Network Security Approach based on Traffic Engineering Fast ReRoute with support of Traffic Policing

Oleksandr Lemeshko[a], Oleksandra Yeremenko[a], Maryna Yevdokymenko[a], Anastasiia Shapovalova[a], and Valentyn Lemeshko[a]

[a] *Kharkiv National University of Radio Electronics, 14 Nauky ave., Kharkiv, 61166, Ukraine*

Abstract

The work is devoted to the approach development and investigation of the network security providing based on Traffic Engineering Fast ReRoute with support of Traffic Policing. The corresponding flow-based mathematical model has been developed where the technological task of secure fast rerouting was presented in the form of a linear programming problem. The novelty of the proposed model is the modification of load balancing conditions and bandwidth protection during fast rerouting, which in addition to the Quality of Service, also considers the probability of compromising the link as an indicator of network security. The routing solutions obtained within the proposed model are aimed at reducing the overload of communication links with a high probability of compromising by redistributing traffic for transmission through more secure network links. The advantage of the proposed solution is that in the conditions of congestion the load balancing is realized on the principles of Traffic Engineering and, if necessary, differentiated limitation of the load entering the network. An additional advantage of the proposed optimization model is its linearity, which focuses on the low computational complexity of the corresponding protocol implementation in practice. Numerical research of the Secure TE-FRR-TP model has confirmed the adequacy and efficiency of routing solutions made on its basis, both in terms of ensuring network security, resilience, and load balancing with traffic policing based on priorities.

Keywords

Cyber resilience, redundancy, fast ReRoute, traffic engineering, traffic policing, security metric, probability of compromise.

1. Introduction

In modern conditions of information society development, more and more attention is paid to the development of network (telecommunication) technologies in improving the Quality of Service (QoS), Quality of Reliability (QoR), and network security in terms of Quality of Protection (QoP) [1–3]. The same network means, mechanisms and protocols are often connected to the solution of such tasks. According to the results of research on a promising trend in telecommunications, it is the improvement of routing protocols, which contribute to the creation of functionality and provide a full-fledged means of ensuring service quality, resilience, and security [4–10]. The most effective way to improve routing protocols is to review the mathematical models and computational methods (algorithms) on which they are based [11–13].

Owing to software modifications and settings, modern protocol solutions have long gone beyond the rather limited functionality of combinatorial algorithms (Dijkstra and Bellman-Ford) to find the shortest path on the graph [14]. Therefore, modern protocols even support multipath and fault-tolerant routing with load balancing, mainly on paths with equal cost metrics [15]. However, the future of routing protocols is seen by many scientists [11–14, 16–18] in the use of flow-based mathematical models and

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine

EMAIL: oleksandr.lemeshko.ua@ieee.org (A.1); oleksandra.yeremenko.ua@ieee.org (A.2); maryna.yevdokymenko@ieee.org (A.3); anastasiia.shapovalova@nure.ua (A.4); valentyn.lemeshko@nure.ua (A.5)
ORCID: 0000-0002-0609-6520 (A.1); 0000-0003-3721-8188 (A.2); 0000-0002-7391-3068 (A.3); 0000-0003-0701-1282 (A.4); 0000-0003-1564-8873 (A.5)

optimization methods for route calculation and load balancing. Within the framework of flow-based solutions, additional opportunities are opened for providing QoS simultaneously on several indicators, full implementation of fault-tolerance functions with the protection of structural elements of the network and its bandwidth [11–17], as well as secure routing [13, 19–22]. Therefore, the task of supporting these important functionalities within a single mathematical model, which would take into account aspects of Quality of Service based on load balancing, resilience, and network security, is gaining relevance.

2. Flow-based Model of the Network Security Providing based on Traffic Engineering Fast ReRoute with Support of Policing

In this work, the approach of the network security providing based on Traffic Engineering Fast ReRoute with support of Traffic Policing (Secure TE-FRR-TP) is presented that is a further development of the models proposed in [23–26]. The following parameters are introduced into the corresponding flow-based model:

$G=(R,E)$	graph describing the network structure;
$R=\{R_i;\, i=\overline{1,m}\}$	set of nodes (network routers);
$E=\{E_{i,j};\, i,j=\overline{1,m};\, i\neq j\}$	set of edges (network links);
$R_i^*=\{R_j : \exists E_{j,i}\in E;\ j=\overline{1,m};\ i\neq j\}$	subset of routers incident to the R_i router;
$\varphi_{i,j}$	link capacity;
K	set of flows circulating in the network ($k\in K$);
$x_{i,j}^k$	control variables that determine the fraction of intensity of the *k*th flow in the link $E_{i,j}$ of the primary path;
$\overline{x}_{i,j}^k$	control variables that determine the fraction of intensity of the *k*th flow in the link $E_{i,j}$ of the backup path;
β^k	proportion of the intensity of the *k*th flow that receives a denial of service when using the primary path;
$\overline{\beta}^k$	proportion of the intensity of the *k*th flow that receives a denial of service when using the backup path;
s_k	source node;
d_k	destination node;
λ^k	average intensity (packet rate) of the *k*th flow in packets per second (1/s);
$u_{i,j}^k$	control variables that represent the upper bound values of routing variables of the primary and backup paths;
α	control variable that numerically determines the upper bound of the network links utilization;
α_{TH}	threshold of the upper bound of the network links utilization;
$p_{i,j}$	probability of link $E_{i,j}$ compromise;
$v_{i,j}$	weighting coefficients related to the probability of link $E_{i,j}$ compromise;
$w_k=PR^k+1$	weighting coefficients based on the priority of the *k*th flow (PR^k) transmitted over the primary path;
$\overline{w}_k=PR^k+0.5$	weighting coefficients based on the priority of the *k*th flow (PR^k) transmitted over the backup path.

The result of solving the technical task of network security providing based on Traffic Engineering Fast ReRoute with support of policing is a calculation of two types of routing variables $x_{i,j}^{k}$ and $\overline{x}_{i,j}^{k}$ for the primary or backup path. When the multipath strategy is used for routing variables of both types, the following constraints implied on them [24, 26]

$$0 \le x_{i,j}^{k} \le 1 \text{ and } 0 \le \overline{x}_{i,j}^{k} \le 1. \tag{1}$$

The flow conservation conditions aimed at ensuring the connectivity of the calculated primary and backup multipath also should be met [23]:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} x_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^{k} = 0;\ k \in K,\ R_i \ne s_k, d_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^{k} = 1-\beta^{k};\ k \in K,\ R_i = s_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^{k} = \beta^{k}-1;\ k \in K,\ R_i = d_k; \end{cases} \tag{2}$$

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} \overline{x}_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} \overline{x}_{j,i}^{k} = 0;\ k \in K,\ R_i \ne s_k, d_k; \\ \sum\limits_{j:E_{i,j}\in E} \overline{x}_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} \overline{x}_{j,i}^{k} = 1-\overline{\beta}^{k};\ k \in K,\ R_i = s_k; \\ \sum\limits_{j:E_{i,j}\in E} \overline{x}_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} \overline{x}_{j,i}^{k} = \overline{\beta}^{k}-1;\ k \in K,\ R_i = d_k. \end{cases} \tag{3}$$

During the process of fast rerouting, the link $E_{i,j} \in E$ protection scheme under multipath routing strategy over the backup multipath, the following condition is used [23, 25]:

$$0 \le \overline{x}_{i,j}^{k} \le \delta_{i,j}^{k}, \tag{4}$$

where

$$\delta_{i,j}^{k} = \begin{cases} 0, \text{ when protecting the link } E_{i,j}; \\ 1, \text{ otherwise}. \end{cases} \tag{5}$$

Linear conditions (4) and (5) are needed to guarantee that the protected link $E_{i,j} \in E$ will not be included in the backup path.

In the case of the node $R_i \in R$ protection, conditions (4) and (5) are used for protecting the adjacent links to this node [23], namely:

$$0 \le \overline{x}_{i,j}^{k} \le \delta_{i,j}^{k} \text{ under } R_j \in R_i^{*},\ j = \overline{1,m} \tag{6}$$

where $\delta_{i,j}^{k}$ are determined according to (5).

Within the presented approach of the network security providing based on Traffic Engineering Fast ReRoute with support of Traffic Policing, the model proposes to introduce the following modified conditions for preventing overloading in order to provide both load balancing and network security under the parameter of the probability of the network link compromising [26]:

$$\sum_{k\in K} \lambda^{k} \cdot u_{i,j}^{k} \le \alpha v_{i,j} \varphi_{i,j},\ E_{i,j} \in E, \tag{7}$$

where

$$x_{i,j}^{k} \le u_{i,j}^{k} \text{ and } \overline{x}_{i,j}^{k} \le u_{i,j}^{k}, \tag{8}$$

$$0 \le u_{i,j}^{k} \le 1, \tag{9}$$

$$0 \le \alpha \le \alpha_{TH}. \tag{10}$$

It should be noted that α_{TH} is determined by the QoS level requirements for the network. Moreover, the novelty of the approach is the introduction in conditions (11) the $v_{i,j}$ coefficients, the boundaries of which are following [24, 26]:

$$v_{i,j} = \begin{cases} 0, & \text{if} \quad p_{i,j} = 1; \\ 1, & \text{if} \quad p_{i,j} = 0. \end{cases} \qquad (11)$$

With the increase of the probability of link compromise $p_{i,j}$ from 0 to 1, the weighting coefficient $v_{i,j}$ should decrease from 1 to 0. Different variants of the functional representation of the dependence $v = f(p)$ that meet the conditions (11). The simplest case is linear functional dependence [24, 26]:

$$v_{i,j} = 1 - p_{i,j}\,. \qquad (12)$$

Using the conditions (7) ensures that the separate link utilization is determined by the probability of its compromising.

In this work, as an example, the following power function is considered:

$$v_{i,j} = 1 - p_{i,j}^{n}\,, \qquad (13)$$

where $n \ge 1$ [26].

As can be seen from Fig. 1, increasing the parameter *n* in (13) reduces the sensitivity of the load balancing to the threat to network security [26].

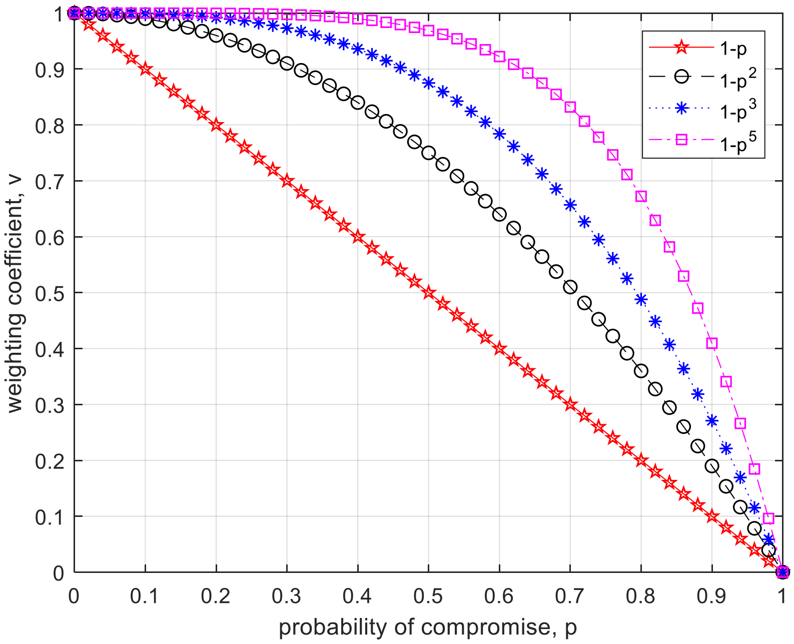

Figure 1: Models of functional dependence of weighting coefficient on the probability of compromise

As an optimality criterion of the problem solution of the network security providing based on the Traffic Engineering Fast ReRoute with support of policing the following function has been selected:

$$J = \sum_{k \in K} w_k \cdot \beta^k + \sum_{k \in K} \bar{w}_k \cdot \bar{\beta}^k + c \cdot \alpha \to \mathbf{min} \qquad (14)$$

under condition

$$w_k > \bar{w}_k > w_p > \bar{w}_p > \ldots > c\,, \qquad (15)$$

where the priority PR^k of the *k*th flow must be higher than the priority PR^p of the p^{th} flow and $c = 0.25$.

As priority values, 3 bits of IP precedence in the IP packet header can be used within the range from 0 to 7, as well as DSCP (Differentiated Services Code Point) values that vary from 0 to 63 [23].

Taking all into account, the optimality criterion (14) aimed at minimizing the conditional costs of the consistent solution of the FRR, TE, and TP technological tasks. However, conditions (7)-(11) and (13) are responsible for the load balancing the packet flows over the network links with minimum probability of compromise.

Also, should be noted that the first term in (14) determines the conditional cost of denials to maintain flows being transmitted through the primary paths. The second term is the cost of denials of servicing the flows being transmitted in the backup paths. While the third term is a weighted upper bound of the network link utilization.

3. Numerical Research of the Mathematical Model of Secure TE-FRR-TP

The analysis of the proposed approach and corresponding mathematical model of Secure TE-FRR-TP has been conducted on several network configurations for the multiple flows case with different priorities. Therefore, the main features of the model are explained in the network example shown in Fig. 2. The input data for numerical research such as link capacities and their probabilities of compromise are presented in Table 1.

Let us provide a solution of the Secure TE-FRR-TP for the case of two flows transmission using the scheme of link $E_{11,12}$ protection. Assume the following flows characteristics:

- R_1 is the source node, R_{16} is the destination node, flow intensity is changing within the range $\lambda^1 = 10 \div 1100$ 1/s, $PR^1 = 4$ is flow priority;
- R_5 – source node, R_{12} is the destination node, flow intensity is changing within the range $\lambda^2 = 10 \div 1100$ 1/s, $PR^2 = 1$ is flow priority.

For the presented example, suppose that the threshold of the upper bound of the network links utilization is α_{TH} =0.65 and power function is $v_{i,j} = 1 - p_{i,j}^2$, where $n = 2$.

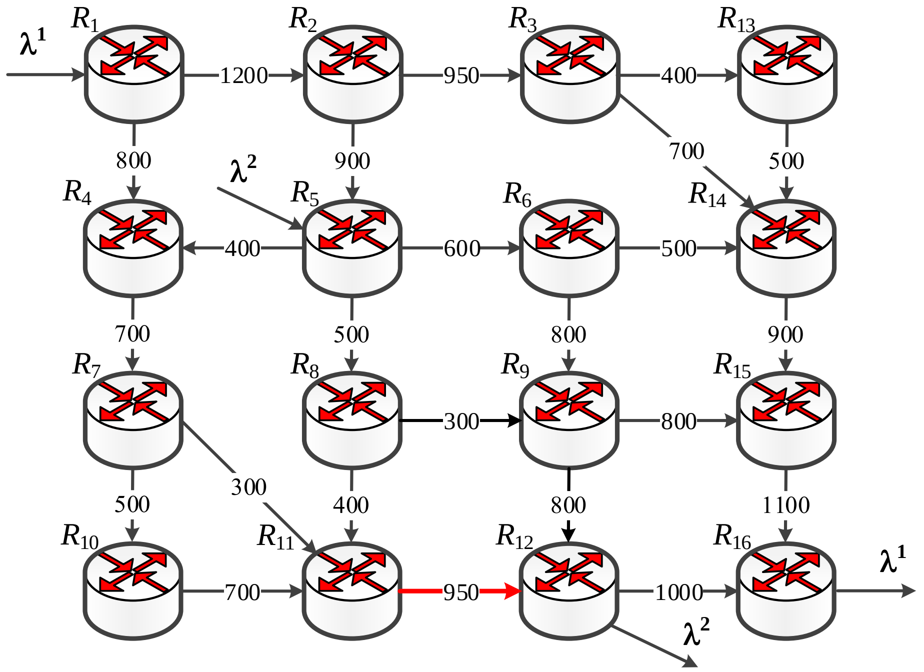

Figure 2: Network structure for numerical research

As can be seen from the results of the research presented in Fig. 3, with the increase of the network load, the upper bound of the network link utilization also gradually increased. The absence of sharp fluctuations in the values α (Fig. 3) has a positive effect on the whole network QoS. Under these conditions, at low network load, when $\lambda^1 \le 750$ 1/s and $\lambda^2 \le 590$ 1/s, the fulfillment of condition $0 \le \alpha \le \alpha_{TH}$ (10) did not cause a limitation of the intensity of the flow at the network edge and $\beta^1 = \overline{\beta}^1 = \beta^2 = \overline{\beta}^2 = 0$ (Figure 3).

Table 1

Input data for investigation the network security approach based on Traffic Engineering Fast ReRoute with support of Traffic Policing

Network Link	Capacity, 1/s	Probability of Compromise, $p_{i,j}$	Network Link	Capacity, 1/s	Probability of Compromise, $p_{i,j}$
$E_{1,2}$	1200	0.2	$E_{7,10}$	500	0.4
$E_{2,3}$	950	0.5	$E_{8,11}$	400	0.2
$E_{1,4}$	800	0.3	$E_{9,12}$	800	0.5
$E_{2,5}$	900	0.4	$E_{10,11}$	700	0.3
$E_{3,14}$	700	0.1	$E_{11,12}$	950	0.2
$E_{5,4}$	400	0.5	$E_{3,13}$	400	0.1
$E_{5,6}$	600	0.2	$E_{13,14}$	500	0.3
$E_{4,7}$	700	0.2	$E_{6,14}$	500	0.4
$E_{5,8}$	500	0.1	$E_{14,15}$	900	0.2
$E_{6,9}$	800	0.4	$E_{9,15}$	800	0.5
$E_{7,11}$	300	0.1	$E_{15,16}$	1100	0.3
$E_{8,9}$	300	0.3	$E_{12,16}$	1000	0.2

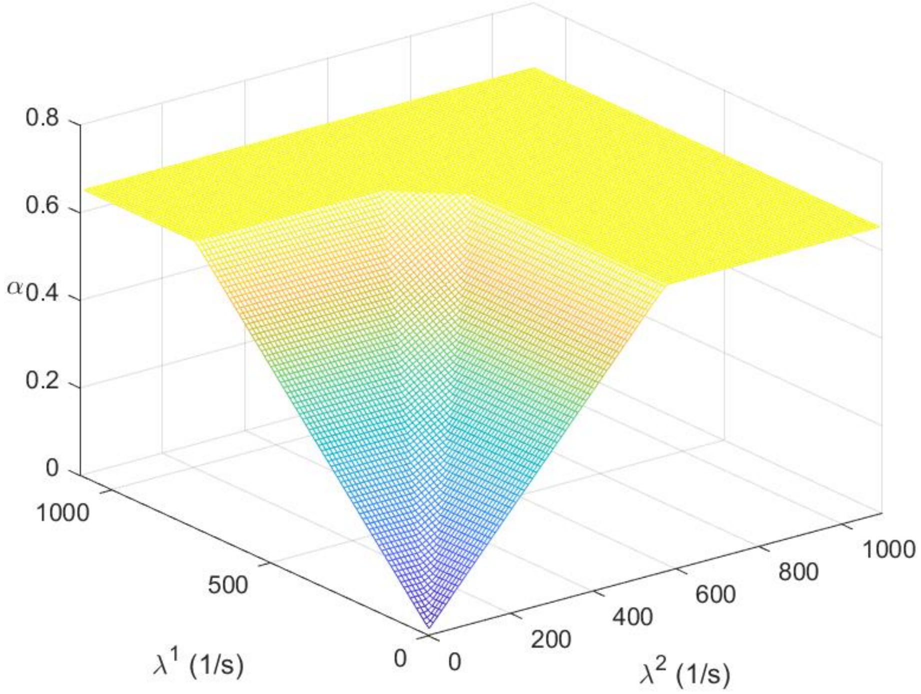

Figure 3: Dependence the upper bound of the network links utilization from the transmitted flows intensities

However, with excessive load on the network, condition (10) was met in a way when $\alpha = \alpha_{TH}$ (Fig. 3) by limiting the intensities of flows that transmitted over both the primary and backup multipath. According to Figures 3-7, traffic limitation for transmitted flows were based on the following principles:

- The limitation was applied to the flow that was the source of overload under condition (10);
- If the overload was created by several flows, the limitation primarily concerned the flow with lower priority in accordance with condition (15);
- Load balancing was performed consistent with condition (7) so that communication links with a lower probability of compromising were loaded more than less secure links.

Therefore, the study showed that with these initial data (Table 1), the first (high-priority) packet flow during the use of the primary multipath was the least limited in its intensity. In support of the above principles, the first flow was limited in the event that it created an overload of links that were part of both the primary and the backup multipath (Fig. 4 and Fig. 5).

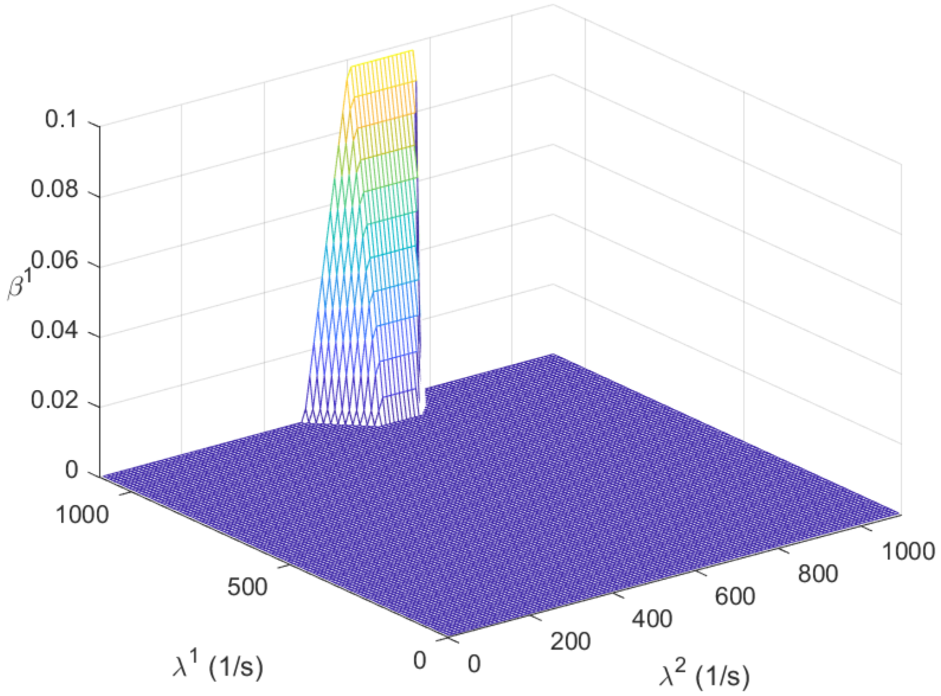

Figure 4: The solution of the Secure TE-FRR-TP problem for the first flow of packets (primary path)

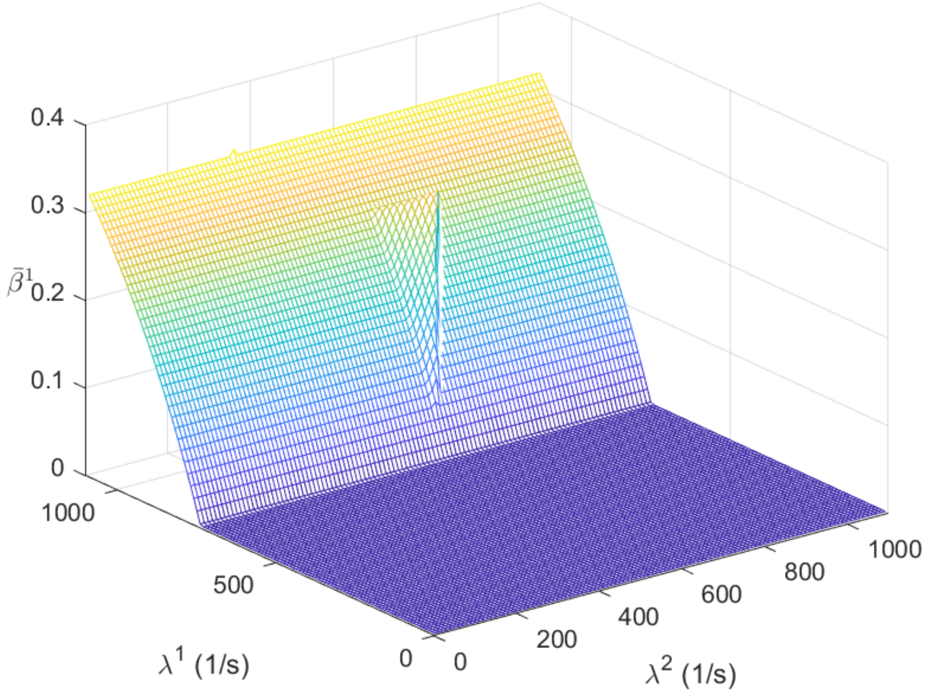

Figure 5: The solution of the Secure TE-FRR-TP problem for the first flow of packets (backup path)

However, earlier than all and with greater intensity, the second (low-priority) flow was limited when using the backup multipath (Fig. 6). Somewhat later and with less intensity, the second flow was limited when using the primary multipath (Fig. 7).

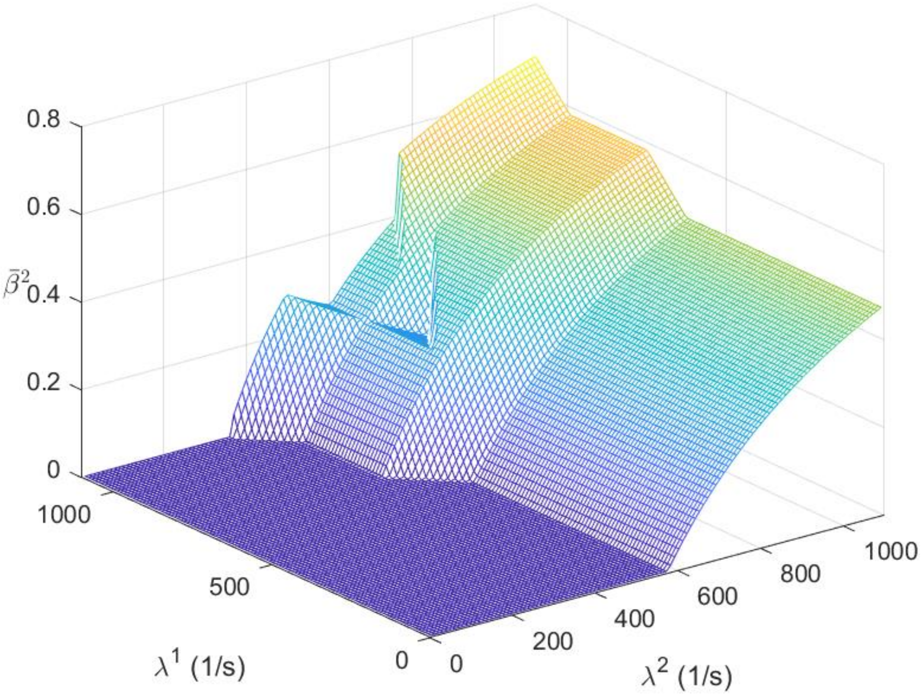

Figure 6: The solution of the Secure TE-FRR-TP problem for the second flow of packets (backup path)

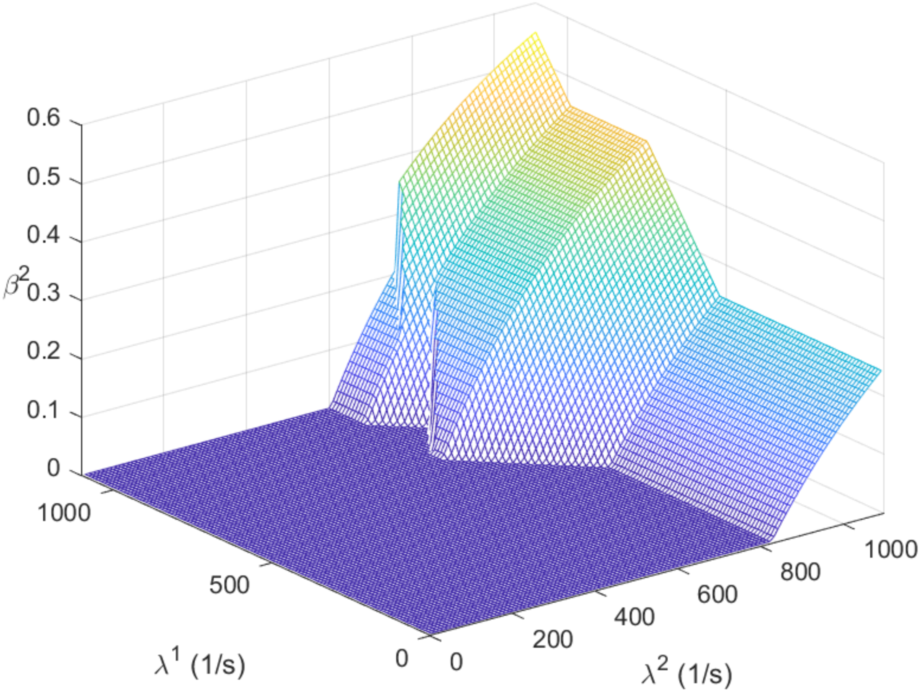

Figure 7: The solution of the Secure TE-FRR-TP problem for the second flow of packets (primary path)

4. Conclusion

In modern telecommunication networks, the operation of protocols is aimed at achieving a high level of Quality of Service, resilience, and security. Therefore, an important scientific and applied task is the adaptation of promising solutions for fault-tolerant routing (fast rerouting) with load balancing to the requirements of network security. Thus, the relevant problem is formulated and solved in the work, which is related to the development of a flow-based model of the network security providing based on Traffic Engineering Fast ReRoute with support of Policing, namely Secure TE-FRR-TP. Within this model, the problem of secure fast rerouting was presented in the form of a linear programming problem when the criterion was condition (14), and the constraints were expressions (1)–(11), (13), and (15).

The novelty of the proposed model is the modification of load balancing conditions and bandwidth protection during fast rerouting (7), which in addition to the Quality of Service, also considers the probability of compromising the link as an indicator of network security. The routing solutions obtained within the proposed model are aimed at reducing the overload of communication links with a high probability of compromising by redistributing traffic for transmission through more secure network links.

However, it should be borne in mind that the proposed solution is a compromise in solving the tasks of ensuring the Quality of Service, on the one hand, and improving fault-tolerance and network security, on the other. Implementation of schemes for the protection of structural elements of the network and its bandwidth requires the introduction of redundancy in the use (reservation) of network resources. Taking into account the network security indicators within the model (1)–(15) also leads to underloading of the most insecure communication links according to their probability of compromise. Because network resources are always limited, these measures can lead to network overload, which is accompanied by a limit on the load at its edge. The advantage of the proposed solution is that in the conditions of congestion the load balancing is realized on the principles of TE and, if necessary, differentiated limitation of the load entering the network, according to the values of IP-priority and packet flow intensity. An additional advantage of the proposed optimization model Secure TE-FRR-TP is its linearity, which focuses on the low computational complexity of its protocol implementation in practice.

5. References

[1] R. Bruzgiene, L. Narbutaite, T. Adomkus, P. Pocta, P. Brida, J. Machaj, E. Leitgeb, P. Pezzei, H. Ivanov, N. Kunicina, A. Zabasta, Quality-Driven Schemes Enhancing Resilience of Wireless Networks under Weather Disruptions, in: Rak J., Hutchison D. (Eds.), Guide to Disaster-Resilient Communication Networks, Computer Communications and Networks, Springer, Cham, 2020, pp. 299–326. doi: 10.1007/978-3-030-44685-7_12.

[2] A. Z. Dodd, The Essential Guide to Telecommunications (Essential Guide Series), Pearson, 2019.

[3] R. White, E. Banks, Computer Networking Problems and Solutions: An innovative approach to building resilient, modern networks, 1st ed., Addison-Wesley Professional, 2018.

[4] S. Gupta, Security and QoS in Wireless Sensor Networks, 1st ed., eBooks2go Inc, 2018.

[5] D. Medhi, K. Ramasamy, Network routing: algorithms, protocols, and architectures, Morgan Kaufmann, 2017.

[6] I. Strelkovskaya, I. Solovskaya, Using spline-extrapolation in the research of self-similar traffic characteristics, J. Electr. Eng. 70(4) (2019) 310–316. doi: 10.2478/jee-2019–0061.

[7] I. Strelkovskaya, I. Solovskaya, A. Makoganiuk, Spline-extrapolation method in Traffic forecasting in 5G networks, J. Telecommun. Inf. Technol. 3 (2019) 8–16. doi: 10.26636/jtit.2019.134719

[8] L. Globa, M. Skulysh, O. Romanov, M. Nesterenko, Quality Control for Mobile Communication Management Services in Hybrid Environment, in: Ilchenko M., Uryvsky L., Globa L. (Eds.), Advances in Information and Communication Technologies, volume 560 of Lecture Notes in Electrical Engineering, Springer, Cham, 2019, pp. 76–100. doi: 10.1007/978-3-030-16770-7_4.

[9] A. A. Semenov, O. O. Semenova, O. M. Voznyak, O. M. Vasilevskyi, M. Y. Yakovlev, Routing in telecommunication networks using fuzzy logic, in: 2016 17th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM), IEEE, 2016, pp. 173–177. doi: 10.1109/EDM.2016.7538719.

[10] J. Papan, P. Segec, P. Paluch, J. Uramova, M. Moravcik, The new Multicast Repair (M-REP) IP fast reroute mechanism, Concurr. Comput. Pract. Exp. 32(13) (2020). doi: 10.1002/cpe.5105.

[11] O. Lemeshko, O. Yeremenko, Enhanced method of fast re-routing with load balancing in software-defined networks, J. Electr. Eng. 68(6) (2017) 444–454. doi: 10.1515/jee-2017-0079.

[12] O. Lemeshko, O. Yeremenko, N. Tariki, Solution for the default gateway protection within fault-tolerant routing in an IP network, Int. J. Electr. Comput. Eng. Syst. 8(1) (2017) 19–26. doi: 10.32985/ijeces.8.1.3.

[13] O. Yeremenko, O. Lemeshko, A. Persikov, Secure Routing in Reliable Networks: Proactive and Reactive Approach, in: Shakhovska N., Stepashko V. (Eds.) Advances in Intelligent Systems and Computing II. CSIT 2017, volume 689 of Advances in Intelligent Systems and Computing, Springer, Cham, 2018, pp. 631–655. doi: 10.1007/978-3-319-70581-1_44.

[14] T. Gomes, L. Jorge, R. Girão-Silva, J. Yallouz, P. Babarczi, 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, Springer, Cham, 2020, pp. 429–453. doi: 10.1007/978-3-030-44685-7_17.

[15] J. Papán, P. Segeč, P. Palúch, Ľ. Mikuš, M. Moravčík, The survey of current IPFRR mechanisms, in: Janech J., Kostolny J., Gratkowski T. (Eds.), Proceedings of the 2015 Federated Conference on Software Development and Object Technologies. SDOT 2015., volume 511 of Advances in Intelligent Systems and Computing, Springer, Cham, 2015, pp. 229–240. doi: 10.1007/978-3-319-46535-7_18.

[16] R. Girão-Silva, T. Gomes, L. Martins, D. Tipper, A. Alashaikh, A centrality-based heuristic for network design to support availability differentiation, in: Proceedings of the 16th International Conference on the Design of Reliable Communication Networks DRCN 2020, IEEE, Milano, Italy, 2020, pp. 1–7, doi: 10.1109/DRCN48652.2020.1570603040.

[17] J. Rak, D. Papadimitriou, H. Niedermayer, P. Romero, Information-driven network resilience: Research challenges and perspectives, Opt. Switching Netw. 23(2) (2017) 156–178. doi: 10.1016/j.osn.2016.06.002.

[18] A. Mendiola, J. Astorga, E. Jacob, M. Higuero, A survey on the contributions of Software-Defined Networking to Traffic Engineering, IEEE Commun. Surv. Tutor. 19(2) (2017) 918–953. doi: 10.1109/COMST.2016.2633579.

[19] U. Palani, G. Amuthavalli, V. Alamelumangai, Secure and load-balanced routing protocol in wireless sensor network or disaster management, IET Inf. Secur. 14(5) (2020) 513–520. doi: 10.1049/iet-ifs.2018.5057.

[20] M. V. Patil, V. Jadhav, Secure, reliable and load balanced routing protocols for multihop wireless networks, in: Proceedings of the 2017 International Conference on Intelligent Computing and Control (I2C2) Proceedings, IEEE, 2017, pp. 1–6. doi: 10.1109/I2C2.2017.8321936.

[21] N. Kumar, Y. Singh, Trust and packet load balancing based secure opportunistic routing protocol for WSN, in: Proceedings of the 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC) Proceedings, IEEE, 2017, pp. 463–467. doi: 10.1109/ISPCC.2017.8269723.

[22] S. Li, S. Zhao, X. Wang, K. Zhang, L. Li, Adaptive and secure load-balancing routing protocol for service-oriented wireless sensor networks, IEEE Syst. J. 8(3) (2013) 858–867. doi: 10.1109/JSYST.2013.2260626.

[23] O. Lemeshko, O. Yeremenko, A.M. Hailan, M. Yevdokymenko, A. Shapovalova, Policing based traffic engineering fast ReRoute in SD-WAN architectures: approach development and investigation, in: Al-Bakry A. et al. (Eds.), New Trends in Information and Communications Technology Applications. NTICT 2020, volume 1183 of Communications in Computer and Information Science, Springer, Cham, 2020, pp. 29–43, doi: 10.1007/978-3-030-55340-1_3.

[24] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, T. Radivilova, D. Ageyev, Secure based traffic engineering model in softwarized networks, in: Proceedings of the IEEE International Conference on Advanced Trends in Information Theory ATIT, IEEE, 2020, pp. 1–4.

[25] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, A.M. Hailan, A. Mersni, Cyber resilience approach based on traffic engineering fast reroute with policing, in: Proceedings of the 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IEEE, 2019, pp. 117–122. doi: 10.1109/IDAACS.2019.8924294.

[26] O. Lemeshko, A. Shapovalova, A. M. K. Al-Dulaimi, O. Yeremenko, M. Yevdokymenko, Flow-based routing model with load balancing under network security parameters, Inf. Telecommun. Sci. 2 (2020) 44–50. doi: 10.20535/2411-2976.22020.44-50.