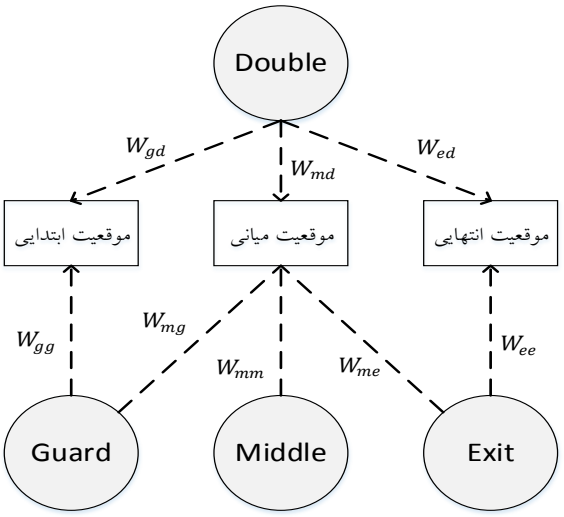
$$W_{me}E + W_{ee}E = E \quad (۵)$$

معادلات (۱) و (۲) از این حقیقت ناشی می‌شوند که پهنای باند باید در سه موقعیت مسیر به صورت یکنواخت تقسیم شوند. شکل (۳) به گونه‌ای سعی دارد از زاویه‌ای دیگر مفهوم هر یک از وزن‌های موجود (ضریب حضور هر یک از رله‌ها در موقعیت‌های متفاوت یک مدار) در جدول (۱) را بیان کند.

جدول (۱). پارامترها

پارامترها	تعریف
G	مجموع پهنای باند رله‌هایی که برچسب Guard روی آن‌ها خورده است.
D	مجموع پهنای باند رله‌هایی که برچسب Guard و Exit (دوتایی (Double)) روی آن‌ها خورده است.
E	مجموع پهنای باند رله‌هایی که برچسب Exit روی آن‌ها خورده است.
M	مجموع پهنای باند رله‌هایی که هیچ برچسبی روی آن‌ها نخورده است.
T	مجموع پهنای باند تمام رله‌ها
W_{gd}	وزن و احتمال انتخاب رله‌هایی که برچسب Guard و Exit دارند، برای اینکه در موقعیت ابتدایی قرار بگیرند.
W_{md}	وزن و احتمال انتخاب رله‌هایی که برچسب Guard و Exit دارند، برای اینکه در موقعیت میانی قرار بگیرند.
W_{ed}	وزن و احتمال انتخاب رله‌هایی که برچسب Guard و Exit دارند، برای اینکه در موقعیت انتهایی قرار بگیرند.
W_{me}	وزن و احتمال انتخاب رله‌هایی که برچسب Exit دارند، برای اینکه در موقعیت میانی قرار بگیرند.
W_{mg}	وزن و احتمال انتخاب رله‌هایی که برچسب Guard دارند، برای اینکه در موقعیت میانی قرار بگیرند.
W_{gg}	وزن و احتمال انتخاب رله‌هایی که برچسب Guard دارند، برای اینکه در موقعیت ابتدایی قرار بگیرند.
W_{ee}	وزن و احتمال انتخاب رله‌هایی که برچسب Exit دارند، برای اینکه در موقعیت انتهایی قرار بگیرند.

این الگوریتم دارای ۵ معادله و ۷ متغیر است. به منظور به دست آوردن ۷ متغیر ذکرشده در جدول (۱)، معادلات مذکور کافی نمی‌باشند. به همین منظور نیاز به ۲ معادله کمکی دیگر است. بنابراین با توجه به مجموع مقادیر پهنای باند رله‌ها با برچسب Guard و Exit، سعی در حل این معادلات می‌کنیم.



شکل (۳). گراف وزن‌دهی رله‌ها در موقعیت‌های متفاوت مسیر

با حل ۵ معادله به دست آمده در شرایط متفاوت، ضریب حضور هر یک از رله‌ها در موقعیت‌های متفاوت یک مدار (ابتدایی- میانی- انتهایی) به دست می‌آید.

در ادامه این معادلات را در ۳ وضعیت احتمالی زیر با توجه به مقادیر G، E و T حل می‌کنیم.

۱) $E \geq T/3$ و $G \geq T/3$ (در موقیعت‌های ابتدایی و انتهایی با کمبود پهنای باند مواجه نیستیم)

۲) $G < T/3$ و $E < T/3$ (در موقیعت‌های ابتدایی و انتهایی با کمبود پهنای باند مواجه هستیم)

۳) $G < T/3$ یا $E < T/3$ (در یکی از دو موقعیت ابتدایی یا انتهایی با کمبود پهنای باند مواجه هستیم)

حال معادلات را در سه حالت مذکور بررسی می‌کنیم.

۴-۱. حالت اول ($G \geq T/3$ و $E \geq T/3$)

در این حالت همان‌طور که مشخص است، وضعیت رله‌های با برچسب Guard و Exit مساعد است. به‌طورکلی می‌توان یک نتیجه‌گیری انتزاعی داشت به‌طوری‌که در هر زمان که شرایط خیلی خوب و یا خیلی بد بود، آنگاه تصمیم‌گیری برای ما راحت‌تر است. بنابراین در این حالت چون شرایط خیلی خوب است (در هر دو موقعیت ابتدایی و انتهایی دچار کمبود پهنای باند نیستیم)، ایده‌آل‌ترین حالت را در نظر می‌گیریم درنتیجه از رله‌های با برچسب Double برای هر سه موقعیت به صورت یکسان بهره می‌گیریم، یعنی باید داشته باشیم:

$W_{ed} = W_{gd} = W_{md}$

طبق رابطه (۳) از ۵ معادله اصلی داریم:

$$W_{ed}+W_{gd}+W_{md}=1 \rightarrow \begin{cases} W_{ed}=1/3 \\ W_{gd}=1/3 \\ W_{md}=1/3 \end{cases} \quad (۶)$$

بنابراین تا اینجا سه وزن از ۷ وزن را به دست آوردیم. برای به دست آوردن بقیه وزن‌ها از همین یافته‌ها با توجه به ۵ معادله اصلی به‌صورت آنچه در ادامه آورده می‌شود، استفاده می‌کنیم.

از روابط (۱)، (۴) و (۶) رابطه (۷) و همچنین از روابط (۲)، (۵) و (۶) رابطه (۸) به دست می‌آید.

$$2W_{gg}G-W_{me}E=M+G \quad (۷)$$

$$W_{gg}G+W_{me}E=E \quad (۸)$$

بنابراین از رابطه (۴) و (۷) و همچنین از رابطه (۵) و (۸) به ترتیب W_{gg} و W_{me} به دست می‌آید.

$$W_{gg}=\frac{M+G+E}{3G} \quad (۹)$$

$$W_{me}=\frac{2E-M-G}{3E} \quad (۱۰)$$

۴-۲. حالت دوم ($E < T/3$ و $G < T/3$)

در این شرایط مثل حالت اول اوضاع خیلی مساعد نیست چراکه مجموع پهنای باند رله‌هایی که برچسب Exit دارند و همچین رله‌هایی که برچسب Guard دارند از میانگین پهنای باندها کمتر است. پس در این حالت رله‌هایی که برچسب Double دارند حائز اهمیت می‌باشند و در تخصیص آن‌ها به دیگر موقعیت‌ها باید سیاست مناسبی اتخاذ کنیم. چون شرایط زیاد مناسب نیست، نمی‌توانیم تنها با پارامترهای اخیر تصمیم‌گیری کنیم، بنابراین باید دنبال پارامترهای دیگر باشیم. ازجمله پارامترهایی که می‌تواند به ما برای تصمیم‌گیری کمک کند، دو پارامتر رابطه (۱۱) می‌باشند.

$$\begin{cases} R=Min(E,G) \\ S=Max(E,G) \end{cases} \quad (۱۱)$$

اکنون با توجه به پارامترهای تعریف‌شده می‌توانیم زیر حالت‌های دیگری را برای اتخاذ تصمیم مناسب در نظر بگیریم.

۴-۲-۱. زیر حالت اول از حالت دوم: ($R + D < S$)

این زیر حالت می‌گوید، مجموع حداقل پهنای باند بین رله‌های Exit و Guard و رله‌های با برچسب Double از حداکثر پهنای باند بین Exit و Guard، کمتر است. به عبارتی در حالت دوم این شرایط تقریباً بدترین حالت ممکن است. چراکه در این حالت ما حتی در رله‌های با برچسب Double هم کمبود داریم. همان‌طور که قبلاً گفتیم، وقتی شرایط خیلی بد شود تکلیف ما هم به عبارتی مشخص‌تر است. با توجه به شرایط واضح است که دیگر نباید از رله‌های با برچسب Exit، Guard و Double در موقعیت میانی استفاده کرد چراکه در هر سه موقعیت دچار کمبود پهنای باند هستیم و باید این کمبود را جبران کنیم، یعنی($W_{md}+W_{mg}+W_{me}=0$). البته چون اوضاع در بدترین حالت خودش به سر می‌برد واضح است که باید رله‌های با برچسب Exit را در تنها در موقعیت انتهایی و رله‌های با برچسب Guard را در موقعیت ابتدایی قرار دهیم. ($W_{gg}=W_{ee}=1$).

تا اینجا ۵ وزن از ۷ وزن را با توجه به شرایط تعریف‌شده به دست آوردیم. اما دو وزن دیگر مستقیماً به اینکه حداقل و حداکثر پهنای باند بین رله‌های با برچسب Exit و Guard کدام است، مربوط است. بنابراین زیر بخش‌های دیگری را به‌صورت زیر در نظر می‌گیریم.

❖ **زیر حالت اول از ۴-۲-۱: ($E < G$)**

وقتی مجموع پهنای باند رله‌هایی که برچسب Exit دارند کمتر از رله‌های با برچسب Guard باشد و از طرفی در مجموع پهنای باند رله‌ها با برچسب Double هم محدودیت داریم، یعنی نمی‌توانیم از Double ها به هر دو موقعیت بدهیم، بلکه فقط باید آن را برای یک موقعیت که وضعیت خوبی ندارد، استفاده کنیم. بنابراین واضح است که تمام رله‌های Double را باید به $Min(E,G)$ یعنی E اختصاص دهیم. ($W_{gd}=0, W_{ed}=1$).

❖ **زیر حالت دوم از ۴-۲-۱: ($E \geq G$)**

این زیر حالت برعکس زیر حالت قبلی است بنابراین داریم: ($W_{gd}=1, W_{ed}=0$).

بنابراین در زیر حالت ۴-۲-۱، ۵ وزن به صورت ثابت و دو وزن دیگر بسته به مقدار حداقلی مجموع پهنای باند رله‌هایی با برچسب Exit و Guard، تعیین شدند.

۴-۲-۲. زیر حالت اول از حالت دوم: ($R + D \geq S$)

این زیر حالت برعکس زیر حالت ۳-۲-۱ است. بنابراین می‌توان گفت شرایط خیلی خوب نیست اما به بدی حالت ۳-۲-۱ نیست، چراکه حداقل در رله‌های Double خیلی کمبود نداریم. پس با توجه با این نکات، تصمیم‌گیری ما کمی سخت‌تر می‌شود. بنابراین نیاز به یک پارامتر کمکی دیگر هم داریم که ما اینجا پارامتر M یا همان مجموع پهنای باند مربوط به رله‌های خنثی را در نظر می‌گیریم. با توجه به مقدار پارامتر M و مقایسه آن با یک مقدار معیار مثل میانگین، زیر حالت‌هایی را تعریف می‌کنیم و طبق آن‌ها و ۵ رابطه اصلی، وزن‌ها را به دست می‌آوریم.

❖ **زیر حالت اول از ۴-۲-۲: (M < T/3)**

این زیر حالت می‌گوید رله‌هایی با برچسب خنثی خیلی زیاد نیست. بنابراین باید از رله‌هایی با برچسب غیر خنثی هم مقداری به رله وسط بدهیم. از طرفی می‌دانیم که در Double ها هم خیلی کمبود نداریم. (وضعیت رله‌های Double به مراتب از دیگر رله‌ها بهتر است) اکنون با یک فرض ادامه می‌دهیم. فرض می‌کنیم در این شرایط، بخواهیم در موقعیت ابتدایی حداکثر پهنای باند را داشته باشیم. با توجه به اینکه رله‌های با برچسب Guard در وضعیت خوبی نیستند، برای اغنای این فرض مجبوریم تمام رله‌های با برچسب Guard را به خود موقعیت ابتدایی بدهیم. یعنی $W_{gg} = 1$. گفتیم فرض ما بر این است که در موقعیت ابتدایی رله‌ای با پهنای باند حداکثری قرار بدهیم. از طرفی هم در Double ها خیلی هم کم نداشتیم اما به‌هرحال نمی‌توانیم ادعا کنیم که تمام Double ها را با توجه به فرض، در موقعیت ابتدایی قرار دهیم؛ چراکه ما در رله‌های با برچسب خنثی هم وضعیت خوبی نداریم. بنابراین مصالحه‌ای بین این شرایط و فرضی که کردیم، باید انجام بگیرد. این مصالحه می‌تواند به این صورت در نظر گرفته شود که احتمال قرارگیری رله با برچسب Double به موقعیت میانی و موقعیت ابتدایی یکسان باشد. بنابراین داریم: $W_{md} = W_{gd}$. در واقع ما برای ارضای فرضی که کردیم با توجه به شرایط بالادستی، تمام توان خود را هزینه کردیم. البته قابل توجه است که در این زیر حالت می‌توان نشان داد: $E < M, G < M$.

در این زیر حالت با توجه به این شرایط و فرضی که در بالا عنوان شد، به کمک ۵ رابطه اصلی می‌توانیم بقیه وزن‌ها را به صورت زیر به دست بیاوریم.

$$W_{gg} = 1 - W_{mg} \rightarrow W_{gg} = 1 \rightarrow W_{mg} = 0 \quad (۱۲)$$

$$\begin{aligned} W_{gg}G + W_{gd}D &= M + W_{md}D + W_{me}E \\ &+ W_{mg}G \rightarrow G + W_{gd}D \\ &= M + W_{gd}D + W_{me}E \end{aligned} \quad (۱۳)$$

بنابراین W_{me} به صورت رابطه (۱۴) به دست می‌آید.

$$W_{me} = \frac{G - M}{E} \quad (۱۴)$$

همچنین W_{ee} به صورت رابطه (۱۵) به دست می‌آید.

$$\begin{aligned} W_{me}E + W_{ee}E = E \rightarrow W_{me} \rightarrow W_{ee} \\ = \frac{E - G + M}{E} \end{aligned} \quad (۱۵)$$

سپس طبق رابطه‌های (۱۶) و (۱۷)، W_{gd} طبق رابطه (۱۸) به دست می‌آید.

$$\begin{aligned} W_{ed}D + W_{md}D + W_{gd}D = D \rightarrow W_{gd} \\ = W_{md} \rightarrow 2W_{gd} + W_{ed} \\ = D \end{aligned} \quad (۱۶)$$

$$\begin{aligned} W_{gg}G + W_{gd}D = W_{ee}E + W_{ed}D \\ \rightarrow W_{gd}D - W_{ed}D \\ = W_{ee}E - G \end{aligned} \quad (۱۷)$$

$$W_{gd} = \frac{E + M + D - 2G}{3D} \quad (۱۸)$$

همچنین می‌توان از رابطه (۱۶)، W_{ed}را به صورت رابطه (۱۹) به دست آورد.

$$\begin{aligned} W_{ed} = \frac{D - 2W_{gd}}{D} \rightarrow W_{ed} \\ = \frac{D - 2E + 4G - 2M}{3D} \end{aligned} \quad (۱۹)$$

و درنهایت W_{md} طبق رابطه (۲۰) تعریف می‌شود.

$$W_{md} = W_{gd} = \frac{1 - W_{ed}}{2} \quad (۲۰)$$

قابل ذکر است که در بالا ما شرایط خاصی را در نظر گرفتیم و با توجه به یک فرض، پیش رفتیم، اما در حالت کلی این شرایط خیلی لب مرزی است و ممکن است خیلی وقت‌ها اتفاق نیافتد و یا به عبارتی با این فرمول‌بندی برخی اوقات وزن‌ها کوچک‌تر از صفر و یا بزرگتر از یک شوند، بنابراین برای اطمینان بیشتر فرض‌های خود را مبتنی بر این منطق قرار می‌دهیم که در هر دو موقعیت ابتدایی و انتهایی کمبود پهنای باند داریم. (منطق واقعی‌تر و بدون فرض خاص) ازاین‌رو ما دیگر از رله‌های با برچسب *Exit* و *Guard* فقط به خودشان می‌دهیم یعنی $W_{gg} = 1, W_{ee} = 1$ به‌عبارتی‌دیگر ریسک نمی‌کنیم و از رله‌های با برچسب Exit به رله‌های میانی چیزی نمی‌دهیم. حالا با این شرایط جدید مثل بالا دوباره وزن‌ها را به دست می‌آوریم.

طبق رابطه (۴) و (۵) به ترتیب داریم، $W_{mg} = 0$ و $W_{me} = 0$ همچنین طبق رابطه‌های (۳) و (۲) به ترتیب رابطه‌های (۲۱) و (۲۲) به دست می‌آیند.

$$W_{ed}D = D - W_{gd}D - W_{md}D \quad (۲۱)$$

$$G + W_{gd}D = E + W_{ed}D \quad (۲۲)$$

با جمع طرفین رابطه‌های (۲۱) و (۲۲)، رابطه (۲۳) به دست می‌آید.

$$2W_{gd}D + W_{md}D = E + D - G \quad (۲۳)$$

همچنین با توجه به رابطه (۱) داریم:

$$G + W_{gd}D = M + W_{md}D \rightarrow W_{gd}D - W_{md}D = M - G \quad (۲۴)$$

بنابراین طبق رابطه‌های (۲۳) و (۲۴)، W_{gd} به صورت رابطه (۲۵) به دست می‌آید.

$$W_{gd} = \frac{E + D + M - 2G}{3D} \quad (۲۵)$$

با استفاده از رابطه‌های (۲۳) و (۲۵) می‌توان W_{md} را به صورت رابطه (۲۶) به دست آورد.

$$W_{md} = \frac{D - 2M + G + E}{3D} \quad (۲۶)$$

همچنین با توجه به رابطه‌های (۲۲) و (۲۵)، W_{ed} طبق رابطه (۲۷) به دست می‌آید.

$$W_{ed} = \frac{D - 2E + G + M}{3D} \quad (۲۷)$$

همچنین با توجه به رابطه‌های (۲۶) و (۲۷) می‌توان W_{gd} را به صورت رابطه (۲۸) به دست آورد.

$$W_{gd} = 1 - W_{ed} - W_{md} \quad (۲۸)$$

❖ **زیر حالت دوم از ۴-۲-۲: ($M > T/3$)**

وقتی تعداد رله‌های با برچسب خنثی از میانگین بیشتر است واضح است که دیگر نیاز نیست رله‌ها با برچسب Double در موقعیت میانی قرار بگیرند به عبارتی: $W_{md} = 0$ و بقیه روابط همانند زیر حالت قبل است. اگر به روابط حالت قبل دقت کنید، مشخص است که اگر $M > T/3$ آنگاه W_{md} منفی می‌شود. بنابراین $W_{md} = 0$ در نظر می‌گیریم و $W_{gd} = 1 - W_{ed}$.

۴-۳. حالت سوم: $E < T/3$ یا $G < T/3$

در حالت سوم برعکس حالت دوم E و G هم‌زمان از میانگین کمتر نیستند بلکه این اتفاق برای یکی از این دو می‌افتد. بنابراین اوضاع مثل حالت دوم خیلی نامناسب نیست، یا به عبارتی حداقل از حالت دوم بهتر است. بنابراین دیگر نیاز به دو پارامتر کمکی برای تحلیل نیست بلکه یک پارامتر می‌تواند به ما کمک کند تا بتوانیم زیر حالت‌های مختلف را بررسی کنیم و درنهایت وزن‌ها را در هرکدام از حالت‌ها به دست بیاوریم. یکی از پارامترهایی که می‌توانیم در نظر بگیریم به صورت رابطه (۲۹) است.

$$S = Min(E, G) \quad (۲۹)$$

۴-۳-۱. زیر حالت اول: $S + D < T/3$

در این زیر حالت مجموع پهنای باند S (حداقل بین E و G) و D از میانگین کمتر است. بنابراین خیلی شرایط خوب نیست اما خیلی هم بد نیست. اکنون با توجه به اینکه کدام یک از مقادیر E و G حداقل است زیر حالت‌های دیگری در نظر می‌گیریم و وزن‌ها را برای آن شرایط به دست می‌آوریم.

❖ **زیر حالت اول از ۴-۳-۱: $S = G$**

در این حالت شرایط برای موقعیت ابتدایی خیلی بد است، پس باید به‌گونه‌ای این شرایط بد را جبران کنیم اما چگونه؟ مثلاً Double ها را به موقعیت ابتدایی اختصاص دهیم و از طرفی رله‌های با برچسب Guard را هم فقط در موقعیت ابتدایی قرار می‌دهیم. یعنی $W_{gd} = 1, W_{gg} = 1$ وقتی شرایط را این‌گونه در نظر گرفتیم، واضح است که از رله‌های Double دیگر چیزی به موقعیت وسطی و انتهایی نمی‌رسد و از طرفی از رله‌های با برچسب Guard هم چیزی به رله وسطی نمی‌رسد. به‌عبارت‌دیگر داریم: $W_{md} = W_{ed} = W_{mg} = 1$

۵ وزن از ۷ وزن را به دست آوردیم. برای به دست آوردن ۲ وزن دیگری بهتر است پارامتر دیگر M را هم دخیل کنیم، به صورتی که اگر $E < M$ آنگاه مجبوریم از E به موقعیت میانی هم چیزی ندهیم یعنی $W_{me} = 0$ در غیر اینصورت لزومی ندارد که از E به رله وسطی چیزی ندهیم. بنابراین با توجه به شرایط بالا دیگر وزن‌ها ازجمله وزن W_{me} را به دست می‌آوریم. از رابطه‌های (۱)، (۲) و (۵) به ترتیب رابطه‌های (۳۰)، (۳۱) و (۳۲) به دست می‌آید.

$$G + D = M + W_{me}E \rightarrow W_{me} = \frac{G + D - M}{E} \quad (۳۰)$$

$$G + D = W_{ee}E \rightarrow W_{ee} = \frac{G + D}{E} \quad (۳۱)$$

$$W_{ee} = 1 - W_{me} \rightarrow \frac{G + D}{E} = 1 - \frac{G + D - M}{E} \rightarrow \frac{G + D}{E} = \frac{E - G - D + M}{E} \rightarrow G + D = \frac{E + M}{2} \quad (۳۲)$$

با توجه به رابطه‌های (۳۰) و (۳۲) و همچنین با استفاده از رابطه‌های (۳۱) و (۳۲)، W_{me} و W_{ee} به ترتیب از رابطه‌های (۳۳) و (۳۴) به دست می‌آیند.

$$W_{me} = \frac{E - M}{2E} \quad (۳۳)$$

$$W_{ee} = \frac{E + M}{2E} \quad (۳۴)$$

❖ **زیرحالت دوم از ۴-۳-۱: ($S = E$)**

در این زیر حالت شرایط برای انتخاب رله برای موقعیت

انتهایی خیلی خوب نیست بنابراین به‌گونه‌ای باید این شرایط را جبران کنیم، اما چگونه؟ رویکرد دوباره مثل زیر حالت قبل است. در زیر حالت قبل رله‌های با برچسب Double را به موقعیت ابتدایی نسبت می‌دادیم، اما در این زیر حالت Double ها را به موقعیت انتهایی نسبت می‌دهیم و رله‌هایی با برچسب Exit را فقط در موقعیت انتهایی نسبت می‌دهیم. یعنی : $W_{ee} = W_{ed} = 1$ وقتی چنین شرایطی را در نظر می‌گیریم، طبیعتاً دیگر از E نمی‌توانیم چیزی به رله وسطی دهیم همچنین از Double هم نمی‌توانیم به موقعیت ابتدایی و یا میانی دهیم چون همه‌ی آن‌ها را هزینه کردیم. به عبارتی داریم: $W_{md} = W_{gd} = W_{me} = 0$

۵ وزن از ۷ وزن را به دست آوردیم. برای به دست آوردن ۲ وزن دیگر بهتر است پارامتر M را هم دخیل کنیم به صورتی که اگر $G < M$ آنگاه مجبوریم از رله‌های با برچسب Guard در موقعیت میانی استفاده نکنیم یعنی $W_{mg} = 0$ در غیر این صورت لزومی ندارد که از رله‌های با برچسب Guard در موقعیت میانی قرار دهیم. بنابراین با توجه به شرایط بالا دیگر وزن‌ها ازجمله وزن W_{mg} را به دست می‌آوریم.

از رابطه‌های (۱)، (۲) و (۴) به ترتیب رابطه‌های (۳۵)، (۳۶) و (۳۷) به دست می‌آید.

$$W_{gg}G = M + W_{mg}G \rightarrow W_{mg} = \frac{E + D - M}{G} \quad (۳۵)$$

$$W_{gg}G = E + D \rightarrow W_{gg} = \frac{E + D}{G} \quad (۳۶)$$

$$W_{gg} = 1 - W_{mg} \rightarrow \frac{E + D}{G} = 1 - \frac{E + D - M}{G} \rightarrow E + D = \frac{G + M}{2} \quad (۳۷)$$

با توجه به رابطه‌های (۳۵) و (۳۷) و همچنین رابطه‌های (۳۶) و (۳۷)، W_{mg} و W_{gg} به ترتیب از رابطه‌های (۳۸) و (۳۹) به دست می‌آید.

$$W_{mg} = \frac{G - M}{2G} \quad (۳۸)$$

$$W_{gg} = \frac{G + M}{2G} \quad (۳۹)$$

۴-۳-۲. زیرحالت دوم: $(S + D \geq T/3)$

در این زیر حالت شرایط از زیر حالت ۴-۳-۱ کمی بهتر است چراکه حاصل جمع حداقل مجموع پهنای باند E و G و D ها از میانگین پهنای باندها بیشتر است. بنابراین با توجه به اینکه حداقل مجموع پهنای باند بین E و G کدام است، زیر حالت‌های دیگری تعریف می‌شود و طبق آن، وزن‌ها را به دست می‌آوریم.

❖ **زیر حالت اول از ۴-۳-۲: $(S = G)$**

در این زیر حالت شرایط موقعیت ابتدایی خیلی خوب نیست، پس باید با توجه به زیر حالت‌های بالاتر این شرایط نامناسب را برای موقعیت ابتدایی جبران کنیم. اولین کاری که می‌توانیم انجام دهیم، این است که از رله‌های با برچسب Guard فقط در موقعیت ابتدایی استفاده کنیم. $(W_{gg} = 1)$ و از طرفی چون شرایط خیلی هم بد نیست پس لزومی ندارد که تمام Double ها را به موقعیت ابتدایی بدهیم و اگر بخواهیم می‌توانیم از رله‌هایی با برچسب Exit هم برای رله‌های میانی هزینه کنیم. درنتیجه احتمال اینکه از Double ها را در موقعیت انتهایی یا میانی استفاده کنیم با هم برابر است به عبارتی: $W_{ed} = W_{md}$ اکنون با توجه به این شرایط و با استفاده از ۵ رابطه اصلی می‌توانیم دیگر وزن‌ها را به‌صورت زیر به دست بیاوریم:

از رابطه‌های (۱)، (۵)، (۲) و (۳) به ترتیب رابطه‌های (۴۰)، (۴۱) و (۴۲) به دست می‌آید.

$$G + W_{gd}D = M + W_{ed}D + W_{me}E \quad (۴۰)$$

$$G + W_{gd}D = (1 - W_{me})E + W_{ed}D \quad (۴۱)$$

$$W_{ed}D + W_{ed}D + W_{gd}D = D \rightarrow W_{ed} = \frac{1 - W_{gd}}{2} \quad (۴۲)$$

با توجه به رابطه‌های (۴۰) و (۴۲)، W_{gd} طبق رابطه (۴۳) به دست می‌آید.

$$\frac{3}{2}W_{gd}D - W_{me}E = M - G + \frac{1}{2}D \rightarrow W_{gd} = \frac{M - 2G + D + E}{3D} \quad (۴۳)$$

همچنین با توجه به رابطه‌های (۴۱) و (۴۲)، W_{me} به‌صورت رابطه (۴۴) به دست می‌آید.

$$\frac{3}{2}W_{gd}D - W_{me}E = E - G + \frac{1}{2}D \rightarrow W_{me} = \frac{E - M}{2E} \quad (۴۴)$$

درنهایت W_{ee}، W_{ed} و W_{md} به ترتیب با استفاده از رابطه‌های (۴۵)، (۴۶) و (۴۷) به دست می‌آیند.

$$W_{ee} = 1 - W_{me} \quad (۴۵)$$

$$W_{ed} = \frac{1 - W_{gd}}{2} \quad (۴۶)$$

$$W_{md} = W_{ed} \quad (۴۷)$$

❖ **زیر حالت دوم از ۴-۳-۲: $(S = E)$**

در این زیر حالت شرایط برای موقعیت انتهایی خیلی خوب نیست، پس باید با توجه به زیر حالت‌های بالا، این شرایط

نامناسب را جبران کنیم. اولین کاری که می‌توانیم انجام دهیم، این است که از رله‌های با برچسب Exit فقط به خود موقعیت انتهایی بدهیم. ($W_{ee} = 1$) و از طرفی چون شرایط خیلی هم بد نیست پس لزومی ندارد که تمام Double ها را در موقعیت انتهایی قرار دهیم و اگر بخواهیم از رله‌هایی با برچسب Guard هم می‌توانیم برای رله‌های میانی هزینه کنیم، درنتیجه احتمال اینکه از Double ها در موقعیت‌های ابتدایی و میانی استفاده کنیم باهم برابر هستند به عبارتی: $W_{gd} = W_{md}$.

اکنون با توجه به این شرایط و با استفاده از ۵ رابطه اصلی می‌توانیم دیگر وزن‌ها را مثل زیر حالت قبل به دست بیاوریم. با توجه به رابطه (۱)، W_{gg} طبق رابطه (۴۸) به دست می‌آید.

$$W_{gg}G + W_{gd}D = M + W_{gd}D + (1 - W_{gg})G \rightarrow W_{gg} = \frac{M+G}{2G} \quad (۴۸)$$

از رابطه (۲) و (۴۸)، W_{gd} طبق رابطه (۴۹) به دست می‌آید.

$$W_{gd} = \frac{2E + 2D - M - G}{6D} \quad (۴۹)$$

و درنهایت W_{ed}، W_{md} و W_{mg} به ترتیب طبق رابطه‌های (۵۰)، (۵۱) و (۵۲) به دست می‌آیند.

$$W_{ed} = 1 - 2W_{gd} \rightarrow W_{ed} = \frac{D - 2E + G + M}{3D} \quad (۵۰)$$

$$W_{md} = W_{gd} \quad (۵۱)$$

$$W_{mg} = 1 - W_{gg} \quad (۵۲)$$

۵. الگوریتم انتخاب مسیر در شبکه تُر

پس از محاسبه وزن یا ضریب مربوط به قرارگیری هر یک از رله‌ها در مسیر، کاربر در زمان تشکیل مدار از این مقادیر به منظور انتخاب سه رله مناسب برای مسیر مورد نظر خود استفاده می‌کند. با توجه به اینکه نوبت به انتخاب کدام یک از رله‌های مسیر (موقعیت اول، دوم یا سوم) است، ضرایب W_g، W_m، W_e، W_d به صورت متفاوتی به دست می‌آید. الگوریتم (۱) نحوه محاسبه هر یک از این ضرایب را نشان می‌دهد.

با توجه به اصول پنج‌گانه ذکر شده در بخش ۴، فرمول‌های موجود در الگوریتم (۱) بدیهی به نظر می‌رسد. حال با توجه به ضرایب محاسبه شده، طبق الگوریتم (۲) یک رله برای موقعیت مورد نظر در مسیر انتخاب می‌شود.

به منظور تشکیل مسیر و انتخاب سه رله برای موقعیت‌های ابتدایی، میانی و انتهایی مسیر، الگوریتم (۲) باید ۳ مرتبه فراخوانی شود. در هر مرتبه با توجه به موقعیتی که قرار است رله در آن قرار بگیرد، ابتدا مجموع پهنای باند رله‌ها با توجه به ضرایب محاسبه شده توسط الگوریتم (۱) به دست می‌آید و سپس با انتخاب یک عدد تصادفی تا مقدار مجموع، رله‌ای انتخاب می‌شود که مجموع پهنای باند رله‌ها تا آن رله به آن مقدار برسد.

الگوریتم (۱). نحوه محاسبه ضرایب پهنای باند برای انتخاب هر یک از رله‌های مسیر در شبکه‌ی تُر

۱) درصورت تلاش برای یافتن رله Guard:

$$W_g = W_{gg}, W_m = W_{gm}, W_e = 0, W_d = W_{gd}$$

۲) درصورت تلاش برای یافتن رله Exit:

$$W_g = 0, W_m = W_{em}, W_e = W_{ee}, W_d = W_{ed}$$

۳) درصورت تلاش برای یافتن رله Middle:

$$W_g = W_{mg}, W_m = W_{mm}, W_e = W_{me}, W_d = W_{md}$$

الگوریتم (۲). نحوه انتخاب رله‌های تشکیل دهنده یک مسیر در شبکه‌ی تُر

۱) برای تمام رله‌ها (i) تکرار کن:
۱-۱) اگر رله‌ای برچسب Exit و Guard داشت، آنگاه:
$bw = b[i] * W_g * W_e$
۱-۲) اگر رله‌ای برچسب Guard داشت، آنگاه:
$bw = b[i] * W_g$
۱-۳) اگر رله‌ای برچسب Exit داشت، آنگاه:
$bw = b[i] * W_e$
۱-۴) در غیر اینصورت، آنگاه:
$bw = b[i] * W_m$
۱-۵) محاسبه کن:
totalbw $= totalbw + bw$
پایان تکرار ۱.
۲) عدد تصادفی rand_{bw} را تا totalbw انتخاب کن
۳) برای تمام رله‌ها (i) تکرار کن:
۳-۱) اگر رله‌ای برچسب Exit و Guard داشت، آنگاه:
$temp = temp + b[i] * W_g * W_e$
۳-۲) اگر رله‌ای برچسب Guard داشت، آنگاه:
$temp = temp + b[i] * W_g$
۳-۳) اگر رله‌ای برچسب Exit داشت، آنگاه:
$temp = temp + b[i] * W_e$
۳-۴) در غیر اینصورت:
$temp = temp + b[i] * W_m$
۳-۵) اگر $temp > rand_{bw}$، آنگاه iامین رله را برگردان.
پایان تکرار ۳.

۶. نتیجه‌گیری

مهم‌ترین عامل تأثیرگذار در کارایی و امنیت شبکه‌های گمنامی نحوه‌ی انتخاب مسیر از میان رله‌های تشکیل‌دهنده مدار است. شبکه تُر به‌عنوان یکی از پرمخاطب‌ترین نرم‌افزارهای گمنام ساز، به‌منظور فراهم نمودن گمنامی با تأخیر کم طراحی‌شده ولی کاربران این شبکه گاهی حین استفاده با تأخیرهای زمانی طولانی روبرو می‌شوند. در این مقاله، ابتدا بعد از توضیح مختصر در مورد

عملکرد شبکه تُر، نحوه محاسبه وزن یا احتمال انتخاب رله‌ها در پروتکل مسیریابی به‌طور کامل مورد بررسی و کنکاش قرار گرفت و دلیل استفاده از روابط وزن دهی در این پروتکل به‌طور کامل اثبات و تبیین شد. همچنین روابط مورد استفاده در این پروتکل برای اولین بار در این مقاله به‌صورت منطقی و ریاضی اثبات و الگوریتم انتخاب مسیر در شبکه گمنامی‌تر به‌طور کامل تفسیر شده است.

۷. مراجع

[1] R. Dingledine, N. Mathewson, and P. Syverson, "TOR: The second generation onion router", In Proceedings of the Usenix Security Symposium, 2004.

[2] K. Loesing, S. Murdoch, and R. Dingledine, "A Case Study on Measuring Statistical Data in the Tor Anonymity Network", In Proceedings of Financial Cryptography and Data Security, 2010. L. Overlier and P. Syverson, "Locating hidden

[3] servers", In Proceedings of the 27th IEEE Symposium on Security and Privacy, pp. 100-114, 2006. DOI: 10.1109/SP.2006.24

[4] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker,"Low-resource routing attacks against anonymous systems",In Proceedings of the 2007 Workshop on Privacy in the Elec-tronic Society (WPES), 2007.

[5] J. Douceur, "The Sybil Attack", In Proceedings of the 1st International Peer To Peer Systems Workshop (IPTPS), 2002.

[6] A. Johnson, P. F. Syverson, R. Dingledine, and N. Mathewson,"Trust-based anonymous communication: adversary models and routing algorithms", In ACM CCS, 2011.

[7] V. Sassone, E. ElSalamouny, and S. Hamadou, "Trust in crowds: Probabilistic behaviour in anonymity protocols", In Symposium on Trustworthy Global Computing, TGC. Springer Lecture Notes on Computer Science 88–102, 2010.

[8] A. Johnson, and P. Syverson, "More anonymous onion routing through trust", In IEEE Computer Security Foundations Symposium, 2009.

[9] M. Edman, and P. Syverson, "As-awareness in tor path selection", In ACM CCS, 2009.

[10] N. Feamster, and R. Dingledine, "Location diversity in anonymity Networks", In ACM Workshop on Privacy in the Electronic Society, Washington, DC, 2004.

[11] A. Panchenko, J. Renner, "Path Selection Metrics for Performance-Improved Onion Routing", Proceedings of the Ninth Annual International Symposium on Applications and the Internet, pp. 114-120, 2009. DOI: 10.1109/SAINT.2009.26

[12] M. Akhoondi, C. Yu, and H. Madhyastha, "LASTor: A Low-Latency AS-Aware Tor Client", In Proceedings of the 2012 IEEE Symposium on Security and Privacy, pp. 476–490, 2012. DOI: 10.1109/SP.2012.35

[13] The Tor Project, Tor directory protocol, version 3, https://git.torproject.org/checkout/tor/master/doc/spec/dir-spec.txt, 2018.