APPROACH
Jurnal Teknologi Penerbangan
ISSN : 2548-8090 e-ISSN : 2548-810X

Pengamanan Sinyal Ads-b Menggunakan Algoritma Blow-Fish

Endroyono[1], Renato L.[2], Suhanto[3], Bambang Bagus H.[3]
[1)]Institut Teknologi Sepuluh Nopember (ITS) Surabaya
[2)]Aerospace Engineering, ISAE-SUPAERO, Toulouse France
[3)]Politeknik Penerbangan Surabaya (d.h. ATKP)

Email : endroyono@ee.its.ac.id

ABSTRACT

Currently ADS-B is becoming an important part of modern flight systems. With the technology, the aircraft can determine its position, altitude and speed based on GPS data received via satellite and broadcast the signal as a tracking tools for traffic management by air traffic control, in lieu of secondary radar. Currently the nature of the ADS-B broadcast signal is open and can be received freely. It is assumed, however, that the ADS-B signal must be secured one day, as in military applications and other applications. For that purpose, ADS-B signals security design using a very famous code in the world of data communications, i.e.Blow-Fish algorithm. The simulation using baseband signal shows that the processing time in average is 79.09 milliseconds to add security code, with very small correlation coefficient (-0.004716), and it takes a very long time to break the code using brute force method, depend on the length of bits.
***Keyword**:ADS-B, baseband, security code, brute-force,*

ABSTRAK

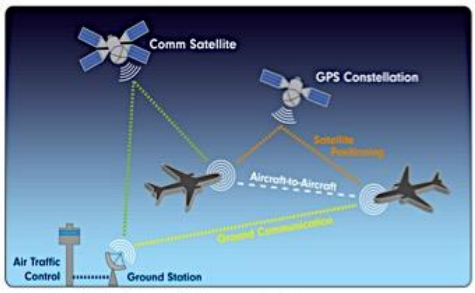
Saat ini ADS-B menjadi bagian penting pada sistem penerbangan modern. Dengan teknologi yang dipunyai pesawat dapat menentukan posisinya, ketinggian dan kecepatan berdasar data GPS yang diterima lewat satelit dan membroadcast sinyal tersebut dalam rangka alat bantu tracking bagi manajemen traffic oleh air traffic control, sebagai pengganti secondary radar. Saat ini sifat sinyal broadcast ADS-B adalah terbuka dan dapat diterima secara bebas. Akan tetapi diasumsikan, bahwa suatu saat dibutuhkan sistem ADS-B yang harus aman, seperti pada aplikasi militer dan aplikasi lain. Untuk itu dilakukan perancangan pengamanan sinyal ADS-B menggunakan algoritma Blow-Fish yang sangat terkenal di dunia komunikasi data. Hasil simulasi sinyal baseband menunjukkan, bahwa diperlukan waktu proses rata-rata untuk menambahkan security code adalah selama 79.09 milidetik, dengan koefisien korelasi yang sangat kecil (-0,004716), dan membutuhkan waktu yang lama untuk menembus secara *brute force*, tergantung panjang bits.

Kata Kunci: *ADS-B, baseband, security code, brute-force,*

APPROACH
Jurnal Teknologi Penerbangan
ISSN : 2548-8090 e-ISSN : 2548-810X

I. PENDAHULUAN

Di dunia penerbangan modern, sistem ADS-B menjadi salah satu alat bantu yang sangat efektif untuk *Air Traffic Management*. ADS-B adalah teknologi yang memungkinkan pesawat mengirimkan informasi penerbangan seperti posisi, ketinggian, dan kecepatan secara otomatis, berbasis data GPS dari satelit. Dengan adanya ADS-B pilot maupun ATC akan mempunyai kemampuan monitoring dan tracking melalui display, sebagaimana yang dilakukan oleh radar sekunder. Melalui ADS-B, data pesawat, *call-sign*, ketinggian dan termasuk *heading* dapat dipancarkan (broadcast) dan diterima secara terbuka.



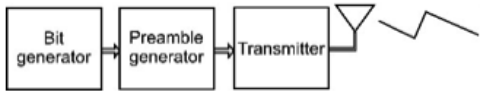
Gambar 1. Transmisi ADS-B antar Pesawat dan ke Air Traffic Control di darat

Dalam kondisi normal, jelas peran ADS-B tidak perlu diragukan. Akan tetapi, dengan semakin bebas dan murahnya perangkat penerima ADS-B yang dijual bebas membuat teknik ini membutuhkan pelindung, khususnya pada penerbangan penting, termasuk penerbangan militer, pesawat kepresidenan dan sebagainya.

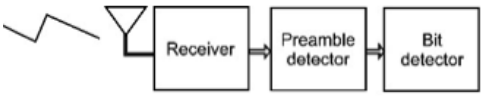
Untuk itulah melalui penelitian ini, dilakukan simulasi penerapan pengkodean keamanan (security code) untuk melindungi informasi ADS-B agar hanya dapat dibuka oleh penerima yang memang berhak atau berwenang menerimanya.

II. METODE

Dalam melakukan evaluasi terhadap proses dan hasil pengkodean security untuk ADS-B ini dilakukan simulasi sinyal *baseband* dari sistem ADS-B dari pesawat ke stadium di darat. Sebagaimana diketahui model baseband tidak tergantung pada frekuensi operasional, yaitu frekuensi 1090 MHZ dan 978 MHz.

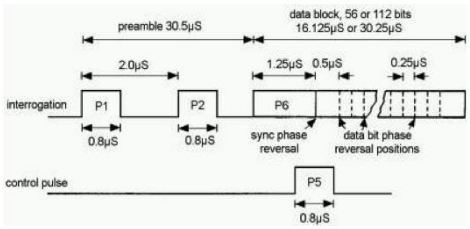


Gambar 2. Aliran sinyal pencar ADS-B

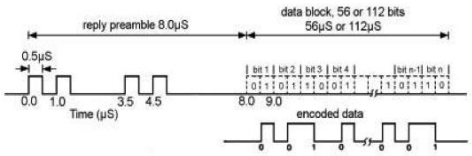


Gambar 3. TraAliran sinyal terima ADS-B

Sistem uji adalah sinyal ADS-B dengan format *frame Mode S Reply Extended Squitter downlink [6]*. Sinyal baseband yang diproses mempunyi format sinyal baseband sebagai berikut:



Gambar 4. Format Mode-S Interrogation



Gambar 5. Format Mode-S Reply

Format data terdiri dari elemen yang terdiri dari 112 bit data, dengan struktur frame sebagai berikut.

36 bit SYNC	272 bit PAYLOAD	112 bit FEC PARITY

Gambar 6. Format Frame Universal Access Transmitter

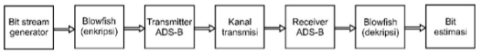
8 bit CONTROL	24 bit A/C ADDRESS	56 bit ADS MESSAGE	24 bit PARITY

Gambar 7. Frame Mode-S Extended Squitter

Dalam rangka menjaga keamanan dari sisi autentifikasi, kerahasiaan, dan integritas pesan; penelitian ini berusaha melakukan perlindungn terhadap *eaves-dropping*, *jamming*, *message injection*, *message deletion*, dan *message modification*. Perlindungn

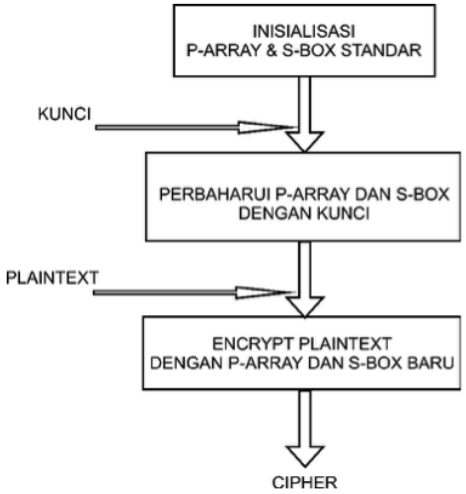
ISSN : 2548-8090 e-ISSN : 2548-810X

dilakukan melalui upaya enkripsi simetris bertahap, menggunakan algoritma Blow-Fish. Intinya Blow-fish disisipkan sebelum transmitter dan setelah receiver.



Gambar 8. Integrasi Blow-fish ke ADS-B

Algoritma blow-fish bekerja sesuai diagram alir di gambar 9. Gambar 9 adalah contoh sebagian pseudp-code untuk melakukan inisialisasi blow-fish 8 bit, sebagai ilustrasi. Setelah validasi sistem transmisi ADS-B, jelas harus dilakukan validasi terhadap proses enkripsi dan dekripsi dengan Blow-fish.



Gambar 9. Diagram alir algoritma Blow-fish

Inisialisasi P-array[1x18] dan S-box[4x2] dengan nilai tetap (maksimum 4 bit dalam format binernya) yang diambil dari digit desimal Pi secara berurutan

Ubah nilai tiap anggota P-array & S-box ke biner sehingga P-array = 72 bit dan S-box[4x2] masing-masing 4 bit

Input Key dengan panjang diantara 1 – 56 bit

(Biner P-array) XOR (Biner Key yang diulang sampai sepanjang 72 bit)

Encrypt data bernilai 0 semua (8 bit) dengan Blowfish, *dengan P-array dan S-box yang ada*

Hasil enkripsi (8 bit) dipakai untuk menggantikan P1 (4 bit) dan P2 (4 bit)

Hasil enkripsi di-encrypt dengan Blowfish *lagi*

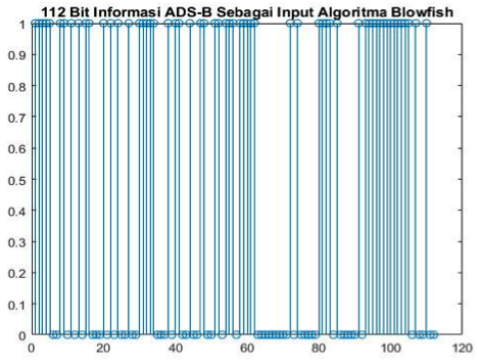
Hasil enkripsi terbaru dipakai untuk menggantikan P3 dan P4

Proses diulang sampai semua anggota P-array dan S-box diganti dengan nilai yang baru

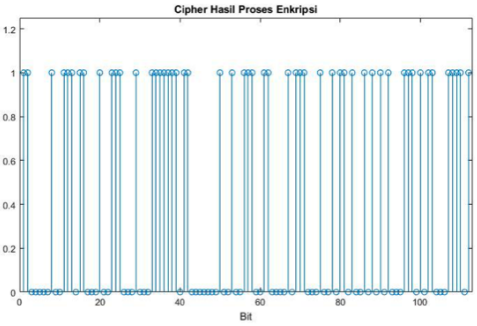
Gambar 10. Pseudo-code inisialisasi Blow-fish 8 bit.

III. HASIL DAN ANALISIS

Berdasarkan metodologi yang dirancang di bab II, maka dilakukan simulasi. Validasi dilakukan sejak dari pembangkitan sinyal, format frame input algoritma Blow-fish, hingga uji kinerja enkripsi menggunakan metode cryptanalysis.



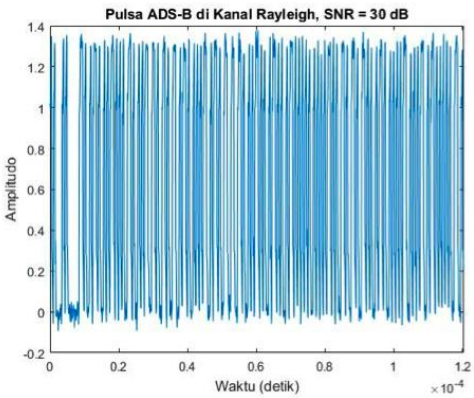
Gambar 11. Contoh sinyal dari Frame Generator



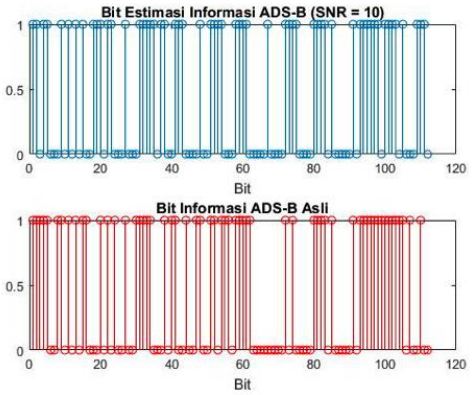
Gambar 12. Contoh sinyal hasil enkripsi

Setelah lewat kanal, sinyal mengalami distorsi. Walaupun demikian, apabila sistem bekerja sempurna, receiver masih akan dapat melakukan deskripsi kembali, sebagaimana ilustrasi Gambar 14.

APPROACH
Jurnal Teknologi Penerbangan
ISSN : 2548-8090 e-ISSN : 2548-810X



Gambar 13. Sinyal broadcast ADS-B



Gambar 13. Perbandingan sinyal ADS-B kirim dan terima pada SNR 10 dB.

Uji pertama yang dilakukan adalah ujia korelasi, yaitu uji untuk menunjukkan ketidak miripan hasil enkripsi dengan sinyal aslinya. Tabel 1 merupakan sebagian hasil yang menunjukkan, bahwa korelasi antara sebelum dan sesudah adalah sangat kecil. Artinya tidak ada kemiripan bentuk sinyal.

Tabel 1. Korelasi sinyal sebelum dan sesudah enkripsi

Jenis Data	Nilai
Rata-rata	-0,004716
Standar Deviasi	0,111474
Nilai Maksimum	0,3273
Nilai Minimum	-0,3267
Jumlah Data Kategori Korelasi Lemah	98
Jumlah Data Kategori Korelasi Sedang	2

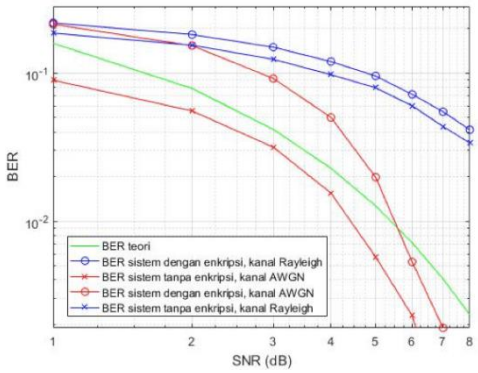
Untuk melihat keberhasilan proses, dilakukan uji criptanalyse terhadap hasil enkripsi melalui *brute-force attack* pada blow-fish 8 bit hingga 64 bit. Dari sisi waktu deskripsi, ternyata 1 key membutuhkan waktu minimal 0,05794 detik. Dengan demikian bila digunakan blow-fish 8 bit akan ada 256 kemungkinan kunci dan untuk 64 bit akan ada 2^{64} kemungkinan key.

Semuanya keunggulan itu bisa didapat hanya dengan waktu proses enkripsi dan dekripsi yang sangat singkat, sebagaimana contoh di tabel 1.

Tabel 2. Waktu proses enkripsi-deskripsi

Jenis Nilai	Waktu Proses Sebelum Penambahan Algoritma Blowfish (detik)	Waktu Proses Setelah Penambahan Algoritma Blowfish (detik)		
		Durasi Demodulasi	Durasi Dekripsi	Total
Maksimum	0,001879	0,008688	0,133460	0,142148
Minimum	0,000401	0,000886	0,057940	0,058827
Rata-rata	0,000752	0,001533	0,077554	0,079088

Perlu diingat, bahwa akan dimungkinkan terjadi kesalahan terhadap sinyal yang ditransmisikan dari pesawat ke ATC, yang diakibatkan oleh redaman media dan penyebab lain yang menyebahkan berubahnya nilai signal to noise ratio, SNR. Sebagaimana contoh hasil simulasi sinyal tanpa enkripsi dan sinyal dienkripsi setelah melalui kanal AWGN dan Rayleigh sebagai berikut.



Gambar 14. BER sinyal hasil enkripsi di berbagai kanal.

IV. PENUTUP

Berdasarkan metodologi yang dipilih dan hasil simulasi yang telah dilakukan, dapat disimpulkan, bahwa:

1. Algoritma Blow-fish telah berhasil diterapkan dalam rangka enkripsi terhadap sinyal baseband ADS-B, dalam rangka memberikan kemanan lebih terhadap sinyal ADS-B yang saat ini dipancarkan secara broadcast dan terbuka.

ISSN : 2548-8090 e-ISSN : 2548-810X

2. Sinyal hasil deskripsi mempunyai korelasi yang rendah dengan sinyal ADS-B asli. Meskipun demikian, hasil enkripsi telah berhasil dideskripsi kembali dalam rangka mengevaluasi kinerjanya pada pemancar-penerima ADS-B, dengan waktu proses rata-rata 79.09 mili detik
3. Untuk melakukan deskripsi 1-key menggunakan komputer membutuhkan waktu proses sekitar 0,05794 detik, sehingga butuh waktu lebih lama jika kode semakin panjang.
4. Sebagimana dalam model umum telekomunikasi, SNR dari ADS-B harus dijaga dalam rangka menjaga BER yang dipersyaratkan.

Saran untuk pengembangan dari penelitian ini adalah SDM penerbangan Indonesia perlu bersiap dalam penerapan konsep ini walaupun saat ini belum masuk di ICAO maupun FAA. Selain algoritma, masih banyak pengembangan lain terkait telekomunikasi penerbangan dan alat bantu navigasi modern yang dapat dilakukan di perhuruan tinggi bidang penerbangan (poltek penerbangan), termasuk eks ATKP.

DAFTAR PUSTAKA

[1] Eurocontrol. *ADS-B for Dummies*

[2] International Civil Aviation Organization, 2003, *What is ADS-B?*

[3] Air Facts, *ADS-B Diagram. <http>*

[4] Hableel, Eman, Joonsang Baek, Young-Ji Byon, and Duncan S. Wong., 2015, *How to Protect ADS-B: Confidentiality Frameworkfor Future Air Traffic Communication*. The 2015 IEEE INFOCOM International Workshop on Mobility *Management* in the Networks of the Future World.

[5] Adsb-decode-guide.readthedocs.io, 2017, *ADS-B Decoding Guide — ADS-B Mode-S Decoding Guide documentation.*

[6] International Civil Aviation Organization, 2003, *Manual for the Universal Access Transceiver (UAT).*

[7] L., Srinivas B., Anish Shanbhag, Austin Solomon D'Souza, October 2014, *A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm*. International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Special Issue 5, ISSN (Online) 2320-9801.

[10] Schneier, Bruce. *Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), Fast Software Encryption*, Cambridge Security Workshop Proceedings (Dec. 1993), Lecture Notes in Computer Science (LNCS) Springler verlag Vol. 809, pp. 191-204, 1993, ISBN 3- 540-58108-1.

[11] Elminaam, D. S. Abdul, H. M. Abdul Kader, M. M. Hadhoud, 2009, *Performance Evaluation of Symmetric Encryption Algorithms*. Communications of the IBIMA, Vol. 8, ISSN 1943-7765.

[13] Albaichi, Ashwak, Faudziah Ahmad, Ramlan Mahmod, 2013, *Security Analysis of Blowfish Algorithm*. ISBN 978-1-4673-5256-7/13.

[14] Mandal, Akash Kumar, Mrs. Archana Tiwari, 2012, *Analysis of Avalanche Effect in Plaintext of DES using Binary Codes*. International Journal of Emerging Trends and Technology in Computer Science (IJETTCS), Volume 1, Issue 3, September October 2012, ISSN 2278-6856.

[15] Tahir, N., M. Naufal bin M. Saad, Brahim Belhaouari Samir, 2010, *Binary Pulse Position Modulation (BPPM) Bit Error Rate (BER) Analysis in Turbulent Atmospehere.* Vol. 2 No. 1, ISSN 2180-1843.