KHARKIV NATIONAL UNIVERSITY OF RADIO ELECTRONICS

Qualifying scientific work
on manuscript rights

EL HAJ SLEIMAN BATOUL HADI

UDC 621.391

DISSERTATION

OPTIMIZATION MODELS OF FAULT-TOLERANT AND SECURE ROUTING IN A TELECOMMUNICATION NETWORK OVER DISJOINT PATHS

Specialty 172 – Telecommunications and Radio Engineering

Field of study 17 – Electronics and Telecommunications

Applied for the degree of Doctor of Philosophy (Ph.D.)

The dissertation contains the results of the author's own research. The use of other authors' ideas, results, and texts is referenced to the appropriate source
_______________Sleiman B.

DocuSigned by:
Batul Hadi El Khazh Sleiman
AB5F2AB2488845C...
12/25/2023

DS

Supervisor
Yevdokymenko M.O.
Doctor of Engineering Sciences,
Professor

Kharkiv – 2023

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Кваліфікаційна наукова
праця на правах рукопису

ЕЛЬ ХАЖ СЛЕЙМАН БАТУЛ ГАДІ

УДК 621.391

ДИСЕРТАЦІЯ

ОПТИМІЗАЦІЙНІ МОДЕЛІ ВІДМОВОСТІЙКОЇ ТА БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ШЛЯХАМИ, ЩО НЕ ПЕРЕТИНАЮТЬСЯ

Спеціальність 172 – Телекомунікації та радіотехніка

Галузь знань 17 – Електроніка та телекомунікації

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _______________Слейман Б.

Науковий керівник
Євдокименко М.О.
доктор технічних наук,
професор

12/25/2023

Харків – 2023

АНОТАЦІЯ

Ель Хаж Слейман Батул Гаді. Оптимізаційні моделі відмовостійкої та безпечної маршрутизації в телекомунікаційній мережі шляхами, що не перетинаються. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 172 – Телекомунікації та радіотехніка. – Харківський національний університет радіоелектроніки, Харків, 2023.

У дисертаційній роботі розв'язано актуальну науково-практичну задачу, яка полягає в оптимізації процесів відмовостійкої та безпечної маршрутизації за шляхами, що не перетинаються, в телекомунікаційних мережах (ТКМ) шляхом розробки, вдосконалення та дослідження відповідних математичних моделей.

Результати проведеного у роботі аналізу підвередили важливість та пріоритетність забезпечення якості обслуговування (QoS), відмовостійкості та мережної безпеки у сучасних і перспективних телекомунікаційних мережах. При цьому акцентовано увагу на тому, що для досягнення цієї мети має бути максимально використано функціонал передових технологій управління трафіком і, особливо, протоколів маршрутизації. Новітні протоколи маршрутизації повинні підтримувати багатошляхові рішення, розраховувати шляхи, які забезпечують високі показники якості обслуговування та мережної безпеки, а також результативно реалізують схеми локального, сегментного та глобального захисту (резервування) пропускної здатності та елементів мережі в умовах їх одиничних і множинних відмов.

Встановлено, що на перший план виходять задачі щодо вдосконалення математичних моделей, методів і протоколів маршрутизації в ТКМ з їхньою адаптацією під сучасні вимоги. Ефективним напрямком удосконалення моделей і методів маршрутизації є використання шляхів, які не перетинаються, що дозволяє ввести, а в подальшому ефективно та оптимально

використати надлишковість мережного ресурсу для системного підвищення рівня QoS, відмовостійкості та мережної безпеки.

У дисертаційній роботі вдосконалено математичні моделі QoS-маршрутизації в телекомунікаційній мережі шляхами, що не перетинаються. Наукова новизна першої математичної моделі полягає у введенні нових умов балансування пропускної здатності маршрутів і використанні оновленого критерія оптимальності маршрутних рішень, що дозволило забезпечити у процесі маршрутизації максимізацію як кількості, так і сумарної пропускної здатності розрахованих шляхів. Аналіз результатів дослідження показав, що використання запропонованої моделі дає змогу забезпечити максимально можливу пропускну здатність маршрутного рішення, поданого множиною шляхів, що не перетинаються, у випадках високої неоднорідності мережі, тобто коли пропускні здатності каналів зв’язку ТКМ значно відрізняються.

Наукова новизна другої математичної моделі полягає у введенні нових білінійних умов забезпечення гарантованої сумарної пропускної здатності маршрутів, що дало змогу розрахувати шляхи, які мають пропускну здатність, не нижчу за встановлений поріг (вимоги). Виконання цих умови залежно від форми обраного критерію оптимальності може досягатись або на підставі збільшення кількості задіяних маршрутів, що не перетинаються, або шляхом підвищення порогового значення щодо їхньої мінімальної пропускної здатності. Використання вдосконалених моделей дозволило підвищити сумарну пропускну здатність розрахованих шляхів, що не перетинались в ТКМ, від 1,5-10% до 18,6-42%.

У роботі отримали подальший розвиток математичні моделі безпечної QoS-маршрутизації за шляхами, що не перетинаються. Новизна запропонованих моделей полягає у використанні комплексного критерію оптимальності маршрутних рішень, який поруч з показниками пропускної здатності враховує параметри мережної безпеки каналів зв’язку – імовірності їхньої компрометації. Це дозволило забезпечити розрахунок такої множини шляхів у ТКМ, які, по-перше, не перетинались; по-друге, їхня кількість була максимально можливою; по-третє, їхня сумарна пропускна здатність була або максимально можливою, або не нижче заданої; по-четверте, ймовірність компрометації цих шляхів була мінімальною. На розрахункових прикладах продемонстрована функціональність запропонованих математичних моделей, їхня працездатність та адекватність, а також ефективність з погляду реалізації безпечної маршрутизації в ТКМ. Встановлено, що забезпечення гарантій щодо пропускної здатності мультишляху відбувається, як правило, із певним, а іноді і значним запасом, так як лінійні умови забезпечення гарантованої QoS сформульовані для найгіршого випадку, коли всі розраховані та включені у оптимальний мультишлях маршрути, мають приблизно однакому пропускну здатність.

Результати дослідження показали, що застосування запропонованих моделей безпечної маршрутизації в ТКМ дозволяє знизити ймовірність компрометації мультишляхів від 13 до 19% залежно від рівня мережної безпеки каналів зв’язку; знизити ймовірність компрометації конфіденційних повідомлень у середньому від 23-27% до 47-55% для різних варіантів компрометації каналів і маршрутів мережі. Застосування запропонованої моделі безпечної маршрутизації із забезпеченням гарантій щодо рівня якості обслуговування за показником пропускної здатності дозволило покращити ймовірність компрометації мультишляху в середньому від 9-11,5% до 19,5-47% для різних випадків значень імовірностей компрометації каналів зв’язку.

В процесі дослідження вдосконалено модель швидкої перемаршрутизації з підтримкою схем захисту шляху *n*:1 та пропускної здатності мережі, адаптованих під одношляхову та багатошляхову стратегії маршрутизації. Новизна запропонованої моделі полягає у введенні оновлених умов захисту пропускної здатності мережі, що дозволило реалізувати схему захисту шляху *n*:1 без пропорційного збільшення розмірності оптимізаційної задачі. В результаті досліджень встановлено, що при реалізації схеми 2:1 для основного маршруту вдалось підвищити пропускну здатність на 49% та знизити середню міжкінцеву затримку пакетів майже на 40%. При реалізації схеми 3:1 вдалось підвищити пропускну здатність основного маршруту на 86%, а також знизити середню міжкінцеву затримку пакетів для основного маршруту майже на 57,4%, для першого резервного – на 11,7%, а для другого резервного – на 53,6%.

Спільною позитивною рисою запропонованих моделей маршрутизації є їхня орієнтація на отримання саме оптимальних мережних рішень. Застосування оптимальних рішень сприяє покращенню обраних показників якості обслуговування, відмовостійкості та мережної безпеки. Використання цих моделей орієнтує на розв'язання оптимізаційних задач цілочисельної оптимізації. Залежно від типу моделі та введених обмежень на керуючі змінні у роботі засобами середовища MATLAB та бібліотек Python успішно розв'язувались задачі змішаного цілочисельного лінійного або нелінійного програмування. Переважно лінійний характер запропонованих моделей маршрутизації та зменшення кількості маршрутних змінних, які підлягали розрахунку, сприяло зниженню складності їхньої обчислювальної реалізації в разі практичного використання як частини програмного забезпечення маршрутизаторів або SDN-контролерів.

Перспектива подальших досліджень в сфері відмовостійкої маршрутизації стосується реалізації схем захисту не тільки пропускної здатності, але й середньої затримки, імовірності втрат пакетів, а також значень показників якості сприйняття та мережної безпеки.

Запропоновано систему рекомендацій щодо практичного використання запропонованих у роботі рішень з відмовостійкої та безпечної маршрутизації у програмно-конфігурованих мережах. На прикладі використання симулятора Cisco Modeling Labs продемонстровано особливості практичної реалізації розроблених у дисертації рішень. Запропоновано, щоб контролер мережі автоматично збирав та оновлював інформацію щодо стану мережі: її топологію, пропускні здатності каналів зв'язку, вимоги користувачів (потоків) до рівня QoS, QoR та мережної безпеки. Рекомендовано, щоб контролер на основі зібраної інформації про стан мережі розраховував маршрути, що не перетинаються, з використанням програмної реалізації запропонованих моделей маршрутизації у середовищі Python. У подальшому контролер може передавати інформацію про розраховані маршрути на маршрутизатори ТКМ шляхом їхнього програмного віддаленого конфігурування за протоколом SSH з використанням бібліотеки Python Paramiko.

У роботі наведено приклади автоматизованого збору та обробки інформації про стан мережної безпеки елементів ТКМ за допомогою розробленого для цього програмного забезпечення. Представлені фрагменти коду у середовищі MATLAB та на мові Python, який може виконуватись для розрахунку шуканих маршрутів на контролері (сервері) мережі.

Результати дисертаційної роботи впроваджені у ТОВ «СМАРТ ПАВЕР» під час розробки програмного забезпечення для додаткового налаштування мережного обладнання телекомунікаційних мереж з метою підвищення якості обслуговування та мережної безпеки; у ТОВ «Омега Солюшинс» при розробці практичних рекомендацій щодо підвищення рівня мережного захисту та відмовостійкості в телекомунікаційних мережах; у навчальному процесі Харківського національного університету радіоелектроніки на кафедрі інфокомунікаційної інженерії імені В.В. Поповського у процесі викладання дисципліни «Маршрутизація в інфокомунікаціях». Впровадження результатів роботи підтверджено відповідними актами.

За результатами досліджень опубліковано 17 наукових праць, у тому числі 1 монографія, 4 статті у наукових фахових виданнях України, 3 статті та розділи колективних монографій у іноземних періодичних виданнях, які індексуються у базах WoS та/або Scopus; 9 матеріалів міжнародних конференцій, 7 з яких проіндексовані у базах WoS та/або Scopus.

Ключові слова: телекомунікаційна мережа, маршрутизація, маршрут, шлях, оптимізація, модель, протокол, критерій, якість обслуговування, трафік, балансування, безпека, швидка перемаршрутизація, надійність.

ABSTRACT

El Haj Sleiman Batoul Hadi. Optimization models of fault-tolerant and secure routing in a telecommunication network over disjoint paths. – Qualifying scientific work on manuscript rights.

Dissertation for the Doctor of Philosophy (Ph.D.) degree in specialty 172 – Telecommunications and Radio Engineering. – Kharkiv National University of Radio Electronics, Kharkiv, 2023.

The dissertation solves an actual scientific and practical problem of optimizing the fault-tolerant and secure routing processes over disjoint paths in telecommunication networks (TCNs) by developing, improving, and investigating appropriate mathematical models.

The analysis results confirmed the importance and priority of Quality of Service (QoS), fault tolerance, and network security in modern and prospective telecommunication networks. It is emphasized that to achieve this goal, the functionality of advanced traffic management technologies, and especially routing protocols, should be used to the maximum extent possible. The latest routing protocols should support multipath solutions, calculate paths that provide high indicators of Quality of Service and network security, and implement schemes of local, segment, and global protection (redundancy) of bandwidth and network elements under conditions of single and multiple failures.

The problems of improving mathematical models, methods, and protocols of routing in TCN with their adaptation to modern requirements come to the forefront. An effective direction of routing models and methods improvement is the use of disjoint paths, which allows the introduction and further effective and optimal use of the network resources redundancy for systemic increase of QoS level, fault tolerance, and network security.

The mathematical models of QoS routing in a telecommunication network over disjoint paths are improved in the dissertation work. The scientific novelty of

the first mathematical model consists of introducing new conditions for balancing the routes' capacity and using an updated optimality criterion of routing solutions, which allowed to ensure the maximization of the number and total capacity of the calculated paths in the routing process. The analysis of the study results showed that using the proposed model makes it possible to ensure the maximum possible bandwidth of the routing solution represented by a set of disjoint paths in cases of high network heterogeneity, i.e., when the bandwidths of TCN links differ significantly.

The scientific novelty of the second mathematical model consists of introducing new bilinear conditions to ensure guaranteed total routes' capacity, which allows calculating paths with a bandwidth not lower than the established threshold (requirement). Depending on the form of the chosen optimality criterion, these conditions can be met either by increasing the number of disjoint routes involved or by raising the threshold for their minimum bandwidth. Improved models increased the total bandwidth of the calculated disjoint paths in TCN from 1.5-10% to 18.6-42%.

Mathematical models of secure QoS routing over disjoint paths have been further developed in this work. The proposed models' novelty lies in using a complex optimality criterion of routing solutions, which, along with bandwidth indicators, considers the network security parameters of communication links – the probability of their compromise. This made it possible to calculate such a set of paths in TCN, which, firstly, did not intersect; secondly, their number was the maximum possible; thirdly, their total bandwidth was either the maximum possible or not lower than the specified one; fourthly, the compromise probability of these paths was minimal. Computational examples demonstrate the functionality of the proposed mathematical models, their efficiency and adequacy, as well as their effectiveness in terms of implementing secure routing in TCN. It is established that the provision of guarantees for the multipath bandwidth occurs, as a rule, with a certain, and sometimes significant, margin since the linear conditions for ensuring the guaranteed

QoS are formulated for the worst case when all routes calculated and included in the optimal multipath have approximately the same bandwidth.

The research results have shown that the application of the proposed models of secure routing in TCN allows for a decrease in the multipath compromise probability from 13 to 19% depending on the level of network security of communication links and reduce the compromise probability of confidential messages on average from 23-27 to 47-55% for different cases of compromise probability of links and routes of the network. Applying the proposed model of secure routing with Quality of Service guarantees in terms of bandwidth has improved the probability of multipath compromise from 9-11.5% to 19.5-47% on average for different cases of values of links compromise probabilities.

The research improves a fast rerouting model with support for *n*:1 path protection and network bandwidth protection schemes adapted to single path and multipath routing strategies. The novelty of the proposed model consists of the introduction of updated network bandwidth protection conditions, which allowed the implementation of the *n*:1 path protection scheme without a proportional increase in the dimensionality of the optimization problem. As a result of the research, it is established that at the implementation of the 2:1 scheme for the primary route, it was possible to increase bandwidth by 49% and reduce the average packet delay by almost 40%. When implementing the 3:1 scheme, it was possible to increase the bandwidth of the primary route by 86% and reduce the average end-to-end packet delay for the primary route by almost 57.4%, for the first backup route by 11.7%, and for the second backup route by 53.6%.

A common positive feature of the proposed routing models is their focus on obtaining optimal network solutions. Using optimal solutions helps improve selected Quality of Service, fault tolerance, and network security indicators. The use of these models focuses on solving integer optimization problems. Depending on the model type and the restrictions imposed on the control variables, MATLAB and Python libraries have successfully been used to solve mixed integer linear or nonlinear programming problems. The predominantly linear nature of the proposed routing models and the reduction in the number of routing variables to be calculated helped to reduce the complexity of their computational implementation in the case of practical application as part of router software or SDN controllers.

The prospect of further research in the field of fault-tolerant routing concerns the implementation of protection schemes not only for the bandwidth but also for the average delay, packet loss probability, and the values of the Quality of Experience and network security indicators.

A system of recommendations for the practical use of the solutions for fault-tolerant and secure routing in Software-Defined Networks is proposed in the work. Using the Cisco Modeling Labs simulator as an example, the work demonstrates the peculiarities of the practical implementation of the solutions developed in the dissertation. The network controller is proposed to automatically collect and update information about the network state: its topology, bandwidth of communication links, user (flows) requirements to QoS, QoR, and network security level. Based on the collected information about the network state, it is recommended that the controller calculates disjoint routes using a software implementation of the proposed routing models in the Python environment. In the future, the controller can transmit information about the calculated routes to TCN routers by their remote software configuration via SSH protocol using the Python Paramiko library.

The work provides examples of automated collection and processing of information about the state of network security of TCN elements using the developed software. Fragments of code in MATLAB environment and Python language are presented, which can be executed to calculate the required routes and network controller (server).

The results of the dissertation work are implemented in Ltd "SMART POWER" when developing software for additional configuration of network equipment of telecommunication networks to improve the Quality of Service and network security; in Ltd "OMEGA SOLUTIONS" when developing practical recommendations for increasing the level of network protection and fault tolerance in telecommunication networks; in the educational process of the Kharkiv National

University of Radio Electronics at the V.V. Popovskyy Department of Infocommunication Engineering in the course of teaching the discipline "Routing in Infocommunications". Implementation of the work results is confirmed by the corresponding certificates.

According to the research results, the 17 scientific works have been published, including 1 monograph, 4 articles in specialized scientific publications of Ukraine, 3 articles and collective monographs chapters in foreign periodicals, which are indexed in WoS and/or Scopus databases; 9 papers of international conferences, 7 of which are indexed in WoS and/or Scopus databases.

Keywords: Telecommunication Network, Routing, Route, Path, Optimization, Model, Protocol, Criterion, Quality of Service, Traffic, Balancing, Security, Fast Rerouting, Reliability.

LIST OF PUBLICATIONS ON THE DISSERTATION SUBJECT

Monographs:

1. Лемешко, О.В., Єременко, О.С., Євдокименко, М.О., Шаповалова, А.С., Слейман, Б., 2022. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах: Монографія. Харків: ХНУРЕ, 2022. 198 с. DOI: https://doi.org/10.30837/978-966-659-378-1

Articles in specialized scientific publications:

2. Лемешко, А.В., Еременко, А.С., Персиков, А.В., Слейман, Б., 2019. Модель безопасной маршрутизации на основе определения максимального количества непересекающихся путей для минимизации вероятности компрометации конфиденциальных сообщений. Радіотехніка: Всеукраїнський міжвідомчий науково-технічний збірник, 197, С. 31-37. URL: http://openarchive.nure.ua/handle/document/9645

3. Невзорова, О.С., Слейман, Б., Мерсні, А., Сухотеплий, В.М., 2019. Вдосконалення потокової моделі багатоадресної маршрутизації на принципах технології Traffic Engineering. Проблеми телекомунікацій, 2(25), С. 27-36. DOI: https://doi.org/10.30837/pt.2019.2.02

4. Єременко, О.С., Євдокименко, М.О., Слейман, Б., 2020. Удосконалена модель швидкої перемаршрутизації з реалізацією схеми захисту шляху та пропускної здатності в програмно-конфігурованих мережах. Сучасний стан наукових досліджень та технологій в промисловості, 1(11), С. 163–171. DOI: https://doi.org/10.30837/2522-9818.2020.11.163

5. Лемешко, О.В., Грачов, Ю.В., Слейман, Б., 2020. Дослідження методу безпечної маршрутизації конфіденційних повідомлень за шляхами, які не перетинаються. Проблеми телекомунікацій, 2(27), С. 43-55. DOI: https://doi.org/10.30837/pt.2020.2.04

Articles in foreign publications:

6. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Sleiman, B., 2020. Fast

ReRoute Model with Realization of Path and Bandwidth Protection Scheme in SDN. Advances in Electrical and Electronic Engineering, 18(1), pp. 23-30. DOI: https://doi.org/10.15598/aeee.v18i1.3548

7. Lemeshko, O., Yeremenko, O., Yevdokymenko, M. and Sleiman, B., 2019, April. System of Solutions the Maximum Number of Disjoint Paths Computation Under Quality of Service and Security Parameters. In Conference on Mathematical Control Theory, pp. 191-205. Cham: Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-58359-0_10

8. Lemeshko, O., Yeremenko, O., Yevdokymenko, M. and Sleiman, B., 2023, March. Research and Development of Bilinear QoS Routing Model over Disjoint Paths with Bandwidth Guarantees in SDN. In International Conference on Computer Science, Engineering and Education Applications, pp. 223-235. Cham: Springer Nature Switzerland. DOI: https://doi.org/10.1007/978-3-031-36118-0_20

Proceedings of scientific and technical conferences:

9. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Ilyashenko, A. and Sleiman, B., 2019, July. Traffic engineering fast reroute model with support of policing. In 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), pp. 842-845. IEEE. DOI: https://doi.org/10.1109/UKRCON.2019.8880006

10. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Sleiman, B., Hailan, A.M. and Mersni, A., 2019, July. Computation Method of Disjoint Paths under Maximum Bandwidth Criterion. In 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), pp. 161-164. IEEE. DOI: https://doi.org/10.1109/AIACT.2019.8847756

11. Lemeshko, O., Yeremenko, O., Yevdokymenko, M. and Sleiman, B., 2019, December. Enhanced solution of the disjoint paths set calculation for secure QoS routing. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), pp. 210-213. IEEE. DOI: https://doi.org/0.1109/ATIT49449.2019.9030520

12. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Sleiman, B., Segeč, P. and Papán, J., 2020, May. Advanced Performance-Based Fast ReRouting Model with Path Protection. In 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 23-28. IEEE. DOI: https://doi.org/10.1109/DESSERT50317.2020.9125034

13. Yevdokymenko, M., Manasse, M., Zalushniy, D. and Sleiman, B., 2017, October. Analysis of methods for assessing the reliability and security of infocommunication network. In 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), pp. 199-202. IEEE. DOI: https://doi.org/10.1109/INFOCOMMST.2017.8246379

14. Yevdokymenko, M., Sleiman, B., Harkusha, S. and Harkusha, O., 2018, October. Method of fault tolerance evaluation in conditions of destabilizing factors influence in infocommunication network. In 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), pp. 571-574. IEEE. DOI: https://doi.org/10.1109/INFOCOMMST.2018.8632077

15. Lemeshko, O., Yeremenko, O., Yevdokymenko, M. and Sleiman, B., 2019, September. Improvement of the calculation model the set of disjoint paths with maximum bandwidth. In 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1-4. IEEE. DOI: https://doi.org/10.1109/UkrMiCo47782.2019.9165311

16. Євдокименко, М.О., Єременко, О.С., Слейман, Б., 2019. Тензорна модель швидкої перемаршрутизації із захистом рівня якості обслуговування. Третя міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології». Збірник наукових праць. Харків: ХНУРЕ, С. 132. URL: http://openarchive.nure.ua/handle/document/8535

17. Yeremenko, O., Yevdokymenko, M., Sleiman, B., Omowumi, S.O., 2020. Fast ReRouting Flow-based Model with Implementation of Path Protection. Proceedings of Fourth International Scientific and Technical Conference on Computer and Information Systems and Technologies, Kharkiv, Ukraine. NURE, p. 83. DOI: https://doi.org/10.30837/IVcsitic2020201458

CONTENT

LIST OF ABBREVIATIONS AND CONVENTIONS

CM	Confidential Message
CML	Cisco Modeling Labs
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DiffServ	Differentiated Services
EIGRP	Enhanced Interior Gateway Routing Protocol
EPSS	Exploit Prediction Scoring System
FRR	Fast ReRoute
IntServ	Integrated Services
IP	Internet Protocol
MILP	Mixed Integer Linear Programming
MINLP	Mixed Integer NonLinear Programming
MPLS	Multiprotocol Label Switching
NIST	National Institute of Standards and Technology
NP	Network Performance
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
QoR	Quality of Resilience
QoS	Quality of Service
QoE	Quality of Experience
RIP	Routing Information Protocol
SPREAD	Secure Protocol for Reliable dAta Delivery
SSH	Secure Shell
TCN	Telecommunication Network
TE	Traffic Engineering
VoIP	Voice over Internet Protocol

INTRODUCTION

Relevance of the research problems. Improving the efficiency of modern and prospective telecommunication networks directly depends on the amount of available network resources and the level of development of technologies for its management. Traditionally, the network resource is understood as the bandwidth of communication links and computing power of network devices (switches, routers, controllers). Technologies of Physical and Link layers of the Open Systems Interconnection (OSI) reference model laid a robust foundation for the rapid development of TCN in providing information-communication services. However, it is only possible to guarantee the Quality of Service (QoS) by ensuring efficient allocation of network resources between packet flows generated by network applications [1-8].

Quality of Service assurance has been and remains a complex multidimensional problem in which technologies, protocols and mechanisms of all seven OSI layers strongly contribute. Traditionally, an essential role in providing QoS is assigned to the OSI Network layer, which solves IP addressing, routing, and other traffic management tasks – packet marking (IP-prioritization), queuing and allocation of interface bandwidth between them, traffic profiling (shaping and policing), resource reservation, etc. [7-17].

One of the most complex tasks of traffic management and QoS provisioning is the task of packet routing. The routing protocols are responsible for determining the routes that should contain the most productive (high-speed) reliable and secure routers and communication links. In this case, as the analysis [16-25] has shown, the most favorable conditions for increasing TCN reliability, fault tolerance, and network security are provided precisely by routing using disjoint paths. Using disjoint paths, on the one hand, allows the localization of probable network equipment failures in TCN and the use of a reserve resource, and on the other hand, simplifies the analytical calculation and further analysis of fault tolerance and network security indicators.

Successful solution of routing problems is entirely based on a holistic mathematical description of the telecommunication network and systematic consideration of many internal and external factors affecting the state of TCN. First of all, we are talking about mathematical modeling of the network topology, its functional parameters, traffic characteristics, and Quality of Service indicators. In packet routing over disjoint paths, the world's scientists have made significant progress [26-35]. However, the issues of improvement and further adaptation of known theoretical solutions to the requirements related to the optimization of TCN operation from the point of view of using the available network resource and achieving extreme values of the leading indicators of Quality of Service and network security, implementation of schemes of local, segmental and global protection (redundancy) of network parts, especially in the conditions of their multiple failures, are still open.

Thus, the current **scientific and practical task** is to optimize the processes of fault-tolerant and secure routing over disjoint paths in telecommunication networks by developing, improving, and researching appropriate mathematical models.

Relation to scientific programs, plans, and topics. The dissertation work was carried out according to the plan of scientific work of the V.V. Popovskyy Department of Infocommunication Engineering at the Kharkiv National University of Radio Electronics within the framework of the state budgetary theme d/b No 344 "Development of algorithmic and software for cyber resilient information and communication systems and networks of critical infrastructures" (state registration number 0123U100128). In addition, the dissertation is related to the implementation of the provisions of the "Concept of State Policy in the Field of Digital Infrastructure", "National Security Strategy of Ukraine", "Concept of Development of Digital Competencies until 2025", "Concept of Telecommunications Development in Ukraine", recommendations on "Reforms in the field of information and communication technologies and development of the information space of Ukraine".

Purpose of the dissertation work. The purpose of the dissertation is to improve the Quality of Service and network security indicators by ensuring the fault tolerance of TCN when implementing protection (redundancy) schemes for network elements in the event of their possible single or multiple failures.

To solve the scientific and applied problem, the following **research tasks** were solved in the work:

– analysis of theoretical and applied solutions for fault-tolerant and secure routing in telecommunication networks;

– development and research of routing models with Quality of Service assurance in telecommunication networks using disjoint paths;

– improvement and research of secure routing models with Quality of Service assurance in telecommunication networks using disjoint paths;

– development and research of optimization model of fast rerouting in telecommunication networks with implementation of path and bandwidth protection schemes in TCN;

– development of recommendations on the practical implementation of the proposed routing models in Software-Defined telecommunication networks.

The object of research – routing processes in telecommunication networks over disjoint paths.

The subject of research – optimization models of fault-tolerant and secure routing in telecommunication networks over disjoint paths**.**

Research Methods. In the process of development and improvement of mathematical models of routing, the apparatus of operations research, set theory, and graph theory were used. To solve the optimization problems of fault-tolerant and secure routing formulated in the work, the methods of mathematical programming implemented in the Python language and the Optimization Toolbox of MATLAB environment were used. Cisco Modeling Labs (CML) simulator was used to develop recommendations on the practical use of the solutions proposed in this work.

Scientific results developed personally by the dissertator and their novelty:

1. Mathematical models of QoS routing in a telecommunication network over disjoint paths have been improved. The scientific novelty of the first mathematical model consists of introducing new conditions for balancing the bandwidth of routes and using an updated optimality criterion of routing solutions, which allowed to ensure the maximization of the number and total capacity of the calculated paths in the routing process. The scientific novelty of the second mathematical model consists of introducing new bilinear conditions to ensure a guaranteed total bandwidth of routes, which allows calculating the paths having bandwidth not lower than the established threshold (requirement).

2. Mathematical models of secure QoS routing over disjoint paths were further developed. The novelty of the proposed models lies in the use of a complex optimality criterion of routing solutions, which, along with bandwidth indicators, takes into account the network security parameters of communication links – the probability of their compromise. This made it possible to calculate such a set of paths in TCN, which, firstly, did not intersect; secondly, their number was the maximum possible; thirdly, their total bandwidth was either the maximum possible or not lower than the specified one; fourthly, the compromise probability of these paths was minimal.

3. A fast rerouting model with support for *n*:1 path protection and network bandwidth protection schemes adapted to single path and multipath routing strategies is improved. The proposed model's novelty consists of introducing updated conditions for network bandwidth protection, which allows the implementation of the *n*:1 path protection scheme without a proportional increase in the dimensionality of the optimization problem.

Validity and reliability of scientific results, conclusions, and recommendations formulated in the dissertation were confirmed by the results of numerous computational examples for different sets of initial data on the network topology, bandwidths, and probabilities of compromise of its communication links; correct use of the known mathematical apparatus represented by graph theory, set theory, as well as methods of mathematical programming. The implementation certificates and approbation at numerous international conferences supported the scientific results' validity.

Practical value of the results of the dissertation. The practical value of the research results consists in the fact that the mathematical models proposed in the dissertation can become an integral part of mathematical and algorithmic software of routers and controllers of telecommunication networks, the basis of promising protocols of fault-tolerant and secure QoS-routing and fast rerouting. The results obtained were used at the enterprise Ltd "OMEGA SOLUTIONS ", Ltd "SMART POWER", as well as in the educational process of the V. V. Popovskyy Department of Infocommunication Engineering of the Kharkiv National University of Radio Electronics in the process of conducting lectures and practical classes in the course "Routing in infocommunications" for first (bachelor's) level students of specialty 172 – Electronic Communications and Radio Engineering.

Personal contribution of the dissertator. The author obtained all the main scientific results covered in the dissertation work independently. In addition,

– in the monograph [36], the dissertator participated in the preparation of the fifth section, namely "Mathematical models of secure and fault-tolerant routing in telecommunication network over disjoint paths" and subsection 6.2 "Method of secure routing of confidential messages in telecommunication networks over disjoint paths";

– in the article [37], the dissertator researches the model of secure routing with the definition of the maximum number of disjoint paths to minimize the compromise probability of confidential messages;

– in [38], the dissertator studied the processes of multicast routing on the principles of Traffic Engineering technology;

– in [39, 41], the dissertator has improved and investigated the mathematical model of fast rerouting with the implementation of the scheme of path and bandwidth protection in Software-Defined Networks;

– in the publication [40], the dissertator proposed and investigated a method of secure routing of confidential messages over disjoint paths;

– in the article [42], the dissertator has compared QoS indicators and network security indicators, which are provided by the analyzed system of solutions for calculating disjoint paths in TCN;

– in [43], the author improved and investigated the model of secure QoS routing with guaranteed bandwidth of calculated disjoint paths.

Approbation of the dissertation results. The main results of the dissertation were reported and approved at 10 international scientific conferences [43-52]:

– IEEE 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, 2017;

– IEEE International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018;

– IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2019;

– IEEE 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2019;

– IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019;

– IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, Ukraine, 2019;

– 3rd International Scientific and Technical Conference «Computer and Informational Systems and Technologies», Kharkiv, Ukraine. NURE, 2019;

– IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2020;

– Fourth International Scientific and Technical Conference on Computer and Information Systems and Technologies, Kharkiv, Ukraine. NURE, 2020;

– 6th International Conference on Computer Science, Engineering and Education Applications (ICCSEEA'2023), Warsaw, Poland, 2023.

Publications. According to the research results, the 17 scientific works have been published, including 1 monograph, 4 articles in specialized scientific publications of Ukraine, 3 articles and collective monographs chapters in foreign periodicals, which are indexed in WoS and/or Scopus databases; 9 papers of international conferences, 7 of which are indexed in WoS and/or Scopus databases.

Structure and scope of the dissertation. The dissertation consists of the introduction, five chapters, and conclusions, 115 references on 16 pages, and 1 appendix on 3 pages. The total volume of the dissertation is laid out on 156 pages of typewritten text, contains 34 figures (6 figures take up 4 full pages), and 18 tables (3 tables take up 4 full pages). The main text of the dissertation is 110 pages.

CHAPTER 1

ANALYSIS OF THE PLACE AND ROLE OF ROUTING TASKS IN TELECOMMUNICATION NETWORKS

1.1. Characterization of Traffic Management Tasks in Telecommunication Networks

1.1.1. Main Trends in the Development of Telecommunication Networks

The analysis conducted in this work [1-6, 15-17, 36, 53, 54] showed high rates of development of telecommunication systems and networks, which is primarily due to the following main factors:

– significant expansion of the list of infocommunication services provided and supported by means of TCN;

– rapidly increasing demands on the Quality of Service level of network users, especially about bandwidth;

– aggravation of problems of ensuring information and network security, reliability, and fault tolerance of the TCN;

– accelerated growth in network users' number, mobility, and territorial distribution.

These factors lead to further complications of the principles of construction and functioning of TCN, the level of their convergence, and heterogeneity. Every year, the list and variety of terminal, network, and server devices and their software are expanding. The requirements are improving network protocols of all OSI levels. Thus, modern TCNs are complex organizational and technical systems built on open standards to ensure hardware and software compatibility of terminal and network equipment. The multiservice nature of modern and prospective TCNs should be accompanied by high reliability, fault tolerance, and availability.

In addition, more and more network tasks related to monitoring, analyzing, and controlling the state of TCN must be solved automatically or automated using efficient control equipment (servers, controllers, etc.) and protocols. This primarily concerns real-time processes, where human administrator intervention can introduce additional delays and, often, errors into the control loop.

On the other hand, the more TCN functions are transferred to network technologies and separate protocols, the more acute the problem of providing scalability of network solutions. Increasing network load, increasing level of service differentiation, and diversity of communication equipment complicate the work of network protocols and require their continuous improvement, including in the direction of ensuring high scalability of TCN.

The selection of certain network technologies when constructing multiservice telecommunication networks depends on the degree of satisfying a *set of requirements* dictated by all participants of the information and communication process – users, telecommunication operators, and manufacturers of various telecommunication equipment and software [1-3, 36]. The main requirement for TCNs is to fulfill its main function – to provide users with a wide range of communication services while ensuring a specified level of quality of service, resilience, and security.

The complex set of requirements for modern TCNs can be summarized as follows [1-3]:

– provide a wide range of gradations for *customer Quality of Service,* support for service classes;

– high TCN *performance* based on the efficient use of network resources (link, buffer, computing, software and information);

– TCN *reliability* both at the operational level (*fault-tolerance*) and at the packet delivery level (probability of delivery);

– high *scalability*, that is, the ability of TCN to retain their efficiency indicators within a given range in the conditions of increasing network size, number of users, and services, which is achieved by TCN segmentation and the use of hierarchical structural and functional construction;

– support for complex *network security* hardware and software solutions that should be provided at all levels of service delivery.

To meet the above requirements and consider the main trends in the development of modern TCN, the creation and operation of a Software-Defined Network (SDN) is now being actively implemented in practice [5, 6]. The main principles of SDN operation include separation of the user data transmission level from the management level; availability of a unified, vendor-independent interface between the management level and the data transmission level; increasing the level of network management centralization; virtualization of physical network resources, etc.

1.1.2. Analysis of Telecommunication Network Performance Indicators

A telecommunication network, like any other complex system, requires an assessment of its efficiency level using a variety of indicators. First of all, it is about the indicators of Quality of Service, reliability (fault tolerance), and network security. As shown in [1-4, 53-55], to determine the level of QoS, indicators are used, which, depending on the measurement method, are divided into Quality of Experience (QoE) and Network Performance (NP) indicators. QoE indicators characterize the degree of satisfaction with the service at the user level, and NP indicators – at the network level.

QoE values are represented by the corresponding Mean Opinion Score (MOS) [58-60]. In addition to network and traffic parameters, they are also influenced by the characteristics of terminal equipment.

Network Performance metrics are traditionally categorized into three types:

– bandwidth indicators (minimum, average, and maximum packet rate);

– time indicators, which are represented by the average delay and jitter (delay variation) of packets;

– reliability indicators related to the level (probability) of packet losses.

The ITU-T Y.1541 recommendation (Table 1.1) provides examples of requirements for quantitative values of specific NP indicators [57].

Table 1.1

IP network QoS class definitions and network performance objectives

Network performance parameter	Nature of network performance objective	QoS Classes					
		Class 0	Class 1	Class 2	Class 3	Class 4	Class 5
IPTD	Upper bound on the mean IPTD	100 ms	400 ms	100 ms	400 ms	1 s	U
IPDV	Upper bound on the $1-10^{-3}$ quantile of IPTD minus the minimum IPTD	50 ms	50 ms	U	U	U	U
IPLR	Upper bound on the packet loss probability	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	U
IPER	Upper bound	1×10^{-4}					U
"U" means "unspecified" or "unbounded". IPTD – IP packet Transfer Delay IPDV – IP packet Delay Variation IPLR – IP packet Loss Ratio IPER – IP packet Error Ratio							

Table 1.2 shows examples of QoS classes according to ITU-T recommendation Y.1541 and the list of network mechanisms and technologies used to provide them [57].

Table 1.2

Guidance for IP QoS classes

QoS class	Applications (examples)	Node mechanisms	Network techniques
0	Real-time, jitter-sensitive, high interaction (VoIP, Video Teleconference)	Separate queue with preferential servicing, traffic grooming	Constrained routing and distance
1	Real-time, jitter sensitive, interactive (VoIP, Video Teleconference).		Less constrained routing and distances
2	Transaction data, highly interactive (Signaling)	Separate queue, drop priority	Constrained routing and distance
3	Transaction data, interactive		Less constrained routing and distances
4	Low loss only (short transactions, bulk data, video streaming)	Long queue, drop priority	Any route/path
5	Traditional applications of default IP networks	Separate queue (lowest priority)	Any route/path

To assess the level of reliability and fault tolerance of equipment and the whole network (Quality of Resilience, QoR), the Availability Factor (AF) can be used as an indicator [16]. This indicator is calculated as the ratio of the time when the device (network) was in an operable state to the total operation time of the device (network). Since the AF value ranges from 0 to 1, it is sometimes interpreted practically as the probability that the device (network) is operable.

To analyze the level of network security, a set of indicators, such as Common Vulnerability Scoring System (CVSS) and Exploit Prediction Scoring System (EPSS), can be used [36, 53, 54]. In some cases, the CVSS Scores and EPSS Scores are used in parallel with information security risk indicators and the probability of compromising a confidential message, router, link, path, or network in general.

As shown by the analysis [1, 16, 55], to ensure the specified indicators values of QoS, reliability (fault tolerance), and network security, it is necessary to use the functionality of all OSI layers systematically. This is especially true for the OSI network layer (Table 2.1), where the following main tasks of traffic management are solved [3, 7, 8]:

- Classification and Marking of Traffic (packets);
- Congestion Management (Scheduling);
- Congestion Avoidance;
- Traffic Shaping and Traffic Policing;
- Resource Reservation;
- Routing.

Most of the above traffic management tools are implemented at network nodes and are focused on local improvement of QoS, QoR, and network security. Routing tools play an essential role in providing end-to-end TCN performance indicators. The routing protocols can select optimal packet transmission routes regarding Quality of Service, reliability, or network security [1, 7, 8]. In practice, this is usually done administratively by tuning the appropriate routing metrics and then using DUAL, Bellman Ford's, and Dijkstra's algorithms. The efficiency of routing solutions in general is determined by the type of the used mathematical model and method (algorithm) of route calculation.

1.2. Classification of Routing Solutions in Telecommunication Networks

Nowadays, there are quite many different types of routing solutions. They can be classified by conditionally dividing them into certain classes (groups) according to the chosen classification feature. First of all, route solutions, depending on the purpose and type of performance indicators which these solutions are aimed at improving, can be divided into [1, 7, 8, 16, 21]:

- QoS routing, in which the goal is to improve the Quality of Service indicators (Table 1.1);

– fault-tolerant routing aimed at improving the reliability and availability of network elements, its services, and TCN in general;

– secure routing implemented to improve the level of network security;

– hybrid routing, where several dissimilar QoS, QoR, and network security metrics are improved simultaneously.

Fault-tolerant routing solutions are based on introducing a certain redundancy associated with protecting one or another element (one or more) of the network in case of failure. That is, it is necessary to calculate a backup path that does not include the failed network element next to the primary route. The main reasons that can lead to service failures on the part of network equipment are as follows:

– low reliability, e.g. due to aging or accidental operating conditions;

– hardware or software failures caused, e.g., by power supply problems, etc.;

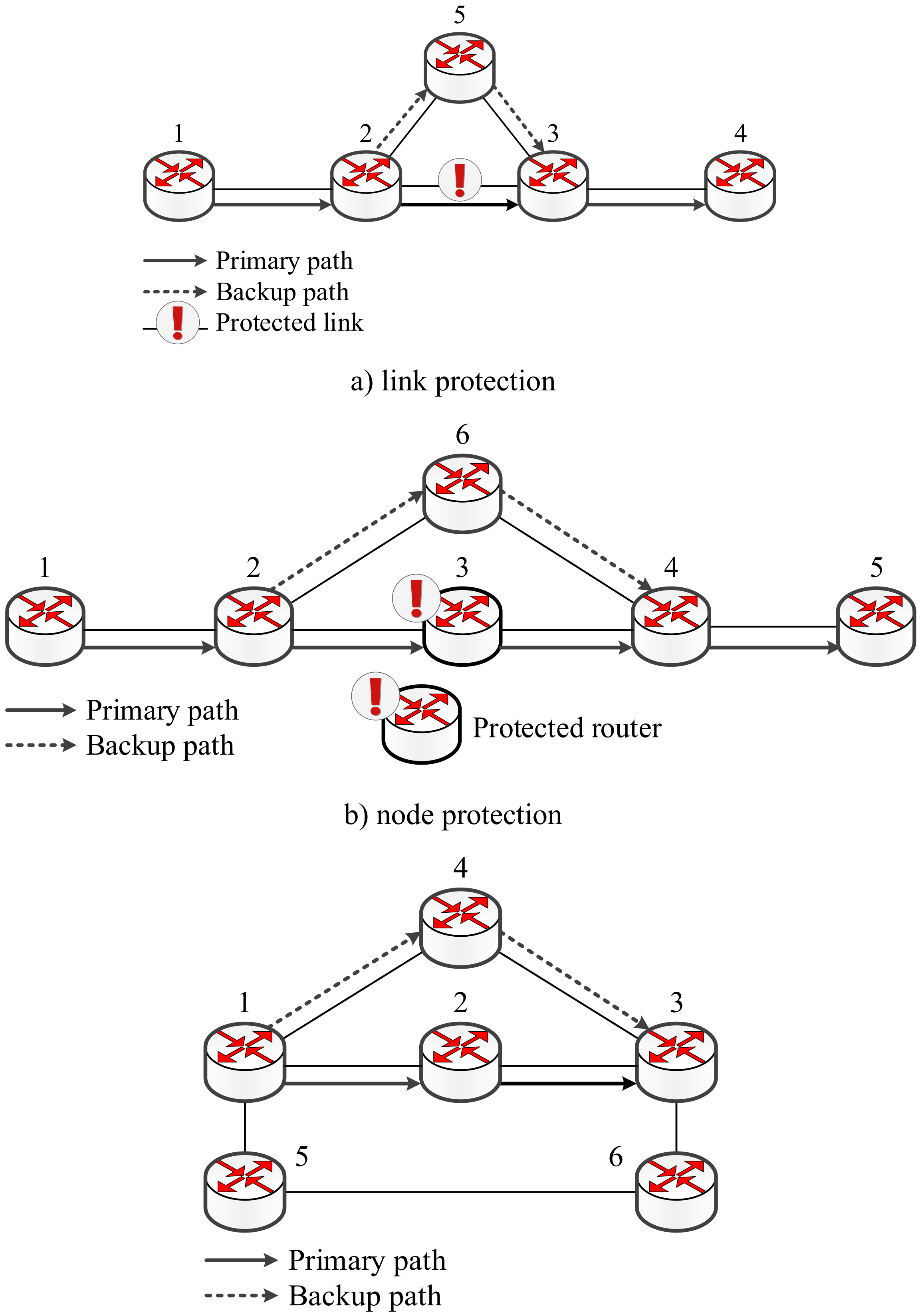
– network traffic overload, which may be caused by inefficient network configuration or critical network load in general;

– compromise by the attacker as a result of successful execution of network attacks;

– hostile diversions, natural disasters.

Fault-tolerant routing can be divided into local, segment, and global protection. Local protection includes protection (redundancy) schemes for a link (Fig. 1.1 a) or a node (Fig. 1.1 b) [1, 16]. Segment protection is used when multiple failures of several TCN links and/or nodes occur. Global protection can protect the primary route (Fig. 1.1 c) when the backup route does not share common elements with the primary route except for border routers – source-destination pair [1, 16].

The EIGRP (Enhanced Interior Gateway Routing Protocol) is an example of a fault-tolerant routing protocol. In this protocol, the primary routes are stored in the routing table, and the backup routes are stored in the topology table [7, 8]. Due to the presence of precomputed backup paths, the routing process is greatly accelerated. Instead of tens of seconds, applying a backup solution takes tens of milliseconds, so such solutions belong to the Fast ReRoute (FRR) class.



a) link protection

b) node protection

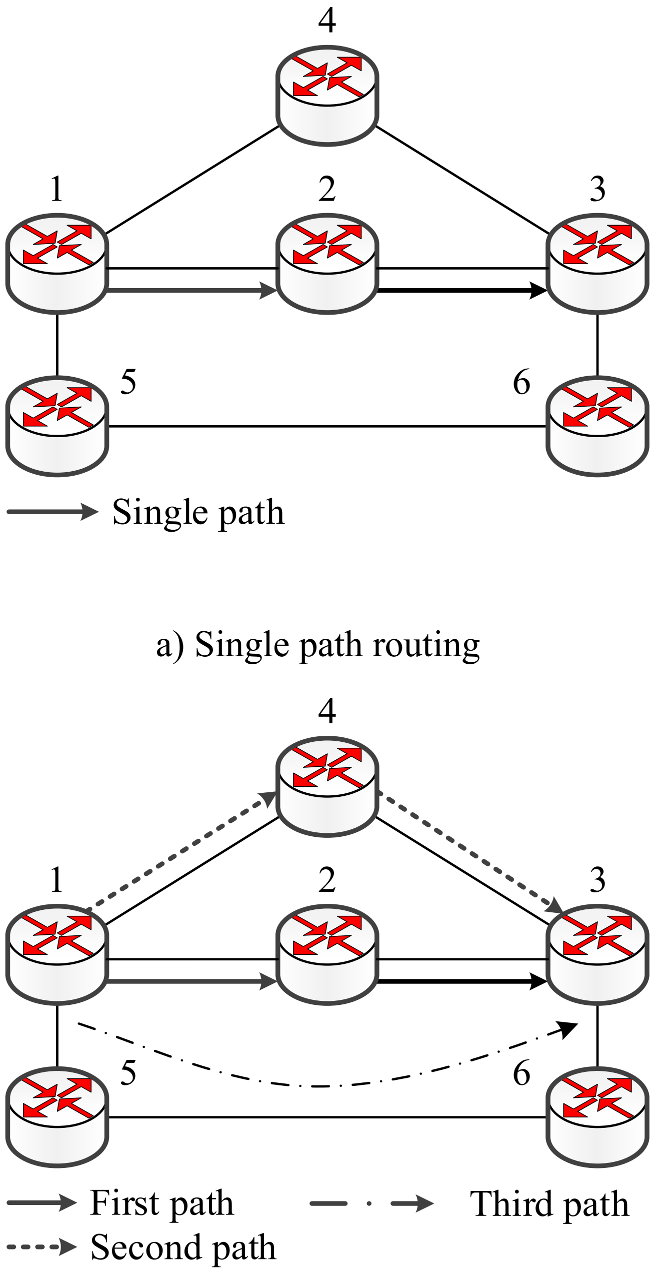
c) path protection

Fig. 1.1. Local and global protection schemes

In general, not only nodes, links, and routes can be protected, but also Quality of Service indicators. This happens when both the primary and backup paths are guaranteed a certain level of QoS, most often concerning, for example, bandwidth. In this case, the primary and backup paths must have a bandwidth that is equal to the established norm. Depending on the requirements regarding the level of reliability and fault tolerance in the routing process, one or another type of redundancy can be implemented [1, 16]:

- 1+1 scheme, in which the data flow is transmitted both over the primary and over the backup route;
- 1:1 scheme, when for each primary route a backup one is created over which the data will be transmitted in case of failure of the primary path;
- *n*:1 scheme, in which one backup path is created for n primary paths (facility backup);
- 1:*n* scheme, in which n backup paths are created for one primary;
- *n*:*m* scheme, which is the most common case where *m* backup paths are supported for *n* primary (working) paths.

Depending on the number of calculated and used paths, a distinction is made between a single path and multipath routing (Fig. 1.2). In single path routing, a single route is calculated between a pair of "source-destination" border routers. In multipath routing, there should be two or more such routes between "source-destination" routers. A multipath is the set of distinct paths used in the routing process between a single pair of "source-destination" routers. Implementing multipath routing in practice is more complex both computationally and in terms of support. However, multipath routing is considered to be a more efficient solution for QoS, QoR, and network security.



a) Single path routing

b) Three path routing

Fig. 1.2. Examples of single- and multipath routing

Among multipath solutions, there is a separate class of solutions that deals with the computation and utilization of disjoint paths. Paths are disjoint if they have no common network elements except source and destination border routers. Figure 1.2 b shows an example of using three disjoint paths.

As shown in papers [18-23], using a set of disjoint paths is a compromise solution to the relatively high computational complexity associated with the computation of both the routes themselves and indicators of the QoS, fault tolerance, and network security.

1.3. Overview of Promising Solutions in the Field of Fault-Tolerant, Secure and QoS Routing in Telecommunication Networks

1.3.1. Analysis of Routing Solutions over Disjoint Paths

As described in works [22, 23], using a set of disjoint paths is a proactive means of ensuring and improving the reliability and fault-tolerance of the network, since the failure of one route will not affect the performance of others. In implementing the reactive approach to increasing the fault tolerance TCN, it is necessary to compute both the primary and the backup routes, which do not intersect by nodes or links [22].

As shown in [19, 20], using a set of disjoint paths is the main condition for implementing secure routing. Thus, the more routes it is possible to use during the fragmented transmission of a confidential message, the less the probability of its compromise can be provided by the network.

Therefore, the scientific and practical task related to developing efficient computation models and methods for finding the maximum number of disjoint paths that can be used in developing appropriate routing protocols in providing QoS, QoR, and network security is relevant.

As shown by the analysis [21-35], in publications devoted to solving routing problems, enough attention is paid to calculating the disjoint routes set and *k*-path routing. The peculiarities of these approaches are presented below.

Thus, in [26], a complex solution is proposed: a secure fault-tolerant routing scheme with a disjoint multipath calculation based on a distributed and in-network verification scheme. However, the presented schemes are heuristic and oriented only to applications in wireless sensor networks.

However, in [22], the method of secure fast rerouting of messages in the network, related to the class of proactive and reactive solutions to provide a given level of information security, has been developed. The novelty of the method is that in the event of a breach of the requirements of information security in the network caused by an increased probability of compromising one or a set of composite disjoint paths included in the primary multipath, the transmission of parts of the confidential message with the provision of the specified values of the probability of its compromise will be implemented already by a set of precomputed backup composite paths, implementing the protection of either the primary multipath in general or one or more predefined composite paths that are included in this primary multipath.

In [27], the algorithms for determining a node-disjoint path pair visiting specified nodes are proposed. In this work, the heuristics were presented, which allow providing the solution of finding a minimum cost disjoint pair of primary and backup paths. At that time, the authors tried to find a solution, which should be close to the optimum, within a reasonable running time.

However, the limitation of the presented solution is the single path routing strategy used under consideration. In turn, in [28], an effective heuristic of global path protection with obtaining the maximum-bandwidth disjoint paths (primary and backup) is presented. The advantages of the proposed solution are the QoS support (bandwidth protection) and sufficient computational complexity.

The works [29-31] are devoted to the tasks of calculating exactly the *k* paths. Thus, in [29], a solution was found to search for a set of disjoint paths between the source and destination, so that the total length of the paths is minimized and a given weight budget bounds the weight. In [32], authors pay attention to the issue of reducing the total time necessary to calculate the primary and backup end-to-end disjoint paths. The paper shows that this problem is relevant for the situation when network equipment fails, leading to several attempts to determine the corresponding alternative paths and periodic updates of the fault-tolerant routing scheme.

The node-disjoint multipath routing algorithm for wireless mesh networks was proposed in [33]. This work introduces the source routing in the routing discovery process, and the node-disjoint routes are calculated. The advantage of this node-disjoint multipath selection lies in the fact that this algorithm is easy to realize. In [34], an improved and simplified algorithm is proposed to calculate the disjoint minimal path set. The advantages of this solution are its efficiency and accuracy, and the ability to analyze the reliability of large-scale networks.

Work [35] also presents a heuristic algorithm for *k*-path QoS routing, in which it is necessary to find *k* disjoint paths from the source to the destination when fulfilling the requirements for Quality of Service. It is known that the task of finding *k* paths belongs to an NP-complete class. This task is formulated as an optimization problem for Boolean programming, and a heuristic algorithm is proposed for solving this problem, the efficiency of which is proved and demonstrated on numerical examples. While in [25], a linear optimization model is proposed for calculating the maximum number of disjoint paths with the minimum probability of compromising a confidential message.

Thus, the analysis of existing solutions has shown the urgency of developing an effective computational model of the maximum number of disjoint paths in multipath routing with the possibility of its application as an algorithmic base of the corresponding protocol solutions, which should be oriented on ensuring the QoS, QoR, and network security.

1.3.2. Analysis of Existing Works on QoS-Routing over Disjoint Paths

The analysis [42, 61-73] shows that multipath routing over disjoint paths is an effective solution for better resource allocation, scalability, network resilience, and security. Moreover, such an approach for multipath routing is often utilized for Quality of Service and Quality of Experience improvement. Consider in more detail the results of some recent research in this area.

Thus, in [63] the need to develop search algorithms for multiple disjoint paths is substantiated. Furthermore, the corresponding algorithms must satisfy the demands of computational complexity to achieve scalability. Having such a set of routes adds more value to the multipath. In addition, it is noted that a set consisting of only two disjoint paths is usually used. This approach is widely used in fault-tolerant routing, where one route is used as the primary and the other as a backup. Thus, in [63] an efficient algorithm for calculating multiple disjoint paths with acceptable computational cost and ensuring scalability is proposed and investigated. Moreover, in [64], the authors propose One-Shot Multiple Disjoint Path Discovery Protocol (1S-MDP) that can provide both node-disjoint or link-disjoint paths.

The widespread use and application of disjoint paths routing are found in Mobile Ad-hoc Networks (MANETs). The specifics of this type of network impose certain limitations when developing routing algorithms. First, you should consider the dynamics of the MANET topology, error-less data broadcasting, and the need to ensure a high level of fault tolerance and security. For example, in [65], a link-disjoint multipath routing method was proposed to choose the shortest path from multiple paths in MANET. Moreover, the simulation results proved the possibility of using and efficiency in the traffic load of the proposed method in a dynamic environment.

Also, many current research works relate to improving the Quality of Service during QoS routing and implementing the strategy of disjoint multipath routing [66-71], including applying the Traffic Engineering (TE) concept principles [68]. Additionally, in [69], the authors consider adaptive multipath routing over both shortest and non-shortest disjoint paths.

While in [71], a novel multipath transport scheme for real-time multimedia using disjoint multipath and segment routing in Software-Defined Networks is proposed. It is noted that satisfactory Quality of Experience (QoE) level currently remains an urgent task. Thus, in the solution [71], the SDN controller centrally calculates multiple disjoint paths meeting bandwidth requirements and load balancing in the network. In this case, sub-flows are transmitted over disjoint paths to reduce the end-to-end delay and improve QoE.

Whereas, in [11-13, 74, 75], the tensor QoS routing approach is used, which is promising and allows providing QoS indicators when transmitting flows of different classes. These models can be used for centralized route calculation on SDN and SD-WAN controllers.

1.3.3. Analysis of Methods and Mechanisms of Secure Routing in TCN

As the analysis of [1, 19, 22, 25, 26, 36, 76-85] has shown, multipath secure routing is widely used in technologies such as Software-Defined Networking (SDN), IoT, MANET, SDN-VANET, etc. Let us consider some of them in more detail.

In [77], a new heuristic approach for *Secure Multi-Party Computation* (SMPC) routing is proposed. In this case, routing involves coordination between mutually "untrustworthy" parties leading to the requirements, according to which the Border Gateway Protocol (BGP) provides autonomy, flexibility, and confidentiality through distributed policy-based execution of decisions throughout the iterative route calculation. This approach has poor convergence and makes scheduling and ensuring resilience challenging. Hence, in [77] a fundamentally different approach to the SMPC-based multi-party route computation is proposed, which provides a better guarantee of privacy than the BGP and allows deploying new paradigms of policies.

In [78], a secure overlay routing algorithm is further developed based on the probabilistic key redistribution scheme, which has become widely used in wireless networks. A scalable solution for high-dimensional networks with more than one thousand nodes is proposed based on the *Deterministic Dijkstra-based Algorithm* (DDA) algorithm, which allows the calculation of optimal secure paths in overlay wireless networks under the time complexity, which is much lower than in the original algorithm. In addition, in [78], an appropriate approximation for finding the path close to the optimal one with an accuracy of up to 1% compared to the DDA is proposed.

In [19], mechanisms of SPREAD (*Secure Protocol for Reliable dAta Delivery*) and H-SPREAD (*Hybrid Secure Protocol for Reliable dAta Delivery*) enhancement of secure messaging in MANET are presented and investigated. The basic idea is to split the confidential message into several fragments – parts, and then transfer these parts from a source to a destination over a set of disjoint paths so that even if a certain number of parts of the message is compromised, the secret message as a whole remains uncompromised. The overall system architecture is proposed: a mathematical model for creating and reconstructing parts of a message, optimal distribution of its parts in several paths from a security perspective, and approaches for multipath calculation in MANET networks.

In [79], it is proposed to consider information security risks when choosing a route in TCN. This is ensured by the appropriate formation of routing metrics when they, together with the QoS indicators, consider the risk indicators of information security of the routing system elements. This approach allows to dynamically select the most secure route for transmitted flows, both in the conditions of active attacks and in the passive risk analysis of the routing system.

The main disadvantage of existing works is that they cannot explicitly satisfy both network security requirements and Quality of Service parameters. Therefore, it is relevant to develop an appropriate model of the disjoint paths set calculation for *Secure QoS Routing*, which allows the calculation of a set of routes that meets network security requirements together with QoS indicators.

1.3.4. Analysis of Methods and Mechanisms of Fault-Tolerant Routing in TCN

The analysis [1-8, 16-18, 86-111] showed that the task of using routing protocols and traffic management means for the coordinated assurance of QoS, fault-tolerance and network security in the network becomes urgent. Furthermore, the requirements for computational complexity and scalability of the network solutions have increased.

The means of Fast ReRouting are applied in the case of a particular network element (link, node, segment or the entire path) failure when the transmitted packet flow should be switched to the backup one [1, 16-18]. Besides, FRR-related technological routing solutions may support several redundancy schemes: 1+1, 1:1, *n*:1, 1:*n*, *n*:*m* [16]. Usually, the technical task of FRR is formulated as a calculation of a set of disjoint paths [62, 90, 101, 107], which meets the requirements for increasing the routing fault tolerance regarding the protection of paths and their bandwidth.

It should be noted that routing with disjoint paths is an effective functional tool for increasing the reliability of the TCN [16-18]. In this case, the primary and several backup routes are selected among the set of calculated paths, with the implementation of one or another local or global protection scheme (redundancy) of the TCN. Therefore, during the fast rerouting in the event of failure of the primary path caused by overload or failure of one or another network element, the packets will be almost instantly (with a delay of 40-50 ms) switched to the backup path.

As shown by the analysis [1, 16-18, 22, 32, 36, 98], a large part of the known theoretical solutions regarding routing over disjoint paths, in favor of low computational complexity and acceptable scalability, is based on heuristic algorithms. However, such solutions generally do not fully consider the features of the structural and functional construction of modern TCNs and do not provide the maximum values of the selected performance indicators for the network, for example, its performance or security level. Unlike heuristic algorithms, optimization models and methods are increasingly being used for solving multipath routing problems over disjoint paths, taking into more detail the features of statement and final solution requirements. This is especially true of ensuring optimal values of TCN performance indicators [1, 22, 36].

1.3.5. Analysis of Fast ReRoute Solutions in Software-Defined Networks

The significant interest in Software-Defined Networks (SDN) is due to many reasons and advantages compared to traditional networks. The use of softwarized networking approaches makes it possible to make traffic management more flexible and use optimization techniques for different purposes [1, 5, 6]. The practical application of SDN solutions is directly related to increasing the efficiency of providing a given level of Quality of Service [5]. Since the control plane is separated from the data plane, containing network equipment, the so-called router's programming based on table-based forwarding becomes possible [5, 36].

Due to various reasons and requirements for Quality of Service, fault tolerance, and security, different types of SDN architectures are used [5, 36, 94, 111]. Fig. 1.3 represents the primary differences between conventional (traditional) networks and SDN [1, 5, 36]. At the same time, one should consider the existing deployment of communication networks, which include both SDN devices and traditional network equipment. In this way, hybrid SDNs are organized [1, 5].

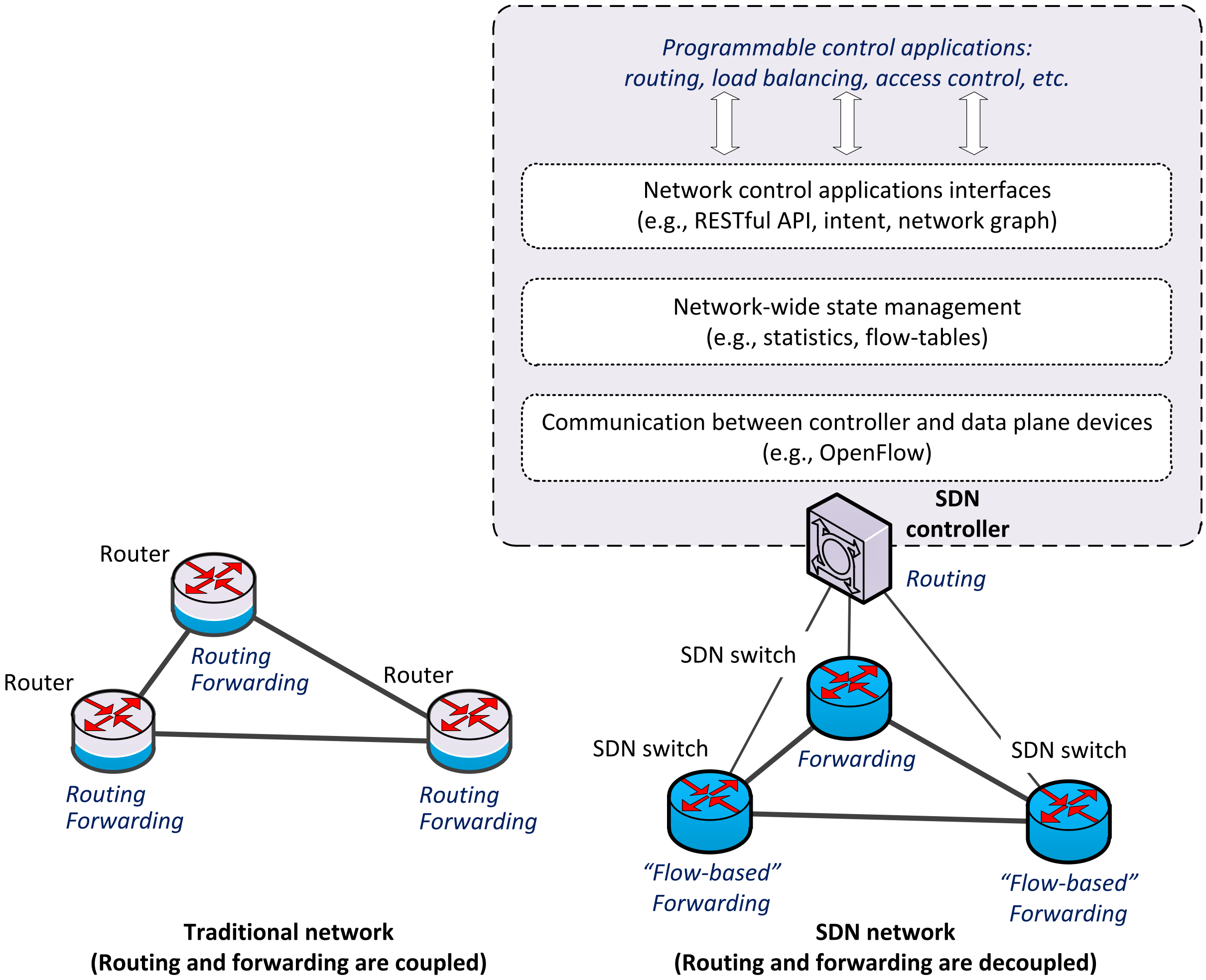

Programmable control applications:
routing, load balancing, access control, etc.
Network control applications interfaces
(e.g., RESTful API, intent, network graph)
Network-wide state management
(e.g., statistics, flow-tables)
Communication between controller and data plane devices
(e.g., OpenFlow)
SDN
controller
Routing
SDN switch
Forwarding
SDN switch
SDN switch
"Flow-based"
Forwarding
"Flow-based"
Forwarding
Router
Routing
Forwarding
Router
Router
Routing
Forwarding
Routing
Forwarding
Traditional network
(Routing and forwarding are coupled)
SDN network
(Routing and forwarding are decoupled)

Fig. 1.3. Difference between traditional networks and SDN [1, 43]

It is noted that appropriate routing tools are actively used to ensure the

Quality of Service, network security, and fault tolerance under established requirements [1, 16-18]. One of the well-known directions is disjoint routing solutions. Therefore, the presented work is devoted to improving the mathematical model of routing by disjoint paths, which can serve as a basis for QoS routing protocols in the SDN data plane.

As known, within the framework of Software-Defined Networks, the distribution of the data plane and control plane is performed. In this case, if a particular network element (link, node, segment or the entire path) fails, it must be detected, and the controller must take certain steps to quickly restore the transmission of the affected data flows [1, 16, 94, 96]. The number and type of such failures, as well as the need for reconfiguration and rerouting calculations, increases the load on the network controllers. Existing Fast ReRoute mechanisms for IP/MPLS networks can be migrated to SDN, but in this case, the OpenFlow switch limited routing tables and the complexity of FRR implementation should be taken into account [94, 97].

During FRR, the implementation of the main schemes for protecting network elements from failures is a key technological challenge in deploying both enterprise and global SDNs of different types [16, 17]. The multiservice of modern networks requires the implementation of not only schemes of protection of its topological elements – link, node, path, but also protection of the Quality of Service level in the network as a whole [10-14]. As the first step in this direction, we can consider the protection of bandwidth [99-101] with the future prospect of protecting other QoS indicators: the average end-to-end delay, the acceptable packet loss [74, 75, 102], etc.

Quite often, the technical task of FRR is formulated as a task for calculating a set of disjoint paths [1, 16]. This formulation of the task meets the requirements for increasing the fault tolerance of routing solutions, especially in need of protection of paths and their bandwidth. Consequently, the actual scientific and practical task of developing and researching the Fast ReRoute model with a realization of the path and bandwidth protection scheme, which can be used in MPLS for SDN, seems to be relevant. In this case, the model should provide scalability of the resulting solutions and low computational complexity of their subsequent protocol implementation.

An analysis of existing solutions has shown the relevance of developing approaches to fast rerouting in the direction of implementing MPLS in the SDN (Table 1.3). In general, modern approaches to the use of mechanisms for fast rerouting in the SDN when implementing various protection schemes of network elements, such as classical (link, node, etc.), and specific schemes for this type of networks, can be divided into heuristic, graph and flow-based [97, 103-111]. A more detailed description of the solutions analyzed is presented in Table 1.3.

From Table 1.3, it is possible to conclude that the most common methods for solving FRR problems are heuristic approaches, and among the schemes for increasing resilience, the local protection (link, node or controller protection) is still prevalent. However, it is known that the flow-based approaches, usually based on the optimization of the rerouting tasks, which primarily aim at optimizing the use of available network resources, are the most promising [109-111].

Among the disadvantages of existing solutions when implementing MPLS SDN FRR it should be noted that the implementation of the protection scheme of the path with a 1:*n* redundancy scheme, as a rule, leads to an increase in *n* times the size of the optimization problem in calculating the routes [99-102]. If a solution is proposed for a multipath FRR, the need to formulate and solve a nonlinear optimization problem occurs [99]. These factors critically impact the computational complexity and scalability of protocol routing solutions that an SDN controller must centrally obtain.

The aim of the research is to improve the known solutions of performance-based Fast ReRouting, directed towards path protection with the maximum bandwidth of the used routes and links, which they include.

Table 1.3

MPLS SDN FRR Related Researches

Ref.	Description of Contribution	Protection Scheme	Key Technologies Used
[103]	The mechanism of recovery for rerouting of flows in the case of link failures for multi-radio multi-channel Software-Defined Wireless Mesh Networks (SD-WMN) is proposed, where the recovery time and bandwidth of the communication links as key indicators for assessing the performance of recovery scenarios after failures are selected. Type of solution: heuristic. Advantages: reducing the recovery time compared to conventional routing protocols at the best achievable bandwidth.	Link protection	SD-WMN
[97]	The solution for local fast recovery in SDN without controller intervention in the case of a single node or link failure if it is topologically possible is proposed. The possibility of using (remote) loop-free alternates ((r) LFAs) in fast rerouting in SDN is shown. Type of solution: heuristic. Advantages: maximizing coverage, minimizing computational complexity, detecting and avoiding looping.	Link protection, node protection	SDN, LFA

Continuation of Table 1.3

[104]	The mechanism of destination-specific Maximally Redundant Trees (dMRTs) with the aim of the use the fast rerouting in SDN and Hybrid SDN is presented. Type of solution: heuristic. Advantages: less overhead in SDN, shorter backup path, high scalability.	Link protection, node protection	MPLS FRR, SDN, Hybrid SDN MRT
[105]	A fast failure recovery scheme in SDN under multi-controller concept is proposed, where the main controller is responsible for controlling the network in the normal state, while the other controllers are standby controllers for the network control in a failure state. For calculating the control paths and disjoint path planning, the use of the K-best path algorithm is proposed. Type of solution: heuristic. Advantages: recovery time is less than 50 ms, the mechanisms can be used for recovery after failures of both control and data paths.	Controller protection, link protection, node protection	SDN, Multi-controller, In-band controlled OpenFlow Networks
[106]	Proactive recovery schemes in SDN are proposed for local failures based on the aggregation of traffic flows, with a decrease in the involvement of controllers in this process, in order to reduce the requirements for the controller`s computing power and the amount of control traffic generated during the recovery process. Type of solution: heuristic. Advantages: reduced recovery time and recovery specific control traffic, low memory requirement in switching components.	Link protection, node protection	SDN, Fast-Failover (FF)

Continuation of Table 1.3

[107]	The algorithm of Local Fast ReRoute (LFR) in SDN is proposed, where according to the flow aggregation strategy, LFR provides fast recovery by reducing the number of flow operations between the SDN controller and the switches. Type of solution: heuristic. Advantages: reduced the failure recovery time, minimized the total number of flow entries in the network.	Link protection	SDN, Local Fast ReRoute
[108]	The mechanism for updating routing and rerouting tables in case of the communication links failures in SDN with the support of acceptable QoS is proposed. Type of solution: graph model. Advantages: improving QoS by reducing packet routing delays and the data loss rate in case of a persistent link failure.	Link protection	SDN, IPFRR, QoS
[109]	The paper proposes a Hybrid-Hie solution for fast rerouting, which allows determining the ratio of the distribution of transmitted flows in the backup paths in accordance with their predicted utilization. Type of solution: flow-based model, optimization problem statement. Advantages: effective recovery in case of failure of interdomain communication links, load balancing, and recovery path stretch.	Link protection, multi-link protection	Hybrid SDN, SD-WAN, Traffic Engineering, Inter-domain routing, Intra-domain routing

Continuation of Table 1.3

[110]	The effective solution of optimizing restoration with segment routing in SDN is developed. Type of solution: flow-based model, optimization problem statement. Advantages: significant capacity benefits achievable from this optimized restoration with segment routing.	Link protection, node protection, Shared Local Restoration	SDN, Segment Routing
[111]	The bicriteria multiobjective algorithm with a maximum flow under minimum cost model to provide a balanced and resilient approach in an MPLS/SDN topology is proposed. Type of solution: optimization problem statement. Advantages: reduced routing complexity and path computation time, balanced network utilization, decreasing recovery time.	Link protection, node protection	MPLS/SDN, Traffic Engineering, QoS

To achieve the set aim, the following research problems have to be solved:

– using the mathematical model under the strategy of multipath routing;
– analytical formulation of path and bandwidth protection (reservation) schemes;
– stating the optimization problem of performance-based FRR and selection of optimality criterion;
– numerical research of the performance-based FRR model and obtaining results that prove its adequacy.

1.4. Formulation of the Scientific and Practical Task and Individual Research Objectives

The analysis of the current state and future solutions for implementing QoS, fault-tolerant, and secure routing carried out in the previous subsections allowed us to state that the direction associated with further improvement of routing tools is quite relevant. Introducing new technologies (e.g., SDN) requires the latest theoretical solutions to form the basis of mathematical and algorithmic software of routers and SDN controllers.

Found that it is the routing along disjoint paths that can provide the:

- efficient load balancing in the network to improve QoS level;
- implementation of basic global protection schemes to increase the level of TCN fault tolerance;
- increased network security;
- simplified calculation and computation of basic QoS, QoR, and network security metrics.

These advantages can only be realized in practice by developing new or improving existing mathematical models and routing methods over disjoint paths. Thus, the current **scientific and practical task** is to optimize the processes of fault-tolerant and secure routing over disjoint paths in telecommunication networks by developing, improving, and researching appropriate mathematical models.

To solve the set scientific and applied problem, the following research tasks were **solved in the work**:

- analysis of theoretical and applied solutions for fault-tolerant and secure routing in telecommunication networks;
- development and research of routing models with quality-of-service assurance in telecommunication networks using disjoint paths;
- improvement and research of secure routing models with quality of service assurance in telecommunication networks using disjoint paths;

– development and research of optimization model of fast rerouting in telecommunication networks with implementation of path and bandwidth protection schemes in TCN;

– development of recommendations on practical implementation of the proposed routing models in software-configured telecommunication networks.

1.5. Conclusions to the First Chapter

1. At the present time, the effectiveness of the telecommunication network is largely determined by the level of routing tasks being solved. It should be noted that multipath strategy support is an important feature of most current routing protocols used in IP and MPLS networks. This class of solutions ensures a balanced use of network (information, link, and buffer) resources. For that reason, multipath routing has been and continues to be an effective means of ensuring end-to-end Quality of Service, network security, and resilience of TCN.

2. As shown by the analysis, routing protocols are one of the effective means for ensuring the Quality of Service and network security. In addition, implementation of the multipath packet routing strategy maximizes QoS, and the use of a set of disjoint paths, in turn, ensures the highest level of network security when transmitting confidential data. The effectiveness of network protocols depends directly on the adequacy of the underlying mathematical models, methods, and computational algorithms.

3. The disjoint paths routing is a special case of multipath routing. The more disjoint paths are used, the better TCN indicators on the QoS, security, or resilience will be achieved, depending on the path selection criterion. However, it is known that the effectiveness of network protocols depends directly on the adequacy of the underlying mathematical models, methods, and calculation algorithms. Experts in this field have accumulated much experience. The analysis showed that existing QoS routing solutions do not always consider network security parameters. Conversely, secure routing does not generally help provide the required Quality of Service.

4. Integrating hard QoS and network security over disjoint paths without common links or nodes can enhance the performance and reliability of data transmission in networks. This integration offers several advantages, such as fault tolerance, increased bandwidth, and improved security.

5. The combination of secure routing, QoS and Fault tolerance is a worthwhile topic that involves designing and implementing network protocols and systems that can provide high performance and robust protection for data flow due to shared goals, such as preventing unauthorized access, ensuring data integrity, and avoiding network congestion. However, they also have some trade-offs, such as the overhead of encryption and authentication, resource reservation, and signaling complexity. Therefore, researchers have proposed various models and methods to balance fault tolerance, security, and QoS in different network scenarios. Therefore, the current work aims to develop and investigate the QoS, fault tolerance and security-aware routing over disjoint paths.

6. The purpose of the dissertation is to improve the Quality of Service and network security indicators by providing TCN fault tolerance in implementing protection schemes (redundancy) of network elements in the case of probable single or multiple failures. This goal can be achieved by revising and improving mathematical models and routing methods over disjoint paths based on new fault tolerance, security, and QoS principles.

CHAPTER 2

QUALITY OF SERVICE ROUTING MODELS IN TELECOMMUNICATION NETWORKS

This chapter develops a system of mathematical routing models to calculate disjoint paths to improve Quality of Service level. Within the framework of the proposed mathematical models, the problems of calculating disjoint paths are presented in the optimization form. To solve the optimization problems formulated in this chapter, the methods of integer and mixed integer linear programming, embedded in the Optimization Toolbox of MATLAB environment, were used.

Depending on the form of the chosen optimality criterion and the introduced system of constraints, the calculation result may be a set of paths with a maximum or predetermined number, the use of which is oriented to improve the TCN performance indicators, primarily related to bandwidth. Routing solutions aim to increase the calculated disjoint routes' bandwidth or provide predetermined values of this important QoS indicator. Increasing the bandwidth of routes has a positive impact on improving other Quality of Service indicators – average delay, jitter, and packet loss probability.

The linear nature of expressions, which form the basis of the developed routing models, criteria and constraints of the formulated optimization problems for the calculation of disjoint paths, should contribute to the acceptable computational complexity of their technological implementation in SDN as the basis of algorithmic software support of promising routing protocols.

The main results of the chapter are published in [36, 38, 42, 43, 45, 50, 51].

2.1. Basic Mathematical Model for Calculating Disjoint Routes in Telecommunication Networks

The analysis of known solutions [16-18, 22, 25-35] for solving the problem of calculating routes in a disjoint network allowed us to choose as a basic mathematical model of path calculation the one proposed and preliminarily investigated in [25]. The following notation will be introduced in this section to describe the selected model:

$G=\left(R,E\right)$	graph describing the network structure;
$R=\left\{R_i;\, i=\overline{1,m}\right\}$	set of vertices that simulate routers;
$E=\left\{E_{i,j};\, i,j=\overline{1,m};\, i\neq j\right\}$	set of edges representing links;
s_k	source node of packets of the *k*th flow;
d_k	destination node of packets of the *k*th flow;
K	set of flows for transmitting in the network, $k\in K$;
$a_{i,j}^{k}$	control variables, each of which determines whether the $E_{i,j}\in E$ link belongs to the set of calculated disjoint paths for transmission of the *k*th flow;
$\varphi_{i,j}$	capacity of $E_{i,j}\in E$ link, measured in packets per second, pps;
M^k	integer parameter characterizing the number of disjoint paths used by the *k*th flow;

$w_{i,j}$ weighting coefficients related to the capacity of link $E_{i,j} \in E$.

Fig. 2.1 shows the graph model of TCN in the accepted labels.

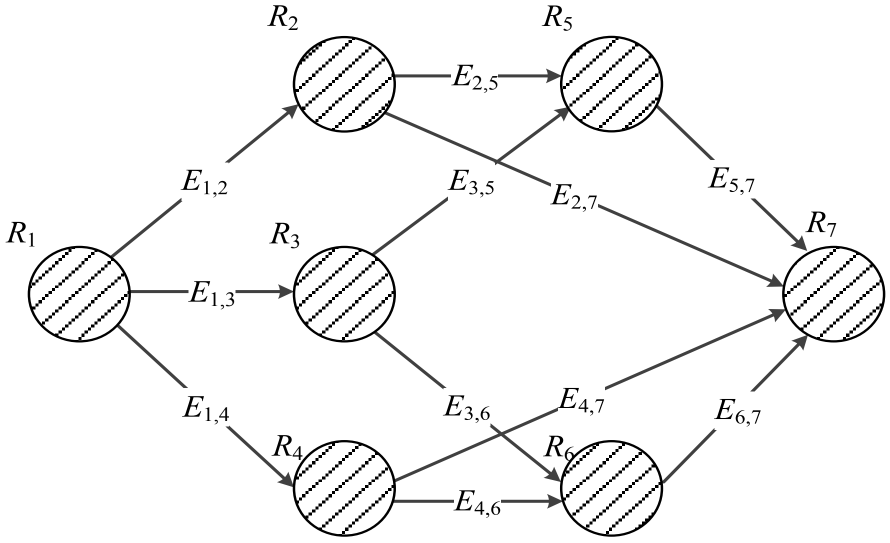


Fig. 2.1. Graph model of telecommunication network

As a result of solving the problem of calculating disjoint paths, it is necessary to define a set of variables $a_{i,j}^{k}$, the number of which corresponds to the product $|K| \cdot |E|$. Several constraints are imposed on the $a_{i,j}^{k}$ routing variables. Thus, according to their physical meaning, the following conditions take place:

$$a_{i,j}^{k} = \begin{cases} 1, & \text{if link } E_{i,j} \text{ is using under the } k\text{th flow transmission;} \\ 0, & \text{otherwise.} \end{cases} \qquad (2.1)$$

Also, the following conditions for a pair of source and destination of the *k*th flow packets nodes must be satisfied [25, 36]:

$$\sum_{j:E_{i,j}\in E} a_{i,j}^{k} = \mathrm{M}^{k},\ k\in K,\ R_i = s_k; \tag{2.2}$$

$$\sum_{j:E_{j,i}\in E} a_{j,i}^{k} = \mathrm{M}^{k},\ k\in K,\ R_i = d_k. \tag{2.3}$$

The fulfillment of conditions (2.2) and (2.3) guarantees that the number of links (paths) leaving the source node is the same as the number of links (paths) entering the destination node of the *k*th packet flow.

At the same time, for the transit nodes TCN $\left(R_i \neq s_k, d_k\right)$ within the basic model, the following additional system of constraints is imposed on the routing variables [25, 36]:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} a_{i,j}^{k} \le 1, \quad k\in K; \\ \sum\limits_{j:E_{j,i}\in E} a_{j,i}^{k} \le 1, \quad k\in K; \\ \sum\limits_{j:E_{i,j}\in E} a_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} a_{j,i}^{k} = 0, \quad k\in K. \end{cases} \tag{2.4}$$

The physical meaning of the first condition in the system (2.4) is that from a transit node R_i, packets of the *k*th flow can be transmitted using at most one link (path). Fulfillment of the second condition in system (2.4) must ensure that in the transit node R_i, packets of the *k*th flow can arrive using no more than one link (path). The implementation of the third condition from system (2.4) is responsible for the fact that from a transit router R_i, packets of the *k*th flow can be transmitted only if they have previously arrived at this node. For a telecommunication network in general, the fulfillment of the constraint system (2.4) must guarantee the following conditions:

first, involved communication links ensure the connectivity of each specific calculated path*;*

second , calculated paths will not intersect, i.e., they can share only source (s_k) and destination (d_k) nodes.

Depending on the formulation of the problem of calculating disjoint paths in TCN, the value of the positive integer parameter M^k can either be preset, that is, be a known value, or maximized, for example, when it is necessary to determine the maximum number of paths of a similar class. In this case, the optimality criterion of routing decisions can be the condition of maximization of such an object function:

$$J = \mathrm{M}^k. \tag{2.5}$$

However, in any case, the following condition takes place:

$$\mathrm{M}^k \geq 1. \tag{2.6}$$

In the general case, the range of available values M^k directly depends on the network topology, the network nodes' connectivity level, and the degree of the graph *G* vertices, which simulate the source and destination routers.

Consequently, the problem of calculating disjoint paths that do not intersect within the basic model (2.1)-(2.6) is formulated in an optimization form [36]. The optimality criterion is the maximum of the object function (2.5), focusing on maximizing the number of calculated paths that do not intersect. On the control variables $a_{i,j}^k$ and M^k the constraints (2.1)-(2.4), (2.6) are imposed. The formulated optimization problem belongs to the class of Integer Linear Programming (ILP) since linear forms represent the optimality criterion and constraints, and the control variables are either Boolean (2.1) or integer (2.6).

2.2. Mathematical Model of QoS Routing in TCN Using Disjoint Paths that Provide Maximum Bandwidth

In the first section, it was noted that the main Quality of Service indicator is the bandwidth provided (allocated) to this or that flow of packets. The quantitative values of other QoS indicators, both time and reliability indicators, largely depend on the amount of allocated bandwidth of links and routes. First, these are the average delay, jitter and packet loss probability. Therefore, in this work, the study of QoS routing problems focuses on ensuring the Quality of Service in terms of bandwidth by modifying the basic model of packet routing over disjoint paths given in subsection 2.1.

The basic mathematical model (2.1)-(2.6) can also be modified in QoS routing to provide maximum or specified bandwidth using the calculated set of disjoint paths. For this purpose, it is necessary to introduce additional conditions into the structure of the basic model to ensure high Quality of Service in terms of bandwidth. Therefore, we denote by the β_{path}^{k} minimum threshold value for the bandwidth of any set of disjoint paths used to transmit packets of the *k*th flow. Since the calculated paths do not overlap, it determines the minimum threshold value β_{path}^{k} for the bandwidth of any TCN communication links involved in transmitting packets of the *k*th flow. Then, the following condition for balancing the bandwidth of routes can be introduced into the structure of the routing model (by analogy with [27]):

$$a_{i,j}^{k}\varphi_{i,j} + W\left(1 - a_{i,j}^{k}\right) \geq \beta_{path}^{k}, \tag{2.7}$$

where the weighting coefficient W takes the values higher than the maximum bandwidth of $E_{i,j} \in E$ network links.

The fulfillment of condition (2.7) guarantees that each route belonging to the set of paths computed for the *k*th packet flow has a bandwidth of at least β_{path}^{k}.

Then the maximization of the object function J_1 should be chosen as the optimality criterion of solutions to the QoS routing problem by disjoint paths:

$$J_1 = c_{\mathrm{M}}\mathrm{M}^k + c_{\beta}\beta_{path}^{k} - c_v \sum_{E_{i,j}\in E} v_{i,j}a_{i,j}^{k}, \tag{2.8}$$

where the weighting coefficients c_{M}, c_{β}, and c_v determine the importance of each of the components in the expression (2.8).

Introducing the first term in the object function (2.8) is related to maximizing the number of used disjoint paths. The second term is responsible for maximizing the lower boundary value of the bandwidth of the calculated paths. If we restrict ourselves to using only these two terms, then, on the one hand, the lowest-performing path will have a bandwidth equal to the β_{path}^{k}. However, such a solution may not always contribute to the inclusion in the calculated set of the highest bandwidth routes. Therefore, the novelty of the proposed model is the use of the third term in the criterion (2.8), which is introduced by analogy with the metrics of the OSPF and EIGRP [7, 8] protocols to include in the calculated disjoint paths the links with high bandwidth. Thus, it is proposed that in the objective function (2.8), the weighting coefficients (metrics) $v_{i,j}$ taking into account the bandwidth $\varphi_{i,j}$ of the corresponding link $E_{i,j} \in E$ are determined in the following way:

$$v_{i,j} = 10/\varphi_{i,j}. \tag{2.9}$$

It is experimentally established that to implement QoS routing with the calculation of the maximum number of disjoint paths with maximum bandwidth, the weighting coefficients in expression (2.8) must meet the following condition:

$$c_{\mathrm{M}} >> c_{\beta} >> c_{\nu}. \tag{2.10}$$

Thus, the introduction of conditions (2.10) into the model (2.1)-(2.4), (2.6) with the replacement of the optimality criterion (2.5) by (2.8) modified the type of the formulated optimization problem. The solution to the problem of computing the set of disjoint paths with maximum bandwidth was reduced to solving the optimization problem of mixed integer linear programming (MILP) with criterion (2.8) in the presence of linear constraints and conditions (2.1)-(2.4), (2.6)), (2.7), since route variables $a_{i,j}^{k}$ are Boolean, the variable M^{k}, which determines the number of used disjoint paths, takes only integer values. In general, β_{path}^{k} is a real variable because the value of the bandwidth $\varphi_{i,j}$ is not always an integer.

The features of the proposed model will be demonstrated by the following example. The structure of the analyzed network shown in Fig. 2.2 contains seven routers and eleven links. Specifically, its graph model is shown in Fig. 2.1.

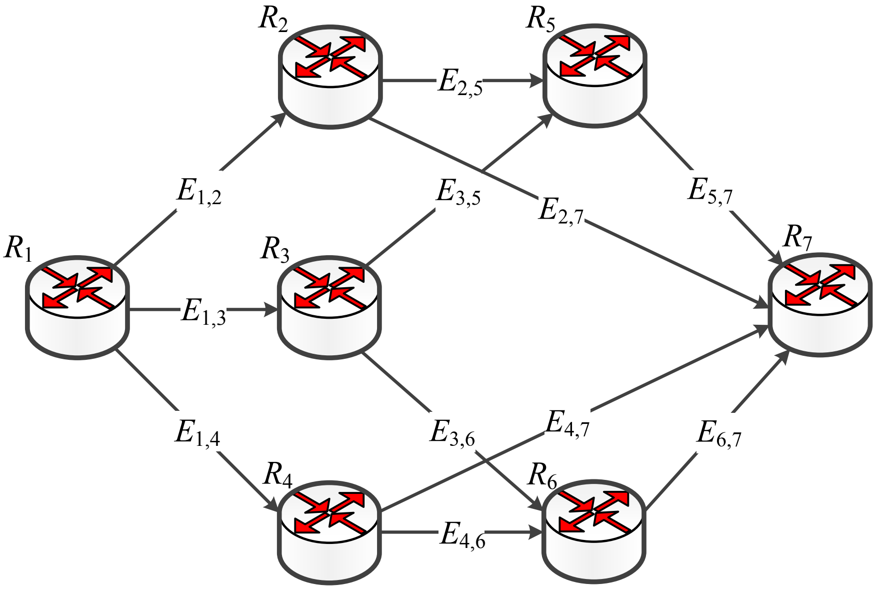


Fig. 2.2. Structure of the telecommunication network analyzed

Let us consider that the first and seventh routers will be the corresponding source and destination nodes of one packets flow. In this example, four cases of input data on link capacity values (Table 2.1) are provided to form a set of disjoint paths under the condition of the proposed model (2.1)-(2.4), (2.6)-(2.10) application.

Table 2.1

Initial Data for the Numerical Study of the Model for Calculating the Set of Disjoint Paths that Provide Maximum Bandwidth

Link	Bandwidth, pps			
	Case 1	Case 2	Case 3	Case 4
$E_{1,2}$	300	220	800	200
$E_{1,3}$	900	210	100	300
$E_{1,4}$	150	240	150	150
$E_{2,5}$	250	190	250	250
$E_{2,7}$	400	200	400	100
$E_{3,5}$	90	180	890	270
$E_{3,6}$	110	190	310	110
$E_{4,7}$	140	210	140	190
$E_{4,6}$	300	185	300	300
$E_{5,7}$	920	180	220	220
$E_{6,7}$	180	190	780	180

On the network structure, which is taken into account in the investigation (Fig. 2.2), the following set of possible paths between the first and seventh routers has been obtained:

$$\begin{cases} L_1 = \{E_{1,2}, E_{2,5}, E_{5,7}\}; \\ L_2 = \{E_{1,3}, E_{3,6}, E_{6,7}\}; \\ L_3 = \{E_{1,4}, E_{4,7}\}; \\ L_4 = \{E_{1,4}, E_{4,6}, E_{6,7}\}; \\ L_5 = \{E_{1,3}, E_{3,5}, E_{5,7}\}; \\ L_6 = \{E_{1,2}, E_{2,7}\}. \end{cases} \qquad (2.11)$$

The research of the proposed model (2.1)-(2.4), (2.6)–(2.10) was conducted, the results of which for the initial data from Table 2.1 are presented in Table 2.2. In addition, the calculation of sets of disjoint paths, was carried out under the condition of two options for using the optimality criterion (2.8): in the absence of the third term (Variant I) and taking into account all three components (Variant II).

The calculations demonstrated that in two cases (Case 2 and Case 4) the introduction of the third term in criterion (2.8) did not affect the nature of the resulting routing solutions. Whereas in Case 1 and Case 3 (Table 2.2), the set of paths calculated by the integral criterion (2.8) had a higher bandwidth (from 1.5% to 10%). For clarity, we will consider Case 3 in more detail (Fig. 2.3 and Fig. 2.4), for which we will show sets of disjoint paths for the corresponding initial (Table 2.1) and resulting data (Table 2.2). The marks in Fig. 2.3 and Fig. 2.4 are similar to the marks used in Fig. 2.1 and Fig. 2.2.

Table 2.2

Results of Calculating the set of Disjoint Paths between the First and Seventh Routers and the Multipath Bandwidth

Case#		Set of disjoint paths			Bandwidth, pps
		Path 1	Path 2	Path 3	
Case 1	I	$\{E_{1,2}, E_{2,5}, E_{5,7}\}$	$\{E_{1,3}, E_{3,6}, E_{6,7}\}$	$\{E_{1,4}, E_{4,7}\}$	500
	II	$\{E_{1,3}, E_{3,6}, E_{6,7}\}$	$\{E_{1,4}, E_{4,7}\}$	$\{E_{1,2}, E_{2,7}\}$	550
Case 2	I	$\{E_{1,3}, E_{3,6}, E_{6,7}\}$	$\{E_{1,4}, E_{4,7}\}$	$\{E_{1,2}, E_{2,7}\}$	600
	II	$\{E_{1,3}, E_{3,6}, E_{6,7}\}$	$\{E_{1,4}, E_{4,7}\}$	$\{E_{1,2}, E_{2,7}\}$	600
Case 3	I	$\{E_{1,4}, E_{4,7}\}$	$\{E_{1,3}, E_{3,5}, E_{5,7}\}$	$\{E_{1,2}, E_{2,7}\}$	640
	II	$\{E_{1,4}, E_{4,6}, E_{6,7}\}$	$\{E_{1,3}, E_{3,5}, E_{5,7}\}$	$\{E_{1,2}, E_{2,7}\}$	650
Case 4	I	$\{E_{1,2}, E_{2,5}, E_{5,7}\}$	$\{E_{1,3}, E_{3,6}, E_{6,7}\}$	$\{E_{1,4}, E_{4,7}\}$	460
	II	$\{E_{1,2}, E_{2,5}, E_{5,7}\}$	$\{E_{1,3}, E_{3,6}, E_{6,7}\}$	$\{E_{1,4}, E_{4,7}\}$	460

Fig. 2.3 shows the multipath calculated under the condition that the third term in the optimality criterion (2.13) is zero. In this case, the bandwidth of multipath is 640 pps (Fig. 2.3). While the use of criterion (2.8) in calculations, taking into account all the terms included in its composition, makes it possible to obtain a set of disjoint paths with the maximum possible bandwidth of 650 pps (Fig. 2.4).

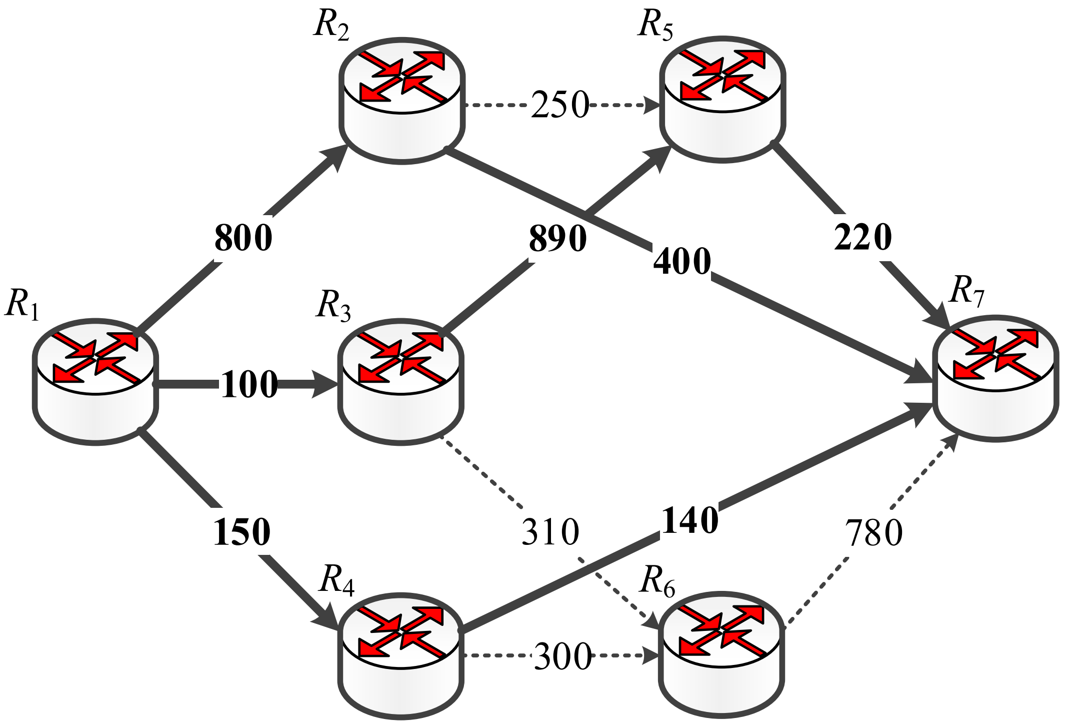


Fig. 2.3. Set of disjoint paths,

when using criterion (2.8) without the last term (Case 3)

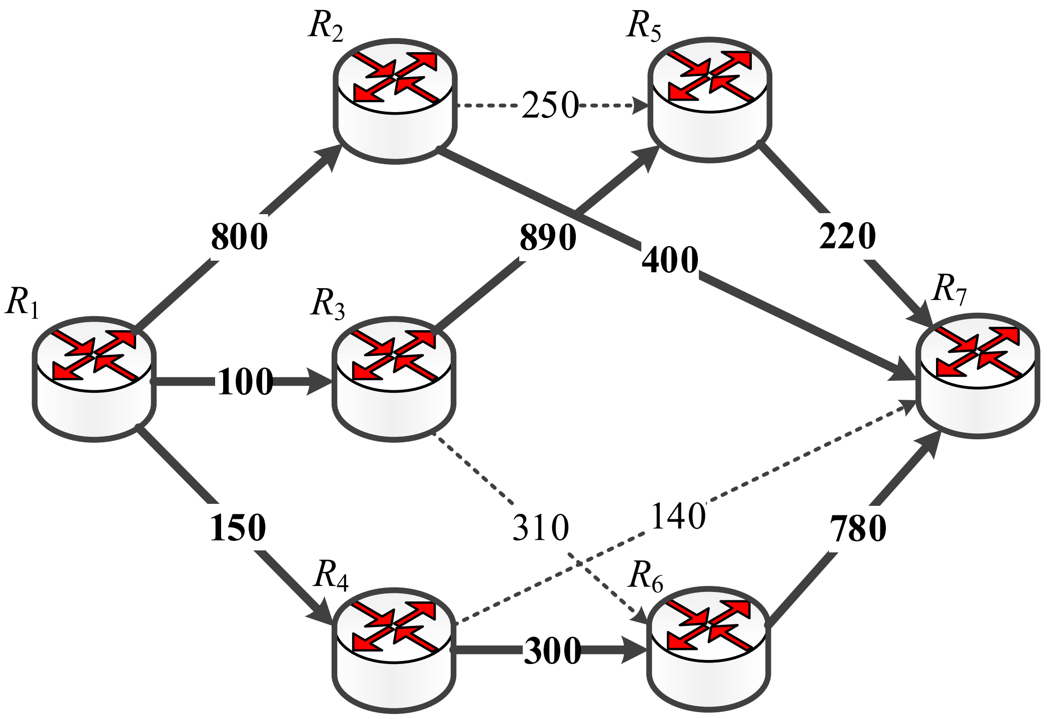


Fig. 2.4. Set of disjoint paths, when using criterion (2.8) (Case 3)

The analysis of calculation results given in Table 2.2 showed that the use of the integral criterion (2.8) allows providing higher bandwidth for the routing solution, represented by the set of disjoint paths, in cases of high heterogeneity of the network, i.e. when the bandwidths of the TCN communication links are quite different. This is typical for Case 1 and Case 3 (Table 2.2).

With research a TCN with homogeneous network architecture, when the bandwidth of its links did not differ so much (Case 2 and Case 4 in Table 2.1), introducing the third term in criteria (2.8) did not affect the total bandwidth of the calculated disjoint paths, which determines the preferred scope of the proposed routing solution.

2.3. Mathematical Model of QoS Routing in TCN Using Disjoint Paths Providing Guaranteed Bandwidth

The peculiarity of using the mathematical model (2.1)-(2.4), (2.6)-(2.10), proposed and investigated in subsection 2.2, is that it focuses on the selection of paths in the TCN that do not intersect and provide the maximum allowable multipath capacity. This is due to applying the appropriate coefficients (2.9), which are analogs of the routing metrics in the optimality criterion (2.8). Increasing the bandwidth allocated to a particular flow allows for improving average delay and packet loss [36].

However, in practice, for certain flows, it is necessary to provide not maximum, but normalized or guaranteed bandwidth. That is, to save network resources to serve the traffic of TCN users, as a rule, requirements are set for the threshold (guaranteed, normalized) value of the network bandwidth (path or multipath) available for use by a particular flow.

For this purpose, let us denote, for example, the threshold value of the bandwidth allocated by the network for the *k* th packet stream by β^k. Therefore, in the model (2.1)-(2.4), (2.6)-(2.10) it is proposed to introduce the following condition:

$$\mathrm{M}^k \beta_{path}^k \geq \beta^k . \qquad (2.12)$$

Therefore, in the general case, the left part of inequality (2.12) is a bilinear form of two types of control variables M^k та β_{path}^k, that characterize the lower bound of bandwidth, which in total provides the use of the calculated paths (multipath). The bound is lowest, as each of these disjoint paths and creates multipath, according to conditions (2.7), has a capacity not lower but may be higher by β_{path}^k. Fulfillment of condition (2.12), depending on the form of the selected optimality criterion, can be achieved either by increasing the number of involved disjoint routes M^k or by raising the boundary value relative to their minimum bandwidth β_{path}^k.

Given the use of the optimality criterion of routing solutions (2.8), the priority of increasing the control variables that are included in the bilinear form in (2.12) will be determined by the hierarchy of values of weighting coefficients.

In the case of introducing conditions (2.12), the optimization problem with criterion (2.8) and the supplemented set of constraints (2.1)-(2.4), (2.6), (2.7), (2.12) will belong to the class of problems of Mixed-integer nonlinear programming (MINLP). However, for example, if the number of paths to be calculated is known in advance $\mathrm{M}^k = \mathrm{const}$, i.e., in criterion (2.8), the first term also becomes a constant, condition (2.12) becomes linear, and the optimization problem remains of the MILP class.

Consider several numerical examples for calculating disjoint paths and providing a given bandwidth on the network structure presented in Fig 2.5.

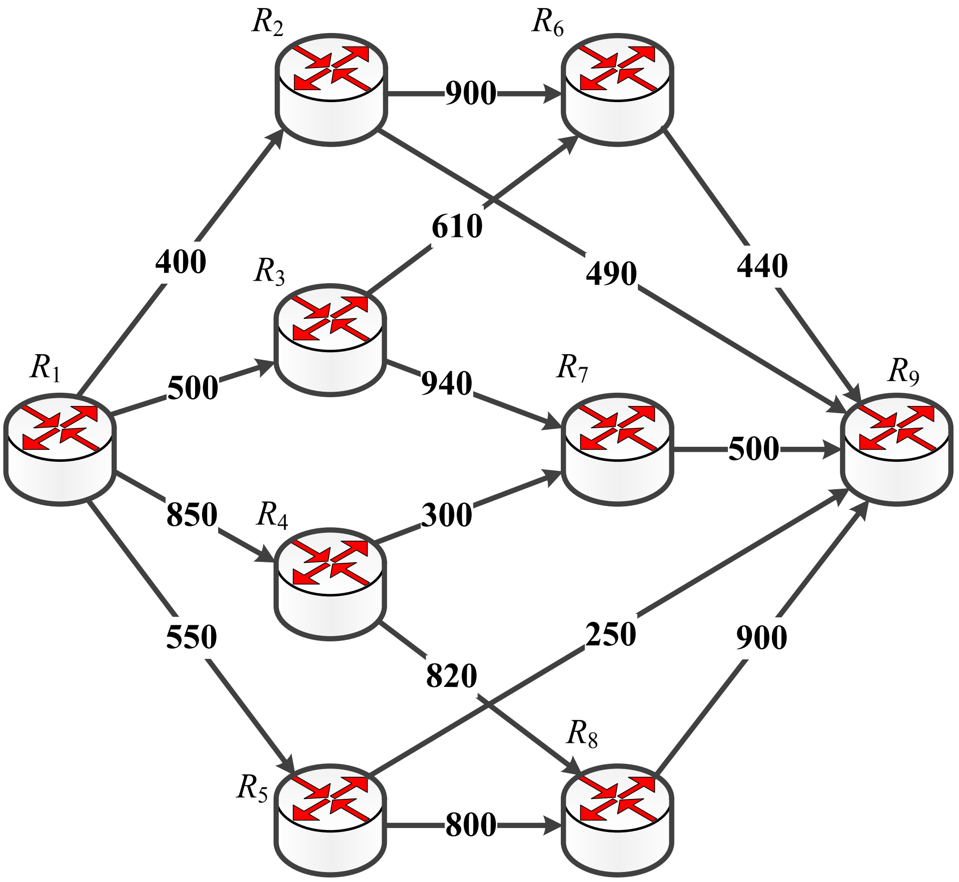


Fig. 2.5. Initial structure of the telecommunication network

For this network structure (Fig. 2.5) in communication link gaps indicate their bandwidth, and the set of available paths and their bandwidth shown in Table 2.3. Then Table 2.4 shows the calculations to determine for one flow transmitted in the network from the first to the ninth router (Fig. 2.6) a set of disjoint paths and guarantees the lower bound of total bandwidth.

Table 2.4 demonstrates possible solutions to the QoS-routing problem using disjoint paths that provide a given bandwidth. Depending on the ratio of weighting coefficients c_{M}, c_{β}, and c_{ν} in (2.8), the use of the model (2.1)-(2.4), (2.6), (2.7), (2.12) allows for obtaining a different set of paths. If condition (2.10) was satisfied, then the fulfillment of condition (2.12) was achieved, as a rule, based on increasing the number of involved disjoint routes M^{k}.

Table 2.3

Characteristics of the Available Paths Between the First and Ninth Routers for the Network Structure Shown in Fig. 2.5

Path#	Path Designation	The set of links that form a path	Path Bandwidth, pps
1	L_1	$\{E_{1,2}, E_{2,6}, E_{6,9}\}$	400
2	L_2	$\{E_{1,2}, E_{2,9}\}$	400
3	L_3	$\{E_{1,3}, E_{3,6}, E_{6,9}\}$	440
4	L_4	$\{E_{1,3}, E_{3,7}, E_{7,9}\}$	500
5	L_5	$\{E_{1,4}, E_{4,7}, E_{7,9}\}$	300
6	L_6	$\{E_{1,4}, E_{4,8}, E_{8,9}\}$	820
7	L_7	$\{E_{1,5}, E_{5,9}\}$	250
8	L_8	$\{E_{1,5}, E_{5,8}, E_{8,9}\}$	550

Table 2.4

Results of Determining the Set of Disjoint Paths that Provide Guarantees Regarding their Lower Bound of Total Bandwidth (*k* = 1)

<table>
<tr><th rowspan="2">β^k</th><th rowspan="2">M^k</th><th rowspan="2">β^k_{path}</th><th colspan="2">The set of paths that are calculated using (2.13), and their total bandwidth</th></tr>
<tr><th>$c_v = 0$</th><th>$c_v \neq 0$</th></tr>
<tr><td rowspan="3">1000 pps</td><td>4</td><td>250 pps</td><td>$\{L_2, L_3, L_5, L_7\}$
1390 pps</td><td>$\{L_2, L_4, L_6, L_7\}$
1970 pps</td></tr>
<tr><td>2</td><td>500 pps</td><td>$\{L_4, L_8\}$
1000 pps</td><td>$\{L_4, L_6\}$
1220 pps</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">400 pps</td><td rowspan="2">$\{L_2, L_4, L_8\}$
1450 pps</td><td rowspan="2">$\{L_2, L_4, L_6\}$
1720 pps</td></tr>
<tr><td>1200 pps</td></tr>
</table>

However, as shown in Table 2.4, it is better to use the network resource economically to satisfy the constraint $c_{\beta} >> c_{\mathrm{M}} >> c_{v}$. Then condition (2.12) was fulfilled based on raising the boundary value relative to the minimum bandwidth $\left(\beta^{k}_{path}\right)$ of the calculated paths. If β^{k} is equal to 1200 pps, then in Table 2.4, only the solutions at M^{k}=3 (Table 2.4, third row) satisfy (Fig. 2.6).

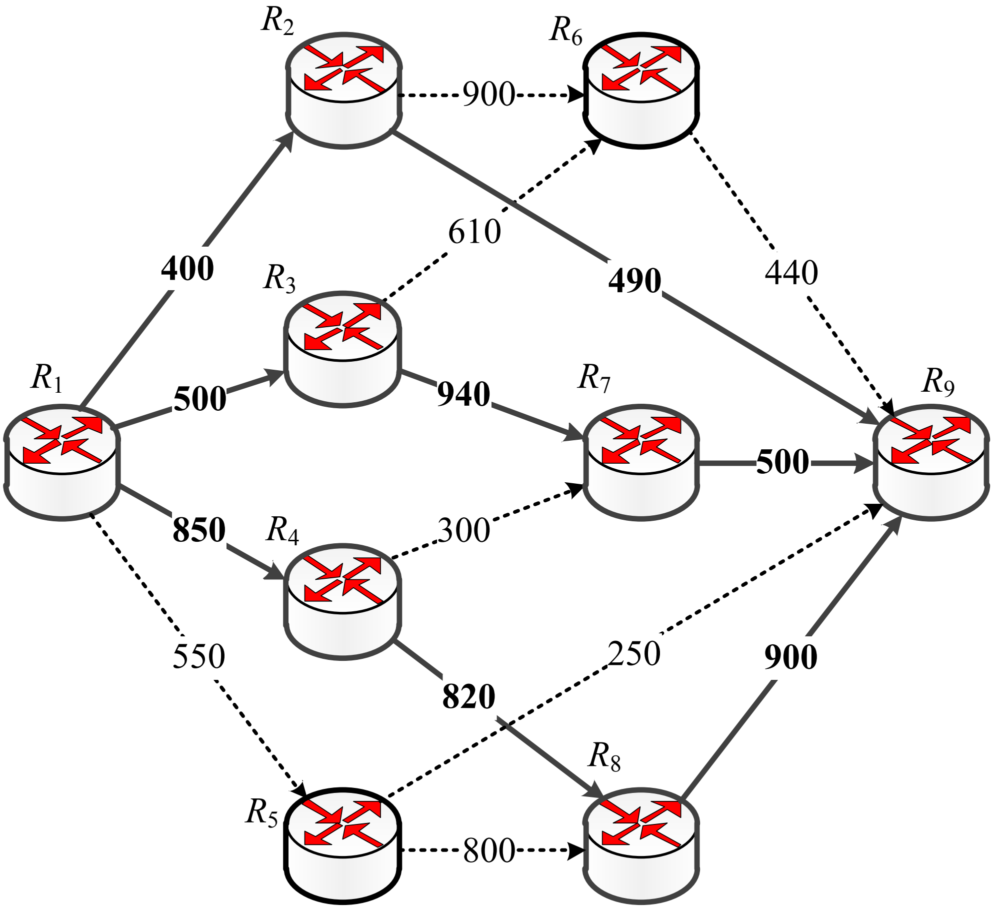


Fig. 2.6. The set of paths $\{L_2, L_4, L_6\}$, calculated using (2.8), under $c_v \neq 0$, and provide total bandwidth 1720 1/pps $\left(\mathrm{M}^{k} = 3\right)$

The introduction of the third term in the objective function (2.8) under $c_v \neq 0$ allowed for including more productive communication links in the set of calculated paths. It was accompanied, as a rule, such a result was accompanied by an increase in the total bandwidth of disjoint paths used in QoS routing (Table 2.4).

The solid line in Fig. 2.6 shows the links involved in the calculated disjoint paths. The dotted line in Fig. 2.6 shows the links not included in the calculated paths. In the gaps of communication links, their bandwidths are indicated.

Fig. 2.7 presents the result of solving the QoS routing problem with the use of two paths $\{L_4, L_6\}$ which disjoint paths and provide bandwidth guarantees in the network (β^k is equal to 1000 pps). Their actual bandwidth (Table 2.4, second row) was 1220 pps.

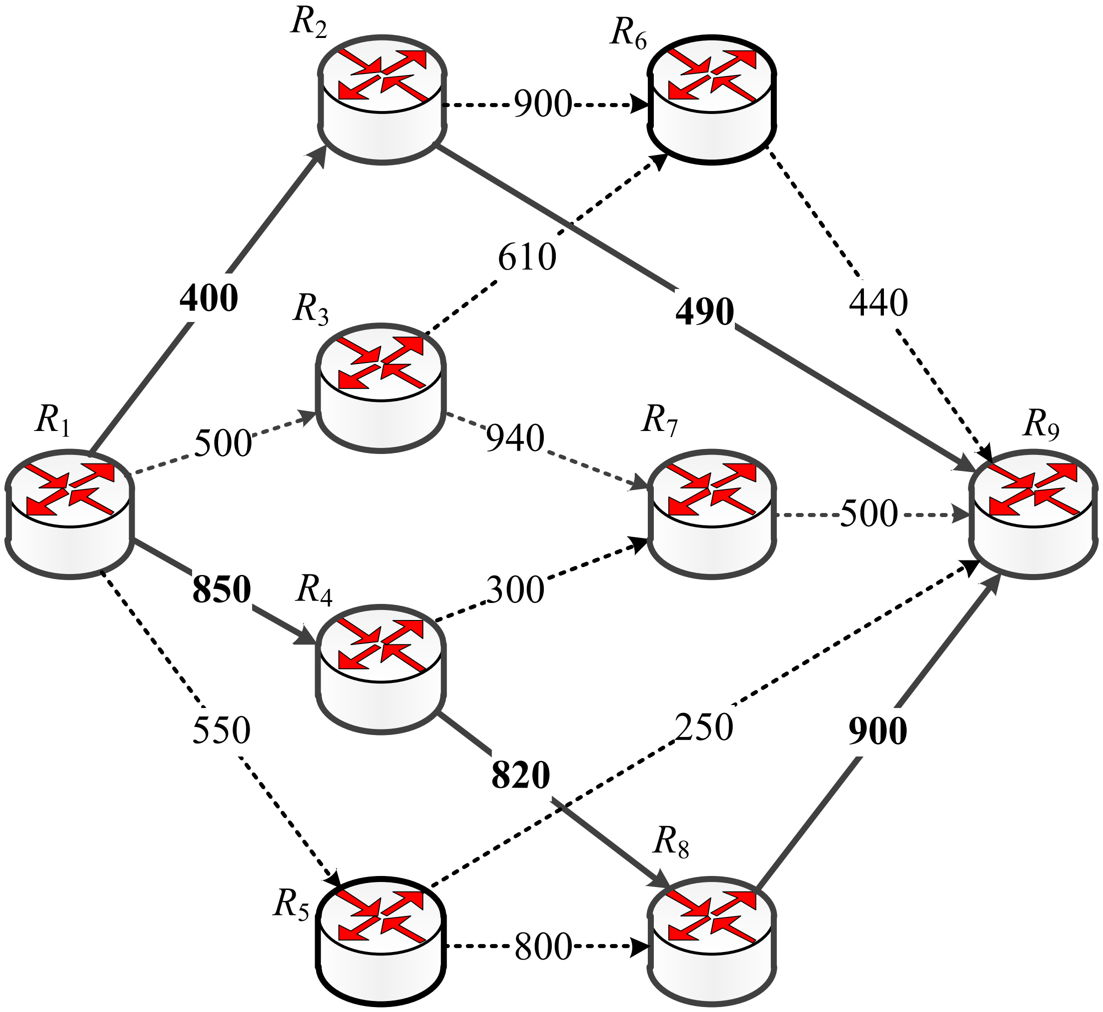


Fig. 2.7. The set of paths $\{L_4, L_6\}$, calculated using (2.8), under $c_v \neq 0$, and provide total bandwidth 1220 pps $\left(\mathrm{M}^k = 2\right)$

Fig. 2.8 shows the case where the QoS guarantee requirements in terms of network bandwidth (β^k = 1000 pps) were met using four disjoint paths $\{L_2, L_3, L_5, L_7\}$ (Table 2.4, first row). This routing solution (Fig. 2.8) is obtained using (2.8) when $c_v = 0$. Then the total bandwidth of the calculated paths was 1390 pps. Increasing the number of used paths in non-intersecting TCNs can also be due to the need to fulfill the requirements of policies regarding the network security level [36].

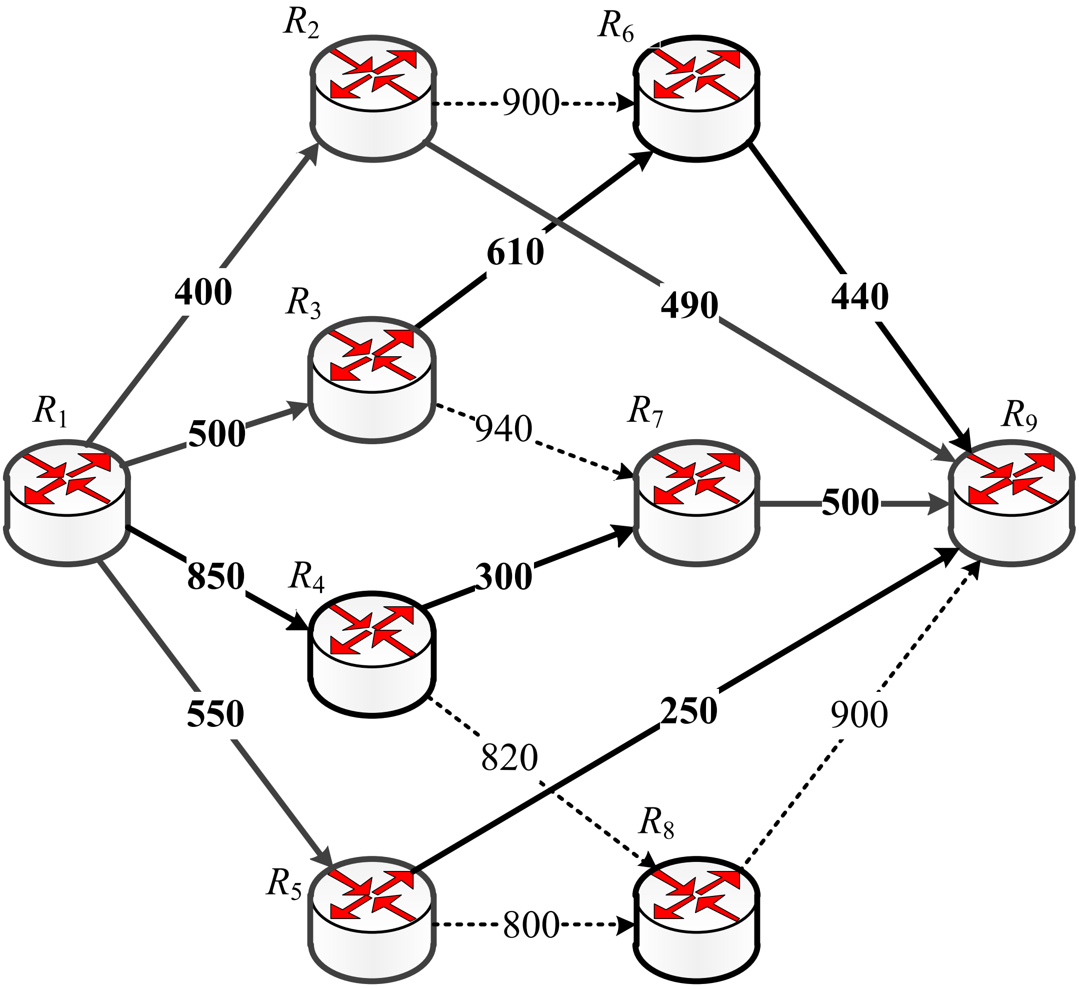


Fig. 2.8. The set of paths $\{L_2, L_3, L_5, L_7\}$, calculated using (2.8), under $c_v = 0$, and provide total bandwidth of 1390 pps $\left(\mathrm{M}^k = 4\right)$

Thus, the use of the modified optimality criterion (2.8) and conditions (2.7), (2.12) increased the total capacity of the calculated paths that did not intersect from 1.5-10% (Table 2.2) to 18.6-42% (Table 2.4).

2.4. Conclusion to the Second Chapter

1. In this chapter, the basic mathematical model (2.1)-(2.4), (2.6) for the calculation of disjoint routes in TCN is justified for use and further improvement. The advantage of the chosen model is that the problem of calculating disjoint paths is presented in an optimization form. The control (routing) variables are Boolean (2.1), and the constraints imposed on them (2.2)-(2.4) are linear. Depending on the specifics of the routing problem formulation, the number of disjoint paths can be predefined (2.6) or maximized (2.5). The formulated optimization problem (2.1)-(2.6) belongs to the class of Mixed Integer Linear Programming problems, since the variables determining the number of used routes (2.6) takes only integer values. The main computational advantage of the basic model is the linearity of conditions (2.2)-(2.6), which greatly simplifies its further protocol realization in practice.

2. The mathematical model of QoS routing in a telecommunication network over disjoint paths is improved. The scientific novelty of the model consists, firstly, in the introduction of conditions for balancing the capacity of routes (2.7) and the use of the optimality criterion of routing solutions (2.8)-(2.10), which allowed to ensure the process of routing maximization of both the number and total capacity of the calculated paths. This was achieved by introducing additional components to the optimality criterion (2.8), selecting routing metrics (2.9), and establishing a hierarchy of weighting coefficients (2.10). Accordingly, the QoS routing problem with disjoint paths remained of the MILP class.

3. The analysis of calculation results has shown that the use of integral criterion (2.8) allows to provide the maximum possible bandwidth of the routing solution (Table 2.2) represented by a set of disjoint paths in cases of high network heterogeneity, i.e., when bandwidths of TCN links differ significantly.

4. The mathematical model of QoS routing in TCN using disjoint paths (2.1)-(2.4), (2.6)-(2.10) has been further developed. The scientific novelty of the model consists of introducing bilinear conditions for ensuring the guaranteed total bandwidth of the paths (2.12). Their fulfillment allows us to calculate the paths having a bandwidth not lower than the set threshold (requirement). Fulfillment of condition (2.12) depending on the form of the chosen optimality criterion can be achieved either on the basis of increasing the number of involved disjoint routes, or by increasing the threshold value relative to their minimum bandwidth.

5. When the optimality criterion for routing solutions (2.8) is used, the priority of increasing the values of the control variables containing the bilinear form in (2.12) will be determined by the hierarchy of the weighting coefficients (2.10) values in (2.8). In this case, the optimization problem with criterion (2.8) and constraint set (2.1)-(2.4), (2.6), (2.7), (2.12) belongs to the class of MINLP problems. However, for example, if the number of paths to be computed is known in advance, then condition (2.12) will become linear and the optimization problem itself will remain in the MILP class. The results of this study (Table 2.4) confirmed the effectiveness of the proposed QoS routing model in TCN (2.1)-(2.4), (2.6)-(2.10), (2.12) in terms of providing guaranteed bandwidth for different variants of the input data, which concerned the number of disjoint routes used.

6. As mentioned in Chapter 1, three main approaches are used to ensure QoS in practice, for example, in IP networks: "best effort service" – service to the best of its ability, i.e., without guarantees and privileges; DiffServ – differentiated service based on priorities; IntServ – integral service, when the network provides guarantees on selected QoS indicators, e.g., bandwidth. Within the proposed solutions, the use of optimality criterion (2.5) is more in line with the features of best effort service. The application of criteria (2.8) is oriented to support the DiffServ approach. Introducing and ensuring the fulfillment of conditions (2.12) allows guaranteeing a packet flow a given level of QoS (IntServ) in terms of the multipath bandwidth, i.e., the set of calculated disjoint paths.

CHAPTER 3

MODELS OF SECURE ROUTING WITH QUALITY OF SERVICE IN TELECOMMUNICATION NETWORKS

In practice, when transmitting packets of specific service flows, one should pay attention to the Quality of Service indicators (bandwidth, average delay, and loss probability) and the network security indicators. This is especially true when transmitting confidential messages and flows to which access should be restricted. Therefore, as mentioned in the first chapter, mathematical models and routing methods are being developed intensively to provide a compromise between the values of QoS indicators and network security indicators [1, 15, 16, 22, 36]. Indeed, it is not uncommon for paths with high bandwidth to be less secure than paths with slightly lower QoS metrics. This aspect should be taken into consideration.

Therefore, the solutions proposed in Chapter 2 are further developed in this section to provide secure QoS routing over disjoint paths. Their development is carried out to improve both QoS and network security. Traditionally, within the framework of the proposed mathematical models, the problems of calculating disjoint paths are presented in an optimization form. Depending on the form of the chosen optimality criterion and the introduced system of restrictions on the routing variables, as a result of calculations, a set of paths with the maximum or predetermined number of paths was determined, the use of which is oriented to improve the TCN efficiency indicators: bandwidth and the probability of packet (message) compromise.

Decisions on the organization of secure routing of confidential data in TCN are based on considering such important indicators of network security as the compromise probability of a link, a route, and disjoint paths. The complexity of mathematical models of secure routing, associated with the joint description of the processes of ensuring the Quality of Service and network security, has not led to the loss of the linear nature of the expressions included in them. In the end, this has traditionally positively affected the computational complexity of the final algorithmic software and protocol solutions.

The main results of the chapter are published in [36, 37, 40, 42, 46, 48].

3.1. Mathematical Model of Secure Routing over Disjoint Paths

In the process of organizing secure QoS routing, the structure of optimization model (2.1)-(2.6) should be modified at the level of optimality criterion or constraints imposed on control variables, taking into account both network security parameters and Quality of Service. Thus, in [25, 37], it is proposed to revise the model (2.1)-(2.6) in the direction of complementation, changing the type of optimality criterion, which will be based on the maximum of such an objective function:

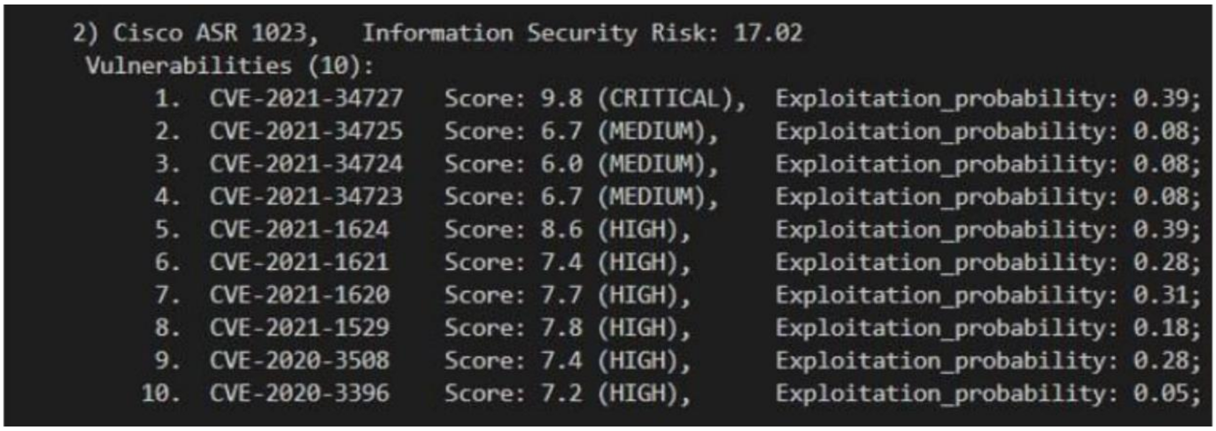
$$J_2 = w_k \mathrm{M}^k - \sum_{E_{i,j} \in E} w_{i,j} a_{i,j}^k . \tag{3.1}$$

In the objective function (3.1), positive weighting coefficients w_k and $w_{i,j}$ determine the respective terms importance. The weighting coefficients $w_{i,j}$ should be selected so that choosing the disjoint paths set is also focused on minimizing their compromise probability [36, 40]

$$w_{i,j} = -\lg\left(1 - p_{i,j}\right), \tag{3.2}$$

where $p_{i,j}$ – is the probability of compromising the $E_{i,j} \in E$ link.

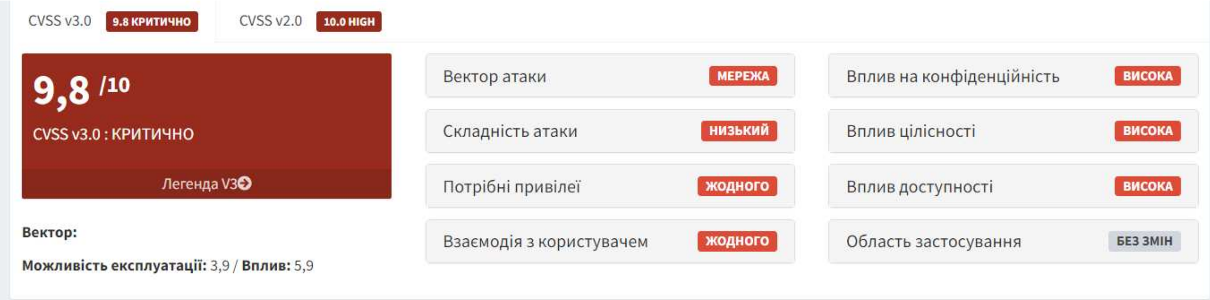
As shown in [36], the probability of compromising a communication link, for example, can be defined as some function of the values of the probabilities of an attacker exploiting vulnerabilities of routers (its hardware and software) of the network connecting this link (Fig. 3.1).



```
  2) Cisco ASR 1023,    Information Security Risk: 17.02
   Vulnerabilities (10):
        1.  CVE-2021-34727   Score: 9.8 (CRITICAL),  Exploitation_probability: 0.39;
        2.  CVE-2021-34725   Score: 6.7 (MEDIUM),    Exploitation_probability: 0.08;
        3.  CVE-2021-34724   Score: 6.0 (MEDIUM),    Exploitation_probability: 0.08;
        4.  CVE-2021-34723   Score: 6.7 (MEDIUM),    Exploitation_probability: 0.08;
        5.  CVE-2021-1624    Score: 8.6 (HIGH),      Exploitation_probability: 0.39;
        6.  CVE-2021-1621    Score: 7.4 (HIGH),      Exploitation_probability: 0.28;
        7.  CVE-2021-1620    Score: 7.7 (HIGH),      Exploitation_probability: 0.31;
        8.  CVE-2021-1529    Score: 7.8 (HIGH),      Exploitation_probability: 0.18;
        9.  CVE-2020-3508    Score: 7.4 (HIGH),      Exploitation_probability: 0.28;
       10.  CVE-2020-3396    Score: 7.2 (HIGH),      Exploitation_probability: 0.05;
```

Fig. 3.1. Example of vulnerability analysis, qualitative and quantitative indicators of Cisco ASR 1023 device network security, including the probability of exploitation probability of a particular vulnerability.

The detailed characterization of vulnerabilities of terminal, server, and network equipment is presented in the databases of commonly known information security vulnerabilities CVE (Common Vulnerabilities and Exposures) and CVSS (Common Vulnerability Scoring System) [36, 53], the content of which is constantly updated (Fig. 3.2).



CVSS v3.0 9.8 КРИТИЧНО CVSS v2.0 10.0 HIGH

9,8 /10

CVSS v3.0 : КРИТИЧНО

Легенда V3

Вектор:

Можливість експлуатації: 3,9 / Вплив: 5,9

Вектор атаки	МЕРЕЖА
Складність атаки	НИЗЬКИЙ
Потрібні привілеї	ЖОДНОГО
Взаємодія з користувачем	ЖОДНОГО
Вплив на конфіденційність	ВИСОКА
Вплив цілісності	ВИСОКА
Вплив доступності	ВИСОКА
Область застосування	БЕЗ ЗМІН

Fig. 3.2. Example of CVE-2021-34727 vulnerability key characteristics analysis (https://www.opencve.io/cve/CVE-2021-34727)

If the following condition is fulfilled in the objective function (3.1) when choosing the weighting coefficients

$$w_k >> w_{i,j}, \tag{3.3}$$

the number of disjoint paths will be maximized in the first place, by analogy with the optimality criterion (2.5). Then, the second term in (3.1) will affect the process of including the most secure links in the calculated set of paths.

If the condition $w_k << w_{i,j}$ holds, then the most secure links will be used first [36]. In the limiting case, it is even reasonable to fix the value of M^k, to ensure that the most secure links are included in the set of fixed number of disjoint paths. In addition to this section, primary attention will be paid to the case related to fulfilling conditions (3.3).

In turn, the probability of compromising the *n*th path in the TCN is calculated as [1, 19, 22, 36, 40]:

$$p_n = 1 - \prod_{E_{i,j} \in L_n} \left(1 - p_{i,j}\right), \tag{3.4}$$

where L_n – is the ordered set of links that make up the *n*th path.

Then the compromise probability of the set of calculated disjoint paths (multipath) is defined as [1, 19, 22, 36, 40]:

$$P_{MP}^k = \prod_{i=1}^{\mathrm{M}^k} p_n \,. \tag{3.5}$$

Thus, the choice of the $w_{i,j}$ is based on the use of expression (3.2) and focused on the inclusion in a set of disjoint paths of links with a minimum compromise probability. The introduction of the logarithm operation in (3.2) is dictated by the fact that when calculating the probability of compromising the paths (3.4) the corresponding probabilities of compromising the links obtained during the solution are multiplied, and the second term in (3.1) is an additive form. Solving the problem of secure routing using disjoint paths in [1, 22, 36] has been reduced to solving the optimization problem of Integer Linear Programming with criterion (3.1) and linear constraints (2.1)-(2.4), (2.6).

3.2. Mathematical Model of Secure QoS Routing over Disjoint Paths

The work proposes to solve the problem of secure QoS routing using disjoint paths, based on integrating the models described in the second section and expressions (3.1)-(3.5). The new solution initially proposes to consider aspects related to improving both the Quality of Service and network security at the stage of selecting the form of the complex optimality criterion for routing solutions based on the maximization of the objective function

$$J_3 = c_{\mathrm{M}}\mathrm{M}^k + c_\beta \beta_{path}^k - c_w \sum_{E_{i,j} \in E} w_{i,j} a_{i,j}^k , \qquad (3.6)$$

where the weighting coefficients c_{M}, c_β, and c_w determine the importance of each of the components in the expression (3.6), and the coefficients $w_{i,j}$ are determined by the expression (3.2). In fact, criterion (3.1) is a special case of (3.6) provided that $c_\beta = 0$, which leads to the realization of directly secure routing in TCN using the maximum number of disjoint paths.

The novelty of the model (2.1)-(2.4), (2.6), (2.7), (3.2)-(3.6) is that the use of the optimality criterion (3.6) allows us to choose the maximum number of paths that, first, disjoint, second, will have a bandwidth not less than the parameter β_{path}^k, whose value is maximized, and third, based on the introduction of the third term in the optimality criterion (3.6) contain communication links with minimum compromise probability. The first two components in (3.6) focus on implementing QoS routing in terms of bandwidth.

Such a formulation of the secure QoS routing problem (2.1)-(2.4), (2.6), (2.7), (3.2)-(3.6) focuses on increasing both the level of network security in TCN by reducing the probability of multipath compromise and increasing its total bandwidth. Thus, when using the secure QoS routing model (2. 1)-(2.4), (2.6), (2.7), (3.2)-(3.6) we talk about differentiated network security and quality of service (DiffServ). Depending on the type of the *k*th flow, the sensitivity to the quality of service and network security indicators of the set of disjoint paths calculated for it can be adjusted by selecting the ratio between the weight coefficients c_{β} and c_{W}.

3.3. Mathematical Model of Secure QoS Routing over Disjoint Paths that Provide Guaranteed Bandwidth

To ensure guarantees of the QoS level of in terms of bandwidth in the implementation of secure routing, it is proposed to formulate the routing problem within the model (2.1)-(2.4), (2.6), (2.7), (2.12), (3.1)-(3.5), in such an optimization formulation:

- the optimality criterion of routing solutions is the maximum of the objective function (3.1);
- constraints (2.1)-(2.4) and (2.7) are imposed on the routing variables $a_{i,j}^{k}$ and the variables β_{path}^{k} for balancing the routes' bandwidth;
- constraints (2.6) and (2.12) are imposed on the balancing variables β_{path}^{k} and the variable M^{k}, that determines the number of disjoint routes involved.

Thus, from the point of view of implementing a secure routing strategy, the use of model (2.1)-(2.4), (2.6), (2.7), (2.12), (3.1)-(3.5) focuses on the class of solutions of the DiffServ type, and from the point of view of QoS routing, the obtained solutions comply with the principles of IntServ. This is due to the fact that the use of optimality criterion (3.1) aims at choosing paths with a high but nonguaranteed level of network security. However, introducing conditions (2.12) into the model structure aims to guarantee the QoS level regarding the β^k bandwidth. Thus, the result of solving the formulated optimization problem is a multipath – a set of disjoint paths of maximum capacity that have a total bandwidth not less than the established requirements β^k, and a minimum compromise probability.

In general, the use of the model (2.1)-(2.4), (2.6), (2.7), (2.12), (3.1)-(3.5) allows us to classify the optimization problem of secure QoS routing along disjoint paths that provide guaranteed bandwidth as a Mixed Integer Nonlinear Programming problem since the constraints (2.12) are bilinear (nonlinear). If the number of disjoint paths used ($\mathrm{M}^k = \mathrm{const}$) is known in advance, then the criteria (3.1) will be simplified, i.e., it will be necessary to minimize a linear objective function of the form

$$J_4 = \sum_{E_{i,j} \in E} w_{i,j} a_{i,j}^k , \qquad (3.7)$$

where coefficients $w_{i,j}$ are determined by the expression (3.2) [36].

In addition, condition (2.12) also becomes linear, and the formulated optimization problem will belong to the MILP class since some of the control variables $a_{i,j}^k$ are Boolean (2.1) and some of them, β_{path}^k, are real numbers.

3.4. Investigation of Mathematical Models of Secure QoS Routing in a Network over Disjoint Paths

3.4.1. Study Results of a Mathematical Model of Secure Routing in a Network over Disjoint Paths

In [37, 42], the adequacy and validation of the model (2.1)-(2.4), (2.6), (3.1) has been verified on the example of the network topology presented in Fig. 3.3. The network consisted of seven routers and nine links, with the first router acting as the sender node and the seventh router as the destination node. Let us consider, for example, two variants of forming a set of disjoint paths when applying the proposed model for the initial data presented in Table 3.1.

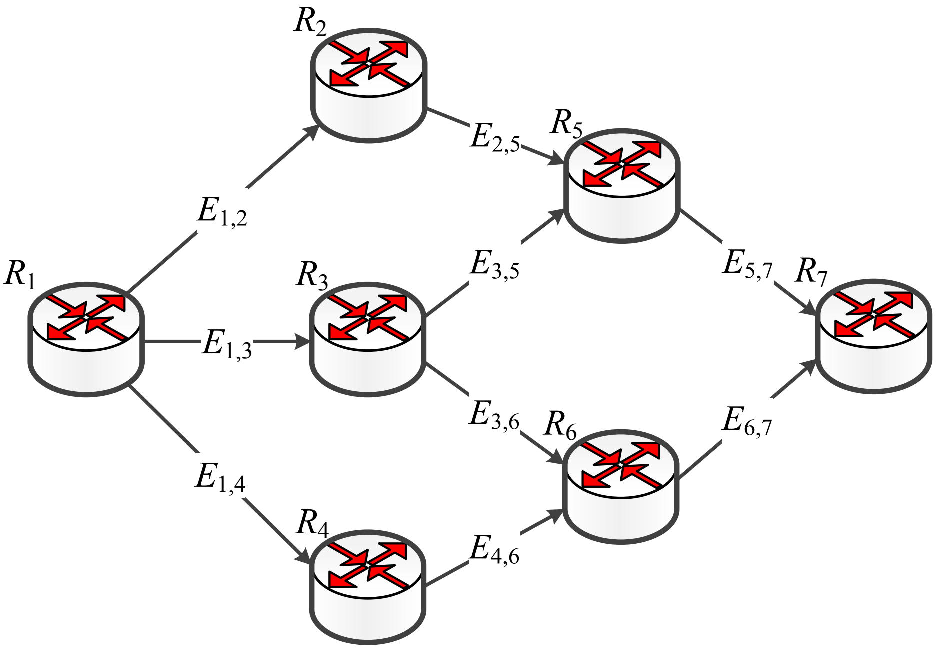


Fig. 3.3. Network structure used to study the secure routing model (2.1)-(2.4), (2.6), (3.1)

Table 3.1

Initial research data

Link	$E_{1,2}$	$E_{1,3}$	$E_{1,4}$	$E_{2,5}$	$E_{3,5}$	$E_{3,6}$	$E_{4,6}$	$E_{5,7}$	$E_{6,7}$
Link compromise probability									
Case 1	0.3	0.2	0.1	0.1	0.3	0.1	0.2	0.1	0.2
Case 2	0.3	0.1	0.1	0.1	0.2	0.1	0.2	0.1	0.2

Within the network structure, under consideration (Fig. 3.3), there is such set of paths between the first and seventh routers: $L_1 = \left\{E_{1,2}, E_{2,5}, E_{5,7}\right\}$; $L_2 = \left\{E_{1,3}, E_{3,5}, E_{5,7}\right\}$; $L_3 = \left\{E_{1,3}, E_{3,6}, E_{6,7}\right\}$; $L_4 = \left\{E_{1,4}, E_{4,6}, E_{6,7}\right\}$.

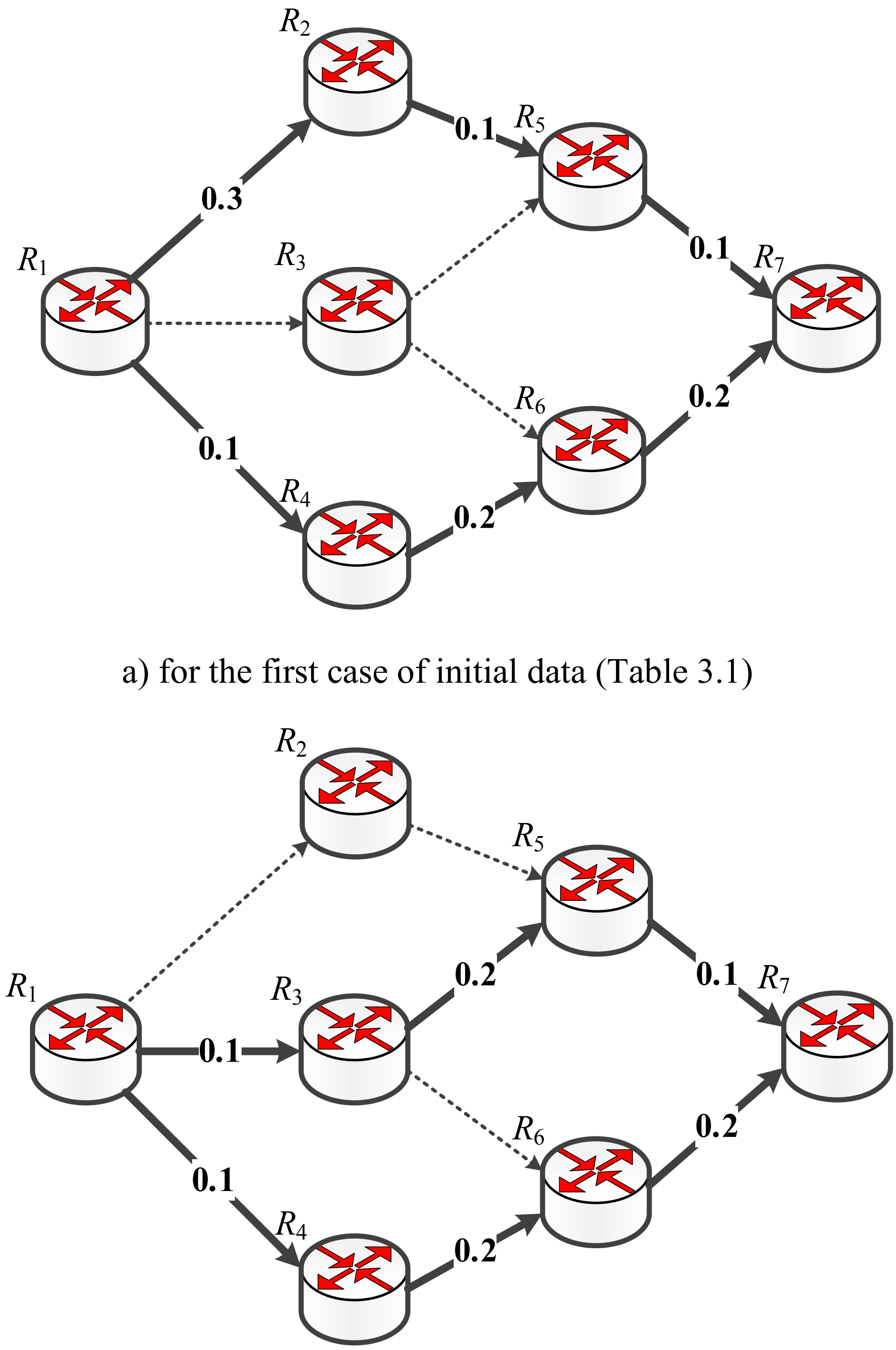
Then, in the determination M^k for each case (Table 3.1), three disjoint variants of the path computation solution (Table 3.2) can be obtained, the use of which provides the corresponding values of the multipath compromise probability (3.5).

Table 3.2

Probability of multipath compromise for different input data and solution options

Multipath	L_1 and L_3	L_1 and L_4	L_2 and L_4
Multipath compromise probability			
Case 1	0.1836	0.1836	0.2103
Case 2	0.1524	0.1836	0.1492

The application of the proposed model (2.1)-(2.4), (2.6), (3.1) made it possible to calculate the optimal multipath as the set of disjoint paths for each of the options for input data on the probabilities of network link compromising (Table 3.1). In the first case, the optimal solution is to use the paths L_1 and L_4 (Fig. 3.4 a) with the provision of $P_{MP} = 0.1836$, the value of which is the minimum among the possible solutions (Table 3.2). In Fig. 3.4, solid lines highlight the communication links that are included in the set of calculated paths that disjoint. The dotted lines show unused links. In the breaks of communication links (Fig. 3.4) the probabilities of their compromise are indicated (Table 3.1).



a) for the first case of initial data (Table 3.1)

b) for the second case of initial data; (Table 3.1)

Fig. 3.4. Variants of calculated optimal multipaths in the network (Fig. 3.3)

For the second case of initial data (Table 3.1) the optimal solution is to use paths L_2 and L_4 (Fig. 3.4 b) of $P_{MP} = 0.1492$, which is also the minimum of the three possible solutions (Table 3.2).

Thus, within the framework of the given computational example it was possible to confirm the adequacy and verify the performance of the mathematical model (2.1)-(2.4), (2.6), (3.1) in terms of the implementation of secure routing in the network on disjoint paths. Application of the model (2.1)-(2.4), (2.6), (3.1) allowed to determine the most secure set of disjoint paths and reduce the probability of multipath compromise (3.5) from 13% to 19% depending on the level of network security of communication links.

3.4.2. Study Results of the Processes of Secure Routing of Confidential Messages in a Network over Disjoint Paths

The model (2.1)-(2.4), (2.6), (3.1) can be used as an important component of the method of secure routing of confidential messages in the network over disjoint paths [40, 42]. The proposed method of secure routing of confidential messages by disjoint paths is based on the sequential solution of two problems:

- determination of disjoint paths in a telecommunication network using model (2.1)-(2.4), (2.6), (3.1);
- secure balancing of fragments (parts) of a confidential message over a set of pre-calculated disjoint paths.

The second problem can be solved, for example, by using the SPREAD (Secure Protocol for Reliable dAta Delivery) mechanism [19]. In [22, 23], a solution to develop and improve the SPREAD mechanism belonging to secure routing tools is proposed. To provide secure routing of a confidential message (CM) in the network, according to the SPREAD mechanism, the following tasks should be solved [19]:

1. Calculation of a set of disjoint paths between given nodes – source and destination.

2. Dividing the transmitted confidential message into set of fragments according to the chosen Shamir's scheme.

3. Distribution of a set of message fragments among a set of routes defined in the process of solving the first problem.

The scheme of dividing a message into fragments in general may be known to an attacker, but he can compromise a confidential message only when he compromises all the paths used for delivery. Therefore, the level of network security in this case depends entirely on the number and security of the paths used to deliver the CM fragments. For this purpose, the use of models (2.1)-(2.4), (2.6), (3.1) is proposed.

In order to explain how the SPREAD mechanism works, the following notations will be used [22, 23]:

- M – number of used disjoint paths in case of routing message parts;
- M_i – number of communication links in *i*th path that can be compromised $\left(i=\overline{1,M}\right)$;
- p_i^j – compromise probability of the *j*th communication link of the *i*th path $\left(i=\overline{1,M}, \quad j=\overline{1,M_i}\right)$;
- $\left(T,N\right)$ – Shamir's scheme parameters, where N – total number of fragments, into which the transmitted message is divided due to application of Shamir's scheme; T – minimum number of fragments, by which it is possible to restore the transmitted message $\left(T \le N\right)$;
- p_i – probability of compromise the *i*th path $\left(i=\overline{1,M}\right)$;
- P_{msg} – probability of compromise the message as a whole in case of its fragmented transmission by the network;
- n_i – integer variable, characterizing the number of CM fragments transmitted by the *i*th path $i=\overline{1,M}$.

Then, the possibility of compromising the *i*th path consisting of M_i parts can be calculated as follows:

$$p_i = 1-\left(1-p_i^1\right)\left(1-p_i^2\right)\ldots\left(1-p_i^{M_i}\right) = 1-\prod_{j=1}^{M_i}\left(1-p_i^j\right). \tag{3.8}$$

For control variables n_i $\left(i=\overline{1,M}\right)$ the following condition must be satisfied [22, 23]:

$$\sum_{i=1}^{M} n_i = N. \tag{3.9}$$

In case of realization of the Shamir’s scheme with parameters $T < N$ conditions must be satisfied [22, 23]

$$N-T+1 \le n_i \le T-1,\ \left(i=\overline{1,M}\right). \tag{3.10}$$

If the scheme without redundancy is used, i.e., the $T = N$, following conditions occur [22, 23]:

$$1 \le n_i \le T-1,\ \left(i=\overline{1,M}\right). \tag{3.11}$$

The probability of compromise of a confidential message divided according to Shamir’s scheme into *N* fragments with subsequent use of *M* paths is determined according to the expression [22, 23]

$$P_{msg} = \prod_{i=1}^{M} p_i\,. \tag{3.12}$$

In fact, expression (3.12) defines the probability of compromise of all disjoint paths that are used to transmit a confidential message fragments. That is, formula (3.12) is an analog of expression (3.5).

The task of secure balancing confidential message fragments over a set of precomputed, e.g., using models (2.1)-(2.4), (2.6), (3.1), *M* paths can also be submitted in an optimization form. The optimality criterion can be the minimum of the target function [22, 23]

$$J_5 = \sum_{i=1}^{M} p_i n_i \,, \tag{3.13}$$

in the presence of constraints (3.9)-(3.11) depending on the type of the chosen Shamir's scheme (with or without redundancy).

The research of the secure routing process of confidential messages organized with the help of the proposed method will be shown in the example of TCN, the structure of which is defined in Fig. 3.5.

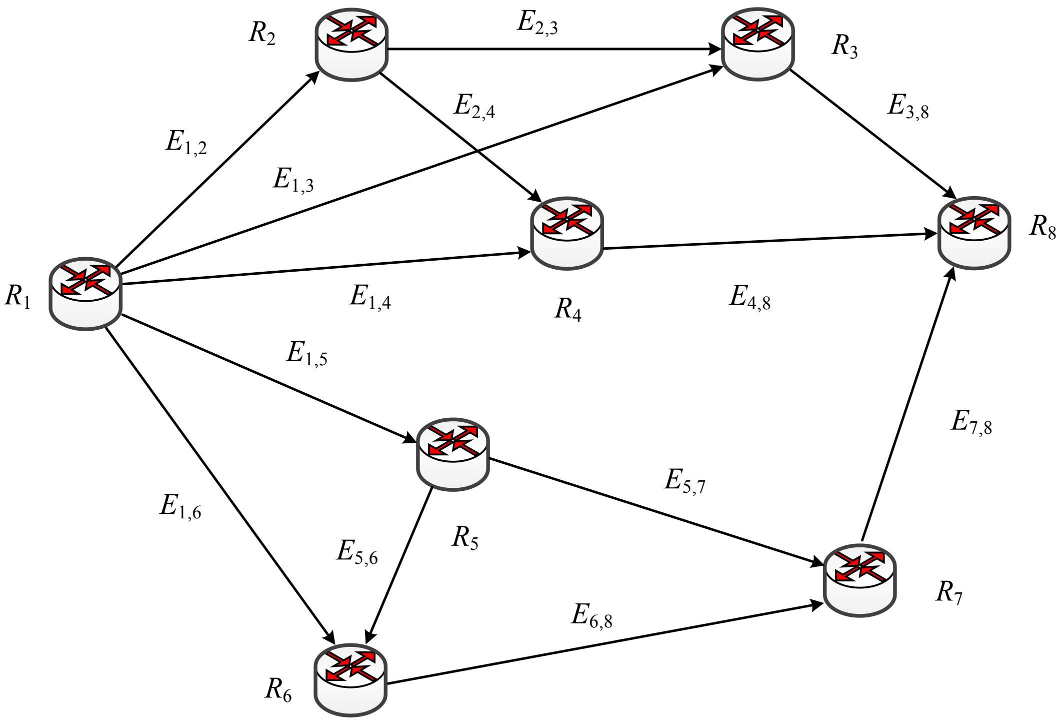


Fig. 3.5. The structure of the telecommunications network under study

The network contains eight routers and thirteen communication links. Suppose that a confidential message needs to be securely transmitted between routers R_1 and R_8. In the course of the study, three variants of compromise probabilities of TCN communication links were considered (Table 3.3).

Table 3.3

Variants of Compromise Probabilities of TCN Links

Variant #	$E_{1,2}$	$E_{1,3}$	$E_{1,4}$	$E_{1,5}$	$E_{1,6}$	$E_{2,3}$	$E_{2,4}$	$E_{3,8}$	$E_{4,8}$	$E_{5,6}$	$E_{5,7}$	$E_{6,7}$	$E_{7,8}$
1	0.1	0.8	0.3	0.4	0.8	0.2	0.5	0.6	0.5	0.4	0.3	0.9	0.2
2	0.9	0.6	0.1	0.2	0.8	0.3	0.1	0.3	0.7	0.4	0.9	0.2	0.1
3	0.1	0.1	0.9	0.9	0.6	0.1	0.3	0.8	0.4	0.6	0.2	0.1	0.1

Then Table 3.4 indicates all possible paths $(L_1 \div L_7)$ between routers R_1 and R_8, which were the sender and receiver of the CM.

Table 3.4

The Probabilities of Path Compromise in TCN for Different Variants of Network Path Compromise

Path		TCN link compromise variant number		
		1	2	3
L_1	$R_1 \to R_2 \to R_3 \to R_8$	0.712	0.951	0.838
L_2	$R_1 \to R_3 \to R_8$	0.92	0.72	0.82
L_3	$R_1 \to R_2 \to R_4 \to R_8$	0.775	0.973	0.622
L_4	$R_1 \to R_4 \to R_8$	0.65	0.73	0.94
L_5	$R_1 \to R_5 \to R_7 \to R_8$	0.664	0.928	0.928
L_6	$R_1 \to R_5 \to R_6 \to R_7 \to R_8$	0.9712	0.6544	0.9676
L_7	$R_1 \to R_6 \to R_7 \to R_8$	0.984	0.856	0.676

The same table shows the probabilities of path $L_1 \div L_7$, compromise calculated according to expression (3.8). The compromise probabilities of multipaths $LL_1 \div LL_7$, containing many disjoint paths are given in Table 3.5. Practically, Table 3.4 shows the compromise probabilities calculated according to formula (3.12).

Using the mathematical model (2.1)-(2.4), (2.6), (3.1) allowed us to determine such a set of used paths that corresponds to the minimum value of the message compromise probability (3.12), which will be transmitted by them in separate fragments. These paths in Table 3.5 for each variant of communication links compromise is highlighted in gray color.

Table 3.5

Multipath Compromise Probabilities in TCN Containing Disjoint Paths for Different Link Compromise Variants

Multipath	Paths contained in a multipath	TCN link compromise variant number		
		1	2	3
LL_1	L_1, L_4, L_5	0.3073	0.6442	0.731
LL_2	L_1, L_4, L_6	0.4495	0.4543	0.7622
LL_3	L_1, L_4, L_7	0.4554	0.5943	0.5325
LL_4	L_2, L_4, L_5	0.3971	0.4878	0.7153
LL_5	L_2, L_4, L_6	0.5808	0.344	0.7458
LL_6	L_2, L_4, L_7	0.5884	0.4499	0.5211
LL_7	L_2, L_3, L_5	0.4734	0.6501	0.4733
LL_8	L_2, L_3, L_6	0.6925	0.4584	0.4935
LL_9	L_2, L_3, L_7	0.7016	0.5997	0.3448

Consequently, the results of the study given in Table 3.4 and Table 3.5 confirmed the adequacy of the model of route recalculation (2.1)-(2.4), (2.6), (3.1) in the telecommunication network. The use of the proposed method and secure routing model allowed, in comparison with other available solutions, the reduction of the probability of compromising confidential messages (Table 3.5): from 23% to 56% for the first variant; from 27% to 47% for the second scenario and from 27% to 55% for the third variant of compromising the links and routes of the network (Tables 3.3 and 3.4).

To illustrate the results obtained, Fig. 3.6-3.8 shows the sets of disjoint paths in TCN , i.e., only the sender (R_1) and receiver (R_8) nodes are common.

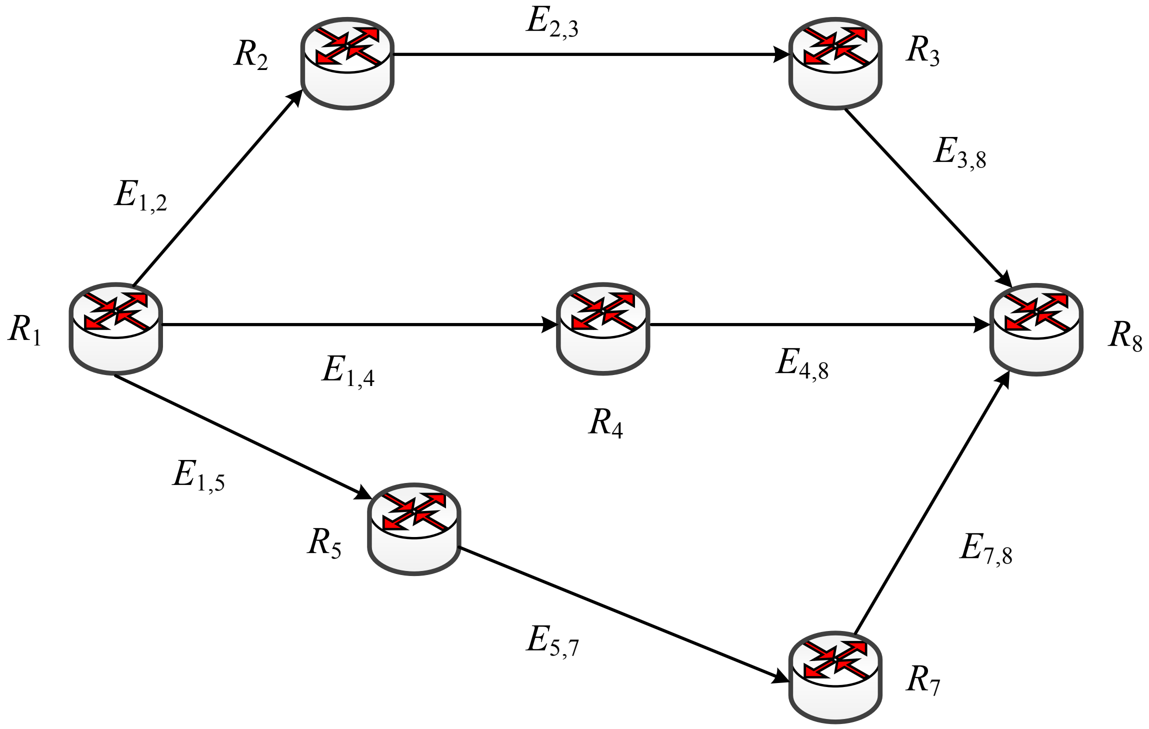


Fig. 3.6. Set of optimal paths L_1, L_4, L_5 for the first variant of TCN communication links compromise $\left(P_{msg} = 0.3073\right)$

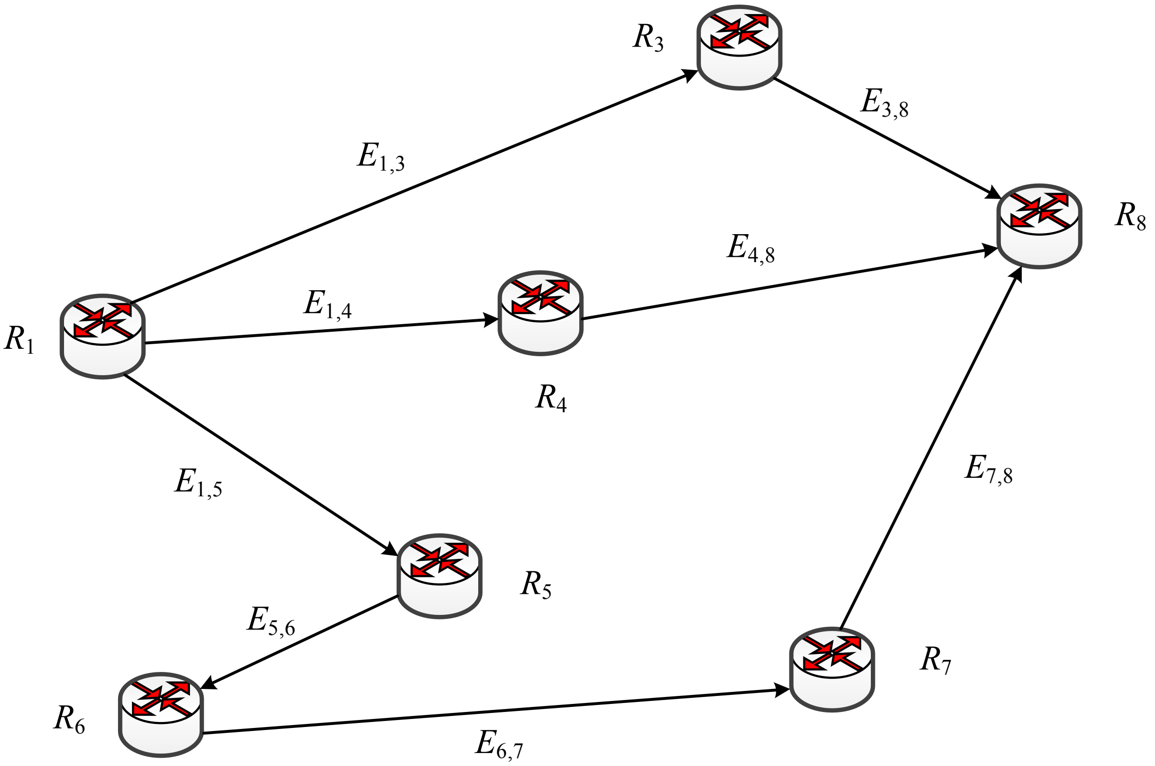


Fig. 3.7. Set of optimal paths L_2, L_4, L_6 for the second variant of TCN links compromise $\left(P_{msg} = 0.344\right)$

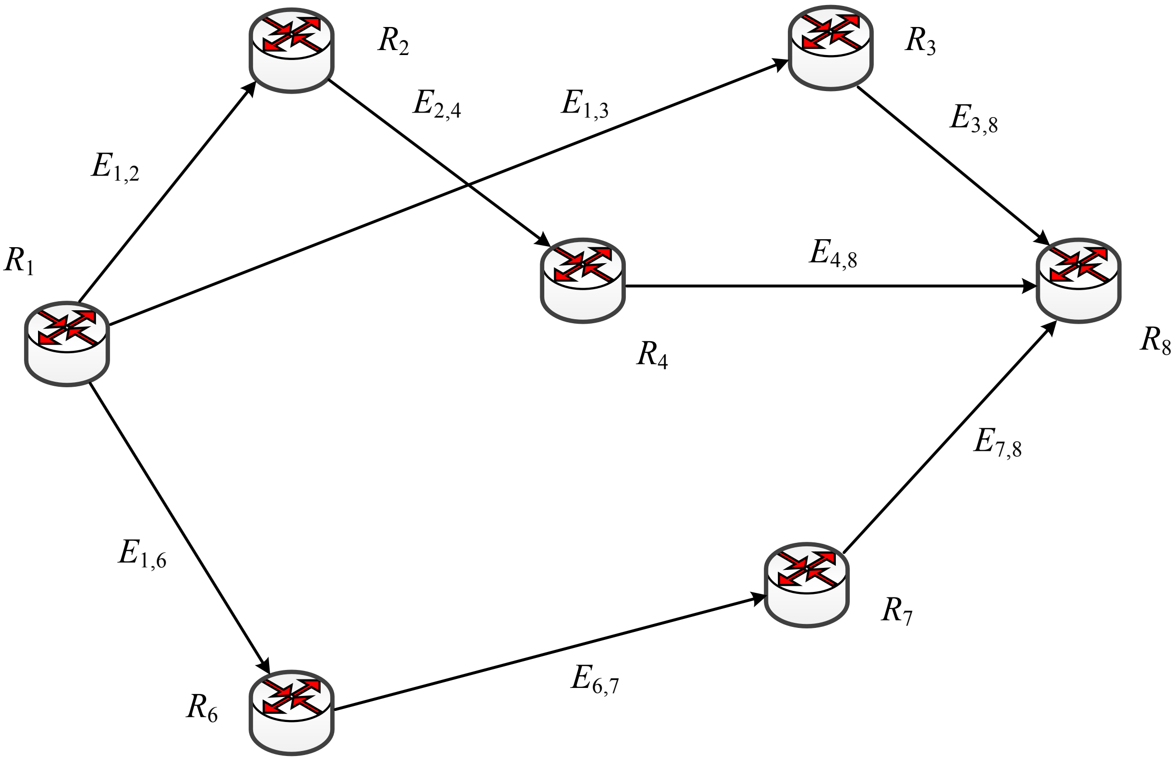


Fig. 3.8. Set of optimal paths L_2, L_3, L_7 for the third variant of TCN links compromise $\left(P_{msg} = 0.3448\right)$

Table 3.6 shows the order of fragmented message transmission in TCN using a set of computed disjoint paths (Table 3.5), for different variants of network link compromise. Shamir's scheme (10, 10) was used to fragment the confidential message. As shown in Table 3.6, the number of fragments transmitted by a particular path corresponded to its compromise probability (3.8) and conditions (3.11).

The higher the path compromise probability, the fewer message fragments were transmitted by it. But always to compromise a message an attacker needs to have compromised all three disjoint routes used for transmission.

Table 3.6

Order of Fragmented Message Transmission in TCN Using a Set of Computed Disjoint Paths for Different Variants of Network Link Compromise

TCN link compromise #	Multipath	Path	Quantity of message fragments, n_i	Path compromise probability
1	LL_1	L_1	3	0.712
		L_4	4	0.65
		L_5	3	0.664
2	LL_5	L_2	3	0.72
		L_4	3	0.73
		L_6	4	0.6544
3	LL_9	L_2	3	0.82
		L_3	4	0.622
		L_7	3	0.676

3.4.3. Research Results of Mathematical Models of Secure QoS Routing in a Network over Disjoint Paths

The peculiarities of the operation of the proposed models of secure QoS routing in a telecommunications network will be demonstrated by the following numerical example. In the structure of the considered network, shown in Fig. 2.2, the first and the seventh routers will be the nodes source and destination of packets, respectively. Four cases of link compromise probabilities are envisioned to form a set of disjoint paths if the proposed models are applied (Table 3.7). In the same table the bandwidths of communication links of the network are specified.

Table 3.7

Initial Data for the Study of Secure QoS Routing Models

Link	BW, pps	Probability of link compromise			
		Case 1	Case 2	Case 3	Case 4
$E_{1,2}$	200	0.4	0.2	0.1	0.1
$E_{1,3}$	270	0.3	0.1	0.2	0.15
$E_{1,4}$	250	0.4	0.3	0.3	0.2
$E_{2,5}$	150	0.2	0.2	0.2	0.1
$E_{2,7}$	220	0.2	0.4	0.4	0.35
$E_{3,5}$	130	0.1	0.1	0.1	0.15
$E_{3,6}$	190	0.2	0.1	0.2	0.1
$E_{4,7}$	230	0.2	0.1	0.4	0.2
$E_{4,6}$	140	0.2	0.3	0.1	0.1
$E_{5,7}$	220	0.3	0.2	0.3	0.15
$E_{6,7}$	280	0.1	0.4	0.2	0.3

The set of possible paths between source and destination nodes is described by the system (2.11). The bandwidths and compromise probabilities of the paths (2.11) available for packet transmission, connected by the sender (R_1) and receiver (R_7), routers, for different cases of network link compromise probabilities are given in Table 3.8.

Table 3.8

The Bandwidth of Paths Available for Packet Transmission Between R_1 and R_7

Path #	Path	BW, pps	Path compromise probability			
			Case 1	Case 2	Case 3	Case 4
1	$\{E_{1,2}, E_{2,5}, E_{5,7}\}$	150	0.6640	0.4880	0.4960	0.3115
2	$\{E_{1,3}, E_{3,6}, E_{6,7}\}$	190	0.4960	0.5140	0.4880	0.4645
3	$\{E_{1,4}, E_{4,7}\}$	230	0.5200	0.3700	0.5800	0.3600
4	$\{E_{1,4}, E_{4,6}, E_{6,7}\}$	140	0.5680	0.7060	0.4960	0.4960
5	$\{E_{1,3}, E_{3,5}, E_{5,7}\}$	130	0.5590	0.3520	0.4960	0.3859
6	$\{E_{1,2}, E_{2,7}\}$	200	0.5200	0.5200	0.4600	0.4150

Table 3.9 shows possible solutions to the routing problem, which include the maximum number of calculated disjoint paths. For each multipath, Table 3.9 shows their bandwidth and the compromise probability. In Table 3.9, for each case of the initial data, the extreme bandwidth values and the multipath compromise probability are grayed out. For example, solution number four represents the multipath that has the maximum bandwidth (620 pps), the maximum boundary value β_{path}^{k} (190 pps),

and the minimum compromise probability (0.1341) for the first case of the initial data on the probability of compromising the network communication links (Table 3.7).

Table 3.9

Calculation Results of the Set of Disjoint Paths

Set #	Disjoint Paths Set	BW multi path, pps	Minimal boundary value β_{path}^{k}	Multipath compromise probability			
				Case 1	Case 2	Case 3	Case 4
1	$\{E_{1,2},E_{2,5},E_{5,7}\}$ $\{E_{1,3},E_{3,6},E_{6,7}\}$ $\{E_{1,4},E_{4,7}\}$	570	150	0.1713	0.0928	0.1404	0.0521
2	$\{E_{1,4},E_{4,6},E_{6,7}\}$ $\{E_{1,3},E_{3,5},E_{5,7}\}$ $\{E_{1,2},E_{2,7}\}$	470	130	0.1651	0.1292	0.1132	0.0794
3	$\{E_{1,4},E_{4,7}\}$ $\{E_{1,3},E_{3,5},E_{5,7}\}$ $\{E_{1,2},E_{2,7}\}$	560	130	0.1512	0.0677	0.1323	0.0576
4	$\{E_{1,3},E_{3,6},E_{6,7}\}$ $\{E_{1,4},E_{4,7}\}$ $\{E_{1,2},E_{2,7}\}$	620	190	0.1341	0.0989	0.1302	0.0694

The calculations demonstrated that in all four cases the introduction of the third term to the criterion (3.6) allowed to obtain a multipath not only with high bandwidth, but also with the minimum value of the compromise probability of the communication links that were contained in the calculated multipath.

In the case when in the criterion of optimality of routing solutions (3.6) the coefficients are normalized in such a way that the condition $c_{\mathrm{M}} \gg c_{\beta} \gg c_{w}$, is fulfilled, the use of the proposed model of secure QoS routing (2.1)-(2.4), (2.6), (2.7), (3.2)-(3.6) provided the fourth numbered solution (Fig. 3.9). It is this solution that corresponds to the highest value of multipath bandwidth and the maximum value of threshold β_{path}^{k} (190 pps) for all cases of link and network route compromise (Table 3.9).

The labels in Fig. 3.9 are similar to the labels used in Fig. 2.3 and Fig. 2.4. The communication link gaps (Fig. 3.9) are indicated by a fraction, wherein the numerator is the compromise probability and in the denominator is the bandwidth of the used link (Table 3.7).

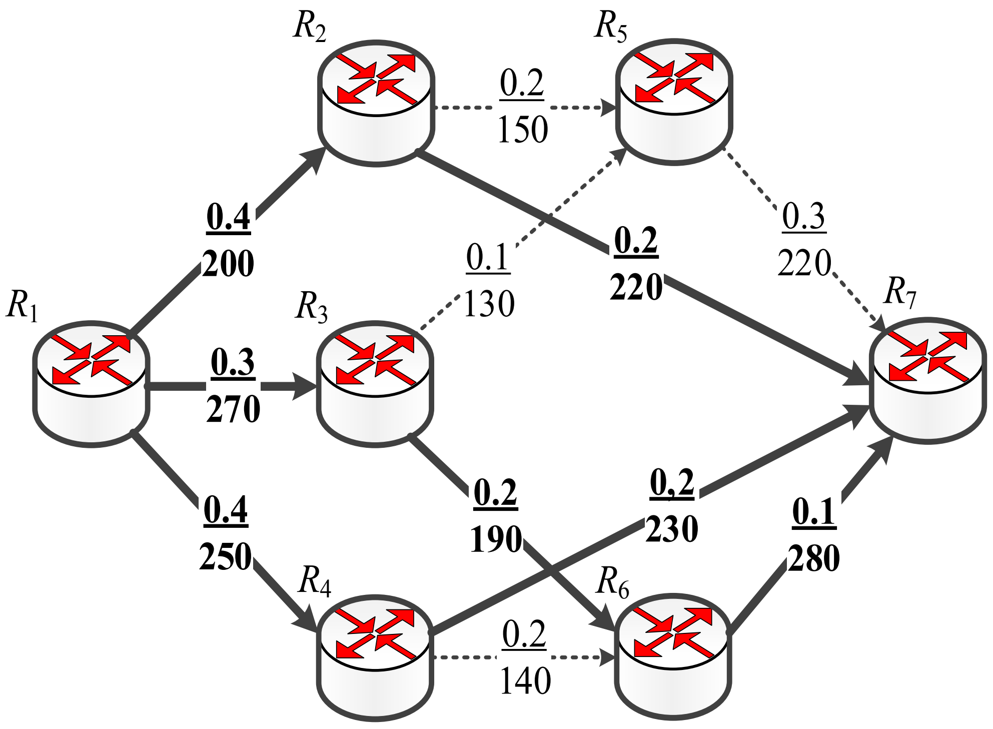


Fig. 3.9. Set of disjoint paths (Case 1)

When in the criterion of optimality of routing solutions (3.6) the coefficients are normalized in such a way that the condition $c_{\mathrm{M}} \gg c_{w} \gg c_{\beta}$, is met, then the use of the model (2.1)-(2.4), (2.6), (2.7), (3.2)-(3.6) provided a solution (Table 3.9), which would correspond to the minimum value of the multipath compromise probability. For example, for the fourth case of initial data on the compromise of links and routes in the network (Table 3.9), the first solution is optimal (Fig. 3.10).

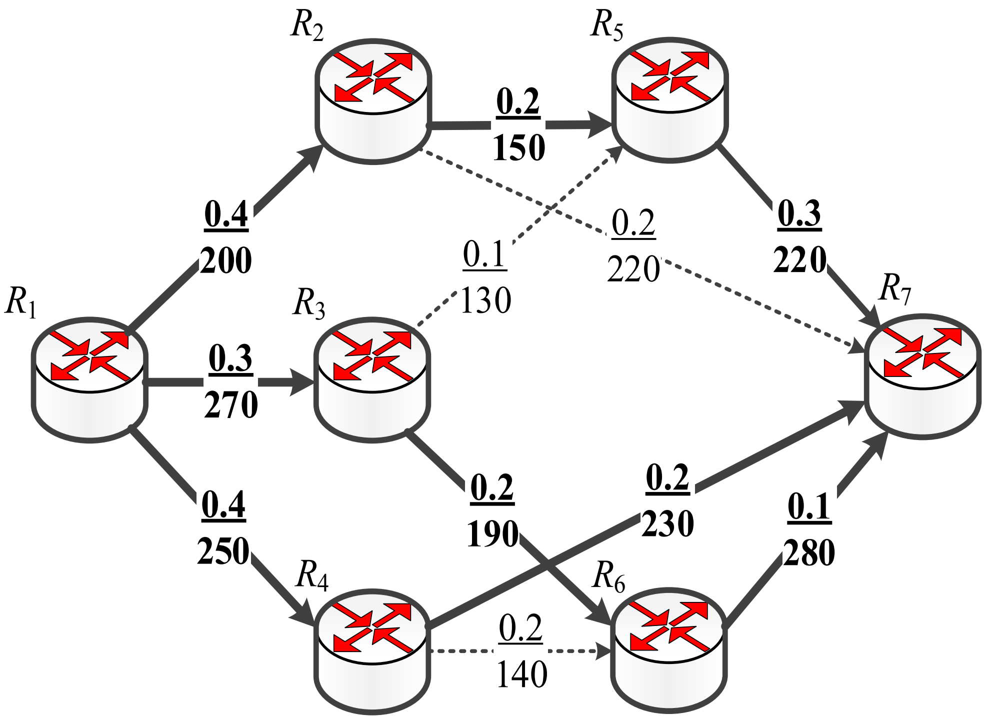


Fig. 3.10. Set of optimal disjoint paths (Case 4)

The analysis of the calculation results is given in Table 3.8 shows that using the integral criterion (3.6) allows us to provide a routing solution to maximize the least productive path's bandwidth and minimize the multipath compromise probability value. The application of the proposed model (2.1)-(2.4), (2.6), (2.7), (3.2)-(3.6) improved the multipath compromise probability from 11.5% to 22% on average for the first case; from 27% to 47% for the second case; from 13% to 19.5% for the third case and from 9.5% to 34.5% for the fourth case of link compromise probability values (Table 3.7).

The sensitivity of packet flow to the indicators of quality of service (bandwidth) and network security can be adjusted in the process of selecting the ratio between a more extended set of weight coefficients c_{β}, c_{v}, and c_{w}. By adjusting the ratio between c_{β} and c_{w} in the criterion (3.6) using the proposed secure QoS routing model (2.1)-(2.4), (2.6), (2.7), (3.2)-(3.6), a solution compromising both the level of quality of service (multipath bandwidth) and the level of network security (compromise probability) can be obtained.

The requirements β^{k} in a constraint condition (2.12) play an important role in the study of the secure QoS routing model over disjoint paths and provide guaranteed bandwidth, (2.1)-(2.4), (2.6), (2.7), (2.12), (3.1)-(3.5), since the optimality criterion (3.1) does not explicitly include parameters related to link and path capacity. At the fulfillment level of conditions (2.12), guarantees should be provided that the multipath using the *k*th packet flow will have a bandwidth of at least β^{k}. The product determines the level of guarantees provided according to the conditions (2.12) by multipath $\mathrm{M}^{k}\beta^{k}_{path}$.

Thus, within the initial data given in Table 3.7 and Table 3.8, depending on the level of requirements β^{k} quite different solutions can be optimal. So, for the first case of initial data (Table 3.7), only the first solution (Table 3.9), if $\beta^{k} \le 570$ pps. For higher bandwidth guarantee requirements, this problem has no solutions.

For the second case of the initial data (Table 3.7), the minimum value of the multipath compromise probability (0.0677) will provide the third solution, provided that $\beta^{k} \le 390$ pps. If the guarantee requirements are in the range of $390 < \beta^{k} \le 450$, then the first solution with a multipath compromise probability of 0.0928 is optimal. When the multipath bandwidth requirements increase and are in the range of $450 < \beta^{k} \le 570$, then the only available and optimal solution is the fourth solution with $P^{k}_{MP} = 0.0989$.

For the third case of initial data (Table 3.7), the minimum value of multipath compromise probability (0.1132) is provided by the second solution provided that

$\beta^k \leq 390$ pps. If the guarantee requirements are in the range of $390 < \beta^k \leq 570$, then the fourth solution with a multipath compromise probability of 0.0989 is again optimal.

When the fourth case of initial data (Table 3.7) was investigated, the minimum value of multipath compromise probability (0.0521) is provided by the first solution at $\beta^k \leq 450$ pps. If the guarantee requirements are in the range of $450 < \beta^k \leq 570$, then the fourth solution with a multipath compromise probability of 0.0989 is traditionally optimal.

Thus, the logic of the secure QoS routing model with guaranteed bandwidth provisioning (2.1)-(2.4), (2.6), (2.7), (2.12), (3.1)-(3.5) is that as optimal, the multipath that, first, has bandwidth not less than the β^k requirement, and, second, provides the minimum value of its compromise probability.

3.5. Conclusion to the Third Chapter

1. This chapter presents a system of mathematical models of secure QoS routing in a telecommunication network over disjoint paths. The common feature of the proposed models is that they reduce the solution of the technological problem of secure QoS routing to the solution of different types of optimization problems. Depending on the set of considered TCN aspects, the models differed in the type of optimality criteria and the set of constraints imposed on the routing variables ($a_{i,j}^k$) and path bandwidth balancing variables β_{path}^k.

2. The mathematical model of secure routing over disjoint paths in the network (2.1)-(2.4), (2.6), (3.1)-(3.5) is analyzed and investigated. A modification of the model is to use an optimality criterion related to the maximization of the objective function (3.1). The model retains its main advantage of linearity. Introduction into the optimality criterion (3.1) of additional components weighted with respect to the values of the compromise probability of TCN links allowed to

ensure the calculation of such disjoint paths (multipath) so that their number is maximized and the compromise probability of these paths (3.4), (3.5) is minimized. This was achieved by the fact that the choice of weighting coefficients in the criterion (3.1) is based on the use of expression (3.3) and is aimed at including in the set of disjoint paths of communication links with a minimum compromise probability. The computational examples given in paragraph 3.4.1 demonstrate the functionality of the proposed mathematical model, its operability, adequacy, and efficiency in terms of implementing secure routing in TCN.

3. The model of secure QoS routing disjoint paths in the network (2.1)-(2.4), (2.6), (2.7), (3.2)-(3.6) is developed and investigated. In the framework of the proposed solution, the aspects related to improving the Quality of Service and network security are taken into account at the stage of selecting the form of the complex optimality criterion of routing solutions (3.6). The use of (3.6), on the one hand, guarantees the search for the most productive paths (the first and second summands are responsible for this), and, on the other hand, the inclusion of the most secure TCN links (the third term) in the set of calculated paths. For this purpose, the path metrics (3.2) related to the network security parameters of the communication links, i.e., their compromise probabilities, were used. This technological problem was reduced to an optimization problem of the MILP class with maximization of the number of paths and their bandwidth, as well as minimization of the multipath compromise probability as a whole in the presence of linear constraints, since the routing variables are Boolean (2.1) and the variables determining the number of routes used take only these integer values (2.6).

The research results (Tables 3.7-3.9) of the proposed model of secure QoS routing over disjoint paths in the network (2.1)-(2.4), (2.6), (2.7), (3.2)-(3.6) have confirmed its adequacy and effectiveness in terms of providing extreme values of multipath bandwidth and/or their compromise. Within the model, the sensitivity of packet flow to Quality of Service (bandwidth) and network security metrics can be adjusted in the process of selecting the relationship between a more extended set of weighting coefficients c_β, c_v, and c_w in the optimality criterion (3.6).

4. In the chapter, to guarantee the level of Quality of Service in terms of bandwidth when implementing secure routing over disjoint paths, a mathematical model represented by expressions (2.1)-(2.4), (2.6), (2.7), (2.12) , (3.1)-(3.5) is proposed. Within this model, the QoS secure routing problem is also formulated in an optimization form. The optimality criterion for routing solutions was the maximum of objective function (3.1), and constraints (2.1)-(2.4), (2.6), (2.7), and (2.12) were imposed on the control variables. The use of the optimality criterion (3.1) aims at selecting paths with a high but unguaranteed level of network security. The introduction of conditions (2.12) into the model is aimed at providing guarantees of the QoS level in terms of bandwidth β^k. Thus, the result of the solution of the formulated optimization problem is a set of disjoint paths that have a total bandwidth not less than the established requirements β^k, and a minimum probability of compromise.

5. The optimization problem formulated to be solved within the model (2.1)-(2.4), (2.6), (2.7), (2.12), (3.1)-(3.5) is generally classified as a MINLP problem, since the constraints (2.12) are bilinear (nonlinear). If the number of used disjoint paths is known in advance ($\mathrm{M}^k = \mathrm{const}$), then the criteria (3.1) will be simplified and the constraints (2.12) will become linear. Then the problem will belong to the class of MILP problems.

6. The results of the investigation of the mathematical model of secure QoS routing over disjoint paths (2.1)-(2.4), (2.6), (2.7), (2.12), (3.1)-(3.5) have confirmed its efficiency in terms of providing guaranteed multipath bandwidth and low probability of its compromise. The sensitivity of the obtained solutions to the QoS guarantee level requirements was revealed (Tables 3.7-3.9). It is established that the provision of guarantees on the multipath bandwidth occurs, as a rule, with a certain and sometimes significant reserve, since the linear conditions (2.12) are formulated for the worst case, when all the routes calculated and included in the optimal multipath have approximately the same bandwidth at the level β_{path}^k.

CHAPTER 4

OPTIMIZATION MODEL OF FAST REROUTING IN TELECOMMUNICATION NETWORKS

The chapter is devoted to the search for solutions to the problem of fault-tolerant routing in telecommunication networks. The analysis of known schemes of redundancy (protection) of network elements [1, 16-18, 36] has shown that implementing a route protection scheme is the most reliable solution for the organization of fault-tolerant routing. This architecture of solutions to improve the reliability of the telecommunications network is maximally adapted to possible single and especially multiple failures of any links or routers over the primary route(s). From the point of view of protecting the QoS level in the network, the routing solution should provide calculation and support of multiple primary and backup routes with the required capacity.

In this chapter, the improvement of the basic mathematical model (2.1)-(2.4), (2.6) is proposed to solve the problems of fault-tolerant routing, namely fast rerouting, when simultaneously with the definition of the primary route a set of backup paths is calculated. Packet flows start using backup paths when the primary route fails, which increases the responsiveness of the network to its possible overload, failures in software and switching hardware, as well as server equipment. The time for switching to a backup route in modern IP/MPLS networks is tens of milliseconds [1, 16]. The solution proposed in this chapter will focus on implementing $n{:}1$ path protection schemes and network bandwidth, i.e., one primary and n backup paths should not cross transit nodes (routers) and TCN links.

The main results of the chapter are published in [36, 39, 41, 42, 44, 47-49, 51, 52].

4.1. Improvement of Fast ReRoute Model with Realization of Path and Network Bandwidth Protection Scheme

In this chapter, all the notations introduced in the previous chapters of the work remain relevant. The improvements realized in this section concern the mathematical model represented by expressions (2.1)-(2.4), (2.6). The network bandwidth threshold β^k introduced in section 2.3, which must be provided for *k*th packet flow, retains its full meaningfulness. However, if the fulfillment of condition (2.12) should be ensured, as a rule, based on the implementation of multipath routing over disjoint paths, i.e., at $\mathrm{M}^k \geq 2$, then in the framework of the improved model of fast rerouting, we will still be talking about the implementation of single path routing.

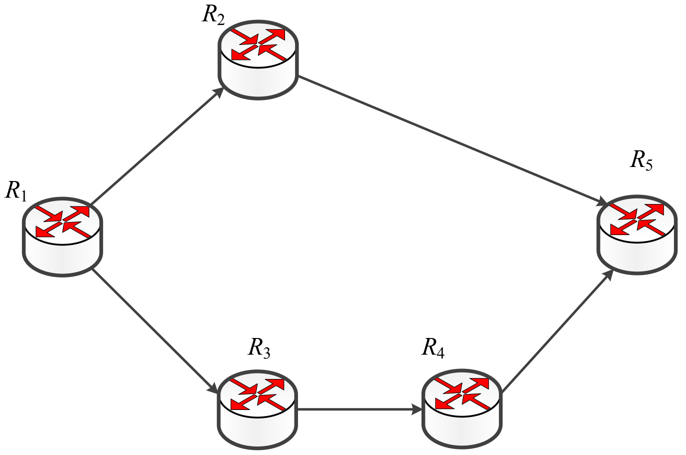
Then, each path calculated for the *k*th packet flow (primary and backup) must have a bandwidth of at least β^k. Taking into account the expression (2.12), the condition of network bandwidth protection for the *k*th packet flow can be formulated as follows:

$$\beta^k_{path} \geq \beta^k . \tag{4.1}$$

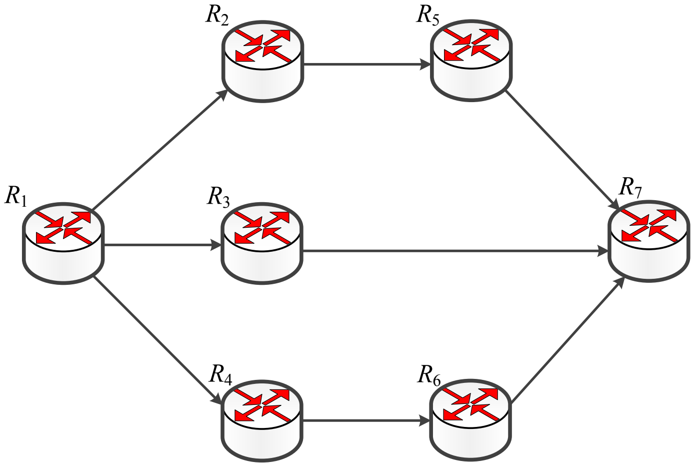
Hence, to implement fast rerouting with *n*:1 path protection, it is necessary for the *k*th packet flow to compute the number of disjoint paths M^k, such that this condition is satisfied:

$$\mathrm{M}^k = n+1 . \tag{4.2}$$

For example, to support a 1:1 scheme, calculate two $\left(\mathrm{M}^k = 2\right)$ disjoint paths (Fig. 4.1 a), one of which will be the primary path (e.g. $R_1 \to R_2 \to R_5$), and the other (e.g. $R_1 \to R_3 \to R_4 \to R_5$) will be the backup paths. When planning a 2:1 scheme, it is necessary to calculate three disjoint paths $\left(\mathrm{M}^k = 3\right)$, already, one of which will again be the primary path (e.g. $R_1 \to R_2 \to R_5 \to R_7$), and the other two (e.g. $R_1 \to R_4 \to R_6 \to R_7$ and $R_1 \to R_3 \to R_7$) will be the backup paths (Fig. 4.1 b). Naturally, the use of the 2:1 scheme is more reliable than the 2:1 scheme, but is associated with the use of additional network resource – routers, communication links and their bandwidth, as it must also be reserved for the selected *k*th and packet flow.



a) *n*=1



b) *n*=2

Fig. 4.1. Examples of *n*:1 redundancy scheme implementation

The following two optimality criteria of solutions to the FRR problem are chosen for research and comparative analysis, one of which is the maximum of the function

$$J_6 = \beta_{path}^k . \tag{4.3}$$

While the other optimality criterion of routing decisions is related to maximization of the objective function modified with respect to (4.3) (analogous to (2.8)):

$$J_7 = c_\beta \beta_{path}^k - c_v \sum_{E_{i,j} \in E} v_{i,j} a_{i,j}^k , \tag{4.4}$$

where the weighting coefficients c_β and c_v determine the importance of each of the components in the expression (4.4). It is expedient to ensure fulfillment of conditions (2.9) and a simplified version of conditions (2.10): $c_\beta >> c_v$.

The first case (4.3) is responsible for maximizing the bandwidth lower bound of each set of the calculated disjoint paths – primary and backup. If we restrict ourselves to criterion (4.3), the lowest-performing path will have a bandwidth equal to the value β_{path}^k. On the other hand, the use of criterion β_{path}^k (4.3) may not always contribute to obtaining a solution when the set of calculated paths forms the most productive communication links. This is due to the fact that the bandwidth of a route determines the included link with the lowest productivity.

Therefore, the advantage of the improved model (2.1)-(2.4), (2.7), (2.9), (4.1), (4.2), (4.4) is the use of the second summand in the criterion (4.4), introduced as in (2.8) by analogy to the metrics of the OSPF and EIGRP routing protocols (2.9) to include in the calculated routes of communication links with high capacity. The additive nature of the second summand in the target function (4.4) also aims at the fact that the calculated routes (primary or backup) will contain the minimum number of communication links.

Consequently, the problem of computing the set of the most productive primary and backup paths to realize fast rerouting reduces to solving a Mixed Integer Linear Programming optimization problem with criterion (4.3) or (4.4) in the presence of linear constraints (2.1)-(2.4), (2.7), (4.1), since the routing variables $a_{i,j}^{k}$ are Boolean and a variable β_{path}^{k} – real number. The introduced conditions (2.1)-(2.4) are responsible for the realization of the path protection scheme, and conditions (2.7), (4.1) – the network capacity protection scheme. To realize real-time computation within the proposed model, the formulated MILP problem should be solved by heuristic methods, e.g., using ant colony optimization algorithms, simulated annealing, Hopfield networks, etc. [36, 41].

The solution of the formulated optimization problem results in a set of disjoint routes. When selecting the primary and backup routes, certain recommendations should be followed:

- it is advisable that within the set of paths exactly the route with the maximum bandwidth corresponds to the primary path;
- if several paths have maximum bandwidth, the route with the minimum number of communication links should be chosen as the primary one;
- backup paths are selected from the remaining routes, according to the reduction of their capacity.

Each of the calculated routes will have the required bandwidth capacity due to ensuring fulfillment of conditions (2.7) and (4.1). In general, the total number of calculated backup paths depends on the chosen redundancy scheme (1:1, 2:1,..., *n*:1) related to the requirements of ensuring reliability and fault tolerance of routing solutions for each packet flow and the network in general.

4.2. Research and Comparative Analysis of the Obtained Routing Solutions Using an Improved Model of Fast ReRouting by Disjoint Paths

The research process compared the routing solutions obtained by model (2.1)-(2.4), (2.7), (2.9), (4.1), (4.2) while using optimality criteria (4.3) and (4.4) for different network structures and redundancy schemes, e.g. 2:1 and 3:1.

As an example, the results of the study will be demonstrated on the network structure shown in Fig. 2.5 when the link gaps indicate their bandwidths (pps). In general, eight paths can be established between the first and ninth routers, which nodes and/or links can intersect. The properties of these paths are summarized in Table 2.3.

4.2.1. Research Results and Comparative Analysis of the Obtained Routing Solutions when Implementing the 2:1 Redundancy Scheme

The first case makes it necessary to realize the scheme of route protection 2:1 when transmitting packets of one flow ($k = 1$) from the first router to the ninth with the requirements of the QoS level in terms of bandwidth at the level of 390 pps. Consequently, the value of the network bandwidth protected in the fast rerouting process is determined at the $\beta = 390$ pps level. Using the computational model (2.1)-(2.4), (2.7), (2.9), (4.1), (4.2) with the optimality criterion (4.3) determined for the realization of the 2:1 redundancy scheme three disjoint paths: L_2, L_4 and L_8 (Fig. 4.2).

Each of these paths (Fig. 4.2) had the bandwidth (Table 2.3) not less than the calculated threshold (β^k_{path} = 400 pps), i.e., conditions (2.7) and (4.1) were fulfilled. That is, a fast rerouting with network bandwidth protection was implemented. In this case, it is reasonable to choose the route L_8 as the primary one, L_4 – as the first backup, and L_2 – as the second backup route in accordance with the increase in their bandwidth.

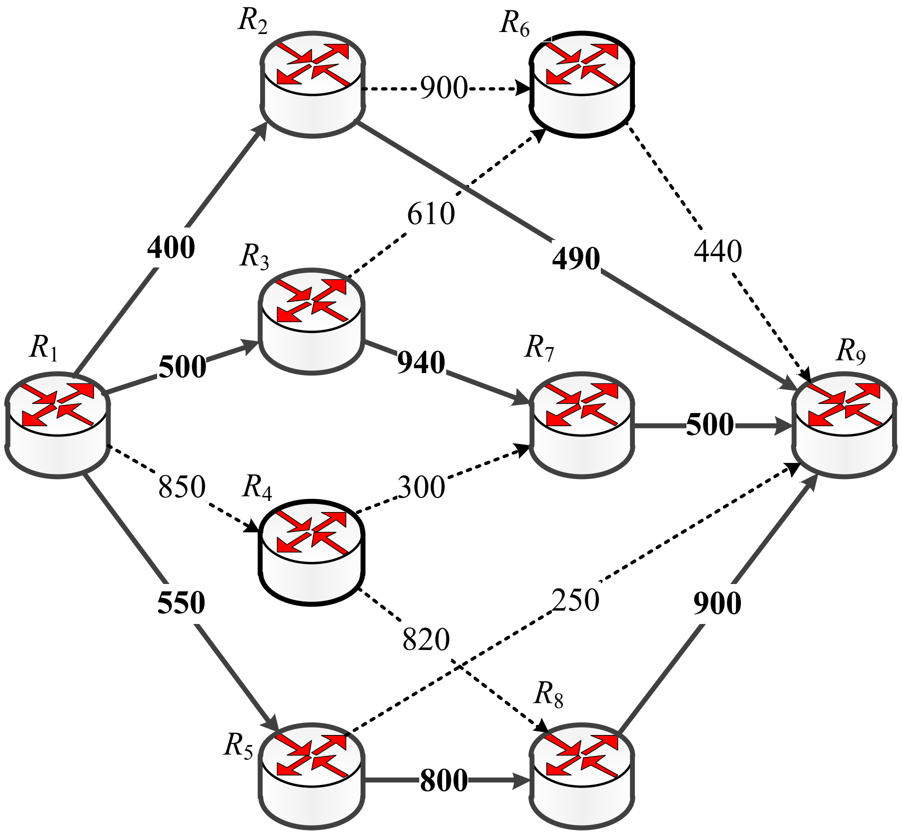


Fig. 4.2. The set of disjoint paths for fast rerouting with implementation of the 2:1 redundancy scheme using the criterion (4.3)

The implementation of the calculation model (2.1)–(2.4), (2.7), (2.9), (4.1), (4.2), but with the optimality criterion (4.4), also determined for implementation redundancy scheme 2:1 the three disjoint paths: L_2, L_4, and L_6 (Fig. 4.3). As in the previous case, each of these paths had the bandwidth (Table 2.3) not less than the calculated threshold (β^k_{path} = 400 1/c).

In this case, it is advisable to choose the route L_6 as the primary one, L_4 – as the first backup, and L_2 – as the second backup route. It is worth noting that using the optimality criterion of routing solutions (4.4) allowed to choose the much more productive route L_6 with the bandwidth of 820 pps instead of L_8 (550 pps), although these two paths contain the same number of links (three each).

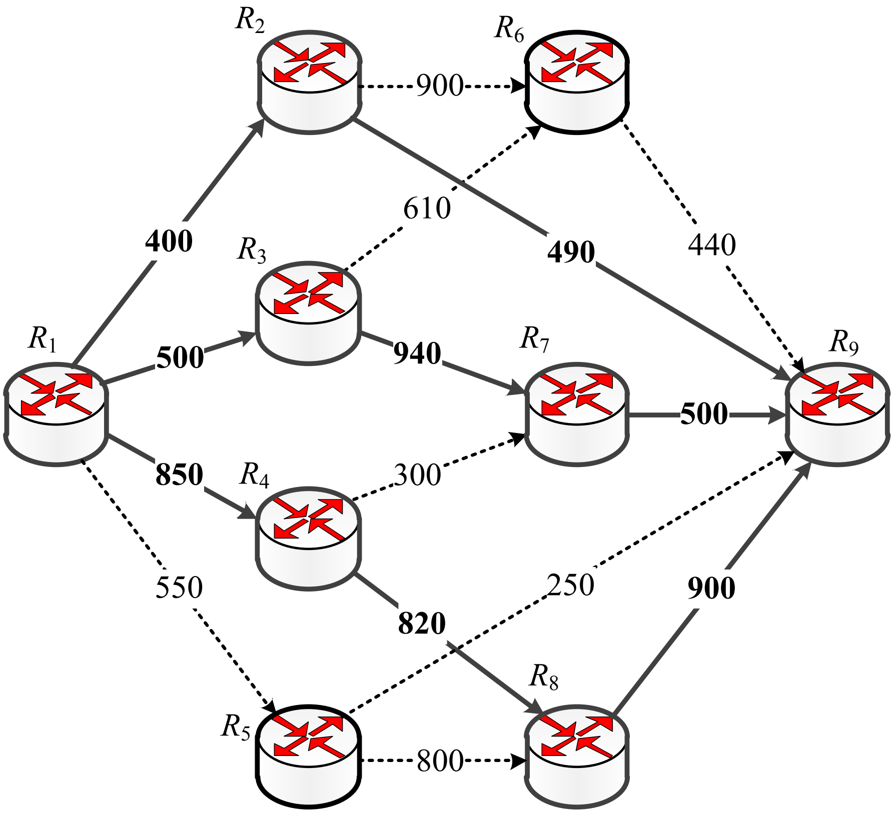


Fig. 4.3. The set of disjoint paths for fast rerouting with implementation of the 2:1 redundancy scheme using the criterion (4.4)

Table 4.1 shows the results of disjoint routes in the case of using model (2.1)-(2.4), (2.7), (2.9), (4.1), (4.2), and optimality criteria (4.3) and (4.4) to realize a 2:1 path protection scheme. At the same time, the average end-to-end packet delay is given for each of the routes if a packet flow with an intensity of 390 pps flows to them.

As shown in Table 4.1, the improved routing model (2.1)-(2.4), (2.7), (2.9), (4.1), (4.2) allows for the computation of primary and multiple backup paths with the implementation of a 2:1 path protection scheme. In this case, each of the paths has a bandwidth not less than the specified one (390 pps). It should be noted that the use of the optimality criterion (4.4) allows to improve another key QoS indicator – the average end-to-end packet delay.

Table 4.1

Calculation Results of Primary and Backup Routes in the Process of Implementation the 2:1 Path Protection Scheme

Path	Path type	Links that form the path	Path bandwidth, pps	Average packet delay along the path, ms
using the optimality criterion (4.3)				
L_8	primary	$\{E_{1,5}, E_{5,8}, E_{8,9}\}$	550	10.6
L_4	first backup	$\{E_{1,3}, E_{3,7}, E_{7,9}\}$	500	20
L_2	second backup	$\{E_{1,2}, E_{2,9}\}$	400	110
using the optimality criterion (4.4)				
L_6	primary	$\{E_{1,4}, E_{4,8}, E_{8,9}\}$	820	6.5
L_4	first backup	$\{E_{1,3}, E_{3,7}, E_{7,9}\}$	500	20
L_2	second backup	$\{E_{1,2}, E_{2,9}\}$	400	110

This indicator within the framework of this study was calculated as the sum of average packet delays on the interfaces of routers and communication links that created this or that route. At the same time, the operation of each interface for this example was modeled by the M/M/1 queuing system, which did not affect the generality of the obtained calculation results. Thus, for the primary route (Table 4.1) it was possible to reduce the average end-to-end packet delay from 10.6 ms to 6.5 ms, i.e., by almost 40%.

4.2.2. Research Results and Comparative Analysis of the Obtained Routing Solutions when Implementing the 3:1 Redundancy Scheme

In the second case, it was necessary to implement a 3:1 path protection scheme with bandwidth requirements at $\beta = 240$ pps, i.e., when transmitting single flow packets from the first router to the ninth router. Here the application of the model (2.1)–(2.4), (2.7), (2.9), (4.1), (4.2) with the optimality criterion (4.3) determined four disjoint paths: L_2, L_3, L_5, and L_7 (Fig. 4.4).

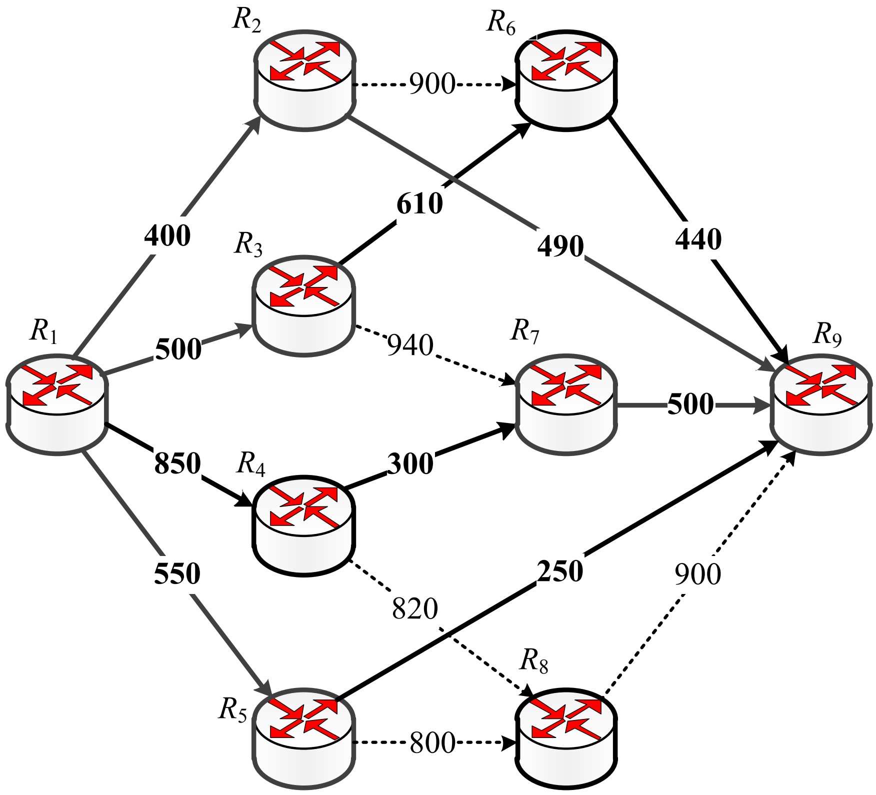


Fig. 4.4. The set of disjoint paths for fast rerouting with implementation of the 3:1 redundancy scheme using the criterion (4.3)

Each path had the bandwidth (Table 2.3) not less than the calculated threshold (β^k_{path} = 250 pps), i.e., conditions were fulfilled (2.7) and (4.1), and fast rerouting was implemented with protection of the network bandwidth. Based on the bandwidth values of these routes, it is advisable to choose the route L_3 as the primary one, L_2 – as the first backup, L_5 – as the second backup, and L_7 – as the third backup route.

The use of the optimality criterion (4.4) determined four disjoint routes for the implementation of the 3:1 redundancy scheme: L_2, L_4, L_6, and L_7 (Fig. 4.5). As in the previous case, each of these paths had the bandwidth (Table 2.3) not less than the calculated threshold (β^k_{path} = 250 pps). Thus, it is reasonable to choose the route L_6 as the primary, and L_4 – first, L_2 – second, and L_7 – third backup paths.

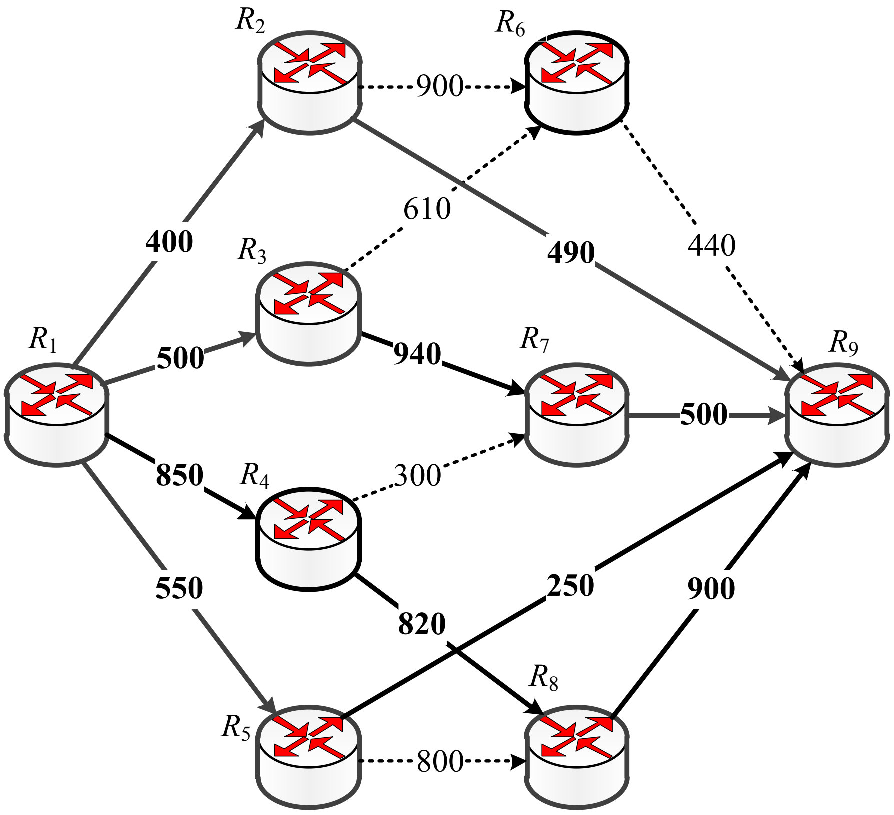


Fig. 4.5. The set of disjoint paths for fast rerouting with implementation of the 3:1 redundancy scheme using the criterion (4.4)

It should be noted that for the realization of the 3:1 redundancy scheme use of the optimality criterion of routing solutions (4.4) allowed to choose not only the primary, but also the first and the second backup routes having higher bandwidth

(Table 2.3) than in the case of using the criterion (4.3). This advantage was also reflected in the corresponding values of the average end-to-end delays of packets transmitted by both the primary and most of the backup routes (Table 4.2). Thus, the average packet delay was reduced by almost 57.4% for the primary path, by 11.7% for the first backup path, and by 53.6% for the second backup paths.

Table 4.2

Calculation Results of Primary and Backup Routes in the Process of Implementation of the 3:1 Path Protection Scheme

Path	Path type	Links that form the path	Path bandwidth, pps	Average packet delay along the path, ms
using the optimality criterion (4.3)				
L_3	primary	$\{E_{1,3},E_{3,6},E_{6,9}\}$	440	11.5
L_2	first backup	$\{E_{1,2},E_{2,9}\}$	400	10.3
L_5	second backup	$\{E_{1,4},E_{4,7},E_{7,9}\}$	300	22.2
L_7	third backup	$\{E_{1,5},E_{5,9}\}$	250	103.2
using the optimality criterion (4.4)				
L_6	primary	$\{E_{1,4},E_{4,8},E_{8,9}\}$	820	4.9
L_4	first backup	$\{E_{1,3},E_{3,7},E_{7,9}\}$	500	9.1
L_2	second backup	$\{E_{1,2},E_{2,9}\}$	400	10.3
L_7	third backup	$\{E_{1,5},E_{5,9}\}$	250	103.2

4.3. Extending the Capabilities of the Proposed Model to Implement Fast ReRouting on Multipath Protection and Network Capacity

The mathematical model proposed in section 4.1 (2.1)-(2.4), (2.7), (2.9), (4.1), (4.2), (4.4) includes a single path variant of fast rerouting organization with the implementation of a path and network capacity protection scheme. This is manifested in the fact (Tables 4.1 and 4.2) that only one route, either the primary or the backup route, is used when transmitting packets of the selected flow. In this case, the fulfillment of conditions (2.7) and (4.1) guarantees that the bandwidth of each of these routes is sufficient separately to serve this flow without causing congestion. This section will demonstrate how the FRR model (2.1)-(2.4), (2.7), (2.9), (4.1), (4.2), (4.4) can be modified to support multipath routing without losing the linear nature of the model and the fault tolerance functionality of TCN. Note that in multipath fast routing, the primary and/or backup solution can be represented by some set of disjoint paths (multipath).

The primary multipath will be understood as a set of routes used to transmit packets of the selected *k*th flow in the absence of failures in the TCN. Then the backup multipath is a set of routes used to transmit packets of the selected *k*th flow in case of detecting failures of elements (routers and/or communication links) of the primary multipath in TCN. Let us introduce a notation for the route protection scheme at the multipath level:

$$n_l : 1_m , \tag{4.5}$$

where *m* and *l* – are parameters indicating the total number of routes included in the primary and backup paths.

Such a notation of the scheme (4.5) limits the cases of organizing redundancy by means of redundant multipaths containing the same quantity (*l*) of regular routes. In general, when implementing fast rerouting in TCN $m, l \geq 1$. For example, in sections 4.1 and 4.2 we considered the cases of fast rerouting in TCN according to the scheme $n_1 : 1_1$, i.e. when $l = m = 1$. In other words, the extreme case when both the primary multipath contained one route and each of the *n* backup multipaths also included one route was realized. In the case of considering the multipath case, the data presented in Fig. 4.1 b), can be interpreted in one of the given ways:

- the scheme is realized $1_2 : 1_1$: the primary multipath contains one route $R_1 \to R_2 \to R_5 \to R_7$, and the backup multipath consists of two routes $R_1 \to R_4 \to R_6 \to R_7$ and $R_1 \to R_3 \to R_7$;
- the scheme is realized $1_1 : 1_2$: the primary multipath contains of two routes, for example $R_1 \to R_2 \to R_5 \to R_7$ and $R_1 \to R_3 \to R_7$, and the backup multipath contains one route $R_1 \to R_4 \to R_6 \to R_7$.

Separately, it should be noted that a necessary condition for the implementation of multi path routing in TCN is the physical presence in the network of the necessary set of disjoint paths. In general, to implement the redundancy scheme (4.5) in the organization of fault-tolerant routing with route protection (multipath), it is necessary that the network physically has a minimum $m + nl$ of disjoint paths. For example, for the network structure investigated in the previous section 4.2 (Figs. 4.2-4.5), the maximum number of disjoint paths was four, which within the equation (4.5) would allow providing redundancy, for example, at the level of such schemes: $2_1 : 1_1$, $3_1 : 1_1$, $1_2 : 1_1$ and $1_2 : 1_2$.

A significant imprint on the possibilities of organizing reservation schemes in TCN is imposed by the requirements to protect the network bandwidth. That is, according to (4.5) *m* routes included in the primary multipath must have a total bandwidth not less than β^k. The same requirement applies to the backup multipaths: *l* routes contained in each of the backup multipaths must also have a total bandwidth not less than β^k.

Thus, in order to realize the redundancy scheme

$$n_m : 1_m, \tag{4.6}$$

based on the above notations, proposed to slightly modify the network capacity protection conditions for the *k*th packet flow (4.1):

$$\beta_{path}^{k} \geq \frac{\beta^{k}}{m}, \qquad (4.7)$$

which complete requirements (2.7).

As conclusion, it should be noted that due to the modification carried out, the mathematical model (2.1)-(2.4), (2.7), (2.9), (4.2), (4.4), (4.7) will now cover the multipath variant of fast rerouting organization with the implementation of path (multipath) protection scheme and network capacity usually in the presence of a minimum of $m(n+1)$ paths that do not intersect.

For clarity, let us demonstrate the peculiarities of using the model of multipath fast rerouting by multipath and bandwidth protection on the example of the network, the topology and characteristics of which are shown in Fig. 2.5 and Table 2.3. Then the routing solution presented in Fig. 4.5 the routing solution can correspond to the problem of multipath fast rerouting with the implementation, firstly, of the multipath protection scheme $1_2:1_2$, and secondly, of the bandwidth protection scheme at the 480 pps level, i.e., $\beta = 480$ pps.

In this case, applying the model (2.1)-(2.4), (2.7), (2.9), (4.2), (4.4), (4.7) again to realize the multipath protection scheme $1_2:1_2$ defined four disjoint routes: L_2, L_4, L_6, and L_7 (Fig. 4.5). According to the conditions and constraints (4.7) of the problem, each of these routes had a bandwidth (Table 2.3) not less than the specified threshold of $\frac{\beta}{2} = 240$ pps, since for the given solution β_{path}^{k}=250 pps. Therefore, in pairs these routes can define the primary and backup multipaths in any combination so that their total bandwidth is not less than $\beta = 480$ pps.

As shown in Table 4.3, the primary multipath can include, for example, the two most productive routes L_6 and L_4, and the backup path – remaining routes L_2 and L_7. Such a choice of routes does not provide a balanced distribution of network bandwidth between the primary and backup multipaths. The main multipath in this case will have a bandwidth of 1320 pps, and the backup multipath – 650 pps, i.e., practically twice less. Such a variant is reasonable to use in cases when the probability of failures of network elements is very low, so the transition to the backup (low-performance solution) is unlikely.

Table 4.3

Calculation Results of Primary and Backup Routes in the Process of Implementation the $1_2:1_2$ Multipath Protection Scheme

Multipath type	Path	Links that form the path	Path bandwidth, pps	Multipath bandwidth, pps
Unbalanced distribution of network bandwidth between multipaths				
Primary	L_6	$\{E_{1,4}, E_{4,8}, E_{8,9}\}$	820	1320
	L_4	$\{E_{1,3}, E_{3,7}, E_{7,9}\}$	500	
Backup	L_2	$\{E_{1,2}, E_{2,9}\}$	400	650
	L_7	$\{E_{1,5}, E_{5,9}\}$	250	
Balanced distribution of network bandwidth between multipaths				
Primary	L_6	$\{E_{1,4}, E_{4,8}, E_{8,9}\}$	820	1070
	L_7	$\{E_{1,5}, E_{5,9}\}$	250	
Backup	L_4	$\{E_{1,3}, E_{3,7}, E_{7,9}\}$	500	900
	L_2	$\{E_{1,2}, E_{2,9}\}$	400	

If the primary multipath includes, for example, two routes L_6 and L_7, and the backup routes L_2 and L_4 (Table 4.3), then a balanced distribution of network bandwidth between the primary and backup multipaths will be ensured. The primary multipath in this case will have a bandwidth of 1070 pps, and the backup multipath will have a bandwidth of 900 pps.

Based on the obtained results of calculations, we can make an intermediate conclusion that in the presence of the required number of routes in the TCN, the use of the improved model of multipath fast rerouting (2.1)-(2.4), (2.7), (2.9), (4.2), (4.4), (4.7) allows, while ensuring the specified level of fault tolerance, to significantly increase the reserved bandwidth of the network. If for the single path case of the primary and backup paths (Table 4.2) it was possible to protect the bandwidth at the level of 240 pps, then with the use of multipath routing this threshold was increased at least twice.

The examples are given in Table 4.3 shows a variant of the model (2.1)-(2.4), (2.7), (2.9), (4.2), (4.4), (4.7), when in case of failure of any element (router and/or link) of the primary multipath, all traffic will be immediately switched to use the backup multipath routes. This approach is the only available solution in case of multiple failures covering elements of all routes of the primary multipath at once.

In case of failure of network elements of one of the routes of the primary multipath, it is not reasonable to refuse to use the remaining operating routes. Especially when their bandwidth is sufficiently high compared to other backup routes. The advantage of the model (2.1)-(2.4), (2.7), (2.9), (4.2), (4.4), (4.7) is that when implementing multipath fast rerouting, all calculated routes are interchangeable to some extent. Not a complete replacement of the primary multipath, but only partial – at the level of replacement (protection) of individual routes, will still provide protection of network capacity with the fulfillment of conditions (2.7) and (4.7).

For example, if when using the primary multipath containing routes L_6 and L_4, he link between the third and seventh routers ($E_{3,7}$), fails, it will lead to the incapacity of only one route – route L_4. In such a case, the backup solution can be the multipath L_6 and L_2, which has a total bandwidth of 1220 pps, which is minimally inferior to the bandwidth of the primary multipath (1320 pps) and significantly exceeds the bandwidth of another backup solution represented by routes L_2 and L_7 (650 pps).

Thus, in the case of multipath protection in TCN at the level of individual routes, it is reasonable to organize the fast rerouting process as follows.

1. Perform a preliminary ranking of the calculated disjoint routes according to their bandwidth capacity.

2. Disjoint routes that have the maximum capacity among all other calculated routes should be attracted to the primary multipath.

3. In case of failure of one of the routes, the next route with the same capacity must be involved in its place.

Then, with the failure of each subsequent route in the TCN, the bandwidth of the multipath that will be used will not decrease rapidly, but as little as possible.

4.4. Conclusion to the Fourth Chapter

1. The model of fast rerouting with the implementation of n:1 path protection scheme and network capacity is improved. This mathematical model is represented by expressions (2.1)-(2.4), (2.7), (2.9), (4.1), (4.2). To obtain optimal routing solutions, two types of optimality criteria related to the maximization of objective functions (4.3) or (4.4), which are linear functions of the capacity lower bound of the primary and a set of backup routes, are proposed for use.

2. The application of the proposed mathematical model allowed to reduce the solution of the technological problem of fast rerouting to the solution of the optimization problem of mixed integer linear programming with modified optimality criteria (4.3) or (4.4) in the presence of linear constraints (2.1)-(2.4), (2.7), and (4.1), since the routing variables are Boolean, and the lower bound of the capacity of the

primary and a set of backup routes is a real number. The advantages of the proposed model are that implementing the *n:*1 path protection scheme does not lead to a proportional increase in the dimensionality of the optimization problem compared to the solutions described in [16].

3. Linearity of the proposed model (2.1)-(2.4), (2.7), (2.9), (4.1)-(4.4) and decrease of the number of routing variables to be calculated (2.1) contributed to the reduction of complexity of its computational implementation in case of practical use as part of the software of routers or SDN-controllers, which are assigned the functions of organizing fast rerouting in the network. The prospect of further research in this area primarily concerns the support of multipath routing strategies, as well as the implementation of schemes to protect not only such an important Quality of Service indicator, such as bandwidth, but also other QoS-indicators – average delay, jitter, packet loss probability, as well as the values of Quality of Experience and network security, which is especially relevant for the transmission of multimedia traffic and confidential data.

4. The chapter provides a comparative analysis of routing solutions obtained using optimality criteria (4.3) and (4.4) within models (2.1)-(2.4), (2.7), (2.9), (4.1), (4.2). The modification of the optimality criterion (4.4) is aimed at ensuring that the set of calculated paths (primary and backup) encompasses routes that not only met the bandwidth requirements (2.7), but also contained the most productive links, thus positively affecting the Quality of Service level, e.g., in terms of the average end-to-end packet delay (Table 4.1 and Table 4.2). Since all the calculated paths had a bandwidth not worse than the specified threshold (4.1), the path that provided the highest bandwidth or the lowest value of the average end-to-end packet delay was selected as the primary one. The other routes were used as backup routes according to the *n:*1 protection scheme in the order of decreasing bandwidth or increasing average end-to-end delay of packets transmitted over these paths.

5. The chapter proposes further improvement of the fast rerouting model over disjoint paths to support multipath solutions both at the level of primary and backup paths. The model (2.1)-(2.4), (2.7), (2.9), (4.1), (4.2), (4.4) enables the

implementation of the reservation scheme $n_m : 1_m$ (4.6). In the process of research, it is established that in the presence of the required number of routes in TCN the application of the improved model of multipath fast rerouting (2.1)-(2.4), (2.7), (2.9), (4.2), (4.4), (4.7) allows to increase significantly the bandwidth of the network under reservation while providing the specified level of fault tolerance.

CHAPTER 5

RECOMMENDATIONS FOR PRACTICAL USE OF THE PROPOSED ROUTING SOLUTIONS IN TELECOMMUNICATION NETWORKS

Traditionally, mathematical routing models can be used as a basis for algorithmic software of network equipment – routers of traditional IP networks and controllers of Software-Defined networks. As a rule, it concerns the implementation of the latest routing protocols, which are part of the specialized software of the specified network devices. An example of such solutions can be graph-based routing models when the task of determining the optimal route is reduced to solving the mathematical problem of finding the shortest path in a weighted graph. Therefore, most distance-vector routing protocols, such as RIP (Routing Information Protocol) and IGRP (Interior Gateway Routing Protocol), are based on the Bellman-Ford algorithm for finding the shortest path. In turn, most link-state routing protocols, such as OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System), and PNNI (Private Network-to-Network Interface) use Dijkstra's algorithm to find the shortest path [7, 8].

5.1. Creating a Network Topology in the CML Simulator

Cisco Modeling Labs (CML), which supports the functionality of relatively modern server and network equipment, was used as a tool for an example of practical implementation of the mathematical solutions proposed in the work. Configuring and simulating most network processes, including IP routing protocols and programming using Python, is convenient. An example of a TCN topology configured in the CML environment is shown in Fig. 5.1, corresponding to the research variant of the network structure shown in Fig. 2.2. Simplified for clarity, the IP-addressing scheme covered twelve subnets with the prefix /24.

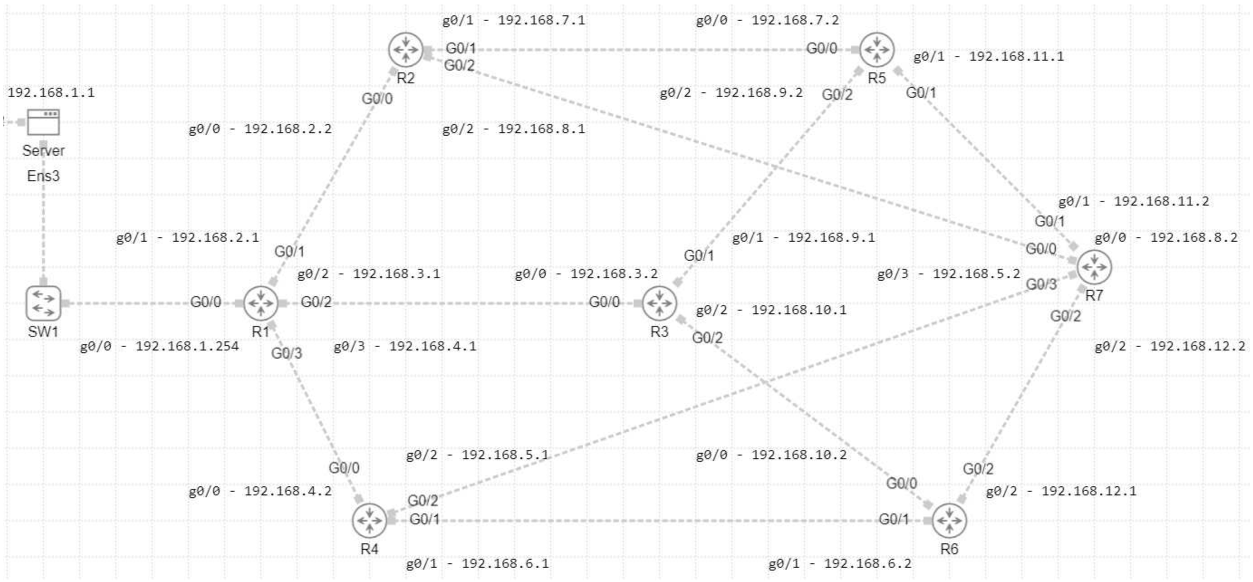


Fig. 5.1. Example of configuring network topology and IP-addressing of interfaces and server devices in CML environment

The routing server, labeled as "Server" in Fig. 5.1, was responsible for organizing network management, i.e., remote software configuration of network equipment when configuring IP-addressing and disjoint routes by the models of fault-tolerant and secure routing proposed in the work.

Routers R1÷R7 (Fig. 5.1) implemented the principles of IP packet routing based on OSPF protocol support. This protocol, as it is known, organizes load balancing on paths having the same metric [7, 8]. To implement the results of calculations on this or that routing model, represented by a set of disjoint paths, an approach based on remote software configuration (setting) of link metrics using the command "`ip ospf cost`" was used. The link metrics included in the set of optimal disjoint paths were calculated so that their sum along each path was equal and minimal compared to other paths.

So, for example (Fig. 5.1), to customize using a set of three pre-calculated disjoint paths (Table 2.2),

$$R1\rightarrow R4\rightarrow R6\rightarrow R7,\quad R1\rightarrow R3\rightarrow R5\rightarrow R7 \quad \text{and} \quad R1\rightarrow R2\rightarrow R7 \qquad (5.1)$$

first, on all routers' interfaces that connected them to other routers, the maximum metric for the OSPF protocol was set to 65535. On other router interfaces, the link metrics were set according to the contents of Table 5.1. Then, each disjoint path (5.1) will have a minimum metric of 30, which guarantees the inclusion of these three routes in the routing tables of TCN routers when transmitting packets from R1 to R7.

Table 5.1

Example of Defining OSPF Network Link Metrics to Implement Secure QoS Routing

Router	Type and number of source interface			
	G0/0	G0/1	G0/2	G0/3
R1	H	10	10	20
R2	H	H	10	H
R3	H	10	H	H
R4	H	10	H	H
R5	H	10	H	H
R6	H	H	10	H
R7	H	H	H	H
H – undefined (any value)				

Suppose it was necessary to implement fast rerouting with path protection in the network, for example, according to the 2:1 scheme (Table 5.2). In that case, the metrics of routes and interfaces should be configured in a different order (Table 5.3). For example, the primary route naturally had the lowest metric, which was 20. The first backup route had a metric of 30, and the second one had a metric of 60.

Table 5.2

Types and Metrics of Disjoint Routes when Implementing Fast ReRouting in the Network

Route type	Route	Route metric
Primary	R1→R2→R7	20
First backup	R1→R3→R5→R7	30
Second backup	R1→R4→R6→R7	60

Table 5.3

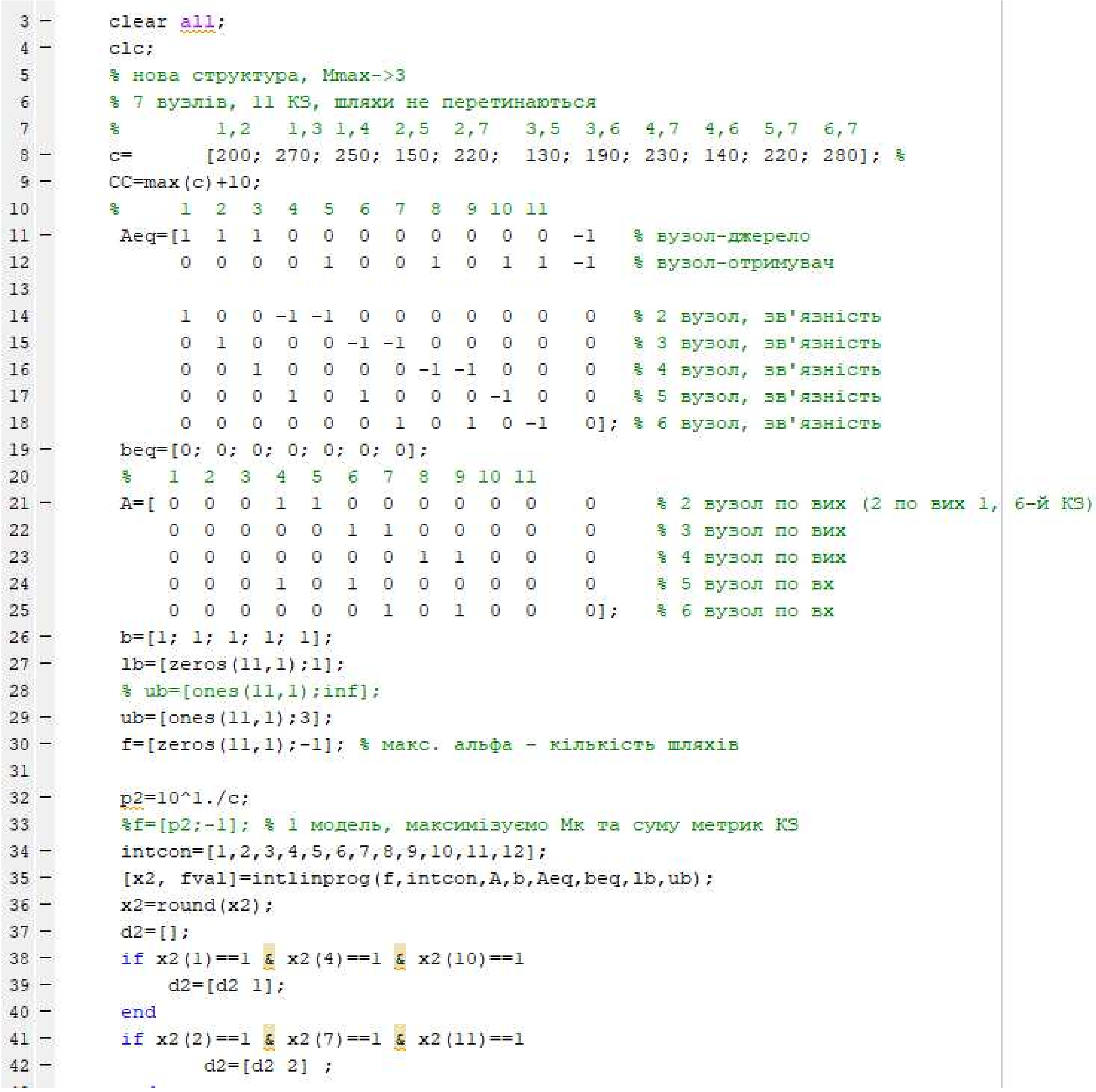
Example of Defining OSPF Network Link Metrics to Implement Fast ReRouting

Router	Type and number of the source interface			
	G0/0	G0/1	G0/2	G0/3
R1	H	10	10	10
R2	H	H	20	H
R3	H	10	H	H
R4	H	20	H	H
R5	H	10	H	H
R6	H	H	20	H
R7	H	H	H	H
H – undefined (any value)				

5.2. Software Implementation of the Proposed Routing Models on the Network Server

Throughout the research, all optimization models presented in chapters 2-4 were implemented in MATLAB. To solve the formulated optimization problems, the Optimization Toolbox capabilities [112, 113], represented by the functions `linprog`, `intlinprog`, `fmincon` and their combinations, were used.

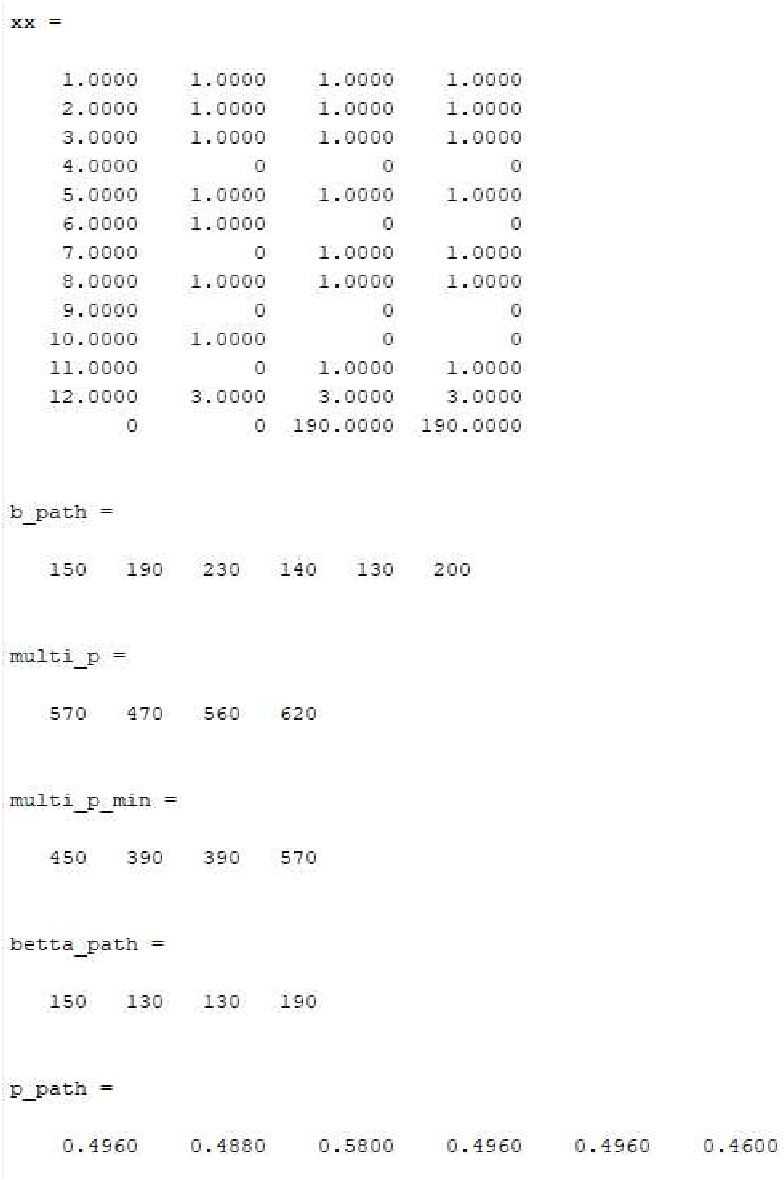
For example, Fig. 5.2 shows a code fragment in the MATLAB environment, which was used to calculate secure disjoint paths and had the maximum bandwidth.



```
clear all;
clc;
% нова структура, Mmax->3
% 7 вузлів, 11 КЗ, шляхи не перетинаються
%         1,2   1,3 1,4  2,5  2,7   3,5  3,6  4,7  4,6  5,7  6,7
c=       [200; 270; 250; 150; 220;  130; 190; 230; 140; 220; 280]; %
CC=max(c)+10;
%      1  2  3  4  5  6  7  8  9 10 11
 Aeq=[1  1  1  0  0  0  0  0  0  0  0  -1   % вузол-джерело
      0  0  0  0  1  0  0  1  0  1  1  -1   % вузол-отримувач

      1  0  0 -1 -1  0  0  0  0  0  0   0   % 2 вузол, зв'язність
      0  1  0  0  0 -1 -1  0  0  0  0   0   % 3 вузол, зв'язність
      0  0  1  0  0  0  0 -1 -1  0  0   0   % 4 вузол, зв'язність
      0  0  0  1  0  1  0  0  0 -1  0   0   % 5 вузол, зв'язність
      0  0  0  0  0  0  1  0  1  0 -1   0]; % 6 вузол, зв'язність
 beq=[0; 0; 0; 0; 0; 0; 0];
 %   1  2  3  4  5  6  7  8  9 10 11
 A=[ 0  0  0  1  1  0  0  0  0  0  0    0     % 2 вузол по вих (2 по вих 1, 6-й КЗ)
     0  0  0  0  0  1  1  0  0  0  0    0     % 3 вузол по вих
     0  0  0  0  0  0  0  1  1  0  0    0     % 4 вузол по вих
     0  0  0  1  0  1  0  0  0  0  0    0     % 5 вузол по вх
     0  0  0  0  0  0  1  0  1  0  0    0];   % 6 вузол по вх
 b=[1; 1; 1; 1; 1];
 lb=[zeros(11,1);1];
 % ub=[ones(11,1);inf];
 ub=[ones(11,1);3];
 f=[zeros(11,1);-1]; % макс. альфа - кількість шляхів

 p2=10^1./c;
 %f=[p2;-1]; % 1 модель, максимізуємо Мк та суму метрик КЗ
 intcon=[1,2,3,4,5,6,7,8,9,10,11,12];
 [x2, fval]=intlinprog(f,intcon,A,b,Aeq,beq,lb,ub);
 x2=round(x2);
 d2=[];
 if x2(1)==1 & x2(4)==1 & x2(10)==1
     d2=[d2 1];
 end
 if x2(2)==1 & x2(7)==1 & x2(11)==1
        d2=[d2 2] ;
```

Fig. 5.2. Code fragment in MATLAB environment to calculate secure disjoint paths

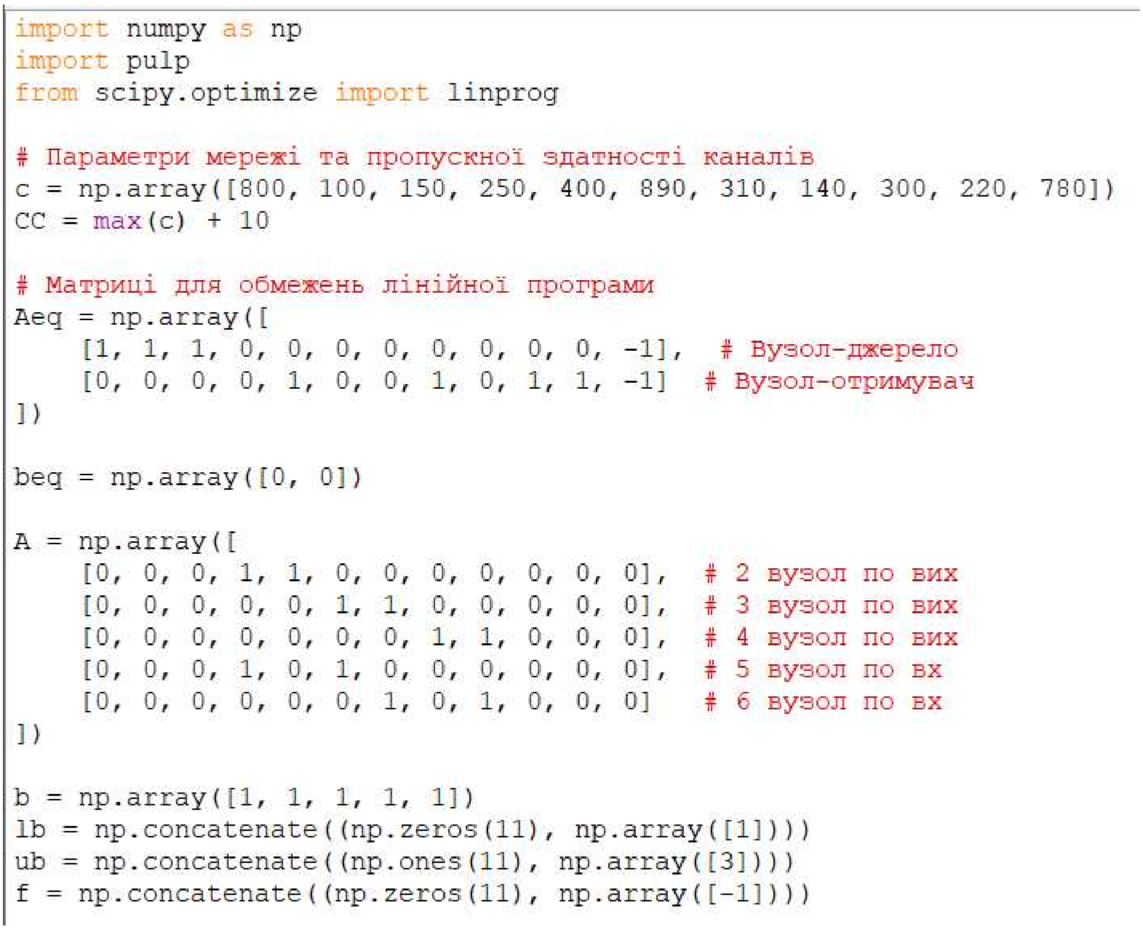
Fig. 5.3 shows the results of the calculations of determining the optimal disjoint paths regarding network security (compromise probability) and bandwidth.



```
xx =

    1.0000    1.0000    1.0000    1.0000
    2.0000    1.0000    1.0000    1.0000
    3.0000    1.0000    1.0000    1.0000
    4.0000         0         0         0
    5.0000    1.0000    1.0000    1.0000
    6.0000    1.0000         0         0
    7.0000         0    1.0000    1.0000
    8.0000    1.0000    1.0000    1.0000
    9.0000         0         0         0
   10.0000    1.0000         0         0
   11.0000         0    1.0000    1.0000
   12.0000    3.0000    3.0000    3.0000
         0         0  190.0000  190.0000


b_path =

   150   190   230   140   130   200


multi_p =

   570   470   560   620


multi_p_min =

   450   390   390   570


betta_path =

   150   130   130   190


p_path =

    0.4960    0.4880    0.5800    0.4960    0.4960    0.4600
```

Fig. 5.3. Results of calculations of determining optimal disjoint paths in terms of network security (compromise probability)

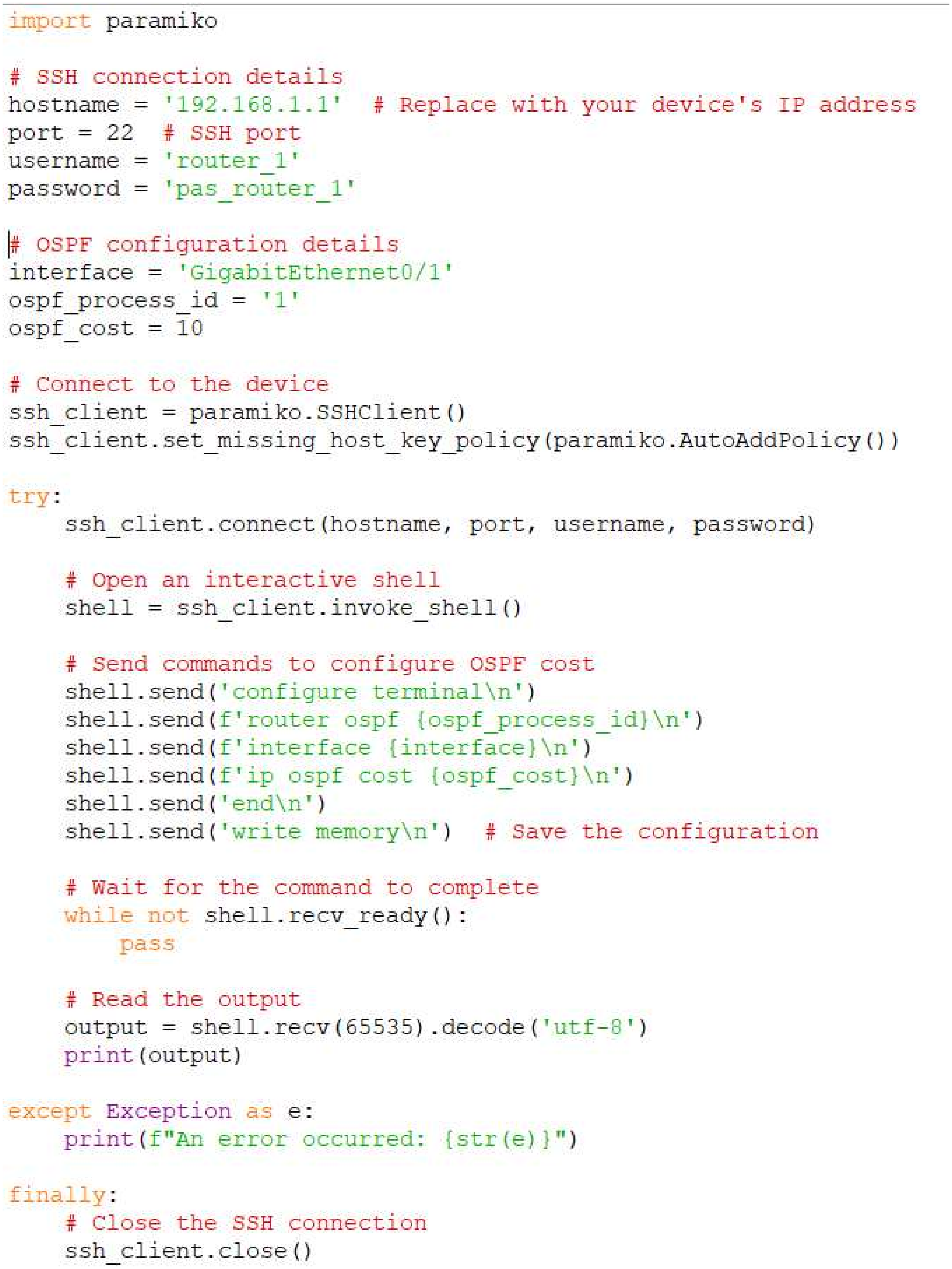
Further, the code of programs executed in the MATLAB environment was adapted to the Python environment (Fig. 5.4) [114, 115].



```
import numpy as np
import pulp
from scipy.optimize import linprog

# Параметри мережі та пропускної здатності каналів
c = np.array([800, 100, 150, 250, 400, 890, 310, 140, 300, 220, 780])
CC = max(c) + 10

# Матриці для обмежень лінійної програми
Aeq = np.array([
    [1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, -1],  # Вузол-джерело
    [0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, -1]  # Вузол-отримувач
])

beq = np.array([0, 0])

A = np.array([
    [0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0],  # 2 вузол по вих
    [0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0],  # 3 вузол по вих
    [0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0],  # 4 вузол по вих
    [0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0],  # 5 вузол по вх
    [0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0]   # 6 вузол по вх
])

b = np.array([1, 1, 1, 1, 1])
lb = np.concatenate((np.zeros(11), np.array([1])))
ub = np.concatenate((np.ones(11), np.array([3])))
f = np.concatenate((np.zeros(11), np.array([-1])))
```

Fig. 5.4. Example of a code fragment in Python environment for solving the problem of Secure QoS routing

A set of software implementations in the Python environment of the optimization models of fault-tolerant and secure routing proposed in this work was performed on the "Server" (Fig. 5.1). This server was as a network controller for determining disjoint paths. Subsequently, on the Server, the results of the computations represented by multipaths such as (5.1) were implemented in the network by remotely programmatically configuring the routing OSPF metrics (Fig. 5.5) shown in Table 5.1. For this purpose, the Python Paramiko library was used to create SSH (Secure Shell) connections for remote software configuration of network equipment. It allowed to automate interaction with remote devices via SSH protocol, including sending commands to configure the OSPF protocol. Through this protocol, the network further built and entered into the routing tables the routes defined by the models proposed in the work.



```python
import paramiko

# SSH connection details
hostname = '192.168.1.1'  # Replace with your device's IP address
port = 22  # SSH port
username = 'router_1'
password = 'pas_router_1'

# OSPF configuration details
interface = 'GigabitEthernet0/1'
ospf_process_id = '1'
ospf_cost = 10

# Connect to the device
ssh_client = paramiko.SSHClient()
ssh_client.set_missing_host_key_policy(paramiko.AutoAddPolicy())

try:
    ssh_client.connect(hostname, port, username, password)

    # Open an interactive shell
    shell = ssh_client.invoke_shell()

    # Send commands to configure OSPF cost
    shell.send('configure terminal\n')
    shell.send(f'router ospf {ospf_process_id}\n')
    shell.send(f'interface {interface}\n')
    shell.send(f'ip ospf cost {ospf_cost}\n')
    shell.send('end\n')
    shell.send('write memory\n')  # Save the configuration

    # Wait for the command to complete
    while not shell.recv_ready():
        pass

    # Read the output
    output = shell.recv(65535).decode('utf-8')
    print(output)

except Exception as e:
    print(f"An error occurred: {str(e)}")

finally:
    # Close the SSH connection
    ssh_client.close()
```

Fig. 5.5. A Python code sample used to remotely programmatically configure OSPF routing metrics on network router interfaces

5.3. Description of Software Implementation of the Methodology for Analyzing the Level of Network Security of Communication Equipment

To ensure an effective solution of secure routing problems using the models proposed in the third chapter, it is necessary to have effective means of vulnerability detection, monitoring, and analysis of network security indicators of TCN elements. To this end, the work uses a software implementation of the methodology for analyzing the level of network security of TCN communication equipment, created at the V.V. Popovskyy Department of Infocommunication Engineering of the Kharkiv National University of Radio Electronics.

The developed program is an innovative tool for analyzing and assessing the security risks of telecommunication systems and networks. It uses data from NVD-NIST (National Vulnerability Database) from the U.S. National Institute of Standards and Technology to perform a detailed analysis of vulnerabilities, the cost of their realization, and the calculation of information security risk for various components of TCN. The program is implemented in the Python 3 environment and includes some critical functionalities:

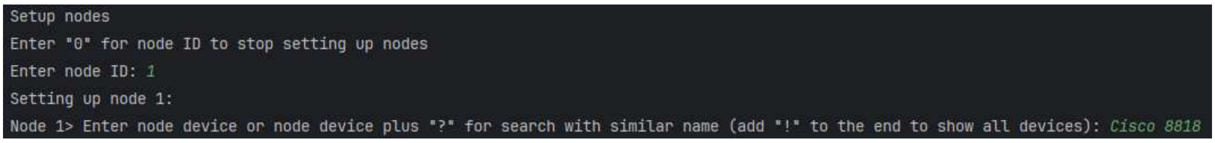
1. Information collection. The program collects automated data on hardware and software vulnerabilities (including operating systems) of network devices from the NVD-NIST database. Data collection takes place in real-time, allowing you to quickly respond to new vulnerabilities or change the current data on existing vulnerabilities.

2. Information Analysis. The collected information is analyzed in detail to determine the severity and potential consequences of vulnerabilities for further calculation of information security risk.

3. Determination of information security characteristics. The program calculates the main characteristics of information security of network parts, including information security risks and probability of vulnerability exploitation in hardware and software of network equipment.

4. Visualization of results. The results of the analysis and calculation of information security indicators can be presented in the form of tables for a better understanding of the program user.

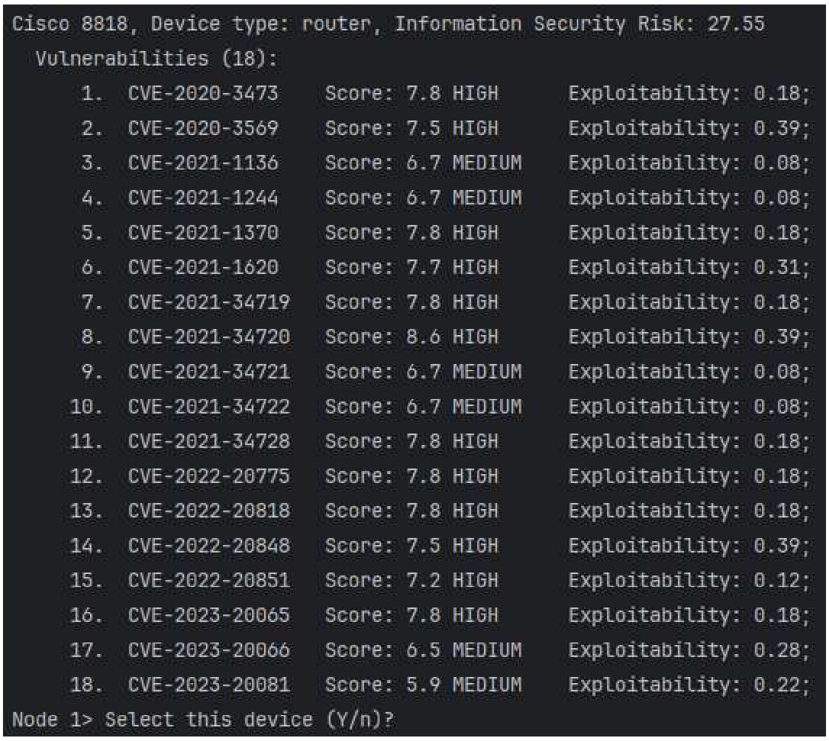
The program's operation can be represented by a sequence of stages of its functioning. In the first stage, select the number of the device in the network and its name. An example of setting the Cisco 8818 router as device number 1 can be seen in Fig. 5.6.



```
Setup nodes
Enter "0" for node ID to stop setting up nodes
Enter node ID: 1
Setting up node 1:
Node 1> Enter node device or node device plus "?" for search with similar name (add "!" to the end to show all devices): Cisco 8818
```

Fig. 5.6. Example of setting the Cisco 8818 router as device #1

After selecting this device, the utility will be able to collect and display up-to-date information about all its vulnerabilities, their characteristics (including the probability of realization), and the calculated risk of the information system (Fig. 5.7).

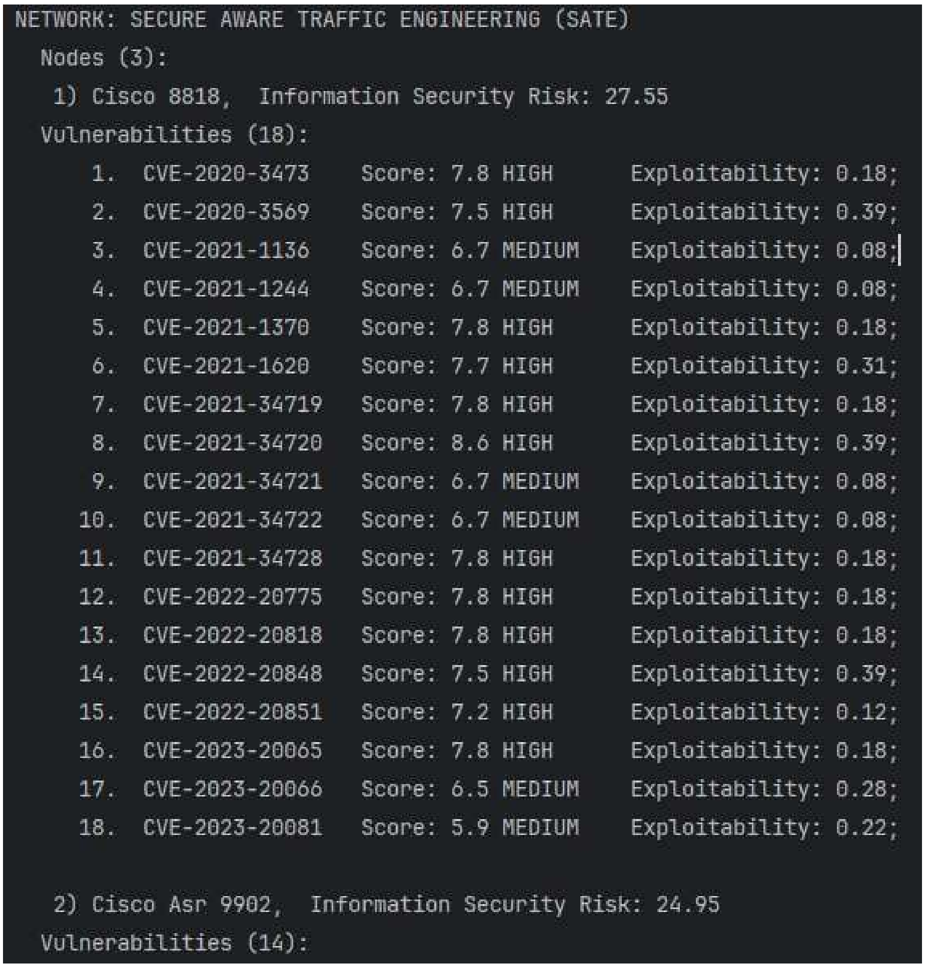


```
Cisco 8818, Device type: router, Information Security Risk: 27.55
  Vulnerabilities (18):
      1.  CVE-2020-3473    Score: 7.8 HIGH      Exploitability: 0.18;
      2.  CVE-2020-3569    Score: 7.5 HIGH      Exploitability: 0.39;
      3.  CVE-2021-1136    Score: 6.7 MEDIUM    Exploitability: 0.08;
      4.  CVE-2021-1244    Score: 6.7 MEDIUM    Exploitability: 0.08;
      5.  CVE-2021-1370    Score: 7.8 HIGH      Exploitability: 0.18;
      6.  CVE-2021-1620    Score: 7.7 HIGH      Exploitability: 0.31;
      7.  CVE-2021-34719   Score: 7.8 HIGH      Exploitability: 0.18;
      8.  CVE-2021-34720   Score: 8.6 HIGH      Exploitability: 0.39;
      9.  CVE-2021-34721   Score: 6.7 MEDIUM    Exploitability: 0.08;
     10.  CVE-2021-34722   Score: 6.7 MEDIUM    Exploitability: 0.08;
     11.  CVE-2021-34728   Score: 7.8 HIGH      Exploitability: 0.18;
     12.  CVE-2022-20775   Score: 7.8 HIGH      Exploitability: 0.18;
     13.  CVE-2022-20818   Score: 7.8 HIGH      Exploitability: 0.18;
     14.  CVE-2022-20848   Score: 7.5 HIGH      Exploitability: 0.39;
     15.  CVE-2022-20851   Score: 7.2 HIGH      Exploitability: 0.12;
     16.  CVE-2023-20065   Score: 7.8 HIGH      Exploitability: 0.18;
     17.  CVE-2023-20066   Score: 6.5 MEDIUM    Exploitability: 0.28;
     18.  CVE-2023-20081   Score: 5.9 MEDIUM    Exploitability: 0.22;
Node 1> Select this device (Y/n)?
```

Fig. 5.7. An example of displaying information about the network security level of a Cisco 8818 router

As shown in Fig. 5.7, the utility displays information about the vulnerability: code, criticality score, and the exploitation probability of this vulnerability (compromise probability). All these data are retrieved from the database when queried, processed, and formatted for informative display.

Once the entire network is installed, the program can integrate information about the network security status of all network devices (Fig. 5.8).



```
NETWORK: SECURE AWARE TRAFFIC ENGINEERING (SATE)
  Nodes (3):
   1) Cisco 8818,  Information Security Risk: 27.55
  Vulnerabilities (18):
      1.  CVE-2020-3473    Score: 7.8 HIGH      Exploitability: 0.18;
      2.  CVE-2020-3569    Score: 7.5 HIGH      Exploitability: 0.39;
      3.  CVE-2021-1136    Score: 6.7 MEDIUM    Exploitability: 0.08;
      4.  CVE-2021-1244    Score: 6.7 MEDIUM    Exploitability: 0.08;
      5.  CVE-2021-1370    Score: 7.8 HIGH      Exploitability: 0.18;
      6.  CVE-2021-1620    Score: 7.7 HIGH      Exploitability: 0.31;
      7.  CVE-2021-34719   Score: 7.8 HIGH      Exploitability: 0.18;
      8.  CVE-2021-34720   Score: 8.6 HIGH      Exploitability: 0.39;
      9.  CVE-2021-34721   Score: 6.7 MEDIUM    Exploitability: 0.08;
     10.  CVE-2021-34722   Score: 6.7 MEDIUM    Exploitability: 0.08;
     11.  CVE-2021-34728   Score: 7.8 HIGH      Exploitability: 0.18;
     12.  CVE-2022-20775   Score: 7.8 HIGH      Exploitability: 0.18;
     13.  CVE-2022-20818   Score: 7.8 HIGH      Exploitability: 0.18;
     14.  CVE-2022-20848   Score: 7.5 HIGH      Exploitability: 0.39;
     15.  CVE-2022-20851   Score: 7.2 HIGH      Exploitability: 0.12;
     16.  CVE-2023-20065   Score: 7.8 HIGH      Exploitability: 0.18;
     17.  CVE-2023-20066   Score: 6.5 MEDIUM    Exploitability: 0.28;
     18.  CVE-2023-20081   Score: 5.9 MEDIUM    Exploitability: 0.22;

   2) Cisco Asr 9902,  Information Security Risk: 24.95
  Vulnerabilities (14):
```

Fig. 5.8. Example of displaying information about a network that, for example, consisted of three devices

The program for analyzing hardware and software vulnerabilities of network equipment based on NVD-NIST database data is a powerful tool for collecting relevant data on the level of network security of TCN elements and the network in general. This information, represented by the compromise probabilities (vulnerability exploitation), is used as input data for solving secure routing problems in the third chapter of this work.

5.4. Conclusions to the Fifth Chapter

1. The optimization models of fault-tolerant and secure routing in TCN over disjoint paths proposed in this work can be used as elements of mathematical and algorithmic software of modern SDN routers and controllers. Prospective routing protocols in Software-Defined Networks can be based on these models.

2. The chapter shows the peculiarities of the practical implementation of the solutions proposed in the dissertation by the example of using the Cisco Modeling Labs simulator. The network controller is proposed to automatically collect and update information about the network state: its topology, bandwidth of communication links, user (flows) requirements to QoS, QoR and network security level.

3. Based on the collected information about the network state, it is recommended that the controller calculates disjoint routes using a software implementation of the proposed routing models in the Python environment. In the future, the controller can transmit information about the calculated routes to TCN routers by their remote software configuration via SSH protocol using the Python Paramiko library.

4. The chapter provides examples of automated collection and processing of information about the state of network security of TCN elements using the developed software. Fragments of code in MATLAB environment and Python language are presented, which can be executed to calculate the desired routes and network controller (server).

CONCLUSIONS

The dissertation successfully solved the scientific and practical problem of optimizing the processes of fault-tolerant and secure routing over disjoint paths in telecommunication networks by developing, improving, and investigating the corresponding mathematical models. Several conclusions can be drawn from the results of the solution of the set task.

1. The rapid development and continuous improvement of information and communication systems towards implementing Future Network technologies is a key priority in ensuring the national economy's competitiveness and any country's defense capability. It should be noted that in addition to Quality of Service requirements, which have already become the classic features of modern networks, the main aim is to ensure a high level of network resilience and security, especially important during network operation in the face of constant destructive influences, both random and purposeful. This can lead to forced changes in the structural and functional network parameters and properties regarding topology, bandwidth, resilience, etc.

2. This work proposes and investigates a system of mathematical optimization models for disjoint path computation in TCNs. Each of these models is focused on implementing certain sets of routing strategies – fault-tolerant, secure, and QoS routing. The joint features of these models are the formulation of route calculation problems in an optimization form, which allows for maximizing the efficiency of network resources (links, paths, and their capacity) in terms of Quality of Service, fault tolerance, and network security.

3. The dissertation improves the mathematical models of QoS routing in a telecommunication network over disjoint paths. The scientific novelty of the first mathematical model consists of introducing new conditions for balancing the routes' bandwidth and using an updated optimality criterion of routing solutions, which allowed to ensure the maximization of the number and total bandwidth of the calculated paths in the routing process. The scientific novelty of the second

mathematical model consists of introducing new bilinear conditions to ensure the guaranteed total bandwidth of routes, which allows the calculation of paths with a bandwidth not lower than the established threshold (requirement). Improved models increased the bandwidth of the calculated disjoint paths in TCN from 1.5-10% to 18.6-42%.

4. Mathematical models of secure QoS routing over disjoint paths have been further developed in this work. The proposed models' novelty lies in using a complex optimality criterion of routing solutions, which, along with bandwidth indicators, considers the network security parameters of communication links – the probability of their compromise. This allowed us to calculate such a set of paths in TCN, which, first, did not intersect; second, their number was the maximum possible; third, their total bandwidth was either the maximum possible or not lower than the specified one; fourth, the compromise probability of these paths was minimal.

5. The results of the study showed that the application of the proposed models of secure routing in TCN allows the reduction of the multipath compromise probability from 13% to 19% depending on the level of network security of communication links; the decrease in the compromise probability of confidential messages on average from 23-27% to 47-55% for different cases of links and routes compromise in the network. Applying the proposed model of secure routing with Quality of Service guarantees in terms of bandwidth has improved the probability of multipath compromise from 9-11.5% to 19.5-47% on average for different cases of compromise probabilities values of communication links.

6. The research process improves a fast rerouting model with support for *n*:1 path protection and network bandwidth protection schemes adapted to single path and multipath routing strategies. The novelty of the proposed model lies in the introduction of updated network bandwidth protection conditions, which allowed the implementation of the *n*:1 path protection scheme without a proportional increase in the dimensionality of the optimization problem. As a result of research, it is established that at the implementation of the scheme 2:1 for the primary route, it was

possible to increase bandwidth by 49% and reduce the average packet delay by almost 40%. When implementing the 3:1 scheme, it was possible to increase the bandwidth of the primary route by 86% and reduce the average end-to-end packet delay for the primary route by almost 57.4%, for the first backup route by 11.7%, and for the second backup route by 53.6%.

7. A system of recommendations for the practical use of the solutions proposed in this work for fault-tolerant and secure routing in Software-Defined Networks is proposed. The example of software implementation of the developed optimization models of fault-tolerant and secure routing in a Python environment and application of the code in the process of remote software configuration of TCN routers in the Cisco Modeling Lab simulator illustrates the recommendations.

8. The results of the dissertation work are implemented

– in Ltd "SMART POWER" when developing software for additional configuration of network equipment of telecommunication networks to improve the Quality of Service and network security;
– in Ltd "OMEGA SOLUTIONS" when developing practical recommendations for increasing the level of network protection and fault tolerance in telecommunication networks;
– in the educational process of the Kharkiv National University of Radio Electronics at the V.V. Popovskyy Department of Infocommunication Engineering in the process of the tutorial of the discipline "Routing in infocommunications".

Implementation of the dissertation work results is confirmed by the corresponding certificates (Appendix A).

REFERENCES

1. Лемешко, О.В., Єременко, О.С., Невзорова, О.С., 2020. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість. Харків: ХНУРЕ. 308 с.

2. White, R., Banks, E., 2018. Computer Networking Problems and Solutions: An innovative approach to building resilient, modern networks 1st Edition. 1 edition. Addison-Wesley Professional. 832 p.

3. Dodd, A.Z., 2019. The Essential Guide to Telecommunications (Essential Guide Series). Prentice Hall; 6 edition. 464 p.

4. Vidal, I., Soto, I., Banchs, A., Garcia-Reinoso, J., Lozano, I., Camarillo, G., 2019. Multimedia Networking Technologies, Protocols, & Architectures (Artech House Communications and Network Engineering), 1st edition, Artech House. 300 p.

5. Blokdyk, G., 2019. Software-Defined Networking SDN production, 1st edition. 5STARCooks. 238 p.

6. Szigeti, T., Zacks, D., Falkner, M. and Arena, S., 2018. Cisco digital network architecture: intent-based networking for the enterprise. Cisco Press. 800 p.

7. Medhi, D., Ramasamy, K., 2018. Network Routing (Algorithms, Protocols, and Architectures), 2nd edition, Elsevier Inc. 1018 p.

8. Cisco Networking Academy, 2014. Cisco Networking Academy, ed. Routing Protocols Companion Guide, 1st Edition, Cisco Press. 792 p.

9. Barkalov, A., Lemeshko, O., Yeremenko, O., Titarenko, L. and Yevdokymenko, M., 2023. Solving Load Balancing Problems in Routing and Limiting Traffic at the Network Edge. Applied Sciences, 13(17), p. 9489. DOI: https://doi.org/10.3390/app13179489

10. Lemeshko, O., Yeremenko, O., Titarenko, L. and Barkalov, A., 2023. Hierarchical Queue Management Priority and Balancing Based Method under the Interaction Prediction Principle. Electronics, 12(3), p. 675. DOI: https://doi.org/10.3390/electronics12030675

11. Lemeshko, O., Papan, J., Yevdokymenko, M. and Yeremenko, O., 2022. Advanced tensor solution to the problem of inter-domain routing with normalized quality of service. Applied Sciences, 12(2), p. 846. DOI: https://doi.org/10.3390/app12020846

12. Lemeshko, O., Papan, J., Yeremenko, O., Yevdokymenko, M. and Segec, P., 2021. Research and development of delay-sensitive routing tensor model in IoT core networks. Sensors, 21(11), p. 3934. DOI: https://doi.org/10.3390/s21113934

13. Yeremenko, O.S., Lemeshko, O.V., Nevzorova, O.S. and Hailan, A.M., 2017. Method of hierarchical QoS routing based on network resource reservation. In 2017 IEEE First Ukraine Conference on electrical and computer engineering (UKRCON), pp. 971-976. IEEE. DOI: https://doi.org/10.1109/UKRCON.2017.8100393

14. Yeremenko, A.S., 2018. A two-level method of hierarchical-coordination QoS-routing on the basis of resource reservation. Telecommunications and Radio Engineering, 77(14). pp. 1231-1247. DOI: https://doi.org/10.1615/TelecomRadEng.v77.i14.20

15. Chapman, C., 2016. Network Performance and Security (Testing and Analyzing Using Open Source and Low-Cost Tools), 1st edition, Syngress. 380 p.

16. Rak, J., 2015. Resilient routing in communication networks (Vol. 118). Berlin: Springer., 1st edition. Springer, 2015. 181 p.

17. Mauthe, A., Hutchison, D., Cetinkaya, E.K., Ganchev, I., Rak, J., Sterbenz, J.P., Gunkelk, M., Smith, P. and Gomes, T., 2016, September. Disaster-resilient communication networks: Principles and best practices. In 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pp. 1-10. IEEE. DOI: https://doi.org/10.1109/RNDM.2016.7608262

18. Gomes, T., Jorge, L., Girão-Silva, R., Yallouz, J., Babarczi, P. and Rak, J., 2020. Fundamental schemes to determine disjoint paths for multiple failure scenarios. Guide to Disaster-Resilient Communication Networks, pp. 429-453. DOI: https://doi.org/10.1007/978-3-030-44685-7_17

19. Lou, W. and Kwon, Y., 2006. H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. IEEE Transactions on Vehicular technology, 55(4), pp. 1320-1330. DOI: https://doi.org/10.1109/TVT.2006.877707

20. Alouneh, S., Agarwal, A. and En-Nouaary, A., 2009. A novel path protection scheme for MPLS networks using multi-path routing. Computer Networks, 53(9), pp. 1530-1545. DOI: https://doi.org/10.1016/j.comnet.2009.02.001

21. Guck, J.W., Van Bemten, A., Reisslein, M. and Kellerer, W., 2017. Unicast QoS routing algorithms for SDN: A comprehensive survey and performance evaluation. IEEE Communications Surveys & Tutorials, 20(1), pp. 388-415. DOI: https://doi.org/10.1109/COMST.2017.2749760

22. Yeremenko, O., Lemeshko, O. and Persikov, A., 2017, September. Secure routing in reliable networks: proactive and reactive approach. In Conference on Computer Science and Information Technologies, pp. 631-655. Cham: Springer International Publishing. Vol 689, pp. 631-655. DOI: https://doi.org/10.1007/978-3-319-70581-1_44

23. Yeremenko, O., Lemeshko, O. and Persikov, A., 2017, September. Enhanced method of calculating the probability of message compromising using overlapping routes in communication network. In 2017 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), Vol. 1, pp. 87-90. IEEE. DOI: https://doi.org/10.1109/STC-CSIT.2017.8098743

24. Yeremenko, O., 2015, October. Enhanced flow-based model of multipath routing with overlapping by nodes paths. In 2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), pp. 42-45. IEEE. DOI: https://doi.org/10.1109/INFOCOMMST.2015.7357264

25. Lemeshko, O., Yeremenko, O., Persikov, A. and Vavenko, T., 2018, September. Mathematical Model of Calculating the Maximum Number of Disjoint

Paths in Secure Routing. In 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1-4. IEEE. DOI: https://doi.org/10.1109/UkrMiCo43733.2018.9047581

26. Challal, Y., Ouadjaout, A., Lasla, N., Bagaa, M. and Hadjidj, A., 2011. Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks. Journal of network and computer applications, 34(4), pp. 1380-1397. DOI: https://doi.org/10.1016/j.jnca.2011.03.022

27. Gomes, T., Martins, L., Ferreira, S., Pascoal, M. and Tipper, D., 2017. Algorithms for determining a node-disjoint path pair visiting specified nodes. Optical Switching and Networking, 23, pp. 189-204. DOI: https://doi.org/10.1016/j.osn.2016.05.002

28. Cruz, P., Gomes, T. and Medhi, D., 2014, November. A heuristic for widest edge-disjoint path pair lexicographic optimization. In 2014 6th International Workshop on Reliable Networks Design and Modeling (RNDM), pp. 9-15. IEEE. DOI: https://doi.org/10.1109/RNDM.2014.7014925

29. Guo, L., 2016. Efficient approximation algorithms for computing k disjoint constrained shortest paths. Journal of Combinatorial Optimization, 32, pp. 144-158. DOI: https://doi.org/10.1007/s10878-015-9934-2

30. Eppstein, D., 1998. Finding the k shortest paths. SIAM Journal on computing, 28(2), pp. 652-673. DOI: https://doi.org/10.1137/S0097539795290477

31. Chang, Z.Z., Zhao, G.Y. and Sun, Y.F., 2013, July. A calculation method for the reliability of a complex k-out-of-n system. In 2013 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE), pp. 204-207. IEEE. DOI: https://doi.org/10.1109/QR2MSE.2013.6625566

32. Myslitski, K. and Rak, J., 2015, July. Evaluation of time-efficiency of disjoint paths calculation schemes. In 2015 17th International Conference on Transparent Optical Networks (ICTON), pp. 1-4. IEEE. DOI: https://doi.org/10.1109/ICTON.2015.7193309

33. Qu, Z., Ren, W. and Wang, Q., 2010, August. A new node-disjoint multi-path routing algorithm of wireless Mesh network. In 2010 International Conference

on Computer, Mechatronics, Control and Electronic Engineering, Vol. 4, pp. 1-3. IEEE. DOI: https://doi.org/10.1109/CMCE.2010.5609590

34. Shi, Y., 2010, November. Calculation of Network System Reliability Based on Improved Disjointed Minimal Path Set. In 2010 International Conference on E-Product E-Service and E-Entertainment, pp. 1-4. IEEE. DOI: https://doi.org/10.1109/ICEEE.2010.5660486

35. Yu, Z., Ni, M., Wang, Z. and Huang, H., 2011, April. Heuristic algorithm for K-disjoint QoS routing problem. In 2011 Fourth International Joint Conference on Computational Sciences and Optimization, pp. 353-356. IEEE. DOI: https://doi.org/10.1109/CSO.2011.145

36. Лемешко, О.В., Єременко, О.С., Євдокименко, М.О., Шаповалова, А.С., Слейман, Б., 2022. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах: Монографія. Харків: ХНУРЕ, 2022. 198 с. DOI: https://doi.org/10.30837/978-966-659-378-1

37. Лемешко, А.В., Еременко, А.С., Персиков, А.В., Слейман, Б., 2019. Модель безопасной маршрутизации на основе определения максимального количества непересекающихся путей для минимизации вероятности компрометации конфиденциальных сообщений. Радіотехніка: Всеукр. міжвід. наук.-техн. збірник, 197, С. 31-37. URL: http://openarchive.nure.ua/handle/document/9645

38. Невзорова, О.С., Слейман, Б., Мерсні, А., Сухотеплий, В.М., 2019. Вдосконалення потокової моделі багатоадресної маршрутизації на принципах технології Traffic Engineering. Проблеми телекомунікацій, 2(25), С. 27-36. DOI: https://doi.org/10.30837/pt.2019.2.02

39. Єременко, О.С., Євдокименко, М.О., Слейман, Б., 2020. Удосконалена модель швидкої перемаршрутизації з реалізацією схеми захисту шляху та пропускної здатності в програмно-конфігурованих мережах. Сучасний стан наукових досліджень та технологій в промисловості, 1(11), С. 163–171. DOI: https://doi.org/10.30837/2522-9818.2020.11.163

40. Лемешко, О.В., Грачов, Ю.В., Слейман, Б., 2020. Дослідження методу безпечної маршрутизації конфіденційних повідомлень за шляхами, які не перетинаються. Проблеми телекомунікацій, 2(27), С. 43-55. DOI: https://doi.org/10.30837/pt.2020.2.04

41. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Sleiman, B., 2020. Fast ReRoute Model with Realization of Path and Bandwidth Protection Scheme in SDN. Advances in Electrical and Electronic Engineering, 18(1), pp. 23-30. DOI: https://doi.org/10.15598/aeee.v18i1.3548

42. Lemeshko, O., Yeremenko, O., Yevdokymenko, M. and Sleiman, B., 2019, April. System of Solutions the Maximum Number of Disjoint Paths Computation Under Quality of Service and Security Parameters. In Conference on Mathematical Control Theory, pp. 191-205. Cham: Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-58359-0_10

43. Lemeshko, O., Yeremenko, O., Yevdokymenko, M. and Sleiman, B., 2023, March. Research and Development of Bilinear QoS Routing Model over Disjoint Paths with Bandwidth Guarantees in SDN. In International Conference on Computer Science, Engineering and Education Applications, pp. 223-235. Cham: Springer Nature Switzerland. DOI: https://doi.org/10.1007/978-3-031-36118-0_20

44. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Ilyashenko, A. and Sleiman, B., 2019, July. Traffic engineering fast reroute model with support of policing. In 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), pp. 842-845. IEEE. DOI: https://doi.org/10.1109/UKRCON.2019.8880006

45. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Sleiman, B., Hailan, A.M. and Mersni, A., 2019, July. Computation Method of Disjoint Paths under Maximum Bandwidth Criterion. In 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), pp. 161-164. IEEE. DOI: https://doi.org/10.1109/AIACT.2019.8847756

46. Lemeshko, O., Yeremenko, O., Yevdokymenko, M. and Sleiman, B., 2019, December. Enhanced solution of the disjoint paths set calculation for secure

QoS routing. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), pp. 210-213. IEEE. DOI: https://doi.org/0.1109/ATIT49449.2019.9030520

47. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Sleiman, B., Segeč, P. and Papán, J., 2020, May. Advanced Performance-Based Fast ReRouting Model with Path Protection. In 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 23-28. IEEE. DOI: https://doi.org/10.1109/DESSERT50317.2020.9125034

48. Yevdokymenko, M., Manasse, M., Zalushniy, D. and Sleiman, B., 2017, October. Analysis of methods for assessing the reliability and security of infocommunication network. In 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), pp. 199-202. IEEE. DOI: https://doi.org/10.1109/INFOCOMMST.2017.8246379

49. Yevdokymenko, M., Sleiman, B., Harkusha, S. and Harkusha, O., 2018, October. Method of fault tolerance evaluation in conditions of destabilizing factors influence in infocommunication network. In 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), pp. 571-574. IEEE. DOI: https://doi.org/10.1109/INFOCOMMST.2018.8632077

50. Lemeshko, O., Yeremenko, O., Yevdokymenko, M. and Sleiman, B., 2019, September. Improvement of the calculation model the set of disjoint paths with maximum bandwidth. In 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1-4. IEEE. DOI: https://doi.org/10.1109/UkrMiCo47782.2019.9165311

51. Євдокименко, М.О., Єременко, О.С., Слейман, Б., 2019. Тензорна модель швидкої перемаршрутизації із захистом рівня якості обслуговування. Третя міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології». Збірник наукових праць. Харків: ХНУРЕ, С. 132.

52. Yeremenko, O., Yevdokymenko, M., Sleiman, B., Omowumi, S.O., 2020. Fast ReRouting Flow-based Model with Implementation of Path Protection.

Proceedings of Fourth International Scientific and Technical Conference on Computer and Information Systems and Technologies, Kharkiv, Ukraine. NURE, p. 83.

53. Stallings, W., 2016. Cryptography and Network Security: Principles and Practice. 7th Edition, Pearson. 768 p.

54. Edgar, T.W. and Manz, D.O., 2017. Research methods for cyber security. Syngress. 428 p.

55. Bruzgiene, R., Narbutaite, L., Adomkus, T., Pocta, P., Brida, P., Machaj, J., Leitgeb, E., Pezzei, P., Ivanov, H., Kunicina, N. and Zabasta, A., 2020. Quality-driven schemes enhancing resilience of wireless networks under weather disruptions. Guide to Disaster-Resilient Communication Networks, pp. 299-326. DOI: https://doi.org/10.1007/978-3-030-44685-7_12

56. ITU-T Rec. Y.1540. Internet protocol data communication service – IP packet transfer and availability performance parameters. July 2016. 57 p. URL: https://www.itu.int/rec/T-REC-Y.1540-201607-I/en.

57. ITU-T Rec. Y.1541. Network performance objective for IP-based services. December 2011. 66 p. URL: https://www.itu.int/rec/T-REC-Y.1541-201112-I/en.

58. ITU-T Rec. G.1011. Reference guide to quality of experience assessment methodologies. July 2016. 26 p. URL: https://www.itu.int/rec/T-REC-G.1011-201607-I/en.

59. ITU-T Recommendation G.107: The E-model: a computational model for use in transmission planning. Geneva. 2015. 30 p.

60. ITU-T Recommendation G.1070 Opinion model for video-telephony applications. Geneva. 2015. 32 p.

61. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Hailan, A.M. and Mersni, A., 2019, September. Cyber resilience approach based on traffic engineering fast reroute with policing. In 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems:

Technology and Applications (IDAACS), Vol. 1, pp. 117-122. IEEE. DOI: https://doi.org/10.1109/IDAACS.2019.8924294

62. Lemeshko, O., Yevdokymenko, M., Yeremenko, O., Hailan, A.M., Segeč, P. and Papán, J., 2019, February. Design of the fast reroute QoS protection scheme for bandwidth and probability of packet loss in software-defined WAN. In 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), pp. 1-5. IEEE. DOI: https://doi.org/10.1109/CADSM.2019.8779321

63. Lopez-Pajares, D., Rojas, E., Carral, J.A., Martinez-Yelmo, I. and Alvarez-Horcajo, J., 2021. The disjoint multipath challenge: Multiple disjoint paths guaranteeing scalability. IEEE Access, 9, pp. 74422-74436. DOI: https://doi.org/10.1109/ACCESS.2021.3080931

64. Lopez-Pajares, D., Alvarez-Horcajo, J., Rojas, E., Carral, J.A. and Martinez-Yelmo, I., 2020. One-shot multiple disjoint path discovery protocol (1S-MDP). IEEE Communications Letters, 24(8), pp. 1660-1663. DOI: https://doi.org/10.1109/LCOMM.2020.2990885

65. Robinson, Y.H., Julie, E.G., Saravanan, K., Kumar, R., Abdel-Basset, M. and Thong, P.H., 2019. Link-disjoint multipath routing for network traffic overload handling in mobile ad-hoc networks. IEEE Access, 7, pp. 143312-143323. DOI: https://doi.org/10.1109/ACCESS.2019.2943145

66. Sreeram, K., Unnisa, A. and Poornima, V., 2019, March. QoS aware multi-constrained node disjoint multipath routing for wireless sensor networks. In 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), pp. 382-385. IEEE. DOI: https://doi.org/10.1109/ICACCS.2019.8728475

67. Sarma, H.K.D., Dutta, M.P. and Dutta, M.P., 2019, December. A Quality of Service Aware Routing Protocol for Mesh Networks Based on Congestion Prediction. In 2019 International Conference on Information Technology (ICIT), pp. 430-435. IEEE. DOI: https://doi.org/10.1109/ICIT48102.2019.00082

68. Zhang, C., Zhang, S., Wang, Y., Li, W., Jin, B., Mok, R.K., Li, Q. and Xu, H., 2020, April. Scalable traffic engineering for higher throughput in heavily-loaded software defined networks. In NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, pp. 1-7. IEEE. DOI: https://doi.org/10.1109/NOMS47738.2020.9110259

69. Besta, M., Domke, J., Schneider, M., Konieczny, M., Di Girolamo, S., Schneider, T., Singla, A. and Hoefler, T., 2020. High-performance routing with multipathing and path diversity in ethernet and hpc networks. IEEE Transactions on Parallel and Distributed Systems, 32(4), pp. 943-959. DOI: https://doi.org/10.1109/TPDS.2020.3035761

70. Hou, A., Wu, C.Q., Zuo, L., Zhang, X., Wang, T. and Fang, D., 2020. Bandwidth scheduling for big data transfer with two variable node-disjoint paths. Journal of Communications and Networks, 22(2), pp. 130-144. DOI: https://doi.org/10.1109/JCN.2020.000004

71. Zhang, W., Lei, W. and Zhang, S., 2020. A multipath transport scheme for real-time multimedia services based on software-defined networking and segment routing. IEEE Access, 8, pp.93962-93977. DOI: https://doi.org/10.1109/ACCESS.2020.2994346

72. Zeng, G., Zhan, Y. and Pan, X., 2021. Failure-tolerant and low-latency telecommand in mega-constellations: The redundant multi-path routing. IEEE Access, 9, pp. 34975-34985. DOI: https://doi.org/10.1109/ACCESS.2021.3061736

73. Kaneko, K., Van Nguyen, S. and Binh, H.T.T., 2020. Pairwise disjoint paths routing in tori. IEEE Access, 8, pp. 192206-192217. DOI: https://doi.org/10.1109/ACCESS.2020.3032684

74. Lemeshko, A.V., Evseeva, O.Y. and Garkusha, S.V., 2014. Research on tensor model of multipath routing in telecommunication network with support of service quality by greate number of indices. Telecommunications and Radio Engineering, 73(15), pp. 1339-1360. DOI: https://doi.org/10.1615/TelecomRadEng.v73.i15.30

75. Lemeshko, O.V. and Yeremenko, O.S., 2016, October. Dynamics analysis of multipath QoS-routing tensor model with support of different flows classes. In 2016 International Conference on Smart Systems and Technologies (SST), pp. 225-230. IEEE. DOI: https://doi.org/10.1109/SST.2016.7765664

76. Mohan, P.M., Gurusamy, M. and Lim, T.J., 2018. Dynamic attack-resilient routing in software defined networks. IEEE Transactions on Network and Service Management, 15(3), pp. 1146-1160. DOI: https://doi.org/10.1109/TNSM.2018.2846294

77. Gupta, D., Segal, A., Panda, A., Segev, G., Schapira, M., Feigenbaum, J., Rexford, J. and Shenker, S., 2012, October. A new approach to interdomain routing based on secure multi-party computation. In Proceedings of the 11th ACM Workshop on Hot Topics in Networks, pp. 37-42. DOI: https://doi.org/10.1145/2390231.2390238

78. Gharib, M., Yousefi'zadeh, H. and Movaghar, A., 2018. Secure overlay routing for large scale networks. IEEE Transactions on Network Science and Engineering, 6(3), pp. 501-511. DOI: https://doi.org/10.1109/TNSE.2018.2812830

79. Snihurov, A. and Chakrian, V., 2015. Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters. Scholars Journal of Engineering and Technology, 3(8). pp. 707-714.

80. Francois, F. and Gelenbe, E., 2016, September. Optimizing secure SDN-enabled inter-data centre overlay networks through cognitive routing. In 2016 IEEE 24th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), pp. 283-288. IEEE. DOI: https://doi.org/10.1109/MASCOTS.2016.26

81. Wang, M., Liu, J., Mao, J., Cheng, H., Chen, J. and Qi, C., 2017. RouteGuardian: Constructing secure routing paths in software-defined networking. Tsinghua Science and Technology, 22(4), pp. 400-412. DOI: https://doi.org/10.23919/TST.2017.7986943

82. Mudgerikar, A. and Bertino, E., 2023, July. Intelligent Security Aware Routing: Using Model-Free Reinforcement Learning. In 2023 32nd International

Conference on Computer Communications and Networks (ICCCN), pp. 1-10. IEEE. DOI: https://doi.org/10.1109/ICCCN58024.2023.10230195

83. Maheswari, S., Mishra, N., Shadaksharappa, B. and Sivanesan, T.M., 2023, July. Secured Dynamic Opportunistic Routing in Ad-hoc Wireless Network. In 2023 2nd International Conference on Edge Computing and Applications (ICECAA), pp. 293-297. IEEE. DOI: https://doi.org/10.1109/ICECAA58104.2023.10212369

84. Shruthi, B.M. and Raju, C., 2023, June. A Comprehensive Analysis on Trust Based Secure Routing Protocol used in Internet of Things (IoTs). In 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC), pp. 1-4. IEEE. DOI: https://doi.org/10.1109/ICAISC58445.2023.10200961

85. Mohanty, R.K., Sahoo, S.P. and Kabat, M.R., 2023, June. A Network Reliability based Secure Routing Protocol (NRSRP) for Secure Transmission in Wireless Body Area Network. In 2023 8th International Conference on Communication and Electronics Systems (ICCES), pp. 663-668. IEEE. DOI: https://doi.org/10.1109/ICCES57224.2023.10192691

86. Mohammadinejad, H. and Mohammadhoseini, F., 2019. Proposing a method for enhancing the reliability of RPL routing protocol in the smart grid neighborhood area networks. International Journal of Computer Network and Information Security, 11(7), p. 21. DOI: https://doi.org/10.5815/ijcnis.2019.07.0

87. Shashi, R.K. and Siddesh, G.K., 2018. QoS oriented cross-synch routing protocol for event driven, mission-critical communication over MANET: Q-CSRPM. International Journal of Computer Network and Information Security, 11(11), p. 18. DOI: https://doi.org/10.5815/ijcnis.2018.11.0

88. Ibraheem, I.K., Al-Hussainy, A.A.-H., 2018. A Multi QoS Genetic-based Adaptive Routing in Wireless Mesh Networks with Pareto Solutions. International Journal of Computer Network and Information Security (IJCNIS), 10(9), pp. 1-9. DOI: https://doi.org/10.5815/ijcnis.2018.09.01

89. Vyas, A. and Satheesh, A., 2018. Implementing security features in MANET routing protocols. International Journal of Computer Network and Information Security, 10(8), pp. 51-57. DOI: https://doi.org/10.5815/ijcnis.2018.08.06

90. Papan, J., Segec, P., Paluch, P., Uramova, J. and Moravcik, M., 2020. The new multicast repair (M-REP) IP fast reroute mechanism. Concurrency and Computation: Practice and Experience, 32(13), p.e5105. DOI: https://doi.org/10.1002/cpe.5105

91. Lemeshko, O., Yeremenko, O. and Tariki, N., 2017. Solution for the default gateway protection within fault-tolerant routing in an IP network. International journal of electrical and computer engineering systems, 8(1.), pp. 19-26. DOI: https://doi.org/10.32985/ijeces.8.1.3

92. Sun, W., Wang, Z. and Zhang, G., 2021. A QoS-guaranteed intelligent routing mechanism in software-defined networks. Computer Networks, 185, p. 107709. DOI: https://doi.org/10.1016/j.comnet.2020.107709

93. Sarma, H.K.D., Dutta, M.P. and Dutta, M.P., 2019, December. A Quality of Service Aware Routing Protocol for Mesh Networks Based on Congestion Prediction. In 2019 International Conference on Information Technology (ICIT), pp. 430-435. IEEE. DOI: https://doi.org/10.1109/ICIT48102.2019.00082

94. Monge, A.S. and Szarkowicz, K.G., 2015. MPLS in the SDN Era: Interoperable Scenarios to Make Networks Scale to New Services. O`Reilly Media, Inc. 2016. 917 p.

95. Perepelkin, D., Ivanchikova, M. and Ivutin, A., 2017, April. Fast rerouting algorithm in distributed computer networks based on subnet routing method. In 2017 27th International Conference Radioelektronika (RADIOELEKTRONIKA), pp. 1-4. IEEE. DOI: https://doi.org/10.1109/RADIOELEK.2017.7936648

96. Rak, J., Papadimitriou, D., Niedermayer, H. and Romero, P., 2017. Information-driven network resilience: Research challenges and perspectives.

Optical Switching and Networking, 23, pp. 156-178. DOI: https://doi.org/10.1016/j.osn.2016.06.002

97. Merling, D., Braun, W. and Menth, M., 2018, June. Efficient data plane protection for SDN. In 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), pp. 10-18. IEEE. DOI: https://doi.org/10.1109/NETSOFT.2018.8459923

98. Rak, J., Hutchison, D., Tapolcai, J., Bruzgiene, R., Tornatore, M., Mas-Machuca, C., Furdek, M. and Smith, P., 2020. Fundamentals of communication networks resilience to disasters and massive disruptions. Guide to Disaster-Resilient Communication Networks, pp. 1-43. DOI: https://doi.org/10.1007/978-3-030-44685-7_1

99. Lemeshko, O., Arous, K. and Tariki, N., 2015, October. Effective solution for scalability and productivity improvement in fault-tolerant routing. In 2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), pp. 76-78. IEEE. DOI: https://doi.org/10.1109/INFOCOMMST.2015.7357274

100. Lemeshko, O. and Yeremenko, O., 2017. Enhanced method of fast re-routing with load balancing in software-defined networks. Journal of Electrical Engineering, 68(6), pp. 444-454. DOI: https://doi.org/10.1515/jee-2017-0079

101. Lemeshko, O. and Yeremenko, O., 2018, February. Linear optimization model of MPLS Traffic Engineering Fast ReRoute for link, node, and bandwidth protection. In 2018 14th international conference on advanced trends in radioelecrtronics, telecommunications and computer engineering (TCSET), pp. 1009-1013. IEEE. DOI: https://doi.org/10.1109/TCSET.2018.8336365

102. Lemeshko, O.V., Garkusha, S.V., Yeremenko, O.S. and Hailan, A.M., 2015, May. Policy-based QoS management model for multiservice networks. In 2015 International Siberian Conference on Control and Communications (SIBCON), pp. 1-4. IEEE. DOI: https://doi.org/10.1109/SIBCON.2015.7147124

103. Tanha, M., Sajjadi, D. and Pan, J., 2018, June. Demystifying failure recovery for software-defined wireless mesh networks. In 2018 4th IEEE

Conference on Network Softwarization and Workshops (NetSoft), pp. 488-493. IEEE. DOI: https://doi.org/10.1109/NETSOFT.2018.8460087

104. Braun, W., Merling, D. and Menth, M., 2018, February. Destination-specific maximally redundant trees: Design, performance comparison, and applications. In 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), pp. 1-8. IEEE. DOI: https://doi.org/10.1109/ICIN.2018.8401580

105. Chan, K.Y., Chen, C.H., Chen, Y.H., Tsai, Y.J., Lee, S.S. and Wu, C.S., 2018, October. Fast failure recovery for in-band controlled multi-controller OpenFlow networks. In 2018 International Conference on Information and Communication Technology Convergence (ICTC), pp. 396-401. IEEE. DOI: https://doi.org/10.1109/ICTC.2018.8539715

106. Thorat, P., Jeon, S. and Choo, H., 2017. Enhanced local detouring mechanisms for rapid and lightweight failure recovery in OpenFlow networks. Computer Communications, 108, pp. 78-93. DOI: https://doi.org/10.1016/j.comcom.2017.04.005

107. Zhang, X., Cheng, Z., Lin, R., He, L., Yu, S. and Luo, H., 2016. Local fast reroute with flow aggregation in software defined networks. IEEE Communications Letters, 21(4), pp.785-788. DOI: https://doi.org/10.1109/LCOMM.2016.2638430

108. Myoupo, J.F., Yankam, Y.F. and Tchendji, V.K., 2018, October. A Centralized and Conflict-Free Routing Table Update Method through Triplets' Lists Vector in SDN Architectures. In 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), pp. 1509-1515. IEEE. DOI: https://doi.org/10.1109/SmartWorld.2018.00261

109. Jia, X., Jiang, Y. and Zhu, J., 2018, April. Link fault protection and traffic engineering in hybrid SDN networks. In IEEE INFOCOM 2018-IEEE

Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 853-858. IEEE. DOI: https://doi.org/10.1109/INFCOMW.2018.8406823

110. Hao, F., Kodialam, M. and Lakshman, T.V., 2016, April. Optimizing restoration with segment routing. In IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications (pp. 1-9). IEEE. DOI: https://doi.org/10.1109/INFOCOM.2016.7524551

111. Alhaqbani, M. and Liu, H., 2017, December. Conceptual Mechanism Software Defined Network Topology in Multiprotocol Label Switching Network Domain. In 2017 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 680-684. IEEE. DOI: https://doi.org/10.1109/CSCI.2017.117

112. Moore, H., 2017. MATLAB for Engineers. Pearson; 5th edition. 688 p.

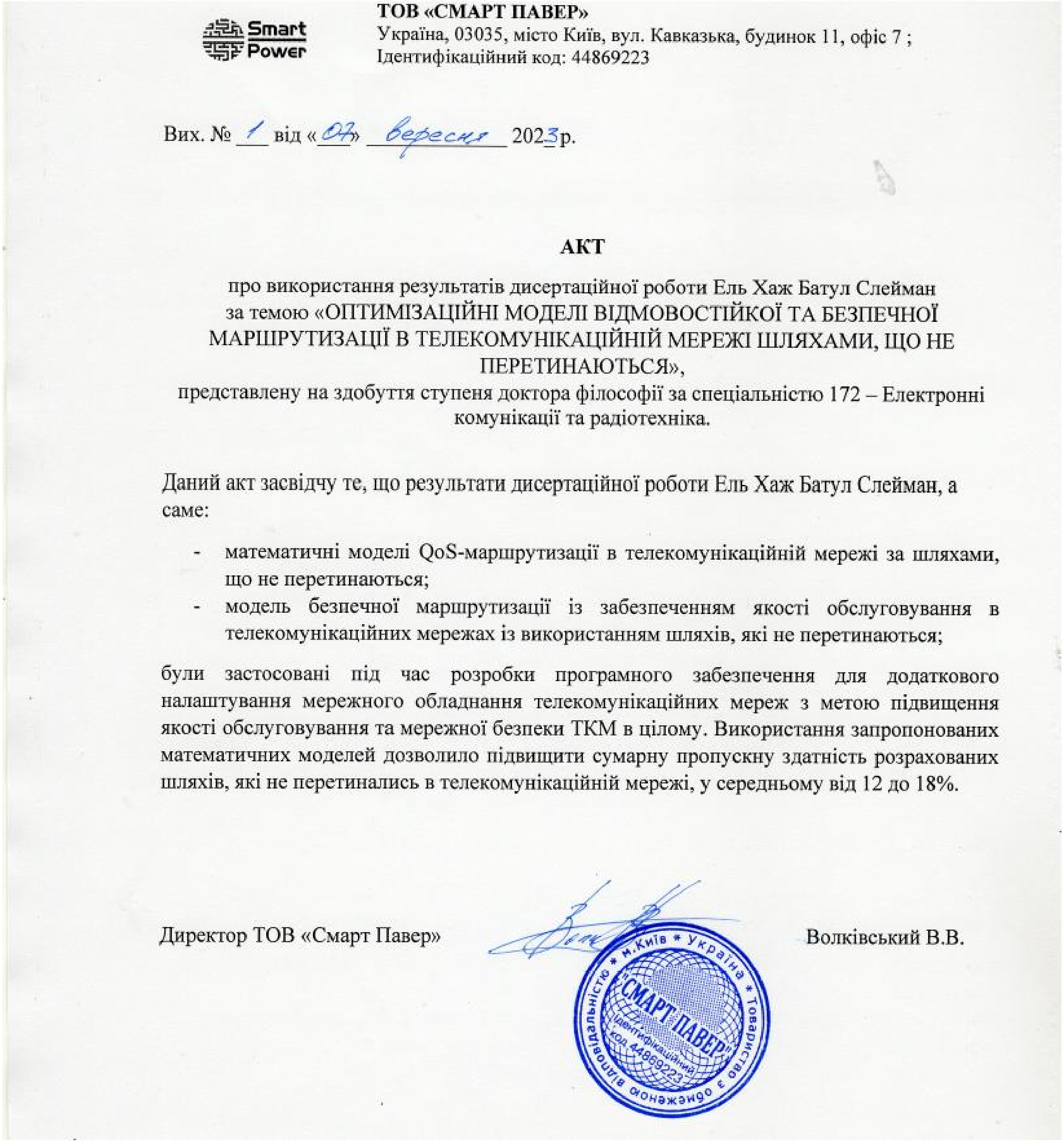
113. Patankar, P. and Kulkarni, S., 2022. MATLAB and Simulink In-Depth: Model-based Design with Simulink and Stateflow, User Interface, Scripting, Simulation, Visualization and Debugging. BPB Publications. 602 p.

114. Kong, Q., Siauw, T. and Bayen, A., 2020. Python programming and numerical methods: A guide for engineers and scientists. Academic Press. 1st edition. 480 p.

115. Johansson, R., 2019. Numerical Python: Scientific Computing and Data Science Applications with Numpy, SciPy and Matplotlib, Apress, Berkeley, CA. 723 p. DOI: https://doi. org/10.1007/978-1-4842-4246-9

APPENDIX A

CERTIFICATES ON THE USE OF RESEARCH RESULTS



Smart Power

ТОВ «СМАРТ ПАВЕР»
Україна, 03035, місто Київ, вул. Кавказька, будинок 11, офіс 7 ;
Ідентифікаційний код: 44869223

Вих. № 1 від «07» вересня 2023р.

АКТ

про використання результатів дисертаційної роботи Ель Хаж Батул Слейман за темою «ОПТИМІЗАЦІЙНІ МОДЕЛІ ВІДМОВОСТІЙКОЇ ТА БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ШЛЯХАМИ, ЩО НЕ ПЕРЕТИНАЮТЬСЯ», представлену на здобуття ступеня доктора філософії за спеціальністю 172 – Електронні комунікації та радіотехніка.

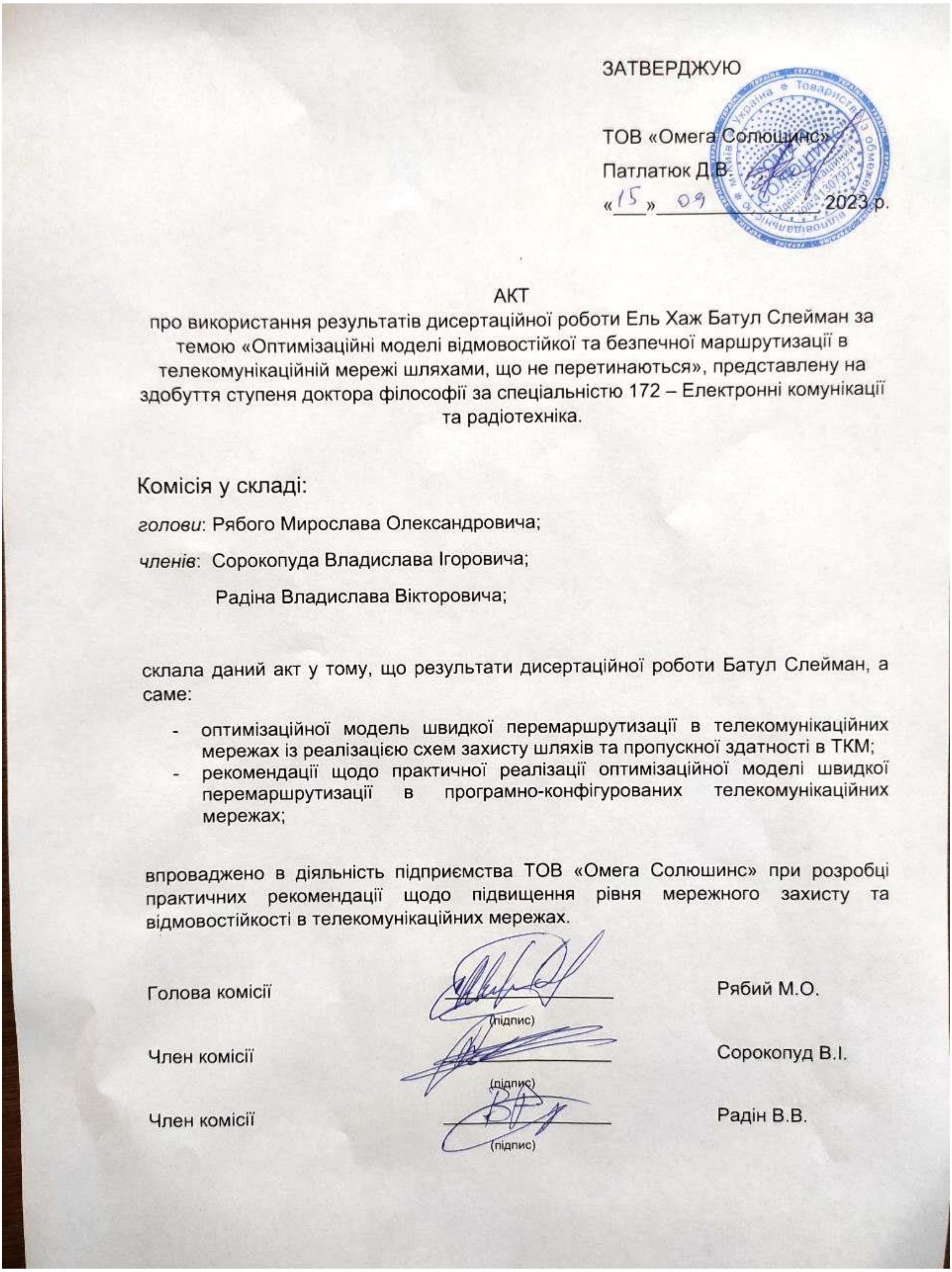
Даний акт засвідчу те, що результати дисертаційної роботи Ель Хаж Батул Слейман, а саме:

- математичні моделі QoS-маршрутизації в телекомунікаційній мережі за шляхами, що не перетинаються;
- модель безпечної маршрутизації із забезпеченням якості обслуговування в телекомунікаційних мережах із використанням шляхів, які не перетинаються;

були застосовані під час розробки програмного забезпечення для додаткового налаштування мережного обладнання телекомунікаційних мереж з метою підвищення якості обслуговування та мережної безпеки ТКМ в цілому. Використання запропонованих математичних моделей дозволило підвищити сумарну пропускну здатність розрахованих шляхів, які не перетинались в телекомунікаційній мережі, у середньому від 12 до 18%.

Директор ТОВ «Смарт Павер» Волківський В.В.

Товариство з обмеженою відповідальністю * м.Київ * Україна *
«СМАРТ ПАВЕР»
Ідентифікаційний код 44869223



ЗАТВЕРДЖУЮ

ТОВ «Омега Солюшинс»
Патлатюк Д.В.
«15» 09 2023 р.

Україна * Товариство з обмеженою відповідальністю * ОМЕГА СОЛЮШИНС * Ідентифікаційний код 41307927

АКТ
про використання результатів дисертаційної роботи Ель Хаж Батул Слейман за темою «Оптимізаційні моделі відмовостійкої та безпечної маршрутизації в телекомунікаційній мережі шляхами, що не перетинаються», представлену на здобуття ступеня доктора філософії за спеціальністю 172 – Електронні комунікації та радіотехніка.

Комісія у складі:

голови: Рябого Мирослава Олександровича;

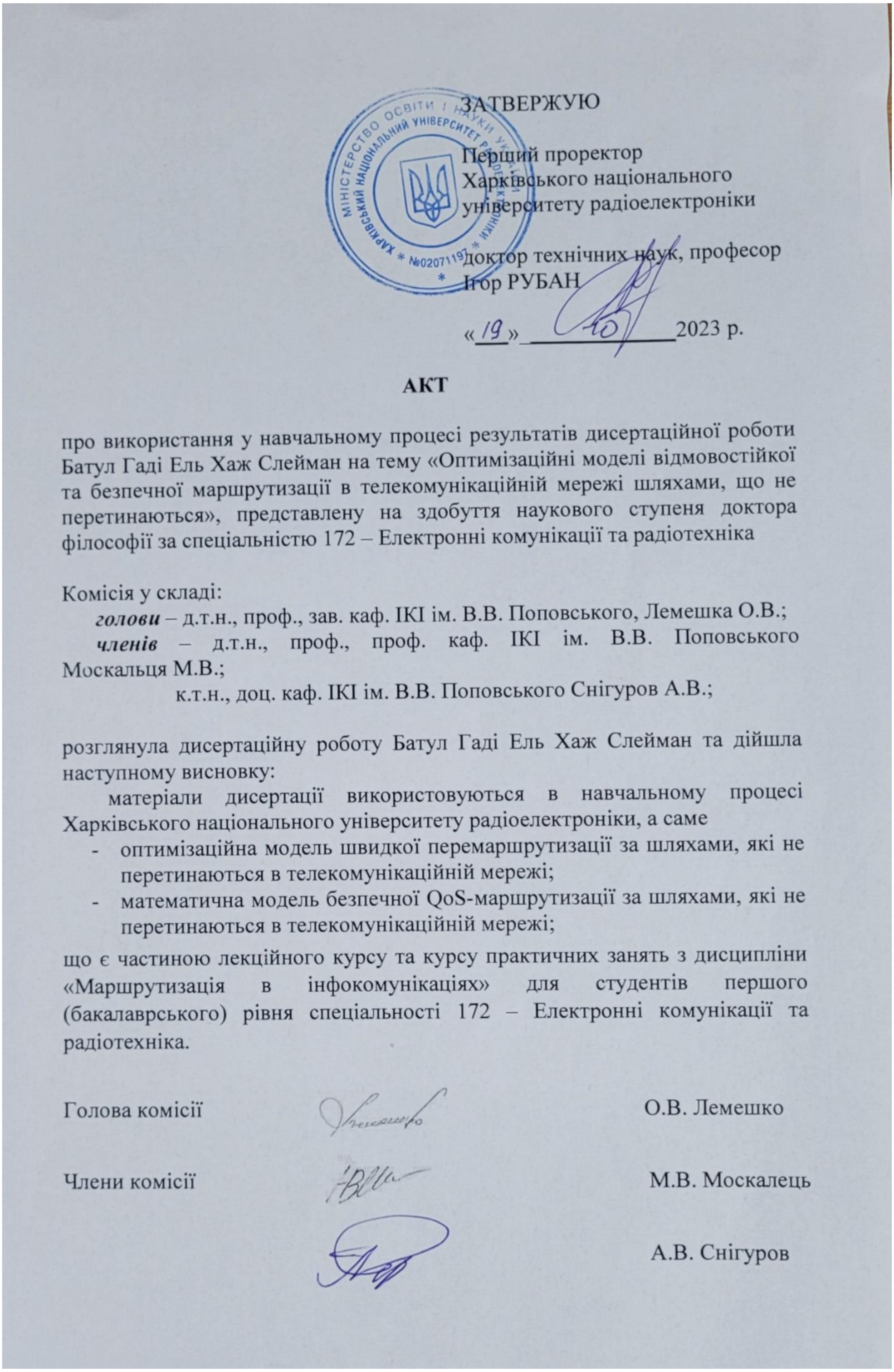
членів: Сорокопуда Владислава Ігоровича;
Радіна Владислава Вікторовича;

склала даний акт у тому, що результати дисертаційної роботи Батул Слейман, а саме:

- оптимізаційної модель швидкої перемаршрутизації в телекомунікаційних мережах із реалізацією схем захисту шляхів та пропускної здатності в ТКМ;
- рекомендації щодо практичної реалізації оптимізаційної моделі швидкої перемаршрутизації в програмно-конфігурованих телекомунікаційних мережах;

впроваджено в діяльність підприємства ТОВ «Омега Солюшинс» при розробці практичних рекомендації щодо підвищення рівня мережного захисту та відмовостійкості в телекомунікаційних мережах.

Голова комісії	____________ (підпис)	Рябий М.О.
Член комісії	____________ (підпис)	Сорокопуд В.І.
Член комісії	____________ (підпис)	Радін В.В.



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ * №02071197 *

ЗАТВЕРЖУЮ

Перший проректор
Харківського національного
університету радіоелектроніки

доктор технічних наук, професор
Ігор РУБАН

«19» 10 2023 р.

АКТ

про використання у навчальному процесі результатів дисертаційної роботи Батул Гаді Ель Хаж Слейман на тему «Оптимізаційні моделі відмовостійкої та безпечної маршрутизації в телекомунікаційній мережі шляхами, що не перетинаються», представлену на здобуття наукового ступеня доктора філософії за спеціальністю 172 – Електронні комунікації та радіотехніка

Комісія у складі:

голови – д.т.н., проф., зав. каф. ІКІ ім. В.В. Поповського, Лемешка О.В.;

членів – д.т.н., проф., проф. каф. ІКІ ім. В.В. Поповського Москальця М.В.;

к.т.н., доц. каф. ІКІ ім. В.В. Поповського Снігуров А.В.;

розглянула дисертаційну роботу Батул Гаді Ель Хаж Слейман та дійшла наступному висновку:

матеріали дисертації використовуються в навчальному процесі Харківського національного університету радіоелектроніки, а саме

- оптимізаційна модель швидкої перемаршрутизації за шляхами, які не перетинаються в телекомунікаційній мережі;
- математична модель безпечної QoS-маршрутизації за шляхами, які не перетинаються в телекомунікаційній мережі;

що є частиною лекційного курсу та курсу практичних занять з дисципліни «Маршрутизація в інфокомунікаціях» для студентів першого (бакалаврського) рівня спеціальності 172 – Електронні комунікації та радіотехніка.

Голова комісії О.В. Лемешко

Члени комісії М.В. Москалець

А.В. Снігуров