This study investigates processes of message transmission via the Internet to a virtual private cloud using Shamir's scheme.

The evolution of the infocommunication infrastructure has led to an increase in the role of cloud services. As a result, the requirements for information protection along the paths of message delivery to the clouds are increasing.

The task addressed is to reduce the probability of compromising messages transmitted by a communication system..

The parameters of the information transmission system that affect the probability of compromise of messages transmitted to the virtual private cloud have been studied. The most vulnerable elements in the communication system were found. To practically implement the Shamir scheme via the Internet, the possibilities of using existing routing technologies were studied.

For information transmission systems with ideal nodes, the overall level of compromise significantly depends on the probability of compromise of one path element, especially for remote clouds. An increase in the probability of compromise on a single hop from 0.03 to 0.1 for 10 hops in a three-path system leads to an increase in the total compromise from 0.02 to 0.28.

Protecting intermediate nodes from attacks is critical for remote clouds. With 10 hops in a three-way communication system, the overall probability of compromise increases fourfold from 0.02 to 0.08 with the same impact of an individual node and hop.

Protecting end nodes for a communication system is of significant importance compared to nodes along the paths. The probability of compromise of end nodes, equal to 0.1, gives an increase in the total level of compromise from 0.03 to 0.21

Keywords: probability of message compromise, Shamir's secret distribution method, virtual private cloud

UDC 004.056
DOI: 10.15587/1729-4061.2025.348570

REDUCING THE LEVEL OF MESSAGE COMPROMISE IN INFORMATION TRANSMISSION SYSTEMS TO VIRTUAL PRIVATE CLOUDS USING SHAMIR'S SCHEME

Artem Marchuk
Corresponding author
PhD*
E-mail: artem.marchuk@nure.ua
Tetiana Kovalenko
PhD*
Svitlana Shtangey
PhD*
Olena Linnyk
PhD
Department of Physical Foundations of Electronic Engineering**
*V.V. Popovskyy Department of Infocommunication Engineering**
**Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166

Received 02.10.2025
Received in revised form 08.12.2025
Accepted date 18.12.2025
Published date 30.12.2025

How to Cite: *Marchuk, A., Kovalenko, T., Shtangey, S., Linnyk, O. (2025). Reducing the level of message compromise in information transmission systems to virtual private clouds using the Shamira scheme. Eastern-European Journal of Enterprise Technologies, 6 (9 (138)), 100–113. https://doi.org/10.15587/1729-4061.2025.348570*

1. Introduction

The growth of information volumes transmitted in the modern world between objects of infocommunication infrastructure leads to a significant complication of networks, hardware, and software, which, in turn, increases the risks of information damage. On the other hand, the methods of influence and hacking of transmitted information flows by attackers are being improved. Therefore, the development of secure communication systems must comply with modern information security standards [1, 2], which are constantly being improved.

Modern infocommunication systems increasingly use Virtual Private Cloud (VPC) infrastructure for data storage and processing, which ensures scalability and flexibility of services. However, the transmission of messages to VPC occurs via the Internet, which is an open and potentially dangerous environment. Even the use of conventional security protocols, such as VPN, TLS, or IPsec, does not guarantee full system stability in the event of compromise of intermediate nodes of the route. This necessitates devising additional mechanisms to reduce the level of compromise and resistance to attacks.

One of the promising approaches is the use of multipath routing in combination with the well-known secret sharing method – Shamir's Secret Sharing (SSS) [3]. The message is divided into fragments that are transmitted via independent routes, which significantly reduces the probability of compromising all information when capturing part of the channels. And the use of the SSS secret sharing method provides the ability to choose a threshold parameter k at which the message cannot be restored if there are fewer parts. This provides mathematically justified cyber resilience and creates conditions for increasing the level of security of data transmitted to virtual cloud infrastructures via the Internet.

The results of the study of methods for reducing the level of message compromise in systems for transmitting to VPC clouds via the Internet will make it possible to improve communication systems used in practice.

The requirements for the security of information flows in the infocommunication environment are constantly increasing; therefore, research into solving the issues of transmitting

messages via the Internet with a low probability of compromise is relevant.

2. Literature review and problem statement

The task of using the Shamir scheme with multipath routing between two nodes with intersecting paths is solved in [4, 5]. Comparisons of the probabilities of compromising messages transmitted in networks with intersecting paths with networks in which the paths do not intersect are given. Recommendations for reducing the probability of compromising a message by using intersecting paths are devised. An analytical solution is proposed for several simple network configurations but research questions on the use of the Shamir algorithm for networks of practical importance remain unresolved. In addition, the issue for the Internet network is not solved.

In work [6], the task of increasing the protection of information transmission using the Multipath TCP (MPTCP) protocol is solved when a mobile terminal is simultaneously connected to several network interfaces. The authors proposed using a method of distributing data over different paths. An attacker cannot obtain data even if s/he observes traffic on a part of all paths. An example with two 4G and Wi-Fi interfaces in a smartphone is considered. The MPTCP module is located on top of TCP and ordinary programs are not aware of the existence of the superstructure. The MPTCP protocol establishes a connection with two or more TCP subflows. The work provides one of the options for implementing multipath routing, which can be used to organize the Shamir scheme over the Internet using the MPTCP protocol. However, the Shamir scheme was not used by the authors to increase the protection of transmitted information. The increase in message security was achieved by scattering data over two paths.

In subsequent works, the possibilities of using the modernized MPTCP protocol [7] to increase the reliability of information transmission by reserving channels were investigated; the security problems of multipath TCP [8] were also considered. The impact of such attacks as denial of service DoS and DDoS, Session Hijacking, SYN interception, etc. were investigated.

To protect data transmission over the MPTCP protocol, a special protocol, Secure Connection Multipath TCP (SCMTCP) [9], was devised, which used elliptic curve cryptography to generate a secret key. This protocol also used a third-party certification center to ensure the authenticity of public keys exchanged between communicating parties.

In the reviewed studies [6–9] on the MTCP protocol the problems of multipath routing with a small number of paths were solved, which makes the use of the Shamir scheme inefficient due to the use of small-degree polynomials. This significantly reduces the level of information protection under the Shamir scheme. However, the problem of organizing a sufficient number of paths to implement the Shamir algorithm with an increased level of message protection was not solved in those papers. The probabilities of compromising messages transmitted over the network were also not considered and not solved.

The capabilities of the Shamir algorithm are described in papers on the use of the Multiprotocol Label Switching (MPLS) protocol in the Internet.

MPLS technology is designed primarily to provide high-speed packet delivery. The MPLS network architecture does not provide encryption of headers or payload. Security issues were not the main issue in the development of this technology. In [10], it was proposed to integrate it with the Shamir SSS secret data sharing scheme to improve security in the MPLS network. The paper solves the problem of comparing the performance of two secret discovery algorithms: the classic Shamir scheme and a modified scheme using only the XOR operation. It is shown that the proposed secret recovery algorithm significantly reduces the processing time for secret distribution and recovery. However, the authors did not study the impact of the values of the combination (k, n), where k is the threshold and n is the number of paths, on the level of information protection when transmitting over the Internet using the SSS scheme. The problem of the impact of elements along the paths from the user to the VPC cloud on the probability of message compromise is not resolved.

MPLS technology is vulnerable to failures due to its architecture. Path recovery is mainly provided by redirecting traffic around the node that failed the LSP path, which leads to significant recovery delays and can lead to packet loss. Such vulnerabilities are critical when transmitting important information. In [11], to ensure fault tolerance in MPLS networks with Multiprotocol Label Switching Traffic Engineering (MPLS TE), the use of the Shamir algorithm with a modified threshold distribution scheme (k, n) and multipath routing is proposed. An IP packet entering the MPLS network was divided into n parts, which were sent to n LSP paths of the MPLS network. To reconstruct the original IP packet, it is enough to obtain k parts. The proposed modernization of the threshold distribution scheme in the Shamir scheme eliminates both single and multiple failures in the communication system. But the probability of message compromise during transmission over the Internet was not considered and solved by the authors.

In [12], an analysis of MPLS networks and ways of their further development are provided. In addition to the technology with MPLS TE traffic engineering, traffic engineering technologies taking into account various MPLS TE DiffServ services and Multiprotocol Label Switching Transport Profile (MPLS TP) technology are considered promising. The MPLS TP standard extends MPLS technology for use in transport networks, combining packet transmission functions with the reliability and capabilities of conventional transport networks such as SDH/SONET. To solve the problem of increasing the level of secure information transmission, it is proposed to use MPLS TE technology with 1 + 1 and 1:1 redundancy. But redundancy cannot provide a high level of message protection, which is provided by the Shamir scheme. The issue of the probability of compromise of messages transmitted in the network is not solved in the work.

Practical use of secret data exchange to increase confidentiality in cloud systems based on the Shamir algorithm is proposed in [13]. The authors developed the Datachest application for storing confidential data in commercial cloud data storage systems using Multicloud technology in combination with the Shamir scheme. It is proposed to divide cryptographic keys into shared resources and store them in different clouds. According to the Shamir algorithm, not the keys themselves were transmitted, but information for their recovery. To do this, polynomials with random coefficients and a secret, which is a free member of the polynomial, were generated at the transmitting end, then for each polynomial the mod residues from the prime number chosen by the sender were calculated. The prime number and individual

mod values were transmitted to each cloud. At the receiving end, the transmitted secret was calculated based on the mod residues stored in different clouds and the prime number that was transmitted to the end user. The power of the polynomial was determined by the selected threshold and was equal to the number of clouds for storing the secret particles. Several cloud providers were used. Each cloud received only one shared resource. After the first stage – key transfer using the Shamir algorithm – the transfer of the encrypted information stream began. This solution improved the security of storing confidential user data in the cloud storage. The proposed Datachest application was used to exchange secret data in the Internet of Things technology. However, the issues of creating paths to the clouds and calculating the levels of compromise and the effects of elements along the paths on the probability of compromising the transmitted messages were not considered in the work.

Cloud servers can store virtually unlimited amounts of data. In this case, a cloud with servers can be considered a centralized object. There are various types of risks associated with centralization, for example, a failure in one of the servers. To avoid such a failure, third parties are involved to provide data backup. To eliminate the need for third parties, in [14] it was proposed to use blockchain to ensure trust and transparency. A decentralized storage was used, which allowed storing data independently on several network nodes in the form of a distributed registry. The Inter Planetary File System (IPFS) file system, which is a P2P peer-to-peer architecture, was proposed as a solution. In this architecture, there is no risk of failure at a single point. It works similarly to the bittorrent technology. Data is stored on a decentralized platform – the IPFS server. To request data, the user is authenticated using digital signatures. Only after this is the request processed, otherwise the transaction will be aborted by the blockchain. Data security was achieved by integrating the encryption scheme into the hashes of the uploaded data on IPFS. These hashes were encrypted by the data owner using the SSS Shamir secret sharing scheme, which divided the hash into n encrypted resources. Encrypted resources were stored in a smart contract. But the problems of creating paths to the clouds and the probability of compromise of transmitted messages in the work have not been solved.

From our review of the literature, a number of conclusions can be drawn. Existing works on the study of the probabilities of message compromise [4, 5] consider issues of transmission through several separate network configurations that do not work as part of the Internet. The level of compromise was calculated for individual cases of compromise values on line segments without taking into account the influence of equipment in the nodes. The choice of compromise thresholds in the Shamir algorithm for schemes for building a communication system with different probabilities of compromise in separate paths and a different number of paths was not studied. The issue of organizing territorially distributed paths on the Internet has not been studied.

From papers [6–12], it can be concluded that the works on the study of secure information transmission over the Internet are focused on the use of backup methods and the improvement of secure information transmission protocols. The issue of creating multiple paths over the Internet for the Shamir scheme was not considered.

In other studies [13, 14], the use of the Shamir scheme with multiple cloud storages and the problem of integrating blockchain technology with Shamir technology were studied. The study of the probability of compromise of a message transmitted over the Internet to virtual private clouds was not conducted.

Thus, the cited papers solved the problems of either improving algorithms for secure message transmission or studying the probability of compromise of messages transmitted over simple network configuration models that do not take into account Internet protocols. Therefore, the processes of message transmission over the Internet using the Shamir scheme to virtual private clouds have not been fully examined. There are a number of unsolved problems in finding ways to reduce the probability of compromise of messages transmitted by the information transmission system.

Practical methods for implementing the Shamir scheme for transmitting messages over the Internet have not been studied. The probability of compromise from the number of hops from one to a neighboring router on the way to the VPC via the Internet and the impact of router compromise on the way of transmitting message particles via the Internet to the VPC have not been identified. No studies have been found on the probability of compromise of messages transmitted using the Shamir scheme to virtual private clouds, depending on the compromise threshold, which varies from the minimum possible to values equal to the number of paths to the VPC cloud via the Internet. The possibilities of using the main existing routing methods in the Internet for the practical implementation of a set of territorially separated paths operating simultaneously for transmitting message particles to the VPC virtual cloud using the Shamir scheme have not been studied.

3. The aim and objectives of the study

The purpose of our study is to increase the level of information protection in information transmission systems to virtual private clouds via the Internet using the Shamir scheme. This will enable the practical implementation of information transmission systems with a low probability of message compromise.

To achieve this goal, the following tasks were set:

– to build a model for transmitting messages from the user's server to a virtual private cloud via the Internet;

– to investigate the influence of the number of hops to the virtual cloud VPC on the probability of message compromise at different values of the probability of compromise on one hop in the Internet and the number of geographically separated paths;

– to determine the influence of the probability of compromise of intermediate and end nodes on the probability of message compromise;

– to investigate the influence of the compromise threshold and its combination with the number of paths in the Internet on the level of message compromise when using the Shamir scheme;

– to investigate the possibility of using conventional routing methods on the Internet for the purpose of practical application for organizing message transmission using the Shamir scheme to virtual private clouds via the Internet.

4. The study materials and methods

The object of our study is the processes of transmitting messages via the Internet to a virtual private cloud using the Shamir algorithm to increase the level of information protection in communication systems.

The paper tested the hypothesis that the probability of compromising a message transmitted from a user to a virtual private cloud via the Internet is a function of the number of paths, the compromise threshold in the Shamir scheme, as well as the probabilities of compromise of network infrastructure communication line elements. It was assumed that reducing the probability of compromising messages could be achieved by increasing the number of paths and choosing a combination of the compromise threshold with the number of paths.

The probabilities of compromising individual nodes and segments of paths between nodes are assumed to be the same along the paths.

The threshold value in the Shamir algorithm, which is an integer, is taken in the range from two to the maximum, which is equal to the number of paths in different implementations of the algorithm.

In a Shamir data transmission system, each path consists of sequentially connected nodes and lines between nodes. The passage of a message through a path can be viewed as a sequence of independent events E_i, where each event corresponds to the successful operation of the i-th element of the path.

If the probability of success p_i of a single event is E_i, then according to classical probability theory [15–17], the probability of the total success of all events along a path containing n consecutive elements is

$$P\left(E_{i1},E_{i2},...E_{in}\right)=\prod_{j=1}^{n}p_{ij}, \quad (1)$$

where p_{ij} is the probability of success of a single event.

Similarly, if for each element the probability of failure p_{ij}^{ns} is known, then the total probability of success is

$$P\left(E_{i1},E_{i2},...E_{in}\right)=\prod_{j=1}^{n}\left(1-p_{ij}^{ns}\right). \quad (2)$$

Accordingly, to calculate the probability of the overall "failure" of a message passing along a path with n elements, the following formula is used

$$P\left(E_{i1}^{ns},E_{i2}^{ns},...E_{in}^{ns}\right)=1-\prod_{j=1}^{n}\left(1-p_{ij}^{ns}\right). \quad (3)$$

The paths in the communication system according to the Shamir scheme operate in parallel (simultaneously). Compromise events on different paths are considered independent. In classical probability theory [15–17], parallel independent events can be combined in two ways:

– "OR" – when the "success" or "failure" of at least one of the events determines the outcome of the entire system. In this case, the total probability is the probability of at least one event occurring;

– "AND" – when the outcome is considered as the joint "success" or "failure" of all parallel events, i.e., all events must occur simultaneously.

For the paths in the communication system according to the Shamir scheme under study, the case "AND" occurs. For example, for the general event "not successful" for the probability of parallel events

$$P_{total}^{ns}=\prod_{k=1}^{m}P_k\left(E_{i1}^{ns},E_{i2}^{ns},...E_{in}^{ns}\right), \quad (4)$$

where m is the total number of parallel events.

For mathematical modeling of the Shamir threshold scheme (n, k) with the total number of parts of the secret k, and its recovery is possible provided that at least n parts are obtained, the binomial distribution is used. According to classical probability theory [15–17], if each part is transmitted independently with the same probability of success p, then the probability that exactly n successful results will be obtained as a result of k independent attempts is described by the binomial

$$P_n=\sum_{j=n}^{k}\binom{k}{j}p_j\left(1-p\right)^{k-j}. \quad (5)$$

The formula summarizes the probabilities of all possible events, where the number of successful events j, starting from $j = n$ to k. The binomial coefficient indicates the number of options for choosing j successful outcomes from k events. The probability p_j is the probability of success j, and $(1 - p)^{k-j}$ is the probability that there will be $(k - j)$ failures.

The following software was used to conduct the research: MATLAB (USA) and Python.

5. Results of research on the probability of message compromise depending on communication system parameters

5. 1. Construction of a model for transmitting messages from a user to a virtual private cloud via the Internet

A message to a virtual private cloud Virtual Private Cloud (VPC) travels (Fig. 1) from the user's server S_1 through a short segment of the line to the router R_1, which connects via the Internet to router R_2, which is an access point to the VPC network. The VPC network can have a different architecture, for example, based on SDN technology and include thousands of servers and tens of thousands of router ports. The user in the cloud is served by server S_2.

To increase the level of security of messages transmitted to a virtual private cloud, the Shamir scheme [3] is used. The message is divided into m parts with a compromise threshold of k. Parts of the message are transmitted along m paths, each part along a separate path. The main environments where the paths run are the Internet and the VPC cloud.

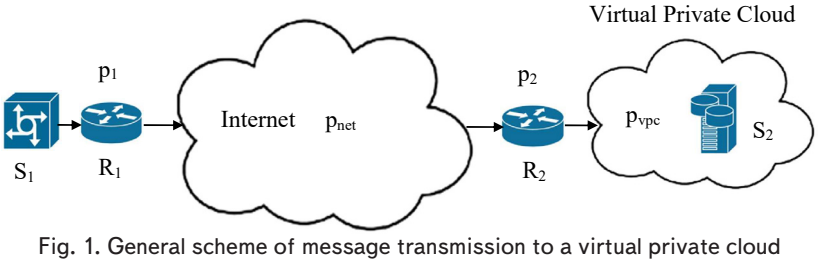


Fig. 1. General scheme of message transmission to a virtual private cloud

The VPC cloud is an isolated cloud environment with its own secure network, within which all elements are under constant control and management of information security tools. To ensure a high level of security and, accordingly, a low probability of compromise of transmitted messages, many tools are used: traffic vulnerability monitoring scanners, intrusion detection and prevention systems, firewalls, and so on. Of course, no system can be completely free from

compromise, but compared to the Internet, the level of compromise of the VPC network can be considered quite small.

In systems with high security requirements, the elements of access to the Internet and the cloud are usually controlled and protected. But the probability of attacks on them is high. Therefore, the study of the effects of end nodes on the level of overall compromise is also important.

The main element of influence on the overall level of probability of message compromise in the communication system is the Internet. This is explained by a very large number of elements: nodes with equipment, communication lines between them, and most importantly, the unpredictability of routes that constantly change according to protocols, usually dynamic routing, for example, OSPF. Therefore, we shall pay attention to the processes of message passage through the Internet.

The first problem is the factor of the user's distance from the access point to the VPC cloud. There can be different options from small – a few hops to significant distances of dozens of hops, and when the Internet network is overloaded, the number of hops can increase significantly due to dynamic routing.

Experimental pinging to access points of well-known clouds, such as Amazon WEB Service (AWS), Google Cloud Platform (GCP), and Azure, located in different cities in Europe, showed that the number of hops was approximately from 10 to 25. Sometimes it was more, which is explained by the above reasons from the level of network load, as well as the presence of access points to the cloud in different cities for the same service provider. In the case of a private VPC cloud, network access points can be located both at similar distances and at distances of only a few hops.

The second problem is the complexity of creating a set of geographically separated paths in the Internet network that work simultaneously.

The developed model of message transmission from the user to the virtual private cloud VPC via the Internet is shown in Fig. 2.

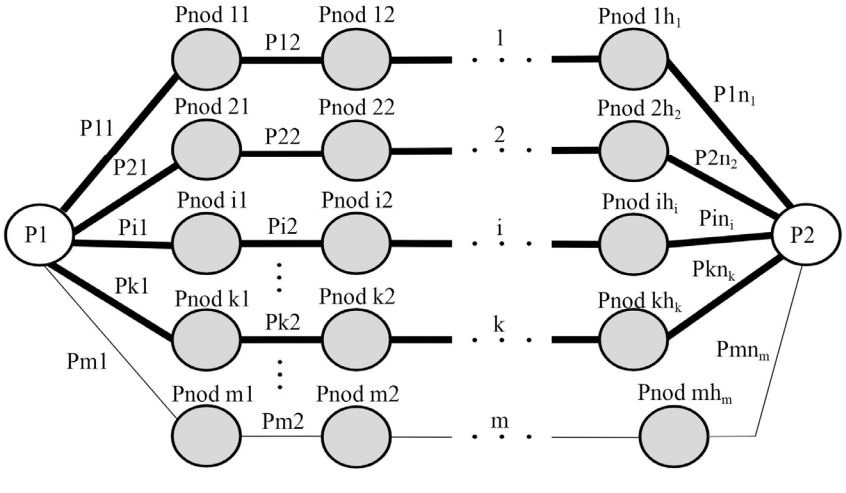


Fig. 2. Model of message transmission from the user to the VPC virtual private cloud via the Internet

A message transmitted over the Internet to a virtual private cloud is divided into m parts, each of which is transmitted along a separate path. There are m parallel paths in total, which are always used. Each path consists of a set of intermediate routers connected in series by communication lines.

To obtain a secret, an attacker must have access to any group of at least k paths of a total number m. The compromise threshold k in the Shamir scheme can be equal to or less than m. The model shows the case when $k < m$. Paths from 1 to k are indicated by bold lines. It should be noted that the group of paths from one to k is not necessarily chosen in ascending order of index. It can be any combination of k paths from a total number of m paths.

The probabilities of message compromise on individual segments of each of the m paths between neighboring nodes of the communication line were denoted by p_{ij}, where j varies from one to the number of segments n_i on path i.

As for the probability of compromise at nodes, there are two different processes of influence at the end nodes and nodes along the paths. At the two end nodes, all paths converge, so the external influence obeys different rules compared to the intermediate ones. The probabilities of compromise at the end nodes are p_1 and p_2.

The probabilities of compromise of intermediate nodes along the paths are denoted by p_{nod} with indices that determine the path number from one to m and the intermediate node number from one to h_i, where h_i is the number of intermediate nodes in the i path. The number of intermediate nodes is always one less than the number of segments $h_i = n_i - 1$.

5. 2. Investigating the influence of the number of hops to the virtual cloud on the probability of message compromise

In the message transmission model (Fig. 2), all channels in each path are arranged sequentially, and the paths in the Internet cloud are "parallel" to each other, and there is a joint compromise of all independent events in the paths – an "AND" type event. Therefore, for the first stage of research, we can use the well-known formulae of classical probability theory.

Distances in the Internet are estimated by the number of hops – the number of data packet hops from one router to the next that the packet overcomes on its way to the end user. The more hops on the path, the longer and more complex the route. As a result, the level of compromise and the delay in message transmission may increase. Taking into account the above, the formulae for the probability of message compromise are:

$$P_{comp} = \prod_{i=1}^{m} p_i, \tag{6}$$

$$p_i = 1 - \prod_{j=1}^{n_i} \left(1 - p_{ij}\right), \tag{7}$$

where m is the number of paths; n_i is the number of hops in path i; p_i is the probability of compromise of path i; p_{ij} is the probability of compromise of hop j of path i.

The above formulae are used for the case when $m = k$, where k is the compromise threshold in the Shamir algorithm; the probabilities of compromise of nodes are not taken into account.

The influence of the user's distance factor from the access point to the VPC cloud is studied. The probabilities of message compromise when passing paths from the number of hops n for different levels of compromise p_{ij} at a distance of one hop are considered. All probabilities of compromise on

all hops of one path are considered the same. Calculations are performed for five values of the probability of compromise on one hop p_{ij} from 0.03 to 0.2, and the number of paths m increases from one to ten. The results of our calculations are shown in Fig. 3.

Analysis of the calculation results reveals a significant dependence of the probability of message compromise P_{comp} on the probability of compromise of one path element p_{ij}. For one path (Fig. 3, *a*) at small p_{ij}, message compromise increases with increasing number of hops slowly (at $p_{ij} = 0.03$ for $n = 10$ probability $P_{comp} = 0.26$). With increasing probability p_{ij}, compromise quickly reaches values that are unacceptable for practical use of the communication system (at $p_{ij} = 0.2$ for $n = 10$ probability $P_{comp} = 0.89$).

With the number of paths $m > 1$ due to the organization of parallel paths, the probability of message compromise decreases. As can be seen from the plots (Fig. 3, *b*), even at a value of $m = 2$, the message compromise for small values of hop probability $p_{ij} = 0.03$ significantly decreases with an increase in the number of hops by approximately 2 times compared to $m = 1$, for example, for $n = 25$ – from 0.53 to 0.28. But the use of the Shamir scheme for the minimum $k = m = 2$ does not provide a high level of protection.

Further increase in the number of paths to $m = 3$ and use of a quadratic polynomial gives even greater gain. At $p_{ij} = 0.03$ the probability P_{comp} compared to one path decreases for $n = 25$ from 0.53 to 0.15. (Fig. 3, *c*). With a significant increase in m, for example, to 10, we have a significant gain in protection against compromise for large distances in the number of hops n. For $n = 25$ there was a decrease in P_{comp} from 0.53 to 0.002. In this case, the probability of compromise may be acceptable for practical use for access to the ports of the edge router of a cloud remote up to 25 hops, especially for small probabilities on one hop.

Such results are especially important when connecting to clouds located outside Ukraine. The number of hops, as a rule, can be, as noted earlier, based on the results of experimental measurements, from 10 to 25. Sometimes more, with increasing Internet load and the influence of dynamic routing.

5. 3. Investigating the influence of the probability of node compromise on the probability of message compromise

It is necessary to pay attention to the presence of equipment in the network nodes that can be attacked. Therefore, it was important to study the influence of compromise in the nodes on the overall level of message compromise. The nodes are located in the path sequentially, so formula (7) is easy to improve. At the first stage of the research, the influence of intermediate nodes was considered without taking into account the two end nodes that are common to all paths.

Formula that takes into account the influence of compromise of intermediate routers in nodes along the paths is

$$P_{comp} = \prod_{i=1}^{m}\left(1-\prod_{j=1}^{n_i}\left(1-p_{ij}\right)\cdot\prod_{h=1}^{n_i-1}\left(1-p_{ih}\right)\right), \quad (8)$$

where p_{ij} is the probability of compromise of hop j in path i; p_{ih} is the probability of compromise of intermediate node h in path i.

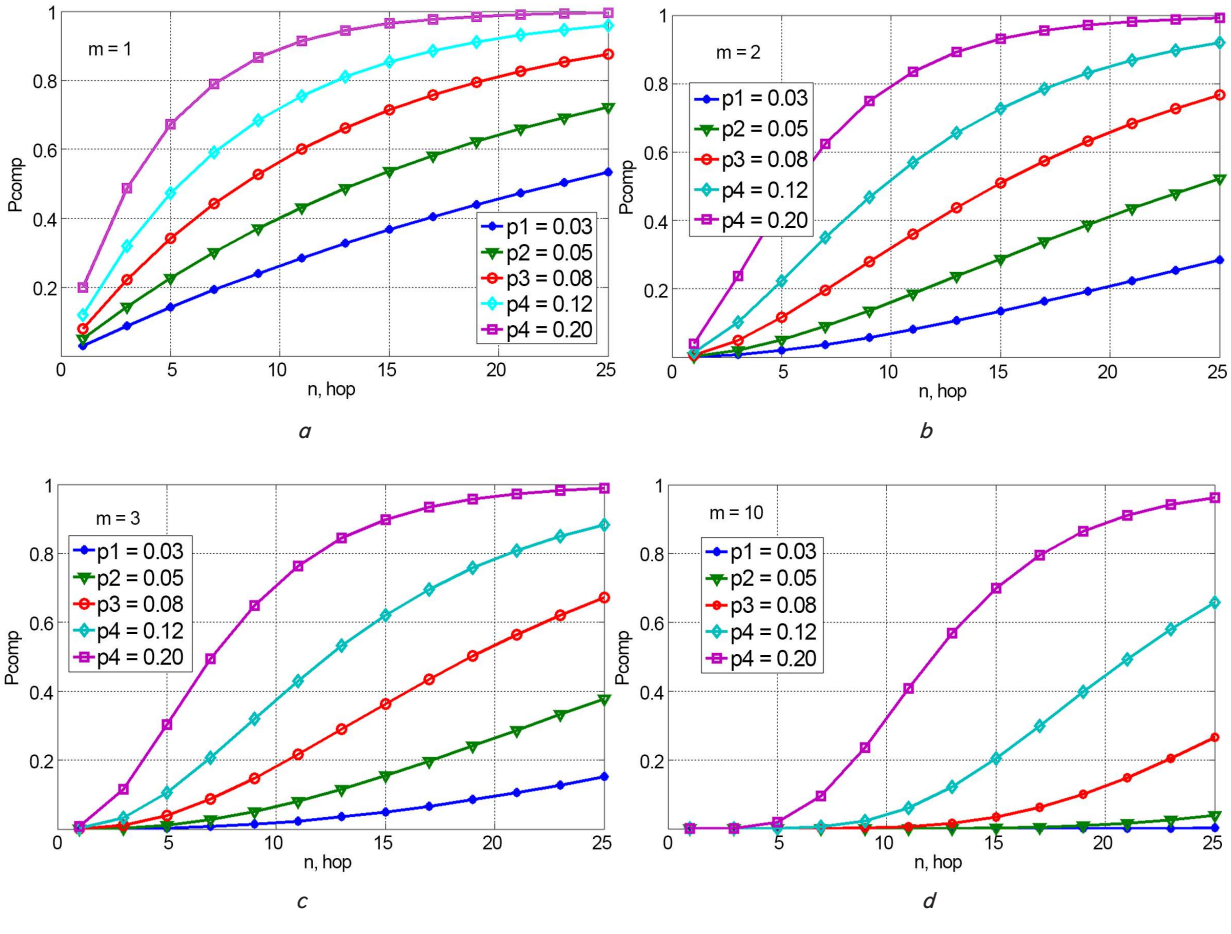


Fig. 3. Probabilities of message compromise depending on the number of hops for different numbers of paths: *a* – for one path; *b* – for two paths; *c* – for three paths; *d* – for ten paths

The first product consists of elements with path number i from the first to m, where m is the total number of paths. The second product consists of elements with hop number j from the first to n_i, where n_i is the number of hops on path i. The third product consists of elements with intermediate node number h from the first to n_{i-1}, where n_{i-1} is the number of intermediate nodes on path i. The number of intermediate nodes is always one less than the number of hops.

The influence of compromise of intermediate nodes in the network on the number of hops for two values: a small number of paths $m = 3$ and a large number $m = 10$ with a constant insignificant probability of compromise on one hop $p_{hop} = p = 0.03$ was studied. The influence of the probability of compromise of intermediate nodes was studied if the probability of compromise of an individual node is the same as the probability of compromise on one hop $p_{nod} = p_{hop}$. In the case of underground electrical cables, the possibility of outsider influence on intermediate nodes is in practice greater than on segments of communication lines. Therefore, studies were conducted for $p_{nod} > p_{hop}$.

The results of the calculations are shown in Fig. 4. In the plots, the probability of compromise of intermediate nodes varied from p_{hop} to $4p_{hop}$. For comparison, the plots show the results for the case of ideal nodes obtained earlier at $p_{nod} = 0$.

With the probability of compromise in nodes equal to the compromise on one hop $p_{nod} = p$, the impact of compromise of intermediate nodes was quite significant.

With the number of hops $n = 10$ and the number of paths $m = 3$, the level of probability of compromise according to the results of the calculations increases in comparison with ideal nodes by four times from 0.02 to 0.08. At significant distances to private VPC clouds for $n = 25$, the level of compromise increases by 3.1 times from 0.15 to 0.47.

Increasing the probability of compromise of intermediate nodes to $p_{nod} = 4p$ leads to a significant increase in the overall probability of compromise of the message. For remote clouds with $n = 25$ and $m = 3$, the probability of compromise is close to unity. Even increasing the value of m to 10 only partially reduces the probability of message compromise from 0.94 to 0.80.

From the comparison of plots in Fig. 4, *a*, *b*, it is clear that increasing m significantly reduces the probability of message compromise for communication systems with closely located clouds.

The impact of compromise of end routers on the overall probability of message compromise was studied. End nodes in the network are common to all paths. If we consider that, unlike paths that are included in parallel, two end nodes are included in series with a set of paths, then we can formulate an expression for calculating the overall probability of compromise P_{comp}

$$P_{comp} = 1 - \left(1 - \prod_{i=1}^{m} \left(\begin{array}{l} 1 - \prod_{j=1}^{n_i} (1 - p_{ij}) \times \\ \times \prod_{h=1}^{n_i - 1} (1 - p_{ih}) \end{array} \right) \times \prod_{v=1}^{2} (1 - p_v) \right). \quad (9)$$

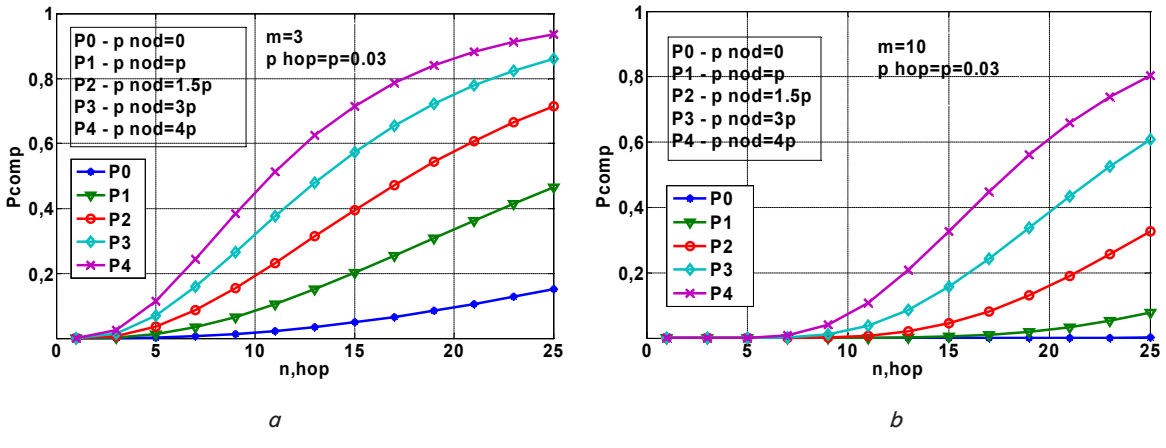
where p_v is the probability of compromising the end node.

The fourth product consists of elements with the number of the end node v from the first to the second.

The calculation according to formula (9) showed (Fig. 5) that the influence of end nodes is significant with a low probability of compromising the set of paths without taking into account the end nodes. For $p1 = 0.20$, the growth coefficient is 2.44, and for $p5 = 0.60$ the coefficient decreases to 1.56. Previous studies show that a low probability of compromising a message occurs at small distances to the VPC cloud and an increase in the number of paths. If we take into account the complexity of organizing a large number of territorially separated paths through the Internet that work simultaneously, then the positive effect of increasing the number of paths is destroyed without proper protection of the end nodes.

The protection of the end nodes for the communication system is more important than the nodes along the paths because they are common to all m paths. Increasing m does not affect the end nodes and it is not possible to correct the effect by increasing the paths. Fig. 6 shows the results of the influence of the level of compromise of two end nodes on the total level of compromise of a message with ideal end nodes.

The most vulnerable to attacks on end nodes are systems with low message compromise probabilities. With a message compromise probability of $p1 = 0.03$ in a system without taking into account the influence of end nodes, increasing the probability of compromise of end nodes to 0.1 led to a significant increase in the overall level of compromise probability from 0.03 to 0.21.



a *b*

Fig. 4. The influence of the probability of node compromise on the level of message compromise at different p_{nod} on the number of hops in a system with ideal edge nodes:
a — for three paths; *b* — for ten paths

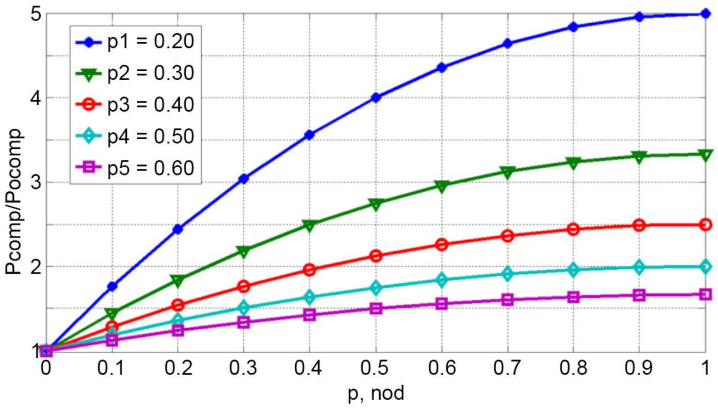


Fig. 5. The coefficient of increase in the probability of message compromise due to the influence of end nodes for different probabilities of total compromise without taking into account the influence of end nodes

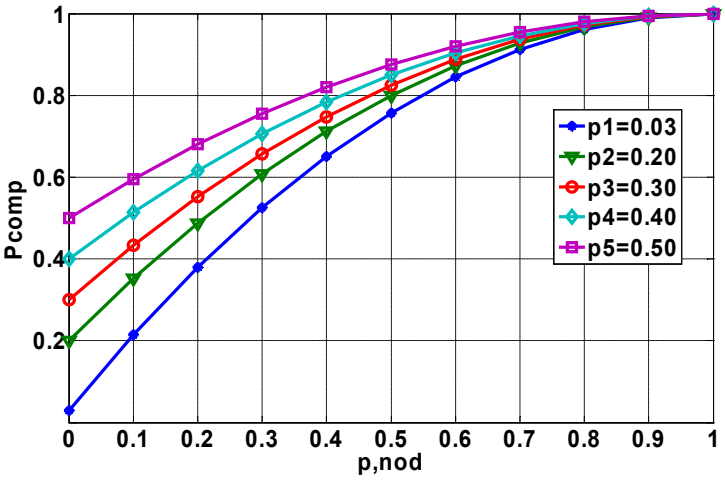


Fig. 6. The influence of end nodes on the probability of message compromise in a communication system

5. 4. Investigating the influence of the compromise threshold on the level of message compromise

In most cases, dynamic routing is used on the Internet. This complicates the organization of a set of geographically separated paths for the practical implementation of the Shamir scheme. On the other hand, the level of protection in the Shamir algorithm depends on the compromise threshold k, which determines the power of the polynomial.

According to the Shamir scheme, the compromise threshold k is the minimum number of parts of the secret that is sufficient for its cracking. The power of the polynomial is chosen to be k–1. The minimum value of $k = 2$. In this case, we have a polynomial of the first power, which is described by a straight line given by two points. The level of protection in such a scheme is weak, therefore, for practical use, $k > 2$ should be taken. For example, at $k = 3$, instead of a polynomial of the first power, there was a square polynomial, due to which the level of protection increased. Polynomials of power $k - 1$ with large values of k can be used to further increase the level of protection. The transmitted message was always divided into m parts, which were transmitted over m paths, each part over a separate path. The number of paths can be $m \geq k$.

A prime number z is chosen, m random polynomials of power k–1 are composed with a free term S, which is a secret, and then the values of the remainder mod z of the sum of the coefficients of each polynomial are calculated for all polynomials. Then the number z was transmitted along all m paths, and along each separate path – one of the m values of mod z. If k any values of mod z are known at the receiving end, then the secret S can be found, but with a smaller number of values of mod z – this is not possible.

Increasing the power of the polynomial increases the level of protection according to the Shamir scheme. But it is necessary to take into account the increase in the complexity of recovering the coefficients of the polynomial. For small powers of the polynomial, the problem of finding the secret is solved by solving a system of linear equations. When the power of the polynomial increases, the solution of the system of linear equations can become numerically unstable, when a small change in the initial data leads to a large and unpredictable change in the solution itself. This method is unreliable for practical use. When using computer calculations, errors can gradually accumulate during calculations due to inaccurate representation of numbers.

The Lagrange interpolation polynomial method is more effective than direct solution of a system of equations, because it allows one to avoid the computationally complex finding of the inverse matrix or the use of Gaussian-type methods for large systems and allows one to avoid errors. But still, when the threshold k is increased, the requirements for the computing power of computers increase. Therefore, choosing a compromise threshold that provides a sufficient level of information protection and does not lead to delays in computer processing for calculating the secret message is an important task.

In the Shamir scheme, the choice of the ratio between the total number of paths m and the compromise threshold k is important.

For mathematical modeling of the Shamir threshold scheme (k, m), the binomial distribution from classical probability theory was used, which determines the probability of finding k parts of the secret out of the total number of parts of the secret m. It was assumed that the probability of compromising each part of the secret transmitted along a separate path is the same for all paths and is equal to p. Then the probability of compromising the secret is

$$P_{comp} = \sum_{j=k}^{m} \binom{m}{j} p_j (1-p)^{m-j}. \quad (10)$$

At $m = k$, the formula is simplified to the form

$$P_{comp} = p^m, \quad (11)$$

which coincides with formula (6) for $p_i = p$ and confirmed the correctness of the previous calculations.

The study of the level of probability of message compromise for different values of p from 0.05 to 0.5 with the number of paths $m = 5, 10$ depending on the choice of the compromise threshold k was conducted. The results are shown in Fig. 7.

The following conclusions were drawn from analysis of the plots (Fig. 7):

– at small values of the threshold k, compromise is more likely, because fewer parts are required and as a result the system is vulnerable;

– with an increase in the threshold k, the probability of compromise decreases sharply, especially the stability of the system increases significantly with small p and large k;

– an increase in the number of paths m with a constant threshold k leads to an increase in the probability of message compromise, which is explained by an increase in the possibilities for attacks.

It should be noted that in Fig. 7 for the case $m = k$, due to the small scale, it is not visible that the probability of compromise $P_{comp} \neq 00$ but is equal to p^m according to formula (11). As a result, increasing the number of paths m reduces the level of compromise, especially in this case, when $m = k$. But this solution has several drawbacks. The choice of large values of m requires the construction of a large number of territorially separated paths through the Internet, which is not a simple task. On the other hand, large values of the threshold k lead to a large number of polynomials with significant powers equal to $k - 1$. And this requires solving the problem of finding the secret, which is a free member of the polynomial in the set of residues mod of the sum of the coefficients of randomly generated polynomials. This, in turn, requires significant computer performance and time consumption. Therefore, for practical use of the Shamir algorithm, it is necessary to use schemes with $k < m$.

To solve the problem of choosing the threshold k, the behavior of the compromise probability P_{comp} as a function of the threshold value for large values of m, for example, for $m = 20$, was considered. The results of the calculations, which are shown in Fig. 8, demonstrate that at large levels of compromise of a single path for $p = 0.5$, a flat region appears at small values of the threshold k in comparison with the results in Fig. 7, *b*. Our calculation showed that a further increase in m led to an expansion of the flat region. Therefore, the more paths m, the larger the threshold k should be taken.

The results from formulae (6) to (11) make it possible to choose different combinations of values of the probabilities of compromise of hops p_{hop}, nodes p_{nod}, the compromise threshold k and the number of paths m through the Internet depending on the task at hand. If we take into account the complexity of organizing territorially separated paths in the Internet, then it is necessary to first consider options with small values of m.

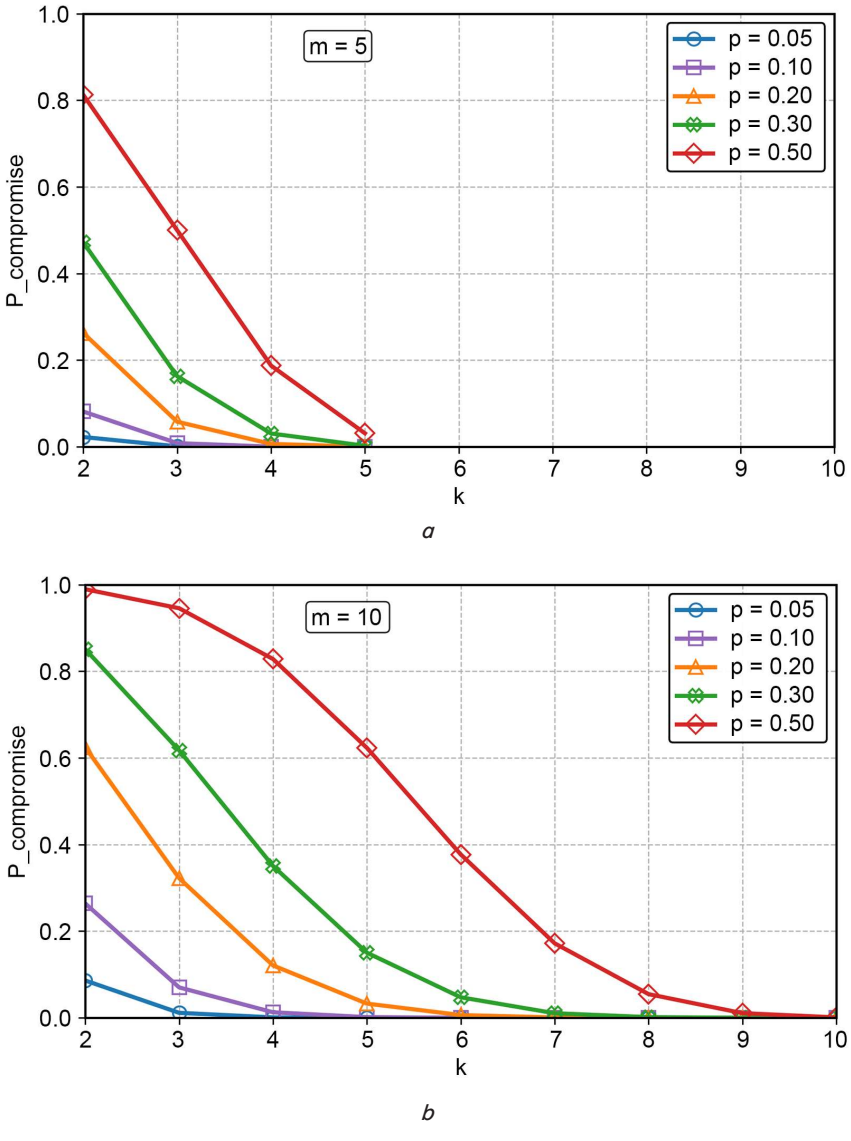


Fig. 7. Probabilities of message compromise depending on the compromise threshold k at different probabilities of compromise p on one path: *a* – for five paths; *b* – for ten paths

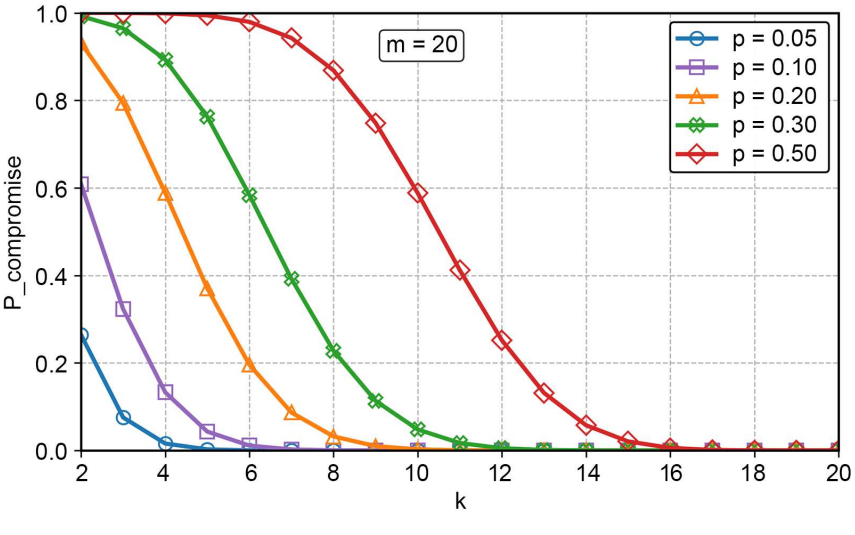


Fig. 8. Probabilities of message compromise depending on the compromise threshold k and different compromise probabilities p on one path for twenty paths

5. 5. Investigating the possibilities of using conventional routing methods for practical implementation of Shamir's scheme

The practical implementation of the Shamir algorithm for transmitting messages over the Internet requires methods for deploying a set of geographically separated paths in the network that work simultaneously. The possibilities of using existing routing technologies were considered, which, as a rule, are designed to build only one path with various reliability requirements, choosing the shortest paths, etc.

One of the simple methods for creating a set of paths is the use of static routing Static Routing [18]. This requires manual configuration of fixed routes in the routing tables of network devices. This method is characterized by ease of configuration in small networks, the absence of additional network load in contrast to dynamic protocols, and increased security, but at the same time requires manual intervention for any changes in the network topology.

Disadvantages of static routing:

– limited scalability for large, constantly changing networks;

– requires manual configuration every time the network topology changes;

– limited redundancy capabilities, for example, in the event of a channel failure.

In the case of remote cloud access points, the number of configurations increases significantly, for example, for the number of hops $n = 25$ and the number of paths $m = 3$, we have more than 70 network devices that require configuration. During operation, some nodes may fail and the system will not be able to perform the task. It will be necessary to configure new paths.

Therefore, static routing can be recommended only for a small number of hops n, when the user is near a private VPC cloud.

To increase the fault tolerance of standard static routing, floating static routing can be proposed – this is a technology for reserving the main route by creating a backup static route with a higher administrative distance than the main one [19]. The backup path is used only if the primary route becomes unavailable, to ensure continuity of network connectivity and redirect traffic to the backup channel until the primary route is restored.

Compared to conventional routing, redundancy increases the resilience of paths to network device failures in nodes but significantly increases the complexity of configuration due to the increase in the number of elements that need to be configured.

Another technology that can be used is MPLS Traffic Engineering (TE) [20, 21]. This is a modification of the standard MPLS technology, which differs from the standard in that it can manage and optimize paths for traffic in the network, instead of relying only on the standard algorithms of the main protocol Interior Gateway Protocol (IGP) for route selection.

In MPLS TE, network administrators can manually create or dynamically define Label Switched Path (LSP) paths for different traffic flows, bypassing the usual routing path.

For traffic management in MPLS TE, the Resource ReSerVation Protocol – Traffic Engineering (RSVP-TE) signaling protocol is used. This protocol extends the standard RSVP to manage traffic in MPLS networks. It is used to build LSP paths with specified characteristics, such as routes, bandwidth restrictions, or other parameters, as well as to reserve network resources.

The above features of MPLS TE technology can be used to solve the problem of creating a set of m geographically diverse paths through the Internet when implementing the Shamir algorithm.

However, the user must rely on third-party administrators to configure the network, which leads to a decrease in the level of cybersecurity.

In addition to the considered solutions, virtual private network technologies VPN [22] can be used to implement the Shamir algorithm with m paths. One method is to create geographically diverse VPN tunnels using multiple providers. In order to increase the level of message security, it is advisable to build VPN tunnels based on the IPsec protocol.

The main disadvantage of the VPN-based approach is the difficulty of creating m independent geographically dispersed tunnels through the Internet by the user unless the services of several providers are used. If m is large enough, the direct use of separate physical servers becomes inefficient and expensive. For example, for $m = 10$, creating ten separate physical VPN nodes is a resource-intensive solution.

Given the need for a set of m servers, hardware or virtual, conventional VPN technology can be used only with a small number of geographically dispersed paths. It should be noted that the use of third-party VPN service providers is not advisable from the point of view of the level of security, which in this case becomes dependent on third-party personnel.

To lay geographically dispersed paths in an MPLS network using VPN technology, one can use MPLS L3VPN technology, which allows one to create logical networks on top of a common physical infrastructure [23].

MPLS L3VPN technology is devoid of the disadvantages of conventional VPN technology, which requires the deployment of a large number of servers to solve the problem of creating a set of m paths. This technology can be used as MPLS TE when implementing the Shamir scheme. Compared to the previous MPLS L3VPN technology, it has a significantly increased level of protection by creating VPN tunnels at layer 3. The disadvantage of this technology is similar to MPLS TE – it is the need to rent and involve third-party administrators to configure the network and, accordingly, reduce the level of security.

Another solution to the problem can be the use of SDN technology [24]. To lay out geographically diverse paths operating simultaneously in an SDN network, a centralized controller can be used, which receives information about the network topology and forwards routing rules to network devices, such as switches and routers. These devices are simplified, and do not contain a pre-installed operating system, the so-called "bare metal". At the transitional stage of technology implementation, conventional switches and routers are used, but with SDN support. Such devices must support SDN protocols, such as OpenFlow, which allow the controller to directly manage their flow tables. These tables determine how packets should be forwarded, which makes it possible to create several parallel geographically diverse paths.

The functions of traffic control and forwarding in SDN are separated, which makes it possible to create a more flexible and scalable network, while the SDN network is controlled by software.

Additionally, SDN can use VPN technology to create secure connections between remote nodes in geographically distributed networks. Due to insufficient geographical coverage, SDN technology cannot currently be used to create m-paths on the Internet. However, this technology

can be effective within private VPC clouds, the security of which is determined by the cloud owners.

Dynamic routing is commonly used in the Internet. To create multiple geographically separated paths that work simultaneously, Multipath Routing can be configured, for example, using Equal-Cost Multi-Path (ECMP) protocols [25–27].

ECMP multipath routing can be used in the Internet by configuring routers to use multiple paths with the same metric to a single destination. This requires that routing protocols, such as BGP or OSPF, discover and form a set of routes with the same cost ECMPset, and then the routing management system distributes traffic over these paths.

ECMP routing makes it possible to create geographically separated paths to implement the Shamir scheme. However, configuring such routing has disadvantages such as the complexity of implementation and the need to support such routing from the hardware and software side. Involving a third-party provider to provide services and configure ECMP multipath routing leads to a decrease in the overall level of secure message transmission.

From the analysis of the main methods for creating a set of m geographically distributed paths in the Internet using the Shamir scheme, three groups of methods can be distinguished. Methods that require the involvement of a third-party service provider and therefore have a reduced level of cyber resilience. These are methods based on MPLS TE, MPLS L3VPN, Multi Routing with ECMP. The second group is more secure because it does not require third-party providers, these are Static Routing, Floating Static Routing, and VPN with servers belonging to the sender of messages. Methods for centralized creation of a set of paths in SDN technology can be attributed to both the first group, in the case of paths through the Internet with SDN service providers, and to the second – when using this technology inside the VPC cloud.

A common drawback for all considered methods is the complexity of organizing large numbers of m distributed paths through the Internet.

6. Research into increasing the information protection in transmission systems to virtual private clouds: results and summary

Unlike [4, 5], in which analysis is limited to simple network configurations with ideal nodes and did not take into account the peculiarities of message transmission over the Internet, our proposed model makes it possible to analyze multipath routes consisting of a different number of elements. This model takes into account the number of hops between routers from the user on the paths to the virtual private cloud, the parameters of the Shamir scheme, and the probability of compromise in individual elements of the communication system.

Compromise of messages during multipath routing on the Internet depends on the influence of a whole complex of factors from the security of nodes and segments of the path to the construction of Shamir schemes and routing methods. In order to study the influence of each factor separately, the mathematical model was gradually complicated.

To model the influence of the number of hops, relations (6), (7) were proposed for the case when the number of paths $m = k$, where k is the compromise threshold in the Shamir algorithm. The probability of compromise of equipment in the nodes was not taken into account. The results (Fig. 3, *a*) for one path showed a significant dependence of the probability of compromise on both the distance to the VPC cloud and the probability of compromise on one path segment. Moreover, for significant probabilities of compromise on one path segment, there is a sharp increase in the total probability of compromise at small distances to the VPC cloud. Already at 10 hops, the level of compromise tends to unity. Due to the use of $m > 1$ parallel paths and the distribution of information between these paths, the total probability of message compromise is significantly reduced (Fig. 3, *a–c*). Especially for large values of m at small distances to the VPC cloud (Fig. 3, *c*).

Our study on the influence of nodes was divided into two parts. To model the influence of intermediate nodes, relation (8) was proposed. The influence of routers in intermediate nodes with a probability of compromise equal to the compromise on one hop on the overall probability of message compromise is quite significant. With the number of hops $n = 10$ and the number of paths $m = 3$, the level of probability of compromise according to the results of calculations increases fourfold compared to ideal nodes from 0.02 to 0.08 (Fig. 4, *a*). The results shown in Fig. 4*b* demonstrate the possibility of a significant reduction in the probability of compromise for clouds that are close to the user, due to an increase in the number of paths along which information is distributed.

To model the influence of end nodes, relation (9) was proposed. The calculation showed that the influence of end nodes is much greater compared to intermediate ones, especially with low probabilities of compromise of a set of paths without taking into account end nodes (Fig. 5, 6). It should be taken into account that the end nodes are common to the entire set of paths. This explains their importance in ensuring the protection of the communication system from attacks. By increasing the number of paths, the influence of the end nodes cannot be reduced, unlike the case of intermediate nodes (Fig. 4). Therefore, ensuring the protection of the end nodes is especially important.

To model the influence of the compromise threshold k and its combination with the number of paths m in the Shamir scheme, relation (10) is proposed, which determines the probability of finding k parts of the secret from the total number of parts of the secret m. Such a mathematical model is valid for the case when the probability of compromising each part of the secret transmitted along a separate path is the same for all paths and is equal to p. According to the Shamir scheme, the compromise threshold k is the minimum number of parts of the secret sufficient for its cracking. The power of the polynomial is chosen to be equal to $k - 1$. The calculation showed that increasing the threshold k reduces the probability of compromising the message (Fig. 7). At high levels of compromise of a single path p and a large number of paths m, a flat region of values of the total probability of compromise appears (Fig. 8) in comparison with the results in Fig. 6, *b*. With further growth of m, this region expands, which indicates the need to choose correspondingly larger values of the threshold k. This is explained by the increase in the field for attacks with a large number of paths m.

The Internet is usually based on the use of dynamic routing protocols that form a single path with specified metrics. For the practical implementation of the Shamir scheme, it is necessary to create a set of geographically separated paths. Routing methods are not always suitable for the Shamir

scheme. Therefore, the paper analyzes the possibilities of using existing routing methods in the implementation of the Shamir scheme for transmitting messages over the Internet. The most acceptable methods for use are methods based on MPLS TE, MPLS L3VPN, Multi Routing with ECMP, but they require a third-party service provider, which reduces their level of cyber resilience. Methods based on Static Routing, Floating Static Routing, and VPN with servers belonging to the sender of messages require complex settings. SDN technology can be distinguished separately, but it is not yet widespread and also requires a third-party service provider. SDN technology is used inside VPC clouds.

When using the results of our work, for example, for dynamic real-time assessment of compromise probabilities using vulnerability scanners, the following limitation should be taken into account: the problem is solved for the case when the probability of compromise of each part of the secret transmitted along a separate path is the same for all paths. In practice, these values may be different. Such a limitation is not important for achieving the goal set in the work.

As a rule, the combination of methods for creating a set of paths through the Internet with the Shamir scheme is used to transmit messages that are keys for decrypting encoded information, which is then transmitted over the network.

Further development of methods for transmitting information over the Internet using the Shamir scheme may involve using the Shamir scheme to transmit the information stream, and not only keys. This requires a significant increase in computing resources. The constant improvement of multi-core processors makes this method acceptable for practical use.

7. Conclusions

1. A model of the probability of message compromise due to the influence of the main parameters of the network infrastructure has been proposed. The model describes the process of message transmission through a set of m parallel independent paths in the Internet, each of which consists of serially connected path segments, intermediate network nodes, and two common end nodes for all paths.

The input parameters of the model are the number of parallel paths m in the Internet that do not intersect; the number of segments n_i and intermediate nodes h_i on each i-th path; the compromise threshold k in the Shamir scheme, which corresponds to the condition $k \leq m$. The model also specifies the values of the probability of compromise of individual elements of the communication system. These are the probabilities of compromise of segments of the i-th path p_{ij}; the probabilities of compromise in intermediate nodes along the i-th path $p_{nod\ i}$ and the probabilities of compromise in the end nodes of the communication system p_1 and p_2.

The output parameter of the model is the overall probability of compromise of a message P_{comp} transmitted over the Internet to a virtual private cloud.

Due to the fact that the model takes into account the probabilities of the elements of each path, it becomes possible to analyze their impact on the overall level of probability of message compromise.

2. When building a communication system for transmitting messages over the Internet using the Shamir scheme, there is a significant dependence of the level of compromise P_{comp} on the probability of compromise of one element of the path p_{ij}. For one path, at small p_{ij}, the compromise of the message increases slowly with an increase in the number of hops (at $p_{ij} = 0.03$ for $n = 10$, the probability P_{comp}, $= 0.26$). With an increase in the probability p_{ij}, the compromise quickly reaches values that are unacceptable for the practical use of the communication system (at $p_{ij} = 0.2$ for $n = 10$, the probability $P_{comp} = 0.89$). With the number of paths $m > 1$, due to the organization of parallel paths, the probability of message compromise decreases. With a significant increase in m, for example, to 10, we have a significant gain in protection against compromise for large distances in the number of hops n. In this case, the probability of compromise may be acceptable for practical use for accessing the ports of the edge router of a cloud remote by $n \approx 25$ hops, especially for small probabilities on one hop.

3. Protection of intermediate nodes from attacks is critically important. At 10 hops in a communication system with three paths, we have an increase in the total probability of compromise by a factor of four from 0.02 to 0.08 with the same impact of an individual node and hop. For remote clouds with 25 hops, the increase is 3.1 times from 0.15 to 0.47. Protection of end nodes for a communication system is more important compared to nodes along the paths because they are common to all m paths. The most vulnerable to attacks on end nodes are systems with low levels of message compromise probability. With a compromise probability of 0.03 in the system without taking into account the influence of end nodes, a compromise probability of end nodes equal to 0.1 increases the overall level to 0.21.

4. The probability of compromise of messages transmitted to a virtual private cloud can be reduced by increasing the threshold k in the Shamir scheme, especially the probability of compromise drops sharply at small p. An increase in the number of paths m with a constant threshold k leads to an increase in the probability of message compromise, which is explained by an increase in the opportunities for attacks. Given the complexity of organizing a set of paths through the Internet, the results obtained for small m are of practical importance.

5. For the practical implementation of a set of geographically dispersed paths in the Internet using the Shamir scheme, three groups of methods can be distinguished. Methods that require the involvement of a third-party service provider and therefore have a reduced level of cyber resilience. These are methods based on MPLS TE, MPLS L3VPN, Multi Routing with ECMP. The second group is more secure because it does not require third-party providers, these are Static Routing, Floating Static Routing, and VPN with servers belonging to the message sender. Methods for centrally creating multiple paths in SDN technology can be classified as both the first group, in the case of paths over the Internet with SDN service providers, and the second – when using this technology inside the VPC cloud.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal,

authorship, or any other, that could affect the study, as well as the results reported in this paper.

Funding

The study was conducted without financial support.

Data availability

All data are available, either in numerical or graphical form, in the main text of the manuscript.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

Authors' contributions

Artem Marchuk – Conceptualization, Methodology, Writing – original draft; **Tetiana Kovalenko** – Software, Writing – review & editing**; Svitlana Shtangey** – Validation, Investigation; **Olena Linnyk** – Investigation, Visualization.

References

1. ISO/IEC 27011:2024. Information security, cybersecurity and privacy protection – Information security controls based on ISO/IEC 27002 for telecommunications organizations. Available at: https://www.iso.org/standard/80584.html
2. ISO/IEC 27033-1:2024. Information technology - Security techniques - Network security - Part 1: Overview and concepts. Available at: https://www.evs.ee/en/evs-iso-iec-27033-1-2024
3. Shamir, A. (1979). How to share a secret. Communications of the ACM, 22 (11), 612–613. https://doi.org/10.1145/359168.359176
4. Lemeshko, O. V., Yeremenko, O. S., Yevdokymenko, M. O., Kovalenko, T. M. (2021). Metodyka rozrakhunku ymovirnosti komprometatsiyi konfidentsiynykh povidomlen pry bezpechniy marshrutyzatsiyi v infokomunikatsiynykh merezhakh z vykorystanniam shliakhiv, yaki peretynaiutsia. Problemy telekomunikatsiy, 2 (29), 15–27. Available at: https://pt.nure.ua/wp-content/uploads/2021/12/212_lemeshko_confidential.pdf
5. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Sleiman, B. (2022). Modeliuvannia ta optymizatsiya protsesiv bezpechnoi ta vidmovostiykoi marshrutyzatsiyi v telekomunikatsiynykh merezhakh. Kharkiv: KhNURE, 198. https://doi.org/10.30837/978-966-659-378-1
6. Kato, T., Cheng, S., Yamamoto, R., Ohzahata, S., Suzuki, N. (2018). Proposal and study on implementation of data eavesdropping protection method over Multipath TCP communication using data scrambling and path dispersion. International Journal on Advances in Security, 11 (1&2), 118–126. Available at: https://personales.upv.es/thinkmind/dl/journals/sec/sec_v11_n12_2018/sec_v11_n12_2018_9.pdf
7. Dani, V., Nagar, S., Pawar, V. (2022). An Analysis of Multipath TCP for Improving Network Performance. Innovations in Bio-Inspired Computing and Applications, 160–169. https://doi.org/10.1007/978-3-030-96299-9_16
8. Popat, K., Kapadia, V. V. (2021). Multipath TCP Security Issues, Challenges and Solutions. Information, Communication and Computing Technology, 18–32. https://doi.org/10.1007/978-3-030-88378-2_2
9. Chaturvedi, R. K., Chand, S. (2020). Multipath TCP security over different attacks. Transactions on Emerging Telecommunications Technologies, 31 (9). https://doi.org/10.1002/ett.4081
10. Veni, S., Kadhar Nawaz, G. M. (2013). A new Approach to Enhance Security in MPLS network. International Journal of Computer Science and Network Security, 13 (2). Available at: https://scispace.com/pdf/a-new-approach-to-enhance-security-in-mpls-network-3wmckuoafr.pdf
11. Alouneh, S., Agarwal, A., En-Nouaary, A. (2009). A novel path protection scheme for MPLS networks using multi-path routing. Computer Networks, 53 (9), 1530–1545. https://doi.org/10.1016/j.comnet.2009.02.001
12. Ridwan, M. A., Radzi, N. A. M., Wan Ahmad, W. S. H. M., Abdullah, F., Jamaludin, Md. Z., Zakaria, M. N. (2020). Recent trends in MPLS networks: technologies, applications and challenges. IET Communications, 14 (2), 177–185. https://doi.org/10.1049/iet-com.2018.6129
13. Čuřík, P., Ploszek, R., Zajac, P. (2022). Practical Use of Secret Sharing for Enhancing Privacy in Clouds. Electronics, 11 (17), 2758. https://doi.org/10.3390/electronics11172758
14. Naz, M., Al-zahrani, F. A., Khalid, R., Javaid, N., Qamar, A. M., Afzal, M. K., Shafiq, M. (2019). A Secure Data Sharing Platform Using Blockchain and Interplanetary File System. Sustainability, 11 (24), 7054. https://doi.org/10.3390/su11247054
15. Leon-Garcia, A. (2022). Probability, Statistics, and Random Processes for Electrical Engineering. Pearson, 650. Available at: https://www.goodreads.com/book/show/24331653-probability-statistics-and-random-processes-for-electrical-engineering
16. Ross, S. M. (1997). Introduction to Probability Models. Academic Press. 702. https://www-elec.inaoep.mx/~rogerio/IntrodProbabModels.pdf
17. Grimmett, G., Stirzaker, D. (2020). Probability and Random Processes. Oxford University Press, 688. Available at: https://global.oup.com/academic/product/probability-and-random-processes-9780198847595?cc=ua&lang=en&
18. Types of Static Routes Explained. Available at: https://www.computernetworkingnotes.com/ccna-study-guide/types-of-static-routes-explained.html
19. Static Routing vs. Dynamic Routing: What's the Difference? (2025). Available at: https://www.indeed.com/career-advice/career-development/dynamic-routing-vs-static-routing

20. MPLS Configuration Guide, Cisco IOS XE 17.x. Available at: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/mpls/b-mpls/m_mp-te-autotunnel-0.html
21. Monge, A. S., Szarkowicz, K. G. (2015). MPLS in the SDN Era. O'RELLY, 920.
22. Song L. (2022). Set Up Your Own IPsec VPN, OpenVPN and WireGuard Server (Build Your Own VPN). Amazon, 147. Available at: https://www.amazon.com/IPsec-OpenVPN-WireGuard-Server-Build/dp/B0BQ99KH38
23. Bhalerao, V., Sarode, S. (2021). A Review Paper on MPLS L3 VPNs Architecture. International Journal of Scientific and Research Publications (IJSRP), 11 (6), 524–527. https://doi.org/10.29322/ijsrp.11.06.2021.p11469
24. Goransson, P., Black, C. (2014), Software Defined Networks. A Comprehensive Approach. Elsevier, 436. https://doi.org/10.1016/c2013-0-00167-3
25. ECMP. Available at: https://www.cisco.com/c/en/us/td/docs/security/cdo/cloud-delivered-firewall-management-center-in-cdo/managing-firewall-threat-defense-services-with-cisco-defense-orchestrator/m-routing-ecmp.pdf
26. Equal Cost Multipath Load Sharing - Hardware ECMP. Docs Hub. Available at: https://docs.nvidia.com/networking-ethernet-software/cumulus-linux-44/Layer-3/Routing/Equal-Cost-Multipath-Load-Sharing-Hardware-ECMP/
27. AWS networking and content delivery. Additional ECMP Paths. Available at: https://000092.awsstudygroup.com/4-transitgatewayandvpn/4.4-ecmppaths/