Investigation of the Secure Paths Set Calculation Approach Based on Vulnerability Assessment

Maryna Yevdokymenko[1], Oleksandra Yeremenko[2], Anastasiia Shapovalova[3], Maryna Shapoval[4], Volodymyr Porokhniak[5], and Natalja Rogovaya[6]

[1,2,3,4,5]*Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, 61166, Ukraine*
[6]*Poltava University of Economics and Trade, 3, Koval St., Poltava, 36000, Ukraine*

Abstract
An approach to the calculation of secure paths based on the routing model taking into account information security risks using the basic vulnerability criticality metrics is proposed and investigated. The approach for calculating route metrics uses obtained expressions, which characterize the information security risk in network links in the case of existing vulnerabilities. The results of the investigation showed that within the approach of calculating secure paths with increasing packet traffic, the paths in the network that contained links with the lowest weights, i.e. had the least weight of compromise, were loaded first. The transmission of the packet flow after overloading the more secure path was carried out in the following paths according to the values of the weights of the communication links. The paths in the network that contained the links with the highest weights were loaded last.

Keywords [1]
Infocommunication network, secure path, information security risks, vulnerability, base score

1. Introduction

Today the task of information security of infocommunication networks (ICN) in conditions of increasing number of attacks and intrusions is relevant. This is due to the fact that the construction of secure networks in the constant development of infocommunication technologies and, consequently, the growing number of heterogeneous attacks is unfortunately not possible and requires constant implementation of protection mechanisms at all levels of the Open Systems Interconnection model (OSI). The “bottleneck” is the rapid response to emerging intrusions and minimizing the spread of network attacks and the resulting damages. The successful conduct of information security violations of ICN can be caused by many reasons: from the presence of vulnerabilities in the operating systems of network equipment to the incorrect hardware and software configurations when configuring protection mechanisms, and so on. In this regard, information on the network it is necessary to transmit along more secure paths.

Therefore, special attention should be paid to ICN protection methods that are used at the network level, such as traffic analyzers, Virtual Private Network (VPN), firewalls, intrusion prevention and detection systems, countermeasures systems and others, including the use of secure routing protocols, thanks to which it is possible improve security in ICN [1-8].

As a result of the analysis of existing protocol solutions (SEAD, SRP, SAODV, SLSP, ARIADNE) [9-20], it is noted that improving the efficiency of secure routing solutions usually requires appropriate improvement of existing and development of new mathematical models and methods based on adequate

MoMLeT+DS 2021: 3rd International Workshop on Modern Machine Learning Technologies and Data Science, June 5, 2021, Lviv-Shatsk, Ukraine

EMAIL: maryna.yevdokymenko@ieee.org (M. Yevdokymenko); oleksandra.yeremenko.ua@ieee.org (O. Yeremenko); anastasiia.shapovalova@nure.ua (A. Shapovalova); maryna.shapoval@nure.ua (M. Shapoval), volodymyr.porokhniak@nure.ua (V. Porokhiak); nataljarogovaja35@gmail.com (N. Rogovaya)
ORCID: 0000-0002-7391-3068 (M. Yevdokymenko); 0000-0003-3721-8188 (O. Yeremenko); 0000-0003-0701-1282 (A. Shapovalova); 0000-0002-2937-7288 (M. Shapoval); 0000-0003-2924-0369 (V. Porokhiak); 0000-0002-5189-9058 (N. Rogovaya)

consideration of information about the state of ICN: network topology, flow characteristics, bandwidth and network security indicators of elements (nodes and links).

To address the shortcomings and corresponding further improvement protocols and secure routing models formulated the following requirements:

- taking into account the features of the structural and functional construction of the ICN;
- support of the flow-based nature of various types of traffic;
- taking into account the security parameters of both individual network elements and the ICN as a whole;
- taking into account the information security risks based on existing and identified vulnerabilities on network elements;
- redirect traffic to more secure paths;
- support of recommended quality of service indicators;
- acceptable computational complexity and scalability of final solutions for further protocol implementations.

Based on the above requirements, an urgent task arises to develop and investigate secure paths set calculation approach based on a routing model. At the same time, the calculation of secure paths is based on the methodology for assessing information risks through the criticality of vulnerabilities that are present on network nodes.

The method of assessing information security risks using basic metrics for criticality of network node vulnerabilities was chosen because to assess the spread of an attack in the infocommunication network it is necessary to understand the cause of the attack, as a result of exploiting an existing vulnerability in the network, and possible damage.

When analyzing the existing solutions [21-23] for vulnerability assessment and subsequent damage, it was found that their main drawback is their narrow focus on certain network elements, individual applications, services and resources. As a result, it is difficult to assess the risks in the network as a whole. Based on this, the paper proposes to assess vulnerabilities at the level of network elements.

2. Secure Paths Set Calculation Approach Based on Vulnerability Assessment

The proposed approach based on a routing model, in which the network structure is described by the graph $G = (R, E)$, where $R = \{R_i; i = \overline{1,m}\}$ is a set of vertices simulated by routers and $E = \{E_{i,j}; i,j = \overline{1,m}, i \neq j\}$ the set of edges representing communication links in the ICN [24-27]. Then each edges $E_{i,j} \in E$ is matched to its bandwidth $\varphi_{i,j}$(1/s).

Let a set of packet flows K circulate in the ICN, which are generated by the respective network applications. For each kth flow the following initial data are known:

λ^k is the average intensity of kth flow, which is measured in packets per second (1/s);

s_k and d_k is the source and destination nodes of packets of the kth flow, respectively.

Then the order of routing in the network is determined by route variables $x_{i,j}^k$ each of which characterizes the portion of the kth flow in the link between the ith and jth nodes (routers) of the network.

Based on the physical content of the used route variables, depending on the implemented routing strategy, the conditions of the form are imposed on them.

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

or

$$0 \leq x_{i,j}^k \leq 1. \tag{2}$$

The introduction of condition (1) is responsible for the implementation of a single path routing simultaneous use of single path solutions), in which variables $x_{i,j}^k$ can take the extreme of their possible values – zero or one (1).

In addition, the flow conservation conditions are introduced for the routing variables:

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

If conditions (3) are met, the absence of packet loss on each router and in the network as a whole is guaranteed, and the connectivity of the calculated routes between the source and the destination nodes of the packets of the kth flow is ensured.

To prevent congestion of ICN communication links, the following conditions need to be met [28]:

$$\sum_{k\in K} \lambda^k x_{i,j}^k \leq \varphi_{i,j},\ \ E_{i,j}\in E. \tag{4}$$

The number of conditions (4) corresponds to the number of communication links in the network.

To assess information security risks, the following conventions are additionally introduced into the model. $U = \{U_i^q; q = \overline{1,Q},\ i = \overline{1,m}\}$ is a set of vulnerabilities that are detected on the nodes (routers) of the ICN, where U_i^q is the qth vulnerability on the ith node; $U_i^* \in U$ is the set of vulnerabilities on the ith node of the ICN; BS_i^q is the criticality index of the qth vulnerability on the ith node, calculated using the basic metrics of the vulnerability assessment system, which are presented in the recommendation NIST CVSS v3.1 [28], and characterizes the contingent damages from the use of the vulnerability U_i^q by the attacker; P_i^q is the probability of exploiting the qth vulnerability by an attacker on the ith node of the network, which in physical terms is the probability of compromise.

The Common Vulnerability Assessment System (CVSS) is widely accepted as the primary method for assessing the criticality of software vulnerabilities. Because it is not possible to effectively manage what cannot be measured as an industry standard, CVSS provides accurate measurements. The system allows users to see the main characteristics of the vulnerability and quantitative models for the formation of scores that were used in it. CVSS manages to assess vulnerabilities in terms of their criticality. It consists of three metrics: basic, temporal and user environment [28].

Each group consists of a set of indicators. Base score metrics determine the criticality of a vulnerability. Thus, each of the vulnerability indicators must be evaluated against the vulnerable component, and reflect the properties that lead to a successful attack.

Then to calculate the information security risk based on exploiting of existing vulnerabilities on the ith node of the ICN used the following expression:

$$R^i = \sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q. \tag{5}$$

To calculate base score metrics, an equation is used to weigh the relevant metrics and make an estimate (0 to 10) based on a series of measurements and assessments by security experts, with a score of 10 being the most vulnerable. In particular, when base values are assigned values, the base equation calculates a score between 0 and 10, and creates a vector.

According to the NIST recommendation, damage on basic vulnerability metrics at network nodes [28] are calculated as

$$BS_i^q = (0{,}6 \cdot Imp_i^q + 0{,}4 \cdot Ex_i^q - 1{,}5) \cdot f(Imp_i^q) \tag{6}$$

where $Imp_i^q$is the potential damage from the use of the qth vulnerability by an attacker on the ith node of the network; Ex_i^q is the complexity of exploiting the qth vulnerability by an attacker on the ith node 0on a network node.

Thus, the potential damage from the use of the vulnerability is calculated as [28]:

$$Imp_i^q = 10{,}41\left[1 - \left(1 - Conf_i^q\right) \cdot (1 - Int_i^q\right) \cdot \left(1 - Av_i^q\right)], \tag{7}$$

where $Conf_i^q$ is the damage from violation of confidentiality of information transmitted by the network and cannot be obtained by an unauthorized, for example, external, user (attacker);
Int_i^q is the damage from violation of network integrity, characterized by modification, change and destruction of information by an unauthorized user (attacker) in the ICN;
Av_i^q is the damage from violation of network resource availability in case of exploiting the qth vulnerability on the ith node of ICN.

The values of these metrics presented in the recommendation NIST CVSS v.3 [28].

The complexity of exploiting the vulnerability is calculated using the following expression:

$$Ex_i^q = 20 \cdot Ac_i^q \cdot Au_i^q \cdot AcV_i^q, \tag{8}$$

where Ac_i^q is the indicators of vulnerability assessment, describing the complexity of access (access vector);
Au_i^q is the indicator of the vulnerability assessment system that is responsible for authentication requirements;
Au_i^q is the indicator of the vulnerability assessment system, which reflects the method of exploiting the qth vulnerability on the ith node, which is physically characterized by the "remoteness" of the attacker, i.e. the number of devices and/or access restrictions through which the attacker can reach the ith node in the ICN to attack.

These indicators are the basic metrics [28], which characterize the overall complexity of the attack in the use of a vulnerability on the ith node of the network.

The potential damage function $f(Imp_i^q)$ according to [28] takes the value 0, if there is no damage, i.e. $f\left(Imp_i^q\right) = 0$. In this case, the scenario where the potential damage is present will be considered $(Imp_i^q \neq 0)$. That is, in further calculations it is used $Imp_i^q = 1.176$.

Then to quantify the worst case scenario, the information security risk in case of compromise of the link $E_{i,j} \in E$ leaving the ith node, characterizes the following expression of exponential nature [28]:

$$R_{i,j} = w_{i,j} \cdot \ln \sum_{U_i^q \in U_i^*} e^{BS_i^q} \tag{9}$$

where $w_{i,j}$ is the weights (weight of compromise), which are used to assess the risk posed by the use of vulnerabilities on the ith node of the network. In fact, the weights $w_{i,j}$ quantitatively characterize the potential damage in the case of exploiting the existing vulnerabilities on the ith node of the network.

Note that in the case when the compromise of the link $E_{i,j} \in E$ occurs only due to the use of vulnerabilities on the ith node, then the information security risks of the node and the link are identically equal, i.e.

$$\sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q = w_{i,j} \cdot \ln \sum_{U_i^q \in U_i^*} e^{BS_i^q} \tag{10}$$

The calculation of the weights $w_{i,j}$ is based on the assumption that the communication link $E_{i,j} \in E$ will be compromised due to the compromise of the ith node, i.e. by exploiting the existing vulnerabilities on this node.

In this case, the probability of compromising the ith node depends on the presence and exploiting of vulnerabilities on it and is calculated as an information security risk.

Considering (5)–(10), the value of each of the weights $w_{i,j}$ can be calculated using the following expression:

$$w_{i,j} = \frac{\sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q}{\ln \sum_{U_i^q \in U_i^*} e^{BS_i^q}}. \tag{11}$$

To calculate secure paths, the following linear optimality criterion was chosen [29]:

$$\sum_{k \in K} \sum_{E_{i,j} \in E} w_{i,j} x_{i,j}^k \Rightarrow min, \tag{12}$$

where weights $w_{i,j}$ are route metrics that have to take into account the basic security characteristics of links.

3. Investigation of the Secure Paths Set Calculation Approach Based on Vulnerability Assessment

The investigation of the proposed approach flow model of secure routing for confirmation of its efficiency and adequacy of the received results of calculation is carried out. Within the calculation example, the structure of the infocommunication network shown in Fig. 1.

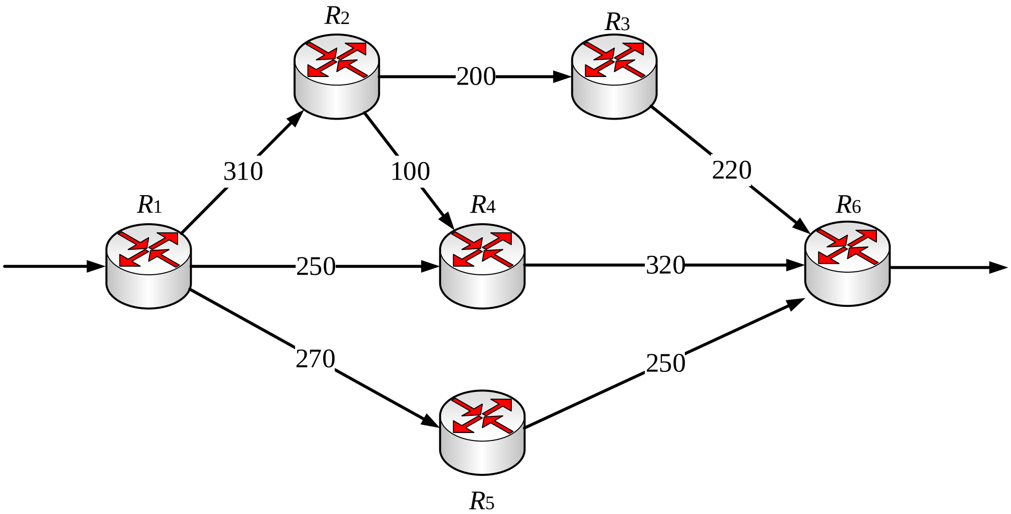

Figure 1: The studied fragment of the structure of ICN

The network consists of six nodes (routers). In the process of investigation, one flow was generated, i.e. $k = 1$, when the source node of packets was a router R_1, and the destination node is a router R_6.

The intensity of the packet flow varied from 0 to 710 1/s. The breaks in the communication links (Fig. 1) show their bandwidth (1/s).

Expression (11) was used together with expressions (5) – (10) to calculate the weights $w_{i,j}$ ($E_{i,j} \in E$). In this case, the criticality index of qth vulnerability on the ith node of the ICN, which depended on the basic metrics of the vulnerability assessment system, was determined for different routers with the corresponding probability of exploiting this qth vulnerability on the ith node of the network P_i^q, as shown in table 1.

In table 1 each node (router) of the network had a special description of the existing vulnerability according to the database of well-known vulnerabilities of information security CVE. This CVE database is designed to collect, store and disseminate information about identified vulnerabilities. Each vulnerability is provided with an identification number, a description, and a number of publicly available descriptive links.

Table 1
Characteristics of network equipment vulnerabilities

Node	Router	Base score BS_i^q	The probability of exploiting the vulnerability P_i^q	CVE description of the vulnerability	The criticality level of the vulnerability
R_1	Cisco RV042	7,2	0,1	CVE-2020-3294	High
R_2	Cisco Small Business RV160W	5,5	0,3	CVE-2021-1289	Medium
R_3	D-Link DIR-817LW A1-1.04	4,6	0,2	CVE-2020-14098	Medium
R_4	Xiaomi RM1800	7,5	0,3	CVE-2020-14098	High
R_5	Cisco RV260	9,8	0,7	CVE-2021-1292	Critical
R_6	Juniper EX2300	5,8	0,4	CVE-2019-0002	Medium

For example, the first node R_1, which is the Cisco RV042 router, is characterized by vulnerability CVE-2020-3294. In this case, CVE-2020-3294 is a unique number that describes a vulnerability in the Cisco RV042 router management web interface. Exploiting this vulnerability allows an authenticated remote attacker with administrative privileges to execute arbitrary code on the affected device and send large requests to the damaged device, causing the stack to overflow.

To assess the effectiveness, a comparative analysis of the proposed approach (1) – (12) (model 1), with the flow model, based on the metrics of the EIGRP protocol (model 2). The results of solving the routing problem using the developed model 1 and model 2 are given in table 2 and in fig. 2 and fig. 3, respectively, on which the communication links with the highest critical weights are indicated in red.

Table 2
The results of comparative analysis of model 1 and model 2 (with intensity 450 1/s)

Link	Bandwidth $\varphi_{i,j}$ (1/s)	Model 1		Model 2
		Flow intensity, 1/s	Weights $w_{i,j}$	Flow intensity, 1/s
$E_{1,2}$	310	200	0.09	0
$E_{1,4}$	250	250	0.09	225
$E_{1,5}$	270	0	0.09	225
$E_{2,3}$	200	200	0.29	0
$E_{2,4}$	100	0	0.29	0
$E_{3,6}$	220	200	0.19	0
$E_{4,6}$	300	250	0.29	220
$E_{5,6}$	260	0	0.69	230

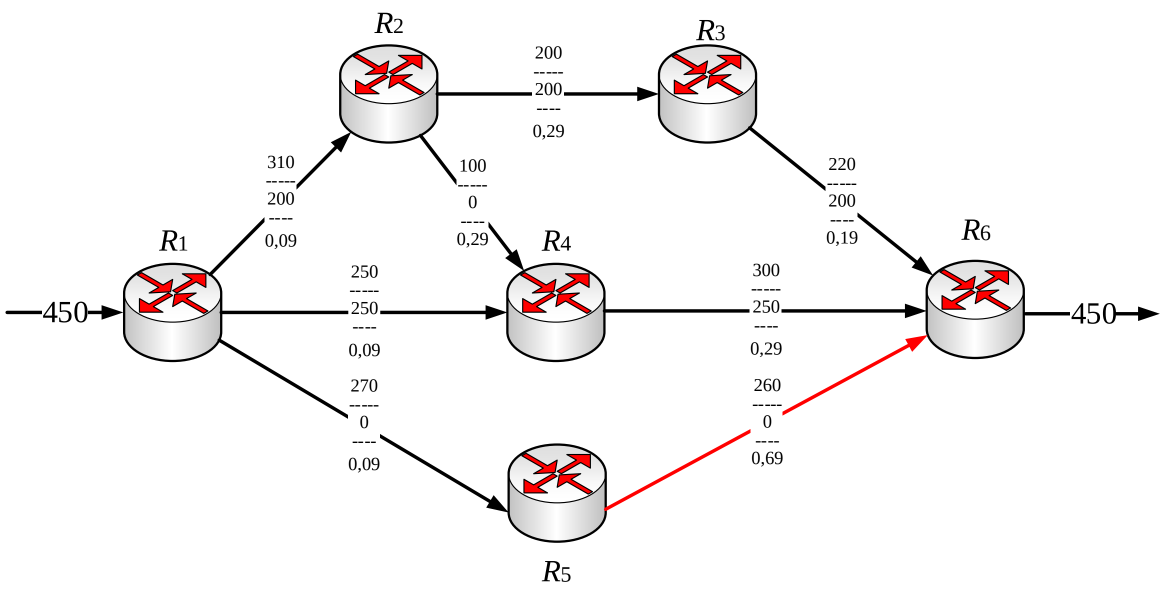

Figure 2: The result of solving the routing problem using model 1

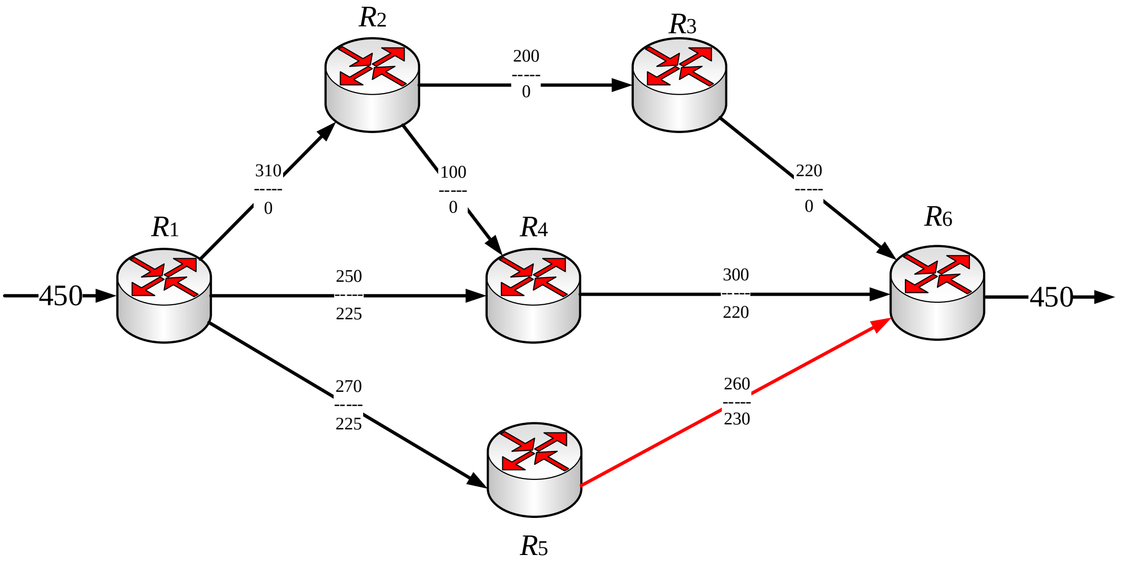

Figure 3: The result of solving the routing problem using model 2

As shown in Fig. 2, due to the solution of the route problem using the proposed model (model 1), the total weight (weight of compromise) of routes in the network was as follows, as shown in table 3.

Table 3
The weight of path compromise depends on the criticality of nodes and communication links

№	Paths	The total weight of compromise relative to the critical vulnerabilities of network nodes
1	$R_1 \rightarrow R_4 \rightarrow R_6$	0.38
2	$R_1 \rightarrow R_5 \rightarrow R_6$	0.78
3	$R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6$	0.57
4	$R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_6$	0.67

In general, the results of the use of paths in the ICN for different packet flow intensities when using models 1 and 2 are given in table 4.

As shown in Fig. 2, as a result of solving the route problem using the proposed approach (model 1), the packet flow with an intensity of 250 1/s was transmitted by the route R_1→R_4→R_6, which contained the least vulnerable communication links. During the congestion of this route, the rest of the flow was transmitted in the following vulnerable paths: R_1→R_2→R_3→R_6 (150 1/s) and R_1→R_2→R_4→R_6 (50 1/s).

At the same time, it should be noted that the path R_1→R_5→R_6, which contained the most weight-vulnerable communication links at an intensity of 450 1/s, was not used at all.

Unlike model 1, when using model 2, the best in terms of bandwidth, number of interceptions (hops) and in this case the least vulnerable path R_1→R_5→R_6 was loaded first (up to 260 1/s inclusive). As a result, the most vulnerable path R_1→R_5→R_6, the links of which had the best bandwidth, transmitted the packet flow with higher intensity and amounted to 230 1/s, compared to other paths.

Table 4

The procedure for using paths in the ICN for different packet flow intensities

Packet flow intensity, λ^1 1/s	Model 1	Model 2
	Paths	
$\lambda^k \in (0; 250]$	R_1→R_4→R_6	R_1→R_5→R_6
$\lambda^k \in (250; 400]$	R_1→R_4→R_6 R_1→R_2→R_3→R_6	R_1→R_4→R_6 R_1→R_5→R_6
$\lambda^k \in (400; 450]$	R_1→R_4→R_6 R_1→R_2→R_3→R_6 R_1→R_2→R_4→R_6	R_1→R_4→R_6 R_1→R_5→R_6
$\lambda^k \in (450; 710]$	R_1→R_4→R_6 R_1→R_2→R_3→R_6 R_1→R_2→R_4→R_6 R_1→R_5→R_6	R_1→R_4→R_6 R_1→R_5→R_6 R_1→R_2→R_3→R_6 R_1→R_2→R_4→R_6

4. Conclusion

An approach to the calculation of secure paths based on the routing model taking into account information security risks using the basic vulnerability criticality metrics is proposed and investigated. The approach is based on a routing model (1) – (12). The model is based on the conditions of implementation of single- and multipath routing (1), (2), flow conservation (3) and prevention of congestion of communication links of the ICN (4). Within the proposed approach, the problem of secure routing is formulated in an optimization form with the criterion of optimality (5).

In the process of describing the proposed approach, the apparatus of operations research and set theory was used. Graph theory was used to describe the topology of infocommunication networks. In order to form route metrics during the organization of secure routing, elements of risk theory were used. Linear programming methods implemented in the MATLAB Optimization Toolbox were used to solve secure routing optimization problems.

The validity and reliability of the proposed approach was confirmed by the results of analytical modeling and the correct use of mathematical apparatus. The adequacy of the obtained solutions was confirmed by the correctness of the choice of initial data in accordance with the NIST recommendations.

The advantage of the approach is that the calculation of route metrics uses expressions (12), which characterize the risk of information security in ICN communication links and in accordance with the recommendations of NIST CVSS v.3 take into account losses from breach of confidentiality and integrity of information. case of use of existing vulnerabilities; take into account indicators of the complexity of the application of vulnerabilities at network nodes and access to network elements in particular and the network in general due to the use of these vulnerabilities.

The paper compares the proposed approach and model with the metrics of the EIGRP protocol. The results of the study showed that within the approach of calculating secure paths with increasing packet traffic, the paths in the network that contained communication links with the lowest weights, i.e. had the least weight of compromise, were loaded first. The transmission of the packet flow after overloading the more secure path was carried out in the following paths according to the values of the weights of the communication links. The paths in the network that contained the communication links with the highest weights were loaded last.

In contrast to the proposed approach, paths within the EIGRP multipath routing model were loaded according to their bandwidth and number of hops, without taking into account the risks of information security in general.

It should be noted that for the worst case scenario in the process of exploiting the vulnerability at the network node, i.e. under the condition of 100% compromise of the communication link with the highest weight, the gain compared to traditional models in the area of low loads ICN was 37%, in the area of medium loads - 25 % and gradually decreased.

The practical value of the proposed result is that the proposed approach can be the basis of mathematical and algorithmic support of promising secure routing protocols in both traditional infocommunication and software-defined networks. Prospects for the development of the obtained solutions should be recognized as a synthesis of models and methods of secure routing that can guarantee a given level of network security based on the calculation and use of appropriate routes in ICN. The proposed approach to the formation of route metrics can be applied comprehensively in the process of solving routing problems of both network security indicators and service quality indicators.

5. References

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

[2] T. Edgar, D. Manz, Research Methods for Cyber Security, 1st edition. Syngress, 2017. 428 p

[3] O. Yeremenko, O. Lemeshko, A. Persikov, Secure Routing in Reliable Networks: Proactive and Reactive Approach, Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, Springer, Cham. Vol. 689. 2018. P. 631–655. doi:10.1007/978-3-319-70581-1_44.

[4] M. Yevdokymenko, M. Manasse, D. Zalushniy, B. Sleiman, Analysis of Methods for Assessing the Reliability and Security of Infocommunication Network, Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the Fourth International Scientific-Practical Conference, Kharkov, Ukraine, 10–13 October, 2017. P. 199–202. doi: 10.1109/INFOCOMMST.2017.8246379.

[5] M. Yevdokymenko, A. Shapovalova, O. Voloshchuk, A. Carlsson, Proactive Approach for Security of the Infocommunication Network Based on Vulnerability Assessment. Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the Fifth International Scientific-Practical Conference, Kharkov, Ukraine, 9–12 October 2018. P. 609–612. doi: 10.1109/INFOCOMMST.2018.8632079.

[6] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, A. M. Hailan, A. Mersni, Cyber Resilience Approach Based on Traffic Engineering Fast ReRoute with Policing. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS): Proceedings of the 10th IEEE International Conference, Metz, France, 2019. P. 117–122. doi: 10.1109/IDAACS.2019.8924294.

[7] A. A. Sagare, R. Khondoker, Security Analysis of SDN Routing Applications, SDN and NFV Security, Lecture Notes in Networks and Systems, Springer, Cham, Vol. 30. 2018. P.1–17. doi: 10.1007/978-3-319-71761-6_1

[8] S. Pattanavichai, Comparison for network security scanner tools between GFI LanGuard and Microsoft Baseline Security Analyzer (MBSA), International Conference on ICT and Knowledge Engineering (ICT&KE): Proceedings of the 15th, International Conference, Bangkok, 2017. P. 1–7. doi: 10.1109/ICTKE.2017.8259628.

[9] J. Li, Z. Yang, X. Yi, T. Hong, X. Wang, A Secure Routing Mechanism for Industrial Wireless Networks Based on SDN, International Conference on Mobile Ad-Hoc and Sensor Networks (MSN): Proceedings of the 14th International Conference, China, 2018. P. 158–164. doi: 10.1109/MSN.2018.000-2.

[10] M. Wang, J. Liu, J. Mao, H. Cheng, J. Chen, C. Qi, Route Guardian: Constructing secure routing paths in software-defined networking, Tsinghua Science and Technology, Vol. 22. 2017. No. 4. P. 400–412. doi: 10.23919/TST.2017.7986943.

[11] A. Snihurov, V. Chakrian, Improvement of EIGRP Protocol Routing Algorithm Based on Information Security Metrics. International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T-2015): Proceedings of the Second International Conference, Kharkiv, 2015. P. 263–265. doi: 10.1109/INFOCOMMST.2015.7357331.

[12] O. Lemeshko, M. Yevdokymenko, O. Yeremenko, T. Radivilova, D. Ageyev, N. Kryvinska, Fast ReRoute Tensor Model with Quality of Service Protection Under Multiple Parameters, Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, Springer, Cham, 2020. No. 48. P. 489–512. doi:10.1007/978-3-030-43070-2_22.

[13] Q. Gu, H.C.A. Tilborg, S. Jajodia, Secure Routing Protocols, Encyclopedia of Cryptography and Security, Springer, Boston, MA, 2011. doi: 10.1007/978-1-4419-5906-5_641.

[14] W. Lou, W. Liu, Y. Fang, SPREAD: enhancing data confidentiality in mobile ad hoc networks, IEEE Computer and Communications Societies (*INFOCOM):* Proceedings of the International Conference, Hong Kong, China, 2004. No. 4. P. 2404–2413. doi: 10.1109/INFCOM.2004.1354662.

[15] A. Aggarwal, S. Gandhi, N. Chaubey, Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs, International Conference on Advanced Computing & Communication Technologies (ACCT): Proceedings of the Fourth International Conference, Rohtak, India, 2014. P. 432–438. doi: 10.1109/ACCT.2014.95.

[16] R. Shashikala, C. Kavitha, Secured data integrity routing for Wireless Sensor Networks, *International Conference on Advances in Electronics Computers and Communications (ICAECC):* Proceedings of the International Conference, Bangalore, India, 2014. P. 1–6. doi: 10.1109/ICAECC.2014.7002419.

[17] G. K. Wadhwani, S. K. Khatri, S. K. Muttoo, Critical Evaluation of Secure Routing Protocols for MANET, *International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*: Proceedings of the International Conference, Greater Noida, India, 2018. P. 202–206. doi: 10.1109/ICACCCN.2018.8748725.

[18] J. Govindasamy, S. Punniakody, A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. *Electrical Systems and Information Technology*, 2018. No. l 5(3). P. 735–744. doi: 10.1016/j.jesit.2017.02.002.

[19] D. Medhi, K. Ramasamy, Network Routing, Second Edition: Algorithms, Protocols, and Architectures. The Morgan Kaufmann Series in Networking, 2nd Edition, Cambridge, MA, USA, Elsevier Inc. 2018.

[20] K. Sinchana, C. Sinchana, H. L. Gururaj, B. R. Sunil Kumar, Performance Evaluation and Analysis of various Network Security tools, *International Conference on Communication and Electronics Systems (ICCES):* Proceedings of the International Conference, Coimbatore, India, 2019. P. 644–650. doi: 10.1109/ICCES45898.2019.9002531.

[21] W. Streilein, K. Kratkiewicz, M. Sikorski, K. Piwowarski, S. Webster, PANEMOTO: Network Visualization of Security Situational Awareness Through Passive Analysis, SMC Information Assurance and Security Workshop (IAW): Proceedings of Security Workshop, West Point, NY, USA, 2007. P. 284–290. doi: 10.1109/IAW.2007.381945.

[22] J. Li, M. Huo and S. Chao, "A Study of Information Security Evaluation and Risk Assessment," 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), 2015, pp. 1909-1912, doi: 10.1109/IMCCC.2015.405.

[23] A. Hamed and H. K. Ben Ayed, "Privacy risk assessment for Web tracking: A user-oriented approach toward privacy risk assessment for Web tracking," 2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2016, pp. 1-6, doi: 10.1109/CCECE.2016.7726741.

[24] E. Mauro, "Best Practice and Common Practice in Risk Assessment," 2019 Petroleum and Chemical Industry Conference Europe (PCIC EUROPE), 2019, pp. 1-11, doi: 10.23919/PCICEurope46863.2019.9011636.

[25] ISO/IEC 15408-1:2009. Information technology, Security techniques Evaluation criteria for IT security, Part 1: Introduction and general model. URL: https://www.iso.org/standard/50341.html.

[26] Abedin M., Nessa S., Al-Shaer E., Khan L. Vulnerability analysis For evaluating quality of protection of security policies. Quality of Protection (QoP): Proceedings of the 2nd ACM Workshop, 2006. P. 49–52. doi: 10.1145/1179494.1179505.

[27] O. Lemeshko, M. Yevdokymenko, O. Yeremenko, A. Shapovalova, Z. Hu, S. Petoukhov, I. Dychka, M. He, Investigation of Load-Balancing Fast ReRouting Model with Providing Fair Priority-Based Traffic Policing. Advances in Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing. Springer, Cham. Vol. 1247. 2020. P. 108–119. doi: 10.1007/978-3-030-55506-1_10.

[28] K. Scarfone, K. Scarfone, P. Mell, NIST Special Publication 800-94 Revision 1 (Draft) Guide to intrusion detection and prevention systems (IDPS)., National Institute of Standards and Technology, 2012. URL: http://csrc.nist.gov/publications/drafts/800-94- rev1/draft_sp800-94-rev1.pdf.

[29] R. Roehrkasse, "Linear programming in operations research," in *IEEE Potentials*, vol. 9, no. 4, pp. 39-40, Dec. 1990, doi: 10.1109/45.65868.