EMERGING WIRELESS TECHNOLOGIES TO IMPROVE AIRBORNE AVIATION SECURITY

Lori J Brown
Western Michigan University, College of Aviation

Keywords: *In-flight, Wireless technologies, Communication Systems, Security, Aviation*

Abstract

Wireless communication has changed the dynamics of the working environment and workforce mobility. Without being tethered to a fixed location, a wireless terminal can be concealed from passengers in a commercial aircraft. This provides a tight and discreet connection between pilots and flight attendants to improve aviation safety. For this purpose, the in-flight wireless communication system should be specified according to requirements in size, ease of operation, robustness, durability, fault tolerance, security, and cost effectiveness. In addition, it is important to consider end device localization and radio frequency interference with aviation navigation.

1.0 Introduction

Several platforms for wireless ad hoc and sensor networks can be utilized and tailored for an in-flight discreet wireless communication system. A low-rate wireless network can be a good start towards a cost effective solution. These network standards and specifications include ZigBee over IEEE 802.15.4 for embedded sensing, medical data collection, and home automation, WirelessHART for industrial applications like process monitoring and control, IEEE 1451 for smart sensors, and EnOcean for wireless communication in building automation [4].

A wireless sensor network requires end node miniaturization and energy efficiency. These are also objectives of the proposed in-flight wireless system. A wireless communication device used by the flight attendant should be small enough to fit into a pocket or be disguised, for example, a collar decoration. This makes it necessary to employ current technologies of wireless system-on-chip transceivers and compact form factor antennas. To make the system robust- either the communication links should be established at all times, or a self-test should be performed regularly to ensure the pilots that the end devices are on standby and functioning properly. However, the end devices are not allowed to consume energy aggressively in order to sustain long hours of commercial flight. This makes radio front-end design and network power management challenging [4].

2.0 Improved Communication needed between the Cabin and Flight Deck

Communication gaps have been cited as causation factors in fatal accidents, such as, Dryden [5], and Kegworth [10] (1989), ValuJet [12] (1996), and Helios [8] (2005). Most recently, the failed bombing attempt of Northwest Airlines flight 253 (2009) raised questions of gaps, which impeded communications between the cabin and flight deck. The US Federal Aviation Administrator (FAA) Randolph Babbitt, indicated that the pilots of Northwest Airlines Flight 253 were not alerted that a passenger had tried to ignite a bomb on the flight. The pilots stated they had a problem, only after landing in Detroit, Michigan [3, 9].

Babbitt (2010) told a House subcommittee [9]:

There was a communication gap between the cabin and the flight deck crew, which left pilots unaware that there had been an alleged bombing attempt on-board. The flight deck crew reported they had someone who had attempted to set firecrackers off, so it didn't elevate to anyone — whether it was the cockpit or air traffic control — to anything of great seriousness at that point.

Air traffic controllers did not divert the aircraft to a remote location, "nor did the cockpit get very excited about it," Babbitt said [9]. When the aircraft was on the ground, pilots and airport personnel became aware of the bomb. Minutes and seconds lost in communication gaps, are valuable to communicate with ground operations, warn other aircraft in the air, or land the aircraft.

Resolving in-flight security threats of this type, typically involves four main stages: [11]

- Identifying the threat and notifying affected agencies
- Sharing pertinent information and collaboratively assessing the severity of the threat
- Deciding on and carrying out the appropriate in-flight response, such as initiating a diversion
- If necessary, completing the law enforcement response when the flight has landed

Options for response to an in-flight security threat include either (1) ordering the aircraft to divert from its flight plan by denying it access to U.S. airspace or requiring it to land at a U.S. airport different from its intended destination, or (2) launching military fighter jets to monitor or intercept the aircraft [11]. Although only a small percentage of in-flight security threats are serious enough to divert aircraft from its original destination, it is imperative that correct information relayed in a timely manner.

Crew communications and coordination are critical as they relate to the survival of all onboard and the overall control of the aircraft, and is the primary point of failure during live situational scenarios.

As reported to the committee on homeland security (July, 2012). On May 22, 2012 a French language translator on US Airways flight 787 from Paris, France to Charlotte, North Carolina encountered a female passenger with an alarming note written in French. Indicating, "She was coming to the U.S. to ask for assistance in saving her life. The note claimed said she had been used as a guinea pig by doctors for the past 10 years, and that she had undergone surgery against her will. She believed that she had been surgically implanted with a device that was out of her control. She said she was afraid to return to France and afraid for her safety because of things she had written" [14].

After the note was translated the flight attendant shared the note with the other flight attendants and captain. The passenger had indicated she thought she may have been surgically implanted with a device which may cause harm. After two medical professionals examined her, the determined it was unlikely she actually had some device implanted. They also believed the scars looked more like ones resulting from an accident and not from a recent surgery. Their joint assessment was that there was nothing visible or tangible to indicate she posed any threat [14].

The passenger was restrained and the3 flight was diverted to Bangor, Maine.

Once on the ground in Bangor immigration/customs officers came on and removed her via the aft left aircraft stairs. They took all her belongings with them. Once she was removed, the captain came on the PA system and explained the real circumstances to the passengers. The FBI came on and took my statement, and the flight eventually continued on to Charlotte, NC USA.

The flight attendants indicated to the committee of homeland security (July, 2012), "we addressed the situation that day the best we could given our limited resources in the operational environment. Fortunately, the threat we encountered did not involve a terrorist; if it had it would have probably ended tragically."

The aircraft in the incident was an older Boeing 767, with the only way to communicate during the event to the authorities was through the flight deck headset. When the flight attendant was recounting the information from the doctors about the exam to our ground support group I had to use the headset in the flight deck [14].

The Association of Flight Attendants (AFA) has supported the development of discreet, secure, hands-free, wireless communications systems, as authorized by the Homeland Security Act of 2002, as one means to prevent a potentially catastrophic security breach by terrorists. The device will allow all crewmembers the ability to communicate from anywhere in the aircraft at any time under any circumstance [14].

Each personal device must have capability for encrypted, bidirectional communications to allow plain language communications during crisis situations; this will ensure security and reduce confusion.

This is yet one more example of how difficult it is for flight attendants to communication with pilots' inflight via the interphone. More importantly how crucial a wireless device could be in saving the lives of many in such events which continue to threaten security.

A device that is discreet, or as small and innocuous as possible, could allow all crew members to carry on their person the ability to communicate from anywhere in the aircraft. Each personal device must have capability for encrypted, bidirectional communications [3,4].

The International Transport Workers Federation and the Association of Flight Attendants has called for security of the system through use of dedicated hardware components that are accessible only to authorized personnel such as crew members and, potentially, any active law enforcement officers who may have presented credentials to the crew prior to the flight. The hands-free concept will allow crew members under both general emergency (e.g., medical crises, emergency evacuations) and security threat conditions to use their hands to protect themselves, the cockpit, other crew members, passengers, and the aircraft while continuing to coordinate and communicate with the cockpit, the ground, and the rest of the crew. A device possessing such characteristics must be wireless [3, 4, 15].

Currently, the only communication device available for the flight attendants, air marshals, and the flight deck crew, is the aircraft interphone. The interphone, typically used for public announcements and normal communication between the cabin and flight deck, is usually located in the forward or aft cabin [1, 7]. This isolated location, may limit the flight attendants' ability to reach the interphone, especially during busier phases of flight [4]. Aircraft interphones have been proven easily rendered inoperative (9/11 attacks and Operation Atlas [7, 8]. If the current system is disabled, the flight attendants would not be able to alert the pilots without alarming the hijackers or causing panic in the cabin. These minutes and seconds are very crucial, the pilots need as much warning as possible of a security breach, to attempt to land the airplane. The Association of Professional Flight Attendants [1] "strongly supports the need for hands-free wireless communication devices, which is not available through the current aircraft interphone systems, now mandated". Flight attendants spend much of their time in aircraft aisles away from interphones located in service galleys and near their jump seats. "A flight attendant who suspects a security breach and is working in the cabin could potentially be half the distance of the aircraft away from notifying the flight crew of the threat" [1,3,4].

3.0 Research Required

Research is required to evaluate these novel tools and approaches to confront homeland security issues. Studies are necessary to: 1.) Identify breakthrough technologies to mitigate the likelihood of individual radical and/or violent behavior, resulting in catastrophic airline casualties, and 2.) Understand whether the Crew Alert Monitoring System and other technologies can provide discreet communication to the cockpit, and allow the pilots more time to land the airplane, in the event of a security breach or other compromising emergency in the cabin, and 3.) Identify any radio interference and possible operational issues with crew and passengers in ground tests onboard transport aircraft.

4.0 Technology Considered

Several platforms for wireless ad hoc and sensor networks can be utilized and tailored for an in-flight discreet wireless communication system. A low-rate wireless network can be a good start towards a cost effective solution. These network standards and specifications include ZigBee over IEEE 802.15.4 for embedded sensing, medical data collection, and home automation, Wireless HART for industrial applications like process monitoring and control, IEEE 1451 for smart sensors, and EnOcean for wireless communication in building automation [4].

A wireless sensor network requires end node miniaturization and energy efficiency. These are also objectives of the proposed in-flight wireless system. A wireless communication device used by the flight attendant should be small enough to fit into a pocket or be disguised, for example, a collar decoration. This makes it necessary to employ current technologies of wireless system-on-chip transceivers and compact form factor antennas. To make the system robust- either the communication links should be established at all times, or a self-test should be performed regularly to ensure the pilots that the end devices are on standby and functioning properly. However, the end devices are not allowed to consume energy aggressively in order to sustain long hours of commercial flight. This makes radio front-end design and network power management challenging [3, 4].

The in-flight wireless system should tolerate fault alarms caused by mis-operations and support bidirectional communications for the flight attendants to receive the pilots confirmation. It should also be secure against any intentional or unintentional system breakthrough. To achieve these, ultra-low power digital signal processors can be embedded to play an important role of implementing sophisticated coding and signal processing algorithms [4].

STG Aerospace of U.K. has developed a wireless, discreet cabin alert system to enable the crewmembers to alert the flight deck of a security breach [2, 3,4]. The system provides the flight crew with an audible alert, coupled with a visible cockpit annunciation signal. The signal will indicate an alert, while giving a "zonal" location. The system also includes a door intercom to provide the additional audio communication between the cabin and the flight deck sides of the cockpit door [2, 3, 4].

The purpose of this system is to provide the following functionality [2, 3, 4]:

1. When a person authorized to access the cockpit seeks entry, the existing visual identification through the cockpit door, coupled with a new audio intercom confirmation that the door area is clear.
2. In the event of an attack on a cabin crewmember, or other security breach in the cabin, a system is provided to enable the cabin crew to alert the flight crew of the emergency event, this will be achieved by using discreet wireless “Panic Buttons” provided to the crewmembers.

3. The communication and alerts recorded onto the cockpit flight recorder can be relayed from the flight deck to: the relevant Security Operations Center; Air Traffic Control National Hostage; Rescue Team and local crisis response teams; Local Airport Emergency Responders;

and Military responders. This technology will allow effective communication, while keeping the cost and weight to a minimum to meet the economic constraints of U.S. Airlines, as well as other potential users [11].

4.1 Crew Alert Monitoring Device (CAMS)

The STG Aerospace Crew Alert Monitoring device (CAMS), a wireless device that is an ultra- secure cabin alert and monitoring system, using small donut shaped alarm units held on person of each cabin crew, or FAMS, which, when activated, sends an alarm signal to the cockpit, effectively warning them of trouble, and the expectation of escalation of that trouble to the cockpit [2, 11]. The STG Aerospace technologies, the first of its kind, were well positioned in 2001, just after the September 11th terrorist attacks in the United States. Unfortunately aircraft manufactures and airlines have yet to install such devices. The signal also tells the cockpit where in the aircraft the alarm was triggered, and therefore an indication of the time, which may be available to them to undertake appropriate actions before attempts at intrusions to the cockpit. The system also provides a means of voice communication between cabin crew and pilot at the cockpit door, and combined with the use of the door peephole provides the pilots with a good means of monitoring if anyone wishing entry to the cockpit is under stress and possible coercion. The system is aircraft specific, extremely secure, has 'designed in' safeguards against inadvertent activation, and meets all the needs of those most closely affected - the pilots, cabin crew and passengers.

The system also includes a flight deck door intercom to provide the additional audio communication between the cabin and the flight deck sides of the cockpit door as recommended in previous proposed rules making in the United States. The audio link will be combined with the currently installed video or door viewer, whichever is installed [2, 4].

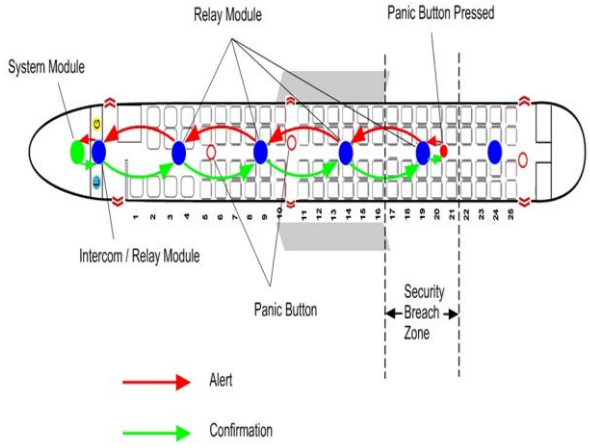

Fig. 1 Inflight Wireless System(STG Aerspace)

The system consists of four parts (Fig. 1):Panic Button, System Module, Relay Module. And Intercom.

4.1.1 Description of device

1. A CAMS panic button is to be carried by crewmembers to provide discreet alert.

2. A CAMS System Module (CSM) placed in the cockpit by the entry door, providing audio communications to the intercom along with audible and visual alerts when a panic button has been activated.

3. CAMS Relay Modules (CRM) to act as wireless transceivers for propagation of the alert signal through the aircraft. The designs of these will mimic that of the
CAMS System Module, but will be installed out of sight in the cabin ceiling area.

4. A CAMS Intercom unit for outside the cockpit door area, to provide audio confirmation. This is coupled with the existing visual confirmation provide by video or through the door viewing device. The CAMS system will have a specific aircraft ID to stop interference between adjacent aircraft systems on the ground. There will be 2048 possible IDs available, allocated at installation. This means that the probability of two aircraft having the same

specific ID is over four million to one and the probability of one having an incident or test while the other aircraft is close enough is a multiple of that figure [2, 4].

4.1.2 Radio Frequency Performance Testing

The CAMS uses a 2.4GHz spread-spectrum radio transmission to send a signal from the panic buttons worn by the cabin crew. The same radio channel is used to signal the panic button location from the receiver points in the cabin roof to the control panel in the cockpit. It is crucial that we the technical capability of such wireless systems and the ability to provide useful and reliable information in an operational environment [2 ,4].

A number of radio frequency measurements and tests of the equipment will be required[5].

1. To validate the operation of wireless communication systems in an aircraft cabin
2. To investigate the operational safety margins in normal use (i.e. how much excess signal strength is provided when body shadowing etc. is present)
3. To confirm, via analysis and ground test, non-interference with the aircraft communications and navigation systems
4. To investigate the potential for harmful interference from the aircraft and passenger electronic devices
5. To investigate the performance differences between a lightly-loaded and heavily occupied cabin

4.1.3 Analytical Approach

The radio measurement tests will be carried out in two environments, a test aircraft, and the cabin simulator. The test aircraft is representative of a large passenger aircraft with operational communications and navigational aids, but necessarily will not be available for long periods with different patterns of passenger seating. The cabin simulator gives considerable flexibility for changing the loading of the cabin section and investigating the effects of local shadowing (masking) of the radio signal as the position where the panic buttons are worn are altered [3, 4, 8].

4.1.4 Aircraft tests recommended

It is suggested that a CAMS or other wireless system is temporarily installed in a test aircraft. A series of tests to examine coverage will be defined in a test plan and approved by the aircraft operator before the test. This will include test items such as [2, 4]:

1. Confirmation of operation in all zones of the aircraft
2. Mapping the accuracy of zone identification dependent on position of the initiating panic button in the aircraft, different positions of the panic button on the wearer.
3. Using a modified wireless cockpit unit to indicate the signal strength received by sensors
4. Operation of communication devices and navigational instrument when operating the wireless system to detect potential interference.

4.1.5 Analysis of interference

The potential for the wireless system to generate interference to aircraft systems will be studied using the guidelines laid out in RTCA DO-294B Guidance on Allowing Transmitting Portable Electronic Devices (T-PEDS) on Aircraft and RTCA DO-307 - Aircraft Design

and Certification for Portable Electronic Device (PED) Tolerance [2, 4].

In addition, the potential for a T-PED or other device to interfere with the operation of the CAMS system will be investigated.

A report will be produced outlining the results of the interference investigation and any further tests will be defined for running on the aircraft simulator [2,4].

4.1.6 Aircraft simulator tests

A second wireless or CAMS wireless system should be installed in the aircraft simulator and used for the behavioral experiments. The Behavioral (human) Factors of this study are as follows:

- Identify how discreet the traditional means of communication between the cabin and the cockpit is;
- Identify how discreet the wireless communication between the cabin and the cockpit is;
- Identify the amount of time lapse between the trigger event (security breach) and effective communications from the cabin to the flight deck, when using the intercom method.
- Identify the amount of time lapse between the trigger event (security breach) and effective communications from the cabin to the flight deck, when using the wireless communication method.
- Identify effectiveness of door entry procedures: The first will involve the traditional interphone method and a second method would involve visual identification of the door area, coupled with an audio confirmation procedure. Through a viewing device installed in the flight deck door, one person on the flight deck would view the door area and identify the person seeking access. Then a crewmember would provide audio confirmation that the door area is clear while viewing the outside door area. For example, before providing audio confirmation to the flight deck, the crewmember would assure that no passengers are standing near the door area, and. that no passenger is in any forward lavatory.
- Test security levels 1-5 and procedures for use

In addition to the behavioral experiments, a series of tests will need to be run to examine any change in operation with different cabin occupant loading. The aircraft simulator represents a portion of a single-aisle cabin, and consequently the results of tests can be compared and verified against a single (e.g. front) section of the main aircraft tests [2,4].

RF tests in the aircraft simulator include items such as [2, 4]:

1. Investigation of the signal strength margin fully loaded and lightly loaded with passengers
2. Investigation of the ability to interfere with the wireless system using a T-PED such as a wireless laptop connection
3. Investigation of the ability to interfere with the system using a purpose-built interferer [2,4].

5.0 Conclusions and Future Work

As wireless networks evolve over time, there is an increasing interest in combining location awareness with communications. The fastest growing area of location awareness applications is in wireless local and personal area networks. Localization techniques for wireless networks can be leveraged to improve the effectiveness of the in-flight wireless communication system. Upon receiving an alert from the cabin crew, the pilot should be able to locate the flight attendant who initiated the

signal for appropriate response and notifying others of the troubled zone [4].

The wireless sensor networks, for example those under the IEEE 802.15.4/ZigBee standard, operate on unlicensed frequency bands of 868.0-868.6 MHz in Europe, 902-928 MHz in North America, and 2400-2483.5 MHz worldwide. Beyond these three bands, the IEEE802.15.4c study group is considering the newly opened 314-316 MHz, 430-434 MHz, and 779-787 MHz bands in China, while the IEEE 802.15 Task Group 4d is defining an amendment to the existing standard to support the new 950 MHz-956 MHz band in Japan. In order to minimize interference with existing aviation radio, the proposed in-flight wireless communication system operates on the 2400-2483.5 MHz industrial scientific and medical (ISM) band [4, 6]. This should not cause considerable interference with the current five navigation frequency bands: Very High Frequency (VHF) Omni-directional Radio Range (VOR) and Instrument Landing System (ILS) Localizer, 108-118 MHz; ILS Glide Slope, 329-335 MHz; Distant Measuring Equipment (DME); Traffic Alert and Collision Avoidance System, 960-1215 MHz; and GPS, 1227.5 and 1575.42 MHz. Europe is getting ready for a decision on the final phase of the deployment of 8.33 kHz radios. Their mandatory use in all European airspace by 2018 would solve the long-standing European frequency shortage problem [4. 6].

References

[1] Air Safety Week. Modified cockpit security measures proposed. *ASW*, 2007.

[2] Braithwaite S, and STG Aerospace, Commercial in confidence, CAMS system description. STG Aerospace, 2008.

[3] Brown L, and Rantz B. The efficacy of flight attendant/pilot communication, in a post-9/11 environment: viewed from both sides of the fortress door. *International Journal of Applied Aviation Studies, (IJAAS)*, Federal Aviation Administration, Summer 2010.

[4] Brown, L., Cerullo, A., Dong, L., (2011). **Technology Engineering and Management in Aviation**, Chapter 11, IGI Global, Publishing, .Evon Abu Taieh (EDS).

[5] Dryden. Commission of inquiry into the air Ontario crash. *Moshansky*. Toronto, Canada, 1992.

[6] Eurocontrol. (2010). Communications, navigation and surveillance at the heart of the future ATM system. *Eurocontrol Skyway Magazine, (Winter, 2010).*

[7]Fleisher L. Terror response is tested 'OPERATION ATLAS'. *Boston Globe,* June 5th, 2005.

[8]Federal Aviation Administration. Communication and coordination between flight crew members and flight attendants. *Advisory Circular No. 120-48*. 1992.

[8]Greece. Aircraft accident report. Helios airways flight HCY522, Boeing 737-31S. AAIBSB, Accident investigation report, 2006. Retrieved from: http://www.skybrary.aero/bookshelf/books/1170.pdf

[9]House of Transportation and Infrastructure Committee Aviation Subcommittee Representatives. *The agency's call to action on airline safety and pilot training. Congress, Feb. 04, 2010.*

[10]Kegworth Great Britain. *Report 4/1990, on the accident of boeing 737-400. The Department of Transport, Air Accidents Investigation Branch*. United Kingdom, 1989.
http://www.aaib.gov.uk/publications/formal_reports/4_1990_g_obme.cfm.

[11] Seidenstat P, and Splane, F. (Eds.) Onboard security. *Protecting Airline Passengers in the Age of Terrorism*. Greenwood Publishing, 2009.

[12]ValuJet. In-flight fire and impact with Terrain *Aircraft Accident Report***,** Flight 592. 1996.

[13]Western Michigan University. *Grant spurs groundbreaking aviation research.* 2010. www.wmich.edu/wmu/news/2010/04/069.shtml

[14] 89th Legislative AFA Affairs Chair, Colby Alonso, before The Committee on Homeland Security Subcommittee on Transportation Security U.S. HOUSE OF REPRESENTATIVES WASHINGTON, DC. July 10, 2012

[15]111th Congress, US transportation security information act, H.R. 2200, section 235. *House report on cabin crew communication.* 111-123, Library of Congress, GPO, 2010.