UDC 004.7+004.052

[1]**Zhukov I.A.**, doctor of engineering sciences,
orcid.org/0000-0002-9785-0233,
[1]**Pechurin N.K.**, doctor of engineering sciences,
orcid.org/0000-000-1727-7455,
[2]**Kondratova L.P.**, candidate of engineering sciences,
orcid.org/0000-0002-9170-4198,
Pechurin S.N., candidate of engineering sciences,
orcid.org/0000-0002-4098-5727

ONE-DIRECTIONAL PARSING FUNCTION FOR INFORMATION SECURITY IN COMPUTER NETWORKS OF UNMANNED AERIAL VEHICLES

[1]National Aviation University
[2]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

zhuia@ukr.net
nkpech@i.ua
ljupav@ukr.net

Introduction

Various protocols for ensuring the security of information, in particular, its confidentiality and integrity of transmitted data, in wireless computer telecommunication systems are presented in the IEEE 802.11, IEEE 802.16, IEEE 802.16x standards groups. [1]. At the same time, the corresponding functions and services are performed at each level of the Reference Model for Open Systems Interconnection [2]; for example, security tools are implemented at the physical level, at the level of access to the data transmission medium, WEP and WPA authentication and encryption mechanisms using static and dynamic keys, respectively, are at the highest levels [3,4].

The rapid introduction of unmanned aerial vehicles into the aviation sector, opening up prospects for the domestic aviation industry, also opens up prospects for the production of adequate information technologies. Obviously, the growth in the number of simultaneously functioning computer systems located on separate UAVs will lead to the need to integrate disparate aircraft into a computer network. This is especially true in situations where UAVs have not only a civilian purpose. Then the security of the information generated in the individual components of the network and transmitted, possibly by the method of packet switching, for example, according to the ITU (CCITT) X.25 standard, to the subscriber (s) becomes of particular importance due to the vulnerability, which is, in fact, completely automatic in unmanned systems, control technologies (in particular, guidance) of UAVs of various types [5].

The article develops the approach considered in [6], the essence of which is the coding of primary information with the tools of the formal languages and grammars theory on using in the development the ways to increase the information security of wireless data transmission systems in the computer networks of unmanned aerial vehicles.

The problem statement

For the analysis of each computer component installed on a separate UAV, a modeling method similar to that used in the construction of the Reference Model of Open Systems Interaction is used. The method provides for decomposing the system into levels with attributing data conversion functions and services to each level, for example, modulation, coding, transmission rate selection, fragmentation, transmission and reception of PDUs, confidentiality, data integrity, authentication and encryption functions. The PDU conversion functions also implement encapsulation and decapsulation procedures,

respectively, at the transmitting, receiving (as well as a pair of intermediate, communicating during transmission) stations.

The structure of, for example, a MAC frame is represented by a header, data, and trailer of a link layer PDU.

In a wireless network using FHSS and DSSS technologies, at the PLCP sublayer of the physical layer, the protocol addresses are translated into their equivalent hardware addresses contained in the format of the TCP/ IP protocol address translation protocol encapsulated in the hardware frame of the ARP message [7]. The information security function parameters presented in the PLCP PDU frame header and the MAC frame header indicate the coding scheme and encryption technology (WEP, WPA, WPA2) provided by the DSSS technology. The control field of the header frame contains a parameter characterizing the encryption technology.

It is necessary, given the high degree of unauthorized accessibility of radio channels used in the infrastructure of UAV computer networks, to propose an improvement in the encryption method based on the use of unidirectional parsing functions.

Solution of the problem

Let us consider the encryption and decryption procedure itself, proposed in [6], and based on the use of one-way parsing functions, using the example of systems where the fragmentation function is implemented. The fragmentation is used to increase the probability of successful transmission of a small length *PDU* over a wireless medium. The fragmentation function parameters are presented in the sequencing field of the MAC frame header, where the frame sequence number and the frame fragment number are indicated. The transmission of a frame fragment is activated by a bit in the frame control field. Figure shows the frame structure of the *PLCP* sublayer with a nested link layer frame for *DSSS* technology [7].

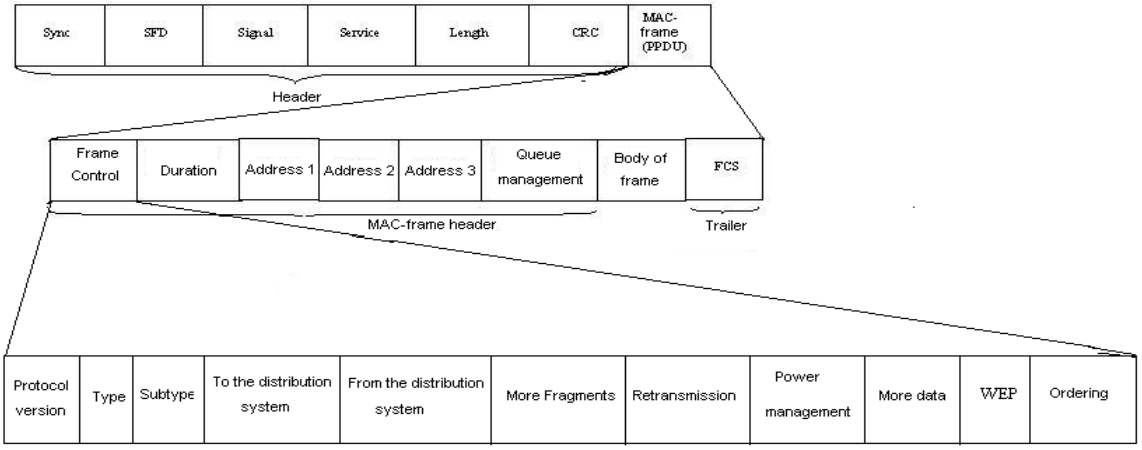

Figure. Frame format of PLCP sublayer with a nested frame of link layer for an IEEE 802.11 wireless network with DSSS technology

The features of the proposed improved encryption-decryption procedure are as follows.

The resulting sentence in terminal symbols is sequentially transmitted from the lower level (node) to the upper levels of the parsing model. In the case of the classical reference model for the interaction of open systems, there are 7 nodes (levels in the terminology of the reference model).

The decryption key is the parameters of the transition route from node to node.

In the case of the reference model, where the set of terminal symbols T = {0.1}, the hacking problem, i.e., identification of a message from the source of primary information, from the point of view of route discovery, is trivial.

Even if the functions of the physical layer of the model are detailed, as suggested in [7], although the power of the set T

increases, the probability of hacking during the communication session of the UAV system decreases slightly.

In the case of a regular language represented by a state machine, this is a route through the network where the arcs are weighted by a specific production rule.

It is clear that if we use a sequential n-level model (the cardinality of the set of non-terminal symbols of N is $|N|$), and as production rules – left-linear, right-linear or type of $n \Rightarrow t$ grammatical rules (in the Reference Model, this is a fixed rule for constructing an encapsulated PDU, a protocol, for each level), then with the power of the set of terminal symbols $|T|$, we have $|T|$ route options by nodes (states of the state machine).

If we use a hierarchical n-level model, and as production rules – all the same left-linear, right-linear or type of $n \Rightarrow t$ grammatical rules (in the Reference Model, this corresponds to the presence of several rules for constructing encapsulated PDUs of each of the seven levels), then with the power of the set of terminal symbols $|T|$, we have approximately $3 \bullet n \bullet |T|$ route options for nodes (machine states).

It is proposed to apply two methods to increase the degree of information security in the UAV computer network from unauthorized access due to: a) increasing the number of routes in parsing by moving from a tree-like hierarchical tree model to a network structure; b) increasing the number of vertices in the network structure (network) of grammatical analysis, identified by the non-terminal mark "sentence", which act as "false targets" for the system of unauthorized search for the source of primary information (unauthorized "pointing" at the source of primary information).

An example of a one-way parsing function on a data-link-physical interface

The model is represented by a set of rules for the production of the metalanguage of the Reference Model with a context-sensitive grammar of $G=<VT, VH, \sigma, P>$. *Here* $VT = \{0, 1, \varepsilon, A, B, C, D, LH1, LH2, SEQ\_NUM, MFR, FCS\}$ is the alphabet of terminal symbols with designations of *LH1, LH2, SEQ_NUM, MFR* for the given parameters in the headers of the frame of the physical layer and the MAC sublayer of the link layer, characterizing the length of the frame and fragmentation, *FCS* for the checksum; the set of {0,1} is used in forming a sequence of bits in the headers of the frame and checksum; the set of $\{A,B,C,D,\ldots\}$ is used in forming the a sequence of bits in the frame data field: $VH = \{PPDU, HEADER, DATA, TRAILER, SS, FC\}$ – the auxiliary alphabet of non-terminal symbols: SS, FC – the auxiliary metavariables used to form the headers of the physical and MAC sublayer of the link layer; $\sigma = PPDU \in VH$ – the initial non-terminal character; P – the set of rules for a context-sensitive grammar of type of $\xi_1 A \xi_2 \to \xi_1 v \xi_2$, $A \in V_H$, $\xi_1, \xi_2 \in \left(V_H \bigcup V_T\right)^*$, $v \in F(V) \left| F(V) = V_H \bigcup V_T \right.$, $\left(V_H \bigcup V_T\right)^* = V_H \bigcup V_T \bigcup \varepsilon$, ε – the empty chain. In this case, the designation of ε for an empty string it is used when the protocol data *PDU* header is completed.

The set of P includes the following translation rules of *PDU*:

PPDU → HEADER PPDU | HEADER DATA TRAILER;

HEADER → SS LH1 FC SEQ_NUM|SS LH1 FCS FC SEQ_NUM;

FC SEQ_NUM → FC MFR LH2 SEQ_NUM|FC MFR LH2;

FC → 0 FC 1 | 0 FC |1 FC | ε;

SS → 0 SS 1 |0 SS | 1 SS | ε;

DATA → A | B | C | D ….;

TRAILER → FCS.

Conclusions

1. The multiple use of production rules for generating sentences of a (regular) language in the processes of inter-level transformations and transmission of PDUs from a true primary information generator through nodes of UAV wireless computer network allows creating pseudo-sources of the primary information, which makes unauthorized identification difficult.

2. The analysis of the tree-like hierarchical parsing model makes it possible to increase the degree of information protection in the UAV computer network from unauthorized access by increasing the number of routes to the source in conditions of regularity of the language.

3. The analysis of the network model makes it possible to increase the number of vertices identified by the non-terminal label "sentences", which act as "false targets" for systems of unauthorized search for a source of primary information or unauthorized "pointing" at it. The unsolved problems include the choice of a method for exchanging keys for decrypting the decryption “route” parameters and assessing the influence of the chosen method on the effectiveness of the proposed procedure itself. The direction of further research is to clarify the possibility of applying the proposed encryption-decryption method, in terms of establishing pseudo-sources of primary information, to the task of targeting various types of unmanned aerial vehicles.

References

1. Guide to Internetworking Technologies. – [4th edition]. – M.: Publishing house "Williams", 2005. – 1040 p.

2. *Roshan P., Leary J.* 802.11 Wireless LAN Fundamentals. – M.: Publishing house "Williams", 2004. – 304 p.

3. *Lisetsky Yu.M., Bobrov S.I.* WiMAX networks. Implementations and prospects // Control Systems & Machines. –2008. – №4. – P. 88-92.

4. *Sumina G.A., Kozhanov E.A., Stepina A.N.* Information security in wireless networks // Telematics-2008: Proceedings of the XV All-Russian Scientific and Methodological Conference, St. Petersburg, June 23-26, 2008. – SPb., 2008. – P. 187-188.

5. Zhukov I.A. Implementation of integral telecommunication environment for harmonized air traffic control with scalable flight display systems // Aviation. – 2010. – №14 (4). – P. 117-122.

6. *Pechurin N.K., Kondratova L.P., Pechurin S.N.* Application of formal grammar tools for reclassifying the functions of the reference model of open systems interaction in a wireless computer network // Problems of informatization and management: a collection of scientific works – 2012. – Release №1 (37). – P. 89-94.

7. *Zhukov I.A., Pechurin N.K., Kondratova L.P., Pechurin S.N.* Representation of the interaction between the levels of a computer network of DSSS and FHSS by a model of regular languages and grammars // Electronic simulation. – 2014. – Vol.36, №2. – P. 49-55.

Zhukov I.A., Pechurin N.K., Kondratova L.P., Pechurin S.N.

ONE-DIRECTIONAL PARSING FUNCTION FOR INFORMATION SECURITY IN COMPUTER NETWORKS OF UNMANNED AERIAL VEHICLES

The tools of the formal languages and grammars theory are proposed to be used in developing the ways to increase the information security of wireless data transmission systems in computer networks of unmanned aerial vehicles (UAV). Multiple use of production rules for generating sentences of a (regular) language in the processes of inter-level transformations and transmission of PDUs from a

true primary information generator through UAV wireless computer network nodes allows to create the pseudo-sources of primary information, which hinders unauthorized access.

Keywords: *OSI/ISO reference model; protocol data unit; context-sensitive languages and grammars; parsing; fragmentation; computer system component.*

Жуков І.А., Печурін М.К., Кондратова Л.П., Печурін С.М.

ОДНОНАПРЯМОВА ФУНКЦІЯ ГРАМАТИЧНОГО РОЗБОРУ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ МЕРЕЖАХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Інструментарій теорії формальних мов і граматик пропонується застосувати для розробки способів підвищення інформаційної захищеності бездротових систем передачі даних комп'ютерних мереж безпілотних літальних апаратів. Багаторазове застосування продукційних правил генерування речень (регулярної) мови в процесах міжрівневих перетворень та передачі PDU від істинного генератора первинної інформації через вузли бездротової комп'ютерної мережі БПЛА дозволяє створити псевдоджерела первинної інформації, що ускладнює несанкціонований доступ.

Ключові слова*: еталонна модель ВВС/МОС; протокольний модуль даних; контекстно-залежні мови та граматики; граматичний розбір; фрагментація; компонент комп'ютерної системи.*