UDC 004.056: 519.766.23 DOI: 10.18372/2073-4751.77.18662

[1]**Pechurin M.K.**, doctor of engineering sciences,
orcid.org/0000-0003-1727-7455,
e-mail: nkpech@i.ua,
[2]**Kondratova L.P.**, candidate of engineering sciences,
orcid.org/0000-0002-9170-4198,
e-mail: ljupav@ukr.net,
[2]**Pechurin S.M.**, candidate of engineering sciences,
orcid.org/0000-0002-4098-5727,
e-mail: serg11se@i.ua

IEEE 802.15.1 MAC-TO-PHYSICAL LEVEL TRANSITION PROTOCOL AND ONE-DIRECTIONAL PARSING FUNCTION

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

Introduction

The choice of methods for protecting the interaction processes of UAV systems of the first class largely depends on the fact that this class includes light, low-power aircraft with small values of such quantitative characteristics as the maximum take-off weight, transmitter power, available height and radius of action, energy consumption level, etc. [1]. As a result, we have significant limitations in available information, computing and telecommunication resources [2]. The low speed of data transmission through the wireless environment, limited computing power, the amount of RAM, the need to use economical computing algorithms lead to a relatively low level of safety of operating UAVs. To methods of solving the problem of organizing safe (in the sense of protected) functioning of interconnected UAV systems there are devoted, for example, works [3-6]. In particular, in work [3] it is proposed to use normative models to find the optimal topology of the computer and telecommunications network, ensuring the high-quality implementation of functions by the UAV complex due to the increase in the degree of integration and the decrease in the radio emission intensity of the interacting UAV complex components; in work [4] the proposed statistical approach for protection against new, previously unknown attacks and malicious software; in work [5] – the method of the investigation and the prediction of cyber incidents based on methods and tools of data collection using global search systems, aggregation of information flows and intellectual analysis of extracted data; in work [6] – resource distribution method, which allows determining the minimum resource of tools of destructive influence and their optimal distribution in order to achieve the required level of disruption of the information exchange efficiency in communication systems. IEEE 802.11–802.16 recommendations deal with cryptography, authentication, encryption, etc. mechanisms (see, for example, [7, 8]).

In works [9-11], a method of PDU conversion with a toolkit of regular languages and grammars is proposed, which makes it possible to build algorithms for asymmetric encryption systems that do not require large computing resources.

This opus analyzes one important function of IEEE 802.15.1, which can be useful in the implementation of secure, reliable information exchange in the conditions of low bandwidth of wireless channels and the presence of interference in wireless systems – the function (procedure) of inter-level transformation of the PDU of the MAC sub-level of the channel level into PDU of the physical layer of the Open Systems Interconnection Reference Model for first-class interoperable UAVs.

The statement of the problem: description of the PDU conversion procedure as a prototype of the formal model

Using the example of the physical layer and MAC sub-layer of the channel layer of the Reference model of interaction of open systems [12] for interacting UAVs of the first class, taking into account the main recommendations of IEEE 802.15.1 regarding the protection of information from unauthorized access, determine the possibility and feasibility of using symmetric encryption systems and asymmetric ones based on unidirectional functions grammatical analysis, under the conditions of implementation of fragmentation procedures.

"Economical" implementation of the encryption function can be implemented using encryption algorithms from the WEP class, which are simple and effective enough for use in the conditions of a functioning 1st class UAV system. Here, a stream encryption algorithm is used based on the organization of the key stream followed by merging with the upstream text stream. Such a simple method is dangerous because of the possibility of unauthorized identification of repetitions of the ascending text.

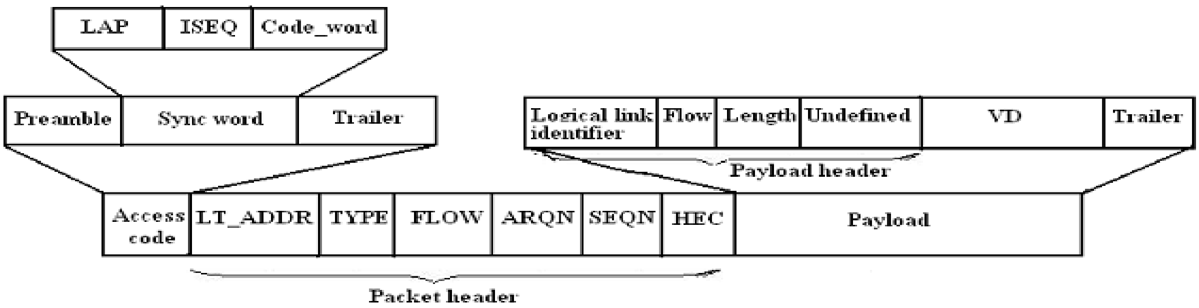
In works [10, 11], it is proposed to use the "one-directional function" of forming language sentences with the help of grammar, which plays the role of a key in the encryption system, in order to prevent the possibility of unauthorized determination of the ascending text.

Let's explore the possibility of transitioning to a wider class of languages, with the aim of applying an approach to the formation of a key flow with a key, the essence of which is a specific generative grammar. To do this, we describe in detail the PDU formatting procedure, limiting ourselves to the transition from the MAC sublayer to the physical layer using the IEEE 802.15.1 standard as an example.

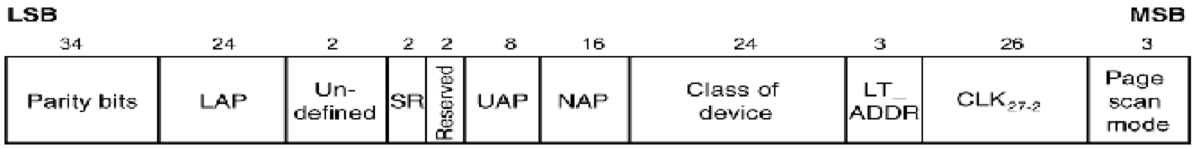
A physical network radio channel can be shared by a group of synchronized devices with a common clock and FHSS frequency hopping pattern forming a piconetwork [7]. In PPDU protocol data module format, a nested header is formed in Payload field of the physical layer (Fig.1a) by encapsulation, adding information from MAC sub-layer of the channel layer. The parameters of the error detection, encryption, and authentication functions presented in the fields Access_code of the access code to the channel, Packet_header of PPDU packet header of the physical layer, and Payload_header of the payload header of the MAC sub-channel layer characterize the level of information integrity, which allows to minimize redundancy as much as possible, and also determine the scheme on using cryptographic keys by the network devices. Activation of the confidentiality, authentication and encryption mechanism is provided by the parameter contained in the FLOW field of the physical level headers Packet_header and Payload_header on the MAC sub-level of the channel level based on the LMP communication management protocol. The LMP protocol has the highest priority compared to the L2CAP logical connection management and adaptation protocol; if it is necessary to transmit a LMP message, the connection is immediately provided. For LMP messages, an asynchronous packet of type DM1 is used as part of the payload, including the Payload_header and the CRC code.

The standard supports 15 types of synchronous and asynchronous packets, from which 4 types of packets (ID, NULL, POLL, FHS) are control. The 68-bit ID packet consists of the Access_code (Preamble and Sync_word) and is intended for requests and paging. NULL, POLL packets have a length of 126 bits, consist of the access code Access_code (preamble, Sync_word, Trailer) and the packet header Packet_header (Fig. 1a). The packet header, including HEC, consists of 18 bits (fields LT_ADDR – receiver address, TYPE – packet type, FLOW – flow control, ARQN – confirmation of correctness of reception, SEQN – determination of packet sequence, HEC – header checksum), after coding with speed 1/3 FEC header length reaches 54 bits. In the NULL packet, establishment for the confirmation of connection or data reception is provided, in the POLL packet, the obligation of the recipient to respond is provided. The FHS is a special control packet containing the Payload field, including the Payload_header. The payload contains information about the LAP address (lower address part), UAP (upper address part), NAP (insignificant address part), device class Class_of_device and clock frequency CLK_{27-2} of the transmitter (see Fig. 1b). The 8-bit Payload_header header includes the LLID identifier of the logical channel, the FLOW bit, and the LENGTH payload length indicator.

We have signs of transformation with typical signs of fragmentation; using this fact and the above description, let's make a PDU PPDU conversion model during the transition between the physical and MAC sub-layers of the channel layer.



a)



b)

Fig. 1. The general format of IEEE 802.15.1 packet with FHSS technology (a)
and FHS control packet payload format (b).

Problem solving: construction of a formal PDU PPDU conversion model

The transformation model of *PPDU* protocol module at the physical level and the MAC sub-level of the channel level of the open systems interaction reference model will be represented by a set of metalanguage production rules with a context-dependent (CD) grammar of kind $G=<V_H,V_T,\sigma,P>$, where V_N is the set of nonterminals; V_T is the set of terminals; P is the set of rules; σ is the initial non-terminal character (σ=PPDU). Elements of V_N, V_T sets are specified in accordance with the names for the components of the IEEE 802.15.1 standard package as in Fig. 1. The set of nonterminals V_N = {PPDU,Access_code, Header, Payload, Trailer, Preamble, Sync_word, VD, ISEQ, Data_Payload}. The set of terminals V_T = {0,1,Code_word, LAP, UAP, NAP, LT_ADDR, TYPE, FLOW, ARQN, SEQN, HEC, VOICE, DATA_U, LLID, LENGTH, CRC, Parity_bits, SR,Class_device,CLK,Page_scan_mode}, ISEQ is the metavariable, which characterizes the informational sequence of synchronized word, P is the set of rules CD grammar of type $\xi_1 A \xi_2 \to \xi_1 v \xi_2$, $A \in V_H$, $\xi_1, \xi_2 \in \left(V_H \bigcup V_T\right)^*$, $v \in F(V) \middle| F(V) = V_H \bigcup V_T$, $\left(V_H \bigcup V_T\right)^* = V_H \bigcup V_T \bigcup \varepsilon$, ε is an empty chain, used when completing the formation of the information sequence of the synchronized word of the access code of data to the radio channel. The set of rules of metalanguage production is represented by the following sentences:

PPDU → Access_code Header Payload | Access_code (1)

Access_code → Preamble LAP ISEQ Code_word Trailer | Preamble LAP ISEQ Code_word (2)

Preamble → 0101 | 1010 (3)

ISEQ → 0 ISEQ 1 | 0 ISEQ | 1 ISEQ | ϵ (4)

Header Payload → Header | Header Payload (5)

Payload → Header VD Trailer | Header VD (6)

Header VD → Header Data_Payload | Data_Payload (7)

Header → LT_ADDR TYPE FLOW ARQN SEQN HEC | LLID FLOW LENGTH (8)

Trailer → 0101 | 1010 | CRC (9)

Data_Payload → DATA_U | VOICE | Parity_bits LAP SR UAP NAP Class_device LT_ADDR CLK Page_scan_mode (10)

An example of using a model to form language sentences from control and information packets

The procedure for forming CD-grammar sentences for control and information packets consists in the generation of a certain sequence according to the requests of master and slave network devices in the piconet, starting from the ID packet to identify the slave device. Having identified this network devic, sentences are formed indicating the real hours of the master type device to determine the sequence of time slots where the transmission-reception data packets are located. Authentication and encryption functions are implemented by transferring transactions to the LMP communication management protocol using an asynchronous packet of type DM1. The method to implement the encryption-decryption functions is based on a scheme with asymmetric keys K1 and K2, respectively, as described in [10]. The data encryption function is performed at the representative level of the Reference Model of Open Systems Interaction in order to protect information from unauthorized access; its implementation is accompanied by the transformation of information, which is performed on the basis of Hopfield, Elman and similar neural networks [13].

The formation of out taking into account LMP-protocol messages. Let's sentences for asynchronous packet DM1 is carried consider the examples to form the CD-grammar sentences based on production rules (1)-(10) of the data protocol module conversion model for some types of packets.

Applying the production rules (1)-(4) of the *PPDU* transformation model, we will form a chain of terminals to identify the slave device by sequentially replacing the non-terminals of the V_N set. Using the ID package, we get the following sequence of substitutions:

PPDU → Access_code→ Preamble LAP ISEQ Code_word →0101 LAP 001101 Code_word.

It is assumed that the lower address part of the LAP is represented as 0… 1 …0; information sequence ISEQ as part of the synchronized word has the form 001101.

Using the FHS package, we will form a chain of terminals indicating the real hours of the master device. We get the following sequence of substitutions:

PPDU → Access_code Header Payload → Preamble LAP ISEQ Code_word Trailer Header Payload → Preamble LAP ISEQ Code_word Trailer LT_ADDR TYPE FLOW ARQN SEQN HEC Payload → 0101 LAP 001101Code_word 1010 LT_ADDR 0010110 HEC Payload → 0101 LAP 001101Code_word 1010 LT_ADDR 0010110 HEC Header VD Trailer → 0101 LAP 001101Code_word 1010 LT_ADDR 0010110 HEC Header Data_Payload Trailer → 0101 LAP 001101 Code_word 1010 LT_ADDR 0010110 HEC LLID FLOW LENGTH Parity_bits LAP SR UAP NAP Class_device LT_ADDR CLK Page_scan_mode CRC.

For an FHS packet, the LT_ADDR value is completely zero, the FLOW bit is set to 1. The terminal chain is converted to:

0101 LAP 001101 Code_word 1010 000 0010110 HEC 00 1 LENGTH Parity_bits LAP SR UAP NAP Class_device 000 CLK Page_scan_mode CRC

Using an asynchronous package of type DM1, we will form a chain of terminals taking into account the transaction of the LMP protocol regarding the implementation of the encryption-decryption function. The sequence of substitutions looks like this: PPDU → Access_code Header Payload → Preamble LAP ISEQ Code_word Trailer Header Payload → Preamble LAP ISEQ Code_word Trailer LT_ADDR TYPE FLOW ARQN SEQN HEC Payload → 0101 LAP 001101Code_word 1010 LT_ADDR 0011111 HEC Payload; PPDU → 0101 LAP 001101Code_word 1010 LT_ADDR 0011111 HEC Header VD Trailer → 0101 LAP 001101Code_word 1010 LT_ADDR 0011111 HEC Header Data_Payload Trailer → 0101 LAP 001101Code_word 1010 LT_ADDR 0011111 HEC LLID FLOW LENGTH Data_U CRC.

In the last received terminal chain, the logical connection identifier value is set to 11 for LMP messages, the FLOW bit is set to 1. The terminal chain is converted to:

0101 LAP 001101Code_word 1010 LT_ADDR 0011111 HEC 11 1 LENGTH Data_U CRC.

With using a control packet of the POLL type, we will form a chain of terminals taking into account the calculation of the checksum in the header data as an implementation of the error detection/correction function. The sequence of substitutions looks like this: PPDU → Access_code Header Payload → Access_code Header → Preamble LAP ISEQ Code_word Trailer Header → Preamble LAP ISEQ Code_word Trailer LT_ADDR TYPE FLOW ARQN SEQN HEC.

The LT_ADDR value for a POLL type packet is completely zero, the FLOW bits of the data flow control and ARQN of the confirmation of the correct reception are set to 1. The chain of terminals is transformed into the form:

0101 LAP 001101 Code_word 1010 000 0001110 HEC.

Thus, we have signs of sentences that are classified as belonging to context-dependent language.

Conclusions

The sentences generated during the implementation of the PDU inter-level conversion procedure of the MAC sub-level of the channel and physical layers of the Reference model of the interconnection of open systems for interacting UAVs of the first class, taking into account the recommendations of IEEE 802.15.1 regarding the protection of information from unauthorized access, are classified as sentences of context-sensitive language.

The analysis of the developed model shows that in order to apply a protection method based on the unidirectional function of grammatical parsing of regular language sentences, it is necessary to exclude the procedure considered in IEEE 802.15.1 from the protocol stack of the Reference Model of Open Systems Interaction.

References

1. STANAG 3700 Ed: 8 /AJP-3.3 Ed. B. Allied Joint Doctrine for Air and Space Operations. Washington : NATO Standardization Office (NSO), 2016. 100 p.
2. Zhukov I. A. et al. The model balancing parallel processing of photo- videoframes in computing cluster for UAV. *Problems of informatization and management*. 2017. Vol. 4, no. 60. P. 26–29. DOI: 10.18372/2073-4751.4.12816.
3. Pechurin N. K. et al. Models of the topologies for the weak-emitting telecommunication system of interacting UAVs. *Problems of informatization and management*. 2022. Vol. 4, no. 72. P. 48–54. DOI: 10.18372/ 2073-4751.72.17461.
4. Drovovozov V. I., Vodopianov S. V., Zhuravel S. V. Protection of vehicle networks against unauthorized access through isolation of exchange protocols. *Problems of informatization and management*. 2022. Vol. 4, no. 72. P. 26–34. DOI: 10.18372/2073-4751.72.17458.

5. Puchkov O. et al. OSINT investigation to detect and prevent cyber attacks and cyber security incidents. *Information Technology and Security*. 2021. Vol. 9, no 2(17). P. 209–218. DOI: 10.20535/2411-1031.2021.9.2.249921.

6. Sholokhov S. et al. Optimization of resources distribution of radio suppression means and destructive program impact on electronics networks. Information *Technology and Security*. 2022. Vol. 10, no 2(19). P. 230–240. DOI: 10.20535/2411-1031.2022.10.2.270464.

7. 802.15.1 IEEE Standard for Information Computer Society. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs). New York : IEEE Computer Society, 2005. URL: http://standards.ieee.org/getieee802/downloadtechnology.

8. 802.11ax-2021 IEEE Standard for Information Technology. Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks. Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN. New York : IEEE, 2021. DOI: 10.1109/IEEESTD.2021.9442429.

9. Zhukov I. A. et al. Representation of the interaction between the levels of a computer network of DSSS and FHSS by a model of regular languages and grammars. *Electronic modeling*. 2014. Vol. 36, no. 2. P. 49–55.

10. Pechurin N. K., Kondratova L. P., Pechurin S. N. The modeling of the secure intra-layer interaction in wireless computer networks by the facilities of the formal grammars' and languages' theory. *Problems of informatization and management*. 2014. Vol. 4, no. 48. P. 82–87. DOI: 10.18372/2073-4751.4.8042.

11. Zhukov I. A. et al. One-directional parsing function for information security in computer networks of unmanned aerial vehicles. *Problems of informatization and management*. 2021. Vol. 4, no. 68. P. 17–21. DOI: 10.18372/2073-4751.68. 16521.

12. ISO/IEC 7498-1:1994(E). Information technology. Open System Interconnection. Basic Reference Model: The Basic odel. Geneva : ISO/IEC, 1994. 62 p.

13. Su R. et al. Scalable learned image compression with a recurrent neural networks-based hyperprior. *2020 IEEE International Conference on Image Processing (ICIP)* : proceedings, Abu Dhabi, UAE, 25–28 October, 2020 / IEEE. Piscataway, 2020. P. 3369–3373. DOI: 10.1109/ICIP40778.2020.9190704.

Pechurin M.K., Kondratova L.P., Pechurin S.M.

IEEE 802.15.1 MAC-TO-PHYSICAL LEVEL TRANSITION PROTOCOL AND ONE-DIRECTIONAL PARSING FUNCTION

The procedure of inter-level transformations of PDUs is considered on the example of the MAC sub-level of the channel and physical levels of the Reference model of the interconnection of open systems for interacting UAVs of the first class, taking into account the main recommendations of IEEE 802.15.1 regarding the protection of information from unauthorized access. Distinctive features of first-class UAV computer systems and networks are low transmission speed and limited computing power of computer equipment. The recommendations regarding the relationship between the channel and physical layers, subject to the application of the IEEE 802.15.1 standard to ensure the security of the UAV system with resource limitations, are considered in detail, on the basis of which a model in the class of models of formal grammars is built. The analysis of the model showed that in order to apply the method of protection based on the unidirectional function of grammatical analysis of regular language sentences, it *is necessary to exclude the considered procedure from the protocol stack of the Reference Model of Open Systems Interaction.*

***Keywords**: wireless computer network; reference model of open systems interaction; PDU; context-dependent grammars and languages; IEEE 802.15.1.*

Печурін М.К., Кондратова Л.П., Печурін С.М.

ПРОТОКОЛ IEEE 802.15.1 ПЕРЕХОДУ ВІД MAC ДО ФІЗИЧНОГО РІВНЯ ТА ОДНОНАПРАВЛЕНА ФУНКЦІЯ ГРАМАТИЧНОГО РОЗБОРУ

Розглядається процедура міжрівневих перетворень PDU на прикладі підрівня MAC канального та фізичного рівнів Еталонної моделі взаємоз'вязку відкритих систем для взаємодіючих БПЛА першого класу з урахуванням основних рекомендацій IEEE 802.15.1 стосовно захисту інформації від несанкціонованого доступу. Відмінними особливостями комп'ютерних систем і мереж БПЛА першого класу є невисока швидкість передачі та обмежена обчислювальна потужність комп'ютерного обладнання. Детально розглянуто рекомендації стосовно взаємозв'язку канального та фізичного рівнів при умові застосування стандарту IEEE 802.15.1 для забезпечення захищеності системи БПЛА з обмеженнями в ресурсах,на основі чого побудовано модель в класі моделей формальних граматик. Аналіз моделі показав, що для застосування способу захисту, основаного на однонаправленій функції граматичного разбору речень регулярної мови, необхідно виключити розглянуту процедуру зі стеку протоколів Еталонної моделі взаємодії відкритих систем.

***Ключові слова**: безпроводова комп'ютерна мережа; Еталонна модель взаємодії відкритих систем; PDU; контекстно-залежні граматики та мови; IEEE 802.15.1.*