

Improving The Security of the Anonymous Network Using QMNTR Encryption

Mohammad Mahdi Daneshvar Jalairi ¹, Parviz Rashidi khazaei* ²

¹ Master's student, Urmia University of Technology, Urmia, Iran. Email: m.m.daneshvar@it.uut.ac.ir

² Assistant Professor, Urmia University of Technology, Urmia, West Azarbaijan, Iran.

(Correspondence: p.rashidi@uut.ac.ir)

ARTICLE INFO

Article history:

Article Type: Research paper

Receive: 30 June 2025

Revise: 04 August 2025

Accept: 09 September 2025

Available online: 03 October 2025

Keywords:

Anonymity Network Architecture

QMNTR encryption

LRS Digital Signature

ABSTRACT

In the context of the Internet and network, secure data exchange along with the anonymity of sender and receiver has been one of the main needs of users. Therefore, various types of anonymity networks have been designed and developed. The architecture of the anonymity network and the structural weakness of the encryption system used in them have caused numerous security problems. With the advancement of quantum computing, many attacks have been designed and successfully disrupted the security of the anonymity network. Various mechanisms have been proposed to improve the security of anonymous networks, some of which are only theoretical and cannot be implemented, and others have serious weaknesses and vulnerabilities that cannot be used. The breaking of Encryption systems, the vulnerability of classic digital signatures, and non-resistant cryptographic algorithms against quantum attacks are among the important weaknesses of the architecture of anonymous networks. To overcome these challenges, a secure structure using a QMNTR encryption system and LRS digital signature based on the onion routing structure has been proposed to secure the anonymous network. The results of Research and technical evaluation show that the proposed architectural structure improves the ability to deal with all kinds of threats and ensures the reliability of relays in the anonymity network. In addition, with appropriate time complexity, the security of key distribution has increased and the communication overhead has been reduced. Using an LRS digital signature has also helped improve the anonymous network's security and has achieved acceptable performance.

Cite this article: Daneshvar Jalayeri, M. M., & RASHIDI KHAZAEI, P. (2025). Improving anonymity network security using QMNTR encryption. *Electronic and Cyber Defense*, 13(3), 17- 40. 2025

DOI: <https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.3.2>



OPEN ACCESS

© The Author(s). retain the copyright and full publishing rights

Publisher: Imam Hossein University

بهبود امنیت شبکه گمنامی با استفاده از رمزنگاری QMNTR

محمد مهدی دانشور جلایری¹، پرویز رشیدی خزاعی^{2*}

¹ دانشجو کارشناسی ارشد فناوری اطلاعات، دانشگاه صنعتی ارومیه. ایمیل: m.m.daneshvar@it.uut.ac.ir

² استادیار، دانشگاه صنعتی ارومیه، ارومیه، ایران. (نویسنده مسئول: p.rashidi@uut.ac.ir)

چکیده	مشخصات مقاله
در بستر اینترنت و شبکه، تبادل امن داده‌ها به همراه گمنامی فرستنده و گیرنده یکی از نیازهای اصلی کاربران بوده است. از این رو، انواع شبکه‌های گمنامی طراحی و توسعه پیدا کرده‌اند. معماری شبکه گمنامی و ضعف ساختاری سیستم رمزنگاری به کاررفته در آن‌ها باعث بروز مشکلات امنیتی متعددی شده است و با پیشرفت پردازش‌های کوانتومی، حملات متعددی طراحی و به طور موفقیت‌آمیزی امنیت شبکه گمنامی را مختل کرده است. سازوکارهای مختلفی برای بهبود امنیت شبکه‌های گمنامی ارائه شده است که برخی از آنان صرفاً جنبه نظری داشته و قابل پیاده‌سازی نبوده و برخی دیگر نیز دارای ضعف‌ها و آسیب‌پذیری‌های جدی هستند که قابلیت استفاده ندارند. شکسته شدن دستگاه‌های رمزنگاری، آسیب‌پذیر بودن امضاءهای دیجیتال کلاسیک و الگوریتم‌های رمزنگاری غیر مقاوم در برابر حملات کوانتومی از جمله ضعف‌های مهم معماری شبکه‌های گمنامی می‌باشند. برای غلبه بر این چالش‌ها، ساختاری امن با به کارگیری سیستم رمزنگاری QMNTR و امضاء دیجیتال LRS مبتنی بر ساختار مسیریابی پبازی، جهت امن سازی شبکه گمنامی پیشنهاد شده است. نتایج بررسی‌ها و ارزیابی فنی نشان می‌دهد ساختار معماری پیشنهادی توانایی مقابله با انواع تهدیدات را بهبود داده و باعث تضمین قابلیت اطمینان به رله‌ها در شبکه گمنامی شود. به علاوه، با پیچیدگی زمانی مناسب، امنیت توزیع کلید را افزایش و سربار ارتباط را کاهش داده است و با به کارگیری امضاء دیجیتال LRS، به ارتقای امنیت شبکه گمنامی کمک نموده است و کارایی قابل قبولی نیز دارد.	تاریخچه مقاله: نوع مقاله: علمی - پژوهشی دریافت: 09 تیر 1404 بازنگری: 13 مرداد 1404 پذیرش: 18 شهریور 1404 ارائه آنلاین: 11 مهر 1404 کلیدواژه‌ها: ساختار شبکه‌های گمنامی امضاء دیجیتال رمزنگاری QMNTR امضاء دیجیتال LRS

1. مقدمه

داده و مطابق با معماری رمزنگاری شبکه گمنامی ساختار جدیدی پیشنهاد شده است.

در این ساختار سیستم رمزنگاری QMNTR [6] جایگزین رمزنگاری کلاسیک خواهد شد که امضاء دیجیتال LRS⁵ [7] نیز در کنار آن به کارگیری می شود. رمز و امضاء ارائه شده به عنوان یک جایگزین برای سیستم رمزنگاری کلاسیک جهت بهبود امنیت و عملکرد شبکه گمنامی معرفی خواهد شد. با استفاده از الگوریتم رمزنگاری QMNTR، به عنوان یکی از انواع نسل جدید دستگاه های رمزنگاری مقاوم در برابر حملات کوانتومی، با افزایش پیچیدگی الگوریتم نسبت به نسخه های پیشین خود باعث ارتقاء امنیت شبکه گمنامی خواهیم شد. به کارگیری امضاء دیجیتال LRS کمک خواهد کرد که ناشناسی بدون قید و شرط فراهم شود. همچنین به کار بردن امضاء دیجیتال LRS بسیاری از مشکلات امضاءهای حلقه معمولی را حل خواهد کرد و بسیار بهینه تر و امن تر خواهد بود [7].

دیدگاه پیر شور جهت توسعه الگوریتم های کوانتومی چندجمله ای برای فاکتورگیری اعداد صحیح و محاسبه لگاریتم های گسسته، علاقه به محاسبات کوانتومی را به شدت افزایش داد. الگوریتم های پیر شور [8] به سرعت فوق العاده ای نسبت به الگوریتم های کلاسیک دست یافتند و برای مسائل خارج از حوزه مکانیک کوانتومی اعمال شدند و می توانند برای شکستن دستگاه های رمزنگاری استفاده شود [9]. در نتیجه بایستی در استفاده از رمزنگاری کلاسیک بازنگری جدی داشته باشیم و اگر بخواهیم بازهم از همان روش های کلاسیک برای تشکیل کلید استفاده کنیم، نیاز است کلید عمومی را با طول بیشتر از 2048 کیلوبیت انتخاب نماییم که به راحتی قابل شکسته شدن توسط پردازش های کوانتومی فعلی نباشد.

این موضوع خود مشکلات زیادی در بردارد از جمله مهم ترین این مشکلات، موضوع ارتباطات بلادرنگ در روابط گمنام است. سنگین شدن کلید عمومی باعث افزایش تأخیر در تبادل اطلاعات در شبکه می شود که به توانایی پردازش در شبکه بستگی دارد، و صرفاً در شبکه با تأخیر بالا کارایی مناسب تری دارد. از این رو محققان اقدام به طراحی و پیاده سازی سامانه های رمزنگاری پیچیده، جدید و سبک مبتنی بر هم گشت یا کانولوشن⁶ در ریاضیات کردند.

یکی از اولین انواع آن سامانه های رمزنگاری NTRU⁷ بود [10]. این سیستم رمزنگاری یک نمونه از سامانه های رمزنگاری احتمالاتی است که پس از ابداع این سیستم رمزنگاری، انواع مختلفی از آن

تاکنون روش های متعددی برای امن سازی، محرمانگی و یکپارچگی محتوای پیام های رد و بدل شده در بسترهای ارتباطی، ارائه شده است. شبکه های گمنامی¹ به طور کلی به منظور ایجاد بستر امن تبادل داده استفاده می شوند. پژوهشگران حوزه امنیت گمنامی را [1] یک ویژگی امنیتی مهم تلقی می کنند و پیاده سازی آن را برای رسیدن به ارتباطی با ویژگی امنیت مضاعف لازم، می دانند. مسیریابی پیاپی² یکی از برجسته ترین روش های طراحی یک شبکه ای گمنامی است [2] که در چهار دهه گذشته معرفی و به صورت گسترده ای از آن استفاده شده است [3]. ساختار آن بر شبکه چند رله ای پایه گذاری شده و برای ارتباط با هر رله یک بستر امنیتی مستقل ایجاد می کند. آغاز پروژه شبکه گمنامی در آزمایشگاه تحقیقاتی نیروی دریایی ایالات متحده بود که در اواخر سال 2003 توسعه این پروژه به خارج از ارتش آمریکا برای بهبود امنیت و حریم خصوصی کاربران اینترنت تحت عنوان سامانه تر³ سپرده شد. تر به سرعت در بستر اینترنت مورد اقبال عمومی قرار گرفت، طوری که در ژانویه سال 2010 حدود 1000 رله عمومی داشت و این تعداد در ژانویه 2015 به 8000 رله افزایش یافت که امروزه دارای حداقل 7000 رله⁴ تثبیت شده است. از آنجاکه این شبکه همواره بستری برای فعالیت های مخرب نیز بوده است رقیب جدی برای دولت هایی محسوب می شود که به دنبال ایجاد نظارت و محدودیت در بستر اینترنت هستند به عنوان مثال دولت روسیه طی یک مسابقه ای که در جولای 2014 برگزار شد عنوان کرده بود در صورتی که هر شهروند روسی بتواند باعث ایجاد رخنه و خراب کاری در شبکه تر بشود 110000 دلار پاداش دریافت می کند. بررسی پژوهش های انجام شده نشان داده است شبکه گمنامی هنوز هم آسیب پذیر است [4]. پژوهشگران برای بهبود امنیت شبکه گمنامی، سیستم رمزنگاری NTRU را جایگزین سیستم رمزنگاری کلاسیک RSA نموده و جهت حفظ حریم خصوصی از امضای دیجیتال از NSS به جای الگوریتم های چکیده ساز استفاده کردند که NSS به عنوان یک مکمل برای سیستم رمزنگاری NTRU به کار گرفته شد [5]. با توجه به آسیب پذیری های وارده طی چند سال گذشته در معماری NTRU که در بخش 3-5 به آن ها اشاره خواهیم کرد، ضرورت ایجاد می کند معماری شبکه گمنامی را بازطراحی کرده و آن را بهبود بخشیم. بدین منظور معماری شبکه گمنامی را مورد بازنگری قرار

¹ Anonymity Networks² Onion Routing³ Tor⁴ Relay⁵ linkable Ring Signatures⁶ Convolution⁷ Number Theory Research Unit

شد و به سهم خود نوعی اصلاح ساختار معماری در شبکه گمنامی برای مقابله با حملات جدید است. پروتکل توزیع کلید شبکه گمنامی با استفاده از الگوریتم رمزنگاری *QMNTTR* و امضا دیجیتال *LRS* بهبود داده شده تا در برابر حملات تأثیر گزار بر روی تبادل کلید و انواع حملات مردمیانی در شبکه گمنامی مقاومت کافی داشته باشد. نتایج حاصل از پژوهش ارائه شده در مقایسه با پژوهش‌های پیشین نشان می‌دهد روش پیشنهادی در برابر انواع حملات شامل: حملات کوانتومی، منع سرویس^۳، تحلیل ترافیک^۴ و مردمیانی^۵، از مقاومت کافی برخوردار بوده و گمنامی بدون قید و شرط را در شبکه تأمین، و امنیت فرآیند توزیع و تبادل کلید را بهبود داده است.

ساختار مابقی مقاله به این شرح است که در بخش دوم ساختار شبکه گمنامی ارائه شده است. در بخش سوم تعریف مسئله و آسیب‌پذیری‌های شبکه گمنامی به همراه برخی از چالش‌های کنونی آن مطرح می‌شود. در بخش چهارم مشکلات فعلی معماری شبکه گمنامی بحث و بررسی شده که ضروری است بازطراحی معماری شبکه گمنامی با رعایت آن‌ها صورت گیرد. در بخش پنجم رمزنگاری *QMNTTR* و امضاء دیجیتال *LRS* معرفی شده است. در بخش ششم نحوه پیاده‌سازی روش پیشنهادی تشریح شده است که در پایان قسمت آسیب‌پذیر پروتکل توزیع کلید به لحاظ امنیتی ارتقاء پیدا خواهد کرد. در بخش هفتم، روش پیشنهادی از جوانب مختلف تجزیه و تحلیل شده است که نتایج ارزیابی، بهبود امنیت شبکه گمنامی را نشان می‌دهد. در بخش هشتم نتیجه‌گیری و در بخش نهم نیز پیشنهادها و کارهای آتی در خصوص موضوع تحقیق ارائه شده است.

2. ساختار شبکه گمنامی پیشنهادی

یکی از اشتباهات رایج در طراحی شبکه گمنامی این است که کاربر شبکه به‌عنوان بخشی از شبکه گمنامی در نظر گرفته شود و خود وظیفه پیدا کردن رله‌های موجود در شبکه، انتخاب و تشکیل مسیر را بر عهده داشته باشد. به‌وسیله این نوع طراحی آسیب‌پذیر، فهرستی از تمامی سامانه‌های موجود در شبکه قابل استخراج است. علاوه بر این در صورت آلوده بودن سیستم کاربر شبکه گمنامی، امنیت زیرساخت شبکه گمنامی طراحی شده با چالش مواجه خواهد شد. مهاجم از طریق آلوده کردن سیستم کاربر مسیرهای ارتباطی را از طریق روش‌هایی مانند تجزیه و تحلیل ترافیک شناسایی کرده که با تغییر در الگوی جریان شبکه گمنامی، جریانی خاص به‌وسیله روش‌هایی نظیر

توسط محققین با استفاده از ساختارهای جبری متفاوتی پیشنهاد شده است که سیستم رمزنگاری *QMNTTR* یکی از جدیدترین توسعه‌های *NTRU* اولیه است. امروزه محاسبات کوانتومی مورد توجه بسیاری از پژوهشگران قرار گرفته که ابداع انواع سامانه‌های رمزنگاری که اخیراً پس از *QMNTTR* توسعه پیدا کرده‌اند خود دلیل واضحی برای این موضوع است و می‌توان به سامانه‌های رمزنگاری *QOTRU, NTRSH, AHQTR, QOCNTR, QSTRU* اشاره کرد [11]. روش‌های مقاوم‌سازی پیشین در شبکه گمنامی بر اساس مؤلفه‌هایی نظیر: تغییر اندازه بسته به یک مقدار معین و استفاده از مؤلفه لایه گذاری (افزودن دنباله‌هایی از بسته‌ها و ترافیک ساختگی) عمل می‌کردند. گلوگاه اصلی این روش‌ها افزایش سربار چند صد برابری در پهنای باند و سربار زمانی، و به تبع آن عدم امکان استفاده عملی از روش‌های مقاوم‌سازی مبتنی بر این دو مؤلفه بود. عدم وجود پهنای باند کافی و عدم امکان افزایش طول کلید در معماری سیستم رمزنگاری و تسهیل در اجرای حمله منع سرویس و امکان حذف بسته‌های با اندازه ثابت حاصل از روش مقاوم‌سازی در رله اول (محل اعمال حمله)، عدم توانایی مؤثر در پیشگیری از وقوع دیگر حملات و حمله اثر انگشت^۱ از دیگر مشکلات این روش‌ها بود. واضح است که شکستن مستقیم گمنامی از طریق پروتکل مورد استفاده در این معماری امنیتی معادل با شکستن الگوریتم رمز خواهد بود و فقط با استفاده از روش‌های پردازش کوانتومی شکستن الگوریتم رمز در شبکه گمنامی امکان‌پذیر است. پیشرفت قابل توجه در ارائه رویکردهای جدید برای طراحی انواع حملات بر روی شبکه‌های گمنامی و سامانه‌های رمزنگاری از یک‌سو و لزوم استفاده روزافزون از شبکه‌های گمنامی در بستر اینترنت از سوی دیگر، موجب ایجاد انگیزه‌ی بیشتر برای ارائه یک شبکه گمنامی مقاوم در برابر انواع حملات در بین پژوهشگران شده است. با توجه به اهمیت امنیت ارتباطات و حفظ گمنامی در کاربردهای آتی نظیر شبکه‌های اجتماعی و اینترنت اشیاء^۲ و دیگر سامانه‌های گمنامی زیرساختی، ضرورت ارائه روش‌های مقاوم‌سازی جهت ارتقاء درجه گمنامی در کاربردهای گفته را تأیید می‌کند.

از این‌رو در چند سال اخیر، موج جدیدی از پژوهش‌ها برای ارائه انواع روش‌های مقاوم‌سازی پدید آمده است. در این پژوهش روشی برای تبادل کلید و رمزنگاری در سطح شبکه گمنامی بر اساس روش‌های پیشین ارائه شده است که به‌کارگیری و پیاده‌سازی آن در شبکه گمنامی باعث افزایش امنیت پیکره سیستم در برابر حملات کوانتومی و دیگر حملات مهم شد خواهد

³ Denial of Services Attack (DOS)

⁴ Traffic Analysis Attack

⁵ Man-In-The-Middle (MITM)

¹ Fingerprint Attack

² Internet of Thing

گره‌هایی که پهنای باند بیشتری دارند، احتمال بیشتری دارد برای انتخاب در مدار به‌کارگیری شوند. قبل از ساخت یک مدار جدید یک مسیر تولید می‌شود، انتخاب این مسیر نیز محدودیت‌هایی دارد. به این صورت که یک روتر دومرتبه برای یک مسیر انتخاب نمی‌شود، بیش از یک روتر در یک زیر شبکه معین برای یک مسیر انتخاب نمی‌شود، و در آخر روتر های غیرقابل اجرا یا نامعتبر انتخاب نمی‌شوند مگر در صورتی که پیکربندی شده باشند [14].

رله (relay): رله‌ها وظیفه دریافت داده از نود قبلی و انتقال آن به آخرین گره را بر عهده دارند. بسته‌های ارسالی و دریافتی در یک پروتکل مشخص شده طراحی و تبادل می‌شوند.

سرورهای دایرکتوری: مسیریابی پیازی [15] از یک مکانیسم غیر ایمن و غیرمتمرکز کشف گره به نام *In-band Status* استفاده می‌کرد که به این خاطر سرورهای دایرکتوری را طراحی کردند. گره‌های شبکه در این روش به جای این که اطلاعات مرتبط با خود را با گره‌های دیگر به اشتراک بگذارند می‌توانند از طریق امضاء کردن آن‌ها با سرور دایرکتوری شبکه گمنامی این کار را انجام دهند. گره‌ها بر اساس فلگ اختصاص داده شده توسط سرورهای دایرکتوری به چهار نوع طبقه‌بندی می‌شوند: گره‌های *Guard*، *Exit*، *Middel* و *Double* که به ترتیب با G ، M ، E و D مشخص می‌شوند. گره‌هایی که دارای فلگ های *Guard* و *Exit* هستند *Dnode* به آن‌ها اختصاص داده می‌شود و گره‌هایی که دارای فلگ *Guard* و *Exit* نیستند *Mnode* در نظر گرفته می‌شود [16].

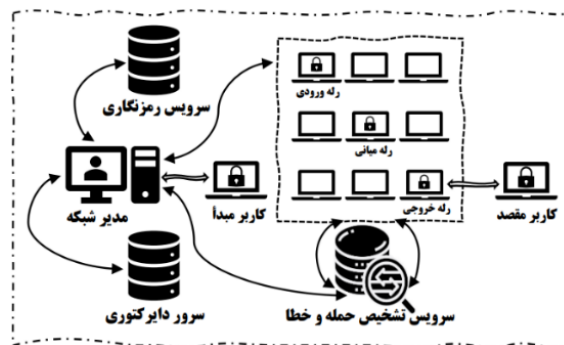
اگر P_m ، P_{en} و P_{ex} به ترتیب رله میانی^۱، رله ورودی^۲، و رله خروجی^۳ باشند، وزن پهنای باند برای گره‌های شبکه گمنامی از نوع t که در موقعیت p در حال سرویس دهی هستند را می‌توان با $W_{p,t}$ نشان داد که در آن t برابر G ، E ، M or D و $t = p$ نیز برابر P_m ، P_{en} ، P_{ex} است. در عمل سرورهای دایرکتوری شبکه گمنامی مقادیر $W_{p,t}$ را بر اساس چند قانون محاسبه و آن‌ها را در شبکه در یک فایل تجمیع و از طریق سرور دایرکتوری منتشر می‌کند. فرض کنید $B(n_i)$ و $T(n_i)$ به ترتیب پهنای باند و نوع گره در شبکه گمنامی باشند، احتمال تقریبی انتخاب گره n_i برای سرویس دهی در مدار در موقعیت P را می‌توان بر اساس رابطه (1) تعیین کرد [17].

$$P_{(p,n)} = W_{p,T(n_i)} B(n_i) / \sum_j W_{p,T(n_j)} B(n_j) \quad (1)$$

سرویس تشخیص حملات و مدیریت خطا: از آنجاکه مدیر شبکه تنها با رله‌های ابتدایی به صورت مستقیم ارتباط دارد و دستورات موردنظر خود را از همین طریق برای رله‌های میانی و انتهایی و

نشانه‌گذاری مبتنی بر فاصله [12] نشانه‌گذاری شده و در مرزهای خروجی شبکه آن جریان ردیابی می‌گردد. در نهایت پس از رهگیری شبکه اقدام به نفوذ در زیرساخت شبکه، تحلیل معماری و اجرای انواع حملات بر روی مؤلفه‌های مختلف شبکه گمنامی می‌کند.

با در نظر گرفتن موارد گفته شده ضروری است یک شبکه گمنامی ایمن، مقیاس پذیر و متمرکزتر مطابق روش پیشنهادی طراحی بشود که قابلیت به کارگیری در انواع کاربردها را داشته باشد و از آخرین مکانیسم‌ها و فناوری‌ها در پیاده‌سازی معماری آن استفاده شود. یک شبکه گمنامی را می‌توان به بخش‌های مختلفی تقسیم کرد که پیوند ناپذیری بین اجزای شبکه از اهمیت بسیار بالایی برخوردار است. بدین منظور اجزا و نحوه پیکربندی شبکه گمنامی را به همراه وظایف مؤلفه‌های آن به تفکیک در ادامه ارائه خواهیم کرد.



شکل (1): اجزای شبکه گمنامی پیشنهادی

1-2. اجزا شبکه گمنامی

مدیریت شبکه: وظیفه این نود تنظیم، مدیریت و پیکربندی ویژگی‌های هر یک از رله‌های موجود و کلیه ارتباطات و مدارهای تشکیل شده در بستر شبکه است و می‌تواند در هر جایی از بستر شبکه یا زیرساخت استقرار یابد به نحوی که بتواند با دیگر مؤلفه‌ها ارتباط برقرار کرده و دستورات مربوطه را ارسال کند که بنا به دلایل امنیتی باید ویژگی پیوند ناپذیری در برابر رله‌ها در آن رعایت شود.

مسیریابی پیازی و ایجاد مدار: ترافیک شبکه به وسیله معماری مسیریابی پیازی از طریق ایجاد مداری از گره‌ها تبادل می‌شود و هر گره صرفاً گره قبلی و بعدی خود را می‌شناسد. داده‌ها در شبکه گمنامی قبل از رسیدن به مقصد از چند گره عبور می‌کنند و به چنین انتخابی از گره‌ها مدار گفته می‌شود که هر مدار به مدت 10 دقیقه استفاده و بازیابی می‌شود [13]. برای افزایش عملکرد و ناشناسی شبکه این مسیر از طریق یک الگوریتم مسیریابی پیچیده انتخاب می‌شود که این الگوریتم گره‌ها را بر اساس پهنای باند گره انتخاب می‌کند.

¹ Middel Relay

² Guard Relay

³ Exit Relay

به نحوی که درخواست را طبق هر پروتکلی که دریافت کرده باشد متناسب با آن پاسخ خواهد داد.

در روش پیشنهادی دو نوع مدار می‌تواند تشکیل شود در نوع اول تشکیل مدار در شبکه مطابق سیستم کلاسیک شبکه گمنامی تر از طریق 3 رله در هر مدار ایجاد می‌شود و در نوع دوم مدیر شبکه می‌تواند از بین رله‌های موجود چندین مدار با مسیرهای مختلف جهت امنیت بیشتر ایجاد کند. مدیر شبکه کلید عمومی نشست را بین گره‌ها به اشتراک می‌گذارد، با هر گره مسیریابی را در شبکه انجام می‌دهد یک شناسه مدار به نام *CellHeader* برای مدار تنظیم می‌کند و پس از ایجاد مدار فرآیند انتقال پیام را انجام می‌دهد. پیام دریافت شده را از طریق پروتکل مربوطه، به اولین رله در مدار رسانده و آن را باز می‌کند. پیام دریافتی به سلول‌هایی با اندازه ثابت 512 بایت که حاوی یک *Payload* و یک *Header* در هر سلول است، تقسیم می‌شود.

از طریق کلیدهای عمومی که در مدار توسط مدیر شبکه به اشتراک گذاشته شده است رله موردنظر بسته داده را دریافت کرده و با کلید خصوصی خود یک‌لایه از رمزنگاری را پس از رمزگشایی آن حذف می‌کند و آدرس رله بعدی را به دست می‌آورد، این روند تا گره خروجی ادامه دارد تا پیام از طریق شبکه به صورت متن ساده به مقصد خود برسد. دستورات پیکربندی که از طریق مدیر شبکه گمنامی ارسال و مدیریت می‌شود، به دودسته دستورات کنترل گره‌های شبکه و دستورات کنترل جریان داده در شبکه تقسیم می‌شوند که در جداول شماره (1) و (2) نشان داده شده‌اند [16].

درخواست کاربر جهت اتصال به شبکه گمنامی از طریق پروتکل *TCP* در یک پورت و آدرس معین به مدیر شبکه می‌رسد و مدیر اتصال را به وسیله پروتکل تعریف شده برقرار کرده، سپس یک مدار جدید و یک مسیریاب خروجی برای آن انتخاب می‌کند. پایان دادن به جریان شبکه گمنامی مطابق یک جریان *TCP* است. برای آدرس‌دهی سلول‌های رله، کلاینت یک *Digest* به آن‌ها اختصاص می‌دهد که به طور مکرر در فرآیند تبادل داده، تشکیل مدار و رمزنگاری سلول‌ها تکرار می‌شوند. هنگامی که یک سلول به یک رله در مدار می‌رسد، سلول رمزگشایی می‌شود، اطلاعات لازم از هدر آن استخراج شده و برای رله بعدی ارسال می‌شود و یا به صف مدار خروجی (مدار فعال) می‌رود.

هر اتصال مدار دارای یک بافر خروجی است که از طریق آن داده‌ها را به رله بعدی به روش *FIFO* ارسال می‌کند. به طور کلی یک اتصال واحد در مدارهای متعدد به اشتراک گذاشته می‌شود، صف‌های مدار حاوی سلول‌ها در بافر خروجی مالتی پلکس

دیگر رله‌ها در سراسر شبکه ارسال می‌کند در صورت وجود خرابی یا قطعی در یکی از رله‌های میانی این امکان وجود دارد از یک رله به بعد بقیه رله‌های مدار در دسترس نباشند. به منظور حل این مشکل به طور خودکار با استفاده از داده‌های موجود در شبکه ادامه اتصال مدار از مسیر دیگری برقرار خواهد شد. در صورتی هم که رله قطع شده رله خروجی باشد با استفاده از داده‌های موجود آخرین رله مدار به عنوان رله انتهایی تعیین می‌شود و مدار از مسیر دیگری ارتباط خود را برقرار می‌کند تا رله میانی در هر مدار مشارکت داشته باشد.

دریافت و بررسی گزارش حملات و رویدادها در شبکه گمنامی یکی از مؤلفه‌های اصلی در حفظ امنیت و مدیریت رله‌ها است. سرویس تشخیص حملات و مدیریت خطا در شبکه رویدادها و گزارش‌های را دریافت می‌کند. این سرویس از طریق پروتکل *SNMP* و ترکیب توابع فیلتر توزیع ترافیک می‌تواند راه‌اندازی می‌شود. امروزه تجزیه و تحلیل ترافیک شبکه‌ها از طریق روش‌های یادگیری عمیق [18] و روش‌های مبتنی بر هوش مصنوعی بدون ناظر [19] امکان‌پذیر است. دستورات شبکه گمنامی به دودسته تقسیم می‌شوند که در ادامه به آن‌ها اشاره خواهیم کرد.

پورت‌های مختلفی نیز جهت برقراری ارتباط با رله تعیین می‌شود به عنوان مثال هر رله به جز پورت‌های کنترلی برای دریافت دستورات و پورت‌های داده‌ای برای تبادل داده، یک پورت مجزا برای گزارش‌های دارد. به این صورت که هر رله می‌تواند گزارش‌های خود را از طریق رله‌های میانی با ایجاد یک مدار آن‌ها را به سرویس تشخیص حملات و مدیریت خطا تحویل داده و پس از بررسی و پالایش برای مدیر شبکه گمنامی ارسال شود تا در مورد آن تصمیم‌گیری کند.

سرویس رمزنگاری شبکه: با توجه به نوع به کارگیری از سامانه گمنامی می‌توان آن را طوری طراحی کرد، که از طریق این سرویس حتی طول کلیدها و نوع الگوریتم رمزنگاری را مشخص کرد که توسط مدیر شبکه در هنگام ایجاد مدار اولیه می‌تواند تعیین شود.

2-2. پیکربندی شبکه گمنامی

هر رله در شبکه بایستی دارای یک آدرس *IP* باشد، از آنجایی که مدیر شبکه باید بتواند در صورت نیاز با رله‌ها ارتباط برقرار کند و بین مدیر و آن رله یک مدار تشکیل می‌شود.

کاربر برای اتصال به سرویس گمنامی باید با رله ابتدایی هر مدار ارتباط برقرار کند. رله خروجی در مدار وظیفه پاسخ به درخواست‌های کاربر را بر عهده دارد و بر اساس نوع درخواست پذیرفته شده از طریق رله‌های قبلی خود عمل خواهد کرد

2-3. آسیب پذیری الگوریتم های کوانتومی

جدول (3): حملات قابل اجرا در سامانه های رمزنگاری [22]

نوع رمزنگاری	حملات قابل اجرا
<i>NTRU</i>	<i>Brute force attack, attack on private key, meet in the middle attack, multiple transmission attack, lattice attack</i>
<i>CTRU</i>	<i>Brute force attack, attack on private key, meet in the middle attack, multiple transmission attack, attack on public key using Popov normal form</i>
<i>MaTRU</i>	<i>Brute force attack, meet in the middle attack, lattice attack</i>
<i>QTRU</i>	<i>Brute force attack, lattice attack, message expansion</i>
<i>NNRU</i>	<i>Brute force attack, meet in the middle attack, multiple transmission attack, lattice attack doesn't work.</i>
<i>ETRU</i>	<i>Brute force attack, attack on private key, meet in the middle attack, multiple transmission attack</i>
<i>OTRU</i>	<i>Brute force attack, meet in the middle attack, multiple transmission attack, message expansion</i>
<i>ILTRU</i>	<i>Brute force attack, attack on private key, meet in the middle attack, multiple transmission attack</i>
<i>GR-NTRU</i>	<i>Brute force attack, attack on private key, meet in the middle attack, multiple transmission attack, lattice attack</i>

ابتدا پژوهشگران برای بهبود امنیت شبکه گمنامی سیستم رمزنگاری کلاسیک *RSA* را جایگزین سیستم رمزنگاری کوانتومی *NTRU* کردند این روش دارای ضعف ها [8] و آسیب پذیری هایی بود [21] که کارایی و امنیت شبکه گمنامی را از طریق حملات موفق بسیاری که امروزه بر روی این نوع از سامانه های رمزنگاری صورت می گیرد تحت تأثیر قرار می داد [4].

علاوه بر این پژوهشگران انواع حملات قابل اجرا بر روی هر یک از سامانه های رمزنگاری کوانتومی را بررسی کرده اند که در جدول شماره (3) به طور خلاصه به آن ها اشاره شده است.

3-3. حملات کوانتومی در شبکه گمنامی

حمله *Quantum Insert* در شبکه گمنامی به تغییر مسیر داده ها در پاسخ به نتایج مربوط است [23]، نوعی دیگری از حملات مربوط به افزونه های سمت مرورگر است. علاوه بر آن از سایر حملاتی که می توان به آن ها اشاره کرد، حملات *Transmission-Time* است که از دسته حملات اثر انگشت محسوب می شوند و قابلیت حمله مردمیانی را ایجاد می کنند [24].

4-3. آسیب پذیری نسل دوم شبکه گمنامی

نسل دوم شبکه گمنامی با انجام اصلاحات عمیق ساختاری و بهبود معماری، توسط دینگلدین و همکاران [25] به کمک آزمایشگاه تحقیقات نیروی دریایی ایالات متحده توسعه پیدا کرد. معماری ارائه شده توسط آن ها در فرآیند تبادل اطلاعات و تبادل کلیدهای رمزنگاری از الگوریتم های *AES-128* برای رمزنگاری

می شوند، اگر سلول ها به طور کامل از صف مدار به بافر خروجی منتقل شوند آن مدار به صورت غیرفعال بررسی می گردد.

در هر پرش یا اصطلاحاً یک هاپ، یکپارچگی شبکه گمنامی لازم است بررسی شود. هنگامی که یک کلاینت از طریق کلید عمومی خود با یک رله جدید ارتباط برقرار می کند، به وسیله ای امضاء دیجیتال تأیید داده ها صورت می گیرد.

عملیات های شبکه گمنامی طبق جداول (1) و (2) صورت می گیرد. شناسه مدار، شناسه سلول ها و مسیرها در شبکه گمنامی توصیه می شود به نحوی تعیین و پیاده سازی شوند که از دید مرکز فرماندهی و کنترل یا یک ناظر بیرونی خاصیت پیوند ناپذیری داشته باشند.

جدول (1): بسته دستورات کنترل گره های شبکه [16]

<i>Circ ID</i>	<i>CMD</i>	<i>Data</i>
----------------	------------	-------------

جدول (2): بسته دستورات کنترل جریان داده [16]

<i>Circ ID</i>	<i>Relay</i>	<i>Stream ID</i>	<i>Digest</i>	<i>Len</i>	<i>CMD</i>	<i>Data</i>
----------------	--------------	------------------	---------------	------------	------------	-------------

3. آسیب پذیری رمزنگاری شبکه گمنامی

در بستر اینترنت، گمنامی موضوع بسیار مهمی است و به این منظور محققان انواع شبکه های گمنامی را طراحی کرده اند [4]. با ظهور پردازش های کوانتومی امنیت شبکه های گمنامی و دستگاه های رمزنگاری به کارگیری شده در آن ها با چالش های زیادی مواجه شده اند که در ادامه به برخی از آن ها اشاره خواهیم کرد [20].

3-1. شکسته شدن سامانه های رمزنگاری کلاسیک

با توسعه یافتن پردازش های کوانتومی و همچنین وقوع حملات جدید، بررسی ساختار رمزنگاری کلاسیک در شبکه های گمنامی ضروری است [20]. لزوم ارائه یک معماری مقاوم در برابر حملات کوانتومی باعث شده تا معماری رمزنگاری شبکه گمنامی بازبینی و اصلاح شود [5]. این حملات تأثیرات مخربی بر روی سامانه های رمزنگاری مبتنی بر لگاریتم گسسته و ریاضیات دارند به طوری که کلیدهای رمزنگاری به راحتی و در کسری از ثانیه از طریق فن های تجزیه اعداد قابل شکستن و شناسایی است [8].

می‌شود. این مرجع صدور گواهی مشکلاتی در توزیع سربرار محاسبات، تأیید و ابطال گواهی‌ها دارد که کیونگ با بررسی این مرجع صدور گواهی، رمزنگاری بدون گواهی را ارائه کرده است. این روش مشکل مدیریت گواهی را در رمزنگاری با کلید عمومی، و مشکل ذخیره کلید در رمزنگاری مبتنی بر هویت را حل می‌کند، در نهایت برای ارتقا روش خود نیز راهکارهایی را ارائه کرده است [29].

3-5-3. حمله مردمیانی در تبادل کلید NTRU

سیلورمن و همکاران [30] از این روش جهت نفوذ به سیستم رمزنگاری NTRU استفاده کرده‌اند. در پژوهش انجام‌شده توسط کیونگ، عملیات تبادل کلید سیستم NTRU بررسی‌شده و نتایج آن اثبات کرده است که NTRU در معرض حمله مردمیانی قرار دارد. مشابه همین آسیب‌پذیری که گفته شد در مرحله مبادله کلید الگوریتم دیفی هلمن^۲ نیز یافت شده است که با استفاده از ZKP^۳ از آن جلوگیری شده است. (در رمزنگاری روشی است که طرف (اثبات‌کننده) می‌تواند به‌طرف (تصدیق‌کننده) ثابت کند بیانیه یا گواهی ارائه‌شده صحیح است).

این روش فقط صحت بیانیه را تصدیق می‌کند و هیچ اطلاعات اضافه‌ای را به‌جز این حقیقت که بیانیه واقعاً صحت دارد ارسال نمی‌کند. ویجی کومار و همکاران [31] از طرح ZKP برای حل مشکل حمله مردمیانی در NTRU استفاده کرده‌اند و نتایج آن‌ها نشان داد که حتی با ZKP نیز NTRU بازهم در برابر حملات مردمیانی آسیب‌پذیر است.

3-5-4. حمله ترکیبی مردمیانی در NTRU

یک روش ترکیبی جدید توسط خوشنویسان و منوچهری [32] مبتنی بر حمله معروف مردمیانی جهت نفوذ به سیستم رمزنگاری NTRU ارائه شد.

این روش دارای پیچیدگی زمانی و مکانی کمتری نسبت به سایر حملات همچون روش ونگ است. با توجه به موارد گفته‌شده مبادله کلید NTRU در معرض حمله مردمیانی قرار دارد که ارائه یک‌راه حل مناسب برای جلوگیری از این حمله‌بر روی NTRU هنوز یک مشکل غیرقابل حل تا به این لحظه بوده، و همواره به‌عنوان یک تهدید بزرگ برای این سیستم رمزنگاری محسوب می‌شود. گراهام [33] از طریق دست‌کاری مقادیر NTRU و ترکیب آن با این آسیب‌پذیری یک نوع حمله ترکیبی دیگری را بر روی این سیستم رمزنگاری پیاده‌سازی کرد.

داده‌ها، الگوریتم RSA-1024 جهت رمزنگاری کلید جلسات، و از الگوریتم تبادل کلید دیفی-هلمن DH-1024 برای تبادل کلیدها به همراه تابع چکیده ساز SHA-1 استفاده کرده و برای برقراری ارتباط بین رله‌های داخل شبکه از پروتکل TLS بهره‌برداری کرده‌اند که تمامی آن‌ها جزو الگوریتم‌های رمزنگاری کلاسیک بوده و دارای آسیب‌پذیری‌های بسیاری هستند و پرداختن به آن‌ها خارج از موضوع پژوهش خواهد بود.

3-5-5. مشکلات بازطراحی شبکه گمنامی با NTRU

بازطراحی معماری نسل دوم شبکه گمنامی نخستین بار توسط کرباسی و همکاران [5] از صورت گرفت و یک معماری جدید مبتنی بر سیستم رمزنگاری NTRU و امضاء دیجیتال NSS ارائه شد. در نتیجه معماری شبکه گمنامی در برابر برخی از تهدیدات و حملات کوانتومی بهبود پیدا کرد که آسیب‌پذیری‌ها و مشکلات معماری ارائه‌شده توسط آن‌ها در ادامه بررسی می‌شود.

3-5-1. رمزگشایی ناموفق NTRU

یکی از چالش‌های NTRU این است که گاهی عملیات رمزگشایی با موفقیت انجام نمی‌شود. از روش‌های مطرح‌شده برای حل این مشکل تنظیمات مناسب و انتخاب صحیح پارامترهای رمزنگاری است. با انتخاب صحیح پارامترها و تنظیمات اولیه مناسب هنگام رمزنگاری می‌توانیم احتمال عدم موفقیت در رمزگشایی را کاهش دهیم. اکنون حملاتی که از این آسیب‌پذیری بهره‌برداری می‌کنند نشان می‌دهد روش مطرح‌شده کارایی چندانی مناسبی در عمل نداشته است و منجر به این می‌شود امنیت رمزنگاری NTRU را تحت تأثیر قرار دهد. به‌عنوان مثال در پژوهش صورت گرفته توسط گراهام و همکاران [26] تأثیر شکست‌های رمزنگاری^۱ بر امنیت رمزنگاری NTRU به‌طور دقیق بررسی‌شده و همچنین حملاتی را مطرح کرده‌اند که از این شکست‌های رمزگشایی برای بازیابی کلید خصوصی استفاده می‌کنند. در مورد این آسیب‌پذیری و بازیابی کلید خصوصی از این طریق، جان آ. پرووس [27] در دانشگاه واترلو کانادا به رمزگشایی ناقص در سیستم رمزگشایی NTRU پرداخته و یک مدل حمله‌بر روی NTRU ارائه کرده است. همچنین در پژوهش صورت گرفته توسط نیتاج [28] نیز یک حمله برای بازیابی کلیدهای خصوصی ارائه‌شده است.

3-5-2. مشکلات PKI در توزیع سربرار محاسبات

رمزنگاری NTRU

رمزنگاری کلید عمومی، نیاز به احراز هویت دارد. احراز هویت کلید عمومی توسط یک گواهی کلید عمومی صادرشده از یک مرجع صدور گواهی در زیرساخت کلید عمومی (PKI) انجام

² Diffie-Hellman

³ Zero Knowledge Proof

¹ Decryption Failure

3-5-4. حملات پخشی بر روی NTRU

نوع دیگری از حملات بر روی این سیستم رمزنگاری، حملات پخشی^۱ نام دارد که برای اولین بار توسط آستاد [32] مطرح شد. این نوع حمله مهاجم را قادر می‌سازد تا پیام ارسال شده توسط فرستنده را بازیابی کرده و آن را به چندین گیرنده تحویل دهد. دینگ و همکاران [34] یک حمله پخشی توسعه یافته دیگری به نام حملات پخشی جبر^۲ ابداع کردند. این حمله یک پیام واحد را که چندین مرتبه با استفاده از کلیدهای عمومی NTRU رمزنگاری شده، بازیابی می‌کند.

3-5-5. الگوریتم رمزگشایی BDD

نقاط ضعف موجود در رمزنگاری NTRU سبب شد یک الگوریتم رمزگشایی کارآمد به نام BDD^۳ [30] پیاده‌سازی و برای حمله به رمزنگاری NTRU استفاده شود.

3-5-6. حمله بازیابی پیام

از دیگر حملاتی که اخیراً بر روی سیستم رمزنگاری NTRU منتشر شده است، حمله بازیابی پیام^۴ است که عملکرد آن توسط ماریوس [35] توصیف گشته و در نهایت موفقیت حمله اثبات شده است.

4. بهبود شبکه گمنامی

در بخش گذشته به ضعف‌های سیستم رمزنگاری شبکه‌های گمنامی اشاره کردیم. در این قسمت معایب معماری شبکه گمنامی را بر اساس پژوهش صورت گرفته توسط دینگلدین [36] بررسی کرده و در ادامه به ارائه راهکارهایی برای افزایش سرعت و بهبود شبکه گمنامی خواهیم پرداخت.

کنترل ازدحام: ازدحام را می‌توان از طریق به‌کارگیری یک پروتکل غیرقابل اعتماد مانند UDP برای پیوند های مابین رله‌های شبکه گمنامی بهبود بخشید. روش پیشنهادی دیگر برای کنترل ازدحام^۵ در شبکه گمنامی به‌کارگیری پروتکل PCTCP است که توسط گلدبرگ [37] طراحی شده است و امنیت شبکه را از طریق پروتکل IPSec تأمین می‌کند. یک راه حل دیگر مهار کردن پروتکل‌هایی است که پهنای باند زیادی را در شبکه درخواست می‌کنند.

ظرفیت شبکه: طبق پروژه متریک [38] دانلود یک مگابایت در شبکه تر حدود 6 ثانیه طول می‌کشد. با توجه به این که ترافیک از

چندین رله عبور می‌کند مقدار کل داده‌های منتقل شده در شبکه چند برابر شده و پهنای باند استفاده شده در شبکه افزایش می‌یابد که در این حالت با داشتن n گره در مدار مقدار ترافیک منتقل شده در $(n+1) * 2$ ضرب می‌شود. از آنجایی که در معماری کلاسیک شبکه گمنامی به‌طور پیش‌فرض از 3 رله استفاده می‌شود که یک تبادل داده 1 گیگابایتی در آن منجر به هزینه‌ای برابر 8 گیگابایت می‌شود که با افزایش گره‌های مسیریاب در شبکه ظرفیت آن‌ها نیز باید افزایش پیدا کند.

انتخاب مسیر: الگوریتم انتخاب مسیر بار شبکه را به‌طور یکنواخت نمی‌تواند توزیع کند. در این حالت استفاده از یک الگوریتم مسیریابی بهتر می‌تواند ظرفیت کلی شبکه را افزایش دهد. آخرین پژوهش صورت گرفته در این زمینه الگوریتم طراحی شده در دانشگاه شیکاگو است که با ترکیب معیارهای مختلف، فرآیند انتخاب مسیر بین گره مبدأ و مقصد را انجام می‌دهد [39]، که پس از آن پژوهش حسینیان [40] به‌طور کامل به ارزیابی و تفسیر الگوریتم مسیریابی شبکه تر پرداخته است.

مدیریت تأخیر و خطاهای اتصال: کلاینت‌های شبکه گمنامی در مدیریت تأخیر و خرابی‌های اتصال عملکرد مناسبی ندارند. در صورتی که گسترش مدار با شکست مواجه شود کل مدار رها می‌شود. بر اساس ساختار شبکه گمنامی پیشنهادی می‌توان طوری شبکه را پیکربندی کرد که در صورت عدم موفقیت تشکیل مدار و یا خرابی آن ارتباط از طریق مسیر دیگری برقرار شود یا از طریق مرکز فرماندهی و کنترل مدیریت شود که مدیر شبکه نسبت به هرگونه اختلال در کمترین زمان آگاهی پیدا کند.

بارگیری داده‌ها از سرورهای دایرکتوری: بسیاری از هزینه‌های بالای شبکه گمنامی حاصل دانلود اطلاعات توسط کلاینت‌ها از سرورهای دایرکتوری و سربرار اتصالات TLS بین گره‌های شبکه است. طبق گفته دینگلدین حذف رکورد خالی برنامه TLS می‌تواند سربرار هدر TCP/IP را تا 6/3 درصد کاهش دهد. جایگزینی این مرجع مرکزی با یک جزء غیرمتمرکز در شبکه می‌تواند سربرار شبکه را کاهش دهد و عملکرد آن را تا حدودی بهینه کند و به این معنی است که ما بیشتر دوست داریم ساختار شبکه گمنامی را غیرمتمرکز ببینیم. ساختار غیرمتمرکز دارای مشکلات خاص خود است. اگرچه تحقیقات زیادی در مورد تمرکززدایی شبکه گمنامی صورت گرفته است و به‌عنوان یک موضوع مهم مطرح است اما هنوز استفاده از روش‌های متمرکز مناسب‌تر است که معایب نبود سرورهای دایرکتوری را تشریح کردیم.

¹ Broadcast Attack² Algebra Broad Cast Attack³ Bounded Distance Decoding⁴ Message Recovery Attack⁵ Congestion Control

$QTRU$ عمل می‌کند. در نهایت با در نظر گرفتن قدرت امنیتی و محاسبات پیچیده‌تر به لحاظ امنیتی عملکرد بهتری دارد [6].

جدول (4): مقایسه پیچیدگی الگوریتم‌های رمزنگاری [43]

شماره	رمزگشایی	رمزنگاری	کلید	الگوریتم
1	$2\dot{C}$ and $1A$	$1\dot{C}$ and $1A$	$1\dot{C}$	$NTRU$
2	$16\dot{C}$ and $1A$	$8\dot{C}$ and $1A$	$8\dot{C}$	$BITRU$
3	$24\dot{C}$ and $4A$	$8\dot{C}$ and $4A$	$8\dot{C}$	$BOTRU$
4	$32\dot{C}$ and $12A$	$16\dot{C}$ and $8A$	$16\dot{C}$	$BCTRU$
5	$32\dot{C}$ and $4A$	$16\dot{C}$ and $4A$	$16\dot{C}$	$QTRU$
6	$64\dot{C}$ and $4A$	$32\dot{C}$ and $4A$	$32\dot{C}$	$PQTRU$
7	$45\dot{C}$ and $6A$	$18\dot{C}$ and $6A$	$36\dot{C}$	$NTRS$
8	$189\dot{C}$ and $6A$	$18\dot{C}$ and $6A$	$54\dot{C}$	$NTRSH$
9	$1024\dot{C}$ and $8A$	$64\dot{C}$ and $8A$	$64\dot{C}$	$OTRU$
10	$96\dot{C}$ and $8A$	$6\dot{C}$ and $8A$	$64\dot{C}$	$NTRTE$
11	$256\dot{C}$ and $8A$	$64\dot{C}$ and $8A$	$64\dot{C}$	$QOBTRU$
12	$1088\dot{C}$ and $4A$	$80\dot{C}$ and $4A$	$80\dot{C}$	$QMNTR$
13	$38\dot{C}$ and $8A$	$32\dot{C}$ and $8A$	$80\dot{C}$	$QOTRU$
14	$1536\dot{C}$ and $16A$	$17\dot{C}$ and $16A$	$17\dot{C}$	$TOTRU$
15	$4096\dot{C}$ and $16A$	$256\dot{C}$ and $16A$	$256\dot{C}$	$HXDTRU$

جدول (4) جزئیات الگوریتم‌های کوانتومی را به‌طور خلاصه نشان می‌دهد که $\dot{C}$ میزان پیچیدگی ضرب کانولوشن و A میانگین جمع چندجمله‌ای فرآیند رمزنگاری و رمزگشایی الگوریتم را نشان می‌دهد. در این جدول پیچیدگی تولید کلید رمزنگاری و رمزگشایی، به ترتیب از پایین به بالا مرتب‌شده است. منطقی است که با افزایش پیچیدگی الگوریتم، امنیت آن بهبود پیدا کرده است، اما سرعت فرآیند رمزنگاری و رمزگشایی کاهش پیدا می‌کند [43].

به‌کارگیری $QMNTR$ با توجه به ارث‌بری ویژگی‌های مثبت و قدرت سیستم رمزنگاری $NTRU$ و دیگر دستگاه‌هایی نظیر $QTRU$ به همراه مقاومت بالا و مناسب در برابر حملات کوانتومی همچنین به خاطر سنگین‌تر بودن محاسبات به‌کاررفته در سیستم رمزنگاری در مقایسه با سامانه‌های رمزنگاری دیگر به همراه کاربردهای عام دیگر این سیستم رمزنگاری شامل به‌کارگیری در رای‌گیری الکترونیکی و تراکنش‌های مالی و به‌طور کلی برنامه‌هایی که به‌صورت هم‌زمان و توزیع‌شده از چندین منبع استفاده می‌کنند، می‌تواند کارایی مناسبی داشته و آن را از دیگر سامانه‌های رمزنگاری متمایز کند.

5. معرفی رمزنگاری $QMNTR$ و امضاء LRS

سیستم رمزنگاری $NTRU$ به‌وسیله جبر کوآترنیونی^۱ با جایگزینی حلقه اصلی در $NTRU$ بهبود پیدا کرد و ساختار جدیدی به نام $QTRU$ معرفی شد که یک سیستم رمزنگاری چندبعدی است. $QMNTR$ نیز بهبودیافته $QTRU$ بوده که با استفاده از یک ساختار ریاضی جدید با دو کلید عمومی و پنج کلید خصوصی طراحی شده است، که این اصلاح سیستم کلید عمومی را قوی‌تر و ایمن‌تر کرده است. حسن یاسین [6] بر اساس یک ساختار ریاضی جدید با به‌کارگیری جبر کوآترنیونی، $QTRU$ را بهبود داده و آن را $QMNTR$ نامیده است، و اثبات آن نشان می‌دهد که سیستم رمزنگاری $QMNTR$ از $QTRU$ هم ایمن‌تر است. $QTRU$ یکی از توسعه‌های ابتدایی سیستم $NTRU$ بود که توسط ملکیان و همکاران [41] طراحی، و ابداع شد.

سپس یک سیستم رمزنگاری کلید عمومی غیر انجمی با سرعت بالا به نام $OTRU$ پیاده‌سازی کردند [42]. این سیستم رمزنگاری با سرعت بالا هشت بردار داده را به‌صورت موازی در هر دور رمزنگاری می‌کند. $OTRU$ اولین قدم در طراحی سامانه‌های رمزنگاری کلید عمومی با جبر غیر انجمی بود که توانست به‌عنوان نقطه شروعی برای طراحی سایر سامانه‌های رمزنگاری غیر انجمی با ساختار جبری متفاوت و ویژگی‌های بهتر شود. $NTRU$ به 4 پارامتر که اعداد صحیح بودند بستگی داشت، که هرکدام از پارامترهای عمومی آن تعریف خاص خود را دارد. این پارامترها در رمزنگاری $QMNTR$ به 8 پارامتر افزایش پیدا کرده‌اند. لازم به ذکر است سیستم رمزنگاری $QMNTR$ بهبودیافته سیستم $QTRU$ است. در رابطه شماره (2) سطح امنیتی کلیدهای رمزنگاری این دو سیستم، با در نظر گرفتن پارامترهای عمومی آن‌ها مقایسه شده است [6].

$$QMNTR \left(\frac{N!}{(d_g!)^2 (N-2d_g)!} \right)^4 \left(\frac{N!}{(d_u!)^2 (N-2d_u)!} \right)^4 \left(\frac{N!}{(d_s!)^2 (N-2d_s)!} \right)^4$$

$$QTRU \left(\frac{N!}{(d_g!)^2 (N-2d_g)!} \right)^4 \quad (2)$$

رابطه فوق جهت تخمین امنیت و احتمال موفقیت حملات، ارائه شده است که هر یک از عبارات به‌طور خلاصه یک فضای جستجو خاص را برای تخمین تعداد حالات یا گزینه‌های ممکن نشان می‌دهند. با توجه به ضرایب این دو سیستم رمزنگاری، سطح امنیتی کلید رمزنگاری $QMNTR$ سه برابر $QTRU$ بوده و سطح امنیت پیام در $QMNTR$ دو برابر $QTRU$ است. $QMNTR$ از نظر سرعت با توجه به جدول شماره (4) کمی ضعیف‌تر از

¹ Quaternion Algebra

محاسبات سیستم رمزنگاری به قدرت پردازش قابل توجهی نیاز دارد که امروزه با افزایش توان محاسبات سامانه‌های پیشرفته امکان پردازش داده‌ها تا سطوح بسیار بالایی امکان پذیر است.

موفقیت آمیز نبودن عملیات رمزگشایی در برخی از حالت‌های خاص سیستم رمزنگاری *NTRU* یکی از چالش‌های مطرح شده این سیستم رمزنگاری است که راه حل مناسبی تاکنون برای آن ارائه نشده است.

پژوهشگران از این آسیب پذیری برای بازیابی کلیدهای خصوصی و طراحی انواع حملات بر روی *NTRU* استفاده کرده‌اند که به آن اشاره شد و در صورت استفاده از آن در شبکه گمنامی می‌تواند تهدید بزرگی برای امنیت و کارایی شبکه محسوب شود.

طراحی شبکه گمنامی پیشنهادی ضمن حل مشکلات مطرح شده، گمنامی را تا سطوح بسیار بالایی تضمین خواهد کرد. بهبود بخش آسیب پذیر پروتکل توزیع کلید با کارگیری امضاء دیجیتال *LRS* در رمزنگاری *QMNTR* و استفاده آن در شبکه گمنامی پیشنهادی، روش جدیدی بوده که تاکنون پیاده سازی نشده و علاوه بر آن تا به این لحظه هیچ گونه آسیب پذیری خاصی نیز در خصوص معماری پیشنهادی منتشر نشده است.

6. تشریح و پیاده سازی روش پیشنهادی

در این بخش مطابق با معماری رمزنگاری شبکه گمنامی ساختار جدیدی پیشنهاد داده ایم. در روش پیشنهادی سیستم رمزنگاری *QMNTR* جایگزین *NTRU* خواهد شد که امضاء دیجیتال *LRS* در کنار آن به کارگیری می‌شود. بنابراین شبکه گمنامی طراحی شده علاوه بر نداشتن آسیب پذیری‌های رمزنگاری *NTRU* در برابر حملات جدید کامپیوترهای کوانتومی نیز مقاومت بسیار بالایی خواهد داشت.

6-1. به کارگیری امضاء دیجیتال *LRS* در کنار

سیستم رمزنگاری *QMNTR*

مشابه آنچه توسط کینگ پیاده سازی شده بود [7]، طرح امضاء دیجیتال *LRS* را می‌توان مانند دیگر طرح‌های امضاء دیجیتال [46] بر مبنای سیستم رمزنگاری *QMNTR* پیاده سازی کرد که در مرحله تولید کلید، سیستم رمزنگاری *QMNTR* و امضاء دیجیتال *LRS* هر دو بتوانند از یک کلید عمومی یکسان استفاده کنند. بر اساس این روش می‌توان حجم محاسبات در شبکه گمنامی را کاهش داد. کینگ و همکاران خود اثبات کارایی و امنیت طرح خود را بر اساس مدل امنیتی *UALRS* ارزیابی کرده‌اند که این مدل توسط *Liu* [7] ارائه شده است.

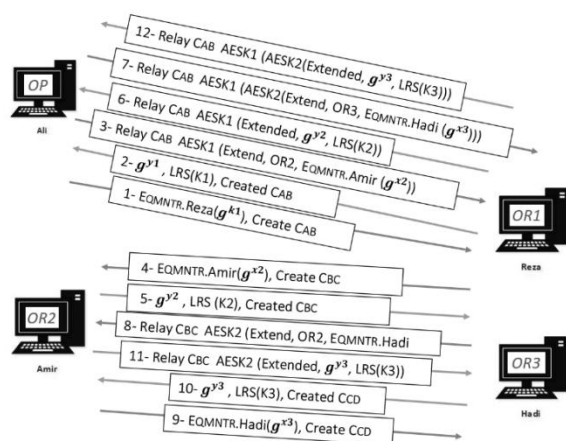
همان طور که می‌دانیم نحوه رمزنگاری در شبکه‌های ترکیبی^۱ به صورت لایه‌ای بوده که معماری ابتدایی تر نیز این گونه است. روش پیشنهادی ما نیز مانند معماری پایه شبکه‌های گمنامی پیاده سازی می‌شود. در معماری شبکه کلاسیک تر امنیت بیشتر بر اساس تعداد لایه‌ها بیان می‌شد و اکثر ارزیابی‌های امنیتی بر مبنای حداقل و حداکثر لایه‌های ارتباطی مورد نیاز بود. در روش پیشنهادی علاوه بر ویژگی‌های فوق بر روی جنبه‌های دیگری مانند مقاومت در مقابل حملات کوانتومی و ارتقا امنیت سیستم توزیع کلید و رمزنگاری تأکید خواهیم کرد. به طور کلی با پیاده سازی رمزنگاری *QMNTR* و نسل‌های آینده این نوع از سامانه‌های رمزنگاری در ساختارهای گمنام ساز مبتنی بر شبکه می‌توان گام مهمی در راستای ارتقا این نوع شبکه‌ها برداشت.

کینگ و همکارانش برای کاهش سایز امضاء، ارتقای کارایی تولید امضاء و تأیید طرح *UALRS* [44] مبتنی بر شبکه‌ها در مطالعات صورت گرفته و آزمایش‌ها انجام شده یک طرح *LRS* مبتنی بر *NTRU* طراحی کردند که معماری آن در [7] توضیح داده شده است. پژوهشگران از طریق بررسی طرح‌های احراز هویت مختلف مبتنی بر مسائل فاکتورگیری اعداد صحیح بزرگ و لگاریتم گسسته، دریافتند که این دسته از طرح‌های احراز هویت در برابر حملات کوانتومی مقاومت کافی را ندارند، لذا بایستی به انتخاب و پیاده سازی طرح‌های ایمن تر که مقاومت مناسبی در برابر حملات کوانتومی دارند بپردازند [45].

امضاء دیجیتال *LRS* ناشناسی بدون قید و شرط را برای ما فراهم می‌کند و به کار بردن آن به جای توابع چکیده ساز، بسیار ایمن تر خواهد بود، که بسیاری از مشکلات امضاءهای حلقه معمولی را حل خواهد کرد. ناشناسی یا گمنامی بدون قید شرط بدین معنی است با فرض وجود 1 کاربر در *RS* احتمال وجود هر دشمنی با قدرت محاسباتی و زمان نامحدود، به درستی نشان داده شود. طراحی یک *RS* با ناشناسی بدون قید و شرط کار دشواری نیست.

در واقع اکثر طرح‌های سنتی *RS* می‌تواند ناشناسی بدون قید و شرط را برآورده کنند. این طرح امضاء دیجیتال احراز هویت سریع می‌تواند به عنوان یک مکمل برای بهبود امنیت سیستم رمزنگاری *QMNTR* پیاده سازی شود و از کلیدهای عمومی و خصوصی آن استفاده کند که از ویژگی‌های مهم آن می‌توان به جعل ناپذیری، نداشتن *Trap door* و امکان به کارگیری در سامانه‌های رمزنگاری مختلف اشاره کرد. در نهایت با به کارگیری امضاء دیجیتال *LRS* و احراز هویت داده‌های تبادل شده مهاجم داخل شبکه نمی‌تواند پیام‌ها و داده‌های جعلی خود را به کلاینت ارسال کند. در این حالت با احراز هویت داده‌های تبادل شده پیچیدگی بار محاسباتی که به کل شبکه اضافه می‌شود در کنار

¹ Mix Network



شکل (2): مراحل توزیع کلید و ارسال پیام در شبکه

پس از آن که اطلاعات مجموعه کلیدهای مسیر در اختیار علی قرار گرفت، مرحله تولید کلید جلسه آغاز می‌شود، لازم به ذکر است که این کلید صرفاً برای استفاده در همان مدار بوده و برای رمزنگاری در همان جلسه و نشست به کار می‌رود. در معماری جدید پیشنهادی ارائه شده برای انتقال نیمه کلید مورد نظر در پروتکل توافق دیفی-هلمن لازم است تا نیمه کلید رمز شود، در این ساختار نیمه کلید اول توسط *QMNT* رمز شده و نیمه کلید بعدی و همچنین کلید نهایی در سمت گره مقصد در آخر ایجاد می‌شود که با روش *LRS* امضاء شده و به مبدأ بازمی‌گردد. در نهایت پس از انتقال درست اطلاعات و بررسی آن در شبکه طبق معماری شبکه گمنامی کلیدهای $K1$ تا $K3$ تشکیل می‌شوند که همان کلیدهای جلسه و نشست در گره‌های میانی به شمار می‌روند. با توجه به این که ساختار توزیع کلید دیفی-هلمن از سیستم هشینگ قوی برای تبادل کلید استفاده می‌کند توافقات به صورتی تعیین می‌شود که در سراسر شبکه یکپارچگی حفظ گردد. امنیت پروتکل دیفی-هلمن مبتنی بر دشواری حل مسئله لگاریتم گسسته است که باید مواردی در ارتباط با امنیت این پروتکل لحاظ گردد. در این خصوص در بخش سوم به آسیب‌پذیری‌های سامانه‌های رمزنگاری مبتنی بر لگاریتم گسسته اشاره کردیم.

در صورتی که تحت شرایط خاصی این الگوریتم به کارگیری نشود شکستن امنیت این پروتکل و یافتن کلید رمز مشترک با استفاده از الگوریتم‌هایی مانند پولیگ - هلمن نسبتاً آسان و در زمان کوتاهی قابل انجام خواهد بود [48]. به‌تازگی پژوهشگران حوزه رمزنگاری اقدام به پژوهش بر روی الگوریتم‌های تبادل کلید کوانتومی کرده، که هنوز قابلیت به کارگیری، مانند سامانه‌های رمزنگاری کوانتومی، به صورت عمومی را ندارند و به عنوان حوزه پژوهشی بسیار جدیدی مطرح شده‌اند [49,50].

در نهایت طرح *LRS* مبتنی بر *QMNT* را نیز هم می‌توان از همان روش اثبات کرد. نتایج اثبات شده توسط کینگ و همکاران او نشان داد که طرح پیشنهادی آن‌ها ناشناسی بدون قید و شرط را برآورده می‌کند. همچنین جدیدترین و کارآمدترین طرح‌های امضاء توسط کینگ و همکاران او مورد تحلیل و بررسی قرار گرفته که این طرح عملکرد مناسب‌تری را نسبت به دیگر پژوهش‌های انجام شده در این حوزه به خود اختصاص داده است [44,47].

در ادامه با طراحی مجدد معماری شبکه گمنامی، جایگاه این دو فن را در سیستم رمزنگاری مشخص خواهیم کرد. لازم به ذکر است نحوه تولید کلیدها و فرآیند رمزنگاری و رمزگشایی سیستم رمزنگاری *QMNT* در [6] آمده است. در این معماری امضاء دیجیتال *LRS* به دلیل توانایی‌های امنیتی بهتر، جایگزین بسیار مناسبی برای روش *NSS* بوده که می‌تواند امنیت ایجاد کلید جلسه و انتقال امن کلید را ارتقا دهد و غیر از محرمانگی کلید، هویت دارنده کلید، جعل ناپذیری، هویت پیام، یکپارچگی پیام، عدم انکار در ارتباطات و مهم‌تر از همه ناشناسی بدون قید و شرط را فراهم کند که نسبت به طرح پیشین خود یعنی *NSS* بسیار قوی‌تر است.

6-2. بهبود پروتکل توزیع

برای ارتقاء شبکه گمنامی از آخرین و قوی‌ترین فن‌های موجود جهت بهبود قسمت‌های آسیب‌پذیر خصوصاً پروتکل توزیع کلید استفاده می‌شود، که این بهبود در این بخش از طریق پیاده‌سازی معماری پیشنهادی صورت می‌گیرد.

علی به عنوان گره آغازین و ارسال‌کننده داده در شبکه گمنامی کار خود را شروع می‌کند، در ابتدا لازم است تا برای شروع ارتباط گمنام کلیدهای عمومی گره‌های میانی مدار را به دست آورد تا بتواند به صورت لایه‌ای اطلاعات را با الگوریتم *QMNT* رمز کرده و به مقصد برساند. مسیرها از طریق *CircID* مشخص می‌گردند که در انتقال از هر لایه به لایه دیگر به سلول‌ها نیز تعلق گرفته تا داده‌ها به صورت گمنام تبادل شوند، طبق شکل (2) از علی به هادی مسیرهای *CAB*، *CBC* و *CCD* تشکیل و کلیدهای عمومی گره‌های میانی نیز از طریق الگوریتم *QMNT* تولید شده‌اند. برای انتقال امن اطلاعات شبکه باید حداقل دارای 3 گره میانی باشد.

مثال مطرح شده صرفاً برای تشریح عملکرد شبکه گمنامی با 2 گره صورت گرفته است که در شکل (2) هادی را رله خروجی در نظر می‌گیریم. اطلاعات بایستی به صورت بسته‌هایی از داده مرحله به مرحله ارسال شود و ترتیب ارسال نیز بر اساس قوانین شبکه گمنامی به انجام می‌شود.

است. رضا با کلید $K1$ اطلاعات لایه اول را رمزگشایی کرده و می‌داند که بسته باید برای امیر ارسال شود اما محتویات بسته را نمی‌داند چون از کلید جلسه‌ی $K2$ اطلاعی ندارد. همچنین امیر بسته را با کلید جلسه‌ی $K2$ رمزگشایی کرده و می‌داند بسته‌ای باید به هادی برسد. این تنها نمونه‌ای از نحوه رمزنگاری لایه‌ها و پروتکل‌های استفاده‌شده است که در دولایه میانی طراحی‌شده است. برای حفظ امنیت سیستم لازم است لایه‌ها به حداقل 3 لایه انتقال یابد که باعث افزایش مراحل خواهد شد. دستوره‌های به‌کاررفته در هر مرحله به شرح شکل شماره (2) است، که ارسال بسته داده از گره شماره 1 (علی) به گره شماره 4 (هادی) را توسط 2 گره میانی، از طریق پروتکل اصلاح‌شده شبکه گمنامی را نشان می‌دهد. پس از دریافت بسته (توافق نیمه کلید) توسط هادی، آخرین کلید نیز تولیدشده و همین مراحل رو به عقب اجرا می‌شوند، نهایتاً در مرحله‌ی دوازدهم کلیدهای $k1$ تا $k3$ توافق شده و می‌توان تبادل داده، و اجرای دیگر دستورات را از طریق شبکه گمنامی اصلاح‌شده آغاز کرد.

با افزایش تعداد گره‌های مسیر ارتباطی، تنها مجموع پردازش‌ها در شبکه گمنامی بیشتر می‌شود و تغییری در ماهیت و روش‌های رمزنگاری یادشده، انجام نخواهد شد. دستورات به‌کاررفته در مثال مطرح‌شده به ترتیب به‌صورت زیر است.

- 1- $E_{QMNT, Reza}(g^{x1}), Create C_{AB}$
- 2- $g^{y1}, LRS(K1), Created C_{AB}$
- 3- $Relay C_{AB} AESK1 (Extend, OR2, E_{QMNT, Amir}(g^{x2}))$
- 4- $E_{QMNT, Amir}(g^{x2}), Create C_{BC}$
- 5- $g^{y2}, LRS(K2), Created C_{BC}$
- 6- $Relay C_{AB} AESK1 (Extended, g^{y2}, LRS(K2))$
- 7- $Relay C_{AB} AESK1 (AESK2(Extend, OR3, E_{QMNT, Hadi}(g^{x3})))$
- 8- $Relay C_{BC} AESK2 (Extend, OR2, E_{QMNT, Hadi}(g^{x3}))$
- 9- $E_{QMNT, Hadi}(g^{x3}), Create C_{CD}$
- 10- $g^{y3}, LRS(K3), Created C_{CD}$
- 11- $Relay C_{BC} AESK2 (Extended, g^{y3}, LRS(K3))$
- 12- $Relay C_{AB} AESK1 (AESK2(Extended, g^{y3}, LRS(K3)))$

7. تجزیه و تحلیل روش پیشنهادی

همواره دغدغه طراحان و کاربران سامانه‌های گمنامی این بوده است که سامانه گمنامی مورد استفاده و طراحی‌شده بتواند سطح امنیتی قابل قبولی را ارائه کند. پژوهشگران این حوزه نیز به این بخش از مطالعات در مورد شبکه‌های گمنامی آن‌طور که شایسته است به آن نپرداخته‌اند. به‌غیراز روش محاسبه درجه گمنامی، تنها کار پژوهشی صورت گرفته در این خصوص مرتبط می‌شود به مقاله استیون مرداک [51] که نتایج او نشان می‌دهد توسعه‌ی انواع روش‌های اندازه‌گیری میزان گمنامی ارائه‌شده و به‌کارگیری معیارهای بهتر جهت ارزیابی سامانه‌های گمنامی اهمیت بالایی دارد، که تاکنون روش جامع و دقیقی در این حوزه ارائه نشده است.

به‌کارگیری رمزنگاری کوانتومی در رمزنگاری داده‌های تبادل شده نیز تا به این لحظه میسر نبوده و صرفاً می‌توان کلیدهای یک ارتباط را از طریق آن‌ها رمز کرده و امنیت کلیدهای رمزنگاری را از آن طریق ارتقاء داد. انتظار می‌رود در آینده‌ای بسیار نزدیک روند تکاملی موارد گفته‌شده به‌سرعت طی شود و به‌صورت عملی مورد استفاده قرار گیرد. مسئله مهم دیگری که مطرح است این است که امضاء دیجیتال NSS یک روش احراز هویت و امضاء دیجیتال مکمل سیستم رمزنگاری کلید عمومی $NTRU$ بود.

از آنجایی که LRS نیز پس‌از آن برای $NTRU$ طراحی‌شده است، ضروری است جهت به‌کارگیری LRS برای سیستم رمزنگاری $QMNT$ ملاحظات خاصی در نظر گرفته شود تا بتوانیم از این دو فناوری در کنار یکدیگر استفاده کنیم، که به آن اشاره کردیم. پس از توزیع درست کلید در شبکه گمنامی اطلاعات با الگوریتم ایمن AES رمز می‌شوند. در این معماری برای افزایش ضریب امنیتی الگوریتم AES از نوع 256 بیتی آن استفاده‌شده است. همان‌طور که می‌دانیم لایه‌های بیشتر در شبکه گمنامی می‌تواند ضریب امنیت را به‌صورت نمایی بالا ببرد، که در اینجا نشان‌دهنده اهمیت توزیع امن کلید در لایه‌های شبکه گمنامی است. در نهایت همان‌طور که شبکه گمنامی در برابر حملات کوانتومی بایستی مقاومت کافی داشته باشد با اصلاح کلی معماری شبکه گمنامی از طریق پیاده‌سازی طرح LRS مبتنی بر $QMNT$ امنیت شبکه گمنامی تا سطوح بسیار بالایی قابل تضمین خواهد بود.

6-3. مراحل رمزنگاری شبکه گمنامی پیشنهادی

مراحل رمزنگاری همواره بر مبنای معماری شبکه گمنامی در هر اصلاحی ثابت خواهد بود به این صورت که مطابق با روش‌های پیشین در مرحله اول با توجه به شکل شماره (3) ابتدا علی درخواست خود، مبنی بر ساخت کلید جلسه با رضا را به او ارسال می‌کند. این درخواست شامل یک‌نیمه کلید است که توسط کلید عمومی رضا و با رمزنگاری $QMNT$ رمز شده است. انتقال اطلاعات در نهایت صورت گرفته و در گره رضا رمزگشایی می‌شود. در مرحله دوم رضا در پاسخ کلید نهایی را تولید کرده و با روش LRS امضاء نموده و آن را به علی ارسال می‌نماید. در این مرحله کلید جلسه‌ی $K1$ (ارتباط بین علی و رضا) تولید می‌گردد.

همین روند در مرحله سوم توسط علی اما برای توافق کلید با امیر انجام می‌شود. نکته مهم این است که اطلاعات موردنظر توسط کلید عمومی امیر رمز شده و با انتقال اطلاعات از مسیر رضا، برای وی قابل‌رؤیت نیست. در مرحله چهارم، پنجم و ششم تشکیل کلید جلسه‌ی $K2$ (ارتباط بین علی و امیر) ایجاد می‌شود. در مرحله‌ی هفتم نیز نیمه کلید توافقی با هادی ارسال خواهد شد. توجه کنید که برای گذر از هر لایه (یعنی رضا و امیر) یک مرحله رمزنگاری و رمزگشایی با الگوریتم $AES-256$ فراهم‌شده

انجام دهد، می‌تواند خود را به‌عنوان یکی از رله‌های شبکه معرفی کند.

در این حالت در وهله اول مهاجم باید از طریق تحلیل شبکه الگوریتم کاری آن را پیدا کرده و سپس اقدام لازم را انجام دهد که کاری پیچیده، سخت، و غیرممکن خواهد بود و روش ما در برابر موارد گفته‌شده مقاومت کافی را دارد.

7-2. بهبود درجه گمنامی

درجه گمنامی دستگاهی است که در اجلاس فناوری افزایش حریم خصوصی (*PET*) در سال 2002 پیشنهاد شد. دو مقاله ایده اصلی استفاده از آنتروپی را به‌عنوان مبنایی برای اندازه‌گیری رسمی ناشناسی مطرح کردند که این ایده‌های ارائه‌شده با تفاوت‌های بسیار جزئی در تعریف نهایی درجه گمنامی بسیار مشابه یکدیگر بودند [52]. درجه گمنامی علاوه بر سامانه‌های گمنامی، امروزه معیاری برای اندازه‌گیری در حوزه‌هایی نظیر حریم خصوصی، بلاک چین، ارز دیجیتال، و... نیز است که در ادامه به آن بیشتر اشاره خواهیم کرد.

در حالت کلی حملات مختلفی بر روی معماری و ساختار شبکه گمنامی تأثیرگذار هستند، از آنجایی که بسیاری از آسیب‌پذیری‌ها در شبکه گمنامی ناشی از ضعف الگوریتم‌های رمزنگاری است، استفاده از یک ساختار رمزنگاری ایمن و قدرتمند باعث ارتقاء درجه گمنامی و بهبود امنیت خواهد شد.

با توجه به آسیب‌پذیری‌های گفته‌شده در خصوص معماری روش‌های پیشین که از طریق پردازش‌های کوانتومی و موارد دیگر مورد مخاطره قرار می‌گرفتند، تحلیل مستقیم پروتکل می‌تواند به‌صورت عملی قابل انجام باشد. هرگونه شکست در گمنامی یا کاهش درجه گمنامی از طریق تحلیل مستقیم پروتکل، کاملاً وابسته به معماری امنیتی مورداستفاده در ساختار شبکه گمنامی است که روش ما در برابر این شکست مقاومت بسیار بالایی از خود نشان می‌دهد. در اکثر سناریوهای مربوط به انتقال داده از جمله بلاک چین، محاسبات ابری و *Edge Computing* فرستنده داده معمولاً می‌خواهد ناشناس باشد درحالی‌که برای گیرنده قابل‌اعتماد بودن داده‌ها اهمیت دارد. امضاء دیجیتال *LRS* یک فناوری خوبی است که ضمن برآوردن الزامات فوق می‌تواند به بهبود درجه گمنامی یک رابطه کمک کند. درجه گمنامی تنها معیار رسمی ارائه‌شده تا به این لحظه برای اندازه‌گیری میزان گمنامی یک عضو از میان یک مجموعه است. مفهوم درجه گمنامی به‌صورت یک طیف برای تمامی انواع گمنامی قابل‌تعریف بوده که از اصل آنتروپی نظریه اطلاعات در یک توزیع احتمال بهره می‌برد و بر اساس احتمالاتی که مهاجم پس از مشاهده سیستم به کاربران تخصیص می‌دهد محاسبه

مرداک صرفاً به شناخت و تبیین اهمیت این موضوع پرداخته و خود او نیز راه‌حل مناسبی ارائه نکرده است. طبق بررسی‌های انجام‌گرفته، برای ارزیابی امنیتی سامانه‌های گمنامی هنوز معیار ثابت و مشخصی ارائه نشده که بتوانیم به‌صورت عملیاتی آن را به‌کارگیری کنیم. از طرفی دیگر هر شبکه گمنامی اجزا و مؤلفه‌های خاص خود را دارد که ارائه یک معیار مشخص برای اندازه‌گیری سطح امنیتی آن، ارزیابی شبکه گمنامی را پیچیده‌تر می‌کند و می‌توان آن را به‌عنوان یک چالش در حوزه شبکه‌های گمنامی بررسی کرد. در روش پیشنهادی علاوه بر مبدأ و مقصد ارتباط، داده‌های تبادل شده نیز غیرقابل‌شناسایی هستند که در ادامه این بخش نتایج کلی حاصل از ارزیابی سامانه گمنامی پیشنهادی بررسی و در حد امکان با پژوهش‌های مرتبط مقایسه خواهد شد.

7-1. تحلیل روش پیشنهادی در برابر حملات تأثیرگذار بر روی تبادل کلید

در این بخش، مقاومت روش پیشنهادی در برابر چند حمله مهم، که بیشترین اثرگذاری را بر روی فرآیند توزیع و تبادل کلید در شبکه گمنامی دارند، بررسی‌شده است. طبق مطالعات صورت گرفته بر روی پژوهش‌های انجام‌شده در این خصوص، بیشترین حملاتی که بر روی پروتکل توزیع و تبادل کلید تأثیرگذار هستند در دسته‌بندی حملات مرد در وسط قرار می‌گیرند این حملات در شبکه گمنامی عبارت‌اند از:

- *Induced Tor Guard Selection*
- *Off-Path Mitm (Man in the middle Attack)*
- *Types of DOS Attacks*
- *BotNet Abuse*

آسیب‌پذیری‌های موجود در مرحله تبادل کلید باعث ایجاد فرصت مناسبی برای مهاجمان شبکه گمنامی شده است به‌نحوی که مهاجمان می‌توانند به‌راحتی خود را به‌عنوان یکی از رله‌های شبکه گمنامی معرفی کنند. ویژگی ناشناسی بدون قید و شرط و جعل ناپذیری در مرحله تبادل کلید، با استفاده از امضاء دیجیتال *LRS* در معماری شبکه منجر به تضمین قابلیت اطمینان به کلیه رله‌ها در شبکه گمنامی خواهد شد.

با به‌کارگیری ساختار پیشنهادی و با فرض این‌که مهاجم توانسته است سرویس تشخیص حملات و مدیریت خطا را دور بزند، تحت برخی شرایط خاص در صورتی‌که بتواند در ابتدای تشکیل مدار به کلیدهای عمومی رله‌ها دسترسی پیدا کرده و یک نشست از طریق کلیدی که در اختیار دارد با دیگر رله‌های شبکه گمنامی ارتباط برقرار کند و سپس فرآیند تبادل کلید خود را با الگوریتم *LRS*

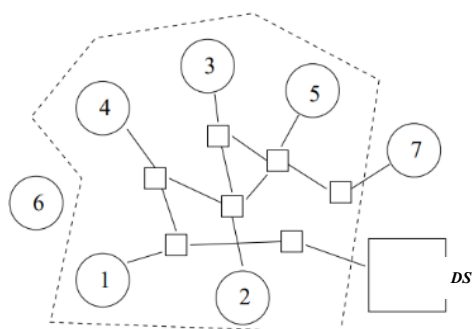
اولویت انتخاب رله‌ها برای قرارگیری در مدار شبکه گمنامی، بر اساس پهنای باند اعلام شده آن‌ها به سرور دایرکتوری است. با در نظر گرفتن شرایط گفته شده، میزان پایداری کیفیت ارتباط و همچنین یکسان بودن قدرت پردازش رله‌ها در کنار هم بایستی تحت یک استاندارد خاص در نظر گرفته شده باشد که در صورت افت کیفیت سرویس برای برقراری ارتباط، مقیاس‌پذیری و شرط احتمال یکسان انتخاب رله‌ها در مدار بایستی تا حد قابل قبولی حفظ گردد. بررسی‌ها نشان داده است که درجه گمنامی برای ارزیابی سطح حریم خصوصی دستگاه‌ها و اندازه‌گیری مقدار اطلاعاتی که مهاجم با به‌کارگیری سناریوهای مختلف از طریق طراحی یک حمله خاص به دست می‌آورد کاربرد دارد [52].

انواع حملات و مدل‌های مختلف آن در شبکه گمنامی پیاده‌سازی شده است. به‌عنوان مثال مهاجمی را در نظر می‌گیریم که توانایی این را دارد تا مجموعه‌ای از مسیرهای ممکن را محدود کند و زیرمجموعه‌ای از اعضای شبکه گمنامی یا همان رله‌ها را به دست آورد که این زیرمجموعه حاوی فرستنده‌های احتمالی داده در سراسر شبکه گمنامی خواهند بود.

در این حالت به‌صورت انتزاعی می‌توان در نظر گرفت با انجام حمله *Brute Force* بر روی هر کدام از رله‌ها، تمام مسیرهای معکوس ممکن، به فرستنده/گیرنده را می‌شود به دست آورد. یا به‌جای این روش مهاجم می‌تواند برخی از رله‌ها را در اختیار خود داشته و تعدادی از رله‌های مجموعه شبکه گمنامی را حذف کند.

شکل شماره (4) نمونه‌ای کوچک از یک شبکه گمنامی را نشان می‌دهد. با توجه به شکل در مجموع 7 رله در این سیستم وجود دارد و ما فرض می‌کنیم که مهاجم موفق شده است رله/کاربر شماره 6 و 7 را از مجموعه رله‌های فرستنده/گیرنده احتمالی حذف کند. اگر N اندازه مجموعه ناشناس یا شبکه گمنامی ما باشد حداکثر آنتروپی برای N کاربر برابر است با:

$$H_M = \log_2(N) \quad (6)$$



شکل (3): مثال درجه گمنامی [52].

می‌گردد. باید به این نکته اشاره کرد که در یک شبکه گمنام، درجه گمنامی را می‌توان با افزایش تعداد کاربران یا تعداد رله‌های میانی بهبود داد. اما باید توجه داشت که افزایش تعداد کاربران یا طبقات، با کم تأخیر بودن شبکه در تضاد است و بایستی شرایط کاربردی آن نیز مورد توجه قرار گیرد. لازم به ذکر است در صورتی که مدل حمله توسط مهاجم تغییر کند نتایج به‌دست آمده دیگر معتبر نیستند. پژوهشگران بین‌ناشناسی داده و ناشناسی اتصال تمایز قائل می‌شوند. ناشناسی داده به معنی فیلترینگ هر نوع شناسایی اطلاعات از داده‌های تبادل شده در یک برنامه خاص است و ناشناسی اتصال به معنی پنهان کردن هویت مبدأ و مقصد در طول تبادل داده‌ها است.

این نکته حائز اهمیت است که درجه گمنامی میزان ناشناسی اتصال را می‌تواند ارزیابی‌اند. اغلب سامانه‌های گمنامی کم تأخیر، درجه گمنامی مناسبی را ارائه می‌دهند اما با مشکل مقیاس‌پذیری مواجه هستند که این مسئله از طریق یک طراحی مناسب کنترل خواهد شد. درجه حریم خصوصی به تعداد رله‌های در معرض خطر در مقابل تعداد کل شرکت‌کنندگان در شبکه نیز بستگی دارد. منطقی است که با بهبود امنیت پروتکل توزیع کلید، درجه گمنامی نیز مطابق با آن افزایش پیدا کند.

درجه گمنامی با استفاده از رابطه (2) تعریف می‌شود، که در این رابطه $H(x)$ برابر با آنتروپی شبکه گمنامی پس از وقوع حمله و H_M معادل با بیشترین آنتروپی که شبکه گمنامی می‌تواند داشته باشد است [52].

$$d = \frac{H(x)}{H_M} \quad (3)$$

که آنتروپی شبکه از طریق رابطه (3) محاسبه می‌شود. در رابطه pi برابر با احتمال انتخاب یک رله از میان N رله همسان است، که N برابر تعداد کل رله‌های موجود است.

$$H(x) = -\sum_{i=1}^N pi \log_2(pi) \quad (4)$$

در ضمن بیشترین درجه گمنامی زمانی حادث می‌شود که تمامی رله‌ها از احتمال یکسانی برای انتخاب شدن برخوردار باشند و درواقع احتمال هر رله برابر $\frac{1}{N}$ باشد. در این صورت مقدار H_M از رابطه (5) محاسبه می‌شود.

$$H_M = -\sum_{i=1}^N \frac{1}{N} \log_2\left(\frac{1}{N}\right) = -\log_2(N) \quad (5)$$

با در نظر داشتن تعریف درجه‌ی گمنامی، مقدار آن عددی در بازه [0 و 1] است که درجه‌ی گمنامی صفر ("0") به مفهوم فاش و قابل اثبات بودن هویت فرستنده پیام و درجه‌ی گمنامی یک ("1") به معنای اینکه همه اعضای مجموعه گمنامی با احتمال یکسانی فرستنده پیام می‌باشند، است.

شبکه نشان نمی‌دهد که با توجه به شرایط گفته‌شده روش پیشنهادی منجر به بهبود درجه گمنامی خواهد شد.

با بهبود معماری شبکه گمنامی از طریق روش پیشنهادی و به‌کارگیری سیستم رمزنگاری *QMNT* و امضاء دیجیتال *LRS* احتمال دسترسی مهاجم به شبکه مطابق با مدل حمله مطرح‌شده با توجه به عدم امکان تحلیل مستقیم پروتکل بسیار سخت و غیرقابل‌تصور است.

LRS نه تنها ویژگی *RS* معمولی مانند صحت، جعل ناپذیری و ناشناسی را برآورده می‌کند، بلکه می‌تواند برای قضاوت در مورد این‌که آیا دو امضاء متفاوت توسط یک امضاء کننده امضاء شده‌اند (همان قابلیت پیوند) استفاده شود.

امضاء حلقه قابل پیوند می‌تواند تعیین کند آیا دو امضاء کننده یکسان در حلقه عضو هستند یا خیر. به بیانی دیگر می‌توان گفت *LRS* در شرایطی که ناشناس بودن و تکرارناپذیری لازم است نیز مفید است که منجر به بهبود درجه گمنامی شده است.

3-7. تحلیل و ارزیابی پروتکل توزیع کلید

پژوهشگران در ارزیابی پروتکل‌ها و سامانه‌های امنیتی غالباً معیارهای میزان پردازش، حافظه موردنیاز، و پهنای باند مصرف‌شده توسط پروتکل‌ها و الگوریتم‌ها را موردبررسی قرار می‌دهند. واضح است که از لحاظ سرعت کارایی، الگوریتم‌های *NTRU* و *NSS* به علت ساختاری ساده‌تر و محاسبات کمتر، عملکرد بسیار سریع‌تری داشته باشند.

مشکلات سیستم رمزنگاری *NTRU* علی‌الخصوص موفقیت‌آمیز نبودن رمزگشایی در حالت‌های خاص و انواع حملات طراحی‌شده از این طریق، توانایی مقاومت آن را در برابر مهاجمین قوی با مشکل مواجه کرده است. با توجه به این‌که در روش پیشین این مکانیسم بخش اصلی پروتکل توزیع و تبادل کلید را تشکیل می‌داد، نمی‌تواند گمنامی را در شبکه به‌خوبی تأمین کند. ساختار توسعه‌یافته رمزنگاری *QMNT* و ترکیب آن با امضاء دیجیتال *LRS* معماری بسیار پیچیده و قوی‌تری را جهت ارائه سرویس گمنامی ایجاد می‌کند. در حملات تحلیل ترافیک بر روی شبکه گمنامی، مهاجم به دنبال جمع‌آوری اطلاعاتی نظیر شناسه مدارهای شبکه، رله‌ها و مکان استقرار آن‌ها، معماری شبکه گمنامی و نحوه پیاده‌سازی آن، و تشخیص جریان ترافیک شبکه است. جمع‌آوری، دسته‌بندی و پردازش این اطلاعات می‌تواند باعث شناسایی موقعیت مرکز فرماندهی و کنترل و اجزای مهم شبکه گمنامی شود و از این طریق امکان بروز حملات منع سرویس در بستر شبکه گمنامی افزایش می‌یابد.

تصور کنید که مهاجم زیرمجموعه‌ای از مجموعه ناشناس *S* را به دست آورده است که حاوی فرستنده/گیرنده احتمالی در شبکه هستند که اندازه زیرمجموعه *S* برابر با رابطه (7) است.

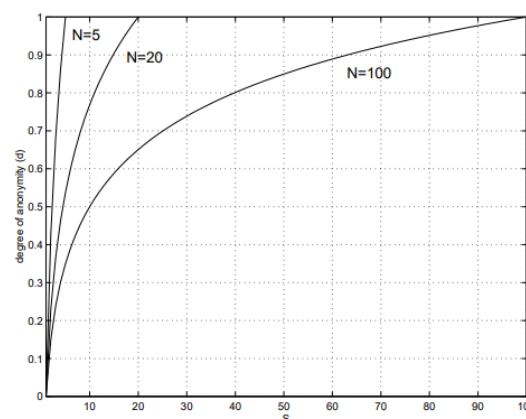
$$S = (1 \leq S \leq N) \quad (7)$$

با در نظر گرفتن این‌که مهاجم نمی‌تواند احتمالات متفاوتی را به کاربران متعلق به این زیرمجموعه اختصاص دهد بر اساس رابطه (8) خواهیم داشت:

$$p_i = \frac{1}{S}, 1 \leq i \leq S; p_i = 0, S+1 \leq i \leq N \quad (8)$$

درنهایت با توجه به مثال مطرح‌شده، آنتروپی پس از حمله، و درجه گمنامی شبکه برابر با رابطه (9) است.

$$H(X) = \log_2(S). d = \frac{H(X)}{H(M)} = \frac{\log_2(S)}{\log_2(N)} \quad (9)$$



شکل (4): درجه گمنامی محاسبه‌شده یک شبکه مبتنی بر مسیریابی پیازی را با توجه به مجموعه *S* برای $N=5$, $N=20$ و $N=100$ نشان می‌دهد [52].

با توجه به نمودار بالا و موارد گفته‌شده *S* تعداد رله‌های فرستنده و گیرنده احتمالی در اختیار مهاجم و *N* تعداد کل رله‌ها است. به‌عنوان مثال برای به دست آوردن درجه گمنامی $d \geq 0.8$ داریم: برای $N=5$ به $S \geq 3$ نیاز داریم، برای $N=20$ کاربر به $S \geq 12$ نیاز داریم، و برای $N=100$ به $S \geq 40$ نیاز داریم. به این صورت که با افزایش *S* احتمال در اختیار داشتن رله‌ها توسط مهاجم کاهش می‌یابد و با کاهش آن مهاجم نمی‌تواند احتمالات متفاوتی را به کاربران متعلق به زیرمجموعه خودش اختصاص دهد.

معماری قدرتمند روش پیشنهادی، مقاومت بسیار بالایی در برابر نفوذ مهاجم و در اختیار گرفتن زیرمجموعه‌ای از کاربران شبکه دارد که از به دست آوردن هرگونه اطلاعات به‌وسیله‌ی سناریوهای مختلف توسط مهاجم در مورد شبکه گمنامی جلوگیری می‌کند و مهاجم قادر نیست احتمالات متفاوتی را به کاربران متعلق به زیرمجموعه‌ای که در اختیار دارد نسبت دهد. درنتیجه مهاجم امکان نفوذ نداشته و عملکرد مناسبی از خود در

افزایش پیچیدگی به کاررفته در این سیستم رمزنگاری مقاومت آن را در برابر انواع حملات کوانتومی تضمین خواهد کرد و به کارگیری آن باعث شکستناپذیر شدن پروتکل توزیع و تبادل کلید و عدم اجرای موفق انواع حملات جهت شکستن کلیدهای به کاررفته در شبکه گمنامی شده است. بدیهی است که میزان پیچیدگی عملیات، و مدت زمان پردازش مورد نیاز برای شکستن الگوریتم رمزنگاری با توجه به قدرت مناسب سیستم رمزنگاری به صورت منطقی افزایش خواهد یافت که در این حالت تحت هیچ شرایطی شکستن خود الگوریتم رمز توجیه منطقی نخواهد داشت و مهاجم بایستی روش های دیگری را طراحی و به کارگیری کند.

2-3-7. تحلیل امنیت و کارایی امضاء دیجیتال پروتکل توزیع کلید

با صرف نظر از بیان کاربردهای خاص حوزه امضاء دیجیتال، اهداف و تمرکز اصلی آن ها همواره بر روی اجرای احراز هویت و کمک به حفظ یکپارچگی داده ها بوده است.

علاوه بر آن معیارهایی نظیر عدم انکار، کارایی، هزینه، بازده زمانی، انعطاف پذیری، قابلیت پیوند و غیره... نیز در خصوص ارزیابی آن ها مورد توجه پژوهشگران این حوزه قرار گرفته است.

آسیب پذیری ها و بازده پایین امضاءهای دیجیتال مبتنی بر لگاریتم گسسته و ریاضیات باعث طراحی و توسعه طرح های جدیدتری بر پایه محاسبات کوانتومی شد که امضاء دیجیتال *NSS* به عنوان یک مکمل برای سیستم رمزنگاری *NTRU* در گذشته معرفی شده بود. نتایج مقایسه کارایی و سرعت بین *NSS* و امضاءهای دیجیتال قبل از آن مانند *RSA* و *ECDSA* نشان دهنده تحولی بسیار عظیم در حوزه به کارگیری الگوریتم های رمزنگاری و امضاءهای دیجیتال مقاوم در برابر حملات کوانتومی بود [53]. امنیت امضاء دیجیتال *LRS* همانند نسخه پیشین خود یعنی *NSS* وابسته به سیستم رمزنگاری *NTRU* و مقاومت در برابر حملات کوانتومی است، در نتیجه امنیت بسیار بالایی را فراهم می کند. سرعت چشم گیر روند مطالعات و پژوهش های صورت گرفته در دهه اخیر بر روی امضاءهای حلقه قابل پیوند (*LRS*) نشان دهنده لزوم اهمیت به کارگیری آن ها در معماری های امنیتی عصر حاضر است [54, 55].

جداول تهیه شده در بخش های بعد آخرین نتایج ارزیابی صورت گرفته توسط پژوهشگران بر روی امنیت و کارایی انواع امضاءهای دیجیتال *LRS* را نشان می دهد که عملکرد الگوریتم امضاء دیجیتال کینگ [7] همان الگوریتم به کارگیری شده در پروتکل توزیع و تبادل کلید پیشنهادی، در این جداول با دیگر طرح های امضا دیجیتال در ابعاد مختلف بررسی، مقایسه و ارزیابی شده است. امضاء دیجیتال *LRS* به دلیل کارایی و توانایی بالا در تأمین

ارائه گمنامی بدون قید و شرط توسط الگوریتم *LRS* در کنار به کارگیری از یک تابع فیلتر توزیع ترافیک این امکان را به شبکه می دهد که در برابر حملات تحلیل ترافیک نیز مقاومت کافی را داشته باشد. در طراحی شبکه گمنامی از طریق روش پیشنهادی، در نظر گرفتن توانایی محاسباتی رله های شبکه از اهمیت بسیار بالایی برخوردار است و نبایستی تأثیر منفی در کارایی شبکه داشته باشد. با توجه به محاسبات پیچیده و زیاد الگوریتم های به کارگیری شده میزان توانایی پردازش در رله ها باید پاسخ گوی نیازمندی های شبکه گمنامی طراحی شده از این طریق باشد.

اصلی ترین مزیت به کارگیری *NTRU* و *NSS* در شبکه گمنامی، مقدار کمتر سربار محاسباتی بود. در روش پیشنهادی نیز سربار پردازشی زیادی بر روی رله ها توسط شبکه گمنامی تحمیل نمی شود که قادر به پردازش آن نباشند.

با به کارگیری سخت افزار مناسب می توان مقدار سربار محاسباتی اضافی روش پیشنهادی را پوشش داد. مطالعه و بررسی نتایج پژوهشگران حوزه امنیت نشان داده است که همواره میزان گمنامی به دست آمده غالباً با میزان کارایی شبکه رابطه معکوس خواهد داشت، درواقع هر چه الگوریتم یا پروتکل از نظر ارائه سرویس های گمنامی و امنیتی قوی تر باشد میزان کارایی و سرعت به دلیل افزایش پردازش اطلاعات و سربار محاسبات تا حدودی کاهش می یابد، استفاده از سخت افزارهای پیچیده تر و پردازنده های قوی می تواند به بهبود کارایی رله ها کمک قابل توجهی داشته باشد. با توجه به موارد گفته شده در ادامه تحلیل امنیتی اجزای مهم پروتکل توزیع کلید را با در نظر گرفتن معیارهای مختلف بررسی خواهیم کرد.

1-3-7. تحلیل و ارزیابی سیستم رمزنگاری

بررسی میزان پیچیدگی عملیات به کاررفته در سیستم رمزنگاری را می توان به عنوان یکی از پارامترهای تحلیل و ارزیابی در نظر گرفت. در جدول شماره (4) تعداد عملیات های سامانه های رمزنگاری مختلف بررسی و ارائه شد که با توجه به مقادیر جدول، سیستم رمزنگاری *NTRU* برای تولید کلید، یک مرتبه ضرب کانولوشن، برای رمزنگاری یک مرتبه ضرب کانولوشن و یک مرتبه جمع چندجمله ای نیاز داشت، و در آخر برای رمزگشایی نیز دو مرتبه ضرب کانولوشن و یکبار جمع چندجمله ای صورت می گرفت، که در مقایسه با سیستم رمزنگاری پیشنهادی ما یعنی *QMNTR* این مقادیر مشابه فوق به ترتیب به 80 مرتبه عمل ضرب کانولوشن، 80 مرتبه عمل ضرب و 4 مرتبه عمل جمع چندجمله ای و 1088 مرتبه عمل ضرب و 4 مرتبه عملیات جمع بر روی چندجمله ای ها صورت می گیرد.

تائید اعتبار	الگوریتم امضاء	KeyPair	الگوریتم
$(2lm + 3)TMul$	$(2l + 4m + 3l - 2)TMul$	$(2m - 1)TMul + TInv$	GW [56]
$lTMul$	$lTMul + 2TSd + 2TRs$	$TMul + TTrap + TSam$	Qing[7]
$(lm + 1)TMul$	$(lm + m)TMul$	$(2m - 1)TMul + TInv$	AM [57]
$(lm + 1)TMul$	$(lm + m + l - 1)TMul$	$mTMul$	RS[55]
$(lm + 1)TMul$	$(lm + m + l - 1)TMul$	$mTMul$	LRS[55]

لازم به ذکر است، به هنگام محاسبه پیچیدگی زمانی از محاسبه برخی از عملیات‌های سبک مانند عملکرد هش و انتخاب اعداد تصادفی صرف‌نظر شده است، و عمدتاً هزینه زمانی ضرب چندجمله‌ای $(TMul)$ و وارونگی چندجمله‌ای $(TInv)$ در محاسبات در نظر گرفته شده است. محاسبه زمان اجرای الگوریتم‌های *Gaussian sampling algorithm*، *rejection sampling algorithm*، *trapdoor generation algorithm* و *Sample Pre algorithm* هر کدام به ترتیب با TRs ، TSd و $TTrap$ و $TSam$ نشان داده می‌شوند، که در [7] $TTrap$ ، TSd و TRs ها برای *Signature* و *KeyPair* استفاده می‌شود. همان *KeyPair* همان ترکیب کلید عمومی و خصوصی است که به ترتیب برای رمزگذاری و رمزگشایی داده‌ها استفاده می‌شوند.

نتایج ارزیابی جدول شماره (6) نشان می‌دهد که هزینه امضاء و هزینه تائید یا *Verification Cost* در طرح چنگتنگ کو [55] کمتر از طرح امضاء کارلوس و همکاران [56] است و هزینه *KeyPair* آن نیز از طرح‌های کارلوس [56] و طرح ون‌گو [57] کم‌تر است. طرح امضاء دیجیتال *LRS* کینگ [7] در *KeyPair* و دیگر موارد نسبت به طرح‌های کارلوس [56] و طرح ون‌گو [57] عملکرد مطلوب‌تری دارد که در پروتکل توزیع کلید از آن استفاده کرده‌ایم.

با توجه به این‌که در شبکه گمنامی عملیات رمزنگاری و رمزگشایی به‌صورت لایه‌ای انجام می‌شود، پیچیدگی زمانی کم‌تر در هر مرحله می‌تواند بار محاسباتی شبکه را کاهش دهد که در طرح کینگ پیچیدگی زمانی مطلوبی را نسبت به دیگر طرح‌ها مخصوصاً در *KeyPair* مشاهده می‌کنیم و با استفاده آن در روش پیشنهادی پیچیدگی زمانی مناسبی خواهیم داشت.

3-2-3-7. تحلیل کارایی و بررسی عملکردی

در جدول (7) طرح چنگتنگ کو با چهار طرح دیگر من جمله [7] از نظر عملکرد بررسی و ارزیابی شده است [55]. هر دو امضاء حلقه انکارپذیر و امضاء حلقه قابل پیوند امضاءهای حلقه‌ای با ویژگی خاص خود هستند که می‌توانند برای کاربردهای مختلف به‌کارگیری شوند. امضاء حلقه قابل‌انکار می‌تواند ثابت کند که عضو حلقه در صورت لزوم و به دلیل منطقی عملیات امضاء را انجام نداده است در برابر آن امضاء حلقه قابل پیوند می‌تواند

گمنامی بدون قید و شرط، جعل ناپذیری و قابلیت پیوند، سربار ارتباط و پیچیدگی زمانی کمتر، باعث تمایز خود با طرح‌های دیگر امضاءهای دیجیتال شده است. همچنین داده‌های حاصل‌شده نشان می‌دهد در مقایسه با دیگر طرح‌ها نسبتاً منابع کمتری مصرف می‌کند و این موضوع بسیار بااهمیت است. درنتیجه با استفاده از امضاء دیجیتال *LRS* در پروتکل توزیع کلید امنیت و کارایی شبکه گمنامی ارتقاء یافته است.

1-2-3-7. تحلیل و مقایسه سربار ارتباط

در جدول (5) نسبت زمانی که صرف تلاش برای برقراری ارتباط با اعضاء حلقه صورت می‌گیرد یا همان سربار ارتباط امضاء دیجیتال بررسی، ارزیابی و مقایسه شده است که در آن θ برابر است با $\sqrt{n \log n} - mn^{1.5} \log n$ و تعداد اعضای حلقه است.

جدول (5): مقایسه سربار ارتباط (به بیت) [55]

اندازه امضاء	کلید خصوصی	کلید عمومی	الگوریتم امضا
$2mn \log \theta + 2ln + (m + 1)n \log p$	$2mn \log p$	$mn \log p$	GW [56]
$nl \log p$	$2n \log p$	$n \log p$	Qing [7]
$2mn \log \theta + 2n$	$2mn \log p$	$mn \log p$	AM [57]
$2mn \log \theta + 2n$	$2mn \log p$	$mn \log p$	RS[55]
$2mn \log \theta + 2n$	$2mn \log p$	$mn \log p$	LRS[55]

به‌طور خلاصه نتایج حاصل از جدول نشان می‌دهد که اندازه کلید عمومی، کلید خصوصی، طرح‌های [55] با طرح [56] برابر است. اندازه امضاء طرح‌های [55] و [57] برابر است و درنهایت اندازه امضاء [55] در مقایسه با طرح کینگ [7] بزرگ‌تر است.

به بیانی دیگر هرچه کلید عمومی، کلید خصوصی، و اندازه امضاء کوچک‌تر باشد سربار ارتباط کم‌تری را خواهیم داشت که به‌طور مشخص با توجه به مقادیر ارائه‌شده در جدول روش پیشنهادی سربار ارتباطی کم‌تری دارد و نشان‌دهنده این است که امضاء دیجیتال *LRS* در مدت‌زمان کم‌تری می‌تواند با اعضای حلقه خود ارتباط برقرار کند.

2-2-3-7. تحلیل و مقایسه پیچیدگی زمانی

محاسبه پیچیدگی زمانی اجرای الگوریتم‌های امضاء دیجیتال جهت ارزیابی کارایی الگوریتم از اهمیت بالایی برخوردار بوده که در ادامه پیچیدگی زمانی طرح‌های امضاء مختلف بررسی و ارزیابی شده است. با توجه به جدول شماره (6) حرف m تعداد اجزای یک بردار چندجمله‌ای و l تعداد اعضای حلقه است.

جدول (6): مقایسه بین هزینه‌های زمانی $(Time Cost)$ [55]

رمزگشایی و رمزنگاری را انجام ندهد علاوه بر آن پیش از عبور ترافیک از شبکه داخلی در آخرین گام داده‌ها رمزنگاری شده نباشند و همچنین در اولین گام در خروج از میزبان نیز انتقال داده به همین شکل انجام گرفته باشد، امکان شناسایی و رهگیری ترافیک توسط این نوع سامانه‌ها با چالش بزرگی مواجه خواهند شد که به‌عنوان یکی از مخاطرات و گلوگاه‌های این دسته از سامانه‌ها می‌تواند در نظر گرفته شود.

با در نظر گرفتن این شرایط در صورتی امکان تشخیص موفق وجود خواهد داشت که قابلیت رهگیری تعبیه شده در سامانه از قدرت بسیار بالایی برخوردار باشد. به‌عنوان مثال از طریق تغییر بخشی از داده‌های تبادل شده و رهگیری مسیر جریان داده می‌توان به مسیر ایجاد شده توسط شبکه گمنامی پی برد. با توجه به این‌که در روش ارائه شده هیچ‌کدام از کاربران شبکه به‌عنوان بخشی از شبکه گمنامی در نظر گرفته نمی‌شوند و تمام عملیات انجام شده بر عهده رله‌ها قرار دارد و همچنین کلیه تبادلات نیز تحت نظر سرویس تشخیص حملات انجام شده که در صورت هرگونه تغییر مخرب در داده‌ها، فعالیت شبکه را متوقف خواهد کرد. همچنین در کنار آن با استفاده از تابع پالایه توزیع ترافیک امکان اجرای حملات تحلیل ترافیک از مهاجم سلب شده است. در نتیجه امکان مسدود کردن و رهگیری ترافیک به همراه تحلیل معماری شبکه گمنامی از طریق روش پیشنهادی با در نظر گرفتن موارد گفته شده بسیار سخت و تا حد زیادی غیرممکن خواهد بود.

5-7. مقایسه پژوهش‌های مرتبط با روش پیشنهادی

انواع سامانه‌ها و شبکه‌های گمنامی با رویکردها و معماری‌های مختلف طراحی و توسعه پیدا کرده‌اند، که هرکدام از آن‌ها کارایی مختلفی داشته و به‌منظور اهداف خاص موردنظر خود به‌کارگیری می‌شوند.

مقایسه دقیق بین پژوهش‌های مرتبط با سامانه گمنامی پیشنهادی، به دلیل وجود تفاوت بین اهداف و کاربرد انواع شبکه‌های گمنامی مورد ارزیابی، تفاوت در معماری به‌کارگیری شده در سامانه‌ها، پارامترها و اجزای مختلف انواع سامانه‌ها، و تنظیمات آن‌ها با سامانه پیشنهادی و همچنین عدم وجود یک معیار و قالب ثابت و مشخص در حوزه ارزیابی شبکه‌های گمنامی، مقایسه بین آن‌ها را به امری بسیار پیچیده تبدیل کرده که فقدان پژوهشی مشابه و یک مجموعه داده ارزیابی شده در این زمینه آن را سخت‌تر هم خواهد کرد.

بنابراین با انتخاب شبیه‌ترین پژوهش‌های انجام شده به لحاظ معماری در این زمینه، مقایسه‌ای بین روش پیشنهادی، و دیگر روش‌ها با در نظر گرفتن سنجه‌های مختلف، بر اساس چند معیار

تعیین کند آیا دو امضاء کننده یکسان در حلقه عضو هستند یا خیر که امروزه پژوهشگران این حوزه در تلاش هستند یک طرح امضاء حلقه قابل پیوند و قابل انکار طراحی کنند. با توجه به نتایج جدول (7) می‌توانیم به این نتیجه برسیم که تنها طرح چنگتانگ کو [55] و طرح کینگ [7] در برابر حملات کوانتومی ایمن هستند.

طرح [7] با داشتن قابلیت پیوند و مقاومت در برابر حملات کوانتومی سطح امنیتی بسیار بالایی را نسبت به اغلب طرح‌های امضاء ارائه می‌دهد که با استفاده از آن در روش پیشنهادی مقاومت شبکه گمنامی در برابر انواع حملات، خصوصاً حملات کوانتومی افزایش پیدا کرده است.

جدول (7): مقایسه عملکرد امضاءهای دیجیتال [55]

قابلیت پیوند	قابلیت انکار	مقاومت کوانتومی	الگوریتم امضا
دارد	ندارد	ندارد	LJ [58]
ندارد	دارد	دارد	GW [56]
دارد	ندارد	دارد	Qing [7]
ندارد	ندارد	دارد	AM [54]
ندارد	ندارد	دارد	RS [55]
دارد	ندارد	دارد	LRS [55]

4-7. تحلیل عملکرد روش پیشنهادی در برابر سامانه‌های مسدودکننده ترافیک گمنام

سامانه‌های مختلفی جهت تشخیص ترافیک شبکه گمنامی مبتنی بر مسیریابی پیزی و دیگر ترافیک‌های گمنام و مخرب در شبکه طراحی و توسعه یافته‌اند که امروزه از روش‌هایی نظیر یادگیری عمیق برای مدل‌سازی رفتار و سپس تحلیل جریان ترافیک شبکه استفاده می‌شود [59].

به‌غیر از این روش ساختارهای متنوع دیگری توسط پژوهشگران این حوزه طراحی و توسعه پیدا کرده‌اند که پرداختن به همه آن‌ها خارج از موضوع این تحقیق است [60-61].

به‌طور کلی این سامانه‌ها ترافیک شبکه را به‌صورت بر خط بررسی کرده سپس وجود ترافیک گمنام یا مخرب در خروجی میزبان‌های شبکه را بررسی می‌کند و در صورت احراز شرایط، فعالیت میزبان را به روش مخصوص خود متوقف می‌کند که می‌توان ترافیک سامانه گمنامی پیشنهادی را از طریق پیاده‌سازی یک محیط آزمایشگاهی در برابر این نوع سامانه‌ها قرارداد و در آخر ترافیک تبادل شده را ارزیابی کرد.

در صورتی‌که ارتباط با شبکه داخلی از طریق شبکه گمنامی به نحوی انجام گرفته باشد که کاربر نهایی یا میزبان / رله عملیات

مشترک و نتایج حاصل شده از تحلیل‌های این فصل بین آن‌ها صورت گرفته است.

جدول (۸): مقایسه با پژوهش‌های پیشین

شبکه گمنامی	حملات کوانتومی	حملات منع سرویس	تحلیل ترافیک بدون قید و شرط	ناشناسی	حملات MITM
روش پیشنهادی	✓	✓	✓	✓	✓
سامانه [5]	✓	×	✓	×	×
سامانه [25]	×	×	×	×	×
سامانه [62]	×	✓	×	×	✓
سامانه [63]	×	✓	✓	×	×
سامانه [64]	✓	×	×	×	✓
سامانه [65]	×	✓	✓	×	×
سامانه [66]	×	✓	✓	×	×

در جدول (۸) مقایسه‌ای کلی بین روش پیشنهادی و سایر پژوهش‌های مرتبط جهت بهره‌برداری و اثبات قدرت سامانه پیشنهادی ارائه شده است.

با توجه به جدول (۸) نتایج ذیل حاصل می‌گردد:

✓ فقط روش پیشنهادی ما و سامانه [5] و [64] در برابر انواع حملات کوانتومی مقاومت کافی را دارد.

✓ در مقایسه با روش‌های دیگر تنها روش پیشنهادی ماست که به علت معماری خاص خود توانایی مقاومت در برابر انواع حملات را خواهد داشت.

✓ نسل دوم شبکه گمنامی در برابر حملات مطرح شده مقاومت لازم را ندارد و نشان‌دهنده منسوخ شدن معماری این نوع از شبکه‌های گمنامی است.

✓ فقط سامانه‌های [25]، [62] و [64] نمی‌توانند از خود در برابر حملات تحلیل ترافیک مقاومت نشان دهند.

✓ با استفاده از امضاء دیجیتال LRS که ویژگی جعل ناپذیری را در مرحله تبادل کلید روش پیشنهادی برقرار می‌کند، امکان اجرای موفق حملات MITM بر روی رله‌ها از مهاجم سلب خواهد شد.

✓ با استفاده از امضاء دیجیتال LRS ویژگی ناشناسی بدون قید

و شرط در شبکه گمنامی برقرار می‌شود. امضاء دیجیتال LRS باعث تضمین قابلیت اطمینان رله‌ها در ساختار پیشنهادی شده و رله‌های تأیید شده به مشابه اعضاء حلقه عمل می‌کنند. بنابراین صرفاً رله‌ای که از طریق LRS تأیید شده باشد در مجموعه رله‌ها دارای اعتبار بوده و

تعیین این‌که از کدام کلید برای تأیید رله استفاده شده از نظر محاسباتی غیرممکن است.

7-6. نوآوری‌های پژوهش

در نظر گرفتن کاربر به‌عنوان بخشی از شبکه به‌نحوی که خود وظیفه مسیریابی را بر عهده داشته باشد از اشتباهات رایج طراحی شبکه گمنامی بود که در ساختار پیشنهادی پیکربندی شبکه مطابق آنچه در پژوهش گفته شد تغییر پیدا کرده است.

همچنین پژوهشگران به جنبه‌هایی نظیر جعل ناپذیری و ناشناسی بدون قید و شرط در شبکه گمنامی تاکنون نپرداخته بودند که بازطراحی معماری، رفع معایب، تجمیع و یکپارچه‌سازی انواع مکانیسم‌ها در ساختار پیشنهادی علاوه بر ارتقاء شبکه باعث تأمین قابلیت‌های امنیتی مانند مقاومت در برابر ره‌گیری شبکه، طراحی انعطاف‌پذیر، تشخیص و جلوگیری از نفوذ مهاجمین، مسیریابی چند مسیری، انتخاب مسیر بهینه، مدیریت خطا و تأخیر، طراحی پیوند ناپذیر، و کنترل ازدحام شد.

روش ارائه شده پویایی لازم جهت به‌کارگیری در انواع کاربردها را داشته و از آخرین فناوری‌ها در پیاده‌سازی معماری آن استفاده شده است.

باوجود ارائه نوآوری پژوهش حاضر در بخش‌های مختلف مقاله و توضیح آن‌ها، جدول شماره (۹) شاخص‌ترین جنبه‌های مهم نوآوری‌های ارائه شده را به تفکیک بیان می‌کند.

جدول (۹): نوآوری‌های پژوهش

بررسی جنبه‌های مختلف نوآوری	اجزا ساختار شبکه پیشنهادی
پیوند ناپذیری، مقاومت در برابر حملات تحلیل ترافیک	مرکز فرماندهی و کنترل
مسیریابی بهینه، افزایش پهنای باند، کنترل ازدحام	مسیریابی و ایجاد مدار
رفع خطاهای شبکه و مسیریابی، جلوگیری از نفوذ و اجرای حملات	تشخیص حملات و مدیریت خطا
ارتقاء سیستم رمزنگاری از طریق جایگزینی (رمزنگاری QMNT و امضاء دیجیتال LRS)	سرویس رمزنگاری شبکه گمنامی

8. نتیجه‌گیری

یکی از قسمت‌های مهم این پژوهش تحلیل پروتکل توزیع و تبادل کلید بود که با ذکر مثال‌های مختلف آن را ارزیابی کردیم. همچنین در ادامه معیارهای گمنامی و کارآمدی روش پیشنهادی را نسبت به روش قبلی بررسی کردیم که کلیه موارد بررسی شده قدرتمندی و امنیت روش پیشنهادی را نشان داده است. به‌علاوه

مکانیسم‌های امنیتی که امروزه برای حفظ حریم خصوصی در شبکه‌ها و سازمان‌ها مورد استفاده قرار می‌گیرد و با توجه به وضعیت سامانه‌های آن‌ها، بررسی این مسئله که چگونه می‌توانیم معماری گمنامی در شبکه را در کنار هر یک از این مکانیسم‌های امنیتی ارائه کنیم، به عنوان یک طرح، می‌تواند مورد تحقیق توسط پژوهشگران این حوزه قرار گیرد.

- پیاده‌سازی یک معماری غیرمتمرکز بهینه برای شبکه گمنامی
- طراحی و پیاده‌سازی الگوریتم‌های کوانتومی بهتر جهت به کارگیری در تبادل داده‌ها و رمزنگاری آن‌ها در بسترهای مختلف
- ارائه یک معیار ارزیابی غیر از روش درجه گمنامی برای تعیین سطح امنیتی انواع سامانه‌های گمنامی
- طراحی و پیاده‌سازی سامانه‌های هوشمند تشخیص ترافیک گمنام در شبکه

10. مراجع

- [1] Egner, André, et al. "Introducing SOR: SSH-based onion routing." 2012 26th International Conference on Advanced Information Networking and Applications Workshops. (pp. 280-286) IEEE, 2012. <https://doi.org/10.1109/WAINA.2012.89>.
- [2] Bennett, Krista, and Christian Grothoff. "GAP—practical anonymous networking." International Workshop on Privacy Enhancing Technologies. Berlin, Heidelberg: Springer Berlin Heidelberg, (pp. 141-160), 2003. https://doi.org/10.1007/978-3-540-40956-4_10.
- [3] G. Danezis and C. Diaz, "A survey of anonymous communication channels," Technical Report MSR-TR-2008-35, Microsoft Research, Tech. Rep., 2008. <https://www.microsoft.com/en-us/research/wp-content/uploads/2008/02/tr-2008-35.pdf>.
- [4] Karunanayake, Ishan, et al. "De-anonymisation attacks on tor: A survey." IEEE Communications Surveys & Tutorials 23.4 (2021): 2324-2350. <https://doi.org/10.1109/COMST.2021.3093615>.
- [5] A. Hasani Karbasi, "Designing Anonymous Communication System by Lattice-Based Cryptography", Journal of Electronic & Cyber Defence Vol 2, No. 3, 2014. Available: <https://sid.ir/paper/243126/en>.
- [6] Yassein, Hassan R., Asia A. Abidalzahra, and Nadia M. Al-Saidi. "A new design of NTRU encryption with high security and performance level." AIP Conference Proceedings. Vol. 2334. No. 1. AIP Publishing LLC, 2021. doi.org/10.1063/5.0042312.
- [7] Ye, Qing, et al. "Efficient Linkable Ring Signature Scheme over NTRU Lattice with Unconditional Anonymity." Computational Intelligence and Neuroscience p.8431874 (2022). <https://doi.org/10.1155/2022/8431874>.
- [8] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a

الگوریتم امضاء دیجیتال LRS از منظر معیارهای گفته شده و نتایج حاصل از جدول‌ها تحلیل شد. سپس روش پیشنهادی را در برابر سامانه‌های جدید کنترل ترافیک گمنام، بررسی و ارزیابی کردیم که در نهایت با استخراج معیارهای ارزیابی مشترک برای شبکه گمنامی نتایج حاصل از جدول (8) ارائه شد.

گمنامی امروزه به عنوان یک اصل اساسی در روابط بین مؤلفه‌ها در نظر گرفته شده است. با افزایش روزافزون تهدیدات سایبری علیه اهداف مختلف، نیازمندی به کارگیری انواع سامانه‌های گمنامی و رعایت ویژگی‌های امنیتی دیگری مانند پیوند ناپذیری و مقیاس پذیری بیش از پیش احساس شده است و از سویی دیگر با تنوع حملات طراحی شده بر روی این دسته از سامانه‌ها نیاز به بهبود مستمر معماری به کاررفته در آن‌ها ضروری است تا همواره توانایی مقابله با انواع تهدیدات نوین سایبری را داشته باشند.

آسیب پذیری‌های موجود در مرحله تبادل کلید شبکه گمنامی این فرصت را به مهاجم می‌داد که از طریق روش‌هایی مانند حمله مردمیانی به راحتی خود را به عنوان یکی از رله‌های شبکه گمنامی معرفی کند.

ویژگی ناشناسی بدون قید و شرط و جعل ناپذیری در مرحله تبادل کلید که حاصل استفاده از امضاء دیجیتال LRS است باعث تضمین قابلیت اطمینان رله‌ها در شبکه گمنامی شد.

همچنین مشکلات موجود در ساختار سیستم رمزنگاری NTRU و توانایی پایین امضاء دیجیتال NSS نسبت به فناوری‌های پس از خود، باعث کاهش ضریب امنیتی ایجاد کلید جلسه و انتقال امن کلید در شبکه گمنامی شده بود که با ترکیب سیستم رمزنگاری QMNTR و امضاء دیجیتال LRS در کنار طراحی مناسب ارائه شده، معماری قدرتمندی پیشنهاد و شبیه‌سازی شد.

ساختار ارائه شده در روش پیشنهادی ضمن اینکه توانایی مقابله با انواع تهدیدات را دارد از درجه گمنامی و کارایی مناسبی برخوردار بوده و امنیت پروتکل توزیع و تبادل کلید شبکه گمنامی را بهبود داده است که با به کارگیری امضاء دیجیتال LRS سربرار ارتباط، پیچیدگی زمانی و کارایی مناسبی را ارائه می‌دهد.

9. پیشنهادها و پژوهش‌های آتی

اقدامات قابل انجام در پژوهش‌های آتی بدین شرح ارائه می‌گردند:

- پیاده‌سازی سامانه گمنامی با استفاده از یک معماری پایه قدرتمند و بهینه‌تر
- بازطراحی شبکه گمنامی با استفاده از سامانه‌های رمزنگاری قدرتمند و جدیدتر و الگوریتم‌های امضاء دیجیتال بهینه‌تر
- به کارگیری سیستم پیشنهادی در کنار مکانیسم‌ها و سامانه‌های امنیتی دیگر، به این صورت که پس از بررسی کلی سازوکار و

- Learning," in IEEE Access, vol. 12, pp. 67860-67879, 2024, <https://doi.org/10.1109/ACCESS.2024.3400213>.
- [20] SPIEGEL Staff, Quantum Spying: GCHQ Used Fake LinkedIn Pages to Target Engineers!, DER SPIEGEL, November 2013.
- [21] van Vredendaal, Christine. "Reduced memory meet-in-the-middle attack against the NTRU private key." LMS Journal of Computation and Mathematics 19.A (2016): 43-57. <https://doi.org/10.1112/S1461157016000206>.
- [22] Singh, Sonika, and Sahadeo Padhye. "Generalisations of NTRU cryptosystem." Security and Communication Networks 9.18 (2016): 6315-6334. <https://doi.org/10.1002/sec.1693>.
- [23] Goodin, D. "How the NSA might use Hotmail, Yahoo or other cookies to identify Tor users." Ars Technica (2013). <http://arstechnica.com/security>.
- [24] Zhu, Ye, et al. "Correlation-based traffic analysis attacks on anonymity networks." IEEE Transactions on Parallel and Distributed Systems 21.7 (2009): 954-967. <https://doi.org/10.1109/TPDS.2009.146>.
- [25] Dingleline, Roger, Nick Mathewson, and Paul F. Syverson. "Tor: The second-generation onion router." USENIX security symposium. Vol. 4. 2004. <https://dl.acm.org/doi/10.5555/1251375.1251396>.
- [26] Howgrave-Graham, Nick, et al. "The impact of decryption failures on the security of NTRU encryption." Annual International Cryptology Conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003. https://doi.org/10.1007/978-3-540-45146-4_14.
- [27] Proos, John. "Imperfect decryption and an attack on the NTRU encryption scheme." Cryptology ePrint Archive (2003). <https://ia.ca/2003/002>.
- [28] Nitaj, Abderrahmane. "Cryptanalysis of NTRU with two public keys." Cryptology ePrint Archive (2011). <https://doi.org/10.1109/ISEASP.2017.7976980>.
- [29] Shim, Kyung-Ah. "Security vulnerabilities of four signature schemes from NTRU lattices and pairings." IEEE Access 8 (2020): 85019-85026. <https://doi.org/10.1109/ACCESS.2020.2990413>.
- [30] Xu, Liqing, et al. "Vulnerable Public Keys in NTRU Cryptosystem." Chinese Annals of Mathematics, Series B 41.5 (2020): 657-664. <https://doi.org/10.1007/s11401-020-0225-6>.
- [31] Yadav, Vijay Kumar, S. Venkatesan, and Shekhar Verma. "Man in the middle attack on NTRU key exchange." Communication, Networks and Computing: First International Conference, CNC 2018, Gwalior, India, March 22-24, 2018, Revised Selected Papers 1. Springer Singapore, 2019. https://doi.org/10.1007/978-981-13-2372-0_2.
- [32] S. Khoshnevisan, K. manochehri — "New Method Base on MITM Attack on NTRU Encryption system", Research in Science and Technology - Istanbul-Turkey quantum computer." SIAM review 41.2 (1999): 303-332. <https://doi.org/10.1137/S0036144598347011>.
- [9] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978):120-126. <https://doi.org/10.1145/359340.359342>.
- [10] Hoffstein, Jeffrey, Jill Pipher, and Joseph H. Silverman. "NTRU: A ring-based public key cryptosystem." International algorithmic number theory symposium. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998. pp. 267-288. <https://doi.org/10.1007/BFb0054868>.
- [11] Abo-Alsood, H. H., and H. R. Yassein. "QOTRU: A New Design of NTRU Public Key Encryption Via Qu-Octonion Subalgebra." Journal of Physics: Conference Series. Vol. 1999. No. 1. IOP Publishing, 2021. <https://dx.doi.org/10.1088/1742-6596/1999/1/012097>.
- [12] [A. Ahmadi, M. Dehghani, M. Saleh Esfehiani, "A Problem Solving Method to Boundary of Interval Based Watermark in Anonymous Network Flows", Journal Of Electronical & Cyber Defence Vol. 5, No. 2, 2017, Serial No. 18 \(in persian\). https://ecdj.ihu.ac.ir/article_200141_cfff7f6f5afa0a3158d587f66e5719dd.pdf](https://ecdj.ihu.ac.ir/article_200141_cfff7f6f5afa0a3158d587f66e5719dd.pdf).
- [13] Wang, Tao, et al. "Congestion-aware path selection for Tor." Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected, Papers 16 98-113. Springer Berlin Heidelberg, 2012. doi.org/10.1007/978-3-642-32946-3_9.
- [14] The Tor Stack Exchange, "Tor client pick Tor nodes for circuit creation," Retrieved from <http://tor.stackexchange.com/questions/113/how-does-a-tor-client-pick-tor-nodes-for-circuit-creation> on July 21, 2018.
- [15] Jagerman, Rolf, et al. "The fifteen year struggle of decentralizing privacy-enhancing technology." arXiv preprint, arXiv:1404.4818 (2014). <https://arxiv.org/abs/1404.4818>.
- [16] Ahmad, Imran, et al. "A New Look at the TOR Anonymous Communication System." Journal of Digital Information Management 16.5 (2018): 223. <https://doi.org/10.6025/jdim/2018/16/5/223-229>.
- [17] Wang, Xiao, et al. "An empirical analysis of family in the Tor network." 2013 IEEE International Conference on Communications (ICC). IEEE, 2013. (pp. 1995-2000). <https://doi.org/10.1109/ICC.2013.6654817>.
- [18] [M.Asadi, S. parsa, M. A. Jebreil, V.Majidnezhad "P2P Botnet Detection Using Deep Learning Method", Journal of Electronical & Cyber Defence Vol. 8, No. 2, 2020, Serial No. 30 \(In persian\). https://dor.isc.ac/dor/20.1001.1.23224347.1399.8.2.1.3](https://dor.isc.ac/dor/20.1001.1.23224347.1399.8.2.1.3).
- [19] Z. Zhong, C. Xie and X. Tang, "Intrusion Traffic Detection and Classification Based on Unsupervised

- security." Indonesian Journal of Electrical Engineering and Computer Science 28.2 (2022): 1164-1173. <http://doi.org/10.11591/ijeecs.v28.i2.pp1164-1173>.
- [44] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Linkable ring signature with unconditional anonymity," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 1, pp. 157–165, 2013. <https://doi.org/10.1109/TKDE.2013.17>.
- [45] Wang, Shangping, Ru Zhao, and Yaling Zhang. "Lattice-based ring signature scheme under the random oracle model." International Journal of High Performance Computing and Networking 11.4 (2018): 332-341. <https://doi.org/10.1504/IJHPCN.2018.093236>.
- [46] Zhang, Huang, et al. "Anonymous post-quantum cryptocash." International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018. https://doi.org/10.1007/978-3-662-58387-6_25.
- [47] Beullens, Ward, Shuichi Katsumata, and Federico Pintore. "Calamari and Falafel: logarithmic (linkable) ring signatures from isogenies and lattices." International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-64834-3_16.
- [48] Pohlig, Stephen, and Martin Hellman. "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (corresp.)." IEEE Transactions on information Theory 24.1 (1978): 106-110. <https://doi.org/10.1109/TIT.1978.1055817>.
- [49] Escribano Pablos, José Ignacio, and María Isabel González Vasco. "Secure post-quantum group key exchange: Implementing a solution based on Kyber." IET Communications 17.6 (2023): 758-773. <https://doi.org/10.1049/cmu2.12561>.
- [50] W. Li et al., "High-rate quantum key distribution exceeding 110 Mb s⁻¹," Nat. Photon., vol. 17, no. 5, pp. 416–421, May 2023 <https://doi.org/10.1038/s41566-023-01166-4>.
- [51] Murdoch, Steven J. "Quantifying and measuring anonymity." International Workshop on Data Privacy Management. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. https://doi.org/10.1007/978-3-642-54568-9_1.
- [52] Diaz, Claudia, et al. "Towards measuring anonymity." International Workshop on Privacy Enhancing Technologies. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. https://doi.org/10.1007/3-540-36467-6_5.
- [53] Hoffstein, Jeffrey, et al. "NTRUSIGN: Digital signatures using the NTRU lattice." Cryptographers' track at the RSA conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003. https://doi.org/10.1007/3-540-36563-X_9.
- [54] Odoom, Justice, et al. "Linked or unlinked: A systematic review of linkable ring signature schemes." Journal of Systems Architecture 134 (2023): 102786. <https://doi.org/10.1016/j.sysarc.2022.102786>.
- 14 March 2016 (in Persian). Available: <https://sid.ir/paper/858473/fa>.
- [33] Howgrave-Graham, Nick. "A hybrid lattice-reduction and meet-in-the-middle attack against NTRU." Advances in Cryptology-CRYPTO 2007: 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007. Proceedings 27. Springer Berlin Heidelberg, (pp. 150-169) 2007. https://doi.org/10.1007/978-3-540-74143-5_9.
- [34] Ding, Jintai, Yanbin Pan, and Yingpu Deng. "An algebraic broadcast attack against NTRU." Information Security and Privacy: 17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, July 9-11, 2012. Proceedings 17. Springer Berlin Heidelberg, 2012. http://dx.doi.org/10.1007/978-3-642-31448-3_10.
- [35] Adamoudis, Marios, and Konstantinos A. Draziotis. "Message recovery attack to NTRU using a lattice independent from the public key." arXiv preprint arXiv:2203.09620 (2022). <https://doi.org/10.48550/arXiv.2203.09620>.
- [36] Dingledine, Roger, and Steven J. Murdoch. "Performance Improvements on Tor or, Why Tor is slow and what we're going to do about it." Online: <http://www.torproject.org/press/presskit/2009-03-11-performance.pdf> (2009): 68.
- [37] AlSabah, Mashael, and Ian Goldberg. "PCTCP: per-circuit TCP-over-IPsec transport for anonymous communication overlay networks." Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. 2013. <https://doi.org/10.1145/2508859.2516715>.
- [38] Tor Metrics Project website, "Tor project Anonymity online," Available at <https://metrics.torproject.org>.
- [39] Xu, Liqing, et al. "Vulnerable Public Keys in NTRU Cryptosystem." Chinese Annals of Mathematics, Series B 41.5 (2020): 657-664. <https://doi.org/10.1007/s11401-020-0225-6>.
- [40] [S. H. Hosseinian Barzi, M. Anarfarhad, "Evaluation and proof of routing algorithm in Tor anonymity network", Scientific Journal of Electronic & Cyber Defense Vol. 11, No. 3, Autumn 2023, Serial No. 43. \(in persian\) \[dori.net/dor/20.1001.1.23224347.1402.11.2.1.4\]\(https://doi.org/10.1007/s11401-020-0225-6\)](https://doi.org/10.1007/s11401-020-0225-6).
- [41] Malekian, Ehsan, Ali Zakerolhosseini, and Atefeh Mashatan. "QTRU: a lattice attack resistant version of NTRU PKCS based on quaternion algebra." preprint, Available from the Cryptology ePrint Archive: <http://eprint.iacr.org/2009/386.pdf> (2009).
- [42] Malekian, Ehsan, and Ali Zakerolhosseini. "OTRU: A non-associative and high speed public key cryptosystem." 2010 15th CSI international symposium on computer architecture and digital systems. IEEE, pp. 83-90. 2010. <https://doi.org/10.1109/CADS.2010.5623536>.
- [43] Abdulwahhab, Saba Alaa, Qasim Mohammed Hussein, and Imad Fakhri Al-Shaikhli. "An overview of number theory research unit variant development

- 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC). Vol. 2. IEEE, 2017. <https://doi.org/10.1109/IHMSC.2017.133>.
- [62] Elgzil, Abdelhamid, et al. "Cyber anonymity based on software-defined networking and Onion Routing (SOR)." 2017 IEEE conference on dependable and secure computing. pp. 358-365 , IEEE, 2017. <https://doi.org/10.1109/DESEC.2017.8073856>.
- [63] Kita, Kentaro, et al. "Producer anonymity based on onion routing in named data networking." IEEE Transactions on Network and Service Management 18.2 (2020): 2420-2436. <https://doi.org/10.1109/TNSM.2020.3019052>.
- [64] Ghosh, Satrajit, and Aniket Kate. "Post-Quantum Forward-Secure Onion Routing: (Future Anonymity in Today's Budget)." International Conference on Applied Cryptography and Network Security. Cham: Springer International Publishing, pp.263-286, 2015. https://doi.org/10.1007/978-3-319-28166-7_13.
- [65] Yang, Lei, and Fengjun Li. "mTor: A multipath Tor routing beyond bandwidth throttling." 2015 IEEE Conference on Communications and Network Security (CNS). IEEE, pp. 479-487 2015. <https://doi.org/10.1109/CNS.2015.7346860>.
- [66] AlSabah, Mashaal, et al. "The path less travelled: Overcoming Tor's bottlenecks with traffic splitting." Privacy Enhancing Technologies: 13th International Symposium, PETS 2013, Bloomington, IN, USA, July 10-12, 2013. Proceedings 13. Springer Berlin Heidelberg, pp. 143-163, 2013. https://doi.org/10.1007/978-3-642-39077-7_8.
- [55] Cao, Chengtang, Lin You, and Gengran Hu. "A Novel Linkable Ring Signature on Ideal Lattices." Entropy 25.2 (2023): 237. <https://doi.org/10.3390/e25020237>.
- [56] Aguilar Melchor, Carlos, et al. "Adapting Lyubashevsky's signature schemes to the ring signature setting." Progress in Cryptology–AFRICACRYPT 2013: 6th International Conference on Cryptology in Africa, Cairo, Egypt, June 22-24, 2013. Proceedings 6. Springer Berlin Heidelberg, 2013. https://doi.org/10.1007/978-3-642-38553-7_1.
- [57] Gao, Wen, et al. "Lattice-based deniable ring signatures." International Journal of Information Security 18 (2019): 355-370. <https://doi.org/10.1007/s10207-018-0417-1>.
- [58] Liu, Joseph K., Victor K. Wei, and Duncan S. Wong. "Linkable spontaneous anonymous group signature for ad hoc groups." Information Security and Privacy: 9th Australasian Conference, ACISP 2004, Sydney, Australia, July 13-15, 2004. Proceedings 9. Springer Berlin Heidelberg, (pp. 325-335) ,2004. https://doi.org/10.1007/978-3-540-27800-9_28.
- [59] Farhad Fathi, "Discovering and Blocking Botnets Command and Control Channels in the Anonymous Network with Onion Routing (TOR) ", Master. Thesis, Electrical and Computer Engineering, Tarbiat Modares University, October, 2019.
- [60] Ling, Zhen, et al. "Torward: Discovery, blocking, and traceback of malicious traffic over tor." IEEE Transactions on Information Forensics and Security 10.12 (2015): 2515-2530. <https://doi.org/10.1109/TIFS.2015.2465934>.
- [61] Deng, Ziye, et al. "Identifying tor anonymous traffic based on gravitational clustering analysis." 2017