ISSN 2355-3286

Metode Deteksi '*Potential Security Threats*' Pada ADS-B Data dengan Memonitor EM Emisi Radiasi pada Jaringan Ethernet

Reza Septiawan*[1], I Made Astawa[2], Arief Rufiyanto[3], Tahar Agastani[4], Rizky Rahmatullah[5], Ahmad Mundhola[6]
ElectroMagnetic Compability Laboratorium: PTE (Centre of Electronics Technology)
BPPT (Badan Pengkajian dan Penerapan Teknologi/Indonesian Agency for the Assessment and Application of Technology), Indonesia
reza.septiawan@bppt.go.id
made.astawa@bppt.go.id
arief.rufiyanto@bppt.go.id
tahar.agastani@bppt.go.id

Diterima 1 Juni 2019
Disetujui 24 Juni 2019

***Abstract*-Precision, Navigation, and Timing (PNT) system based on Global Navigation Satellite System (GNSS) becomes significant in the air traffic management, especially in the use of Automatic Dependent Surveillance Broadcast system (ADS-B) for air traffic monitoring. Therefore the integrity of GNSS is significant to provide a reliable data necessary for ADS-B. GNSS Interference due to intentional or unintentional surrounding signal source may decrease the integrity of GNSS signal and therefore may result in the in-accurate position data of ADS-B message. ADS-B message itself is also vulnerable from potential security threats in their network. This paper proposed a methodology to detect potential security threats of ADS-B network system for both GNSS signal and ADS-B data by measuring and monitoring the electromagnetic radiated emission from ethernet cable IPv4 Cat5.**

Index Terms- Security Threats, ADS-B, GNSS, radiated emission, electromagnetic, unintentional interference, radio disturbance characteristics

I. PENDAHULUAN

Permasalahan terkait aspek keamanan pada pemanfaatan ADS-B sebagai *surveillance system* pada *air traffic management* mulai dirasakan meningkat dengan meningkatnya penggunaan ADS-B pada pesawat-pesawat komersial. Dimana data ADS-B dapat secara terbuka diterima oleh pengguna serta secara terbuka format data dari ADS-B message dapat diakses oleh umum. Pada pesawat komeresial digunakan *SSRMode-S with extended squitter* yang merupakan kombinasi dari ADS-B data dengan format tradisional *surveillance system*, Mode-S dan disebut 1090ES. Sehingga ADS-B dapat diintegrasikan dengan *Mode-S transponder*. Format *ADS-B message* 1090ES digambarkan pada gambar 1 dimana struktur datalink nya pada gambar 2 [1]. 1 frame data=8 microsecond preamble dan 112 microsecond data blok nya (total 120 microsecond per dataframe)

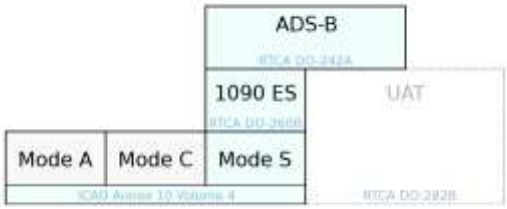


Figure 1. ADS-B hierarchy [1]

Gambar 1 ADSB-message [1]

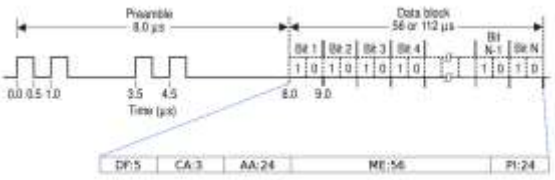


Figure 2. 1090 ES Data Link [1]

Gambar 2. Data link ADS-B [1]

Selain kemungkinan serangan terhadap ADS-B system pada lapisan jaringan system manajemen lalu lintas, perlu juga diperhatikan kemungkinan serangan terhadap sinyal GNSS yang menjadi masukan untuk lokasi pada data ADS-B. *Integrity* dari sinyal GNSS sangat penting untuk memastikan

ketersediaan dan *reliability* dari data navigasi dan informasi dari *air traffic management*.

ADS-B system dirancang tanpa memperhatikan aspek keamanan dan kerentanannya terhadap ancaman dari luar. Penjelasan perihal potensi ancaman yang mungkin dihadapi dalam ADS-B system dibahas pada [2]. Apabila tidak diantisipasi lebih dahulu maka potensi ancaman terhadap system ADS-B dapat mengganggu keamanan pengaturan lalu lintas udara serta keselamatan pilot serta penumpangnya. Makalah ini mencoba memberikan salah satu alternative metode untuk mendeteksi potensi ancaman terhadap system ADS-B dengan cara memonitor emisi pada kabel UTP untuk mendeteksi perubahan karakteristik lalu lintas data pada system ADS-B yang dapat mengindikasikan adanya potensi serangan terhadap system ADS-B. Selain itu dengan memperhatikan potensi interferensi sinyal GNSS di sekitar lokasi ADS-B maka dapat mengurangi kemungkinan terjadinya gangguan pada system ADS-B.

Pada [3] dibahas pula salah satu cara untuk mencoba mengamankan system ADS-B dengan menggunakan ADS-Bsec (ADS-B secured) secara pengamanan menggunakan key management infrastructure. Sedangkan pada metode dalam makalah ini pengamanan dilakukan baik dengan menentukan penempatan ADS-B pada lokasi yang relative potensi interferensi nya kecil serta memonitor perubahan emisi pada kabel UTP nya. Diharapkan metode ini dapat lebih awal memitigasi kemungkinan potensi gangguan pada system ADS-B.

Makalah ini akan membahas metode untuk mendeteksi potensi gangguan pada ADS-B message yang digunakan pada pesawat komersil dengan memonitor emisi elektromagnetik yang diradiasikan dari kabel ethernet IPv4 Cat 5. Pembahasan dimulai dengan identifikasi potensi gangguan pada lapisan jaringan air traffic management serta gangguan pada sinyal GNSS.

II. METODE PENELITIAN

Dalam rangka mendeteksi potensi gangguan pada ADS-B message maka dilakukan penelitian terkait potensi gangguan yang dapat muncul pada jaringan ADS-B maupun pada sinyal GNSS. Gangguan terkait sinyal GNSS akan berupa potensi RFI sedangkan gangguan terkait pengiriman data ADS-B dengan cara mengukur emisi radiasi elektromagnetik dari kabel ethernet IPv4 Cat 5 dengan load minimum (32 bytes) sebagai representasi dari jaringan ADS-B yang normal, serta mengukur emisi radiasi elektromagnetik dari kabel ethernet IPv4 Cat 5 pada saat load nya mencapai 10Kbytes sebagai representasi lonjakan traffic yang potensial disebabkan oleh meningkatnya serangan berupa message injection/spoofing pada jaringan ADS-B. Berdasarkan data hasil pengukuran tersebut akan dianalisa kemungkinan untuk membandingkan nilai emisi radiasi elektromagnetik dari kabel ethernet dengan load minimum dibandingkan dengan kabel ethernet dengan *load maximum*. Sebagai *testbed* digunakan tiga modul ADS-B receiver yang menerima secara bersamaan di lab PTE BPPT untuk kemudian dikirimkan datanya ke server.

A. Potensi gangguan pada data ADS-B

Identifikasi potensi gangguan data ADS-B pada jaringan air traffic.

Terdapat dua ukuran panjang ADS-B message sesuai yang dispesifikasikan pada Mode S yaitu 56 bit dan 112 bit. Pada ADS-B message menggunakan 112bit format. Dalam rangka menjaga keamanan ADS-B pada jaringan system lalu lintas udara, maka harus diperhatikan integrity dari:

a. *Data Integrity*: memastikan bahwa data yang dikirimkan oleh pengirim adalah sama dengan yang diterima dan tidak dimodifikasi oleh pihak lain

b. *Source integrity*: memastikan bahwa data yang diterima berasal dari pengirim yang mengklaim sebagai pengirim yang legitimate

c. *Data origin authentication* memastikan bahwa data yang diterima berasal dari lokasi yang diklaim oleh pengirim

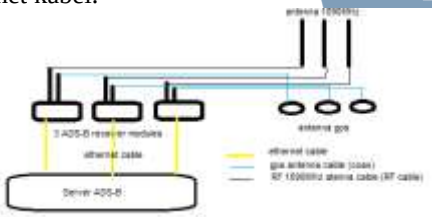
Dalam rangka memastikan hal tersebut diatas diperlukan untuk mengidentifikasi potensial serangan-serangan yang mungkin dihadapi oleh ADS-B system. Pada [4] dibahas perihal jenis-jenis serangan yang dapat membahayakan keamanan dari ADS-B datalink:

- *Eavesdropping:* merupakan jenis serangan terhadap keamanan pada jaringan datalink ADS-B berupa menyadap unsecured broadcast transmissions. Jenis serangan ini disebut pula Aircraft Reconnaissance
- *Jamming:* merupakan jenis serangan yang relative mudah dengan menggunakan single node (baik ground station ataupun pesawat) atau area dengan lebih dari beberapa node untuk membuat tidak berfungsinya node tersebut untuk mengirim dan menerima ADS-B message dengan cara mengirim signal dengan relative

daya yang besar pada 1090MHz frequency pada Mode S.

- *Message injection*: merupakan jenis serangan yang digunakan untuk menginjeksi non legitimate messages pada jaringan system lalu lintas udara. Berhubung tidak tersedianya pengecekan authentikasi yang diimplementasikan pada lapisan datalink, maka dengan mudah penyerang membuat replica data ADS-B sesuai format ADS-B message untuk kemudian diinjeksi pada system.

Pada makalah ini akan mencoba untuk mendeteksi *potensial security threat* pada data yang berupa serangan jamming ataupun message injection. Pada kedua jenis serangan ini terjadi lonjakan jumlah data (data transmission load) yang besar sekali pada kabel Ethernet. Sebagai testbed digunakan 3 modul ADS-B receiver yang masing-masing terkoneksi dengan antenna GPS dan mengirimkan data ADS-B ke server melalui Ethernet cable. Pengamatan dilakukan selama 15 menit untuk memantau jumlah data yang ditransmisikan pada saat tersebut dalam rangka memperoleh gambaran normal load data pada Ethernet kabel.



Gambar 3 Konfigurasi pengujian

Gambar 4 Modul ADS-B receiver beserta antenna GPS dan antenna RF 1090 dan Ethernet kabel dari modul ADS-B receiver ke server

Gambar 5 Server penerima dan display tampilan ADS-B data

Berdasarkan pengamatan yang dilakukan selama 934 detik (15.567 menit) dimulai dari tanggal 18 juni 2019 jam 12:09:05 s/d 12:24:39. Pengiriman data ADS-B dilakukan sesuai dengan format ADS-B dimana 1 frame data ADS-B teridiri dari 8bit preamble dan 112 bits data ADS-B akan dikirimkan dengan kecepatan 120µsec perframe data. Selama periode pengamatan tersebut diperoleh data ADS-B sebanyak 104.857 valid data dari ketiga modul ADS-B receiver. Maka selama periode pengamatan tersebut jaringan Ethernet akan dibebankan oleh transmisi data dari ketiga modul ADS-B receiver ke ADS-B server dengan beban sebesar 1.684 bytes persecond (1,684kBps). Sehingga dengan asumsi bahwa terjadi peningkatan arus lalu lintas penerbangan 2x lipat dari arus lalu lintas penerbangan pada saat pengamatan, akan terjadi lonjakan menjadi sekitar 4kbps pada kabel Ethernet yang menghubungkan ketiga modul ADS-B receiver dengan ADS-B server.

Sehingga apabila terjadi lonjakan beban transmisi data yang melebihi dari 4kbps pada kabel jaringan di lokasi pengamatan, dapat diasumsikan terjadi anomaly yang salah satunya dapat disebabkan oleh *potensi security threat* dengan jenis jamming atau message injection.

B. Identikasi gangguan interferensi pada sinyal GNSS

Selain kemungkinan serangan terhadap ADS-B system pada lapisan jaringan system manajemen lalu lintas, perlu juga diperhatikan kemungkinan serangan terhadap sinyal GNSS yang menjadi masukan untuk lokasi pada data ADS-B. Integrity dari sinyal GNSS sangat penting untuk memastikan ketersediaan dan reliability dari data navigasi dan informasi dari air traffic management. Beberapa makalah telah membahas perihal software Analisa untuk melihat integrity dari sinyal GNSS seperti GAMIT [5] dan GLOBIT [6] demikian juga perihal integrity sinyal GPS L1 maupun L2 di Merapi [7]. Integrity dari sinyal GNSS sangat mudah diganggu oleh interferensi dikarenakan lemahnya kekuatan sinyal GNSS (-132dBW/m2) [8] pada saat akan

diterima oleh pelanggan. Sehingga baik sumber RF interferensi yang disengaja ataupun yang tidak dengan sengaja akan dengan mudah mengganggunya. Seperti ITU Radio Regulations Section IC radio stations and systems article 1.166 perihal elektromagnetik interferensi (EMI) maupun Radio Frekuensi Interferensi (RFI) merupakan efek dari energi yang tidak diinginkan pada penerimaan sinyal radio [5]. Potensi gangguan interferensi pada GNSS tidak hanya pada frekuensi kerjanya tetapi juga pada frekuensi 1240.rMHz seperti dibahas pada [9,10] yang menjelaskan perihal kemungkinan gangguan RFI pada sinyal GNSS seperti:

a. Loss of Receiver Tracking dimana RFI sangat kuat untuk mengganggu proses tracking sinyal satelit

b. Penurunan nilai sinyal to noise/carrier to noise (SNR/CNO)

c. Peningkatan EMI/RFI pada pseudo range ataupun phase measurement.

GNSS inteferensi tidak hanya berasal dari sumber RF yang berada pada rentang frekuensi yang sama, tetapi juga dari sinyal RF yang memiliki harmonisa mendekati frekuensi kerja GNSS seperti disebutkan terkait rekomendasi penggunaan frekuensi yang ramah terhadap GNSS sinyal [11]. Pada table 1 dan 2 diberikan beberapa sumber RF yang potensi untuk mengganggu pemanfaatan sinyal GNSS.

Table 1. EMI types and the Caracteristics of Various EMI Sources [12]

Type of EMI	Typical source	Characteristic of EMI
intentional	noise jammers	Wideband Gaussian
	Spread sprectrum jammers	Wideband spread spectrum
	Continuous Wave (CW) jammers	Narrowband swept Continuous Wave
		Narrowband Continuous Wave
unintentional	TV transmitter harmonics, near band microwave link transmitters	Wideband phase frequency modulation
	Near field of pseudolites	Wideband spread spectrum
	Radar transmitters	Wideband pulse
	AM Stations/CB transmitter harmonics	Narrowband Phase/ Frequency Modulation
	FM Station transmitter harmonics	Narrowband swept Continuous Wave
	Near band unmodulated transmitter's carriers	Narrowband Continuous Wave

Table 2. EMI Types and Potential Interfence in GPS Frequency [12]

GNSS signal	EMI sources	Frequency (MHz)	Interfere with GNSS signal
GPS L1 (1575.42 MHz)	Harmonics of VHF Communication for Air Traffic Control (ATC)	118-137.5	12^{th} and 13^{th} harmonics
	UHF TV and GSM700	782-788	2^{nd} and 3^{rd} harmonics
	Amateur radio	220-225	7^{th} harmonic
	Personal pivacy devices	Swept frequency car jammers (L1 and Galileo E5/1215 MHz)	Effective at a range of 1km to 8km depending on power of jammer
GPS L2 (1227.60 MHz)	Radio Navigation on Earth	1215-1240	In band

Beberapa algorithma yang dapat memperkuat penerimaan sinyal GPS yang lemah dibahas pula di [12] dengan menggunakan deviasi dari Carrier Noise Ratio (CNR) maupun menggunakan frekuensi track deviation.

Pada makalah ini, dilakukan deteksi potensi security threat berupa potensi gangguan interferensi pada perangkat GNSS. Telah dilakukan pengukuran potensi tersebut selama 3 hari di Serpong Banten. Pada hasil scanning tersebut diperoleh beberapa sinyal yang berpotensi dapat mengganggu penerimaan sinyal GNSS pada harmonisa nya diantara rentang frekuensi 450 MHz s/d 790 MHz dan antara 900 MHz s/d 1800 MHz. Meskipun begitu tidak diperoleh inband interferensi sinyal

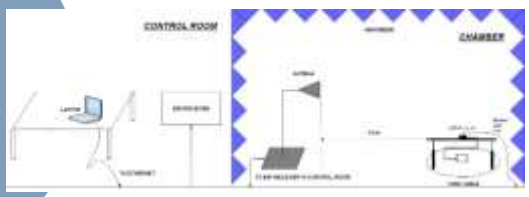
pada frekuensi kerja GPS baik L1 (1575.42MHz) maupun L2 (1227.60 MHz), hanya terdapat potensi gangguan EMI/RFI outband pada GPS L1 2nd dan 3rd harmonics [13].

C. Metode deteksi potensi 'security threat' dengan memonitor emisi elektromagnetik

Pada makalah [14] diulas perihal emisi elektromagnetik yang diradisikan oleh Ethernet kabel 10baseT dibandingkan dengan kabel RS232 beserta beberapa perbandingan solusi untuk mengurangi emisi tersebut. Emisi elektromagnetik yang diradiasikan oleh Ethernet kabel terlihat jelas pada saat dilakukan pengukuran pada jarak 10m dan pada rentang frekuensi rendah. Radiasi elektromagnetik (EMI) dapat diklasifikasikan menjadi dua jenis differential mode dan common mode. Pada differential mode radiasi EMI dihasilkan oleh jalur PCB maupun kabel yang tidak teratur secara simetri dalam rangka mengurangi kemungkinan terjadinya putaran arus dalam kabel/rangkaian. Sedangkan common mode radiasi EMI merupakan *'ground noise'* yang melalui cable. Pada makalah ini dibatasi untuk menggunakan common mode radiasi EMI untuk mendeteksi potensi 'security threat'.

Emisi radiasi sinyal elektromagnetik (EMI) dari kabel Ethernet IPv4 Cat 5 akan berubah bergantung dengan beban transmisi data yang dialirkan dalam kabel tersebut. Dalam rangka mendeteksi potensi security threat jenis *jamming* tersebut yang berpotensi meningkatkan beban transmisi kabel data yang melonjak tinggi, maka dilakukan pengujian emisi radiasi di EMC *(Electromagnetic Compatibility) chamber* Badan Pengkajian dan Penerapan Teknologi (BPPT) menggunakan kabel Ethernet IPv4 Cat5 untuk mentransmisikan paket data sebesar 32 bps dibandingkan dengan paket data sebesar 10kbps.

Gambar 6. Pengujian EMC di laboratorium EMC



Gambar 7. Konfigurasi pengujian

Tabel 3. Perbedaan emisi radiasi elektromagnetik (EMI) pada perubahan data yang ditransmisikan

transmisi data (bps)	Min. (dBµV)	rata-rata (dBµV)	Max. (dBµV)
32	45.12	46.02	48.08
10000	47.78	48.54	51.01
perbedaan	2.66	2.52	2.94

Pada table diatas terlihat bahwa terjadi peningkatan nilai emisi elektromagnetik yang dipancarkan oleh kabel Ethernet tersebut sekitar 2.55 dBµV s/d 2.94 dBµV. Berdasarkan hasil pengujian ini dapat disimpulkan bahwa apabila terjadi peningkatan emisi radiasi yang lebih besar dari 2.94dBµV dari kabel Ethernet maka kemungkinan adanya *potensi security* threat pada pengiriman data ADS-B.

III. KESIMPULAN

Potensi gangguan keamanan pada jaringan ADS-B dalam pengaturan lalu lintas penerbangan sangat penting untuk dideteksi lebih awal. Salah satu jenis security threat pada jaringan ADS-B adalah

berbentuk *jamming* ataupun *message injection*. Makalah ini memberikan metode baru untuk mendeteksi peningkatan load data transmisi pada kabel Ethernet IPv4 Cat 5 dengan cara memonitor perubahan emisi elektromagnetik yang diradiasikan oleh kabel Ethernet akibat lonjakan load data yang disebabkan oleh jamming ataupun message injection tersebut. Berdasarkan hasil pengujian dengan mengubah load data dari 32 bps menjadi 10KBps terjadi perubahan emisi radiasi elektromagnetik dengan rata-rata sekitar 2.5dBµV. Perubahan nilai emisi radiasi elektromagnetik ini dapat menjadi parameter untuk mendeteksi potensi security threat pada jaringan ADS-B. Selain itu potensi security threat terhadaµp sinyal GNSS yang digunakan pada ADS-B untuk penentuan lokasi juga dapat dideteksi dengan cara mengamati potential sumber interferensi baik yang disengaja (intentional) maupun yang tidak disengaja (unintentional). Dalam rangka mengurangi potensi gangguan EMI terhadap GNSS diharapkan pada saat penempatan ADS-B ground station memperhatikan beberapa panduan yang ada [15-18]. Selain itu perlu dilakukan pengamatan baik secara mandiri *(stand alone)* maupun secara jaringan *(network sensors)* terkait potensi sumber interferensi yang dapat mengganggu penerimaan sinyal GNSS [19-24].

DAFTAR PUSTAKA

[1] Martin Strohmeier∗, Vincent Lenders+, Ivan Martinovic, Security of ADS-B: State of the Art and Beyond ∗ ∗University of Oxford, United Kingdom,

[2] Camilo Andres Pantoja Viveros, Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts, Master Thesis, UNIVERSITY OF TARTU Institute of Computer Science

[3] Thabet Kacema, et al. , ADS-Bsec: A novel framework to secure ADS-B, Science Direct, ICT Express 3 (2017) 160–163

[4] Donald L. McCallie, Exploring Potential ADS-B Vulnerabilities in The FAA'S NextGen Air Transportation System, Graduate Research Projcet, Department of The Air Force, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio.

[5] Herring, TA, King, RW, Floyd, MA, dan Mc Clusky, SC. GAMIT Reference Manual Release 10.6. Massachusetts: Departement of Earth, Atmospheric, and Planetary Sciences Massachusetts Institute of Technology. 2015.

[6] Herring, TA, King, RW, Floyd, MA, dan McClusky, S.C. GLOBK Reference Manual Release 10.6. Massachusetts: Departement of Earth, Atmospheric, and Planetary Sciences Massachusetts Institute of Technology, 2015.

[7] Rahmad, A. A, et. Al. Analysis of Gunung Merapi GPS CORS station data by Scientific Software GAMIT/GLOBK 10.6 (in Indonesia Analisa Pengolahan Data Stasiun GPS CORS Gunung Merapi Menggunakan Perangkat Lunak Ilmiah GAMIT/GLOBK-). *JURNAL TEKNIK ITS*. 2016; 5(2).

[8] Jan-Joris, IntroductionGNSS RF interference (NLR). 2018.

[9] Matthias Wildemeersch, EC Joint Research Centre, Security Technology Assessment Unit. 'Radio Frequency Interference Impact Assessment on Global Navigation Satellite Systems'. EUR 24242 EN- January 2010

[10] Hees, Jan Van, *GPS/GNSS Interference Mitigation*. 56th Meeting of the CGSIC GNSS+ 2016 Conference Portland, Oregon. September 12-13. 2016

[11] Rec. ITU-R M.1905. 1 RECOMMENDATION ITU-R M.1905. Characteristics and protection criteri a for receiving earth stations in the radionavigation-satellite service (space-to-Earth) operating in the band 1 164-1 215 MHz. 2012

[12] Bakker P. Master Thesis Effects of Radio Frequency Interference on GNSS Receiver Output' TU Delft. Accessed in 2018.

[13] Reza Septiawan, Agung Syetiawan, Arief Rufiyanto, Nashrullah Taufik, Budi Sulistya, Erik Madyo Putro, GNSS interference reduction method for CORS site planning, Telkomnika Journal Vol 17 no. 3, June 2019.

[14] Richard A. Snay1 and Tomás Soler. Continuously Operating Reference Station CORS History, Applications, and Future Enhancements. *Journal of Surveying Engineering*. 2008: November: 95-104.

[15] Pattinson M. Standardization of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation. GNSS Agency (GSA), ENC2016, Helsinki. 2016

[16] Darren Burns and Robert Sarib, *Standards and Practices for GNSS CORS Infrastructure*, Networks, Techniques and Applications, FIG Congress Sydney Australia. 2010

[17] Ferrara, Giorgia & Bhuiyan, Mohammad Zahidul H & Hashemi, Seyedamin & Thombre, Sarang & Pattinson, Michael. How can we ensure GNSS receivers are robust to real-world interference threats?. 2018.

[18] M Pattinson, et al., Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation [STRIKE3]. European GNSS Agency (GSA),

[19] Zahidul Bhuiyan, Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation [STRIKE3]: Characterizing the Threats, GNSS Timing Resilience Receiver Workshop. 17th April, 2018.

[20] Muna Alnadaf, Outcome of ACAC/ICAO GNSS Workshop, Cairo/11th February 2018

[21] Arienzo, Loredana. (2010). RF Interference Vulnerability Assessment for GNSS Receivers. JRC Scientific and Technical Reports. 2010; 5-21.

[22] Jonas Lindström. GNSS Interference Detection and Localization using a Network of Low Cost Front-End Modules. Luleå University of Technology. 2007.

[23] Oscar Isoz. Interference Detection and Localization in GPS L1 Band. Lulea University of Technology. 2013

[24] Sheridan, Kevin, Ying, Yeqiu, Whitworth, Timothy. Pre and Post-Correlation GNSS Interference Detection within Software Defined Radio," *Proceedings of the 25th ION GNSS*, Nashville, TN, September 2012. 3542-3548