UDC 621.391

RESEARCH AND DEVELOPMENT OF THE SECURE ROUTING FLOW-BASED MODEL WITH LOAD BALANCING

O. YEREMENKO, M. PERSIKOV, V. LEMESHKO, B. ALTAKI
Kharkiv National University of Radio Electronics

Abstract *– The article is devoted to developing and researching the model of secure routing with load balancing in SD-WAN-based networks. In addition, an analysis of numerical research results using Python, GEKKO Optimization Suite, and NumPy has been carried out. The technical task of secure routing with load balancing was formulated as an optimization problem with quadratic optimality criterion. Such a criterion form allows for balancing the flow shares transmitting in the network. The simulation results showed that the link load (namely, the transmitted part of the flow) under study decreases with an increased probability of the link compromise. The analysis of the calculated results revealed the value of the security and performance ratio metric when the model is most sensitive to the network link compromise probability deterioration. That is, the best sensitivity of the model to the network security indicator (compromise probability) appears when the ratio between performance and security metric takes values of 100 to 300. Therefore, the presented model of secure routing with load balancing with an additive metric that accounts for network performance and security allows using network resources more efficiently but also considers the link compromise probability in making routing decisions.*

Анотація *– Стаття присвячена розробці та дослідженню моделі безпечної маршрутизації з балансуванням навантаження в мережах на основі SD-WAN. Крім того, проведено аналіз результатів чисельних досліджень за допомогою Python, GEKKO Optimization Suite та NumPy. Технологічне завдання безпечної маршрутизації з балансуванням навантаження сформульовано у формі оптимізаційної задачі з квадратичним критерієм оптимальності. Така форма критерію дозволяє збалансувати частки потоків, що передаються в мережі. Результати моделювання показали, що досліджуване навантаження на канал зв'язку (а саме передана частина потоку) зменшується зі збільшенням імовірності компрометації каналу. Аналіз числових результатів виявив значення співвідношення метрик продуктивності та безпеки, коли модель найбільш чутлива до погіршення ймовірності компрометації каналу зв'язку мережі. Тобто найкраща чутливість моделі до показника мережної безпеки (імовірності компрометації) проявляється, коли співвідношення метрик продуктивності та безпеки приймає значення від 100 до 300. Тому представлена модель безпечної маршрутизації з балансуванням навантаження з адитивною метрикою, яка враховує продуктивність і безпеку мережі, дозволяє ефективніше використовувати мережні ресурси, але також враховує ймовірність компрометації каналу зв'язку під час прийняття маршрутних рішень.*

Introduction

Currently, deploying such network architectures as Software-Defined Wide Area Networks (SD-WAN) meets new cybersecurity threats that require specific security solutions [1-6]. In turn, approaches used for analysis include modeling and simulating network infrastructure using attributes, functionalities, operations, and behaviors to support various security analysis viewpoints, recognizing and appropriately managing associated security risks. Despite the available network infrastructure protection approaches, effectively modeling the complex behavior of interconnected network elements and configuring their protection remains challenging.

A significant problem with underlying communication networks is the dynamic nature of the network applications and their environment. It means that the Quality of Service (QoS) and security requirements of the transferred data flows can vary over time [5, 6]. Therefore, for the applications to perform securely and effectively, the underlying network should be flexible enough to dynamically change in response to application requirements and their environment changes. The novel approaches require network solutions to consider network performance and security concurrently [7-12].

Thus, a meaningful way to address this problem is through traffic management by analyzing the network state, predicting, and balancing the transmitted data load over the network resources [10, 11, 13-16]. It is a technique used to adapt the traffic routing to the changes in the network condition. However, the traditional routing techniques do not provide mechanisms to allocate network resources optimally.

To address this problem, the research community made significant efforts toward Traffic Engineering (TE) direction. It proposed new approaches to improve network robustness in response to the growth of traffic demands to QoS and network security [13-17]. Therefore, the joint solutions under load balancing and network security reduce service degradation due to congestion and network elements compromising.

The presented work aims to develop and analyze the model of secure routing with load balancing in the core networks. Therefore, Section I is devoted to a mathematical flow-based model of secure routing with load balancing. Section II contains the modeling results, behavior, and evaluation of the secure routing with load balancing model in the network core.

I. Mathematical Flow-Based Model of Secure Routing with Load Balancing

Within the model, let it be assumed that the following inputs are known [19]:

- n – number of links in the network;
- m – number of nodes in the network;
- s – source node;
- d – destination node;
- (i, j) – network link;
- $c_{i,j}$ – link capacity;
- $p_{i,j}$ – link compromise probability;
- $f_{i,j}^{OSPF}$ – link metric based on performance (link capacity);
- $f_{i,j}^{SEC}$ – link metric based on security parameter (compromise probability);
- r – flow rate arriving at the network (packets per second, pps);
- $x_{i,j}$ – fraction of the flow in the network link between the ith and jth nodes.

Task list for the research and numerical study:

- determine the multipath from the source node to the destination via network links being modeled that is the best within the selected metric;
- construct the dependence of the flow distribution over the paths under the secure routing with load balancing on the ratio between performance and security metrics and link compromise probability.

Let us describe the secure multipath routing with load balancing in the network core task. Then the number of network links n determines the vector $\vec{x}$ dimension, the coordinates $x_{i,j}$ of which characterize the fraction of the flow in the communication link between the *i*th and *j*th nodes. The metric vectors $\vec{f}^{OSPF}$ and $\vec{f}^{SEC}$ dimensions also correspond to the number of network links n. The coordinates $f_{i,j}^{OSPF}$ and $f_{i,j}^{SEC}$ characterize the metric of the link (i,j) between the *i*th and *j*th nodes based on performance (bandwidth) and security (compromise probability). The vector $\vec{x}$ coordinates are subject to the following restrictions in order to implement a multipath routing strategy [1, 15]:

$$0 \le x_{i,j} \le 1,\ i,j = \overline{1,m},\ i \ne j. \tag{1}$$

i.e., the variables $x_{i,j}$ take values from 0 to 1.

The physical meaning of variables (1) determines the possibility of the flow distribution over the network paths, i.e., packets can be transmitted over one or multiple routes.

While solving the routing problem, it is necessary to ensure the fulfillment of the flow conservation conditions for every node and the whole network [14]:

$$\begin{cases} \sum\limits_{j:(i,j)} x_{i,j} - \sum\limits_{j:(i,j)} x_{j,i} = 1 \textit{ for source node;} \\ \sum\limits_{j:(i,j)} x_{i,j} - \sum\limits_{j:(i,j)} x_{j,i} = 0 \textit{ for transit nodes;} \\ \sum\limits_{j:(i,j)} x_{i,j} - \sum\limits_{j:(i,j)} x_{j,i} = -1 \textit{ for destination node.} \end{cases} \tag{2}$$

Let each network link (i,j) will be assigned a metric used in analogy to the OSPF protocol, i.e.,

$$f_{i,j}^{OSPF} = \frac{10^8}{c_{i,j}} \tag{3}$$

where $c_{i,j}$ is the link (i,j) capacity (bandwidth).

While the security-based metric will be determined considering the link (i,j) compromise probability:

$$f_{i,j}^{SEC} = \frac{10^8}{R} p_{i,j} \tag{4}$$

where the ratio between performance and security metrics weighting coefficients R is defined as follows:

$$R = \frac{w^{OSPF}}{w^{SEC}} \tag{5}$$

where $w^{OSPF} = 10^8$.

Then security metric weighting coefficient is obtained as:

$$w^{SEC} = \frac{w^{OSPF}}{R} = \frac{10^8}{R}. \tag{6}$$

In addition to the flow conservation conditions (2), it is necessary to meet the overload prevention conditions for every (i,j) link [1]:

$$r \cdot x_{i,j} \le c_{i,j},\ i,j = \overline{1,m},\ i \ne j. \tag{7}$$

Within the work, the quadratic optimality criterion regarding the routing variables $x_{i,j}$ will be used to implement secure routing with load balancing:

$$J = \min_x \sum_{(i,j)} \left(f_{i,j}^{OSPF} + f_{i,j}^{SEC} \right) \cdot x_{i,j}^2. \tag{8}$$

Therefore, the technical task of secure routing with load balancing is formulated as an optimization problem with constraints (1)-(7) and quadratic optimality criterion (8). The quadratic form allows for balancing the flow shares transmitting in the network.

Within the numerical study, the Python GEKKO Optimization Suite solves the multipath routing optimization problem when several conditions are presented as constraints on equations and inequalities [13-17].

II. Numerical Study of Secure Routing with Load Balancing Mathematical Model

Fig. 1 demonstrates the structure of the network under study. The investigated network characteristics are as follows:

- $n = 6$ – number of links in the network;
- $m = 5$ – number of nodes in the network;
- s – source node is node #1;
- d – destination node is node #5.

Additionally, with every network link (i,j) the following parameters are associated (Table 1):

- $c_{i,j}$ – link bandwidth;
- $p_{i,j}$ – link compromise probability.

The link bandwidth and compromise probability values are shown in link gaps as a fraction (Fig. 1). The nominator is the link capacity, and the denominator is the link compromise probability.

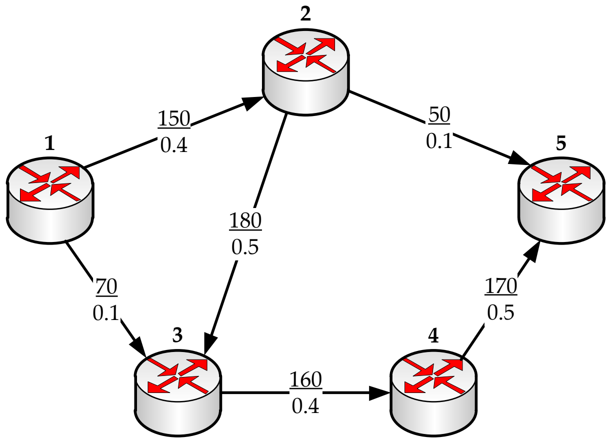

Fig. 1. Structure of the IoT-enabled critical infrastructure network core under study

Table 1. Initial data for numerical research

Link	Bandwidth (pps)	Compromise probability
1→2	150	0.4
1→3	70	0.1
2→3	180	0.5
2→5	50	0.1
3→4	160	0.4
4→5	170	0.5

Within the network structure, the three paths (routes) can be distinguished, namely:

- Path #1: 1→2→5;
- Path #2: 1→3→4→5;
- Path #3: 1→2→3→4→5.

Suppose that the flow with the rate r = 150 pps is transmitted between the first and fifth nodes. While the ratio between performance and security metrics weighting coefficients R varies from 1 to 1000, as shown in Table 2.

Table 2. The flow distribution under the secure routing with load balancing mathematical model (r = 150 pps)

R	1000	600	500	300	100	50	1
Path #1 flow rate, pps	50	50	50	50	50	50	50
Path #2 flow rate, pps	60.5	61.7	62.3	64.4	70	70	70
Path #3 flow rate, pps	39.5	38.3	37.7	35.6	30	30	30

Application of the model (1)-(7) and quadratic optimality criterion (8) for solving the problem of secure routing with load balancing is demonstrated in Table 2. In this case, the flow is distributed among all three paths. The corresponding flow rates for every path and *R* value are also indicated in Table 2.

Let us describe the Python scripts with the Python GEKKO Optimization Suite application responsible for solving the optimization problem (1)-(8).

Firstly, the Python GEKKO Optimization Suite must be installed:

```
pip install gekko
```

Then the initial input data for the numerical study is entered according to the following code snippet:

```
from array import *
from gekko import GEKKO
import numpy as np
# Initialize Model
m = GEKKO()
# c - links capacities
c=[150,70,180,50,160,170]
# c - links compromise probabilities
p=[0.4,0.1,0.5,0.1,0.4,0.5]
# r - flow rate
r=m.Param(value=150)
```

Next, the metrics calculation is performed considering the *R* value entered, as well as routing variables initialization:

```
# f1 - performance metric
# f2 - security metric
R = float(input('Ratio: '))
f_sec = (10**8)/R
f1 = [(10**8)/c[0], (10**8)/c[1], (10**8)/c[2], (10**8)/c[3], (10**8
)/c[4], (10**8)/c[5]]
f2 = [f_sec*p[0], f_sec*p[1], f_sec*p[2], f_sec*p[3], f_sec*p[4], f_
sec*p[5]]
# initialize variables
x1,x2,x3,x4,x5,x6 = [m.Var(lb=0, ub=1) for i in range(6)]
# initial values
x1.value = 0
x2.value = 0
x3.value = 0
x4.value = 0
x5.value = 0
x6.value = 0
```

The flow conservation (2) and overload prevention (7) conditions are implemented as follows:

```
# Equations
m.Equation(x1+x2==1)
m.Equation(x1-x3-x4==0)
m.Equation(x2+x3-x5==0)
m.Equation(x5-x6==0)
m.Equation(x4+x6==1)
m.Equation(r*x1<=c[0])
m.Equation(r*x2<=c[1])
m.Equation(r*x3<=c[2])
m.Equation(r*x4<=c[3])
m.Equation(r*x5<=c[4])
m.Equation(r*x6<=c[5])
```

Finally, the optimization problem solving is performed as:

```
# Objective
m.Minimize((f1[0]+f2[0])*(x1**2)+(f1[1]+f2[1])*(x2**2)+(f1[2]+f2[2])
*(x3**2)+(f1[3]+f2[3])*(x4**2)+(f1[4]+f2[4])*(x5**2)+(f1[5]+f2[5])*(x6**2
))
# Solve simulation
m.options.IMODE = 3  # LP solver
m.solve()
```

The following code presents the resulting solution output:

```
# Results
print('')
print('Results')
print('x1: ' + str(x1.value))
print('x2: ' + str(x2.value))
print('x3: ' + str(x3.value))
print('x4: ' + str(x4.value))
print('x5: ' + str(x5.value))
print('x6: ' + str(x6.value))
print('')
print('Flow rates in links')
xx = [x1.value[0],x2.value[0], x3.value[0], x4.value[0], x5.value[0]
, x6.value[0]]
xx = np.array(xx)
rr = int(r.value[0])
yy = rr*xx
print('y1: ' + str(yy[0]))
print('y2: ' + str(yy[1]))
print('y3: ' + str(yy[2]))
print('y4: ' + str(yy[3]))
print('y5: ' + str(yy[4]))
print('y6: ' + str(yy[5]))
```

Fig. 2 demonstrates the visualization of the secure routing with load balancing problem solving under the $r = 150$ pps shown in Table 2.

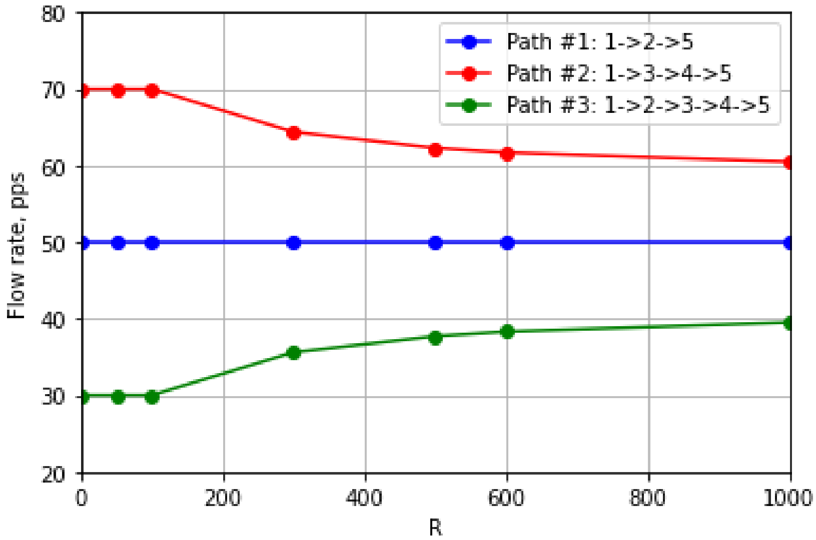

Fig. 2. The flow distribution over the paths under the secure routing with load balancing (r = 150 pps, R=1÷1000)

After decreasing the flow rate to r = 30 pps, the following flow distribution has been obtained (Table 3).

Table 3. The flow distribution under the secure routing with load balancing mathematical model (r = 30 pps)

R	1000	600	500	300	100	50	1
Path #1 flow rate, pps	12.8	13.1	13.2	13.7	15.4	16.8	19.8
Path #2 flow rate, pps	11.5	11.6	11.7	12	13	13.2	10.2
Path #3 flow rate, pps	5.7	5.3	5.1	4.3	1.6	0	0

In turn, Fig. 3 demonstrates the visualization of the secure routing with load balancing problem solving under the r = 30 pps shown in Table 3.

Analysis of the obtained results (Table 2 and Table 3) show that if the flow rate and consequently network load are low (r = 30 pps), then only two routes are used within the multipath in a case of low values of the ratio (R = 1, R = 50):

- Path #1: 1→2→5;
- Path #2: 1→3→4→5.

In the case of the high flow rate (r = 150 pps), all the routes are used in the multipath.

The following numerical results were obtained for the case when the compromise probability $p_{2,3}$ of the (2,3) link varied from 0.1 to 0.8. Table 4. demonstrates the model behavior for this input parameter. Also, R changed within the range from 100 to 1000.

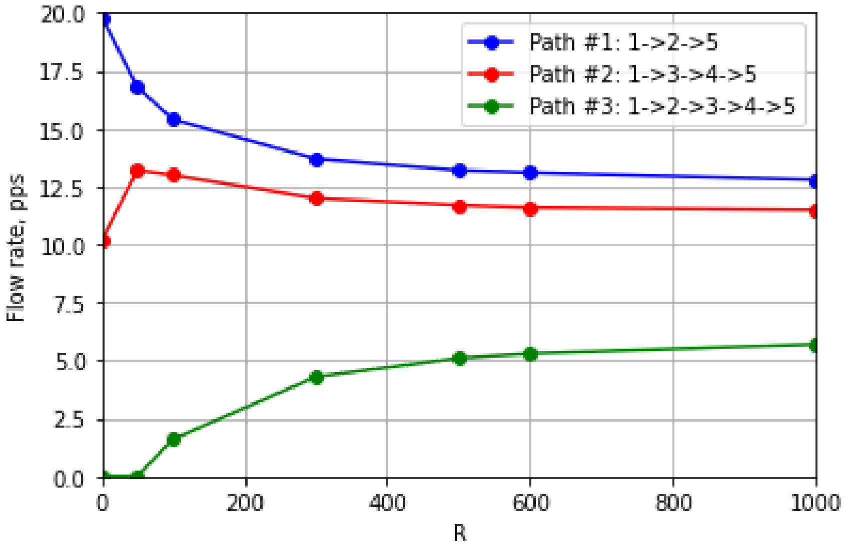

Fig. 3. The flow distribution over the paths under the secure routing with load balancing (r = 30 pps, R=1÷1000)

Table 4. The dynamics of changes in the flow distribution in the multipath depending on the parameter R and the link compromise probability $p_{2,3}$

R	1000		500		300		100	
$p_{2,3}$	0.1	0.8	0.1	0.8	0.1	0.8	0.1	0.8
Path #1 flow rate, pps	21.3	21.5	22	22.1	22.6	22.9	25.6	25.8
Path #2 flow rate, pps	19	19.2	19.3	19.7	19.7	20.2	21.3	21.8
Path #3 flow rate, pps	9.6	9.3	8.7	8.2	7.7	6.9	3.1	2.4

Therefore, the simulation results showed that the link (2,3) load (the transmitted part of the flow) under study decreases with an increased link compromise probability. In addition, the best sensitivity of the model to the $f_{i,j}^{SEC}$ security metric appears when the R ratio takes values of 100 to 300.

In turn, Table 5 and Fig. 4 present the model behavior for the case when r = 50 pps, R = 300, $p_{2,3} = 0.1 \div 0.8$. Numerical calculations have shown a decrease in the share of the flow in the link (2,3) if its compromise probability increases.

Thus, a numerical study of the secure routing with load balancing model in SD-WAN infrastructure network core was conducted. The analysis of the calculated results revealed the value of the security and performance ratio metric when the model is most sensitive to the network link compromise probability deterioration.

Table 5. The flow distribution under the secure routing with load balancing mathematical model ($r = 50$ pps, $R = 300$, $p_{2,3} = 0.1 \div 0.8$)

$p_{2,3}$	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8
Path #1 flow rate, pps	22.6	22.66	22.71	22.76	22.80	22.85	22.89	22.9
Path #2 flow rate, pps	19.7	19.77	19.84	19.91	19.99	20.05	20.12	20.2
Path #3 flow rate, pps	7.7	7.57	7.45	7.33	7.21	7.10	6.99	6.9

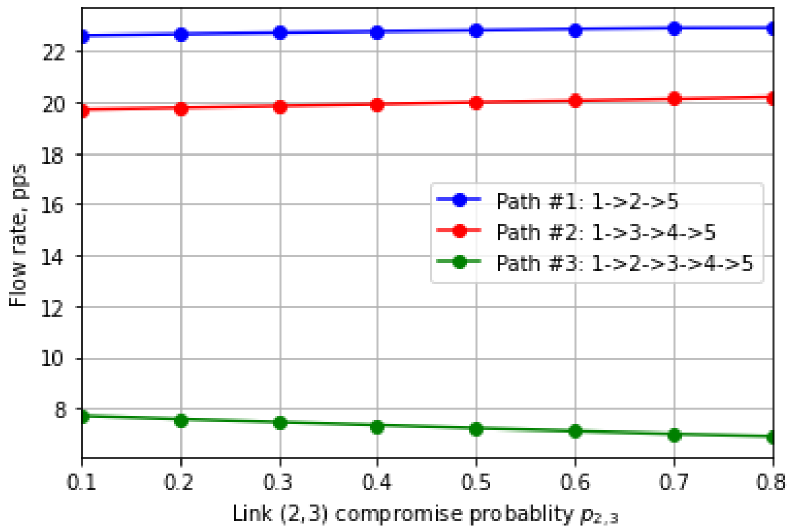

Fig. 4. The flow distribution over the paths under the secure routing with load balancing ($r = 50$ pps, $R = 300$, $p_{2,3} = 0.1 \div 0.8$)

Conclusions

This work is devoted to developing and researching the model of secure routing with load balancing in SD-WAN-based networks. In addition, an analysis of numerical research results using Python, GEKKO Optimization Suite, and NumPy has been carried out.

Hence, the technical task of secure routing with load balancing is formulated as an optimization problem with constraints (1)-(7) and quadratic optimality criterion (8). The quadratic form allows for balancing the flow shares transmitting in the network.

The simulation results showed that the link load (namely, the transmitted part of the flow) under study decreases with an increased probability of the link compromise. The analysis of the calculated results revealed the value of the security and performance ratio metric when the model is most sensitive to the network link compromise probability deterioration. That is the best sensitivity of the model to the $f_{i,j}^{SEC}$ security metric appears when the R ratio takes values of 100 to 300.

Therefore, the presented model of secure routing with load balancing with an additive metric that accounts for network performance and security allows using network resources more efficiently but also considers the link compromise probability in making routing decisions.

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. **DOI**: https://doi.org/10.30837/978-966-659-282-1

2. *Gooley, J., Yanch, D., Schuemann, D., Curran, J.* (2020), Cisco Software-Defined Wide Area Networks: Designing, Deploying and Securing Your Next Generation WAN with Cisco SD-WAN, Cisco Press, 608 p.

3. *Stallings, W.* (2016), Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 768 p.

4. *Kiser, Q.* (2020), 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, Primasta, 242 p.

5. *Gupta, S.* (2018), Security and QoS in Wireless Sensor Networks, eBooks2go Inc, 134 p.

6. *Revathi, S., Geetha, A.* (2017), "A survey of applications and security issues in software defined networking", International Journal of Computer Network and Information Security (IJCNIS), No. 9(3), P. 21-28.

7. *Li, J., Yang, Z., Yi, X., Hong, T., Wang, X.* (2018), "A Secure Routing Mechanism for Industrial Wireless Networks Based on SDN", Proceedings of the 2018 14th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), Shenyang, China, 06-08 December, P. 158-164. **DOI**: https://doi.org/10.1109/MSN.2018.000-2

8. *Diwan, D., Narang, V.K., Singh, A.K.* (2017), "Security Mechanism in RIPv2 EIGRP and OSPF for Campus Network", Computer Science Trends and Technology, No. 5(2), P. 399-404.

9. *Palani, U., Amuthavalli, G., Alamelumangai, V.* (2020), "Secure and load-balanced routing protocol in wireless sensor network or disaster management", IET Information Security, No. 14(5), P. 513-520. **DOI**: https://doi.org/10.1049/iet-ifs.2018.5057

10. *Patil, M. V., Jadhav, V.* (2017), "Secure reliable and load balanced routing protocols for multihop wireless networks", Proceedings of the 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India, 23-24 June, P. 1-6. **DOI**: https://doi.org/10.1109/I2C2.2017.8321936

11. *Kumar, N., Singh, Y.* (2017), "Trust and packet load balancing based secure opportunistic routing protocol for WSN", Proceedings of the 2017 4th International Conference on Signal Processing Computing and Control (ISPCC), Solan, India, 21-23 September, P. 463-467. **DOI**: https://doi.org/10.1109/ISPCC.2017.8269723

12. *Snihurov, A., Chakrian, V.* (2015), "Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters", Scholars Journal of Engineering and Technology, No. 3(8), P. 707-714.

13. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Hailan, A.M., Mersni, A.* (2019), "Cyber resilience approach based on traffic engineering fast reroute with policing", Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and

Advanced Computing Systems: Technology and Applications (IDAACS), No. 1, Metz, France, 18-21 September, P. 117-122. **DOI**: https://doi.org/10.1109/IDAACS.2019.8924294

14. *Yeremenko, O. S., Lemeshko, O. V., Tariki, N.* (2017), "Fast ReRoute scalable solution with protection schemes of network elements", Proceedings of the 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), Kyiv, Ukraine, 29 May - 02 June, P. 783-788. **DOI**: https://doi.org/10.1109/UKRCON.2017.8100353

15. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Lemeshko, V., Persikov, M.* (2021), "Analysis of Secure Routing Processes Using Traffic Engineering Model", Proceedings of the 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, 22-25 September, P. 951-955. **DOI**: https://doi.org/10.1109/IDAACS53288.2021.9660980

16. *Lemeshko, O., Yeremenko, O., Shapovalova, A., Hailan, A. M., Yevdokymenko, M., Persikov, M.* (2021), "Design and Research of the Model for Secure Traffic Engineering Fast ReRoute under Traffic Policing Approach," Proceedings of the 2021 IEEE 16th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), 2021, Lviv, Ukraine, 22-26 February, P. 23-26. **DOI**: https://doi.org/10.1109/CADSM52681.2021.9385253

17. *Chhaytli A., Persikov M.* (2021), "Providing cyber resilience in software-defined networks by secure routing means", Infocommunication technologies and electronic engineering, No.1(1), P. 11-19. **DOI**: https://doi.org/10.23939/ictee2021.01.011