Security and Performance Comparison of Different Secure Channel Protocols for Avionics Wireless Networks

Raja Naeem Akram[†], Konstantinos Markantonakis[†], Keith Mayes[†]
Pierre-François Bonnefoi[‡], Damien Sauveron[‡§] and Serge Chaumette[§]
[†]*Information Security Group Smart Card Centre, Royal Holloway, University of London, Egham, United Kingdom*
[‡]*XLIM (UMR CNRS 7252 / Université de Limoges), Département Mathématiques Informatique. Limoges, France*
[§]*LaBRI (UMR CNRS 5800 / Université de Bordeaux), Talence, France*
Email: {r.n.akram, k.markantonakis, keith.mayes}@rhul.ac.uk,
{pierre-francois.bonnefoi, damien.sauveron}@unilim.fr, serge.chaumette@labri.fr

***Abstract*—The notion of Integrated Modular Avionics (IMA) refers to inter-connected pieces of avionics equipment supported by a wired technology, with stringent reliability and safety requirements. If the inter-connecting wires are physically secured so that a malicious user cannot access them directly, then this enforces (at least partially) the security of the network. However, substituting the wired network with a wireless network - which in this context is referred to as an Avionics Wireless Network (AWN) - brings a number of new challenges related to assurance, reliability, and security. The AWN thus has to ensure that it provides at least the required security and safety levels offered by the equivalent wired network. Providing a wired-equivalent security for a communication channel requires the setting up of a strong, secure (encrypted) channel between the entities that are connected to the AWN. In this paper, we propose three approaches to establish such a secure channel based on (i) pre-shared keys, (ii) trusted key distribution, and (iii) key-sharing protocols. For each of these approaches, we present at least two representative protocol variants. These protocols are then implemented as part of a demo AWN and they are then compared based on performance measurements. Most importantly, we have evaluated these protocols based on security and operational requirements that we define in this paper for an AWN.**

1. Introduction

In today's aircraft, Aircraft Data Networks (ADNs) – highly reliable, efficient and fault-tolerant distributed (real-time) networks – interconnect a large number of avionics sub-systems, enabling data and network management commands (control messages) to be exchanged within a predefined and deterministic time frame. These ADNs have to cater for a number of sub-systems with both critical and non-critical functions. Building a network that efficiently manages these two functions, while still providing a fully deterministic network with guaranteed bandwidth and Quality of Service (QoS), is extremely challenging [1].

These ADNs are basically wired networks that connect multiple devices using a physical connection. Examples of such networks include ARINC 825 [2], ARINC 664/AFDX (Avionics Full DupleX Switched Ethernet) [3, 4] and standard Ethernet. The wiring of these network cables requires an extensive design-time configuration of the aircraft, making post adaptation less flexible, not to mention the potential of wires being eroded and the problem of additional weight. In addition, the network redundancy is based on dissimilar paths, not dissimilar mediums of communication, even though the latter is known to be a better solution.

For these reasons, potentially, for non-critical functions of an aircraft a wired link between two communication points can be replaced with a wireless communication medium. Such a network is referred to as an Avionics Wireless Network (AWN). The potential for wireless communication in the AWN to be eavesdropped and/or modified is comparatively higher than for an ADN. For this reason, all communication between wireless nodes (pieces of equipment) in an AWN should be encrypted. To achieve such secure communication (via encryption), AWN nodes have to establish secure channels between each other, by running a secure channel protocol. In this paper, we have selected seven such secure channel protocols based on three different wireless communication deployment approaches. These selected protocols are then analysed for their suitability from performance and security point of view for AWN deployment.

1.1. Contribution

In this paper, our main focus is on the security and performance analysis of different secure channel protocols for AWNs. Our salient contributions are the following:

1) selection of seven secure channel protocols based on three different setup approaches (pre-shared keys, trusted key distribution, and key sharing protocols);
2) definition of criteria to compare these secure channel protocols along with the related security and performance analysis;
3) implementation of these protocols in a AWN test-bed based on off-the-shelve hardware, so as to be able to make measurements.

1.2. Structure of the Paper

Section 2 briefly presents the generic architecture of Aircraft Data Networks, which constitutes a rationale for considering the benefits of using Wireless Networks. Section 3 discusses different AWN formats and the need for secure channel protocols and proposes a case study in which the secure channel protocols presented in section 5 may take place. Section 4 introduces the studied secure channel deployment scenarios. Section 5 provides the results of the evaluation of several secure channel protocols in a AWN test-bed. Section 6 compares them based on the obtained results according to the defined security and performance criteria. In section 7 we provide a summary of our experiments.

2. Aircraft Data Networks

In this section, we discuss the traditional deployment of a wired network (ADN) in an aircraft. We conclude with a short list of benefits that would result from replacing some non-critical functions of ADN with wireless technology.

2.1. Generic Architecture

A modern aircraft network consists of several data networks, including flight-control and/or crew network (figure 1), and passengers (entertainment) network (figure 2).

Flight-control and/or crew networks consist of a multitude of sub-systems interconnected using wired technology as shown in figure 1. These different avionics sub-systems are connected with end systems that are then interconnected by means of a backbone network using several communication standards like ARINC 429 [5], ARINC 825 [2] or AFDX (ARINC 664 Aircraft Data Network, Part 7) [3, 6]. Each arrow in the figure 1 represents a logical communication link that physically consists of two wires connecting these devices via different paths (dissimilar path redundancy).

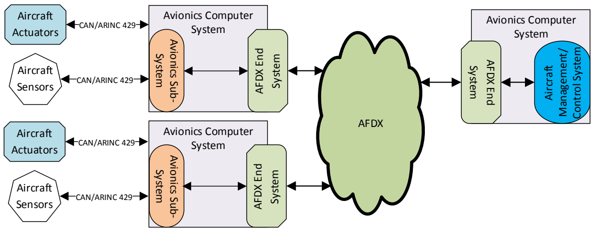

Figure 1. Generic Aircraft (Flight-Control and/or Crew) Data Network with AFDX as an Example

For some specific sub-systems, there are sets of sensors and actuators connected on Controller Area Network (CAN) [7] or ARINC 429 buses for flight control systems [8]. The AFDX or a similar technology is used to interconnect time- and safety-critical sub-systems like environmental control, doors and other utility systems. The AFDX backbone also connects less critical sub-systems like displays providing safety information to passengers, but includes oxygen masks, oxygen flow and audio announcement triggers, and it manages the quality of service accordingly.

As shown in figure 2, the entertainment network can be supported using standard Ethernet technology – it is not a high reliability- and safety-critical network.

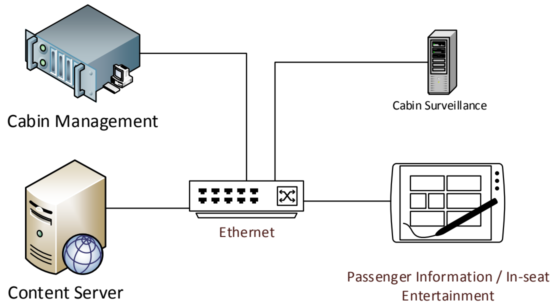

Figure 2. Generic Aircraft (Cabin) Data Network

The type and nature of the network configuration is dependent on the deployment scenario and objectives. However, there is a possibility that the flight control network, crew network and passenger (entertainment) network are all supported by the same wired technology, requiring implementation of network segregation by either physical separation of networks or by stringent firewalls, robust gateways and security policies [9].

2.2. Benefits of Wireless Networks

Whatever the network deployment topology and the communication technology used, one common element remains: the physical wire that connects two or more avionics sub-systems. Wiring an aircraft can be costly in that it includes wiring harness designs, cable fabrication and the associated exploitation cost due to the resulting additional weight. Furthermore, to provide dual redundancy these wires have to connect any two devices via two physically separated paths in the aircraft. Potentially, the wires and the related connectors represent 2-5 percent of an aircraft's weight [10]. The design of the wiring route is heavily dependent on wiring harness design that has to satisfy the challenge of providing separate routing paths for redundant wiring. As the wiring of an aircraft is a time- and labor-intensive activity, post-deployment upgrades or installation of new wire routes or avionics sub-systems can be very expensive [11]. As reported by [10], roughly 30 percent of wires are potential candidates for wireless substitutes. Therefore, as highlighted in [12], wireless solutions have reasonable prospects as long as security, safety and high levels of reliability can be maintained.

3. Avionics Wireless Network

Referring to [12], an AWN is defined as an aircraft network inter-connecting its different components using wireless technology instead of physical wires. Based on this definition, AWNs have been classified into four overlapping deployment architectures [12]:

1) **Wireless Sensor Networks (WSN):** A WSN is a set of intelligent and autonomous systems that can sense physical or environmental conditions and/or act on them. Usually WSN nodes record the designated data and transfer them via a wireless medium to some dedicated nodes (so-called sinks) that act as gateways (as in a wireless mesh network) between the WSN and a third party system, to which the connection can be wired. As some related work has mentioned, such networks are particularly useful in aircraft design [13, 14], especially to monitor moving and/or rotating parts (for example, the landing gear [10] or the engine itself [15]). A WSN can also be useful as an independent network (*i.e.* not connected to the aircraft network) simply to collect and store flight-related data; for instance, to improve the efficiency of an on-ground maintenance crew [16].
2) **Dissimilar Redundancy Network (DRN):** Since aircraft networks must be fault-tolerant, wireless links can be used to build dissimilar redundant networks; this would lower the probability of a potential common mode failure in networks based on the same wired technology. In addition, it decreases the difficulty of routing the wires - as much as possible, and as permitted by the aircraft geometry - using physically disjoint paths. Related work has identified that dissimilar network technologies can provide redundancy, which might enhance the overall reliability [17] in some critical situations compared to "identical redundancy" [18].
3) **Inflight Entertainment Network (IFE):** Since it is one of the least critical networks on board an aircraft, the Ethernet switch of the IFE depicted in figure 2 can be replaced by a wireless access point as described by [19], to offer more custom services without decreasing the overall safety of the aircraft.
4) **Wireless as a Comm-Link:** In this type of AWN, wireless communication links replace the wired links between avionics computing modules as shown in Figure 3. The protocols and the network architecture above the data link layer can remain the same, but at the physical layer, the data is communicated via a wireless medium rather than a wired medium. This type of network can be considered as a partial or a full deployment. In a partial deployment, out of two redundant wired links between aircraft sub-systems only one is replaced by a wireless link. In a full deployment both wired links between the aircraft sub-systems are replaced by wireless links.

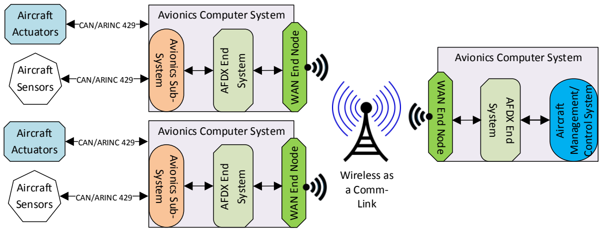

Figure 3. Generic Representation of Wireless as a Comm-Link

3.1. Related Work on Security Concerns

Security and trust have also been subject to analysis by both the academic community and the industry. A brief overview of aircraft information security and some improvements were proposed in [16]. Security assurance research, from airplane production up to operation, was presented in [20, 21]. A general discussion on the security issues related to the aircraft network and aircrafts' internet connectivity is discussed in [22], while [1, 9] discuss the impact of WSNs deployed in aircraft and related security concerns. Security and safety are intrinsically related to each other in general and especially in the context of the aviation industry [23]–[25]. The application and impact of cryptography, and especially the impact of public key cryptography for avionics networks, was evaluated in [26].

Security and the general deployment of AWNs based on wireless-as-a-comm-link have been analyzed in [12], which discusses the security and trust challenges faced by AWNs. Beside this, a crucial component of the security of aircraft devices is the trusted boot process discussed in [27]. The security, trust and assurance issues related to bringing a user device into an aircraft network are evaluated in [28].

3.2. AWN Case Study

When considering the four deployment models discussed above for a wireless technology as part of an aircraft network, one thing is common: all of these options rely on data being transmitted over the air. This potentially makes it easier for an adversary to eavesdrop and/or modify the transmitted pieces of information. To prevent such eventualities, strong cryptography constructs are deployed to create a secure channel. A secure communication channel is encrypted with a key known only by the communicating entities. From an attacker's perspective he/she can still observe the encrypted messages but these should not give him/her any knowledge about the contents of the communication. Regarding the modification of messages, an attacker can modify them but the results (decrypted form of the transmitted message) would potentially not be in his/her control – because he/she does not know the key used to encrypt the message. However, if a strong integrity mechanism is used to secure the channel, any modification would be detected.

Having secure channels for AWN communication is essential. To achieve this, an AWN has to run a secure channel protocol that would result in communicating entities being authenticated, and it also has to generate secure keys that would be used for encrypting the communications. For this reason, regardless of what type of AWN is chosen, it is necessary to set up a secure channel (to enable secure communication), which is the sole focus of this paper: our goal is to evaluate the security and performance of different secure channel protocols. We note that although wireless jamming and Denial-of-Service (DoS) attacks are valid and real concerns for AWNs we do not investigate them here and countermeasures to cope with such attacks are beyond the scope of this paper.

4. Secure Channel Deployment Scenarios

In this section, we discuss the three deployment scenarios that we have defined for the establishment of secure channels in AWNs. Even though these scenarios might not be exhaustive, we believe that they are representative. Wireless communication itself can be deployed either in Access Point (AP) or ad-hoc modes. In this section, we are not concerned with AP and/or ad-hoc modes but with the nature of the key sharing mechanism, the supporting architecture, what is known prior to the execution of the protocol, and the execution of the secure channel protocols themselves. The issues of security and reliability directly related to the AP and the AP/ad-hoc modes are beyond the scope of this paper.

4.1. Pre-Shared Keys

In this scenario, all communicating nodes in an AWN share a symmetric key that is provided either by their manufacturer or by the entity that deploys/configures them. This pre-shared key scenario can be achieved in two different ways. In the first method all the nodes have the same key to encrypt all the messages that they exchange with the other entities. In the second method, the pre-shared key is not used to directly encrypt the messages but to generate a session key. In this scenario the pre-shared key is referred to as the "master key" and a pre-defined algorithm is used to generate session keys.

4.2. Trusted Key Distribution Frameworks (TKDF)

In this scenario, all the nodes in the AWN trust a single entity that is responsible for generating and distributing the session keys that they will use to encrypt their messages. Such an entity is referred as a Trusted Key Distribution Server (TKDS) and all the nodes in the network have to communicate with it. Since not all nodes of the AWN might be in wireless communication range of the TKDS, they thus have to rely on neighboring nodes or on wireless range extenders (relay nodes). Each node in the AWN and the TKDS initially shares a secret key (either a symmetric or asymmetric key) and these keys are used to secure the communication between each of the nodes and the TKDS.

4.3. Key Sharing On Demand

In this scenario, each individual node executes a secure channel protocol with its communicating peers in the network. The aim of this protocol is to authenticate the nodes with each other and to create session keys. For this deployment scenario, no prior sharing of keys is required as the session keys are computed during the execution of the protocol. For entity authentication, some prior knowledge of communicating partners is essential. This is required to successfully authenticate the entities. The process of authentication does not influence the key generation/sharing process in a protocol.

5. Establishing Secure Wireless Connections

The performance of several secure channel protocols has been measured over a wireless comm-link in a AWN test-bed. The results are presented in this section.

5.1. Selected Protocols

Seven different protocols have been considered to establish secure channels over the wireless comm-link of the AWN test-bed. They can be gathered in three different families: secure channels based on pre-shared keys; secure channels based on Trusted Key Distribution Frameworks (TKDFs); and secure channels based on key sharing protocols, as discussed in section 4.

For secure channels based on pre-shared keys, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) and IPSec have been selected. When using WEP, each node has a fixed pre-shared key used to encrypt the data frames using RC4. With WPA-PSK, each node has a pre-shared master key that is used to build session keys during the authentication phase. Compared to the two previous secure channel protocols, IPSec encryption (with fixed pre-shared keys in our experiments) is achieved at the level of layer 3 (*i.e.* network) of the OSI protocol stack instead of layer 2 (*i.e.* data link) for WEP and WPA-PSK.

For secure channels based on TKDFs, two ad-hoc frameworks were developed. The authentication and key distribution phase is based on symmetric keys for the first framework whereas it is based on asymmetric keys for the second framework. In a symmetric key-based TKDF, each node shares a symmetric key with a trusted key distribution server, which uses it to send the session key encrypted with the shared key associated with each communicating node. Then each node decrypts it to use the key to finalize the establishment of the secure channel. For our experiments, the fixed version of the Needham-Schroeder Symmetric Key Protocol, which is the basis of Kerberos, was implemented using AES as the symmetric encryption algorithm.

In an asymmetric key-based TKDF, each node shares a public key with a trusted key distribution server, which uses it to send encrypted session keys that the target node deciphers with its private key. For our experiments, the fixed version of the Needham-Schroeder (so-called Needham-Schroeder–Lowe) public Key Protocol was implemented using RSA as the public key algorithm. In both TKDFs, the distributed session keys are symmetric keys used by the parties to communicate in the network. In our implementations, AES was used as the channel encryption algorithm.

For the secure channels based on key sharing protocols, SSH and SSL were selected.

5.2. Comparison Criteria

For a protocol to support the AWN framework, it should meet, at minimum, the security and operational requirements listed below:

G1) ***Mutual Entity Authentication*****:** All nodes in the network should be able to authenticate with each other so as to avoid masquerading by a malicious entity.

G2) **Asymmetric Architecture:** Certified public keys should be exchanged between the entities to facilitate the key generation and entity authentication process.

G3) **Mutual Key Agreement:** Communicating parties should agree on the generation of a key during the execution of the protocol.

G4) **Joint *Key Control*:** Communicating parties should mutually control the generation of new keys to prevent one party from choosing weak keys or predetermining any portion of the session key.

G5) ***Key Freshness*****:** The generated key should be fresh with regards to the protocol session to prevent replay attacks.

G6) **Mutual *Key Confirmation*:** The communicating parties should provide implicit or explicit confirmation that they have generated the same keys during a run of the protocol.

G7) **Known-Key Security:** Should a malicious user obtain the session key of a particular protocol run, he/she should not be able to retrieve long-term secrets (*private keys*) or *session keys* (future and past).

G8) **Unknown *Key* Share Resilience:** In the event of an unknown key share attack, an entity $\mathcal{X}$ believes that it has shared a key with $\mathcal{Y}$, where the entity $\mathcal{Y}$ mistakenly believes that it has shared the key with entity $\mathcal{Z} \neq \mathcal{X}$. The proposed protocols should adequately protect against this kind of attack.

G9) ***Key* Compromise Impersonation (KCI) Resilience:** If a malicious user retrieves the long-term key of an entity $\mathcal{Y}$, it will enable him to impersonate $\mathcal{Y}$. Nevertheless, compromising the key should not enable him to impersonate other entities [29].

G10) ***Perfect Forward Secrecy*****:** If the long-term keys of communicating entities are compromised, this should not enable a malicious user to compromise previously generated session keys.

G11) **Mutual *Non-Repudiation*:** The communicating entities will not be able to deny that they have executed a protocol run with each other.

G12) **Partial Chosen Key (PCK) Attack Resilience:** Protocols that claim to provide joint key control are susceptible to this type of attack [30]. In this type of attack, if two entities provide separate values to the key generation function then one entity has to communicate its contribution value to the other. The second entity can then compute the value of its contribution in such a way that it can dictate its strength (i.e. it is able to generate a partially weak key). This attack depends upon the computational capabilities of the second entity. The proposed protocols should adequately prevent PCK attack.

G13) **Privacy:** A third party should not be able to know the identities of the AWN nodes.

For a formal definition of the (italicized) terms used in the above list, the reader is referred to [31]. The requirements listed above are used below as a point of reference to compare the selected protocols in Table 1.

For the performance evaluation that we have conducted, the main measurements are related to the time required to establish a secure channel once the wireless link is established (or to establish the secure wireless link for protocols like WEP and WPA-PSK operating at the level of the data link layer). The properties of the keys (e.g. type of keys, key size, and freshness) will be discussed with regards to the performance results.

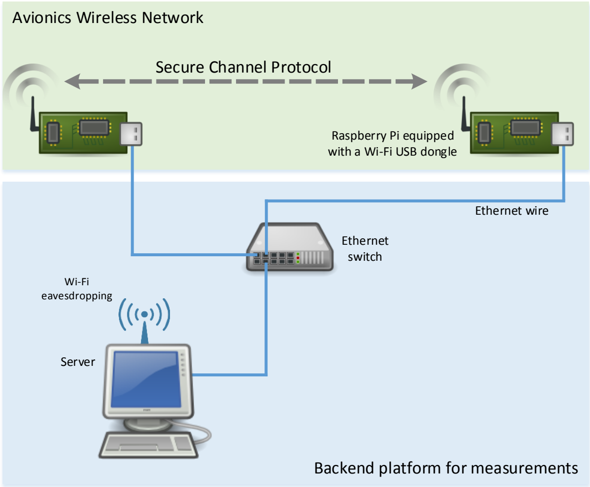
Avionics Wireless Network
Secure Channel Protocol
Raspberry Pi equipped with a Wi-Fi USB dongle
Ethernet wire
Ethernet switch
Wi-Fi eavesdropping
Server
Backend platform for measurements

Figure 4. AWN test-bed

5.3. Test-Bed for Performance Evaluation

In our AWN test-bed each node is a Raspberry Pi model B supplied with a Wi-Fi USB dongle TL-WN722N by TP-LINK. In all our measurements, the nodes were configured in ad-hoc mode.

For all the selected protocols, in our evaluation implementations, only 2 nodes establish a secure channel. However, for the TKDF, a key distribution server is also required and a third node in the ad-hoc network plays this role.

In our AWN test-bed, each node is connected to a backend server by means of an Ethernet connection. This server controls the nodes so as to prepare them for the target scenario and is also in charge of collecting the measurements. Effective measurement can be done internally on the node initiating the secure channel, called a client, or at the level of the network data exchanged between the nodes of the AWN and captured with a Wi-Fi card on the backend server set in monitor mode.

6. Security and Performance Analysis

In this section, we present the security analysis of the selected protocols based on the goals stated above; it is followed by the performance analysis of these protocols. We conclude the section with an overall analysis and with a discussion of some future research directions.

6.1. Security Analysis

Before discussing the analysis of the security goals as met by each protocol presented in Table 1, it is worth noting that several of them can be configured in several manners that may change the way they satisfy the goals and may also change their performance. For instance, we decided to use IPSec with fixed pre-shared keys. This choice is not one that can satisfy the maximum number of goals but this solution is more suitable for resource-constrained wireless nodes. However, Internet Key Exchange (IKE) protocol could have been used and then IPSec would have met additional goals.

When comparing the selected protocols, taking into account the above remark, it is interesting to note that the protocols based on asymmetric cryptosystems are those that meet most of the goals. However, these solutions are known to be costly in terms of time and resource consumption, as confirmed by the performance measurements presented in the following section. The secure channel protocols acting in the low level layers of the OSI stack, like WEP, WPA-PSK (layer 2), or even IPSec (layer 3), fail to satisfy several goals, which is surprising because, usually, security solutions provided at low levels are more generic; they might be expected to ensure better security than solutions working at higher levels. Solutions at these levels that establish more secure channels do exist (e.g. 802.1X and RADIUS server at level 2, IPSec and PKI) but they are not applicable to resource-constrained wireless nodes. Thus, among our selected protocols, solutions that establish secure channels at higher levels (SSH or SSL operate respectively at levels 7 and 5-7) and/or that rely on a server (symmetric and asymmetric TKDF) satisfy more goals. However these solutions are too costly: either they are based on asymmetric cryptosystems (which are costly in terms of resources) or they need a server that is costly in terms of bandwidth, latency and delay.

Table 1. PROTOCOLS COMPARISON ON THE BASIS OF THE STATED GOALS (SEE SECTION 5.2.)

Goals	Protocols						
	WEP	WPA-PSK	IPSec	Symmetric TKDF	Asymmetric TKDF	SSH	SSL
G1.	$-*$	$-*$	$-*$	$*$	$*$	$(*)$	$*$
G2.	$\times$	$\times$	$\times$	$\times$	$*$	$*$	$*$
G3.	$\times$	$-*$	$\times$	$-*$	$-*$	$*$	$*$
G4.	$\times$	$-*$	$-*$	$-*$	$-*$	$(*)$	$(*)$
G5.	$\times$	$*$	$\times$	$*$	$*$	$*$	$*$
G6.	$*$	$*$	$*$	$*$	$*$	$*$	$*$
G7.	$\times$	$*$	$\times$	$*$	$*$	$*$	$*$
G8.	$-*$	$-*$	$-*$	$-*$	$-*$	$*$	$*$
G9.	$\times$	$\times$	$*$	$*$	$*$	$*$	$*$
G10.	$\times$	$\times$	$\times$	$*$	$*$	$*$	$*$
G11.	$\times$	$\times$	$\times$	$\times$	$*$	$*$	$*$
G12.	$*$	$*$	$*$	$*$	$*$	$*$	$*$
G13.	$-*$	$-*$	$-*$	$(*)$	$(*)$	$(*)$	$(*)$

Note: $*$ means that the protocol meets the stated goal, $(*)$ shows that the protocol meets the requirement in certain conditions, $\times$ shows that the protocol cannot meet the stated goal and $-*$ means that the protocol (implicitly) meets the requirement, not because of the protocol messages but because of the prior relationship between the communicating entities.

6.2. Performance Analysis

The practical results obtained on our AWN test-bed confirm the theoretical analysis: asymmetric cryptosystems are costly and solutions relying on a third party (TKDFs) are even more costly. To be fair, it is important to note that we implemented the two TKDF protocols ourselves whereas the implementations of other tested protocols were done by groups of professional developers. Thus our implementations may be optimized, but not to the point where this would change the results by a significant factor. In addition, it can be noted that SSL and SSH operate over a TCP connection, which is more time consuming for the establishment of communication than our implementations of TKDF, which operate over UDP to improve performance (at the expense of the reliability of the connection).

The good performance of WEP and WPA-PSK are related to the fact that the protocols are run by the dedicated hardware and firmware of the Wi-Fi card - optimized for the execution of these protocols. The good results for IPSec are also related to the use of optimized hardware on the Wi-Fi card to execute this protocol - as it is an important protocol for Internet communication.

Table 2. PERFORMANCE COMPARISON OF SELECTED SECURE CHANNEL PROTOCOLS.

Protocol	Key type	Key size (bits)	Establishment (ms)
WEP	RC4	128	2.42
WPA	AES	128	2.55
IPSec	AES	256	2.67
Symmetric TKDF	AES	256	5092.88
Asymmetric TKDF	RSA	2048	14447.63
SSH	RSA	2048	911.21
SSL	RSA	2048	1310.93

Note that in WEP and WPA-PSK in ad-hoc mode, the packet loss was very important, respectively around 50% and 70%. WPA-PSK in AP mode needs the same time to establish the secure channel but the rate of packet lost was only 20%. For IPSec in ad-hoc mode, which encrypts at layer 3 over a plain text channel at layer 2, the rate of packet loss was 0%. Thus, as mentioned in the next section, the connection mode and the layer at which the secure channel should be established are parameters that should be studied in future work.

6.3. Overall Analysis and Future Research Directions

It appears that the selected protocols (all state-of-the-art in computer science security) are too generic, *i.e.* not specifically tailored for the target applications, or do not offer acceptable performance. Therefore, as part of our future research, we are currently experimenting with:

- A new secure and trusted channel protocol that meets all the stated requirements, moving away from large API (Application Programming Interface) based protocols like SSL and IPSec that might introduce implementation-related vulnerabilities.
- Security and reliability of AP and ad-hoc modes in different AWN deployment contexts.

Additionally, we are exploring the following directions:

- Countering wireless jamming and DoS attacks.
- Secure execution on nodes using ARM TrustZone and Intel SGX.

7. Conclusion

In this paper, we have discussed the nature of ADN and how AWNs might provide a valid alternative to wired networks. Any communication that uses a wireless medium has the inherent issue that an attacker can easily access this physical communication link. This can enable the attacker to eavesdrop and/or modify the contents of messages. To avoid this, secure channels are essential to encrypt all messages. For this encryption to be secure and robust, the keys that are used need to be not only secure but also to meet additional security requirements. In this paper, we listed thirteen security goals that we believe any secure channel protocol should meet. Subsequently, we selected seven different secure channel protocols (representative examples from three different wireless deployment scenarios). We developed a test-bed to evaluate their performance. We then compared the seven selected protocols in terms of security and performance.

There is no doubt that extensive work is still required before an AWN can be deployed in an aircraft environment and there are many challenges to overcome. However, in this paper we provide security comparisons and experimental performance data that we believe will be useful for someone wanting to deploy an AWN to enable them to make an informed decision about which features/protocols meet their unique environment and requirements. This paper contributes to the work that needs to be done to make AWNs a robust and secure proposal.

Acknowledgments

The authors from Royal Holloway University of London acknowledge the support of the UK's innovation agency, InnovateUK, and the contributions of the SHAWN project partners. The authors from XLIM acknowledge the support of:

- the SFD (Security of Fleets of Drones) project funded by Région Limousin;
- the TRUSTED (TRUSted TEstbed for Drones) project funded by the CNRS INS2I institute through the call 2016 PEPS ("Projet Exploratoire Premier Soutien") SISC ("Sécurité Informatique et des Systèmes Cyber-physiques");
- the SUITED (Suited secUrIty TEstbed for Drones) and UNITED (United NetworkIng TEstbed for Drones) projects funded by the MIRES (Mathématiques et leurs Interactions, Images et information numérique, Réseaux et Sécurité) CNRS research federation;

The authors from LaBRI acknowledge the support of:

- the TRUSTED (TRUSted TEstbed for Drones) project funded by the CNRS INS2I institute through the call 2016 PEPS ("Projet Exploratoire Premier Soutien") SISC ("Sécurité Informatique et des Systèmes Cyber-physiques");
- the SUITED-BX and UNITED-BX projects funded by LaBRI and its MUSe team.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the position of SHAWN project or any of organisations associated with this project.

References

[1] R. V. Robinson, K. Sampigethaya, M. Li, S. Lintelman, R. Poovendran, and D. von Oheimb, "Secure network-enabled commercial airplane operations: It support infrastructure challenges," in *Proceedings of the First CEAS European Air and Space Conference Century Perspectives (CEAS)*, 2007.

[2] *ARINC 825-3: General Standardization of CAN (Controller Area Network) Bus Protocol for Airborne Use*, Online, ARINC Standard, November 2015.

[3] *ARINC 664: Aircraft Data Network Part 1 - Part 8*, Online, ARINC Standard, June 2006.

[4] N. E. din Safwat, M. A. El-dakroury, and A. Zekry, "Article: The evolution of aircraft data networks," *International Journal of Computer Applications*, vol. 94, no. 11, pp. 27–32, May 2014, full text available.

[5] *ARINC 429: Digital Information Transfer System (DITS)*, Online, ARINC Standard, November 2012.

[6] J. Li, L. Zheng, and J. Yao, "Afdx based avionic data bus architecture design and analysis," in *Autonomous Decentralized Systems, 2009. ISADS'09. International Symposium on*. IEEE, 2009, pp. 1–1.

[7] K. Etschberger, *Controller Area Network*. IXXAT Automation GmbH, August 2001.

[8] G. F. Bartley, *Digital Avionics Handbook*, 3rd ed. CRC Press, 2015, ch. Boeing B-777: Fly-by-Wire Flight Controls, pp. 29–1 – 29–14.

[9] N. Thanthry and R. Pendse, "Aviation data networks: security issues and network architecture," in *Security Technology, 2004. 38th Annual 2004 International Carnahan Conference on*, Oct 2004, pp. 77–81.

[10] "Technical characteristics and operational objectives for wireless avionics intra-communications (waic)," ITU- R: Radiocommunication Sector of ITU, Tech. Rep. ITU-R M.2197, November 2010. [Online]. Available: http://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2197-2010-PDF-E.pdf

[11] D.-K. Dang, A. Mifdaoui, and T. Gayraud, "Fly-by-wireless for next generation aircraft: Challenges and potential solutions," in *Wireless Days (WD), 2012 IFIP*, Nov 2012, pp. 1–8.

[12] R. N. Akram, K. Markantonakis, S. Kariyawasam, S. Ayub, A. Seeam, and R. Atkinson, "Challenges of security and trust in avionics wireless networks," in *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, Sept 2015, pp. 4B1–1–4B1–12.

[13] B. Nickerson and R. Lally, "Development of a smart wireless networkable sensor for aircraft engine health management," in *Aerospace Conference, 2001, IEEE Proceedings.*, vol. 7, 2001, pp. 7–3262 vol.7.

[14] K. Sampigethaya, R. Poovendran, L. Bushnell, M. Li, R. Robinson, and S. Lintelman, "Secure wireless collection and distribution of commercial airplane health data," *Aerospace and Electronic Systems Magazine, IEEE*, vol. 24, no. 7, pp. 14–20, July 2009.

[15] R. Yedavalli and R. Belapurkar, "Application of wireless sensor networks to aircraft control and health management systems," *Journal of Control Theory and Applications*, vol. 9, no. 1, pp. 28–33, 2011. [Online]. Available: http://dx.doi.org/10.1007/s11768-011-0242-9

[16] M. Olive, R. Oishi, and S. Arentz, "Commercial aircraft information security-an overview of arinc report 811," in *25th Digital Avionics Systems Conference, 2006 IEEE/AIAA*, Oct 2006, pp. 1–12.

[17] E. F. Hitt, *Digital Avionics Handbook*, 3rd ed. CRC Press, 2015, ch. Fault-Tolerant Avionics, pp. 5–1 – 5–25.

[18] J. Downer, *When Failure is an Option: Redundancy, reliability and regulation in complex technical systems*. Centre for Analysis of Risk and Regulation, London School of Economics and Political Science, 2009. [Online]. Available: http://eprints.lse.ac.uk/36537/1/Disspaper53.pdf

[19] A. Akl, T. Gayraud, and P. Berthou, "Investigating several wireless technologies to build a heteregeneous network for the in-flight entertainment system inside an aircraft cabin," in *Wireless and Mobile Communications (ICWMC), 2010 6th International Conference on*. IEEE, 2010, pp. 532–537.

[20] S. Lintelman, R. Robinson, M. Li, D. v. Oheimb, R. Poovendran, and K. Sampigethaya, "Security assurance for it infrastructure supporting airplane production, maintenance, and operation," in *Proc. U.S. National Workshop on Aviation Software Systems: Design for Certifiably Dependable Systems (NITRD HCSS-AS), 4-5 Oct 2006, Alexandria, VA*, J. Sprinkle, Ed., 2006, available from http://ddvo.net/papers/HCSS-AS.html.

[21] G. Ladstaetter, N. Reichert, and T. Obert, "It security management of aircraft in operation: A manufacturer's view," SAE Technical Paper, Tech. Rep., 2011.

[22] N. Thanthry, M. S. Ali, and R. Pendse, "Security, internet connectivity and aircraft data networks," *Aerospace and Electronic Systems Magazine, IEEE*, vol. 21, no. 11, pp. 3–7, 2006.

[23] S. Brostoff and M. A. Sasse, "Safe and sound: a safety-critical approach to security," in *Proceedings of the 2001 workshop on New security paradigms*. ACM, 2001, pp. 41–50.

[24] A. Pfitzmann, "Why safety and security should and will merge." in *SAFECOMP*, ser. Lecture Notes in Computer Science, M. Heisel, P. Liggesmeyer, and S. Wittmann, Eds., vol. 3219. Springer, 2004, pp. 1–2. [Online]. Available: http://dblp.uni-trier.de/db/conf/safecomp/safecomp2004.html#Pfitzmann04

[25] M. Paulitsch, R. Reiger, L. Strigini, and R. E. Bloomfield, "Evidence-based security in aerospace: From safety to security and back again." in *ISSRE Workshops*. IEEE, 2012, pp. 21–22. [Online]. Available: http://dblp.uni-trier.de/db/conf/issre/issre2012w.html#PaulitschRSB12

[26] R. Robinson, M. Li, S. Lintelman, K. Sampigethaya, R. Poovendran, D. von Oheimb, and J.-U. Bußer, "Impact of public key enabled applications on the operation and maintenance of commercial airplanes," in *Proc. of the 7th AIAA Aviation Technology, Integration and Operations Conference (ATIO)*. AIAA, 2007, http://ddvo.net/papers/AIAA_ATIO.html.

[27] K. Markantonakis and R. N. Akram, "A secure and trusted boot process for avionics wireless networks," in *2016 Integrated Communications Navigation and Surveillance (ICNS)*, April 2016, pp. 1C3–1–1C3–9.

[28] R. N. Akram and K. Markantonakis, "Challenges of security and trust of mobile devices as digital avionics component," in *2016 Integrated Communications Navigation and Surveillance (ICNS)*, April 2016, pp. 1C4–1–1C4–11.

[29] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key Agreement Protocols and Their Security Analysis," in *Proceedings of the 6th IMA International Conference on Cryptography and Coding*. London, UK: Springer-Verlag, 1997, pp. 30–45. [Online]. Available: http://portal.acm.org/citation.cfm?id=647993.742138

[30] C. Mitchell, M. Ward, and P. Wilson, "Key Control in Key Agreement Protocols," *Electronics Letters*, vol. 34, no. 10, pp. 980 –981, May 1998.

[31] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC, October 1996.