A Method of Securing Data Transferred Between Unmanned Aircraft System and Ground Control Station Based on One-Time Pads

Ivan Avdonin, Marina Budko, Mikhail Budko, Vladimir Grozov, Alexei Guirik
ITMO University
Saint Petersburg, Russian Federation
avdoninivan@mail.ru, {mbbudko, mbudko}@corp.ifmo.ru, alexei.guirik@gmail.com, vladimirgrozov@mail.ru

***Abstract*—The paper provides a method of secure data transmitted and received data onboard the unmanned aircraft vehicle. An encryption method based on one-time pads (the Vernam cipher) is presented. The method uses such advantages of the Vernam cipher as theoretically proven absolute cryptographic security, high encryption speed and implementation simplicity. It allows the memory allocated for one-time pad to be used not only as a storage for key sequences but also as a place for storing the encrypted data.**

I. Introduction

Among advanced researches in the field of intelligent control systems it is necessary to point out the development of mobile robotic systems, in particular, unmanned aerial vehicles (UAV). UAV creation and use excite a strong interest all over the world. One of the most actual problems is the security of data transmission both between UAV devices, units and modules, and between UAV and Ground Control Station (GCS).

The reliable and safe information interaction between the UAV and GCS is necessary for successful execution of flight missions.

Transmitted information includes control commands, telemetry and payload data.

Information interaction between UAV and control console are usually provided by wireless communication link, including Wi-Fi and Internet that requires special actions for information security improvement. It is known that standard security facilities have some vulnerabilities therefore the development of additional security measures is necessary for a safer information transfer.

The various questions related to UAVs development and operation as well as secure data transfer, are considered, for example, in works [1–8].

Security of control commands and telemetry information against unauthorized access is considered in the paper. It is an actual problem because data interception or distortion can result in loss of control and even UAV itself.

To protect UAV links various security services (confidentiality, authentication and integrity) must be used. Presented work is devoted to encryption i.e. the security mechanism that provides for data confidentiality.

Encryption is a powerful method of data securing. However cryptanalysis potential and computers capacity are growing fast and force to look for new encryption ways or to improve already known ones [9]. UAV specific features such as small payload capacity, limited computational resources and potentially high degree of threats also restrict a choice of cryptographic security solutions. Consequently the main criteria of a suitable cryptographic algorithm are their high cryptographic security and encryption speed, as well as simplicity of implementation.

There is a cipher which in many respects satisfies these requirements – the Vernam cipher (one-time pad, OTP). Cryptographic security of this algorithm has been theoretically proven [10], [11]. Recently plenty of works using the idea of OTP both for theoretical researches and for applied problems has been published [7], [12–16].

The work presents a cryptographic protection method of control commands and telemetry data during the transfer between UAV and GCS based on the OTP (the Vernam cipher) – the perfect cipher.

The task of the present work is to outline a possible implementation of OTP encryption technique onboard the UAV to increase transferred data security.

II. Data Encryption Technique

Specific features of data transmission between UAV and GCS require encryption algorithms have high execution speed and provide for improved security, simplicity of implementation and use. On the other hand, limited computing capacity and memory must be considered.

Fast growth of computing power and evolution of cryptanalytic methods can make classical encryption systems inefficient. Almost all cryptosystems have conditional security

because they can be broken under sufficient time and computing power. They are potentially breakable in the future, for example, in case of quantum computer attacks.

Widespread crypto algorithms such as RSA, AES, GOST 28147-89 with time can become less secure. Rising computing power of potential attackers makes the application of alternative encryption systems or combining ciphers of different types more important.

Hence, systems with perfect secrecy are of great interest [10], [17]. As it was shown by Shannon [10], a cipher is considered perfectly secure if the cipher text does not give any information about the corresponding plaintext (except, probably, its length).

One of the best known perfectly secure ciphers is the one-time pad. We shall consider the OTP system which has proved perfect secrecy and high speed of encryption/decryption.

OTP consists of key sequences (pages) set of random data. Three conditions must be met:

- key sequences are truly random,
- the same page cannot be used twice,
- the plaintext should have the same length as the key.

Under such conditions OTP is a perfectly secure cipher. Encryption procedure consists of a plaintext and a secret gamma (key) superposition by means of XOR (exclusive OR) operation.

One-time pad is a symmetric stream synchronous cipher. It has a very simple algorithm and theoretically proven absolute security. Other important property of one-time pad is a high encryption speed because the pad generation and encryption are separate in time, and the elementary operation XOR has hardware support in most of processors. OTP usage does not lead to additional processor load. It is especially important for systems with limited computing resources, as well as for large data arrays (for example, video streams).

OTP technique seems to be the most suitable and promising for UAV data securing against unauthorized access.

III. One-time pad

The one-time pad holds a special place in the family of symmetric encryption algorithms. It was invented by Gilbert Vernam in 1917 for cable messages enciphering.

The essence of the method consists in the following. Plain text $M=(m_1, \ldots, m_N)$ is transformed with secret gamma (key) $K=(k_1, \ldots, k_N)$ into cipher text $C=(c_1, \ldots, c_N)$ by means of XOR operation:

$$C = M \oplus K = (m_1 \oplus k_1, \ldots, m_N \oplus k_N).$$

Decryption is carried out similarly.

It means that the cipher text and the plain text are independent in this system and that OTP has absolute security: as all plain texts are equiprobable, it is impossible to define what plain text is correct. The random key sequence imposed on non-random plain text gives truly random cipher text.

OTP has the perfect secrecy property only under serious requirements to its implementation [10], [11]:

1) A key sequence (a page of the cipher pad) should be a truly random sequence.
2) A key length should not be less than the length of a plain text.
3) Each key should be used only once.
4) Used cipher pad page should be destroyed after the ciphered message is transferred.

The OTP requirements cause the following disadvantages:

1) Significant time and resources for manufacturing, distribution, storage and destruction of keys.
2) Complexity of generating a truly random and long enough key.
3) Problem of reliable cipher pad transfer.
4) Sensitivity to system failures and the need of synchronization.

Nevertheless, there are various possibilities of OTP application when strong requirements are overcome due to:

1) Essentially new solutions.
2) Acceptable reduction of requirements in specific conditions.

There are theoretical works devoted to the Vernam cipher where some possibilities for such reduction are proved. For example, [12] shows that the one-time pad is robust to small deviations from randomness under some conditions.

It is quite expected that essentially new approaches to OTP implementation will appear. For example, combining this encryption technique and neurocryptography [18], [19]. Other possible direction is the usage of keys that have non-numerical nature [20], [21].

For practical implementation of OTP system it is necessary to consider following aspects:

- cipher pad generation,
- its transfer to the message receiver,
- enciphering/decoding itself,
- common organization of crypto security.

IV. Data securing based on one-time pads

UAV data securing requires correct one-time pad application and economical use of onboard computer memory.

Earlier the important requirements at which OTP is absolutely unbreakable have been depicted: the key sequence (cipher pad page) needs to be a truly random sequence which length is not less than the length of a plain text; the key should be used only once and the used page of cipher pad should be destroyed after that. Consider the implementation of the listed requirements.

Especially important and resource-consuming part of Vernam algorithm implementation is one-time pad generation. For the correct work of this encryption algorithm OTP should be a truly random bit sequence. In practice, however, it is very

difficult to generate required random sequence. There are different approaches based on: cryptographic algorithms such as resistant block ciphers (for example, the generator from standard ANSI X9.17); computationally difficult mathematical problems (algorithm BBS, Blum – Blum – Shub [22]); special implementations (/dev/random in Linux) [11], [23]; physical random-noise generator [11]. The necessary degree of randomness depends on the problem being solved.

Using Linux /dev/random it is possible to get access to the system random number generator of Linux kernel which generates random bits. The source of these random values is, for example, the noise of device drivers. The bits corresponding to this noise are accumulated in "chaotic" pool. However, if the pool is empty, the program will wait for the next random bit. Such delays make creating the required long sequences problematic.

Blum–Blum–Shub algorithm which is based on the factorization problem has high cryptographic security for big numbers. However, it has low speed.

Production of a true random bit sequence is not the subject of this work. For experimental researches we use the approach of the widespread standard ANSI X9.17 that uses Triple DES algorithm [11]. The block cipher Triple DES is replaced with the cipher GOST 28147-89 in the Cipher Feedback Mode [24] for one-time pad generation.

Russian Federal standard GOST 28147-89 in the Cipher Feedback Mode is chosen instead of the block cipher Triple DES. The cipher GOST 28147-89 is based on Feistel network. It is known that cipher based on Feistel network produces a strong pseudo-random sequence after four encryption rounds [25]. The GOST algorithm uses 32 rounds and provides a strong pseudo-random sequence. A set of such sequences forms one-time pad pages.

The scheme of one-time pad generation is presented in Fig. 1.

The main part of the process represented on the scheme is generation of cipher gamma block. The cipher has a block size of 64 bits and a key length of 256 bits. Block cipher key must fulfill special requirements. The key must be a set of statistically independent bits in which values 0 and 1 are equiprobable. In this work such key is obtained by means of /dev/random included in Linux kernel.

For such random key generation we use /dev/random device of Linux kernel. In this case random bit sequences are the result of environmental noise collected from device drivers.

Cipher gamma is formed from blocks R_i which length is 64 bits. During each i step of formation of such blocks the algorithm GOST 28147-89 works three times.

For each phase of the algorithm GOST 28147-89 implementation it is necessary to define the initial values of two variables (so-called initialization vector). This vector is formed in special way for each phase. For the first phase these values can be defined as date and time at the beginning of i step of generation (it is named as DT_i on the scheme). Initialization vectors for the second and the thid phases are formed by means XOR operation. Before the second phase the initialization vector is formed as a result of application of XOR operation to the output gamma of the first phase of i step and the output gamma of the third phase of $(i-1)$ step. For the third phase the initialization vector is the result of application of XOR operation to the output gamma of the first phase of i step and the output gamma of the second phase of current, i step. The result of the whole i step is R_i – the next pseudorandom number created after the second phase of the cipher GOST 28147-89 execution. All the blocks R_i are source material for the one-time pad pages formation by means of array of blocks transform into array of pages of needed size.

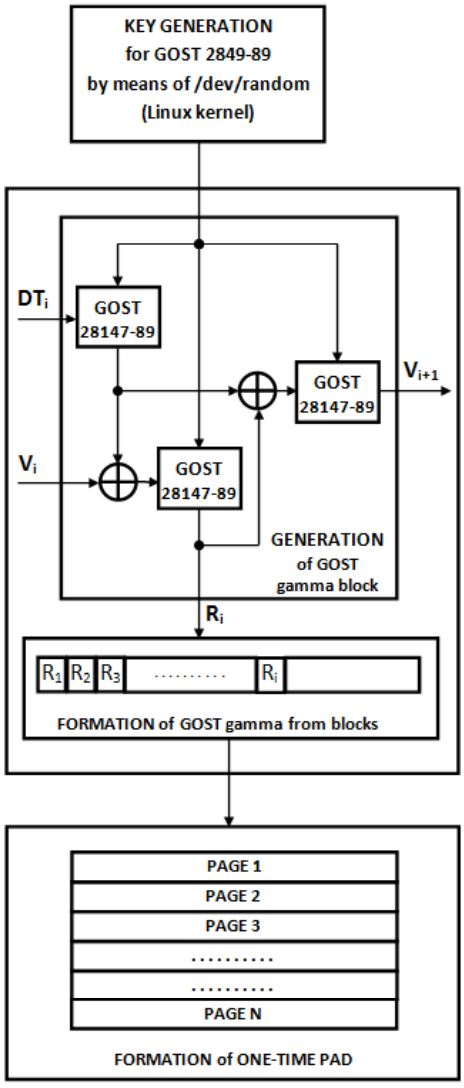

Fig. 1. One-time pad generation. DT_i – current date and value for the beginning of i generation step. V_i – initial value for i generation step. R_i – pseudorandom number, created on i generation step

A page size is determined by the size of transmitted data. The quantity of required pages depends on UAV onboard equipment, mission tasks and flight duration time. OTP is formed before the UAV mission on one of the terminals.

One of the problems of OTP implementation is synchronization of the cipher pad pages for encryption/decryption on terminating devices. It requires transferring of every page number along with the message.

After that OTP encryption is carried out. Arrays containing a plain text and the cipher pad are used as inputs. XOR operation is applied to each bit of this arrays elements. Decryption process includes following steps: extraction of the package number and the number of the used page; checking the integrity. In case of successful check XOR operation is applied to the cipher text and as a result the decrypted text is obtained.

OTP application is correct when every page of the OTP is used only once. For this purpose we offer to combine data encryption/decryption with the present page replacement by the encryption result (Fig. 2).

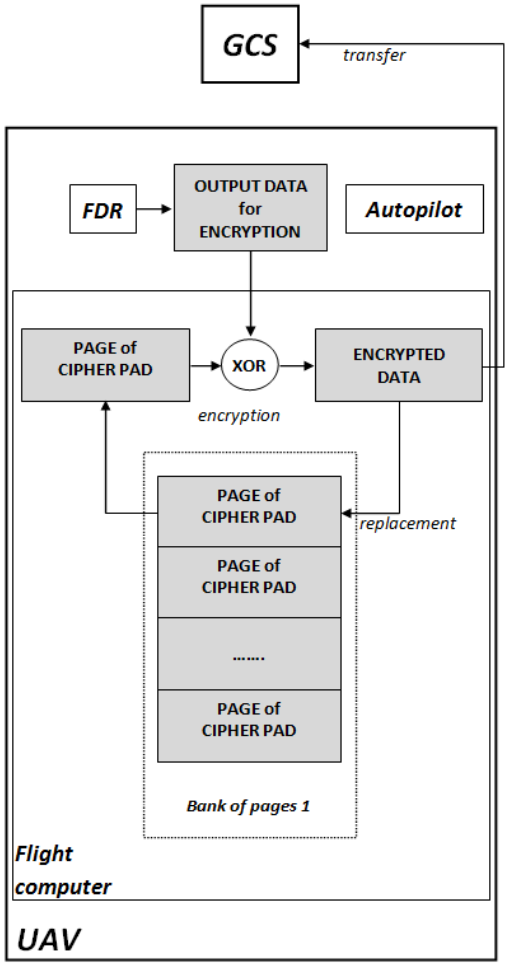

Fig. 2. Encryption. A variant with page replacement by the cipher text

This occurs as follows. Telemetry data are collected by objective control sensors in the time moment *i*. The obtained data are encrypted by means of XOR operation which is executed on the data set *i* and the cipher gamma of the page *i*. The resulting ciphertext is written over the used page, and after that it is sent to the ground control station. This approach provides that every page is disposable.

At the same time the second problem is also solved: the size of necessary storage is reduced that is essential for an onboard computer that has limited computing resources (especially in the case of small UAV).

The feature of the offered securing method is the necessity to use two different one-time pads: one for output, encrypted data (telemetry data and video data received from flight data recorder (FDR)) and another for input, decrypted data (executive instructions transmitted from GCS to UAV).

The used page is cleared, or, if necessary, is replaced with the received encrypted data (Fig. 3).

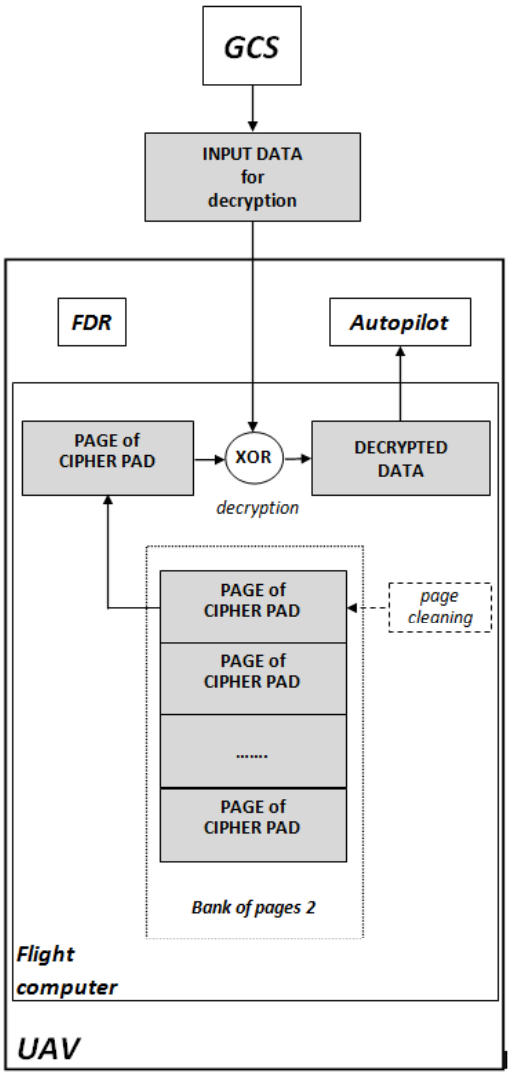

Fig. 3. Decryption. A version with a page clearing

External (command) data set with the number *i* comes on UAV board. The data set is decrypted by using the cipher gamma of the page *i* by means the XOR operation. Then the decrypted data are transmitted to the UAV autopilot for their execution. Cleaning of the used cipherpad page (number *i*) is provided by the record any values (for example, zeros) over the used cipher gamma.

Replacing the used pages with cyphered data allows excluding their simultaneous existence in the onboard computer memory. As a result, the decryption of messages will be impossible if the UAV is intercepted.

The offered method, moreover, provides the way to transform the used pages into a cipher text database. It allows gathering (immediately on the UAV) the information about its condition and course of flight for further detailed processing after landing. Besides, this approach gives the possibility to save data in the case of connection loss with GCS.

Thus, the every cycle of OTP page usage includes:

- encryption/decryption of the next data set,
- deletion of the used page.

Both these operations are performed at the same time.

V. Conclusion

The work deals with a method of securing of transmitted and received data onboard the unmanned aircraft vehicle. The method is based on one-time pad encryption. It uses such advantages of one-time pad as theoretically proven perfect security, high encryption speed and implementation simplicity. It allows usage of the memory allocated for one-time pad not only for the key sequences storage but also for accumulation of the encrypted data. Such replacement of one-time pad pages also solves a problem of used pages destruction and saves memory.

The proposed method allows raising data protection level without additional expenses on significant computational capability and high-capacity memory. Further researches will be focused on: improvement of one-time pad degree of randomness (used pseudo-random sequence must be truly random); solving of data integrity and availability problems; implementation of the method within the limits of the University ITMO project of multirotor UAV; its integration in MAVLink protocol (Micro Air Vehicle Link), commonly used for micro UAVs communication.

Acknowledgment

This work was supported by Russian Science Foundation grant 16-11-00049.

References

[1] Moiseev V.S., *Foundation of the Theory of UAV effective application*. Kazan: Ed. Center "Shkola", 2015.

[2] R. Austin, *Unmanned aircraft systems: UAVS design, development and deployment*. John Wiley & Sons, 2010. A. Talalaev, V. Fralenko, V. Khachumov, "Review of standards and the conceptual design of tools for spacecraft monitoring, control and diagnostics", *Program systems: theory and applications*, vol. 6, no. 26, 2015, pp. 21-43.

[3] K. Mansfield, T. Eveleigh, T.H. Holzer, "Unmanned Aerial Vehicle Smart Device Ground Control Station Cyber Security Threat Model", *in Proc. 13th IEEE Int. Conf. on Technologies for Homeland Security (HST)*, Nov. 2013, pp. 722-728.

[4] K. Hartmann, C. Steup, "The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessmen", *in Proc. 5th Int. Conf. on Cyber Conflict*, Jun. 2013, 24 p.

[5] T. Tanzi, L. Apvrille, J.-L. Dugelay, Y. Roudier, "UAVs for humanitarian missions: Autonomy and reliability", *in Proc. IEEE Global Humanitarian Technology Conference*, Sept. 2014, pp. 271-278.

[6] T. Saarelainen, J. Jormakka, "Tools for future battlefield warriors", *in Proc. 8th European Conference on Information Warfare and Security IDCT10*, Jul. 2010, pp. 223-233.

[7] I.V. Makarov, "Organizing of informational and telemetry services for means of self diagnostics and monitoring of lifecycle of unmanned aerial vehicle based on unified control system", *Izvestiya SFedU. Engineering Sciences*, no. 3, 2014, pp. 21-43.

[8] S. Avdoshin, A. Savelieva, "Cryptanalysis: Yesterday, Today and Tomorrow", *Open System*s, no. 3. 2009, pp. 22-25.

[9] C.E. Shannon, "Communication theory of secrecy systems", *Bell Syst. Tech. J.*, vol. 28, 1949, pp. 656–715.

[10] B. Schneier, *Applied Cryptography, Protocols, Algorithms, and Source Code*. John Wiley & Sons, 1995.

[11] B. Ryabko, "The Vernam cipher is robust to small deviations from randomness", *Problems of Information Transmission*, vol. 51, no. 1, 2015, pp. 82-86.

[12] C. Matt, U. Maurer, "The one-time pad revisited", *in Proc. IEEE International Symposium on Information Theory (ISIT)*, Jul. 2013, pp. 2706-2710.

[13] S. Sampurna, "Unconditionally Secure and Authenticated One Time Pad Cryptosystem", *in Proc. Int. Conf. on Machine Intelligence and Research Advancement (ICMIRA)*, Dec. 2013, pp. 174-178.

[14] R. Du, Z. Sun, B. Wang, D. Long, "Quantum secret sharing of secure direct communication using one-time pad", *Int. J. of Theoretical Physics*, vol. 51, no. 9, 2012, pp. 2727-2736.

[15] Y. Guo, J. Xie, J. Li, M.H. Lee, "An arbitrated quantum signature scheme based on chaotic quantum encryption algorithm", *J. of Modern Physics*, no. 4, 2013, pp. 83-88.

[16] A.Yu. Zubov, *Perfect ciphers*. Moscow: Gelios ARV, 2003.

[17] N.I. Chervyakov, Implementation of artificial neural networks and system of residual classes in cryptography. Moscow: Fizmatlit, 2012.

[18] G. Huang, Ya. Zhou, "A multistage chaotic encryption model combined bp neural network", *in Proc. International Symposium on Computer Science & Technology*, 2007, pp. 33-36.

[19] M. Hirabayashi, H. Kojima, K. Oiwa, "Design of True Random One-Time Pads in DNA XOR Cryptosystem", *Series Proc. in Information and Communications Technology*, vol. 2, pp 174-183.

[20] Y. Chang, C. Xu, S. Zhang, and L. Yan, "Quantum secure direct communication and authentication protocol with single photons", Chinese Science Bulletin, no. 58 (36), 2013, pp.4571-4576.

[21] L. Blum, M. Blum, M. Shub, "A simple unpredictable pseudo-random number generator", *SIAM J. Comput.*, vol. 15 (2), 1986, pp. 364–383.

[22] Z. Gutterman, B. Pinkas, T. Reinman, "Analysis of the Linux random number generator", *in Proc. IEEE Symposium on Security and Privacy*, May 2006, pp. 371-385.

[23] Government Committee of the USSR for Standards, "Cryptographic Protection for Data Processing System, Gosudarstvennyi Standard of USSR (In Russian)", GOST 28147-89, 1989.

[24] M. Luby, C. Rackoff, "How to construct pseudorandom permutations and pseudorandom functions", *SIAM J. Comput.*, vol. 17, 1988, pp. 373-386.