Conference Paper

MAC-PHY Cross-layer design for Secure Wireless Avionics Intra-Communications

Ramiro Robles

CISTER-TR-190626

2019/07/22

MAC-PHY Cross-layer design for Secure Wireless Avionics Intra-Communications

Ramiro Robles

CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: rasro@isep.ipp.pt

https://www.cister-labs.pt

Abstract

This paper presents a framework for medium access control (MAC) and physical (PHY) cross-layer security design of wireless avionics intra-communications (WAICs). The paper explores the different options based on the latest results of MAC-PHY cross-layer design and the available standard technologies for WAICs. Particular emphasis is given to solutions based on multiple-input multiple-output (MIMO) systems and recent developments towards a wireless technology with ultra-low latency and high reliability in the context of 5G and machine-type traffic support. One major objective is to improve WAICs technology and thus match the real -time, reliability and safety critical performance of the internal aeronautics bus technologies such as the ARINC 664 standard. The main identified vulnerabilities and potential solutions are explored and their impact on system design complexity and feasibility for wireless networks on-board aircraft. The solutions are presented in the context of the European project SCOTT (secure connected trustable things) using the recently released reference architecture to analyze the vulnerabilities, security issues and the potential solutions. Other aspects of SCOTT such as trust, privacy, security classes, and safety are also discussed here for the aeronautics domain.

MAC-PHY Cross-Layer Design for Secure Wireless Avionics Intra-Communications

Ramiro Sámano-Robles
Research Centre in Real-time and Embedded Computing Systems, Porto, Portugal; email:rasro@isep.ipp.pt

Abstract—**This paper presents a framework for medium access control (MAC) and physical (PHY) cross-layer security design of wireless avionics intra-communications (WAICs). The paper explores the different options based on the latest results of MAC-PHY cross-layer design and the available standard technologies for WAICs. Particular emphasis is given to solutions based on multiple-input multiple-output (MIMO) systems and recent developments towards a wireless technology with ultra-low latency and high reliability in the context of 5G and machine-type traffic support. One major objective is to improve WAICs technology and thus match the real-time, reliability and safety critical performance of the internal aeronautics bus technologies (e.g., ARINC 664). The main identified vulnerabilities and potential solutions are explored, as well as their impact on system design complexity and feasibility for wireless networks on-board aircraft. The solutions are presented in the context of the European project SCOTT (secure connected trustable things) using the recently released reference architecture for trusted IoT systems. Other aspects of SCOTT such as trust, privacy, security classes, and safety are also discussed here for the aeronautics domain.**

I. Introduction

The number of online objects has reached the number of 10 billion in 2019 [1]. In the era of the Internet of Things (IoT), new issues of reliability, interference, latency, safety, security, and privacy must be addressed [2]. Security threats in the virtual world can now have an impact on real objects, machines, autonomous cars, online printers, smart buildings, aircraft subsystems, etc. This poses a risk not only to the online systems themselves, but also to humans interacting with them.

Cross-layer design is a philosophy where the conventional rules for communication systems are relaxed with the aim of increasing performance [3]. Two or more layers of a system can now exchange information without restriction for purposes of tighter control or optimization. In some cases, layers can be completely merged or co-designed [4]. Cross-layer design can also lead to unwanted issues such as increase of signalling (i.e. loss of efficiency) and in some cases to instability problems [4]. However, in the lower layers of future wireless networks (e.g. 5G), cross-layer design is a cornerstone in increasing efficiency, scalability, security, and low latency.

Wireless networks are proliferating in many aspects and applications. In avionics, Wireless links have been used in applications such as radar, altimeter, aircraft-to-ground communication, etc. However, for avionics intra-communications, wireless has always raised doubts concerning reliability, security, and interference to critical aeronautical subsystems. This trend has changed over the last few of years. It has been shown that modern wireless technology can be a good contender to conventional cabling standards [5][6]. This means wireless technology can now replace or act as redundancy to the main cabling subsystems of a modern aircraft. This has several potential gains such a reduction of weight (which leads to improved fuel consumption, longer ranges or payload capacity), more flexible design (cabling plans are complex and expensive in aircraft design), improved management with troubleshooting, commissioning, and rebooting automatically over-the-air and on-the-fly. Several advantages are foreseen for the use of wireless inside aircraft. Regulation bodies have selected specific frequency bands for the new service called Wireless avionics intra-communications (WAICs) [8]-[11]. WAICs are in their infancy and several steps are still required to boost their adoption. In WAICs, cyber-security attacks can be translated to threats and safety hazards that put in danger an operational aircraft or lead to service disruption, thereby causing great economic losses. The main objective is to enable the concept of "fly-by-wireless" [12]-[15].

This paper presents an analysis of MAC-PHY security and related safety issues for WAICs. This involves the review of tools that can be used to detect, counteract and resolve malicious attacks, operational issues, functional safety hazards, etc. This framework is presented in the context of the SCOTT ECSEL research project (see [7]), which deals with aspects of security, safety, privacy, and trust of IoT applications. SCOTT has 16 use cases and 30 building blocks spanning 5 industrial domains. SCOTT aims to lay the foundations for security and privacy of IoT cross-domain systems.

This paper is organized as follows. Section II presents a typical WAICs system. Section III describes the SCOTT architecture of WAICs. Section IV presents the overall methodology for system vulnerability and security analysis of the WAICs-IoT architecture. Section V presents the MAC-PHY cross-layer framework. Finally, Section VI draws the conclusions.

II. Avionics System model

A WAIC system can be defined as a wireless transmission system where the network devices or nodes are located in the same aircraft. In general, in-flight entertainment systems (IFE) are not considered as part of WAICs. However, design

This work was partially supported by National Funds through FCT/MCTES (Portuguese Foundation for Science and Technology), within the CISTER Research Unit (UID/CEC/04234); also by the Operational Competitiveness Programme and Internationalization (COMPETE 2020) under the PT2020 Partnership Agreement, through the European Regional Development Fund (ERDF), and by national funds through the FCT, within project POCI-01-0145-FEDER-032218 (5GSDN).

of some IFE systems can also be helpful in the design of other WAICs applications. A WAIC system can thus have very diverse purposes, such as [8]: wireless sensing [16]-[17], cable replacement [18], structural health monitoring (SHM) [19]-[21], remote control and maintenance [22], object identification [23], fuel tank level monitoring [17], actuation (flaps), surveying, bus communications [24]-[26], etc .

Consider a generic short-haul aircraft depicted in Fig. 1 as shown originally in [8]. Note that the term WAIC also applies to other types of aircraft such as helicopters [27], aerial drones, etc. From Fig. 1, two types of wireless communication can be identified: internal and external to the aircraft [8]. External and internal networks can experience interference between them too. Therefore, careful design of frequency and resource allocation must be considered. It is also convenient to consider the physical configuration of aircraft. A good WAIC design must consider the optimum number and location of nodes, access points, or signal repeaters/relays, which ensure appropriate coverage where service will be provided. Generic topologies for WAICs in internal and external configuration have been described in the recommendations in [8]-[11]. Internal and external WAIC systems can be defined (see Fig. 2 and 3).

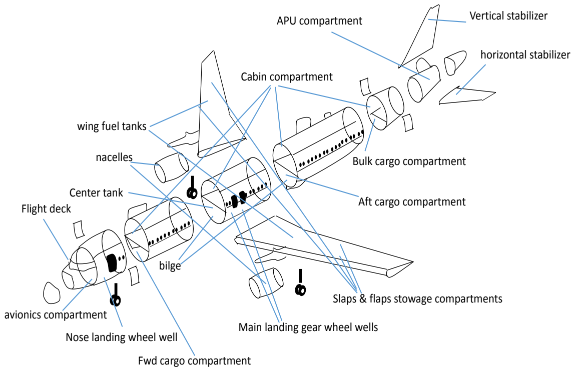

Fig. 1. Reference model of short-haul airplane [8].

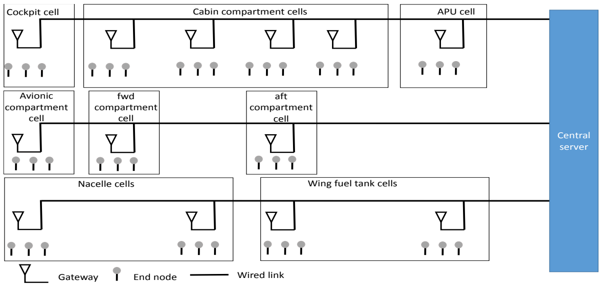

Fig. 2. Generic topology for internal WAICs [8]

Manufacturers define the architecture of aircraft information systems in three parts: Aircraft control domains, Aircraft information system domain, and Passenger entertainment service domain. Usually, information and control system domain follow modern DIMA (Distributed Integrated Modular Avionics) approach which allows fast configuration, set up and management of aircraft information infrastructure. In this aspect it is worth mentioning aircraft bus communication standards such as ARINC 664 [28], which define a real time deterministic version of commercial Ethernet standards. WAICs system will mainly interact with these existing information systems and bus communication standards, and therefore, security, dependability reliability analysis must be conducted in this particular interaction. One of the objectives the MAC-PHY framework proposed in this paper is to improve WAICs to match the real-time and deterministic requirements of the internal aeronautics network standards.

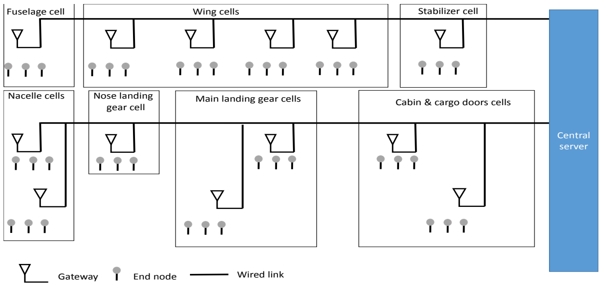

Fig. 3. Generic topology for external WAICs [8]

III. Architecture

The SCOTT reference architecture is a combination of modern IoT architectures using the concept of multiple views or perspectives of the system. Two main views are used in the particular case of the aeronautics domain: The layered entity model and the functional model.

The core of the SCOTT Reference architecture (RA) is the layered physical entity model. The main entity in the SCOTT RA is called WAICs Bubble. A WAICs Bubble will be able to contain one or more wireless sensor or node networks. Each WAIC WSN or node network will be managed by an WAIC Gateway. Therefore, the Bubble Gateway will be in charge of managing all the WAIC Gateways inside the Bubble, while also providing external/internal secure access to the information of Nodes (sensors and actuators) of each WAIC-WSN. This internal/external access to the Bubble information is encapsulated in a set of Bubble Services that can be invoked by internal and/or external users. This also means that all Bubble operation and management of high-level services will be hosted by the WAIC Bubble Gateway. This infrastructure arrangement naturally defines three levels or layers. Level 0 (L0) is the communication technology inside a specific WAIC-WSN. Each WSN can have a different L0 technology. Several WSNs can be hosted by one Bubble Gateway. One or more Bubbles can be deployed on a given aircraft. Level 1 (L1) is the communication technology/architecture inside the DEWI Bubble to connect several WSNs to the corresponding WAIC Bubble Gateway. In WAICs, L1 is the internal aeronautics network of the aircraft, e.g. ARINC 664 bus standard. Level 2 (L2) is the communication technology outside the Bubble. It provides a common external access to the Bubbles.

The SCOTT bubble concept helps system designers to enforce security inside the bubble infrastructure, where the main elements of the internal domain network and the sensors

/actuators attached to this infrastructure reside. Therefore, by explicitly isolating this infrastructure and providing specific mechanisms (secured) that external entities are allowed to access or requests, the security is controlled and therefore external attacks can be conveniently controlled or reduced. The layered entity model of the SCOTT reference architecture applied to a specific application of WAICs is displayed in Fig. 4. The specific application uses a network of densely distributed sensors and actuators to track and compensate the turbulence and skin drag effect. Therefore the network of sensors an actuators, organized in entities called patches and the wireless connection of each patch to the wireless gateways is Level 0 of the architecture. level 1 is the internal aeronautics network and Level 2 is the connection between the on-board with ground control operators.

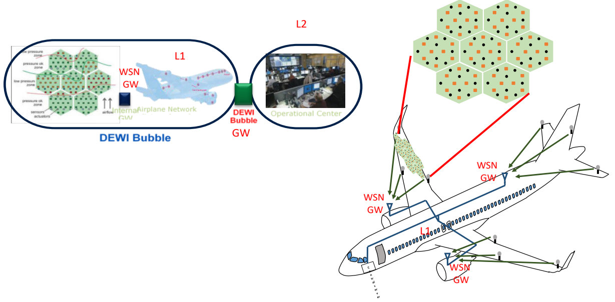

Fig. 4. Layered entity model.

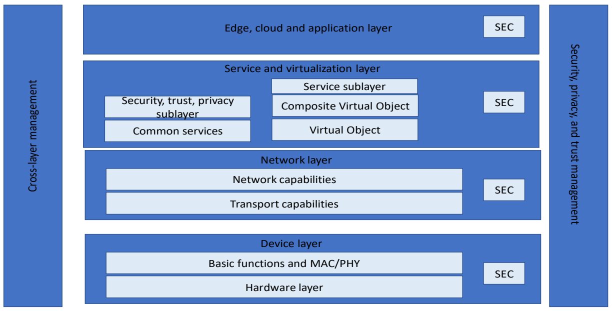

Fig. 5. Functional model SCOTT Reference Architecture

The SCOTT Functional model in Fig. 5 consists of 4 horizontal layers and two vertical layers. The horizontal layers are: device layer (DL), network layer (NL), service and virtualization layer (SVL), and Cloud and application layer (CAL). The two vertical layers are: Security, privacy, and trust layer, and the cross-layer and cross-domain layer. Each layer can have sublayers and a security module. This means SCOTT considers security solutions across different layers of the architecture. Each entity of the architecture can deploy different aspects of the reference functional model.

IV. Vulnerability and attack model(s)

Vulnerability and attack models are being developed for different layers of the aeronautics architecture. A useful reference model used in the SCOTT reference architecture and across the literature of security of IT systems is the Common Criteria. The important aspect from this framework is to identify the main asset, the associated vulnerability, and potential threats(s). From this information it is possible to define the actions that the stakeholders are willing to implement to reduce risk. The following tables show the vulnerabilities identified so far and potential solutions. Table I, Table II and Table III present the vulnerabilities and potential solutions for L0, L1, and L2 layers, respectively. The tables follow the functional model of the SCOTT reference Architecture.

TABLE I
Vulnerabilities L0.

Layer	**vulnerabilities**	Solutions
CAL	N/A	
SVL	DDoS	Packet analysis
NL	DoS, MiM, Spoofing	Auth, encryption
DL	Jamming, eavesdrop, collision	MIMO, beam

TABLE II
Vulnerabilities L1.

Layer	**vulnerabilities**	Solutions
CAL	Spoof ID theft	
SVL	DoS, latency, replay	Packet analysis
NL	DoS, MiM, Spoofing	Auth, encryption
DL	Jamming, eavesdrop, collision	MIMO, beam

TABLE III
Vulnerabilities L2.

Layer	**vulnerabilities**	Solutions
CAL	Spoof ID theft	
SVL	DoS, latency, replay	Firewall L3, tunnelling, Key distribution
NL	DoS, MiM, Spoofing	Authentication, encryption,n
DL	DoS, MiM	PHY-layer aggregation, authentication

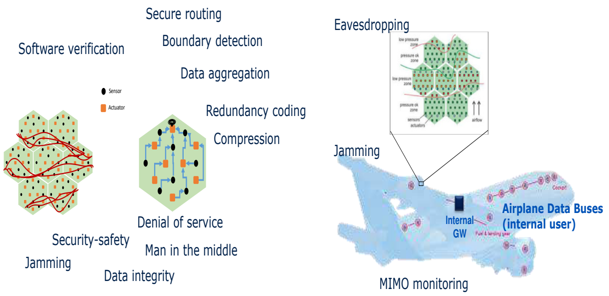

Fig. 6. Vulnerabilities and security solutions SCOTT aeronautics use case

The MAC-PHY cross-layer framework considered in this paper can be used to address not only low level attacks but also issues in different layers. Four examples are given next. An interference jamming attack can be minimized using direction of arrival detection, higher layer processing or a simple passive footprint beamforming that reduces the potential attacks from pre-established directions in the aircraft. The information about the attacker is used in the adaptation, retransmission control, MIMO resource allocation or secure beam-forming.

Eavesdropping is a passive attack common in wireless applications. When using MIMO to manage the information transmitted in different spatial directions, it is possible to deal simultaneously with the reduction of interference and the leakage of information to insecure directions where eavesdroppers might be detected or where there is a high risk.

Intrusion attack can lead nodes to have incorrect or undesirable behaviour, producing data or incorrect feedback to the loop control. Mechanisms are being developed to provide redundancy about the information sensed by different nodes. These mechanisms are based on a combination of PHY, MAC and higher layer reasoning processes. The idea is to detect nodes that have been compromised and adapt all the network to reduce the influence of a compromised node.

Higher layer attacks are also being considered. A denial of service (DoS) attack can be launched in the internal network of the aircraft, producing the lack of contact of the node with the control unit. Different approaches are being considered to address this issue, for example the triggering of an autonomous operation by the network of nodes, distributed decision making, MIMO isolation, etc. DoS attacks in the wireless domain can be isolated using MAC-PHY adaptive interference rejection.

V. MAC-PHY SECURITY FRAMEWORK

The PHY layer of communication systems refers to how the information is encoded in a radio electromagnetic wave. Therefore, PHY layer covers aspects of radio propagation modelling, RF circuit design, encoding, decoding, pre-coding, modulation, filter shaping, etc (see Fig 8). The MAC layer refers to the set of algorithms that help in the management and allocation of the medium to distributed terminals or nodes, including contention algorithms, resource reservation, frame design, feedback channel design, back-off retransmission algorithms (see Fig 9). MAC-PHY cross-layer design refers to the set of PHY or MAC tools that use enriched information from each other into their design or in some cases they are completely co-designed with its counterpart. MAC-PHY cross-layer design is particularly important in wireless networks due to the natural and tight connection of the physical propagation media and the resource management and contention between terminals that share unpredictable and sometimes unreliable fading links. Examples of MAC-PHY cross-layer are shown in Fig. 7.

Conventional PHY-layer security focuses on the use of tools to avoid attacks such as jamming and eavesdropping (see Fig. 8). PHY-layer encryption can be used to improve channel secrecy. Direction of arrival or direction of transmission can also be used in authentication. MIMO tools (e.g. [32]) can be used in detection of attacks, incorrect behavior analysis, and reduction of eavesdropping probability. At the MAC layer, some COTS standard have built in encryption capabilities. MAC identifiers and pilot signals can be subject of attack and therefore mechanisms to avoid these issues can be built in the in the design. MAC-PHY joint design based on multiple antenna and scheduling can direct the relevant information in directions of the intended terminals and induce noise (or collisions) in other risky directions. Retransmisison diversity can be used to reject adaptively jamming attacks while at the same time resolve collisions. MAC-layer is crucial in achieving ultra low latency of future 5G standards. The combination of MAC techniques with the highly directive large MIMO technology provides new interesting aspects for security in the cross-layer regime. Larger degrees of freedom can be used in space-time redundancy coding and encryption directly embedded in the modulation and scheduling of the wireless transmission, rejecting many types of attacks including jamming, eavesdropping, spoofing, denial of service, etc.

In WAICs, sensor readings relayed to the cabin can be subject to many types of attacks that can be reduced with the help of MAC-PHY algorithms. Tampering of sensors can be detected with the combination of MIMO techniques and higher level reasoning. The compromised sensor can be isolated using MIMO techniques to reduce its effects on the rest of the network. MIMO algorithms can be used to detect inconsistencies of sensors using time series and artificial intelligence. Highly directive MIMO algorithms can detect when sensors have been misplaced by errors or with malicious intentions. Collisions induced by attackers introducing extra noise in the network can be detected and minimized by a collision resolution signal processing. Successive interference cancellation can be used to improve network performance, reduce collision resolution periods, but also rejects jamming attacks or reduce the effect of malicious nodes or malfunctioning network elements.

The last decade has witnessed the proliferation of improved MAC algorithms (see Fig. 9) assisted by powerful signal processing tools. This new convergence requires improved modelling and optimization schemes that cross the border of conventional layered design. MAC and PHY layers are now co-designed paving the way for the next generation of algorithms that can be potentially used in avionics scenarios.

In the field of random access, multiple antenna technology or MIMO allows for immediate resolution of conflicts without the need of complex back-off retransmission policies. Random access protocols with multi-packet reception (MPR) have been studied in several scenarios with symmetrical [33] or asymmetrical population [29], with decentralized channel state information available to each terminal [34][35], using game theoretic optimization tools [36], or in combination with retransmission and cooperative diversity schemes [37]. These advances open the possibility for boosting CSMA-based and other contention-based technologies for avionics applications. Avionics scenarios might get benefit from multi-packet reception by reducing the number of retransmissions and hence reduced power consumption and minimized interference to on-board or to external systems. MPR can be also used to reduce the effects of jamming interference and in combination with retransmission diversity can be used for energy harvesting/reuse scenarios, thus reducing negative environmental effects. In avionics, there is a need for a detailed study of which cross-layer technologies for random access can be more effective. Inside the aircraft, spatial diversity could have mixed behaviour. Small distances between terminals tend to degrade space diversity. Instead, time-diversity could be used via induced retransmissions. On the other hand, external networks could experience better space diversity conditions, which might lead to the use of multiple antennas in combination with time-diversity multiple access approaches. Back-off algorithms can also be tuned to the needs of different elements in the network. Structure health monitoring and engine monitoring backlog traffic could be handled in a different way than for example altitude and temperature sensor information.

In centralized systems, cross-layer algorithms involve joint selection of modulation formats, frequency bins, nodes, and beam-forming vectors. This leads to a wide set of solutions that in the field of avionics must be studied in more detail. For example, higher priority can be granted to structural health sensor monitoring traffic and fuel sensors, thus allowing them to be jointly decoded by the same multiple antenna receiver or relayed with priority by other available relay nodes, while temperature and positioning systems can be scheduled with less priority. Interference alignment (IA) and user scheduling can be used in scenarios where terminals or sensor nodes use several antennas. IA allows uses subspace diversity to multiplex and manage interference in wireless networks. In the context of avionics, this can lead to a convenient reduction of interference to critical avionics subsystems transmitting in the null-subspace of their physical location or in the null subspace of their transmission (in the case of other wireless on-board systems). A cross-layer solution for aeronautics can be found in [41]. However, to the best of our knowledge, cross-layer solutions have not been studied in detail in WAICs.

Consider the WAICs system with J nodes, one access point, K interferers and R eavesdropper terminals. The set of nodes contending for access to the WAICs AP is denoted by $\mathcal{T}(n)$ in time slot n. The channel states, and transmission policies of the contending nodes are denoted, respectively, by the variables $\mathcal{H}_{\mathcal{T}}(n)$ and $\mathcal{P}_{\mathcal{T}}(n)$. Note that this model also captures MIMO transmission systems by defining each individual link as the conventional MIMO matrix model with variable $\mathbf{H}_j$. The set of estimated terminals at time slot n is denoted by $\hat{\mathcal{T}}(n)$ and the estimated channel states given by $\hat{\mathcal{H}}_{\mathcal{T}}(n)$. The contention of the scheduled nodes is assumed to be resolved in a finite number of time slots. The collection of channel states and transmission policies in n time slots is defined as the network state information for an epoch slot of n time slots:

$$\mathcal{N}_{\mathcal{T}}(n) = \{\mathcal{S}_{\mathcal{T}}(1), \ldots, \mathcal{S}_{\mathcal{T}}(n)\}$$

Retransmissions are activated by different criteria, leading to a probability of transition that can be written as follows:

$$\Pr\{\mathcal{N}_{\mathcal{T}}(n) | \mathcal{N}_{\mathcal{T}}(n-1)\}$$

The reception probabilities is denoted as:

$$q_{j|\mathcal{N}_{\mathcal{T}}} = \text{Probability of correct packet reception in time slot } n.$$

This reception probability is usually represented as the signal-to-interference-plus noise ratio SINR criterion:

$$q_{j|\mathcal{N}_{\mathcal{T}}} = \Pr\{\Gamma_j > \beta\}.$$

The total throughput can be expressed as the ratio of the correct packet reception to the average number of TTis used to correctly send or resedn the information:

$$T_j = \frac{\sum_{\mathcal{N}_n} \Pr\{\mathcal{N}_n\} q_{j,\mathcal{N}_n}}{\sum_{\mathcal{N}_n} \Pr\{\mathcal{N}_n\} n}.$$

The average latency can be obtained as:

$$D = \sum_{\mathcal{N}_n} \Pr\{\mathcal{N}_n\} n.$$

The set of scheduled nodes and transmission policies can be obtained as an optimization of the reception probabilities of the incumbent nodes and the reduction of the probability of eavesdropping:

$$\{\mathcal{T}_{opt}, n\} = \arg\max_{\mathcal{T}} [q_{\mathcal{T}|\mathcal{N}_n} - q_{eav|\mathcal{N}_n}]$$

Note that by optimizing the probability of correct reception, and with the convenient interference model, it is possible to mitigate interference jamming attacks. The framework uses space and time domain, and provides a useful abstraction of physical layer properties for non orthogonal multiple access, multi-packet reception and retransmission diversity to achieve higher values of throughput, reduced latency and higher resilience to eavesdropping and jamming attacks. The model is also useful for 5G new technologies with large MIMO and 3D-beamforming. It is particularly useful for latency calculations at the MAC level with enriched PHY-layer information such as non orthogonal multiple access (NOMA) [42] and ultra reliable and low latency communications (URLLC) [43].

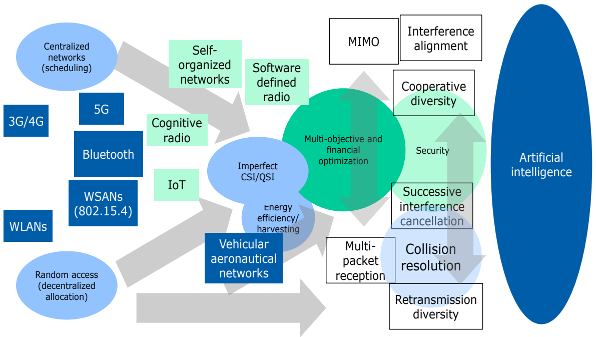

Fig. 7. MAC-PHY cross-layer topics.

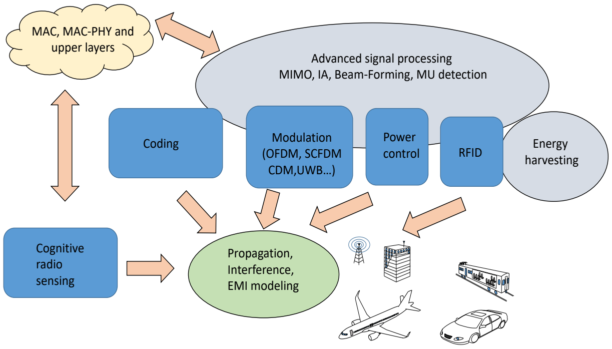
MAC, MAC-PHY and upper layers
Advanced signal processing
MIMO, IA, Beam-Forming, MU detection
Coding
Modulation (OFDM, SCFDM CDM,UWB...)
Power control
RFID
Energy harvesting
Cognitive radio sensing
Propagation, Interference, EMI modeling

Fig. 8. SCOTT PHY-layer tools.

VI. Conclusions

This paper has presented a framework for security analysis of wireless avionics intra-communications. The different tools available today for MAC-PHY cross-layer design of wireless components have been investigated in terms of feasibility,

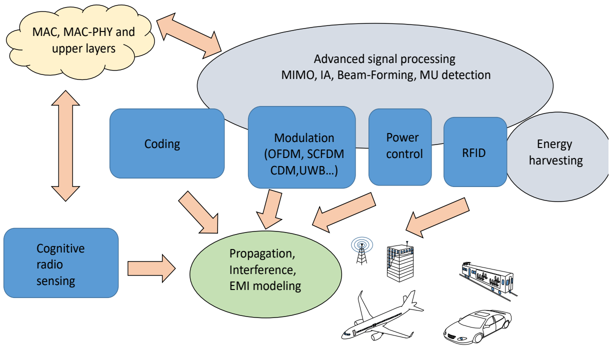
MAC, MAC-PHY and upper layers
Advanced signal processing
MIMO, IA, Beam-Forming, MU detection
Coding
Modulation (OFDM, SCFDM CDM,UWB...)
Power control
RFID
Energy harvesting
Cognitive radio sensing
Propagation, Interference, EMI modeling

Fig. 9. SCOTT MAC-layer tools.

security properties, and performance. New features related to systems such as 5G have been also presented in the context of WAICS, featuring ultra low latency, and high reliability.

References

[1] GSM Intelligence . Available at https://gsmaintelligence.com/

[2] ENISA. Eurpean Network Security Agency. IoT and smart infrastructures. https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot

[3] G. Dimic, N.D. Sidiropoulos, and R. Zhang "Medium access control-physical cross-layer design," *IEEE Sig. Proc. Magazine,* vol. 21, no. 5, pp. 40-50, Sep. 2004.

[4] V. Srivastava and M. Montani, "Cross-layer design: a survey and the road ahead," *IEEE Commun. Magazine,* vol 43, no. 12, pp. 112-119, 2005.

[5] T. Stone, R. Alena, J. Baldwin, and P. Wilson, "A viable COTS based wireless architecture for spacecraft avionics,," *IEEE Aerospace Conference,* 3-10 march 2012 Big Sky MT, pp. 1-11.

[6] J. Liu, I. Demirkiran, T. Yang, and A. Helfrick, "Feasibility study of IEEE 802.15.4 for aerospace wireless sensor networks," *IEEE/AIAA 28th Digital Avionics Systems Conference,* pp.1B.3 (1-10), Oct. 2009.

[7] SCOTT JU Grant Agreement incl. Description of Action (DoA), ECSEL Joint Undertaking, Grant Agreement No. 737422, Part B, 2018-07-11

[8] ITU.R M.2283-0 (12/2013) Technical characteristics and spectrum requirements of Wireless Avionics Intra-Communications systems to support their safe operation

[9] ITU.R M.2067 : Technical characteristics and protection criteria for Wireless Avionics Intra-Communication systems

[10] ITU.R M.2319-0 (2014) Compatibility analysis between wireless avionics intra-communication systems and systems in the existing services in the frequency band 4 200-4 400 MHz

[11] EUROCAE ED-246 Process Specification for Wireless On-board Avionics Networks

[12] D. Graham-Rowe. Fly-by-wireless set for take-off. New Scientist. 9/5/2009, Vol. 203 Issue 2724, pp. 20 .

[13] M. Harrington. "Introduction to wireless systems in aerospace applications. ," *CANEUS Fly-by-wireless workshop,* June 2009, Canada.

[14] O. Elgezabal. "Fly-by-Wireless (FBWSS): Benefits, risks and technical challenges. ," *CANEUS Fly-by-Wireless Workshop,* August 2010, USA.

[15] G. Studor, "NASA Fly-by-Wireless Update," http://hdl.handle.net/2060/20100031691

[16] W. Wilson and G. Atkinson. "Wireless sensing opportunities for aerospace applications," *Sens. and Trans., 2008,* Vol.94, No.7, pp. 83-90.

[17] D. Goldsmith, E. Gaura, J. Brusey, et al. "Wireless sensor networks for aerospace applications-thermal monitoring for a gas turbine engine," *Nanotech Conference and Expo.* :Taylor& Francis, 2009, 507-12.

[18] J. Collins. "The challenges facing U.S. navy aircraft electrical wiring systems," *9th Annual Aging Aircraft Conference,* 2006.

[19] B. Haowei, M. Atiquzzaman, and D. Lilja, "Wireless sensor network for aircraft health monitoring," *1st International Conf. on Broadband Networks, 2004. BroadNets 2004.* pp.748-50, 25-29 Oct. 2004

[20] R.K. Yedavalli and R.K. Belapurkar "Application of wireless sensor networks to aircraft control and health management systems," *Journal on Control Theory Applications, 2011* vol.9, no.1, pp.28-36,

[21] H. Bai, M. Atiquzzaman, and D. Lilja. "Wireless sensor network for aircraft health monitoring," *1st International Conf. on Broadband Networks. IEEE Computer Society,* 2004: 748 - 750.

[22] R. Hamman, "Wireless solutions for aircraft condition based maintenance systems," *IEEE Aerospace Conference , 2002* vol.6, pp.6-2877.

[23] R. Falk, et.al., "High-Assurance Avionics Multi-Domain RFID Processing System," *IEEE International Conf. on RFID,* pp.43,50, April 2008.

[24] B. Sambou, F. Peyrard, and C. Fraboul, "Scheduling avionics flows on an IEEE 802.11e HCCA and AFDX hybrid network," *IEEE Symposium on Computers and Commun. (ISCC),* pp.205,212, 2011.

[25] B. Sambou, F. Peyrard, and C. Fraboul, "AFDX Wireless Scheduler and free bandwidth managing in 802.11e(HCCA)/AFDX network," *7th Int. Wireless Commun. and Mobile Comp. Conf.,* 2011, pp.2109-14.

[26] C. Zhang, J. Xiao, and L. Zhao, "Wireless Asynchronous Transfer Mode based fly-by-wireless avionics network," *IEEE/AIAA 32nd Digital Avionics Systems Conference (DASC),* pp.4C5-1,4C5-9, 5-10 Oct. 2013.

[27] R. Ketcham, J. Frolik, and J. Covell, "Propagation measurement and statistical modeling for wireless sensor systems aboard helicopters," *IEEE Trans. on Aero. and Elec. Sys.,* vol.44, no.4, pp.1609-15, Oct. 2008

[28] INC. Aeronautical Radio. *ARINC Specification 664. Avionics Full-Duplex Switched Ethernet.* Annapolis, Maryland

[29] V. Naware, G. Mergen, and L. Tong, "Stability and delay of finite-user slotted ALOHA with multipacket reception," *IEEE Transactions on Information Theory,* 2005, vol. 51, No. 7, pp. 2636-56.

[30] L. Peng, R.C. de Lamare, and F. Rui "Multiple Feedback Successive Interference Cancellation Detection for Multiuser MIMO Systems," *IEEE Tran. on Wireless Commun.,* vol.10, no.8, pp.2434-39, August 2011

[31] V.R. Cadambe, and S.A Jafar, "Interference Alignment and Degrees of Freedom of the K -User Interference Channel," *IEEE Transaction on Information Theory,* vol.54, no.8, pp.3425-41, Aug. 2008

[32] L. Zhenghui, L. Fengyu, Y. Zhang, L. Xiao, et al. "Capacity and spatial correlation measurements for wideband distributed MIMO channel in aircraft cabin environment," *IEEE WCNC* pp.1175-79, 1-4 April 2012

[33] S. Ghez, S. Verdu and S. Schwartz, "Stability properties of slotted Aloha with multipacket reception capability," *IEEE Transactions on Automatic Control,* Vol. 33, No. 7, pp. 640-649, July 1988.

[34] M.H. Ngo, V. Krishnamurthy, and L. Tong, "Optimal Channel-Aware ALOHA Protocol for Random Access in WLANs With Multipacket Reception and Decentralized Channel State Information," *IEEE Transactions on Sig. Proc.* Vol. 56, No. 6, 2008 , pp. 2575-88.

[35] S. Adireddy and L. Tong, "Exploiting decentralized channel state information for random access," *IEEE Transaction on Information Theory,* Vol. 51, No. 2, 2005, pp. 537 - 561.

[36] M.H. Ngo and V. Krishnamurty, "Game theoretic cross-layer transmission policies in multipacket reception wireless networks," *IEEE Trans. on Signal Processing* , vol. 55, no. 5, May 2007, pp. 1911-26.

[37] R. Samano-Robles, M. Ghogho, and D.C. McLernon, "A multi-access protocol assisted by retransmission diversity and multipacket reception," *IEEE Int. Conf. ICASSP*, Las Vegas, 2008, pp. 3005-8.

[38] J. Gao, C. Fu, Y. Liu, and Y. Wei, "Behavioral modeling and EMC analysis for Tacan system," *IEEE Int. Symp. on Microwave, Antenna, Prop., and EMC for Wireless Comm. (MAPE),* pp.576,579, 1-3 Nov. 2011

[39] Y. Huang and Zhongke Shi, "The anti-interference analysis and design for mode S reply communication of integrated TCAS,," *Congress on Int. Control and Automation (WCICA), 2012,* pp.4467,4471, 6-8 July 2012

[40] C. Zhang, "Terrestrial mobile networks for Air-to-Ground communications of the General Aviation," *Int. Conference on Wireless Communications and Signal Processing (WCSP), 2011* , pp.1,5, 9-11 Nov. 2011

[41] J. Luo, W. Keusgen, A. Kortke, and M. Peter, "A Design Concept for a 60 GHz Wireless In-Flight Entertainment System," *IEEE 68th Vehicular Technology Conference, 2008. VTC 2008-Fall.* pp.1,5, 21-24 Sept. 2008

[42] X. Wei et al., "Software Defined Radio Implementation of a Non-Orthogonal Multiple Access System Towards 5G," in IEEE Access, vol. 4, no. , pp. 9604-9613, 2016.

[43] A. Anand, G. De Veciana and S. Shakkottai, "Joint Scheduling of URLLC and eMBB Traffic in 5G Wireless Networks," IEEE INFOCOM 2018, Honolulu, HI, 2018, pp. 1970-1978.