Research Article

Open Access CrossMark

Method for calculation indicators steganographic systems in multiservice communication networks

Volume 9 Issue 1 - 2023

Bayram Ibrahimov
Department of Radio Engineering and Telecommunication, Azerbaijan

Correspondence: Bayram Ibrahimov, Department of Radio Engineering and Telecommunication, Azerbaijan Technical University, Baku, Azerbaijan, Tel 99470-649-07-79, Email i.bayra@mail.ru

Received: March 13, 2023 | **Published:** March 30, 2023

Abstract

An analysis of the performance indicators multiservice telecommunication networks using the sixth technological order based on the NGN (Next Generation Network) architectural concept and future FN (Future Networks) networks was carried out to build high-performance steganographic systems with increased covert channels throughput, ensuring the achievement of a certain level information security. Comprehensive criteria for the efficiency the functioning steganographic systems are considered and the channel capacity of the steganosystem as a communication system with packet switching is selected. On the basis of the study, a new approach to constructing a method for evaluating complex indicators of the quality of steganographic communication during embedding and extracting hidden data is proposed. The quality of steganographic communication refers to the properties stegano communication to ensure the efficiency of the system, both timely and reliable transmission of messages.

On the basis of the proposed approach, the effectiveness steganographic systems in the construction of covert channels for the transmission secret data transmitted over communication channels was studied. Taking into account the new entropy approach, a method for calculating the indicators of the latent throughput steganographic systems in packet-switched communication networks has been created. As a result of the study calculation method, important analytical expressions were obtained for evaluating complex indicators throughput steganographic systems, such as the throughput of covert channels, the maximum possible value of the performance of a binary source packets, the average packet transmission time with the proposed coding scheme, and the residual throughput of the communication channel.

Keywords: steganographic communication quality, steganographic system, covert channel, packet length, countermeasures, efficiency, residual throughput

Introduction

The intensive development multiservice telecommunication networks based on the concepts of the digital economy, the Fourth Industrial Revolution and the sixth technological order requires the construction steganographic systems with increased capacity of covert channels, ensuring the achievement of a certain level information security.

The studies carried out in[1,2,3] show that multiservice telecommunication networks based on the architectural concepts of the next NGN and future FN generations are today a particularly vulnerable place for information security violations. In this case, it is impossible to guarantee the safety of data during their passage through public media such as electrical and optical communication channels, the Internet, terrestrial, wireless, and space channels. Therefore, messages transmitted over various telecommunication channels using advanced technologies are in particular need to protect information from unauthorized subscriber and network access.

Currently, there are two main directions in solving the problem of protecting information from unauthorized access:[2–5] cryptography and steganography. The purpose cryptography is to hide the content of a message through encryption. Steganography hides the very fact of the existence and transmission of a secret message through covert channels. In this case, not only is the fact forwarding some secret message from Alice to Bob hidden, but Eve does not even know that Alice is communicating with Bob.

The construction of covert channels and ensuring the security of information using the methods, algorithms and tools steganographic systems is an extremely urgent task in telecommunication systems.[1,4–6]

Thus, steganography studies the methods by which the very fact of the transmission multimedia type information is concealed. The studied methods have shown[1–4,6,7] that steganography allows not only covert transmission multimedia data L_i^M , but also to solve the problems of noise-immune authentication, protection of information from unauthorized subscriber and network access, tracking the dissemination information over multiservice telecommunication networks, information search in multimedia databases.

The analysis of publications devoted to steganography allows us to single out works[1–3] published in the territory of the CIS (Countries of Independent States) and foreign countries as the base ones both in terms time of their publication, the number citations, the volume of the material presented, and in terms of the number analyzed and systematized literature sources on selected problem.[4–8] These works outline the approaches, principles and tasks steganography and steg analysis as a communication system.[9–12] There are also known approaches to estimating the capacity of covert channels with noise using information theory methods.[6,8–10]

In this paper, we consider the problem of studying the principle constructing covert channels in multi-service packet-switched telecommunication networks with the introduction methods for countering and estimating the indicators maximum throughput.

Statement of the research problem

It is known[1–4,6,7] that information is presented in the form messages and transmitted in the form of a sequence characters. From the source to the receiver, the message is transmitted through some material medium, which is a communication channel. In steganographic systems, a discrete channel is widely used - this is a communication channel used to transmit discrete messages. Usually, a discrete channel is a set technical means that ensure the transmission of a digital signal. On the basis of a discrete channel, a covert communication channel is implemented to transmit secret messages in the form of a container package.[1,2]

It should be noted that a covert channel is a telecommunications communication channel that sends information using a different method and algorithm, which was not originally intended for this.[1–8,10–12] It is generally accepted that a covert channel is a kind disguised, unauthorized transmission messages to a third party that violates the system security policy. However, covert channels can also be used by authorized users using steganographic methods and algorithms, which are based on the features of the presentation messages transmitted to communication channels.[1–5,12]

In this case, a hidden message of a multimedia type means a variety of methods that modify data and programs, text, audio and video. Strictly speaking, this variant refers to hiding information in text documents, hiding data in speech messages and hiding information in video data or moving images (Data, Audio, Video - D, A, V). Covert channel stegomethods use mainly text, audio and video data as a container.

Due to the fact that the organization hidden attachments is possible mainly due to the redundancy of the type data that is chosen by the carrier, the popularity of using audio and video data for this task is obvious, as the most redundant. Then, when using container packet technology, the length of the hidden message multimedia type is expressed as

$$L_k^M = \sum_{i=1}^{K} L_{i.k} = L_{i.k}^D + L_{i.k}^A + L_{i.k}^V\,,\ i=\overline{1,K} \qquad (1)$$

Based on (1), we assume that during the transmission of hidden information in voice messages $20\,ms$, a packet is formed from $160\,bayt$, every time one information $\Delta t_k = 125\,mks$ is written to the container $1\,bayt$. Therefore, instead of streams of traffic packets, streams of container packets are considered.[1,3,5]

In multiservice networks with packet switching, covert channels are widely used technologies and protocol stack MPLS (MultiProtocol Label Switching) TCP/IP (Transport Control Protocol/Internet Protocol) and IP/MPLS(Internet Protocol/MPLS). The IP/MPLS header consists several labels, like a service packet.

Research and evaluation of the effectiveness steganographic systems

One of the important criteria for the effectiveness of the functioning steganographic systems is the channel bandwidth of the steganosystem as a communication system with packet switching and is described by the following relationship:

$$E_{\acute{y}\hat{o}\,\hat{o}\,.}(\lambda_i,L_i) = W\,[C_{\max}^{ck}(L_{ik},\lambda_{i.k})]\,,\ i=\overline{1,K}\ , \qquad (2)$$

where $E_{\acute{y}\hat{o}\,\hat{o}\,.}(\lambda_i,L_i)-$ functions that take into account the performance indicators of the functioning steganographic systems as communication systems, taking into account the rate arrival of the incoming stream λ_i when transmitting the stream of the $i-$th packet of the traffic container with the length of the hidden message L_i, $i=\overline{1,K}$; $C_{\max}^{ck}(L_{i.k},\lambda_{i.k})-$ the maximum value of the throughput covert channel steganographic packet switched systems, taking into account the speed of the incoming stream $\lambda_{i.k}$ when transmitting a stream $i-$th container packets with length $L_{i.k}$, $i=1,K$. The latter is determined by three indicators of the bandwidth of the channels of the steganosystem as a communication system:

$$\tilde{N}_{\max}^{\hat{c}kc}(L_{i.k},\lambda_{i.k}) = {}^{nk}C_{\max}(\lambda_i,L_i) - C_{\max}^{c\ddot{e}}(\lambda_{i.n},L_{i.n}) - {}_{\max}(\lambda_{i.c},\ {}_{i.c})\,,\ i=\overline{1,K}\ , \qquad (3)$$

where $C_{\max}^{\hat{\imath}kc}(\lambda_i,L_i)-$ total maximum throughput of a communication system using packet-switched steganography systems, taking into account the incoming flow rates λ_i when transmitting the stream of the $i-$th packet with length L_i, $i=\overline{1,K}$; $C_{\max}^{\hat{\imath}k}(\lambda_{i.n},L_{i.n})\ and\ \tilde{N}_{\max}^{\ddot{e}}(\lambda_{i.c},L_{i.c})-$ respectively, the channel capacity of the communication system using steganographic systems (information or useful and service channels), taking into account the speed of the incoming stream $\lambda_{i.n}\ and\ \lambda_{i.c}$ when transmitting the stream of the $i-$th packet with length $L_{i.n}\ and\ L_{i.c}$.

Expressions (1), (2) and (3) characterize the general essence of the efficiency of a steganographic system, taking into account the parameters packets, indicators useful, service and covert communication channels, which make it possible to describe the considered new approach to constructing a method for assessing the quality of steganosystem when embedding and extracting hidden data.

Analysis of indicators residual system throughput

To build a covert channel, a counteraction method was used based on changing the length of each transmitted packet (useful and service), which has a uniform distribution on the set $N\alpha_b^{\hat{o}} \cup \{0\}$, which create an additional load on the common communication channel. An important question that arises in this case is the estimation of the residual throughput steganographic systems when introducing a method for changing the field of a useful and service packet of a hidden message and is equal to:

$$C_{\max}^{res}(L_{i.n}) = \frac{C_{\max}^{okc}(\lambda_i,L_i)}{L_{\bar{\imath}.} + L_{c\acute{n}\acute{o}}(\lambda_i)} \cdot (L_{i.n}+L_{i.c})\,,\ i=\overline{1,K}\ , \qquad (4)$$

where $L_{c\acute{n}\acute{o}}(\lambda_i)-$ the length of the service transmitted packet, taking into account the protocol unit and the control field of the information packet network and link level of the model.

Expression (4) characterizes the residual capacity steganographic systems with the introduction of the method changing the field of the useful and service packet of the covert message and determines the potential of the covert channel.

Taking into account the uniform distribution of the symbol transmitted over the covert channel (due to the largest uncertainty - entropy) and the parameter of the counteraction approach $\alpha_b^{\hat{o}}$, expression (4) will take the following form [6, 8, 9]:

$$C_{\max}^{res}(L_{i.n}) = \frac{C_{\max}^{okc}(\lambda_i,L_i)}{E[L_{\ddot{\imath}\grave{o}}] + L\ \ (k) + {}_b0{,}5\,\alpha^{\hat{o}}} \cdot E[L_i]\,,\ i=\overline{1,K}\ , \qquad (5)$$

where $E[L_i]-$ average length of total transmitted packets over a communication channel;

$\alpha_b^{\hat{o}}$ $-$ the number of code element in the implementation dummy bits per packet, determined by the values of a random variable that has a uniform distribution on the set $N\alpha_b^{\hat{o}} \cup \{0\}$.

Expression (5) determines the loss of the total throughput network steganography as a communication system when using the countermeasure method.

Among the ways to counter information leakage through network covert channels, it is customary to single out detection, elimination, and throughput limitation.[3,8]

Based on the entropy approach in the absence restrictions on the value of the variance σ^2 for a uniform distribution $F(x)=1(\hat{a}-\grave{a})$ has the maximum entropy $H_{V\max}=\ell g_{\ 2}(\hat{a}-\grave{a})$. Given the last assumption and the duration of the transmission of one message $i-$th packets $T(\lambda_i)$, the maximum possible value of the performance of the packet source is determined as follows:

$$I_{n.\max}(\lambda_i)=[H_{V\max}/T(\lambda_i)]<C_{\max}^{ck}(L_{i.k},\lambda_{i.k})\ ,\ i=\overline{1,K} \qquad (6)$$

The fulfillment condition (6) means that the system has a method for optimal coding and decoding data (an efficient method modulation and coding, a signal-code design) transmitted via covert channels, in which the error probability is arbitrarily small $P_{BER}^{\tilde{a}}\to 0$, $H_V(U)=0$

Based on the new approach and using expressions (6), we obtain in a compact form the formula for the maximum value of the covert channel throughput:

$$C_{\max}^{ck}(L_{i.k},\lambda_{i.k})=\frac{\ell og_2 L_{\acute{o}\acute{o}}(k)}{E[T_n(\lambda_i,L_i)]}\ ,\ i=\overline{1,K} \qquad (7)$$

Expression (7) takes into account the indicators of covert channel, the lengths of the network and link layer headers open systems interaction model and is described in a very compact way in comparison with the works obtained by the formula for the covert channel throughput [1, 3, 8, 10].

For engineering calculation, taking into account covert channel indicators $\alpha_b^{\hat{o}}$ and $L_{\acute{o}}\ (k)$, and also with the considered method counteraction, the residual channel throughput is as follows:

$$C_{\max}^{res}(L_{i.n})=\frac{2C_{\max}^{okc}(\lambda_i,L_i)}{2E[L_{\acute{o}\acute{o}}]+L_{b}(k)(\alpha^{\hat{o}}+1)}\cdot E[L_i]\ ,\ i=\overline{1,K} \qquad (8)$$

Expression (8) determines the maximum value of the loss of the total throughput communication channel. In addition, (8) determines the capabilities of the steganography system in the transmission secret data, the efficiency use and potential resources of the covert channel.

Numerical results and interpretation

On the basis of the calculation method, a numerical assessment was made by modeling covert channel indicators in steganographic systems using the Communications Toolbox package - an extension of the standard Matlab environment, R 2019b, designed for calculating and modeling communication systems. The results obtained are explicitly listed in table 1.

The analysis shows that Table 1 shows the important values covert channel indicators , the total maximum value communication channel throughput for some values of the countermeasure method parameter $\alpha_b^{\hat{o}}$ and the average length of the total transmitted packets over the communication channel.

Table 1 Residual system throughput and covert channel parameters for $\alpha_b^{\hat{o}}=(16,...,500)\,bit$

	$E[L_i]$, **byte**	**64**	**100**	**128**	**256**	**328**	**400**	**512**	**640**
Parameters of covert channel and protocol stack IP/MPLS steganography system	$C_{\max}^{oks}(\lambda_i,L_i)$, Kbyte /s	64	128	512	1024	2048	4096	8192	16384
	$L_{\acute{o}\acute{o}}(k)$, byte	5	10	15	20	25	30	32	35
	$C_{\max}^{res}(L_{i.n})$, Kbyte /s	55,35	91,43	330,99	736,36	1466,69	2925,71	5637,51	11335,96
		35,16	50,69	55,28	199,58	217,36	314,32	604,54	1114,62
Relative residual capacity	$\Delta Q(L_{i.n})$,%	63,52	55,44	16,70	15,10	14,82	10,74	10,72	9,83

Thus, from numerical calculations it follows that with an increase in the parameters of the covert channel and the IP/MPLS protocol stack of the steganography system, the maximum value of the residual throughput of the system increases, which meets the requirements for the quality of steganographic communication.

Based on the results modeling covert channel indicators, Figure 1 plots a graphical dependence of the maximum value of the residual system throughput on the covert channel parameter for a given indicator of packet-switched communication networks.

Graphical dependency analysi $C_{\max}^{\hat{o}es}(L_{i.n})=F\{C_{\max}^{okc}(\lambda_i,L_i),\alpha_b\ ,E[L_i]\}$ indicates that an increase in the covert channel parameter $\alpha_b^{\hat{o}}$, leads to a decrease $C_{\max}^{res}(L_{in})\le(2000,...,1960)$ Kbps

a system that meets the quality requirements of steganographic communication when using methods to counter the specified type covert of channels, by randomly changing the parameters packets and communication channels.

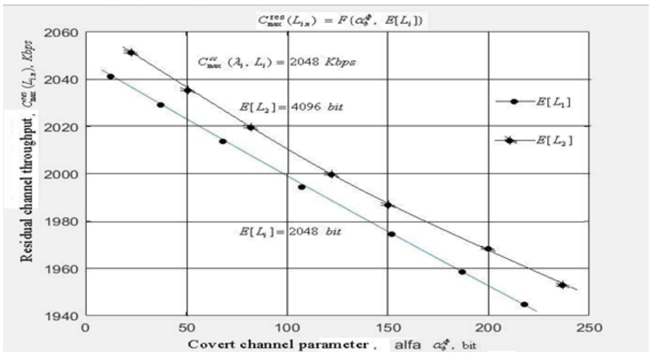

Figure 1 Graphic dependence of the maximum value of the residual throughput system on the parameter covert channel packet switched communication networks.

Citation: Ibrahimov B. Method for calculation indicators steganographic systems in multiservice communication networks. *Int Rob Auto J.* 2023;9(1):40‒43. DOI: 10.15406/iratj.2023.09.00261

In addition, from Fig. 1 it follows that the desired value $C_{\max}^{ocm}(L_{in})$ and its noticeable change begins with the values $\alpha_b^{\hat{o}} \geq (100,...,150)$ bit at $E[L_i] \geq 2000\ bit$ and $C_{\max}^{oks}(\lambda_i, L_i) \geq 2048\, Kbps$.

Efficiency use and distribution throughput system resources steganographic systems

Based on the method calculation and analysis (3), it is possible to determine the maximum value of the covert channel bandwidth steganographic packet-switched systems:

$$C_{\max}^{ck}(L_{i.k}, \lambda_{i.k}) = C_{\max}^{okc}(\lambda_i, L_{i.k}) - C_{\max}^{res}(L_{i.n}) \,,\ i = \overline{1, K} \qquad (9)$$

One of the criteria that allows one to compare the efficiency allocating bandwidth resources of covert data transmission systems is the ratio $C_{\max}^{res}(L_{i.n})$ to the total throughput communication systems $C_{\max}^{okc}(\lambda_i, L_i)$:

$$\Delta Q(L_{i.n}) = 1 - \frac{C_{\max}^{res}(L_{i.n})}{C_{\max}^{okc}(\lambda_i, L_{i.k})} \,,\ i = \overline{1, K} \ , \qquad (10)$$

Expressions (9) and (10) allow estimating the channel resources, temporal and informative characteristics of the covert channel of steganographic systems.

Thus, the performed analysis shows that the possible scenarios for the efficient use covert channel resources in network steganography are not limited to those described in this section.

Conclusion

As a result of the study, a new approach was proposed to create a method for calculating the throughput of covert channel steganographic systems, taking into account the performance indicators packet switched communication networks, methods counteraction control and distribution communication channel resources. On the basis of the calculation method, analytical expressions were obtained for estimating the indicators of the residual system throughput and the average packet transmission time, taking into account the covert channel parameter and the IP/MPLS protocol stack of the steganography system.

The indicators Table 1 and the graphic dependence of the maximum residual throughput on the covert channel parameter are analyzed. It has been established that a strong dependence covert channel throughput $C_{\max}^{ck}(L_{in})$ of the total number parameters $\alpha_b^{\hat{o}}$, $E[L_i]$ and $L_{\acute{o}}\ (k)$ is the main disadvantage steganographic systems using a packet switched communication network and this countermeasure method.

As a result, the throughput of the covert channel, the reliability network operation and protection against unauthorized access along the perimeter subscriber and network communication lines are significantly reduced.

Acknowledgements

None.

Conflicts of interest

Author declares that there is no conflict of interest.

References

1. Ibrahimov BG, İsayev YS, Aydemir ME. Performance of multi service telecommunication systems using the architectural concept of future networks. *Journal of Aeronautics and Space Technologies*. 2023;16(1):41–49 p.
2. Korzhik VI, Yakovlev VA. Fundamentals of cryptography:SP :NTs Intermedia. 2016;1–296 p.
3. Ibrahimov BG, Jafarova EM. *Analysis of information security methods in telecommunication systems using quantum cryptography*. Proceedings of the VIII International Conference Technical Universities: Integration with European and World Education Systems. Izhevsk TU. Russia, Izhevsk. 2019;404–410 p.
4. Shelukhin OI, Kanaev SD. Steganography algorithms and software implementation M: Hotline –Telecom:2018;1–592 p.
5. Belozubova AI, Kogos KG, Lebedev PV. Network covert channels capacity limitation by adding random delays before packet sending. IT Security. 2021;28(4):74–89p.
6. Ibrahimov BG, Takhirova KM. Analysis information security indicators based on network steganography technology. Collection of scientific articles - X-International scientific-technical and scientific-methodical conference. Actual problems of info telecommunications in science and education. SPb : SPbGUT. 2021;411–416 p.
7. Ahsan K, Kundur D. Practical data hiding in TCP/IP. Proceedings of the ACM Workshop on Multimedia Security. 2002: 866–870 p.
8. Cabuk S, Brodley CE, Shields C. *IP covert timing channels: design and detection*. Proceedings of the eleventh ACM conference on computer and communications security. 2004;178–187p.
9. Grusho AA. *On the existence of hidden channels*. Discrete Mathematics.1999;11(1):24–28 p.
10. Ibrahimov BG. Research and estimation characteristics of terminal equipment a part of multiservice communication networks. *Automatic Control and Computer Sciences*. 2010;48(6):54–59 p.
11. Lampson BWA. *Note on the Confinement Problem*. Communications of the ACM. 1973;613–615 p.
12. Ibrahimov BG, Takhirova KM. Research and analysis of information hiding methods in the spatio-temporal domain using steganographic technologies. *Scientific journal Problems of info communications*. 2022;2(16):39–45 p.
13. Ibrahimov BG, Namazov MB, Quliev MN. Analysis performance indicators network multiservice infrastructure using innovative technologies. Proceedings of the 7-th International Conference on Control and Optimization with Industrial Applications (COIA-20). 2020; II:176–178 p.

Citation: Ibrahimov B. Method for calculation indicators steganographic systems in multiservice communication networks. *Int Rob Auto J.* 2023;9(1):40‒43. DOI: 10.15406/iratj.2023.09.00261