Security of Wireless onboard Sensor Network

Andrey N. Petukhov[1], Pavel L. Pilyugin[2]

Department of Critical Information Infrastructures Security
Moscow Technical University of Communications and Informatics
Moscow, Russia
[1]anpetukhov@yandex.ru, [2]ppl@mail.ru

Dmitry A. Ovcharenko

Luxoft Professional LLC

Moscow, Russia

i-want-to-buy-violin@yandex.ru

Abstract. **The paper discusses the construction of a secure sensor network on board a modern civil aircraft using wireless communication technologies. The context of information security (threats, attack scenarios) and the specifics of this context for civil avionics are established. Revealed significant heterogeneity and multidimensional infrastructure on-Board wireless sensor network, the expediency of bringing complex solutions to mobile networks fifth generation (5G) and software defined networking (SDN) to solve security issues onboard wireless sensor network.**

Keywords: **information security, avionics, wireless network, sensor network, software-defined networks.**

I. INTRODUCTION

The existing communication systems of the aircraft, including operational systems on board, as well as various sensors for engines, chassis, range sensors, controllers of state parameters of various components and parts of the aircraft, require complex wiring and the manufacture of wiring harnesses, which adds weight to the aircraft and, in turn, increases fuel consumption. These systems have a well-defined, but still limited reliability and involve double or even triple redundancy, in order to reduce the risk of breakage or defective wiring.

At the same time, wireless technology is already enough to be seriously considered by the aviation industry for use as a means of communication within the aircraft in future generations of aircraft. This is evidenced, in particular, by the launch and development of the Wireless Avionics Intra-Communication project (WAIC) and the working groups of the Aerospace Vehicle Systems Institute (AVSI), which was created by the largest aerospace companies to solve common problems related to wireless avionics [1].

II. WIRELESS ONBOARD SENSOR NETWORK

The main advantages of using wireless onboard sensor communication network (WOSN) are the following:

- reduced volume and complexity of wiring and wiring harness designs with appropriate weight savings and improved overall fuel efficiency (total weight of wires reaches several tons plus up to 30% additional weight to attach the wiring harness to the construction);
- significant expansion of possibilities of reconfiguration of equipment and supplies due to the increased flexibility of installation, use of the mobile equipment;
- reliable control of parameters, moving or rotating units and parts of the aircraft;
- improving the reliability of on-board systems by reducing the level of failures of inconsistent processing of multiple signals of wired redundancy (double or triple) [2].

In addition, the solution ITU-R (WRC-15 Final act) for future WOSN systems defined frequency range 4.2–4.4 GHz [3] (previously it was used only for onboard altimeters). The dedicated frequency range (4.2–4.4 GHz) is designed for safety-related radio communications between avionics components integrated or installed exclusively on board the same aircraft.

Technical (hardware-software) complex of WOSN is characterized by the following defining properties [4]:

- the network is designed for radio communication between avionics components integrated or installed on board the same aircraft;
- radio communication is carried out in an isolated internal network between two or more points on the same aircraft;
- the network covers only applications related to flight control and safety support;

- the network does not support air-to-ground, air-to-satellite or air-to-air (other aircraft) communications;
- the network is not intended to be used for communication or entertainment of passengers in flight;
- network systems operate during all phases of flight, including on the ground;
- aircraft equipped with wireless on-board network systems is operated on a global basis and crosses national borders;
- signals to the wireless network is weakened by the fuselage of the aircraft.

Therefore, the main tasks to be solved in the design of wireless security solutions can be as follows:

- providing network access control, in order to determine which communication participants are on the network, what resources these participants can use and applying access control rules for traffic between these network nodes;
- ensuring the integrity and reliability of the wireless network segment as a critical resource;
- ensuring the security of data transmitted over the network, primarily through security protocols that use algorithms for authentication, encryption and traffic integrity control.

III. FEATURES OF WOSN SECURITY THREATS

When solving these problems and making practical decisions on the information security of the WOSN, it should be borne in mind that this system is operated in conditions, the features of which determine the specifics of the relationship to the threats and vulnerabilities that occur for wireless networks in General. So, on the ground the aircraft is in an area with a high level of physical security. Access to the airfield is limited and controlled, there are systems of control of movement and video surveillance, i.e. there are grounds to assert that the object of protection is in a controlled zone. This complicates the potential for an intruder to get close to the aircraft for the attack on the wireless network. Especially as on the earth, part of critical elements of a network can be inactive. Security measures carried out at the airport during the pre-flight period — baggage control and hand luggage inspection — also limit the possibility of the appearance on board of special equipment, and if it is still delivered there, its use will raise suspicions of the crew.

In flight, the attacker will be limited in time (the maximum duration of the flight in the calculations taken 18 hours), and it may not be enough to collect material and perform the attack. Repeated flight on the same plane will not help the attacker, as each flight can be accompanied by a change of static keys. In principle, it is possible to set the task to raise the algorithmic security to a level that will make inefficient cryptanalysis during the time of flight and thus get rid of many security problems, but most likely this decision will be unacceptably expensive, slow and cumbersome.

The least secure wireless traffic is during connection establishment and exchange. In some cases, in these moments, there may be short-term situations of practical vulnerability of the data transmission system. If you provide for the initialization of the stationary flight operation of the WOSN nodes and communications even before the appearance of passengers in the cabin, then you can deprive a potential attacker of the opportunity to take advantage of a temporary decrease in the level of network security.

Most WOSN nodes are located in fixed locations and have relatively stable activity characteristics. This creates the prerequisites for the use of information about the general stationary picture of electromagnetic radiation on board and makes it possible to quickly indicate the emergence of a new source of radio signal and localize its position in the cabin (short-range radiation sensors in passenger seats, toilets and in the vestibules of the cabin).

These circumstances indicate not so much a reduction in the level of threats to information security, but the specifics of their manifestations and attitude to them in the implementation of specific practical solutions to protect against these threats.

IV. VARIETY OF REQUIREMENTS AND CONDITIONS OF WOSN ELEMENTS

The choice of the underlying communication platform is significantly influenced by the architectural and infrastructural features of the WOSN. The proposed architecture WOSN consists of the following components:

- network node is a network object with the ability to connect and communicate with another network object using a radio interface; a network node can also provide one or more wired interfaces that allow you to interact with objects outside the WOSN;
- gateway node is a network node connecting the WOSN (or parts thereof) to other, usually wired on-board networks, such as the avionics communication network on board the aircraft;
- a leaf node is the network node capable of ensuring the connection between the gateway node and the sensor, actuator or display using the radio interface WOSN (physically the end node may contain the sensor, actuator or display) [2].

When discussing the requirements for the basic IOS communication platform and security features, it is advisable to take into account the data transfer rates and the installation location of the transceiver antennas of the network nodes (on the inner or outer surface of the fuselage). WOSN applications can be divided into two categories that meet the data rate requirements of applications: low-speed applications have data rates below 10 kbit/s, and high-speed applications have data rates above 10 kbit/s. The expected average data rate for low-speed applications inside the aircraft ranges from 10 bps (electrical consumption monitoring) to 800 bps (cabin pressure control) per line. The peak transmission rate on one channel can reach 1 kbit/s (control of electromagnetic radiation on board). For outdoor sensors, the spread of requirements is even greater: the average speed varies from 20 Mbit/s (external door sensors)

to 8 kbit/s (flight control sensors). For high-speed applications inside the aircraft, the expected average speed ranges from 12.5 kbit/s (FADEC engine management interface) to 1.6 Mbit/s (freeze frame in the cockpit or salon) and the peak data rate can reach 4.8 Mbit/s (predictive engine sensors). Transmission speed requirements for high-speed applications outside the aircraft body also vary by several orders of magnitude: for them, the average speed is expected to range from 45 kbit/s (sensors of construction) to 1 Mbit/s (external video cameras) [5].

The prospective WOSN topology is such that the radio transmission of the applications installed inside the aircraft structure and shielded from the outside is provided through wireless subnets, each consisting of a gateway node and one or more end nodes. Each compartment is equipped with at least one gateway node serving all end nodes in the coverage area of that gateway node. Signal attenuation caused by bulkheads or even interior furniture is usually too high for the gateway node to service the compartments, outside of where it is located. Small compartments, such as the cockpit or the electronics compartment, may require only one gateway Assembly, while a large compartment, such as a passenger salon, may require multiple gateway assemblies. For radio applications installed outside the aircraft fuselage and therefore not shielded from the outside, the antennas are installed in places where the attached gateway node can reach all the associated end nodes. For example, the gateway node antenna can be mounted on the top of the fuselage, from where the aircraft edges, wing tips, vertical and horizontal tail and all relevant sensors are viewed. In the other case, the antennas of the gateway units can be installed inside the wheel wells to connect only to the sensors located on the chassis.

Thus, WOSN is characterized by significant heterogeneity, fundamental differences in the operating conditions of the network nodes, configuration dynamics, a variety of schemes and connection routes. All this is accompanied by a gradation of the criticality of applications and infrastructure elements, assuming up to five different levels of qualification requirements of confidence in avionics [6] and, in particular, in its security [7].

V. PROMISING BASIC COMMUNICATION PLATFORM OF WOSN

One of the areas in which solutions are being developed to create a communication platform that meets these conditions is the concept of 5G, a new generation communication network. This concept provides for the creation of a heterogeneous network, which will use different technologies to serve traffic and users of different types on the basis of a combination of developing radio access technologies with new data transmission technologies. It is assumed that in 5G networks devices exchange multiple streams of information simultaneously with nodes of different types, whose task at a particular time is to service this particular device. Each device has its own policy of interaction with the network, taking into account the amount of data transmitted, the amount of allowable delay and other parameters, in particular security requirements. From the who perspective, this means a transition to a network model where the primary is the network node (gateway, the end node), not the base station.

The use of controlled antennas (SDR-technology) capable of changing the radiation pattern will not only increase the speed of data transmission due to the growth of the signal / noise ratio, but also significantly increase the protection of WOSN from jamming and unauthorized listening. To improve the efficiency of network resources use and reliability of its functioning, it is provided to allocate (physically and in time) resources for different types of traffic, and for each network fragment its own data transmission technology can be used (network slicing). Due to the flexibility of the approach, it is possible to fulfill the most diverse and even contradictory requirements of different types of network nodes.

For example, the use of a special slice (ultra-reliable low latency communication) for data transmission with a small delay concept will allow to transfer data with a very short duration of transmission. It will be impossible for the attacker on board the aircraft to intercept such a “radio shot” and, moreover, to simulate it in sync. Since a large number of low-power devices are seen as part of the WSON end nodes, solutions for a slice, which is intended for IoT, are of interest. Following the 5G concept, WSON will become a “layer cake” combining different technologies, the use of each of which will be determined depending on the current requirements of a particular node of the network.

A feature of the 5G solution complex, attractive from the point of view of WOSN security, is a possible implementation of the “device-to-device” technology. Within WOSN, network devices communicate in units or tens of meters from each other, and thanks to this technology, only signal traffic can pass through gateways and wired avionics segments, allows to establish and control connections between network nodes, and the data itself will pass directly between devices.

Today, there is a network technology, based on the separation of management and data traffic. This technology is the software-defined network (SDN). SDN is using special protocols for the interaction of control and transport layers, for instance OpenFlow.. The control layer elements (controllers) can be located in wired avionics segments, they set the current routing scheme, actually controlling the topology (and therefore security) of the network. Elements of the transport layer (switches) carry out packet data transfer between the nodes of the WOSN network (possibly physically combined with them), and create prerequisites for highly effective unification of “classic” network security solutions. In addition, from the point of view of reliability of alternative routing, SDN (capability redundancy) is functionally similar to the plurality of redundant wiring (resources redundancy).

VI. CONCLUSION

For the wireless implementation of software-defined networks, the software of the universal Wi-Fi controller Chandelle has already been created [8]. This controller allows you to manage software-defined networks with a large number of WiFi access points and helps to solve two problems of centralized management of access points in such networks. Firstly, the cost of both access points and controllers developed

by manufacturers that solved the problem of centralized access point management (Cisco, Aruba, Motorola, Juniper, Zyxel) is significantly reduced, and, secondly, the equipment of access points of one manufacturer is compatible with the controllers of another. During the pilot testing of the prototype device, 63 UAP-PRO Ubiquiti access points were operating under its control, providing simultaneous access to more than 9 thousand users (25 thousand connections in peak mode). From the point of view of WOSN security, Chandelle development is interesting with the following features:

- efficient algorithm for dynamic management of frequency-power resources of access points;
- integration with software-defined networks;
- ability to actively oppose external threats;
- detect and localize third-party radiation sources;
- change of access rights of communication participants depending on their location.

Therefore, the SDR & SDN network can be implemented for WOSN.

VII. REFERENCES

[1] Wireless communications for safetyrelated avionics // W. A. Intra-Communications. 2012. URL: http://waic.avsi.aero/.

[2] Technical characteristics and operational objectives for Wireless avionics intra-communications (WAIC): Report M.2197 (ITU-R Report), approved Nov. 2015.

[3] Technical conditions for the use of the aeronautical mobile (R) service in the frequency band 4200–4400 MHz to support wireless avionics intra-communication systems: Report ITU-R M.2283, approved July 2015.

[4] Technical characteristics and protection criteria for Wireless Avionics Intra-Communication systems: Recommendation ITU-R M.2067, approved Nov. 2014.

[5] Technical characteristics and spectrum requirements of Wireless Avionics Intra-Communications systems to support their safe operation: Report ITU-R M.2283, approved Dec. 2013

[6] DO-178C, Software Considerations in Airborne Systems and Equipment Certification. FAA. 2012.

[7] Technical standard for future airbornecapability environment (FACE™) edition 1.0. Open Group, Jan 2012.

[8] Monin S., Shalimov A., Smeliansky R. Chandelle: Smooth and Fast WiFi Roaming with SDN/OpenFlow // Open Network Summit 2014. Santa Clara, 2014.