ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/332569983

A Review of Recent Advances and Security Challenges in Emerging E-Enabled Aircraft Systems

Article *in* IEEE Access · April 2019

DOI: 10.1109/ACCESS.2019.2916617

CITATIONS
0

READS
257

6 authors, including:

Farooq Shaikh
University of South Florida
5 PUBLICATIONS **16** CITATIONS
SEE PROFILE

Mohamed Rahouti
University of South Florida
14 PUBLICATIONS **31** CITATIONS
SEE PROFILE

Kaiqi Xiong
University of South Florida
113 PUBLICATIONS **1,857** CITATIONS
SEE PROFILE

Elias Bou-Harb
University of Texas at San Antonio
85 PUBLICATIONS **785** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Sensors for Suspicious Behavior View project

Software-Defined Networking for Smart City Communication Systems View project

All content following this page was uploaded by Elias Bou-Harb on 23 April 2019.

The user has requested enhancement of the downloaded file.

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

A Review of Recent Advances and Security Challenges in Emerging E-Enabled Aircraft Systems

FAROOQ SHAIKH[1], MOHAMED RAHOUTI[1,4], NASIR GHANI[1,3], (Senior Member, IEEE), KAIQI XIONG[2,4], (Senior Member, IEEE), ELIAS BOU-HARB[5,6], and JAMAL HAQUE[7]

[1]Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: fshaikh@mail.usf.edu and mrahouti@mail.usf.edu)
[2]Cyber Florida and Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620 USA (e-mail: xiongk@usf.edu)
[3]Department of Electrical Engineering and Cyber Florida, University of South Florida, Tampa, FL 33620 USA (e-mail: nghani@usf.edu)
[4]Intelligent Computer Networking and Security Lab, University of South Florida, Tampa, FL 33620 USA
[5]Department of Computer Science, Florida Atlantic University, Boca Raton, FL 33431 USA (e-mail: ebouharb@fau.edu)
[6]Cyber Threat Intelligence Lab, Florida Atlantic University, Boca Raton, FL 33431 USA
[7]Honeywell, Tampa, FL USA (e-mail: Haque@honeywell.com)

Corresponding author: Nasir Ghani (e-mail: nghani@usf.edu).

We would like to acknowledge the National Science Foundation (NSF) who partially sponsored the work under grants #1633978, #1620871, #1620862, #1651280, and BBN/GPO project #1936 through NSF/CNS grant. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied of NSF.

ABSTRACT The continued increase in air traffic along with airline operators gradually adopting IP-based network technologies has led to the transformational concept of e-Enabled or "connected" aircraft. This new framework envisions a single aeronautical communications architecture connecting across the entire spectrum of the aviation sector. However, due to the complex and multidimensional nature of aviation operations, no single technology can achieve the above goal. Instead, building an integrated system which uses multiple communication protocols and architectures, as well as cloud computing and big data analytics, is the most promising way forward. Hence, this paper surveys the latest trends in emerging network communication systems for commercial aviation. A range of cyber-threats are then identified for the e-Enabled aircraft paradigm, along with discussions on related solution methodologies. Note that military aviation security are not considered here.

INDEX TERMS Security, connected aircraft, e-Enabled aircraft, aircraft communication, threats.

I. INTRODUCTION

Aircraft communications is evolving from a conventional radar-based setup to a highly-networked framework via the gradual infusion of many wireless communication technologies, e.g., such as satellite communications (SATCOM), Wi-Max, L-band Digital Aeronautical Communication Systems (LDCAS), Automatic Dependent Surveillance-Broadcast (ADS-B), Aeronautical Mobile Airport Communication System (Aero-MACS), etc. In this new e-Enabled aircraft paradigm, it is envisioned that all key aviation applications and services will be connected to a single integrated communication system built using a range of technologies, e.g., Internet Protocol (IP) networking, global positioning system (GPS) satellites, and other radio frequency (RF) systems. In particular, notable evolutions here include the Next Generation Transport (NextGen) framework being pushed by the U.S. Federal Aviation Administration (FAA) and the Single European Sky ATM Research (SESAR) framework being developed in Europe. Overall, both of these architectures are being designed to provide high-performance air traffic management (ATM) capabilities.

Overall, the key goals of the e-Enabled aircraft paradigm are to provide a more efficient, reliable and safe flying experience and improve the cost efficiency of airline operations. Now, security has always been one of the strong suits of the aviation sector, i.e., owing to the use of proprietary technologies, software, and a range of stringent standards, protocols, and procedures. However, the deployment of new technologies here will inevitably increase the vulnerability of aircraft-based communications to a range of cyber-attacks from different adversaries. Hence, it is critical to understand and address these concerns. Indeed, a preventive rather than

FIGURE 1: Road map of the paper

reactive strategy is the most prudent here. Along these lines, this paper reviews existing communication setups for the aviation sector and highlights the key trends and technologies in emerging next-generation paradigms. A range of security concerns are then highlighted. Note that there is also strong (and growing) interest in new unmanned aerial systems (UAS) for commercial airspace. Hence, some related concerns are also discussed briefly.

The rest of our survey paper is organized as follow and it is also shown in Figure 1. Section II presents an explanatory and detailed overview of the current state of aircraft avionics. Section III then gives a detailed discussion of the e-aircrafts and commercial UAV systems. In Section IV we present a comprehensive overview about commercial aircraft communication and their networking technologies. Section V gives a taxonomic classification and detailed discussion about common security threats and issues in aircraft avionics. Finally, Section VI provides a review of recent advances in current aviation-related security research as well as open research challenges. We then conclude our surveying study in Section VII.

II. CURRENT AIRCRAFT AVIONICS AND DESIGN

It is important to first take a look at the design of avionic systems. Avionics represent an integral part of modern aircraft, and these electronic systems implement a wide range of functionalities including communications, navigation, display, monitoring, maintenance, radar, weather-related updates, etc. Even though flight safety is a very broad area now, one of its key aspects involves the secure operation of on-board avionics. However, increasingly, modern on-board networking systems are starting to interconnect passenger infotainment systems with previously-isolated aircraft information and control domains. This trend poses key concerns for avionics security, and hence it is important to review current and emerging setups in order to identify vulnerabilities.

Emerging next-generation aircraft displays and control suites are expected to provide reliable and expansive information views for aircraft crew, as well as terrestrial ATM operators. Namely, these systems will enable aircraft crew to view system-wide information as well as aid operators with air traffic monitoring. Additionally, future e-Enabled aircraft must also support fail-safe and maintenance-free avionics that leverage built-in control algorithms. Specifically, these

For Review Only

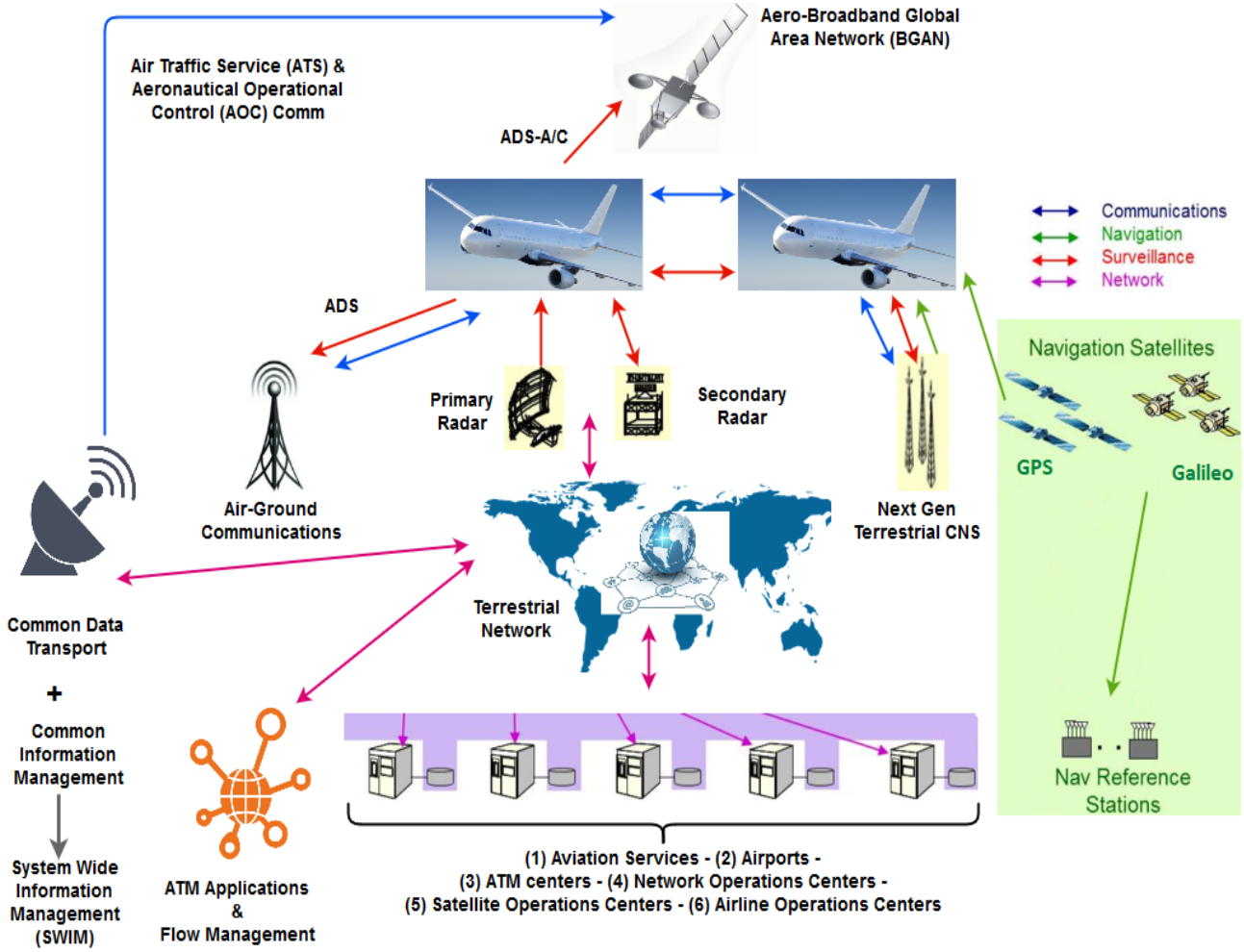

FIGURE 2: The communication infrastructure for e-Enabled aircrafts

designs will include a range of wired and wireless sensors and implement automated failure diagnostics to reduce human dependency (error) in fault detection and correction. The above are just some of the many functions envisioned for next generation avionic systems.

Now the typical (avionic) system design process consists of multiple interrelated procedures, i.e., ranging from requirements specification (by aircraft designers and operators), detailed software and hardware development, to final integration/testing. Functional hazard assessment (FHA) and failure-cause analysis are done at all levels of this process to ensure safe and reliable flight management. Overall, avionics software and hardware development is an iterative process involving failsafe architecture development via the synthesis of functional circuits to implement key system functions [1]. Indeed, many critical safety measures can be implemented here by introducing physical and functional redundancy, isolation and other methods. These designs are further evaluated at each stage of the development process using quality assessments. Finally, developers conduct detailed (hardware, software) integration testing of avionic systems on real aircraft before progressing to a wide range of acceptance tests, i.e., both on the ground and in in-flight.

Now many modern avionic systems make an extensive use of integrated commercial-off-the-shelf (COTS) microprocessors and systems on a chip (SOC) devices. These entities allow designers to implement a wide range of advanced capabilities in a modular and programmable manner. Moreover, these capabilities can be readily modified/adapted by various applications and even shared across multiple domains. Hence, COTS microprocessors and SOC devices are starting to replace discrete components (in legacy avionic designs). Furthermore, multi-core processors are also enabling major updates without the need for substantial system redesign, thereby improving functionality and lowering power/space overheads. However, on a broad level, the FAA (and most other national aviation agencies) have not provided any guidelines or policies regarding the use of COTS or SOC devices in avionic systems. Therefore, as these components become more prevalent, it is essential to develop a formal framework to assess their safety and airworthiness. Indeed these products/devices will likely be prone to the same set of

For Review Only

threats that they may face in other domains in which they are deployed.

Furthermore, carefully note that the overall aviation-based market for many COTS or secure operational environment (SOE) devices is relatively small as compared to other commercial sectors, such as telecommunications, consumer electronics and automobiles [2]. Moreover, applications in these sectors are less susceptible to anomalous behaviors resulting from internal and external events. More importantly, the consequences of any type of processor/chip failures are arguably much more pronounced in aircraft settings than any of these other aforementioned industries.

III. CONNECTED AIRSPACE: E-AIRCRAFT AND COMMERCIAL UAV SYSTEMS

Given the many advances in avionics technologies, it is important to review a typical flight sequence and the associated communication requirements during each stage. This background will play a key role in identifying any potential concerns and developing effective solutions to provide fast, reliable and secure aircraft-based communications.

A. BIG DATA ANALYTICS AND CLOUD COMPUTING

Increased bandwidth capacity and improved sensor/tracking devices in new e-Enabled aircraft paradigms will inevitably lead to a surge in the amount of data being generated. New pilot-focused applications (replacing traditional paper-based maintenance methods) will also add to these data volumes, e.g., Electronic Flight Bag (EFB). However, most aircraft-generated information, including avionics and sensor data, is largely underutilized today. Hence, airline operators are quickly moving to collect this vital information and use it to improve their operations via predictive analysis. As part of this process, it is crucial to transfer the bulk of collected data to large terrestrial datacenter locations, i.e., operating with abundant storage and processing resources. Indeed, this is where the concept of big data analytics and cloud computing comes into play to provide near real-time (if not real-time) situational awareness and much-improved decision support and resource efficiency. For example, an aircraft could continuously transmit black box data to help improve real-time route optimization, identify potential faults, and enhance flight safety. As a result, many aircraft manufacturers are already using a full range of sensors to collect critical information and conduct (off-line) machine learning analysis and optimization for flight routes, fuel costs, wait times, take-off and landing, etc. Along these lines, [3] proposed a scheme to correlate near real-time location information with archived data, thereby enabling predictive analysis of air traffic volume in an airspace region (which in turn improves overall regulation).

The integration of cloud computing into aviation and aerospace industries has been evolving for the past several years. Emerging cloud computing services such as Virtual Desktop Infrastructure (VDI), Policy engines, and Authentication as a Service (AaaS) have made a significant impact on avionic industries and are emerging research directions. For example, Yuan and Yanlin [4] proposed a cloud platform for general aviation flight service management. Majumder and Prasad [5] suggested a solution to control UAVs using cloud platform while permitting multiple users/controllers for a simultaneous communication with the aircraft. In order to achieve a practical applicability of cloud computing in ATM, technical cloud computing elements such as standardized working procedures and controller working position equipment for air traffic controllers have to be assessed. (interested readers may refer to Kampichler and Eier [6] for more details.

Overall, big data analytics and cloud computing technologies are transforming many sectors and various new applications are being developed today. However, the biggest constraint for implementing near real-time sophisticated and reliable data analytics capabilities in the aviation sector is the limitation of air-to-ground bandwidth, i.e., which restricts the collection of a full range of data. Nevertheless, looking ahead, a number of providers are starting to promise much-improved capacities. For example, Gogo's 2Ku service currently supports 5-6 Mbps download speeds, with future projections of up to 70 Mbps.

B. FLIGHT MANAGEMENT SYSTEMS (FMS)

Flight management systems (FMS) are an integral part of modern avionics and include some critical components, e.g., such as radar, navigator, engine control, etc. Increasingly, the latest advances in radar technologies are providing detailed "look-ahead" capabilities of up to 300 miles. Hence, there is further interest to harness this vast amount of information to build in-depth real-time weather maps. Namely, this data is of key importance to other aircraft flying in the vicinity and it can also assist air traffic control (ATC) in achieving more efficient aircraft tracking by correlating such data with ground-based navigation aids and GPS information.

Overall, emerging flight management systems (FMS) will have to integrate different communication architectures and protocols to achieve more efficient, reliable and safe flight performance. Namely, these systems are expected to implement a range of communication capabilities. Foremost, this includes data transfer support for key airline operations, e.g., for flight plans, weather, and text messaging between ground systems and the flight management computer (FMC), etc. In addition, a FMS must also support data transfers for critical navigation operations such as Controller Pilot Data Link Communications (CPLDC) with ATC, satellite-based Automatic Dependent Surveillance-Broadcast (ADS-B) functions, and other required navigation performance (RNP) tasks

for improved safety. As noted in [7], such a performance-based navigation (PNB) system can help improve operational efficiencies in terms of fuel cost, emissions and flight delays. Note that work in [8] has looked at the use of interactive navigation displays that integrate closely with an advanced FMS system to provide a more functional and convenient-to-use human machine interface.

C. END-TO-END CONNECTIVITY

Aircraft must maintain communications connectivity on the ground and in the air. Along these lines, the various standards and technologies in use and being evolved for each stage are discussed here.

1) Terrestrial Stage

The original Aeronautical Telecommunications Network (ATN) addressed some key sustainability issues surrounding the legacy Aeronautical Fixed Telecommunication Network (AFTN). In particular, this standard introduced a global ATM network for efficient air-to-ground and ground-to-ground communications and it has been widely deployed. However, as noted earlier, the U.S. FAA is actively moving to adopt improved wireless broadband technologies as part of its NextGen system. Similarly, the European SESAR 2020 project is also planning a series of research and trials with similar technologies across 24 major airports in the next few years.

Now clearly, terrestrial broadband networks will form a key part of these next-generation frameworks. In particular, the Aeronautical Mobile Airport Communication System (Aero-MACS) has been evolved to support high-speed ground-to-ground communications in airport settings [9]. This system operates in a licensed 5 GHz band spectrum and uses both mobile and fixed connectivity across a wide range of aviation applications. Initial testing by the FAA has shown that Aero-MACS can achieve an order of magnitude higher data rates than other approved wireless alternatives for on-the-ground communications during the taxiing, take-off, and landing stages [9]. Hence, this standard enables the interconnection of a large number of fixed-infrastructure elements, such as weather stations, sensors, radars as well as other mobile assets on the airport surface. As of now, this technology is being deployed in the National Airspace System (NAS) as an enabler to support the Airport Surface Surveillance Capability (ASSC) program, a multilateration system to reduce runway incursions. However, in the future, Aero-MACS will likely evolve to support improved mobile applications by transmitting key textual, graphical and video data directly to the cockpit. These applications can provide airborne access to system-wide information, weather in the cockpit, improved surface situational awareness and safety, surface traffic management, and a host of other air traffic control (ATC) and aeronautical operational control (AOC) applications [10].

However, in light of the high cost and complexity of adding new communications equipment to aircraft, the transition from surface to cockpit operation will likely be a gradual process. Moreover, this transition will require a collective effort from all key stakeholders, e.g., regulatory authorities, network equipment vendors, aircraft manufacturers, airlines, and the research and development community. Nevertheless, ongoing efforts within the USA and Europe to deploy/test Aero-MACS (such as NextGen and SESAR) are on track and will inevitably help establish new global standards for this system.

2) Airborne Stage

Currently the aircraft industry is still using analog voice signals for in-flight communication between pilots in the air and ground-based ATC setups. This communication is done using double-sideband amplitude modulation in the very high frequency (VHF) band from 118-137 MHz. Clearly this technology cannot scale to meet the needs of emerging e-Enabled aircraft. Hence, a major revamp of existing air-to-ground communication systems is required. Along these lines, the International Civil Aviation Organization (ICAO) has proposed to use the L band region from 960-1164 MHz to increase the available spectrum for radio navigation purposes and ensure streamlined integration with legacy systems [10]. This expansion will also provide much-needed capacity to support broader information transfers, e.g., for in-flight surveillance, weather prediction, etc.

Furthermore, satellite-based (SATCOM) systems are also vital for in-flight communication as they provide reliable and secure connectivity for aircraft over oceans and remote areas. Recently, Inmarsat has announced the launch of its GX Aviation system, which promises data rates of up to 50 Mbps over the Inmarsat-5s satellite launched in 2015 [11]. This capability will further complement the company's existing SwiftBroadband services running over its Inmarsat-4 satellites in the L band. Additionally, many other satellite providers (such as Irdium, Viasat and GoGo) are also looking to deploy more constellations to provide similar data rates, i.e., not only for in-flight passenger services but also for AOC and cabin operations.

D. UNMANNED AERIAL SYSTEMS

It is also important to mention the growing interest in UAS platforms for commercial applications. Currently, these systems are mainly being used for military operations and border protection. However, if recent developments are any indication, UAS platforms will move beyond the pursuit of hobbyists and evolve into more complex and sophisticated systems to support new civil and commercial applications,

For Review Only

e.g., surveillance and monitoring, data collection, aerial mapping, spectral and thermal analysis, even cargo delivery, etc. In fact, estimates for the U.S. project close to 13,000 UAS platforms in operation by 2025. Clearly, the introduction of such vehicles in congested national airspaces will only heighten security challenges. However, the related communication and airspace management architectures for UAS are not discussed here, and interested readers are referred to [12] for more details.

IV. COMMERCIAL AIRCRAFT COMMUNICATION AND NETWORKING TECHNOLOGIES

High-bandwidth communication and networking technologies will provide the underlying framework of future aviation networks [13]. As noted earlier, the aviation sector still relies on legacy communication systems and it is only in the past decade that notable efforts have been undertaken to move towards more data-centric communications. Some key related technologies are briefly reviewed here.

A. LOW-EARTH ORBIT SATELLITE NETWORKS

Geostationary satellite systems are being used to support a growing number of telephone and data users over the past two decades. Indeed, SATCOM technology has come a long way from its initial days, where it offered meagre speeds from 600 bps to 9 kbps. For example, several satellite communication operators now offer data rates in the tens of megabits/sec range by using efficient compression, acceleration and modulation techniques. Moreover, future speeds may even start to match ground-based communication rates. In turn, these improvements will also complement satellite-based navigation capabilities.

Satellites have been traditionally used to support voice-based communication, i.e., with pilots initiating calls via secure phone numbers assigned by Inmarsat or Iridium. However, on-board satellite links are increasingly common for data communication as well, i.e., for both passenger entertainment services and ATM. In particular, these evolutions have come about as many satellite providers have started to deploy the latest Ka band technologies. Therefore, as satellite communication systems continue to mature, they will eventually form an integral part of the ATN. Most notably, this is the only aircraft communication technology that can provide the desired capacity scalability over oceanic and remote regions, as well as continental airspace regions [14].

Now many newer satellite networks will likely deploy constellations with larger numbers of smaller satellites to provide more cost-effective spaced-based Internet access. A key example here is the OneWeb initiative which plans to launch 648 small low-orbit satellites operating in the Ku band using the 12-18 GHz spectrum [15]. This grand constellation could potentially achieve speeds in the hundreds of Mbps and even cover very remote terrestrial areas. Another key provider here is Inmarsat, which has recently launched three Ka band satellites to provide speeds of up to 50 Mbps for passenger communications (as well as support for safety services). Iridium has also announced the launch of its Iridium Next network to replace its current constellation of 66 satellites. This new setup will provide a major boost to existing data speeds and is currently being rolled out. Given the current status of these new networks, it is safe to assume that satellite communications will play a major role in e-Enabled aircraft architectures, providing increased speeds and improved service capabilities using a combination of L, Ku and Ka bands along with lower-orbit constellations.

However, carefully note that most of the satellite systems in use (or being deployed) today were developed over a decade ago. Hence, these systems largely lack key cybersecurity provisions, i.e., they have outdated firmware, hardened credentials, insecure protocols, etc. Some of these vulnerabilities and associated mitigation strategies are also discussed later in Section V.

B. IP NETWORKS

Data networks play an important role in aircrafts and require bounded latency; (1) Passenger Information and Entertainment Services (PIES) Systems that are largely COTS based with a limited life-cycle (e.g., Audio on demand (AOD) and Video on Demand (VOD)). (2) Airline information services such as non-essential cockpit data and airline operational data. In last few years, an IP-based network infrastructure was introduced for the use of COTS upshots to provide and support air-to-ground aircraft safety services communications [16]. In 2016, a roadmap for establishing an IP suite was released by the Airlines Electronic Engineering Committee (AEEC) for aeronautical safety services. The suite proposed an architecture to adopt IP technology for international harmonization on sub-network data link usage. Scientists also studied avionics equipment deployed by the ground by air navigation service providers (ANSPs) and air traffic controllers [17]

IP architecture is indeed utilized in ground-to-ground sharing of safety-critical data such as altitude and positioning. However, the air-to-ground part of data communication in e-Enabled aircrafts is still unique to aviation [18]. The deployment of IP-based architecture can promote the usage of multiple data links on e-Enabled aircrafts to support communications sharing, surveillance information under ATM modernization programs, and navigation. Moreover, ACARS supports air-to-ground communications protocol where messages of size smaller than 3.5 kilobytes can be exchanged on-board. Such a protocol supports multiple sub-networks such as high-frequency data link and SATCOM. With this given protocol, several concerns should be brought into attention regarding the air-to-ground IP shifting. Such concerns include cybersecurity challenges and which technologies and protocols should be used to ensure support for AeroMACS

For Review Only

and future SATCOM and LDACS specifications [19]. Note that IP infrastructure may present a backward compatibility with classical ACARS air traffic services such as future air navigation system and AOC. Therefore, there will be a need to find out which technology is put in place when upgrading to IP-based technology. The ground systems must accommodate both existing air-to-ground and traditional data link protocols and message sets.

C. LTE WIRELESS NETWORKS

Overall, cellular technologies have hitherto been underutilized for aviation-based communications. In particular, the integration of LTE-based terrestrial access and airborne platforms flying at over 30,000 feet altitude poses some major design challenges. Moreover, cellular technologies have no presence over oceanic or remote areas. However, cellular integration offers many potential benefits over terrestrial regions versus satellite-based communication. Foremost, cellular networks can also provide much lower latencies as compared to satellites orbiting at almost 36,000 km above the surface of the Earth. Finally, current cellular data speeds are much greater than those of state-of-the-art satellite systems, i.e., potentially ranging up to 200 Mbps over terrestrial flight routes. As such, LTE integration could potentially support a much larger number of users for safety critical applications. Therefore, one could envision a hybrid setup where cellular technologies are used to provide data connectivity for short-medium haul continental flights, with switchover to satellite communications (SATCOM) for transcontinental long-haul flights.

Along these lines, some network carriers have started to look at this potential space, and early initiatives are taking shape. In particular, Alcatel-Lucent has developed a hybrid solution in Europe to combine the advantages of both cellular and SATCOM technologies, called A2G or direct air-to-ground [20]. This design uses a cellular architecture to support communication between aircraft and ground-based (IP) broadband access systems. A prototype has also been tested to provide speeds up to 75 Mbps to an aircraft, with further operation in the Mobile Satellite Service (MSS) band in the 2 GHz range and within 2 x 15 Mhz [21]. However, cellular access will require a revised/dedicated terrestrial network infrastructure consisting of larger cells (versus existing terrestrial LTE setups). Dedicated and harmonized frequency bands are also needed to ensure smooth operation without disturbing established cellular networks. Inevitably, this will entail added regulatory issues and challenges (relating to highly-coveted spectrum resources) and heavy initial investments on part of network carriers. Regardless, it is likely that LTE-based technologies will eventually find their way into commercial aviation networks, and hence their security implications need to be factored in as well.

D. WIRELESS LAN TECHNOLOGIES

Current ground-based airport communication systems use underground cables to provide data connectivity. However, these legacy setups complicate maintenance, leading to increased costs, added downtime and reduced efficiency [19]. However, as noted earlier in Section III, there is a strong push to deploy newer wireless systems to support communications during taxiing, take-off and landing, e.g., as embodied by the Aero-MACS framework [10]. For example in 2016, NASA demonstrated the capability and efficiency of such a wireless system via its System Wide Information Management (SWIM) framework, which successfully transmitted information to a FAA Bombadier Global 5000 test aircraft taxiing at 60-70 mph at Cleveland Hopkins International Airport. Overall, these trends clearly indicate that new wireless-based systems will eventually replace legacy wireline technologies for ground-based airport communications in the coming years.

The L-DACS framework is also another promising candidate for future air-to-ground communication and it is also being recommended by the ICAO. Namely, this framework proposes to use the L band between 960-1164 MHz and will not interfere with legacy systems [22]. The two main candidates here are LDACS1 and LDACS2, of which the former is more promising as it uses orthogonal frequency division multiplexing (OFDM) transmission and adaptive coding/modulation, e.g., versus the latter which uses a more conservative narrowband single carrier system with 200 KHz transmission bandwidth and time division duplexing. Overall, LDACS1 divides the airspace into cells, with each having an assigned centralized ground station (which controls all communication within a cell). Hence, transiting aircraft must register with the closest ground station. Furthermore, it is envisioned that the LDACS system will also be deployed between adjacent channels and extended to provide navigation and surveillance services for ATM, thereby making it the first truly integrated communications navigation and surveillance (CNS) technology.

According to the joint EUROCONTROL and FAA Future Communications Concepts and Requirements Team, LDACS1 will provide coverage of up to 200 nm. However, this range can lead to significant propagation delays. Furthermore, aircraft flying at speeds near or above 1,000 km/h can generate sizeable Doppler shifts, further inhibiting the performance of this design. Finally, L band transmission will inevitably cause increased spectrum scarcity and fragmentation. Note that some of these concerns can be (partially) resolved by using appropriate guard bands and techniques such as frequency pre-compensation and channel coding.

For Review Only

E. ON-BOARD AIRCRAFT WIRELESS SENSOR NETWORKS

As noted earlier, safety and efficiencies are some of the key goals of emerging e-Enabled aircrafts. In light of this, many operators are very concerned about current fly-by-wire systems which help control different functionalities of an aircraft. Namely, these systems use numerous on-board connectors and actuators which are interconnected by an extensive network of intra-aircraft electrical conduits. Overall, hard-wiring poses a wide range of challenges. Foremost, wires can be miles in length and weigh thousands of pounds, i.e., 2-5% of aircraft weight. Indeed, detailed wire harnessing often determines the time required to design a new plane. Furthermore, redundant wiring is widely used (along separate paths), i.e., in case of failure of the main wiring system. Wires can also yield electromagnetic interference, and in cases, act as antennas with unwanted impacts on interconnected system immunity [23]. Moreover, wiring can complicate sensor maintenance and replacement, owing to the need to remove/install wires and connections to central processing systems. Finally, it is difficult to rapidly isolate fault points in wiring setups, and this process is also very susceptible to human error.

In light of the above, avionics wireless networks (AWN) are being proposed to interconnect avionics and sensors on-board aircraft. For example, the Wireless Avionics Intra Communication (WAIC) solution uses short-distance radio communications between two or more points on a single aircraft. This setup uses an exclusive closed wireless network inside the aircraft to replace current wired systems. Overall, the WAIC solution can provide significant cost savings. Moreover, these wireless sensors can be used to monitor the health of an aircraft and all its critical systems. Finally, new functions that were previously difficult to implement (due to installation and operational limitations) can now be realized with the help of AWN setups, e.g., such as engine rotor bearing monitoring and electromagnetic interference detection. These measurements can also be communicated to related entities to make the best use of this information on-board or on the ground.

Now as noted in [23], a number of modulation techniques have been tested to determine the spectrum and omni-directional point source in WAIC setups, e.g., Gaussian minimum shift keying (GMSK), quadrature phase shift keying (QPSK), 16-symbol phase shift keying (16-PSK) and 8-symbol frequency shift keying (8-FSK). According to this study, a WAIC system will likely operate in the 1-10 GHz range with a transmit power of about 10 dBm and a range of up to several meters. In particular, the choice of spectrum will be impacted by a number of factors, such as average application data rate, protocol overhead, multiple aircraft factor, modulation efficiency, etc. Recently, WAIC systems are also being further categorized into subsystems depending upon the location of wireless antennas and data rates, i.e., low inside (LI), low outside (LO), high inside (HI) and high outside (HO). Propagation herein will mostly be non-line of sight, since transceivers will likely not be mounted in visible locations or will be integrated in existing parts. Overall, this wireless setup can help extract much more data from the aircraft during all of its phases of flight. Carefully note that the WAIC scheme is not designed for air-to-ground or air-to-air transmissions. That is, it is only intended to support safety critical operations on-board the aircraft.

It is important to note that aircraft control domains and information systems have always been separated from passenger service systems. However, the above-detailed move towards wireless technology clearly presents many vulnerabilities, as these channels can be manipulated and compromised by adversaries. In many cases, a malicious operator will only need a laptop with a wireless adapter and sufficient knowledge of the related wireless communications and protocols being used to cause problem. Incidentally, none of these devices are prohibited on-board an aircraft today.

F. AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST (ADS-B)

Traditionally radar-based systems have been used to detect aircraft in the air by means of primary and secondary surveillance radars (PSR, SSR). However, ADS-B technology is now being deployed worldwide to replace existing radar-based systems with GPS-based surveillance. In fact, the U.S. FAA plans to have ADS-B systems fully deployed in its airspace by 2020 as part of its NextGen initiative. Most of Europe also plans to achieve the same target by 2030. Overall, ADS-B will help compact airspace by reducing aircraft inter-spacing to under 3 nautical miles. Furthermore, it will also provide additional functionalities such as weather reports, terrestrial mapping, etc. Now current ADS-B systems use conventional global navigation satellite system (GNSS) receivers to transmit 3D aircraft positions along with other spatial data, e.g., velocity, heading, flight number and ATM/ATC-related information. This information is then transmitted using a simple broadcast technique and propagated to other aircraft and ground stations, which in turn relay it to the ATCs in a real-time manner. As such, ADS-B provides a very accurate and long-range air-to-air capability for collision avoidance and conflict resolution.

Furthermore, ADS-B supports two different services, i.e., ADS-B Out and ADS-B In. The former is used by an aircraft to broadcast its positional information every second to assist ATC ground surveillance. Meanwhile, the latter is used by an aircraft to receive information from its neighboring aircrafts. ADS-B IS significantly improver pilot situational awareness by providing access to almost the same data as ground-based ATC operators. Furthermore, the traffic information service-broadcast (TIS-B) facility can also send readable flight information to aircraft, e.g., temporary flight restrictions. This service provides valuable near real-time flight

For Review Only

updates as well. Hence in the future one can expect an adhoc vehicular-type setup where aircraft in a given airspace form a (sub)network to share positional and intent information with each other, i.e., without ATC intervention to improve efficiency and reduce costs.

Now at the detailed transmission level, ADS-B uses two data links, i.e., a 1090 MHz extended squitter for larger aircrafts and a 978 MHz universal access transceiver (UAT) for general aircrafts. However, since this technology is based upon GPS, it is prone to a range of natural and human threats (relating to GPS). It is also important to note that ADS-B messages are unencrypted and use simple error coding, making them very easy to eavesdrops and/or spoof. Indeed these are very major design vulnerabilities. In fact, ongoing advances in cost-effective software-defined radio (SDR) technologies will likely lower the barrier to conducting such nefarious activities. Hence, given the impending scope and scale of ADS-B adoption, it is imperative to consider the full range of cybersecurity threats here and devise effective mitigation strategies. Indeed, the implications of not doing so could result in serious financial losses and endanger human lives.

V. SECURITY CHALLENGES

Overall, the move to e-Enabled aircrafts is being driven by the need to achieve greater efficiency and flight volume, lower cost, and an improved passenger experience [24], [25]. As this migration unfolds, future aircraft and ATC entities will increasingly rely upon (wireless) data communication and broadband IP networking technologies, many of which have been surveyed above, e.g., ADS-B, WAIC, AeroMACS, and LDACS. Nevertheless, the integration of these technologies into safety-critical applications will likely result in the increased usage of common hardware and software components as found in network management tools and operating systems across multiple other sectors/domains. Indeed, the use of commercial of the sleep (COTS) systems will make future e-Enabled setups much more prone to individual and organized cyber-attacks. This issue is a major concern as airlines have traditionally provided one of the safest means of travel due to the high standards set by regulating authorities and their strict implementation by governing bodies.

In light of the above, it is imperative for all stakeholders to analyze possible threat vectors for e-Enabled aircraft and devise effective mitigation strategies. Indeed, various attacks have already occurred in recent years, further stressing the critical need to address this problem area. For example, an Internet attack in 2006 forced the U.S. FAA to shut down some of its ATC systems in Alaska. Another noteworthy incident was the crash of Spanair Flight 5022 (operating a MD82) just after take-off in Madrid-Barajas Airport. The incident killed 154 people and was attributed to a critical onboard central computer being infected with malware. Moreover, another cyber-attack in July 2013 led to the shutdown of passport control systems in Istanbul, leading to major flight delays. Finally, in June 2015 a Polish LOT airlines flight experienced a first of its kind denial of service (DoS) attack on its system, resulting in 22 flights being cancelled or delayed at the Warsaw Chopin Airport [26]. The adversaries here seemingly targeted the computer system that sent critical flight plans to aircraft on the tarmac before take-off. This particular attack successfully blocked that network and shutdown the ability to communicate vital information to airlines and aircraft.

Overall, these events clearly demonstrate the type of chaos and confusion that can result from malicious hackers targeting key aviation-related communication infrastructures. As a result, it is imperative for all stakeholders to analyze possible threat vector to E-enabled aircraft and devise effective mitigation strategies. Indeed, a crucial factor in negating such threats is improved situational awareness and communication between industry, government, and law-enforcement agencies (to share threat information and mitigation data). Accordingly, the following section establishes some of the threat vectors for the future e-Enabled aircraft and provides possible strategies for common security threats, e.g., Figures 4 and 3.

A. NETWORK DOS ATTACKS

By extension of the above, it is conceivable that hackers could try to alter key flight plans as well. Although alert ATC crews and pilots could likely notice and mitigate these fabrications, but however, through DoS attacks, the adversaries could still disrupt flight services, leading to stranded aircraft/passengers and sizeable financial losses.

With the aviation sector increasingly deploying IP-based networking technologies and moving towards packetized-voice communications, large DoS attacks against ATM system components can threaten the entire safety and functioning of e-Enabled aircraft. The situation is even more sober in light of the fact that COTS operating systems are widely-deployed across the aviation industry, yet are still prone to usual malicious exploits designed for such systems. Now ATC personnel could possibly revert back to traditional systems to try to maintain normal operation during such attacks. However, this is not a very feasible option. Foremost, reversion requires that one maintains legacy systems, a very costly endeavor. Additionally, older computing systems will not be able to support the increased level of air traffic data volumes and likely suffer from reduced reliability over time.

Furthermore, as noted earlier in Section IV, the concept of adhoc sky-based networks has also been proposed to interconnect aircraft in flight to exchange spatial and temporal messages (over ADS-B). Such communications will improve situational awareness and decrease reliance on terrestrial ATC. However, these adhoc networks can also be subject to wormhole attacks [27]. Namely, theoretically two non-

For Review Only

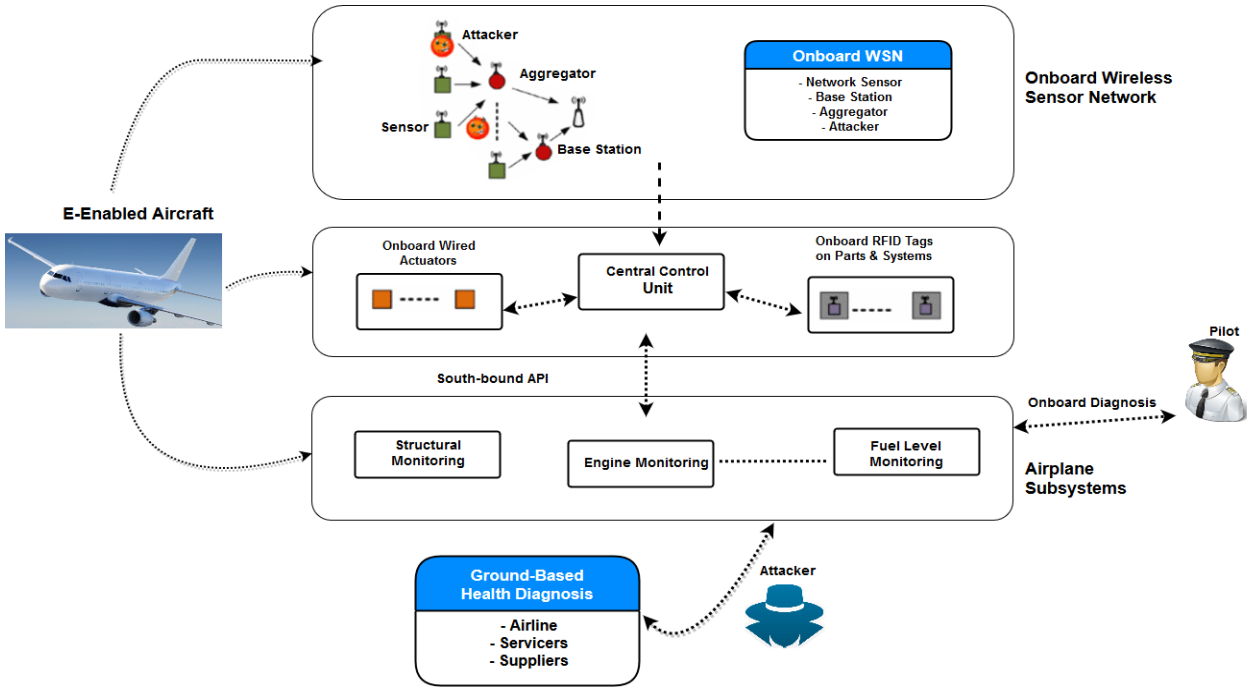

FIGURE 3: Visualization of common vulnerabilities in e-Enabled aircrafts

cooperating (aircraft) nodes can form a tunnel between themselves, and an attacker can record incoming traffic at one end and tunnel it to the other end. This approach can be used to distort network routing or launch rushing attacks to attract more traffic from neighbors (if there is a fast link between two ends of a wormhole). These wormholes can then indulge in DoS attacks at a later stage.

B. COMMUNICATION JAMMING ATTACKS

Navigation systems in next-generation aircraft are heavily dependent on the Global Satellite Navigation System (GNSS) [28]. Hence, the integrity of this system in meeting RNP needs is crucial for maintaining high flight safety standards. Since GPS is the main GNSS technology in use today, it must provide accurate and reliable information [29]. Overall, GPS has a rather complex setup which relies upon information from multiple satellites (a detailed description of this architecture is presented in [30]). As such, this framework also provides multiple avenues for failure and compromise. Most notably, new SDR systems are making it much easier for adversaries to conduct jamming attacks on GPS-based navigation aids in an aircraft. Consider some possibilities here.

Overall, GPS receivers exploit physical signal properties to detect and track locations. Hence, an adversary can exploit related vulnerabilities to impact aircraft safety. Most notably, GPS signals are quite susceptible to interference, making it possible to disrupt operational settings. For example, an attacker can try to decrease signal quality (at the receiver) to below the desired detection threshold [31]. This reduction may cause on-board receivers to lose their lock on satellite signals. Direct/intentional interference or jamming of GPS signals can also be done by emitting a signal close to the GPS spectrum. An adversary with enough means could even emit a more sophisticated GPS-like signal to prevent receivers from acquiring or tracking real signals or causing loss of lock. This is entirely feasible given the relatively low strength of GPS signals and rapid advances and price declines in SDR technologies. Furthermore, interference from other RF transmitters can also complicate GPS signal reception, e.g., such as ultra-wideband radar and personal electronic devices which transmit in the L1/L2 band.

Furthermore, carefully note that many on-board instrument landing systems also use radio altimeters to assist pilots during take-off and landing. Hence, akin to other RF-based systems, these devices can also be compromised by using sophisticated jamming attacks. Although pilots can cross check readings against vertical rate measurements, a clever adversary can further attack both systems to compromise integrity. Hence, even if one system is compromised, it can lead to a difficult situation with increased human error.

C. SPOOFING/IMPERSONATION/MANIPULATION

As mentioned earlier, CPDLC provides data-based message exchange between an aircraft and ATC. Increasingly, this solution is being used to provide an alternative to traditional VHF-based voice communication, particularly in areas where it is supported by ground stations and satellites [32]. Since

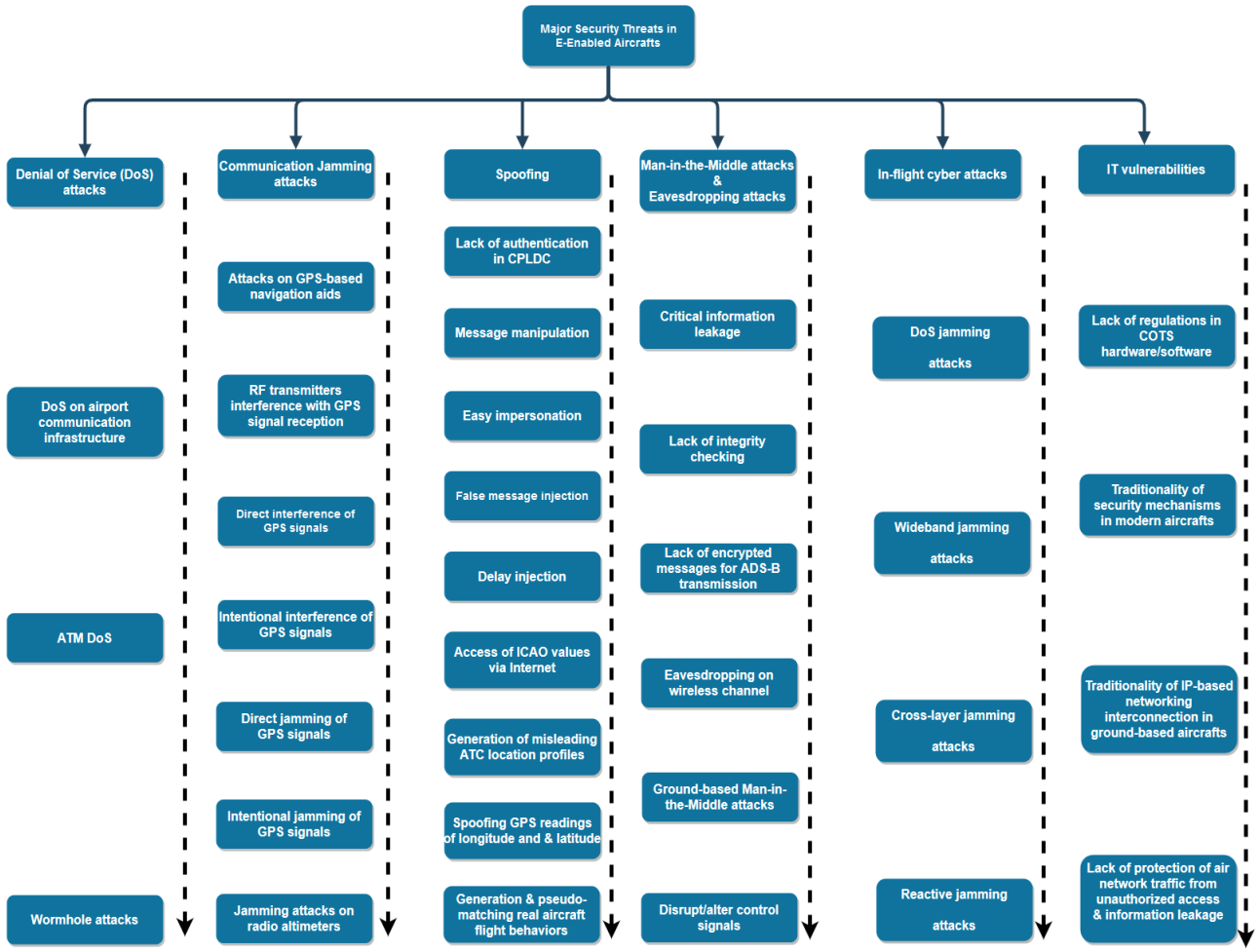

FIGURE 4: Security threats in e-Enabled aircrafts

traditional VHF-based communication suffers from a host of propagation limitations, a technology such as CPLDC can definitely help improve communication efficiency for certain time-critical ATC clearances and pilot requests. However, this technology does not use authentication–a major drawback which induces a host of attack opportunities for adversaries. In particular, these threats range from message manipulation, false message injection, delay injection, etc. Moreover, the lack of authentication also makes impersonation much easier since the adversary only needs to perform a handshake using a location indicator. Specifically, these values are four-character alphanumeric codes issued by the ICAO and can be easily found via the Internet. Hence by using these identifiers, a malicious hacker can eavesdrop and generate location profiles to mislead ATC and/or pass such information along to others. In all, these compromises can lead to unnecessary flight delays, critical safety concerns and increased operational costs, notwithstanding clear risk to passenger and crew safety.

Note that it is also possible to spoof GPS longitude and latitude readings on aircraft in flight (as noted in Section V). These actions can cause receivers to lock on to false signals, and if not detected in time, inject hazardous misleading information resulting in serious navigation errors (even remote steering). Furthermore, the work in [33] shows that it is relatively easy to generate and pseudo-match real aircraft flight behaviors by using accurate flight simulator packages, e.g., such as Flightgear, Spirent GSS7700, etc. The associated ADS-B messages can then be recorded and transmitted to spoof real-world systems, i.e., by leveraging low-cost SDR transmission devices. In light of the above, it is imperative for regulating authorities to address these emerging concerns.

D. EAVESDROPPING/ MAN-IN-THE-MIDDLE ATTACKS

As noted earlier, e-Enabled ecosystems transmit a wide range of information over wireless links interconnecting aircraft, ATC personnel, ground stations, and satellites. This information includes data such aircraft identifiers, geo-location data, and other critical parameters. In general, all of these trans-

missions are vulnerable to information leakage, since malicious adversaries can eavesdrop on wireless channels, i.e., termed as man-in-the-middle (MITM) attacks. This stolen information can then be used in various nefarious ways, such as monitoring aircrafts and on-board individuals or cargos, deciphering flight plans, learning operational procedures, etc. Unfortunately, the lack of integrity checking along with the use of unencrypted messages for ADS-B transmission makes such eavesdropping relatively easy (for even moderately resourceful attackers with SDR systems).

Additionally, other MITM attacks can also be launched both on the ground and in the air. For example, as noted earlier, wireless sensors networks (AWN) are likely going to replace traditional wired fly-by-wire control systems in modern aircraft. Although these networks will be isolated from other communication networks within and outside the aircraft, the inherently open nature of the wireless channel medium makes it easier for an adversary to attempt MITM attacks. Such malicious actions have the potential to disrupt or alter critical control signals essential for the safe operation of aircraft.

E. IN-FLIGHT CYBER-THREATS

As noted earlier, on-board wireless networking technologies in e-Enabled aircrafts provide both Internet access connectivity (for passengers) and critical communications support for operation safety/monitoring of vital aircraft components. However, as the number of wireless devices used by passengers continues to increase, these entities could intentionally or unintentionally interfere with critical aircraft functionalities. Hence it is imperative to separate the passenger and aircraft control domains in the RF domain in order to avoid any unwanted interference, i.e., physical layer separation. Nevertheless, due to the very nature of the wireless communication medium and the ever-evolving range of cyber-threats, it is prudent to assume that any potential attacks should also be mitigated through domain separation and firewalls.

Meanwhile, DoS jamming attacks can also cause disruption or outright breakdown of safety-critical operations. For example, jamming can arise from unintended interference from passenger electronic devices (and the increasing diversity of such devices is posing growing concerns here). Most likely, however, jamming attacks will be initiated by malicious adversaries (on-board or external). These attacks can vary in their type and intensity depending upon the available resources, detection thresholds, and network impacts. For example, some jamming attacks may try to constantly interfere with signals to drive up communication error rates. Although wideband jamming can be most effective here, it will require higher energy resources. As a result, some attackers may try to deploy random and periodic jamming techniques to lower energy usage and avoid detection. Cross-layer jamming and reactive jamming are also some other methods that can be employed to disrupt networks with low resource expenditure. As a result, the best strategy is to develop well-defined mitigation guidelines along with requisite firewall and cryptographic tools, e.g., deploying a feasible periodic control method such that the closed-loop system is stochastically stable and the specified guaranteed cost control performance is achieved [34]

F. IT VULNERABILITIES

Overall, there is a growing trend in the aviation industry to replace traditional analog systems (specialized) with digital systems. Hence, the integration of COTS hardware/software components across this entire domain will likely yield many benefits, e.g., improved efficiency, lower cost, and reduced flight times. However, most of these systems will likely be developed/sourced from external vendors. Moreover, there will likely be little or no regulation of such underlying COTS-based platforms here, at least initially. As such, these developments may open up the entire ecosystem to hitherto unseen threats. For example, the discovery of a vulnerability on a single product can be used to exploit multiple targets owing to the large-scale deployment of such products.

Also, modern aircrafts are constantly generating and transmitting critical data to ATC controllers over open communication channels, e.g., such as the wireless RF spectrum, satellite Ku and Ka bands, etc. Inevitably, these transmissions will strain frequency resources as big data and cloud computing paradigms come into the picture. As a result, traditional security mechanisms such as public key cryptography and message authentication codes need to be redefined to optimize bandwidth usage in aviation settings. Furthermore, ground-based aircraft are also being connected with various off-board systems to enhance traffic control and monitoring operations. However, since this interconnection is being done using ubiquitous IP-based networking technologies, it increases vulnerability to a much wider range of cyber-threats. Moreover, IP-based networking services are already starting to replace traditional voice circuits, i.e., for voice, video, and data transfers. Expectedly, security considerations for these new systems will be vastly different from those for legacy analog voice-based systems. Accordingly, the ICAO has recognized the need to protect air traffic networks from unauthorized access, modification or information leakage [20].

VI. CURRENT RESEARCH AND OPEN CHALLENGES

This section reviews some recent research developments in aviation security and also explores some open research areas. In addition, Tables 1 and 2 also present a taxonomic representation and classification of security solutions for common threats and attacks in aircraft avionics. Foremost, Bernsmed, et al. [56] discussed the necessity of security for data-link services in future aircraft control domain with accordance to different security threat analysis. Furthermore, they also

For Review Only

TABLE 1: Taxonomic classification of proposed solutions in aviation security (Cont.)

Reference	Threat	Contribution
Sampigethaya, et al. [20]	Integrity & failure	A multi-radar framework to enforce integrity checking for ADS-B and provide a backup support in case of hardware/software failures
Valovage [35]	Authentication	A cryptography and authentication scheme to secure ADS-B communications
Fox, et al. [36]	Integrity	Usage of a Kalman filter to verify the integrity of ADS-B messages, but such filters are proven vulnerable to boiling attacks via jamming and message injection [37]
Chiang, et al. [38]	Spoofing	A distance bounding scheme to detect spoofed messages, but the high speed and long distances between senders and receivers were proven to make such detection ineffective
Kovell, et al. [39]	Verification	A technique for group verification over ADS-B messages
Sampigethaya, et al. [40]	Availability, integrity, and anonymity	A security and privacy framework for ADS-B to address key concerns such as availability, integrity and anonymity
Teso [41]	Security and reliability	Demonstration of fingerprinting at multiple layers of the communication stack coupled with improved location estimation and efficient cryptographic algorithms help to improve the security and reliability of ADS-B
Yue and Wu [42]	Privacy	A security framework for ACARS that uses a combination of authentication and encryption to ensure privacy, integrity and authenticity
Roy [43]	Communication security	Adoption of IP-based connectivity for establishing secure aircraft communications along with and an addressing and reporting system
Cruickshank, et al. [44]	IP-based satellite security	A MPEG-2 video transport solution using an unidirectional lightweight encapsulation (ULE) to send IPv4, IPv6 and other data units. A security architecture for future e-Enabled aircraft using IP-based satellite technologies is also proposed
Sampigethaya, et al. [20]	Performance and safety	Demonstration that packet-based technologies adoption between aircraft and ground stations can help to improve performance and increase safety
Nguyen, et al. [45]	Threat detection	An algorithm for attack trees generation from developers and designers perspective to identify potential threats of a UAV system and associate threat models with expected security properties

presented various security requirements that should be fulfilled by future SATCOM data-link systems for ATM. Meanwhile, Sampigethaya, et al. [57] also discussed cyber security needs in unmanned UTM and provided a comprehensive classification and assessment of related security threats in UTM.

Overall, the current work in aviation networking security has mostly focused on securing ADS-B systems. As noted, ADS-B can be used to build ad-hoc networks in the air, thus reducing dependency on ground-based stations and satellite links. However, the inherent security vulnerabilities of ADS-B have impeded its wider adoption. Along these lines, Sampigethaya, et al. [20] outlines a multi-radar framework to provide integrity checking for ADS-B, as well as backup support in case of hardware or other failures. Meanwhile, Valovage [35] presents a cryptography and authentication scheme to secure ADS-B communications. However, this method does not take into account the computational complexity or bandwidth requirements for aviation communications. Meanwhile, Fox, et al. [36] also used a Kalman filter to verify the integrity of ADS-B messages. However as noted in [37], such filters are vulnerable to boiling attacks in which attackers can falsify trajectory data via jamming and message injection. Hence, Chiang, et al. [38] proposed a distance bounding scheme to detect such spoofed messages. However, the high speeds and long distances between senders and receivers here makes it ineffective for aviation networks. Finally, Kovell, et al. [39] and Sampigethaya, et al. [40] studied group verification-based techniques for ADS-B messages. Additionally, Sampigethaya and Poovendran [40] also proposed a security and privacy framework for ADS-B to address key concerns such as availability, integrity and anonymity. However, this effort does not provide a detailed solution to mitigate threats.

Nevertheless, despite the above efforts, ADS-B security is still an open concern. Over and above, various anonymization methods (using random pseudonyms) have been proposed here. However, the strong correlation between aircraft location and the short inter-message duration of ADS-B communications can make these schemes rather impractical. Hence, future efforts must focus on more resource-efficient solutions that account for the dynamic and specialized landscape of aviation networks. As discussed in [41], fingerprinting at multiple layers of the aviation communication stack (cou-

For Review Only

TABLE 2: Taxonomic classification of proposed solutions in aviation security

Reference	Threat	Contribution
Prevot, et al. [32]	Performance and safety	Authentication and encryption mechanisms along with message structure specifications
Davis [46]	Interoperability	Address interoperability issue between different vendor and original equipment manufacturer (OEM) systems in order to provide protection against eavesdropping and message injection/alteration attacks
Shetty [47]	Integration with sensor communication	Address the potential impacts of integrating passenger, crew and (fly-by-wire) sensor communications over a single data link
Ugwoke, et al. [48]	Dos/DDoS	A counter security network model to preempt DoS/DDoS attacks and mitigate relevant vulnerabilities in Airport Information Resource Management Systems (AIRMS)
Li, et al. [49]	ADS-B data attack	A model for analyzing common ADS-B data attack patterns and detection with accordance to flight and ground station capabilities through the integration of various detection methods, e.g., plan of flight validation and detection of group data
Waheed, et al. [50]	Security event failure	A configurable system to collect, monitor, and report failures of security events in aircrafts in real-time to provide a timely detection and prevention of cyber security attacks
Quanxin, et al. [51]	External network threat	An algorithm consisting of a set of aviation network security strategies to mitigate the impact of external network threats against the flight network system
Yoon, et al. [52]	Hijacking	A mechanism to prevent hijacking network channel and physical hardware on commercial UAVs through an additional encrypted communication channel
Leonardi, et al. [53]	Traffic classification	A feature based on the ADS-B message Phase-Pattern to elaborate a classification of the aircraft traffic and distinguish legitimate from fake messages
Hooper, et al. [54]	DoS and buffer-overflow	A fuzzing technique to detect vulnerabilities in Parrot Bebop UAV is to DoS and buffer-overflow attacks
Tohidi, et al. [55]	Induced oscillations	An adaptive control-based allocation method to help unmanned aircraft systems recover from pilot induced oscillations in en efficient manner

pled with improved location estimation and efficient cryptographic algorithms) can help improve the security and reliability of ADS-B.

Additionally, it is important to mention the Aircraft Communication and Addressing Scheme (ACARS), which implements key transfers between aircraft and ground stations, i.e., transferring critical private information such as passenger details, aircraft positions, etc. Since ACARS is used in all phases of flight, i.e., from takeoff to landing, it is important to ensure its security. Again, the availability of cheap and powerful SDR devices poses a range of passive and active attack vulnerabilities here, see [41]. As a result, Yue and Wu [42] proposed a secure ACARS framework that uses a combination of authentication and encryption methods to ensure privacy, integrity and authenticity. However, the adoption of IP-based connectivity will largely obsolete such older mitigation strategies, e.g., such those proposed in [43]. Therefore, more effective/scalable strategies are required for heterogeneous aviation environments.

Modern IP-based (digital) satellite networks are also replacing traditional analog communication networks for aircraft communications. Now various studies have looked at security requirements for such IP-based satellite setups. For example, Cruickshank, et al. [44] presented a MPEG-2 video transport solution which uses unidirectional lightweight encapsulation (ULE) to send IPv4, IPv6 and other data units. Cruickshank, et al. [44] also proposed a security architecture for future e-Enabled aircraft using IP-based satellite technologies. In particular an adaptive security management scheme is presented based upon a proposed SecMan module, which runs a multi-criterion decision-making algorithm (MCDMA) to select the best policy from a pre-defined database. The system proceeds to securely negotiate a set of security protocols for communicating between the two entities, and hashing techniques are also used to reduce computational complexity. This framework also collects network and system information to improve policy selection. Although this contribution provides a comprehensive solution for secure communications (between aircraft, satellites and ground stations), related scalability and quality of service (QoS) issues still need to be addressed.

Some security considerations for IP-based aviation networks are also discussed in [20]. Specifically, the authors note that the adoption of packet-based technologies between aircraft and ground stations will lead to improved performance and increased safety. Increased spectrum capacity, e.g., on new satellite-based links, will also provide new avenues for improving security. Along these lines, further authentication and encryption mechanisms along with message structure

For Review Only

specifications are defined in [58]. Furthermore, the Aeronautical Radio, Inc (ARNIC) Network and Security subcommittee is also working to define a new domain name service (DNS) standards to ensure smoother transition of IP-based aviation networks, i.e., akin to corporate environments [59]. Nevertheless, many issues still need to be addressed here, e.g., interoperability between different vendor and original equipment manufacturer (OEM) systems, protection against eavesdropping and message injection/alteration attacks [46].

Finally, Shetty [47] have discussed the potential impacts of integrating passenger, crew and (fly-by-wire) sensor communications over a single data link. However, since aircraft-based sensor networks are still in the early stages of deployment, it will likely take some time for widespread adoption.

VII. CONCLUSIONS

The e-Enabled aircraft paradigm is being developed to improved operational efficiency, reduce costs and streamline traffic management. This vision integrates upon many different types of communications technologies, such as wireless sensor networks, ADS-B, L-DCAS, next-generation satellites, and ubiquitous IP-based networking. However, the amalgamation of all these diverse technologies across heterogeneous aviation settings will inevitably yield complex infrastructures with increased vulnerability to a full range of cyber-threats. In particular, the implicit security of aviation communications through isolation is no longer guaranteed as various stakeholders move to the digital domain. Hence, emerging next generation aircraft systems must contend with wide-ranging threats ranging from common IT vulnerabilities (akin to those found in traditional corporate settings) to many new specialized/targeted attack vectors.

In light of the above, this paper reviews some key technology trends and advances in the aviation communications sector. It then outlines some critical cybersecurity challenges driven by the transition from analog to digital-based communication systems. In particular, these vulnerabilities include denial of service (DoS) attacks, jamming, spoofing, man-in-the-middle (MITM) attacks, etc. Finally, some current research efforts relating to aviation security are also reviewed including ADS-B and wireless sensor networks, IT threats and communication standards and methodologies. Overall, the aviation industry has always been regarded as one of the safest sectors, owing to its highly-stringent standards and strictly-followed regulations. Hence, it is imperative to identify and address all cyber-threats facing emerging e-Enabled setups in order to ensure the continued safety of millions of travelers and workers across the world.

VIII. APPENDIX

Table 3 presents a list of acronyms used in this paper.

TABLE 3: A summary of used acronyms

Acronym	Description
ACARS	Aircraft Communication and Addressing Scheme
ADS-B	Automatic Dependent Surveillance-Broadcast
Aero-MACS	Aeronautical Mobile Airport Communication System
AFTN	Aeronautical Fixed Telecommunication Network
AIRMS	Airport Information Resource Management Systems
AOC	Aeronautical operational control
ARNIC	Aeronautical Radio Inc
ATC	Air traffic control
ATN	Aeronautical Telecommunications Network
ATM	Air traffic management
ASSC	Airport Surface Surveillance Capability
AWN	Avionics wireless networks
COTS	Commercial-off-the-shelf
CPLDC	Controller Pilot Data Link Communications
DNS	Domain name service
DoS	Denial of service attack
EFB	Electronic Flight Bag
EUROCONTROL	European Organisation for the Safety of Air Navigation
FAA	U.S. Federal Aviation Administration
FHA	Functional hazard assessment
FMC	Flight management computer
FMS	Flight management systems
GMSK	Gaussian minimum shift keying
GNSS	Global navigation satellite system
GPS	Global positioning system
HI	High inside
HO	High outside
ICAO	International Civil Aviation Organization
IP	Internet Protocol
LDCAS	L-band Digital Aeronautical Comm. Systems
LO	Low outside
LOI	Low inside
LTE	Long Term Evolution
MCDMA	Multicriterion decision-making algorithm
MITM	Man-in-the-middle
NAS	National Airspace System
NextGen	Next Generation Transport
OEM	Original equipment manufacturer
OFDM	Frequency division multiplexing
PNB	Performance-based navigation
PSR	Primary surveillance radar
QoS	Quality of Service
RF	Radio frequency
RNP	Required navigation performance
SATCOM	Satellite communications
SDR	Software-defined radio
SESAR	Single European Sky ATM Research
SOC	Systems on a chip
SOE	Secure operational environment
SSR	Secondary surveillance radar
TIS-B	Traffic information service broadcast
UAS	Unmanned aerial systems
UAT	Universal access transceiver
UAV	Unmanned Aerial Vehicle
ULE	Unidirectional lightweight encapsulation
VHF	Very high frequency
WAIC	Wireless Avionics Intra Communication

REFERENCES

[1] N. Raharya and M. Suryanegara, "Compatibility analysis of wireless avionics intra communications (waic) to radio altimeter at 4200–4400 mhz," in Proceedings of the Asia Pacific Conference on Wireless and Mobile. IEEE, 2014, pp. 17–22.

For Review Only

[2] B. Green, J. Marotta, B. Petre, K. Lillestolen, R. Spencer, N. Gupta, D. O'Leary, J. D. Lee, J. Strasburger, A. Nordsieck et al., "Handbook for the selection and evaluation of microprocessors for airborne systems," Tech. Rep., 2011.

[3] S. Ayhan, J. Pesce, P. Comitz, D. Sweet, S. Bliesner, and G. Gerberick, "Predictive analytics with aviation big data," in Proceedings of the Integrated Communications, Navigation and Surveillance Conference (ICNS). IEEE, 2013, pp. 1–13.

[4] Z. Yuan and Q. Yanlin, "Design and implementation of general aviation flight service cloud platform," in Proceedings of the 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). IEEE, 2018, pp. 623–627.

[5] S. Majumder and M. S. Prasad, "Cloud based control for unmanned aerial vehicles," in Proceedings of the 3rd International Conference on Signal Processing and Integrated Networks (SPIN). IEEE, 2016, pp. 421–424.

[6] W. Kampichler and D. Eier, "Cloud based services in air traffic management," in Proceedings of the Integrated Communications, Navigation and Surveillance Conference. IEEE, 2012, pp. 5–1.

[7] S. Miller, "Contribution of flight systems to performance-based navigation," Aero-Journal, 2009.

[8] "Advanced flight management system," AT-One, the ATM Research Alliance.

[9] G. Bartoli, R. Fantacci, and D. Marabissi, "Aeromacs: A new perspective for mobile airport communications and services," Wireless Communications, vol. 20, no. 6, pp. 44–50, 2013.

[10] I. Gheorghisor, A. Leu, S. Bodie, W. Wilson, and F. Box, "Aeromacs implementation analyses," MTR140382, The MITRE Corporation, 2014.

[11] "GX Aviation." https://www.inmarsat.com/aviation/complete-aviation-connectivity/gx-for-aviation [Accessed December 2018].

[12] R. S. Stansbury, M. A. Vyas, and T. A. Wilson, "A survey of uas technologies for command, control, and communication (c3)," in Unmanned Aircraft Systems. Springer, 2008, pp. 61–78.

[13] A. R. Karmarkar and L. Martin, "Aviation communication infrastructure security," in Proceedings of the Integrated Communications, Navigation and Surveillance Conference (ICNS). IEEE, 2012, pp. E7–1.

[14] G. Berzins, F. Ryan, and K. Smith, "Initiation and early development of a worldwide satellite communications system for aviation," Journal of Aeronautical History, pp. 0–4, 2015.

[15] "Oneweb global access." https://www.itu.int/en/ITU-R/space/workshops/SISS-2016/Documents/OneWeb%20.pdf [Accessed December 2018].

[16] E. Fleischman, R. E. Smith, and N. Multari, "Networked local area networks (lans) in aircraft: Safety, security and certification issues, and initial acceptance criteria (phases 1 and 2)," Final Report, December, 2006.

[17] W. Bellamy and J. V. Wagenen, "An ips roadmap for aeronautical safety services," 2017.

[18] G. T. Saccone, M. L. Olive, M. E. Matyas, and D. C. Smith, "Safety services using the internet protocol suite: Benefits, progress, and challenges," in 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC). IEEE, 2015, pp. 2B1–1.

[19] M. Strohmeier, "Security in next generation air traffic communication networks," Ph.D. dissertation, Ph. D. Thesis, University of Oxford, Oxford, UK, 2016.

[20] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty, "Future e-enabled aircraft communications and security: The next 20 years and beyond," Proceedings of the IEEE, vol. 99, no. 11, pp. 2040–2055, 2011.

[21] A. Lucent, "Using air-to-ground lte for in-flight ultra-broadband," Strategic White Paper, 2015.

[22] M. Schnell, U. Epple, D. Shutin, and N. Schneckenburger, "Ldacs: Future aeronautical communications for air-traffic management," Communications Magazine, vol. 52, no. 5, pp. 104–110, 2014.

[23] M. Suryanegara and N. Raharya, "Modulation performance in wireless avionics intra communications (waic)," in Proceedings of the 1st International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE). IEEE, 2014, pp. 434–437.

[24] R. K. Rajasekaran and E. Frew, "Cyber security challenges for networked aircraft," in Proceedings of the Integrated Communications, Navigation and Surveillance Conference (ICNS). IEEE, 2017, pp. 1–15.

[25] H. Duchamp, I. Bayram, and R. Korhani, "Cyber-security, a new challenge for the aviation and automotive industries," 2016.

[26] "Polish airline, hit by cyber attack, says all carriers are at risk." https://www.reuters.com/article/us-poland-lot-cybercrime/polish-airline-hit-by-cyber-attack-says-all-carriers-are-at-risk-idUSKBN0P21DC20150622 [Accessed December 2018].

[27] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," journal on selected areas in communications, vol. 24, no. 2, pp. 370–380, 2006.

[28] K. Alexander and D. Lawrence, "Gnss intentional interference and spoofing," in Technical Report, Federal Aviation Administration, Oct. 2015.

[29] N. W. Paper, "Mitigating the threat of gps jamming: Anti-jam technology," in NovAtel. IEEE, 2012.

[30] W. Y. Ochieng, K. Sauer, D. Walsh, G. Brodin, S. Griffin, and M. Denney, "Gps integrity and potential impact on aviation safety," The Journal of Navigation, vol. 56, no. 1, pp. 51–65, 2003.

[31] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "On perception and reality in wireless air traffic communication security," Transactions on Intelligent Transportation Systems, vol. 18, no. 6, pp. 1338–1357, 2017.

[32] T. Prevot, T. Callantine, P. Lee, J. Mercer, V. Battiste, E. Palmer, and N. Smith, "Co-operative air traffic management: concept and transition," in AIAA Guidance, Navigation, and Control Conference and Exhibit, 2005, p. p. 6045.

[33] B. Haines, "Hacker+ airplanes= no good can come of this," Confidence X, 2012.

[34] M. Wang and B. Xu, "Guaranteed cost control of cyper-physical systems under periodic dos jamming attacks," in Proceedings of the 37th Chinese Control Conference (CCC). IEEE, 2018, pp. 6241–6246.

[35] E. Valovage, "Enhanced ads-b research," in Proceedings of the 25th Digital Avionics Systems Conference, 2006 IEEE/AIAA. IEEE, 2006, pp. 1–7.

[36] D. Fox, J. Hightower, L. Liao, D. Schulz, and G. Borriello, "Bayesian filtering for location estimation," Pervasive Computing, no. 3, pp. 24–33, 2003.

[37] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," Communications Surveys & Tutorials, vol. 17, no. 2, pp. 1066–1087, 2015.

[38] J. T. Chiang, J. J. Haas, and Y.-C. Hu, "Secure and precise location verification using distance bounding and simultaneous multilateration," in Proceedings of the Second Conference on Wireless Network Security. ACM, 2009, pp. 181–192.

[39] B. Kovell, B. Mellish, T. Newman, and O. Kajopaiye, "Comparative analysis of ads-b verification techniques," The University of Colorado, Boulder, vol. 4, 2012.

[40] K. Sampigethaya and R. Poovendran, "Security and privacy of future aircraft wireless communications with off-board systems," in Proceedings of the 3rd International Conference on Communication Systems and Networks (COMSNETS). IEEE, 2011, pp. 1–6.

[41] H. Teso, "Aircraft hacking: Practical aero series," in HITB Security Conference, 2013.

[42] M. Yue and X. Wu, "The approach of acars data encryption and authentication," in Proceedings of the International Conference on Computational Intelligence and Security (CIS). IEEE, 2010, pp. 556–560.

View publication stats