UDC 621.391

OPTIMIZING HARD QOS AND SECURITY WITH DISJOINT PATH ROUTING

Oleksandr V. Lemeshko, Oleksandra S. Yeremenko, Maryna O. Yevdokymenko,
Batoul Sleiman

Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Background. The combination of secure routing and hard QoS 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. Secure QoS routing over disjoint paths is a challenging problem that requires balancing the trade-off between network security and bandwidth guarantees.

Objective. This article investigates a mathematical model that can address secure QoS routing by formulating it as an optimization problem with a linear objective function and linear or bilinear constraints. The objective function aims to minimize the paths compromise probability, while the constraints ensure that the total bandwidth of the paths meets the QoS requirements.

Methods. We use computer simulation of hard QoS and security with disjoint path routing. Also we use mathematical programming methods in order to describe secure QoS routing.

Results. The article presents a numerical study of the model using different scenarios and parameters. The results show that the model can effectively provide secure QoS routing over disjoint paths with a high bandwidth guarantee level and a low compromise probability. The work analyses the sensitivity of the solutions to the QoS requirements and reveals that there is usually some margin in the bandwidth provision.

Conclusions. The proposed model is a promising tool for secure QoS routing over disjoint paths in various network environments.

Keywords: *Quality of Service; security; routing; disjoint paths; bandwidth; compromise probability.*

Introduction

An important place among the means of ensuring the Quality of Service (QoS) in modern information and communication networks (ICNs) is occupied by routing protocols [1, 2]. They are tasked with determining one or more paths along which the specified QoS indicators would be provided. First of all, we are talking about bandwidth, average packet delay, jitter, and packet loss rate [3-8].

It is worth noting that in IP networks, not all protocols meet the requirements for considering multiple QoS indicators when forming metrics and calculating routes. As of now, only the proprietary protocol EIGRP (Enhanced Interior Gateway Routing Protocol) proposed by Cisco [2] takes into account a set of route performance indicators, albeit indirectly, when determining routing metrics:

- number of retransmissions (hops);
- bandwidth;
- packet delay;
- packet loss rate;
- route link utilization.

Within the EIGRP protocol, these indicators are converted into a scalar routing metric traditionally used by routing algorithms, such as DUAL. This approach is quite universal and is used in other IP routing protocols. However, it does not allow us to discuss the guaranteed values of the selected QoS indicators, which is important for most packet flows circulating in modern multiservice ICNs.

In addition, in recent years, network security tasks have come to the fore. Their successful solution is also associated with the involvement of the functionality of all levels of the OSI (Open System Interconnection) model. In this regard, the term "secure routing" appeared when determining routes; in addition to QoS indicators, it is necessary to consider network security indicators [9-12]. The traditional approach is to use an option where the composite protocol metric will additionally take into account another indicator related to network security. This will not lead to revising the set of used route calculation algorithms - Dijkstra, Bellman-Ford, DUAL. However, as the analysis has shown, an approach based on the departure from using graph models for finding the shortest path in a graph and the listed combinatorial optimization algorithms is becoming increasingly common among scientists dealing with routing problems [13-16]. The power of contemporary routers makes it possible to use more modern but also more computationally complex optimization models, methods, and computational

© The Author(s) 2023. Published by Igor Sikorsky Kyiv Polytechnic Institute.
This is an Open Access article distributed under the terms of the license CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/), which permits re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

algorithms, in which, at the level of optimization criteria and introduced constraints, it is possible to more adequately consider the requirements for the values of certain QoS and network security indicators.

In this work, we will consider and investigate an approach to solving the problem of secure QoS routing based on optimizing the process of calculating a given number of disjoint paths along which the bandwidth requirements are guaranteed to be met, and such an important network security indicator as the probability of packet compromise is improved.

Mathematical Model of Secure QoS Routing over Disjoint M-Paths with Guaranteed Bandwidth

We reviewed existing methods [17-20] for finding disjoint paths in a network and selected the basic mathematical model for computing routes, which was introduced and analysed in [15, 16]. We will use the following notation to explain the model in this article:

- $G = (R, E)$ - network structure graph;
- $R = \left\{R_i; i = \overline{1,m}\right\}$ - set of vertices (routers);
- $E = \left\{E_{i,j}; i,j = \overline{1,m}; i \neq j\right\}$ - set of edges (links);
- s_k - sender node (source);
- d_k - receiver node (destination);
- K - network flows ($k \in K$);
- $a_{i,j}^k$ - control variables that establish if the link $E_{i,j} \in E$ is in the set of distinct paths for the *k*th flow;
- $\varphi_{i,j}$ - link $E_{i,j} \in E$ capacity (packets per second, pps);
- M^k - integer constant that determine disjoint paths number;
- $w_{i,j}$ - weighting coefficients connected to the link $E_{i,j} \in E$ capacity;
- $p_{i,j}$ - link $E_{i,j} \in E$ compromise.

To solve the stated problem of sending the *k*th flow over disjoint M-paths, we need to obtain the set of variables $a_{i,j}^k$ under the constraints:

$$a_{i,j}^k \in \{0;1\}. \tag{1}$$

In addition, for every pair of source and destination nodes, the conditions must be satisfied [15, 16]:

$$\sum_{j:E_{i,j}\in E} a_{i,j}^k = \mathrm{M}^k;\ k \in K,\ \ R_i = s_k; \tag{2}$$

$$\sum_{j:E_{j,i}\in E} a_{j,i}^k = \mathrm{M}^k;\ k \in K,\ \ R_i = d_k. \tag{3}$$

Simultaneously, the basic model imposes the following restrictions on transit nodes, $R_i \neq s_k, d_k$, [16]:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} a_{i,j}^k \le 1, \quad k \in K; \\ \sum\limits_{j:E_{j,i}\in E} a_{j,i}^k \le 1, \quad k \in K; \\ \sum\limits_{j:E_{i,j}\in E} a_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} a_{j,i}^k = 0, \quad k \in K. \end{cases} \tag{4}$$

The initial inequality in the system (4) implies that the transit router R_i can only have one path exiting it. Ensuring the satisfaction of the second condition in system (4) is essential to ensure that the transit router R_i is not involved in more than one path within the computed set of disjoint routes. Implementing the third condition from (4) entails that a path can only depart from a transit router R_i if it has previously arrived at that node.

To implement M-Paths routing, it is necessary to predetermine and fix the number of calculated disjoint paths:

$$\mathrm{M}^k \ge 1. \tag{5}$$

In a more comprehensive perspective, the acceptable values represented by M^k are closely connected to the network's configuration. This connection is notably influenced by factors such as the network's topology, the extent of connectivity among nodes, and the degree of vertices in the *G* graph, which simulates the source and destination routers.

The basic mathematical model, represented by equations (1) to (5), can be adjusted for QoS routing to achieve maximum or predefined bandwidth. This adjustment involves employing a calculated set of disjoint paths. Consequently, additional conditions must be introduced within the framework of the basic model to ensure a specific Quality of Service level concerning bandwidth. In this regard, we define β_{path}^k as the minimum threshold value for the bandwidth associated with any set of disjoint paths responsible for transmitting the *k*th packet flow. Therefore, the subsequent condition can be integrated into the routing model, akin to the methodology in [16]:

$$a_{i,j}^k \varphi_{i,j} + W(1 - a_{i,j}^k) \ge \beta_{path}^k. \tag{6}$$

In this context, the weighting coefficients *W* take on values surpassing the maximum bandwidth of links in the network. Compliance with condition (6) guarantees that each route within the computed disjoint paths for the *k*th flow has a bandwidth equal to or exceeding β^k_{path}.

Let's designate as β^k this specific threshold value, for example, as for every *k*th packet flow. Accordingly, within the model outlined by conditions (1) to (6), the subsequent condition is suggested:

$$\mathrm{M}^k \beta^k_{path} \geq \beta^k . \qquad (7)$$

The left side of inequality (7) denotes the minimum bandwidth requirement, collectively enabling the use of the computed paths. This lower limit is guaranteed because, according to conditions (6), each disjoint path has a capacity that is equal to or exceeds β^k_{path}, albeit potentially surpassing it. Depending on the chosen optimality criterion, achieving the conditions outlined in (7) can be accomplished by increasing the number of employed M^k disjoint routes or by raising the threshold β^k_{path} value concerning the minimum bandwidth of the paths.

As a result, in [15, 16], it is suggested to modify the model (1)-(7) by complementing it, altering the type of optimality criterion, which will be based on maximizing such an objective function:

$$J = \sum_{E_{i,j} \in E} w_{i,j} a^k_{i,j} . \qquad (8)$$

Within the objective function (8), the significance of individual terms is determined by positive weights $w_{i,j}$. It is essential to select these weights in a manner that prioritizes the minimization of the compromise probability when selecting the set of disjoint paths [15]:

$$w_{i,j} = -\lg\left(1 - p_{i,j}\right) . \qquad (9)$$

Then the probability of compromise for the *n*th path can be derived according to [3]:

$$p_n = 1 - \prod_{E_{i,j} \in L_n} \left(1 - p_{i,j}\right) , \qquad (10)$$

where L_n is the ordered set of links of the *n*th path.

Finally, the compromise probability of the disjoint paths (multipath) is obtained as [15]:

$$P^k_{MP} = \prod_{i=1}^{\mathrm{M}^k} p_n . \qquad (11)$$

To guarantee QoS bandwidth assurances in secure routing implementations, it is suggested to frame the routing problem using the model (1)-(11) in the following optimization formulation:

- The routing decisions' optimality criterion is defined as the maximum value of the objective function (8).
- Constraints (1)-(4) and (6) are applied to the routing variables $a^k_{i,j}$ and the variables β^k_{path} to maintain balance in the routes' capacity.
- Constraints (5) and (7) are applied to the balancing variables β^k_{path}, influencing the number of disjoint routes engaged.

Hence, in the context of implementing a secure routing strategy, employing the model (1)-(11) emphasizes solutions falling under the DiffServ category. From a QoS routing perspective, the solutions obtained adhere to IntServ principles. This is attributed to the fact that the use of the optimality criterion (8) aims to select paths with a high, albeit non-guaranteed, level of network security. However, the incorporation of conditions (7) into the model structure aims to ensure the QoS level concerning bandwidth β^k. As a result, the solution to the optimization problem yields a multipath – a set of disjoint paths with maximum capacity, ensuring a total bandwidth not below the specified requirements β^k and a minimal compromise probability.

In summary, the application of the model (1)-(11) allows the classification of the optimization problem for secure QoS routing over disjoint paths, providing guaranteed bandwidth, as a Mixed Integer Linear Programming (MILP) problem.

Study results of a mathematical model of secure QoS routing in a network over disjoint paths

When examining the model for secure QoS routing over disjoint paths with guaranteed bandwidth (1)-(11), the requirements β^k specified in constraint (7) play a crucial role. This is because the optimality criterion (8) does not explicitly incorporate parameters related to the bandwidth of links and paths. To meet the conditions outlined in (7), ensuring that the multipath for the *k*th packet flow will maintain a bandwidth not less than β^k. The level of guarantees offered by a particular multipath, as per conditions (7), is determined by the product $\mathrm{M}^k \beta^k_{path}$.

The characteristics of the model for secure QoS routing in a network will be elucidated through a subsequent numerical illustration. In the context of the examined network depicted in Fig. 1, the first and seventh nodes are designated as routers representing the source and destination of the flow, respectively. Implementing the proposed model results in four distinct scenarios, each characterized by varying probabilities of compromising communication links. These scenarios yield sets of disjoint paths, as outlined in Table 1. Additionally, the table provides information on the bandwidths associated with the links in the network.

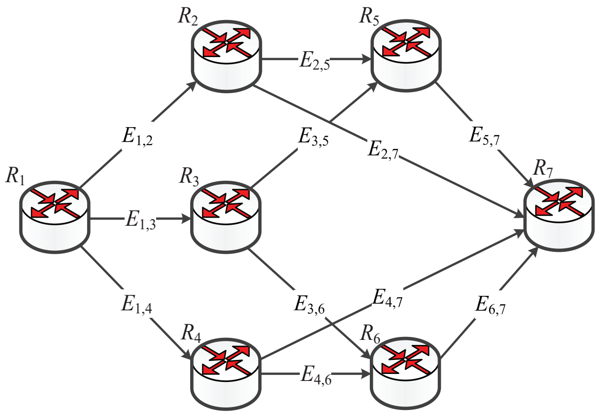

Fig. 1 Structure of the network under study

Table 1. Input data for investigating secure QoS routing models

Link	BW, pps	Link compromise probability			
		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 system (12) outlines the collection of possible routes connecting the source and destination nodes:

$$\begin{cases} L_1 = \{E_{1,2}, E_{2,5}, E_{5,7}\}; \\ L_2 = \{E_{1,3}, E_{3,6}, E_{6,7}\}; \\ L_3 = \{E_{1,4}, E_{4,7}\}; \\ L_4 = \{E_{1,4}, E_{4,6}, E_{6,7}\}; \\ L_5 = \{E_{1,3}, E_{3,5}, E_{5,7}\}; \\ L_6 = \{E_{1,2}, E_{2,7}\}. \end{cases} \tag{12}$$

Table 2 presents the bandwidths and compromise probabilities of the paths (12) available for transmitting packets, linking the source R_1 and destination R_7 routers, under various network link compromise probabilities scenarios.

Table 2. The bandwidth of the paths available for packet transmission between the source and the destination routers

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 displays potential routing solutions, featuring, for instance, two computed disjoint paths. In turn, it provides the bandwidth and compromise probability for each multipath. Additionally, Table 3 shows the extreme bandwidth values and compromise probability for each initial data set.

Table 3. Calculation results of the disjoint paths set

Set #	Disjoint Paths Set	BW, pps	Multipath compromise probability			
			Case 1	*Case 2*	*Case 3*	*Case 4*
1	$\{E_{1,2}, E_{2,5}, E_{5,7}\}$ $\{E_{1,3}, E_{3,6}, E_{6,7}\}$	340	0.3293	0.2508	0.2420	0.1447
2	$\{E_{1,2}, E_{2,5}, E_{5,7}\}$ $\{E_{1,4}, E_{4,7}\}$	400	0.3453	0.1806	0.2877	0.1121
3	$\{E_{1,2}, E_{2,5}, E_{5,7}\}$ $\{E_{1,4}, E_{4,6}, E_{6,7}\}$	290	0.3772	0.3445	0.2460	0.1545
4	$\{E_{1,3}, E_{3,6}, E_{6,7}\}$ $\{E_{1,2}, E_{2,7}\}$	390	0.2579	0.2673	0.2245	0.1928
5	$\{E_{1,4}, E_{4,7}\}$ $\{E_{1,2}, E_{2,7}\}$	450	0.2704	0.1924	0.2668	0.1494
6	$\{E_{1,4}, E_{4,6}, E_{6,7}\}$ $\{E_{1,2}, E_{2,7}\}$	340	0.2954	0.3671	0.2282	0.2058
7	$\{E_{1,3}, E_{3,5}, E_{5,7}\}$ $\{E_{1,2}, E_{2,7}\}$	380	0.2907	0.1830	0.2282	0.1601
8	$\{E_{1,4}, E_{4,7}\}$ $\{E_{1,3}, E_{3,5}, E_{5,7}\}$	430	0.2907	0.1302	0.2877	0.1389

9	$\{E_{1,4}, E_{4,6}, E_{6,7}\}$ $\{E_{1,3}, E_{3,5}, E_{5,7}\}$	320	0.3175	0.2485	0.2460	0.1914
10	$\{E_{1,3}, E_{3,6}, E_{6,7}\}$ $\{E_{1,4}, E_{4,7}\}$	440	0.2579	0.1902	0.2830	0.1672

Subsequently, two types of requirements for the total bandwidth of disjoint paths (β^k) were considered: 300 and 400 pps. In the case when β^k = 300 pps, the optimal routing solutions for different variants of ICN link compromise within the framework of models (1)-(11) are the ones presented in Table 4.

Table 4. Optimal routing solutions for β^k = 300 pps

Compro-mise	Disjoint Paths Set	BW, pps	Multipath compromise probability
Case 1	$\{E_{1,3}, E_{3,6}, E_{6,7}\}$ $\{E_{1,4}, E_{4,7}\}$	440	0.2579
Case 2	$\{E_{1,2}, E_{2,5}, E_{5,7}\}$ $\{E_{1,4}, E_{4,7}\}$	400	0.1806
Case 3	$\{E_{1,3}, E_{3,6}, E_{6,7}\}$ $\{E_{1,2}, E_{2,7}\}$	390	0.2245
Case 4	$\{E_{1,2}, E_{2,5}, E_{5,7}\}$ $\{E_{1,4}, E_{4,7}\}$	400	0.1121

In the case when β^k = 400 pps, the optimal solution for all variants of ICN link compromise is the routing solution represented by the fifth multipath in Table 3, i.e., the paths $\{E_{1,4}, E_{4,7}\}$ and $\{E_{1,2}, E_{2,7}\}$. Only this set of disjoint paths ensured the joint fulfilment of conditions (6) and (7).

Conclusion

This article presents a mathematical model of secure QoS routing in ICNs (1)-(11) using disjoint paths. Within the model, the engineering problem of routing was reduced to solving a MILP-class optimization problem with a linear optimality criterion (8) and linear constraints (1)-(4), (6), and (7). Integers represent the set of variables (1), and the variable β^k_{path} is a real number.

The study of the proposed model for calculating routes for different variants of link compromise and QoS requirements confirmed its effectiveness in providing guarantees for path bandwidth and increasing the level of network security in terms of the compromise probability. The logic of the model was that among those multipaths that met the bandwidth requirements, the option that provided the minimum value of the probability of compromise was selected (Table 4).

During the research, we noticed the robust nature of the obtained routing solutions, which were not sensitive to the level of QoS requirements (β^k). As a rule, bandwidth guarantees were provided with a significant reserve. This is because conditions (6) and (7) focus on the worst case regarding the bandwidth of the routes included in the optimal multipath.

References

1. R. Lacoste and B. Edgeworth, CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide, Cisco Press, 2020.
2. Medhi, D., Ramasamy, K. Network routing: Algorithms, Protocols, and Architectures; Morgan Kaufmann: San Francisco, CA, USA, 2017.
3. I.V. Strelkovskaya and I.N. Solovskaya, "Tensor model of multiservice network with different classes of traffic service", Radioelectron.Commun.Syst., vol. 56, pp. 296–303, 2013, doi: 10.3103/S0735272713060058.
4. I.V. Strelkovskaya, T.I. Grygoryeva and I.N. Solovskaya, "Self-Similar Traffic in G/M/1 Queue Defined by the Weibull Distribution", Radioelectron.Commun.Syst., vol. 61, pp. 128–134, 2018, doi: 10.3103/S0735272718030056.
5. O. Lemeshko, M. Yevdokymenko, O. Yeremenko, A. M. Hailan, P. Segeč and J. Papán, "Design of the Fast ReRoute QoS Protection Scheme for Bandwidth and Probability of Packet Loss in Software-Defined WAN," 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), Polyana, Ukraine, 2019, pp. 1-5, doi: 10.1109/CADSM.2019.8779321.
6. O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, A. M. Hailan and A. Mersni, "Cyber Resilience Approach Based on Traffic Engineering Fast ReRoute with Policing," 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019, pp. 117-122, doi: 10.1109/IDAACS.2019.8924294.
7. W. Sun, Z. Wang and G. Zhang, "A QoS-guaranteed intelligent routing mechanism in software-defined networks", Computer Networks, vol. 185, p.107709, 2021, doi: 10.1016/j.comnet.2020.107709.
8. H. K. Deva Sarma, M. P. Dutta and M. P. Dutta, "A Quality of Service Aware Routing Protocol for Mesh Networks Based on Congestion Prediction," 2019 International Conference on Information Technology (ICIT), Bhubaneswar, India, 2019, pp. 430-435, doi: 10.1109/ICIT48102.2019.00082.

9. A. Mudgerikar and E. Bertino, "Intelligent Security Aware Routing: Using Model-Free Reinforcement Learning," 2023 32nd International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 2023, pp. 1-10, doi: 10.1109/ICCCN58024.2023.10230195.

10. S. Maheswari, N. Mishra, B. Shadaksharappa and T. M. Sivanesan, "Secured Dynamic Opportunistic Routing in Ad-hoc Wireless Network," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, 2023, pp. 293-297, doi: 10.1109/ICECAA58104.2023.10212369.

11. B. M. Shruthi and C. Raju, "A Comprehensive Analysis on Trust Based Secure Routing Protocol used in Internet of Things (IoTs)," 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC), Dharwad, India, 2023, pp. 1-4, doi: 10.1109/ICAISC58445.2023.10200961.

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

13. T. Gomes, L. Jorge, R. Girão-Silva, J. Yallouz, P. Babarczi and J. Rak, "Fundamental Schemes to Determine Disjoint Paths for Multiple Failure Scenarios", in Rak, J., Hutchison, D. (eds) Guide to Disaster-Resilient Communication Networks. Computer Communications and Networks, pp. 429–453, Springer, Cham, 2020, doi: 10.1007/978-3-030-44685-7_17.

14. D. Lopez-Pajares, E. Rojas, J. A. Carral, I. Martinez-Yelmo and J. Alvarez-Horcajo, "The Disjoint Multipath Challenge: Multiple Disjoint Paths Guaranteeing Scalability," in IEEE Access, vol. 9, pp. 74422-74436, 2021, doi: 10.1109/ACCESS.2021.3080931.

15. O. Lemeshko, O. Yeremenko, M. Yevdokymenko and B. Sleiman, "System of Solutions the Maximum Number of Disjoint Paths Computation Under Quality of Service and Security Parameters", in Ilchenko, M., Uryvsky, L., Globa, L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol. 152, pp. 191–205, Springer, Cham, 2021, doi: 10.1007/978-3-030-58359-0_10.

16. O. Lemeshko, O. Yeremenko, M. Yevdokymenko and B. Sleiman, "Research and Development of Bilinear QoS Routing Model over Disjoint Paths with Bandwidth Guarantees in SDN", in Hu, Z., Dychka, I., He, M. (eds) Advances in Computer Science for Engineering and Education VI. ICCSEEA 2023. Lecture Notes on Data Engineering and Communications Technologies, vol. 181, pp. 223–235, Springer, Cham, 2023, doi: 10.1007/978-3-031-36118-0_20.

17. D. Lopez-Pajares, J. Alvarez-Horcajo, E. Rojas, J. A. Carral and I. Martinez-Yelmo, "One-Shot Multiple Disjoint Path Discovery Protocol (1S-MDP)," in IEEE Communications Letters, vol. 24, no. 8, pp. 1660-1663, Aug. 2020, doi: 10.1109/LCOMM.2020.2990885.

18. Y. H. Robinson et al., "Link-Disjoint Multipath Routing for Network Traffic Overload Handling in Mobile Ad-hoc Networks," in IEEE Access, vol. 7, pp. 143312-143323, 2019, doi: 10.1109/ACCESS.2019.2943145.

19. K. Kaneko, S. V. Nguyen and H. T. T. Binh, "Pairwise Disjoint Paths Routing in Tori," in IEEE Access, vol. 8, pp. 192206-192217, 2020, doi: 10.1109/ACCESS.2020.3032684.

20. K. Sreeram, A. Unnisa, V. Poornima and S. Chaudhari, "QoS aware Multi-Constrained Node Disjoint Multipath Routing for Wireless Sensor Networks," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 382-385, doi: 10.1109/ICACCS.2019.8728475.

Лемешко О.В., Єременко О.С., Євдокименко М.О., Слейман Батул

Оптимізація процесів забезпечення гарантованої якості обслуговування та мережної безпеки під час маршрутизації шляхами, що не перетинаються

Проблематика. Поєднання безпечної маршрутизації та Hard QoS є важливою темою, яка передбачає розробку та впровадження мережних протоколів і систем, здатних забезпечити високу продуктивність і надійний захист потоків даних завдяки спільним цілям. Безпечна QoS-маршрутизація шляхами, що не перетинаються, є складною проблемою, яка вимагає компромісу між безпекою мережі та гарантіями щодо пропускної здатності.

Мета. У цій статті досліджується математична модель, яка може вирішити проблему безпечної маршрутизації QoS, сформулювавши її як оптимізаційну задачу з лінійною цільовою функцією і лінійними або білінійними обмеженнями. Цільова функція спрямована на мінімізацію ймовірності компрометації шляхів, тоді як обмеження гарантують, що сумарна пропускна здатність шляхів відповідає вимогам QoS.

Методи. Використовується комп'ютерне моделювання Hard QoS та безпеки при маршрутизації шляхами, що не перетинаються. Також використано методи математичного програмування для опису безпечної QoS-маршрутизації.

Результати дослідження. У статті представлено чисельне дослідження моделі з використанням різних сценаріїв і параметрів. Результати показують, що модель може ефективно забезпечувати безпечну QoS-маршрутизацію шляхами, що не перетинаються, з високим рівнем гарантії пропускної здатності та низькою ймовірністю компрометації. В роботі проаналізовано чутливість рішень до вимог QoS і виявлено, що зазвичай існує певний запас у забезпеченні пропускної здатності.

Висновки. Запропонована модель є перспективним інструментом для безпечної QoS-маршрутизації шляхами, що не перетинаються, у різних мережних середовищах.

Ключові слова: *Якість обслуговування; безпека; маршрутизація; шляхи, що не перетинаються; пропускна здатність; імовірність компрометації.*