High Confidence Networked Control for Next Generation Air Transportation Systems

Pangun Park, Harshad Khadilkar, Hamsa Balakrishnan, and Claire J. Tomlin

***Abstract*—This paper addresses the design of a secure and fault-tolerant air transportation system in the presence of attempts to disrupt the system through the satellite-based navigation system. Adversarial aircraft are assumed to transmit incorrect position and intent information, potentially leading to violations of separation requirements among aircraft. We propose a framework for the identification of adversaries and malicious aircraft, and then for air traffic control in the presence of such deliberately erroneous data. The framework consists of three mechanisms that allow each aircraft to detect attacks and to resolve conflicts: fault detection and defense techniques to improve Global Positioning System (GPS)/inertial navigation, detection and defense techniques using the Doppler/received signal strength, and a fault-tolerant control algorithm. A Kalman filter is used to fuse high frequency inertial sensor information with low frequency GPS data. To verify aircraft position through GPS/inertial navigation, we propose a technique for aircraft localization utilizing the Doppler effect and received signal strength from neighboring aircraft. The control algorithm is designed to minimize flight times while meeting safety constraints. Additional separation is introduced to compensate for the uncertainty of surveillance information in the presence of adversaries. We evaluate the effect of air traffic surveillance attacks on system performance through simulations. The results show that the proposed mechanism robustly detects and corrects faults generated by the injection of malicious data. Moreover, the proposed control algorithm continuously adapts operations in order to mitigate the effects these faults. The ability of the proposed approaches to defend against attacks enables reliable air traffic operations even in highly adversarial surveillance conditions.**

***Index Terms*—Automatic dependent surveillance—Broadcast, intelligent control, misbehavior detection, next generation air transportation systems.**

I. Introduction

THE Next Generation Air Transportation System (NextGen) plan supported by the Federal Aviation Administration (FAA) aims to enhance the safety and efficiency of air transportation systems [1], [2]. The air traffic surveillance network is a critical part of NextGen operations, responsible for safety, traffic efficiency, and pilot assistance [3]. In NextGen, aircraft will carry new wireless communication and computing platforms, and have enhanced sensing capabilities. Interconnected aircraft not only collect information about themselves and their environment, but they also exchange this information in real time with other nearby aircraft. Wireless communication can operate beyond the line-of-sight constraints of radar and vision solutions, and thus enables cooperative approaches for air traffic management.

Security is an essential consideration for upgrades in the air transportation system, because there is the risk of making malicious behavior easier [2], [4]. The high level of decentralization in NextGen has both advantages and disadvantages: a rich set of tools is offered to pilots and authorities, but a formidable set of vulnerabilities also develops. There are potentially many hundreds of millions of communication devices in nationwide NextGen. It is recognized that in such a system, each communication component represents a new point of system vulnerability, and the system must be analyzed to understand and mitigate the impact of an attack at such points. For instance, an adversary may induce loss of separation between aircraft by injecting incorrect data in the satellite-based navigation system. These adversaries inject false surveillance information to create a "malicious" aircraft without the aircraft's knowledge. This misinformation may be re-transmitted by the aircraft, thus spreading to the rest of the network. As programmable sensors and actuators become more pervasive in NextGen, implementing appropriate security mechanisms will become even more critical to the overall safety and performance of the system.

The primary obstacle for designing a secure air transportation system is the tight coupling between communication, computation, and control. There are several challenges in securing NextGen air traffic management. First, many of the envisioned safety and pilot-assistance applications impose strict deadlines on message delivery. Security mechanisms must take these constraints into consideration and work with low processing and messaging overhead. Otherwise, it would suffice for an adversary to generate a high volume of false messages and overload resources. Second, since position dissemination is crucial for air traffic management, incorrect position information has severe impact on both safety and efficiency. Each aircraft needs

Manuscript received February 14, 2013; revised December 03, 2013; accepted January 05, 2014. Date of publication August 28, 2014; date of current version November 18, 2014. This work has been supported in part by the NSF under CPS:ActionWebs (CNS-931843), by ONR under the HUNT (N0014-08-0696) and SMARTS (N00014-09-1-1051) MURIs and by grant N00014-12-1-0609, by AFOSR under the CHASE MURI (FA9550-10-1-0567). Recommended by Associate Editor P. Tabuada.

P. Park was with the Department of Electrical Engineering and Computer Science, University of California at Berkeley, Berkeley, CA, USA. He is now with the Electronics and Telecommunications Research Institute, 305-700 Daejon, Korea (e-mail: pgpark@etri.re.kr).

H. Khadilkar was with the Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA, USA. He is now with IBM Research, India (e-mail: harshadk@mit.edu).

H. Balakrishnan is with the Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA, USA (e-mail: hamsa@mit.edu).

C. J. Tomlin is with the Department of Electrical Engineering and Computer Science, University of California at Berkeley, Berkeley, CA, USA (e-mail: tomlin@eecs.berkeley.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2014.2352011

to know not only its own position but also those of other aircraft in its neighborhood. Global Positioning System (GPS) signals are weak, can be spoofed, and are prone to jamming [5], [6]. Existing solutions such as frequency hopping do not completely solve the problem [7]. Third, to locate the aircraft in three-dimensional space, a minimum of four distance measurements to neighboring aircraft are required for triangulation. However, it is hard to obtain reliable measurements in the presence of adversaries across an air traffic surveillance network.

Finally, employing defense-in-depth methodologies, including fail-safe devices and fail-secure functionality, is a necessary part of any serious effort to protect NextGen. However, even a robust combination of such security systems is not sufficient for addressing the vulnerabilities of such a complex control system. The above is especially true when reliable operations must continue despite failures in the system. To address this complex problem and provide comprehensive security, all of the communication, computation, and control systems must be safeguarded in NextGen.

This paper addresses the fault detection and defense problem of air traffic surveillance networks in enroute areas. Ground infrastructure in these areas is sparse, and several regions are not covered by ground stations. Hence, the main detection and defense mechanisms are implemented onboard aircraft. We assume that aircraft regularly broadcast their status (e.g., position, speed, and direction) along with warnings about potential dangers using wireless communication [3]. Further, to simplify the presentation in this paper, all aircraft are assumed to fly at the same altitude. This assumption is generally valid in enroute areas, yet the analysis is straightforward to generalize to the case in which aircraft change altitude. We propose mechanisms combining the detection and defense algorithms of surveillance networks with a fault-tolerant control algorithm. Specifically, this consists of three mechanisms that allow aircraft to detect attacks and to resolve conflicts (violations of minimum separation requirements): (1) Fault detection of the GPS signal that increases the integrity of the GPS/Inertial Navigation System (INS) navigation loop in adversarial environments; (2) Distributed detection and defense techniques using the Doppler effect and the Received Signal Strength (RSS) measurement of received messages in order to verify aircraft position through the GPS/INS system; and (3) A fault-tolerant control algorithm that accounts for the uncertainty of surveillance information by introducing additional separation. In contrast to other position verification approaches, our detection and defense mechanisms are designed for a general network environment where nodes or beacons can move and no special hardware for ranging is available.

The remainder of this paper is organized as follows. Section II summarizes related work including localization techniques and control algorithms. Section III describes the models used for the air traffic and surveillance systems. Section IV presents the proposed system architecture. In Section V, we present the state and measurement dynamics. Section VI explains the GPS/INS loop that estimates the position of aircraft. Section VII proposes a self-localization algorithm using the Doppler effect and RSS measurements. Section VIII presents a fault detection technique using RSS measurements. Section IX describes a static verification algorithm to detect malicious aircraft. Section X presents the control algorithm, and the system performance is evaluated in Section XI. Finally, Section XII summarizes the contributions of the paper.

II. Related Work

During recent years, many localization techniques have been proposed for a variety of wireless network applications [8]. We only provide a brief survey on localization techniques suitable for air traffic surveillance networks. The localization approaches of air traffic networks differ in their assumptions about network deployment and hardware capabilities.

Centralized localization techniques would be impractical for air traffic surveillance networks because of the high communication costs and inherent delay, hence we focus on distributed localization techniques [9]. Distributed localization methods use only limited communication with nearby nodes [10]. These methods can be classified as range-based or range-free. Range-based techniques use distance estimates or angle estimates in location calculations, while range-free solutions depend only on the contents of received messages. Range-based approaches utilize time of arrival [11], time difference of arrival of two different signals [12], angle of arrival [13], RSS [14], and Doppler shifts [15], [16]. Some of these techniques require expensive separate hardware [11]–[13]. Moreover, stationary models of radio signals are not realistic assumptions since RSS measurements can be very sensitive to the channel environment [14]. The range-based approach using Doppler shifts is less susceptible to multi-path propagation than the RSS-based ranging approach [14], [17], since reflections do not change the frequency of the signal. The Doppler effect has been used extensively to estimate the velocity of tracked objects or to improve the accuracy of tracking systems [15], [16]. In [15], the self-localization of sensors is developed based on measuring Doppler shifts in a tone that is emitted from a mobile beacon. Each static node updates its location information by using the location and heading of the beacon as well as the frequency of the acoustic tone. On the other hand, in [16], the tracked node transmits a signal and stationary nodes measure the Doppler shifts of the transmitted signal. A number of stationary nodes are deployed around the tracked node and the tracked node cooperates with the tracking system.

None of these schemes address the problem encountered in air traffic surveillance, in which both the nodes and the beacons can move. They can be adapted for mobile networks by refreshing location estimates frequently, but are not designed with any explicit consideration for how mobility affects the localization performance. The only work we are aware of that considers localization with mobile nodes and beacons is in [18]. They use the sequential Monte Carlo Localization method for the random waypoint mobility model. Although it is very frequently used in mobile ad hoc networks, this mobility model is not realistic. The particle set can become easily diffused, dispersing across the image plane in the LOP of the enroute layout. Moreover, this localization technique is vulnerable to internal adversaries, since range-free localization depends only the contents of received messages. In addition, the particle-based approximation of filtered density is not sufficient to characterize the tail behavior of true density. This problem becomes more severe when the outliers are existent.

Previous localization techniques are vulnerable to several kinds of attacks, and an attacker may be able to disrupt the integrity or availability of all known localization techniques. A secure range-free localization technique was developed in [19]. However, it cannot detect and remove compromised beacon nodes. A number of authors have proposed using time-of-fight measurements and the speed of light to securely gain location information about untrusted parties. A time-bounded protocol is proposed as a defense against man-in-the-middle attacks on cryptographic identification schemes [20]. This protocol can be used to verify the proximity of two devices connected by a wired link. A protocol using temporal packet leashes is proposed for wireless networks to defend against similar attacks [21]. A new distance bounding protocol is proposed based on ultrasound and radio wireless communication in [22]. The protocol can only make an approximate decision about whether or not a claimer is within a certain region. These systems either require specific hardware or rely on an infrastructure of verifiers to check positions. However, these assumptions are not likely to hold in air traffic surveillance networks. It is desirable to be able to verify neighbors' position without any additional or dedicated devices. Furthermore, most techniques require beacon nodes to be numerous and evenly distributed so that they can cover the whole network. We are interested in performing localization in a more general network environment where no special hardware for ranging is available, the prior deployment of beacon nodes is unknown, the beacon density is low, and the node distribution is irregular.

Jamming attacks have been used as Denial-of-Service (DoS) attacks against different applications using wireless communications. In [23], several techniques for the detection of various jamming attacks are proposed and evaluated at MAC layer. The structure of this problem has been investigated in order to identify tradeoffs and capture the impact of different parameters on performance [24]. Optimal attack and network defense strategies were derived for the case of a single-channel wireless sensor network. The authors assume that all network nodes are uniformly distributed and that the topology is static. Countermeasures for coping with jammed regions in wireless networks have been studied in [7] and [25]. In [25], the use of low density parity check codes was proposed to cope with jamming. Further, an anti-jamming technique was proposed for 802.11b that involved the use of Reed-Solomon codes. In [7], a three-dimensional modulation scheme, known as message-driven frequency hopping (MDFH), was proposed. The basic idea of MDFH is that part of the message acts as the pseudo-random sequence for carrier frequency selection at the transmitter. The selection of carrier frequencies is directly controlled by the encrypted information stream rather than by a predefined pseudo-random sequence as in conventional FH, in order to improve the system spectral efficiency.

The increasing importance of security in vehicular networks has attracted [26]. Sybil attacks [27], in which an adversary creates an illusion of traffic congestion by claiming multiple identities, are known always be possible except under unrealistic assumptions of resource and coordination among entities without a logically centralized authority. Several techniques to detect Sybil attacks in ad hoc networks, including radio resource testing, registration, and position verification have been studied [28]. Position verification is a more promising approach for vehicular networks, since radio resource testing relies on specific assumptions on radio modules and registration alone is not effective. A distributed detection scheme of Sybil attacks is proposed for networks in which a set of fixed base stations overhear a malicious node [29]. This scheme will not suit enroute air traffic management, since ground base stations are sparse, and several regions are not even covered.

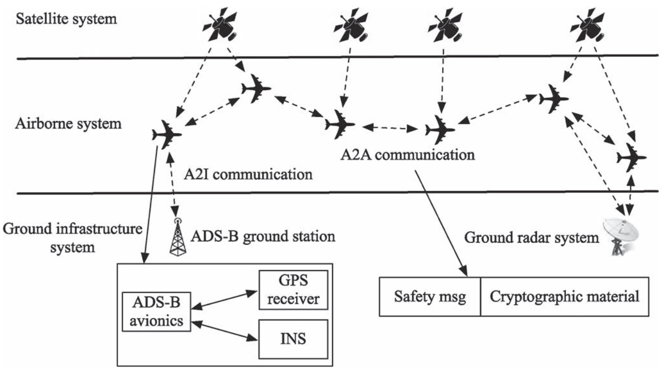


Fig. 1. Proposed framework in enroute airspace.

Several studies in the past decade have addressed the control of air traffic in a distributed setting [30]–[33]. However, these studies have not considered a combination of decentralized control with measurement and state uncertainty, nor have they addressed security issues with the proposed protocols. Eulerian models of air traffic such as [32] are useful when the perspective is strategic rather than tactical. Centralized algorithms such as those proposed in [34] can handle the computational requirements, but such approaches are limited in their scope when individual aircraft need to carry out conflict detection and resolution. In order to guarantee safety in the presence of uncertainty, the theory of reachable sets has been shown to be highly effective [31]. However, the computational requirements of this method are too prohibitive for fast distributed control. To the best of the authors' knowledge, this paper is the first one to propose a framework combining detection and defense surveillance with robust control. The proposed protocol is both computationally light and robust to uncertainty, as well as accidental or deliberate faults in measurement.

III. Framework

The proposed framework with its components is illustrated in Fig. 1. The direction of the arrows represents the flow of information. The infrastructure of NextGen is comprised of the mobile units (aircraft) and ground facilities. Aircraft-to-Aircraft (A2A) and Aircraft-to-Infrastructure (A2I) communication will enable safety-critical applications that provide warnings about accidents, traffic conditions and other events [2]. Secure air transportation systems are assumed to rely on public key cryptography and digital signatures to protect A2A and A2I messages in NextGen.

A. Communication Protocols

Automatic Dependent Surveillance-Broadcast (ADS-B) is designed to increase the safety, capacity, and efficiency of the airspace by enhancing information sharing between aircraft and ground facilities [3]. This system provides transmission ranges of typically 60 to 100 nm, with data rates in the 1 Mbps range. ADS-B uses 1090 MHz frequency band, different from the operation bandwidth of GPS systems [6]. Safety messages are signed and include the coordinates and time stamp of the sender. When an aircraft validates a certificate, it checks whether its credential has been revoked. If the credential is not revoked, it verifies the key used to sign the message and, once this is done correctly, it verifies the message. After validating an ADS-B message, an aircraft stores the information in its location table. Since our detection and defense mechanisms are distributed and localized, we assume that most neighboring aircraft in the airspace can be trusted. This allows aircraft to use information from reliable neighbors in order to identify malicious aircraft. It is reasonable to expect that only a relatively small percentage of aircraft (less than 10%) would be malicious.

B. Adversary Model

The reliability of safety-critical control systems can be threatened by a wide variety of failure modes, including failures of the communication links, sensors, controllers, and/or actuators. While some failure modes result in complete loss of control, others would only result in loss of reliable control.

In this paper, we consider adversaries or attackers that disrupt the air traffic management by attacking the satellite-based navigation system. Any of these attacks can affect air traffic management. There is a difference between malicious and non-malicious misbehavior. Non-malicious misbehavior is typically random, and can be detected easily. On the other hand, it is difficult to handle a sophisticated attack that exploits weaknesses in the satellite-based navigation system. An attacker can sufficiently modify messages to pass outlier detection tests. For example, adversaries could jam satellite signals within their range and thus selectively or completely prevent the GPS updates. Further, a GPS spoofing attack broadcasts a slightly more powerful signal that the legitimate one, and then slowly deviates away towards the position desired by the attacker [5]. Therefore, the system needs to provide more comprehensive protection from malicious misbehavior. The proposed defense mechanisms apply to both malicious and non-malicious misbehavior.

IV. Solution Overview

This section provides an overview of the proposed architecture of the Misbehavior Detection System (MDS) whose role is to detect off-nominal aircraft. Each aircraft executes this system, which functions in a distributed and localized manner. The details of each component are given in subsequent sections.

A necessary part of the design of autonomous systems is the inclusion of fault detection and identification algorithms which ensure that aircraft operate in a safe and reliable manner. The MDS protects the interface between aircraft networks, onboard control units, and data and services required by other aircraft, as illustrated in Fig. 2. This system constantly monitors the status of onboard systems and provides real-time detection of attacks. Further, the MDS controls the data flow from external sources to the aircraft. We consider two approaches for position verification in the MDS: a GPS/INS integrated system and a Doppler/RSS fusion process. A Kalman filter is used to fuse high frequency inertial sensor information with low frequency GPS data in the GPS/INS integrated system. The Kalman filter estimates the errors in position and velocity using the difference between external GPS sensor information and inertial indicated information. An error propagation model is used to fuse the observed and predicted positions and velocities. These parameters are fed back to the INS unit. To verify aircraft position through GPS/INS system, the detection and defense mechanisms are designed using the Doppler effect and RSS measurements of received ADS-B messages. An Extended Kalman Filter (EKF) is used to estimate the distance to neighboring aircraft. Given an adequate number of neighbors, the current position is obtained by using the Minimum Mean Square Estimate (MMSE). Then, a Kalman filter predicts the position of an aircraft based on the model of state dynamics. Once the Doppler/RSS-based position is obtained, predicted positions are compared to the ones estimated by the GPS/INS system. If the two differ by more than a predefined threshold, the GPS/INS position is deemed adversarial and rejected.

The estimated distance to neighboring aircraft is also used to verify neighbors' reported position through ADS-B. If the estimated distance does not match with distance information of a received ADS-B message, the verifying aircraft discards that message. Furthermore, we propose a simple detection technique using the history of RSS measurements to verify aircraft position. The control algorithm is responsible for computing the control action of an aircraft based upon the new observation. The control algorithm accounts for the uncertainty of the surveillance information in the detected malicious data. We emphasize that our mechanisms rely on the availability of prior information collected during periods of time when it deems it is not under attack. In contrast to other position verification approaches, we do not rely on special hardware or on preinstalled infrastructure [11]–[13, 29].

V. System Model

This section presents the modeling of aircraft dynamics and various measurement models. As discussed in the previous section, two different measurement models are used to design the detection and defense mechanisms: GPS/INS system and Doppler/RSS system.

A. System Dynamics

The state of a moving aircraft at time k is defined by the vector $\mathbf{x}(k) = (x(k), y(k), \dot{x}(k), \dot{y}(k), \ddot{x}(k), \ddot{y}(k))$ where $x(k)$ and $y(k)$ specify the position, $\dot{x}(k)$ and $\dot{y}(k)$ specify the speed, and $\ddot{x}(k)$ and $\ddot{y}(k)$ specify the acceleration in the x and y

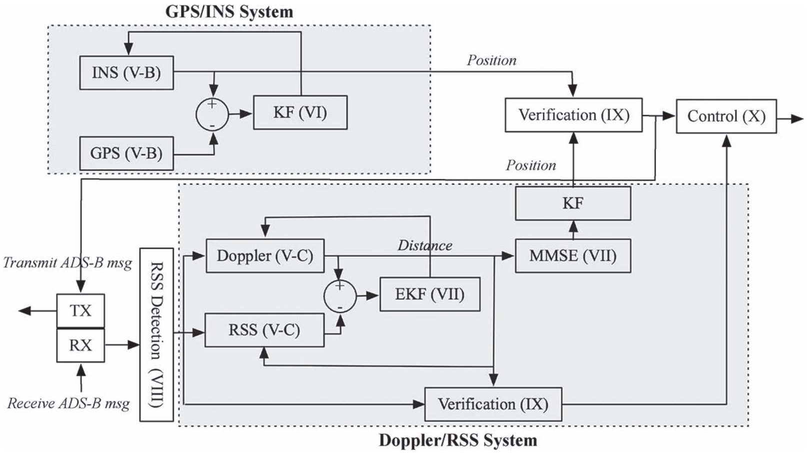


Fig. 2. System architecture of misbehavior detection system. We add the section number corresponding to the explanation of each component.

directions in a two-dimensional space. The aircraft dynamics can be described by a discrete-time linear time-invariant model

$$\mathbf{x}(k) = \mathbf{F}\mathbf{x}(k-1) + \mathbf{w}(k) \tag{1}$$

where $\mathbf{x}(k) \in \mathbb{R}^6$ is the state vector, $\mathbf{F}$ is the state transition matrix, and $\mathbf{w}(k) \in \mathbb{R}^6$ is white Gaussian noise with zero mean and covariance matrix $\mathbf{Q}(k) > 0$, i.e. $E[\mathbf{w}(k)] = 0$ and $E[\mathbf{w}(k)\mathbf{w}(k)^T] = \mathbf{Q}(k)$. The covariance matrix $\mathbf{Q}(k)$ of $\mathbf{w}(k)$ is $\mathbf{Q}(k) = \sigma_w^2 I$, where I denotes the unit matrix and σ_w is the standard deviation. Note that the system model does not include the input set. The control input is based on the information of GPS/INS system. However, the information resource of GPS/INS system is not secure under attack.

The time scale for reaction to events as described in this paper is of the order of several seconds. We therefore assume that the changes in velocity are accomplished by the next time step of the simulation. Maximum and minimum velocity is specified in the optimization problem, and includes the physical limits of the aircraft at the given altitude in Section X. Furthermore, since the time scale for reaction is long, it is not required to capture computationally intensive equations of state dynamics, such as the six degree of freedom models used in simulators. The state dynamics in this paper are modeled as a Wiener-sequence acceleration model [35]. This model provides a good compromise between complexity and performance in the modeling of aircraft dynamics. In such a model, $\mathbf{F}$ and $\mathbf{w}$ are equal to

$$\mathbf{F} = \begin{pmatrix} I_2 & \Delta_t I_2 & \frac{\Delta_t^2}{2} I_2 \\ O_2 & I_2 & \Delta_t I_2 \\ O_2 & O_2 & I_2 \end{pmatrix}$$

and $\mathbf{w}(k) = \begin{pmatrix} (\Delta_t^2/2)B \\ \Delta_t B \\ B \end{pmatrix} \psi(k)$ where Δ_t is the elapsed time since the last time step, and $\psi(k) \in \mathbb{R}$ is zero mean white Gaussian noise with assumed known covariance. $I_2 \in \mathbb{R}^{2\times 2}$ is the identity matrix, $O_2 \in \mathbb{R}^{2\times 2}$ is a zero matrix, and $B \in \mathbb{R}^{2\times 1}$ is a matrix for which all elements are equal to 1. The state error depends on the length of time between two calibrations using surveillance information, which in turn depends on the network performance and security. For instance, adversaries can jam GPS signals within their range to increase the time interval between calibrations of GPS receivers. Since control stability is expected to be subject to a maximum latency in the sensing layer of the network, it is necessary to ensure that the time difference between two calibrations satisfies the maximum latency acceptable to the control algorithm. We derive the value of the maximum allowable latency in Section X-F.

The general measurement model is represented as

$$\mathbf{z}(k) = \mathbf{H}\mathbf{x}(k) + \mathbf{v}(k) \tag{2}$$

where $\mathbf{z}(k) \in \mathbb{R}^m$ is the measurement vector of the sensor and $\mathbf{H} \in \mathbb{R}^{m\times n}$ is the measurement matrix. $\mathbf{v}(k) \in \mathbb{R}^m$ is white Gaussian observation noise with zero mean and with assumed known covariance matrix $\mathbf{R}(k) = E[\mathbf{v}(k)\mathbf{v}(k)^T]$.

In the next subsections we will describe the two specific measurement models that we use in the proposed architecture. Accurate analysis of measurement error is essential to ensuring effective data fusion of GPS/INS system and Doppler/RSS system, as we will discuss in Sections VI and VII. Furthermore, the error bound of measurement error is critical for controller design. Additional separation is introduced to compensate for the uncertainty of surveillance information due to adversaries. Hence, it is essential to characterize the uncertainties in position and velocity for aircraft. This is discussed in detail in Section X.

B. Measurement Dynamics of the GPS/INS

A simple measurement model for GPS is,

$$\mathbf{z}_{\mathrm{gps}}(k) = \mathbf{H}_{\mathrm{gps}}(k)\mathbf{x}(k) + \mathbf{v}_{\mathrm{gps}}(k) \tag{3}$$

where $\mathbf{H}_{\mathrm{gps}} = \begin{pmatrix} \mathbf{I}_2 & \mathbf{O}_2 & \mathbf{O}_2 \\ \mathbf{O}_2 & \mathbf{I}_2 & \mathbf{O}_2 \\ \mathbf{O}_2 & \mathbf{O}_2 & \mathbf{O}_2 \end{pmatrix}$, $\mathbf{z}_{\mathrm{gps}}(k) \in \mathbb{R}^6$ is the GPS measurement vector, and $\mathbf{v}_{\mathrm{gps}}(k) \in \mathbb{R}^6$ is zero mean white Gaussian noise with known covariance $\mathbf{R}_{\mathrm{gps}}(k)$.

The observed variable from the inertial sensor is the acceleration for the Inertial Measurement Unit (IMU) in an absolute frame of reference. A simplified IMU measurement model is

$$\mathbf{z}_{\text{imu}}(k) = \mathbf{H}_{\text{imu}}\mathbf{x}(k) + \mathbf{v}_{\text{imu}}(k) \tag{4}$$

where $\mathbf{H}_{\text{imu}} = \begin{pmatrix} \mathbf{O}_2 & \mathbf{O}_2 & \mathbf{O}_2 \\ \mathbf{O}_2 & \mathbf{O}_2 & \mathbf{O}_2 \\ \mathbf{O}_2 & \mathbf{O}_2 & \mathbf{I}_2 \end{pmatrix}$, $\mathbf{z}_{\text{imu}}(k) \in \mathbb{R}^6$ is the IMU measurement vector, and $\mathbf{v}_{\text{imu}}(k) \in \mathbb{R}^6$ is zero mean white Gaussian noise having known covariance $\mathbf{R}_{\text{imu}}(k)$. The processed acceleration measured by the IMU is integrated to obtain velocity and position. Each aircraft estimates the state $\mathbf{x}(k)$ using the measurement model in (3) and (4).

The error bounds of IMU sensors provide an explicit measure of the IMU performance, when it is the sole means of navigation (due to GPS outage) [36], [37]. The stochastic errors in inertial sensors cause the subsequent numerical integrations of the measurements to exhibit an ever increasing variance. By using Euler's method, the variance of double integrated wide-band noise is

$$\sigma_x^2 = t_s^4 \sigma_\omega^2 \frac{k(k+1)(2k+1)}{6}$$

where t_s is the sampling interval, σ_ω is the standard deviation of wide-band noise, and k is the number of samples. Note that the variance in position error due to wide-band noise is a function of the sampling interval, the noise variance and time. Thus, without any external resetting properties, white noise will cause an unbounded error growth in the IMU sensors.

C. Measurement Dynamics of Doppler Effect and RSS

To verify aircraft position through GPS/INS system, we propose a technique for the self-localization of aircraft using the Doppler effect and the RSS measurements. This section describes the measurement dynamics of Doppler effect and RSS of received ADS-B messages for aircraft localization.

A well known phenomenon that is observed when objects move relative to each other is the Doppler effect. The Doppler effect describes this situation in which an object transmits a signal and moves relative to an observer, the frequency of the observed signal will be shifted and the magnitude of the shift depends on the frequency of the signal and the velocity of the transmitter and observer relative to each other. In the method proposed, the frequency offset in the receiver is used as the observed state for distance estimation and localization. Modern air traffic control radars use the Doppler effect to discriminate moving aircraft from stationary targets [38]. Even though several localization techniques based on Doppler effect have been proposed, none of these schemes target the case when nodes and beacons can move [15], [16]. Using the Doppler effect in our proposed architecture as a verification of GPS/INS is attractive since it relies on the smoothness of the Doppler shift and the ability to predict it with low, essentially constant errors over long periods of time. This is in contrast to the IMU sensors, whose error grows exponentially with time. Further, this approach is robust, since reflections do not change the frequency of the signal.

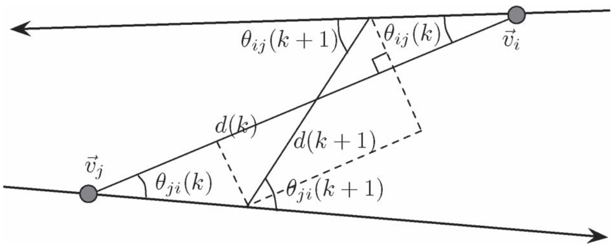


Fig. 3. Geometry for calculating the distance and relative angle between aircraft using the Doppler effect.

The frequency of the signal observed by a receiver moving relative to a transmitter can be written as follows:

$$f_r = f_t - \frac{f_t}{c}\left(\vec{v}_{ij} \cdot \frac{\vec{r}_{ij}}{r_{ij}}\right) \tag{5}$$

where f_r is the detected frequency, f_t is the frequency of the transmitted radio signal, c is the speed of the light, $\vec{v}_{ij}$ is the relative velocity of the receiver, $\vec{r}_{ij}$ is the range vector from the transmitter i to the receiver j, and $\vec{r}_{ij}/r_{ij}$ is the unit length vector. Equation (5) allows us to compute the relative speed of the tracked aircraft to the receiver, if the transmitted frequency f_t is known. Note that estimating the transmitted frequency with sufficient accuracy is required in the ADS-B standard [3]. Equation (5) can be written in a scalar form as follows:

$$f_r = f_t - \frac{f_t}{c} v_{ij} \cos\theta_{ij}$$

where v_{ij} is the relative scalar velocity between the receiver and the transmitter and θ_{ij} is the angle between the range vector and the direction of travel of the receiver. Therefore

$$\Delta f = \frac{v_{ij}\cos\theta_{ij}}{-\lambda_t} \tag{6}$$

where $\Delta f = f_r - f_t$ and wavelength $\lambda_t = c/f_t$. Consequently, we use (6) to compute the relative angle of the transmitter and the receiver, if the difference between the two frequencies as well as the relative speed are known. Note that estimating the frequency difference is possible using the radio transceiver on the aircraft. We assume that aircraft communicate their speeds as measured by the IMU sensors via ADS-B.

Consider the geometrical layout shown in Fig. 3. Let the distance between aircraft i and j at time k be $d(k)$, their respective velocity vectors be $\vec{v}_i(k)$ and $\vec{v}_j(k)$, and the relative angles be $\theta_{ij}(k)$ and $\theta_{ji}(k)$. Then, the distance between them is given by

$$d(k+1) = \Big[(d(k) - v_i\Delta_t\cos\theta_{ij} - v_j\Delta_t\cos\theta_{ji})^2 + (v_i\Delta_t\sin\theta_{ij} + v_j\Delta_t\sin\theta_{ji})^2\Big]^{0.5} \tag{7}$$

where Δ_t is the elapsed time since the last time step. Moreover, the update equation for the relative angle θ_{ij} is

$$\theta_{ij}(k+1) = \frac{\pi}{2} + \theta_{ij}(k) - \cos^{-1}\left(\frac{v_i\Delta_t\sin\theta_{ij}(k) + v_j\Delta_t\sin\theta_{ji}(k)}{d(k+1)}\right).$$

Since $d \gg |v_i \Delta_t \sin\theta_{ij}(k) + v_j \Delta_t \sin\theta_{ji}(k)|$, we approximate

$$\cos^{-1}\left(\frac{v_i\Delta_t \sin\theta_{ij}(k) + v_j\Delta_t \sin\theta_{ji}(k)}{d(k+1)}\right) \approx \cos^{-1}\left(\frac{v_i\Delta_t \sin\theta_{ij}(k) + v_j\Delta_t \sin\theta_{ji}(k)}{d(k)}\right).$$

By using the Taylor series expansion for the arccos function, the approximated update of the relative angle θ_{ij} is

$$\theta_{ij}(k+1) = \theta_{ij}(k) - \frac{v_i\Delta_t \sin\theta_{ij}(k) + v_j\Delta_t \sin\theta_{ji}(k)}{d(k)}.$$

We can derive a similar iterative update equation for the other relative angle, θ_{ji}.

We define the new state vector at time k as $\mathbf{x}_{\mathrm{dop}}(k) = (d(k), \theta_{ij}(k), \theta_{ji}(k))$ where $d(k)$ specifies the distance between aircraft i and j, θ_{ij} and θ_{ji} specify the relative angle in a two-dimensional space. The distance between aircraft can be described by a discrete-time nonlinear model

$$\mathbf{x}_{\mathrm{dop}}(k+1) = f_{\mathrm{dop}}\left(\mathbf{x}_{\mathrm{dop}}(k)\right) + \mathbf{w}_{\mathrm{dop}}(k) \tag{8}$$

$$\mathbf{z}_{\mathrm{dop}}(k) = h_{\mathrm{dop}}\left(\mathbf{x}_{\mathrm{dop}}(k)\right) + \mathbf{v}_{\mathrm{dop}}(k) \tag{9}$$

where $\mathbf{x}_{\mathrm{dop}}(k) \in \mathbb{R}^3$ is the state vector, $f_{\mathrm{dop}}(\mathbf{x}_{\mathrm{dop}}(k))$ is the state transition matrix, $\mathbf{w}_{\mathrm{dop}}(k) \in \mathbb{R}^3$ is white Gaussian noise with zero mean and covariance $\mathbf{Q}_{\mathrm{dop}}(k) > 0$. The covariance matrix $\mathbf{Q}_{\mathrm{dop}}(k)$ is given by $\mathbf{Q}_{\mathrm{dop}}(k) = \sigma_d^2 I$, where I denotes the unit matrix and σ_d is the standard deviation. $\mathbf{z}_{\mathrm{dop}}(k) \in \mathbb{R}^2$ is the measurement vector of the sensor, $\mathbf{v}_{\mathrm{dop}}(k) \in \mathbb{R}^2$ is the white Gaussian observation noise with zero mean and a known covariance $\mathbf{R}_{\mathrm{dop}}(k) = E[\mathbf{v}_{\mathrm{dop}}(k)\mathbf{v}_{\mathrm{dop}}(k)^T]$. Finally, $h_{\mathrm{dop}}(\mathbf{x}_{\mathrm{dop}}(k))$ is the measurement matrix.

The state model is

$$f_{\mathrm{dop}}\left(\mathbf{x}_{\mathrm{dop}}(k+1)\right) = \begin{pmatrix} d(k+1) \\ \theta_{ij}(k) - \frac{v_i\Delta_t \sin\theta_{ij}(k)+v_j\Delta_t \sin\theta_{ji}(k)}{d(k)} + w_1 \\ \theta_{ji}(k) - \frac{v_i\Delta_t \sin\theta_{ij}(k)+v_j\Delta_t \sin\theta_{ji}(k)}{d(k)} + w_2 \end{pmatrix} \tag{10}$$

where $d(k+1)$ is given in (7). The error in distance estimation depends on the length of time between two calibrations, which depends on the performance of ADS-B. The measurement model for the Doppler effect is

$$h_{\mathrm{dop}}\left(\mathbf{x}_{\mathrm{dop}}(k)\right) = \begin{pmatrix} \frac{v_{ij}\cos\theta_{ij}(k)}{-\lambda_t} + v_1 \\ \frac{\vec{v}_{ji}\cos\theta_{ji}(k)}{-\lambda_t} + v_2 \end{pmatrix}. \tag{11}$$

Now, we present a widely-used radio signal propagation model considering two factors that may incur signal attenuation: path loss and shadowing [17]. The received power P_r (measured in dB) that the aircraft receives from a particular transmitter at time t_k can be modeled as

$$P_r(t_k) = P_t(t_k) - PL_0 - 10\alpha(t_k)\log\left(\frac{d(t_k)}{d_0}\right) + X_g \tag{12}$$

where $P_t(t_k)$ is the transmission power in dBm, d_0 is a reference position, $d(t_k)$ is the position where the signal strength is measured, PL_0 is a correction constant which describes the additional loss at a reference position, $\alpha(t_k)$ is called the path loss exponent, and X_g is a Gaussian random variable with zero mean and standard deviation σ_g. The path loss exponent normally ranges from 2 to 6 (default value $\alpha = 2$ in ADS-B network [39]).

VI. Sensor Fusion for GPS and INS

A Kalman filter is used to fuse GPS and INS information. The GPS/INS loop uses a full two-dimensional inertial navigation unit as an internal sensor and a differential GPS unit as an external sensor. The actual implementation proposed for the GPS/INS integration loop is presented in Fig. 2. The Kalman filter is extensively used for GPS/INS data fusion [36], [37]. We adapt the standard GPS/INS integration loop for an adversarial environment: in particular, we include fault detection of the GPS signal by designing an error threshold derived from statistical reasoning and a condition on the Geometric Dilution of Precision (GDOP) [40] value to determine whether the GPS data is valid. The validation procedure uses the innovations and their associated covariances evaluated by the filter to determine the whiteness and unbiasedness of the innovations. The chi-squared distribution test provides a validation process which utilizes the theoretical properties of the innovation sequence. The threshold value is determined prior to the fusion process and represents the probability that a particular observation lies within an ellipsoid. The GDOP error mechanism arises when the trilateration geometry of the measurement sensors generates Lines-of-Position (LOP) which are nearly collinear (i.e., not orthogonal). Two positions are nearly collinear if they lie almost on the same line, that is, if the angle between them is small. When such a condition exists, the measurement errors can be blown up to determine a position.

The uncertainty in the GPS fix, or reported position, can increase depending on the aircraft's environment, that is, the uncertainty increases when the system is under attack through jamming or injection of malicious navigation messages. The GPS fixes have to be constantly monitored in order to determine if they are faulty. The GDOP indicator is considered to determine the rejection threshold of the measurement, depending on the geometry of the satellites. During the rejection of erroneous position GPS fixes, the fusion process remains at the prediction stage, and subsequently, the INS determines the navigation states. For GPS/INS-based navigators, these analytical results provide simple predictions of the robustness of the systems to temporary GPS outage.

VII. Data Fusion in Doppler/RSS Loop

This section describes an approach to the self-localization of aircraft using the Doppler effect and the RSS measurements. The objective of this algorithm is to verify GPS positions using independently received ADS-B messages. Each aircraft broadcasts its own location to its neighbors using ADS-B. Neighboring aircraft measure their separation from their neighbors and use the Doppler effect and RSS measurements to estimate their own positions. The fusion process estimates aircraft position in three phases as illustrated in Fig. 2. An EKF is first used to estimate the distance to neighboring aircraft using the Doppler effect and RSS measurements. We use the EKF because we are dealing with a nonlinear relationship between observed frequency and inter-aircraft distance as explained in Section V-C. The EKF utilizes RSS observations in order to determine the distance error, and this is then used to correct the distance estimated using the Doppler effect.

We calibrate the path loss exponent factor of the RSS-based ranging technique. Assuming that the path loss exponent is slowly varying, the RSS is used to estimate the current distance and the path loss factor can be calculated from the estimated distance using the EKF. Given d_0 and PL_0, the distance d and the path loss factor α are computed from (12). Given a ranging technology that estimates aircraft separation, a MMSE is used to estimate the actual position of the aircraft. In order to construct confidence intervals, we estimate the covariance matrix of the estimated position. We use the exponentially weighted moving standard deviation since the sample size may be small in enroute areas [41]. Finally, a Kalman filter is used to predict the position by using the model for state dynamics described in Section V-A.

Algorithm 1: Estimation of distance and channel model.

```
Input: Initialization $k = 0, w = 0.9, \alpha = 2$
Output: $d, \alpha, \sigma_g$
begin
    for ever do
        // RSS Verification
        $PL(k)$ ;
        // Path loss exponent update
        $\tilde{\alpha} = \frac{PL(k) - PL_0}{10 \log\left(\frac{d(k)}{d_0}\right)}$ ;
        $\alpha(k+1) = w\alpha(k) + (1 - w)\tilde{\alpha}$
        // Current distance update using RSS
        $\tilde{d} = d_0 10^{\frac{PL(k) - PL_0}{10\alpha(k+1)}}$ ;
        // Distance update using EKF
        $d(k+1) = \mathrm{EKF}(d(k), \Delta f, \tilde{d})$
        // Variance update
        $\overline{P}_r(k) = P_t(k) - PL_0 - 10\alpha(k+1) \log\left(\frac{d(k)}{d_0}\right)$ ;
        $\sigma_g^2 = \frac{1}{N} \sum_{i=1}^{N} \left(P_r(k) - \overline{P}_r(k)\right)$ ;
        $k = k + 1$
```

VIII. RSS Detection

In this section, we investigate the feasibility of using signal strength measurement to verify aircraft position. By successively measuring RSS variations, we obtain an estimate of the evolution of relative position between aircraft. This rough localization gives a sufficiently accurate indication of the coherence of the RSS measurements. The objective of the detection algorithm is to allow aircraft i to estimate the signal strength received from an aircraft j, based on previous RSS measurements. Such an approach can detect the intrusion of a malicious aircraft in the network. Let us consider the situation in which the aircraft i measures the strength of the received signal P_r from aircraft j at t_{k-1}. The possible locations of aircraft j with velocity v_j in the future form a circle whose center is the previous position of aircraft i and whose radius is equal to $v_j \Delta_t$ at $t_k = t_{k-1} + \Delta_t$. Aircraft i measures the maximum RSS, $P_r^{\max}(t_k)$, when aircraft j is at the nearest position to aircraft i, and the minimum RSS, $P_r^{\min}(t_k)$, when the aircraft j is at the most distant position from aircraft i $P_r^{\min}(t_k) \leq P_r(t_k) \leq P_r^{\max}(t_k)$. The maximum velocity of aircraft is limited by physical laws to $v_{\max}$. Therefore, a claimed position update should be within a predicted space window, calculated around the aircraft's previous position and a radius of $2v_{\max}\Delta_t$. From the radio propagation model, the RSS at time t_k is

$$P_r(t_k) = P_r(t_{k-1}) + \log\left(\frac{d(t_{k-1})}{d(t_k)}\right) + X_g. \qquad (13)$$

The RSS measured by the aircraft i should belong to the interval of $(P_r^{\min}(t_k), P_r^{\max}(t_k))$ at $t_k = t_{k-1} + \Delta_t$. If the RSS differs from the predicted signal strength for each neighboring aircraft by more than the defined thresholds, the receiver can deem the received signal as the product of an attack. Our localization technique uses only the history of RSS to deliver a reliable and fast detection. We verify the RSS measurement by using one sample z-test [42].

IX. Position Verification

We present a simple statistical algorithm to detect whether an aircraft is transmitting its actual position. Various model-based fault detection techniques have been discussed in [43]. Each aircraft executes this algorithm when enough measurements from a neighbor are collected. We divide the observation period, T, into discrete time intervals, $t_1, \ldots, t_n$. The claimed positions of an aircraft i form a sequence: $\rho(t_1), \ldots, \rho(t_n)$, and the estimated positions: $\tilde{\rho}(t_1), \ldots, \tilde{\rho}(t_n)$ where n is the sample size. Assuming that i is a nominal aircraft, the estimated position $\tilde{\rho}(t_i)$ contains only random errors and should follow a normal distribution. The difference $d_i = \tilde{\rho}(t_i) - \rho(t_i)$ should follow the standard normal distribution with mean $\mu_0 = 0$ and variance σ_0^2. Since the mean should be μ_0, the two-tailed t-test [42] is

$$|t| = \left| \frac{\bar{d} - \mu_0}{\frac{\sigma}{\sqrt{n}}} \right|$$

where $\bar{d}$ is the mean of the samples and σ is the standard deviation of the samples. The number of degrees of freedom in this test is $n - 1$.

X. Control Algorithm

The different detection and defense mechanisms presented in this paper significantly limit the options of adversaries, but these mechanisms are still insufficient for addressing some vulnerabilities. Whether due to inadvertent failure, error, or malicious action, reliable control also requires corrective mechanisms and fault-tolerant algorithms.

Fig. 4 shows a simplified model of a small section of enroute airspace. It depicts the intersection of four jet routes at the same altitude. This results in four intersection points 100 kilometers apart, and a total of 12 links. Designated intersections of two or more paths in the airspace are known as fixes, while the straight-line paths between two fixes are called links. Assuming that the jet routes are unidirectional, the flight path of each aircraft includes two orthogonal intersections.

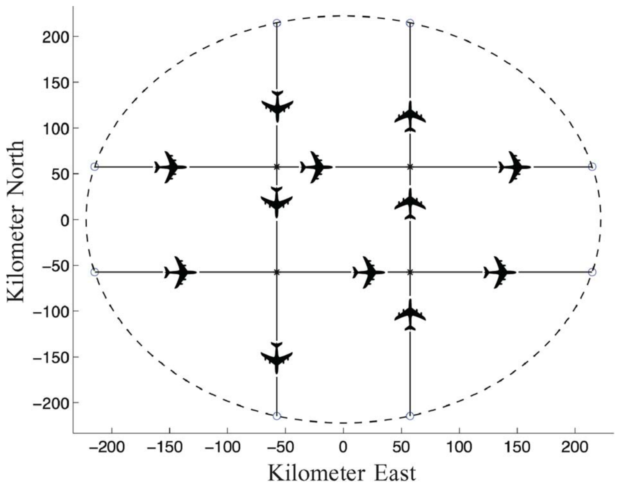


Fig. 4. A simplified layout of enroute airspace, which we use in our simulations.

A. Objectives and Constraints

We propose a control algorithm to minimize the flight times of aircraft from origin to destination points in the airspace representation. The primary control variable in this formulation is a change in velocity. A minimum separation requirement between each pair of aircraft is imposed for safety. The primary objective of the control algorithm is to meet this separation standard with a predefined minimum probability in adversarial environments. From an implementation perspective, it is also desirable to reduce the number of trajectory modifications [44]. An aircraft is sent to a holding pattern (assumed to be an elliptical trajectory designed to introduce separation between aircraft) only if no feasible velocity is found to resolve a projected conflict. The proposed control algorithm is considered to be automatically implementable by the aircraft implicated in a potential conflict. This would be in the form of advisories from the onboard algorithm providing information to the pilot. We assume that the aircraft under attack will not make any aggressive maneuvers, that is, its heading and velocity changes will be small.

The relative geometry between a given pair of aircraft depends on the links that they currently occupy. Broadly, any two links in the network in Fig. 4 can be classified as being *paired* or *unpaired*. Two links are said to be paired if they lead to the same fix, otherwise they are said to be unpaired. This distinction is important when considering the separation requirement between aircraft. If two aircraft are on paired links, the point of closest approach between them may occur before the merge point. In the next section, a geometrical constraint on the velocity of the trailing aircraft in a paired merge is derived.

B. Velocity Constraint for Paired Merges

Consider the geometrical layout shown in Fig. 5. Let us define the "time of contact" to be the time instance when aircraft B receives a broadcast from aircraft A for the first time. Let the relative position of aircraft A with respect to B at the time of contact be $\vec{r}_0$, their respective velocity vectors be $\vec{v}_A$ and $\vec{v}_B$, and the merge angle be $\theta = \pi/2$. Let the relative velocity be given by $\vec{v}_r = \vec{v}_A - \vec{v}_B$ and the angle between $\vec{r}_0$ and $\vec{v}_r$ by ϕ. Then the distance and time of closest approach between A and B can be calculated using the relations derived in [45]. The time of closest approach is given by

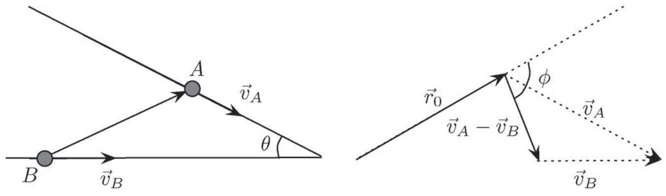


Fig. 5. Geometry for calculating the distance of closest approach.

$$t_c = -\left(\frac{\vec{r}_0 \cdot \vec{v}_r}{\vec{v}_r \cdot \vec{v}_r}\right)$$

and the relative position at the instant of closest approach is

$$\vec{r}_c = \vec{r}_0 + \vec{v}_r t_c = \vec{r}_0 - \vec{v}_r \left(\frac{\vec{r}_0 \cdot \vec{v}_r}{\vec{v}_r \cdot \vec{v}_r}\right).$$

The magnitude of the distance of closest approach is given by

$$r_c^2 = \vec{r}_c \cdot \vec{r}_c = r_0^2 \sin^2\phi.$$

Let the minimum separation required between two aircraft at any time be $s_{\min}$. The maximum allowable value of ϕ is defined by the minimum separation requirement $s_{\min}$ and an additional value ϵ, and is given by

$$r_0^2 \sin^2\phi = (s_{\min} + \epsilon)^2 \quad \Rightarrow \quad \sin\phi = \frac{s_{\min} + \epsilon}{r_0}. \tag{14}$$

The additional separation ϵ is added to $s_{\min}$ in order to meet the separation constraint with a probability β. The function of this additional separation is to compensate for the effect of adversaries. The value of ϵ is a function of the uncertainties in position and velocity for the two aircraft. If the uncertainties are assumed to be Gaussian and independent, $\epsilon = \sigma\Phi^{-1}(1 - \beta/2)$, where σ is the standard deviation of the position and Φ is the cumulative Gaussian function. The higher the value of β and/or the measurement uncertainty, the more conservative the control strategy. Note that the initial distance between A and B should be more than $(s_{\min} + \epsilon)$ for (14) to be valid. The value of ϕ decreases monotonically after initial contact, and the point of closest approach is reached when $\phi = \pi/2$. Therefore, if the initial value of ϕ is less than $\pi/2$, the distance between A and B increases monotonically. To maximize v_B while still maintaining separation, it should satisfy (14) with $\phi > \pi/2$. Finally, this constraint is not active if $\phi < \pi/2$, or if the projected point of closest approach is beyond the merge point.

C. Optimal Velocities for Paired Merges

Suppose aircraft A and B are at a distance s_A and s_B respectively from the merge point in Fig. 5. The optimal velocities v_A and v_B that minimize the time at which the trailing aircraft B reaches the merge point are given by

$$\begin{aligned} \min_{v_A, v_B} \quad & \frac{s_B}{v_B} \\ \text{s.t.} \quad & v_A \le v_{A,\max},\ v_B \ge v_{B,\min} \quad \text{(Feasibility)} \\ & v_B \le f(v_A, s_A, s_B) \quad \text{(Separation)}. \end{aligned} \tag{15}$$

Here, the constraint f on v_B considers the uncertainty of surveillance information due to adversaries, as explained in Section X-B. Optimal values of v_A and v_B can be calculated using Lagrange multipliers, and are given by $v_A = v_{A,\max}$, with v_B satisfying the separation constraint with equality. Note that this result simplifies the implementation of the decentralized version of the problem. Since aircraft A always flies at the maximum feasible velocity (subject to physical constraints and upstream traffic) and transmits this $v_{A,\max}$ as part of its ADS-B broadcast, aircraft B is able to compute its own optimal velocity unilaterally.

D. Synthesized Control Strategy

The nominal control algorithm uses local information received from ADS-B transmissions. In this paper, each ADS-B message is assumed to include a time stamp, and the maximum and minimum achievable velocities of the aircraft. Position and velocity reports are included in ADS-B by default. Conflict detection is carried out in a pairwise fashion for each pair of aircraft. When an aircraft A receives a broadcast from aircraft B for the first time, it first decides whether the new aircraft is likely to be a factor in its own trajectory. Only two types of engagements carry the risk of a conflict: aircraft that are on the same link, or on intersecting links approaching the same intersection point. In the above scenario, if aircraft B is on the same link and ahead of aircraft A, conflict resolution is the responsibility of aircraft A. It ensures that its own velocity is low enough to not risk a breach of the separation standard with aircraft B. On the other hand, if aircraft B is on another link but heading to the same intersection point, a pairwise precedence order first needs to be calculated. Aircraft A has precedence if its projected time at the intersection is earlier than that for aircraft B. In that case, aircraft A does not carry out any resolution maneuver. If aircraft B is expected to cross the intersection before aircraft A, the optimal velocity for aircraft A is calculated. Hence, resolution maneuvers (if required) are computed for the aircraft that are lower in the priority order. Consequently, an aircraft that is ith in the priority order could have up to $(i-1)$ downward adjustments of its computed velocity while the control algorithm is processing data. If the computed velocity is less than the least feasible velocity, it is commanded to enter a holding pattern in order to maintain separation. Finally, in addition to the detection of a new aircraft, an aircraft recalculates its velocity if there is a change in state (link, velocity or hold) of another aircraft already being tracked. Since each pair of aircraft decides on a mutual order at the merge point, a unique ordering of all aircraft heading to a given merge point is developed.

Due to stochastic transmission times and possible packet loss, state updates between aircraft are asynchronous. However, the time stamp within each ADS-B message allows the estimation of the current state of each aircraft, and also reduces the likelihood of inconsistent calculations in the distributed algorithm. Additionally, it guards against a mismatch caused by the clocks on two aircraft not being synchronized. As long as all aircraft use the transmitted time stamps, computations will be consistent.

E. Handling Untrustworthy Aircraft

When a transmitting aircraft is judged to be untrustworthy, only the distance to the aircraft and the relative velocity is assumed to be reliable. The distance to the aircraft is obtained by using the Doppler effect and RSS of received ADS-B messages as illustrated in Algorithm 1. A modified version of the nominal control algorithm is used by the receiving aircraft, in order to ensure separation from the compromised aircraft. A projection of the expected relative distance and velocity is made using the last known reliable report. The uncertainty in this position and velocity is then estimated using the difference from the measured distance and velocity. The uncertainty in state for the aircraft under attack is much larger than the aircraft which has nominal navigational performance.

When an aircraft determines that it is under attack, the control algorithm commands it to fly straight and level at the current velocity. While this strategy may not be feasible in congested arrival airspace with predefined approach paths, it is reasonable for enroute airspace. Moreover, it ensures that the aircraft does not make any maneuvers that are not expected by the surrounding traffic. It retains maximum accuracy of the INS as explained in Section VI. Finally, it also guarantees that the aircraft will fly out of the area under attack in a finite amount of time.

F. Challenges to Control Implementation

There are several issues to overcome before the proposed algorithm can be implemented in practice. There is a non-zero probability that two aircraft are projected to reach their merge point at exactly the same time. In this case, the asynchronous nature of ADS-B transmissions proves beneficial [3]. The control algorithm is set to give precedence to the other aircraft in case of deadlock. Since it is very likely that one aircraft receives a state update before the other, it will already have slowed down by the time the other aircraft begins its computations. Even if message delivery is nearly simultaneous and both aircraft reduce their own velocities, a small time difference between the adjustments will be sufficient to resolve the deadlock in the next computation cycle.

The same logic can be extended to non-cooperative aircraft in the airspace. If an aircraft that is expected to slow down does not do so, other aircraft can modify their own velocities in order to deconflict with it. This control logic can be used in the case of mixed ADS-B equipage or malicious ADS-B system. Actual non-cooperative behavior can be differentiated from message reception failure by using the State Update Interval (SUI) to calculate the probability of no messages being received by the aircraft in a given time window. We define the SUI as the elapsed time between successive state vector reports. The SUI is important from the point of view of stability of the control algorithm, for example, if an aircraft has to slow down suddenly.

The maximum allowable SUI that retains network stability is derived below. It is assumed that aircraft arriving earlier at the merge point have higher priority, and that they can change their velocities without considering the aircraft behind them. Suppose aircraft A, flying at velocities v_A, and B, flying at v_B, from Fig. 5 have previously made contact while at distances s_A and s_B from the merge point, and aircraft A has priority.

Aircraft A reduces its velocity to $v'_A \leq v_A$ while at a distance d_A from the merge point. Aircraft B, which is at distance d_B from the merge point, needs to adjust its own velocity to maintain separation with aircraft A. Nominally, aircraft A would reach the merge point after a further time $t_A = d_A/v_A$, which is changed to $t'_A = d_A/v'_A \geq t_A$. The instant of closest approach can be approximated by assuming that aircraft B is going to be in conflict with aircraft A at a time $(t'_A - t_A)$, before aircraft A arrives at the merge point. η_A denotes the maximum allowable SUI after which aircraft B can receive an update from aircraft A, and still not have to enter a holding pattern. In other words, aircraft B flies at its original velocity for a further time η_A, after which it slows to $v_{B,\min}$ until aircraft A is at the merge point. At this time, aircraft B needs to be at a distance $s_{\min} + \epsilon$ from it, where ϵ is the additional padding required due to adversaries. Equating the distance covered by aircraft B up to time t_A in the nominal case and up to time t'_A under the actual case, yields

$$d_B - s_{\min} - \epsilon = \underbrace{v_B\eta_A + v_{B,\min}\left(\frac{d_A}{v'_A} - \eta_A\right)}_{\text{Actualscenario}} = \underbrace{v_B\frac{d_A}{v_A}}_{\text{Original scenario}}.$$

Simplifying the above equation, the maximum allowable SUI for communication from aircraft A to aircraft B is

$$\eta_A = \frac{\frac{d_A}{v_A}v_B - \frac{d_A}{v'_A}v_{B,\min}}{v_B - v_{B,\min}}. \tag{16}$$

Equation (16) suggests that as d_A decreases, that is, as aircraft A approaches the merge point, it needs to provide faster updates in case of velocity changes. If aircraft B is already flying at its minimum speed ($v_B = v_{B,\min}$), then $v'_A = v_A$, that is, aircraft A cannot slow down without causing aircraft B to change its trajectory to maintain separation. In the nominal case, $v_A = v'_A$ and (16) implies $\eta_A = d_A/v_A$. Aircraft A only needs to transmit an update when it reaches the merge point, supporting the assumption that control computations need only be run when aircraft transition from one link to another. For any $v'_A < v_A$, the maximum allowable SUI is less than d_A/v_A, that is, there must be an update before aircraft A arrives at the intersection. Note that the minimum update interval is independent of position uncertainty. This is because the uncertainties are introduced into the formulation as an additive term to the minimum separation, they cancel out when considering only a change in aircraft velocity.

XI. Performance Evaluation

We evaluate the performance of the proposed system in terms of the congestion and instability of air traffic management along with the performance of the detection and defense algorithms under attack. The simulations are carried out using a simple model of air traffic operations, depicted in Fig. 4. For the simulations presented in this section, we assume that an adversary is located in the center of the enroute layout in Fig. 4. We consider a nominal range R, within which adversarial transmissions can be received. We fix the maximum attack range $R = 100$ km that covers the most congested area of the enroute layout. We call this the area under attack. The more powerful radios an adversary has, the higher its potential impact can be. For instance, adversaries can lock on actual GPS signals for a period of time when entering an area under attack. We abstract the physical properties of the adversarial equipment and consider the periods of time it can cause unavailability and keep the receiver locked on the spoofed signal. We conjecture that persistent disruption of data transmission is the worst form of attack, as it has the most severe impact. Further, a sophisticated attacker could selectively inject malicious data while avoiding detection.

We evaluate the effectiveness of the detection and the defense algorithms in a variety of setups, to gain insight into the role of each component of the system. We capture the uncertain nature of air traffic demand by the assumption that aircraft appear at the boundary of the simulated region as a Poisson process with average inter-arrival time $\lambda = 300$ s. To account for future traffic levels, 1.5 times ($\lambda = 200$ s) and 3 times the current traffic level ($\lambda = 100$ s) are also simulated. Individual flights are simulated from their initial appearance 200 km from the center, until their arrival to the fixes in Fig. 4. The simulation data was obtained from 6 experiments, with each repetition lasting 5.5 hours.

A. GPS Jamming Attack

An adversary jams the GPS signal in a nominal range $R = 100$ km with a certain attack probability per second. Whenever an aircraft gets GPS data, it either uses it to estimate the position or it rejects the GPS data if it deems it unreliable.

Fig. 6 shows the average position error and average number of holds per hour as a function of different attack probabilities $p = 0, \ldots, 1$ for traffic loads $\lambda = 100$, 200, 300 s, with the vertical bars indicating the standard deviation of the samples around the average. The attack probability $p = 1$ has the most severe impact since GPS system is completely jammed. The key metric for evaluating a defense technique is the accuracy of the position estimates under attack. Further, holding patterns in the airspace are an indicator of congestion and instability within the network. We see that the onset of instability is immediate for the highest traffic case, indicating that the nominal stability margin is quite small. These holds are necessary when just a velocity change by an aircraft cannot guarantee safety. In dense traffic, one holding pattern typically causes a cascade of holding patterns upstream, affecting a large section of the airspace.

In Fig. 6(a), the average position error increases as the attack probability increases due to the GPS jamming attack. The gate function of the GPS/INS system rejects jammed GPS signals. The position error increases quadratically when it is the sole means of navigation as explained in Section V-B. During the affected portion of the trajectory, the filter remains in the prediction stage and the IMU runs stand-alone. As the uncertainties of position and velocity increase, the control algorithm increases the separation between aircraft to guarantee the safety. Fig. 6(b) emphasizes the unstable nature of the network as the frequency of GPS jamming attack increases. We observe the increase in position error as the air traffic load increases under GPS jamming attack. The position of aircraft suddenly changes when it enters the holding mode under the high traffic load. Hence, the uncertainty in the observed error of the IMU increases as the traffic load increases under GPS jamming attack.

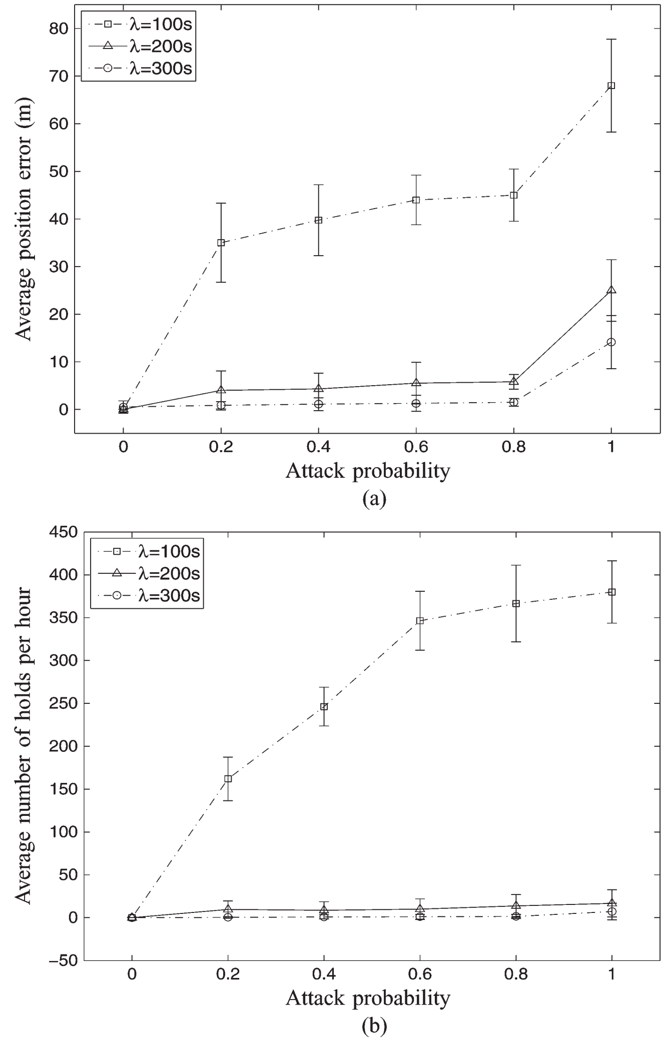


Fig. 6. Average position error and average number of holds per hour as a function of different attack probabilities $p = 0, \ldots, 1$ for different traffic loads $\lambda = 100$, 200, 300 s. The vertical bars indicate the standard deviation as obtained from 6 experimental runs of 5.5 hours each.

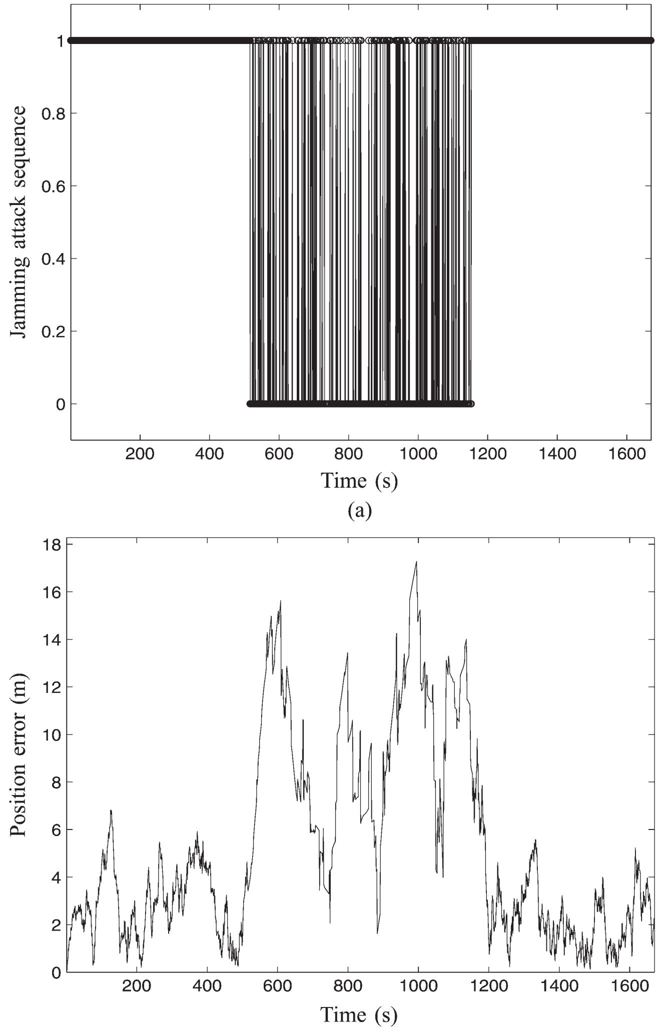


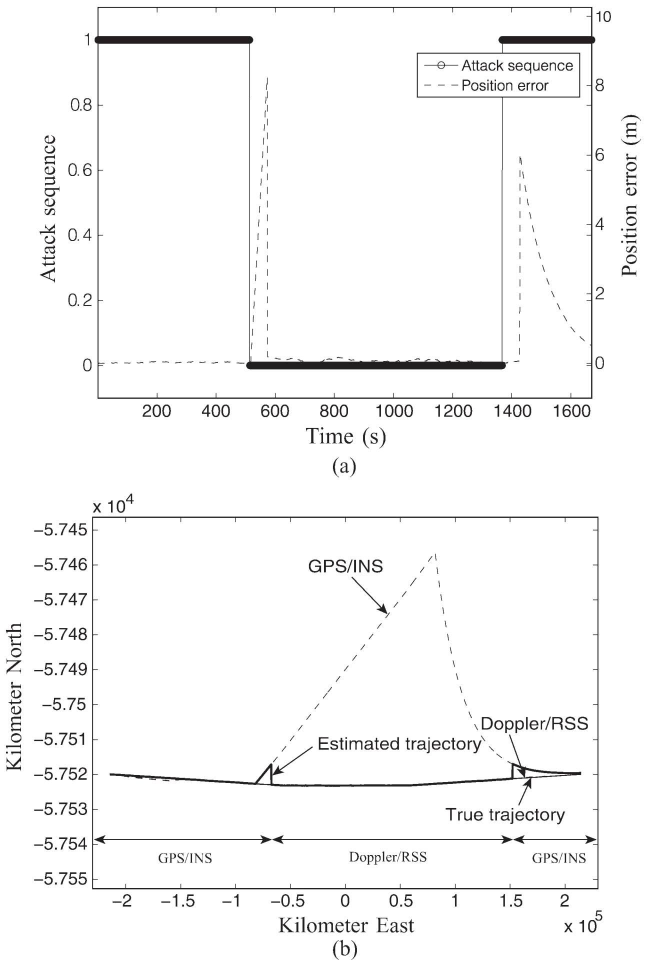
Fig. 7. Jamming attack sequence and position error of GPS/INS integrated system.

However, the error of the Kalman filer is not significant around several meters.

In Fig. 6(b), the proposed detection and defense algorithm efficiently stabilizes the traffic for nominal traffic arrival rates $\lambda = 200$, 300 s. The average number of holds increases as the traffic arrival rate increases. The current architecture cannot cope with higher traffic load $\lambda = 100$ s, and experiences a continuous increase in the number of holds in the airspace, most of which have been delayed in the central region. While holding patterns are generated in bursts, low to moderate traffic loads allow the airspace to recover and resume smooth operations. However, traffic accumulates if more holds are generated before this recovery is complete for high traffic loads. Furthermore, the effect of attack probability is significant for smaller interval of air traffic generation $\lambda = 100$ s due to the higher traffic loads. The benefits of using a GPS/INS integrated system are seen to be quite small for high traffic loads. Hence, the system with high traffic demand becomes unstable even by a relatively unsophisticated jamming attack.

At the normal air traffic load $\lambda = 200$, 300 s, the proposed system yields essentially the same level of average number of holds, because the conflict detection and resolution time is similar due to the similar position accuracy for $\lambda = 200$, 300 s. Overall, for short unavailability periods, the GPS/INS integrated system can be effective. As long as the position error does not grow significantly, the GPS jamming attack can be detected and efficiency defended.

Fig. 7 shows the evolution of position error due to a jamming attack, for a single aircraft with attack probability $p = 0.8$ and traffic load $\lambda = 200$ s over the duration of the flight. The aircraft starts at a location 50 km North, 200 km East of the origin and moves towards 50 km North, -200 km East. In Fig. 7(a), the spikes are time instances where packets are received. Fig. 7(b) presents the fused result of the navigation loop onboard the aircraft. After the aircraft crosses the boundary of the region under attack, errors build up until the aircraft leaves the vulnerable region. The gate function rejects the incorrect GPS fixes until the end of the vulnerable region where there is a slight adjustment since the uncertainty in the IMU solution is, at this stage, greater than that of the GPS fix. It shows the effectiveness of the Kalman filter, which keeps the position error less than 20 m. Even at this very high attack probability, the estimator and controller are able to guarantee safety.



(a)

(b)

Fig. 8. Error of estimated position, attack sequence, true trajectory, estimated trajectory, GPS/INS trajectory, and Doppler/RSS trajectory of a single aircraft for the fraction of malicious aircraft $p = 0.1$ and traffic load $\lambda = 200$ s.

B. Sophisticated GPS Attack

Even though INS can be effective for short unavailability periods of GPS signals, a sophisticated adversary can remain undetected if the system only relies on GPS and INS. The adversary could interfere with GPS messages and inject malicious navigation messages while avoiding detection [5].

Therefore, we now evaluate the Doppler/RSS system and its control performance by measuring how its estimated position errors, detection delay, and number of holds vary for different scenarios. Fig. 8 shows the error in the estimated trajectory, attack sequence, true trajectory, and estimated trajectory of a single aircraft with the fraction of malicious aircraft $p = 0.1$ and traffic load $\lambda = 200$ s. The aircraft starts in a position 50 km North, 200 km East and moves to a direction 50 km North, -200 km East. As the aircraft approaches the boundary of the vulnerable region, GPS/INS errors will increase due to the GPS spoofing attack. GPS fixes occur when the aircraft departs from this region. Fig. 8(a) presents an enhanced view of the attack sequence. The spikes are time instances where correct GPS signals are received. Fig. 8(b) shows a two-dimensional projection of the true trajectory and estimated trajectory using the GPS/INS system and the Doppler/RSS system. The estimated position presents the fused result using either GPS/INS system or Doppler/RSS system. Since a simple fault detection of the GPS/INS system is not able to reject the sophisticated GPS attack, the fused data is drawn into the vulnerable region. A significant position error is created because of the spoofing attack over a short period of time. However, the fusion algorithm of the Doppler/RSS loop is robust in its position estimates since it relies on the received signal information from neighboring aircraft instead of GPS signals.

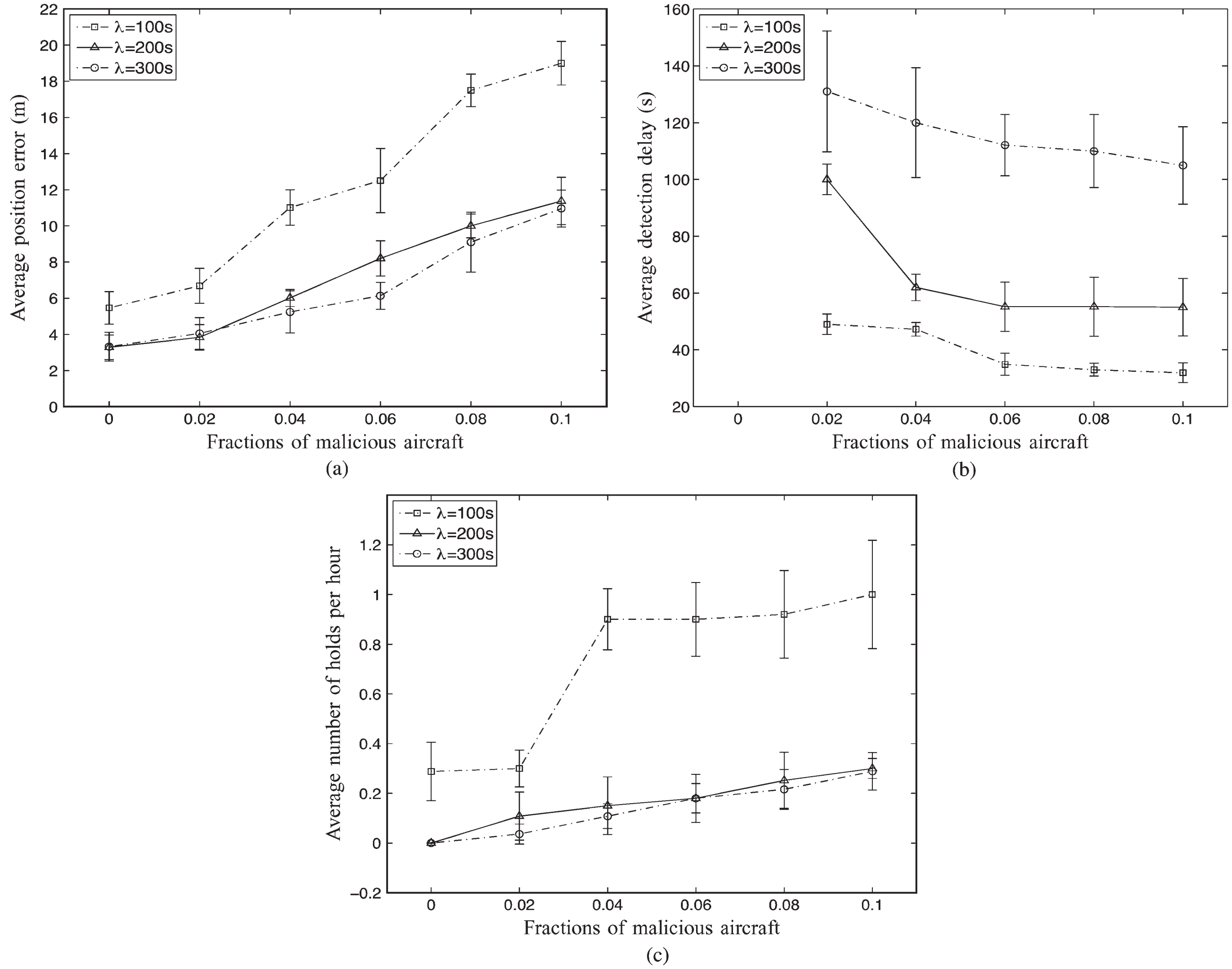
In Fig. 8(b), the estimated position switches from GPS/INS system to Doppler/RSS system when the position verification fails at time 580 s. By comparing with the attack sequence, we see that the detection delay of GPS spoofing is 70 s. The detection delay, which is the time required for the detection of an adversary by a receiver, is an important metric for evaluating the performance of the detection algorithm. When the trajectory difference between the GPS/INS system and Doppler/RSS system is small, the estimated position relies on the estimated position of GPS/INS system. Fig. 8(a) shows the spikes in error corresponding to switches between different systems.

Fig. 9 shows the average position error in the Doppler/RSS estimate, average detection delay, and average number of holds per hour for traffic loads $\lambda = 100$, 200, 300 s, as a function of different fractions of malicious aircraft $p = 0, \ldots, 0.1$. Fig. 9(a) shows the average error in the position estimates from the Doppler/RSS system when the aircraft density varies. By comparing position errors for traffic loads $\lambda = 200$, 300 s, increasing the density of aircraft improves the position accuracy using the Doppler/RSS system since aircraft will receive more location messages from neighboring aircraft. Note that increasing the density of aircraft makes localization easier, but it also increases the number of malicious aircraft in our setup. The number of correct aircraft available for estimating the position decreases as the fraction of malicious aircraft increases. Hence, the average position error of Doppler/RSS system increases as the fraction of malicious aircraft increases. When the filter detects a malicious aircraft, it rejects the information from this aircraft when it estimates its position.

Fig. 9(b) shows how the detection delay of malicious aircraft correlates with network density. Each aircraft verifies its own position using the hypothesis test based on received neighbor information. Since the accuracy of the Doppler/RSS system improves as aircraft density increases, the detection delay is significantly improved. In Fig. 9(c), even though the traffic arrival rate increases, the average number holds does not significantly increase. For the two cases with $\lambda = 200$, 300 s, the average number holds are approximately equal, because the conflict detection and resolution time is similar due to the similar position error and detection delay. The proposed Doppler/RSS system and control algorithm improve the detection and resolution time of conflicts for the safety constraints, and also provide a high level of efficiency in the system.

C. Operation Under a Challenging Scenario

The Doppler/RSS system can be effective for detecting and defending against a possibly sophisticated GPS adversary, when the fraction of malicious aircraft is small. As long as the number of malicious aircraft due to sophisticated GPS attacks does not grow significantly, a sophisticated GPS attack can



(a)

(b)

(c)

Fig. 9. Average position error, average detection delay, and average number of holds per hour as a function of different fractions of malicious aircraft $p = 0, \ldots, 0.1$ for traffic loads $\lambda = 100, 200, 300$ s.

be detected. However, for a sufficiently high number of sophisticated GPS adversaries, the attack can remain undetected. We study even extreme conditions, because the system has to remain operational under these conditions. Malicious aircraft are implemented as follows. Whenever a malicious aircraft is about to send an ADS-B message to announce its present position, it selects a fake position on the field and applies it to the ADS-B message (instead of its real position). We assume that the GPS/INS system is not able to detect this malicious aircraft. Whenever an aircraft gets a data packet, it estimates the distance by using the Doppler/RSS system. We consider a challenging scenario where the number of correct aircraft is less than three due to its poor GDOP indicator. Hence, it is not feasible to estimate the position using the Doppler/RSS system. Note that it is not trivial to directly modify the ADS-B system since most commercial aircraft are currently equipped with a hardware security module, whose purpose is to store and protect sensitive information. The control algorithm becomes conservative since it only relies on the distance estimation using the Doppler/RSS system.

Fig. 10 shows the average number of holds per hour as a function of different fractions of malicious aircraft $p = 0, \ldots, 0.1$ for various traffic loads $\lambda = 100$, 200, 300 s. The number of holds significantly increases as the fraction of malicious aircraft increases. The system with high traffic loads becomes unstable even with a small fraction of malicious aircraft. Hence, if the ADS-B system is malicious or faulty, then the system easily becomes unstable even if the GPS/INS system is active.

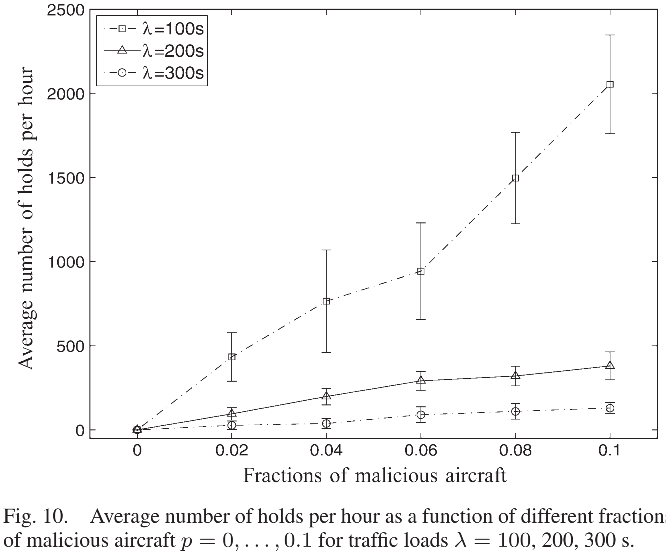


Fig. 10. Average number of holds per hour as a function of different fractions of malicious aircraft $p = 0, \ldots, 0.1$ for traffic loads $\lambda = 100$, 200, 300 s.

XII. Conclusions and Future Work

This paper proposes a framework for a secure and fault-tolerant system in the presence of adversaries across an air traffic surveillance network. Our detection and defense mechanism is a distributed and localized approach in which each aircraft can detect the reception of malicious signals, and then reject unreliable location reports generated by the attack. A Kalman filter is used to fuse high frequency inertial sensor information with low frequency GPS data. We also propose a technique for the position verification and localization of an aircraft that utilizes, the Doppler effect and RSS of the received ADS-B messages from neighboring aircraft. This estimated neighboring information is then used to verify the aircraft's own position by means of Kalman filtering. By accounting for the uncertainty of surveillance information, we design a control algorithm to minimize the flight time while meeting the safety constraints in adversarial environments. We evaluate the effect of security breaches on the air traffic management through simulation. Simulation results show that the proposed algorithms are capable of robustly detecting faults caused by malicious aircraft. Moreover, the filter using the Doppler effect and the RSS is shown to be able to detect sophisticated GPS attacks. The proposed control algorithm continuously adapts system operations to avoid and tolerate malicious faults.

The simple model considered in this paper, while providing valuable insights, could be extended, for example, by considering control inputs. The tradeoff between computation complexity and efficiency of misbehavior detection systems is important for practical implementation. Another related direction is the formal analysis of the proposed architectures by considering realistic NextGen scenarios.

References

[1] *NextGen Implementation Plan*, FAA, 2011. [Online]. Available: http://www.faa.gov/nextgen/media/NextGen_Implementation_Plan_2011.pdf

[2] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty, "Future e-enabled aircraft communications and security: The next 20 years and beyond," *Proc. IEEE*, vol. 99, no. 11, pp. 2040–2055, Nov. 2011.

[3] *Minimum Aviation System Performance Standard for Automatic Dependent Surveillance Broadcast (ADS-B)*, RTCA, 2002, DO-242A.

[4] J. Weiss, *Protecting Industrial Control Systems From Electronic Threats*. Momentum Press, 2010.

[5] J. V. Carroll, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," Volpe Center for the Office of the Secretary of Transportation, 2001, Tech. Rep.

[6] B. H. Wellenhoff, H. Lichtenegger, and J. Collins, *Global Positioning System: Theory and Practice*. Berlin, Germany: Springer–Verlag, 1997.

[7] Q. Ling and T. Li, "Message-driven frequency hopping: Design and analysis," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1773–1782, 2009.

[8] N. Patwari, J. Ash, S. Kyperountas, A. Hero, R. Moses, and N. Correal, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 54–69, 2005.

[9] Y. Shang, W. Ruml, Y. Zhang, and M. P. J. Fromherz, "Localization from mere connectivity," in *ACM MobiHoc*, 2003.

[10] S. Capkun, M. Hamdi, and J.-P. Hubaux, "GPS-free positioning in mobile ad hoc networks," *Cluster Comput.*, vol. 5, pp. 157–167, 2002.

[11] E. Xu, Z. Ding, and S. Dasgupta, "Source localization in wireless sensor networks from signal time-of-arrival measurements," *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2887–2897, 2011.

[12] A. Savvides, C.-C. Han, and M. B. Strivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *ACM MobiCom*, 2001.

[13] D. Niculescu and B. Nath, "Ad hoc positioning system (APS) using AOA," in *IEEE INFOCOM*, 2003.

[14] P. Bahl and V. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *IEEE INFOCOM*, 2000.

[15] R. Kozick and B. Sadler, "Sensor localization using acoustic doppler shift with a mobile access point," in *IEE/SP SSP*, 2005.

[16] B. Kusy, A. Ledeczi, and X. Koutsoukos, "Tracking mobile nodes using rf doppler shifts," in *ACM SenSys*, 2007.

[17] A. Goldsmith, *Wireless Communications*. Cambridge, MA: Cambridge University Press, 2005.

[18] L. Hu and D. Evans, "Localization for mobile sensor networks," in *ACM MobiCom*, 2004.

[19] L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization for wireless sensor networks," in *ACM WiSe*, 2004.

[20] S. Brands and D. Chaum, "Distance-bounding protocols," in *EUROCRYPT*. Berlin, Germany: Springer–Verlag, 1993.

[21] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. IEEE INFOCOM*, 2003.

[22] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *ACM WiSe*, 2003.

[23] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *ACM MobiHoc*, 2005.

[24] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 8, pp. 1119–1133, 2010.

[25] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," *ACM SIGMOBILE Mobile Comput. and Commun. Rev.*, vol. 7, no. 3, pp. 29–30, 2003.

[26] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 84–95, 2009.

[27] J. R. Douceur, "The sybil attack," in *IPTPS*, 2002.

[28] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis defenses," in *ACM/IEEE IPSN*, 2004.

[29] S. Capkun and J.-P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *IEEE INFOCOM*, 2005.

[30] A. Bicchi and L. Pallottino, "On optimal cooperative conflict resolution for air traffic management systems," *IEEE Trans. Intell. Transport. Syst.*, vol. 1, no. 4, pp. 221–232, 2000.

[31] I. Mitchell, A. Bayen, and C. Tomlin, "A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games," *IEEE Trans. Autom. Control*, vol. 50, no. 7, pp. 947–957, 2005.

[32] A. Bayen, R. Raffard, and C. Tomlin, "Adjoint-based control of a new Eulerian network model of air traffic flow," *IEEE Trans. Control Syst. Technol.*, vol. 14, no. 5, pp. 804–818, 2006.

[33] C. E. van Daalen and T. Jones, "Fast conflict detection using probability flow," *Automatica*, vol. 45, no. 8, pp. 1903–1909, 2009.

[34] A. Alonso-Ayuso, L. F. Escudero, and F. J. Martin-Campo, "A mixed 0–1 nonlinear optimization model and algorithmic approach for the collision avoidance in ATM: Velocity changes through a time horizon," *Comput. & Oper. Res.*, vol. 39, no. 12, pp. 3136–3146, 2012.

[35] Y. Bar-Shalom, X. R. Li, and T. Kirubajan, *Estimation With Applications to Tracking and Navigation*. New York: Wiley-Interscience, 2001.

[36] H. Liu, S. Nassar, and N. El-Sheimy, "Two-filter smoothing for accurate INS/GPS land-vehicle navigation in urban centers," *IEEE Trans. Vehic. Technol.*, vol. 59, no. 9, pp. 4256–4267, 2010.

[37] A. Vu, A. Ramanandan, A. Chen, J. Farrell, and M. Barth, "Real-time computer vision/DGPS-aided inertial navigation system for lane-level vehicle navigation," *IEEE Trans. Intell. Transport. Syst.*, vol. 13, no. 2, pp. 899–913, 2012.

[38] Z. Li and R. Narayanan, "Doppler visibility of coherent ultrawideband random noise radar systems," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 42, no. 3, pp. 904–916, 2006.

[39] P. Park and C. Tomlin, "Investigating communication infrastructure of next generation air traffic management," in *ACM/IEEE ICCPS*, 2012.

[40] M. Zhang and J. Zhang, "A fast satellite selection algorithm: Beyond four satellites," *IEEE J. Select. Topics Signal Process.*, vol. 3, no. 5, pp. 740–747, 2009.

[41] D. E. Knuth, *Seminumerical Algorithms, The Art of Computer Programming*, vol. 2. Reading, MA: Addison-Wesley, 1981.

[42] E. L. Lehmann and J. P. Romano., *Testing Statistical Hypotheses*. New York: Springer Texts in Statistics, 2005.

[43] I. Hwang, S. Kim, Y. Kim, and C. Seah, "A survey of fault detection, isolation, and reconfiguration methods," *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 3, pp. 636–653, 2010.

[44] M. Lupu, E. Feron, and Z.-H. Mao, "Traffic complexity of intersecting flows of aircraft under variations of pilot preferences in maneuver choice," in *IEEE Conf. Decision and Control*, 2010.

[45] J. Krozel and M. Peters, "Strategic conflict detection and resolution for free flight," in *IEEE Conf. Decision and Control*, 1997.

Pangun Park received the M.S. and Ph.D. degrees in electrical engineering from the Royal Institute of Technology, Sweden, in 2007 and 2011, respectively.

He is a Senior Research Engineer at the IT Convergence Technology Research Laboratory, Electronics and Telecommunications Research Institute, Korea. He has held a postdoctoral research position in Electrical Engineering and Computer Science from the University of California, Berkeley (2011–2013).

Dr. Park received the best paper award at the IEEE International Conference on Mobile Ad-hoc and Sensor System of 2009. His research interests include embedded systems, wireless sensor and actuator networks, air traffic surveillance networks, and cyber-physical systems.

Harshad Khadilkar received the Bachelor's degree from IIT Bombay, Bombay, India, in 2009 and the Master's degree and the Ph.D. degree from MIT, Cambridge, in 2013.

He currently works with IBM's India Research Lab. His research interests lie in the field of modeling and control of large-scale networks such as transportation and energy.

Hamsa Balakrishnan received a B.Tech in Aerospace Engineering from the Indian Institute of Technology, Madras in 2000 and a Ph.D. in Aeronautics and Astronautics from Stanford University in 2006.

She is an Associate Professor of Aeronautics and Astronautics at the Massachusetts Institute of Technology. Between May and December 2006, she was a Researcher at the University of California, Santa Cruz, and the NASA Ames Research Center. Her research interests address various aspects of air transportation systems, including algorithms for air traffic scheduling and routing, integrating weather forecasts into air traffic management and minimizing aviation-related emissions; air traffic surveillance algorithms; and mechanisms for the allocation of airport and airspace resources.

Dr. Balakrishnan was a recipient of the NSF CAREER Award in 2008, the Kevin Corker Award for Best Paper of ATM-2011, and the AIAA Lawrence Sperry Award in 2012.

Claire J. Tomlin received the B.A.Sc. degree in electrical engineering from the University of Waterloo, Canada, in 1992, the M.Sc. degree in electrical engineering from Imperial College, University of London, in 1993, and the Ph.D. degree in electrical engineering from the University of California, Berkeley, in 1998.

She is a Professor of Electrical Engineering and Computer Sciences at Berkeley, where she holds the Charles A. Desoer in Engineering. She held the positions of Assistant, Associate, and Full Professor at Stanford from 1998–2007, and in 2005 joined Berkeley. She has been an Affiliate at LBL in the Life Sciences Division since January 2012. She works in hybrid systems and control, with applications to biology, robotics, and air traffic systems.

Dr. Tomlin received the Erlander Professorship of the Swedish Research Council in 2010, a MacArthur Fellowship in 2006, and the Eckman Award of the American Automatic Control Council in 2003.