P-ISSN:2527-5321
E-ISSN:2527-5941

RANCANGAN APLIKASI ADS-B PADA UAV DAN DRONE KOMERSIL DENGAN RASPBERRY PI 3B

Abdul Azzam Ajhari[1], Juliadi Satyo Pramudito[2], Jonatan Reky Tasyam[3]

[1,2,3]*Badan Siber dan Sandi Negara*
Jl. Harsono RM No.70, Ragunan, Kec. Pasar Minggu, Kota Jakarta Selatan, DKI Jakarta. 12550.
[1]abdul.azzam@bssn.go.id, [2]juliadi.satyo@bssn.go.id, [3]jonatan.reky@bssn.go.id

ABSTRAK

Meningkatnya antusiasme masyarakat dalam menggunakan *Unmanned Aerial Vehicles* (UAV) atau *drone* untuk melakukan kegiatan dengan mudah dan cepat dapat membahayakan keselamatan dan keamanan penerbangan, terutama infrastruktur kritis yang ada di Indonesia. Kerentanan yang dapat membahayakan keselamatan dan keamanan adalah *ketika UAV* atau *drone* diterbangkan pada area Kawasan Keselamatan Operasi Penerbangan (KKOP) tanpa izin. Selain itu, UAV atau *drone* dapat melakukan pengintaian untuk mengumpulkan informasi dalam melakukan aksi berbahaya di kemudian hari ketika melewati batasan wilayah yang telah diatur pada Peraturan Pemerintah (PP) Nomor 4 Tahun 2018 tentang Pengamanan Wilayah Udara Republik Indonesia. Diperlukan pengaplikasian *Automatic Dependent Surveillance-Broadcast* (ADS-B) pada UAV dan *drone* komersil untuk menunjukkan lokasi dengan menggunakan navigasi *Global Positioning System* (GPS). Selain GPS, UAV dan *drone* melakukan pengiriman data mengenai keakuratan lokasi dan data penerbangan seperti ketinggian dan kecepatan, kepada peralatan pendukung yang melakukan pemantauan melalui frekuensi ADS-B. Perangkat ADS-B *prototype* yang dibuat menggunakan komputer ringkas Raspberry PI 3B yang berbasis Linux dengan bahasa pemrograman Python dalam pengaplikasiannya. Dengan jaringan berbasis *Internet Protocol* (IP), ADS-B dapat melakukan pengiriman data informasi melalui frekuensi radio yang dapat diaplikasikan pada UAV dan *drone* dan mengelolanya pada server internal guna meningkatkan *zero accident* pada infratruktur kritis yang ada di Indonesia.

Kata Kunci: UAV, *drone*, ADS-B, GPS, KKOP.

ABSTRACT

Increased public enthusiasm in using Unmanned Aerial Vehicles (UAVs) or drones to carry out activities easily and quickly can endanger the safety and security of aviation, especially the critical infrastructures in Indonesia. Vulnerabilities can put the safety and security in jeopardy when UAVs or drones are flown in the Aviation Operation Safety Area (AOSA) without permission. In addition, UAVs or drones can conduct surveillance to collect information in carrying out dangerous actions in the future when they cross the boundaries stipulated in the Government Regulation (PP) No.4 of 2018 concerning Safeguarding the Republic of Indonesia's Airspace. Automatic Dependant Surveillance-Broadcast (ADS-B) application on commercial UAVs and drones is needed to show location using Global Positioning System (GPS) navigation. In addition to GPS, UAVs and drones transmit data on location accuracy and flight data such as altitude and speed to the supporting equipment that monitors through the ADS-B frequency. The ADS-B device prototype is made using a Linux-based Raspberry PI 3B compact computer with the Python programming language in it's application. With Internet Protocol (IP) based network, ADS-B can send information data through radio frequencies that can be applied to UAVs and drones and manage it on internal servers to increase zero accidents on critical infrastructure in Indonesia.

Keyword: UAVs, drones, ADS-B, GPS, AOSA.

PENDAHULUAN

Frekuensi radio menjadi sebuah teknologi yang mendapatkan perkembangan signifikan dan sangat cepat, melingkupi banyak bidang termasuk infrastruktur jaringan dalam navigasi penerbangan. "ADS-B merupakan bagian dari teknologi CNS/ATM (*Communication Navigation Surveillance/Air Traffic Management*) yang menunjukkan lokasi pesawat menggunakan navigasi satelit GPS dan memungkinkan pesawat untuk mengirimkan lokasi akurat pesawat dan data penerbangan (seperti ketinggian dan kecepatan) ke pesawat terdekat dan Air Traffic Control (ATC)". (Kurniawan, A. P., & D.W. Sumari, A., 2010)

P-ISSN:2527-5321
E-ISSN:2527-5941

Selain GPS, UAV dan *drone* melakukan pengiriman data mengenai keakuratan lokasi dan data penerbangan seperti ketinggian dan kecepatan, kepada peralatan pendukung yang melakukan pemantauan melalui frekuensi ADS-B.

"Ketika sebuah UAV memasuki kawasan yang dilarang dimasuki, seperti bandar udara, tempat yang memiliki privasi maupun tempat yang membutuhkan tingkat keamanan yang tinggi, maka diperlukan cara untuk menghentikan UAV. Beberapa cara untuk menghentikan UAV, yaitu dengan menghentikan secara fisik UAV atau bisa melalui media komunikasi yang digunakan oleh UAV". (Hanif, M., 2018)

Kebijakan pengamanan Wilayah Udara Republik Indonesia yang telah diatur pada PP Nomor 4 Tahun 2018 belum cukup kuat untuk mencegah pelanggaran dalam penggunakan UAV atau *drone* di masyarakat. Tidak teridentifikasinya UAV atau *drone* yang beredar dan masyarakat yang tidak memiliki sertifikasi untuk menerbangkan, menjadi penyebab banyaknya kasus ini mengancam keselamatan dan keamanan infrastruktur kritis di Indonesia.

"Dibutuhkan sistem untuk mengelola data ADS-B dan radar pada suatu perangkat jaringan. NMS (*Network Monitoring System*) merupakan suatu sistem yang dapat digunakan untuk mengelola perangkat-perangkat jaringan berbasis IP." (Alip, N., Fitri, I., & Nathasia, N. D., 2018)

Data yang diterima melalui frekuensi radio ADS-B kemudian diproses untuk disimpan di server internal melalui protokol SNMP (*Simple Network Management Protocol*) untuk mengelola dan mengatur kinerja perangkat jaringan secara jarak jauh. Dengan jaringan berbasis IP (*Internet Protocol*), ADS-B dapat melakukan pengiriman data informasi melalui frekuensi radio yang dapat diaplikasikan pada UAV dan *drone* dan mengelolanya pada server internal guna meningkatkan *zero accident* pada infratruktur kritis yang ada di Indonesia.

METODE PENELITIAN

Pada metodologi ini diambil teknik yang ada pada Python *library* untuk dilakukan *decoding* pesan dalam bentuk Mode-S. *Library* ini mendukung *Downlink Formats* (DF), dimana ADS-B yang dibuat dengan komputer ringkas Raspberry PI 3B menggunakan format DF17 yang berisi informasi data pesawat berupa ICAO *address*, *position*, *altitude*, *velocity* (*ground speed*), *callsign*, dll.
Dalam setiap pesan ADS-B, pengirim (pesawat asal) dapat diidentifikasi menggunakan alamat ICAO.

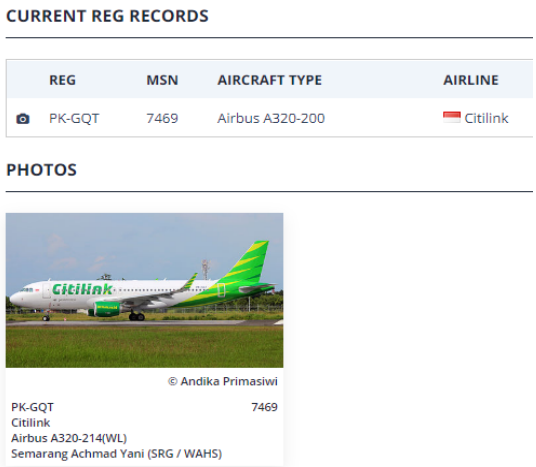
Tabel 1. Identifikasi Pengirim Pesan Pesawat Asal

ICAO address	**8A061E**
Kode Biner	100010100000

Kode tersebut terletak dari 9 hingga 32 bit dalam biner (atau 3 hingga 8 dalam heksadesimal). Alamat ICAO diberikan untuk setiap transponder Mode-S dari sebuah pesawat. Kode ini adalah sebuah pengidentifikasi unik untuk setiap UAV/ *drone* yang akan diaplikasikan. Alamat ICAO tersimpan untuk dapat dilakukan manajemen, seperti contoh tabel diatas dapat diketahui data pesawat dan penerbangannya sebagai berikut:

Tabel 2. Data Pesawat dengan ICAO 8A061E

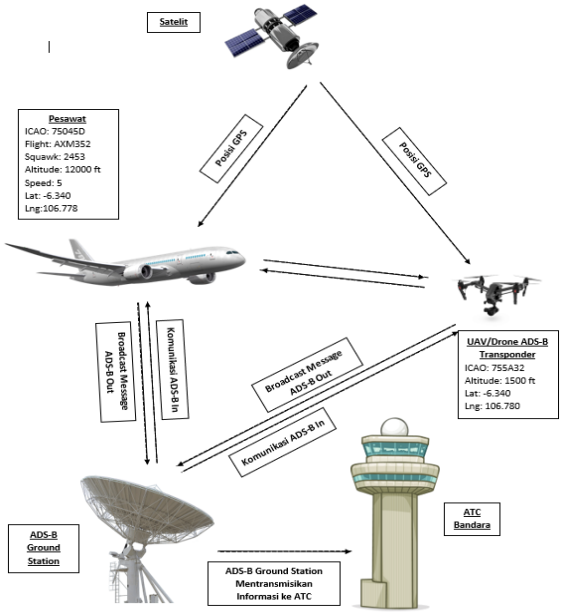
8A061E	
Mode S Code / ICAO 24-bit Aircraft Address	
Hex	8A061E
Decimal	9045534
Octal	42403036
Binary	100010100000011000011110 Bit-reversed 011110000110000001010001
Country	Indonesia



Gambar 1. Riwayat Tersimpan Reg ICAO 8A061E

P-ISSN:2527-5321
E-ISSN:2527-5941

UAV/ *drone* memiliki prospek dalam pengaplikasian ADS-B Transponder yang akan menambah pemasukan negara melalui pajak penggunaan wilayah udara dan sertifikasi pilot yang dapat diberlakukan. Selain itu ADS-B yang ditanamkan dapat mencegah UAV/ *drone* melanggar batasan wilayah yang telah ditentukan.



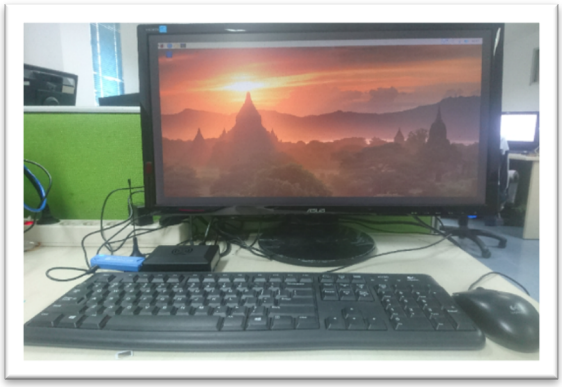
Gambar 2. Komunikasi UAV/Drone ADS-B Transponder

Satelit hanya mengirimkan data GPS atau berperan sebagai GNSS (*Global Navigation Satellite System*) kepada pesawat dan UAV/ *drone* komersil yang telah terpasang ADS-B Transponder. Pesawat dapat melakukan komunikasi dengan pilot UAV/ *drone* melalui frekuensi radio secara langsung atau melalui ADS-B *Ground Station* jika jarak tidak terjangkau. ATC hanya bertugas menerima informasi dari ADS-B *Ground Station* dan melakukan pemantauan lalu lintas penerbangan. UAV/ *drone* yang memiliki ADS-B Transponder hanya boleh dikendalikan oleh pilot yang memiliki izin penerbangan di wilayah tertentu.

HASIL DAN PEMBAHASAN

Pembuatan ADS-B Receiver

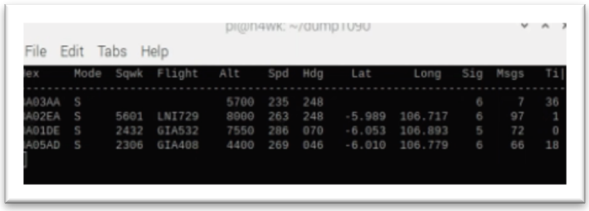
Untuk membuat ADS-B *receiver* atau ADS-B *Ground Station* menggunakan Raspberry PI 3B, tahapan yang dapat dilakukan sebagai berikut:



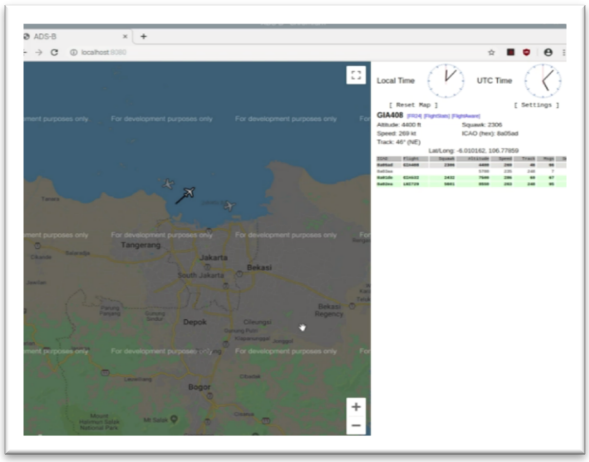
Gambar 3. Raspberry ADS-B Receiver

A. Melakukan Instalasi RTL-SDR
B. Melakukan Instalasi Dump978 dan Dump1090

Aplikasi Dump978 dan Dump1090 yang diinstal pada Raspberry berfungsi untuk menangkap data ADS-B yang dikirimkan oleh pesawat dan UAV/ *drone*, dimana data dapat dilihat dalam bentuk terminal dan diakses melalui browser.



Gambar 4. Tampilan terminal ADS-B Receiver



Gambar 5. Tampilan browser ADS-B Receiver

Pembuatan ADS-B Transponder

Dalam penelitian ini, ADS-B Transponder *prototype* yang dibuat bertujuan untuk meningkatkan *zero accident* pada infrastruktur kritis dalam mendukung keselamatan dan keamanan terutama di sektor penerbangan yang telah diatur pada PP Nomor 4 Tahun 2018.

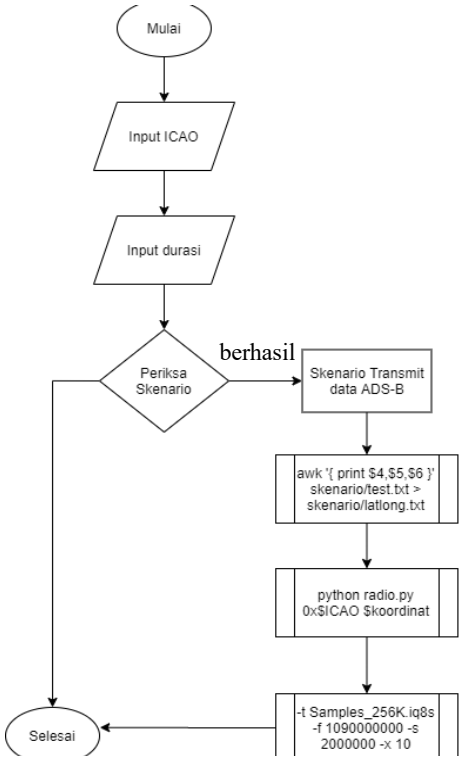
P-ISSN:2527-5321
E-ISSN:2527-5941

ADS-B Transponder yang diteliti dan dilakukan uji coba saat ini mampu melakukan transmit kode ICAO *address* dengan posisi (*latitude* dan *longitude*) yang telah ditentukan untuk ditransmisikan melalui frekuensi 1200 Hz.

Gambar 6. Simulasi ADS-B Transponder

Simulasi dilakukan menggunakan peralatan sebagai berikut:

A. Laptop dengan Sistem Operasi Linux
B. Perangkat Radio Frekuensi *Transmitter*
C. Kemampuan bahasa pemrograman Python untuk membuat skrip.



Gambar 7. Flowchart proses kerja ADS-B transponder

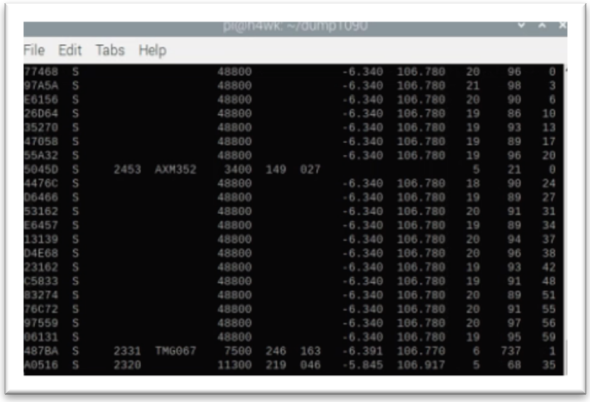
Flowchart diatas menjelaskan secara ringkas cara kerja DF17 ADS-B dengan menggunakan *library* Python yang diaplikasikan ke dalam UAV/ drone.

```
type | time | latitude | longitude | altitude (m) | color | name | desc
T | 2018-10-10 11:44:34 | -6.133076437 | 106.653217189 | 21.7 | Blue | FR CITYLINK JKT-BALI
```

Gambar 8. Data NMEA Pesawat Asli untuk POC *Prototype* ADS-B Transponder

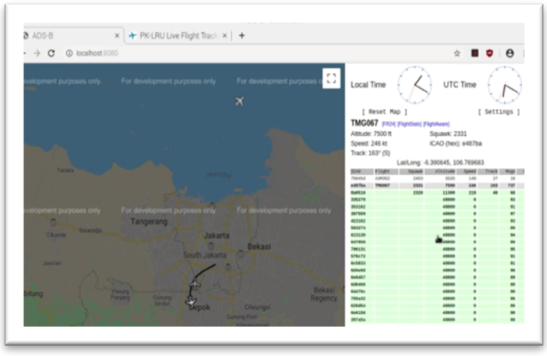
Posisi (*Latitude* dan *Longitude*) dilakukan simulasi secara statis menggunakan rekaman data NMEA (The National Marine Electronics Association) dengan fokus penerbangan terbatas dan dapat dibuat dinamis ketika UAV/ *drone* memiliki sistem GPS.

Frekuensi yang ditransmisikan ADS-B Transponder untuk UAV/ *drone* diperlakukan sama dengan ADS-B pesawat untuk uji coba deteksi pada frekuensi 1200 Hz, sehingga dapat dilakukan pemantauan dalam membedakan ADS-B nya.



Gambar 9. Data Informasi ADS-B Transponder Pesawat dan UAV/ drone

Data tersebut dapat terdeteksi dan menampilkan ikon pesawat penerbangan baik pesawat asli atau UAV/*drone* pada browser sebagai berikut:

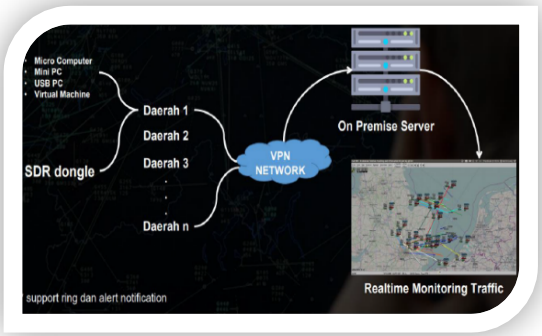


Gambar 10. Tampilan Browser Deteksi Pesawat dan UAV/ drone

P-ISSN:2527-5321
E-ISSN:2527-5941

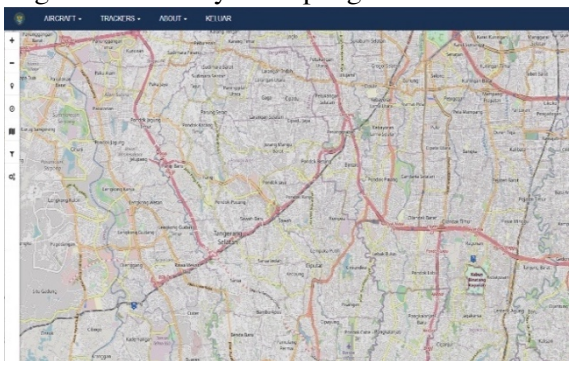
Pembuatan Server Internal

Server dibuat dengan menggunakan NMS yang berbasis IP, sehingga data dapat diproses dan dikontrol dalam sistem manajemennya. NMS sendiri diterapkan pada ADS-B *Ground Station* yang dapat berupa komputer ataupun Raspberry untuk bekerja selama 24 jam setiap hari. Server menggunakan protokol autentikasi Kerberos yang kami beri nama *Private Network VPS Router* (PNVR). PNVR dapat dikatakan sebagai *firewall* sebelum penyerang mencapai pintu server internal yang hanya dapat diakses menggunakan internet lokal kantor. Namun pada penelitian ini, kami hanya memfokuskan pada pengaplikasian *prototype* ADS-B transponder.



Gambar 11. Topologi PNVR Server

Selain sebagai server untuk menyimpan data transportasi udara, PNVR saat ini digunakan sebagai alat dukung untuk mendeteksi frekuensi radio yang berada di kantor BSSN Ragunan dan wilayah Serpong.



Gambar 12. ADS-B yang terkoneksi dengan PNVR

SIMPULAN DAN SARAN

Dari pembahasan sistem ADS-B *prototype* untuk pengaplikasian pada UAV/ *drone* komersil dalam makalah ini, dapat diambil kesimpulan bahwa:

1. ADS-B dapat diaplikasikan untuk mengirimkan data penting termasuk komunikasi antara pesawat dan UAV/ *drone* ke stasiun darat.
2. Pemerintah akan mendapatkan anggaran tambahan melalui pajak wilayah udara yang digunakan oleh UAV/ drone dan sertifikasi pilot-nya dengan sistem masa berlaku.
3. Diperlukan regulasi kebijakan yang baru mengenai celah keamanan dan keselamatan-nya pada sektor penerbangan transportasi udara.
4. Berdasarkan penelitian Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L., & Poovendran, R. yang dilakukan pada tahun 2019 kerentanan keamanan yang dapat terjadi pada ADS-B adalah *Aircraft Spoofing Attack*. Rancangan topologi PNVR Server dapat mencegah penyerangan *Aircraft Spoofing Attack* dengan melakukan verifikasi data pesawat ketika melewati tiap-tiap ADS-B yang dimana datanya tersimpan pada *database* server dengan menggunakan protokol autentikasi Kerberos.
5. Penelitian dan pengujian kerentanan yang telah dilakukan menggunakan *Radio Frequency Transmitter* dengan SDR pada ADS-B dapat melakukan serangan untuk menginterferensi radio komunikasi antara pesawat dengan stasiun darat, DOS *Attack* pada sistem *Air Traffic Monitoring* sampai dengan Duplikasi pesawat (*Replay Attack*) dimana sebelumnya sudah ada penelitian yang dilakukan oleh (Costin, A., & Francillon, A pada, 2012). Dengan demikian dibutuhkan sebuah pedoman *Security Advisory* untuk membatasi penggunaan perangkat berbahaya yang dapat menjadi acuan dan landasan untuk memperkuat infrastruktur kritis terutama pada sektor penerbangan.Perangkat ADS-B yang dibuat untuk diimplementasikan pada UAV/*drone* masih *prototype* dan memiliki kekurangan dari segi fisiknya yang besar, berat, dan fungsi yang di transmisikan terbatas. Diperlukan pengembangan kedepan untuk menghasilkan produk yang dapat digunakan dengan mudah, ringan dan fungsi transmisi yang lebih baik dengan melakukan kerja sama dengan pihak industri lokal.

P-ISSN:2527-5321
E-ISSN:2527-5941

DAFTAR PUSTAKA

Alip, N., Fitri, I., & Nathasia, N. D. (2018). Network Monitoring System Data Radar Penerbangan berbasis PRTG dan ADSB. *JOINTECS (Journal of Information Technology and Computer Science)*, *Vol. 3*(No. 3), 267–272.

Costin, A., & Francillon, A. (2012). Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. *Black Hat USA*, *July 2012*, 1–10.

Hanif, M. (2018). Analisis Sinyal Komunikasi UAV Menggunakan SDR. *Skripsi Jurusan Teknik Elektro, Fakultas Teknik Universitas Lampung*.

Kurniawan, A. P., & D.W. Sumari, A. (2010). Automatic Dependent Surveillance-Broadcast dan Prospek Pengaplikasiannya di TNI-AU. *AAU Journal of Defense Science and Technology*, *Volume 1*(Number 2), 61–66

Leonardi, M., Piracci, E., & Galati, G. (2014). ADS-B vulnerability to low cost jammers: Risk assessment and possible solutions. *2014 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles, TIWDC/ESAV 2014*, 41–46.

Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L., & Poovendran, R. (2019). Detecting ADS-B Spoofing Attacks Using Deep Neural Networks. *2019 IEEE Conference on Communications and Network Security, CNS 2019*, 187–195.