Toward Trusted and Swift UAV Communication: ISAC-Enabled Dual Identity Mapping

Cui, Y., Feng, Z., Zhang, Q., Wei, Z., Xu, C., Zhang, P.

IEEE Wireless Communication 2023

2024.10.08.

Summarized by, Sangwi Kang | swkang@mmlab.snu.ac.kr

Outline

- Introduction
- ISAC : Integrated Sensing and Communication
- ISAC-Enabled Dual Identity Solution
- Solution Structure
- Scenario and Advantage
- Open Challenges
- Conclusion

Introduction

- UAV networks are expected to be a promising carrier for wireless intelligent communication and 6G network
- However, UAV networks implicates security and efficiency issues
  - Simplified verification, removing repetitive feedbacks
- To ensure trusted and swift UAV networks, the UAV should utilize both physical and digital identity
- And the **ISAC (Integrated Sensing and Communication)** can utilize both of them, by achieving S&C functionalities together

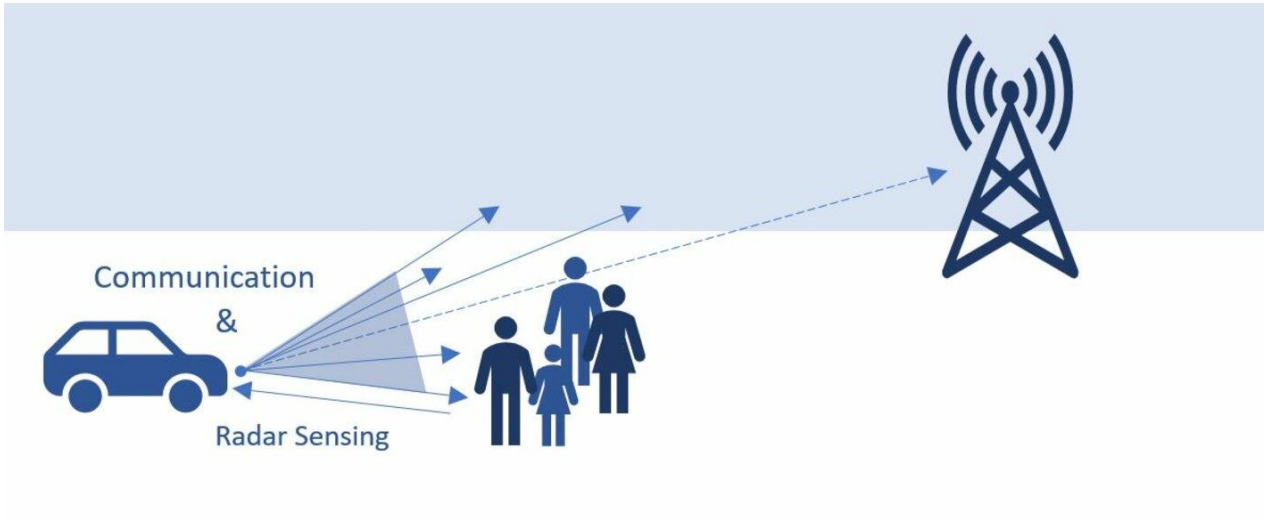
  Sensing & Communication

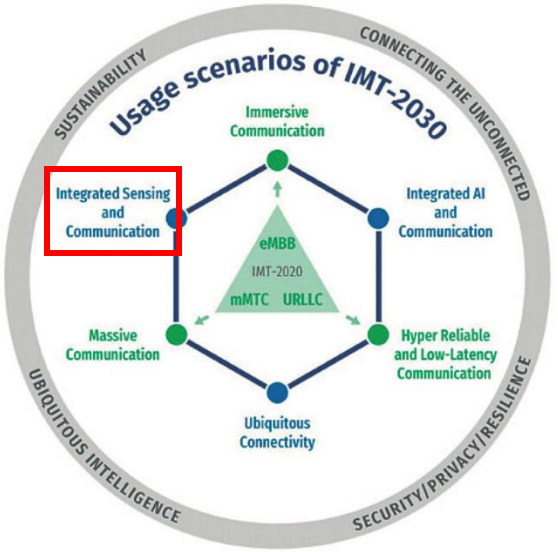
- This paper presents **ISAC-enabled dual identity solution** for trusted and swift UAV communication

ISAC : Integrated Sensing and Communication

- The IMT-2023 vision document was drafted on June 22, 2023, and lays out the future vision for 6G communications
- ISAC is one of the main scenarios for IMT-2030
- Co-existence of S&C (sensing & communication) to **Integrated S&C**

  → **Network as Sensor**





Sixth-Generation Networks and Integrated Sensing and Communications, ETRI Electronics and Telecommunications Trends, 38-6, Dec, 2023

Trustworthy Physical Interfaces, barkhausen institut

ISAC-Enabled Dual Identity Solution

> Overview

- Purpose (Necessary but repetitive process)
  - Removing the tedious communication feedback
  - Removing beam management latency
  - **Ensuring communication security**
- Method
  - **Using the benefits of ISAC technology**

✓ Utilize Rich information of the signal

✓ And the accurate physical features of the echo

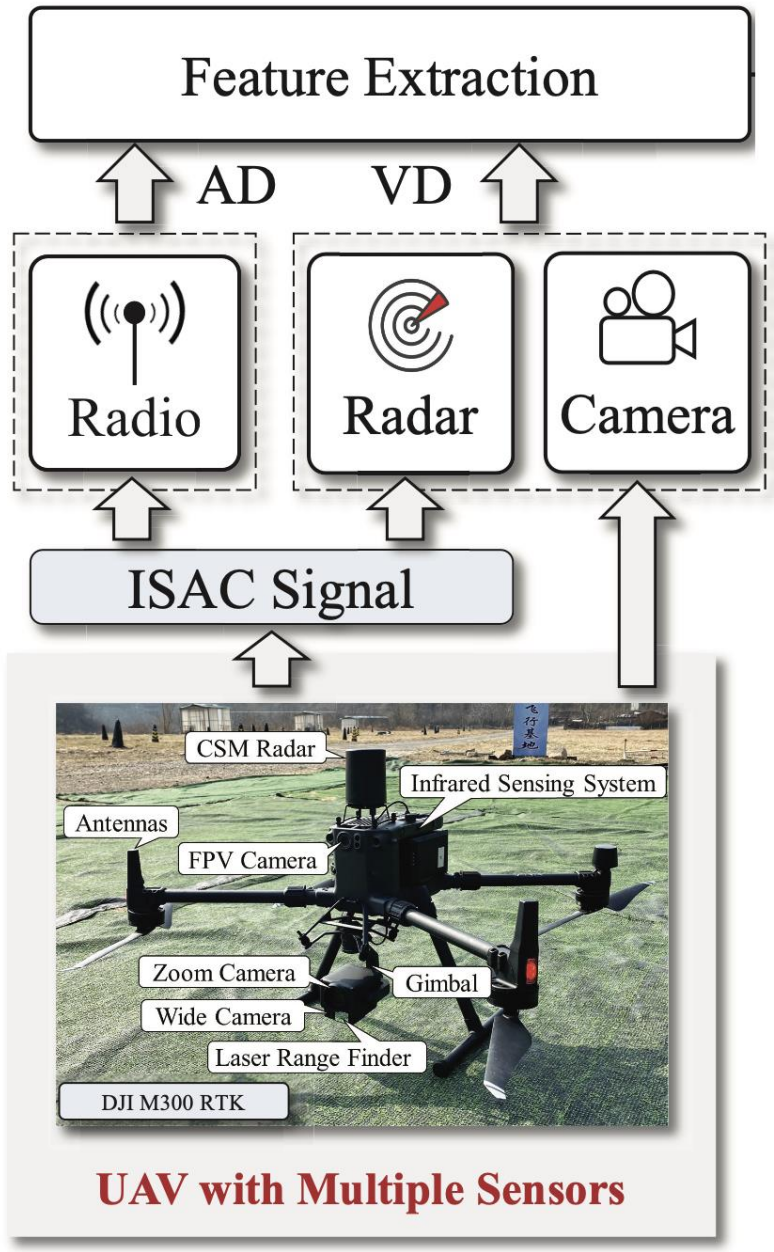
- Structure
  - Feature : Physical identity, digital identity
  - Domain : AD (Auditory Domain), VD (Visual Domain)
  - Modules : Identity production / mapping / management / authentication

→ Get accurate UAV **physical-digital identity mapping**

ISAC-Enabled Dual Identity Solution

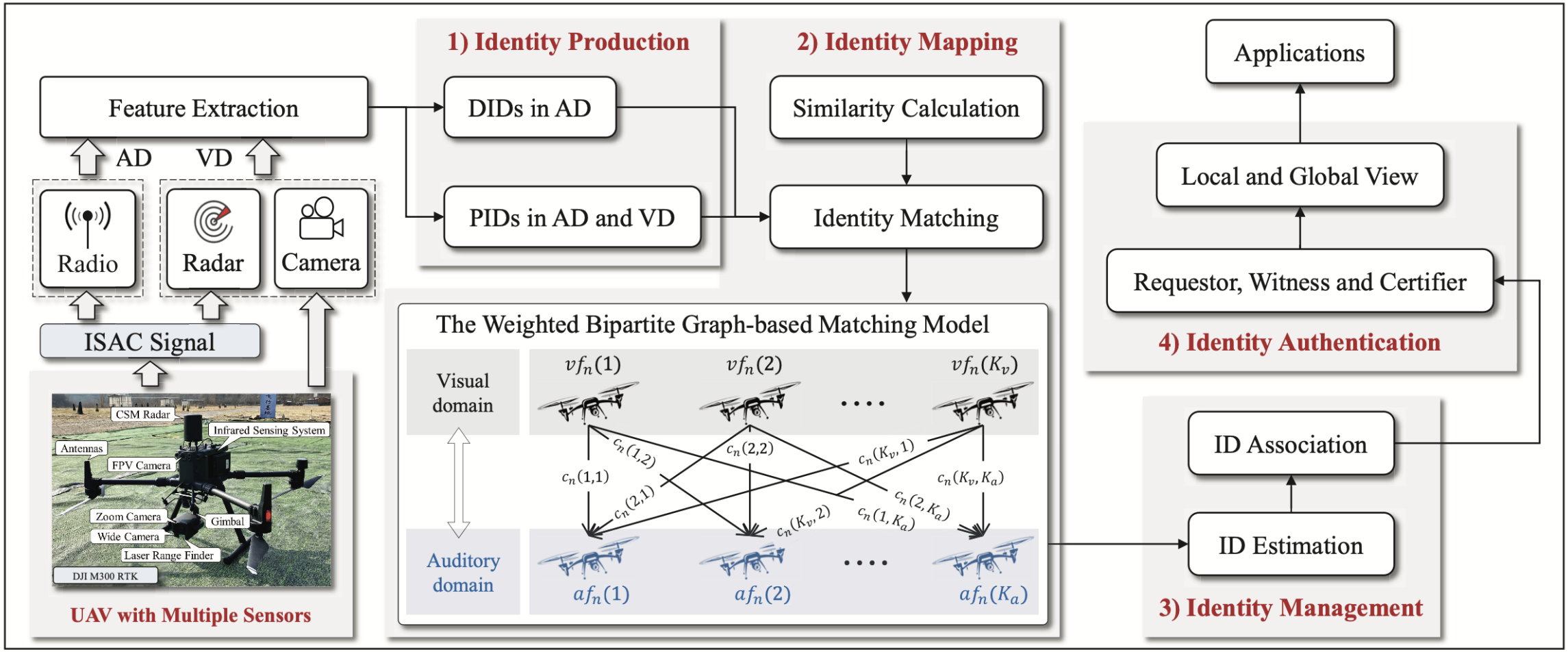
> Terminology

- AD : Auditory Domain
  - Just catch the signal **passively**
  - Obtain the information
- VD : Visual Domain
  - **Actively** sends the signals or use features and sense the environment
- DID : Digital Identity
  - Digital identity for authentication process
  - IP/MAC address, unique keys, RF fingerprint, etc.
  - **Only** obtained from **AD**
- PID : Physical Identity
  - The physical properties of a UAV node
  - Wing type, location, velocity, distance, etc.
  - **Both of the AD and VD** information can be used



Solution Structure

> Overview



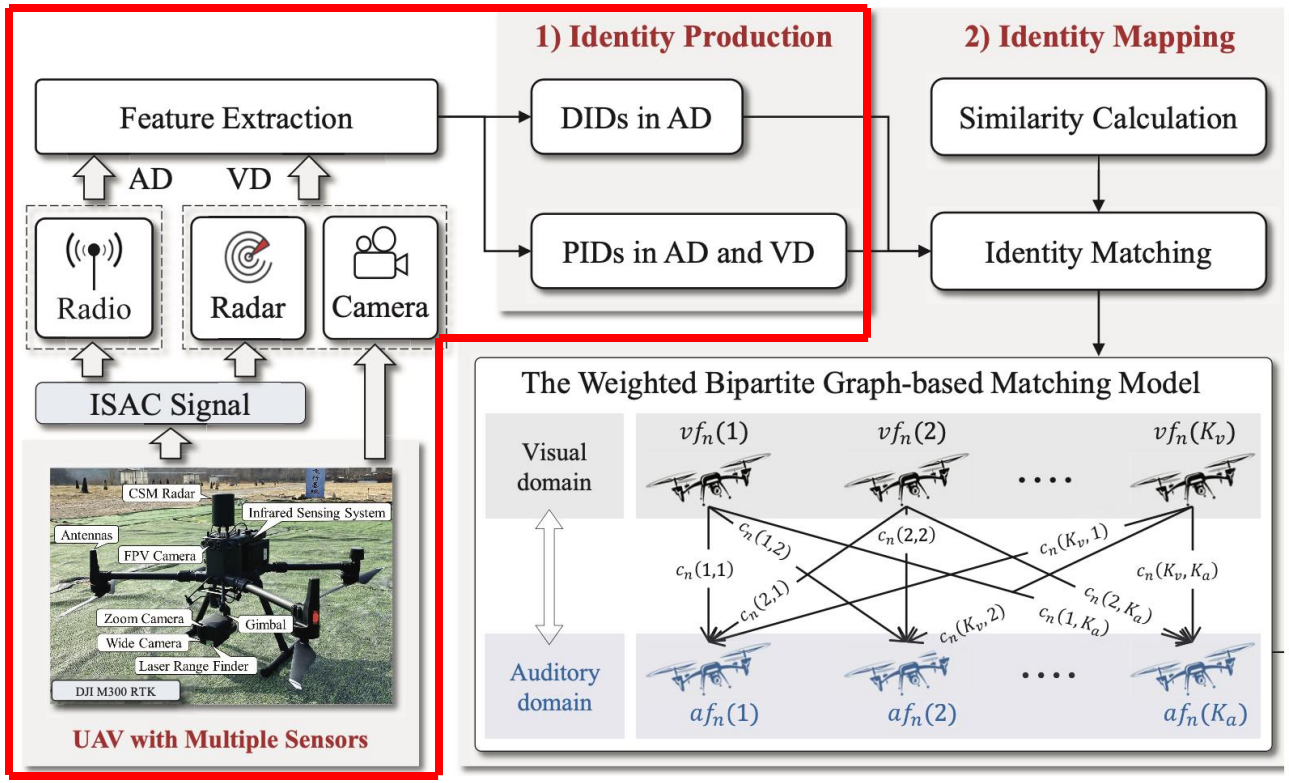
Solution Structure

> Identity Production Module

- Receive information from AD & VD

- Based on the echoes from the ISAC signal, the module can estimate PID
  - Matched-filtering of Doppler-shifted echo
  - Micro-Doppler frequency
- Physical attributes are dynamically weighted
  → Valid for distinguishing the all types of UAVs

- DIDs are only obtained from AD



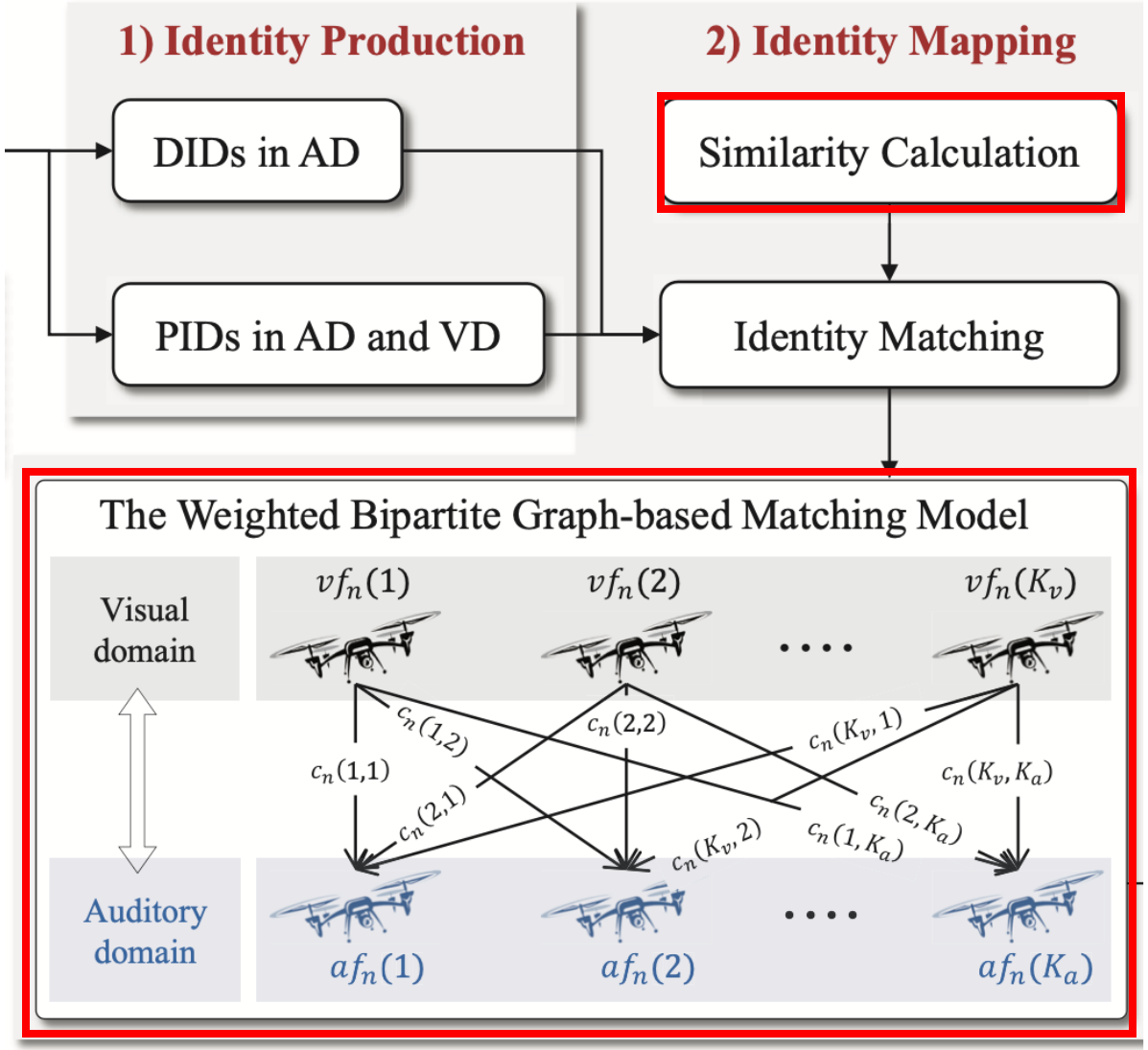
Solution Structure

> Identity Mapping Module

- Receive PID & DID from Identity Production Module

- Calculate the similarity between PID & DID and perform ID matching
- Matching cost $c_n(i,j)$
  - ith identity of VD
  - jth identity of AD

- Matching cost optimization
  - Hungarian algorithm
  - Vampire bat optimizer



Solution Structure

> Identity Management Module

- **In dynamic environment**, it is hard to ensure the accuracy of matching result
- Before the next AD information arrives,
  - Current PIDs from VD
  - Previous PID & DID from AD

- The Identity Management Module **estimates** the current AD information with previous AD information
  - NN or classical Kalman filter
  - Joint probabilistic data association filter
  - Multiple hypothesis tracking

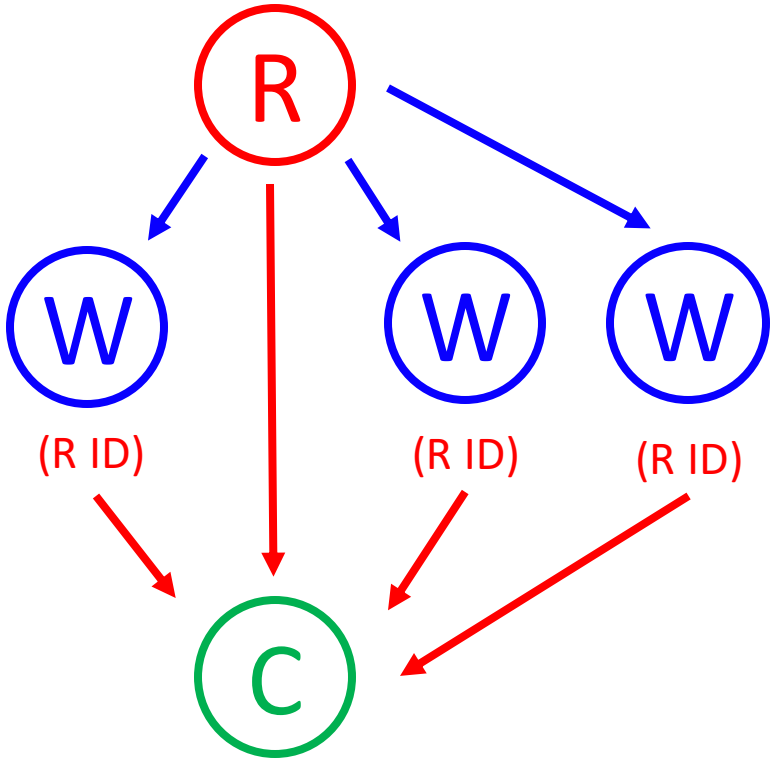
Solution Structure

> Identity Authentication Module

- Identity Authentication Module provides the trusted local and global identity
- Authentication Roles
  - Requestor
  - Witness
  - Certifier

- Performing the **minimum mean-square error for Witness and Requestor**

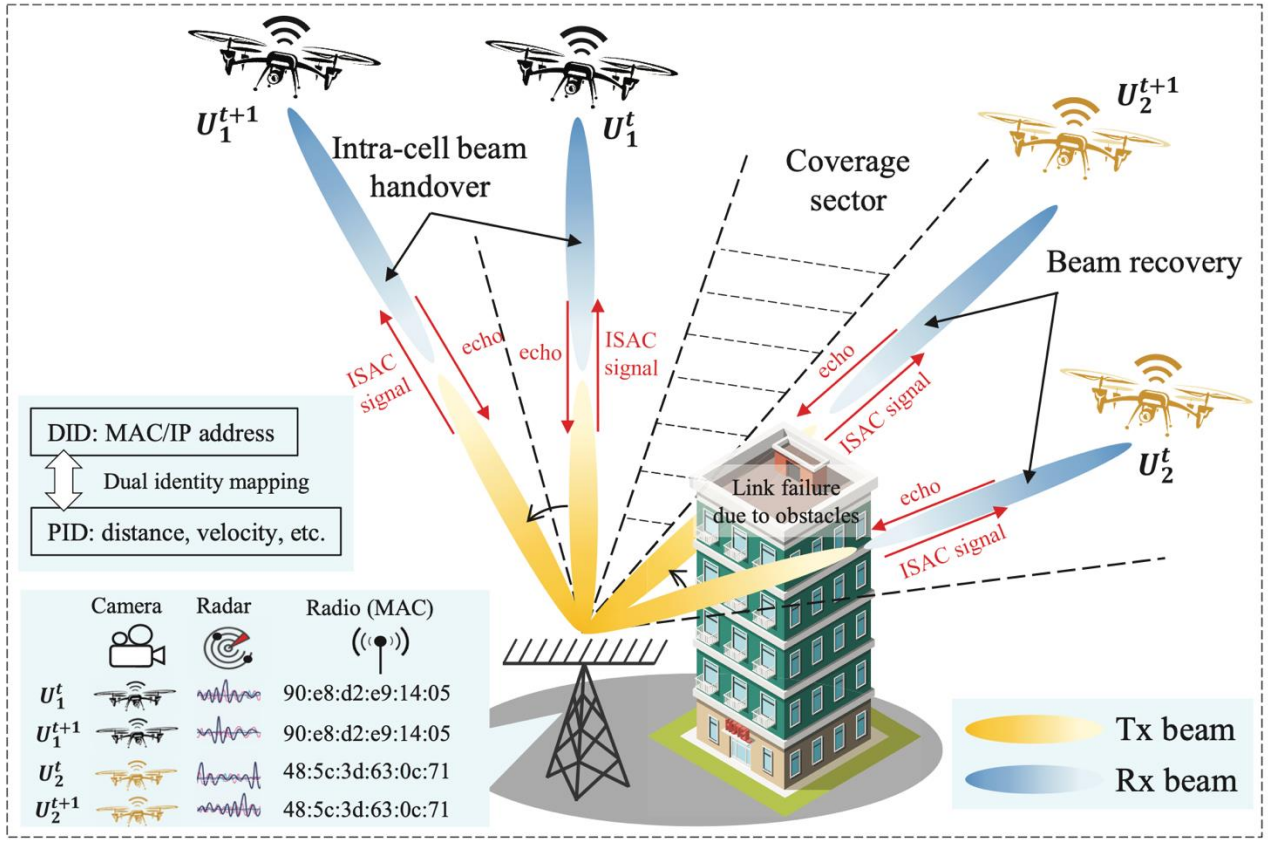
- Maximum common sub-graph also can be used to detect the malicious node



Scenario and Advantage

> Low-Latency Beam Management

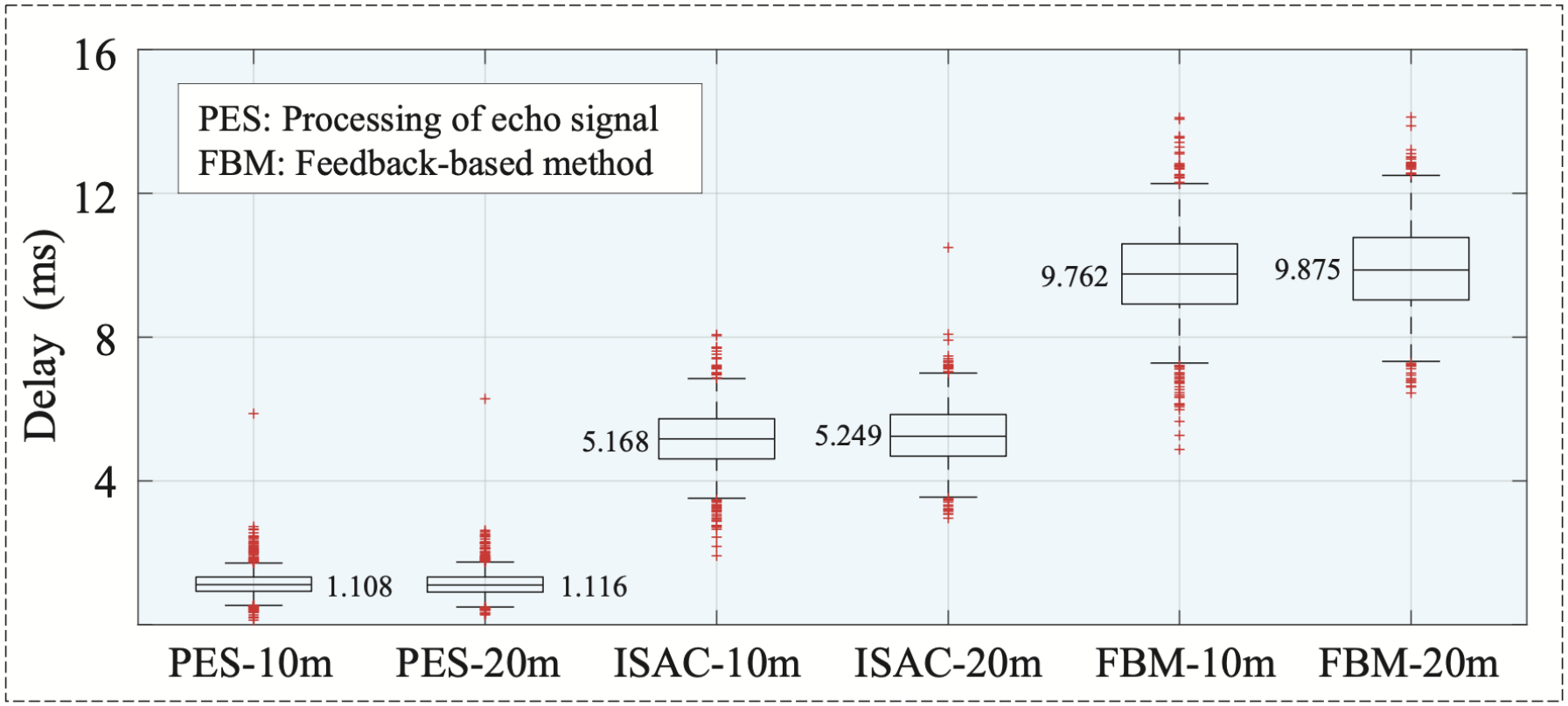
- It is essential that the **BSs quickly find the optimal beam direction** for the UAV
- By **DID to PID mapping**, the BSs can perform a **rapid** beam alignment



Scenario and Advantage

> Low-Latency Beam Management

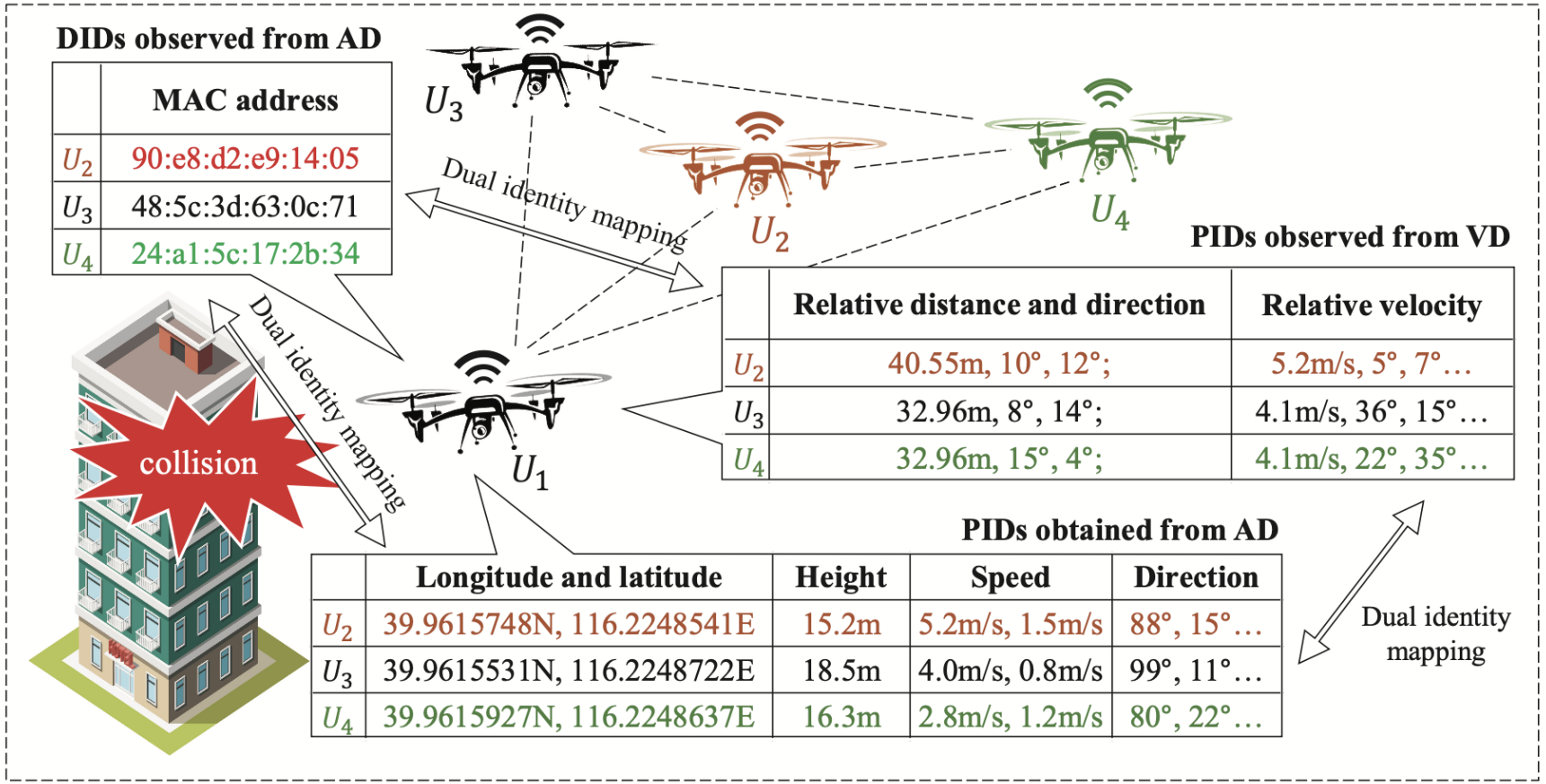
- Reduced communication delay about 4.6ms
- The echo signal processing delay is negligible at about 1ms



Scenario and Advantage

> Swift Transmission of Emergency Messages

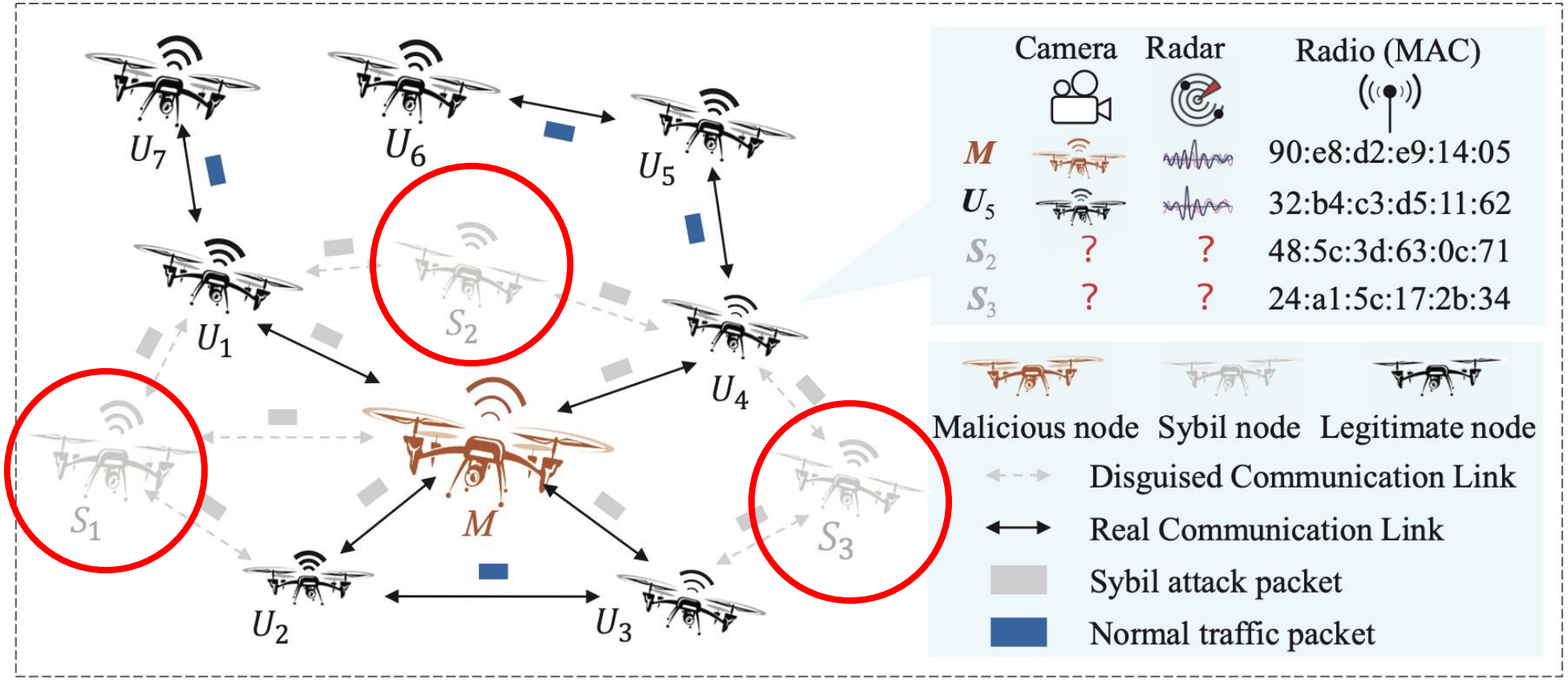
- Traditional broadcasting alert system can cause issues on unintended nodes
- By **PID to DID mapping**, the UAV can deliver the alert to a specific DID



Scenario and Advantage

> Trusted Networking Under Sybil Attack

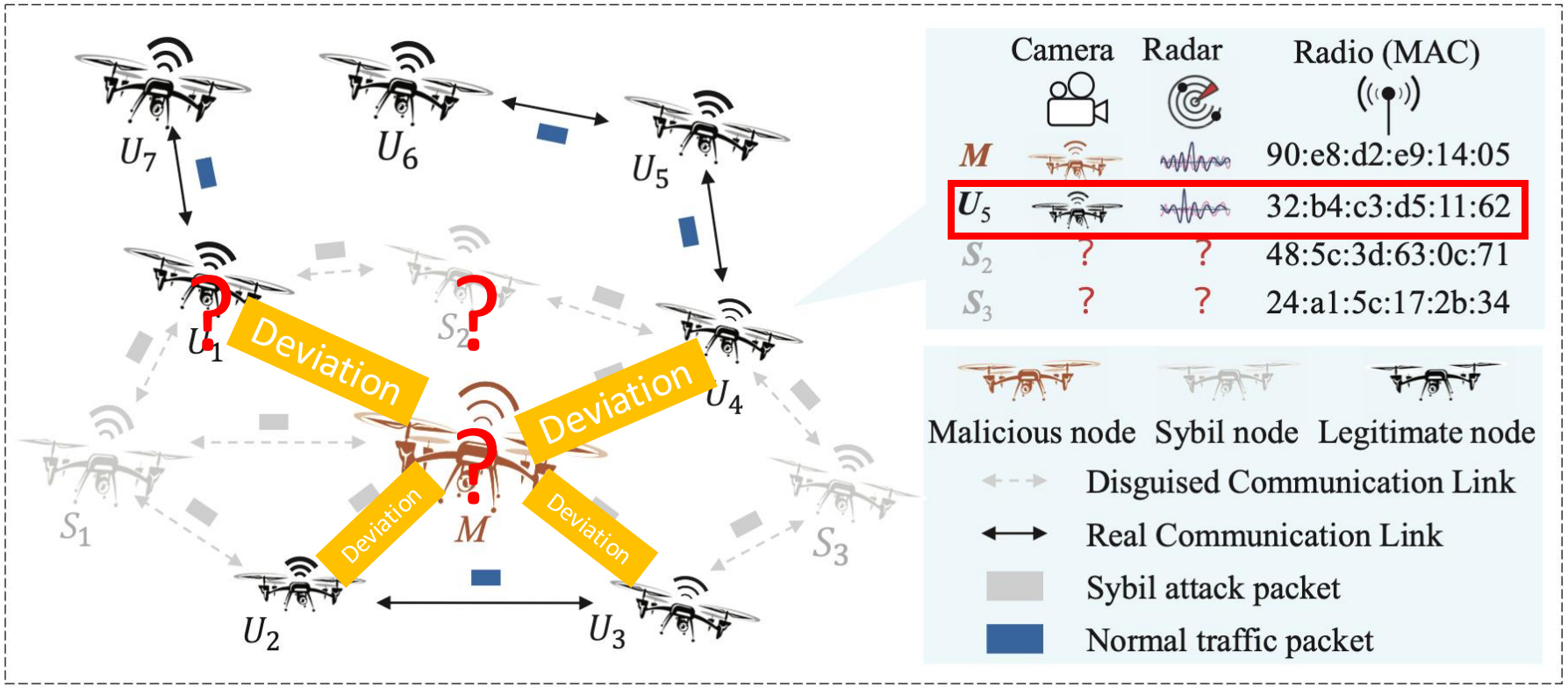
- Sybil Attack
  - A single entity **creates multiple fake identities** on a network
  - Use fake identities to manipulate consensus, distort certain information, etc.



Scenario and Advantage

> Trusted Networking Under Sybil Attack

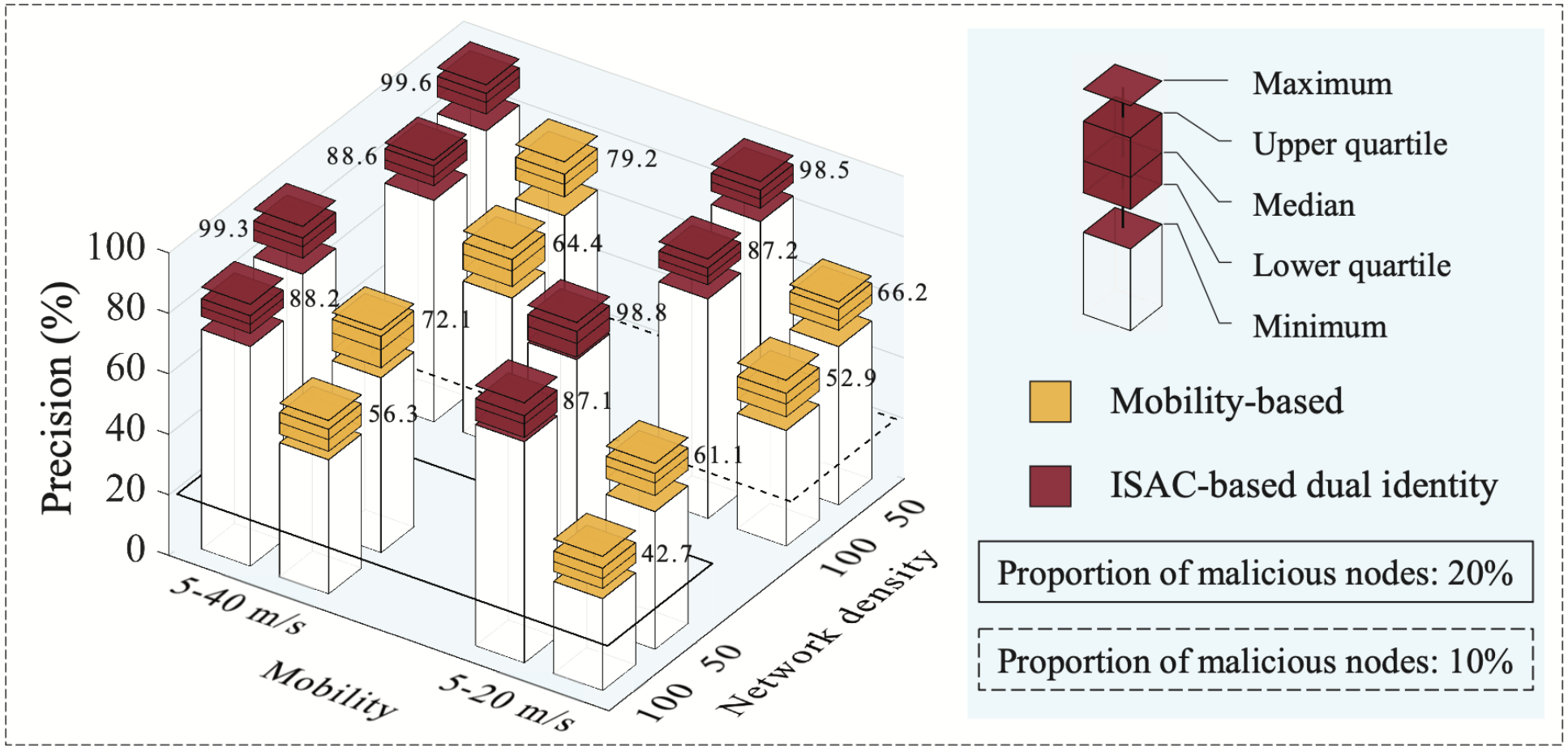
- By PIDs from VD, we know the existence of malicious node
- However, we don't know which one is the actual malicious one
- By **PID to DID mapping**, the UAV can easily distinguish the malicious node



Scenario and Advantage

> Trusted Networking Under Sybil Attack

- Achieved higher precision for various mobility settings and network density



Conclusion

- ISAC technology is essential for UAV networks and 6G communication
- ISAC-Enabled Dual Identity Solution improves the reliability and security of the UAV network
- Specifically, the solution is effective for managing beam alignment and emergency message delivery
- It also raises authentication level for the entire UAV network

- The authors showed the usefulness of ISAC for UAV networks, and it was meaningful point to cover form a security and authentication perspective
- However, ISAC can be vulnerable, so it’s important to consider the security of the ISAC itself