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

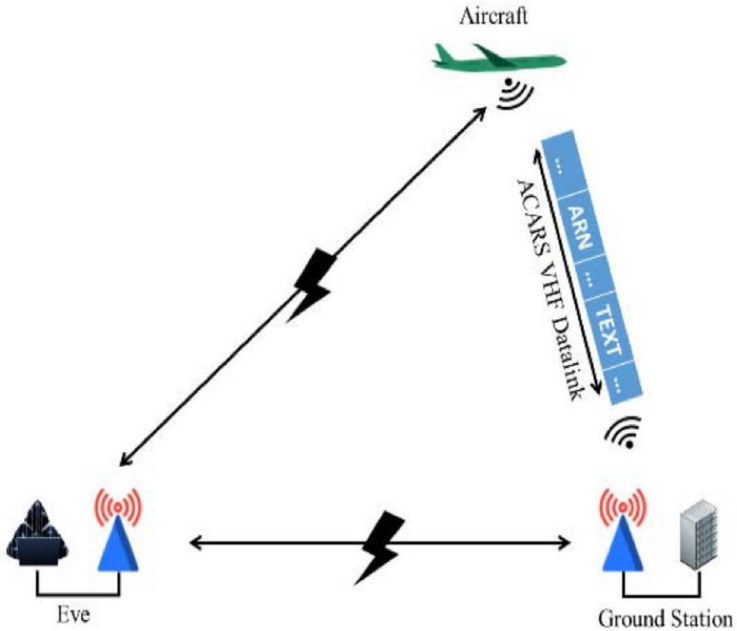
攻擊者透過竊聽，輕鬆接收和解析訊息

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	1	1	7	1	2	1	1
Example	<SOH>	2	..B1120	<NAK>	5Z	3	<STX>

Field Name	MSN	FlightID	Text	Siffix	BCS	BCS Suffix
Length	4	6	0-210	1	2	1
Example	M01A	CA5276	HELLO	<ETX>		<DEL>



ACARS協定缺乏安全考慮

安全考慮

無身分驗證

通道未加密

主動攻擊:

- 建構合法的虛假訊息欺騙系統
- 重送攻擊

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

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。

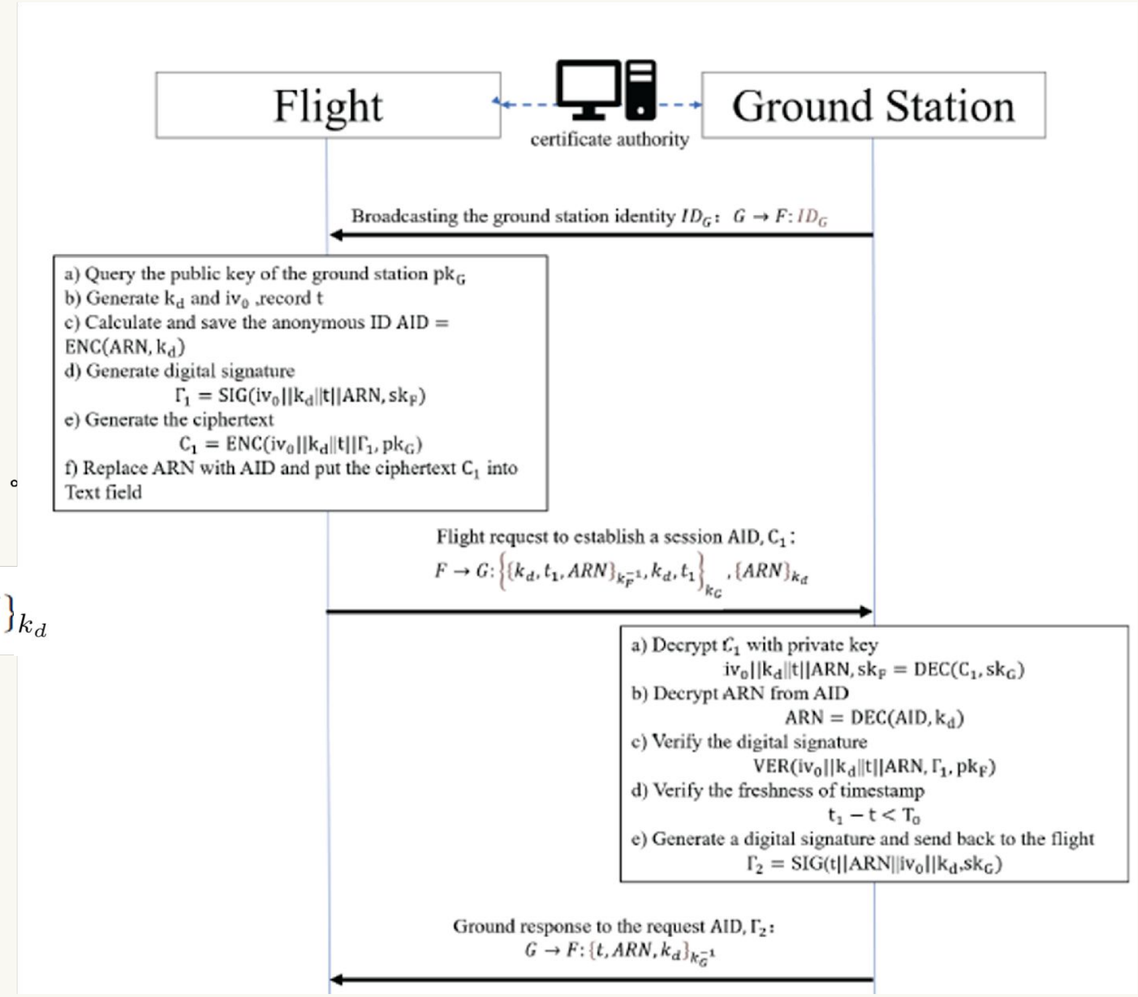
$$G \rightarrow F : ID_G$$

Step 2：飛機發起會議建立的請求並傳送給地面。

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

Step 3：地面站驗證飛機的請求，並發送回應。

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



k_d

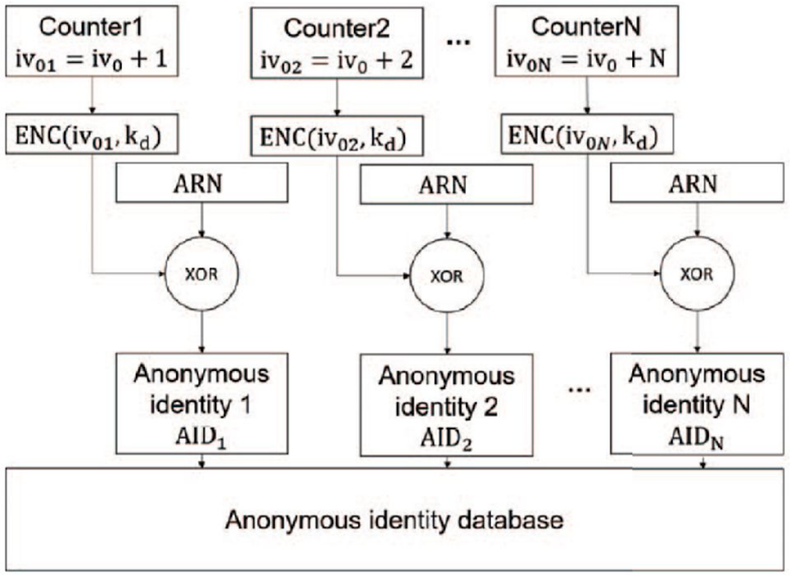
會議建立協定

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

a) Generate the abonymous identifies
$$\text{AID}_i = \text{ENC}(iv_{0i}, k_d, \text{ARN})$$
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。

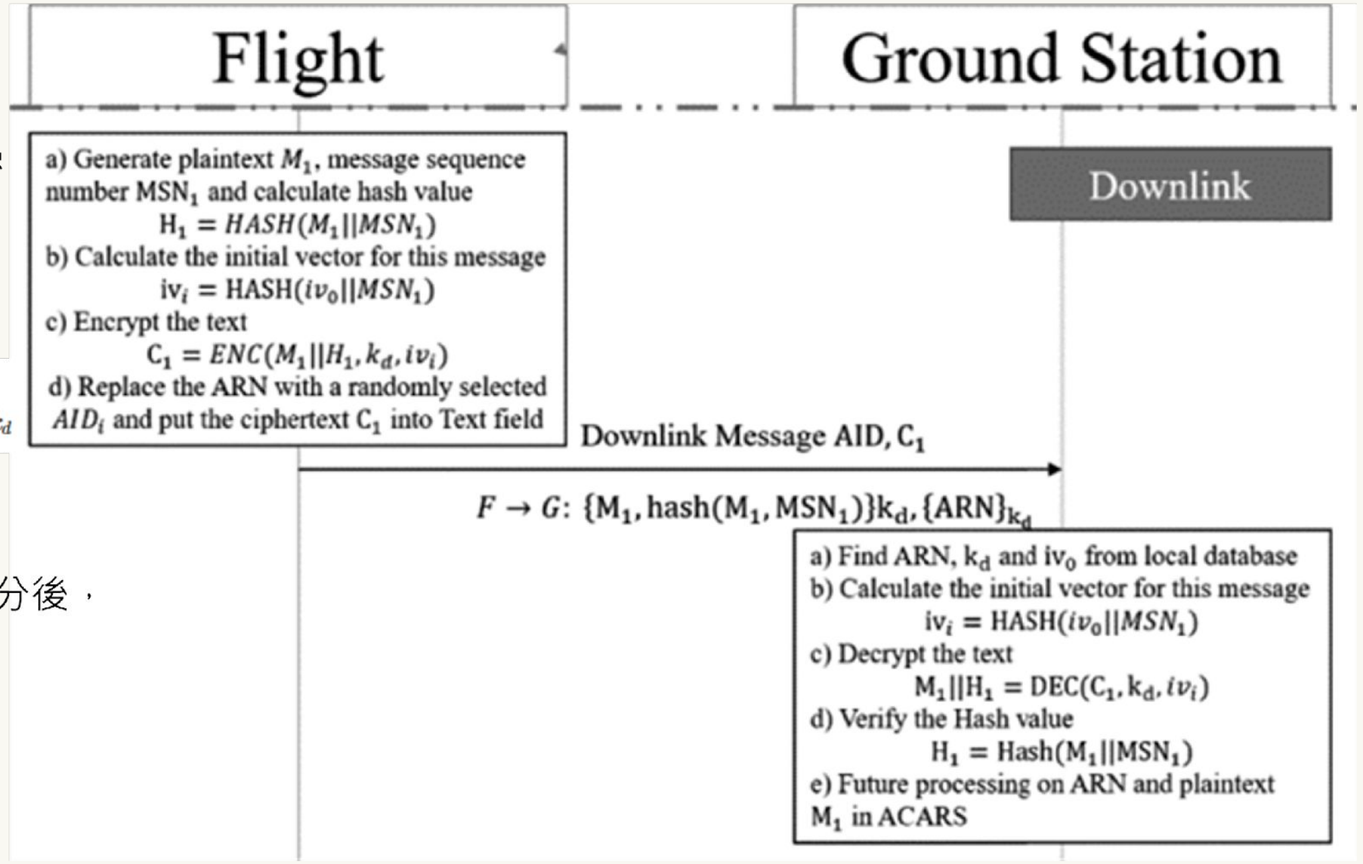


傳輸協定

Step1：飛機向地面站透過匿名身分發送加密消息。

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

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。



安全分析和性能評估

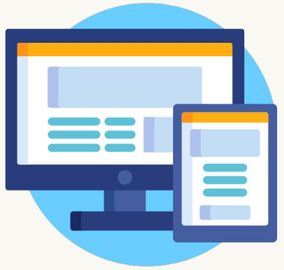
- 根據 Burrows, Abadi & Needham (BAN logic)
- Automated Validation of Internet Security Protocols and Applications (AVISPA)

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	$G\mid \equiv F \overset{k_d}{\Leftrightarrow} G$
GOAL2	$G\mid \equiv ARN$
GOAL3	$F\mid \equiv G\mid \equiv F \overset{k_d}{\Leftrightarrow} G$
GOAL4	$F\mid \equiv G\mid \equiv ARN$
GOAL5	$G\mid \equiv F\mid \equiv F \overset{k_d}{\Leftrightarrow} G$
GOAL6	$G\mid \equiv F\mid \equiv ARN$

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!