 DOI: https://doi.org/10.12345/gcjsygl.v5i12.7766

Discussion on the Security Risk Analysis and Preventive Measures of the Radio and Electronic Internal Communication Network in Civil Aviation Aircraft

Haoran Tang

AMECO, Chengdu, Sichuan, 610000, China

Abstract

With the development of science and technology, more advanced technologies are available, more and more problems answered, also become more and more convenient people's life, especially travel, advanced science and technology makes travel no longer difficult, especially in the field of civil aviation aircraft, the development of wireless communication network to further improve the safety of the aircraft Although the wireless communication network technology is not particularly mature compared with the previous wired data transmission, but due to the shortcomings of wired data transmission has been gradually exposed, so it is necessary to promote the radio electronic internal communication network (WAIEC) research This paper mainly through the research of WAIC network technology, for its security issues are studied and analyzed, and the corresponding risk countermeasures are made.

Keywords

civil aviation aircraft; radio electronic intercommunication; network security; preventive measures

浅谈民航飞机无线电电子内部通信网络的安全风险分析及防范措施

唐浩然

北京飞机维修工程有限公司，中国·四川 成都 610000

摘　要

随着科学技术的发展，更多先进的技术得以问世，更多的难题得到了解答，人们的生活也变得越来越便捷，尤其是出行方面，先进的科学技术使得出行变得不再困难重重，尤其是在民航飞机领域，无线通信网络的发展使得飞机的安全性得以进一步提高。虽然较以往的有线数据传输，无线通信网络技术还不是特别成熟，但是由于有线数据传输的短板已经慢慢被暴露出来，所以需要促进对无线电电子内部通信网络（WAIC）的研究。论文主要通过对 WAIC 网络技术进行的研究，针对其安全问题进行研究分析，并且对相应的风险做出应对措施。

关键词

民航飞机；无线电电子内部通信；网络安全；防范措施

1 引言

航空电子技术的发展对民用航机来说意义重大，其发展促进了民用航机性能的进一步提升，对民用航机的安全做出了重大保障。同时，民用航机的自动化水平也随之提高。为了机载电子设备通过机载电子系统的数据总线进行数据传输。目前，进一步减轻重量，降低成本，提高飞行器的安全性与可靠性，使用无线局域网技术来替代大部分有线通信，是未来的发展方向之一。

目前，无线电子通信技术在应用方面也存在一些问题。特别是无线局域网技术的安全性成为安全的焦点。民航作为将安全高于一切的作为准则的行业，更加需要解决安全性的问题。

2 民航无线电通信系统

民用航空的通信一般分成两个：前舱通信和后舱通信。前舱包括：机载与地面无线通信、飞机与飞机之间的通信、

【作者简介】唐浩然（1985-），男，中国四川成都人，本科，工程师，从事民航飞机电子电气维修、民航飞机维修基本技能培训等研究。

 DOI: https://doi.org/10.12345/gcjsygl.v5i12.7766

雷达测控、飞行控制等；后舱主要是乘客上网。

2.1 前舱通信

民用航空的前舱通信都是专用频谱、专用系统、专业设备，一般来说都是飞机制造商集成第三方通信系统。例如，空客都是集成欧洲各大专业通信公司产品，一般不会开放给第三方，连民用机场的通信指挥系统、雷达系统、监测系统都是这些公司垄断，几乎不可能采用移动网络设备商 (爱立信 / 诺基亚 / 华为 / 中兴) 的产品 [1]。一方面航空通信设计低、中、高频段低语音、数据、雷达等复杂设备的小规模设计和集成，另一方面普通的通信设备商不理解民用航空的业务流，而民用航机和机场都需要一个完整的系统，通信设备只是一小部分。

2.2 客舱卫星通信

当前民用航空的后舱通信基本上是 offline 或者卫星通信，世界上大部分航班不提供乘客数据业务，以前提供卫星电话的费用也很贵。随着民用航空竞争的加剧，中东土豪航空公司 (阿联酋航空 / 卡塔尔航空 / 土耳其航空等) 开始普及机上数据通信，这带动了欧洲几大航空公司也开始提供机上数据通信；而美国航机的乘客数据通信也很早就有提供，但是以收费为主。民用航空的后舱数据接入主要是卫星回传，在低轨道高通量卫星商用之前，卫星数据宽带非常昂贵，所以机上乘客通信免费的数据带宽都很小，基本上只能发发文字和小图片，有保障的数据接入费用非常高。美国有家公司建设几百个 CDMA 基站覆盖大部分美国本土主要航线，相对低成本提供数据回传，但是由于 CDMA 带宽有限 (几 Mbps)，机上数据体验不好，这家公司目前计划升级到 LTE 网络 [2]。欧洲德电联合诺基亚也计划建设一张覆盖欧洲大部分航线的 LTE 网络，并已经建设了部分。

3 无线通信网络中存在的安全风险

3.1 被动攻击

主要有监视明文、揭秘通信数据、口令嗅探和通信量分析四种。

监视明文主要是获取在通信传输中未被加密的信息；解密通信数据则是通过密码分析，破解网络中传输的加密数据；口令嗅探即捕获用于各类系统访问的口令；通信量分析是通过对外部通信模式的观察来获取关键信息。

3.2 主动攻击

主动攻击又分为修改传输中的数据、信息重放、会话拦截、伪装成授权的用户、拒绝服务等，由于是无线通信网络，要是安全防范措施不到位，很容易受到攻击，有心术不正者可能会利用非法 AP 进行中间人欺骗攻击，及时采取了 VPN 等保护措施也难以避免这种攻击行为，中间人攻击则对授权客户端和 AP 进行双重欺骗，进而对信息进行窃取和篡改。更有甚者，还会利用系统软件中的漏洞、恶意代码、缺陷等等对系统进行攻击，对客户信息造成威胁。

3.3 临近攻击

邻近攻击是指未授权者可物理上接近网络、系统或设备，从而可以修改、收集信息，或使系统拒绝访问。接近网络可以进入或公开秘密，也可以是两者都有。一般分为三种：第一种是攻击者通过漏洞获取系统管理权，从而修改或窃取信息如登陆者的 IP 地址、用户名密码等等；第二种是攻击者获取系统的访问控制权，进而干涉系统的正常运行；第三种是对设备进行物理破坏，一般是攻击者获取了系统物理设备访问权。

4 攻击手段及其应对措施

在民航飞机无线电电子内部通信网络中，最容易遇到的事信息重放与网络窃听、信道堵塞、安全协议攻击、物理安全攻击等，下文将针对性的对应对措施进行阐述 [3]。

4.1 信息重放与网络窃听

面对此类主动攻击，最好的办法就是对数据进行加密。但是存在能量的消耗不当问题，或者占用资源的资源过多等问题。而且传统网络的公密钥机制，需要一个中心节点来进行统一的密钥调配，但在 WAIC 中，有许多的节点的地位是相同的，不存在一个真正的中心节点，因此不可能使用公密钥的方法。因此应使用一些轻量级的加密算法。

4.2 应对信道堵塞

因为 WAIC 尚处于研究阶段，针对信道堵塞还没有具体的解决方案，只能通过相关的协议设计，尽量去避免问题的发生。

4.3 应对安全协议攻击

因为需要满足无线网络自身的特殊需求，所以其本身的安全协议是存在一定的局限性的，所以使用者在使用之前需

 DOI: https://doi.org/10.12345/gcjsygl.v5i12.7766

要对安全协议进行充分的了解。另外，因为 WAIC 系统需要满足内部四种应用类型的不同速率不同信道的数据传输，所以可能需要采用不同的无线通信协议，因此在不同的层次，不同的协议，合理的使用相应的安全控制方案，做到这点是极其重要的。

4.4 应对物理安全攻击

针对物理攻击，外来侵犯者可以从各种可能的渠道获得相关的物理设备，然后进行破坏，所以就需要对相关工作人员进行相关的专业培训，尤其是网络安全的培训，工作人员需要具备足够的网络安全意识，并且最基本的是要懂得相关的网络安全技术。同时相关单位需要加强安全审核制度的力度，加强相关检查审核力度，才可能最大程度地保证 WAIC 系统的安全。另外还需要社会工程学攻击，这两者交集甚多，需要结合考虑。

4.5 针对程序安全攻击

针对程序安全攻击，最主要也是首要的就是需要程序开发者在开发阶段就考虑到程序可能面对的攻击手段，并且有针对性地做出相应的设计来应对这些攻击，以此保证程序的安全性。由于现在都需要进行敏捷开发 [4]。这就对构建一个完整的安全体系造成了困难。而且敏捷开发的两个重要的原则：

①能用的软件时最主要的进度标准。

②经常交付可以工作的软件，交付时间越短越好。

由于开发时间较短，相关的网络安全团队很难根据软件可能面对的攻击进行全方面的考虑，可能会有漏洞，所以在进行设计时，程序的可靠性是一方面，另一方面还需要针对程序的可拓展性展开设计，方便下一次迭代时能够保证下一个开发周期的安全需求。并且在软件实施期间，需要针对攻击事件进行记录，以便设计师能根据这些数据进行分析，找出系统的漏洞，提供相应的补丁，或者在下一个开发周期时修复这一漏洞。

5 结语

现阶段，大数据时代来临，科技发展进步的同时，面对的危险也逐步提升，WAIC 利用无线网络系统来代替有线的数据传输，虽然可以极大地减少线路短路或线路缺陷等导致的事故，对于飞机的运营来说有极大的好处，同时减少飞机的重量，但是相关的网络安全问题不容小觑，论文只是简单介绍了 WAIC 可能面对的安全风险，以及相关可能的应对措施。相信随着技术的进步，随着越来越多专业人士对于此研究的深入，在不久的将来，安全性可靠性能够得到更好的解决，WAIC 能被更多的投入使用，为人类造福。

参考文献

[1] 付海涛 . 浅析民航网络信息系统的安全防范措施 [J]. 数字通信世界 ,2017(10):49.

[2] 张彦 . 民航无线电通信干扰分析及防范此类干扰的对策研究 [J]. 数码世界 ,2019(3):35.

[3] 鲁霞 , 何欢 , 胡仲殊 , 等 . 网络安全风险分析及运维防范措施 [J]. 网络安全技术与应用 ,2017(1):19-20.

[4] 赵明川 . 浅谈民航无线电干扰的防范 [J]. 电子制作 ,2017(16):84-85.