Key Distribution Mechanism in Secure ADS-B Networks

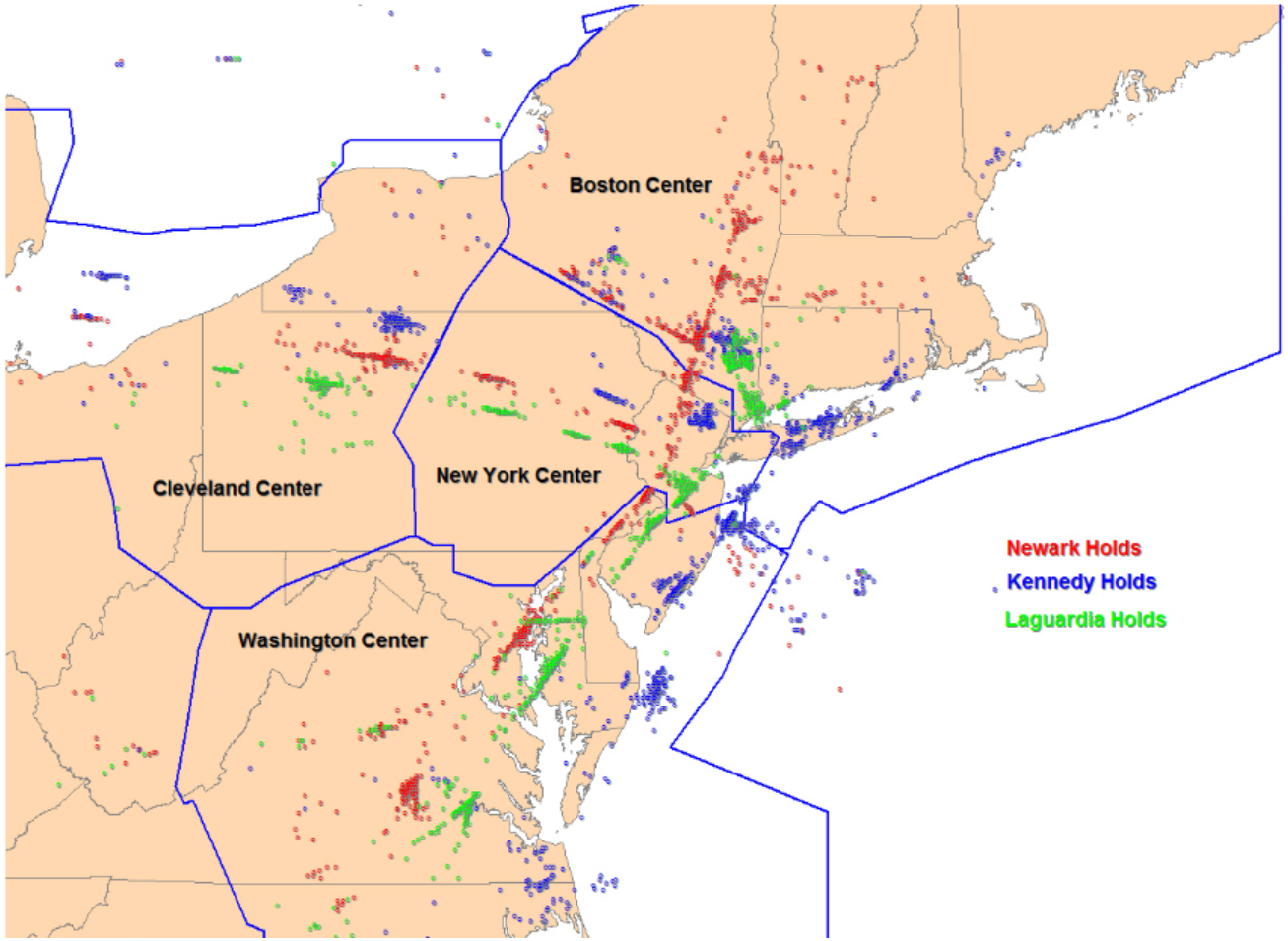
Thabet Kacem, Duminda Wijesekera, Paulo Costa, Jeronymo Carvalho

George Mason University

Márcio Monteiro, Alexandre Barreto

Instituto de Controle do Espaço Aéreo

Need for ADS-B



ADS-B Modes of Operation

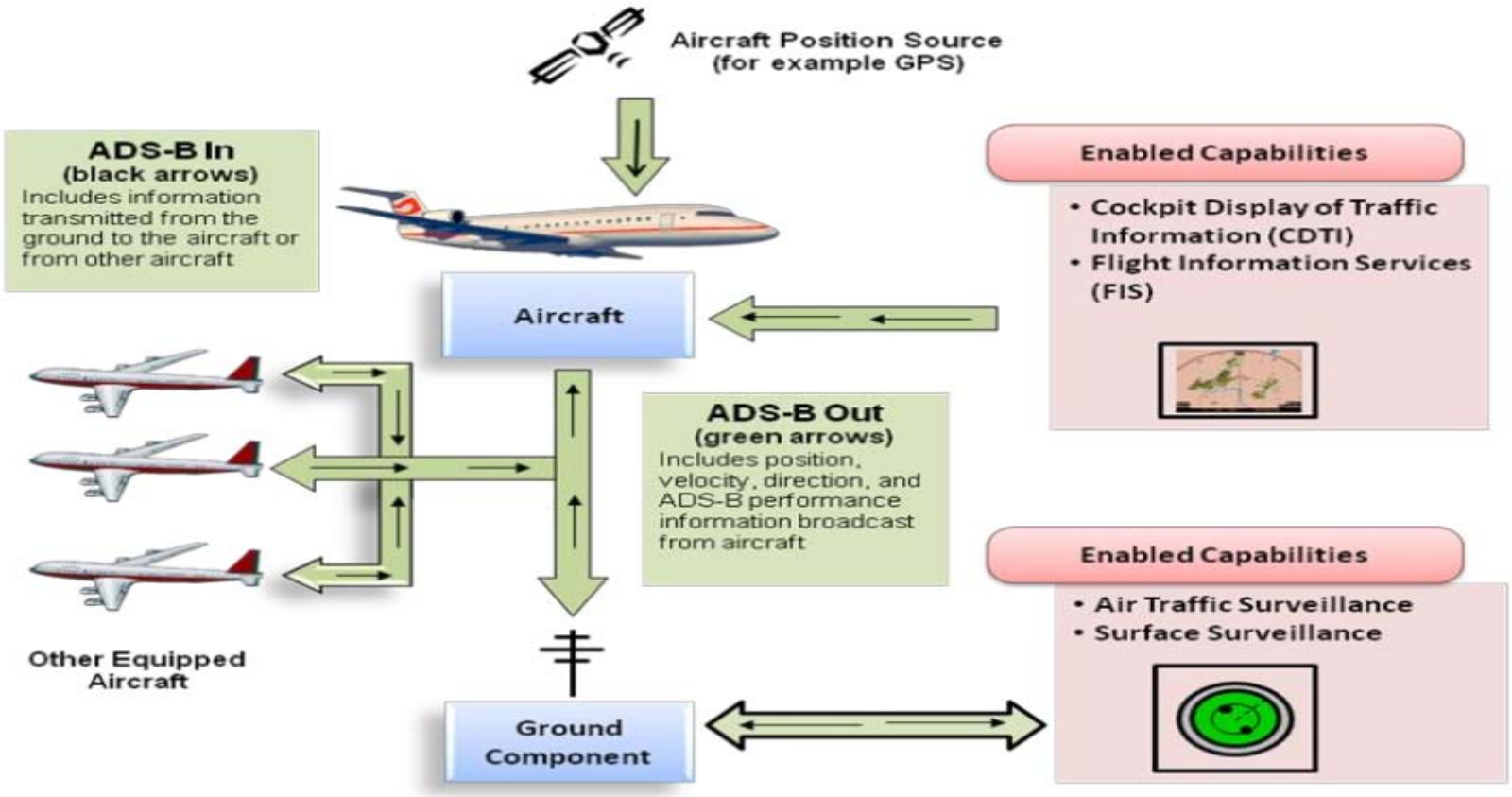
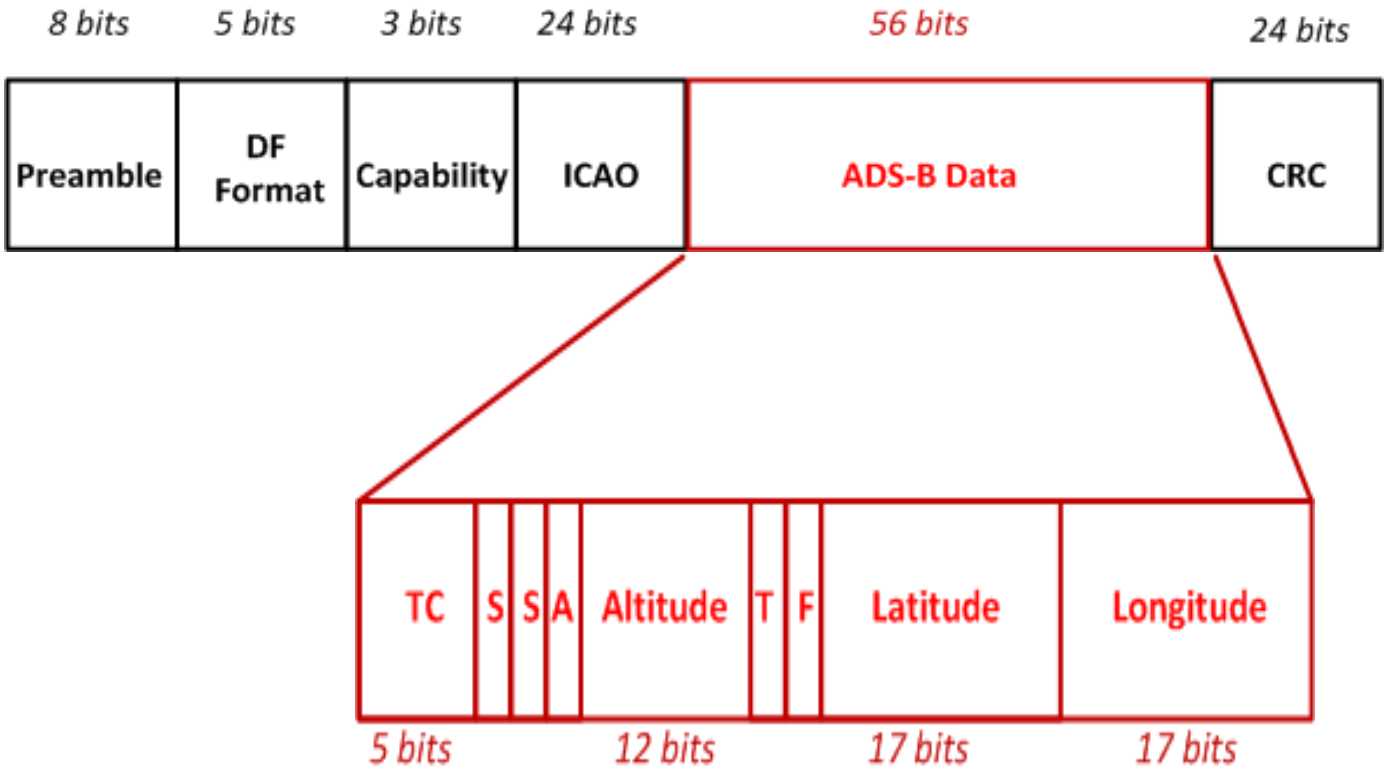


Figure 1—ADS–B System Overview

www.faa.gov/nextgen/implementation/programs/adsb/media/ADSB In ARC Report with transmittal letter.pdf

ADS-B MODE S Packet Format



Motivation

- Lack of Integrity & Authentication
- Secure ADS-B using HMAC
- **Challenge:**
  - **Design appropriate key distribution mechanisms for the HMAC algorithm taking into consideration the nature of the airspace**

Outline

- ADS-B Attack Taxonomy
- Secure ADS-B Framework
- Key Distribution of HMAC Keys
  - Key Distribution in Ideal Conditions
  - Key Distribution in Unforeseen Conditions
- Protocol Verification
- Main Contributions

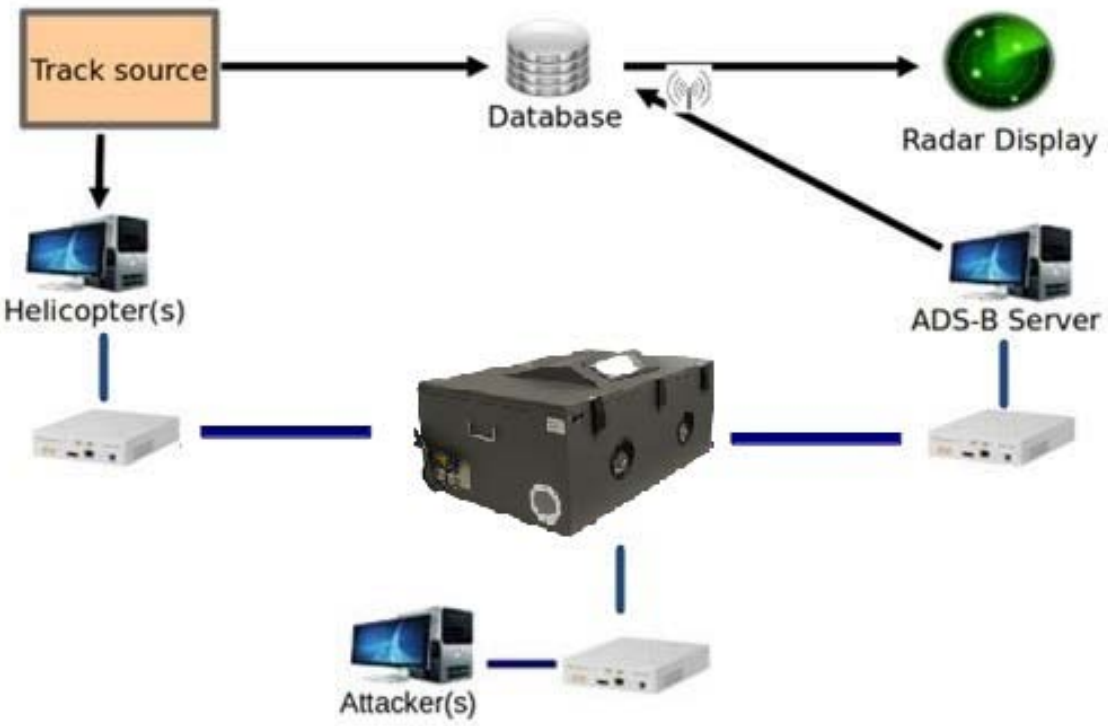
Outline

- ADS-B Attack Taxonomy
- Secure ADS-B Framework
- Key Distribution of HMAC Keys
  - Key Distribution in Ideal Conditions
  - Key Distribution in Unforeseen Conditions
- Protocol Verification
- Main Contributions

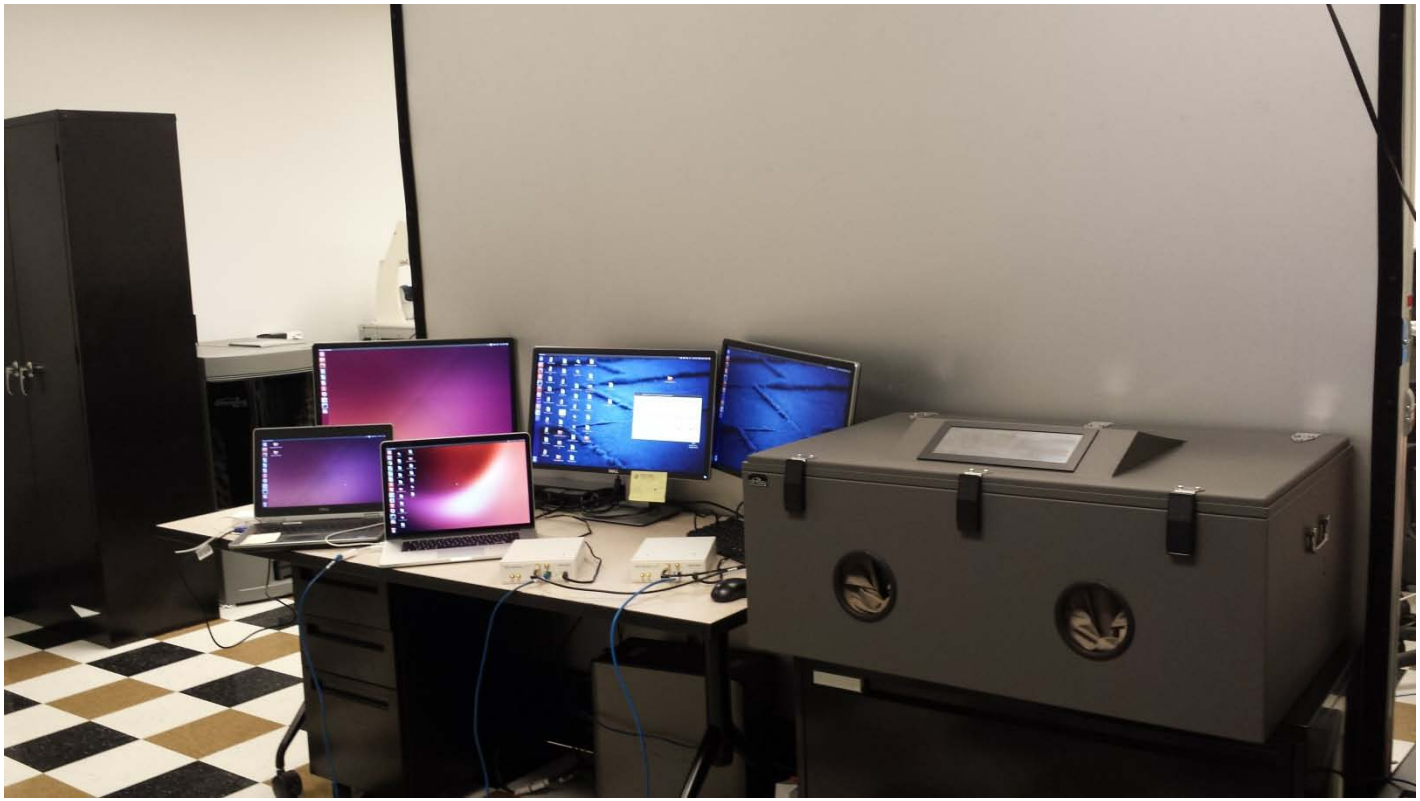
ADS-B Taxonomy

- **Classification Criteria:**
  - Difficulty of implementation of the attack
  - Location of the radio device used for the attack
- **Categories:**
  - Medium-level attacks
  - Advanced-level attacks
  - Expert-level attacks

ADS-B Test Bed



Radio and Radar Lab at GMU

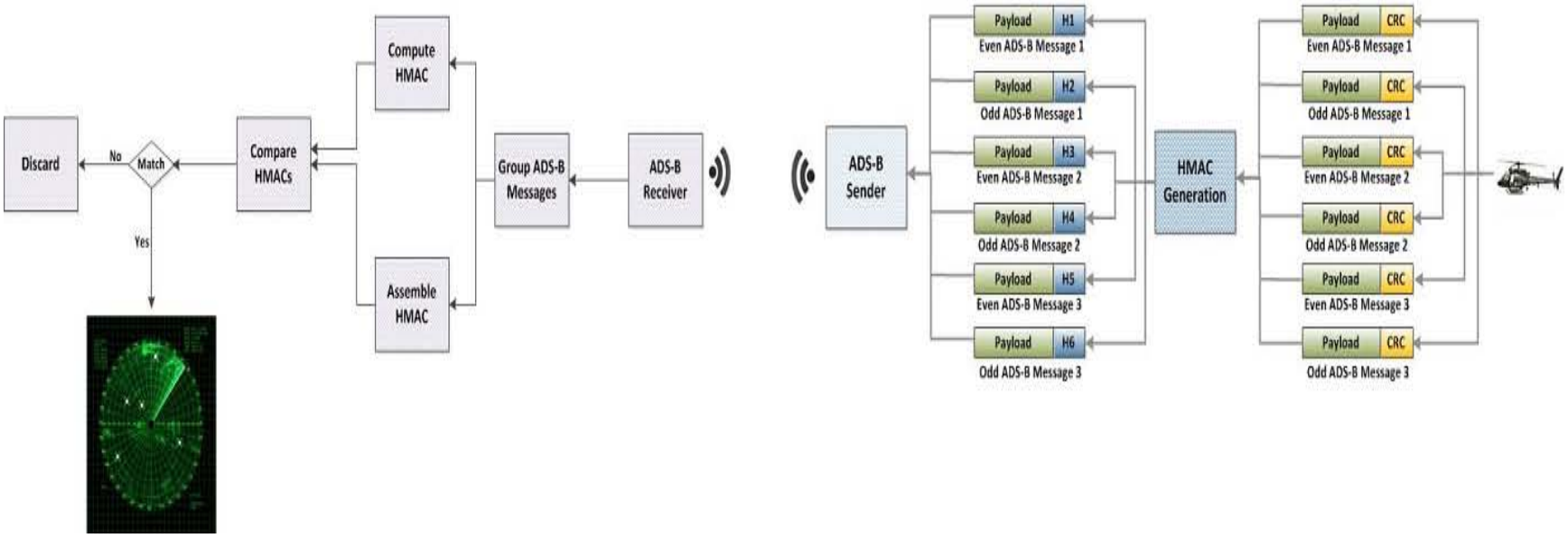


http://radio.vse.gmu.edu/

Outline

- ADS-B Attack Taxonomy
- Secure ADS-B Framework
- Key Distribution of HMAC Keys
  - Key Distribution in Ideal Conditions
  - Key Distribution in Unforeseen Conditions
- Protocol Verification
- Main Contributions

High-level view



Pseudo-code of Secure ADS-B Receiver

```
1       ADSBReceiver receiver = new ADSBReceiver();
2       Map<String, Queue> bucket = new HashMap<String, Queue>();
3       String icao = null;
4       Queue queue = null;
5       String computedHMAC=null, receivedHMAC=null;
6
7       While(receiver.hasNewMessage())
8       {
9       String message = receive.getMessage();
10      String icao = message.getICAO();
11
12      if (!bucket.containsKey(icao))
13      {
14            queue = new Queue();
15      }
16      else
17      {
18            queue = bucket.get(icao);
19      }
20      queue.enque(message);
21      bucket.put(icao,queue);
22      if(queue.size()>6)
23      {
24            String packets = extractPackets(queue);
25            String portions = extractHMAC(packets);
26            receivedHMAC = concatHMAC(portions);
27            String payloads = extractLongPayload(packets);
28            computedHMAC = computeHMAC(payloads, key);
29            if(computedHMAC.equals(receivedHMAC)
30            {
31            processMessages(bucket, icao);
32            }
33      }
34  }
```

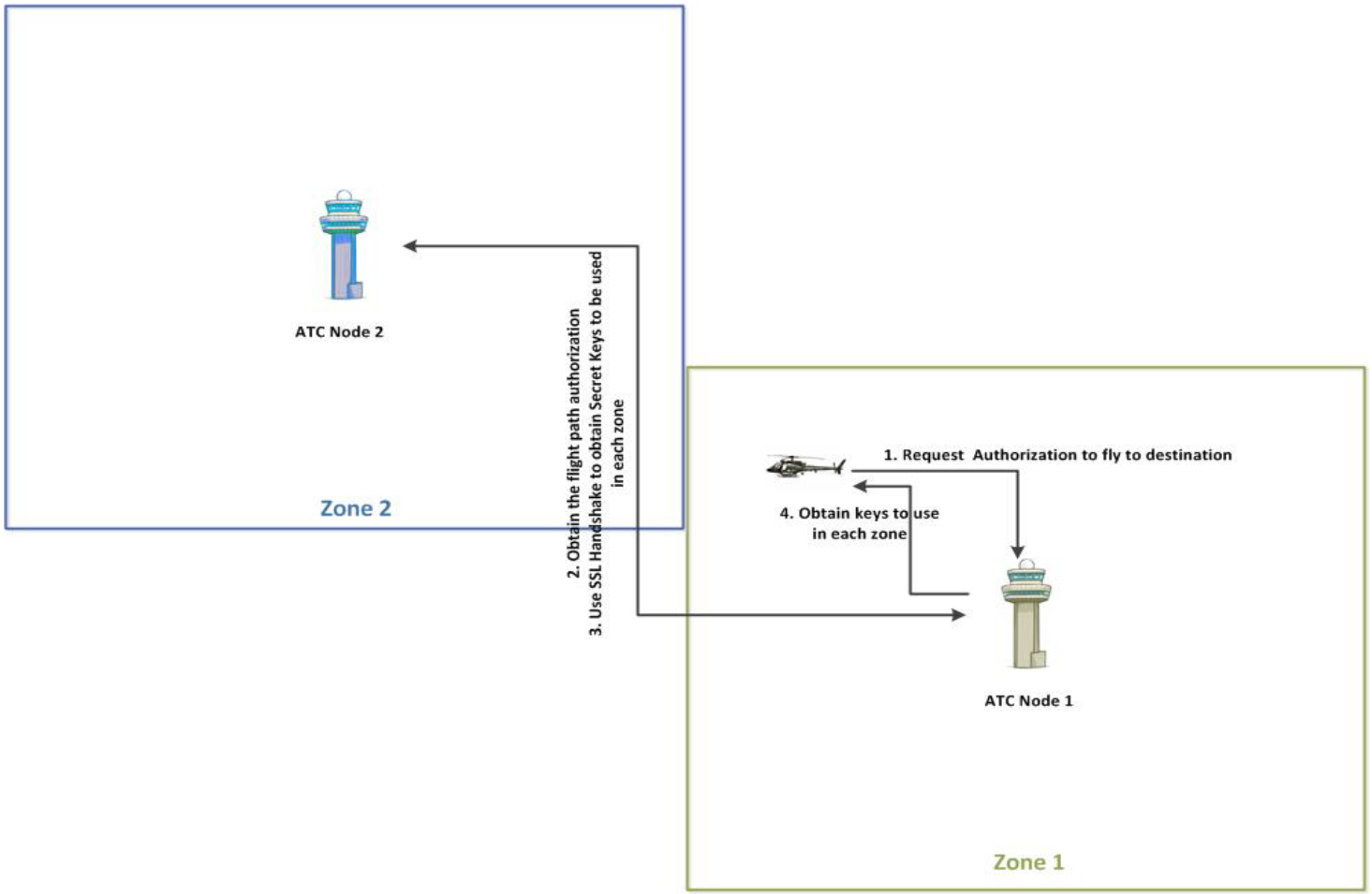
Outline

- ADS-B Attack Taxonomy
- Secure ADS-B Framework
- Key Distribution of HMAC Keys
  - Key Distribution in Ideal Conditions
  - Key Distribution in Unforeseen Conditions
- Protocol Verification
- Main Contributions

Outline

- ADS-B Attack Taxonomy
- Secure ADS-B Framework
- Key Distribution of HMAC Keys
  - Key Distribution in Ideal Conditions
  - Key Distribution in Unforeseen Conditions
- Protocol Verification
- Main Contributions

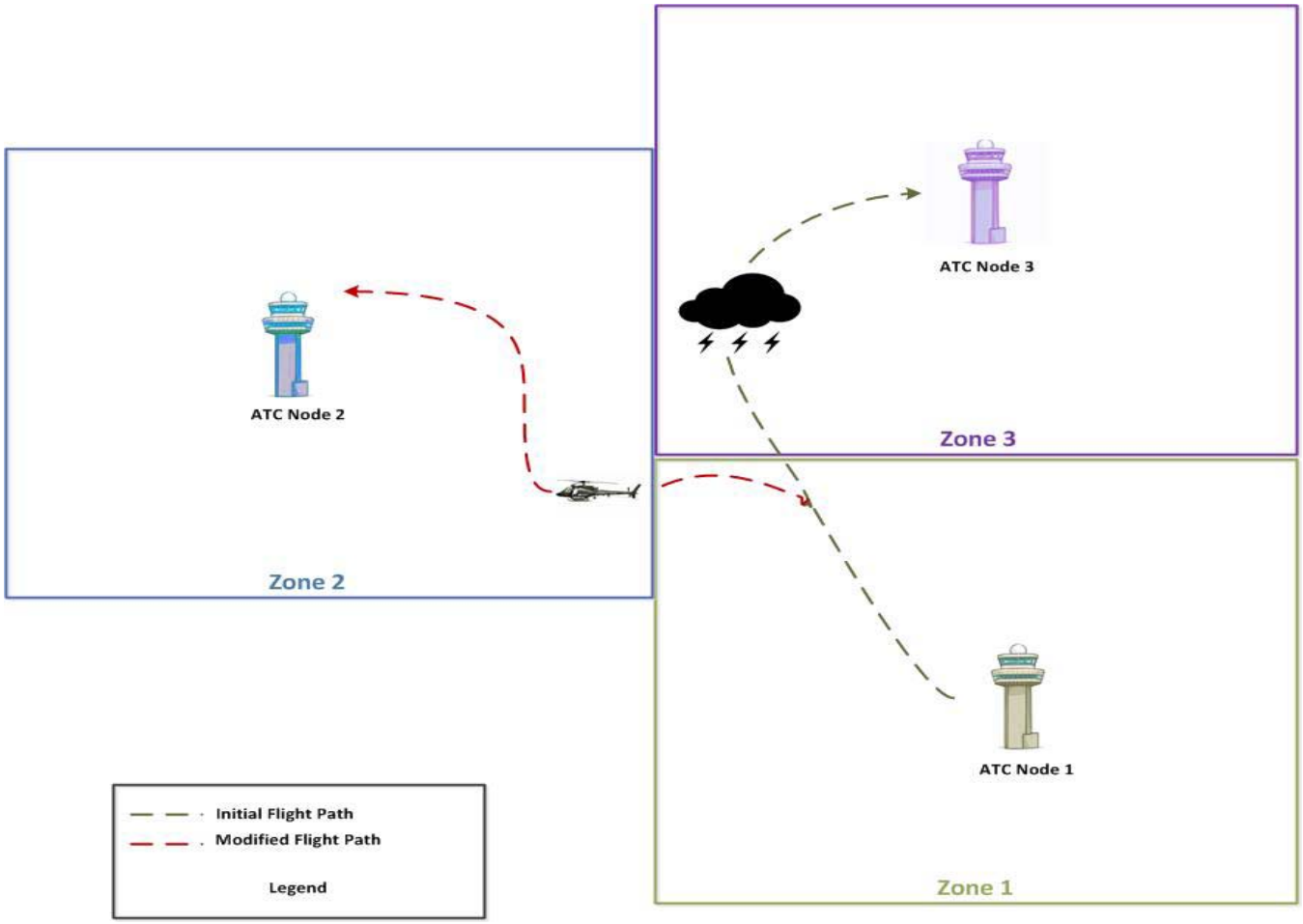
Scenario


ATC Node 2
Zone 2
2. Obtain the flight path authorization
3. Use SSL Handshake to obtain Secret Keys to be used in each zone
1. Request Authorization to fly to destination
4. Obtain keys to use in each zone
ATC Node 1
Zone 1

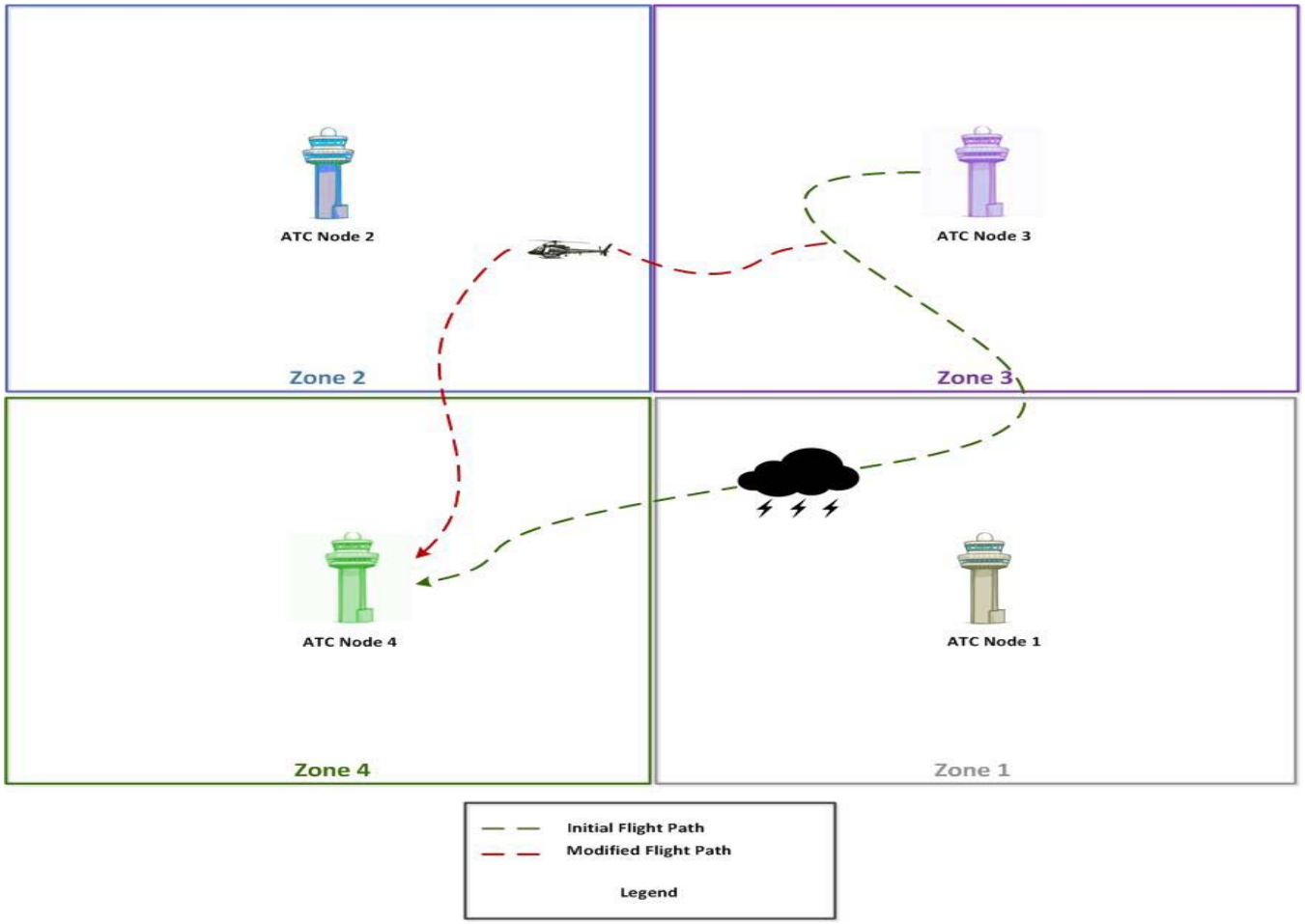
Outline

- ADS-B Attack Taxonomy
- Secure ADS-B Framework
- Key Distribution of HMAC Keys
  - Key Distribution in Ideal Conditions
  - Key Distribution in Unforeseen Conditions
- Protocol Verification
- Main Contributions

Scenario 1


ATC Node 3
ATC Node 2
ATC Node 1
Zone 3
Zone 2
Zone 1
Initial Flight Path
Modified Flight Path
Legend

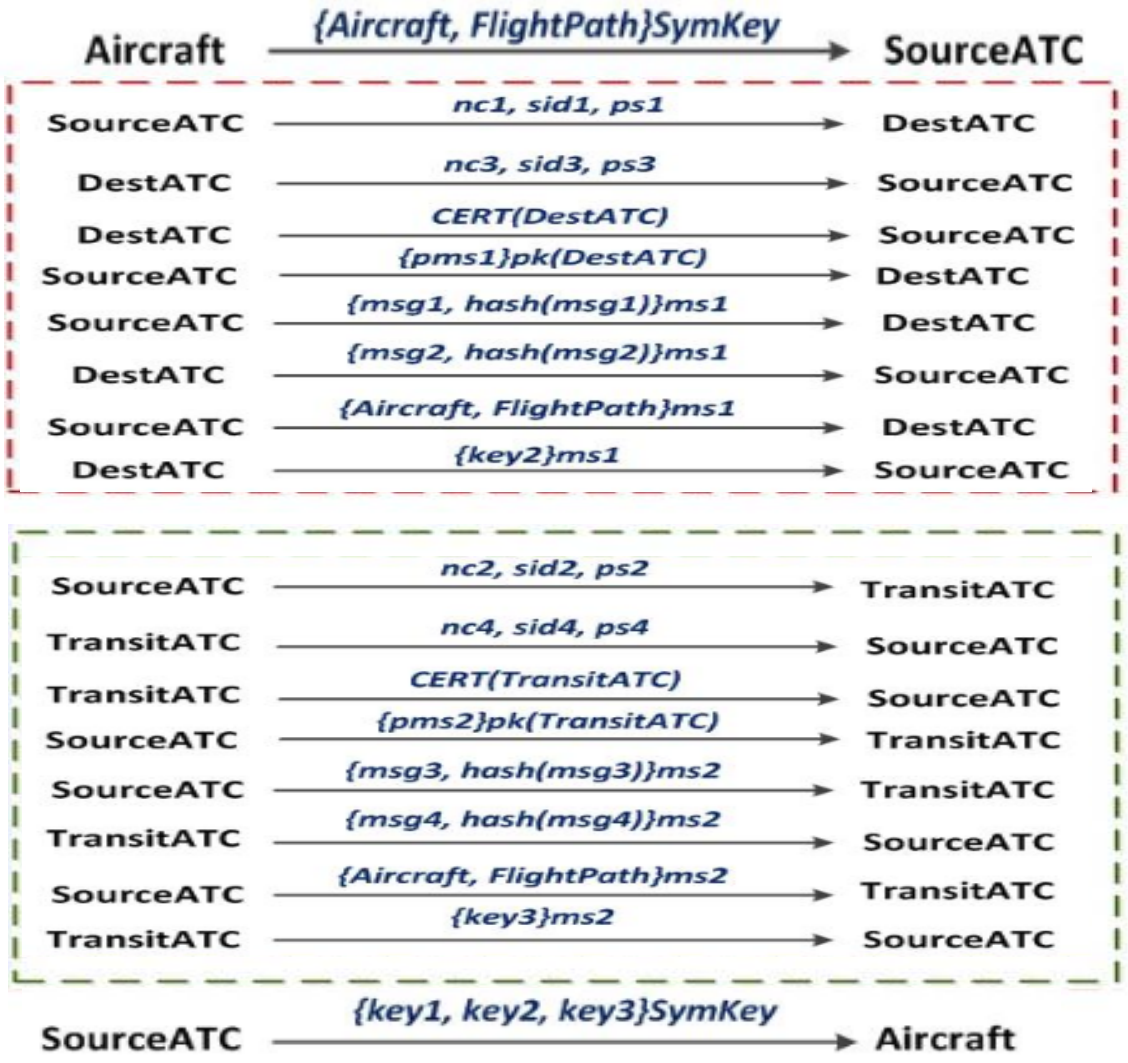
Scenario 2


ATC Node 2
ATC Node 3
Zone 2
Zone 3
ATC Node 4
ATC Node 1
Zone 4
Zone 1
Initial Flight Path
Modified Flight Path
Legend

Outline

- ADS-B Attack Taxonomy
- Secure ADS-B Framework
- Key Distribution of HMAC Keys
  - Key Distribution in Ideal Conditions
  - Key Distribution in Unforeseen Conditions
- Protocol Verification
- Main Contributions

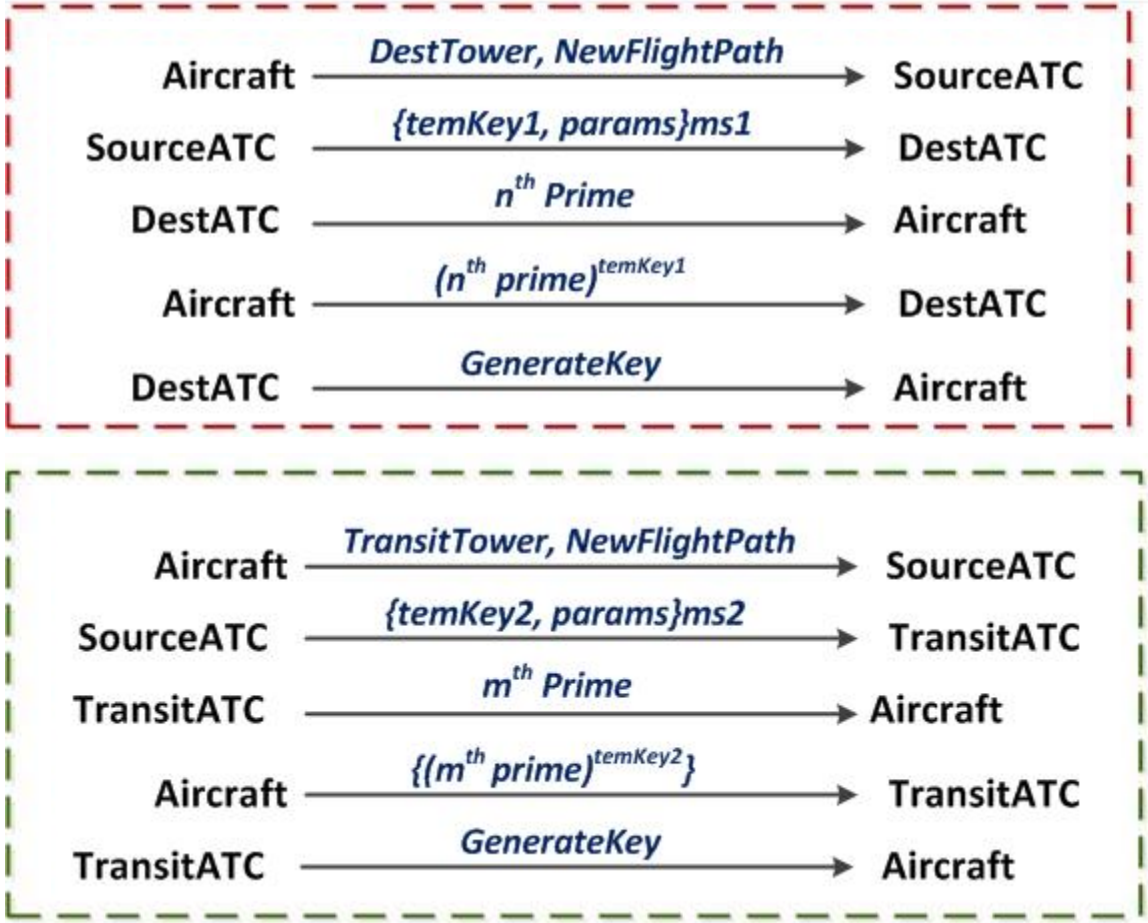
Initial Key Distribution



Handshake between SourceATC and DestATC to exchange key to be used by aircraft using master key

Handshake between SourceATC and TransitATC to exchange key to be used by aircraft using master key

Key Exchange in Unforeseen Conditions



Aircraft changes flight path due to bad weather in the destination. Therefore, it needs to negotiate new key with the new destination

Aircraft changes flight path due to bad weather in the one of the transit zones. Therefore, it needs to negotiate new key with the new transit zone

Outline

- ADS-B Attack Taxonomy
- Secure ADS-B Framework
- Key Distribution of HMAC Keys
  - Key Distribution in Ideal Conditions
  - Key Distribution in Unforeseen Conditions
- Protocol Verification
- Main Contributions

Main Contributions

- We proposed an approach based on HMAC to secure ADS-B by providing authenticity and integrity
- We described the key distribution scheme in:
  - Ideal conditions
  - Unforeseen conditions
- Key exchange protocol verification using Scyther tool

The end

- Thank you very much !!
- Questions ?!