FRAMEWORK PARA IMPLANTAÇÃO DE SISTEMAS EVTOL – REQUISITOS TÉCNICOS

Alfredo Almeida de Araujo, João Batista Camargo Jr., Lester de Abreu Faria
Universidade de São Paulo, Escola Politécnica, Programa de Pós-Graduação em Eng. Elétrica

*** Corresponding author e-mail address**: alfredo.araujo@usp.br

PAPER ID: SIT228

ABSTRACT

This article aims to define the necessary requirements for the creation of a communication framework aimed at operating an autonomous navigation system for vertical landing and take-off aircraft, with electric motorization (eVTOL). This framework has the function of enabling the control, communication and navigation of the aircraft, so that it is possible to replace the management currently performed by the control towers existing in the aerial systems, with an autonomous control system. With the evolution of artificial intelligence technology and electric motorization, it will be possible to develop aircrafts with the specific objective of performing aerial mobility in large urban centers, becoming an alternative to the current means of transport. Specifically, as part of the navigation system, a compatibility of the systems currently used by satellite should occur, in order to meet the needs imposed by the application in question. In addition, due to the critical nature that this application imposes, it is suggested what adaptations the communication networks will need to have for a safe and available service. Therefore, electronic warfare techniques should be incorporated into the networks, creating countermeasures and electronic counter countermeasures to be used in case of attack.

Keywords: autonomous vehicles, mobility, satellite communication, 5G network.

1. INTRODUÇÃO

Atualmente, tem sido uma tendência mundial entre os maiores fabricantes de aeronaves o desenvolvimento uma nova geração de veículos para transporte de pessoas, visando à mobilidade urbana, e com foco em veículos movidos à energia elétrica, a fim de serem mais silenciosos e menos poluentes. Empresas como Boeing, Airbus, Embraer, Uber, Hyundai, Daimler, Toyota e Velocopter investem centenas de milhões de dólares em pesquisa e já possuem protótipos funcionais, não autônomos (Automative-iq, 2020).

Entende-se que, em um primeiro momento, tais veículos deverão ser tripulados como atualmente ocorre em serviços de taxi aéreo, ou seja, necessitando da presença de uma torre de comando, onde são gerenciados cada um dos voos, definição de rotas, corredores, gestão do espaço aéreo, etc. e provendo, desta forma, autorizações de partida e controle de aterrisagem de cada voo. No entanto, a expectativa é de que, em cerca de 10 anos (Gartner group, 2019), tais sistemas sejam totalmente autônomos, ou seja, sem piloto, e, portanto, não havendo a necessidade de uma torre de comando para a gerência do espaço aéreo e controle das partidas e chegadas dos voos.

Estas aeronaves autônomas serão capazes de voar em um espaço aéreo reservado, a fim de não conflitar com drones de pequeno porte (chamados de sUAS – Small Unmanned Aircraft System), os quais atualmente já fazem serviços de entregas de encomendas (Flytrex, 2020), em espaços aéreos compreendidos entre 100 pés de altitude, nem tampouco com as aeronaves comerciais de grande porte de asa fixa, que voam acima de 1000 pés. Com isso, há uma faixa de aproximadamente 900 pés onde os eVTOLs poderão operar.

A fim de que a funcionalidade do voo autônomo possa ser atingida, deverá ser implantada, entre outras coisas, uma rede de comunicação com a segurança e a resiliência necessárias para garantir o mínimo de compatibilidade com os padrões de segurança e disponibilidade atualmente aplicados à aviação comercial. Tal rede deve ter alta capacidade de tráfego de dados e baixíssima latência, a fim de garantir uma resposta rápida o suficiente para as manobras necessárias para o voo, além das redundâncias necessárias para atingir os níveis de disponibilidade desejados.

Para tanto, a proposta a ser avaliada durante este trabalho é a utilização da rede móvel 5G (quinta geração) (EMBRAER X), uma vez que ela tem alta capacidade de tráfego (acima de 1 Gbps) e já está sendo implantada em diversos países, incluindo o Brasil (Ministério da Ciência, Tecnologia, Inovações e Comunicações, 2019). Além disso, a latência para o trecho aéreo do sistema é menor que 1ms, sendo fim-a-fim menor que 10ms, e dando, numa análise preliminar, condições técnicas para sua utilização como sistema de comunicação a ser empregado nos eVTOL.

Para se atingir uma maior disponibilidade da rede como um todo, poderá ser analisada ainda uma segunda rede de comunicação, complementar à primeira, tais como, as redes VSAT por satélite em banda Ka, as quais têm alcance global e que são capazes de cobrir possíveis áreas de sombra da rede 5G, podendo ainda ser uma contingência em caso de falha ou sobrecarga da 5G. Estas redes, atualmente disponíveis através de diversas operadoras espalhadas pelo globo, atuam por meio de satélites geoestacionários, posicionados em órbitas fixas. Porém, há uma nova geração de satélites em desenvolvimento, patrocinada por empresas como Oneweb, Starlink e Amazon (One Web, 2020, Starlink, 2020, Spacenews, 2019), que consiste de satélites menores, os quais estarão posicionados em órbita baixa, e constituirão de constelações que poderão chegar a centenas de unidades, provendo, desta forma, acesso à Internet em banda larga de forma contínua em qualquer parte do globo, e aumentando sobremaneira a disponibilidade da comunicação.

Este sistema, assim como atualmente acontece com as aviações civil e militar, deve ser considerado como um ambiente de segurança, uma vez que, além das vidas que estão sendo transportadas, há ainda a população que pode ser atingida por uma aeronave, estando esta sob falha mecânica, falha de hardware ou software ou falha motivada por falta de comunicação, esta última podendo ter sido causada por uma ação

intencional, uma invasão da rede, e consequente manipulação e controle remoto da aeronave (spoofing).

Por fim, empresas como a Amazon, e outras, estão colocando em seu portfólio entregas de livros e produtos por meio de drones, os quais, estão suscetíveis a ataques e interferências eletromagnéticas (Yaacoub, J. et al., 2020). Na Austrália, no mês de abril de 2019, foi iniciado oficialmente o serviço de entrega de encomendas por drones, pela empresa Wing (pertencente à Google). Atuando nos Estados Unidos e Nova Zelândia, também há a empresa Flirtey.

Dessa forma, o objetivo do presente trabalho é apresentar os possíveis sistemas que podem compor o framework, de tal forma que este possa prover as funções de comunicação, entre aeronaves e com o sistema de gerenciamento do espaço aéreo, e a navegação, para prover com precisão a localização da aeronave, informação esta que será utilizada pelo sistema de gerenciamento do espaço aéreo para controlar todas as aeronaves em voo e em solo, aguardando autorização para decolagem.

2. REQUISITOS TÉCNICOS

O framework base proposto pelo presente trabalho está baseado essencialmente em duas frentes distintas, as quais se mostram necessárias para que as aeronaves possam realizar seus voos de forma totalmente autônoma: i. comunicação, para que haja a troca de informações da aeronave com o centro de gerenciamento e também entre as próprias aeronaves; e ii. o geo-referenciamento, para que estas tenham a informação exata da sua localização e altitude, a fim de que estes dados sejam informados ao centro de gerenciamento para o controle de cada uma das aeronaves que estão em voo na região.

2.1 COMUNICAÇÃO

Este sistema é responsável pela transmissão segura e contínua dos dados referentes às condições da aeronave (Keysight Technologies, 2018), tais como nível de bateria, velocidade, dados do sistema de gerenciamento da aeronave (como possíveis defeitos), informações do sistema de detecção de colisões e do radar meteorológico, localização e altitude (estes últimos dados provenientes do sistema de localização), bem como o recebimento de informações provenientes do centro de gerenciamento, para definição de origem e destino, autorização de decolagem e pouso, determinação e correção de rota.

Devido à importância crítica deste sistema, a transmissão deve ser segura, tanto do ponto de vista eletromagnético (o sistema deve ter a capacidade de suportar ataques intencionais e interferência natural da transmissão), quanto do ponto de vista lógico, com ataques provenientes de hackers, que têm o intuito de gerar sobrecarga da rede (ataques DDoS, por exemplo) e alterações de informações, o que poderia gerar a interrupção do serviço ou acidentes como colisões entre aeronaves.

Por outro lado, como forma de garantir uma disponibilidade compatível com a aviação civil atual, é proposta a utilização de duas formas de comunicação simultâneas: redes móveis 5G (quinta geração) e serviços VSAT (transmissão por satélite) em Banda Ka. Esta disposição visa tanto a aumentar a redundância da rede quanto cobrir possíveis regiões de sombra nas células da rede 5G, bem como possíveis interrupções do serviço por satélite, em virtude de instabilidade climática, por exemplo.

A utilização simultânea de ambas se daria de forma espalhada, na qual as informações trafegariam preferencialmente pela rede 5G, devido à sua baixa latência e, em caso de congestionamento, falha ou ausência de sinal, em função da aeronave trafegar em uma região onde não haja cobertura da rede móvel, a transmissão seria comutada automaticamente para o serviço Banda Ka.

2.1.1. REDES MÓVEIS 5G

As redes móveis de quinta geração estão sendo adotadas em diversos países pelo mundo (Ministério da Ciência, Tecnologia, Inovações e Comunicações, 2019), e têm como principais diferenciais, em relação às gerações anteriores, o aumento de velocidade para upload e

download, que podem chegar a até 10 Gbps e 20 Gbps respectivamente, em função de utilização de largura de banda consideravelmente maior, uma vez que se utilizam faixas de frequência menos congestionadas, além de uma baixíssima latência, de cerca de 1 ms na interface aérea (Keysight Technologies, 2018). Em especial este último se mostra como um fator extremamente importante para que haja uma resposta rápida da aeronave em função de uma mudança de parâmetro e controle de voo. Outra característica importante é a de suportar velocidades de até 500 km/h dos terminais conectados, o que garante a conexão das aeronaves mesmo no seu limite de velocidade de deslocamento. No caso dos eVTOL, a expectativa de velocidade de cruzeiro das aeronaves é de 320 km/h, o que garante uma perfeita conexão com a rede 5G (Neto, E. et al., 2019).

Além destas características, a rede 5G também proporciona novas funcionalidades de rede, quais sejam (Keysight Technologies, 2018):

- Network Slicing: permite que a rede móvel seja dividida em redes lógicas distintas, cada uma com uma configuração diferente de acordo com sua função, como acesso broadband (eMBB) maciço entre máquinas, como IoT (mMTC) e o que se aplica a este trabalho, o ultra confiável e de baixa latência (URLLC). Para cada uma dessas redes, pode ser configurado um nível diferente de QoS, tempo de resposta (latência da rede), consumo de energia, velocidade em que o dispositivo pode se locomover, quantidade de elementos conectados, e redundância de elementos de rede, garantindo assim uma maior disponibilidade do serviço.

- Comunicação entre dispositivos: Este recurso permite que dispositivos 5G se conectem uns aos outros, sem a necessidade de conexão com o core da rede, o que, aplicado à uma aeronave, permitiria que esta se comunicasse com as aeronaves próximas para a troca de informações de posicionamento, velocidade e condições de tráfego, por exemplo.

2.1.1.1 VULNERABILIDADES

Entretanto, entende-se que a utilização de redes 5G para o controle e comunicação de eVTOL pode levar também a algumas vulnerabilidades. Tais ameaças presentes na rede móvel 5G podem ser divididas em dois grupos distintos:

- Ameaças eletromagnéticas: onde verificam-se ruídos nas frequências utilizadas pelas redes móveis, em uma potência maior que o recebido pelos terminais provenientes das torres de transmissão e, quando somados a estes, anulam o sinal, fazendo com que a conexão com a rede seja interrompida. A maioria dos bloqueadores disponíveis no mercado, os quais possuem venda controlada somente para órgãos de segurança, tem o alcance de algumas dezenas de metros. Porém, quando estes são acoplados a antenas de maior ganho, como as do tipo Yagi, podem aumentar este raio de ação, bem como se colocadas em pontos estratégicos, como próximos aos pontos de desembarque dos eVTOL, podem comprometer o serviço, gerando a necessidade de paralisação das atividades durante o período do ataque. Uma forma de prevenção deste tipo de ataque é a utilização de serviços complementares, como as redes de satélite em banda Ka.

- Ameaças lógicas: as redes 5G tem os seus elementos de núcleo todos virtualizados (VNF – Virtual Network Functions), ou seja, não há equipamentos físicos para a comunicação, como havia até as redes 4G (LTE). Todos os serviços de rede prestados são softwares instalados em servidores e, desta forma, possuindo as mesmas vulnerabilidades que os sistemas corporativos, por exemplo. Assim sendo, devem ser implantados na rede serviços de proteção como sistemas de detecção e prevenção de invasão (IDS/IPS) e criptografia do tipo TLS (Transport Layer Security) entre as VNFs, para que a comunicação entre estes elementos seja segura e tenha processos de validação de identidade confiáveis, e não permitindo, desta forma, que uma máquina externa (invasora) se passe por um elemento da operadora e assim tenha acesso ao núcleo da rede.

Outro tipo de ataque possível é o DDoS (Distributed Denial of Service), que consiste em utilizar os clientes de rede invadidos por hackers (no caso as próprias aeronaves), para atacar os servidores da rede. Neste ataque, os terminais geram um fluxo de dados excessivo nos servidores (tráfego de rede), os quais não suportam a carga adicional e têm os serviços interrompidos, a partir da paralização das aplicações residentes nos servidores. Estes ataques também geram tráfego superior à capacidade nos links de comunicação, congestionando-os e consequentemente gerando perda de pacotes acima do volume tolerável, em função da expiração do tempo de vida destes.

Assim, tanto a rede quanto as aeronaves devem ser protegidas. Do lado da rede, deverão ser utilizados sistemas Anti-DDoS existentes do mercado, que analisam os dados trafegados e, por meio de algoritmos, identificam os possíveis ataques em função das anomalias geradas na rede, tomando a proteção necessária para bloqueá-los (Huawei, 2016). Já do lado das aeronaves, deve ser feita a proteção contra a invasão do seu sistema de bordo, por meio de uma autenticação segura e de firewall, de forma a evitar que esta seja controlada remotamente, que seja utilizada para gerar o fluxo de dados excessivo no núcleo da rede.

2.1.2 REDES VSAT EM BANDA KA

Os satélites que formam as redes VSAT possuem alcance continental e podem prover acesso a redes privadas e à Internet sem áreas de sombra nos grandes centros urbanos, gerando assim uma redundância às redes 5G. As redes em Banda Ka trabalham com frequências entre 29 e 30 GHz para uplink (da Terra para o espaço) e entre 17,2 e 20,2 GHz para downlink (no sentido contrário) (Microwaves & RF, 2018), atingindo velocidades de até 50 Mbps no downlink. Aeronaves remotas não tripuladas, como o General Atomics Reaper (General Atomics, 2015), que realizam missões de até 27 horas ininterruptas, utilizam, ao invés da banda Ka, a Banda Ku para comunicação, usando uma faixa de frequência inferior (de 13,75 a 14,5 GHz para uplink e de 10,7 a 12,75 GHz para downlink), entretanto se mostrando menos susceptível aos efeitos atenuantes da chuva, apesar de ter uma taxa de transferência de dados inferior à Banda Ka. A fim de contornar esse problema de atenuação, entende-se que é possível empregar uma maior potência de transmissão na estação terrena e utilizar modulação e codificação adaptativa (Microwaves & RF, 2018) e, assim, aproveitar os benefícios da maior taxa de transmissão das redes em Banda Ka em quaisquer condições atmosféricas.

Um outro ponto importante nas comunicações por satélite é o atraso gerado, em virtude da distância do satélite, o qual geralmente é geoestacionário, ou seja, está posicionado a 36.000 km de altitude. Este atraso, da ordem de dois segundos (Salles, F., janeiro/2020), pode ser mitigado com a utilização de uma rede VSAT do tipo malha (mesh), a qual possibilita a comunicação entre pontos remotos da rede, ao invés da topologia tradicional do tipo hub, na qual há uma estação concentradora, tendo cada ponto que enviar seus dados para esta estação a fim de que sejam retransmitidos para a estação de destino, aumentando assim o percurso.

2.1.2.1 VULNERABILIDADES

Como todo sistema de transmissão de dados baseado em ondas eletromagnéticas, neste também existe a possiblidade de haver a degradação e alteração do conteúdo de forma intencional. No caso específico de transmissões via satélite, isso se mostra possível por meio de sistemas inclusive disponíveis no mercado, os quais foram desenvolvidos para anular a transmissão realizada pelo satélite a partir do solo (Los Angeles Air Force Base. (2020).

Para mitigar tal tipo de ataque, uma alternativa viável é a utilização de feixe de laser para a comunicação da aeronave com o drone. Este experimento está em testes pela Força Aérea dos Estados Unidos, por meio do sistema ALCoS (acrônimo de Airborne Laser Communication System), conectado ao drone MQ-9 Reaper (General Atomics, 2020). Como uma transmissão por laser atua numa faixa de frequência muito maior do que as bandas de micro-ondas (no caso, bandas C, Ku e Ka), a

interferência nesta faixa é extremamente complexa, dificultando qualquer intenção de interrupção ou adulteração de sinal, entretanto devendo estar disponível somente nas fases de decolagem e pouso, bem como nas fases imediatamente anteriores, uma vez que depende de visada direta entre pontos.

2.2 NAVEGAÇÃO

2.2.1 SISTEMAS GNSS

Os sistemas GNSS (acrônimo de Global Navigation Satellite System) têm por função a geração de informação de posição de um determinado terminal, por meio de redes de satélites posicionados em órbitas de média altitude (cerca de 20.000 km), e que, a partir da visualização pelo terminal de pelo menos 3 satélites no espaço, tornar possível realizar a trilateração e consequente cálculo da sua posição (Kaplan, E. D.; Hegarty, C. J., 2006). Com a visualização de um quarto satélite, o sistema também pode calcular a altitude do terminal. Atualmente existem seis sistemas operacionais, lançados por diversos países (GPS, 2020):

- GPS (Global Positioning System), do governo norte-americano, composto por 24 satélites distribuídos em 6 órbitas distintas, que operam nas frequências de 1.575,42 MHz (L1), 1.227,60 MHz (L2) e 1.176,45 MHz (L5), dispondo de serviços para o público civil em geral e para os ramos militares e governamentais do governo norte-americano, onde é inserido um código para encriptação dos dados e aumento da precisão das medidas, fazendo com que o sinal consiga ser lido somente por terminais autorizados (chamado de modo M). O governo norte-americano está implantando atualmente, de forma progressiva, a terceira geração de satélites (chamado de Block III) (GPS, 2020);

- GLONASS (GLObalnaya NAvigatsionnaya Sputnikovaya Sistema – Sistema de Navegação Global por Satélite em russo), serviço disponibilizado pelo governo russo, que é formado por uma constelação de 24 satélites, porém distribuídos em 3 órbitas somente, atuando nas frequências de 1.602 MHz (F1) e 1.246 MHz (F2) (GLONASS, 2020).

- Galileo – Sistema implantado pelo União Européia, tem a previsão de funcionamento de 30 satélites (24 operacionais e 6 de reserva), distribuídos em 3 órbitas, estando atualmente com 22 satélites operacionais. Neste sistema os sinais são distribuídos em 3 faixas (E1, E2 e L1), que operam em 1.575,42 MHz (European Global Navigation Satellite Systems Agency, 2020).

- BeiDou Navigation Satellite System (BDS) (Bússola em chinês), possui uma rede planejada de 35 satélites, dos quais 34 estão operacionais. A diferença deste sistema para os demais é que são utilizadas também órbitas geoestacionárias, além de estabelecer uma comunicação duplex entre os segmentos espacial e terrestre para a realização de medidas de posição dos usuários. A frequência utilizada pelo sistema é de 2.491,75 MHz (BEIDOU, 2020).

- Indian Regional Navigation Satellite System (IRNSS), também chamado de NavIC (acrônimo de Navigation with Indian Constellation), sistema desenvolvido pelo governo indiano, que possui uma constelação de 7 satélites, todos já operacionais, que realizam a cobertura do Oceano Índigo e partes da Ásia e Oceania, além da costa leste da África. Assim como o sistema chinês, há uma mescla de órbitas médias (onde se localizam 4 satélites) e geoestacionárias (contendo os 3 satélites restantes). Opera nas bandas 1.176,45 MHz (L5) e 2492.028 MHz (S) (ISRO, 2020).

- Quasi-Zenith Satellite System (QZSS), também conhecido como Michibiki, desenvolvido pelo governo japonês, tem cobertura regional, atendendo às regiões da Ásia e Oceania. O projeto contempla um conjunto de 7 satélites, dos quais 4 estão operacionais no momento. Estão dispostos em órbita elíptica, e por isso, apesar de estarem a uma altitude de cerca de 42.000 km, não são geoestacionários (QZSS, 2020). Diferentemente dos outros sistemas, seus satélites, na segunda geração, não possuem relógios atômicos embarcados, utilizando para a sincronização de horário um sistema

específico. As frequências utilizadas são compatíveis com o sistema GPS norte-americano.

Na proposta desenvolvida nesse trabalho de framework para os veículos eVTOL, estes sistemas têm um papel preponderante, pois proverão a posição de cada aeronave para que o sistema de controle aéreo possa realizar a gestão das aeronaves em voo, bem como daquelas que aguardam liberação para tal. Para tal utilização, o sistema da aeronave pode utilizar receptores que recebam dados de mais de uma das redes citadas, aumentando, desta forma, a segurança e disponibilidade, uma vez que reduz a possibilidade de perda de sinal com os satélites.

2.2.1.1 VULNERABILIDADES

Devido ao SNR (Signal to Noise Ratio – Relação Sinal-Ruído) ser muito baixo, em função da distância do receptor GNSS até o satélite, estes sistemas se tornam muito suscetíveis à interferência intencionais ou não. Dentre as possíveis interferências, podem ser destacadas (Spirent, 2018):

- Não intencionais – atmosféricas (cintilação e atividade solar), transmissão multicaminho (reflexão do sinal transmitido em edifícios e outros objetos de grande porte) e áreas de campo magnético intenso, como regiões próximas a centrais de conversão de energia, transformadores, linhas de transmissão e torres de celular;

- Intencionais – jamming, que consiste no bloqueio de sinal recebido pelos receptores GNSS, spoofing, que trata do comprometimento da informação recebida por meio de um sinal falso transmitido por um equipamento atacante, adulterando, por exemplo, as coordenadas do ponto que o usuário se encontra e hakking, onde é feita a manipulação da camada de software do dispositivo, com o intuito de interpretação do sinal recebido do satélite.

No que diz respeito às interferências intencionais, foco deste estudo, existem diversas ocorrências de ataques, nas quais houve interrupção de sinal ou comprometimento da informação recebida pelos terminais (Faria, L. A. et al., 2018, Faria, L. A.; Silvestre C. A.; Correia, M. A. F., 2016). Em (Faria, L. A. et al., 2018), foi realizado um estudo com a simulação de um ataque do tipo spoofing, onde foram inseridas coordenadas incorretas em diversos tipos de terminais e analisados os seus resultados. Em terminais de menor complexidade, como GPS veicular e smartphone, a coordenada incorreta foi completamente aceita pelo terminal. Já em terminais mais complexos, como os utilizados em aeronaves, houve a identificação do falso sinal e a negação deste, porém os equipamentos não receberam os sinais corretos, o que poderia deixar vulnerável a navegação da aeronave.

Em (Faria, L. A. et al., 2018) é avaliada a influência do EIRP, (Effective Isotropic Radiated Power, em inglês, ou potência isotrópica radiada equivalente) do transmissor de um equipamento de ataque no alcance deste sinal, com o intuito de realizar jamming, no qual foi verificado o nível de interferência de sinal no receptor, a fim de determinar a distância em que não há impacto do transmissor atacante no receptor, preservando assim a recepção do sinal original.

Como forma de proteção do receptor aos ataques do tipo jamming e spoofing, existem no mercado equipamentos que podem ser agregados à aeronave, tais como o Cobham GPS Anti-Jam (Cobham, 2018). Estes equipamentos realizam a proteção dos códigos C(A), P(Y) e M que compõem o sinal GPS, além dos novos padrões de antena, que possibilitam a identificação da direção de incidência do sinal atacante, preservando a recepção do sinal original.

Outra forma de mitigar o impacto gerado por um ataque nos sistemas GNSS é a utilização do serviço eLORAN (Enhanced Long Range Navigation) (Faria, L. A.; Silvestre C. A.; Correia, M. A. F., 2016), o qual está disponível em grande parte do Hemisfério Norte, sendo constituído por uma grande rede de transmissões terrenas e se diferenciando dos sistemas GNSS por possuir uma alta relação sinal ruído, o que o torna mais difícil de sofrer jamming e spoofing, além de proporcionar

uma cobertura maior, atingindo inclusive espaços cobertos (Stanford University – Dept. of Engineering., 2020).

2.2.2 SISTEMA ADS-B

O sistema de vigilância ADS-B (acrônimo de Automatic Dependent Surveillance – Broadcast) possibilita a recepção e transmissão de dados entre as aeronaves e o centro de controle do espaço aéreo, com as informações referentes a parâmetros de voo como: posição, altitude, velocidade, identificação, radial, destino, origem e razão de subida/descida. Estes dados são coletados dos diversos sensores da aeronave, incluindo o receptor GNSS. Assim, o centro de controle do espação aéreo tem a situação da atitude real e precisa de cada aeronave, dando mais precisão nas atividades, principalmente em regiões com alta densidade de tráfego, aumentando em demasia a segurança do ambiente. Em comparação com os sistemas de radar utilizados atualmente, este sistema representa um grande avanço, pois tem à sua disposição uma quantidade maior de dados em um único sistema, o qual realiza a fusão destes. Na maioria dos ambientes, estes dados são provenientes dos radares primários e secundários, dos controles manuais dos controladores aéreos e de informações trocadas por comunicação de voz entre os pilotos e os controladores, aumentando, desta forma, a probabilidade de erros devido à complexidade do sistema e quantidade de interações realizadas. Há também a questão de custo, na qual o sistema ADS-B se mostra como uma grande redução em relação aos radares empregados atualmente.

Alguns países, como os Estados Unidos, já estão empregando o sistema ADS-B, onde, a partir de janeiro de 2020, todas as aeronaves devem obrigatoriamente utilizar o sistema (Federal Aviation Administration, 2020). No Brasil, ele está em uso na região de Campos, no Rio de Janeiro, nas aeronaves que fazem a ligação entre o continente e as plataformas de petróleo (Departamento de Controle do Espaço Aéreo, 2020).

O sistema possui duas modalidades de comunicação: ADS-B Out, onde a aeronave envia os dados coletados para o centro de controle do espaço aéreo somente. Já na modalidade ADS-B In, a aeronave possui a capacidade de recepção de dados, como de congestionamento do espaço aéreo proveniente do centro de comando e de outras aeronaves, e sendo, desta forma, uma alternativa viável, com complementação dos sistemas TCAS (acrônimo de Traffic Collision Avoidance System – Sistema Anticolisão de Tráfego) atualmente empregados em aeronaves de médio e grande porte. São utilizadas duas frequências distintas: 978 MHz, conhecido como UAT (Universal Access Transceiver), que é o modo mais comum de uso, no qual há a transmissão das informações descritas anteriormente. Na frequência de 1.090 MHz, são utilizados os modos A, C e S nos transponders, podendo transmitir informações adicionais (Federal Aviation Administration, 2016). Nas aeronaves de pequeno porte, é utilizado o sistema TAS (Traffic Advisory/Alerting System), que atua em conjunto com o receptor GPS (UK Airprox Board, 2015).

A presente proposta de implantação de framework do sistema de navegação para as aeronaves eVTOL prevê a utilização de ambos sistemas, ADS-B e TCAS, para aumento da precisão das informações geradas e transmitidas para o centro de controle do espaço aéreo e da redundância, uma vez que um sistema pode atuar em caso de falha do outro. O sistema TCAS opera das frequências de 978 e 1.090 MHz.

3 CONCLUSÃO

Os veículos aéreos movidos a eletricidade têm ganhado relevante espaço no desenvolvimento de novos produtos dos principais fabricantes mundiais de aeronaves, devido não só à economia que podem trazer, mas ainda na redução de emissão de poluentes que proporcionam. Para proporcionar um aumento de capacidade de tráfego aéreo, redução de custos e melhoria na segurança do voo, a automação do voo é um caminho vislumbrado, com diversas pesquisas sendo desenvolvidas pelo mercado, tanto para o meio civil como militar, e já estando previsto para a próxima década. Para tanto, são necessários

serviços de telecomunicações com alta velocidade, segurança, resiliência e baixa latência, tanto para a comunicação da aeronave com o centro de controle como entre aeronaves próximas, além dos sistemas de navegação, que devem ser precisos e altamente disponíveis. Esta pesquisa preliminar descreveu os sistemas que podem ser utilizados para tais aplicações, englobando aqueles sistemas já disponíveis no momento e os que assim estarão no futuro próximo. Caracteriza-se por um estudo preliminar, sendo aprofundado com a definição das adequações necessárias nos sistemas de comunicação às exigências do meio aeronáutico em termos de qualidade e nível de serviço, além de aprofundar o desenvolvimento de medidas de proteção (contra contramedidas eletrônicas) para evitar ataques que possam ser feitos à infraestrutura, tanto nos ambientes eletromagnéticos quanto nos lógicos.

Assim, apesar de neste trabalho termos determinado e mapeado os sistemas passíveis de utilização no framework em pauta, entende-se que maiores detalhamentos serão realizados em trabalhos futuros, nos quais se determinarão a implementação dos sistemas, bem como, por meio de indicadores e relações de compromisso, apresentar-se-ão soluções passíveis de implementação para diferentes cenários, seja de custo, de desempenho, ou de quantidade de infraestrutura, abordando eficiência e segurança em todos eles.

Referências

Automative-iq. (2020). Top five automotive and aircraft industry partnerships. Acesso em 05 jun 2020 de: https://www.automotive-iq.com/autonomous-drive/articles/top-five-automotive-aircraft-industry-partnerships.

Gartner group. (2019). 5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies. Acesso em 17 fev 2020 de: https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019/.

Flytrex. (2020). Acesso em 05 jun 2020 de: https://flytrex.com/

EMBRAER X. Flight Plan 2030. Acesso em 04 nov 2019 de: https://embraerx.embraer.com/global/en

Ministério da Ciência, Tecnologia, Inovações e Comunicações (2019). Estratégia Brasileira de Redes de Quinta Geração (5G). Acesso em 28 abr 2020 de: https://www.mctic.gov.br/mctic/opencms/sessaoPublica/sessao_publica/estrategia5g.html

One Web. (2020). Acesso em 04 jun 2020 de: https://www.oneweb.world/

Starlink. (2020). Acesso em 04 jun 2020 de: https://www.starlink.com/

Spacenews. (2019). Amazon planning 3,236-satellite constellation for internet connectivity. Acesso em 04 jun 2020 de: https://spacenews.com/amazon-planning-3236-satellite-constellation-for-internet-connectivity/

Yaacoub, J. et al. (2020). Security analysis of drones systems: Attacks, limitations and recommendations. Beirute: Elsevier Enhanced Reader, 39p.

Keysight Technologies. (2018). The ABCs OF 5G New Radio Standards. Acesso em 28 abr 2020 de: https://www.keysight.com/br/pt/assets/7018-06362/ebooks/5992-3406.pdf

Keysight Technologies. (2018). 5G New Radio Standards. Acesso em 02 mai 2020 de: https://www.keysight.com/br/pt/assets/7018-06362/ebooks/5992-3406.pdf

Neto, E. et al. (2019). Trajectory-based Urban Air Mobility (UAM) Operations Simulator (TUS). São Paulo: Escola Politécnica USP, 32p.

Huawei. (2016). Huawei AntiDDoS8000 DDoS Protection System. Acesso em 20 mai 2020 de: https://carrier.huawei.com/en/products/fixed-network/b2b/Security/DDoS-Protection-System/AntiDDoS8000

Microwaves & RF. (2018). What Makes Ka-band Systems Tick?. Acesso em 07 mai 2020 de:

https://www.mwrf.com/technologies/systems/article/21849025/what-makes-kaband-systems-tick
General Atomics (2015). General Atomics MQ-9 Reaper / Predator B Data Sheet. 2015. Acesso em 07 mai 2020 de: https://www.ga-asi.com/images/products/aircraft_systems/pdf/Predator_B021915.pdf
Salles, F. (janeiro/2020). O Ataque ao Líder Militar do Irã. Aero Magazine, São Paulo, ano 25, ed. 308, pag 70-74.
Los Angeles Air Force Base. (2020) Counter Communications System Block 10.2 achives IOC, ready for the dogfihter. Acesso em 20 mai 2020 de: https://www.losangeles.af.mil/News/Article-Display/Article/2111775/counter-communications-system-block-102-achieves-ioc-ready-for-the-warfighter/
General Atomics. (2020). GA-ASI Successfully Tests Air-To-Space Laser Communication System. Acesso em 27 abr 2020 de: http://www.ga.com/ga-asi-successfully-tests-air-to-space-laser-communication-system
Kaplan, E. D.; Hegarty, C. J. (2006). Understanding GPS: Principles and Applications. 2nd. Ed. Mariland: Artech House. 703 p.
GPS. (2020). Acesso em 05 jun 2020 de: https://www.gps.gov/systems/gnss/
GPS. (2020). Acesso em 05 jun 2020 de: https://www.gps.gov/systems/gps/space/
GLONASS. (2020). Acesso em 05 jun 2020 de: https://www.glonass-iac.ru/en/
European Global Navigation Satellite Systems Agency. (2020). Acesso em 05 jun 2020 de: https://www.gsa.europa.eu/
BEIDOU. (2020). Acesso em 05 jun 2020 de: http://en.beidou.gov.cn/.
ISRO. (2020). Acesso em 05 jun 2020 de: https://www.isro.gov.in/irnss-programme
QZSS. (2020). Acesso em 05 jun 2020 de: https://qzss.go.jp/en/
Spirent. (2018) Fundamentals of GPS Threats. Acesso em 16 mai 2020 de: https://www.spirent.com/-/media/white-papers/positioning/fundamentals-of-gps-threats.pdf
Faria, L. A. et al. (2018). Susceptibility of GPS–Dependent Complex Systems to Spoofing. São José dos Campos: Instituto Tecnológico de Aeronáutica, 11 p.
Faria, L. A.; Silvestre C. A.; Correia, M. A. F. (2016). GPS-Dependent Systems: Vulnerabilities to Eletromagnetic Attacks. São José dos Campos: Instituto Tecnológico de Aeronáutica, 11 p.
Faria, L. A. et al. (2018). GPS Jamming Signal Propagation in Free-Space, Urban and Suburban Environments. São José dos Campos: Instituto Tecnológico de Aeronáutica, 8 p.
Cobham. (2018). Cobham GPS Anti-Jam Solutions for Air, Land and Sea Datasheet. Acesso em 08 abr 2019 de: https://www.cobham.com/media/2059118/anti-jam-gps-family-brochure-web.pdf
Stanford University – Dept. of Engineering. (2020). LORAN and eLoran. Acesso em 19 mai 2020 de: https://gps.stanford.edu/research/early-research/loran-and-eloran
Federal Aviation Administration. (2020). Acesso em 05 jun 2020 de: https://www.faa.gov/nextgen/programs/adsb/
Departamento de Controle do Espaço Aéreo. (2020). Acesso em 05 jun 2020 de: https://www.decea.gov.br/?i=midia-e-informacao&p=pg_noticia&materia=sistema-ads-b-comeca-a-operar-na-bacia-de-campos
Federal Aviation Administration (2016). Pilot´s Handbook of Aeronaltical Knowledge. Oklahoma City: 524 p.
UK Airprox Board. (2015). ACAS/TCAS/TAS. Acesso em 18 mai 2020 de: https://www.airproxboard.org.uk/Topical-issues-and-themes/ACAS/TCAS/TAS/