Air Traffic Management Security: ADS-B as an Example

Dr. Thabet Kacem

Email: thabet.kacem@udc.edu

UNIVERSITY OF THE DISTRICT OF COLUMBIA 1851

IARIA

Dr. Thabet Kacem

Education:

- January 2010: Master in Computer Science, University of the District of Columbia
- May 2016: PhD in Information Technology, George Mason University

Appointments:

- 2016-2022: Tenure-track assistant professor of Computer Science at the University of the District of Columbia
- 2022-Present: Tenured associate professor of Computer Science at University of the District of Columbia
- 2022-Present: Affiliate Faculty at the C4I Center at George Mason University

Outline

- Research Interests & Vision
- Air Traffic Management Overview
- ADS-B Security Problem
- Related Work
- ADS-Bsec Framework
- Evaluation Results
- Conclusion and Future Challenges

Outline

- Research Interests & Vision
- Air Traffic Management Overview
- ADS-B Security Problem
- Related Work
- ADS-Bsec Framework
- Evaluation Results
- Conclusion and Future Challenges

Research Interests & Vision

Intelligent Transportation Systems

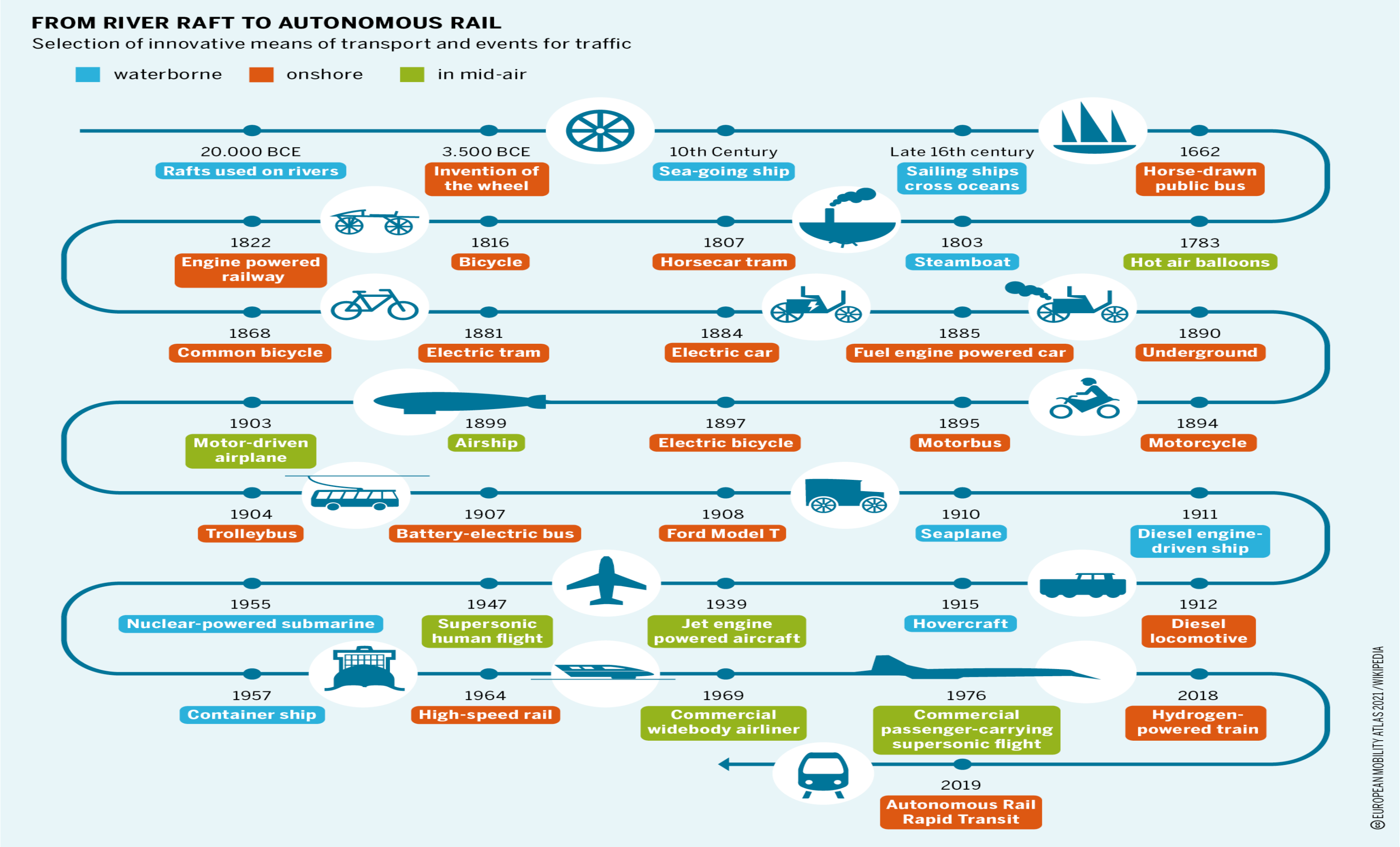
CPS & Critical Infrastructure

Cyber Security

Smart Cities

Blockchains

Research Vision



Cont'd

"Intelligent Transportation Systems (ITS) apply a variety of technologies to monitor, evaluate, and manage transportation systems to enhance efficiency and safety", US DOT

<u>Main Benefits of ITS:</u>

- Safety
- Better Management
- Efficiency
- Cost Effectiveness

Cont'd

- Concerns:

Cyber Security

Environmental Risks

Supply Chain Resiliency

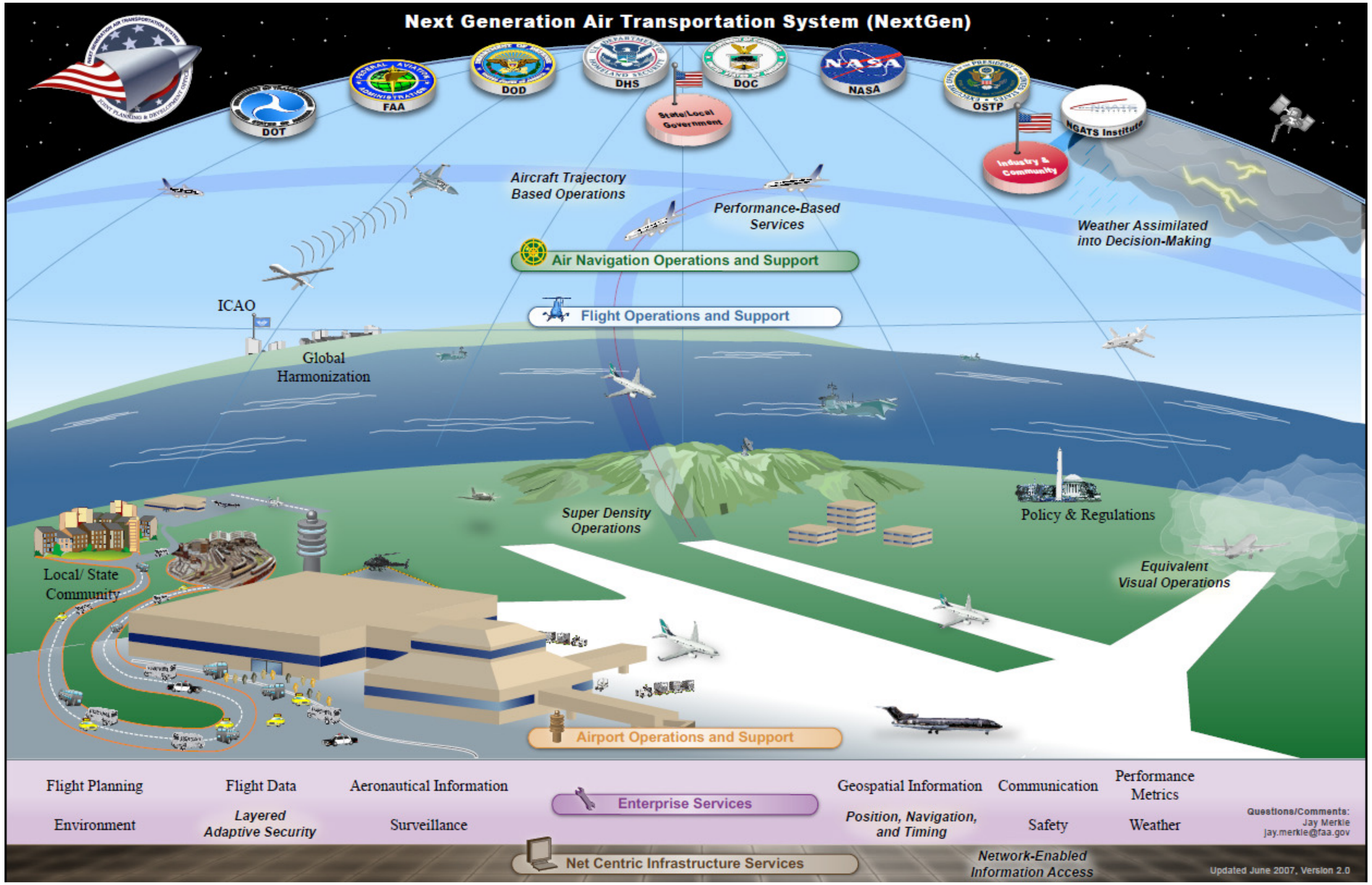
- Research Vision: How can we address the security concerns of ITSs so that they live up to their full potential of revolutionizing the human life quality?

Outline

- Research Interests & Vision
- Air Traffic Management Overview
- ADS-B Security Problem
- Related Work
- ADS-Bsec Framework
- Evaluation Results
- Conclusion and Future Challenges

Air Traffic Management Overview

Cont'd –NextGen Project



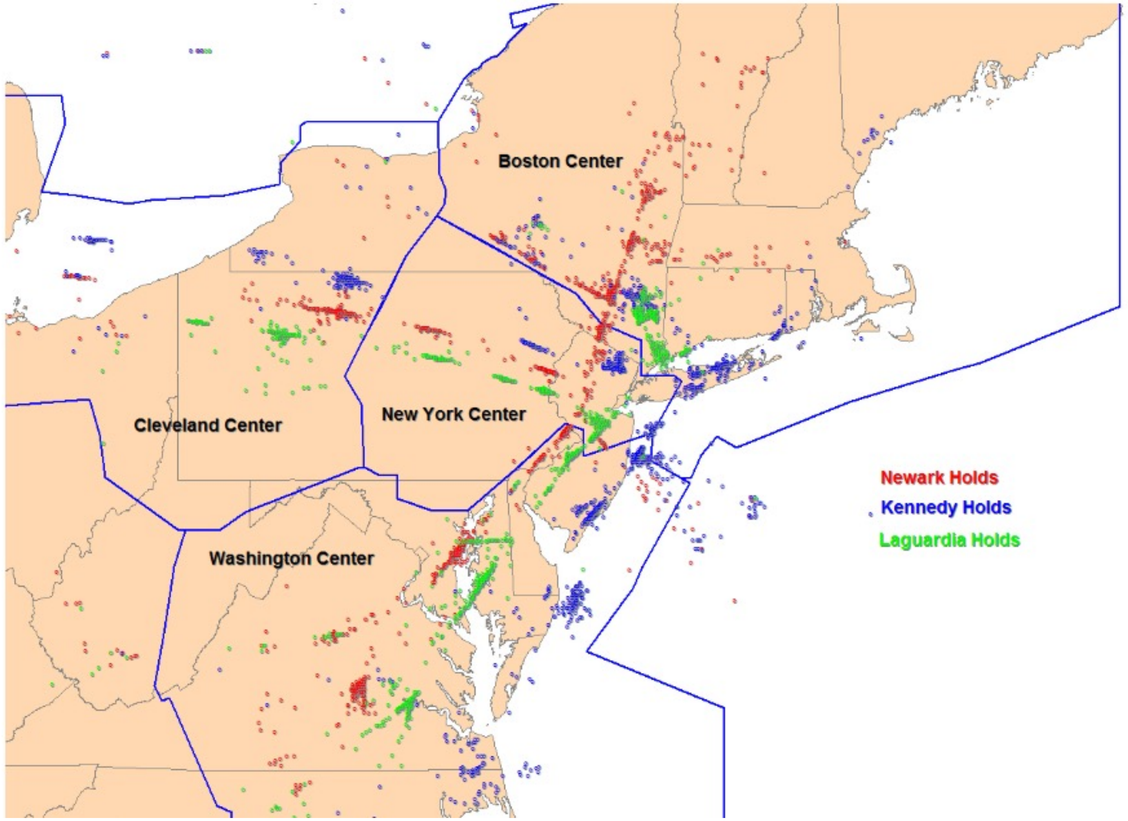
Outline

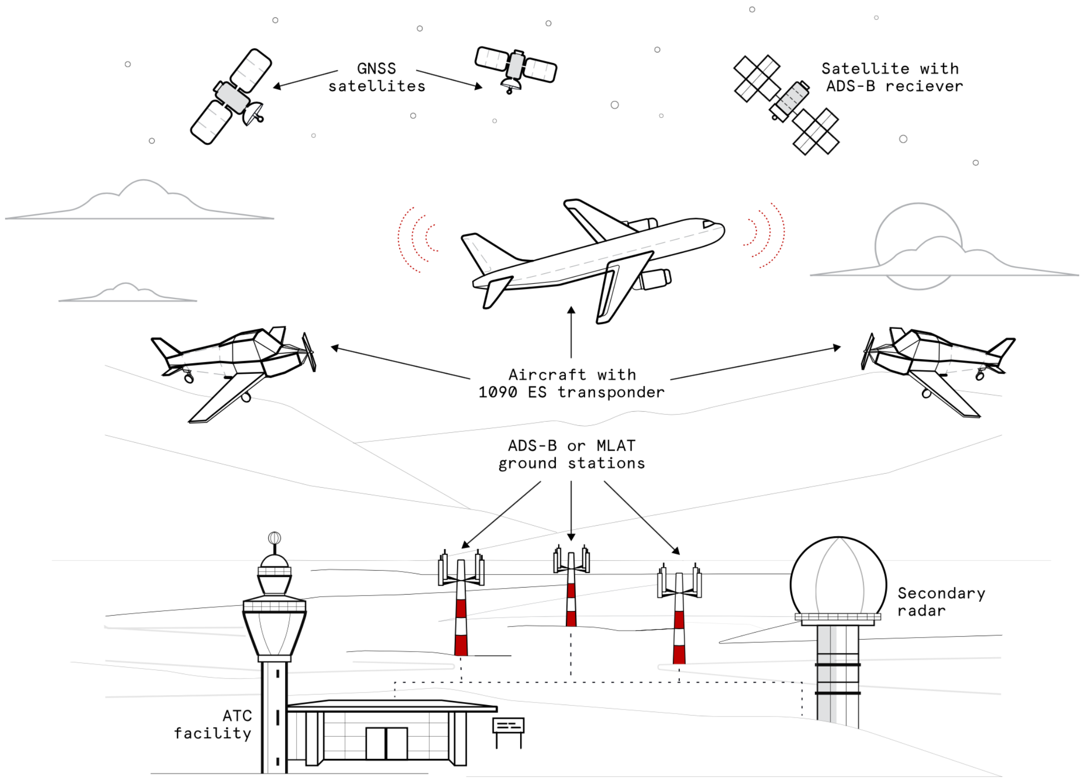
- Research Interests & Vision
- Air Traffic Management Overview
- ADS-B Security Problem
- Related Work
- ADS-Bsec Framework
- Evaluation Results
- Conclusion and Future Challenges

ADS-B Security Problem

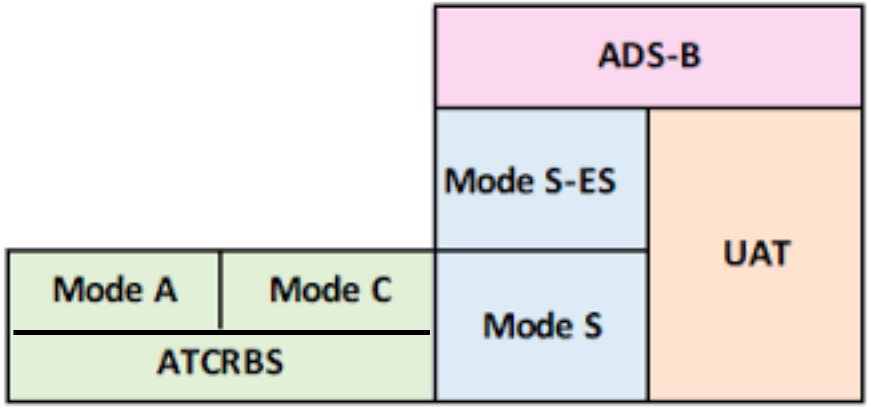
Traditional Surveillance Technologies	ADS-B advantages
• Primary Surveillance Radar (PSR) • Secondary Surveillance Radar (SSR)	• Better Accuracy • Capability to be deployed in remote areas • Less operational & maintenance Costs

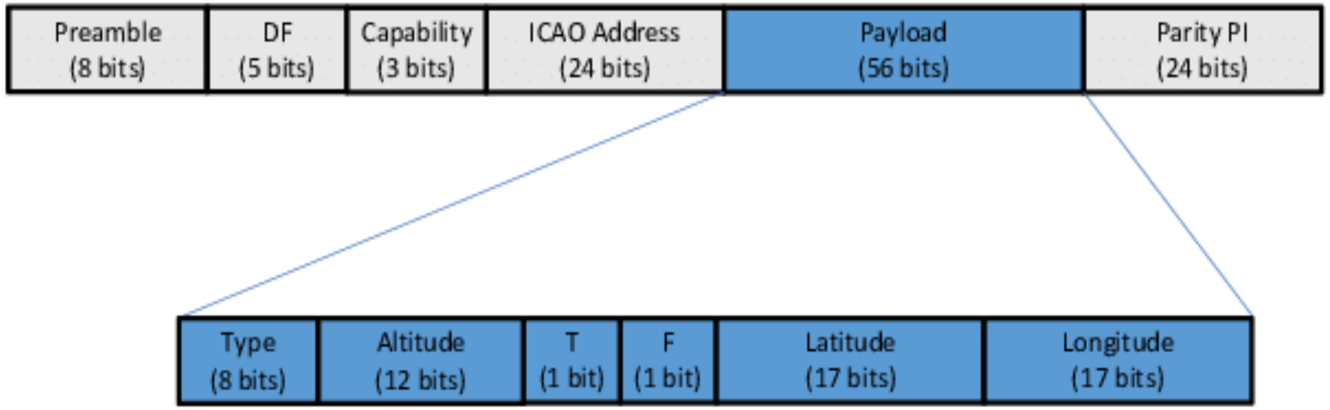
Cont'd – How ADS-B Works





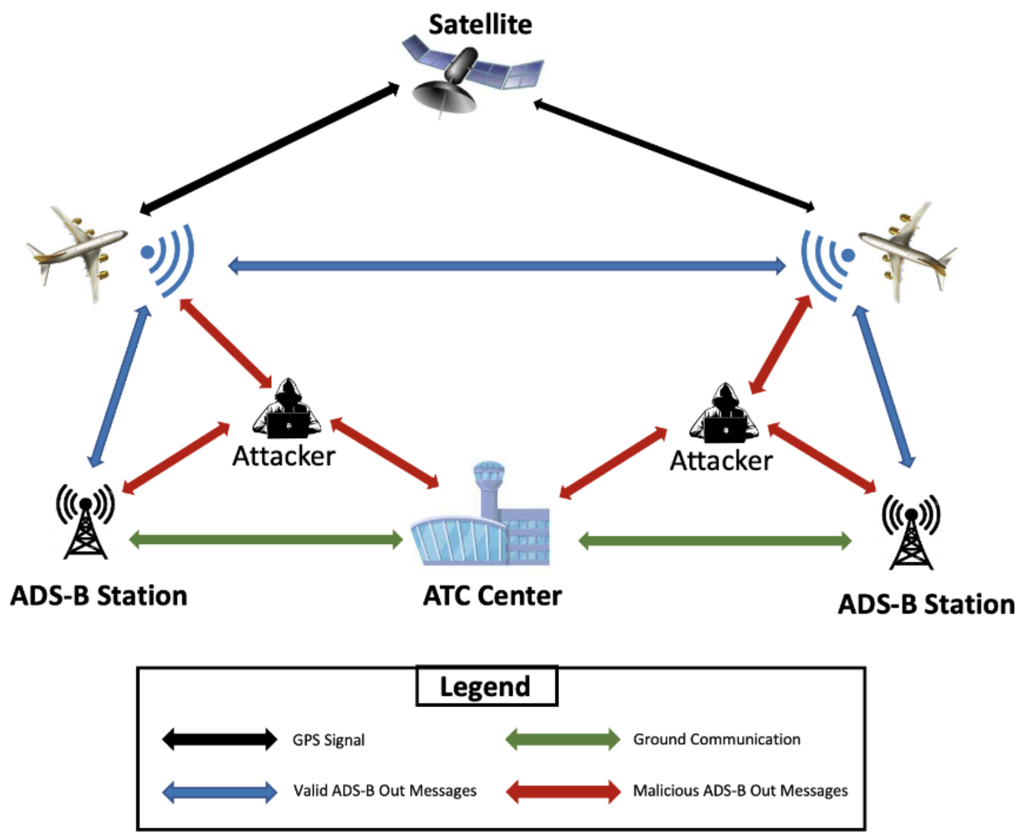
Cont'd – ADS-B Message Format





Cont'd – ADS-B Threat Model

- Types of Attacks:
  - Eavesdropping
  - GPS Spoofing
  - Jamming
  - Replay Attacks
  - Ghost Aircraft Injection
  - Multiple Ghost Aircraft Injection



Outline

- Research Interests & Vision
- Air Traffic Management Overview
- ADS-B Security Problem
- Related Work
- ADS-Bsec Framework
- Evaluation Results
- Conclusion and Future Challenges

Related Work

Cryptographic Approaches

- Rationale: Add digital signature data in extra ADS-B messages
    - Pan et al
    - Yang et al
- Weakness: not scalable and may increase error rate, and may require changing the message format

Artificial Intelligence Approaches

- Rationale: Use machine learning and/or deep learning classifiers
    - Ying et al
    - Habler and Shabtai
- Weakness: these approaches are not preventive, not much insight on the type of the attacks

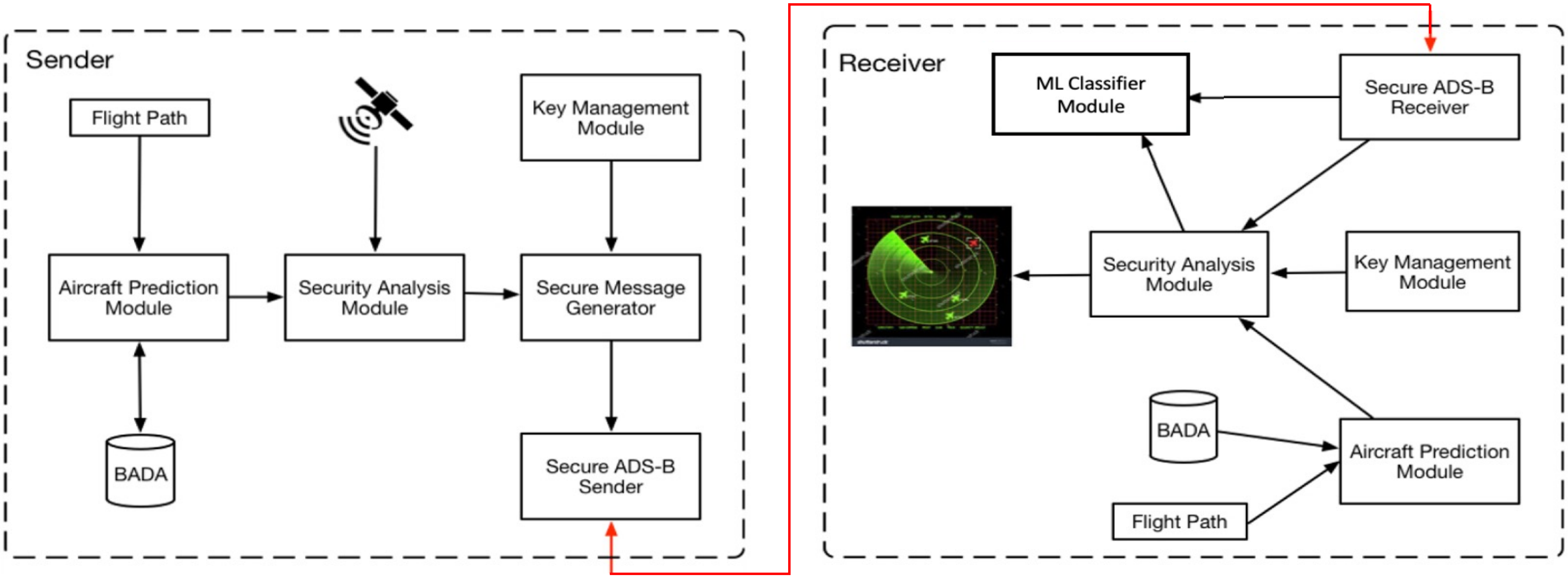
Location Verification Approaches

- Rationale: Use the time difference of arrivals from nearby aircraft
    - Strohmeier et al
    - Kaune et al
- Weakness: requires several multilateration stations, no message attribution

Outline

- Research Interests & Vision
- Air Traffic Management Overview
- ADS-B Security Problem
- Related Work
- ADS-Bsec Framework
- Evaluation Results
- Conclusion and Future Challenges

ADS-Bsec Framework –Overview



ADS-Bsec – Secure Message Generator

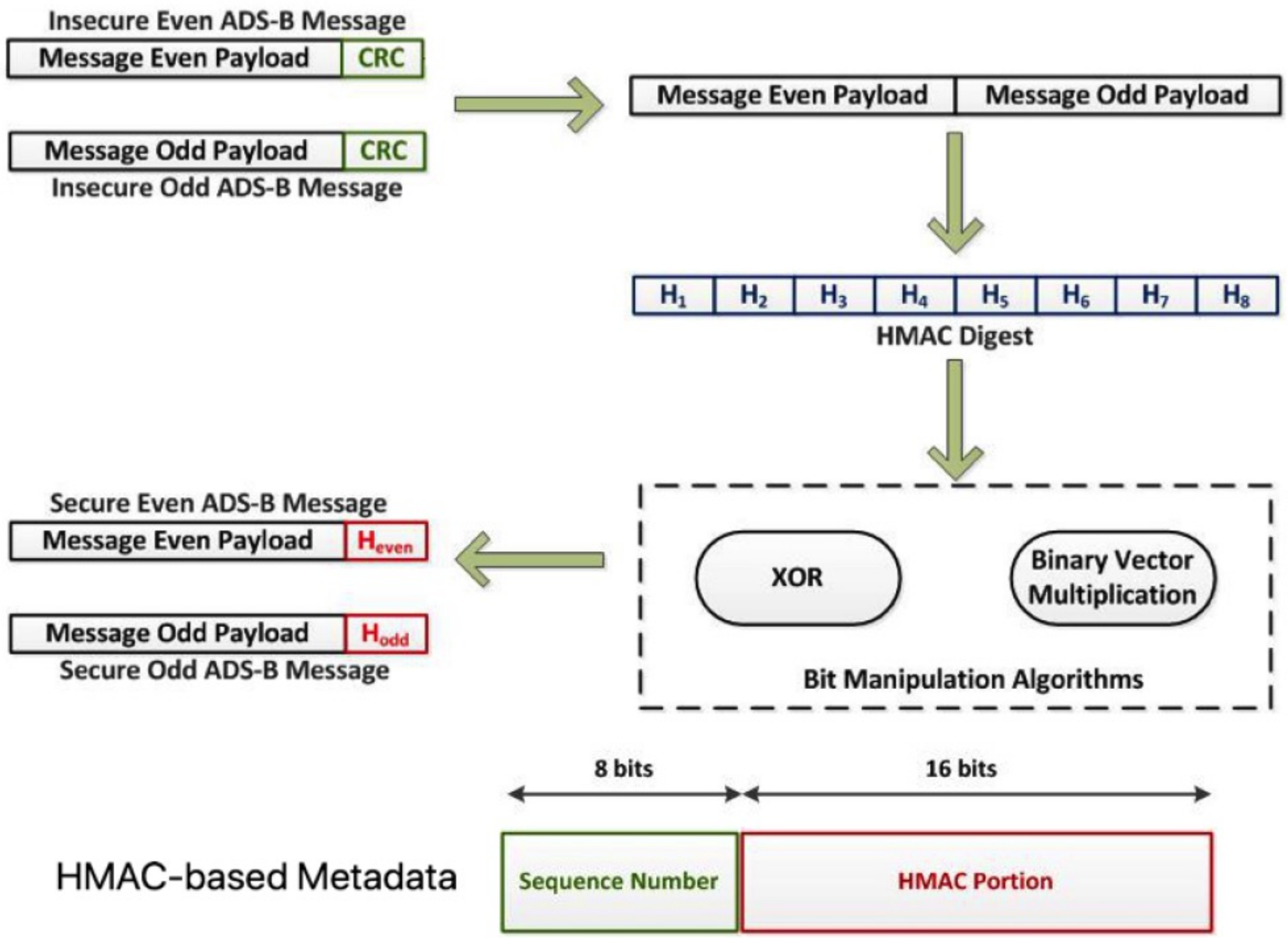
Rationale: Replace the Cycle Redundancy Check (CRC) field with a security metadata based on Keyed Hash Message Authenticated Code (HMAC)

- This is a software change that does not require any hardware change
- There is no need for an ADS-B message format modification
- The power of the HMAC lies mainly in the length of the key
- No need for sending extra data that harm the scalability of the approach

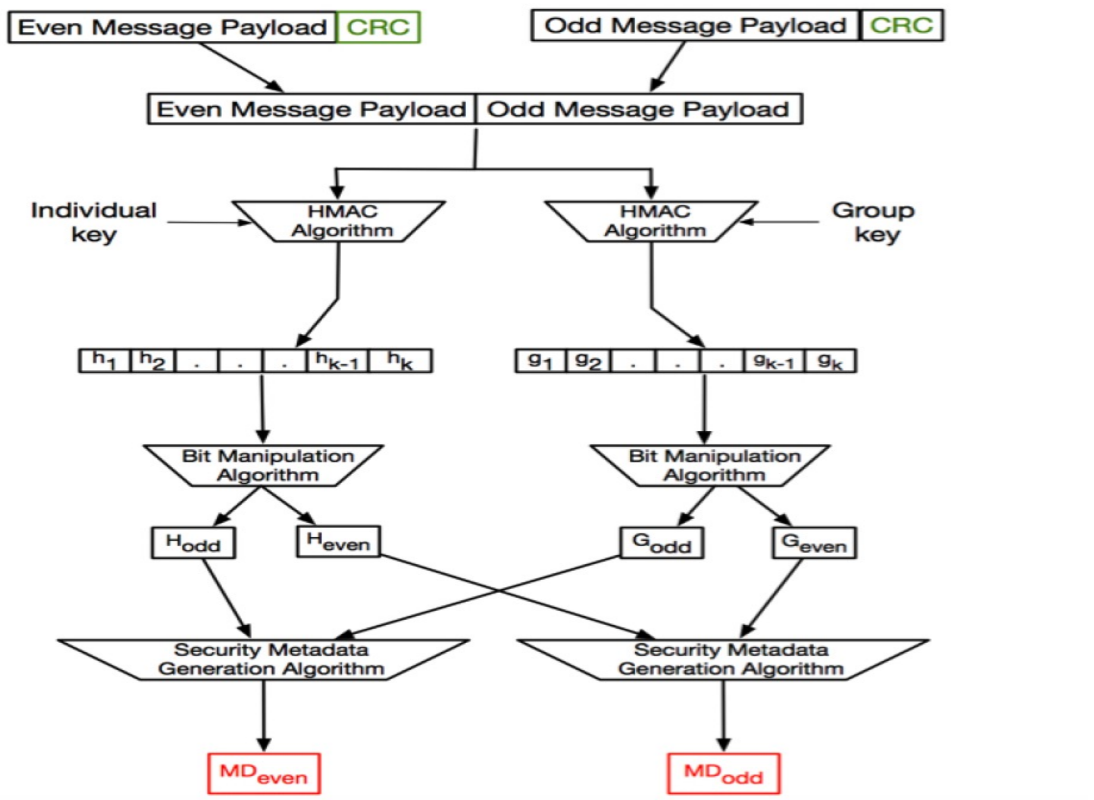
Two variants of the secure message generator:

- Version 1: ADS-B Out only
- Version 2: Both ADS-B Out and ADS-B In

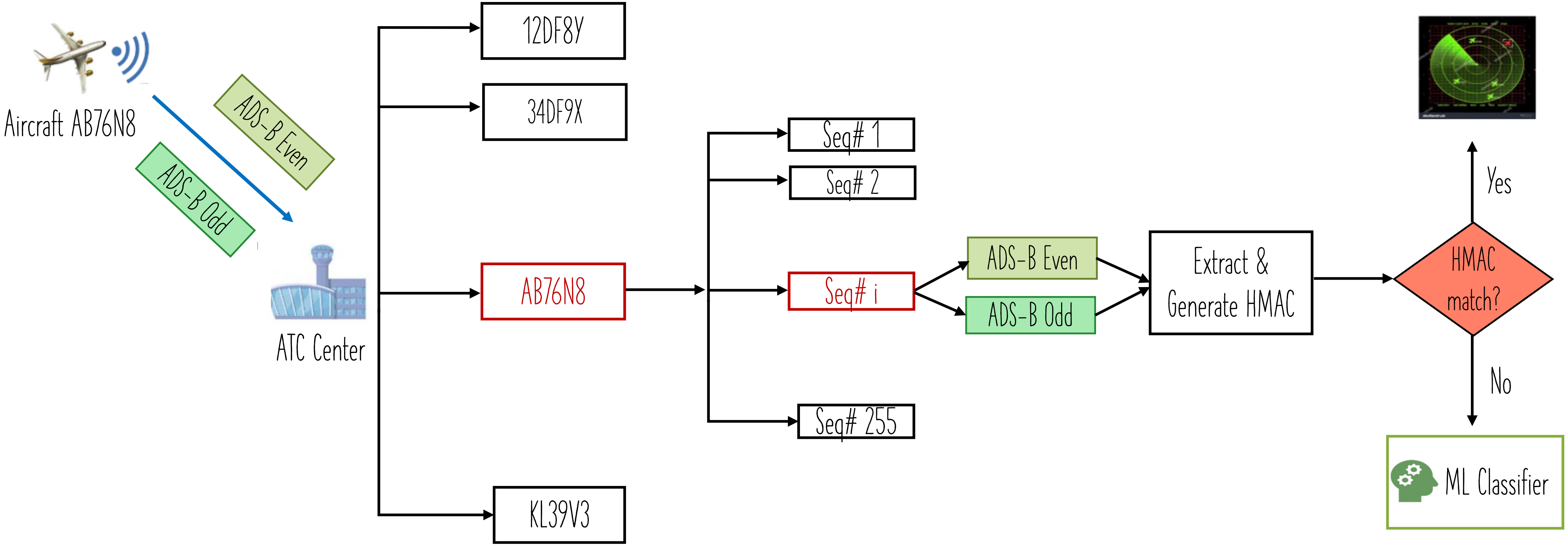
Cont'd – Version 1



Cont'd – Version 2



ADS-Bsec – Security Analysis Module



ADS-Bsec – Key Management Module

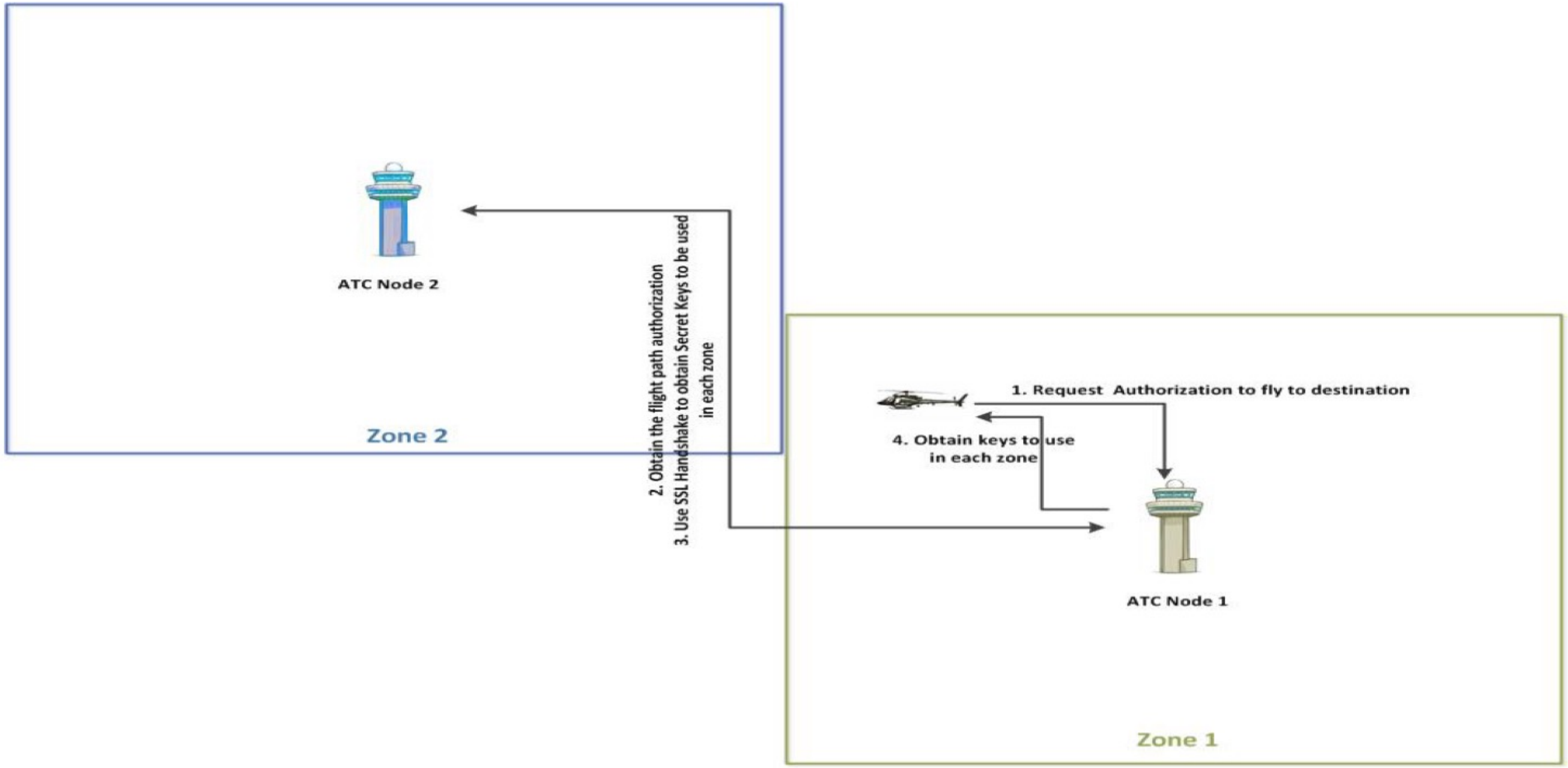
Rationale:

- PKI schemes are difficult to deploy to share ADS-B keys mainly due to trust issues
- Symmetric keys are more adequate
- Delegate the initial key distribution to the ATC Center of departure

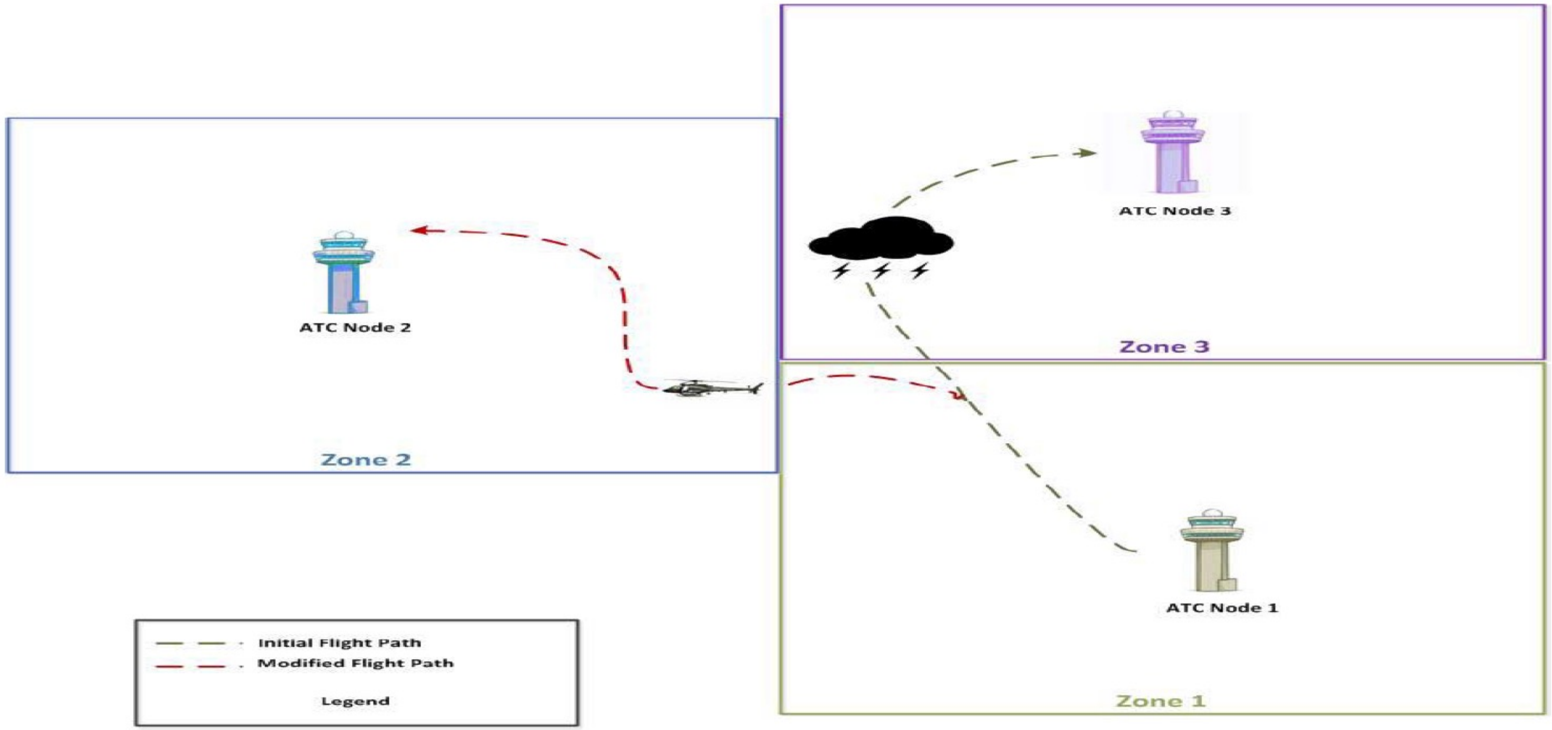
Key Exchange Constraints:

- Ideal flight conditions
- Unforeseen flight changes
- ADS-B Out vs ADS-B In and ADS-B Out

Cont'd – Ideal Flight Conditions



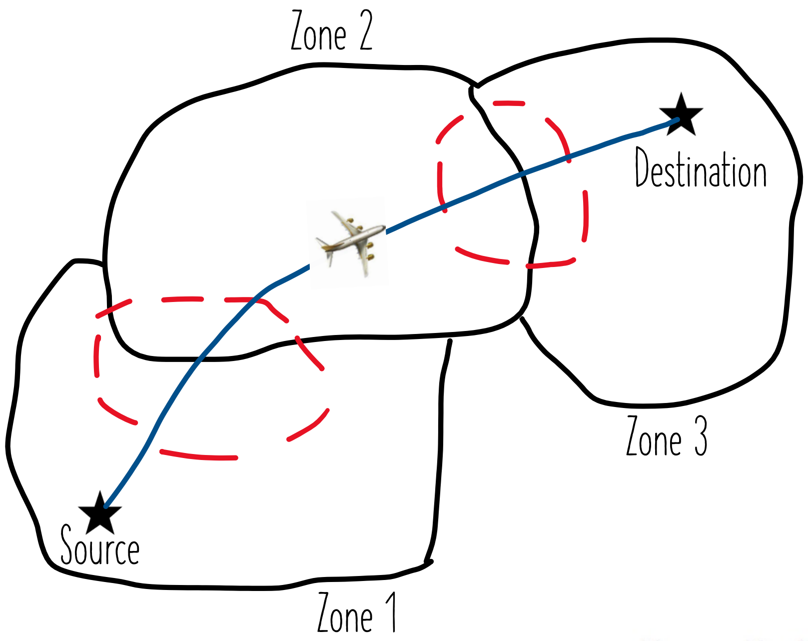
Cont'd – Unforeseen Flight Changes



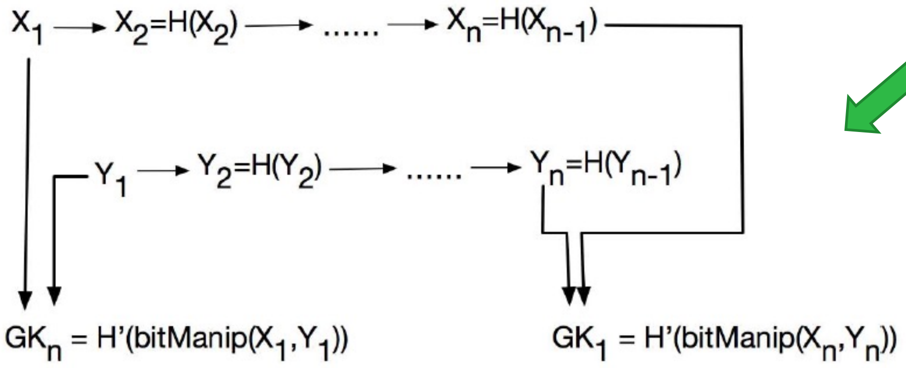
Cont'd – Key Exchange for ADS-B In and ADS-B Out

- Rationale:
  - Nearby aircraft, equipped with ADS-B In, receive ADS-B messages from each other
  - All aircraft in a given zone generate their security metadata using a group key that is generated from seed keys
- The granularity of the groups are inspired from the airspace subdivision by the authorities (e.g. Flight Information Regions)
- Group keys need to be updated every time a member joins or leaves the group
- Each day is subdivided into time intervals depending on the frequency of aircraft in that zone
  - Seeds are generated in μTesla-like fashion

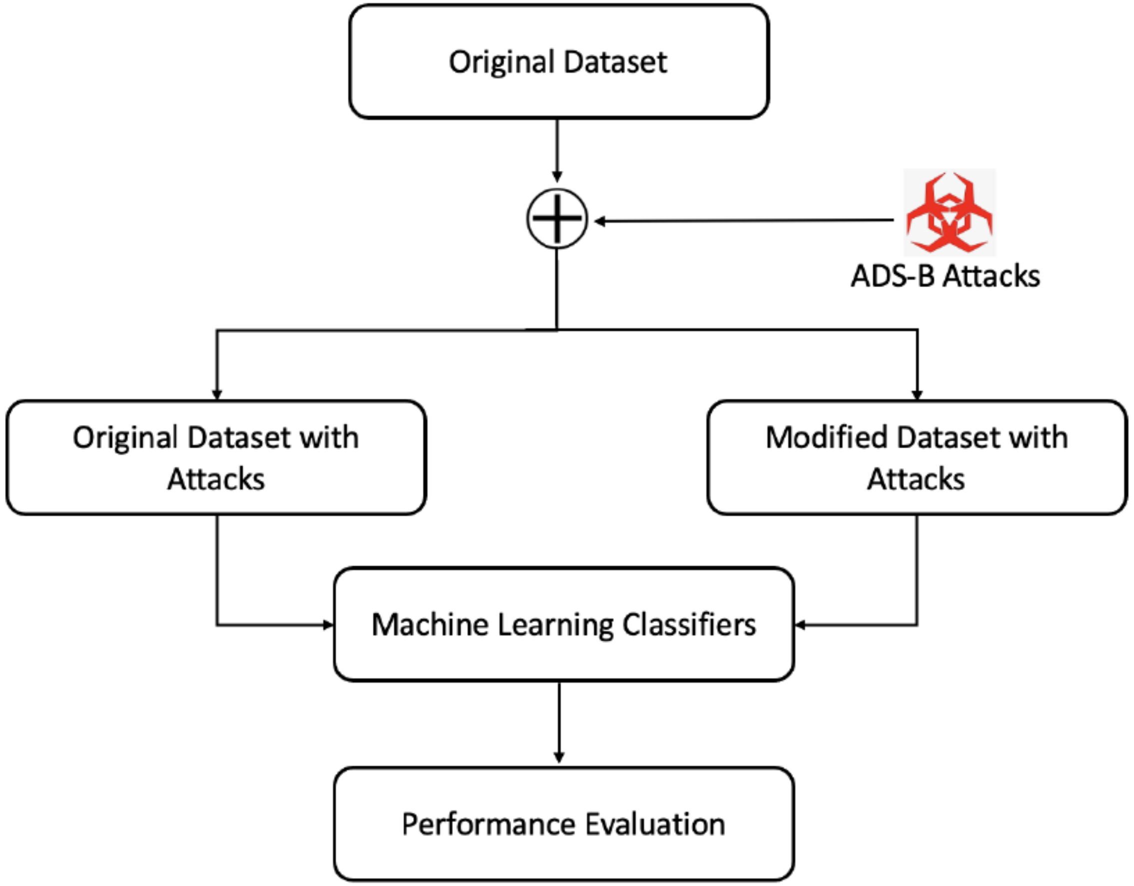
Cont'd



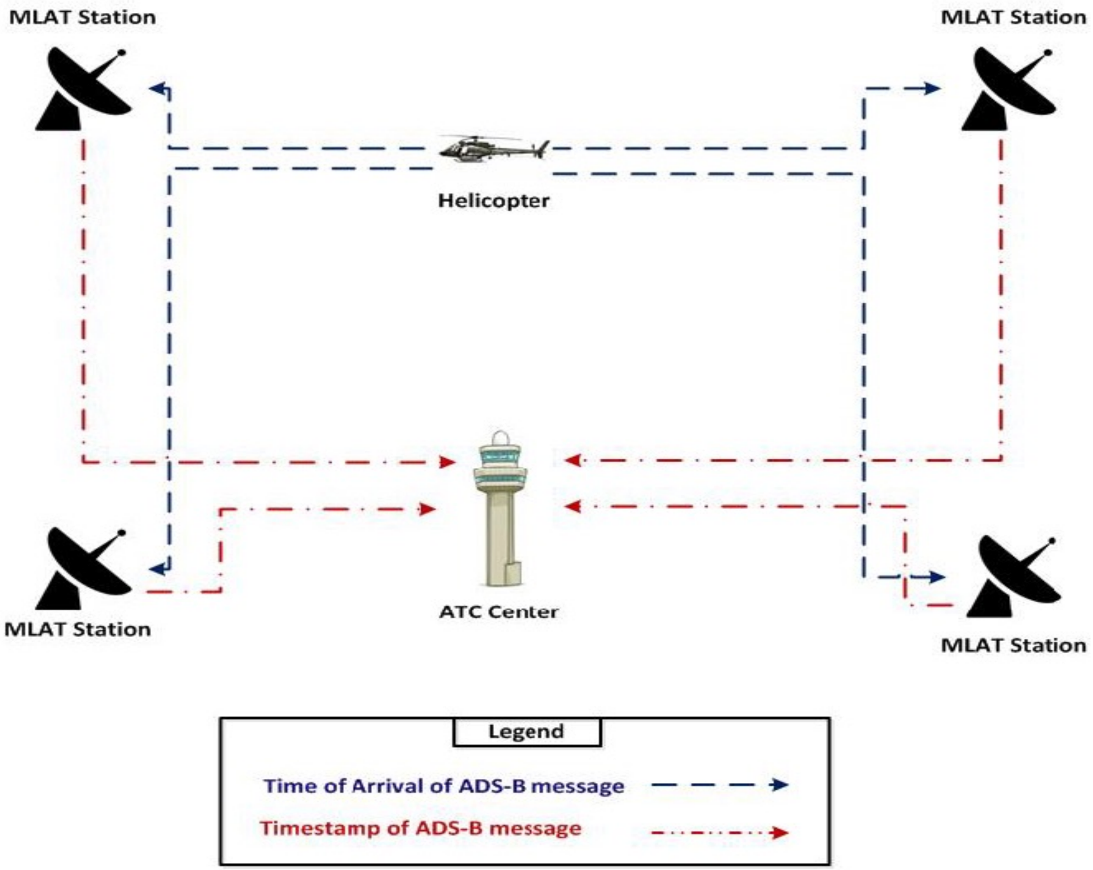
	Zone 1	Zone 2	Zone 3
Zone 1	a_{11}	a_{12}	a_{13}
Zone 2	a_{21}	a_{22}	a_{23}
Zone 3	a_{31}	a_{32}	a_{33}



ADS-Bsec – ML Classifier



ADS-Bsec – Radio-Location Module



Cont'd – Computing the TODT

$$\tau_n = t_n + p_n$$

$$t_n = \frac{\sqrt{(x_n - x_E)^2 + (y_n - y_E)^2 + (z_n - z_E)^2}}{C}$$

$$\tau_i - \tau_j = (t_i - t_j) + (p_i - p_j)$$

$$\tau_i - \tau_j = t_i - t_j + \mathcal{N}(0, 2\sigma^2)$$

Cont'd – Detecting bogus ADS-B Messages

Algorithm: Detection of Bogus ADS-B Messages

Initialize arrays to store the Cartesian coordinates of both the MLAT sensors and the emitters;

while t <*endTime* **do**

- Store the coordinates of each emitter in its corresponding array;
- Run the multilateration algorithm to determine the location of the emitter based on the collected TDOT values;
- Apply Kalman Filter to improve the location estimation;
- Compute the horizontal difference h_{Diff} between the estimated and reported position;
- **if** $h_{Diff} < Threshold$ **then**
  - ADS-B message is valid
- **else**
  - ADS-B message is malicious

Outline

- Research Interests & Vision
- Air Traffic Management Overview
- ADS-B Security Problem
- Related Work
- ADS-Bsec Framework
- Evaluation Results
- Conclusion and Future Challenges

Evaluation Results

Crypto Module

- Measure the sending time and receiving time of secure ADS-B messages
- Compare the overhead of the added security vs the original protocol
- Study the effect of the implementation of the Key Management Module

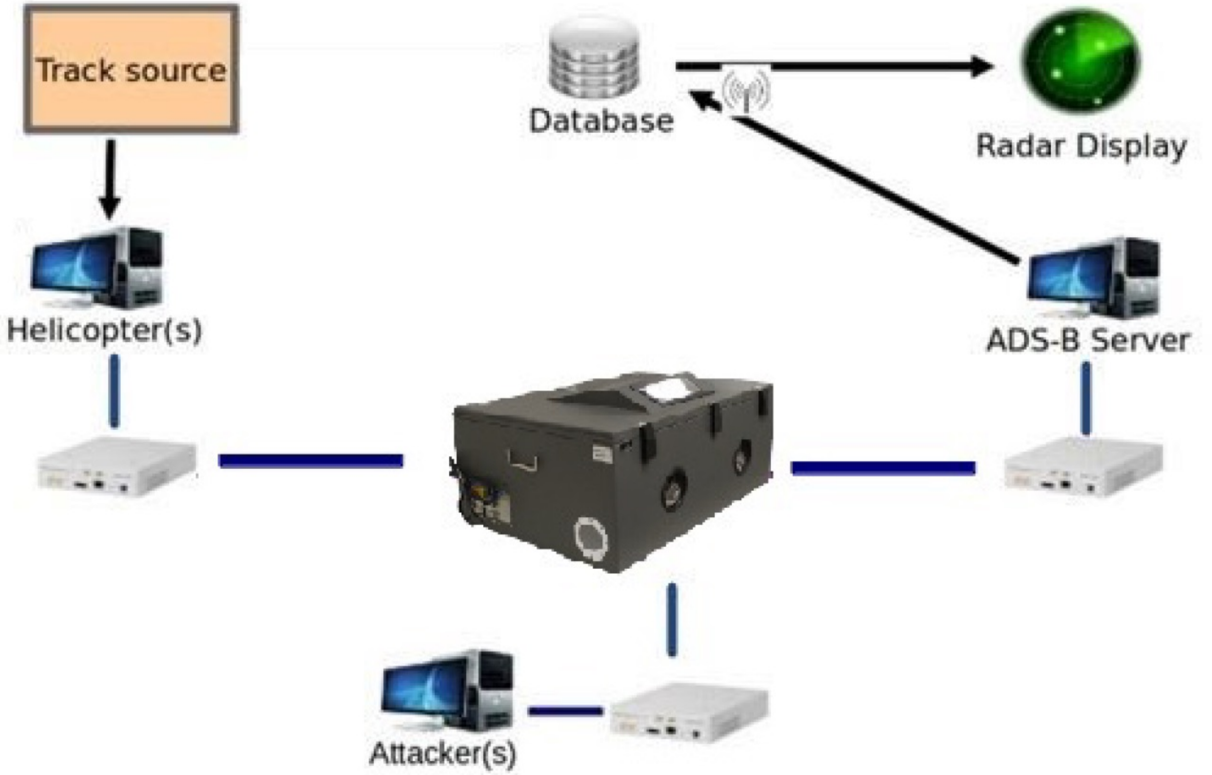
AI Module

- Measure the classification accuracy, sensitivity and specificity of the ML classifier
- Compare the classification scores of the original vs modified datasets

Location Verification

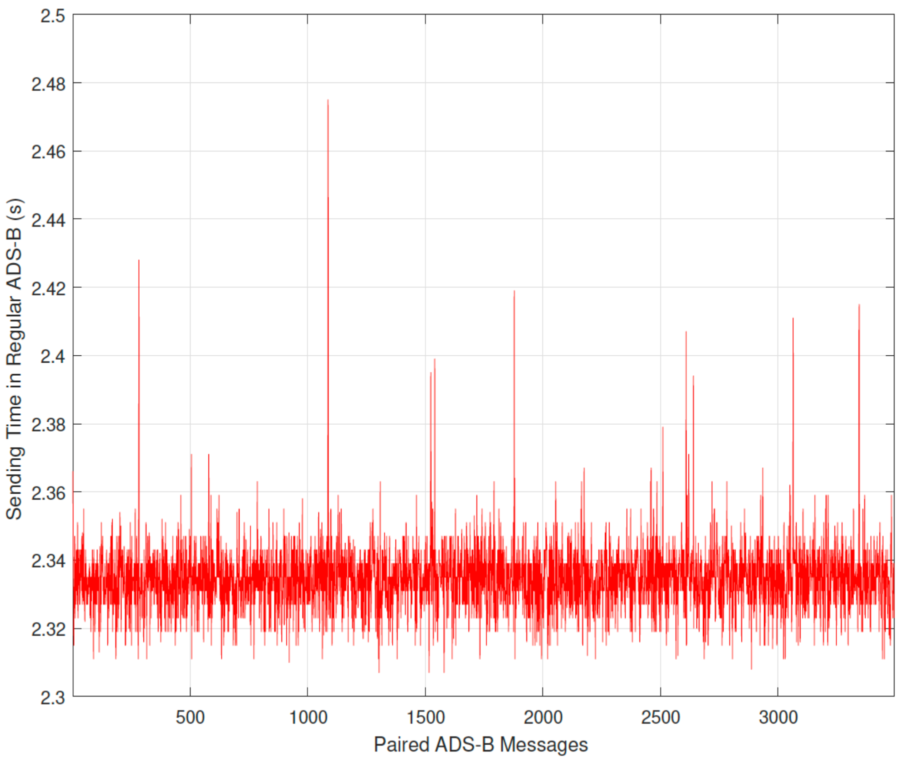
- Comparing TDOT vs TDOA
- Location estimation using TDOT
- Detecting malicious ADS-B messages

Cont'd – Crypto-Module Evaluation

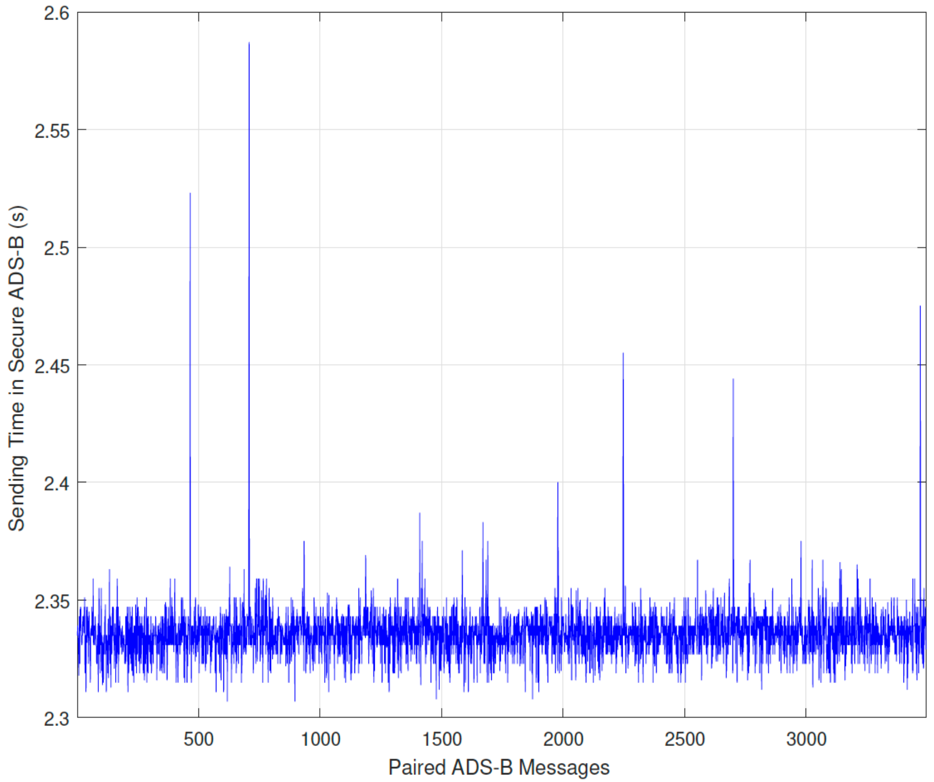


The ADS-Bsec Test Bed

Cont'd – Sending Time

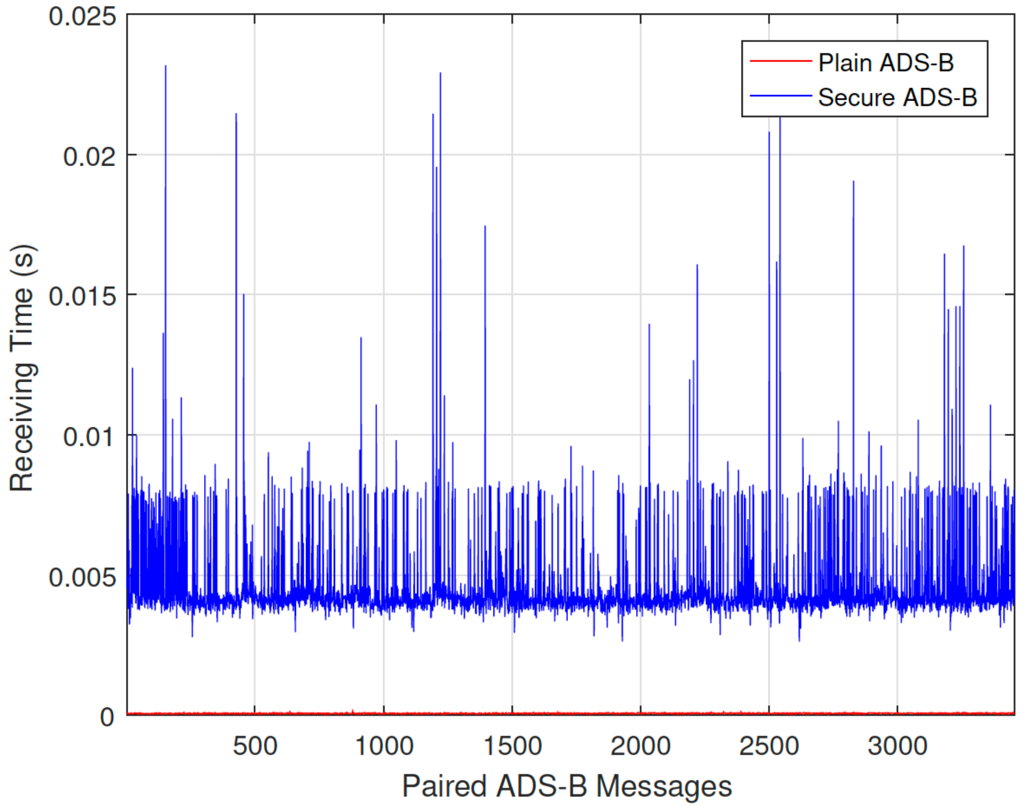


Sending Time Plain ADS-B



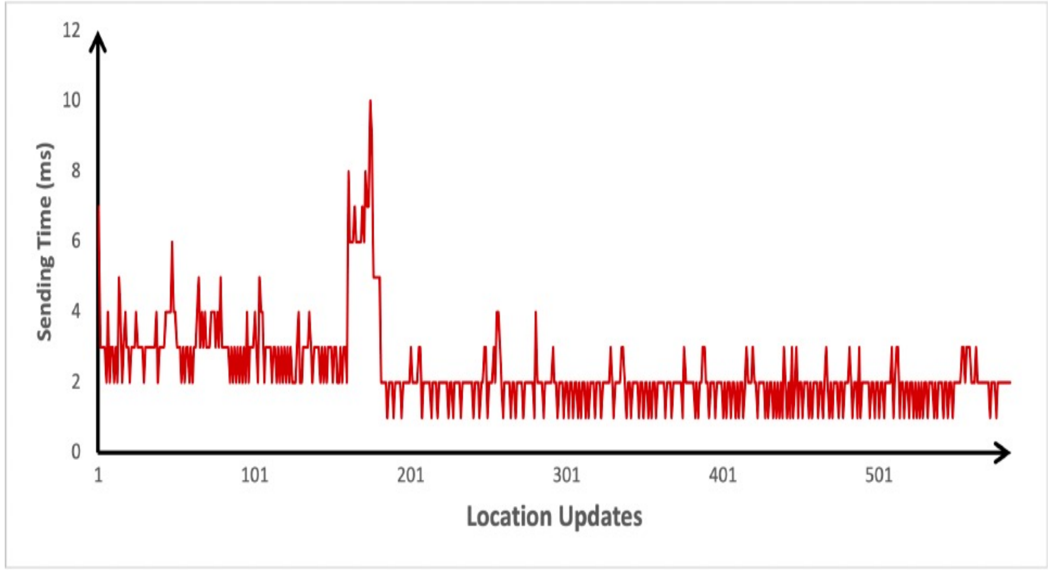
Sending Time Secure ADS-B

Cont'd – Receiving Time

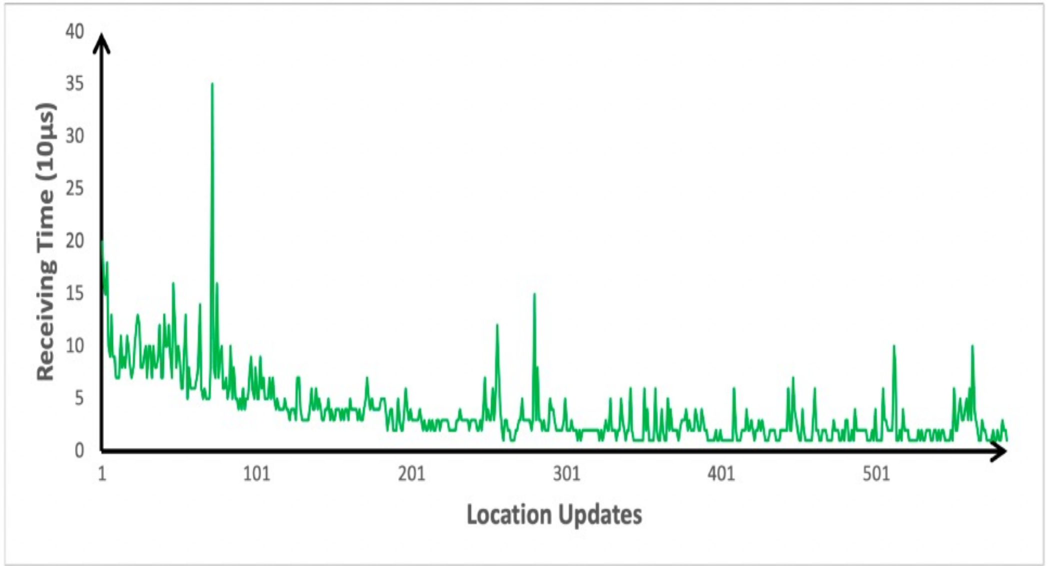


Cont'd – Key Management

Cont'd



Sending Time with SHA1 and 128-bit key



Receiving Time with SHA1 and 128-bit key

Cont'd – AI Module Evaluation

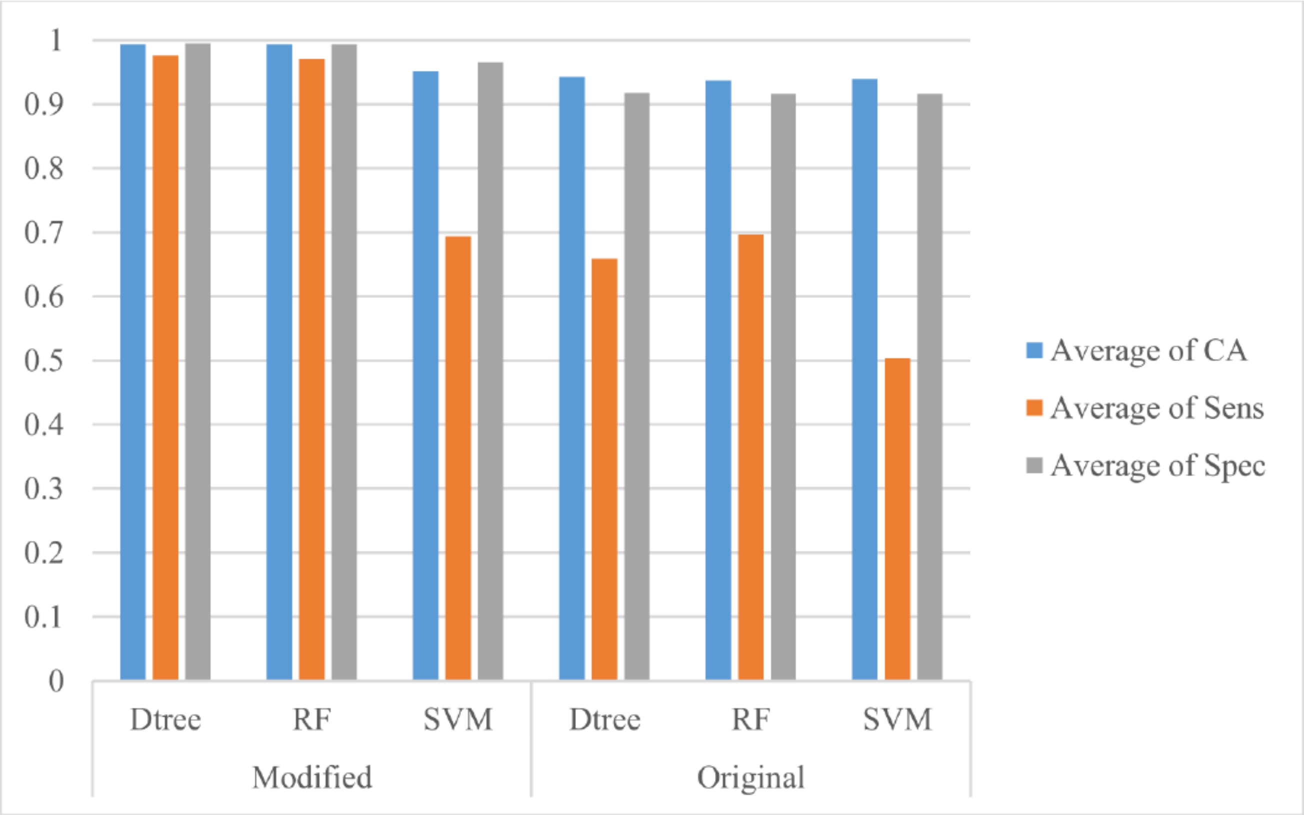
CLASSIFICATION RESULTS WITH ORIGINAL DATASET.

Percentage	Classifier	CA	Sens	Spec
95-05	Dtree	0.96	0.69	0.92
95-05	SVM	0.97	0.51	0.92
95-05	RF	0.97	0.71	0.92
90-10	Dtree	0.95	0.68	0.92
90-10	SVM	0.94	0.49	0.92
90-10	RF	0.94	0.70	0.92
85-15	Dtree	0.92	0.61	0.92
85-15	SVM	0.91	0.50	0.91
85-15	RF	0.90	0.69	0.91

CLASSIFICATION RESULTS WITH MODIFIED DATASET.

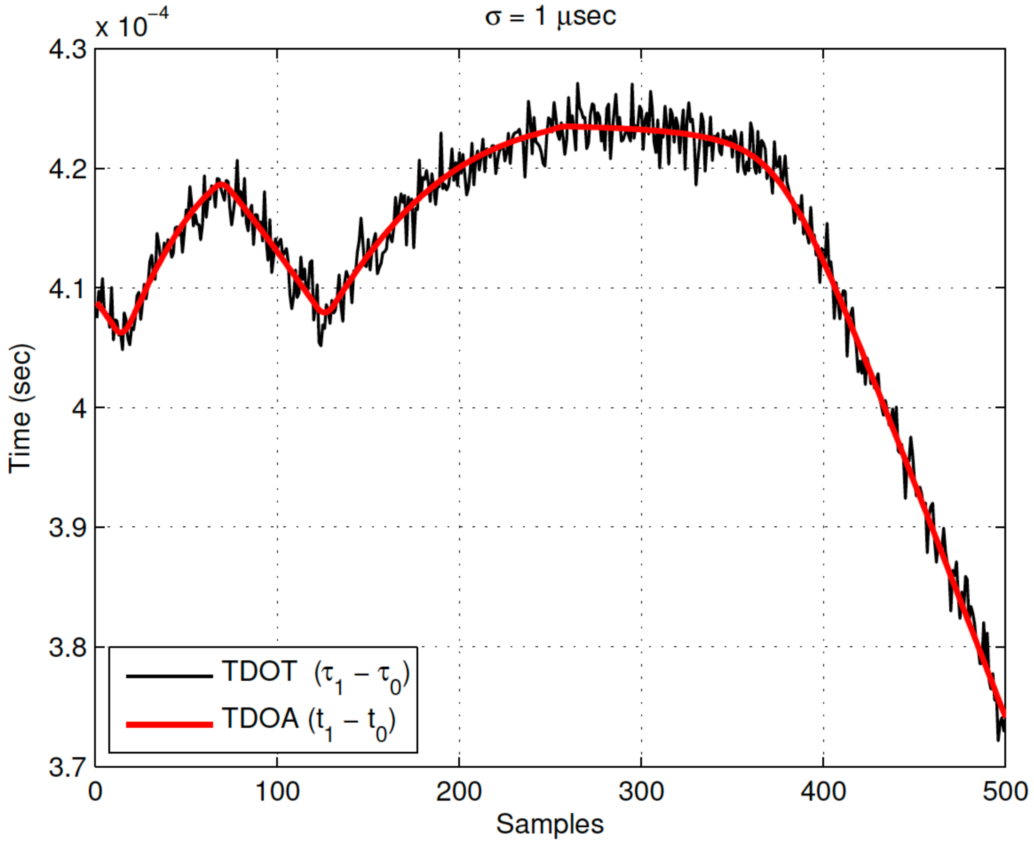
Percentage	Classifier	CA	Sens	Spec
95-05	Dtree	0.99	0.97	0.99
95-05	SVM	0.94	0.69	0.97
95-05	RF	0.99	0.97	0.99
90-10	Dtree	1.00	0.98	1.00
90-10	SVM	0.96	0.71	0.96
90-10	RF	0.99	0.97	0.99
85-15	Dtree	0.99	0.97	0.99
85-15	SVM	0.94	0.69	0.97
85-15	RF	0.99	0.97	0.99

Cont'd

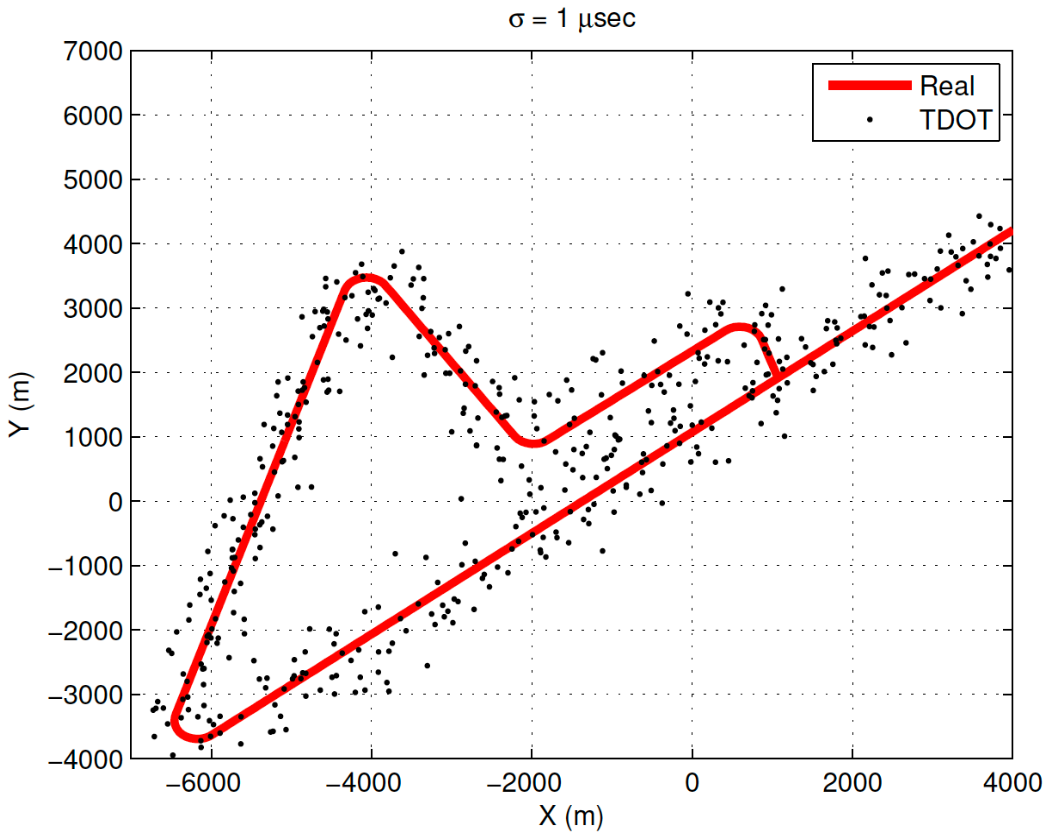


Average Classification Score: Original dataset vs Modified dataset

Cont'd – Radio Location Module Evaluation

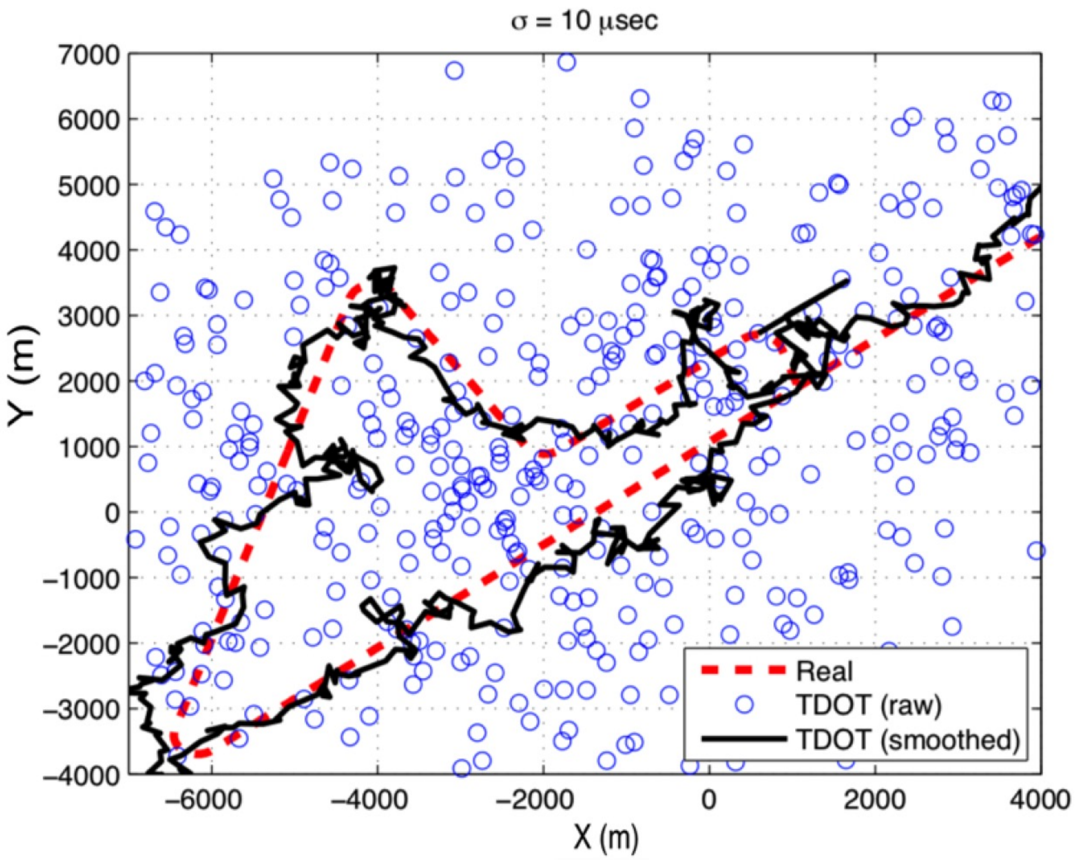


TDOA vs TDOT

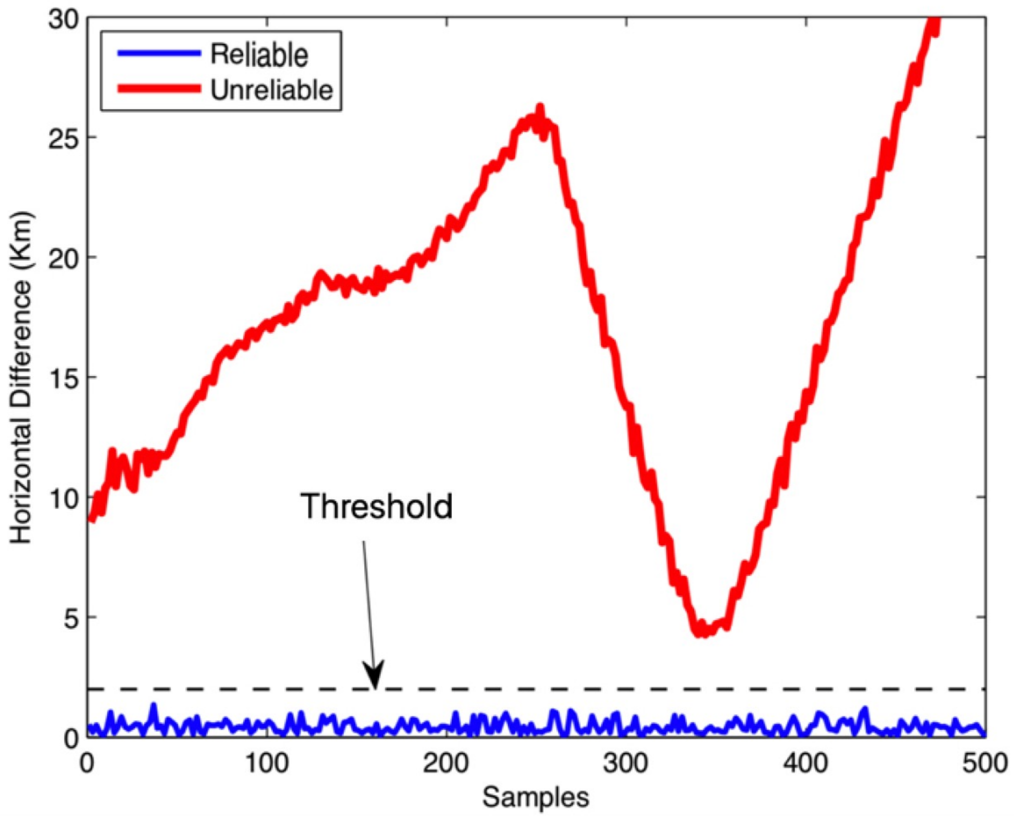


Location Estimation using TDOT

Cont'd



Effect of Kalman Filter on Location Estimation



Detecting Malicious ADS-B Messages

Outline

- Research Interests & Vision
- Air Traffic Management Overview
- ADS-B Security Problem
- Related Work
- ADS-Bsec Framework
- Evaluation Results
- Conclusion and Future Challenges

Conclusion

ADS-Bsec framework addresses the security problems of ADS-B from a holistic approach without altering the packet format or requiring new equipment

It combines novels cryptographic, artificial intelligence and location verification techniques to provide the integrity and authenticity of the ADS-B messages

The findings are supported by a set of experiments that assess the performance of the key modules of ADS-Bsec

Achievements

Patents

1. ADS-Bsec: A Holistic Framework to Secure ADS-B. US Patent Number 11/022/696.

Selected Conference Publications

1. **Thabet Kacem**, Alexandre Barreto, Duminda Wijesekra and Paulo Costa, "A Key Management Module for Secure ADS-B", 2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC 2022), Macau, China, September 2022.
2. **Thabet Kacem**, Aydin Kaya, Ali Seydi Keceli, Cagatay Catal, Duminda Wijesekera and Pualo Costa, "ADS-B Attack Classification Using Machine Learning Techniques", 2021 IEEE Intelligent Vehicle Symposium (IV21), Workshop on Security Challenges in Intelligent Transportation Systems (SCITS) Workshop, Nagoya, Japan, September 2021.
3. **Thabet Kacem**, Alexandre Barreto Duminda Wijesekera, and Paulo Costa."Extending ADS-B for Mixed Urban Air Traffic". 37th AIAA/IEEE Digital Avionics Systems Conference (DASC 2018), London, UK, October 2018.
4. **Thabet Kacem**, Duminda Wijesekera and Paulo Costa, "Key Distribution Scheme for Aircraft Equipped with Secure ADS-B IN", 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC 2017), Yokohama, Japan, October 2017.
5. **Thabet Kacem**, Duminda Wijesekera, Paulo Costa and Alexandre Barreto, "Secure ADS-B Framework 'ADS-Bsec'", 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC 2016), Rio de Janeiro, Brazil, November 2016.
6. **Thabet Kacem**, Duminda Wijesekera, Paulo Costa and Alexandre Barreto, "An ADS-B Intrusion Detection System", The 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-16), Tianjin, China, August 2016.

Cont'd

7. **Thabet Kacem**, Duminda Wijesekera, Paulo Costa, Marcio Monteiro, Alexandre Barreto and Jeronymo Carvalho, “Secure ADS-B Design & Evaluation”, IEEE International Conference on Vehicular Electronics and Safety (ICVES 2015), Yokohama, Japan, November 2015.

8. **Thabet Kacem**, Jeronymo Carvalho, Duminda Wijesekera, Paulo Costa, Marcio Monteiro and Alexandre Barreto, “Risk-adaptive Engine for Secure ADS-B Broadcasts”, SAE 2015 AeroTech Congress & Exhibition (SAE AeroTech 2015), Seattle, WA, September 2015.

9. Marcio Monteiro, Alexandre Barreto, **Thabet Kacem**, Jeronymo Carvalho, Duminda Wijesekera and Paulo Costa, “Detecting Malicious ADS-B Broadcasts Using Wide Area Multilateration”, The 34th Digital Avionics Systems Conference (DASC 2015), Prague, Czech Republic, September 2015.

10. Marcio Monteiro, Alexandre Barreto, **Thabet Kacem**, Duminda Wijesekera and Paulo Costa, “Detecting Malicious ADS-B Transmitters Using a Low-Bandwidth Sensor Network”, The 18th International Conference on Information Fusion (Fusion 2015), Washington, DC, July 2015.

11. **Thabet Kacem**, Duminda Wijesekera, Paulo Costa, Jeronymo Carvalho, Marcio Monteiro and ALexandre Barreto, “Key Distribution Mechanism in Secure ADS-B Networks”, Integrated Communication, Navigation and Surveillance Conference (ICNS 2015), Herndon, VA, April 2015.

12. **Thabet Kacem**, Duminda Wijesekera and Paulo Costa, “Integrity and Authenticity of ADS-B Radars”, IEEE Aerospace Conference (AeroConf 2015), Big Sky, MT, March 2015.

Cont'd

Selected Journal Publications

1. **Thabet Kacem**, Duminda Wijesekera and Paulo Costa. "ADS-Bsec: A Holistic Approach to secure ADS-B". IEEE Transactions on Intelligent Vehicles, October 2018.
2. **Thabet Kacem**, Alexandre Barreto, Duminda Wijesekera and Paulo Costa, "ADS-Bsec: A novel framework to secure ADS-B". ICT Express, 2017, pp.160-163.

Future Challenges

1

Risk of adversarial attacks on ML and DL approaches to detect ADS-B Security Problems

2

Universal Access Transceiver (UAT) Security

3

ACAS-X Security

4

Unmanned Aircraft System Traffic Management Security

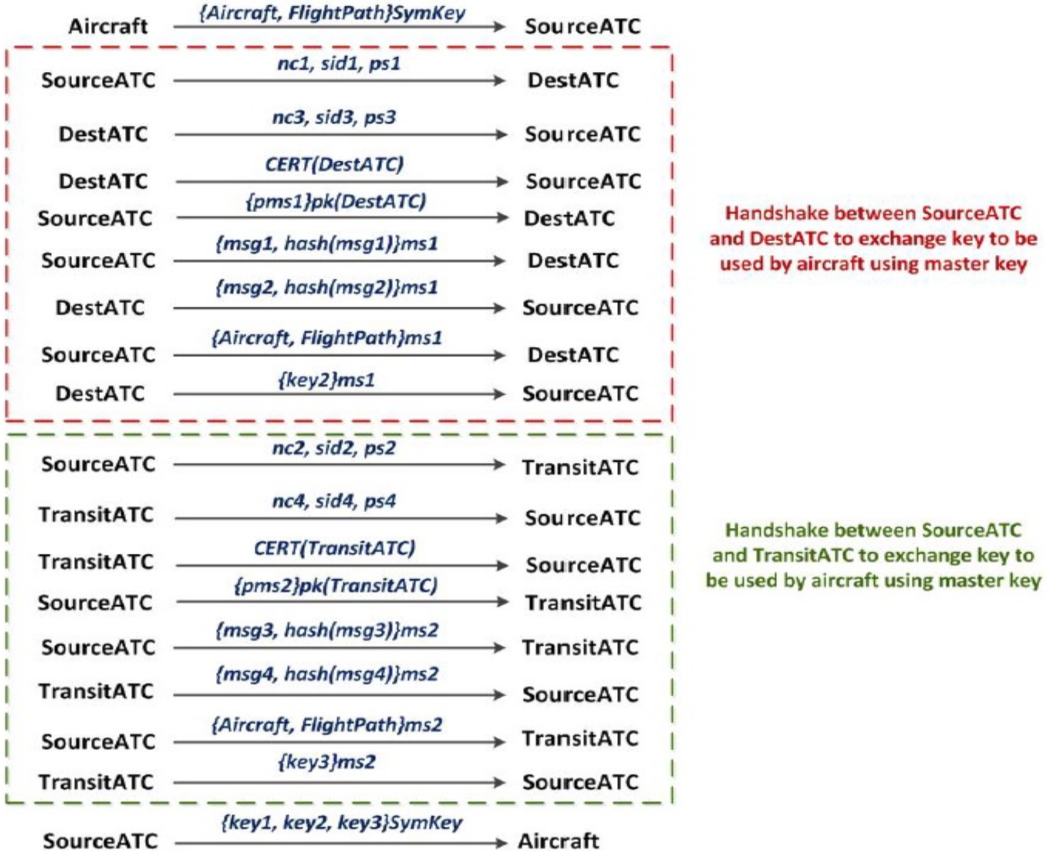
5

Security of other transportation protocols such as the AIS and IoV

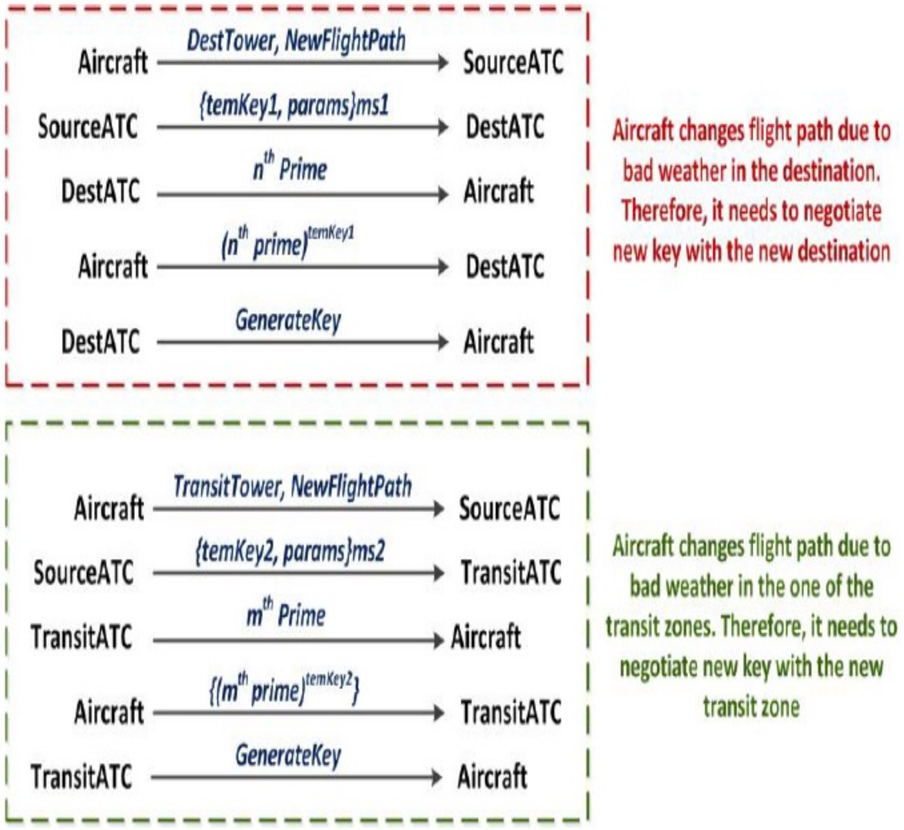
Thank you very much

Backup Slides

Cont'd – Formal Key Exchange Protocol

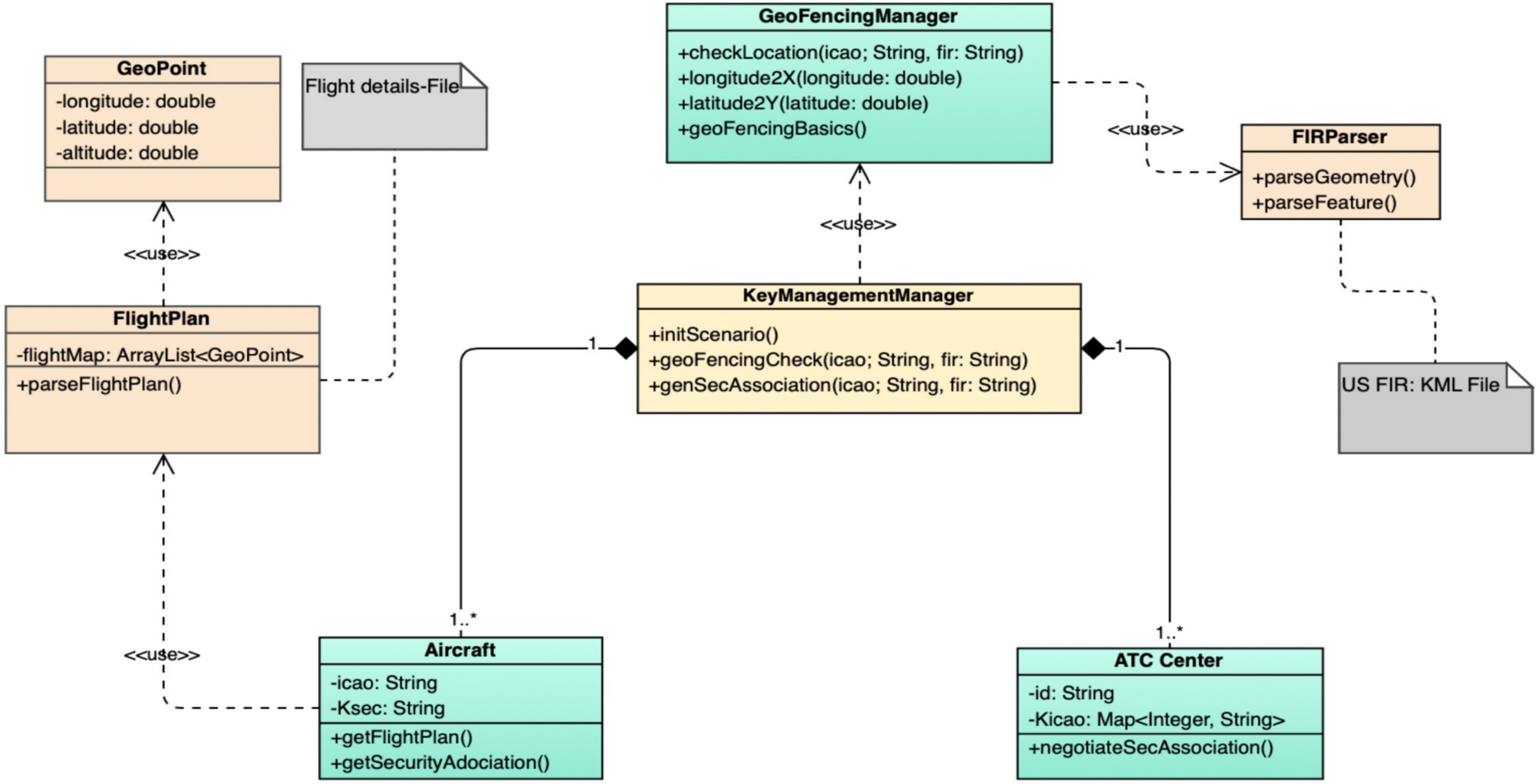


Initial Key Exchange Protocol



Flight Change Key Echange Protocol

Cont'd – Key Management Module Class Diagram



Future Challenges – The Bigger Picture

Create a new research lab focusing on Intelligent Transportation Systems Security

- Aligned with GMU participation in CyManII and VA Cyber Initiative
- Promotion of MS and PhD theses
- Foster research collaboration between faculty members at GMU and beyond

Support the research with a proper educational foundation

- Develop new courses on:
  - ITS Security
  - Critical Infrastructure Security
  - Smart Cities Security

Apply for research Grants. Some potential programs include:

- DOT: University Transportation Centers (UTC) Competition
- FAA: Aviation Research Grants Program
- NSF: SaTC, CPS, S&CC