Development of Secure Routing Algorithms in Computer Networks

***Ibraim DIDMANIDZE*[1] *Mikheil DONADZE*[2], *Besik BERIDZE*[3], *Zebur BERIDZE*[1], *Didar DIDMANIDZE*[1], *Tengiz DIDMANIDZE*[3]**

[1]Batumi Shota Rustaveli State University, Center for Languages and Information Technologies, Batumi, 6010, Georgia
[2]Batumi Shota Rustaveli State University, Department of Computer Science, Batumi,6010, Georgia
[3]Batumi Shota Rustaveli State University, Department mathematik, Batumi,6010, Georgia

Correspondence: *ibraim.didmanidze@bsu.edu.ge

Abstract

The paper delves into the contemporary information security challenges within computer networks. It scrutinizes the existing methods of message packet routing, identifying several drawbacks associated with them. When examining issues concerning information security, it's crucial to consider the unique characteristics of this aspect of security. Security forms an integral part of information technologies, a field evolving at an unprecedented pace. The paper addresses the challenges associated with developing secure routing algorithms within Wide Area Network (WAN) environments. The paper presents and elucidates on novel secure routing algorithms characterized by a qualitatively innovative approach to resolving security concerns. Thanks to a novel suite of essential features in each variant of the proposed method, which includes specifying information about the communication network's structure, initial data regarding network nodes and users, and calculating integrated security metrics, secure routes between network nodes are meticulously selected from all available communication pathways among users. This ensures that network users are furnished with a secure route.
The paper pertains to the realm of information communication and can serve as a valuable resource for planning or developing new network connections in networks like corporate intranets and extranets.

KEY WORDS: *computer networks, routing algorithms, information security.*

Citation: Didmanidze, I.; Donadze, M.; Beridze, B.; Beridze, Z.; Didmanidze, D.; Didmanidze, T. (2024). Development of Secure Routing Algorithms in Computer Networks. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959. DOI 10.3849/cndcgs.2024.331.

1. Introduction

Information security stands as a paramount facet of integrated security, regardless of the level at which it's considered - be it national, industrial, corporate, or personal [1, 2].

What holds significance here are not merely individual solutions such as laws, training courses, or software and hardware products, which undergo periodic updates. Rather, it's the mechanisms for generating novel solutions that enable us to keep pace with the rapid advancements in technology. Information security has not only become exceedingly crucial but has also emerged as a highly trendy and lucrative field of endeavor. It's quite natural that the interests of numerous departments, companies, and individuals clash in this domain, leading to a struggle for spheres of influence, and sometimes even for survival. Connecting an organization to a global network like the Internet notably enhances the organization's efficiency and unlocks a plethora of new opportunities for growth and development. Simultaneously, the organization must prioritize establishing a robust system for protecting its informational resources, catering to those who wish to utilize, modify, or enhance them. Irrespective of the particulars, the organization's security system when operating in global networks should be oriented towards safeguarding its information resources [2].

In such circumstances, it becomes imperative to explore new approaches to guaranteeing information security. One of these areas involves managing the routes of information exchange between users within a communication network [6, 11-13].

The TCP/IP stack is not entirely secure and leaves room for various types of attacks. To execute such attacks, an attacker needs access to one of the systems connected to the Internet. This access can be obtained, for instance, by hacking into a system or by utilizing a computer connected to the Internet [3]. Attacks on TCP/IP generally fall into two categories: passive and active. In passive attacks, the attacker's actions at the TCP level are limited to monitoring available data or communication sessions. Eavesdropping, for example, entails intercepting network traffic and analyzing it. Due to the lack

Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic

of encryption in TCP/IP traffic, an attacker equipped with appropriate tools can intercept sessions of TCP/IP packets and extract usernames and passwords. It's important to note that this type of attack is difficult to detect because it doesn't alter the network flow. Attackers frequently employ passive scanning to determine the TCP ports on which domains respond to network requests. A typical scanning program will reveal connections to different ports and report port numbers to the attacker [4].

The current methods of routing message packets exhibit several drawbacks, such as insufficient adaptation to changes in the network structure, low communication security, and various other limitations. Selecting a transmission route involves establishing the sequence of transit network nodes through which messages should be forwarded to the intended recipient. This selection process typically occurs within the network nodes of the provider operators. The presence of nodes with low security levels creates conditions for network intrusions, consequently diminishing communication security [7, 8].

The approaches outlined in the paper and the algorithm presented are geared towards enhancing communication security by effectively managing information exchange routes between network users.

The model presented in the paper closely aligns with the technical essence of "The method of choosing a route to be used for equal commutation in the network" employed in routers. The method involves presetting initial data that includes the quality criteria of the routes. Information regarding the structure of the communication network, including the addresses of network nodes and the existence of connections between them, is stored within the router. A set of possible communication routes is established. Upon receiving a message intended for a target network address, a route is selected based on predetermined route quality criteria, and messages are transmitted along the chosen route.

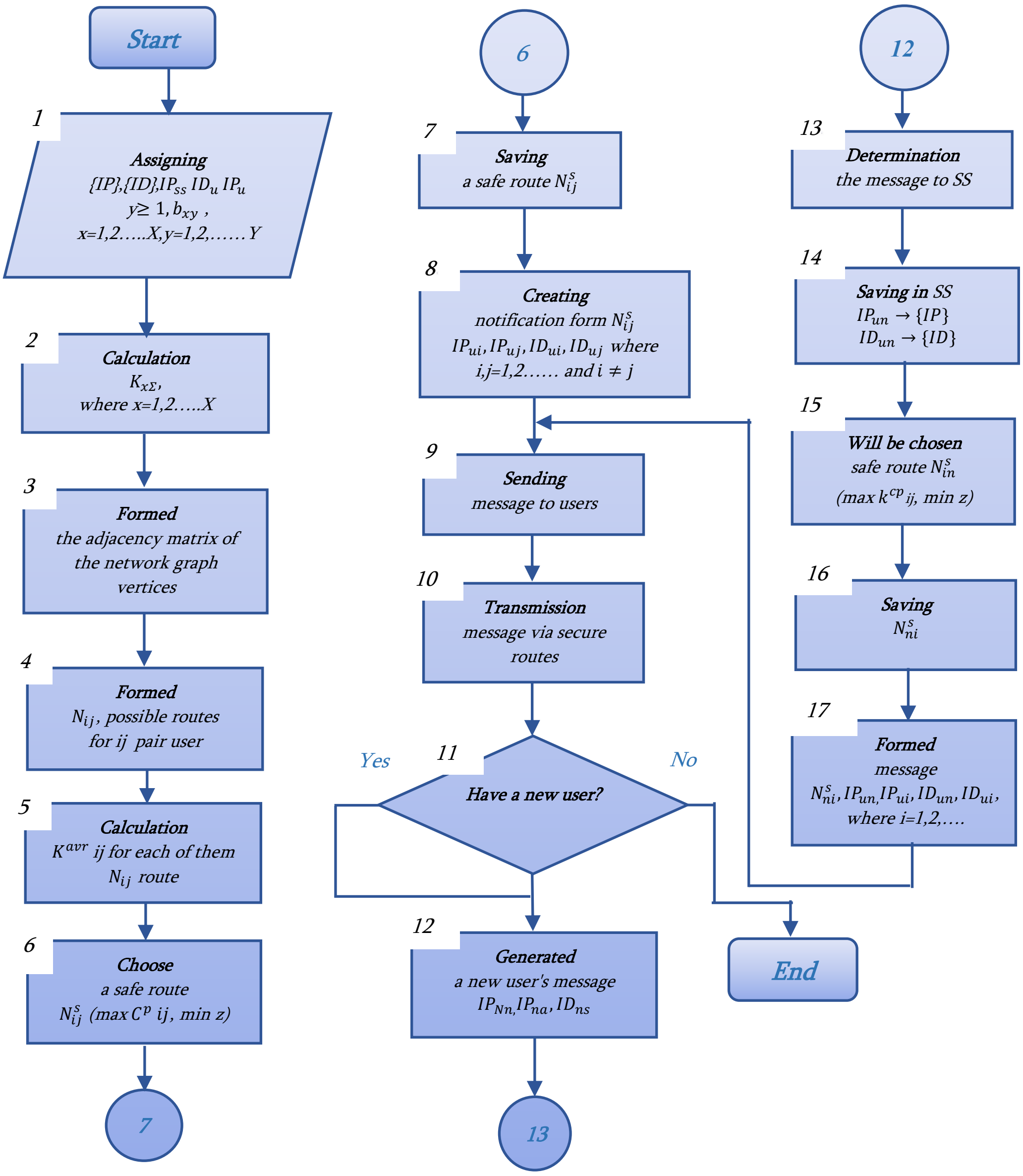

Fig. 1. The block diagram of the first version of the secure routing algorithm for message packets

Nevertheless, a drawback of this method is the relatively low security of communication when utilizing the selected route for information exchange among users in the communication network [10]. A secure routing algorithm for message packets is introduced, comprising two versions for selecting a secure route within a communication network.

The first version (Fig.1.) pertains to a communication network where each node possesses $X \geq 2$ connections. Initial data is pre-assigned to the network nodes, and information regarding the network structure is recorded, including the IP_{Nn} addresses of the network nodes and their connectivity. A set of N potential communication routes is generated, from which a secure route is selected for transmitting messages.

N_{ij} represents the graph tree of the communication network, illustrating the routes between users i and j, and is calculated by the formula:

$$N_{ij} = B_0 * B_0^T,$$

Where $B_o = M * K$ is the matrix of neighboring vertices of the graph representing the communication network, with $M = M_p - 1, K$ - representing the number of rows and columns of the matrix respectively. M_p - denotes the number of adjacent rows of the original matrix, equal to the total number of communication network nodes; B_0^T represents the transposed matrix of B_o.

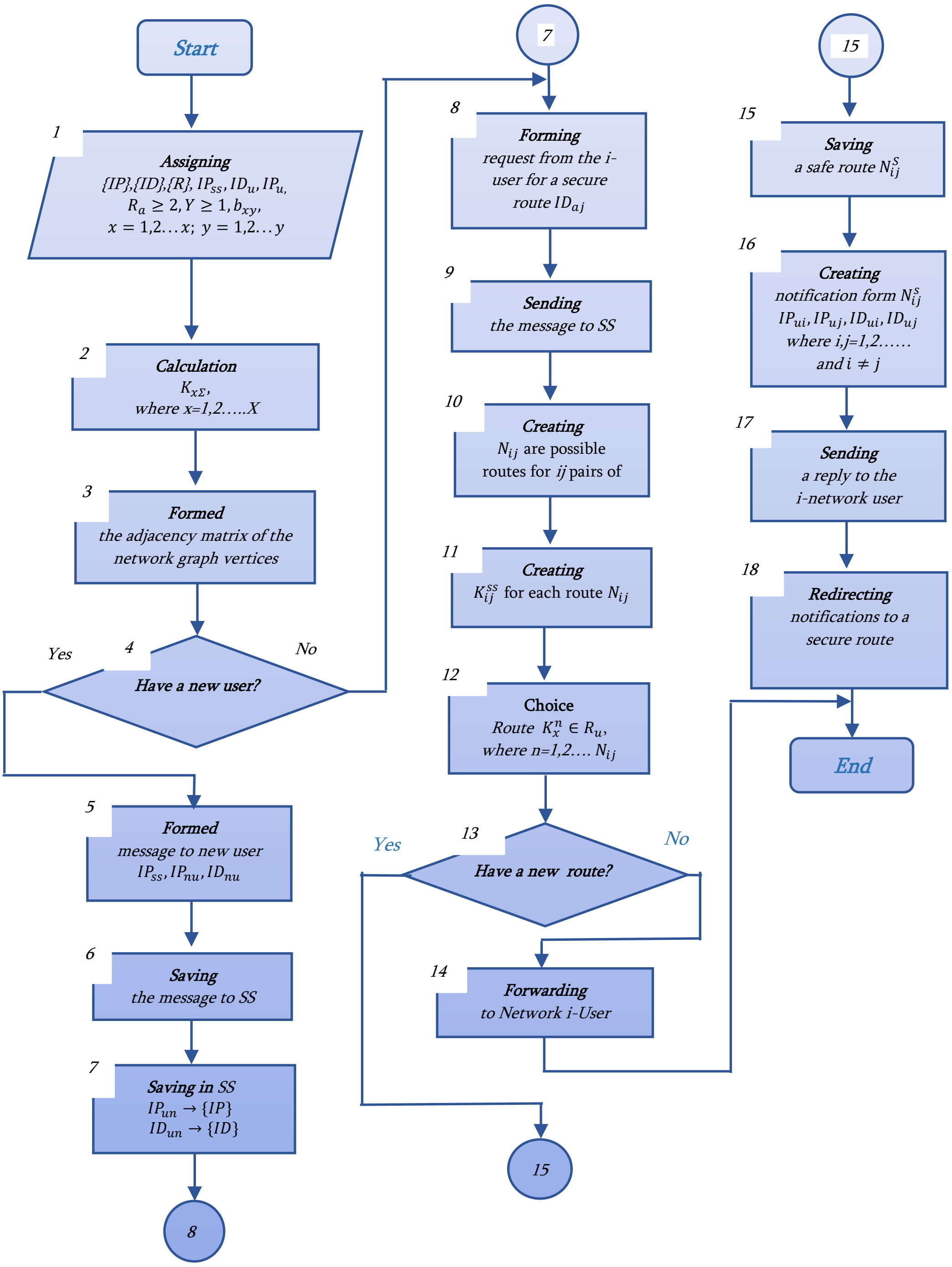
Start
1
Assigning
{IP},{ID},{R}, $IP_{ss}, ID_u, IP_u,$
$R_a \geq 2, Y \geq 1, b_{xy},$
$x = 1,2\ldots x;\ y = 1,2\ldots y$
2
Calculation
$K_{x\Sigma}$,
where x=1,2…..X
3
Formed
the adjacency matrix of the network graph vertices
4
Have a new user?
Yes
No
5
Formed
message to new user
$IP_{ss}, IP_{nu}, ID_{nu}$
6
Saving
the message to SS
7
Saving in SS
$IP_{un} \rightarrow \{IP\}$
$ID_{un} \rightarrow \{ID\}$
8
7
8
Forming
request from the i-user for a secure route ID_{aj}
9
Sending
the message to SS
10
Creating
N_{ij} are possible routes for ij pairs of
11
Creating
K_{ij}^{ss} for each route N_{ij}
12
Choice
Route $K_x^n \in R_u$,
where n=1,2…. N_{ij}
13
Have a new route?
Yes
No
14
Forwarding
to Network i-User
15
15
15
Saving
a safe route N_{ij}^S
16
Creating
notification form N_{ij}^s
$IP_{ui}, IP_{uj}, ID_{ui}, ID_{uj}$
where i,j=1,2……
and $i \neq j$
17
Sending
a reply to the i-network user
18
Redirecting
notifications to a secure route
End

Fig. 2. The block diagram of the second version of the secure routing algorithm for message packets

The second version of the algorithm addresses a communication network where each node possesses $X \geq 2$ connections. Initial data are pre-assigned to the network nodes, and information regarding the structure of the communication network is recorded, including the IP_{Nn} addresses of the network nodes and their connectivity possibilities. A set of *N* potential communication routes is established, from which a secure route is selected to transmit messages.

In contrast to the previous algorithm, the predefined initial data now includes, in addition to the structural and identification arrays of the network, the security indicator of the permitted route, the IP_{Nn} address of the security server, the corresponding ranks of the information to be transmitted in the network R_{inf}, and the complex security indicators $k_{x\Sigma}$ of the network nodes. The number of routes N_{ij} in the communication network graph between network users *i* and j is calculated by the formula:

$$N_{ij} = |B_o \times B_o^T|$$

Where $B_o = M * K$ - is the matrix of neighboring vertices of the graph representing the communication network, with $M = M_p - 1, K$ - representing the number of rows and columns of the matrix respectively. M_p -denotes the number of adjacent rows of the original matrix and is equal to the total number of communication network nodes; B_0^T -represents the transposed matrix of B_o.

2. Principle of Operation of Secure Routing Algorithms

To facilitate the exchange of information between users within a communication network, a secure communication route must be chosen from the set of available routes connecting the network's users. Routing a message entail identifying the sequence of nodes within the transit network through which the message should traverse. Determining the route poses a challenging task, particularly when numerous potential routes exist between a pair of users. Route determination involves selecting one or more routes from the set of possible options based on specific criteria. In existing methods of route selection, typical criteria include nominal bandwidth, congestion of communication channels, delays introduced by channels, number of intermediate network transit nodes, reliability of channels, and network transit nodes. However, in many cases, a contradiction arises between the need to ensure communication security and these existing methods. The proposed method (versions) seeks to address this issue. Accordingly, the first version of the presented method is implemented as follows.

In general, Fig. 3 depicts a communication network comprising: 1. X network nodes, 2. Security server, 3. Network users, 4. Combined physical communication lines. The number of nodes X in the network is greater than or equal to two. All these elements are identified using identifiers common in the TCP/IP protocol stack, such as network IP addresses. The set of addresses connecting users and network nodes to the communication network does not overlap. The transmission of messages between network users occurs through network nodes, with the most secure connection being selected from all possible communication routes. Connections between network elements are characterized by only two values: the presence of a connection and its absence. Other parameters of the communication lines are considered constant and are not taken into account, as the most probable and easily implemented method of unauthorized monitoring of information exchange in the communication network is through connection to its nodes.

Fig. 1 illustrates a block diagram outlining the sequence of actions performed in the first option of selecting a secure route in the communication network of the developed method, where the following notations are introduced:

- {IP} - structural array;
- {ID} - identification array;
- IP_{ss} - the network address of the security server;
- ID_u - User ID;
- IP_u - user's network address;
- Y - the number of security parameters of network nodes to be considered;
- b_{xy} -Value of security parameter y of network node *x*, where x *= 1.2, ..., X, y = 1.2, ..., Y;*
- $k_{x\Sigma}$ - complex security indicator of each x network node;
- N_{ij} - the number of communication network graph trees corresponding to the set of possible communication routes between *i* and *j* network users, where *i = 1.2,..., j = 1,2,..., and i ≠ j;*
- K_{ij}^{avr} - the average security indicator of the communication route between network *i* and *j* users;
- N_{ij}^S **-** secure communication route between users of network *i* and *j*;
- Z_n- n number of graph tree vertices, where *n = 1,2,...,* N_{ij}, corresponding to the number of network nodes;
- **SS** - security server.
- In the second version, Fig. 2. the following additional notations have been introduced:
- {R} - an array of compatibility between R_u ranks of users and complex indicators of security of network nodes $k_{x\Sigma}$;

- R_u - Ranks of network users.

At the initial stage, initial data are set on the security server, including structural {IP} and identity {ID} arrays, security server address IP_{ss}, identifiers ID_u and IP_u addresses of users connected to the communication network, as well as security parameters for each network node X, where $x = 1, 2,..., X, Y \geq 2$ and their value b_{xy}, where $y = 1,2,...,Y,$ which are given in Table 1.

Table 1.
Initial data identifiers security parameters for each network node X

y x	1	2	…	Y
1	b_{11}	b_{12}		b_{13}
2	b_{21}	b_{22}		b_{23}
…				
X	b_{x1}	b_{x2}		b_{xy}

Structural array *{IP}* – stores data about the addresses of the IP_{SS} security server, IP_{Nn} nodes and IP_u network users, as well as information about the presence of a connection between them (Table 2), which is characterized by only two values, "1" - the presence of a connection and "0" - its absence.

Table 2.
Characterization the presence of connection

	IP_{SS}	IP_{n1}	IP_{n2}	IP_{n3}	IP_{n4}	IP_{n5}	IP_{ni}	IP_{nj}	IP_{nn}
IP_{SS}		1	0	0	0	0	0	0	0
IP_{n1}	1		1	1	1	0	0	0	0
IP_{n2}	0	1		0	1	1	1	0	0
IP_{n3}	0	1	0		1	1	0	1	0
IP_{n4}	0	1	1	1		1	0	0	1
IP_{n5}	0	0	1	1	1		0	0	0
IP_{ni}	0	0	1		0	0		0	0
IP_{nj}	0	0	0	1	0	0	0		0
IP_{nn}	0	0	0	0	1	0	0	0	

Identification array *{ID}* - the array stores data about ID_{SS} security server identifiers, ID_u of communication network users and corresponding IP_u addresses of network users and IP_{SS} security server addresses (Table 3).

Table 3.
Identification array *{ID}*

Network Host Address	Network Host Identifier
IP_{SS}	ID_{SS}
IP_{ui}	ID_{ui}
IP_{uj}	ID_{uj}
. . .	. . .
IP_{un}	ID_{un}

Security parameters of network nodes are established based on recognized standards from ISO/IEC JTC 1/SC 27. The values of security parameter y = 1 for b_{x1} nodes of the network are defined according to the specifications provided by the manufacturers of the network node devices, which can be obtained from physical addresses. For instance, let's consider a node N_{n1}, with a hypothetical physical address like 00:01:e3:3F:D4:E1. The first three values of this address may indicate the manufacturer, corresponding to a value of the security parameter $b_{11} = 0.3$. Similarly, the security parameter values b_{x1} for network nodes *Nn2-Nn5* are determined as $y = 1$, along with the security parameter values b_{xy} for all $Y \geq 2$.

For each node X of the network, based on its security b_{xy} parameters, the values of the complex security index $k_{x\Sigma}$ are calculated. The calculated indicators are presented in Table 4.

The complex security index $k_{x\Sigma}$ for each node x of the network is calculated either by summing $k_{x\Sigma} = \sum_{y=1}^{y} b_{xy}$ or by multiplying $k_{x\Sigma} = \prod_{y=1}^{y} b_{xy}$ or by the arithmetic mean of the node b_{xy} security parameters $k_{x\Sigma} = (\sum_{y=1}^{y} b_{xy})/y$.

Table 4.

The calculated indicators

Network Node	k_{Σ}
1	$k_{1\Sigma}$
2	$k_{2\Sigma}$
x	$k_{x\Sigma}$
X	$K_{X\Sigma}$

The method of calculating the complex security index $k_{x\Sigma}$ fundamentally does not impact the outcome of selecting a secure route. The computed values of the security complex index $k_{x\Sigma}$ for each node x in the examined variant of the communication network, considering the values of the corresponding security parameters b_{xy}, are provided in Tab.5.

Table 5.

Values of b_{xy} nodes

Network nodes $x = 5$	Host security settings $Y = 3$				x-node security complex index $k_{x\Sigma}$		
	$y = 1$	$y = 2$	$y = 3$		$\sum b_{xy}$	$\prod b_{xy}$	$(\sum b_{xy})/Y$
$x = 1$	0,3	0,13	0,4		0,83	0,0156	0,276666667
$x = 2$	0,3	0,16	0,4		0,86	0,0192	0,286666667
$x = 3$	0,2	0,1	0,34		0,64	0,0068	0,213333333
$x = 4$	0,5	0,2	0,25		0,95	0,025	0,316666667
$x = 5$	0,05	0,08	0,01		0,14	0,00004	0,046666667

Next, a matrix of neighboring vertices of the network graph is created. In this matrix, IP_{SS} addresses of network nodes and IP_a addresses of network users are organized into a structured array, along with details about the connections between nodes and network users. Methods for generating the matrix of neighboring vertices of a graph are well-documented [9]. The matrix representing the neighboring vertices of the communication network graph will take the following structure as is presented in Table 6.

Table 6.

The neighboring vertices of the communication network graph structure

$b=$

	Nn_1	Nn_2	Nn_3	Nn_4	Nn_5
Nn_1	0	1	1	1	0
Nn_2	1	0	0	1	1
Nn_3	1	0	0	0	1
Nn_4	1	1	0	0	1
Nn_5	0	1	1	1	0

Afterward, network ID_a, ID_{SS} identifiers, along with IP_a and IP_{SS} addresses of network users and security Server, are collected in the identification array.

Each n- tree of a communication graph, where $n = 1,2,\ldots,$ N_{ij} consists of $z_n$vertices corresponding to the number of nodes in the network. The total number of trees N_{ij} in the communication network graph between network users i and j can be determined by different methods. In the presented method, the total number of communication graph trees N_{ij} is formed by using the neighboring vertices of the matrix.

By deleting any row of the matrix B, we get the initial B_0 and the matrix B_0^Ttransposed with it:

$$B_0 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}; \; B_0^T = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

The calculation of the number of trees N_{ij} between users *i* and j of the communication network graph is performed by multiplying the obtained matrices B_0 and B_0^T, and then finding its determinant.

$$N_{ij} = |B_0 \times B_0^T| = \begin{pmatrix} 3 & 2 & 2 & 1 \\ 2 & 2 & 2 & 0 \\ 2 & 2 & 3 & 1 \\ 1 & 0 & 1 & 3 \end{pmatrix} = 5$$

Establishing communication routes between users based on the graph tree of the communication network entails identifying all potential communication paths while excluding blocked routes that are unsuitable for message transmission.

Reasoning and objectively selecting a potentially safe communication route from the set of N_{ij}*=5* between network users *i* and j involves calculating the average security indicator k_{ij}^{avr}**.** It is obtained as network nodes by calculating the complex security indicator, i.e. the arithmetic mean k_{Σ}^{n}, and includes connection *n-th* communication routes $k_{ij}^{avr} = (\sum k_{\Sigma}^{x})/z_n$.

As a result of calculating the complex security index of the network nodes in various methods, the communication routes formed between network users *i* and *j* with the average security index k_{ij}^{SS} are calculated. The results are presented in Table 7.

Table 7.

Values of the complex security indicator of network nodes

Route N_{ij} = 5	Number of nodes on *n*-route	Z_n number of nodes on the *n*-th route	Average safety indicator of the *n*-th route		
n = 1	123	3	0,78	0,0139	0,26
n = 2	1234	4	0,82	0,0167	0,27
n = 3	12345	5	0,68	0,0133	0,23
n = 4	235	3	0,55	0,0087	0,18
n = 5	2345	4	0,65	0,0128	0,22

A secure route between users *i* and *j* of network N_{ij}^{s} is selected based on the highest value of its average security index k_{ijn}^{SS} . If several routes with equal average safety values are found, the shortest route is selected from the identified routes. This means selecting the route with the smallest number of Z_n nodes in it. Afterward, the selected route is memorized. From the results presented in the table, it can be seen that for all calculation methods, the second *n = 2* routes have the highest values of the average security index k_{ij}^{avr}, which are shaded accordingly. It can be concluded that the calculation method of $k_{x\Sigma}$ does not directly affect the result of choosing a secure route. This way, a set of all possible route options between all users of the network is formed.

The result is generated via messages that include memorized routes N_{ij}^{S} between *i* and all *j* users, ID_{aj} identifiers, and IP_{aj}addresses of all j users. Afterward, generated messages are sent to all *i*-users in the network. Thus, each user of the network is informed about secure routes that can be established between all other users of the network.

To transmit messages between users, the message ID_a is selected based on the recipient's IP_a address and the secure N_{ij}^{S} route to the user, after which the message is delivered to the recipient. Well-known routing protocols such as RIP, OSPF, NLSP, BGP serve to transmit user information (source-specified routing) using routing methods and facilitate information exchange from the source to the receiver along a designated route. Thus, users have the option to send messages directly via a designated secure route. When a new user connects to the communication network, a message is generated for them, containing the IP_{n4} address of the N_{n4} network node, the recipient's ID_{an} identifier, and the recipient's IP_{an} address. The generated message is sent to the security server, where it is stored in structural and identification arrays, updating the information in the communication network's security server. Following a similar process as described earlier, secure communication routes are selected and stored between the new user and all *j* users of the network.

At the next stage, a message is formed containing information about the network structure and its users. These messages, which include stored information about secure communication routes, are generated from each existing user *j* of the network to the new user and sent accordingly. Consequently, the new user is informed of secure routes to all other users in the network, while the remaining users are notified of available secure routes to the new user within the network.

In the initial version of the method, secure routes are selected based on the communication network's structure, initial data about network nodes and users, and the calculation of complex security indicators for network nodes. By managing information exchange routes, the aim is to enhance the security of communication between users within the network.

The second variant of the method introduces a new concept of ranks for network users. In this version, the selection of a secure route between network users occurs only upon the user's request and based on predetermined user ranks. If a secure communication route is unavailable, the user is notified accordingly.

Figure 2 illustrates the block diagram depicting the sequence of actions for the second version of the method, which involves the selection of a secure route in the communication network.

At the initial stage, similar to the first variant of the method, the initial data is specified on the security server.

In the initial data, unlike the first variant of the method, the security index k^{perm} of the permissible route is not specified. In addition, compared to the second variant of the method, the correspondence matrix of R_a rank *{R}* of the users and the complex security indicators $k_{x\sum}$ of the network nodes are introduced. The array *{R}* contains the corresponding values of the ranks of network nodes $R_a \geq 2$ users and complex security indicators $k_{x\sum}$. For example, the user rank $R_a = 1$ corresponds to the $k_{x\sum}$ values of complex security indicators of network nodes from 0 to 0.2. After setting the initial data, similarly as in the third variant of the method, for each network node *x*, the complex security index $k_{x\sum}$ is calculated from the values of its security parameters b_{xy}. The calculated indicators are given in the table.

In the initial data, unlike the first variant of the method, the security index k^{perm} of the permissible route is not specified. Additionally, compared to the second variant of the method, the correspondence matrix of R_a rank *{R}* of the users and the complex security indicators $k_{x\sum}$ of the network nodes are introduced. The array *{R}* contains the corresponding values of the ranks of network nodes $R_a \geq 2$ users and complex security indicators $k_{x\sum}$. For example, the user rank $R_a = 1$ corresponds to the $k_{x\sum}$ values of complex security indicators of network nodes from 0 to 0.2. After setting the initial data, similarly as in the third variant of the method, for each network node *x*, the complex security index $k_{x\sum}$ is calculated from the values of its security parameters b_{xy}. The calculated indicators are given in the table.

Subsequently, similar to the first variant, the adjacency matrix of the vertices of the network graph is created. In the event of connecting a new user to the communication network, similar to the third variant of the method, a message is generated containing the *NS4* IP_{ns4} address of the network node to which they are connected, as well as the ID_{an} and IP_{an} addresses of their identifiers. The generated message is sent to the security server, where it is stored in structural and identification arrays. This process updates the information about the structure of the communication network and network users. Then, a message containing the user-recipient identifier ID_a is formed. Similarly, to the third variant of the presented method, its address IP_a and secure route N_{ij}^{s} are selected. Afterward, the message is transmitted to the receiving user using the chosen route.

In addition, as proposed in the second variant of the method, the set of possible communication routes between network users *i* and *j* is created in the form of trees of the communication network graph N_{ij}. Unlike the first variant of the method, the secure communication route N_{ij}^{s} between the *i*- and *j*-users of the network is selected if the complex security indicators $k_{nx\sum}$ of the nodes included in it correspond to the equal or higher rank R_{ai} of the *i* user of the network. For example, for network user *i* $R_{ai} = 1$, the complex indicators of security of $k_{nx\Sigma}$ nodes satisfy the selected secure communication route N_{ij}^{s} and are in the range of values from 0 to 0.2 (Table 8).

Table 8.

The network is selected if the complex security indicators of the nodes are included in it

Rank of Network users $R_a \geq 2$	$k_{x\Sigma}$
1	0…0,2
2	0,2…0,4
3	0,4...0,6
4	0,6...0,8
5	0,8...1

In this way, a secure communication route between users *i* and *j* is selected at the request of user *i* of the network and according to the predetermined ranking of the users of the network. In addition, as in the first variant of the method, secure route N_{ij}^{s} including backup route is protected, message generation N_{ij}^{s} and j user's address IP_{aj} and the generated message is sent to network *i* user.

If there is no secure route between network users *i* and *j*, meaning there is no route among the possible communication routes where the security indicators of the nodes included in it match the rank of the user, a response is generated and sent to network user i indicating the absence of a secure route to network user *j*.

Contrary to the first variant of the method, the secure communication route N_{ij}^{s} between the *i*- and *j*-users of the network is chosen if the complex security indicators $k_{nx\sum}$ of the nodes included in it align with the equal or higher rank of information transmitted in the network $R_{inf\ i}$. For instance, if the information to be transmitted to the network user *i* has a rank of $R_{inf\ i} = 1$, then the security complex indicator $k_{nx\sum}$ in the chosen secure communication route N_{ij}^{s} falls within the range of values from "0 to 0.2".

The complex security indicators $k_{nx\sum}$ of the nodes involved in the established communication routes serve as the foundation for an objective evaluation of the selected secure communication paths between network users. They enable us to take into account the essential conditions required for choosing a secure route in communication.

Therefore, the second algorithm of the method also achieves the intended technical outcome - enhancing the security of communication among network users.

Figure 3 illustrates an example of selecting a secure route to a security server in a communication network between users *i* and *j*.

The complex security indicators $k_{nx\sum}$ of network communication nodes and their security parameters b_{xy} are calculated, and the values are presented in Table 3.

From the example provided, it's evident that utilizing the second version of the secure route enables the exclusion of transit nodes with a low level of security within the network. This helps mitigate the risk of unauthorized access to messages transmitted by users in the network. In this example, as illustrated in the calculation table, N_{S5} demonstrates high values of the network security index $k_{5x\sum}$ and user security parameters b_{5y}, which are highlighted accordingly (Figure. 3).

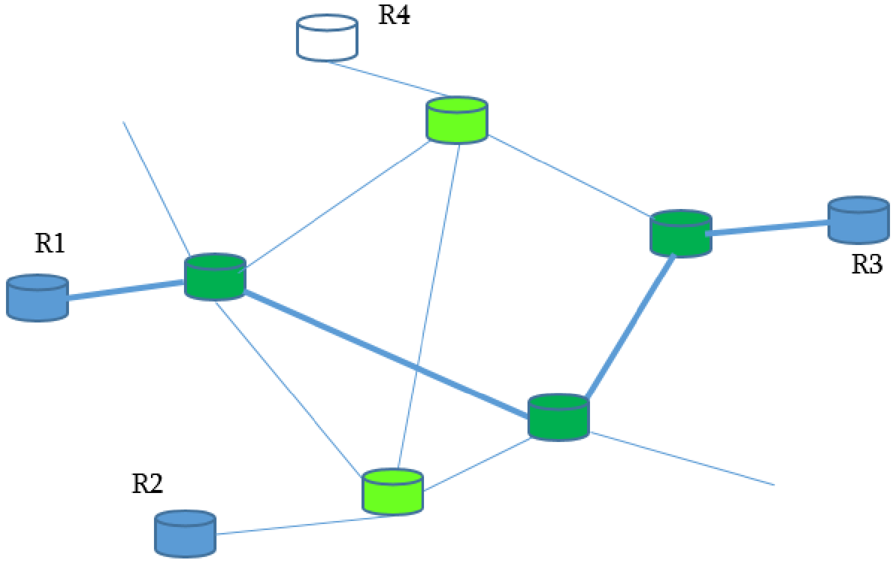

Fig. 3. An example of selecting a secure route to a security server in a communication network

Table 9.

The indicators of complex security $k_{nx\Sigma}$ for communication nodes

Network node	Security settings of network nodes b_{xy}			Security indicator of Network node
	y=1	*y=2*	*y=3*	$k_{x\Sigma}$
Nn = 1	0,3	0,13	0,4	*0,83*
Nn = 2	0,3	0,16	0,4	0,86
Nn = 3	0,2	0,1	0,34	0,64
Nn = 4	0,5	0,2	0,25	0,95
Nn = 5	0,5	0,08	0,01	0,14

Thus, the chosen secure communication pathway, delineated by bold lines, between users *i* and *j* traverses through the transit nodes of the network, characterized by the highest security rating. This minimizes the likelihood of unauthorized interference in the exchange of information between network users.

Conclusion

From the examples provided, it is evident that utilizing the proposed method for selecting a secure route enables the exclusion of low-security transit nodes within the network, which significantly reduces the risk of unauthorized interference with transmitted messages.

Based on the findings presented in the paper, it can be concluded that both options of secure route selection in the proposed method led to enhanced communication security by effectively controlling information exchange routes among users in the communication network.

The algorithm represents a novel approach to addressing security concerns and aims to mitigate the drawbacks associated with existing methods of routing message packets in computer networks.

References

1. **Halabi B.,** Internet Routing Architectures, 2nd Edition, Cisco Press, 2001
2. **Medhi D., Ramasamy K.**, Network Routing Algorithms, Protocols and Architectures, 2017
3. **Bonaventure O**. Computer Networking: Principles, Protocols and Practice. Rel.0.25, 2011
4. **Stack E.** Computer Networking: The Complete Guide, 2019
5. **Goodrich M.T**. Efficient and Secure Network Routing Algorithms, 2001
6. **Vyas D., Patel R., Ganatra A.** Survey of Distributed Multipath Routing Protocols for Traffic Management, International Journal of Computer Applications (0975-8887), Vol. 63-No.17, February 2013, p. 42-48. https://research.ijcaonline.org/volume63/number17/pxc3885652.pdf
7. Classification of Routing Algorithms, https://www.geeksforgeeks.org/classification-of-routing-algorithms/
8. Fixed and Flooding Routing algorithms, 2013, https://www.geeksforgeeks.org/fixed-and-flooding-routing-algorithms/
9. **Busacker R.G., Saaty T. L.** Finite Graphs and Networks, M,1965
10. **Forshaw J.** Attacking Network Protocols. No Starch Press, 2017
11. **Jin, J., & Ahn, S.** A Multipath Routing Protocol Based on Bloom Filter for Multi-hop Wireless Networks. Mobile Information Systems, 2016, 1-10.
12. **Yih-Chun Hu, Perrig A.** … Efficient Security Mechanisms for Routing Protocols, https://www.cs.rice.edu/~dbj/pubs/ndss03-efficient.pdf
13. **Myoung Lee G., Choi Jin S**. A survey of multipath routing for traffic engineering, https://shorturl.at/IO278

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of CNDCGS 2024 and/or the editor(s). CNDCGS 2024 and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.