AIR TRAFFIC SIMULATOR FOR PASSIVE ADS-B SURVEILLANCE SYSTEM

Jiří Kratochvíl[(a)], Karel Šimerda[(b)]

[(a),(b)]Faculty of Electrical Engineering and Informatics, University of Pardubice

[(a)]jiri.kratochvil@student.upce.cz, [(b)]karel.simerda@upce.cz

ABSTRACT

This contribution presents a concept of a hybrid air traffic simulator which will be used for ADS-B message validation algorithm testing. These validation algorithms will be used in a passive ADS-B surveillance system. In real life, it is not possible to experiment with data communication disruption of an air traffic by injecting spoof targets. It could lead to endangerment of people in aircrafts and even whole air traffic control. It is thus necessary to realize such attacks on data communication only in a simulated environment. Before attempting to create such environment, appropriate and thorough specification is needed. Simulation of an aircraft transponder can be very complex and may not entirely correspond to the behavior of real transponders. Because of that, the simulator will be using real captured data from ground stations in addition to simulated airborne targets.

Keywords: ADS-B communication, validation, simulator

1. INTRODUCTION

ADS-B (Automatic Dependent Surveillance – Broadcast) is a technology for unidirectional data transmission from an aircraft. It is a broadcast, which means that one aircraft is transmitting while an arbitrary number of receivers are receiving signal. Transmitters are not synchronized with each other and multiple aircrafts can transmit at once. Emission of ADS-B messages is automatic and is not dependent on any input from outside of aircraft. This is unlike other surveillance systems, e.g., primary or secondary surveillance radars, where radars placed on the ground are actively participating in a surveillance system's function. The ADS-B Airborne Position Message broadcast rate is 2 messages per second, more specifically the time interval between two consecutive Airborne Position Messages from the same aircraft is 0.4 – 0.6 of a second (EUROCAE 2009). Transmitted messages lack any encryption, so anyone can eavesdrop on the communication. The format of ADS-B messages is public and described in document from EUROCAE (European Organisation for Civil Aviation Equipment). This document contains Minimum Operational Performance Standards of airborne equipment for ADS-B (EUROCAE 2009). The ADS-B format description can be found on the internet for free (Sun 2017). Moreover, there are open source tools and libraries for ADS-B message decoding, such as *gr-air-modes* library for *GNU Radio* tool, which makes message decoding easy even for non-professionals.

1.1. Attacks on ADS-B

Due to many, sometimes even free, materials describing the ADS-B format, carrying out a passive attack on the ADS-B system is very easy. It is simply eavesdropping on broadcasted messages from aircrafts. That alone does not pose any threat to the air traffic, but this type of attack is usually the first step of an active attack (Schäfer et al. 2013).

Active attack means that adversary send messages. This can influence the ADS-B system in several ways from creating new spoof targets up to deletion of messages from real aircrafts. All of these attacks are composed from one of three basic actions or their combination. Basic actions are message insertion, message deletion and message modification (Schäfer et al. 2013). In addition to absence of encryption, ADS-B does not authenticate the sender, and thus identity of this transmitter cannot be verified from the received message only. To overcome this shortcoming, use of another technology, such as passive locator, multilateration or data fusion is needed. However, each one of these technologies contribute to greater complexity of the system for message reception and processing. In addition to that, it is necessary to use algorithms that can work with data from these multiple systems and thus validate received messages. The simulator designed in this paper will be used mainly for testing such algorithms for passive surveillance systems.

2. AIR TRAFFIC SIMULATION

The simulator designed in this paper is not a general air traffic simulator, although there are some shared ideas and concepts. It is of great importance to realistically represent target trajectories through the airspace. For example, an airborne target cannot suddenly change the direction of its motion to a perpendicular direction and should fly at a speed in some given range (greater than stall speed and lower than maximal speed). In addition to that, the radius of aircraft turns should be appropriate to its speed.

This simulator is focused on an air traffic simulation from the perspective of the passive locator and ADS-B

communication. Passive locator is an ADS-B message receiver with an ability to determine the direction from which an ADS-B message was received. The emulator of ADS-B transponder will be created, which will then periodically broadcast messages for each airborne target. Transponder is a device on board of an aircraft. This device emits a coded signal with information about the aircraft.

2.1. Airborne Target Trajectory

The question arises in the scope of the designed simulator as how to effectively work with airborne target trajectories. It is necessary to choose appropriate representation of trajectories that will enable both a programmatical generation and manual designing, depending on user's needs. There are four options for such representation:

- List of points in 3-D space.
- Curve in 3-D space.
- Waypoints.
- Aircraft vectoring.

Representing trajectory as a time-sorted list of points in 3-D space is advantageous form the viewpoint of programmatical generation of trajectories, but it is not appropriate when considering manual designing and memory efficiency. Because the simulator will be using recorded data from a real air traffic, this representation may be the most convenient one for this usage.

Better than the list of points in 3-D space, is to use a curve, which will describe required trajectory. Then it is enough for a program or for a user to set control points, which will determine the actual shape of the curve. As the most appropriate type of curve for aircraft trajectory representation seems to be B-spline curve. This curve belongs to the C2 differentiability class. Curves from the C2 differentiability class have continuous derivatives up to and including the second order (Delahaye et al. 2014). From the physical viewpoint, this means that an airborne target cannot abruptly change acceleration during its movement along the trajectory.

A very simple way how to design a trajectory by hand is a usage of waypoints. These waypoints are points in space (in this case it is three-dimensional space), which determine the shape of the aircraft's trajectory. Two types of waypoints are used in practice: fly-by waypoints and fly-over waypoints. A fly-by waypoint specifies that an aircraft should start a turn to change its current course to the next course before reaching this point. On the other hand, a fly-over waypoint specifies that an aircraft should fly through this point first before it starts a turn to change its course (Federal Aviation Administration 2015). Depiction of these types of waypoints is in the Figure 1.

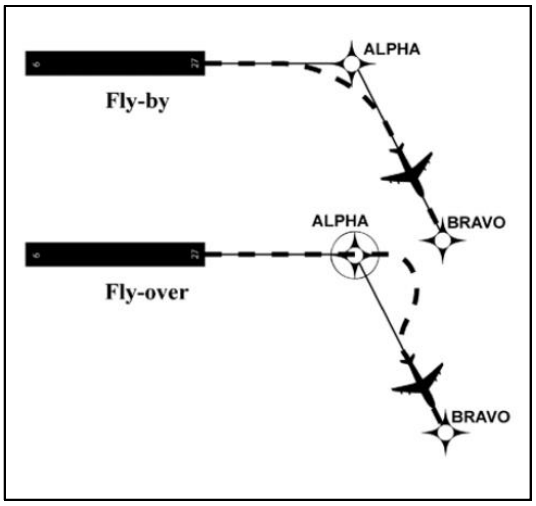

Figure 1: Types of Waypoints

The last mentioned option how to move an airborne target along a trajectory is to completely leave out the predefined trajectory and change aircraft's position using a user-given scenario. That corresponds to an aircraft vectoring; controlling aircraft's trajectory based on instructions for the aircraft's pilot, received from an air traffic control. Such instructions can have the form of this excerpt:

1. Fly 100 km at constant altitude without change of heading.
2. Perform +3° turn.
3. Fly 50 km at constant altitude without change of heading.
4. Descend at 3° angle for 10 km.

The main objective of the simulator is not a planning of efficient trajectories, but planning of such trajectories that would be indistinguishable from trajectories of real aircrafts, given that simulated airborne target should represent a real aircraft. Another case is spoof targets. Their trajectory can be realistic, but does not have to be. That depends on how much the attacker is sophisticated.

2.2. Target's Movement Along the Trajectory

When the trajectory is created, the target must fly along that trajectory during the simulation run. Its flight parameters need to be realistically represented, which is especially the case of velocity. To achieve this goal, it is possible to use the flight dynamics model, which represents an aircraft's behavior under different forces such as thrust, lift and other. Then there are multiple possibilities how to let aircraft fly along a specified trajectory. All of them are basically different forms of autopilot. Another, convenient way of representing a realistic movement of an aircraft is usage of recorded data from a real air traffic. This will obviously lead to the realistic representation of airborne targets.

2.2.1. Computation of Model Inputs

Computation of model inputs is performed as a computation of appropriate equations, which describe the behavior of the aircraft. This model is represented as a system of ordinary differential equations. Through appropriate equivalent modifications of these equations, new equations are made where independent variables are required changes of trajectory. The result is the control input for given model of the aircraft (Quanbeck 1982). This way of controlling aircraft models is rather complicated and does not reckon with wind forces and dynamically changing environment, for example. Another and simpler solution is to use a system which will be able to pilot an aircraft model. For this purpose, a PSD controller or neural network could be used.

3. SIMULATOR DESIGN

In this paper, a design of the simulator for ADS-B message validation algorithm testing is described. This simulator provides a means for simulation of realistic air traffic on an appropriate level of abstraction from the viewpoint of passive ADS-B surveillance systems. It can also work with spoof targets. Since there are multiple coordinate systems used in the simulation and surveillance systems, it is an important feature of the simulator that it can convert coordinates between these coordinate systems. Simulation is performed in a 3-D cartesian coordinate system. However, positional data received from airborne targets contained in the ADS-B messages are in WGS-84 geodetic coordinate system (EUROCAE 2009). Moreover, passive locator reports only the angle at which the ADS-B message was received.

3.1. Simulator Requirements

Main simulator requirements are these:

1. Simulator must realistically represent behavior of airborne targets with emphasis on the following attributes:
   - Movement in airspace must take place with realistic parameters, such as smoothness of movement along trajectory (no abrupt changes), appropriate radii of turns, etc.
   - Aircrafts' speed must be appropriate at all points of trajectory.
   - Parameters of received ADS-B message must correspond to transmission from given position in 3-D space, where was transmitter placed at the time.
   - Appropriate representation of an aircraft transponder must be used. It will send messages in correct intervals, it will contaminate position measurement by error with given statistical properties, etc.
2. Simulator must permit simulation of spoof targets which emit messages with parameters that are not in accordance with a simulated situation.
3. Simulator must be able to generate appropriate random variables with realistic parameters.
4. For the performance testing of validation algorithms, the simulator must be able to simulate up to 400 targets at once.
5. Simulator must be able to convert position information between requested coordinate systems.

3.2. Sources of Nondeterminism

Several random variables or random processes will be used in the simulator. It is necessary to retrieve statistical parameters from the real modelled system for each one of them, and then apply them in the simulator accordingly. These sources of nondeterminism are:

- Occurrence of an observational error in airborne target position measurement by INS/GNSS.
- Time delay between performing position measurement and according ADS-B message emission.
- Occurrence of an observational error in passive locator measurement.
- Random errors during message transmission which leads to message dropping by receiver.

INS/GNSS position measurement is contaminated by an error depending on the source of position information. INS/GNSS is a term for systems that measure spatial position. INS (Inertial Navigation System) uses information about aircraft's rotation and acceleration from IMU (Inertial Measurement Unit), and thus can compute a new position relative to the last position information. GNSS (Global Navigation Satellite System) is based on different principles. For a position measurement, it uses satellites orbiting around the Earth. GNSS is thus an umbrella term for GPS, GLONASS, Galileo and other satellite-based systems.

For modelling of a GPS error, the Rayleigh probability distribution is commonly used. But individual measurements are, rather, realizations of random variables in a Gauss-Markov random process, because observational errors are time-correlated (Mohleji and Wang 2010).

Another source of a nondeterminism in the simulator is a delay between the time when aircraft's position is measured and the time when message with this position is emitted. If this delay is too long, position information becomes outdated since the aircraft has meantime traveled a non-negligible distance.

If this is not taken into account when creating validation algorithms with help from this simulator, it could lead to marking real aircraft as spoof target because of noncorresponding information from ADS-B messages and computed position from the passive locator or multilateration system.

Errors are also present in passive locator measurements. A passive locator measures direction from which the message from an aircraft or from an adversary was

received. It is thus an angular error. Parameters of this random process are unknown. Simulation experiments will verify whether designed message validation algorithms are applicable for processing of information from a passive locator with a specific measurement error. This measurement error will be the subject of simulation experiments too. Which parameters should a passive locator have for practical use, will be tested.
In practice, it happens that received ADS-B message is damaged and cannot be repaired. If the number of such messages is low (in the order of units), the performance of the whole system will not significantly degrade. Performance evaluation of the simulated system with a different probability of the message dropping will be a subject of simulation experiments too.

3.3. Description of Design

The simulator will be based on a simulation core, using periodic activity sampling, which is a technique of continuous simulation. Trajectories of all airborne targets are recomputed with a very short period of time (in order of fractions of a second). But since there are also discrete activities present in the simulator, simulation will be discrete-continuous.

3.3.1. Entities

Four types of entities are present in simulator:

- *Airborne Target*
- *Spoof Target*
- *ADS-B Message*
- *Ground Receiver*

Airborne Targets are mobile temporary entities, whose position information are contained in ADS-B messages. They are representation of real aircrafts inside the simulator, whose movement along trajectories is modelled. *Airborne Targets* use a realistic model of movement.
Spoof Targets are temporary entities, which represent spoof targets created by some attacker. Their positions are also contained in ADS-B messages, which are broadcasted to other receivers. Movement of these *Spoof Targets* can be either realistic in the case of sophisticated attacker or simplified and not very realistic otherwise.
ADS-B Messages are endogenous temporary entities, which carry information about airborne targets or spoof targets. In the simulator, they move from the originating transmitter, which can be aircraft or adversary, to the corresponding receiver. Multiple message entities are created for each transmission. The number of entities is determined by the number of receivers, because one message is created for every pair of current transmitter and receiver. Duration of a message entity movement through space depends on the distance between the transmitter and the receiver.
Ground Receivers are endogenous permanent entities at fixed coordinates on the ground. Their purpose is to receive ADS-B messages and register times of their reception. If the receiver is also a passive locator, it will also determine the direction from where the message was sent (with appropriate measurement error).

3.3.2. Activities

Important activities present in the simulation model are:

- *Aircraft's position measurement by INS/GNSS system.*
- *Message assembly in aircraft's transponder.*
- *Message transmission from transmitter to receiver.*
- *Aircraft flight.*

Aircraft's position measurement by INS/GNSS system is a discrete activity. Measurement of the position has a non-zero duration. For example, GNSS systems typically output position information at the rate of 1 second, so the duration will be 1 s. At the end of this activity, event *Transponder position update* is scheduled. It is not an update of the aircraft's actual position in the simulated space. It is an update of the measured position inside the transponder in the same way as in a real aircraft.
Message assembly in aircraft's transponder is a discrete activity, which represents assembly of an ADS-B Airborne Position Message with a duration from the [400,600] ms interval. This duration variation leads to a random delay between the measurement of an aircraft's position and message emitting; which is implicitly specified by a delay between the last occurrence of event *Transponder position update* and next event *ADS-B message emission*. Activities *Aircraft's position measurement by INS/GNSS system* and *Message transmission from transmitter to receiver* are running in parallel, but independent of each other.
The position of an aircraft is encoded in the CPR format. This reduces the number of bits needed for encoding of an airborne target position from 45 bits to 35 bits. Outcome of this is that there are two types of messages – odd CPR format position messages and even CPR format position messages. Aircraft is then sending in turns even format and odd format messages. To be able to determine the global position of an aircraft unambiguously, one must receive both odd and even CPR format position messages within 10 seconds. It is specified that 2 messages should be transmitted in 1 s (EUROCAE 2009). In the best case, both (one odd and one even) messages should be received during 1 s.
At the end of a *Message assembly in aircraft's transponder* activity, event *ADS-B message emission* is scheduled. When the simulator engine is processing this event, next activity *Message assembly in aircraft's transponder* is started and so are activities *Message transmission from transmitter to receiver*, which means that transmission from transmitter to all of receivers in range is started. As mentioned before, it is multiple activities, one for each pair of transmitter – receiver.

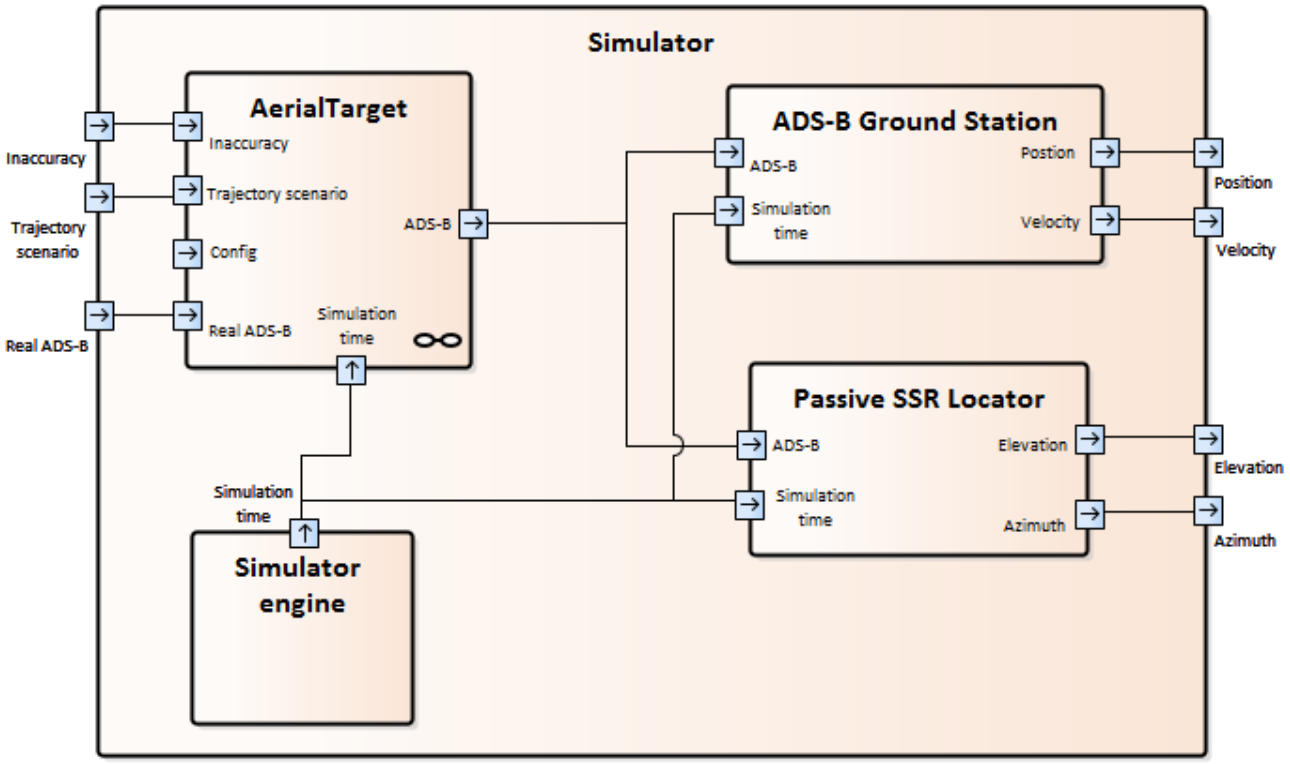

Figure 2: Modules of the Simulator

Message transmission from transmitter to receiver is a discrete activity. Duration of this activity and thus the duration of the message transmission is computed from the propagation speed of an electromagnetic signal through the airspace and the distance of the appropriate receiver from the transmitter. At the end of this activity, event *Message reception at ground station* is scheduled. *Aircraft flight* is a continuous activity, which represents a flight of an aircraft. It is periodically sampled by the simulator engine.

3.3.3. Events

In the scope of the simulator, these events are occurring:

- *Transponder position update*
  - This event occurs when the GNSS/INS module finishes measurement of a position. Current position is updated in the Transponder module.
- *ADS-B message emission*
  - This event occurs when the Transponder module finishes message assembly. Transfer to all receivers in range begins.
- *Message reception at ground station*
  - This event occurs upon message reception at the receiver. Receiver then reacts appropriately to the module type (ADS-B or passive locator). This behavior is described in the next chapter.

4. SIMULATOR ARCHITECTURE

From the viewpoint of the simulator creation and possible extension, it is convenient to create multiple standalone modules from which the simulator will comprise. Depiction of those modules and their interconnection is shown in the Figure 2. Modules themselves are described in next chapters together with their crucial outputs and inputs.

4.1. Simulator engine

The *Simulator engine* stands in the core of the whole simulator. It performs activity scanning, event scheduling and subsequent event processing. It initiates and coordinates functionality of individual modules. The engine in this simulator is based on the activity scanning method. The simulator engine increments the simulation time periodically with sufficiently small step Δt. The size of this step is dependent on the speed of the fastest simulated target, see chapter 3.2. In the Figure 3 can be seen what events occur in the simulator and at what time. These events are represented by boxes.

- PU is a pseudo-event, which occurs periodically with fixed time step during the continuous activity *Aircraft flight*. It is not an actual event in the simulation. It is the update of the aircrafts' position. In the picture, the time step is 0.1 s. However, concrete value is a matter of simulator's configuration. This time step is the Δt with which the simulator engine advances simulation time.

ISBN 978-88-97999-85-0; Affenzeller, Bruzzone, Jiménez, Longo and Piera Eds.

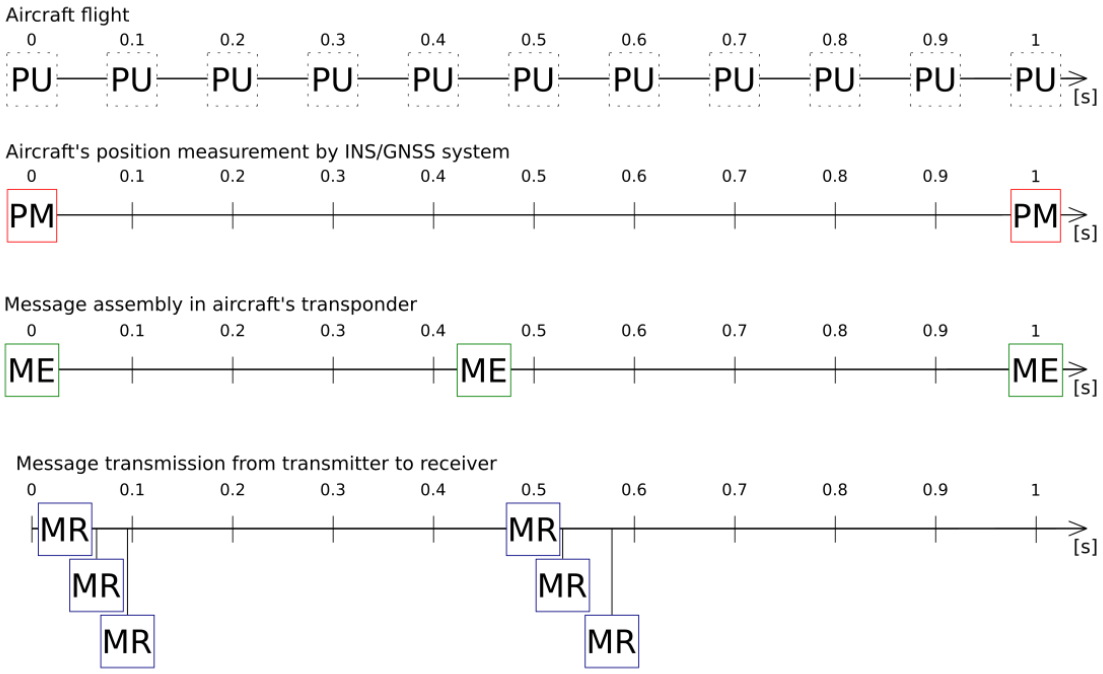

Figure 3: Events Occurence

- PM is the *Transponder position update* event, which occurs at the end of the *Aircraft's position measurement by INS/GNSS system* activity.
- ME is the *ADS-B message emission* event, which occurs at the end of the *Message assembly in aircraft's transponder*.
- MR is the *Message reception at ground station* event, which occurs at the end of the *Message transmission from transmitter to receiver* activity.

Due to the fact that the simulator engine is based on the activity scanning method, some events need more complex processing. As can be seen in the Figure 3, positions of all airborne targets in the simulated airspace are periodically updated at fixed time intervals. But some events can occur between two position updates and are dependent on a precise position information. It is therefore needed to temporarily compute current position at the given time of such event. But this updated position should be visible only for appropriate event, so the computation of the new position does not interfere with periodic updates of aircrafts' positions, which should be visible globally inside the simulator. This is true for events *Transponder position update* and *ADS-B message emission*. Both needs as precise information about current position as possible. Otherwise, if for example, an event *ADS-B message emission* is processed and uses current aircraft's position without computed correction, retrieved position information will not correspond to the position at the time of the event. It will be outdated.

- Input:
  - Events, which should be scheduled at some time in the future.
- Output:
  - Simulation time for modules in the scope of the simulator.

4.2. Trajectory module

This module deals with a representation of a target on its trajectory. In this simulator the module, which can load a user scenario, is realized. This scenario is in the form of instructions for a target movement and corresponds to the aircraft vectoring, mentioned in the chapter 2.1. More trajectory modules, which could for example work with 3D curves, are planned.

- Input:
  - Parameters for the specific trajectory. Currently, it means user scenario with vectoring instructions.
  - Simulation time from the *Simulator engine*.
- Output:
  - Precise target position at the current simulation time.

ISBN 978-88-97999-85-0; Affenzeller, Bruzzone, Jiménez, Longo and Piera Eds.

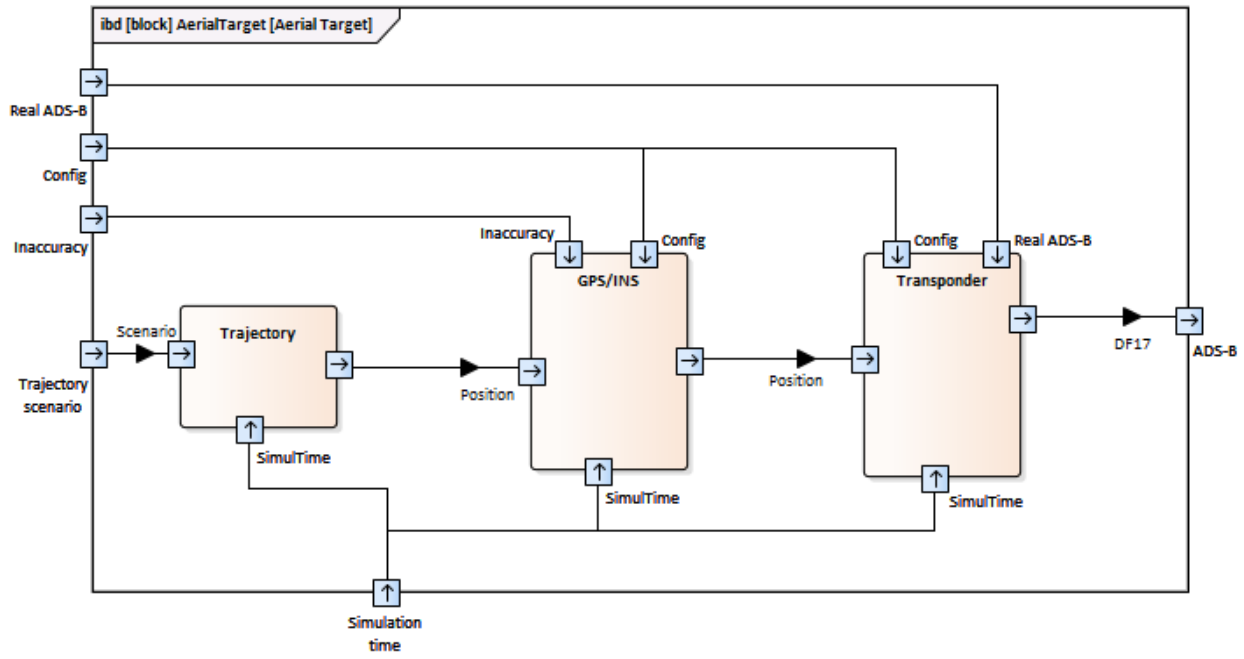

Figure 4: Inner Structure of the Aerial Module

4.3. GNSS/INS module

The *GNSS/INS module* generates measurement errors of an aircraft's GNSS/INS system. This error is generated in accordance with a user-chosen NAC. NAC stands for Navigation Accuracy Category and specifies precision of the positional information based on the type of position measurement source (EUROCAE 2009):

- Input:
  - Inaccuracy is chosen by user.
  - Chosen configuration of the position data source.
  - Position information from *Trajectory module*.
  - Simulation time from the *Simulation engine*.
- Output:
  - Target position with a measurement error added.

4.4. Transponder module

The *Transponder module* assembles and transmits messages from targets as mentioned in chapter 3.3.2 in the *Message assembly in aircraft's transponder* activity's description. Transponder periodically starts *Message assembly in aircraft's transponder* activity with appropriate duration. This module can also use already existing messages, which were obtained, for example, from real air traffic. A message assembly activity has the duration randomly generated and, in addition to that, it runs in parallel with an *Aircraft's position measurement by INS/GNSS system* activity. This leads to a new random variable, which is a random delay between the measurement of the position and the transmission of the message with that position.

- Input:
  - Position information contaminated by an error from the *GNSS/INS module*.
  - Real ADS-B data.
  - Simulation time from the *Simulation engine*.
  - User configuration.
- Output:
  - ADS-B messages in the DF-17 format together with coordinates of the message transmission origin.

4.5. Aerial Target module

The *Aerial Target module* is composed from the previous three modules; the *Trajectory module*, *GNSS/INS module* and the *Transponder module*, as can be seen in the Figure 4. This *Aerial Target module* represents individual aerial targets with a configuration given by these three modules. This module is also a base module for the *Spoof Target module*, which represents spoof targets. Due to the fact that this module's main objective is to group the three modules together, inputs of this module are made of inputs of inner modules. The same holds for outputs.

- Input:
  - Parameters for a trajectory (user scenario with vectoring instructions).
  - Chosen configuration of the position information source.
  - Real ADS-B data.
  - Simulation time from the *Simulation engine*.
- Output:
  - Output from the *Transponder module*.

ISBN 978-88-97999-85-0; Affenzeller, Bruzzone, Jiménez, Longo and Piera Eds.

4.6. Spoof Target module

This module is derived from the *Aerial Target module*. It contains information about real trajectory of the attacker's transceiver; in addition to the information from the original module. Frequent case of such trajectory will be a static point in the 3D space, which will correspond to the static attacker.

- Input:
  - All inputs from the *Aerial Target module*.
  - Trajectory scenario of the attacker's transceiver.
- Output:
  - Output of the *Aerial Target module*.

4.7. ADS-B Ground Station module

The *ADS-B Ground Station module* receives ADS-B messages. It stores the time of the message reception, and then sends the message data to the output for subsequent processing.

- Input:
  - Ground station coordinates.
  - ADS-B messages together with physical characteristics of these messages (position of the transceiver at the time of the transmission).
- Output:
  - Received data, especially position and velocity.

4.8. Passive Locator module

The *Passive Locator module* also receives ADS-B messages, but only processes the direction from where the message was received.

- Input:
  - Same as *ADS-B Ground Station module.*
- Output:
  - Azimuth of the incoming message signal.
  - Elevation of the incoming message signal.

4.9. MLAT module

The *MLAT module* is composed of multiple *ADS-B Ground Station* and/or *Passive Locator* modules. It combines functionality of those modules into one. Moreover, it computes time differences of the message arrivals at individual receivers. From these time differences of arrival (TDOAs), the origin of the transmission can be computed. This is the technique known as multilateration (MLAT).

- Input:
  - All inputs from multiple *ADS-B Ground Station* and/or *Passive Locator* modules.
- Output:
  - All outputs from the *ADS-B Ground Station* and/or *Passive Locator* modules.
  - Messages' time differences of arrival.

5. CONCLUSION

This article described problematics of an air traffic simulation from the viewpoint of a passive surveillance system. Brief description of the ADS-B technology was presented, together with its shortcomings and types of feasible attacks. Possible representations of airborne target trajectories and means of moving airborne targets along these trajectories were described. The last part dealt with the actual design of the simulator. It presented random values which will be generated during simulation and entities, activities and events that will be represented in the simulator. Also, separate modules that the simulator will comprise were described. The simulator is still in development and it is reckoned that some modules will be modified, so they will model real system more precisely. Simulator will be used to create ADS-B message validation algorithms for use in passive ADS-B systems made of passive locators.

REFERENCES

Sun, J., 2017. ADS-B Decoding Guide. Available from: https://adsb-decode-guide.readthedocs.io/ [accessed 6 March 2017].

Federal Aviation Administration, 2015. Aeronautical Information Manual: Official Guide to Basic Flight Information and ATC Procedures.

EUROCAE, 2009. ED-102A, Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B).

Schäfer M., Lenders V., Martinovic I., 2013. Experimental Analysis of Attacks on Next Generation Air Traffic Communication. In: Jacobson M., Locasto M., Mohassel P., Safavi-Naini R., eds. ACNS 2013: Applied Cryptography and Network Security. Lecture Notes in Computer Science, vol 7954. Berlin, Heidelberg: Springer, 253–271.

Delahaye D., Puechmorel S., Tsiotras P., Féron E., 2014. Mathematical models for aircraft trajectory design: A survey. In: Electronic Navigation Research Institute, eds. Air Traffic Management and Systems. Lecture Notes in Electrical Engineering, vol 290. Tokyo: Springer, 205–247.

Quanbeck, D. B., 1982. Methods for generating aircraft trajectories. Alexandria: Center for Naval Analyses.

Mohleji, S. C., Wang, G., 2010. Modeling ADS-B Position and Velocity Errors for Airborne Merging and Spacing in Interval Management Application. The MITRE Corporation. Available from: https://www.mitre.org/sites/default/files/pdf/10_3030.pdf [accessed 8 October 2016].