Protection of information presented as pseudo-probabilistic display in the information exchange channels of UMV

D V Moiseev, E N Mashenko, V V Nikishin and L I Lukina
Sevastopol state university, 33 Universitetskaya str., Sevastopol, Russia, 299053

E-mail: dmitriymoiseev@mail.ru

Abstract. The work considers the fundamental possibility of using a pseudo-probabilistic form of information representation for its protection when transmitting over open communication channels. Data transmission is becoming one of the priorities for ensuring sustainable, continuous, operational and stealthy management of unmanned vehicles. This is due to the wide use of automation, digital information, integration of various systems and means of control, management, etc. Data traffic with a large number of video images increases in an avalanche, and it is necessary to transmit information with guaranteed delivery and minimal delays.

1. Introduction
It is known that today Ethernet is the most frequently used technology for the formation of LAN, both for civil and special purposes, including military. The development of this technology and the component base for its implementation goes in two directions: increasing the speed of data transfer and developing solutions for complex operating conditions [1].

At the moment, there is an urgent issue of protecting information transmitted over open communication lines and especially over Ethernet networks. Data transmission is becoming one of the priorities for ensuring sustainable, continuous, operational and stealthy management of unmanned vehicles (UMV).

Existing devices for information security inside computer networks are based on the principles of deterministic cipher systems, or deterministic cipher, such as GOST 28147-89. The block diagram of "channel" network encoders is also known [2]. This network encoder scheme includes: an ethernet module and an encoder (cipher processor). The microprocessor consists of a control unit, a computer, and a data input / output buffer [2]. During reception, information is sent to the device on the ethernet module, which unpacks the IP packet, and the packet data block is sent to the cipher processor, which, in turn, decrypts the data block using deterministic ciphers. The decryption algorithm is embedded in the computer, and the information is transmitted in reverse order.

2. Building a vulnerability detection model
It is known that the representation of a discrete signal in a probabilistic form allows to obtain a number of advantages - reducing the hardware volume and increasing the processing speed [3 – 5].

In general terms, the essence of a stochastic or probabilistic transformation is that any probability of the converted quantity can be associated with a certain probability. The conversion process itself is performed in accordance with the rule [4]:
\( y_y = \begin{cases} 
1 & \text{at } x_i > R(t_y) \\
0 & \text{at } x_i \leq R(t_y) 
\end{cases} \), \hspace{1cm} (1)

where \( x_i \) – value of the converted signal \( X(t) \);

\( R(t_y) \) – \( j \)-th value of the auxiliary random signal \( R(t) \) changing in the measurement interval, \( i = 1, N \) – number of signal conversion cycles \( X(t) \);

\( j = 1, K \) – the number of statistical tests for each \( x_i \) value within the time interval \( \Delta t = t_{i+1} - t_i \);

\( y_{ij} \) – value of the probabilistic display of the signal \( x_i \) from the series: \( Y(t) = \{y_{i1}, y_{i2}, \ldots, y_{ij}, \ldots, y_{iK}\} \).

It should be noted that the probabilistic information display has several advantages, one of which is strength and also the fundamental possibility of a probabilistic linear transformation with a variable number of independent statistical tests, each value of the original signal, represented either in analog or digital form that allows parallel signal processing to carry out his cryptographic protection.

Let’s define the mathematical expectation (ME) of the probabilistic display of information:

\[
M[Y(t)] = P(y_y = 1) = P[R(t) < x_i = r] = F_{x_i}(R) .
\]

Thus, the probability of «1» appearing in the probabilistic display is ME from the mapping and is numerically equal to the value of the integral distribution law [4] of the auxiliary random signal \( R(t_y) \) under the condition of comparison \( x_i \).

Of particular interest is the case when the auxiliary random signal \( R(t_y) \) obeys a uniform distribution law [3] in accordance with the rule:

\[
y_y = \begin{cases} 
0 & \text{at } x_i < 0 \\
0 & \leq x_i \leq 1 \\
1 & \text{at } x_i > 1
\end{cases} \hspace{1cm} (3)
\]

In this case, the last expression for ME (2) takes the form:

\[
M[Y(t)] = P(y_y = 1) = x_i ,
\]

in other words we have the case of linear probabilistic transformation.

The most important consequence of the expressions for ME is the fact that the value of \( x_i \) is recoverable from the probabilistic mapping, that is, it is possible to reverse the conversion of the "probability – value of the signal" (number, amplitude, frequency, phase, etc.). Indeed, a priori knowing the law of distribution of the auxiliary random signal \( R(t_y) \) and defining the ME of a probabilistic mapping, that is, the ordinate of the integral \( F_{x_i}(R) \) by functional transformation, we can determine the value of \( x_i^* \), which is an estimate \( x_i \) [3]. As such an assessment that meets the requirements of non-bias, consistency and efficiency, in accordance with Chebyshev’s theorem, it is accepted:

\[
x_i^* = (M[Y(t)]) = \frac{1}{K} \sum_{j=1}^{K} y_{ij} .
\]

(5)
Since for non-positional representation of information in the form of a probabilistic display, the main one is the probabilistic nature of the formation of a sequence of "1" and "0" and the probabilistic nature of the number of "1" in the sequence, this leads to an additional error in the probabilistic transformation.

This leads to the conclusion that in order to reduce, and in the boundary case eliminate, the error of the probabilistic transformation, we should abandon the second characteristic feature of the probabilistic mapping, which for this case we will call «pseudo-probabilistic» [6 – 8]. This can be achieved by changing the algorithm for generating the probability map (1), setting the number of "1" in the probability map in advance according to the expression:

$$P(y_{ij} = 1) = x_i.$$  \hspace{1cm} (6)

However, to preserve the properties of the probabilistic map, the distribution of units in the pseudo-probabilistic map must remain uniform.

Each probability map has the properties of synchronicity and independence of each member of the map from any other. Using these properties and applying probabilistically represented discrete signals makes it possible to simplify functional nodes for performing arithmetic and logical operations, and thus dramatically reduce their hardware volume by hundreds of times.

The most important conclusion from the analysis of the probability transformation is that the value of the original parameter $x_i$ can be restored from its probabilistic mapping $Y_i(t)$, what makes it possible to reverse the conversion of the probability–value parameter by evaluating it to meet the requirements of non-bias, consistency, and efficiency.

In this case, for a single-line unipolar non-positional representation of information in the form of a pseudo-probabilistic mapping, the value of the converted value is either always positive or always negative, and the pseudo-probabilistic mapping itself will have the form:

$$Y_i(t) = \{ y_{i1}; y_{i2}; \ldots y_{ig}; \ldots y_{iG} \},$$  \hspace{1cm} (7)

where $g = \overline{I,G}$ – the number of the digit in the probabilistic display, moreover $G=2^L-1$, where $L$ – the number of digits required for the positional representation of the converted value $X_i$.

Note that $L$ must be selected based on the maximum value of the converted parameter $X_{\text{max}} = L \geq \left[ \log_2 (X_{\text{max}}) \right]$, where $X_{\text{max}} = \text{MAX} \{ X_i \}$.

In order for the number of “units” in the pseudo-probabilistic mapping to be strictly equal to the weight of the converted value $X_i$, it is necessary that the probability of the appearance of one “unit” in the pseudo-probabilistic mapping $Y_i(t)$ be equal to:

$$P(y_{ij} = 1) = P_i(Z = Z_t) = \frac{x_i}{2^L - 1}. \hspace{1cm} (8)$$

To take advantage of the presentation of information in the form of probabilistic mappings, it is necessary that the distribution of “units” in the pseudo-probabilistic mapping $Y_i(t)$ be independent, uniform and stochastic.

Since the values of the auxiliary random function $R(t)$ are formed at discrete moments of time, the function in them can only be in one of its states $r_{ig}$ with probability $P_{ig}(t)$ as a consequence, for any $t$ has the form in accordance with (3):

$$\sum_{g=1}^{G} P_{ig}(t) = 1, \hspace{1cm} (9)$$
since the resolving input of the full binary decoder from the output of the comparison scheme will receive exactly $X_i$.

The diagram of the converter of digital information to non-positional pseudo-probabilistic mapping is shown in the figure 1 [10].

![Figure 1. Block diagram of a digital information converter to a non-positional pseudo-probabilistic mapping.](image)

The structure of this scheme consists of:
DC – decoder.
Counter.
DCS – digital comparison scheme for "equality".
The result register.
GEDRS – generator of evenly distributed random sequences.

Thus, the equality of each term of the pseudo-probabilistic mapping to one, as in the classical case of the probability transformation, is directly proportional to the converted value. The transformation time $t_{tr}$ is also proportional to $x_i$, that is

$$t_{tr} = \frac{x_i}{f_{cf}},$$

where $f_{cf}$ – clock frequency of the probabilistic processor.

From the expression (10) it follows that the faster the device is, the higher its clock frequency and the less the greater the number of "1" must be entered in the register. With the same clock frequency of the probabilistic processor and the maximum value $x_i$ of the comparable error of the probabilistic transformation, it is possible to achieve a speed of 700 times more [10 – 12].

Based on this, when performing the reverse transformation, the error of the probability transformation is minimized, and the speed increases significantly, since the number of tests required to form a probability map is equal to the weight of a binary number, and does not exceed it many times, as in the cases of linear and nonlinear probability transformation of information.

The technical and economic efficiency of the proposed converter of binary positional code to probabilistic representation consists in the use of an accelerated algorithm for forming a probabilistic display, which eliminates the conversion error and significantly increases the performance.

Thus, we can conclude that the previously considered algorithms for converting any signal to a probabilistic map have a common drawback – the inverse relationship between the conversion accuracy and performance.
Using the algorithm for converting the signal to a pseudo-probabilistic mapping allows to increase the speed of the probability processor by approximately three orders of magnitude at a given accuracy, while preserving the reliability and hardware volume indicators.

Thus, to protect information from unauthorized access, a linear unipolar probabilistic transformation of the source information presented either in analog or digital form should be performed, so that the attacker is not allowed to perform statistical tests of each converted value of the source information. Arithmetic and logical operations can be performed on the converted signal, as well as receiving and transmitting via telecommunications. For reverse transformation to a digital code or analog signal, according to the expression for \( ME \), it is necessary to determine the ME estimate of probabilistic mapping \( X^*(t) \) and by functional transformation go to the desired value \( X(t) \).

The information subject to cryptographic protection is received at the input of the transmitter, inside which it is converted into a probabilistic display, which in this case represents the encoded signal, and is transmitted through the communication channel to the receiver, inside of which the decryption is performed.

Interception of the probabilistic display in the communication channel and iteration of all possible values of \( i \) with the appropriate analysis allows you to decrypt the message in a finite time only if the law of distribution of the auxiliary random signal \( R(t_i) \) is known. If the distribution law of the auxiliary random signal \( R(t_i) \) is unknown, the cryptanalysis problem becomes practically impossible to solve.

3. Conclusion
Using the probabilistic form of information representation allows you to take advantage of not only the known advantages: a relatively small hardware volume, the ability to function in real time, increased noise immunity, but also an additional advantage expressed in the form of cryptographic protection of data represented by a probabilistic display.

These advantages can improve the reliability and efficiency of storage, processing and data transfer in control systems of UMV.

Acknowledgments
This work was supported by the Russian Foundation for Basic Research (projects № 19-29-06023/19).

References
[1] Prokofieva L P, Lurie M N and Shcherbakov V V 2010 Fiber-optic communication in military equipment, Photon-Express 2 24-6
[2] Panasenko S P and Rakitin V V 2002 Hardware encoder, PC world 8 77-83
[3] Moiseev D 2019 Methodology of Probabilistic Representation and Transformation of Information, International Multi-Conference on Industrial Engineering and Modern Technologies FarEastCon 19229264 DOI: 10.1109/fareastcon.2019.8934304
[4] Moiseev D V, Sapoznikov NE and Chuzikova-Proskurnina O D 2016 Application of the probabilistic form of data representation in correlation-extreme systems, Environmental monitoring systems 5 47-52
[5] Sapoznikov N E and Moiseev D V 2015 Performing arithmetic operations of addition and multiplication on probabilistically presented parallel data, Multi-core processors, parallel programming, PLD, signal processing systems 5 46-54
[6] Sapozhnikov N E, Moiseev D V and Shokin A G 2012 New methods of noise-resistant coding of information, East European Journal of Advanced Technology. 6/9 26-9
[7] Sapoznikov N E, Moiseev D V and Chuzikova-Proskurnina O D 2016 Comparison of various forms of not position probabilistic display of information, Environmental monitoring systems, 4 66-73
[8] Sapozhnikov N, Polyakov A and Moiseev D 2019 Advantages of Using the Probabilistic Form of Information Representation in Information-Control Systems, *2019 International Science and Technology Conference "EastConf"* 2 1-6 DOI: 10.1109/EastConf.2019.8725406

[9] Sapozhnikov N, Bryukhovetskiy A, Polyakov A and Moiseev D 2018 Modeling performing calculations over the data presented in a probabilistic form, *MATEC Web of Conferences* 224 32-39 DOI: 10.1051/matecconf/201822404019

[10] Moiseev D V 2020 Intelligent decision - making support on the level of encryption of information transmitted in the UMV information exchange channels, *International Scientific Conference "Advanced Technologies in Aerospace, Mechanical and Automation Engineering"* 734 012086 DOI: 10.1088/1757-899X/734/1/012086

[11] Sapozhnikov N E, Moiseev D V and Beyner P S 2013 Evaluation of accuracy and speed with a probabilistic form of presentation of information, *News of NTU KhPI* 38 34-9

[12] Moiseev D, Polyakov A and Parfentsev M 2019 Hardware-Software Complex for Modeling and Reliability Analysis of Systems for Various Purposes, *2019 International Multi-Conference on Industrial Engineering and Modern Technologies* 19229264 DOI: 10.1109/FarEastCon.2019.8933931