Detecting GNSS spoofing of ADS-B equipped aircraft using INS

Birendra Kujur
MMAE Department
Illinois Institute of Technology
Chicago, USA
bkujur@hawk.iit.edu

Samer Khanafseh
MMAE Department
Illinois Institute of Technology
Chicago, USA
khansam1@hawk.iit.edu

Boris Pervan
MMAE Department
Illinois Institute of Technology
Chicago, USA
pervan@iit.edu

***Abstract*—In this paper, we develop a novel method to detect Global Navigation Satellite Systems (GNSS) spoofing for an Automatic Dependent Surveillance-Broadcast (ADS-B) equipped aircraft. The Federal Aviation Administration (FAA) has mandated [18] all civil aircraft to be ADS-B Out equipped by January 1, 2020. The ADS-B Out broadcast sent to Air Traffic Control (ATC) consists of the aircraft's position, velocity, and other aircraft-specific information, all of which being unencrypted, poses a serious integrity threat. With readily available ADS-B trackers [19], [20], a spoofer can accurately track an aircraft to generate a spoofed trajectory that can go undetected [11].**

We propose a novel method to modulate the ADS-B Out position broadcast such that a spoofed trajectory generated using the modulated ADS-B will be detectable by comparing Inertial Navigation System (INS) positions against those obtained using the spoofed GNSS signal. The amplitude of ADS-B modulation is selected to exceed the nominal INS error covariance so that spoofing is observable. In this work, we analytically quantify the magnitude of ADS-B modulation that will be sufficient for spoofing detection.

During scenarios of GNSS signal jamming and spoofing, reauthentication of a reacquired GNSS signal is necessary to maintain integrity. During a GNSS outage, given enough time, the INS solution drift will grow large enough such that the spoofed GNSS solution might be within the INS error covariance envelope and go undetected. For GNSS outage scenarios we propose continuous modulation of ADS-B position and analytically quantify the magnitude such that spoofing of the GNSS signal is detectable after signal is re-acquired.

***Index Terms*—ADS-B, INS, GNSS, spoofing**

I. Introduction

The civil infrastructure of safety critical fields such as aviation, maritime, and terrestrial navigation rely heavily on Global Navigation Satellite Systems (GNSS). The civil GNSS signal structure is publicly known and vulnerable to spoofing attacks, which endangers public safety [1]. A typical spoofing attacks could consist of a period intentional jamming of the authentic radio-frequency signals and followed by broadcast of a predetermined faulty signal to the user. The fault can be injected to cause gradual position or time offsets. Potential detection techniques include signal processing techniques, cryptographic authentication [2], spoofing discrimination using spatial processing by antenna arrays, automatic gain control schemes [3], [4], GNSS signal direction of arrival comparison [5], code and phase rate consistency checks [6], high-frequency antenna motion [7], and signal power monitoring techniques [8]. Some of these methods are indeed effective but they have various computational, logistical, and physical limitations.

Augmenting data from auxiliary sensors such as Inertial Measurement Units (IMU), barometric altimeters, and independent radar sensors to discriminate spoofing has also been proposed [9], [10]. The first stochastic description and quantification of the performance of an IMU-based GNSS spoofing monitor against worst-case faults was introduced by us [11]–[17]. We specifically investigated anti-spoofing solutions utilizing IMUs since all modern vehicles are equipped with them, thereby requiring minimal additional cost or system modification. An IMU is immune to external interference, which makes it an excellent candidate for countermeasure against GNSS spoofing attacks. INS, when used in the navigation solution in various integration schemes with GNSS (uncoupled, loosely-, tightly-, or ultra-tightly coupled), provides redundancy to the system and a direct means of resisting spoofing attacks.

ADS-B is a next generation surveillance technology incorporating both air and ground aspects that provides Air Traffic Control (ATC) with an accurate picture of an aircraft's three-dimensional position in en route, terminal, approach, and surface operations [18]. The aircraft provides the airborne portion in the form of a broadcast (ADS-B Out) of its identification, position, altitude, velocity, and other information. Aircraft equipped with ADS-B In capability can also receive these broadcasts and display the information to improve the pilot's situational awareness. The FAA has mandated that aircraft be equipped with ADS-B Out capability by January 1, 2020 to be compliant to fly in airspace classes A and B, where most civil aircraft operate. The FAA plans to use ADS-B as ATC's sole source for aircraft tracking and to revert to back up surveillance systems, such as secondary surveillance radar (SSR), whenever GNSS position sources can no longer meet integrity requirements.

The ADS-B broadcast is not encrypted and hence can be used by anyone to track an aircraft's position [19]. Currently, there has been no directive by the FAA for any future plans to encrypt the ADS-B. Also, encrypting ADS-B would amount to significant cost and time expense. In our prior work [11]–[17], we showed that a spoofer capable of accurately tracking an aircraft can generate a worst-case spoofing trajectory that can go undetected. Access to ADS-B broadcast allows the spoofer to track an aircraft without the need to employ sophisticated radar or an electro-optical targeting system. Readily available low-cost ADS-B tracking systems [20] make an aircraft more vulnerable to spoofing.

II. En route Aircraft

In this work, we consider an en route scenario where an aircraft utilizes a tightly-coupled INS/GNSS architecture, and its position and velocity estimates from a Kalman Filter (KF) are used for both navigation and ADS-B Out.

A. Tightly-coupled INS/GNSS architecture

An Inertial Navigation System (INS) provides the navigation solution as states of aircraft position r_x, r_y, r_z, velocity v_x, v_y, v_z, and attitude ϕ, θ, ψ (Euler angles), using IMU measurements. The aircraft states are,

$$\mathbf{x}_{A/C} = \begin{bmatrix} r_x & r_y & r_z & v_x & v_y & v_z & \phi & \theta & \psi \end{bmatrix}^T. \tag{1}$$

An IMU consists of tri-axis accelerometers and gyroscopes to provide measurements of acceleration and body angular rate. The acceleration measurements are integrated once to obtain velocity and then again to get position, whereas attitude is obtained by integrating angular rate measurements. These IMU measurements have errors (biases and noise), therefore the integrated outputs drift over time. In a tightly-coupled INS/GNSS architecture, a KF uses raw code and carrier measurements to estimate INS error states to arrest the drift.

In the KF, the IMU measurement $\widetilde{u}$ is modeled as a true measurement u^* corrupted by a time-varying bias b and additive White-Gaussian noise (WGN) η_u:

$$\widetilde{u} = u^* + b + \eta_u. \tag{2}$$

The additive WGN η_u is commonly derived from specifications on velocity random walk (VRW) for the accelerometers and angular random walk (ARW) for the gyroscopes. The bias is modeled as a first order Gauss-Markov random process (GMRP) with time constant τ_b and driving WGN ν_b. The driving WGN for the bias is derived from sensor specifications on the accelerometer and gyroscope bias instabilities:

$$\dot{b} = -\frac{1}{\tau_b} b + \nu_b. \tag{3}$$

The bias dynamics are included in the process model by augmentation of bias states $\mathbf{x}_{bias}$ to the aircraft state vector. The states for the three different IMU axes for both acceleration and angular rate measurements are

$$\mathbf{x}_{bias} = \begin{bmatrix} b_{a_x} & b_{a_y} & b_{a_z} & b_{\omega_x} & b_{\omega_y} & b_{\omega_z} \end{bmatrix}^T. \tag{4}$$

For the GNSS measurement model we assume the aircraft utilizes only single frequency GNSS measurements while en route, without any differential corrections, which is typical of today's RAIM environment. However, the concepts are equally applicable to dual frequency multi constellation GNSS, as well as terminal and precision approach scenarios. Equation (5) shows the GNSS measurement equation. The code measurement ρ for each satellite is composed of the true range p, satellite and receiver clock biases dt_{sv} and dt_{rc}, code ionospheric delay I_ρ, code tropospheric delay T_ρ, code mulitpath m_ρ, and receiver code thermal WGN $\nu_{th_{(\rho)}}$. Similarly, the carrier phase measurement $\lambda\phi$ for each satellite is composed of true range p, satellite and receiver clock bias dt_{sv} and dt_{rc}, carrier ionospheric phase advance I_ϕ, carrier tropospheric delay T_ϕ, carrier phase mulitpath m_ϕ, carrier phase cycle integer ambiguity N_ϕ, and receiver carrier thermal WGN ν_{th_ϕ}. Code ionospheric delay I_ρ is of the same magnitude as carrier ionospheric phase advance I_ϕ but opposite in sign, and code tropospheric delay T_ρ is of the same magnitude as carrier tropospheric delay T_ϕ (with the same sign):

$$\begin{aligned} \begin{bmatrix} \rho \\ \lambda\phi \end{bmatrix} = \begin{bmatrix} p \\ p \end{bmatrix} + \begin{bmatrix} c\,(dt_{rc} - dt_{sv}) \\ c\,(dt_{rc} - dt_{sv}) \end{bmatrix} + \begin{bmatrix} I_\rho \\ -I_\phi \end{bmatrix} + \begin{bmatrix} T_\rho \\ T_\phi \end{bmatrix} \\ + \begin{bmatrix} m_\rho \\ m_\phi \end{bmatrix} + \begin{bmatrix} 0 \\ \lambda N_\phi \end{bmatrix} + \begin{bmatrix} \nu_{th_{(\rho)}} \\ \nu_{th_{(\phi)}} \end{bmatrix} \end{aligned} \tag{5}$$

where, c is the speed of light in vacuum and λ is the carrier wavelength.

All the GNSS measurement errors need to be accounted for in the KF. Satellite clock offsets cdt_{sv} are available from the navigation message. After satellite clock offset correction, there are still residual errors due to satellite clock and ephemeris parameter uncertainty. These residual errors r_{sv} are be modeled [21] as a first order GMRP with a time constant $\tau_{r_{sv}}$ of 2 hours subject to driving WGN $\nu_{r_{sv}}$. These errors are modeled to have a standard deviation of 2 m. Equation (6) represents the first order GMRP model for satellite clock and ephemeris residual errors.

$$\dot{r}_{sv} = -\frac{1}{\tau_{r_{sv}}} r_{sv} + \nu_{r_{sv}}. \tag{6}$$

The receiver clock offset cdt_{rc} can be compensated by modeling the receiver clock with a constant clock offset drift rate model. The clock offset r_{rc} is modeled to drift with a constant rate $\dot{r}_{rc}$ over time as shown by (7),

$$\begin{bmatrix} \dot{r}_{rc} \\ \ddot{r}_{rc} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} r_{rc} \\ \dot{r}_{rc} \end{bmatrix} + \begin{bmatrix} w_{r_{rc}} \\ w_{\dot{r}_{rc}} \end{bmatrix} \tag{7}$$

where, $w_{r_{rc}}$ and $w_{\dot{r}_{rc}}$ are WGN for clock offset and clock offset drift rate, respectively. The variance of these WGN can be obtained using typical Allan Variance coefficients for various Timing Standards such as TCXO, OCXO, etc.

The ionospheric delay can be corrected using the ionospheric correction T_{iono} from the Klobachaur model and the residual errors r_i are modeled [21] to have a standard deviation given by (8),

$$\sigma_i = \sqrt{\max\left[(\tfrac{cT_{iono}}{5})^2, (F_{pp}\tau_{vert})^2\right]} \tag{8}$$

where, F_{pp} is the obliquity factor and τ_{vert} is calculated given the geomagnetic latitude [21]. Since ionospheric delay is a slowly changing error it can be modeled as a first order GMRP with a time constant of 2 hours and driving WGN ν_{r_i}:

$$\dot{r}_i = -\frac{1}{\tau_{r_i}} r_i + \nu_{r_i}. \tag{9}$$

The troposheric delay can be largley corrected with the model specified in [21], and the residual errors r_t can be modeled [21] as a first order GMRP with a time constant of 30 minutes. The standard deviation for this error is

$$\sigma_t = 0.12\ m(el) \quad \text{(meters)} \tag{10}$$

where, $m(el)$ is the mapping function of satellite elevation [21]. Equation (11) shows the first order GMRP model of tropospheric residual error r_t,

$$\dot{r}_t = -\frac{1}{\tau_{r_t}} r_t + \nu_{r_t} \tag{11}$$

where, ν_{r_t} is the driving WGN for tropospheric residual errors.

Multipath is modeled [21] as a first order GMRP with time constant τ_m of 25 seconds and driving WGN ν_m.

$$\dot{m} = -\frac{1}{\tau_m} m + \nu_m \tag{12}$$

The standard deviation for code multipath error is assumed conservatively to be 5 m [21] and for carrier 0.02 m.

The constant carrier phase cycle integer ambiguities along with all the residual error states described above are treated as GNSS error states to be augmented to the state vector:

$$\mathbf{x}_{GNSS} = \begin{bmatrix} {r_{sv}}^{1:n} & r_{rc} & \dot{r}_{rc} & {r_i}^{1:n} & {r_t}^{1:n} & m_\rho^{1:n} & m_\phi^{1:n} & \lambda N_\phi^{1:n} \end{bmatrix}^T \tag{13}$$

where, n is the number of satellites.

The final state vector of the INS/GNSS system is then

$$\mathbf{x} = \begin{bmatrix} \mathbf{x}_{A/C} & \mathbf{x}_{bias} & \mathbf{x}_{GNSS} \end{bmatrix}^T. \tag{14}$$

The INS system dynamics are linearized to obtain the linear augmented error states ($\delta\mathbf{x}$) and process model to be utilized in the KF. The error-state process model in discrete time can be represented as,

$$\delta\mathbf{x}_{k+1} = \mathbf{\Phi}_k\, \delta\mathbf{x}_k + \mathbf{\Gamma}_{w_k}\, \mathbf{w}_k \tag{15}$$

where, $\mathbf{\Phi}$ is the state transition matrix, $\mathbf{\Gamma}_{\boldsymbol{w}}$ is the process noise model, and $\mathbf{w}$ is the additive noise with process noise covariance $\mathbf{Q}$.

The error-state measurement model in discrete time is represented as,

$$\delta\mathbf{z}_k = \mathbf{H}_k\, \delta\mathbf{x}_k + \boldsymbol{\nu}_k \tag{16}$$

where, $\mathbf{H}$ is the observation matrix, and $\boldsymbol{\nu}$ is the measurement noise with measurement noise covariance $\mathbf{V}$.

B. Spoofing scenario

The spoofing method we assume here is that the spoofer takes position and velocity information from ADS-B and predicts the aircraft's future positions. The spoofer then creates satellite signals corresponding to these future aircraft positions and transmits them with higher power. The spoofer would want to mimic the authentic signals in the beginning such that there is not a noticeable discrepancy between the authentic and spoofed signal. Once the spoofed signal is acquired by the aircraft the spoofer can then slowly deviate the aircraft to a false trajectory. We consider the worst case scenario where the spoofer has a general knowledge of the aircraft's navigation architecture and can also reasonably compensate for the GNSS error states. Any uncertainty of these states will act against the spoofer, but it is difficult to take quantitative integrity credit for this.

The KF measurement update equation at any time k for the system states can be written as

$$\hat{\mathbf{x}}_k = \bar{\mathbf{x}}_k + \mathbf{L}_k(\mathbf{z}_k - \mathbf{H}_k\bar{\mathbf{x}}_k). \tag{17}$$

where, $\bar{\mathbf{x}}_k$ is the predicted state vector prior to the measurement and $\mathbf{L}$ is the Kalman Gain. We now introduce vectors $\mathbf{r}_k$ and $\mathbf{v}_k$ to represent the three dimensional position and velocity state vectors within the system state vector $\mathbf{x}$. The updated (post measurement) position and velocity state estimate vectors $\hat{\mathbf{r}}_k$ and $\hat{\mathbf{v}}_k$ are used for navigation and broadcast out via ADS-B, the latter represented as $\hat{\mathbf{r}}_{k_{ADS-B}}$ and $\hat{\mathbf{v}}_{k_{ADS-B}}$. The spoofer utilizes both of these to predict future aircraft position $\bar{\mathbf{r}}_{k+1_s}$ as,

$$\bar{\mathbf{r}}_{k+1_s} = \hat{\mathbf{r}}_{k_{ADS-B}} + (\hat{\mathbf{v}}_{k_{ADS-B}} \times \Delta t) \tag{18}$$

where, Δt is the time difference between the spoofer's acquisition of the ADS-B and transmission of spoofed GNSS signal. Using this predicted position the spoofer then converts this information to range domain using the equation

$$\mathbf{z}_{k+1_s} = \mathbf{H}_{k+1}\bar{\mathbf{x}}_{k+1_s}. \tag{19}$$

Here, we assume that the spoofer is able to synchronize to the GPS time and has reasonable knowledge of navigation system architecture. This is the worst case scenario since this allows him to reasonably compensate for other states. The spoofed range signal ($\mathbf{z}_{k+1_s}$), when it reaches the aircraft, gets corrupted with local multipath ($\mathbf{m}'$) and receiver thermal noise ($\boldsymbol{\nu}_{th}$), and thus the measured spoofed signal received by the aircraft becomes

$$\mathbf{z}_{k+1_{s(A/C)}} = \mathbf{z}_{k+1_s} + \mathbf{m}' + \boldsymbol{\nu}_{th}. \tag{20}$$

The position alert limit requirement for the en route phase of flight is 2 nmi [22]. Typical horizontal position and velocity error standard deviations for integrated INS/GNSS are about 6 m and 2 cm/s, respectively. Because INS is calibrated using GNSS prior to spoofing, a spoofer injecting a GNSS position and velocity fault consistent with this nominal uncertainty cannot be detected using INS. If the spoofed GNSS signal results in a position and velocity solution consistent with the above-mentioned nominal uncertainties of 6 m and 2 cm/s, it will likely go undetected.

Fig. 1 illustrates this scenario. It shows a typical cross track position error of an en route aircraft during level flight. The solid lines show cross track position error standard deviation. Until time $k = 5$, the aircraft is receiving authentic GNSS signals and using them to determine its positions. Position errors are represented with dots. At time $k = 5$, the spoofer receives the aircraft's ADS-B information and predicts the aircraft's position for time $k = 6$. For time $k = 6$, the spoofer returns a spoofed signal of higher power. The aircraft then

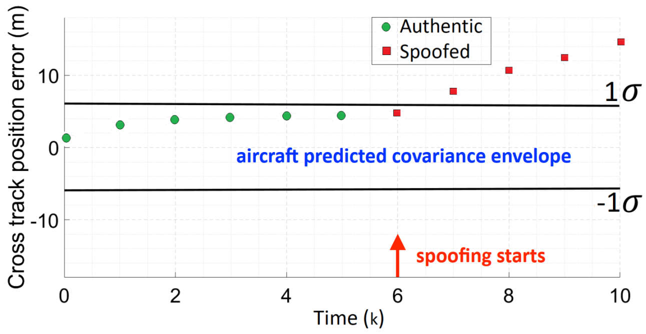

Fig. 1. Illustration of spoofing scenario.

receives the spoofed signal and uses it to determine position for time $k = 6$. Since this signal gives a position solution error within the nominal error standard deviation of 6 m, it would appear as authentic. The spoofer can then slowly divert the aircraft along a false trajectory by slowly injecting small successive deviations. The squares represent the position solution errors due to spoofed signals. The spoofer's advantage comes from the fact that he has the knowledge of the aircraft's true position and velocity as determined by the aircraft itself.

III. ADS-B Modulation and Position Domain-Innovation Monitor

The ADS-B Out broadcast of position and velocity has certain accuracy and integrity requirements. Within ADS-B, the aircraft sends out Navigation Accuracy Category for Position (NAC$_P$), Navigation Accuracy Category for Velocity (NAC$_V$) and Navigation Integrity Containment (NIC). The NAC$_P$ and NAC$_V$ specify with 95% probability a bound on the reported ADS-B position and velocity errors. To operate in civil airspace the minimum nominal requirements for NAC$_P$ and NAC$_V$ level are 8 and 1, respectively. These levels correspond to 92.6 m and 10 m/s [18]. This means that there is significant margin such that an aircraft can broadcast ADS-B Out purposely with some bias, or other modulation, in its position and velocity, while still being within the accuracy requirements of ADS-B. A spoofer using ADS-B broadcast would then generate a spoofed trajectory based on the modulated value of position and velocity.

We propose to transmit a modulated position which can be as simple the true position (i.e., as estimated by the aircraft) with an additive offset. We also propose a snapshot position domain-innovation monitor where we compare the position solution generated from the received GNSS measurements to the predicted position from the INS/GNSS KF. Recall, from (17) at any time k, the measurement update equation can be rewritten as,

$$\Delta \mathbf{x}_k = \hat{\mathbf{x}}_k - \bar{\mathbf{x}}_k \tag{21}$$

where,

$$\Delta \mathbf{x}_k = \mathbf{L}_k(\mathbf{z}_k - \mathbf{H}_k\bar{\mathbf{x}}_k). \tag{22}$$

Here, we can explicitly see that $\Delta \mathbf{x}_k$ represents the difference in the state vector obtained from the current GNSS measurements and the predicted state vector. Before updating our states in the KF, we would want to authenticate the GNSS signal. Hence we choose the test statistic as the difference between the received GNSS measurement $\mathbf{z}_k$ and the predicted measurement $\mathbf{H}_k\bar{\mathbf{x}}_k$ from the INS:

$$q_k = \mathbf{u}^T \Delta \mathbf{x}_k \tag{23}$$

where, $\mathbf{u}$ is a single column vector that extracts the desired position direction along which the ADS-B offset was applied. Expanding (23) we get

$$q_k = \mathbf{u}^T \mathbf{L}_k(\mathbf{z}_k - \mathbf{H}_k\bar{\mathbf{x}}_k) \tag{24}$$

For an authentic signal the test statistic has a zero mean and variance:

$$\text{var}(q_k) = \mathbf{u}^T\mathbf{L}_k(\mathbf{H}_k\bar{\mathbf{P}}_k\mathbf{H}_k^T + \mathbf{V}_k)\mathbf{L}_k^T\mathbf{u} \tag{25}$$

where, $\bar{\mathbf{P}}_k$ is the position error covariance matrix prior to the measurement update.

Thus, threshold T_k for a desired false alarm allocation can be set as a multiple (k_{FA}) of the standard deviation of the test statistic (q_k) distribution

$$T_k = k_{FA} \times \sqrt{\mathbf{u}^T\mathbf{L}_k(\mathbf{H}_k\bar{\mathbf{P}}_k\mathbf{H}_k^T + \mathbf{V}_k)\mathbf{L}_k^T\mathbf{u}} \tag{26}$$

For example, if the requirement is 10^{-5}, the threshold would be set at $4.42 \times \sqrt{\mathbf{u}^T\mathbf{L}_k(\mathbf{H}_k\bar{\mathbf{P}}_k\mathbf{H}_k^T + \mathbf{V}_k)\mathbf{L}_k^T\mathbf{u}}$.

When the spoofer creates signals corresponding to satellite range measurements using ADS-B information, we assume that the spoofer does not add any noise to these signals. We assume that the spoofed signals reach the aircraft antenna only with additive multipath error and receiver thermal noise.

At time k, the ADS-B position information is sent out by the aircraft with an offset position vector $\mathbf{b}_k$

$$\hat{\mathbf{r}}_{k_{ADS-B}} = \hat{\mathbf{r}}_k + \mathbf{b}_k. \tag{27}$$

The spoofer receives this position information and predicts the position at time $k+1$ using velocity information as

$$\bar{\mathbf{r}}_{k+1_s} = \hat{\mathbf{r}}_{k_{ADS-B}} + (\hat{\mathbf{v}}_{k_{ADS-B}} \times \Delta t). \tag{28}$$

With the aforementioned spoofing scenario from section II-B, the resulting spoofed measurement seen by the aircraft is,

$$\mathbf{z}_{k+1_{s(A/C)}} = \mathbf{H}_{k+1}\bar{\mathbf{x}}_{k+1_s} + \mathbf{m}' + \boldsymbol{\nu}_{th}. \tag{29}$$

Now for the spoofed signal the test statistic is

$$\begin{aligned} q_{k+1} = \mathbf{u}^T\mathbf{L}_{k+1}(\mathbf{H}_{k+1}(\bar{\mathbf{x}}_{k+1_s} + \mathbf{m}' + \boldsymbol{\nu}_{th}) \\ -\mathbf{H}_{k+1}\bar{\mathbf{x}}_{k+1}). \end{aligned} \tag{30}$$

Since we assume that the spoofer is reasonably able to compensate for all other system states, the expected difference between the states predicted by spoofer $(\bar{\mathbf{x}}_{k+1_s})$ and the actual system states $(\bar{\mathbf{x}}_{k+1})$ is

$$\bar{\mathbf{x}}_{k+1_s} - \bar{\mathbf{x}}_{k+1} = \bar{\mathbf{b}}_k \tag{31}$$

where, $\bar{\mathbf{b}}_k$ has the same length as state column vector $\bar{\mathbf{x}}_{k+1}$ and includes the 3×1 offset column vector

$$\bar{\mathbf{b}}_k = [\mathbf{b}_k \;\; \mathbf{0}]^T. \tag{32}$$

Thus, with further simplification, (30) becomes

$$q_{k+1} = \mathbf{u}^T\mathbf{L}_{k+1}(\mathbf{H}_{k+1}\bar{\mathbf{b}}_k + \mathbf{m}' + \boldsymbol{\nu}_{th}). \tag{33}$$

From (33) it can be seen that the mean of the test statistic at $k+1$ will shift due to offset vector $\mathbf{b}_k$, and the noise is due to the multipath ($\mathbf{m}'$) and thermal noise experienced by the spoofer's signal. Let $\mathbf{M}'$ be the diagonal matrix with elements accounting for the variances of the multipath error ($\mathbf{m}'$) and thermal noise ($\boldsymbol{\nu}_{th}$). Note that the multipath and thermal noise are zero mean. Thus, the mean and variance of the test statistic distribution are

$$\text{mean}(q) = \mathbf{u}^T\mathbf{L}_{k+1}\mathbf{H}_{k+1}\bar{\mathbf{b}}_k \tag{34}$$

$$\text{var}(q) = \mathbf{u}^T\mathbf{L}_{k+1}\mathbf{M}'\mathbf{L}_{k+1}^T\mathbf{u}. \tag{35}$$

Thus, when the spoofer utilizes modulated ADS-B information to generate spoofed GNSS signals, the offset $\mathbf{b}$ causes the test statistic to shift by a factor of $\mathbf{u}^T\mathbf{L}\mathbf{H}\bar{\mathbf{b}}$. Spoofing is detected when

$$q_k > T_k. \tag{36}$$

Fig. 2 illustrates how the test statistic distribution would be influenced given that the spoofer uses modulated ADS-B information to generate the spoofed signal. When an authentic signal is received, the test statistic would lie within the spoof free distribution with zero mean and variance of $\mathbf{u}^T\mathbf{L}(\mathbf{H}\bar{\mathbf{P}}\mathbf{H}^T + \mathbf{V})\mathbf{L}^T\mathbf{u}$. Once the spoofer uses the modulated ADS-B position to create the spoofed signal, the test statistic mean is shifted by a bias $\mathbf{u}^T\mathbf{L}\mathbf{H}\bar{\mathbf{b}}$. Since this received spoofed signal is affected by the multipath error and thermal noise, it will have a distribution with variance $\mathbf{u}^T\mathbf{L}\mathbf{M}'\mathbf{L}^T\mathbf{u}$.

For low missed detection rates we would want the spoofed distribution to be relatively far away from the threshold. Thus, given a probability of missed detection (P_{MD}) requirement, the mean of the spoofed distribution needs to be at an appropriate multiple (k_{MD}) of the standard deviation of the spoofed distribution. Note that the ADS-B offset sent out at time k will appear in the spoofed measurement at time $k+1$, but the threshold used at time $k+1$ will be based on position error covariance values at $k+1$ to ensure that the false alarm allocation is satisfied. This creates a time lag between expected relation between the mean of spoofed distribution and the threshold. Thus if there is a change in the spoof free distribution from time k to $k+1$, the threshold will shift. Hence, the ADS-B offset needs to be created accounting for predicted covariance for next time step. Thus, offset $\mathbf{b}$ needs to be chosen such that

$$\mathbf{u}^T\mathbf{L}_{k+1}\mathbf{H}_{k+1}\bar{\mathbf{b}}_k = k_{FA}\times\sigma_{\bar{x}_{k+1}} + k_{MD}\times\sigma_{{m'}_{k+1}} \tag{37}$$

where,

$$\sigma_{\bar{x}_{k+1}} = \sqrt{\mathbf{u}^T\mathbf{L}_{k+1}(\mathbf{H}_{k+1}\bar{\mathbf{P}}_{k+1}\mathbf{H}_{k+1}^T + \mathbf{V}_{k+1})\mathbf{L}_{k+1}^T\mathbf{u}} \tag{38}$$

and,

$$\sigma_{{m'}_{k+1}} = \sqrt{\mathbf{u}^T\mathbf{L}_{k+1}\mathbf{M}'\mathbf{L}_{k+1}^T\mathbf{u}}. \tag{39}$$

Note that $\mathbf{L}_{k+1}, \bar{\mathbf{P}}_{k+1}, \mathbf{H}_{k+1}$ and $\mathbf{V}_{k+1}$ are predicted by the aircraft at current time epoch k. Since the ADS-B position is constrained by the NAC$_P$ requirement of ADS-B, it cannot exceed the maximum estimated position uncertainty ($\mathbf{EPU}_{max}$) for that level [18]. For a NAC$_P$ level 8, $\mathbf{EPU}_{max}$ is 92.6 m. Thus, the aircraft needs to ensure that the position offset needs to meet the constraint equation

$$\mathbf{u}^T\bar{\mathbf{b}}_k + 2\sqrt{\mathbf{u}^T\hat{\mathbf{P}}_k\mathbf{u}} \leq \mathbf{EPU}_{max}. \tag{40}$$

Jamming and Spoofing

A more difficult case arises if the spoofer would use signal jammers to restrict access to authentic signals for some period and then transmit the spoofed signal to the aircraft. This jamming period could last from a few seconds to minutes in duration. An aircraft needs to validate the reacquired signal after a period of GNSS outage since the outage could occur either due to the spoofer using signal jammers or due to some other temporary, non-malicious source.

During a GNSS outage, the aircraft would utilize the INS-only position solution for navigation and ADS-B. Since the INS position solution drifts over time, the position error covariance of the aircraft will increase. As soon as the GNSS signal is received and validated, this error covariance will shrink back to nominal values. Fig. 3 is an illustration of such a scenario when a GNSS outage occurs. It shows typical position errors for an en route aircraft for such a scenario, where a GNSS outage occurs at time $k = 6$ and the signal is reacquired at time $k = 23$. The solid lines represent the position error covariance for the aircraft cross-track direction.

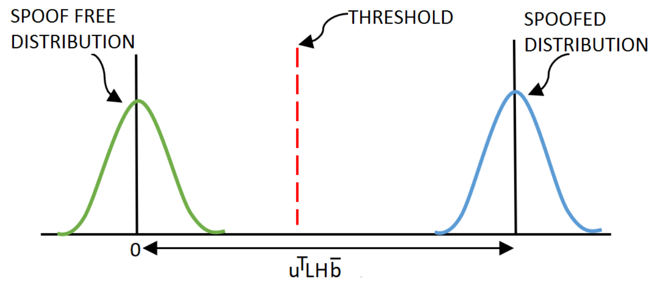

Fig. 2. Illustration of test statistic distribution change due to spoofed signal.

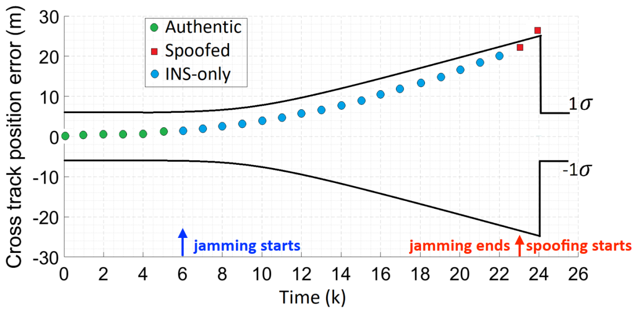

Fig. 3. Illustration of GNSS outage or jamming and re-acquisition.

As soon as the GNSS outage occurs at $k = 6$, the INS-only position error standard deviation starts to drift. Dots represent the position error from authentic GNSS signals until time $k = 5$ and from the INS-only solution after time $k = 5$. When a GNSS signal is received at time $k = 23$, the position error covariance shrinks. Here the squares represent the position error due to the reacquired signal, which is yet to be validated.

After jamming the GNSS signals, ADS-B is still the spoofer's best source to determine the aircraft position. Because the INS-only position error covariance $\bar{\mathbf{P}}$ increases with time it is clear from (37) that the ADS-B offset must also increase proportionally to the position error standard deviation. This will ensure that the spoofer's knowledge of aircraft position is always outside the uncertainty region of the INS-only solution. Note that due to increasing position error covariance during INS coasting, the aircraft may also have to update the $\mathrm{NAC_P}$ and NIC values in its ADS-B Out message.

Results and Discussion

The test scenario that we consider to evaluate the position domain-innovation monitor is for an aircraft equipped with navigation grade IMU, receiving single frequency GNSS code and carrier measurements. The aircraft has a tightly-coupled INS/GNSS architecture for navigation and ADS-B. The aircraft receives authentic signals for some time and then experiences GNSS signal jamming. The aircraft is sending out ADS-B position with some offset that the spoofer utilizes to generate the spoofed signal.

Fig. 4 illustrates the test scenario considered. The figure shows the aircraft receiving authentic GNSS signals for the first 60 s and then GNSS jamming is experienced for the next 60 s. At each time epoch the aircraft sends out a modulated ADS-B position and the position domain-innovation monitor checks for spoofing. Note that this figure shows the effect on test statistic distribution due to ADS-B modulation as shown in Fig. 2 over time. The spoofed test statistic distribution, with one standard deviation envelope, is shown as the blue shaded region in the figure. The threshold shown in the figure is determined from the spoof-free distribution of the test statistic. When jamming starts, $\bar{\mathbf{P}}$ increases with time causing the threshold to increase proportionally. Thus, when jamming occurs, the ADS-B offset also increases causing the spoofed distribution to move away sharply. The P_{MD} depends on the magnitude of the (spoofed) multipath noise distribution standard deviation. A larger multipath error on the spoofed signal would cause the spoofed distribution of the test statistic to span a larger area and thus could ostensibly increase chances of missed detection. If we refer to Fig. 2, this would mean the tails of the spoofed distribution would cross over the threshold. However, it is implicitly accounted for by the position offset as defined in (37). Given example false alarm and missed detection probability allocations of 10^{-5} and 10^{-7}, respectively, we choose appropriate values of k_{FA} and k_{MD} and then use (37) to compute the ADS-B cross track position offsets shown in Fig. 5. The figure also shows that

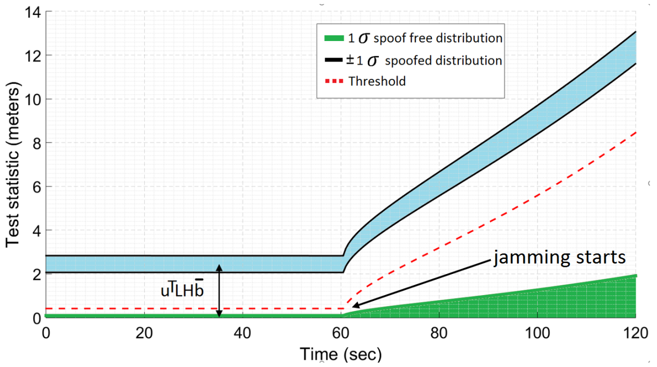

Fig. 4. Illustration of distribution of the test statistic during spoofing.

P_{MD} remains constant throughout. The standard deviation of the multipath error for the spoofed signal for this test scenario is 5 m and 0.02 m for code and carrier signals, respectively. It is further interesting to note that during a period of GNSS outage continuity has already been interrupted, so the false alarm allocation can be potentially be relaxed to reduce k_{FA}, which would mitigate to some extent the increasing ADS-B offset needed to maintain the desired constant P_{MD}. This novel approach of ADS-B modulation along with position domain-innovation monitoring not only addresses jamming-then-spoofing scenarios but also avoids any questions of when to start monitoring because it operates continuously. Future work for this study includes evaluating and protecting against potential spoofer countermeasures, for example attempts to "de-bias" using random counter-offsets. One scenario that can be thought of is the spoofer trying to send a signal counter-biased with offset drawn from a uniform distribution over the one standard deviation limit of ADS-B position. Thus, the probability of the test statistic being inside the threshold increases to be simply the ratio of limits of threshold to that of ADS-B position standard deviation. This distribution certainly would have higher P_{MD} than that of the simplistic aforementioned multipath distribution.

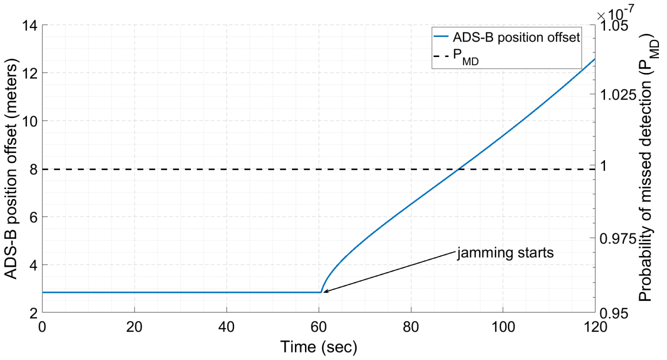

Fig. 5. Probability of missed detection and ADS-B position offset.

Conclusion

In this work, we first expose the vulnerabilities of an ADS-B equipped aircraft to spoofing. We show that a spoofer with access to ADS-B information can easily and accurately track aircraft, enabling the generation of false GNSS trajectories that can go undetected even with INS-aiding. Then we introduce a novel method of adding modulated offsets to ADS-B Out position reports, which can be a highly effective anti-spoofing measure for INS equipped aircraft. We propose a position domain-innovation monitor that would detect spoofed GNSS signals created using modulated ADS-B information. We also address the jamming-then-spoofing scenario where continuous modulation of ADS-B during GNSS outage situations would ensure that the spoofed signal is detectable with low probability of missed detection.

References

[1] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, and B. W. O'Hanlon, "Assessing the spoofing threat: development of a portable GPS civilian spoofer," in Proc. IEEE/ION PLANS, Savannah, GA, 2008, pp. 2314–2325.

[2] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys, "A proposed navigation message authentication implementation for civil GPS anti-spoofing," in Proc. IEEE/ION PLANS, Portland, OR, 2011, pp. 2314–2325.

[3] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," Navigation, vol. 59, no. 4, pp. 281–290, Winter. 2012.

[4] J. Nielsen, A. Broumandan, and G. Lachapelle, "Spoofing detection and mitigation with a moving handheld receiver," GPS World, vol. 21, no. 9, pp. 27–33, Sep. 2010.

[5] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM," in Proc. ION GNSS+, Nashville, TN, 2012, pp. 3007–3016.

[6] S. Moshavi, "Multi-user detection for DS-CDMA communications," IEEE Communications Magazine, vol. 34, no. 10, pp. 124–135, Oct. 1996.

[7] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," in Proc. ION GNSS+, Nashville, TN, 2013, pp. 2949–2991.

[8] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables," International Journal of Satellite Communications and Networking, vol. 30, no. 4, pp. 181–191, Jul. 2012.

[9] P. F. Swaszek, R. J. Hartnett, and K. C. Seals, "GNSS spoof detection using independent range information," in Proc. ION ITM, Monterey, CA, 2016, pp. 739–747.

[10] black A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," Journal of Field Robotics, vol. 31, no. 4, pp. 617–636, 2014.

[11] S. Khanafseh, et. al., "GPS Spoofing Detection Using RAIM with INS Coupling," in Proc. ION PLANS Conference, Monterey, CA, 2014.

[12] C. Tanil, S. Khanafseh, and B. Pervan, "Impact of Wind Gust on Detectability of GPS Spoofing Attack Using RAIM with INS Coupling," in Proc. IEEE/ION PNT Conference, Honolulu, HI, 2015, pp. 1232–1239.

[13] C. Tanil, S. Khanafseh, and B. Pervan, "GNSS spoofing attack detection using aircraft autopilot response to deceptive trajectory," in Proc. ION GNSS+, Tampa, FL, 2015, pp. 3345–3357.

[14] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "Kalman filter-based Innovation monitor to detect GNSS spoofers capable of tracking aircraft position," in Proc. IEEE/ION PLANS, Savannah, GA, 2016, pp. 1027–1034.

[15] C. Tanil, S. Khanafseh, and B. Pervan, "An Innovation monitor against GNSS Spoofing Attacks during GBAS and SBAS- assisted Aircraft Landing Approaches," in Proc. ION GNSS+, Portland, OR, 2016.

[16] C. Tanil, S. Khanafseh, and B. Pervan, "Detecting Global Navigation Satellite System spoofing using inertial sensing of aircraft disturbance," Journal of Guidance, Control, and Dynamics, vol. 40, no. 8, pp. 2006–2016, 2017.

[17] C. Tanil, S. Khanafseh, M. Joerger, B. Pervan, "An Innovation monitor to Detect GNSS Spoofers Capable of Tracking Aircraft Position," IEEE Transactions on Aerospace and Electronics, vol. 54, no. 1, pp. 131–143, Feb 2018.

[18] Advisory Circular, Department of Transportation, Federal Aviation Administration: Subject: Airworthiness Approval of Automatic Dependent Surveillance - Broadcast (ADS-B) Out Systems: AC-20-165..

[19] "How flight tracking works," retrieved October 21, 2019 from https://www.flightradar24.com/ how-it-works.

[20] "Build your own ADS-B receiver," retrieved October 21, 2019 from https://www.flightradar24.com/build-your-own..

[21] RTCA DO-316, Minimum Operational Performance Standards for Global Positioning System/ Aircraft-Bases Augmentation System Airborne Equipment.

[22] RTCA DO-208, Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System.