UDC 621.391

FLOW-BASED ROUTING MODEL WITH LOAD BALANCING UNDER NETWORK SECURITY PARAMETERS

[1]Oleksandr V. Lemeshko, [1]Anastasia S. Shapovalova, [2]Aymen Mohammed Khodayer Al-Dulaimi,
[1]Oleksandra S. Yeremenko, [1]Maryna O. Yevdokymenko

[1]Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
[2]Al-Farahidi University, Baghdad, Iraq

Background. In modern telecommunication networks, the functioning of network protocols is aimed at achieving a high level of Quality of Service and network security. Therefore, an urgent scientific and applied problem is the adaptation of routing solutions with load balancing to the requirements of network security. The novelty of the proposed model is the modification of the load balancing conditions, in which, in addition to the link bandwidth (Quality of Service indicator), the probability of its compromise (network security indicator) is also taken into account. The routing solutions obtained within the framework of the proposed model are aimed at reducing the overload of network links that have a high probability of compromise by switching traffic to more secure links.

Objective. Developing the flow-based routing model with load balancing, which takes into account the parameters of network security.

Methods. Analysis of all known publications on load balancing and network security. Synthesis of a load balancing flow-based routing model. Study of the influence of network security parameters of communication links on routing and load balancing processes.

Results. A new condition for load balancing is proposed, which is a modification of the existing Traffic Engineering solution based on accounting the network security parameters - the probabilities of compromising communication links.

Conclusions. In routing with load balancing, parameters of network security should be considered. Depending on the network state and user requirements, different models of network security parameters for load balancing processes can be used.

Keywords: routing; network; compromise; model.

Introduction

In modern telecommunication networks (TCNs), the solution of technological problems related to the provision of a given Quality of Service (QoS) and ensuring network security, as a rule, is inconsistent [1-3]. In addition, various technologies, protocols and mechanisms are used, which, as a result, does not allow to realize the maximum efficiency of network performance as a whole. For example, the introduction of additional traffic analyzers, VPN solutions, firewalls can negatively affect the TCN performance and introduce additional delays in the packet transmission across the network. On the other hand, the introduction of the latest protocols and systems for automatic network and traffic management can negatively affect the level of network security [1, 2].

Routing protocols have always been and remain an effective solution for improving the Quality of Service based on balanced loading of the TCN [2, 4]. However, the latest trend in the development of the theory and practice of routing is the implementation of the principles of so-called secure routing [5-10]. The purpose of its application in modern telecommunication networks is to ensure a fuller consideration of network security indicators related to both structural and functional parameters of the network and traffic characteristics in the traffic routing [5]. It is proved that the efficiency of a routing protocol largely depends on the type of mathematical model and calculation method underlying it. Therefore, to make the solution of problems maximally consistent in order to ensure a high level of both Quality of Service and network security, all necessary measures should be taken at the level of mathematical description of the routing process.

Overview of solutions for secure routing

The analysis of current solutions in the direction of the development of secure load-balanced routing mechanisms and protocols has been performed [6-11]. Some of the approaches are shown below.

Thus, in [7] the optimization algorithm was improved within the framework of the proposed secure load-balanced routing protocol (SLBR) together with a logical clustering technique and an efficient key management system. The SLBR protocol developed for wireless sensor networks. In turn, in [8] the LBSTAR as a reliable, secure, and load efficient routing protocol has been proposed for performance improvement in multihop wireless networks and is a further development of E-STAR protocols enhancing their functionality.

In [9] there is the trust and packet load balancing based opportunistic routing protocol (TPBOR) presented as a new trust and packet load balancing based opportunistic routing. The TPBOR uses the broadcasting abilities of wireless links, utilizes the trusted nodes for secure routing process, and provides energy efficiency.

The works [5, 11, 12] should be mentioned as the approach where the fast rerouting process based on Traffic Engineering has been used for cyber resilience improvement.

A review of the known approaches to routing [4-14] allows concluding that promising routing solutions for QoS level improvement should be based on the flow characteristics and ensure effective load balancing in the TCN. Thus, there is a relevant scientific and applied problem related to the development of a mathematical model of secure routing in the TCN, which belongs to the class of flow-based solutions and adapts the principles of load balancing to the requirements of network security.

Routing model with load balancing under network security parameters

Let the topology of MPLS network be described by the graph $G=(R,E)$, where $R=\{R_i; i=\overline{1,m}\}$ is the set of routers in the network, and $E=\{E_{i,j}; i,j=\overline{1,m}; i\neq j\}$ is the set of links. Let us denote the bandwidth of the communication link by $\varphi_{i,j}$, which is modeled by an arc $E_{i,j}$.

For an adequate analysis of load balancing processes in the TCN, a multi-flow case will be considered. Therefore, we denote that K is a set of unicast packet flows, for example, which are transmitted over the network. Then the main characteristics of k th unicast flow will include: s_k is the source router; d_k is the destination router; λ^k is the average intensity of packets of the k th flow measured in packets per second (1/s).

The result of solving the routing problem is calculation of a set of routing variables $x_{i,j}^k$. Each of these variables characterizes the proportion of the intensity of the k th flow within the link $E_{i,j}\in E$. In order to ensure effective load balancing in the TCN, it is necessary to implement the multi-path routing. Therefore, the following constraints are imposed on routing variables

$$0\le x_{i,j}^k\le 1. \qquad (1)$$

To ensure that there is no packet loss and to ensure unicast paths connectivity, route variables are also subject to constraints, which are represented by the flow conservation conditions on each specific router and in the TCN in general:

$$\begin{cases}\sum\limits_{j:E_{i,j}\in E} x_{i,j}^k-\sum\limits_{j:E_{j,i}\in E} x_{j,i}^k=0;\ k\in K,\ R_i\neq s_k,d_k;\\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k-\sum\limits_{j:E_{j,i}\in E} x_{j,i}^k=1;\ k\in K,\ R_i=s_k;\\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k-\sum\limits_{j:E_{j,i}\in E} x_{j,i}^k=-1;\ k\in K,\ R_i=d_k.\end{cases} \qquad (2)$$

Then the average intensity of the k th flow packets within the link $E_{i,j}\in E$ (1/s)) can be calculated as follows:

$$\lambda_{i,j}^k=\lambda^k x_{i,j}^k.$$

The analysis of the works devoted to load balancing in the TCN showed [11-14] that a very effective solution in this direction is to implement the provisions of the Traffic Engineering (TE) concept. This solution is based on the idea of minimizing the overloading of all communication links in the TCN during routing. This should reduce the probability of creating congested areas on the network if there are underloaded communication links. And the minimization of coefficients of utilization, which within the model (1), (2) will be determined by the formula

$$\alpha_{i,j}=\frac{\sum\limits_{k\in K}\lambda^k x_{i,j}^k}{\varphi_{i,j}}, \qquad (3)$$

always helps reduce packet delays and packet losses in these links and in the network as a whole.

In [12, 13], it is proposed to implement the formulated principle within the flow-based model (1)-(3) at the level of modification of the known condition to prevent congestion of network communication links.

$$\sum_{k \in K} \lambda^k x_{i,j}^k \le \varphi_{i,j} . \qquad (4)$$

After modification, it will take the following form:

$$\sum_{k \in K} \lambda^k x_{i,j}^k \le \alpha \varphi_{i,j} , \qquad (5)$$

where α is the additional control variable that numerically determines the upper bound of the network links utilization (3), (5) and obeys the following conditions [11-13]

$$0 \le \alpha \le 1 . \qquad (6)$$

The optimality criterion for the routing solutions that meet the requirements of the Traffic Engineering concept [13] will be the minimum of the bound α, that is

$$\min_{x,\alpha} \alpha . \qquad (7)$$

Thus, the problem of routing with load balancing according to the Traffic Engineering principles is formulated in optimization form with criterion (7) and constraints (1), (2), (5) and (6). Its solutions are aimed at ensuring optimal load balancing with minimization of utilization coefficients for each of the network communication links. To expand the functionality of the above solution for the routing problem in the direction of considering the parameters of network security in terms of load balancing (5) it is necessary to make some modifications.

In the general case, each communication link $E_{i,j} \in E$ is associated with a set of parameters that characterize its level of security. One of the most important of these parameters is the probability of link compromise, which is denoted by $p_{i,j}$. In this case, the values of these security parameters are considered to be known values and are determined by statistics on the effectiveness of the Intrusion Prevention System (IPS) installed on the routers. The main idea of the solution proposed in this paper is to ensure more intensive use of links with minimal probabilities of compromise, and vice versa – links with high $p_{i,j}$ should be loaded minimally or even completely blocked. Therefore, the improved version of the load balancing conditions (5) will look as follows:

$$\sum_{k \in K} \lambda^k x_{i,j}^k \le \alpha v_{i,j} \varphi_{i,j} , \qquad (8)$$

where in the right part of the inequation the weighting coefficient $v_{i,j}$ must meet such boundary conditions

$$v_{i,j} = \begin{cases} 0, & \text{if } p_{i,j} = 1; \\ 1, & \text{if } p_{i,j} = 0. \end{cases} \qquad (9)$$

That is, in the case of increasing the probability of compromise $p_{i,j}$ from 0 to 1, the weighting coefficient $v_{i,j}$ should decrease from 1 to 0. In this paper it is proposed to investigate the following functional dependence of weighting coefficients $v_{i,j}$ and probabilities of link compromise:

$$v_{i,j} = 1 - p_{i,j}^k , \qquad (10)$$

where $k \ge 1$ (Fig. 1).

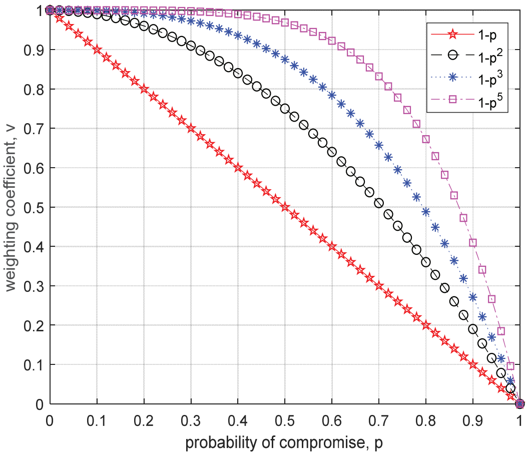

Fig.1 Variants of functional dependence of weighting coefficients $v_{i,j}$ on probabilities of communication links compromise $p_{i,j}$

As can be seen from Fig. 1, increasing the parameter k in function (10) reduces the sensitivity of the load balancing means to the network security threat. For example, the corresponding communication link will be underloaded by 10% under the condition k=5 only at $p_{i,j} = 0.63$; in the case of k=3 it will be underloaded at $p_{i,j} = 0.47$, and if *k*=1, underloading will take place at $p_{i,j} = 0.1$.

As a result of the performed modifications the problem of load balancing under network security parameters is formulated in the optimization form. Here the criterion of optimality was condition (7), and constraints were expressions (1), (2), (5) and (8). This optimization problem belongs to the class of linear programming problems, for the solution of which scientists have proposed algorithms that are quite efficient from a computational point of view [15].

Research of routing and load balancing process with under network security parameters

The study of routing and load balancing processes, organized taking into account network security indicators, is carried out in the work. As an example, the structure of the TCN has been chosen, which is presented in Fig. 2. In Fig. 2 the breaks of communication links show a fraction, in which the numerator indicates the link bandwidth, and the denominator indicates the probability of its compromise. Packets of two flows, which had intensities $\lambda^1 =$ 600 1/s and $\lambda^2 =$400 1/s, were transmitted in the network between the routers R_1 and R_{12}.

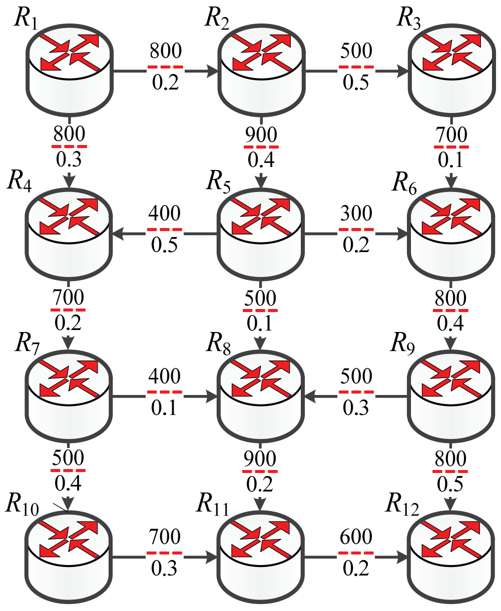

Fig.2. Investigated fragment of the network.

In the study we compared the solutions obtained using the original Traffic Engineering routing model (1), (2), (5)-(7) and the proposed model (1), (2), (5), (7), (8)-(10). The results of the calculations are given in Tables 1 and 2, which are represented by the values of flow intensities in the respective communication links ($\lambda^k_{i,j}$), as well as by the coefficients of utilization (3). Table 1 shows the results of comparison of Traffic Engineering solution and the proposed model at *k*=2.

Table 1. Comparison of Traffic Engineering and secure based Traffic Engineering solutions (*k*=2).

Link	$p_{i,j}$	Traffic Engineering solution			Secure Based Traffic Engineering solution (*k*=2)		
		$\lambda^1_{i,j}$	$\lambda^2_{i,j}$	$\alpha_{i,j}$	$\lambda^1_{i,j}$	$\lambda^2_{i,j}$	$\alpha_{i,j}$
$E_{1,2}$	0.2	292.3	323.1	0.769	346.3	362.9	0.886
$E_{2,3}$	0.5	0	307.7	0.615	346.3	0	0.693
$E_{1,3}$	0.3	307.7	76.9	0.481	253.7	37.1	0.364
$E_{2,4}$	0.4	292.3	15.4	0.342	0	362.9	0.403
$E_{3,6}$	0.1	0	307.7	0.44	346.3	0	0.495
$E_{5,4}$	0.5	0	0	0	0	0	0
$E_{5,6}$	0.2	215.4	15.4	0.769	0	121.9	0.406
$E_{4,7}$	0.2	307.7	76.9	0.549	253.7	37.1	0.416
$E_{5,8}$	0.1	76.9	0	0.154	0	241	0.482
$E_{6,9}$	0.4	215.4	323.1	0.673	346.3	121.9	0.585
$E_{7,8}$	0.1	307.7	0	0.769	253.7	0	0.634
$E_{9,8}$	0.3	0	0	0	0	0	0
$E_{7,10}$	0.4	0	76.9	0.154	0	37.1	0.074
$E_{8,11}$	0.2	384.6	0	0.427	253.7	241	0.55
$E_{9,12}$	0.5	215.4	323.1	0.673	346.3	121.9	0.585
$E_{10,11}$	0.3	0	76.9	0.11	0	37.1	0.053
$E_{11,12}$	0.2	384.6	76.9	0.769	253.7	278.1	0.886

Table 2 shows the results of comparison of solutions obtained using the proposed model at *k*=3 and *k*=5.

Table 2. Comparison of secure based Traffic Engineering solutions for *k*=3 and *k*=5.

Link	$p_{i,j}$	Secure Based Traffic Engineering solution (*k*=3)			Secure Based Traffic Engineering solution (*k*=5)		
		$\lambda^1_{i,j}$	$\lambda^2_{i,j}$	$\alpha_{i,j}$	$\lambda^1_{i,j}$	$\lambda^2_{i,j}$	$\alpha_{i,j}$
$E_{1,2}$	0.2	581.8	77.8	0.825	600	25.2	0.782
$E_{2,3}$	0.5	363.6	0	0.727	378.7	0	0.757
$E_{1,3}$	0.3	18.2	322.2	0.425	0	374.8	0.468
$E_{2,4}$	0.4	218.2	77.8	0.329	221.3	25.2	0.274
$E_{3,6}$	0.1	363.6	0	0.519	378.7	0	0.541
$E_{5,4}$	0.5	0	0	0	0	0	0
$E_{5,6}$	0.2	218.2	0	0.727	221.3	0	0.738
$E_{4,7}$	0.2	18.2	322.2	0.486	0	374.8	0.535
$E_{5,8}$	0.1	0	77.8	0.156	0	25.2	0.05
$E_{6,9}$	0.4	581.8	0	0.727	600	0	0.75
$E_{7,8}$	0.1	18.2	0	0.045	0	0	0

$E_{9,8}$	0.3	0	0	0	0	0	0
$E_{7,10}$	0.4	0	322.2	0.644	0	374.8	0.75
$E_{8,11}$	0.2	18.2	77.8	0.107	0	25.2	0.028
$E_{9,12}$	0.5	581.8	0	0.727	600	0	0.75
$E_{10,11}$	0.3	0	322.2	0.46	0	374.8	0.535
$E_{11,12}$	0.2	18.2	400	0.697	0	400	0.667

The resulting values of the upper threshold for coefficients of utilization (3), which is denoted by α^*, and the objective function of criterion (7) for all compared solutions are shown in Table 3.

Table 3. Analysis of values of α^* and α for the four compared solutions.

Comparison criteria	Traffic Engineering solution	Secure Based Traffic Engineering solution		
		k=5	k=3	k=2
α^*	0.7692	0.7815	0.8245	0.8864
α	0.7692	0.7818	0.8312	0.9234

Based on the results of the comparative analysis, a number of conclusions can be drawn.

First, the load balancing solutions obtained with the proposed model were based on adequate consideration of three main characteristics of communication links: bandwidth (QoS), probability of compromise (network security) and link location in the network topology. As a rule, those links with high bandwidth and low probability of compromise were loaded more intensively. This is clearly seen in Table 1 when the links, which had a minimum probability of compromise (0.1 or 0.2) compared to Traffic Engineering solution, had coefficients of utilization (3) that either increased (for $E_{1,2}$, $E_{3,6}$, $E_{5,8}$, $E_{8,11}$, $E_{11,12}$), or remained approximately at the previous rather high level (for $E_{5,6}$, $E_{4,7}$ and $E_{7,8}$). Most links with a high probability of compromise (from 0.3 to 0.5), such as links $E_{6,9}$, $E_{7,10}$, $E_{9,12}$ and $E_{10,11}$, began to be used less intensively, i.e. reduced their load on the indicator (3).

Second, within the proposed routing solutions when the coefficient k (from 5 to 2) in expression (10) decreased, the intensity of links utilization with a high probability of compromise decreased, and the intensity of more secured links utilization, on the contrary, increased (Tables 2 and 3). This also led to an increase in the values of α^* and α . A similar conclusion can be drawn from the results of the analysis of Table 3 when the increase in the coefficient k led to a decrease in the impact on the load balancing process for the network security parameters of communication links.

Third, the nature of the curves shown in Fig. 1 and the simulation results presented in the Tables showed a low sensitivity of routing solutions when using function (10) for small values of communication links compromise probabilities, especially at $k \geq 3$. This determines the scope of the proposed solutions in terms of threats to network security.

Conclusion

Thus, the relevant problem is formulated and solved in the work, which is related to the development of a flow-based routing model with load balancing under network security parameters. Within this model, the problem of secure routing was presented in the form of a linear programming problem when the criterion was condition (7), and the constraints were expressions (1), (2), (5) and (8).

According to the results of the study, the routing solutions obtained with the help of the proposed model take into account both the bandwidth of communication links and their security parameters represented by the probabilities of compromise when determining the order of load balancing. A comparative analysis of the obtained results showed that the use of function (10) in general adequately influenced the solution of the secure routing problem. It has been found that as k decreases during load balancing, links with a lower probability of compromise are loaded more intensively thus unloading more links that are dangerous from the point of view of communication links compromise. At $k > 5$, the influence of network security parameters, represented by low values of the probability of communication links compromise, on the process of load balancing in the TCN is significantly reduced.

References

1. Gupta S. Security and QoS in Wireless Sensor Networks // 1st Edition. eBooks2go Inc. – 2018. – 134 p.

2. Kiser Q. Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats // Kindle Edition. – 2020. – 122 p.

3. Revathi S., Geetha A. A survey of applications and security issues in software defined networking // International Journal of Computer Network and Information Security (IJCNIS). – 2017. – Vol. 9(3). – pp. 21-28. https://doi.org/10.5815/ijcnis.2017.03.03

4. Lemeshko O. V., Yevseyeva O. Y., Garkusha S. V. A tensor model of multipath routing based on multiple QoS metrics // 2013 International Siberian Conference on Control

and Communications (SIBCON) Proceedings. – 2013. – pp. 1-4. https://doi.org/10.1109/SIBCON.2013.6693645

5. Yeremenko O., Lemeshko O., Persikov A. Secure routing in reliable networks: proactive and reactive approach // Shakhovska, N., Stepashko, V. (eds.) CSIT 2017. AISC, Springer, Cham. – 2018. – Vol. 689 – pp. 631–655. https://doi.org/10.1007/978-3-319-70581-1_44

6. Shaik M. S., Mira F. A Comprehensive Mechanism of MANET Network Layer Based Security Attack Prevention // International Journal of Wireless and Microwave Technologies (IJWMT) – 2020. – Vol. 10(1). – pp. 38-47 https://doi.org/10.5815/ijwmt.2020.01.04

7. Palani U., Amuthavalli G., Alamelumangai V. Secure and load-balanced routing protocol in wireless sensor network or disaster management // IET Information Security. – 2020. – Vol. 14(5). – pp. 513-520. https://doi.org/10.1049/iet-ifs.2018.5057

8. Patil M. V., Jadhav V. Secure, reliable and load balanced routing protocols for multihop wireless networks // 2017 International Conference on Intelligent Computing and Control (I2C2) Proceedings. – 2017. – pp. 1-6. https://doi.org/10.1109/I2C2.2017.8321936

9. Kumar N., Singh Y. Trust and packet load balancing based secure opportunistic routing protocol for WSN // 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC) Proceedings. – 2017. – pp. 463-467. https://doi.org/10.1109/ISPCC.2017.8269723

10. Li S ., Zhao S., Wang X., Zhang K., Li L. Adaptive and secure load-balancing routing protocol for service-oriented wireless sensor networks // IEEE Systems Journal. – 2013. – Vol. 8(3). – pp. 858-867. https://doi.org/10.1109/JSYST.2013.2260626

11. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Hailan A. M., Mersni A. 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) Proceedings. – 2019. – Vol. 1. – pp. 117-122. https://doi.org/10.1109/IDAACS.2019.8924294.

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

13. Lemeshko O., Yeremenko O. Linear optimization model of MPLS Traffic Engineering Fast ReRoute for link, node, and bandwidth protection // 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET) Proceedings. – 2018. – pp. 1009-1013. https://doi.org/10.1109/TCSET.2018.8336365

14. Mendiola A., Astorga J., Jacob E., Higuero M. A survey on the contributions of Software-Defined Networking to Traffic Engineering // IEEE Communications Surveys & Tutorials. – 2017. – Vol. 19(2). – pp. 918-953. https://doi.org/10.1109/COMST.2016.2633579

15. Vanderbei R. J. Linear programming: foundations and extensions // Springer Nature. 2014. – Vol. 285. – 414 p.

Лемешко О.В., Шаповалова А.С., Аль-Дулаймі А.М.К., Єременко О.С., Євдокименко М.О.

Потокова модель маршрутизації з балансування навантаження з врахуванням параметрів мережної безпеки

Проблематика. В сучасних телекомунікаційних мережах функціонування мережних протоколів направлене на досягнення високого рівня якості обслуговування та мережної безпеки. Тому актуальною науковою та прикладною задачею є адаптація маршрутних рішень з балансуванням навантаження під вимоги мережної безпеки. Новизною запропонованої моделі є модифікація умов балансування навантаження, в яких крім пропускної здатності каналу (показника якості обслуговування) також враховується ймовірність його компрометації (показник мережної безпеки). Отримані в межах запропонованої моделі маршрутні рішення направлені на зменшення завантаженості каналів зв'язку, які мають високу ймовірність компрометації, шляхом перенаправлення трафіка на більш безпечні канали.

Мета досліджень. Розробка потокової моделі маршрутизації з балансування навантаження, яка враховує параметри мережної безпеки.

Методика реалізації. Аналіз всіх відомих публікацій, присвячених задачам балансування навантаження та мережної безпеки. Синтез потокової моделі маршрутизації з балансування навантаження. Дослідження впливу параметрів мережної безпеки каналів зв'язку на процеси маршрутизації та балансуванням навантаження.

Результати досліджень. Запропоновано нова умова балансування навантаження, яка є модифікацією існуючого рішення Traffic Engineering, заснованої на врахуванні параметрів мережної безпеки – ймовірностей компрометації каналів зв'язку.

Висновки. При маршрутизації з балансуванням навантаження варто враховувати параметри мережної безпеки. В залежності від стану мережі та вимог користувачів можна використовувати різні моделі впливу параметрів мережної безпеки на процеси балансуванням навантаження.

Ключові слова: маршрутизація; мережа; компрометація; модель.

Лемешко А.В., Шаповалова А.С., Аль-Дулайми А.М.К., Еременко А.С., Евдокименко М.А.

Потоковая модель маршрутизации по балансировке нагрузки с учетом параметров сетевой безопасности

Проблематика. В современных телекоммуникационных сетях функционирование сетевых протоколов направлено на достижение высокого уровня качества обслуживания и сетевой безопасности. Поэтому актуальной научной и прикладной задачей является адаптация маршрутных решений с балансировкой нагрузки под требования сетевой безопасности. Новизной предлагаемой модели является модификация условий балансировки нагрузки, в которых кроме пропускной способности канала (показателя качества обслуживания) также учитывается вероятность его компрометации (показатель сетевой безопасности). Полученные в рамках предложенной модели маршрутные решения направлены на уменьшение загруженности каналов, которые имеют высокую вероятность компрометации, путем перенаправления трафика на более безопасные каналы.

Цель исследований. Разработка потоковой модели маршрутизации с балансировкой нагрузки, которая учитывает параметры сетевой безопасности.

Методика реализации. Анализ всех известных публикаций, посвященных задачам балансировки нагрузки и сетевой безопасности. Синтез потоковой модели маршрутизации с балансировкой нагрузки. Исследование влияния параметров сетевой безопасности каналов связи на процессы маршрутизации и балансировки нагрузки.

Результаты исследований. Предложено новое условие балансировки нагрузки, которое является модификацией существующего решения Traffic Engineering, основанной на учете параметров сетевой безопасности – вероятностей компрометации каналов связи.

Выводы. При маршрутизации с балансировкой нагрузки следует учитывать параметры сетевой безопасности. В зависимости от состояния сети и требований пользователей можно использовать различные модели влияния параметров сетевой безопасности на процессы балансировки нагрузки.

Ключевые слова: маршрутизация; сеть; компрометация; модель.