Journal of Computer Virology and Hacking Techniques (2023) 19:341–349
https://doi.org/10.1007/s11416-022-00428-z

ORIGINAL PAPER

Covert channel limitation via special dummy traffic generating

Anna Epishkina[1] · **Nikolay Karapetyants**[1] · **Konstantin Kogos**[1] · **Philip Lebedev**[1]

Received: 14 January 2022 / Accepted: 13 April 2022 / Published online: 16 May 2022

Abstract
Covert channels in information systems may cause a protected data leakage and lead to violation of data confidentiality or integrity. Moreover, some types of covert channels can function even in case of network data encryption, tunneling or traffic firewall protection. A technique to eliminate such channels is traffic normalization which means sending packets with equal lengths and fixed header fields with equal inter-packets delays that leads to significant decreasing of efficient communication channels capacity and missing of functional capabilities of network protocols. Another way to counteract covert channel is to detect an active channel and limit it capacity. In this paper, we investigate covert channel protection means in packet networks based on their capacity limitation. We suggest a technique to counteract data leakage via covert channel based on dummy traffic generating and estimate maximum residual capacity of covert channel in case of counteracting measures for stream and block encryption of traffic and different distributions for covert channel and dummy traffic. Also we give recommendation for choosing the parameters of counteraction tool.

1 Introduction

A communication channel is a covert channel if it is based on a transfer that uses changes in resource states [1]. Another definition of covert channel uses a term information security policy that means a set of security rules, procedures, or guidelines for an organization. According to [2], covert channel is any communication channel, which can be used by the process in order to transmit data in a way that violates system security policy. Since resource access control systems always have resource allocation policies that work within an implementation, covert channels should be defined as channels that appear due to resource allocation policies and resource management implementation [3].

Let M be a model of non-discretionary security policy, $I(M)$ is its implementation in operating systems. Thus any potential link between subjects $I(S_h)$ and $I(S_i)$ in $I(M)$ is a covert channel if this link isn't allowed in a model M [4].

Let's consider the main threats caused by covert channels. They are as follows:

– Malware implementation;
– Transfer attacker's commands to agents for execution;
– Leakage of cryptographic keys and passwords;
– Leakage of individual information objects.

The first step to counteract information leakage via covert channels is to search for potential covert channels. After covert channel identification its potential should be assessed to determine the damage that its functioning can cause to the system. First, channel capacity should be calculated. This analysis is especially important because elimination of covert channels may be an unacceptable, besides, some scientists [5] believe that it is practically impossible to eliminate all covert channels in a computer system. Thus, in some cases, it is necessary to focus only on counteraction of covert channels with high capacity [2]. After identification and analysis of a potential covert channel, a decision is made to limit its capacity, to eliminate it or to audit.

The paper is organized as follows. Section 1 presents the basic method for covert channel capacity estimation. In Sect. 2 we describe a method to limit cover channel using dummy traffic. In Sect. 3 we give a parameters of covert channel and counteraction tool in case of stream encryption of traffic for different distribution in covert channel and dummy traffic. Section 4 is devoted to block traffic encryption. In Sect. 5 we observe partial synchronization and give recommendation to choose a required parameters. Conclusion contains the summary of the work and the directions of further research.

✉ Anna Epishkina
avepishkina@mephi.ru

[1] Moscow Engineering Physics Institute, National Research Nuclear University MEPhI, Moscow, Russia

2 Covert channel capacity

We investigate covert channels resistant to traditional security measures as data encryption, tunneling or traffic firewall protection. We assume different parameters of storage covert channels based on packets lengths modification, timing covert channels based on inter-packet delays modulation and hybrid covert channels combining both ways of information encoding.

To estimate covert channels capacity ν we use a technique based on evaluating of mutual information of random variables X and Y describing input and output characteristics of covert channel

$$\nu = \max_X \left\{ \frac{I(X,Y)}{\tau} \right\}, \tag{1}$$

where τ is—average transmission time of one packet [6].

Mutual information of random variables X, Y we estimate as

$$I(X,Y) = H(Y) - H(Y|X), \tag{2}$$

where $H(Y) = -\sum_{i=1}^{n} p_{out}(i) \log_2 p_{out}(i)$ is entropy of random variable Y, $H(Y|X) = -\sum_{j=1}^{n} p_{in}(j)\left(\sum_{i=1}^{n} p_{out}(i|j) \log_2 p_{out}(i|j)\right)$ is conditional entropy of random variable Y comparatively to random variable X, $p_{in}(j)$ is probability to send symbol 'i', $p_{out}(i)$ is probability that a receiver recognizes symbol 'i', $p_{out}(i|j)$ is conditional probability that a receiver recognizes symbol 'i' when symbol 'j' is sent.

3 Covert channel capacity limitaion using dummy traffic

Next, we suggest a technique to counteract data leakage via covert channel based on dummy traffic generating. We observe hybrid covert channel based on packets lengths modification and on inter-packet delays modulation. At first, we will gain parameters of storage covert channel. Countermeasure consists in sending of dummy packets with length distribution L_{DT}. From the point of view of the effective communication channel capacity, it is necessary to send dummy packets with as small length as possible. Distribution L_{DT} should obey the non-increasing law , we will start from the length l_{fix} and add one bit at a time.

We examine random generation of dummy traffic as deterministic generation is easily tracked, hence is inefficient. In our case dummy packet is sent on average k packets, where k is a parameter of counteraction tool. A violator sends synchronization packets of a special type, that decreases a number of informative packets in a covert channel and allows one to reduce errors that are caused by the counteraction tool. Thus, a violator codes data in packets, adds special packets and then dummy packets are inserted into the outgoing traffic.

We researched the following cases:

- In dummy traffic all lengths from l_{fix} to 1500 bytes are used, we send synchronization packets and combine special packets and special dummy packets in a covert channel;
- In dummy traffic not all lengths rom l_{fix} to 1500 bytes are allowed, we construct a covert channel without errors using packets lengths that aren't used in counteraction tool (in this case there is no use of synchronization packets), aslo we biuld a covert channel with errors and can use synchronization packets and special dummy packets and their combination.

The covert channel capacity is

$$\nu = \left(1 - \frac{1}{E(K)}\right) \max_{\{p_L(i)\},n} \frac{\beta(H(L_{out}) - H(L_{out}|L))}{E(L_{out}) + \beta T}. \tag{3}$$

In the formula the factor $\left(1 - \frac{1}{E(K)}\right)$ means that dummy packets doesn't send information. This is the general view of the formula. As we don't obtain timing covert channel, then $T = \tau$. We should notice that if the distribution L_{DT} is equiprobable, in a covert channel lengths should't be less than l_{fix}. If the distribution L_{DT} is a decreasing distribution, it may be rational to use lengths from l_{fix} plus some constant s.

Output distribution L_{out} covers the same lengths as the length distribution in the covert channel L_{CH}. Also dummy traffic influence on distribution L_{out}, that forms as a weighted sum of distribution L_{CH} and truncated length distribution in dummy traffic L^*_{DT}. Truncated length distribution means zeroing probabilities for packets with lengths not included in the covert channel alphabet, it indicates packets that a violator defines and discards.

Let's consider an example of distribution of dummy traffic for stream encryption:

$$L_{DT} = \begin{pmatrix} l_{fix} & l_{fix}+1 \ldots & l_{fix}+n_C-1 & l_{fix}+n & \ldots l_{fix}+n_{DT}-1 \\ p_{DT}(1) & p_{DT}(2) \ldots & p_{DT}(n) & p_{DT}(n+1) & \ldots \quad p_{DT}(n_{DT}) \end{pmatrix}. \tag{4}$$

Than if the covert channel alphabet is $\{1, 2, 3, \ldots, n\}$ and the constant $s = 0$, the corresponding truncated distribution L^*_{DT} is equal to

$$L_{DT}{}^* = \begin{pmatrix} l_{fix} p_{DT}(1) & l_{fix}+1 \ldots & l_{fix}+n_C-1 & l_{fix}+n_C & \ldots & l_{fix}+n_{DT}-1 \\ & p_{DT}(2) \ldots & p_{DT}(n_C) & 0 & \ldots & 0 \end{pmatrix} = \begin{pmatrix} l_{fix} & l_{fix}+1 & \ldots & l_{fix}+n_C-1 \\ p_{DT}(1) & p_{DT}(2) & \ldots & p_{DT}(n_C) \end{pmatrix}. \quad (5)$$

Next we find the distribution L_{out}. Let μ be the proportion of dummy packets that have lengths from the covert channel alphabet,

$$\mu = \sum_{i=1+s}^{n+s} p_D(i), \quad (6)$$

where $s \in \{0, 1, \ldots, n_D - n_C\}$ is a shift.

Our calculations give the formula for L_{out}

$$L_{out} = \left(1 - \frac{\mu}{E(K)}\right) L_C + \frac{\mu}{E(K)} L^*_D = \frac{(E(K)-\mu)\, L_C + \mu L^*_D}{E(K)}. \quad (7)$$

We should notice that now L_{out} isn't a distribution, as the summ of probabilities is less than 1 if $\mu \in (0; 1)$, but next we call it a distribution for convenience. Calculated L_{out} gives

$$E(L_{out}) = \frac{(E(K)-\mu)E(L_C) + \mu E(L^*_D)}{E(K)}. \quad (8)$$

Thus, effective capacity of communication channel with a counteraction tool is

$$\beta' = \frac{\left(1 - \frac{1}{E(K)}\right) E(L)}{\left(1 - \frac{1}{E(K)}\right) E(L) + \frac{1}{E(K)} E(L_D)} \beta = \frac{(k-1)E(L)}{(k-1)E(L) + E(L_D)} \beta, \quad (9)$$

where L is initial distribution of packet lengths in the communication channel.

In the following sections, we will specify some special cases.

4 Stream traffic encryption

Is a case of stream encryption all possible packet lengths are present in dummy traffic. After dummy packet sending the sender and receiver of the hidden channel became out of synchronization. In order to rebuild synchronization we observe special packets transmitting [7]. A receiver fixes special packet, determine lengths of the next F–1 packets, restores the characters of the hidden transmitted message and waits for the arrival of the next special packet. Here F is a parameter of covert channel determining the synchronization frequency. In this type of countermeasures lengths of transmitted packeds don't change and dummy packets sending only leads to the need for periodic synchronization (Fig. 1, SP stands for special packet).

As average packet follow-up time τ doesn't depend on the value of the covert channel parameter F, we will estimate ν as maximum of mutual information of random variables described input and output paremeteras of a covert channel

$$\nu = \left(1 - \frac{1}{E(K)}\right) \max_{F, L_C} \frac{\beta(H(L_{out}) - H(L_{out}|L_C))}{E(L_{out}) + \beta T}, \quad (10)$$

so we have a covert channel capacity as bit per packet.

As each packet with a number F tramsmitted via covert channel is used only for synchronization we can calculate the mutual information $I(X,Y)$

$$\nu = \left(1 - \frac{1}{E(k)}\right) \max_{F, L} \left\{ \frac{F-1}{F} \frac{I^*(L_C, L_{out})}{\frac{E(L_{out})}{\beta} + T} \right\}, \quad (11)$$

where $I^*(X, Y) = H(Y) - H(Y|X)$ is mutual information of random variables X, Y calculated when excluding packages of a special type.

Conditional entropy of a random variable L_{out} comparatively to random variable L we estimate as

$$H(L_{out}|L_C) = \frac{\sum_{r=0}^{F-2} H_r(L_{out}|L_C)}{F-1}, \quad (12)$$

when from the moment of synchronization to the arrival of a dummy packet, r packets were transmitted via a covert channel.

Forming of conditional entropy $H(L_{out}|L)$ using $H_r(L|L)$ is illustrated in Fig. 2, where 0 stands for conditional entropy $H_0(L_{out}|L)$, 1 stands for conditional entropy $H_1(L_{out}|L)$, 2 stands for conditional entropy $H_2(L_{out}|L)$, x means that packet is discarded.

The author's investigation gives the following formulas for a probability that from a moment of syncronization to dummy packet arrival r packets are transmitted via covert

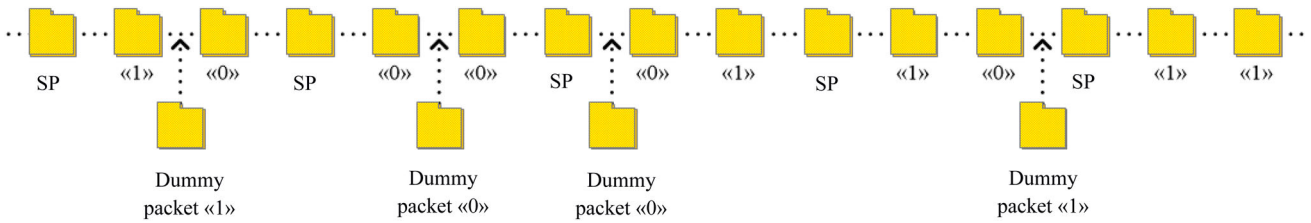

Fig. 1 Binary covert channel with random dummy traffic generation

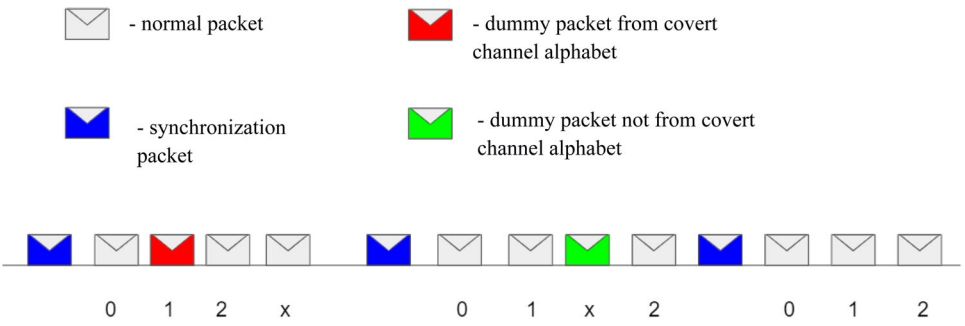

Fig. 2 Conditional entropy forming

channels and at least one of them is a dummy packet $P_{DP}(r)$ and conditional probability $P_{r\_out}(i|j)$:

$$P_{DP}(r) = \sum_{c=0}^{r} \frac{\mu}{2k-1} = \mu \frac{r+1}{2k-1}, \tag{13}$$

$$P_{r\_out}(i|j) = \mu \frac{r+1}{2k-1} p_{out}(i) + \delta_{ij}\left(1 - \mu \frac{r+1}{2k-1}\right). \tag{14}$$

In the formula $p(i)$ is a probability toget symbol 'i' distribution L_{out} and δ_{ij} is Kronecker symbol, which is $\delta_{ij} = 1$ for $i = j$ and in other cases $\delta_{ij} = 0$.

4.1 Uniform distribution of dummy traffic

In a case of uniform distribution L_D from l_{fix} to 1500 bytes a probability of sending of a dummy packet with any length is

$$p_D(i) = \frac{1}{12001 - l_0} = \frac{1}{n_D}, \tag{15}$$

where $n_D = 12001 - l_{fix}$ is a number of dummy packets with different lengths.

Due to uniform distribution there is no need to shift covert channel alphabet and $s = 0$. Thus, an intruder have to built covert channel based on the smallest packets' lengths from l_{fix}. Hence, output distribution is

$$L_{out} = \frac{\left(E(K) - \frac{n_C}{n_D}\right) L_C + \frac{n_C}{n_D} L_D^*}{E(K)}. \tag{16}$$

We will also find the average packet length in the output distribution, the entropy and the covert channel capacity:

$$E(L_{out}) = \frac{\left(E(K) - \frac{n_C}{n_D}\right) E(L_C) + \left(\frac{n_C}{n_D}\right)^2 \left(l_{fix} + \frac{n_C - 1}{2}\right)}{E(K)}, \tag{17}$$

$$H(L_{out}) = -\sum_{i=1}^{n_C} \frac{\left(E(K) - \frac{n_C}{n_D}\right) p_C(i) + \frac{n_C}{n_D} p_D(i)}{E(K)} \log_2 \frac{\left(E(K) - \frac{n_C}{n_D}\right) p_C(i) + \frac{n_C}{n_D} p_D(i)}{E(K)}. \tag{18}$$

$$\nu = \left(1 - \frac{1}{E(k)}\right)$$

$$\max_{F,L} \left\{ \frac{F-1}{F} \frac{H(L_{out}) - \frac{\sum_{r=0}^{F-2} H_r(L_{out}|L_C)}{F-1}}{\frac{\left(E(K) - \frac{n_C}{n_D}\right) E(L_C) + \left(\frac{n_C}{n_D}\right)^2 \left(l_{fix} + \frac{n_C - 1}{2}\right)}{\beta E(K)} + T} \right\}. \tag{19}$$

Covert channel parameters are alphabet power n and probability distribution for sending packet with each length L and frequency of synchronization packet transmitting F. Length's distribution L_D^* and distribution of dummy packets sending K are parameters of a counteraction tool.

4.2 Uniform distribution in covert channel

If L has a uniform distribution, a probability $p(i) = \frac{1}{n}$ and average packet length is $E(L) = l_{fix} + \frac{n_C - 1}{2}$. Entropy and conditional probability are as follows:

$$H(L_{out}) = -n_C \left(\frac{1}{n_C} - \frac{n_D - n_C}{k n_D^2} \right) \log_2 \left(\frac{1}{n_C} - \frac{n_D - n_C}{k n_D^2} \right), \tag{20}$$

$$P_{r\_out}(i\,|\,j) = \frac{n_C}{n_D} \frac{r+1}{2k-1} \left(\frac{1}{n_C} - \frac{n_D - n_C}{k {n_D}^2} \right) + \delta_{ij} \left(1 - \frac{n_C}{n_D} \frac{r+1}{2k-1} \right). \tag{21}$$

For simplicity, we introduce the following notation:

$$a(r) = P_{r\_out}(i|j),\ i \neq j,\ \ b(r) = P_{r\_out}(i|i). \tag{22}$$

Then the conditional entropy is

$$H_r(L_{out}|L_C) = -(n_C - 1)a(r) \log_2 a(r) - b(r) \log_2 b(r). \tag{23}$$

Covert channel capacity in a case of counteracting is

$$v = \left(1 - \frac{1}{k}\right) \max_{F, L_C} \left\{ \beta \frac{F-1}{F} \frac{-n_C \left(\frac{1}{n_C} - \frac{n_D - n_C}{k n_D^2} \right) \log_2 \left(\frac{1}{n_C} - \frac{n_D - n_C}{k n_D^2} \right) - \frac{\sum_{r=0}^{F-2} H_r(L_{out}|L_C)}{F-1}}{\frac{\left(k - \frac{n_C}{n_D} + \left(\frac{n_C}{n_D}\right)^2\right)\left(l_{fix} + \frac{n_C - 1}{2}\right)}{k}} + \beta T \right\}. \tag{24}$$

Further, we used numerous calculation to find the optimal values of the covert channel parameters n, F and covert channel capacity for a different values of counteraction tool parameter k.

Figure 3 shows the dependence of the residual covert channel capacity from the covert channel parameters n and F for $k = 3$ and uniform distribution in covert channel and in dummy traffic.

Figure 4 depicts the dependence between the residual covert channel capacity and counteraction tool parameter k for optimal covert channel parameters.

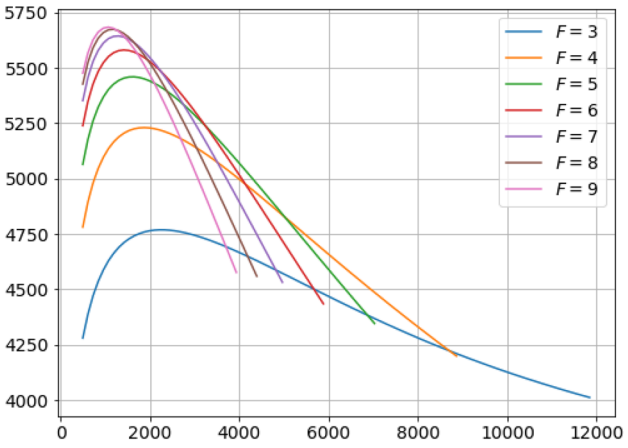

Fig. 3 The dependence between residual covert channel capacity and covert channel parameters n and F for $k = 3$

4.3 Some other distributions

We used numerous calculations to obtain optimal covert channel parameters and residual covert channel capacity for $k = \{3; 10\}$ for uniform distribution of dummy packets lengths and different distribution of packets lengths in covert channel (Table 1).

The main conclusion of calculations is that the most reasonable distribution is hyperbolic, if we fix the residual covert channel capacity. Otherwise, the fraction of dummy packets in the output traffic increases with the transition to a more decreasing distribution of dummy traffic.

4.4 Block traffic encryption

For the case of block encryption we make the same operations as for stream encryption. The only difference is for the

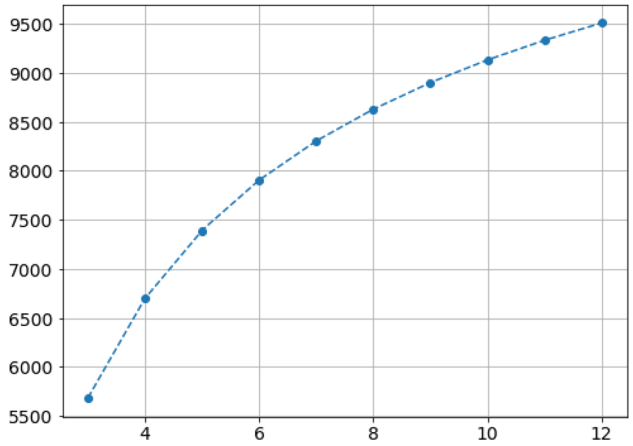

Fig. 4 The dependence between the residual covert channel capacity and counteraction tool parameter k

value of $E(L)$. The general form of covert channel capacity is evaluated with the same formula (10). If dummy traffic and covert channel have uniform distribution, we have the following formulas:

$$E(L_{out}) = \frac{\left(k - \frac{n_C}{n_D} + \left(\frac{n_C}{n_D}\right)^2\right)\left(l\left(\left\lceil \frac{l_{fix}+n_D}{l}\right\rceil + \frac{n_C-1}{2}\right)\right)}{k}, \tag{25}$$

$$v = \left(1 - \frac{1}{k}\right) \max_{F,L} \left\{ \beta \frac{F-1}{F} \frac{-\frac{\sum_{r=0}^{F-2} H_r(L_{out}|L_C)}{F-1}}{\frac{\left(k - \frac{n}{n_D} + \left(\frac{n_C}{n_D}\right)^2\right)\left(l_b\left(\left\lceil \frac{l_{fix}+n_D}{l_b}\right\rceil + \frac{n_C-1}{2}\right)\right)}{k} + \beta T} \right\}, \tag{26}$$

where l_b is block length.

We obtained all parameters for the case of block length equal to 64 bits.

Figure 5 shows the dependence between residual covert channel capacity and covert channel parameters n and F for $k = 3$ and uniform distribution in covert channel and dummy traffic for block encryption. Figure 6 demonstrates dependence between residual covert channel capacity and counteraction tool parameter k for optimal cover channel parameters and uniform distribution in covert channel and dummy traffic.

We used numerous calculations to obtain optimal covert channel parameters and residual covert channel capacity for $k = \{3; 10\}$ for uniform distribution of dummy packets lengths and different distribution of packets lengths in covert channel (Table 2).

5 Combined approach

In this approach, we send synchronization packets once for F packets. If we receive packet with a length not from covert channel alphabet, we identify it as special dummy packet and discard. Moreover, more likely after dummy packet normal packet should go. Let's consider conditional entropy (Fig. 7, all symbols are the same as in Fig. 2). If the special (green) packet is received, it's discarded and the counter in conditional entropy is reset. In other words, the partial synchronization occurs.

Let's consider the case when special packets divide the sequence of normal packets into $n = \{1, 2, ..., F-1\}$ continuous subsequences. If $n = 1$ original sequence isn't divided and large n doesn't occur in practice. Let $\overrightarrow{p}_{cond.entr.}(n)$ be probability distribution for conditional entropy $H_r(L^*_{out}|L_C)$, where L^*_{out} is truncated distribution. The conditional entropy is

$$H(L^*_{out}|L) = \sum_{n=1}^{F-1} C_{F-2}^{n-1} \left(\frac{\alpha}{2k+1}\right)^{n-1} \left(1 - \frac{\alpha}{2k+1}\right)^{F-1-n} < \overrightarrow{p}_{cond.entr.}(n), \overrightarrow{H}(L^*_{out}|L_C) >, \tag{27}$$

where $<,>$ is scalar product of vectors, $\overrightarrow{H}(L^*_{out}|L_C)$ is vector with components $(H_1(L^*_{out}|L_C), H_1(L^*_{out}|L_C), \ldots, H_{F-2}(L^*_{out}|L_C))$ and α is a fraction of special packets in dummy traffic.

We have to notice that when synchronization is done with only synchronization packets, F should be less then k/μ, but if we use the combined approach, F can exceed k/μ. In this

Table 1 Parameters for stream encryption and uniform distribution of dummy packets lengths

k	Distribution	Uniform	Parabolic	Linear	Hyperbolic	Exponential	Poisson
3	F	9	9	9	10	58	73
	IPv4						
	$v(bit/\sec.)$	5682,71	5586,16	5531,83	4255,00	1427,94	1064,66
	n	1063	1089	1102	829	11	6
	β'/β	0,7014					
	IPv6						
	$v(bit/\sec.)$	5661,85	5565,38	5511,12	4240,13	1425,05	1062,57
	n	1052	1077	1089	819	11	6
	β'/β	0,4244					
10	F	11	10	10	11	103	135
	IPv4						
	$v(bit/\sec.)$	9132,02	9023,90	8959,27	6747,27	1962,90	1457,26
	n	2901	3283	3353	2668	12	6
	β'/β	0,9136					
	IPv6						
	$v(bit/\sec.)$	9102,19	8994,11	8929,47	6747.27	1959,15	1454,52
	n	2871	3249	3318	2668	12	6
	β'/β	0,7684					

Table 2 Parameters for block encryption and uniform distribution of dummy packets lengths

k	Distribution	Uniform	Parabolic	Linear	Hyperbolic	Exponential	Poisson
3	F	5	5	5	5	9	11
	IPv4						
	$v(bit/\sec.)$	2428,16	2350,18	2302,90	1929,45	1104,06	862,87
	n	47	48	49	37	7	4
	β'/β	0,7022					
	IPv6						
	$v(bit/\sec.)$	2414,52	2336,58	2289,38	1919,01	1100,17	860,27
	n	46	47	48	37	7	4
	β'/β	0,4286					
10	F	6	5	5	5	15	17
	IPv4						
	$v(bit/\sec.)$	4546,37	4489,66	4451,69	3639,40	1695,90	1294,97
	n	140	185	185	185	8	5
	β'/β	0,9139					
	IPv6						
	$v(bit/\sec.)$	4527,69	4471,64	4433,27	3625,09	1691,53	1291,86
	n	139	182	182	182	8	5
	β'/β	0,7714					

Table 4 Parameters for block encryption and uniform distribution of dummy packets lengths

k	Distribution	Uniform	Parabolic	Linear	Hyperbolic	Exponential	Poisson
3	F	7	6	6	7	90	90
	IPv4						
	$v(/)$	2514,17	2428,17	2378,24	2001,37	1960,21	1665,12
	n	41	45	46	33	6	6
	β'/β	0,7022					
	IPv6						
	$v(/)$	2499,53	2413,92	2364,08	1990,13	1961,74	1667,12
	n	40	45	45	32	6	6
	β'/β	0,4286					
10	F	7	6	5	5	20	25
	IPv4						
	$v(/)$	4563,35	4492,73	4451,95	3639,67	1724,01	1317,53
	n	116	149	185	185	8	5
	β'/β	0,9139					
	IPv6						
	$v(/)$	4543,39	4473,38	4433,53	3625,36	1719,51	1314,31
	n	114	148	182	182	8	5
	β'/β	0,7714					

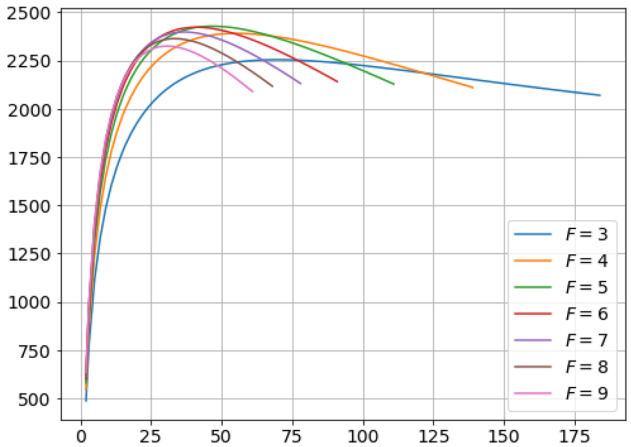

Fig. 5 The dependence between residual covert channel capacity and n for $k = 3$

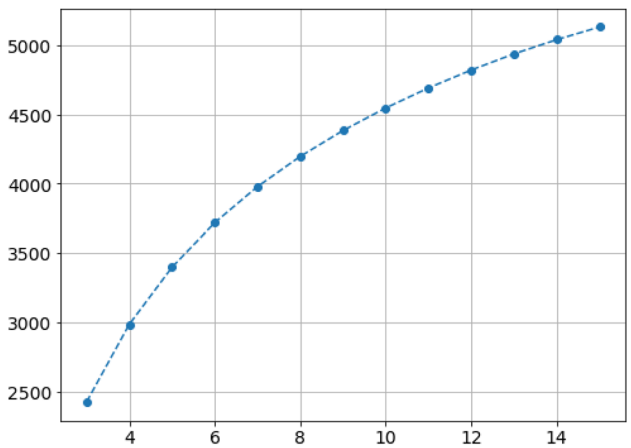

Fig. 6 The dependence between residual covert channel capacity and counteraction tool parameter k

case the probability of receiving at least one dummy packet between synchronization and r packets sending can be equal to one. Therefore, it is reasonable to decrease a number of synchronization packets, that is to increase F.

We used numerous calculations to obtain covert channel capacity $k = \{3; 10\}$ for different distributions of packets lengths in covert channel for IPv4 and IPv6 with stream encryption, distribution of packet lengths in dummy traffic was uniform (Table 3). The case of block encryption is illustrated in Table 4.

When dummy traffic is uniformly distributed, a violator haven't to shift an alphabet, but in case of nonuniform distributions of dummy traffic it is reasonable to shift a covert channel alphabet form l_{fix} to $l_{fix} + s$, where the shift is s, $s \in \{0,1,\ldots,n_{DT}\text{-}n_{CC}\}$.

6 Conclusion

In this paper we presented a method to limit cover channels using dummy traffic. Parameters of covert channel and counteraction tool for stream and block traffic encryption were evaluated. Different distributions for packets lengths in covert channel and dummy traffic were examined. Finally,

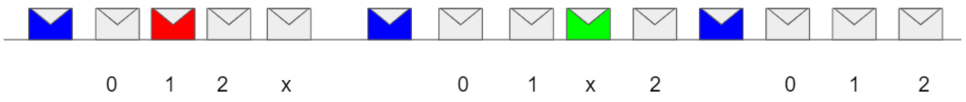

Fig. 7 Conditional entropy in combined approach

Table 3 Parameters for stream encryption and uniform distribution of dummy packets lengths

k	Distribution	Uniform	Parabolic	Linear	Hyperbolic
3	F	45	44	26	68
	IPv4				
	$\nu(/)$	5595,00	5874,58	5808,03	4399,29
	n	789	807	892	522
	β'/β	0,7014			
	IPv6				
	$\nu(/)$	5972,23	5851,97	5785,75	4383,35
	n	778	796	881	523
	β'/β	0,4244			
10	F	13	12	12	13
	IPv4				
	$\nu(/)$	9241,10	9117,69	9043,74	6673,03
	n	2744	2993	3033	1987
	β'/β	0,9136			
	IPv6				
	$\nu(/)$	9210,67	9087,21	9013,22	6651,34
	n	2715	2961	3000	1964
	β'/β	0,7684			

we gave recommendation to choose a required parameters for counteraction tool.

Further investigation can be concerned with combination of counteraction tools, for example, full traffic normalization for storage covert channel with full traffic normalization for timing covert channel and full traffic normalization for storage covert channel with random packets delay.

Acknowledgements This work was supported by the Ministry of Science and Higher Education of the Russian Federation (state assignment project No. 0723-2020-0036).

Funding Ministry of Science and Higher Education of the Russian Federation, 0723-2020-0036, Anna Epishkina.

References

1. Schaefer, M., Gold, B., Linde, R., Scheid, J.: Program confinement in KVM/370. In: Proceedings of the 1977 ACM Annual Conference, pp. 404–410 (1977)
2. Latham, D.C.: Department of defense trusted computer system evaluation criteria, Department of defense 5200.28-STD, p, 116 (1985)
3. Huskamp, J.C.: Covert communication channels in timesharing systems: PhD Thesis., Berkeley: Engineering University of California, p. 606 (1978)
4. Tsai, C.-R., Gligor, V.D., Chandersekaranm, C.S.: A formal method for the identification of covert storage channels in source code. IEEE Trans. Softw. Eng. **16**(6), 74–87 (1990)
5. Moskowitz, I.S., Kang, M.H.: Covert channels—here to stay? In: Proceedings of the 9th annual conference on computer assurance, pp. 235–244 (1994)
6. Epishkina, A., Frolova, D., Kogos, K.: A technique to limit hybrid covert channel capacity via random increasing of packets' lengths. Procedia Comput. Sci. **190**, 231–240 (2020)
7. Luo, X., Chan, E., Zhou, P., Rocky, K.: Robust network covert communications based on TCP and enumerative combinatorics. IEEE Trans. Dependable Secure Comput. **9**(6), 890–902 (2012)

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH (“Springer Nature”).
Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users (“Users”), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use (“Terms”). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.
These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.
We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.
While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.
These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.
To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.
Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.
If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com