# A compatible and identity privacy-preserving security protocol for ACARS

M11109106 方宇翔 M11109139 卿頤亭 M11109114 呂佳玲 M11209205 楊明瑋 M11209202 黃雅婄 M11209218 黃奕瑄

# Aircraft Communications Addressing and Reporting System (ACARS)

空中傳輸簡訊的數位資料鏈系統

ACARS協定設計時缺乏安全考慮

→易受到攻擊

訊息以明文形式傳輸

→ 攻擊者易解析/產生ACARS訊息

# 現有解決方法

空地資料鏈安全問題

#### IBS 和 IBE

⇒身份隱私無法受到保護

#### **AEALV**

→識別飛機的合法性

保護隱私和 身份驗證架構

#### CNS/ATM 和 Security ACARS

→機密性、身分驗證和完整性

#### **AMS**

→機密性和真實性

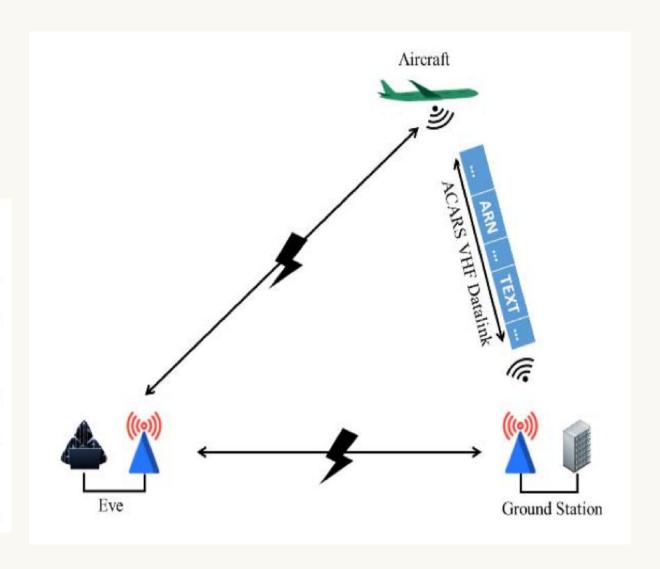
## 安全模型

#### 攻擊者透過竊聽, 輕鬆接收和解析訊息

#### 依據ARINC 618標準, ACARS訊息以明文儲存

#### ACARS MESSAGE FRAME FORMAT IN ARINC 618 [1]

Field Name	SOH	Mode	ARN	TAK	Label	DBI	STX
Length Example	1 <soh></soh>	1 2	7 B1120	1 <nak></nak>	2 5Z	1 3	1 <stx></stx>
Field Name	MSN	FlightID	Text	Siffix	BCS	BCS Suffix	
Length Example	4 M01A	6 CA5276	0-210 HELLO	1 <etx></etx>	2	1 <del></del>	



# ACARS協定缺乏安全考慮





#### 無身分驗證

#### 主動攻擊:

- 建構合法的虛假訊息欺騙系統
- 重送攻擊



通道未加密

#### 被動攻擊:

• 竊聽

# 協議設計目標



● 保密性

防止訊息文字洩漏給未經授權的使用者



● 身分驗證 確保訊息來自合法航班或地面站



●訊息完整性

確保接收到的 ACARS 訊息在傳輸過程中不會被修改或遺失 透過MAC和數位簽章機制實現



● 保護飛機身份隱私 加密ACARS訊息中的ARN欄位

# 協議說明

ACARS 地對空資料鏈匿名安全會話協定分兩個階段:

- 1. 會議建立協定
- 2. 傳輸協定

#### $k_d$

## 會議建立協定

與地面站建立安全身分認證、 交換會議所需的密鑰和參數

Step 1:地面站廣播其身份。

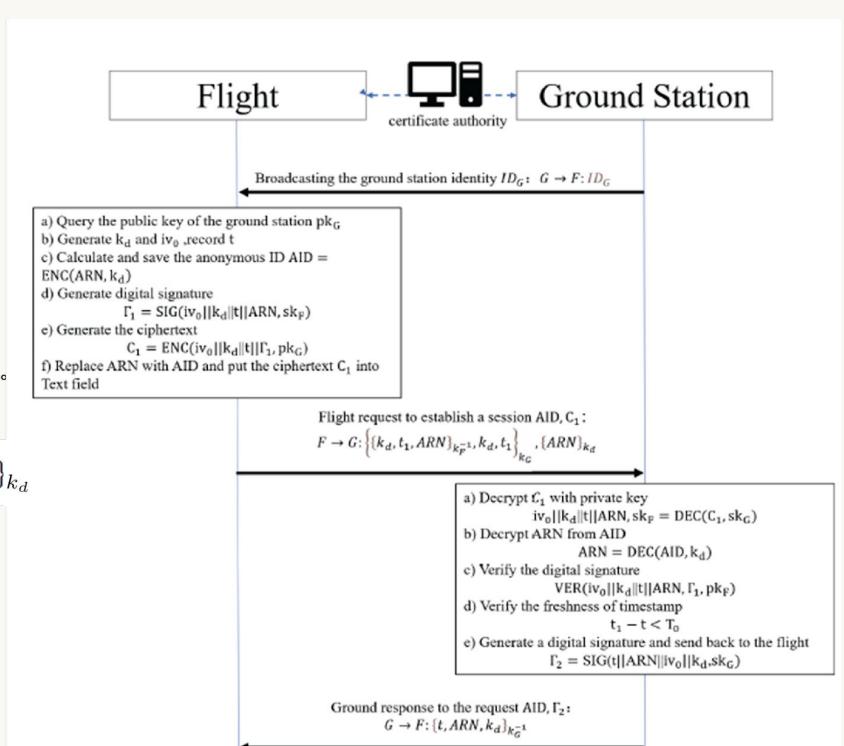
 $G \to F : ID_G$ 

Step 2:飛機發起會議建立的請求並傳送給地面。

$$F \to G : \{\{k_d, t, ARN\}k_F^{-1}, k_d, t\}_{k_G}, \{ARN\}_{k_d}\}$$

Step 3: 地面站驗證飛機的請求,並發送回應。

 $G \rightarrow F: \{t, ARN, k_d\}_{k_G^{-1}}$ 



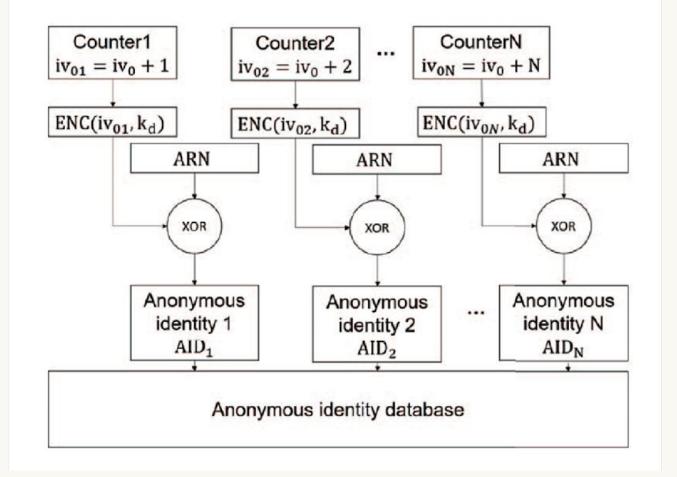
# 會議建立協定

Step 4: 在飛機驗證地面站的請求後,雙方生成N個匿名身份。

a) Verify the signature  $VER(t||ARN||iv_0||k_d,pk_G)$  b) Generate the abonymous identifies  $AID_i = ENC(iv_{0i},k_d,ARN)$  where  $iv_{0i} = iv_0 + i, 1 \le i \le N$ 

a) Generate the abonymous identifies  $AID_i = ENC(iv_{0i}, k_d, ARN)$  where  $iv_{0i} = iv_0 + i, 1 \le i \le N$ 

● 通過對稱加密生成飛機的匿名身份資料庫。



#### 傳輸協定

Step1:飛機向地面站透過匿名身分發送加密 消息。



 $F
ightarrow G:\{M_1, \operatorname{hash}(M_1||MSN_1)\}_{k_d}, ARN_{k_d}$ 

Step2: 地面站透過匿名身分資料庫驗證身分後, 透過Hash值比對,確保訊息完整性。

#### Flight

- a) Generate plaintext  $M_1$ , message sequence number MSN<sub>1</sub> and calculate hash value  $H_1 = HASH(M_1||MSN_1)$
- b) Calculate the initial vector for this message  $iv_i = HASH(iv_0||MSN_1)$
- c) Encrypt the text

 $C_1 = ENC(M_1||H_1, k_d, iv_i)$ 

d) Replace the ARN with a randomly selected AIDi and put the ciphertext C1 into Text field

**Ground Station** 

Downlink

Downlink Message AID, C1

 $F \rightarrow G: \{M_1, hash(M_1, MSN_1)\}k_d, \{ARN\}_{k_d}$ 

- a) Find ARN, kd and ivo from local database
- b) Calculate the initial vector for this message  $iv_i = HASH(iv_0||MSN_1)$
- c) Decrypt the text

 $\mathbf{M}_1||\mathbf{H}_1 = \mathrm{DEC}(\mathbf{C}_1, \mathbf{k}_d, iv_i)$ 

d) Verify the Hash value

 $H_1 = Hash(M_1||MSN_1)$ 

e) Future processing on ARN and plaintext

M<sub>1</sub> in ACARS

# 安全分析和性能評估

- → 根據 Burrows, Abadi & Needham (BAN logic)
- → Automated Validation of Internet Security Protocols and Applications (AVISPA)



身分驗證

**Authentication** 



加密目標

**Secrecy goals** 



網路安全協定

應用程序自動驗證

# BAN logic 安全分析和性能評估

Goals	Expression		
GOAL1	$G  \equiv F \stackrel{k_d}{\Leftrightarrow} G$		
GOAL2	$G  \equiv ARN$		
GOAL3	$F  \equiv G  \equiv F \stackrel{k_d}{\Leftrightarrow} G$		
GOAL4	$F  \equiv G  \equiv ARN$		
GOAL5	$G  \equiv F  \equiv F \stackrel{k_d}{\Leftrightarrow} G$		
GOAL6	$G  \equiv F  \equiv ARN$		

# 績效評估

	Confidentiality	Authentication	Integrity	Identity Privacy
[8]	✓		✓	
[10]		✓	✓	
[13]		✓	✓	✓
[19]	✓			
[20]	✓	✓	✓	
[21]	✓	✓	✓	
[26]		✓	✓	
Proposed	✓	✓	✓	✓

## 結論

- ACARS資料鏈匿名安全會議協議
  - 。會議建立和傳輸流程
  - 。使用非對稱密碼和對稱密碼確保機密性和完整性
- 優勢
  - 。保護身分隱私
  - 。通過形式分析和模擬驗證安全性
  - 。與ACARS標準相容,實際部署可行

# Thanks!