e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2020. № 1
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2020. № 1

UDC 004.056

A METHOD OF THE TRANSMITTED BLOCKS INFORMATION INTEGRITY CONTROL

Tanygin M. O. – Dr. Sc., Associate Professor, Head of the department of Information Security, Southwest State University, Kursk, Russian Federation.

Alshaeaa H. Y. – Post-graduate student of the department of Information Security, Southwest State University, Kursk, Russian Federation.

Kuleshova E. A. – Post-graduate student of the department of Information Security, Southwest State University, Kursk, Russian Federation.

ABSTRACT

Context. For the proper operation of the hardware and software systems, it is necessary that the hardware component receives data only from the corresponding software. Otherwise, the data received from extraneous programs that can be perceived and processed by the device, which can lead to errors in the operation of the device or even a complete loss of its functionality or data.

Objective. In order to increase the reliability of legal software data and identify the challenges of the transfer of blocks, this article focuses on a comprehensive study of the problems arising from the transmission of information in the form of separate data blocks.

Method. The methods of integrity control in modes of transmission are described. The method based on hashes and block delivery time is analyzed in detail, analysis the methods of reducing the probability of errors occurring in the receiver and the possibility of reducing the reception of the extraneous blocks when receiving individual blocks of information. This is done by using a set of mathematical equations. And measure the extent of the effect of intensity of receiving extraneous blocks and hash field length.

Results. In the process of analyzing systems in which information is transmitted by block, when using the method of formation of information chains based on the method the hashes and the delivery time of the block, where we note, when the value of the hash field is equal to 6 or more, the probability of occurrence of duplicate branches is acceptably low. Where, when hash field more then 6, the parameter of length of a chain practically does not affect the final probability of constructing a chain from the extraneous blocks. The very same value of the probability of constructing a false chain, the length exceeding the chain of legal blocks at hash field more 6 is about1 10–3, which it's acceptable for real information transmission systems.

Conclusions. Based on the analysis, we can conclude that in systems in which information is transmitted block by block, when using the method of generating information chains based on the hash and block arrival time, with a hash field of 6 or more, the probability of occurrence of duplicate branches is acceptably low.

KEYWORDS: probability calculation, messages limited in length, authentication control, hash field length, duplicating branches in a chain.

ABBREVIATIONS

FB is a foreign block;

FC is a foreign chain.

NOMENCLATURE

F_{hash} is a hash-function;

H is a length of the hash field;

K is a parameter of simulated (intensity of receiving extraneous block);

L is a length of a chain;

N is a number of block;

P_B – probability of receiving blocks from of the correct chain;

p_C is a probability of adding the first incoming foreign block to the chain;

$p(i)$ is a binomial law of the received blocks are distributed;

P_{FB} – probability of receiving the foreign block;

$p(n_{FB},l)$ – probability of obtaining the receiver exactly n_{FB} blocks during the time of obtaining l legal blocks;

S_{false} is a block from another chain;

S_{rec} is an incoming data block;

$S_{\text{rec}}^{\text{hash}}$ is a hash part of the incoming block;

S_r^{inf} is an information part of the incoming block number r.

INTRODUCTION

Technology block-chain, that integration into a structured sequence of information, which represented in the form of separate blocks due to the use of the cryptographic hashing functions, it has recently gained wide popularity.

The identification information of the received block is compared with the information processed according to rules of information from the information blocks that already received by the receiver to the present moment, and, in case of coincidence, the block is added to the sequence as shown in Figure (1).

As practice shows, the approaches used in modern blockchain systems, where the large blocks of information are structured and unacceptable for chains consisting of small size blocks, accordingly, having hashes with a length that does not allow us to talk about a negligible probability of their coincidence, as in the case of standardized algorithms for cryptographic hashing. We are talking about blocks of information that size up to several tens of bits, which are used in radio identification systems, as instructions for the program the control of devices, etc. [6].

DOI 10.15588/1607-3274-2020-1-18

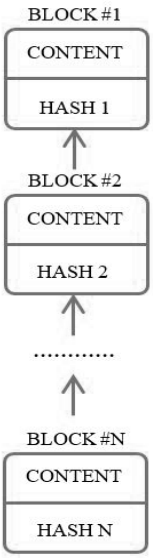

Figure 1 – Blocks that are combined into a sequence based on the identification information

The object of study is a comprehensive study of the problems arising from the transmission of information in the form of separate data blocks.

The subject of study is the methods of integrity control in modes of transmission are described. The method based on hashes and block delivery time is analyzed in detail, analysis the methods of reducing the probability of errors occurring in the receiver and the possibility of reducing the reception of the extraneous blocks when receiving individual blocks of information.

The purpose of the work is to increase the reliability of legal software data and identify the challenges of the transfer of blocks.

1 PROBLEM STATEMENT

There are many options for formation of identification data of information blocks and their analysis.

1. Only the hash of the previous blocks is used as identification data. The receiver analyzes the hashes of all received blocks and determines the location of the newly received blocks.

2. Only the hash of the previous blocks is used as identification data, but the receiver when determining the location of the block in the chain, takes account the time of its receipt. That means, if the one block arrived at the receiver later than the other, then in the formed chain it should take place with a higher index.

3. The hash of the previous blocks and the block index in the chain are used as identification data. The block index in the chain refers to uniquely positions of the block in the chain, while the hash is used exclusively to prevent extraneous blocks from entering to the chain.

Each of the described approaches has advantages and disadvantages for determining the membership of the chain block.

Based on the calculation of hashes, there is a little repetition of the information if it is compared with a method based on the calculation of hashes and the block index in the chain. The disadvantage is the complexity of determining the location of the block in the chain, because this requires comparing with the all hashes blocks in the chain. And if the chain is longer, that mean, this process will take a long time.

The disadvantage of the method based on the calculation of hashes and the delivery time of the block is the impossibility of responding this situation, when the information block issued earlier came as a result of delays later than the subsequent one. This situation is possible in telecommunication networks (wired and remote communication). In addition, the algorithm becomes more complicated to separate the blocks from several chains, in the case, when the blocks formed by several sources are transmitted through one communication channel. The advantage of this method includes the fact that the delivery time of the block itself adds more information about the block and its place in the chain. At the same time, it does not create additional redundancy information, which allows achieving the same reliability transmission characteristics as in the method based on hash functions, with a shorter length of the hash field itself.

The method of identifying the block based on the hash and the block index in the chain is the most reliable, both in terms of the reliability of the receiver separation of information blocks of different chains, and in terms of the algorithmic complexity of the formation of the block chains themselves. In the latter case, the block index determines a uniquely place in the chain [10]. But this is causing the main drawback of this method – the length of the chain is limited because the maximum size which is determined by the bit width of the index field. In addition, we obtain additional information redundancy, since instead of a probabilistic approach to determining the place of a block in chains by its hash (which means losing some of the information, and hence a decrease in the length of additional fields) we have a strictly defined index value [11, 12].

Let's consider in more detail one of the methods – based on hashes and block delivery time. The incoming data block S_{rec} consists of the information part $S_{\text{rec}}^{\text{inf}}$ and the hash result $S_{\text{rec}}^{\text{hash}}$, that obtained from the data of the previous block of the chain [13, 14]:

$$S_{\text{rec}} = \left\{ S_{\text{rec}}^{\text{inf}} \mid S_{\text{rec}}^{\text{hash}} \right\}. \quad (1)$$

If the hash, calculated from block number *r*, the last chain block at the current moment, coincides with the hash $S_{\text{rec}}^{\text{hash}}$, then the block S_{rec} will be added to the chain and becomes the last one:

$$S_{\text{rec}}^{\text{hash}} = F_{\text{hash}}\left(S_r^{\text{inf}}\right) \quad (2)$$

It is natural, with this approach raises the issue of collisions. If a block from another chain S_{false} (while we do

DOI 10.15588/1607-3274-2020-1-18

not consider how it was formed as a result of the actions of intruders or because availability of several sources of chain formation) arrives to the receiver, and its hash matches with the hash that obtained from the last block of the current chain:

$$S_{\text{false}}^{\text{hash}} = F_{\text{hash}}\left(S_r^{\text{inf}}\right), \quad (3)$$

this "extraneous" block will be added to the chain as block number r+1, and the "correct" block number r+1 that comes after it will be ignored because of the mismatch of its own hash with another hash, that obtained from the data of the "extraneous" block:

$$S_{\text{r+1}}^{\text{hash}} \neq F_{\text{hash}}\left(S_{\text{false}}^{\text{inf}}\right) \quad (4)$$

To prevent this situation, it is necessary to compare the hash of the received block not only with the hash from the last block of the chain, but also with all hashes that obtained from all the blocks that make up the chain until the present moment. Let a_{j+1} is a number of words, received in the receiver, the hash of which coincided with the hash formed from the j-th word in the chain:

$$\begin{aligned} &S_{j,a_j} = S_{\text{rec}}, a_j = a_j + 1, \\ &\text{if } S_{\text{rec}}^{\text{hash}} = F_{\text{hash}}\left(S_j^{\text{inf}}\right), \; j = \overline{1,r}. \end{aligned} \quad (5)$$

But as a result, the chain of blocks is processed by the receiver and transformed into a tree, as shown in Figure (2), where the numbers refer to the block numbers in the corresponding chain, and the number in bracket refer to the branch number of the block in the block tree.

In addition to the complexity of storing that similar to the tree structure, like this approach leads to a number of problems that we will be considered below.

The problem of duplicating branches in a chain occurs when the hash of the received block coincides not only with the hash of the last block of the chain, but also with a hash that obtained from one of the earlier blocks. As a result of this situation, when receiving subsequent blocks, they will be attributed not only of the main chain as shown in the figure (2), but also to the secondary, since their hashes will completely satisfy the inclusion condition both one, and another branch of the chain.

There are three methods to resolve this problem. The first method is to choose the longest chain from all the possible branches of the chain.

The second method involves changing the format of the blocks, where there is one hash from several consecutive blocks of a chain that controls on the sequence of these blocks. This would reduce, though not completely exclude, the possibility of the formation of such side branches in the chain [15, 16].

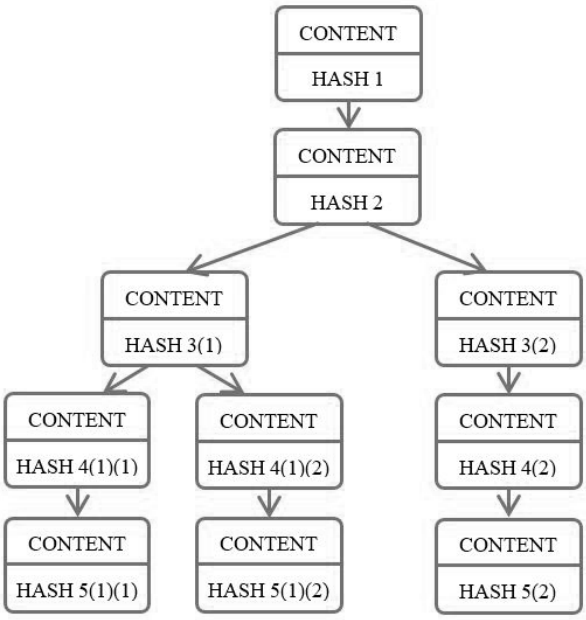

Figure 2 – Block tree, arising as a result of the coincidence of the hash of the received block with the hash of the last block in the chain

The third method is to periodically check the length of all the chains and cutting those that do not correspond to the threshold conditions. For example, the length of the chain is less than the length of the maximum chain by a fixed value L. In this case, we allow the erroneous to the removal of the correct chain. The present work is devoted to the consideration of this method and the study of its characteristics.

In system where the positioning of the block is carried out exclusively by matching the hash of the current block, the probability of duplicate chains is determined only by the hash field length H in bits. In turn, the probability of incorrect selection of chains depends on the value of L – the difference between the length of the longest chain in the tree and the shortest one that has not yet been cut off. Below we describe a method that allows you to determine the relationship between these two parameters and the probability of erroneous deletion of the correct chain.

2 REVIEW OF THE LITERATURE

At the same time, similar approaches have been used earlier to authentication of two subjects of exchange information [1–3]. The principle of interaction between the source (the generator of information blocks) and the receiver (recipient of information blocks) is based on the fact that identification information generated in some way is added to a block and usually add a hash of one or several previous information blocks, which allows to accurately determine, firstly, the identity of the specific sequence of the information block, secondly, the place of the block in sequence.

Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority. This iterative process confirms the integrity of

DOI 10.15588/1607-3274-2020-1-18

the previous block, all the way back to the original genesis block. Because of the properties of hash functions, a slight change in data will change the hash drastically. This means that any slight changes made in any block, will change the hash which is stored before this block and so on and so forth [4, 5]. This will completely change the chain, which is impossible.

With the rapid development of transfer blocks technology, different industries gradually realize technological superiority. In the meantime, there are still some technical challenges and limitations in mass transfer technologies and data to the real source. A good example for this is the problems and security risks in blockchain application are becoming more and more obvious, such as 51% attack [7] and limited size of block [8]. Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any transfer blocks technology has a specified algorithm for scoring different versions of the history so that one with a higher value can be selected over others. In order to identify the challenges of the transfer of blocks, this paper is a comprehensive study of the problems that arise from the use of the method the hashes and the delivery time of the block and the possibility of reducing the reception of extraneous blocks [9].

The problem of embedding the extraneous block in a chain occurs when the one or several blocks of extraneous chains fall into the gap between two adjacent blocks of the chain, the hashes of which satisfy the condition of their inclusion in the chain. As a result, the chain extends over these several extraneous blocks. If, by analogy with the problem of duplicating chains, compare the hash of the incoming block not only with the hash from the last block of the chain, but also with all hashes that obtained from all the blocks included in the chain until the present moment, then we get a tree in which the longest chain is a chain with extraneous blocks. The correct chain is shorter than the maximum chain by one or more blocks. Accordingly, of the methods described above to counter the formation of erroneous chains, the only acceptable can only be the control of individual consecutive blocks by using an additional hash field [17, 18].

3 MATERIALS AND METHODS

To find the dependence between values L and H and the probability of incorrect chain clipping, we apply the same mathematical model as in [19]. Let's imagine the process of receiving information blocks by the receiver (both blocks of the correct chain, and the extraneous blocks – blocks of other chains and random blocks that received by the receiver) as a random Poisson process, this a process without a background in which the probability of obtaining the next block does not depend on how much the period that blocks were received before it. Let the intensity of obtaining extraneous blocks K times more than the intensity of the formation of blocks of the legal or correct chain:

$$P_{FB} = K \times P_B. \quad (6)$$

Since we are using a method based on the elimination of those chains that are less than the maximum by any number L, it's logical to check the hash of each newly obtained block for a match with the hashes of not all blocks and branches of the chain, but only with those that belong to the branches that depart from the last L blocks of the longest chain to the present moment. To do this we assume that the longest chain to the beginning of the simulation consists entirely of legal blocks and the number of these blocks is N.

Let in this time, during the receiver receives l blocks, the number of extraneous blocks will be n_{FB}. This number will be distributed according to the Poisson law with the expectation $K \times l$:

$$p(n_{FB}, l) = \frac{(K \cdot l)^{n_{FB}} \times e^{-(K \cdot l)}}{n_{FB}!}. \quad (7)$$

The probability of adding a block to any chain is determined by the width of the hash field: $p_C = 2^{-H}$, where H – is the length of the hash field in bits.

Next, we will implement the following reasoning. Each block comes independently of the other and can be simultaneously added to the several branches. If we consider a specific block, the first incoming foreign block will be added to the chain after it with probability p_C, and ignored with probability $(1 - p_C)$. For the second and third block that came, the probabilities are similar. The probability of forming a chain of three blocks will be $(p_C)^3$, the probability of forming a chain of two blocks will be the sum of three terms:

– $p_C \times p_C \times (1 - p_C)$ – The probability that the first two blocks are added and the third is ignored.

– $p_C \times (1 - p_C) \times p_C$ – The probability that the first and third blocks will be added and the second is ignored.

– $(1 - p_C) \times p_C \times p_C$ – The probability that the second and third blocks will be added and the first is ignored.

The probability of forming a chain from one block will also be equal to the sum of three terms:

– $p_C \times (1 - p_C) \times (1 - p_C)$ – probability that the first block will be added,

– $(1 - p_C) \times p_C \times (1 - p_C)$ – probability that the second block will be added,

– $(1 - p_C) \times (1 - p_C) \times p_C$ – probability that the third block will be added.

The probability of ignoring all the blocks (the construction of length a chain is zero) will be $(1 - p_C)^3$. Similar reasoning can be carried out for an arbitrary number of extraneous blocks. It can be seen, the probability of adding to an arbitrary block of a branched chain of length i of blocks from n_{FB} of the received blocks are distributed according to the binomial law:

$$p(i) = C^i_{n_{FB}} \cdot (p_C)^i \cdot (1 - p_C)^{n_{FB-i}}. \quad (8)$$

DOI 10.15588/1607-3274-2020-1-18

Let us define the probability p_{FC} of constructing a chain from the extraneous blocks, where length longer than the number of legal blocks. This will happen in the event that during the time during which the receiver receives and writes a new block to the chain, from the block under the number N will be built a branch not less than 2 extraneous blocks, from the block under the number $N-1$ will be built a branch not less than 3 extraneous blocks, etc., up to the block under the number ($N–L$ + 1), from the length of a chain (L+ 2) and more should be constructed as shown in Figure (3).

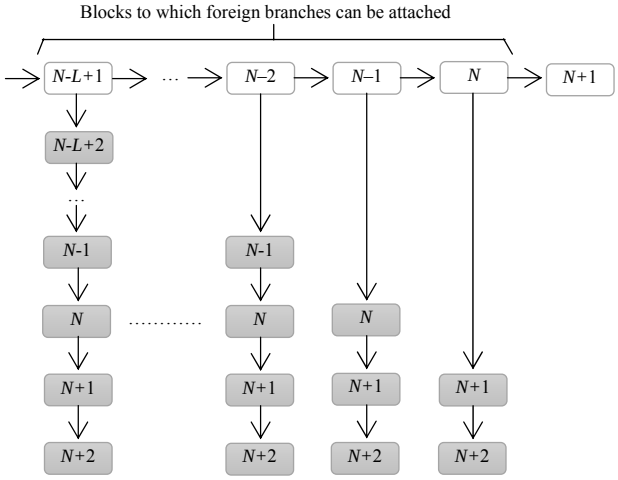

Figure 3 – Building a chai that length is longer than number of legal blocks

Since all branches consisting of their extraneous blocks (in the figure shows hatching), are being built independent of each other and in the general case can consist of the same blocks, the probabilities of their construction are independent of each other. Then probability of finding the number of extraneous blocks in n_{FB} will be defined as:

$$p(n_{FB}) = \sum_{i=1}^{L} \left\{ \sum_{j=1+i}^{n_{FB}} C_{n_{FB}}^{j} \cdot (p_C)^j \cdot (1-p_C)^{n_{FB}-j} \right\}. \quad (9)$$

In common case, combining the received expression with the formula for $p(n_{FB}, l)$ at l=1:

$$p_{FC} = \sum_{v=2}^{\infty} \left\{ \frac{K^v \times e^{-K}}{v!} \times \sum_{i=1}^{L} \left[\sum_{j=1+i}^{v} C_v^i \cdot (p_C)^j \cdot (1-p_C)^{v-j} \right] \right\}, \quad (10)$$

$$v \geq i+1.$$

4 EXPERIMENTS

In Figure (4) are presented graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, the intensity of receiving extraneous blocks K and the length of the hash field H in bits and the number of blocks L which extraneous blocks can be attached.

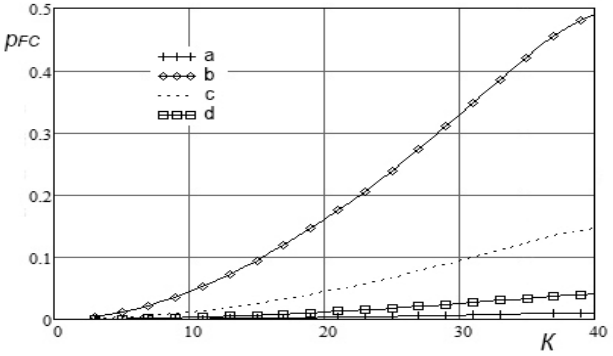

Figure 4 – the graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, the intensity of receiving extraneous blocks K and the length of the hash field H in bits with L =4.
a) H = 5; b) H = 6; c) H = 7; d) H = 8

Calculations show the number of blocks L which blocks can be joined by extraneous blocks, does not effect on the probability of constructing a long chain from extraneous blocks.

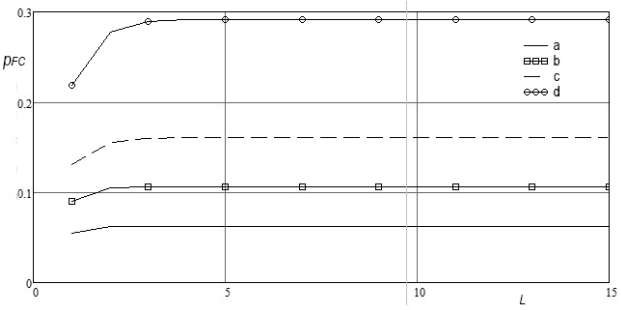

Figure 5 – graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, from the parameter L and the intensity of receiving extraneous blocks K for a fixed hash field length H = 4.
a) K = 3; b) K = 4; c) K = 5, d) K=7

This is easily explained by the fact that the probability of constructing long chains of extraneous blocks is negligible, if compared with the probability of constructing branches with a length of one or two blocks. like this chains can be lead to the error of determining the longest chain that only starting from the last (the penultimate legal block of a chain).This is clearly to seen in the figure (5), where the graphs dependence of p_{FC} on L that represent a practically horizontal straight line starting with the values L = 3 ... 5.

5 RESULTS

Based on the graphs received, we can conclude what contribution to the final probability of the p_{FC} that make certain of its components. It can be seen that depending on the value intensity of receiving extraneous blocks K, the sum of the probabilities of constructing side chains that are more than legal blocks length, from the last 2 is

DOI 10.15588/1607-3274-2020-1-18

from 80% to 95% of the total probability of constructing side chains from all L last blocks. For the sum of probabilities for the last 4 blocks, this is increases to 98% – 99.9%. These values will be useful to us in the future, when modeling of the receiver by the receiver of more than one legal of block or in the situations, when the time of obtaining the last legal block by the receiver is already available, in addition to the main a number of side chains.

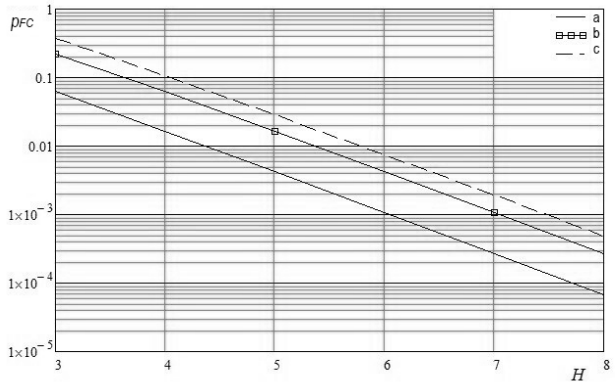

Figure 6 – graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, the length of the hash field H and the intensity of receiving extraneous blocks K with $L = 5$.
a) $K = 3$; b) $K = 6$; c) $K = 8$

Finally, we explore the impact length of the hash field on the probability of constructing a long chain of extraneous blocks. In Figure (6) shows this dependence for greater clarity on a logarithmic scale. It can be seen this is practically an exponential dependence of the form $p_{\text{FC}} = k1 \times e^{-k2 \cdot H}$.

As an intermediate result, we can say that there is no great need to increase the parameter L – the number of blocks to which incoming blocks can be attached. If there are no additional conditions, it can be selected in the range from 3 to 6, varying only the length of the hash field during transmission, that depending on the observed intensity of receiving extraneous blocks. This parameter can be calculated dynamically as a ratio of the number of information blocks that received during a certain period, to the maximum lengthening for the same period of the longest chain [19].

Next, we simulate the interval during the receiver received more than one legal block. To do this, consider the chains that were formed at the time of obtaining N blocks (Figure (7)). In addition to the main chain, the chain V^N – V^{N-L+2} to which the resulting blocks can be attached. This is due to the fact that the chain V^{N-L+1} it will be impossible to join the blocks because to the above limitations. Also, based on the results that obtained above, we can say that the probability the length of the chain V^{N-L+1} will exceed the number L is negligible if compared with the total probability p_{FC} (Depending on the length of the field, were the values from $10^{-12}$to 10^{-8}).

Strictly speaking, each chain like this will be representing a bush the chains of arbitrary length.

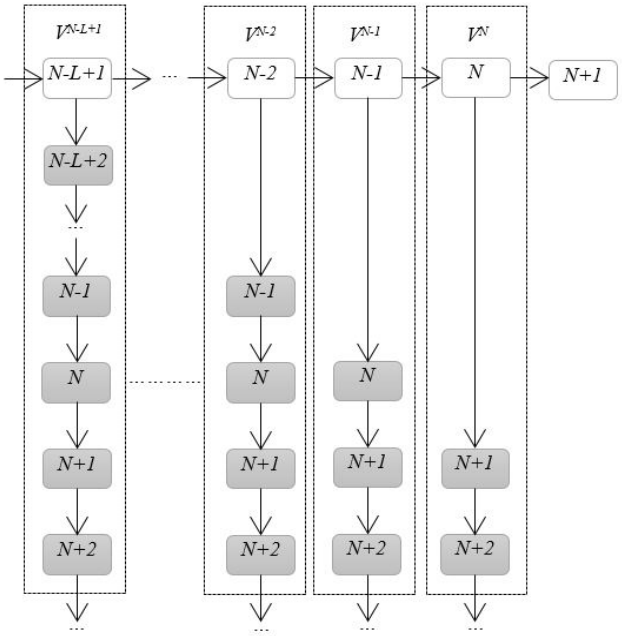

Figure 7 – The chains formed to the moment of obtaining N+1 legal block

Now we must take into account, that the chain V^N is formed from the extraneous blocks that obtained by the receiver between obtaining N and N+1 blocks, the chain V^{N-1} is formed from extraneous blocks that obtained by the receiver between obtaining N–1 and N+1 blocks, the chain V^{N-2} is formed from extraneous blocks that obtained by the receiver between obtaining N–2 and N+1 blocks, etc. Accordingly, the final probability of constructing a complex chain exceeding the main length, that determined by the sum of the probabilities of constructing chains V^N – V^{N-L+2} corresponding lengths. For a chain with the number V^{N-i} it is equal to (i +2).

For a chain V^{N-i}, by analogies with formula (5), the expression takes the form:

$$p_{V^{N-i}} = \sum_{v=i+2}^{\infty} \frac{((i+1)\times K)^v \times e^{-((i+1)\times K)}}{v!} \sum_{j=v}^{\infty} C_v^j \cdot (p_C)^j \cdot (1-p_C)^{v-j}. \quad (11)$$

In General, considering that the construction of each of the L chains – is an independent event, the probability that at least one of them will exceed to the length of the chain from legal blocks:

$$p_{FC} = 1 - \prod_{i=0}^{L-1} (1 - p_{V^{N-i}}) =$$

$$= 1 - \prod_{i=0}^{L-1} \left\{ 1 - \sum_{v=i+2}^{\infty} \frac{((i+1)\times K)^v \times e^{-((i+1)\times K)}}{v!} \left[\sum_{j=v}^{\infty} C_v^j \cdot (p_C)^j \cdot (1-p_C)^{v-j} \right] \right\}. \quad (12)$$

The dependence of the probability p_{FC} on the parameter L is shown in Figure (8).

DOI 10.15588/1607-3274-2020-1-18

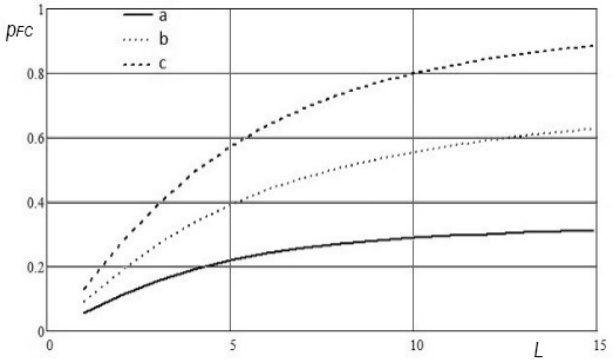

Figure 8 – graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, from the parameter L and the intensity of receiving extraneous blocks K for a fixed hash field length H =3
a) K = 3; b) K = 4; c) K =5

6 DISCUSSION

It can be seen that starting from L = 10, the increase of the probability of constructing a false chain is insignificant. The length of the hash field has the greatest impact on this probability. In the Figure (9) shows the dependence of p_{FC} on H and K. The region, that the most significant of the absolute values fall for the probability of constructing a false chain, it occurs in the range from H = 3 to H = 6. In the same range, the influence of the parameter value of L on the required probability is significantly reduced.

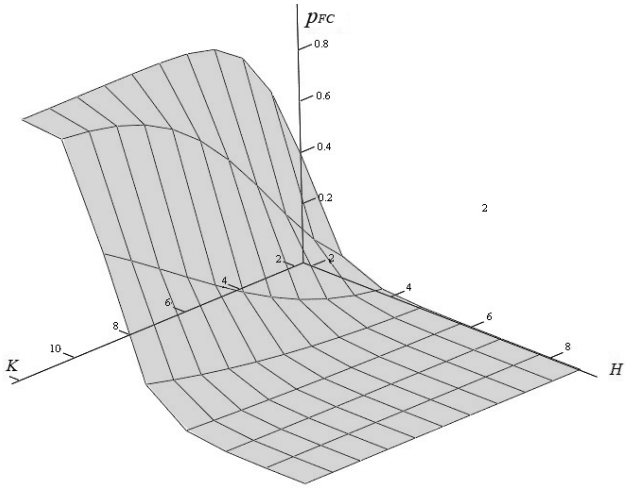

Figure 9 – graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, the length of the hash field H and the intensity of receiving extraneous blocks K with L = 4

Figure (10) shows the relative dependence of the value of p_{FC} on H for different values of L. For 1 at each point, the probability of constructing a false chain at L = 18 is adopted. It can be seen, when H> 6, the parameter of L practically does not affect the final probability of p_{FC}. The very same value of the probability of constructing a false chain, the length exceeding the chain of legal blocks at H> 6 is about1 10^{-3}, which it's acceptable for real information transmission systems.

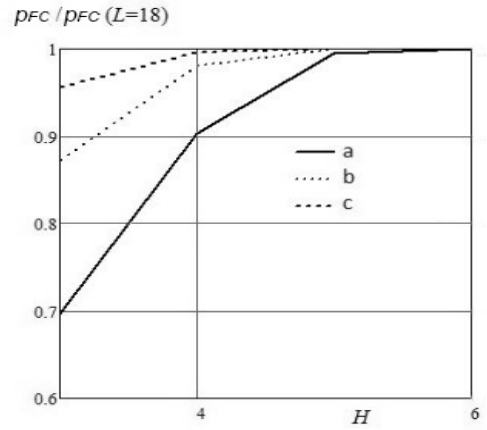

Figure 10 – Graph of the ratio of the value p_{FC} for different values of the parameter L to the value of p_{FC} at L = 18 (intensity of receiving extraneous blocks K = 5).
a) L = 6; b) L = 10; c) L =14

CONCLUSIONS

The above allows us to conclude that in the process of analyzing systems in which information is transmitted by block, when using the method of formation of information chains based on the method the hashes and the delivery time of the block, where we note, when the value of the hash field is equal to 6 or more, the probability of occurrence of duplicate branches is acceptably low. Where, when hash field more then 6, the parameter of length of a chain practically does not affect the final probability of constructing a chain from the extraneous blocks. The very same value of the probability of constructing a false chain, the length exceeding the chain of legal blocks at hash field more 6 is about1 10^{-3}, which it's acceptable for real information transmission systems.

ACKNOWLEDGEMENTS

This work was supported by the Federal State Budget Institution "Russian Foundation for Basic Research" on the basis of the grant "Research on the resistance of machine-based encryptors based on cellular automata to algebraic cryptanalysis" (Contract No. 19–31–90069 \ 19).

REFERENCES

1. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: NIST Special Publication 800–38A. Gaithersburg, Maryland, October 2010. 11p.
2. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. NIST Special Publication 800–38C. Gaithersburg, Maryland, May 2004. 25p.
3. Tanygin M. O., Tipikin A. P. Architecture of system of hardware restriction of access to information on a computer hard disk, *Telecommunications*, 2006, No. 3, pp. 44–46.
4. Knudson L. Block Chaining Modes of Operation. NIST First Modes of Operation Workshop [Electronic resource]. October 2010. Access mode: http://csrc.nist.gov/groups/ST/toolkit/BCM/workshops.html.

DOI 10.15588/1607-3274-2020-1-18

5. Gervais A., Ghassan O., Wüst K., Glykantzis V., Ritzdorf H., Capkun S. On the Security and Performance of Proof of Work Blockchains [Electronic resource], 2016. – Access mode: https://eprint.iacr.org/2016/555.pdf.
6. Black J., Rogaway P. and Shrimpton T. CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. Advances in Cryptology, *CRYPTO '00*. Santa Barbara, California, 2000, pp. 197–215.
7. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015, 152 p.
8. McGrew D., Viega J. The Security and Performance of the Galois/Counter Mode (GCM) of Operation, *In Proceedings: Indocrypt*, 2004, pp. 343–355.
9. Tanygin M.O. Method of Control of Data Transmitted Between Software and Hardware, *Computer Science and Engineering: Materials of the IV International Conference of Young Scientists CSE-2010*. Lviv, Publishing House of Polytechnics, 2010, pp. 344–345.
10. Bellare M., Kilian J., Rogaway P. The security of the cipher block chaining message authentication code, *JCSS*, 1994, Vol. 3, No. 3, pp. 341–358.
11. Stallings W. NIST Block Cipher Modes of Operation for Authentication and Combined Confidentiality and Authentication, *Cryptologia*, 2010, pp. 225 – 23.
12. Stallings W. The Advanced Encryption Standard. Cryptologia, 2002, No. 26, pp. 165–188.
13. Tanygin M.O. Calculation of the probability of collisions when using the message authentication algorithm, *News SWSU*, 2012, pp. 179–183.
14. Gubarev A. V., Tanygin M. O. Research of dependence of time of searching legal instruction words from the width of the buffer the received instruction words, Telecommunications, 2015, pp. 21–26.
15. Stallings W. NIST Block Cipher Modes of Operation for Confidentiality, *Cryptologia,* 34(2), pp. 163–175.
16. Tilborg H. C. Encyclopedia of Cryptography and Security. Heidelberg, Springer, 2005, pp. 11–15.
17. Lipmaa H. P., Rogaway P., and Wagner D. CTR Mode Encryption. NIST First Modes of Operation Workshop [Electronic resource]. Access mode: http://csrc.nist.gov/groups/ST/toolkit/BCM/workshops.html.
18. Voydock V., Kent S. Security Mechanisms in High-Level Network Protocols, *Computing Surveys,* June 1983, pp. 135–171.
19. Tanygin M.O., Search and elimination of collisions in information exchange through open communication channels, *Problems of Informatics in Education, Management, Economics and Technology: a collection of articles of the Xth International Scientific and Technical Conference.* Penza, Privolzhsky House of Knowledge, 2010. pp. 62–64.

Received 30.05.2019.
Accepted 23.11.2019.

УДК 004.056

МЕТОД КОНТРОЛЮ ЦІЛІСНОСТІ ПЕРЕДАНИХ БЛОКІВ ІНФОРМАЦІЇ

Танигін М. О. – канд. техн. наук, доцент, завідувач кафедрою інформаційної безпеки, Південно-Західний державний університет, м. Курськ, Росія.

Алшаиа Х. Я. – аспірант кафедри інформаційної безпеки, Південно-Західний державний університет, м. Курськ, Росія.

Кулешова О. О. – аспірант кафедри інформаційної безпеки, Південно-Західний державний університет, м. Курськ, Росія.

АНОТАЦІЯ

Актуальність. У статті приділено увагу всебічному вивченню проблем, що викликають передачу інформації у вигляді окремих блоків даних (кадрів, фреймів).

Метод. Описані методи контролю цілості у таких способах передачі. Детально розглянуто метод на основі ґешів і часу доставки блоку, проаналізованих методами зниження ймовірності помилок, відновлюючих прийомів при приєднанні окремих блоків інформації.

Результати. У процесі аналізу систем, в яких інформація передається блоком, при використанні методу формування інформаційних ланцюгів на основі методу хешів і часу доставки блоку, де ми зазначаємо, коли значення ґеш-поля дорівнює 6 і більше, ймовірність появи повторюваних гілок є прийнятно низькою. Де, коли ґеш-поле більше 6, параметр довжини ланцюга практично не впливає на остаточну ймовірність побудови ланцюга із сторонніх блоків. Саме це значення ймовірності побудови помилкового ланцюга, довжина якого перевищує ланцюжок легальних блоків у ґеш-полі більше 6 становить приблизно 10^{-3}, що є прийнятним для реальних систем передачі інформації.

Висновки. На основі проведеного аналізу можна зробити висновок, що в системах, в яких інформація передається поблоково, при використанні методу формування інформаційних ланцюжків на основі ґешу і часу надходження блоку, при величині поля ґешу від 6 і більше ймовірність виникнення дублюючих гілок є прийнятно низьклю.

КЛЮЧОВІ СЛОВА: розрахунок ймовірності, повідомлення обмеженої довжини; контроль автентичності; довжина ґеш-поля; дублювання гілок у ланцюжку.

УДК 004.056

МЕТОД КОНТРОЛЯ ЦЕЛОСТНОСТИ ПЕРЕДАВАЕМЫХ БЛОКОВ ИНФОРМАЦИИ

Таныгин М. О. – канд. техн. наук, доцент, заведующий кафедрой информационной безопасности, Юго-Западный государственный университет, г. Курск, Россия.

Алшаиа Х. Я. – аспирант кафедры информационной безопасности, Юго-Западный государственный университет, г. Курск, Россия.

Кулешова Е. А. – аспирант кафедры информационной безопасности, Юго-Западный государственный университет, г. Курск, Россия.

DOI 10.15588/1607-3274-2020-1-18

АННОТАЦИЯ

Актуальность. В статье уделяется внимание всестороннему изучению проблем, возникающих при передаче информации в виде отдельных блоков данных (кадров, фреймов).

Метод. Описаны методы контроля целостности в таких способах передачи. Детально рассмотрен метод на основе хешей и времени доставки блока, проанализированы методы снижения вероятности ошибок, возникающих в приёмнике при приёме отдельных блоков информации.

Результаты. В процессе анализа систем, в которых информация передается по блокам, при использовании метода формирования информационных цепочек на основе метода хэшей и время доставки блока, где мы отмечаем, когда значение хеш-поля равно до 6 или более, вероятность появления дублирующих ветвей является приемлемо низкой. Когда хеш-поле больше 6, параметр длины цепочки практически не влияет на конечную вероятность построения цепочки из посторонних блоков. Само же значение вероятности построения ложной цепочки, длина которой превышает цепочку допустимых блоков в хэш-поле больше 6, составляет примерно 10^{-3}, что приемлемо для реальных систем передачи информации.

Выводы. На основе проведенного анализа можно сделать вывод, что в системах, в которых информация передаётся поблоково, при использовании метода формирования информационных цепочек на основе хеша и времени поступления блока, при величине поля хеша от 6 и более вероятность возникновения дублирующих ветвей приемлемо низка.

КЛЮЧЕВЫЕ СЛОВА: расчет вероятности, сообщения ограниченной длины, контроль подлинности, длина хеш-поля, дублирование ветвей в цепочке.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: NIST Special Publication 800–38A. Gaithersburg, Maryland, October 2010. 11p.
2. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. NIST Special Publication 800–38C. Gaithersburg, Maryland, May 2004. 25p.
3. Tanygin M. O. Architecture of system of hardware restriction of access to information on a computer hard disk / M. O. Tanygin, A. P. Tipikin // Telecommunications. – 2006. – № 3. – P. 44–46.
4. Knudson L. Block Chaining Modes of Operation. NIST First Modes of Operation Workshop [Electronic resource] / L. Knudson. – October 2010. – Access mode: http://csrc.nist.gov/groups/ST/toolkit/BCM/workshops.html.
5. Gervais A. On the Security and Performance of Proof of Work Blockchains [Electronic resource] / [A. Gervais, O. Ghassan, K. Wüst et al.] – 2016. – Access mode: https://eprint.iacr.org/2016/555.pdf.
6. Black J. CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. Advances in Cryptology / J. Black, P. Rogaway, and T. Shrimpton // CRYPTO ‘00. – Santa Barbara, California. – 2000. – P. 197–215.
7. Swan M. Blockchain: Blueprint for a New Economy / M. Swan. – O’Reilly Media, Inc., 2015. – 152 p.
8. McGrew D. The Security and Performance of the Galois/Counter Mode (GCM) of Operation / D. McGrew, J. Viega // In Proceedings: Indocrypt. – 2004. – P. 343–355.
9. Таныгин М. О. Метод контроля данных, передаваемых между программным и аппаратным обеспечением / М. О. Таныгин // Информатика и вычислительная техника: материалы IV Международной конференции молодых ученых CSE-2010. – Львов : Изд-во Политехники, 2010 – С. 344–345.
10. Bellare M. The security of the cipher block chaining message authentication code / M. Bellare, J. Kilian, P. Rogaway // JCSS. – 1994. – Vol. 3, No. 3. – P. 341–358.
11. Stallings W. NIST Block Cipher Modes of Operation for Authentication and Combined Confidentiality and Authentication / W. Stallings // Cryptologia. – 2010. – P. 225–23.
12. Stallings W. The Advanced Encryption Standard. Cryptologia. – 2002. – № 26. – P. 165–188.
13. Таныгин М.О. Расчет вероятности коллизий при использовании алгоритма аутентификации сообщений / М.О. Таныгин // Новости ЮУрГУ. – 2012. – С. 179–183.
14. Губарев А. В. Исследование зависимости времени поиска юридического слова инструкции от ширины буфера полученного слова инструкции / А. В. Губарев, М. О. Таныгин // Телекоммуникации. – 2015 – С. 21–26.
15. Stallings W. NIST Block Cipher Modes of Operation for Confidentiality / W. Stallings // Cryptologia. – 34(2). – P. 163–175.
16. Tilborg H. C. Encyclopedia of Cryptography and Security / H. C. Tilborg // Heidelberg: Springer. – 2005. – P. 11–15.
17. Lipmaa H. CTR Mode Encryption. NIST First Modes of Operation Workshop [Electronic resource] / H. P. Lipmaa, P. Rogaway, and D. Wagner. – Access mode: http://csrc.nist.gov/groups/ST/toolkit/BCM/workshops.html.
18. Voydock V. Security Mechanisms in High-Level Network Protocols / V. Voydock, S. Kent // Computing Surveys. – June 1983. – P. 135–171.
19. Таныгин М. О. Поиск и устранение коллизий при обмене информацией по открытым каналам связи / М. О. Таныгин // Проблемы информатики в образовании, управлении, экономике и технологии: сборник статей X Международной научно-технической конференции. – Пенза : Приволжский Дом знаний. – 2010. – С. 62–64.

DOI 10.15588/1607-3274-2020-1-18