
بسم الله الرحمن الرحيم

دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

شبیه‌سازی و آنالیز رفتار شبکه الگورند در حضور تراکنش‌های باهزینه

گزارش پروژه کارشناسی

فاطمه رحمانی

استاد پروژه

دکتر محمد حسین منشئی

۱۳۹۹

فهرست مطالب

فهرست تصاویر

فهرست جداول

چکیده

تخصیص پاداش به گره‌ها در شبکه الگورند، فارغ از بررسی فعالیت مفید این گره‌ها در شبکه است. این موضوع می‌تواند باعث شود گره‌های شبکه برای کاهش هزینه‌های خود از انجام مسئولیت‌هایشان سرباز زنند. با فرار گره‌ها از انجام مسئولیت‌های خود، این شبکه در آینده با مشکلات بزرگی روبرو خواهد شد. در این پروژه با توجه به نوع شبکه مورد استفاده، معیاری برای اندازه‌گیری فعالیت مفید گره‌ها معرفی می‌شود تا شبکه براساس اندازه‌گیری این معیار، به هر گره پاداش مستحق او را تخصیص دهد. درنهایت کارایی، جزئیات پیاده‌سازی و سربارهای ایجاد شده در شبکه برای پیاده‌سازی این روش، براساس شبیه‌ساز طراحی شده برای شبکه الگورند به دقت بررسی می‌شود.

واژه‌های کلیدی: زنجیره بلوکی، الگورند

فصل اول

مقدمه

اگر ما در یک دنیای ایده‌آل زندگی می‌کردیم که یک سیستم کنترل مرکزی برای مدیریت‌های مالی وجود داشت که همه به آن اعتماد داشتند و از هرگونه حمله سایبری در امان بود بسیاری از مشکلات حال حاضر سیستم مالی را نداشتیم ولی ما در چنین دنیای ایده‌آلی زندگی نمی‌کنیم و برای حل مشکلات موجود به استفاده از سیستم‌های توزیع شده[1] برای مدیریت مالی روی آورده‌ایم.

محدودیت‌های موجود در سیستم‌های پولی و مدل‌های مالی در گذشته منجر به معرفی و گسترش رمزارزها[2] شدند که پایه آن‌ها براساس زنجیره بلوکی[3] غیر قابل تغییری است که تراکنش‌ها[4] و اطلاعات کاربران یا حتی قراردادهای هوشمند[5] به صورت توزیع شده در آن ثبت می‌شود.

یکی از رمزارزهای موفق در این حوزه بیت‌کوین[6] است که گسترش بسیار زیادی در سال‌های اخیر داشته است. این رمزارز به صورت موفق توانسته است سیستم کنترل مرکزی را از سیستم مالی حذف کند و شفافیت را به سیستم مالی بیافزاید؛ ولی این رمزارز نیز اشکالات و محدودیت‌هایی دارد. یکی از محدودیت‌های مهم

[1] Distributed
[2] Cryptcurrancy
[3] Block Chain
[4] Transaction
[5] Smart Contract
[6] BitCoin

موجود در بیت‌کوین تعداد تراکنش‌هایی است که می‌تواند ثبت کند. در واقع به دلیل ایجاد امنیت در این سیستم نرخ ایجاد و تایید تراکنش‌ها محدود به ۳ تا ۷ تراکنش در ثانیه است که این نرخ در برابر یک سیستم موجود مثل پی‌پال[۱] با نرخ ۴۵۰ تراکنش در ثانیه یا ویزانت[۲] با نرخ تراکنش در حدود ۵۶ هزار تراکنش در ثانیه، قابل مقایسه نیست. این مسئله باعث شده است که گسترش این رمزارز در مقیاس جهانی ممکن نباشد.

محدودیت‌های موجود در بیت‌کوین باعث شده است پلتفرم‌های جدیدی با ایده‌های جدیدتر به وجود بیایند تا این محدودیت‌ها را از بین ببرند، به طور مثال برخی از مدل‌ها تلاش کرده‌اند که سازوکار مبتنی بر اثبات کار[۳] در بیت‌کوین را با ایده‌هایی مثل استفاده از کمیته[۴]، شبکه‌های پرداخت[۵] و زنجیره‌های جانبی[۶] بهینه سازی کنند. برخی دیگر نیز تلاش کرده‌اند سازوکار مبتنی بر اثبات کار در بیت‌کوین را با سازوکارهای جدید مبتنی بر اثبات سهام[۷]، مبتنی بر اثبات سوختن[۸] یا مبتنی بر اثبات زمان مصرفی[۹] جایگزین کنند. در برخی از ایده‌ها هم به جای استفاده از یک زنجیره بلوکی خطی از یک گراف جهت‌دار بدون دور[۱۰] برای افزایش کارایی استفاده شده است.

یکی از این رمزارزها که سعی در حل مشکل مقیاس‌پذیری بیت‌کوین داشته‌است، رمزارز الگورند[۱۱] است که یک سازوکار محاسباتی مبتنی بر سهام ارائه داده است و نرخ تراکنش‌ها را در حدود ۱۲۵ برابر نسبت به بیت‌کوین افزایش داده است. ولی این رمزارز نیز مشکلات متعددی دارد؛ از جمله اینکه فعالیت گره‌ها در شبکه را برای پاداش دادن به آن‌ها در نظر نمی‌گیرد و این موضوع ممکن است در آینده باعث مشکلاتی برای این رمزارز باشد. در این پروژه به بررسی دقیق مسئله موجود پرداخته سپس راه‌حلی برای این مشکل پیشنهاد می‌دهیم و درنهایت راه‌حل ارائه شده را بر اساس شبیه‌ساز طراحی شده برای شبکه الگورند تحلیل می‌کنیم.

---

[1] Paypal
[2] VisaNet
[3] Proof of Work
[4] Committee
[5] Payment Networks
[6] Side Chain
[7] Proof of Stake
[8] Proof of Burn
[9] Proof of ElapsedTime
[10] Directed Acyclic Graph(DAG)
[11] Algorand

فصل دوم

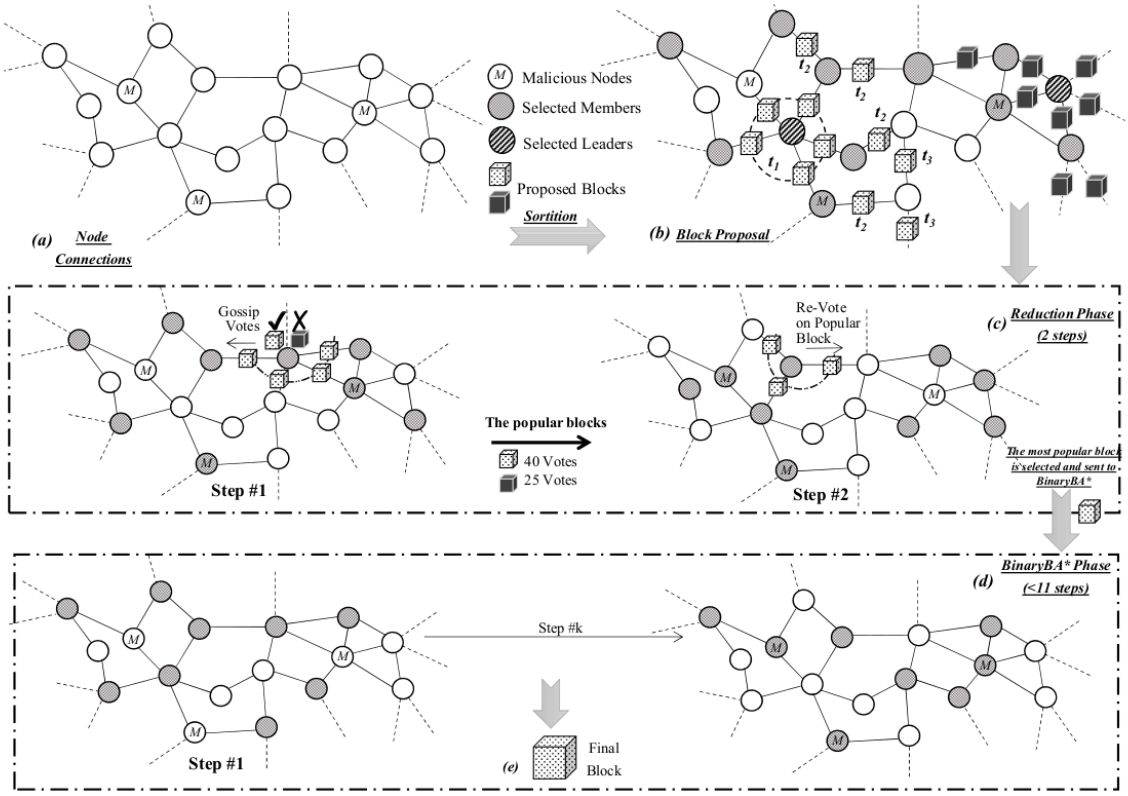
الگورند

قصد داریم در این فصل به صورت خلاصه پروتکل الگورند را معرفی کنیم. از آنجایی که توضیح و تشریح همه بخش‌های این پروتکل مقدور نیست، تنها قسمت‌های مرتبط با این پروژه به صورت خلاصه بررسی می‌شود. درصورت نیاز به توضیحات بیشتر به مقاله اصلی الگورند[۴] یا [۸] مراجعه کنید.

قرارداد در بستر یک سیستم غیر متمرکز باید مبتنی بر اثبات موضوعی از سمت کاربران این سیستم باشد؛ به طور مثال در پروتکل‌های مبتنی بر اثبات کار، برای توافق روی یک بلاک و گسترش زنجیره‌بلوکی، کاربران باید پازلی را حل کنند و با اثبات یافتن پاسخ پازل، بلاک را به زنجیره‌بلوکی بیافزایند.

الگورند یک پروتکل مبتنی بر اثبات سهام است؛ در این پروتکل برای توافق روی یک بلاک کل سیستم با هم تعامل کرده و هر کاربر به اندازه سهام خود در توافق روی بلاک تاثیر خواهد داشت. در این سیستم همه کاربران برابر هستند، یعنی به دو دسته کاربران معمولی که تراکنش اضافه می‌کنند و کاربرانی که می‌توانند بلاک به سیستم اضافه کنند، تقسیم نمی‌شوند. به همین دلیل کاری که هر کاربر باید انجام دهد بسیار کمتر از پروتکل‌های مبتنی بر اثبات کار خواهد بود؛ در نتیجه مصرف انرژی کمتری در بردارد و قابلیت مقیاس‌پذیری بسیار بیشتری نسبت به پروتکل‌های مبتنی بر اثبات کار خواهد داشت.

در ادامه، ساختار شبکه و پروتکل ارتباط و توافق مورد استفاده توسط الگورند مختصرا بررسی می‌شود.



شکل ۲ـ۱: شبکه الگورند[۷]

۲ـ۱ ساختار شبکه و ارتباطات

شبکه الگورند، یک شبکه نظیر به نظیر[1] است که در آن هر گره به تعدادی از گره‌های شبکه متصل است. هر گره دارای یک کلید عمومی و خصوصی خاص در شبکه است که با آن‌ها شناخته می‌شود. ساختار شبکه را می‌توانید در تصویر ۲ـ۱ قسمت a مشاهده کنید.

هر کاربر برای ارتباط با هر کدام از گره‌های شبکه از یک ارتباط TCP استفاده می‌کند. پروتکل ارتباطی در این شبکه با نام پروتکل شایعه[2] شناخته می‌شود؛ به این‌صورت که هر گره با دریافت اطلاعات، اعم از اطلاعات بلاک یا تراکنش یا پیام‌های مربوط به پروتکل، آن‌ها را برای همه همسایگان خود ارسال می‌کند. پیام‌های مربوط به پروتکل شامل موارد زیر می‌شود:

- تراکنش‌ها: هر تراکنش در شبکه نشان‌دهنده انتقال الگو (واحد پول در شبکه الگورند) از یک کاربر به کاربر دیگر می‌باشد. با کنار هم قرار گرفتن تعدادی از این تراکنش‌ها یک بلاک ساخته می‌شود. بلاک در شبکه الگورند شامل تعدادی تراکنش یا یک بلاک خالی خواهد بود.
- پیشنهاد بلاک: این پیام شامل یک بلاک با تعدادی تراکنش است که باید به زنجیره بلوکی افزوده شود.

[1] P2P(Peer2Peer)
[2] Gossip Protocol

این بلاک همینطور شامل اثبات قرعه‌کشی[1] است که فرستنده این پیام یک پشنهاددهنده بلاک[2] یا سرگروه است.

- مدارک: به دلیل اینکه ممکن است در شبکه چند پیشنهاددهنده بلاک وجود داشته باشند، برای جلوگیری از ازدحام در لینک‌ها قبل از ارسال بلاک، هر پیشنهاددهنده مدارک خود را شامل اثبات قرعه‌کشی برای بقیه ارسال می‌کند تا سایر گره‌ها بر اساس اولویت هرکدام، منتظر بلاک با بیشترین اولویت بمانند. هر اثبات قرعه‌کشی شامل یک اولویت است که هر کس با دریافت اثبات می‌تواند آن را محاسبه کند.
- رأی‌ها: این پیام شامل یک رای امضا شده همراه با اثبات قرعه‌کشی است.

در این قسمت لازم به ذکر است که در حال حاضر شبکه الگورند قصد دارد از حالت نظیر به نظیر اولیه خارج شده و از شبکه بازپخش[3] در پروتکل خود استفاده کند.

در شبکه بازپخش گره‌ها به دو نوع گره‌های معمولی[4] و گره‌های رله[5] تقسیم می‌شوند. گره‌های رله سهامی ندارند و فقط وظیفه احراز اصالت و پخش اطلاعات در شبکه را بر عهده دارند. گره‌های معمولی باید به تعدادی گره رله متصل شوند و از آن‌ها اطلاعات دریافت کنند. اجرای مراحل مختلف پروتکل برای توافق بر روی بلاک بر عهده گره‌های معمولی خواهد بود. گره‌های رله در شبکه‌ای به صورت زیرساخت شبکه اصلی برای ارسال اطلاعات به هم متصلند و بنابر وظیفه گره‌های رله این گره‌ها به پهنای باند، سرعت و تجهیزات بهتری نسبت به گره‌های معمولی نیاز دارند. سایر موارد مثل انواع پیام‌ها و پروتکل ارتباطی مشابه حالت نظیر به نظیر است.

۲ـ۲ پروتکل توافق

الگورند برای توافق روی بلاک‌ها از پروتکل توافق بیزانسی[6] یا *BA استفاده می‌کند. گره‌ها با اجرای این پروتکل در هر دور روی بلاکی از تراکنش‌ها توافق می‌کنند. در ابتدای هر دور هر کدام از گره‌ها به صورت محرمانه برای خودشان الگوریتم قرعه‌کشی را اجرا می‌کنند، تا متوجه شوند که سرگروه یا پیشنهاددهنده بلاک هستند یا خیر. در صورتی که به عنوان پیشنهاددهنده بلاک انتخاب شده بودند، تراکنش‌های تایید شده را در کنار هم قرار داده و با استفاده از این تراکنش‌ها و چکیده بلاک قبلی ک بلاک ساخته و آن را در شبکه منتشر می‌کنند. این عملیات در تصویر ۲ـ۱ قسمت b مشخص شده‌است. هر گره با دریافت این بلاک‌ها آن‌ها را در بازه زمانی مشخصی نگه‌داری می‌کند تا بلاک با بیشترین اولویت را از میان آن‌ها انتخاب و ذخیره کند.

---

[1] Sortition Proof
[2] Proposer
[3] Relay Network
[4] Participation Node
[5] Relay Node
[6] Byzantine Agreement

پس از این مرحله، هر گره، پروتکل *BA را با بلاک دریافتی با بالاترین اولویت آغاز می‌کند. پروتکل *BA باعث می‌شود که کل گره‌های شبکه روی بلاک مشخصی توافق کنند و آن را به زنجیره بلوکی بیافزایند. پروتکل *BA در دو فاز کاهش[۱] و *BA ـ دودویی[۲] انجام می‌شود که هر کدام از آن‌ها شامل چند مرحله خواهد بود. در هر مرحله گروهی از گره‌ها به صورت تصادفی انتخاب می‌شوند که به آن‌ها اعضای کمیته[۳] گفته می‌شود، این اعضا در هر مرحله براساس رأی‌های قبلی داده شده، به یک بلاک خاص رأی داده و رأی خود را در شبکه پخش می‌کنند. این رأی‌ها باید شامل اثبات قرعه‌کشی نیز باشند تا مشخص شود که رأی‌دهنده عضوی از کمیته بوده است.

- فاز کاهش: این فاز از دو مرحله تشکیل شده است. در مرحله اول اعضای کمیته به چکیده بلاک موردنظر خود(بلاک دریافت شده با بالاترین اولویت) رأی می‌دهند. در مرحله دوم اعضای کمیته بعدی به چکیده بلاکی رأی می‌دهند که در مرحله قبل بیشترین رأی را داشته باشد و از سطح آستانه مشخصی رأی بیشتری آورده باشد. در صورتی که هیچ بلاکی به اندازه سطح آستانه رأی نداشته باشد اعضای کمیته به چکیده بلاک خالی رأی می‌دهند. در نهایت خروجی این مرحله حداکثر یک بلاک از تراکنش‌ها یا یک بلاک خالی خواهد بود، که این خروجی به عنوان ورودی فاز بعد مورد استفاده قرار می‌گیرد. می‌توانید این فاز را در تصویر ۲ ـ ۱ قسمت c مشاهده کنید.

- فاز *BA ـ دودویی: هدف این فاز این است که شبکه بر روی بلاکی که در مرحله قبل بیشترین رأی را آورده توافق کند و در غیر اینصورت بلاک خالی به عنوان بلاک خروجی این فاز در نظر گرفته شود. در حالت معمولی که شبکه قویاً هماهنگ[۴] و پیشنهاددهنده بلاک صادق باشد، این فاز با یک چکیده بلاک ثابت برای اکثر گره‌ها آغاز می‌شود و در همان مرحله اول شبکه روی بلاک مورد نظر توافق می‌کند. در صورتی که شبکه قویاً هماهنگ نباشد ممکن است که این فاز بر روی دو بلاک (بلاک خروجی مرحله قبل و بلاک خالی) توافق کنند، پس با اجرای دوباره مرحله این فاز سعی در توافق بر روی بلاک مورد نظر می‌شود. این فاز در تصویر ۲ ـ ۱ قسمت d مشخص شده‌است.

درنهایت پس از ۱۳ مرحله از اجرای *BA مشخص می‌شود که در این دور شبکه بر روی بلاک خاصی توافق کرده است یا خیر. ممکن است به دلیل اینکه پیشنهاددهنده بلاک مهاجم است طی این مراحل گره‌ها بر روی هیچ بلاکی توافق نکند و به اجرای دور بعد بپردازند.

---

[1] Reduction Phase
[2] BinaryBA* Phase
[3] Committee Members
[4] Strongly Synchronous

فصل سوم

بررسی مسئله

برخلاف بیت‌کوین که تنها به استخراج‌کننده‌هایی که در شبکه فعال هستند و استخراج می‌کنند پاداش داده می‌شود، در شبکه الگورند در حال حاضر به هر گره‌ای که در شبکه آنلاین باشد بعد از پخش بلاک پاداشی متناسب با سهام آن شخص تعلق می‌گیرد. درصورتی که ممکن است این گره در توافق بلاک بی‌تأثیر بوده و در پخش و توافق روی این بلاک مشارکتی نداشته باشد، ولی سیاست الگورند برای پخش پاداش در حال حاضر این موضوع را در نظر نگرفته و به همه گره‌ها پاداش می‌دهد.

هزینه‌هایی که هر نقش در الگورند برای ایفای آن نقش می‌پردازد متفاوت است. در نظر نگرفتن نقش گره‌ها و همکاری گره‌ها در شبکه برای پاداش دادن به آن‌ها، می‌تواند انگیزه‌ای برای گره‌ها باشد که با سایرین تعامل نکنند و با انجام ندادن مسئولیت‌های خود در پروتکل هزینه‌های خود را کاهش دهند. در نهایت نیز پاداش یکسان ساخت بلاک را دریافت کنند. این مشکل با بزرگ‌تر شدن شبکه الگورند بزرگ‌تر هم می‌شود زیرا شبکه الگورند باید درنهایت به همه گره‌های موجود پاداش دهد و با بزرگ‌تر شدن شبکه مقدار این پاداش نیز باید افزایش یابد تا انگیزه لازم برای مشارکت و همکاری در اجرای پروتکل را ایجاد کند، همین‌طور ممکن است با بیشتر شدن گره‌های منطقی‌ای[1] که فقط به فکر سود خود از اجرای الگوریتم هستند و از مشارکت خودداری

[1] Rational

می‌کنند قسمت‌های مهمی از این الگوریتم مختل شود.

در این مرحله، با توجه به ساختار شبکه الگورند، طرح مسئله به دو مسیر کاملا متفاوت تقسیم می‌شود:

۱. الگورند همانند قبل به استفاده از شبکه نظیر به نظیر ادامه دهد.

۲. الگورند شروع به استفاده از شبکه بازپخش در پروتکل خود کند؛ در حال حاضر بنیاد الگورند با تعدادی از موسسات به صورت متمرکز، قراردادی تنظیم کرده است که برای سرعت بخشیدن به روند رشد این رمزارز کمک کنند، این موسسات زیرساخت برای ایجاد شبکه بازپخش را برای الگورند آماده کرده‌اند.

پس در ادامه این دو مسیر را از هم جدا کرده و مشکلات و راه‌حل‌های آن‌ها را جداگانه بررسی و تحلیل می‌کنیم.

۳ـ۱ شبکه نظیر به نظیر

مسئله موجود در شبکه نظیر به نظیر این است که در این شبکه نقش و فعالیت کاربران در میزان پاداش آن‌ها تأثیری ندارد. در صورتی که بدون در نظر گرفتن این موضوع، در آینده فعالیت کل شبکه مختل خواهد شد.

این مسئله را می‌توانیم به صورت ریاضی هم اثبات کنیم؛ در [۷] رفتار گره‌های موجود با یک بازی غیرمشارکتی چند نفره تکرار شونده مدل شده است و اثبات می‌شود درصورتی که الگورند نحوه پخش پاداش را در شبکه خود تغییر ندهد تعادل نش در بازی مدل شده، نقطه‌ای خواهد بود که هیچکدام از گره‌ها در شبکه مشارکتی ندارند. در این مقاله براساس هزینه‌های هر نقش، مقدار پاداش برای او محاسبه شده است و نشان داده می‌شود در صورتی که این مقادیر پاداش به جای پاداش یکسان برای همه نقش‌ها در نظر گرفته شود تعادل نش در بازی مدل شده به همکاری همه کاربران منجر خواهد شد. همین طور پاداشی که سیستم باید به کل کاربران بدهد کاهش خواهد یافت. پاداش نقش‌های مختلف براساس فعالیت و هزینه آن نقش در نظر گرفته می‌شود به طور مثال هزینه‌های هر نقش به این صورت است:

- پیشنهاددهنده بلاک: بررسی تراکنش‌ها، تولید بلاک و پخش شایعه بلاک
- اعتبارسنج‌ها[1]: بررسی اعتبار بلاک ، پخش شایعه بلاک، رای دهی
- سایر گره‌ها: بررسی اعتبار بلاک، پخش شایعه بلاک

براساس این هزینه‌ها در [۷] پاداش متفاوتی به نقش‌ها داده شده که موجب انگیزه برای اجرای درست نقش‌ها در الگورند می‌شود. به‌طور مثال پیشنهاددهنده بلاک و اعتبارسنج‌ها برای دریافت پاداش مختص به این نقش‌ها،

[1] Verifiers

نقش خود را در شبکه به درستی ایفا می‌کنند. ولی در این مقاله به فعالیت سایر گره‌ها توجهی نشده است و این موضوع نیز می‌تواند مشکلات بزرگی برای شبکه بیافریند.

تعداد زیادی از گره‌های شبکه فاقد نقش خاصی در پروتکل هستند و این گره‌ها فارغ از اینکه در پخش و توافق بلاک تأثیری داشته‌اند یا خیر از پاداش یکسانی برخوردار خواهند شد. پس با عدم همکاری در مراحل پروتکل و پخش نکردن شایعه‌ها می‌توانند هزینه‌های خود را کاهش داده و پاداش یکسانی دریافت کنند و با پخش نشدن شایعه‌ها ممکن است کل شبکه یا قسمتی از آن آسیب ببینند. پس در این پروژه تلاش می‌کنیم پاداش‌دهی نهایی را به نحوی به مشارکت گره‌ها در شبکه مرتبط کنیم، تا این مشکل در شبکه به وجود نیاید.

پس مسئله موجود را می‌توانیم این‌گونه مطرح کنیم که چطور فعالیت گره‌های عادی برای پخش بلاک در شبکه را تشخیص دهیم و سعی کنیم فقط به گره‌هایی که فعالیت بیشتری داشته‌اند پاداش دهیم. در این صورت گره‌های شبکه، انگیزه اجرای درست شایعه را خواهند داشت و شبکه الگورند به جای پاداش دادن به کل گره‌های شبکه می‌تواند به تعداد کمتری از گره‌ها پاداش دهد. پس باید سازوکاری معرفی کنیم تا گره‌هایی که فعالیت بیشتری داشته‌اند را شناسایی کرده و در نهایت پاداش به این گره‌ها تخصیص داده شود. در غیر این‌صورت با بزرگ شدن شبکه الگورند، هزینه گزافی باید توسط بنیاد الگورند برای پاداش به گره‌ها در نظر گرفته شود.

یکی دیگر از مشکلاتی که در حال حاضر در شبکه الگورند وجود دارد ایجاد گره‌های سیبل[1] توسط مهاجم است که خود سهامی ندارند ولی در شبکه وجود دارند و می‌توانند گیرنده پیام‌های منتشر شده در شبکه باشند. برای تشخیص گره‌های فعال در شبکه سعی می‌کنیم این مشکل را نیز در نظر گرفته و سعی در برطرف کردن آن داشته باشیم.

۳ـ۲ شبکه بازپخش

در این حالت یعنی استفاده الگورند از گره‌های رله در کنار گره‌های معمولی، هزینه گره‌ها و نقش‌های مختلف بسیار متفاوت از حالت قبل خواهد بود و نیاز به بررسی مجدد دارند. پس باید هزینه هر نقش در شبکه بازپخش را دوباره بررسی و اندازه‌گیری کرد.

لازم است به این موضوع اشاره کنیم که مسئله قبلی که در حالت نظیر به نظیر با آن مواجه بودیم، در این شبکه وجود ندارد. چون گره‌های عادی وظیفه‌ای برای پخش شایعه ندارند و فقط درصورت پذیرش نقش پاداش دریافت می‌کنند، که این نقش بر اساس تابع قرعه‌کشی و در جریان پروتکل مشخص می‌شود . هم‌چنین می‌توان پاداش گره‌های عادی را با هزینه‌های موجود آن‌ها محاسبه کرد.

[1] Sybil Node

از آنجایی که الگورند به تازگی از این گره‌ها در شبکه خود استفاده کرده است مستندات دقیقی از نحوه قرارگیری این گره‌ها در کنار گره‌های معمولی و تعداد و ظرفیت آن‌ها نداریم ولی سعی می‌کنیم با تخمین براساس دانسته‌های موجود، این نوع شبکه را نیز تحلیل کنیم. در حال حاضر گره‌های رله در شبکه موسساتی هستند که قراردادهای ۲ تا ۵ ساله برای ارائه خدمات به شبکه الگورند دارند و به ازای این خدمات، الگو یعنی سهام الگورند دریافت می‌کنند[۱]. پس از پایان این مدت شبکه الگورند برای حفظ غیرمتمرکز بودن باید به همه اجازه برعهده گرفتن نقش رله در شبکه را بدهد و براساس خدماتی که برای شبکه دارند به آن‌ها پاداش تعلق گیرد.

مسئله جدید در شبکه بازپخش در همین جا کاملا مشخص است. بر چه اساسی باید به گره‌های رله پاداش دهیم؟ آیا نیاز است قبل از پاداش دادن صداقت این گره‌ها در ارائه خدمات بررسی شود؟ در شبکه‌ای که غیرمتمرکز است بر چه اساسی باید مقدار این پاداش برای هر گره به صورت جداگانه مشخص شود؟

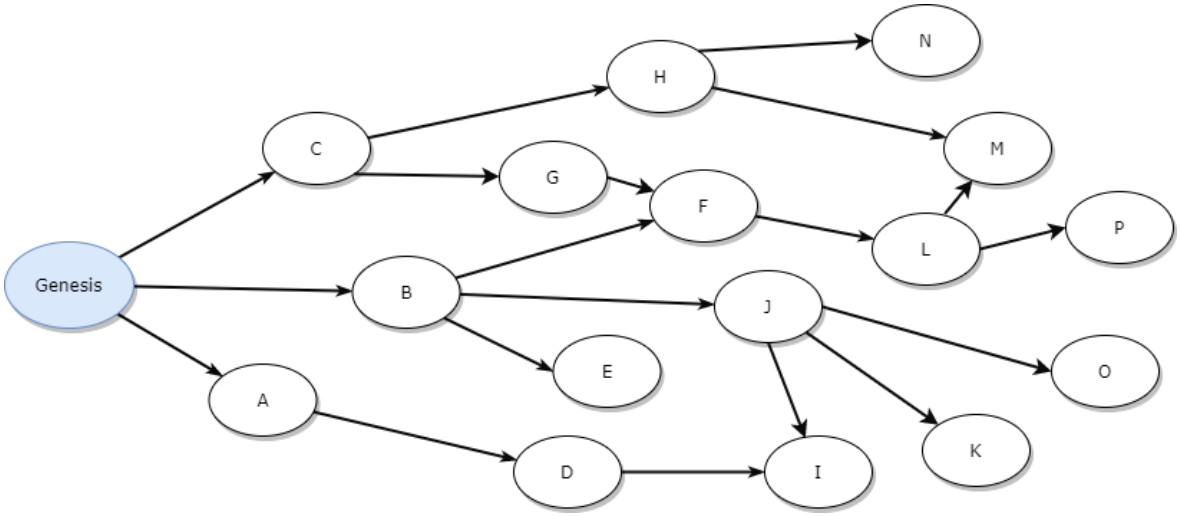
فصل چهارم

شبکه نظیر به نظیر، ارائه راه حل

در این فصل قصد داریم ایده‌هایی برای حل مسئله مطرح شده برای شبکه نظیر به نظیر ارائه دهیم. جزئیات پیاده سازی و مشکلات و پیچیدگی‌های اضافه شده با استفاده از این راه حل در فصل بعدی به تفصیل بررسی خواهد شد.

در شبکه الگورند در هر مرحله چند پیشنهاددهنده برای شبکه انتخاب می‌شوند که وظیفه ساخت بلاک را دارند و این بلاک را در شبکه پخش می‌کنند. در نهایت احتمالا کل شبکه بر روی بلاک منتشر شده توسط یکی از پیشنهاددهنده‌ها که دارای سهام بیشتری است توافق می‌کند. پس برای ساده‌سازی مسئله موجود ما می‌توانیم فرض کنیم که بقیه مراحل اعم از اجرای الگوریتم قرعه‌کشی برای مشخص شدن نقش‌ها و الگوریتم *BA برای رای‌گیری و توافق نهایی روی بلاک نهایی در شبکه انجام شده است و به بررسی آن‌ها در این گزارش نپردازیم. پس با ساده کردن شبکه با این فرض، مسئله را این‌گونه مطرح می‌کنیم؛ در شبکه نظیر به نظیر الگورند، یکی از گره‌های شبکه (پیشنهاددهنده بلاک با بالاترین اولویت)، بلاکی را ساخته و با شروع از این گره، بلاک ساخته‌شده در کل شبکه منتشر می‌شود.

با ساده کردن شبکه به این‌صورت، می‌توانیم نحوه‌ی تشخیص و پاداش‌دهی به گره‌هایی که فعالیت بیشتری داشته‌اند را بهتر تحلیل کنیم.



شکل ۴ـ۱: گراف تعاملات

۴ـ۱ گراف تعاملات

شایعه پیام‌ها در کارایی شبکه الگورند تأثیر بسیار زیادی دارند ولی شایعه پیام‌های کوچکی مثل پیام‌های مشخص‌کننده الویت[1]، هزینه خاصی برای گره‌ها ندارد. در صورتی که بررسی بلاک و شایعه پیام‌های بلاک[2] یکی از هزینه‌های اصلی برای هر گره محسوب می‌شود و هر گره برای کاهش هزینه‌های خود می‌تواند از انجام این مسئولیت فرار کند. این مسئولیت یکی از کلیدی‌ترین عملیات‌ها در کل فرآیند توافق بلاک در شبکه است؛ از این رو برای پاداش دادن به تعداد کمتری از گره‌ها می‌توانیم معیار انتخاب را میزان مشارکت گره برای پخش بلاک معتبر در شبکه در نظر بگیریم.

در صورتی که شبکه را بر اساس فرضیاتی که در قسمت قبل بررسی کردیم ساده کنیم، می‌توانیم گرافی از تعاملات گره‌ها برای پخش بلاک جدید بسازیم که مشخص می‌کند هر گره از چه گره‌ای بلاک معتبر را دریافت کرده است. در تصویر ۴ـ۱ می‌توانید گراف تعاملات مورد نظر را مشاهده کنید.

یکی از مشکلاتی که سعی در برطرف کردن آن داریم گره‌های سیبل با سهام صفر در شبکه است، برای اینکه از ارسال بلاک به گره‌های سیبل جلوگیری کنیم، باید هر گره از گرفتن بلاک از یک گره با سهام صفر خودداری کند؛ این خودداری کردن شامل همه گره‌هایی است که در شاخه‌ی منبع بلاک قرار دارند، منظور از شاخه منبع، مسیری در گراف است که بلاک از گره پیشنهاددهنده به گره مورد نظر رسیده است. با گذاشتن این شرط گره‌ها برای اینکه در شاخه نامعتبر قرار نگیرند قبل از ارسال بلاک، صفر نبودن سهام گیرنده را بررسی می‌کنند.

برای اینکه هر گره بتواند همه گره‌ها را در شاخه منبع بررسی کند باید به مسیر رسیدن بلاک به خودش

[1]Priority Gossip Messages
[2]Block Gossip Messages

دسترسی داشته باشد پس هر گره پس از دریافت بلاک ،نام خود را در پیام مربوط به بلاک مورد نظر درج می‌کند. از آنجایی که هر گره از مسیر گره‌های قبل از خود باخبر است اقدام به ارسال بلاک به آن‌ها نخواهد کرد و در گراف تعاملات توصیف شده، دور وجود نخواهد داشت؛ پس این گراف یک گراف جهت دار بدون دور خواهد بود.

پس از پخش بلاک در شبکه و توافق همه گره‌ها روی بلاک مورد نظر هر گره می‌داند که در چه شاخه‌ای از گراف تعاملات مورد نظر قرار دارد ولی هیچکدام از آن‌ها از ساختار کل گراف باخبر نیست. برای ساخته شدن گراف تعاملات در پایان همه مراحل، یک مرحله جدید به عنوان پخش منبع باستفاده از پروتکل شایعه در شبکه اضافه می‌کنیم، که هر گره یک یا چند گره را به عنوان منبع خود معرفی می‌کند. در این‌صورت هر گره نهایتا می‌تواند با دریافت همه این پیام‌ها از شبکه، گراف تعاملات را در خود ایجاد کند.

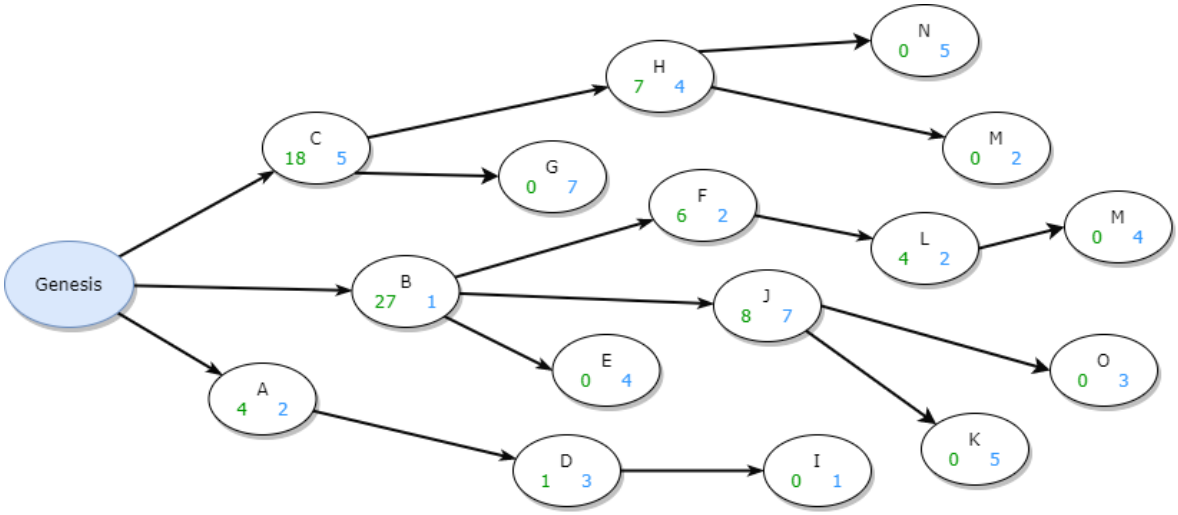
در شبکه الگورند برای کاهش سربار شبکه هر گره‌ای که بلاک را دریافت نکرده باشد خودش به سایر گره‌های همسایه اعلام می‌کند تا در صورت داشتن بلاک برای او بلاک مورد نظر را ارسال کنند. پس در این شبکه برای یک گره دوبار بلاک ارسال نخواهد شد مگر اینکه دو یا چند همسایه تقریبا به صورت همزمان این بلاک را برای او ارسال کنند. در این‌صورت گره اولین بلاکی که دریافت کرده است را قبول و بقیه را رد می‌کند، پس هر گره فقط یک گره را به عنوان منبع خود معرفی می‌کند. معرفی کردن چند گره به عنوان منبع هم سربار شبکه را افزایش می‌دهد هم برای گره مورد نظر سربار محاسباتی و هزینه اضافی خواهد بود. پس از این به بعد فرض می‌کنیم که هر گره فقط می‌تواند یک گره را به عنوان منبع خود اعلام کند، تا هم از سربار محاسباتی برای هر گره بکاهیم، هم از تعداد و حجم پیام‌های انتقالی در شبکه کم کنیم. با این فرض گراف جهت‌دار بدون دور تعاملات به درخت تعاملات تبدیل می‌شود.

یکی از نکات جالب در مورد این درخت این است که گره‌هایی که در پخش بلاک هیچ مشارکتی نداشته‌اند برگ‌های درخت خواهند بود. البته گره‌هایی که در مراحل آخر نیز بلاک را دریافت کرده‌اند برگ‌های این درخت هستند ولی این موضوع با اینکه در پخش بلاک مشارکتی نداشته‌اند تناقضی ندارد، یعنی شاید قصد مشارکت داشته باشند ولی در این مرحله فرصتی برای این کار نداشته‌اند.

اگر فرض کنیم که همه گره‌ها در انتشار بلاک مشارکت می‌کنند و بلاک را برای q گره دیگر ارسال می‌کنند، درخت تعاملات یک درخت کامل خواهد بود که برگ‌های آن گره‌های سطح آخر درخت هستند پس نسبت برگ‌ها به کل گره‌های درخت را می‌توانیم از رابطه زیر محاسبه کنیم:

$$\frac{Leaves}{All\ Nodes} = \frac{q^{n-1}}{\frac{q^n-1}{q-1}} = \frac{q^{n-1}(q-1)}{q^n-1} \approx \frac{q-1}{q} \qquad (۱-۴)$$

پس اگر نرخ ارسال بلاک یعنی q برابر عدد 8 باشد، تقریبا $7/8$ از گره‌ها برگ هستند پس با حذف آن‌ها



شکل ۴ـ۲: امتیازدهی براساس سهام گره‌های دریافت کننده
سهام هر گره با رنگ آبی در گوشه سمت راست و امتیاز او با رنگ سبز در گوشه سمت چپ مشخص شده است.

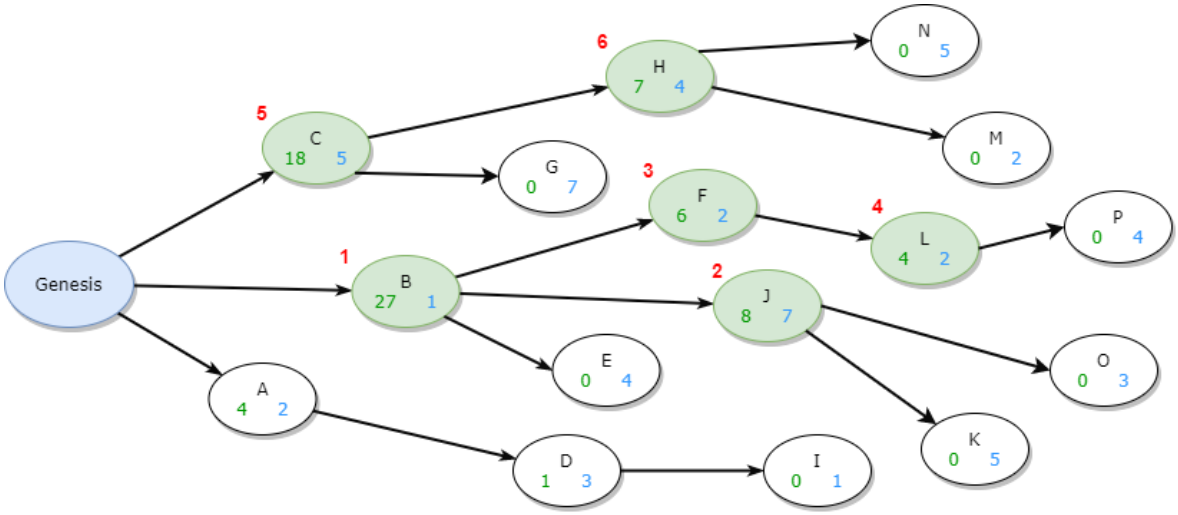
فقط 1/8 گره‌ها برای پاداش دادن باقی‌خواهند ماند، پس اگر فقط برگ‌های درخت را حذف کنیم به نتیجه قابل تاملی می‌رسیم و در بدترین حالت حداقل نیمی از گره‌های کل شبکه برای پاداش دادن انتخاب نمی‌شوند که همه کسانی که در پخش بلاک تعامل نداشته‌اند در این دسته قرار خواهند گرفت.

البته با داشتن این درخت می‌توانیم میزان مشارکت گره‌ها یا تأثیر پیام آن‌ها بر روی شبکه را مورد بررسی قرار دهیم و با مشخص کردن معیاری برای مشارکت در شبکه، تعداد کمتری از گره‌های موجود را برای پاداش‌دهی انتخاب کنیم. پس در ادامه معیار مشارکت برای هر گره را مشخص کرده و با استفاده از الگوریتم‌های انتخاب بر اساس معیار معرفی شده، تعدادی از گره‌های شبکه را برای پاداش‌دهی انتخاب می‌کنیم.

۴ـ۲ معیار مشارکت

همانطور که در بخش قبل اشاره کردیم برگ‌های این درخت گره‌هایی هستند که در پخش بلاک نقشی نداشته‌اند ولی به معیار مقایسه‌ای برای میزان مشارکت و تأثیر پیام‌های ارسالی سایر گره‌ها نیز نیاز داریم. به صورت واضحی مشخص است که تعداد گره‌هایی که یک گره برای آن‌ها پیام ارسال کرده است می‌تواند معیاری برای مشارکت گره‌ها باشد ولی این معیار فقط تأثیر مستقیم پیام‌های ارسالی این گره را نشان می‌دهد و برای اضافه کردن تأثیر غیر مستقیم این گره بر روی پخش بلاک می‌توانیم تعداد همه گره‌هایی که در زیر شاخه‌های این گره هستند را به عنوان امتیاز این گره در نظر بگیریم.

موضوع دیگری که باید درنظر بگیریم این است که در الگورند، نقش‌ها به الگوهای یک گره اختصاص می‌یابد؛ در نتیجه هر چقدر سهام یک گره بیشتر باشد قدرت آن در شبکه بیشتر است. پس در نهایت معیار



شکل ۴ـ۳: الگوریتم عمیق‌شونده بازگشتی
گره‌های منتخب با رنگ پس‌زمینه سبز مشخص شده‌اند و ترتیب انتخاب با شماره قرمز نشان داده شده است.

امتیازدهی را براساس سهام گره‌های دریافت کننده بلاک در نظر می‌گیریم. در تصویر ۴ـ۲ می‌توانیم امتیازدهی به گره‌ها براساس این معیار را مشاهده کنیم.

۴ـ۳ الگوریتم انتخاب

برای انتخاب چند گره برای پاداش دادن به آن‌ها، می‌توانیم از این الگوریتم استفاده کنیم.

الگوریتم عمیق‌شونده بازگشتی: در این الگوریتم از گره پیشنهاددهنده بلاک، انتخاب گره‌های منتخب را آغاز می‌کنیم و هر گره‌ای که بیشترین امتیاز را داشته باشد انتخاب کرده و گسترش می‌دهیم. سپس از بین گره‌های گسترش داده شده، یعنی بچه‌های گره منتخب، گره دارای بیشترین امتیاز را انتخاب می‌کنیم و همینطور پایین‌تر رفته تا به جایی برسیم که بچه‌های گره منتخب فقط شامل برگ‌های درخت باشد. در اینصورت یک پله به عقب برمی‌گردیم و گره‌های دیگر که بررسی نشده‌اند را مورد قرار می دهیم. این روند تا جایی ادامه می‌یابد تا به سقف گره‌های مورد نظر برسیم. انتخاب گره‌های نهایی روی درخت با این الگوریتم را می‌توانیم در تصویر ۴ـ۳ مشاهده کنیم.

ایده‌ي انتخاب گره‌ها در الگوریتم عمیق‌شونده بازگشتی این است که همه گره‌های شاخه‌ی پرکار را انتخاب کند چون گره‌های این شاخه تأثیر بیشتری در پخش بلاک داشته‌اند.

خروجی الگوریتم انتخاب، لیستی از گره‌هایی است که مستحق پاداش هستند، معیار پایان انتخاب گره‌ها برای این لیست می‌تواند به دو صورت مشخص شود؛ ۱ـ همانطور که در توضیح الگوریتم ذکر کردیم در هر مرحله تعدادی گره مشخص برای پاداش دهی انتخاب شوند. یعنی تعداد گره‌های لیست نهایی همیشه برابر با

تعدادی است که پروتکل مشخص کرده است. ۲ـ به تعداد گره‌های انتخابی دقت نکنیم و معیار پایان سهام گره‌های منتخب باشد. چون در نهایت پاداش باید براساس سهام این گره‌ها داده شود شاید اگر مقدار سهام گره‌ها در لیست نهایی ثابت باشد معیار خوبی برای پایان دادن به فرایند داشته باشیم.

اگر از الگوریتم عمیق‌شونده بازگشتی برای انتخاب گره‌های منتخب استفاده کنیم، یک گره با اعلام اینکه از چند گره متفاوت بلاک را دریافت کرده است احتمال اینکه در شاخه‌ای قرار بگیرد که کار بیشتری در آن صورت گرفته است را برای خود افزایش می‌دهد؛ پس ممکن است یک گره دروغ‌گو کل شبکه را به عنوان منبع خود اعلام کند تا در هر صورت در لیست نهایی انتخاب شود. ولی با محدود کردن گره‌ها به انتخاب تنها یک گره به عنوان مبدا خود از این موضوع جلوگیری می‌کنیم.

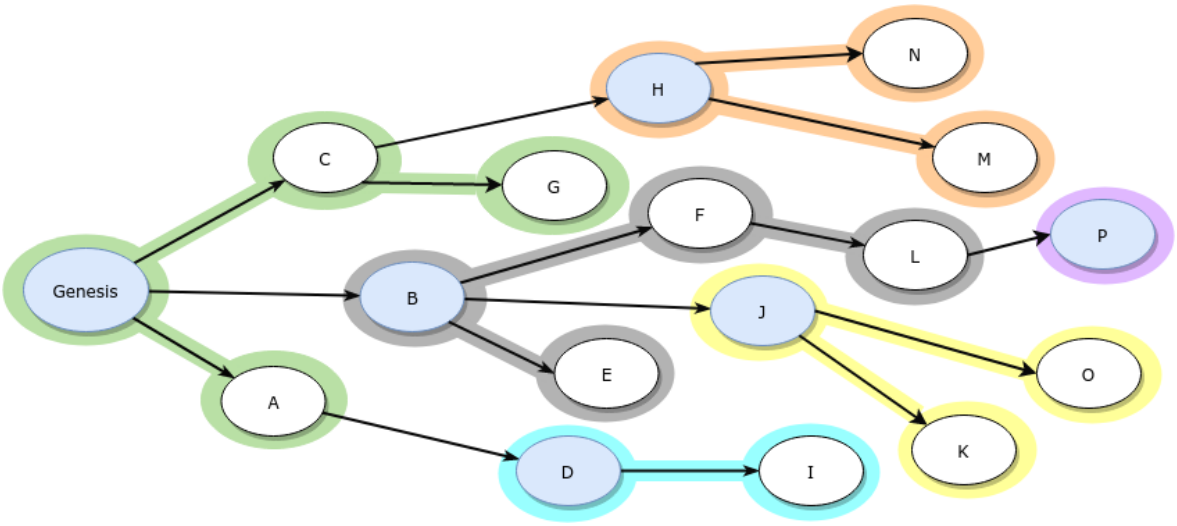
۴ـ۴ ساخت درخت

تا این قسمت گراف تعاملات بین گره‌ها را توصیف کردیم ولی چگونگی ساخت این گراف برای هر گره را مشخص نکردیم. هر گره برای اینکه بتواند تشخیص دهد که کدام یک از گره‌های شبکه حق دریافت پاداش دارند باید بتواند گراف مورد نظر را تشکیل دهد و براساس الگوریتم انتخاب استفاده شده گره‌های منتخب را تشخیص دهد.

برای اینکه هر گره بتواند درخت مورد نظر را بسازد باید از تمام اتصالات موجود باخبر باشد؛ یعنی هر گره به صورت جداگانه باید منبع دریافت بلاک از سمت خودش را معرفی کند. در این صورت باید بعد از به توافق رسیدن روی یک بلاک مشخص، یک بازه زمانی جدید برای ارسال پیام‌های معرفی منبع بلاک در نظر گرفته شود. در این بازه زمانی باید هر گره منبع دریافت بلاک از سمت خودش را به کل شبکه معرفی کند. پس در صورتی که شبکه شامل n گره باشد باید دقیقا n پیام در کل شبکه به صورت شایعه پخش شود.

حجم این پیام‌ها بسیار کم است و پخش شدن چنین پیام کوچکی در شبکه زمان چندانی لازم ندارد، ولی تعداد این پیام‌های کوچک بسیار زیاد است و ممکن است پخش نمایی این پیام‌ها، موجب ایجاد ازدحام در برخی از اتصالات شبکه باشد.

برای کاهش تعداد پیام‌های منتقل شده در بازه زمانی پخش بلاک می‌توانیم در هر قسمت گراف نماینده‌هایی انتخاب کنیم که وظیفه آن‌ها جمع‌آوری تعدادی از پیام‌ها و ارسال آن‌ها به صورت تجمیع‌شده در شبکه است. در این‌صورت تعداد پیام‌هایی که باید در شبکه پخش شوند وابسته به تعداد نماینده‌ها خواهد بود. باید براساس اندازه و ساختار شبکه تعداد این نماینده‌ها تنظیم شود تا حجم پیام ارسالی از سمت هر نماینده زیاد نباشد.



شکل ۴ـ۴: بخش‌بندی گراف با انتخاب نماینده
نماینده‌ها با رنگ آبی مشخص شده‌اند و هر بخش با نماینده آن با رنگ خاصی مشخص شده‌است.

۴ـ۵ انتخاب نماینده‌ها

انتخاب این نماینده‌ها به دو صورت قابل انجام است:

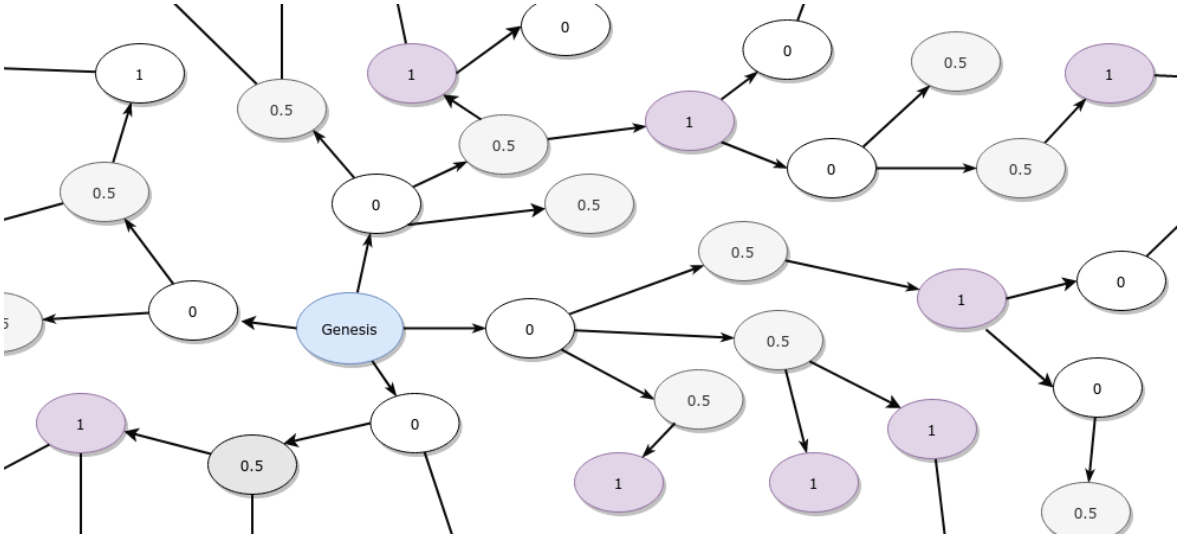
۱. انتخاب نماینده‌ها وابسته به درخت تعاملات: می‌توانیم نماینده‌های مورد نظر را وابسته به پخش یلاک یعنی وابسته به درخت تعاملات انتخاب کنیم. منظور از وابسته به درخت تعاملات این است که هر گره درصورتی که به عنوان نماینده انتخاب شود، نماینده زیرشاخه زیرین خود در درخت خواهد بود. پس هر گره به محض دریافت بلاک نماینده خود را تشخیص می‌دهد.

۲. انتخاب نماینده‌ها به صورت مستقل: منظور از انتخاب مستقل نماینده‌ها این است که نماینده‌های مورد نظر به درخت تعاملات وابسته نباشند، به صورت تصادفی در کل شبکه انتخاب شوند و خود را مستقل از سایر مکانیزم‌های موجود در شبکه تبلیغ کنند. در این شرایط هر گره باید یکی از نماینده‌ها را به عنوان نماینده خود انتخاب کند.

۴ـ۵ـ۱ نماینده‌های وابسته به درخت

هر گره باید با نماینده خود ارتباط برقرار کند، پس باید او را بشناسد. نماینده هر گره، نزدیکترین نماینده به او در شاخه ارسال بلاک است؛ به عبارت دیگر هر گره با دانستن مسیر ارسال بلاک از گره پیشنهاددهنده تا خودش باید آخرین نماینده در مسیر را به عنوان نماینده خود انتخاب کند. برای اینکه همه گره‌ها دارای نماینده‌ای باشند گره پیشنهاددهنده اولین نماینده در این درخت خواهد بود.

با این‌کار شبکه به بخش‌های متمایزی که هر بخش یک نماینده دارد تقسیم می‌شود. این بخش بندی را



شکل ۴ـ۵: متغیر $cntr$
مقدار متغیر $cntr$ در شبکه‌ای با $\alpha = 0.5$

می‌توانید در تصویر ۴ـ۴ مشاهده کنید.

انتخاب تصادفی نماینده‌ها از میان کل گره‌های شبکه موجب تجمع تعداد زیادی گره در بخش‌های با ارتفاع کمتر می‌شود؛ یعنی هر چقدر گره نماینده در ارتفاع کمتری باشد بخشی از گراف که زیرمجموعه او است بزرگتر خواهد بود. هر چقدر یک نماینده در ارتفاع کمتری در درخت تعاملات قرار داشته باشد احتمال بیشتری برای انتخاب شدن برای آخرین نماینده دارد، زیرا در مسیرهای بیشتری از گره‌های برگ تا گره پیشنهاددهنده حضور دارد.

در صورتی که بخش‌بندی گراف به صورت نامتوازن انجام گیرد برخی از پیام‌ها بسیار بزرگ و برخی دیگر بسیار کوچک خواهند بود که این موضوع باعث می‌شود زمانی که باید برای پخش پیام‌ها در نظر بگیریم بیش از اندازه زیاد باشد، زیرا حداقل باید به اندازه زمان لازم برای پخش بزرگترین پیام در شبکه باشد.

برای حل مشکل نامتوازن بودن بخش‌بندی‌های گراف باید نماینده‌ها را به صورتی در گراف انتخاب کنیم که در هر مسیر از پخش به صورت متناوب نماینده‌هایی حضور داشته باشند. به طور مثال اگر بخواهیم نماینده‌ها با نرخ r در هر مسیر تکرار شوند، می‌توانیم قسمتی به نام $cntr$ به پیام بلاک در حال پخش بیافزاییم و با گذشتن بلاک از هر گره به اندازه $\alpha = 1/r$ به مقدار $cntr$ اضافه کنیم. با رسیدن مقدار $cntr$ به مقدار ۱ گره مورد نظر باید به عنوان نماینده انتخاب شود. با این شرایط تضمین می‌شود که در هر مسیر از درخت به صورت متناوب نماینده‌هایی وجود دارند پس احتمال انتخاب نماینده‌ها با ارتفاع کمتر برابر با احتمال انتخاب سایر نماینده‌ها خواهد بود.

در تصویر ۴ـ۵ می‌توانید مقدار $cntr$ در هر گره را مشاهده کنید. گره‌هایی که مستقیما به یک نماینده

متصلند، نباید به عنوان نماینده انتخاب شوند پس مقدار $cntr$ در آن‌ها مجددا روی صفر تنظیم می‌شود.

۴-۵-۲ نماینده‌های مستقل

نماینده‌های مستقل، باید خود را در شبکه جداگانه تبلیغ کنند. در این‌صورت انتخاب تصادفی این گره‌ها مشکلی در بر نخواهد داشت، زیرا هرکدام به اندازه ظرفیت مشخصی که برای هر نماینده در نظر می‌گیریم گره سرویس‌گیرنده انتخاب می‌کنند.

برای انتخاب تصادفی این نماینده‌ها می‌توانیم از تابع قرعه‌کشی استفاده کنیم و در هنگام تبلیغ نیز گره‌های نماینده می‌توانند به وسیله اثبات قرعه‌کشی نقش خود را به بقیه گره‌ها اثبات کنند. هر گره با دریافت تبلیغ این گره‌ها یکی از آن‌ها را به عنوان نماینده خود انتخاب می‌کند و به او درخواست ارسال می‌کند. نماینده مورد نظر درصورتی که ظرفیت برای پذیرش گره جدید داشته باشد او را قبول و در غیر این‌صورت او را رد می‌کند. در صورت رد شدن گره باید به یک نماینده دیگر درخواست ارسال کند. تعداد نماینده‌ها باید طوری انتخاب شود که هر گره یک نماینده داشته باشد.

۴-۵-۳ مقایسه

مشخص است که انتخاب نماینده‌ها وابسته به درخت، تغییرات زیادی روی پروتکل اعمال نخواهد کرد و از پخش بلاک برای تبلیغ و مشخص کردن نماینده‌ها استفاده می‌کند، درصورتی که برای استفاده از نماینده‌های مستقل، باید پیام‌های جداگانه‌ای را در شبکه پخش کنیم.

با این حال وقتی انتخاب نماینده‌ها به پخش بلاک وابسته باشد، نمی‌توانیم تضمین کنیم که هر نماینده، تعداد اعضای زیرمجموعه ثابتی داشته باشد. به خصوص اگر شبکه در دنیای واقعی باشد، تجمع گره‌ها به صورت منطقه‌ای است و بلاک به صورت منطقه‌ای پخش خواهد شد و انتخاب تنظیمات ثابتی برای شبکه‌ای نامتوازن، کار ساده‌ای نخواهد بود. در فصل بعد درمورد تنظیم متغیرهای مربوط به پخش بیشتر صحبت خواهد شد.

مشکل بزرگی که ایده استفاده از نماینده‌ها به دنبال دارد، حمله منع سرویس به این گره‌های خاص در شبکه است. با توجه به این که گره‌های نماینده برای همه یا تعدادی از گره‌ها شناخته شده هستند، در صورت وجود مهاجم در شبکه ممکن است مورد حمله منع سرویس قرار گیرند. در صورتی که یکی از این گره‌ها مورد حمله قرار گیرد بخشی از شبکه که زیرمجموعه اوست از دریافت پاداش محروم می‌ماند. این حمله ممکن است مشکل نسبتا بزرگی در شبکه به وجود آورد. از آنجایی که تبلیغ نماینده‌های مستقل در کل شبکه پخش می‌شود، این موضوع می‌تواند مشکل حمله منع سرویس را تشدید کند. البته مشکل حمله منع سرویس در هر دو مدل وجود دارد.

	نماینده‌های مستقل	نماینده‌های وابسته به درخت
تغییر در پروتکل	زیاد	کم
تعداد اعضای زیرمجموعه	متوازن	نامتوازن
حمله منع سرویس	خطر زیاد	خطر متوسط

جدول ۴ـ۱: مقایسه دو روش انتخاب نماینده

در مقابل برای انتخاب نماینده‌های مستقل می‌توانیم از تابع قرعه‌کشی استفاده کنیم و مطمئن باشیم که کسی خود را به غلط نماینده معرفی نمی‌کند و از آنجایی که تابع قرعه‌کشی بسته به مقدار سهام احتمال انتخاب می‌دهد، یک گره مهاجم فقط با داشتن سهام بسیار زیاد، می‌تواند در شبکه مشکل ایجاد کند.

فصل پنجم

شبکه نظیر به نظیر، تحلیل راه حل

در این قسمت قصد داریم راه‌حل ارائه شده در فصل قبل را از نظر سرباری که به شبکه و گره‌ها اضافه کرده و کارایی راه‌حل بررسی کنیم. به طور قطع اینکه از چه الگوریتم، پروتکل یا ساختمان داده‌ای در پیاده سازی استفاده کنیم در نتیجه نهایی و سربار روی شبکه تأثیر خواهد داشت پس تحلیل‌های انجام شده را بر اساس تنظیمات ممکن دسته‌بندی می‌کنیم و با بررسی کارایی آن‌ها براساس شبیه‌ساز طراحی شده، در نهایت مشکلات و مزیت‌های هرکدام را مشخص می‌کنیم.

یکی از مواردی که هم درترافیک شبکه و هم در زمان پردازشی هر گره تأثیر مستقیم دارد، امضای پیام‌های مختلف در شبکه است که بسته به رمزنگاری و طول کلید مورد استفاده مي‌تواند ویژگی‌های متفاوتی داشته باشد. در حال حاضر در الگورند از امضاهای ایمن‌ـرو به جلو[1] که با یک درخت d-ary تعریف می‌شوند، استفاده می‌شود. این امضاها به اختصار با نام BM-Ed25519 شناخته می‌شود. رمزنگاری دیگری که در این قسمت قصد بررسی آن را داریم، امضای جدیدی است که به صورت اختصاصی برای الگورند ارائه شده است و می‌تواند هزینه‌های احراز اصالت و حجم پیام‌ها را کاهش دهد، این رمزنگاری[۶] در این گزارش با نام اختصاری پیکسل استفاده می‌شود.

[1] Forward-Secure Signatures

در این بخش تحلیل انجام شده برای شبکه‌ای با ۵۰ هزار گره و میانگین تعداد اتصالات ۸ برای هر گره می‌باشد. تعداد اعضای کمیته نیز در مراحل مختلف ۲ هزار گره در نظر گرفته شده است.

۵ـ۱ سربار ترافیک شبکه

در اولین مرحله به پیام بلاک که در حال پخش در شبکه است، اطلاعاتی افزودیم. برای اینکه هر گره بتواند از مسیر رسیدن بلاک به خودش مطلع شود باید در هر مرحله فرستنده بلاک نام خود را به انتهای پیام انتشار بلاک اضافه کرده و آن را ارسال کند. از آنجایی که بلاک به صورت نمایی در شبکه پخش می‌شود ارتفاع درخت تعاملات آنقدر بلند نخواهد بود؛ براساس شبیه سازی انجام شده، در بدترین حالت ارتفاع درخت برابر ۱۵ خواهد بود. پس حجم داده‌هایی که به پیام بلاک افزوده می‌شود قابل توجه نیست و در بدترین حالت کمتر از ۵۰۰ بایت به پیام بلاک افزوده می‌شود که در برابر حجم بلاک مقدار قابل توجهی نیست.

همانطور که در فصل قبل اشاره کردیم، برای اینکه بتوانیم از درخت تعاملات برای پاداش‌دهی استفاده کنیم باید همه گره‌ها از اتصالات کل درخت باخبر شوند و روی ساختار درخت توافق حاصل شود. پس در صورتی که در انتهای دور روی بلاکی توافق کرده باشند در انتهای *BA یک مرحله پخش شایعه برای معرفی منبع باید به پروتکل اضافه شود. در این بازه هر گره می‌تواند مستقلا پیام معرفی منبع خود را در شبکه پخش کند و یا از نماینده‌های تجمیع استفاده کنیم و فقط گره‌های نماینده، پیام معرفی منبع را در شبکه منتشر کنند.

۵ـ۱ـ۱ شایعه مستقل معرفی منبع

در صورتی که در این بازه مشخص شده هر گره بخواهد به صورت جداگانه منبع خود را اعلام کند، برای یک شبکه با ۵۰ هزار گره باید ۵۰ هزار پیام در کل شبکه پخش شود اگر بخواهیم این عدد را با تعداد پیام‌های انتقالی در کل فرآیند *BA مقایسه کنیم، فرایند *BA حداقل ۴ و حداکثر ۱۳ مرحله خواهد داشت که در مجموع حداقل ۸ هزار و حداکثر ۲۶ هزار پیام منتقل می‌شود.

با اینکه حجم این پیام‌ها بسیار کم است و به تنهایی ترافیک زیادی به شبکه تحمیل نمی‌کنند، مجموع این پیام‌ها برای کل شبکه مقدار کمی نخواهد بود، هر پیام باید شامل موارد زیر باشد:

- شناسه گره مبدا و مقصد در مجموع ۶۴ بایت
- سرتیتر بلاک ۳۲ بایت
- امضا برای احراز هویت پیام ۲۵۶ بایت (پیکسل ۱۴۴ بایت)

پس در مجموع در صورت استفاده از BM-Ed25519 هر پیام حجمی برابر ۳۵۲ بایت خواهد داشت و

مجموع کل پیام‌ها در حدود ۱۷ مگابایت خواهد بود. با این که هر پیام حجم نسبتا کمی دارد ولی تعداد این پیام‌ها بسیار زیاد است و برای ارسال هر پیام باید یک کانکشن TCP برقرار شود و در عین حال به دلیل خاصیت تصادفی بودن شایعه ممکن است هر پیام چندین بار به هر گره ارسال شود. پس در کل سربار نسبتا زیادی برای شبکه خواهد داشت.

در صورت استفاده از پیکسل حجم هر پیام ۲۴۰ بایت خواهد بود و مجموع کل پیام‌ها حدود ۱۰ مگابایت خواهد بود. با اینکه حجم پیام‌ها کمتر شده ولی سربار شبکه تقریبا مشابه حالت قبل است و همچنان سربار نسبتا زیادی برای شبکه خواهد داشت.

۵ـ۱ـ۲ شایعه معرفی منبع توسط نماینده‌ها

برای کاهش تعداد پیام‌ها و افزایش کارایی پروتکل، می‌توانیم از ایده نماینده‌های تجمیع استفاده کنیم، در این‌صورت هر گره باید مستقیما به نماینده خود پیام دهد و منبع خود را معرفی کند. ارسال پیام هر گره به نماینده خود نیازمند ترافیک خاصی نیست چون پیام کوچکی به صورت مستقیم برای نماینده ارسال می‌شود. در مرحله نهایی درصورتی که پس از مراحل *BA روی همین بلاکی که نماینده منبع و مقصدهای آن را ذخیره کرده است توافق شد، نماینده پیامی کلی شامل همه اتصالات در بخش خود به صورت شایعه پخش می‌کند. این پیام شامل موارد زیر خواهد بود:

- شناسه گره نماینده ۳۲ بایت
- شناسه دور و مرحله ۸ بایت
- سرتیتر بلاک ۳۲ بایت
- پیام‌های معرفی مبدا تجمیع شده بدون سرتیتر بلاک هرکدام ۳۲۰ بایت(پیکسل ۶۴ بایت)
- امضا برای احراز هویت پیام ۲۵۶ بایت(پیکسل ۱۴۴ بایت)

با استفاده از BM-Ed25519 درصورتی که برای شبکه با ۵۰ هزار گره تقریبا ۲ هزار گره به عنوان نماینده انتخاب کنیم به صورت میانگین هر کدام نماینده ۲۵ گره خواهند بود، پس در کل حجم پیام به صورت میانگین در حدو ۸.۵ کیلوبایت است. با این کار از حجم کل پیام‌ها مقدار قابل توجهی کم نکردیم ولی تعداد آن‌ها و در نتیجه تعداد کانکشن‌های TCP و تعداد پیام‌های تکراری را کاهش دادیم. با این حال حجم پیام‌های تجمیع شده که توسط نماینده ارسال می‌شود هم قابل توجه نیست و پیام با حجم ۱۰ کیلوبایت نیز در شبکه به سرعت پخش می‌شود؛ پس به صورت کلی با این کار از سربار روی شبکه کاسته‌ایم. البته تعداد نماینده‌ها را می‌توانیم

براساس نیاز شبکه تغییر دهیم تا یک تعادل بین حجم پیام‌ها و تعداد آن‌ها حاصل شود و هم بار شبکه و هم زمان لازم برای توافق همه گره‌ها روی درخت کاهش یابد.

درصورتی که از امضای پیکسل استفاده کنیم، هر نماینده هنگام جمع‌آوری پیام‌ها می‌تواند امضای آن‌ها را نیز تجمیع کند پس لازم نیست برای هر پیام ۱۴۴ بایت امضا ذخیره شود و حجم پیام کلی به صورت چشمگیری کاهش می‌یابد. در صورتی که ۵۰۰ نماینده در نظر بگیریم پیام هر کدام در حدود ۷ کیلوبایت و کل پیام‌های معرفی منبع در حدود ۳.۵ مگابایت خواهد بود.(در حدود $\frac{1}{5}$ کل حجم BM- Ed25519)

علاوه بر پیام‌های ارسالی نحوه انتخاب نماینده هم بر سربار شبکه تأثیر خواهد داشت:

- درصورتی که از نماینده‌ها را وابسته به درخت تعاملات انتخاب کنیم، تنها کافیست که شناسه نماینده به انتهای پیام بلاک در حال پخش اضافه شود و اضافه شدن یک فیلد ۳۲ بایتی سربار خاصی برای شبکه نخواهد داشت.

- درصورتی که نماینده‌ها مستقلا انتخاب شوند باید جداگانه خود را در شبکه تبلیغ کنند؛ پس به تعداد نماینده‌ها باید پیام تبلیغ در شبکه پخش شود. هر گره برای اینکه نماینده خود را انتخاب کند باید به یکی از آن‌ها درخواست ارسال کند. نماینده با دریافت پیام درخواست درصورت داشتن ظرفیت، گره را به عنوان زیرمجموعه تایید می‌کند و در غیر این‌صورت او را رد می‌کند. در بدترین حالت هر گره باید چندین بار درخواست برای هر کدام از نماینده‌ها ارسال کند.

  در حالت عادی چون نماینده‌ها به صورت تصادفی از کل شبکه انتخاب می‌شوند هرکس با ارسال درخواست به نزدیک‌ترین نماینده یعنی اولین پیام تبلیغ دریافت شده، نماینده خود را انتخاب می‌کند.

  انتخاب نماینده‌ها به صورت مستقل سربار بیشتری برای شبکه خواهد داشت ولی درصورتی که تعداد نماینده‌ها کم باشد این سربار زیاد نخواهد بود، چون پیام تبلیغ بسیار کوچک است و درخواست‌های ارسال شده از گره‌های عادی به نماینده به اندازه برقراری ارتباط سه جانبه TCP [1]خواهد بود.

۲ـ۵ سربار زمانی

سربار زمانی اضافه شده به کل پروتکل را می‌توانیم به چهار دسته زیر تقسیم کنیم:

۱. زمانی که هر گره شبکه باید قبل از ارسال بلاک برای سایرین صرف تایید مسیر بلاک از پیشنهاددهنده تا خودش بکند. همانطور که در قسمت قبل توضیح داده شد، ارتفاع درخت تعاملات آنقدر بلند نخواهد

[1]TCP Three-way Handshake

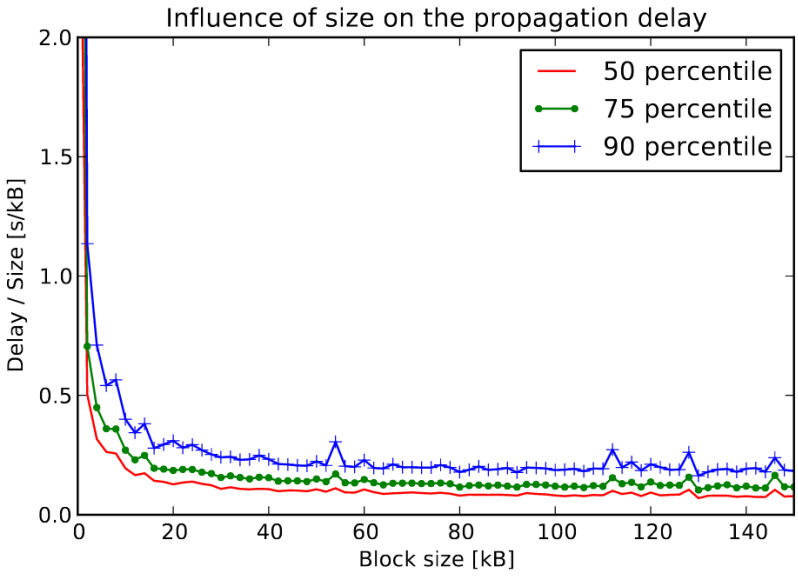
بود که زمان تایید مسیر، زمان قابل توجهی باشد. در هر صورت چون این زمان به تاخیر انتشار پیام‌ها می‌افزاید، شاید لازم باشد بازه زمانی پخش بلاک در پروتکل اصلی به میزان کمی افزایش یابد.

۲. یک بازه زمانی جدید برای پخش شایعه معرفی منبع بلاک باید در انتهای هر دور اضافه شود. همانطور که گفته شد درصورتی که پخش شایعه منبع توسط هر گره انجام شود، در این بازه باید ۵۰ هزار پیام ۳۵۲ بایتی در شبکه پخش شود. براساس [۵] پیام‌های کوچکی که کمتر از یک کیلوبایت حجم دارند در کمتر از یک ثانیه در شبکه پخش می‌شوند ولی به دلیل تعداد زیاد پیام‌های ما عوامل دیگری نیز در این زمان دخیل خواهد بود. به طور مثال چون مجموع حجم همه این پیام‌ها در حدود ۱۸ مگابایت است همه لینک‌های شبکه باید سرعتی بیش از ۱۸ MB/s داشته باشند تا این حجم اطلاعات در یک ثانیه پخش شود، ولی احتمالا اینطور نیست و با پخش شدن این تعداد پیام در برخی لینک‌های شبکه ازدحام رخ خوهد داد که باعث افزایش نمایی تاخیر بسته‌ها و گم شدن تعدادی از آن‌ها می‌شود. یکی از عوامل دیگری که به صورت غیر مستقیم روی پخش این پیام‌های کوچک در شبکه تأثیر خواهد داشت زمان لازم برای پردازش هرکدام در هر گره است، هر گره قبل از پخش پیام باید آن را احراز هویت کند؛ پس در هر گره باید ۵۰ هزار پیام، تایید اصالت شوند. براساس [۳] تایید اصالت هر پیام در حدود ۲۷۳ هزار چرخه ساعت[1] است، در صورتی که از یک پردازنده معمولی با قدرت پردازش ۳ GHz استفاده کنیم، زمان لازم برای تایید اصالت ۵۰ هزار پیام مربوط به این مرحله در حدود ۴.۵ ثانیه خواهد بود. البته این زمان با استفاده از خط‌لوله[2] قابل کاهش است ولی برای استفاده از خط‌لوله برای این روند باید به همه یا حداقل تعدادی از پیام‌ها دسترسی داشته باشیم؛ پس استفاده از خط لوله برای این فرایند با پخش تک به تک پیام‌ها ممکن نخواهد بود.

با توجه به نکاتی که گفته شد تخمین زمان دقیق پخش ۵۰ هزار پیام ۳۵۲ بایتی در شبکه کار ساده‌ای نیست ولی مشخصا این کار سربار زیادی برای شبکه خواهد داشت. لازم به ذکر است درصورتی که از امضای پیکسل استفاده کنیم، این زمان تایید اصالت چندین برابر می‌شود، زیرا پیکسل در احراز اصالت پیام‌های تکی عملکرد ضعیف‌تری از BM-Ed25519 دارد.

اگر بخواهیم از پروتکل دوم یعنی پخش پیام‌ها به صورت تجمیع‌شده توسط نماینده هر بخش استفاده کنیم، علاوه بر بازه زمانی پخش پیام‌ها توسط نماینده، زمانی لازم است تا هر گره منبع خود را به نماینده خود اعلام کند. این مرحله بدون افزایش بار شبکه می‌تواند در بازه زمانی پخش بلاک انجام شود. اگر

[1] Clock Cycle
[2] Pipeline



شکل ۵ـ۱: زمان لازم برای پخش بلاک
زمان لازم برای پخش بلاک در ۹۰، ۷۵ و ۵۰ درصد شبکه[۵]

از این پروتکل استفاده کنیم در بازه زمانی پخش پیام‌های مشخص‌کننده منبع، هر گره، برای پخش پیام کافیست فقط امضای نماینده را بررسی و پیام را پخش کند. پس سربار زمانی روی انتشار پیام از سمت هر گره بسیار کمتر است و به این دلیل که تعدادی از پیام‌های مشخص‌کننده منبع را به صورت همزمان دریافت می‌کند با احراز اصالت این پیام‌ها به صورت یک‌جا زمان و انرژی کمتری برای احراز اصالت کل پیام‌ها خواهد گذاشت. براساس [۳] در صورتی که ۶۴ پیام به صورت همزمان احراز اصالت شوند ۸.۵ میلیون چرخه ساعت نیاز است، یعنی احراز اصالت هرکدام امضاها نصف حالت معمولی زمان خواهد برد. علاوه بر این چون لازم نیست قبل از پخش پیام‌ها کل پیام‌های داخل آن را احراز اصالت کنیم، می‌توانیم همه پیام‌ها را دریافت کنیم و به صورت همزمان همه را تایید کنیم. براساس [۳] می‌توانیم در هر ثانیه ۷۱ هزار امضا را همزمان احراز اصالت کنیم، پس تایید ۵۰ هزار پیام در کمتر از یک ثانیه انجام خواهد شد. بر اساس [۵] زمانی که لازم است تا ۹۰ درصد از گره‌های شبکه یک بسته ۱۰ کیلوبایتی را دریافت کنند ۴ ثانیه است و برای یک بسته ۲۰ کیلوبایتی این زمان به ۶ ثانیه می‌رسد؛ پس می‌توان انتظار داشت، یک بازه با مهلت اتمام ۱۰ ثانیه‌ای برای انتقال همه این پیام‌ها کافی خواهد بود.

درصورتی که از امضای پیکسل استفاده کنیم، هر نماینده می‌تواند مجموعه امضاهای دریافتی را تجمیع کند تا هرکس با دریافت آن تنها لازم باشد یک امضا را تایید کند. از آنجایی که هر گره باید به تعداد نماینده‌ها پیام تکی تایید کند، هرچقدر تعداد این پیام‌های تکی یا به عبارت دیگر تعداد نماینده‌ها کمتر باشد کارایی بیشتری خواهیم داشت. در این شرایط اگر در حدود ۱۰۰ نماینده داشته باشیم در کمتر از

نیم ثانیه کل امضاها تایید می‌شوند و حجم پیام هر نماینده در حدود ۳۲ کیلوبایت خواهد بود که بر اساس [۵] در کمتر از ۸ ثانیه در شبکه پخش خواهد شد.

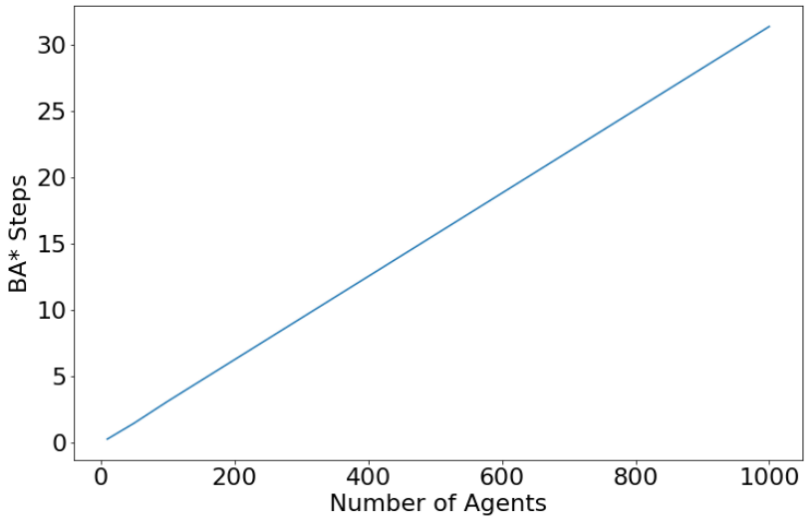
۳. زمانی که صرف ساخت و پیمایش گراف می‌شود. این زمان به الگوریتم مورد استفاده وابسته خواهد بود. در بازه زمانی‌ای که برای شایعه معرفی منبع در نظر گرفته شده است می‌توان با قرار دادن مبدا و مقصد هر پیام در ساختمان داده مناسب درخت تعاملات را همزمان با گرفتن و پخش پیام ساخت. درصورتی که بخواهیم فقط برگ‌های درخت را حذف کنیم لازم به صرف زمان اضافه‌تری نیستیم و فقط ساخته شدن درخت که در زمان پخش شایعه انجام شده، برای این منظور کافی خواهد بود. اگر از الگوریتم‌های انتخاب عمیق‌شونده و عمیق‌شونده بازگشتی استفاده کنیم، دو مرحله ۱ ـ پیمایش درخت و محاسبه امتیاز و ۲ ـ مرحله پیمایش درخت برای انتخاب گره‌های برگزیده، به انتهای هر دور افزوده می‌شود. ولی از آنجایی که هر دو مرحله دارای پیچیدگی زمانی خطی هستند در کسری از ثانیه کل عملیات مشخص شده قابل انجام است و سربار زمانی زیادی برای گره‌ها نخواهد داشت. (این قسمت به صورت دقیق‌تر در بخش پیچیدگی محاسباتی بررسی خواهد شد.)

۴. زمانی که باید پاداش به گره‌های برگزیده تخصیص یابد. به ازای هر چند بلاک باید پاداش محاسبه شده به صورت یک بلاک ساخته شود و همان فرآیندی که برای سایر بلاک‌های شبکه طی می‌شود برای توافق روی آن انجام شود، با این تفاوت که برای تایید آن باید درخت‌های ساخته شده پیمایش شود و پاداش هرکس بر این اساس محاسبه گردد.

۵ـ۳ سربار محاسباتی و حافظه

منظور از سربار محاسباتی مقدار محاسباتی است که هر گره باید انجام دهد. این سربار رابطه مستقیم با میزان مصرف برق دارد و یکی از هزینه‌های قابل توجه برای هر گره محسوب می‌شود. در این قسمت سربار محاسباتی اضافه شده را با سربار محاسباتی موجود برای *BA مقایسه می‌کنیم. سربار محاسباتی هر مرحله از *BA مربوط به احراز اصالت پیام‌های آن است و سربار کلی وابسته به تعداد مراحل آن خواهد بود.

همانطور که در قسمت قبل هم اشاره شد یکی از سربارهای محاسباتی اضافه شده احراز اصالت پیام‌هایی است که برای معرفی منبع ارسال می‌شوند در هر دو حالتی که در قسمت قبل توضیح داده شد درصورت استفاده از BM-Ed25519 باید به تعداد گره‌های شبکه، امضا تایید شود. البته همانطور که گفته شد درصورتی که از نماینده‌ها برای پخش این پیام‌ها استفاده کنیم می‌توانیم این پیام‌ها را در کنار هم همزمان با سربار محاسباتی خیلی کمتری تایید کنیم. در مقام مقایسه سربار محاسباتی اضافه شده بدون استفاده از نماینده‌ها تقریبا دو برابر



شکل ۵ـ۲: سربار محاسباتی استفاده از امضای پیکسل
سربار محاسباتی اضافه شده به هر گره در مقایسه با سربار موجود برای هر مرحله *BA

بدترین حالت *BA و با استفاده از نماینده‌ها نصف بدترین حالت *BA خواهد بود.

اگر از امضای پیکسل استفاده کنیم، تعداد نماینده‌ها تأثیر مستقیمی در سربار محاسباتی خواهد داشت. هر چقدر تعداد این نماینده‌ها بیشتر باشد سربار برای هر گره کمتر خواهد بود. در تصویر ۵ـ۲ می‌توانید سربار اضافه شده بر شبکه را در حضور تعداد نماینده‌های مختلف مشاهده کنید. این نمودار رابطه خطی تعداد نماینده‌ها و سربار محاسباتی را نشان می‌دهد که در مقایسه با مراحل *BA رسم شده است. همانطور که در نمودار هم مشاهده می‌کنید، درصورتی که تعداد نماینده‌ها ۴۰۰ عدد باشد سربار محاسباتی برابر بدترین حالت *BA خواهد بود و در صورتی که ۱۰۰ نماینده برای شبکه انتخاب کنیم سربار برابر بهترین حالت *BA خواهد بود. از آنجایی که تعداد نماینده‌ها روی حجم پیام‌ها نیز تأثیر می‌گذارد متعادل کردن این سربار با سربار زمانی پخش پیام باید مورد بررسی دقیق‌تر قرار بگیرد. در بخش ۵ـ۴ به بررسی بیشتر این مورد خواهیم پرداخت.

به غیر از پیام‌هایی که باید تایید شوند برای ساخت، پیمایش و ذخیره درخت نیاز به محاسبات و حافظه بیشتری داریم. این محاسبات و حافظه به الگوریتم انتخاب وابسته است پس دو حالت را به صورت جداگانه بررسی می‌کنیم:

- حذف برگ‌های درخت: در صورتی که فقط بخواهیم به برگ‌های درخت مورد نظر پاداشی اختصاص ندهیم، کافیست در هنگام دریافت پیام‌های معرفی منبع لیستی از گره‌هایی که نام آن‌ها به عنوان منبع ذکر شده است ذخیره کنیم و در نهایت به آن‌ها پاداش دهیم. پس نیازی به پردازش یا حافظه اضافه‌تر نخواهد بود.

- الگوریتم عمیق‌شونده بازگشتی: برای استفاده از این الگوریتم باید درخت را بسازیم و دوبار روی آن پیمایش انجام دهیم. ساخت درخت در زمان دریافت پیام‌های معرفی منبع قابل انجام است و کافیست که در یک ساختمان داده مناسب ذخیره شوند. شبه‌کد ۱ این عملیات را نشان می‌دهد.

Algorithm 1: Construct The Contribution Tree

```
Result: The Contribution Tree
Tree = [[] for each node];
while New message do
    message = Receive();
    Tree[message.SourceNode].append(message.DestinationNode);
end
```

پس از ساخته شدن درخت باید طبق معیار معرفی شده به گره‌ها امتیاز دهیم، از آنجایی که گراف تعاملات یک درخت است لازم نیست نگران مشترکات شاخه‌های زیرین گره باشیم و برای محاسبه امتیاز تنها کافیست مجموع امتیاز بچه‌های مستقیم گره به علاوه سهام خودشان را محاسبه کنیم. شبه کد ۲ این عملیات را نشان می‌دهد.

Algorithm 2: Compute Node Scores

```
Result: Node Scores
Score = [0 for each node];
ComputeScores(Root)
Function ComputeScores(Tree, CurrantNode) is
    for node in Tree[CurrantNode] do
        if node is not visited then
            ComputeScores(node);
        end
        score[CurrantNode] += score[node] + stake[node];
    end
end
```

از آنجایی که از الگوریتم پیمایش اول عمق روی درخت استفاده کردیم پیچیدگی محاسباتی شبه‌کد ۲ خطی است. حافظه مورد استفاده نیز برحسب تعداد کل گره‌ها خطی است.

در نهایت با داشتن امتیازهای هر گره باید با پیمایش روی درخت گره‌های نهایی را انتخاب کنیم. در پیمایش نهایی درخت برای انتخاب گره‌های مورد نظر باید مسیر طی شده ذخیره شود و اینکه بررسی شدن هر گره نیز باید ذخیره شود. در شبه کد ۳ مراحل این الگوریتم را می‌توانید مشاهده کنید.

پس در مجموع این الگوریتم پیچیدگی محاسباتی و حافظه‌ای خطی خواهد داشت که سربار قابل توجهی برای هر گره در بر ندارد.

در مقایسه این دو الگوریتم می‌توانیم بگوییم که مشخصا فقط حذف برگ‌های درخت تعاملات پیاده‌سازی

Algorithm 3: Select Nodes for block reward

```
Result: Selected Node
SelectedNodes = [];
Stack.push(Root);
CurrantNode = Root;
while len(SelectedNodes) < MaxNodes and stack is not empty do
    if All nodes in Tree[CurrantNode] is visited then
        stack.pop();
        currantNode = Stack.top();
    end
    for node in Sorted(Tree[CurrantNode]) do
        if node is not visited then
            SelectedNodes.append(node);
            stack.push(node);
            CurrantNode = node;
        end
    end
end
```

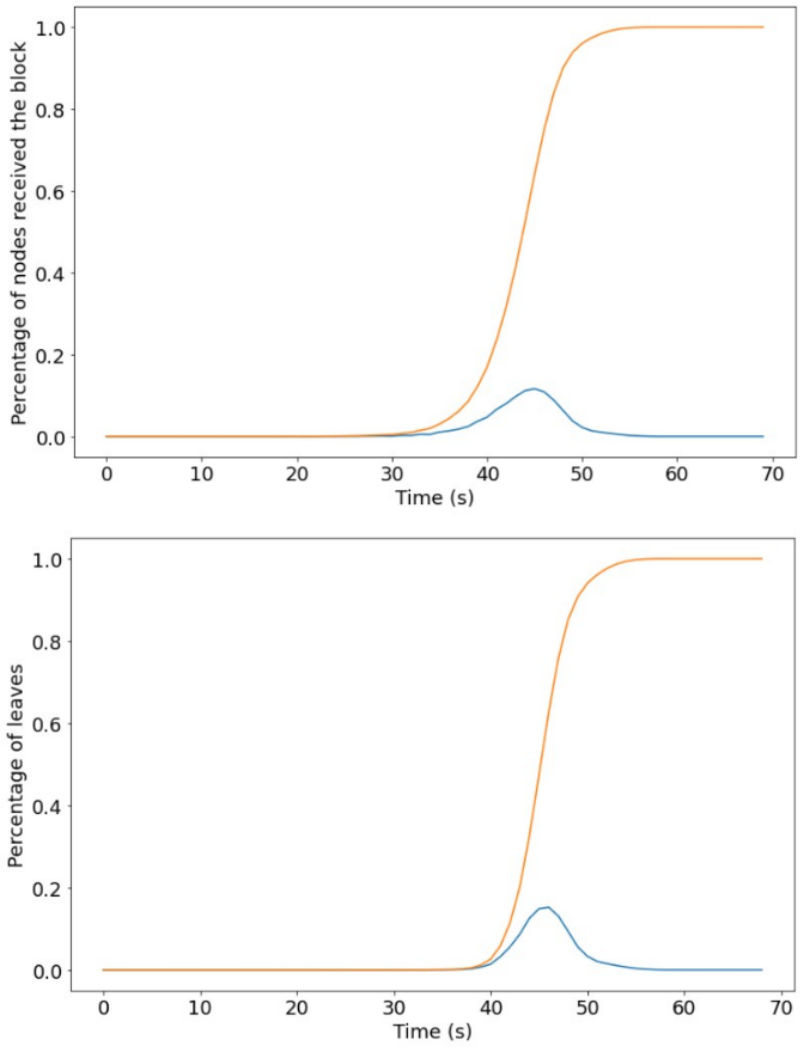
بسیار ساده‌تر و پیچیدگی محاسباتی کمتری دارد ولی تعداد لیست نهایی انتخاب شده متغیر و خارج از کنترل ما خواهد بود. با استفاده از الگوریتم عمیق‌شونده بازگشتی می‌توانیم تعداد یا مجموع سهام لیست نهایی را کنترل کنیم و سربار محاسباتی کمی به کل شبکه افزوده می‌شود.

در کل بعد از اجرای الگوریتم معرفی شده تنها کافیست که لیستی از گره‌های منتخب این دور ذخیره شود و حافظه ثابت زیادی لازم نیست و حافظه‌ای که در جریان ساخت و پیمایش درخت استفاده می‌شود در حد چند مگابایت خواهد بود که بعد از پایان عملیات آزاد می‌شود. در عین حال کل عملیات توصیف شده در هر دو در کسری از ثانیه انجام می‌شود و به دلیل خطی بودن پیچیدگی محاسباتی سربار زیادی برای گره‌ها به حساب نمی‌آید. سربار محاسباتی اصلی اضافه شده به پروتکل همان احراز اصالت کلیه پیام‌هاست که مستقل از الگوریتم انتخاب است.

۴ـ۵ بررسی تنظیمات

در این بخش قصد داریم تأثیرات کلی استفاده از تنظیمات مختلف را روی شبکه بررسی کنیم. یکی از مهم‌ترین مواردی که در این بخش باید مورد بررسی قرار گیرد، تعداد نماینده‌های تجمیع پیام در شبکه است. همانطور که در بخش‌های قبل مشاهده شد کم کردن تعداد این نماینده‌ها می‌تواند در برخی موارد سربار را کاهش داده و در برخی موارد باعث افزوده شدن بر سربار موجود خواهد شد.

درصورتی که نماینده‌ها را مستقل از پخش بلاک انتخاب کنیم، می‌توانیم تعداد آن‌ها را مستقیما تنظیم کنیم ولی درصورتی که نماینده‌ها وابسته به درخت تعاملات انتخاب کنیم، فقط می‌توانیم متغیرهایی که بر روی تعداد

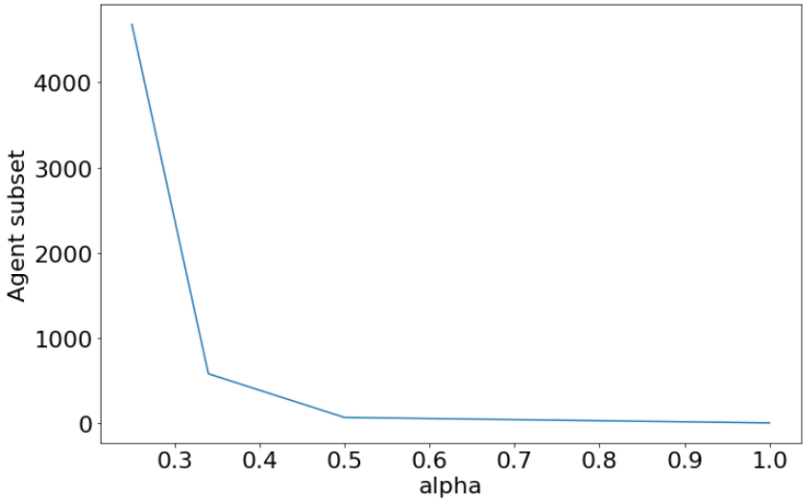


شکل ۵ـ۳: پخش بلاک در شبکه براساس زمان و تعداد برگ‌های درخت تعاملات در همان بازه

نماینده‌ها تأثیر دارند را تنظیم کنیم. پس در مرحله اول تنظیم متغیرهای موثر بر تعداد نماینده‌ها را بررسی می‌کنیم و در مرحله دوم تأثیر تعداد نماینده‌ها بر کارایی پروتکل را تحلیل خواهیم کرد.

۵ـ۴ـ۱ تنظیم متغیرها

در بخش ۴ـ۵ـ۱ متغیری به نام α معرفی شد تا مشکل تصادفی بودن پخش نماینده‌ها را حل کند. این متغیر مستقیما بر تعداد نماینده‌هایی که انتخاب می‌شوند تأثیر خواهد داشت. البته لازم به ذکر است که برای کارکرد درست الگوریتم علاوه بر متغیر α انتخاب نماینده‌ها باید وابسته به زمان نیز باشد. درصورتی که انتخاب نماینده‌ها وابسته به زمان نباشد، نماینده‌هایی که در زمان‌های پایانی پخش بلاک انتخاب می‌شوند تعداد زیر مجموعه بسیار اندکی خواهند داشت و این موضوع باعث می‌شود تعداد زیادی گره به عنوان نماینده انتخاب شوند که کارایی را در بسیاری از موارد کاهش می‌دهد. اگر چه پخش بلاک در نقاط مختلف شبکه، مشابه هم دیگر نیست، می‌دانیم

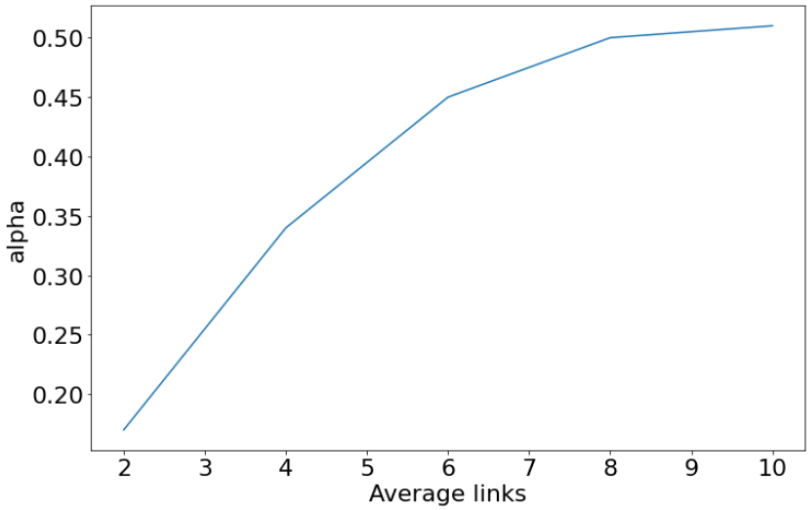


شکل ۵ـ۴: تأثیر α
تأثیر α بر روی تعداد زیر مجموعه نماینده‌ها در شبکه‌ای با میانگین تعداد لینک ۸.

که پخش بلاک به دو زمان کلی تقسیم می‌شود که در بازه زمانی اول بیشتر شبکه خواستار دریافت بلاک هستند و در بازه دوم اکثر گره‌ها بلاک را دریافت کرده‌اند و می‌خواهند آن را برای سایر گره‌ها ارسال کنند. براساس شبیه‌سازی‌های انجام شده در صورتی که انتخاب نماینده‌ها را در نقطه‌ای از زمان که ۴۰ درصد گره‌های شبکه بلاک را دریافت کرده‌اند متوقف کنیم، نتیجه مطلوبی از نظر تعداد نماینده‌ها و تعداد اعضای زیر مجموعه‌ی آن‌ها خواهیم گرفت. همانطور که در تصویر ۵ـ۳ مشاهده می کنید تا قبل از زمان ۴۲ ثانیه(زمانی که ۴۰ درصد از شبکه بلاک را دریافت کرده‌اند)، تعداد برگ‌های درخت تعاملات بسیار کم است، منظور از برگ در این نمودار گره‌هایی است که در نهایت در پخش بلاک موثر نبوده‌اند و بلاک را برای هیچکس ارسال نکرده‌اند، پس تا قبل از این زمان به دلیل اینکه هنوز تعداد زیادی از گره‌های شبکه خواستار دریافت بلاک هستند، هر گره حداقل بلاک را برای یک نفر ارسال کرده است.

پس براساس این توضیحات می‌توانیم انتخاب گره‌های نماینده را در این زمان متوقف کنیم. زیرا از این زمان به بعد اکثر گره‌ها بلاک را برای کسی ارسال نمی‌کنند یا این تعداد بسیار کم خواهد بود که می‌تواند با نماینده‌های سطح بالاتر که قبلا انتخاب شده‌اند کنترل شود. زمان توقف وابسته به اندازه بلاک است، زیرا براساس اندازه بلاک زمان پخش این بلاک در شبکه مشخص می‌شود. از آنجایی که زمان پخش بلاک بر اساس اندازه آن یک رابطه خطی دارد، هر گره با داشتن اندازه بلاک و زمان شروع پخش توسط گره پیشنهاددهنده می‌تواند این زمان را محاسبه کند.

محدود کردن انتخاب نماینده‌ها با زمان فقط جلوی انتخاب بیش از حد این نماینده‌ها را می‌گیرد و متغیر اصلی که تعداد نماینده‌ها و تعداد زیر مجموعه آن‌ها را مشخص می‌کند، متغیر α است. براساس اینکه می‌خواهیم



شکل ۵ـ۵: تنظیم α

تنظیم α برای ثابت نگه‌داشتن تعداد اعضای زیرمجموعه هر نماینده بر اساس میانگین تعداد لینک گره‌ها

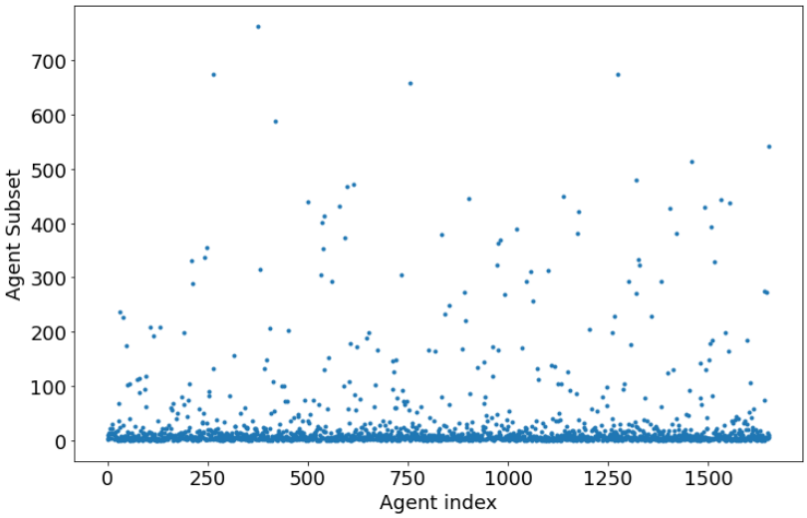
زیرمجموعه هر نماینده در شبکه چند گره باشد و به صورت میانگین هر گره به چند گره دیگر در شبکه متصل است باید متغیر α را تنظیم کنیم. در تصویر ۵ـ۴ تأثیر متغیر α بر تعداد اعضای زیرمجموعه هر نماینده در شبکه‌ای که به صورت میانگین هر گره ۸ لینک دارد را می‌توانید مشاهده کنید. به همین صورت در تصویر ۵ـ۵ با ثابت کردن تعداد اعضای زیرمجموعه روی ۱۰۰، تنظیم α را براساس تعداد لینک‌های گره‌ها بررسی کردیم.

۵ـ۴ـ۲ تعداد نماینده‌ها

اگر نماینده‌ها را وابسته به درخت انتخاب کنیم، با اینکه می‌توانیم با تغییر دادن متغیر α تعداد نماینده‌ها را تنظیم کنیم ولی با شروع پخش از مکان‌های مختلف در شبکه این تعداد متغیر خواهد بود و همینطور در کمتر کردن تعداد این نماینده‌ها محدودیت‌هایی وجود خواهد داشت. به طور مثال می‌توانید در تصویر ۵ـ۶ تعداد اعضای زیر مجموعه ۱۶۰۰ نماینده انتخابی را مشاهده کنید. کاملا مشخص است که پخش گره‌ها بین نماینده‌ها به صورت یکنواخت انجام نشده است و افزایش محدودیت زمانی نیز راه حلی برای این مشکل نیست زیرا باعث افزایش تعداد نماینده‌هایی می‌شود که زیرمجموعه کمی دارند.

همانطور که در بخش‌های قبل بررسی شد، در صورتی که از امضای پیکسل در پروتکل استفاده کنیم، تعداد نماینده‌ها در سربار نهایی تأثیر زیادی خواهد داشت. پس استفاده از نماینده‌های وابسته به پخش بلاک در کنار این امضا منطقی به نظر نمی‌رسد؛ زیرا کم کردن تعداد این نماینده‌ها به اندازه‌ای که برای امضای پیکسل کافی باشد تقریبا غیرممکن است.

پس در صورت استفاده از پیکسل، نماینده‌ها را به صورت مستقل انتخاب می‌کنیم. با اینکه برای انتخاب



شکل ۵ـ۶: تعداد اعضای زیر مجموعه نماینده‌ها
تعداد اعضای زیر مجموعه نماینده‌ها با $\alpha = 0.5$ و محدودیت زمانی ۴۰ ثانیه در یک شبکه با میانگین لینک ۸

نماینده‌ها به صورت مستقل به سربار شبکه کمی افزوده می‌شود، پیکسل آنقدر حجم پیام‌ها را کاهش می‌دهد که در کل سربار شبکه همچنان بسیار بهتر از استفاده BM-Ed25519 خواهد بود. همانطور که در بخش قبل دیدیم، هرچقدر تعداد نماینده‌ها کمتر باشد سربار محاسباتی برای هر گره کمتر خواهد بود با این حال کم کردن این تعداد باعث افزایش حجم پیام‌های هر نماینده می‌شود، در نتیجه باید بازه زمانی پخش این پیام بزرگتر در نظر گرفته شود.

درصورتی که تعداد نماینده‌ها در شبکه ۱۰۰ عدد باشد، پیام هرکدام از نماینده‌ها ۳۲ کیلوبایت خواهد بود که براساس [۵] در زمان ۸ ثانیه در ۹۰ درصد شبکه پخش می‌شود و سربار محاسباتی اضافه شده به هر گره برابر بهترین حالت *BA است. با تنظیم کردن تعداد نماینده‌ها روی ۱۰۰ عدد، سربار افزوده شده از هر دو سمت منطقی است و سربار خیلی زیادی به شبکه افزوده نمی‌شود. البته لازم به ذکر است با افزایش روز به روز سرعت لینک‌ها زمان پخش کاهش خواهد یافت و در شبیه‌سازی انجام شده که سرعت لینک‌ها به روز تر است، انتخاب ۵۰ نماینده برای این شبکه نیز بازه زمانی کمی برای پخش نیاز داشت و با انتخاب این تعداد نماینده سربار محاسباتی نیز نصف بهترین حالت *BA است.

اگر از امضای BM-Ed25519 در پروتکل استفاده کنیم، تعداد نماینده‌ها تأثیر مستقیمی در سربار محاسباتی نخواهد داشت(اگر حداکثر ۱۰ درصد از کل گره‌ها به عنوان نماینده انتخاب شوند). ولی درصورتی که گره‌های شبکه به صورت یکنواخت بین نماینده‌ها تقسیم شوند کارایی پروتکل بهتر خواهد بود؛ زیرا زمانی که برای بازه پخش پیام‌های معرفی منبع باید در نظر گرفته شود به اندازه پخش کامل بزرگترین پیام خواهد بود.

۵-۵ بررسی حملات مهاجمان

یکی از حملات بسیار مهم که در فصل قبل هم به آن اشاره کردیم حمله منع سرویس به نماینده‌های تجمیع پیام است. این نماینده‌ها بر حسب نقش خود باید در شبکه شناخته شده باشند و در زمان پخش بلاک پیام‌های گره‌های زیرمجموعه خود را جمع‌آوری کنند. به همین دلیل این گره‌ها بسیار آسیب‌پذیر خواهند بود و درصورت حمله منع سرویس به آن‌ها قسمتی از شبکه که زیرمجموعه آن‌هاست از گرفتن پاداش محروم خواهد ماند. همانطور که در بخش قبل توضیح دادیم درصورتی که نماینده‌ها مستقل از پخش بلاک انتخاب شوند خطر این حمله هم افزایش خواهد یافت و هر چقدر تعداد نماینده‌ها کمتر باشد تعداد اعضای زیرمجموعه آن‌ها بیشتر خواهد بود و به این حمله حساس‌تر خواهند شد.

علاوه بر نماینده‌ها که نقطه‌های حساس این پروتکل هستند، درصورتی که دقیق‌تر به مراحل ساخت درخت و امتیازدهی توجه کنیم متوجه می‌شویم هر کدام از اتصالات درخت، درست در شبکه پخش نشود، کل زیر مجموعه آن قسمت از گرفتن پاداش محروم خواهند ماند. به عبارت دیگر درصورتی که تصادفا یکی از پیام‌های معرفی منبع در شبکه گم شود یا به صورت صحیح به گره‌های شبکه نرسد، یکی از شاخه‌های درخت تعاملات که توسط این گره به درخت متصل بوده است از درخت جدا می‌شود و در جریان پیمایش و امتیازدهی در نظر گرفته نخواهد شد.

براساس همین مشکل در صورتی که مهاجم بخواهد کل گره‌ها را از گرفتن پاداش محروم کند، می‌تواند به گره‌هایی که در درخت تعاملات در ارتفاع کمتری قرار دارند حمله کند. منظور از گره‌هایی که در ارتفاع کمتر قرار دارند یعنی گره‌هایی که زودتر از بقیه گره‌ها بلاک را دریافت کرده‌اند و گره‌های زیادی زیر شاخه آن‌ها در درخت تعاملات هستند.

این حمله می‌تواند به این صورت باشد که تعدادی از گره‌های سطح پایین درخت در زمان کوتاهی اتصال خود را از دست بدهند و نتوانند پیام معرفی منبع خود را پخش کنند. یا به نماینده‌ی تجمیع این گره‌های با ارتفاع کم حمله شود. به طور مثال از دسترس خارج کردن گره پیشنهاددهنده بلاک در زمان پخش پیام‌های معرفی منبع بلاک می‌تواند کل عملیات مورد نظر را نابود کند. زیرا درمورد ریشه درخت که پیمایش باید از آنجا آغاز شود اطلاعاتی در دسترس نخواهد بود و نمی‌توان به هیچ گره‌ای پاداش داد.

براساس این توضیحات حمله منع سرویس نقطه ضعف بزرگی برای این راه‌حل محسوب می‌شود و می‌تواند علاوه بر حل نکردن مشکل پاداش دادن، فعالیت کل شبکه را مختل کند.

فصل ششم

شبکه بازپخش، ارائه راه حل

در این بخش راه حلی برای مشکلات ایجاد شده در صورت استفاده الگورند از شبکه بازپخش معرفی می‌کنیم. در بخش ۳ مسئله موجود برای این نوع شبکه توضیح داده شد پس در ابتدا باید هزینه گره‌های رله در این شبکه را بررسی کرده و براساس هزینه‌های آن‌ها در قبال خدمات ارائه شده به گره‌های عادی پاداش تخصیص دهیم.

۶ـ۱ هزینه

هزینه‌های موجود برای یک گره رله شامل موارد زیر است:

۱. بررسی تراکنش‌ها و اعتبارسنجی بلاک

۲. اعتبار سنجی پیام‌های پروتکل

۳. پخش بلاک و پیام‌های شایعه به زیرمجموعه گره‌های عادی و سایر گره‌های رله

دو مورد اول از هزینه‌های بالا، هزینه‌های ثابتی است که هر گره رله باید آن را پرداخت کند؛ زیرا حتی اگر فقط یک گره معمولی به عنوان سرویس‌گیرنده به این گره متکی باشد، همه اعتبارسنجی‌ها باید به درستی انجام شود و با انجام این دو کار توسط گره‌های رله بار آن‌ها از دوش سایر گره‌ها برداشته می‌شود. گرچه هزینه سوم

که ارائه خدمات به گره‌های سرویس‌گیرنده است بر اساس تعداد این گره‌ها متفاوت خواهد بود.

از آنجایی که گره‌های رله سهامی ندارند، از توافق بلاک پاداشی دریافت نخواهند کرد ولی برای اینکه هزینه‌های اعمالی روی این گره‌ها پرداخت شود باید به این گره‌ها نیز پاداش تخصیص داده شود. برای اختصاص پاداش به هرکدام از این گره‌های رله باید بدانیم به چند گره عادی سرویس می‌دهد، چون هزینه‌های متغیر این گره‌ها به تعداد گره‌های سرویس‌گیرنده مرتبط می‌شود. پس برای پاداش دادن به این گره‌ها نیاز است معیاری برای اندازه‌گیری خدمات ارائه شده معرفی کنیم.

۲ـ۶ معیار اندازه‌گیری خدمات

قطعا تعداد گره‌های سرویس‌گیرنده معیار خوبی برای هزینه‌های موجود برای گره رله مورد نظر است، ولی در صورتی که فقط متصل بودن به این گره رله مد نظر قرار گیرد و کیفیت و سرعت خدمات نادیده گرفته شود، مشکلات بزرگی در شبکه به وجود خواهد آمد.

هر گره معمولی به صورت میانگین به c گره رله در شبکه متصل می‌شود تا سرعت پخش اطلاعات در شبکه افزایش یابد و درصورت بروز مشکل برای یکی از رله‌ها، گره‌های معمولی متصل به آن از شبکه حذف نشوند. پس با این وجود، اینکه یک گره معمولی دقیقا از کدام‌یک از این گره‌های رله سرویس دریافت می‌کند به صورت دقیق مشخص نیست.

مانند سناریو قبل می‌توانیم معیار اندازه‌گیری مشارکت در پروتکل را بر اساس پخش بلاک محاسبه کنیم، چون پخش بلاک پرهزینه‌ترین ارتباط برای گره‌های رله خواهد بود و مقدار پهنای باند مورد استفاده می‌تواند مستقیما به تعداد پخش بلاک مرتبط باشد.

برای اینکه در یک شبکه غیر متمرکز بتوانیم پاداش گره‌های رله را بر این مبنا محاسبه کنیم باید هر گره رله اثبات کند که بلاک را برای تعداد مشخصی گره معمولی ارسال کرده است. پس هر گره معمولی پس از دریافت بلاک از یک گره رله یک پیام امضا شده براساس سرتیتر بلاک و شناسه رله مورد نظر برای او ارسال می‌کند؛ این پیام نشان‌دهنده دریافت سرویس از این رله خواهد بود و مشخص است که هر رله‌ای که سریعتر بلاک را برای گره‌های سرویس‌گیرنده خود پخش کند پیام‌های امضا شده بیشتری جمع‌آوری خواهد کرد. در ادامه این پیام‌ها را با نام پیام‌های اثبات خدمات خواهیم شناخت.

معیار نهایی که براساس آن باید به گره‌های رله پاداش تخصیص داد، مجموع سهام گره‌هایی است که از او خدمات دریافت کرده‌اند و به او پیام تایید خدمات داده‌اند خواهد بود. درصورتی که فقط تعداد پیام‌ها به عنوان معیار در نظر گرفته شود، ممکن است مهاجمی با ساخت تعداد زیادی گره که سهام کمی دارند، باعث شود به

رله مورد نظرش پاداش بیشتری برسد.

پس از پایان پخش بلاک یک بازه زمانی جدید برای محاسبه پاداش رله‌ها در نظر گرفته می‌شود. در این بازه پیام‌های امضا شده اثبات خدمات در کل شبکه پخش می‌شود و پس از پخش این پیام‌ها، همه گره‌های معمولی می‌توانند میزان پاداش هر گره رله را بر اساس سهام فرستنده پیام‌های اثبات خدمات محاسبه کنند.

۳ـ۶ پخش پیام

در صورتی که شبکه روی یک بلاک توافق کرد، گره‌های رله در بازه‌ای که درنظر گرفته شده باید برای پخش پیام‌های اثبات خدمات اقدام کنند. هر کدام از گره‌های رله باید پیام‌های خود را تجمیع کرده و در این بازه در شبکه پخش کند، همینطور می‌توان برای کمتر کردن سربار به جای اینکه بعد از هربار توافق بلاک یک بازه زمانی در نظر گرفته شود، به ازای هر چند دور یک بازه برای پخش پیام‌ها در نظر گرفته شود و در همان بازه زمانی اضافه شده پاداش این چند دور گره‌های رله به صورت یک بلاک جدید در شبکه توافق گردد.

فصل هفتم

شبکه بازپخش، تحلیل راه حل

در این بخش هزینه‌ها و سربار اضافه شده به پروتکل را با اضافه کردن مکانیزم اندازه‌گیری خدمات گره‌های رله بررسی می‌کنیم و مزایا و معایب این روش را تحلیل می‌کنیم. همانطور که در بخش ۳ به آن اشاره کردیم ساختار شبکه در حضور این گره‌های رله به صورت دقیق مشخص نشده است پس در ابتدا بر اساس دانسته‌های موجود ساختار و تعداد این گره‌ها را برای یک شبکه بزرگ با ۵۰ هزار گره معمولی تخمین می‌زنیم و سپس بر اساس این فرضیات به تحلیل سربار و هزینه‌ها می‌پردازیم.

۷ـ۱ تحلیل شبکه

می‌دانیم که گره‌های معمولی فقط اجازه دارند که به گره‌های رله متصل شوند و برای اینکه اتصالات شبکه قابل اعتماد باشد باید به صورت میانگین به c گره رله در شبکه متصل شوند. با توجه به پهنای باند بالای گره‌های رله خود آن‌ها باید به صورت یک شبکه زیرساخت برای جابه‌جایی اطلاعات بین خودشان به هم متصل باشند، اطلاعات در این شبکه زیرساخت به دلیل پهنای باند بالای لینک‌ها به سرعت پخش می‌شود. پس در این شبکه گره‌های معمولی وظیفه پخش پیام‌ها و بلاک را ندارند[۲].

در شبکه رله، گره‌های معمولی که سرویس‌گیرنده از گره‌های رله هستند، هزینه‌ای برای احراز اصالت پیام‌ها

نمی‌پردازند و این احراز اصالت تنها یک بار توسط گره رله برای همه اعضای زیرمجموعه او انجام می‌شود. پس در کل هزینه احراز اصالت پیام‌ها در شبکه کاهش می‌یابد. هم‌چنین گره‌های معمولی وظیفه‌ای برای پخش اطلاعات ندارند و ترافیک آن‌ها فقط برای دریافت اطلاعات استفاده می‌شود، در عوض ترافیکی که قبلا توسط هر گره برای پخش اطلاعات استفاده می‌شد، مجموعا توسط گره رله برای این کار مصرف خواهد شد.

پس می‌توانیم نتیجه بگیریم هزینه کل این شبکه نسبت به هزینه شبکه نظیر به نظیر کاهش یافته است؛ می‌توان انتظار داشت با اختصاص دادن بخشی از پاداش هر گره در شبکه نظیر به نظیر به گره رله سرویس‌دهنده او، بدون هزینه اضافی شبکه‌ای سریع‌تر و امن‌تر داشته باشیم.

گره‌های رله به جز پهنای باند بالاتر و ترافیک اینترنت بیشتر به ملزومات خاصی نیاز ندارند، زیرا گره‌های معمولی هم در شرایط فعلی توانایی احراز اصالت بلاک و همه پیام‌ها را دارند و کاری که یک گره رله باید انجام دهد چیزی بیش از این نیست، البته درصورتی که سخت‌افزارهای خاص برای رمزنگاری داشته باشد می‌تواند سریع‌تر از بقیه رله‌ها سرویس بدهد و در نتیجه‌ی آن پاداش بیشتری دریافت کند. درصورتی که به یکی از این گره‌ها حمله منع سرویس صورت گیرد تنها کسی که ضرر می‌کند خود اوست؛ زیرا همانطور که گفته شد هر گره به چند گره رله متصل است و برای آسیب زدن به شبکه باید به تعداد زیادی از این رله‌ها حمله صورت گیرد. البته از آنجایی که این گره‌ها باید به دلیل ملزومات پهنای باند، در نقاط خاصی (به طور مثال نقاط تبادل اینترنت[1]) حضور داشته باشند، پس احتمالا ملزومات برای جلوگیری حملاتی مثل منع سرویس را دارا می‌باشند.

براساس [۶] هر گره معمولی به صورت میانگین به ۴ گره رله در شبکه متصل می‌شود و براساس محدودیت‌های حال حاضر پهنای باند برای یک سرور معمولی می‌توانیم فرض کنیم که هر رله می‌تواند به حدود ۴۰۰ گره معمولی سرویس دهد. پس بر اساس این مقادیر برای یک شبکه با ۵۰ هزار گره معمولی حداقل در حدود ۵۰۰ رله نیاز داریم.

۲ـ۷ سربار ترافیک شبکه

مشابه سناریو قبل در شبکه نظیر به نظیر در این قسمت نیز براساس امضای مورد استفاده سربار برای شبکه متفاوت خواهد بود. پس هر کدام جداگانه بررسی خواهد شد.

پیام اثبات خدماتی که توسط هر گره باید برای رله مورد نظرش ارسال شود، شامل موارد زیر است:

- شناسه گره ۳۲ بایت
- شناسه گره رله ۳۲ بایت

[1] Internet Exchange Points(IXP)

- سرتیتر بلاک ۳۲ بایت
- امضا برای احراز هویت پیام ۲۵۶ بایت (پیکسل ۱۴۴ بایت)

درصورت استفاده از امضای BM-Ed25519 حجم هر پیام ۳۵۲ بایت خواهد بود(پیکسل ۲۴۰ بایت). گره رله با دریافت این پیام‌ها بعد از ارسال بلاک به گره‌های مورد نظر، آن‌ها را تجمیع کرده و در بازه زمانی در نظر گرفته شده در شبکه پخش می‌کند. پیام تجمیع شده شامل موارد زیر است:

- شناسه گره رله ۳۲ بایت
- سرتیتر بلاک ۳۲ بایت
- شناسه دور و راند ۸ بایت
- پیام‌های اثبات خدمات بدون سرتیتر بلاک و شناسه رله هر کدام ۲۹۸ بایت (پیکسل ۳۲ بایت)
- امضا برای احراز هویت پیام ۲۵۶ بایت(پیکسل ۱۴۴ بایت)

پس در کل بیشینه حجم پیام تجمیع‌شده هر کدام از این گره‌های رله، ۱۲۰ کیلوبایت است و با توجه به اینکه تعداد کل گره‌های عادی در شبکه را ۵۰ هزار تا فرض کردیم، مجموع پیام‌های همه گره‌های رله در حدود ۱۵ مگابایت می‌شود.

در مقابل درصورتی که از امضای پیکسل استفاده کنیم، پیام تحمیع شده هر کدام از رله‌ها در حدود ۱۲ کیلوبایت و مجموع همه این پیام‌ها در حدود ۱.۷ مگابایت خواهد بود.(یعنی کمتر از $\frac{1}{8}$ مجموع پیام‌های BM-Ed25519)

۳ـ۷ تجمیع پیام‌های اثبات خدمات

همانطور که در فصل قبل اشاره کردیم، می‌توانیم بازه زمانی برای پخش پیام‌های اثبات خدمات که در انتهای هر دور اضافه شده بود را برای چند دور متوالی تجمیع کنیم. این کار مستلزم این است که پیام‌های هر دور را تجمیع کنیم پس احتمالا در نهایت بازه زمانی بزرگتری برای پخش تمام این پیام‌های تجمیع شده در نظر بگیریم.

درصورتی که از امضای BM-Ed25519 استفاده کنیم تجمیع این پیام‌ها حجم آن‌ها را مقدار قابل توجهی تغییر نمی‌دهد، زیرا بیشتر حجم این پیام‌ها مربوط به امضای هر پیام است که غیر قابل حذف است. پس به طور مثال اگر پیام‌های ۱۰۰ دور را روی هم جمع کنیم، بیشینه حجم پیام هر کدام از گره‌ها ۱۲ مگابایت و مجموع

شکل ۷ـ۱: ساختمان داده برای ذخیره پیام‌های تجمیع شده چند دور

کل پیام‌ها در حدود ۱.۴ گیگابایت خواهد شد. زمانی که لازم است تا این مقدار داده در کل شبکه پخش شود بسیار زیاد خواهد بود.

اگر از امضای پیکسل برای این پیام‌ها استفاده کنیم با تجمیع پیام‌ها می‌توانیم حجم قابل توجهی که مربوط به امضای این پیام‌هاست را کمتر کنیم. مثلا اگر پیام‌های ۱۰۰ دور روی هم جمع شوند، حجم پیام هر کدام از رله‌ها ماکسیمم ۶۴۰ کیلوبایت و مجموع کل پیام‌ها ۱۶۰ مگابایت می‌شود.(در حدود $\frac{1}{9}$ مجموع پیام‌های (BM-Ed25519

با این حال این حجم هم مقدار قابل توجهی برای گره‌های رله است؛ زیرا باید این مقدار داده را برای تعداد زیادی گره ارسال کنند و ترافیک زیادی در این مرحله مصرف خواهند کرد. داده‌ای که بیشتر حجم این پیام‌ها را تشکیل می‌دهد شناسه گره‌هایی است که به آن‌ها سرویس داده‌اند، از آنجایی که اتصالات شبکه خیلی سریع تغییر نمی‌کند پس تعداد زیادی از این داده‌ها تکراری است؛ زیرا شناسه گره‌هایی است که به عنوان سرویس‌گیرنده به رله مورد نظر متصل هستند. البته در هر مرحله ممکن است تعدادی از این شناسه‌ها در لیست باشند و در برخی مراحل چون بلاک را از رله‌های دیگر دریافت نکرده‌اند در لیست رله مورد نظر قرار نگیرند.

برای کاهش سربار ترافیک شبکه می‌توانیم به صورتی پیام‌ها را ذخیره کنیم که این داده‌های تکراری حجم اضافی اشغال نکنند. در واقع لازم نیست پیام‌ها را همانطور که هست برای همه ارسال کنیم، می‌توانیم نحوه ذخیره‌سازی آن‌ها را تغییر داده و با تجزیه کردن داده‌ها در مقصد آن‌ها را به حالت قبلی برگردانیم. به طور مثال می‌توانیم از ساختمان داده‌ای که در تصویر ۷ـ۱ توصیف شده است، برای ذخیره سازی این پیام‌ها استفاده کنیم.

اگر از این ساختمان داده برای ذخیره‌سازی داده‌های چند دور استفاده کنیم، فقط یکبار هر شناسه را ذخیره کرده و به ازای هر دور فقط یک بیت برای نشان دادن سرویس گرفتن یا نگرفتن ذخیره می‌کنیم. پس داده‌های هر دور به جای اینکه ۴۰۰ شناسه باشد، شناسه دور و ۴۰۰ بیت است. در این‌صورت داده‌های تجمیع شده ۱۰۰

جدول ۷ـ۱: حجم پیام‌های اثبات خدمات در شرایط مختلف
علامت * به معنای استفاده از ساختمان داده ذخیره است.

	تعداد دور	میانگین حجم پیام هر رله	مجموع کل پیام‌ها	حجم به ازای هر بلاک
BM-Ed25519	۱	29.42 KB	14.36 MB	14.36 MB
	۱۰۰	2.84 MB	1.39 GB	14.23 MB
	۱۰۰۰	28.45 MB	13.89 GB	14.22 MB
BM-Ed25519*	۱	29.43 KB	17.37 MB	14.37 MB
	۱۰۰	2.46 MB	1.20 GB	12.31 MB
	۱۰۰۰	24.46 MB	11.94 GB	12.23 MB
پیکسل	۱	3.33 KB	1.62 MB	1.62 MB
	۱۰۰	0.30 MB	0.15 GB	1.54 MB
	۱۰۰۰	3.09 MB	1.50 GB	1.54 MB
پیکسل*	۱	3.34 KB	1.63 MB	1.63 MB
	۱۰۰	21.46 KB	10.47 MB	0.10 MB
	۱۰۰۰	100.5 KB	49.1 MB	50.28 KB

دور با امضای پیکسل، برای هر گره رله برابر ۲۱ کیلوبایت و مجموع کل پیام‌ها ۱۰.۵ مگابایت خواهد بود. اطلاعات بیشتر در مورد استفاده از این ساختمان داده را می‌توانید در جدول ۷ـ۱ مشاهده کنید. همانطور که مشخص است از این ساختمان داده برای کاهش حجم پیام‌های BM-Ed25519 نیز می‌توان استفاده کرد ولی تفاوت آنقدر محسوس نیست.

۷ـ۴ سربار زمانی

سربار زمانی که به کل پروتکل اضافه می‌شود به دو قسمت کلی زیر تقسیم می‌شود:

۱. زمانی که صرف پخش و احراز هویت پیام‌های اثبات خدمات در شبکه می‌شود؛ این زمان به اندازه پیام‌ها و امضای مورد استفاده وابسته خواهد بود.

درصورتی که از BM-Ed25519 استفاده کنیم، به تعداد پیام‌های اثبات خدمات(تعداد گره‌های شبکه و تعداد دور) به‌علاوه تعداد گره‌های رله باید احراز اصالت انجام دهیم و همینطور حجم پیام‌ها تقریبا به صورت خطی براساس تعداد پیام‌های تجمیع شده افزوده می‌شود. درصورتی که به ازای هر دور پیام‌ها در شبکه پخش شوند در حدود ۶ ثانیه برای پخش پیام‌ها و کمتر از یک ثانیه برای احراز اصالت آن‌ها لازم است. زمان لازم برای پخش پیام‌های تجمیع شده چند دور، زمان قابل قبولی برای پروتکل نخواهد بود.

اگر از امضای پیکسل استفاده کنیم، در هر مرحله تنها باید به تعداد گره‌های رله احراز هویت انجام دهیم، پس زمان احراز هویت مستقل از تعداد گره‌های شبکه و تعداد دور خواهد بود و این زمان با یک پردازنده معمولی تقریبا برابر ۲ ثانیه است. زمان پخش پیام‌ها در شبکه براساس حجم پیام‌های تجمیع شده مشخص می‌شود، به طور مثال پیام‌های تجمیع‌شده ۱۰۰ دور در حدود ۴ ثانیه و پیام‌های تجمیع‌شده ۱۰۰۰ دور

در کمتر از ۲۰ ثانیه پخش می‌شود.

۲. زمانی که پاداش محاسبه شده به گره‌های رله داده می‌شود؛ این زمان مشابه توافق یک بلاک در شبکه خواهد بود و تنها تفاوت آن با یک بلاک معمولی این است که اعتبار سنج‌ها برای تایید آن باید به محاسبه پاداش گره‌های رله از طریق پیام‌های اثبات خدمات بپردازند.

البته باید به این نکته دقت کنیم؛ علاوه بر اینکه داده‌های زمان پخش در شبکه قدیمی هستند، ما اطلاعاتی راجع به زمان پخش در شبکه رله نداریم و قطعا سرعت پخش در این شبکه بسیار بیشتر خواهد بود.

۷ـ۵ سربار محاسباتی

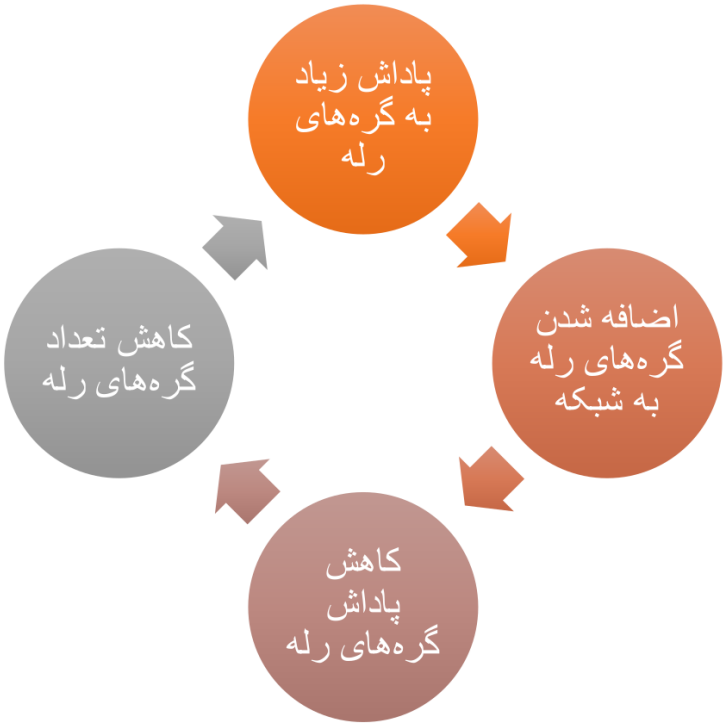
تقریبا تمام سربار محاسباتی اضافه شده، برای احراز هویت پیام‌های ارسالی است. این سربار با استفاده از امضای BM-Ed25519 وابسته به تعداد گره‌های شبکه است و در هر دور باید به تعداد گره‌های شبکه احراز اصالت پیام صورت گیرد. از آنجایی که این احراز اصالت در بسته‌های چندتایی انجام می‌شود، برای شبکه‌ای با ۵۰ هزار گره تقریبا برابر هزینه‌ای است که برای احراز اصالت رای‌های *BA باید صرف شود.

همانطور که در قسمت قبل گفته شد با استفاده از امضای پیکسل تعداد پیام‌هایی که باید احراز اصالت شوند تنها به تعداد گره‌های رله وابسته است، پس تجمیع پیام‌ها هر چقدر بیشتر باشد هر رله سربار کمتری برای احراز اصالت پیام‌ها خواهد پرداخت. البته هر گره رله وظیفه تجمیع امضاها را نیز بر عهده دارد که با بیشتر شدن این تعداد هزینه بیشتری باید پرداخت شود، ولی این هزینه در مقایسه با هزینه احراز اصالت پیام‌های دیگر رله‌ها بسیار کمتر است. در نهایت در هر بار احراز اصالت با ۵۰۰ گره رله تقریبا معادل هزینه‌ای است که برای احراز اصالت رای‌های *BA باید صرف شود.

۷ـ۶ تعداد گره‌های رله

در ابتدای کار برای تحلیل شبکه یک تخمین از حداقل تعداد گره‌های رله در شبکه زده شد، البته با بالا رفتن پهنای باند و سرعت سرورها این حداقل تعداد می‌تواند کمتر هم باشد. به هر حال ممکن است شبکه تعداد بیشتری گره رله داشته باشد، زیرا هرکسی می‌تواند این نقش را به عهده بگیرد.

در فصل قبل هزینه‌های هر گره رله بررسی شد و هزینه‌های آن‌ها به دو قسمت کلی هزینه‌های ثابت و هزینه‌های متغیر تقسیم شد. با اضافه شدن تعداد گره‌های رله از طرفی تعداد گره‌های سرویس‌گیرنده هر کدام کاهش می‌یابد، در نتیجه هزینه‌های متغیر گره رله کاهش می‌یابد و از طرفی برخی هزینه‌ها که به تعداد گره‌های رله وابسته است افزایش می‌یابد. همینطور پاداشی که قبلا میان تعداد کمتری از این گره‌ها تقسیم می‌شد بین تعداد بیشتری گره



شکل ۷ـ۲: چرخه تعداد گره‌های رله در شبکه در طول زمان

تقسیم می‌شود. در این میان گره‌های رله‌ای که سرعت، پهنای باند یا قدرت پردازش کمتری دارند پاداش کمتری دریافت کرده و این پاداش کمتر ممکن است از هزینه‌های ثابت آن گره کمتر باشد. پس این گره رله از شبکه خارج می‌شود.

با خارج شدن تعدادی از این گره‌های رله از شبکه، این فرآیند در جهت برعکس فعال می‌شود و با کمتر شدن تعداد گره‌های رله پاداش بقیه افزایش می‌یابد و همینطور به تعداد بیشتری گره سرویس خواهند داد. این فرآیند که به صورت یک چرخه در شبکه تکرار می‌شود باعث می‌شود تعداد گره‌های رله در شبکه تقریبا ثابت بماند و گره‌هایی که ضعیف‌تر هستند از شبکه حذف شوند. این چرخه را می‌توانید در تصویر ۷ـ۲ مشاهده کنید.

۷ـ۷ مکانیزم تنبیه

از آنجایی که پاداش هر گره رله، وابسته به اظهار دریافت خدمات از گره‌های معمولی است، یک گره می‌تواند با اینکه بلاک را از یک رله دریافت کرده است، به رله دیگری پیام اثبات خدمات بدهد. این اتفاق ممکن است در حالت عادی هم رخ بدهد چون امکان دارد تقریبا همزمان دو گره رله اقدام به ارسال بلاک برای یک گره خاص کنند و گره می‌تواند به هرکدام از آن‌ها تاییدیه بفرستد. با این حال تکرار این وضعیت عادی نیست و به معنای دروغگو بودن گره مورد نظر است.

در این شرایط گره رله می‌تواند از سرویس دادن به این گره خودداری کند؛ می‌توانیم این خودداری را نوعی

تنبیه برای گره مورد نظر در نظر بگیریم. با تکرار این اتفاق در شبکه می‌توان برای این گره تنبیه‌های سخت‌تری نیز در نظر گرفت. مثلا تا مدتی هیچ گره رله‌ای در شبکه به او سرویس ندهد و در این‌صورت نمی‌تواند در پروتکل توافق بلاک مشارکت کرده و پاداشی دریافت کند.

از طرفی ممکن است گره رله در ارائه خدمات کم‌کاری کند. به طور مثال ارسال بلاک که برای او به معنای دریافت پیام اثبات خدمات است را انجام دهد ولی از احراز اصالت رای‌های *BA خودداری کند تا هزینه‌های خود را کاهش دهد. گره‌های عادی سرویس‌گیرنده با مشاهده چنین وضعیتی می‌توانند رله مورد نظر را تنبیه کنند و به رله دیگری متصل شوند تا این گره پاداش کمتری دریافت کند.

امنیت و صحت اطلاعات در یک شبکه رله کاملا وابسته به گره‌های رله در آن است، چون تمام بررسی‌ها و احراز اصالت‌ها توسط این گره‌ها انجام می‌شود. در صورتی که یک یا تعدادی از این گره‌ها مهاجم باشند و اطلاعات غلط به گره‌ها بدهند، ممکن است قسمتی از شبکه را در اختیار بگیرند. البته از آنجایی که گره‌های معمولی به چند گره رله متصل هستند می‌توانند صحت اطلاعات خود را بررسی کند. در صورتی که از دو گره رله دو محتوای متناقض دریافت کردند، می‌توانند خود اقدام به بررسی صحت محتواها کرده و رله خطاکار را تنبیه کنند و از اتصال به او خودداری کنند. در صورتی که به صورت دوره‌ای هر گره معمولی، گره سرویس دهنده خود را تغییر دهد، می‌توان انتظار داشت حتی با تعداد کمی گره رله راستگو شبکه به سمت درستی هدایت شود.

فصل هشتم

نتیجه‌گیری

در فصل‌های قبل مسئله‌های موجود در هر دو مسیر بررسی شد و برای هر کدام راه حلی مبتنی بر ویژگی‌های دو مسیر ارائه شد، همینطور هر کدام از راه حل‌ها به تفصیل تحلیل و بررسی شدند. در این فصل قصد داریم همه تحلیل‌ها را در کنار هم قرار داده و نتیجه نهایی از راه‌حل‌های ارائه شده را بررسی کنیم.

۸ـ۱ شبکه نظیر به نظیر

مسئله موجود در این شبکه پاداش دادن به گره‌هایی است که بیشتر در شبکه فعالیت داشته‌اند. برای تشخیص فعالیت معیاری معرفی کردیم و براساس آن درختی ساخته شد تا بتواند امتیاز هر کس را محاسبه کرده و به افراد لایق پاداش تخصیص دهد. برای ساخت این درخت نیاز بود تا تعداد زیادی پیام تحت عنوان پیام‌های معرفی منبع در شبکه پخش شوند.

همانطور که بررسی کردیم پخش شایعه معرفی منبع به صورت جداگانه توسط هرکدام از گره‌ها سربار زیادی برای شبکه، سربار محاسباتی بالا و سربار زمانی غیر قابل پیش‌بینی خواهد داشت. همینطور به حمله منع سرویس بسیار حساس است و با قطع موقت تعداد کمی از گره‌ها کل پروتکل از کار خواهد افتاد.

با استفاده کردن از نماینده‌های تجمیع کننده پیام، سربار شبکه و محاسبات کاهش چشمگیری خواهد یافت

و سربار زمانی قابل پیش‌بینی‌تر می‌شود. با این حال نماینده‌ها نقاط حساس به حمله منع سرویس هستند.

اگر فرض کنیم در شبکه مهاجمی وجود ندارد، می‌توانیم راه حل را به دو قسمت کلی تقسیم کنیم:

۱. اگر از امضای BM-Ed25519 در پیام‌های شبکه استفاده می‌کنیم، انتخاب نماینده‌ها وابسته به درخت تعاملات گزینه خوبی برای کاهش سربار شبکه خواهد بود؛ زیرا برای کنترل حجم پیام‌های ارسالی، تعداد نماینده‌ها نباید از تعداد خاصی کمتر باشد و تبلیغ نماینده‌های مستقل با افزایش تعداد آن‌ها هزینه زیادی در بر خواهد داشت. البته متغیرهای مربوط به انتخاب نماینده‌های وابسته به درخت باید به دقت براساس شبکه تنظیم شوند.

۲. درصورتی که از امضای پیکسل در پیام‌ها استفاده می‌کنیم، انتخاب نماینده‌ها به صورت مستقل گزینه خوبی خواهد بود. زیرا برای کاهش سربار، تعداد نماینده‌ها باید کم باشند و کم کردن تعداد نماینده‌ها با انتخاب وابسته به درخت ممکن نخواهد بود. همینطور چون تعداد نماینده‌های مستقل کم است، سربار زیادی برای تبلیغ آن‌ها به شبکه اضافه نمی‌شود.

در مقایسه دو حالتی که بررسی کردیم، حالت دوم سربار شبکه، زمان و محاسبات بسیار کمتری برای کل شبکه دارد. ولی درصورتی که الگورند از امضای پیکسل استفاده کند قابل پیاده‌سازی است.[۱]

اگر شبکه را خالی از مهاجم فرض نکنیم، هر دو روش به حمله منع سرویس آسیب‌پذیر هستند. البته مهاجم باید قدرت بالایی داشته‌باشد تا در زمان کوتاهی (در حدود ۱۰ ثانیه) به تعداد زیادی از نماینده‌ها حمله کند و اتصال آن‌ها از شبکه را قطع کند. در روش اول به دلیل اینکه تعداد نماینده‌ها بیشتر است، در نگاه اول آسیب‌پذیری کمتری به این حمله خواهد داشت، ولی مهاجم با حمله به تعداد کمی از نماینده‌ها که در ارتفاع کمی از درخت هستند، می‌تواند تخصیص پاداش را مختل کند. در صورتی که در روش دوم با اینکه تعداد نماینده‌های کمتری وجود دارند، چون هر گره به صورت تصادفی نماینده خود را تعیین می‌کند، مهاجم باید به تعداد زیادی از این نماینده‌ها حمله کند تا کل پروتکل را مختل کند. برای کم کردن آسیب‌پذیری در روش دوم می‌توانیم برای هر گره دو یا چند نماینده در نظر بگیریم، تا با حمله به یکی از نماینده‌ها با احتمال کمتری پروتکل آسیب ببیند. البته با این کار سربار بیشتری بر شبکه تحمیل خواهیم کرد.

اگر فرض کنیم در شبکه تعداد محدودی گره وجود دارند که به حمله منع سرویس آسیب‌پذیر نیستند، می‌توانیم نماینده‌ها را از این مجموعه انتخاب کنیم و آسیب‌پذیری هر دو راه‌حل تا حدود خوبی برطرف خواهد شد، با این فرض در روش اول، پیشنهاددهنده بلاک که اولین نماینده است، به همین مجموعه کوچک محدود می‌شود

[۱] الگورند در برنامه‌های آینده خود ذکر کرده است که به زودی از این رمزنگاری استفاده خواهد کرد.

ولی در روش دوم محدودیتی در انتخاب هیچ‌کدام از نقش‌ها به وجود نمی‌آید.

در نهایت برای جمع‌بندی این قسمت مزایا و معایب استفاده از راه‌حل پیشنهادی را بررسی می‌کنیم.

۸ـ۱ـ۱ مزایا و معایب

+ تخصیص عادلانه پاداش به گره‌های شبکه
+ تخصیص پاداش کمتر به گره‌ها، در نتیجه هزینه کمتر ایجاد تراکنش جدید
+ ادامه حیات شبکه الگورند با بزرگتر شدن شبکه
- ترافیک بیشتر شبکه، مستقل از اندازه بلاک؛ به ازای هر بلاک حداقل ۳.۵ مگابایت ترافیک بیشتر مصرف می‌شود.
- کم شدن مقیاس‌پذیری پروتکل؛ زیرا به صورت مستقیم یا غیرمستقیم هزینه هر گره به اندازه شبکه مرتبط می‌شود.
- حساس‌تر شدن پروتکل به حمله منع سرویس

۸ـ۲ شبکه بازپخش

مسئله موجود در این شبکه تخصیص پاداش به گره‌های رله در شبکه است. گره‌های رله در این شبکه وظیفه ارائه برخی خدمات به گره‌های معمولی را دارند و به ازای این خدمات پاداش دریافت می‌کنند. حال برای تخصیص پاداش به این گره‌ها معیاری تحت عنوان معیار ارائه خدمات معرفی شد تا براساس آن پاداش هر کدام از رله‌ها محاسبه گردد.

همانطور که بررسی شد گرفتن پاداش وابسته به پخش پیام‌های اثبات خدمات مربوط به هرکدام از گره‌های رله در شبکه است. حجم، زمان و محاسبات لازم برای تولید، پخش و بررسی این پیام‌ها وابسته به رمزنگاری مورد استفاده است. میان دو امضای مورد بررسی امضای پیکسل از هر نظر برای این کاربرد مناسب‌تر بود و در کنار ساختمان داده‌ای که برای این مسئله طراحی کردیم، سربار بسیار کمی برای شبکه در بر داشت.

البته برای کمینه کردن سربار در شبکه، لازم است براساس ویژگی‌های آن تنظیمات دقیقی برای آن صورت گیرد. به طور مثال اینکه تجمیع پیام‌های اثبات خدمات برای چند دوره انجام شود، موضوع مهمی است که باید براساس زمان پخش پیام‌ها و وضعیت ثبات شبکه تنظیم شود؛ در صورتی که اتصالات شبکه به سرعت تغییر کنند، طولانی کردن این زمان باعث افزایش بیش از حد اندازه این پیام‌ها خواهد بود و از طرفی کم کردن آن

باعث افزایش سربار محاسباتی برای گره‌های رله می‌شود.

برای کاهش سربار شبکه و امنیت هرچه بیشتر آن بهتر است بعد از هربار پاداش دهی به گره‌های رله، گره‌های معمولی یک یا چند اتصال خود را تغییر دهند(اتصالاتی که ضعیف‌تر هستند) و تا حد امکان در بازه محاسبه پاداش اتصالات خود در شبکه را تغییر ندهند.

در آخر مزایا و معایب این راه حل را بررسی می‌کنیم. گرچه همانطور که در تحلیل‌های گذشته مشاهده کردید، مزایای استفاده از این راه حل قابل مقایسه با معایب آن نیست.

۸-۲-۱ مزایا و معایب

+ شبکه‌ای امن‌تر و سریع‌تر بدون هزینه‌های اضافه
+ تخصیص عادلانه پاداش به گره‌های رله
+ مکانیزم تنبیه برای گره‌های مهاجم و دروغگو در شبکه
+ سربار بسیار کم با تنظیمات درست بر اساس ویژگی‌های شبکه
+ انگیزه برای استفاده از تجهیزات بهتر در شبکه و سرعت بیش‌تر در پیشرفت آن
- حذف گره‌های رله ضعیف‌تر؛ ممکن است باعث شود قدرت‌های بزرگ شبکه را تحت کنترل بگیرند.

References

[1] Algo dynamics. Available at https://algorand.foundation/algo-dynamics.

[2] Algorand node types. Available at https://developer.algorand.org/docs/run-a-node/setup/types.

[3] Ed25519 documentation. Available at https://ed25519.cr.yp.to/.

[4] Chen, J., and Micali, S. Algorand. Available at https://arxiv.org/abs/1607.01341v9.

[5] Decker, C., and Wattenhofer, R. Information propagation in the bitcoin network. Available at https://ieeexplore.ieee.org/document/6688704.

[6] Drijvers, M., Gorbunov, S., and Neven, G. Pixel: Multi-signatures for consensus. Available at https://www.usenix.org/system/files/sec20summer_drijvers_prepub_0.pdf.

[7] Fooladgar, M., Manshaei, M. H., Jadliwala, M., and Rahman, M. A. On incentive compatible role-based reward distribution in algorand. Available at https://arxiv.org/abs/1911.03356.

[8] Gillad, Y. Algorand: Scaling byzantine agreement for cryptocurrancies. Available at https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf.