ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES,
ELECTRONIC ENGINEERING

№ 1 (1), 2021

PROVIDING CYBER RESILIENCE IN SOFTWARE-DEFINED NETWORKS BY SECURE ROUTING MEANS

A. Chhaytli, M. Persikov
Kharkiv National University of Radio Electronics, 14, Nauky Avenue, Kharkiv, 61166, Ukraine

Corresponding author: Persikov M. (e-mail: mihapersikov@gmail.com).

(Received 1 April 2021)

This paper is devoted to solving the technical task of providing cyber resilience utilizing secure routing means in Software-Defined Networks (SDN). The work analyzes the SDN architecture and its main components, the concept of cyber resilience and its means, as well as security issues in SDN. Particular attention is paid to the use of secure routing in software-defined networks. Numerical research of the model of secure multipath routing of fragmented confidential messages in the SDN data plane was conducted. The calculation of the message compromise probability for different values of links compromise probabilities was performed. The obtained results showed that the model of secure multipath routing of fragmented confidential messages with redundancy provides a better balancing of message parts by routes. Results of the numerical study proved the adequacy of the selected secure multipath routing model.

Key words: *SDN; Secure Routing; Cyber Resilience; Compromise Probability; Modeling.*
UDC: 621.391

1. Introduction

Providing the required level of cyber resilience of the infocommunication network is a complex technical task [1–5]. The solution to such problems is impossible without the consistent use of all protocols available in modern networks [6, 7]. Generally, the protocol manages the network resource and its reservation. At the same time, a promising direction of increasing the cyber resilience of the infocommunication network is seen in the effective use of the secure routing functionality.

In general, the principal requirements for modern networking are as follows [6–10]:

- adaptability (dynamic networks response to network conditions);
- automation (automatic propagation of policy changes aimed at minimization of manual work and errors);
- maintainability (new features and capabilities must be seamless with minimal disruption of operations);
- mobility of control functionality (for both mobile user devices and virtual servers);
- integrated security (network applications must integrate seamless security as a core service);
- scalability (ability to on-demand scale up/down the network and its services).

As discussed in [6, 7], the SDN approach splits the switching function between data and control planes on separate devices. At the same time, the data plane is responsible for forwarding packets. In contrast, the control plane provides the so-called “intelligence”, for example, in creating routes, setting priorities, and routing policy parameters to meet Quality of Service (QoS) and Quality of Experience

(QoE), as well as resilience and network security requirements [6–10]. With the help of open interfaces, the switching hardware presents a uniform interface independently from internal implementation details. Moreover, such open interfaces enable networking applications to communicate with the SDN controllers [6].

In turn, cyber-resilience is a framework designed to help infocommunication networks withstand different cyber-attacks [1–5]. However, it is not a single layer of protection but an iterative process that provides the means of recovery from attacks and a way for organizations to structure their defense policies.

It should be mentioned that the scale of connected devices in the modern network and its heterogeneity have made securing more challenging. However, with the advent of softwarized networks, the algorithmic complexity is handled. This enables researchers to design innovative security protocols at the data plane to defend against attacks dynamically [6, 8].

Generally speaking, secure routing protocols aim to increase network security and its cyber resilience. However, proactive and reactive approaches can be distinguished among the secure routing protocols [11–18]:

1. Proactive secure routing protocols are based on a preassessment of security risks and the use of the most secure network elements (links, nodes).
2. Reactive secure routing protocols are based on the on-demand route calculation.

Nevertheless, secure routing protocols are often just improvements of traditional ones, such as RIP, EIGRP, OSPF under using the specified network security metrics (risks, compromise probabilities, etc.).

An example of a proactive approach can be a solution based on providing a given security level [11, 17, 18]. In this case, the transmission of messages divided into parts according to Shamir’s scheme from the source to the destination is organized using secure multipath routing with balancing the number of parts (shares) over disjoint routes [17]. It is necessary to determine the operational order of changing the set of paths used to transmit parts of confidential messages within this task [17, 18].

Therefore, the object of the present research is the process of secure routing in the SDN data plane. The work aims to analyze the selected model of secure routing in the SDN data plane to increase overall network cyber resilience. Research methods are analytical modeling, simulation, formalization, and comparison.

2. Secure Routing Model for SDN Data Plane

One of the directions for ensuring a given level of information security in communication networks is implementing a mechanism based on the multipath routing of the transmitted message previously divided into parts according to Shamir’s scheme [17, 18]. As a result of using such a scheme, it is possible to reduce the probability of compromising the transmitted message because an attacker to compromise the message must compromise all paths, usually non-overlapping, over which parts of the divided message are sent.

Currently, there are known analytical expressions for calculating the probability of compromising the message transmitted in parts over a set of disjoint paths [17, 18]. In addition, it is assumed that the following initial data are known:

- n – number of links in the network;
- m – number of nodes in the network;
- S_{msg} – sender of a transmitted message (source node);
- D_{msg} – receiver of a transmitted message (destination node);
- M – number of used non-overlapping paths in routing message fragments;
- (T, N) – Shamir’s scheme parameters;
- N – total number of fragments, obtained by applying Shamir’s scheme;
- T – minimum number of fragments (T £ N) needed for the message reconstruction;
- p_i^j – probability of compromise jth element (node, link) of ith path;
- M_i – number of elements in the ith path that can be compromised.

During the solving of the secure routing problem, the following parameters should be calculated [53]:

- p_i – probability of compromise the ith path;
- order of distribution of the number of fragments of the transmitted message by paths taking into account the selected Shamir's scheme (T, N);
- x_i – number of fragments, transmitted over the ith path ($i = \overline{1, M}$);
- P_{msg} – probability of compromise for the whole message during its transmission by fragments over the network.

The number of paths used in the network (M) determines the size of the vector $\vec{x}$, the coordinates x_i of which characterize the number of fragments transmitted in the *i*th path between the sending node and the receiving node. Based on the physical meaning of the variables x_i, they are subject to restrictions of the form:

$$x_i \in N_0 (i = \overline{1, M}), \tag{1}$$

where N_0 is the extended natural number, i.e., variables x_i can take only non-negative integer values.

Besides, during the calculation of the control variables x_i ($i = \overline{1, M}$) regulating the allocation of the message fragments over the non-overlapping paths, the following condition [17] must be met:

$$N = \sum_{i-1}^{M} x_i \ . \tag{2}$$

It is assumed that the sender and the receiver are trusted, i.e., the compromise probability of the sender and receiver nodes is equal to zero. Furthermore, within the solution, it is supposed that if the element (node, link) is compromised, all fragments transmitted through the element will also be compromised. Then the probability of compromise of the ***i***-th path consisting of the M_i elements can be calculated by the expression [11]

$$p_i = 1 - \left(1 - p_i^1\right)\left(1 - p_i^2\right)...\left(1 - p_i^{M_i}\right) = 1 - \prod_{j=1}^{M_i}\left(1 - p_i^j\right). \tag{3}$$

In the case of Shamir's scheme with redundancy when $T < N$ the condition below must be satisfied

$$N - x_i < T, (i = \overline{1, M}) \tag{4}$$

while when $T = N$ the following conditions must be met in the non-redundant sharing scheme

$$1 \le x_i \le T - 1, (i = \overline{1, M}) \tag{5}$$

Conditions (5) and (6) ensure that in the case of compromising all the paths except ***i***-th path an adversary cannot reconstruct the whole message. While the probability of message compromise divided into the *N* fragments using Shamir's scheme transmitted over the *M* paths determined by the expression [18]

$$P_{msg} = \prod_{i=1}^{M} p_i . \tag{6}$$

The solution to the problem of secure routing is determining the order of distribution of the number of fragments of the message to be transmitted along paths that do not overlap. In turn, this task can be formalized as a Mixed Integer Linear Programming (MILP) problem, which was solved by the MATLAB Optimization Toolbox, presented by the `intlinprog` subroutine [19, 20].

When solving MILP problems, it is necessary to minimize the objective function represented by the linear form

$$\min_{x} \vec{f}^{\,t} \vec{x},$$

when a number of conditions are met, which are presented in the form of constraints on equations and inequalities

$$A * \vec{x} \le \vec{b};\ Aeq * \vec{x} = \vec{b}eq;\ \vec{lb} \le \vec{x} \le ub$$

where $\vec{f}$, $\vec{x}$, $\vec{b}$, $\vec{b}eq$ are vectors; A and Aeq are matrices of the corresponding size;

$\vec{lb}$ and $\vec{ub}$ are vectors-columns of size *M*.

3. Describing and Solving a Secure Routing Problem in SDN Data Plan in MATLAB

For the numerical example of the SDN data plane topology for the Lebanon Hybrid SDN network, let select the structure shown in Fig. 1 that connects the following cities:

1. Beirut.
2. Tripoli.
3. Al Hermel.
4. Baalback.
5. Sidon.
6. Tyre.
7. Nabatiye.
8. Zahle.

Then the structure of the network (SDN data plane) and the probabilities of compromise of its communication links be presented in Fig. 2. It should be noted that the numbers of nodes correspond to the numbers of cities shown above in Fig. 1.

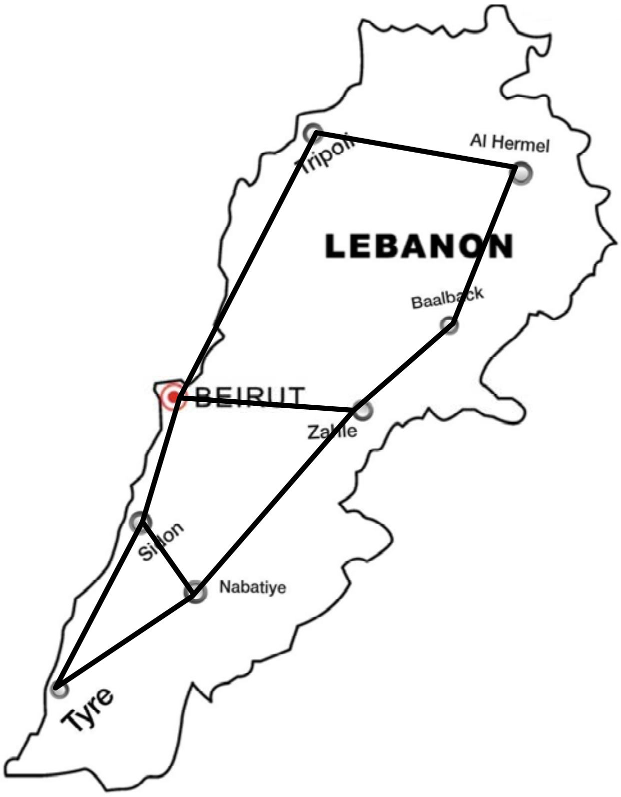

Fig. 1. Example SDN data plane topology for Lebanon

In accordance with Fig. 1 and Fig. 2, input parameters for numerical research are as follows:

- n = 10 – number of links in the network;
- m = 8 – number of nodes in the network;
- S_{msg} = Switch 1 – sender of a transmitted message (source node) – Beirut;
- D_{msg} = Switch 8 – receiver of a transmitted message (destination node) – Zahle.

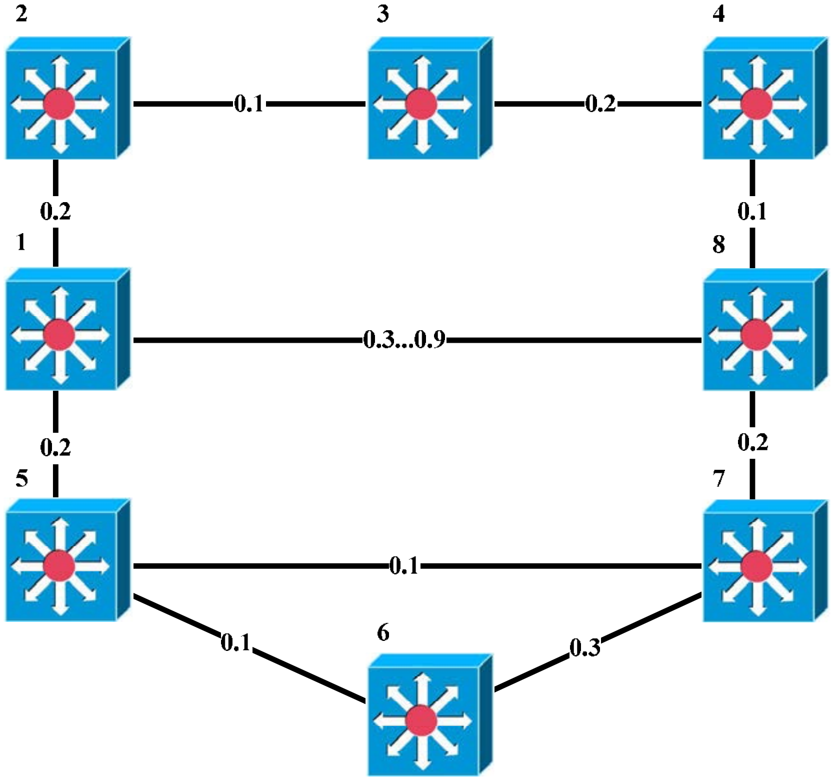

Fig. 2. Network structure under investigation

Following equation (3) and taking into account the given compromise probabilities of the modeled network structure communication links, the values of all possible paths compromise probabilities are calculated and shown in Table 1. Moreover, the compromise probability of the fifth link between nodes 1 and 8 varied from 0.3 to 0.9.

Table 1

Compromise Probabilities of Paths between Switch 1 and Switch 8

No.	Path	Compromise Probability		
		$p_2^1 = 0.3$	$p_2^1 = 0.6$	$p_2^1 = 0.9$
1	1→2→3→4→8	0.4816	0.4816	0.4816
2	1→8	0.3	0.6	0.9
3	1→5→7→8	0.424	0.424	0.424
4	1→5→6→7→8	0.5968	0.5968	0.5968

From the obtained values, we can see paths 3 and 4 overlappings. However, for applying the model from Section 2, we must select the set of disjoint paths for secure routing. Moreover, the compromise probability of the fourth path is higher than for the third path. Consequently, for further numerical research of secure routing on the network structure shown in Fig. 2 we select path No. 1, No. 2, and No. 3.

4. Results of Calculations Utilizing Shamir’s Scheme with and without redundancy

The investigated parameters of Shamir’s scheme (*T*, *N*):

- without redundancy (12, 12) at *T* = *N* = 12;
- with redundancy (10, 12) at *T* = 10, *N* = 12.

Then we form the desired vector $\vec{x}$. Within the model represented by expressions (1)–(4), it has the form:

$$\vec{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}. \quad (7)$$

The size of the metric vector $\vec{f}$ corresponds to the number of paths used in the network *M*, the coordinates f_i of which characterize the compromise probability of the *i*th path (3). Then the vector $\vec{f}$ for example (7) has the form:

$$\vec{f} = \begin{bmatrix} f_1 \\ f_2 \\ f_3 \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}. \quad (8)$$

Next we formalize the condition of the integrity of the message, consisting of *N* fragments:

$$x_1 + x_2 + x_3 = 12 \quad (9)$$

Finally, in accordance with (8) vectors *Aeq* and $\vec{beq}$ are as follows:

$$Aeq = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}; \vec{beq} = 12 . \quad (10)$$

Table 2 presents calculation results and order of distribution of the number of fragments of the transmitted message by paths considering the selected Shamir’s scheme (*T*, *N*) without redundancy.

Table 2

Order of the message fragments distribution by paths taking into account Shamir’s scheme (12, 12) without redundancy

No.	Path	Fragments distribution		
		$p_2^1 = 0.3$	$p_2^1 = 0.6$	$p_2^1 = 0.9$
1	1→2→3→4→8	1	1	1
2	1→8	10	1	1
3	1→5→7→8	1	10	10
P_{msg}		0.0613	0.1225	0.1838

Table 3 presents calculation results and order of distribution of the number of fragments of the transmitted message by paths considering the selected Shamir’s scheme (*T*, *N*) with redundancy.

Graph of the dependence of the message compromise probability as a whole on the changing compromise probability of the fifth link (second path) is presented in Fig. 3.

To sum up, the obtained results show that the model of secure multipath routing of fragmented confidential messages with redundancy provides a better balancing of message parts by routes. Consequently, it will be harder to compromise them.

Taking all into account, the model needs improvements considering effective use of network resources together with the provision of network cyber resilience and demanded level of information security.

Table 3

Order of the message fragments distribution by paths taking into account Shamir's scheme (10, 12) with redundancy

No.	Path	Fragments distribution		
		$p_2^1 = 0.3$	$p_2^1 = 0.6$	$p_2^1 = 0.9$
1	1→2→3→4→8	3	3	3
2	1→8	6	3	3
3	1→5→7→8	3	6	6
P_{msg}		0.0613	0.1225	0.1838

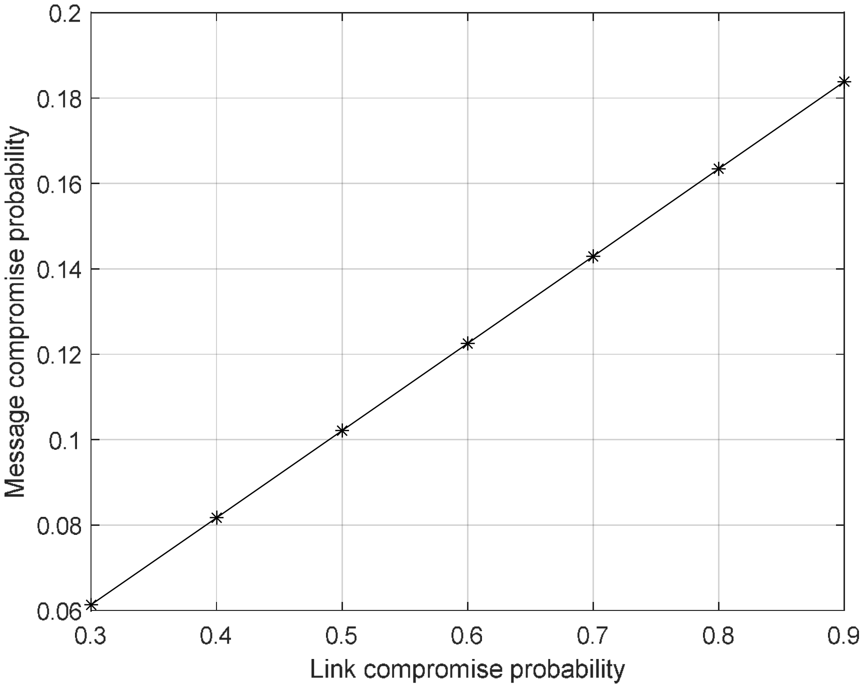

Fig. 3. Dependence of the message compromise probability on changing compromise probability of the fifth link $p_2^1 = 0.3...0.9$

5. Conclusion

The analysis of existing approaches allows to formulate the following requirements for providing cyber resilience of softwarized networks on the data plane:

- adaptive response of the network to possible failures (optimization of the ability to a timely and appropriate response to failures and attacks while limiting their harmful effects on the network functioning);
- use of resource and functional redundancy to protect the critical elements of the network and its resources;
- balanced use of the network resource already in use based on secure multipath routing;
- taking into account the priorities and criticality of transmitting data;
- ensuring the consistency and effectiveness of network elements protection mechanisms.

Therefore, the relevant scientific and practical task is the developing new approaches to ensuring the cyber resilience of SDN-based networks under the requirements of ensuring network resilience, security, and Quality of Service with the support of the secure routing means in the case of network elements compromise (links, nodes, paths).

The presented work is devoted to investigating the secure routing process of fragmented confidential messages in the SDN data plane to improve overall network cyber resilience. The work analyzes the SDN architecture and its main components, the concept of cyber resilience and its means, as well as security issues in SDN.

Particular attention is paid to the use of secure multipath routing in software-defined networks. The corresponding mathematical model was chosen and implemented in the MATLAB environment and Live Script source code. The topology under numerical research for the Lebanon region was selected. The calculation of the message compromise probability for different values of links compromise probabilities was conducted. Results of the numerical study proved the adequacy of the selected secure multipath routing model.

The promising direction is seen in further improvements of existing approaches and models of secure routing towards the support of load balancing and Quality of Service in line with the demanded level of network security.

References

[1] Linkov, I., and Kott, A. (2019), "Fundamental concepts of cyber resilience: Introduction and overview", Cyber resilience of systems and networks, Springer, Cham, pp. 1–25.

[2] Galinec, D., and Steingartner, W. (2017), "Combining cybersecurity and cyber defense to achieve cyber resilience", 2017 IEEE 14th International Scientific Conference on Informatics, IEEE, pp. 87–93.

[3] Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., and McQuaid, R. (2019), "Developing Cyber Resilient Systems: A Systems Security Engineering Approach" (No. NIST Special Publication (SP) 800–160 Vol. 2 (Draft)), National Institute of Standards and Technology.

[4] Dickson, F., and Goodwin, P. (2019), "Five Key Technologies for Enabling a Cyber-Resilience Framework", US45455119, IBM.

[5] Musman, S. (2016), "Assessing prescriptive improvements to a system's cyber security and resilience", 2016 Annual IEEE Systems Conference (SysCon), IEEE, pp. 1–6.

[6] Stallings, W. (2015), Foundations of modern networking: SDN, NFV, QoE, IoT, and Cloud. Addison-Wesley Professional.

[7] Rangan, R. K. (2020), "Trends in SD-WAN and SDN", CSI Transactions on ICT, vol. 8, no. 1, pp. 21–27.

[8] Stallings, W. (2018), Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional.

[9] Liu, Y., Zhao, B., Zhao, P., Fan, P., and Liu, H. (2019), "A survey: Typical security issues of software-defined networking", China Communications, vol. 16, no. 7, pp. 13–31.

[10] Porras, P., Shin, S., Yegneswaran, V., Fong, M., Tyson, M., and Gu, G. (2012), "A security enforcement kernel for OpenFlow networks", Proceedings of the first workshop on Hot topics in software defined networks, pp. 121–126.

[11] Yeremenko, O., Lemeshko, O., and Persikov, A. (2017), "Secure routing in reliable networks: proactive and reactive approach", Conference on Computer Science and Information Technologies. Springer, Cham, pp. 631–655.

[12] Patil, M. V., and Jadhav, V. (2017), "Secure, reliable and load balanced routing protocols for multihop wireless networks", 2017 International Conference on Intelligent Computing and Control (I2C2), IEEE, pp. 1–6.

[13] Li, J., Yang, Z., Yi, X., Hong, T., and Wang, X. (2018), "A Secure Routing Mechanism for Industrial Wireless Networks Based on SDN", 2018 14th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), IEEE, pp. 158–164.

[14] Sagare, A. A., and Khondoker, R. (2018), "Security Analysis of SDN Routing Applications", SDN and NFV Security, Springer, Cham, pp. 1–17.

[15] Francois, F., and Gelenbe, E. (2016), "Optimizing secure SDN-enabled inter-data centre overlay networks through cognitive routing", 2016 IEEE 24th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), IEEE, pp. 283–288.

[16] *Lemeshko, O., Yeremenko, O., Shapovalova, A., Hailan, A. M., Yevdokymenko, M., and Persikov, M. (2021), "Design and Research of the Model for Secure Traffic Engineering Fast ReRoute under Traffic Policing Approach", 2021 IEEE 16th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), IEEE, pp. 23–26.*

[17] *Lou, W., and Kwon, Y. (2006), "H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks", IEEE Transactions on Vehicular Technology, 55(4), pp. 1320–1330.*

[18] *Yeremenko, O. S., and Ali, A. S. (2015), "Secure multipath routing algorithm with optimal balancing message fragments in MANET", Radioelectronics and Informatics. 2015. vol. 1, no. 68, pp. 26–29.*

[19] *Лемешко О. В., Невзорова О. С., Єременко О. С., Євсєєва О. Ю. (2016), Методичні вказівки до практичних занять з дисципліни "Управління та маршрутизація в ТКС" для студентів денної форми навчання спеціальності 6.050903, Телекомунікації, Харків: ХНУРЕ.*

[20] *Duffy, D. G. (2016), Advanced engineering mathematics with MATLAB®, Chapman and Hall/CRC.*

ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ ЗАСОБАМИ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ

А. Шхайтлі, М. Персіков

Харківський національний університет радіоелектроніки, пр. Науки, 14, Харків, 61166, Україна

У статті вирішується технологічне завдання забезпечення кіберстійкості програмно-конфігурованих мереж (Software-Defined Networks, SDN) за допомогою засобів безпечної маршрутизації. У роботі проаналізовано архітектуру SDN та її основні компоненти, концепцію кіберстійкості та її засобів, а також питання безпеки в SDN. Особливу увагу звернено на використання безпечної маршрутизації у програмно-конфігурованих мережах. Здійснено числове дослідження моделі безпечної багатошляхової маршрутизації фрагментованих конфіденційних повідомлень у площині даних SDN. Виконано розрахунок імовірності компрометації повідомлення для різних значень імовірностей компрометації каналів зв'язку. Отримані результати показали, що модель безпечної багатошляхової маршрутизації фрагментованих конфіденційних повідомлень із надмірністю забезпечує кращу збалансованість частин повідомлень за маршрутами. Результати числового дослідження довели адекватність вибраної моделі безпечної багатошляхової маршрутизації.

Ключові слова: *SDN; безпечна маршрутизація; кіберстійкість; імовірність компрометації; моделювання.*