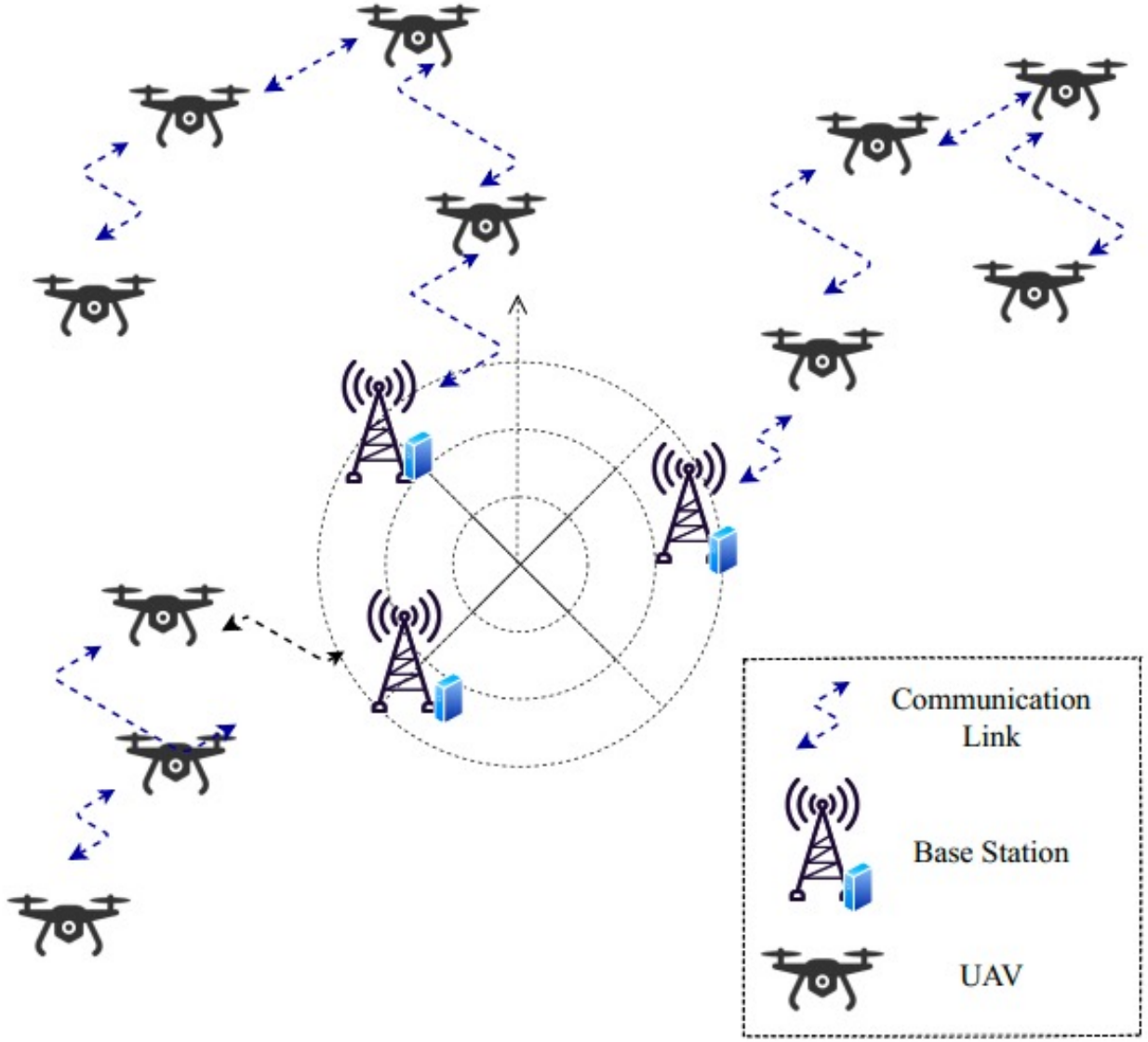
Secure and Trusted Attestation Protocol for UAV Fleets

Gaurang Bansal and Biplab Sikdar
Department of Electrical and Computer Engineering
National University of Singapore

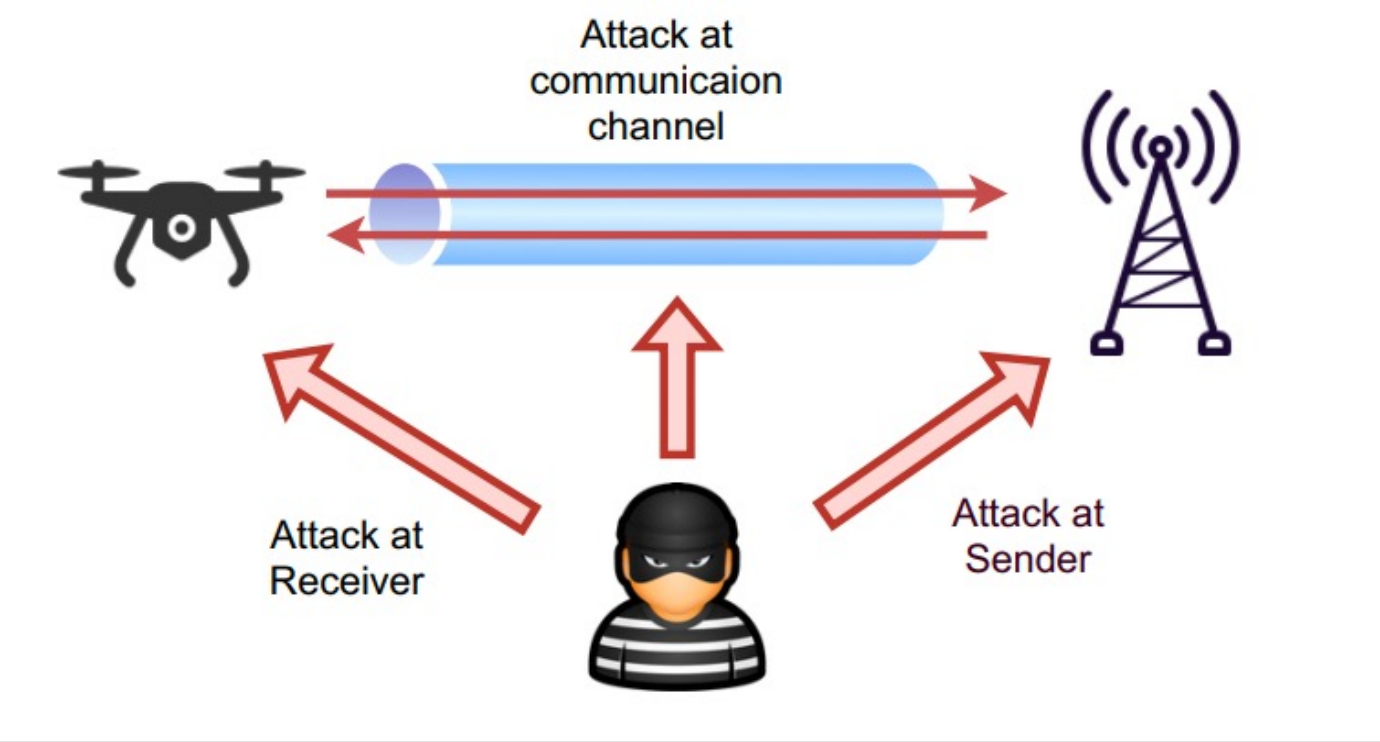
Unmanned Aerial Vehicles (UAVs)

- Small aerial devices
- No pilot required
- Wide range of applications.
  - Medical surveillance in natural disasters
  - traffic monitoring
  - military operations
  - delivery services
  - task offloading

System Model



Threats



- UAV communication's reliance on wireless channels makes it prone to many active attacks such as replay attacks, man-in-the-middle attacks.
- UAVs are located closer to the users; thus, they are more vulnerable to physical attack.

Attack Model

- Attacker can **hear all the unencrypted communication** between the receiver and the sender.
- An adversary has the **ability to masquerade** as a legitimate UAV
- Attacker **can tamper** with the ongoing message exchanges.
- An attacker **may try to eavesdrop** on the transmitted messages, modify these messages, or replay them in the network.
- The attacker can **also capture any UAV**, disrupt any communication, and use brute force computation to decrypt any secret information.

Action speaks louder than words

Authentication and Attestation

Design Goals

1. An UAV and the base station should be able to authenticate each other **successfully mutual**.
2. The base station must be able to identify if the **conversation is happening with an uncompromised legitimate UAV or not**.
3. If the **communicated messages are tampered** with, the receiver (either base station or UAV) must be able to detect the tampering and abort the authentication process
4. **The protocol must be secure against security threats** like replay attacks, masquerade attacks, and man-in-the-middle attacks.
5. A **unique session key** must be generated for each authentication session. There must not exist any other way to generate this session key
6. As the **attacker can physically capture or damage** the UAV, the protocol must be safe against cloning attacks as well as physical attacks

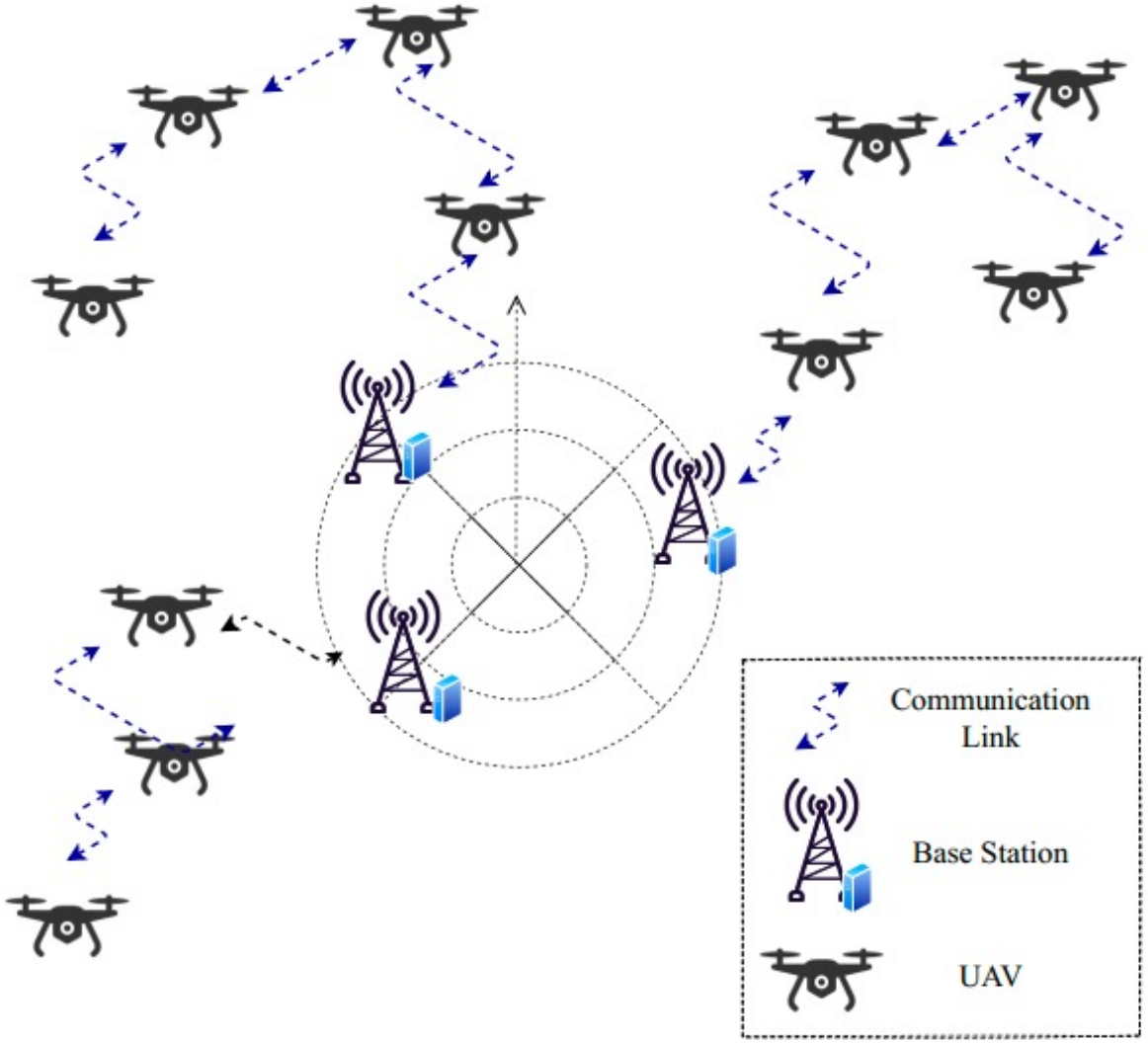
Issues with previous works

- Highly complex
- Computationally intensive
- One-one authentication
- Can’t scale
- Does not handle physical attacks

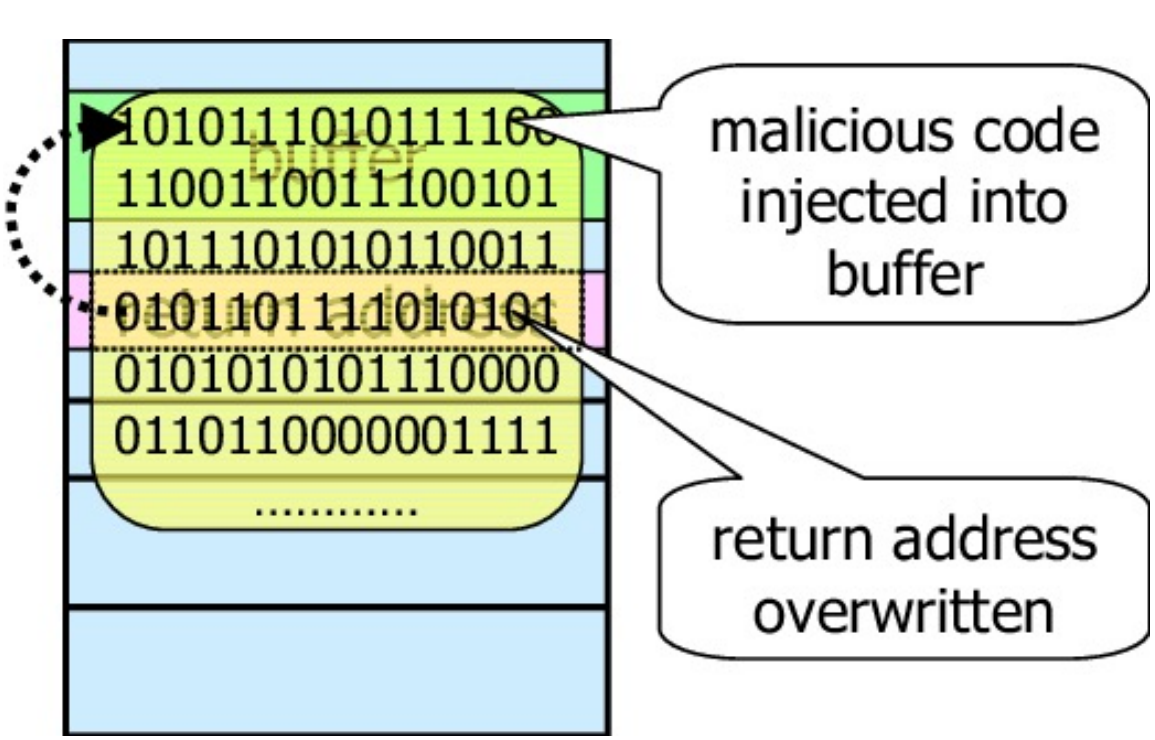
What we propose?

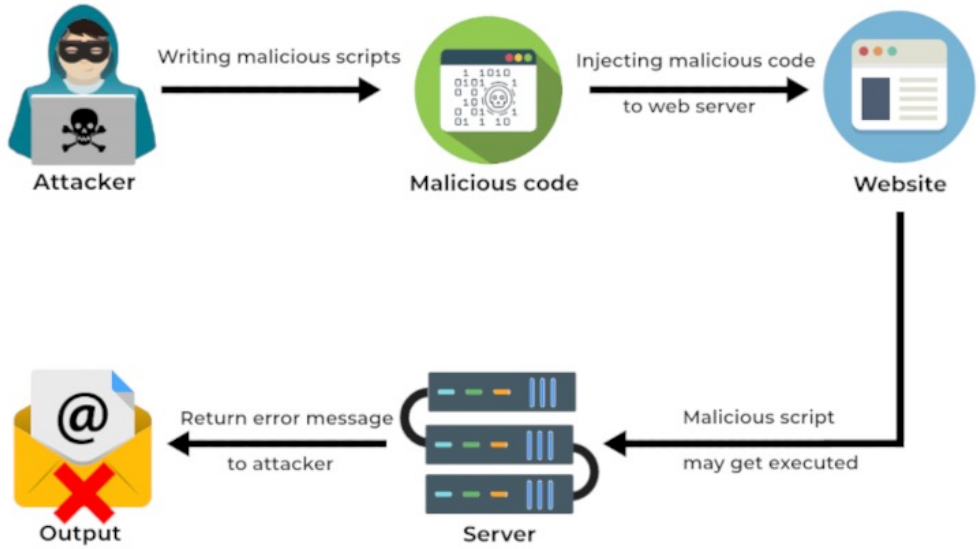
Lightweight authentication and attestation protocol

How?

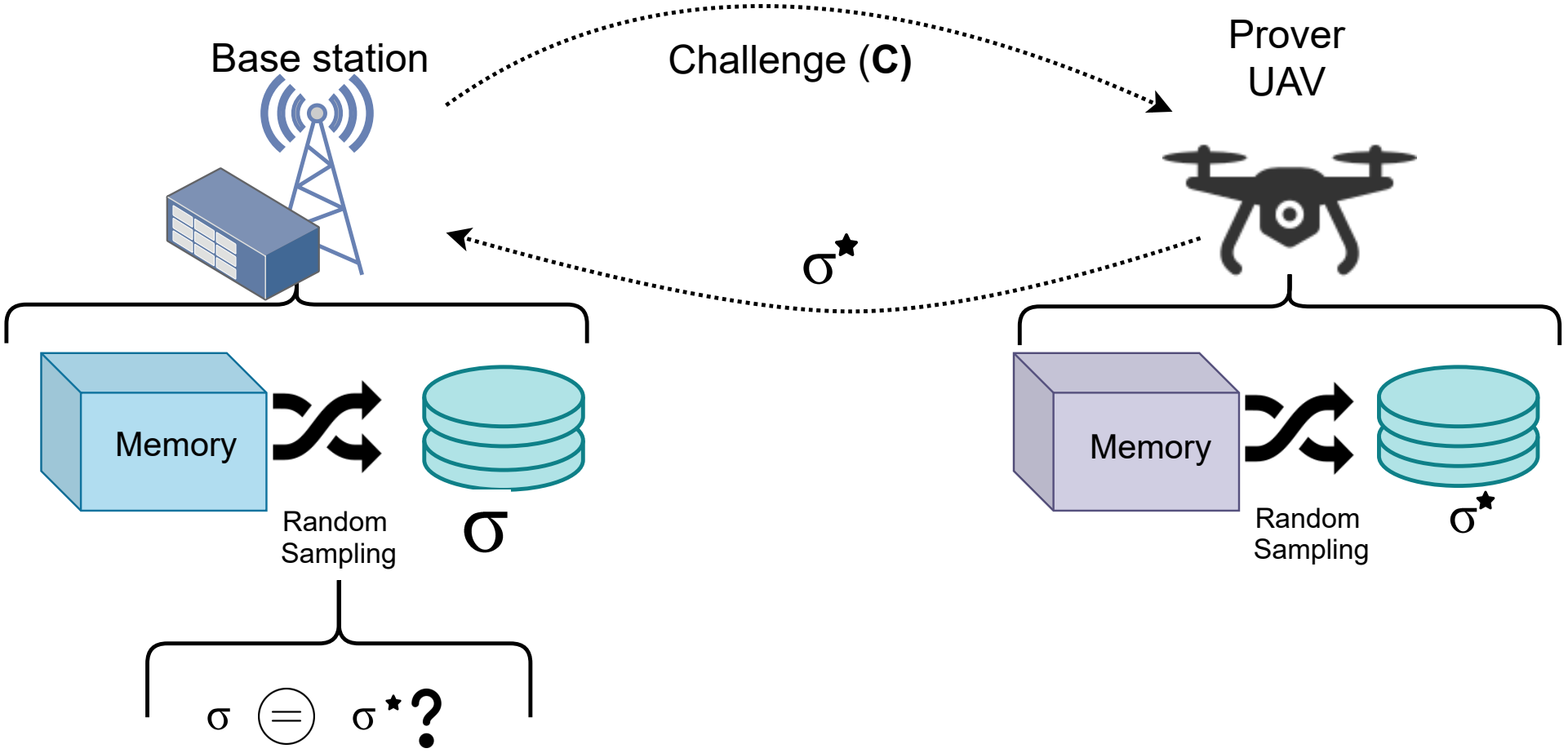


Malacious code Injection

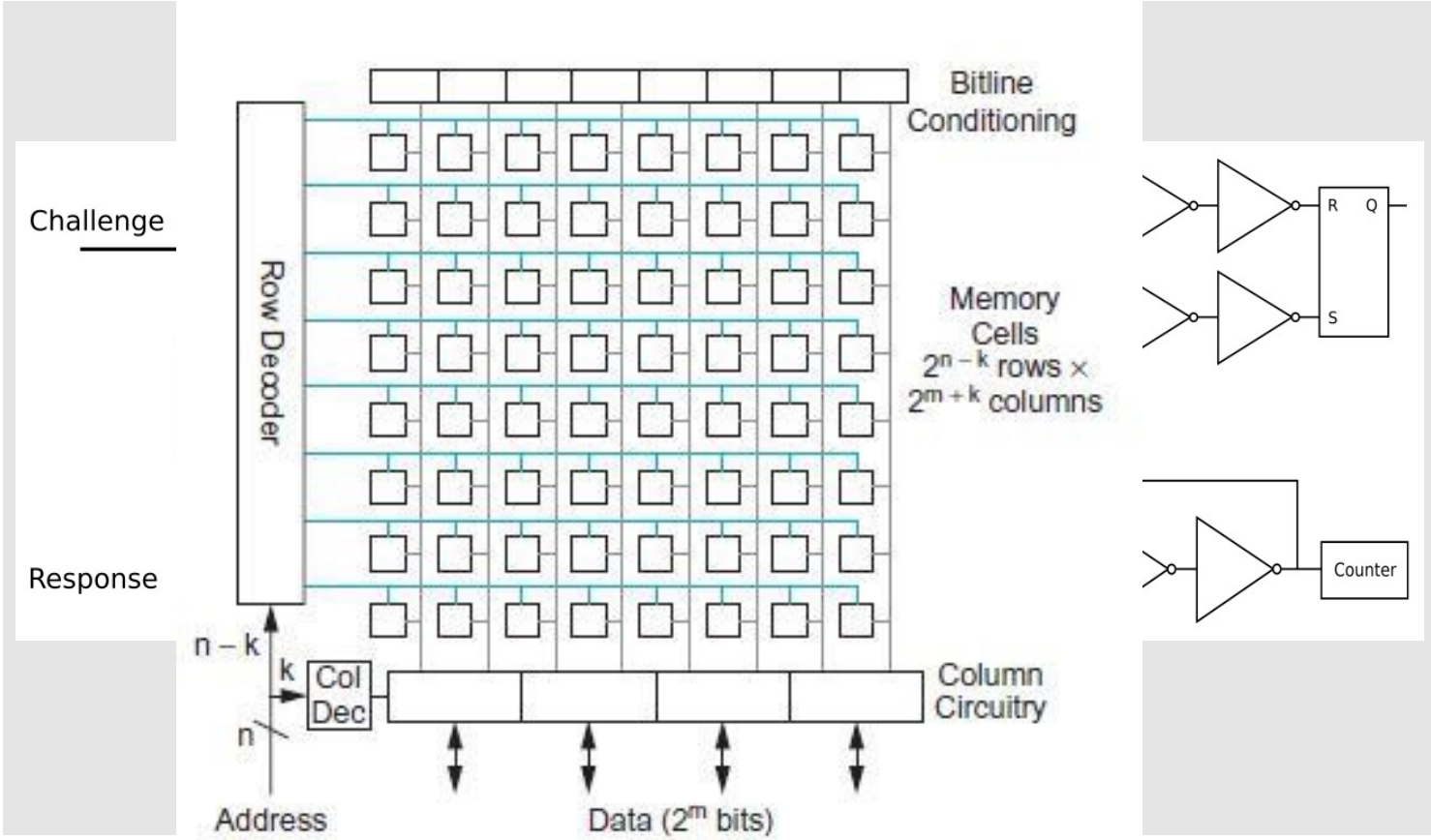




Attestation

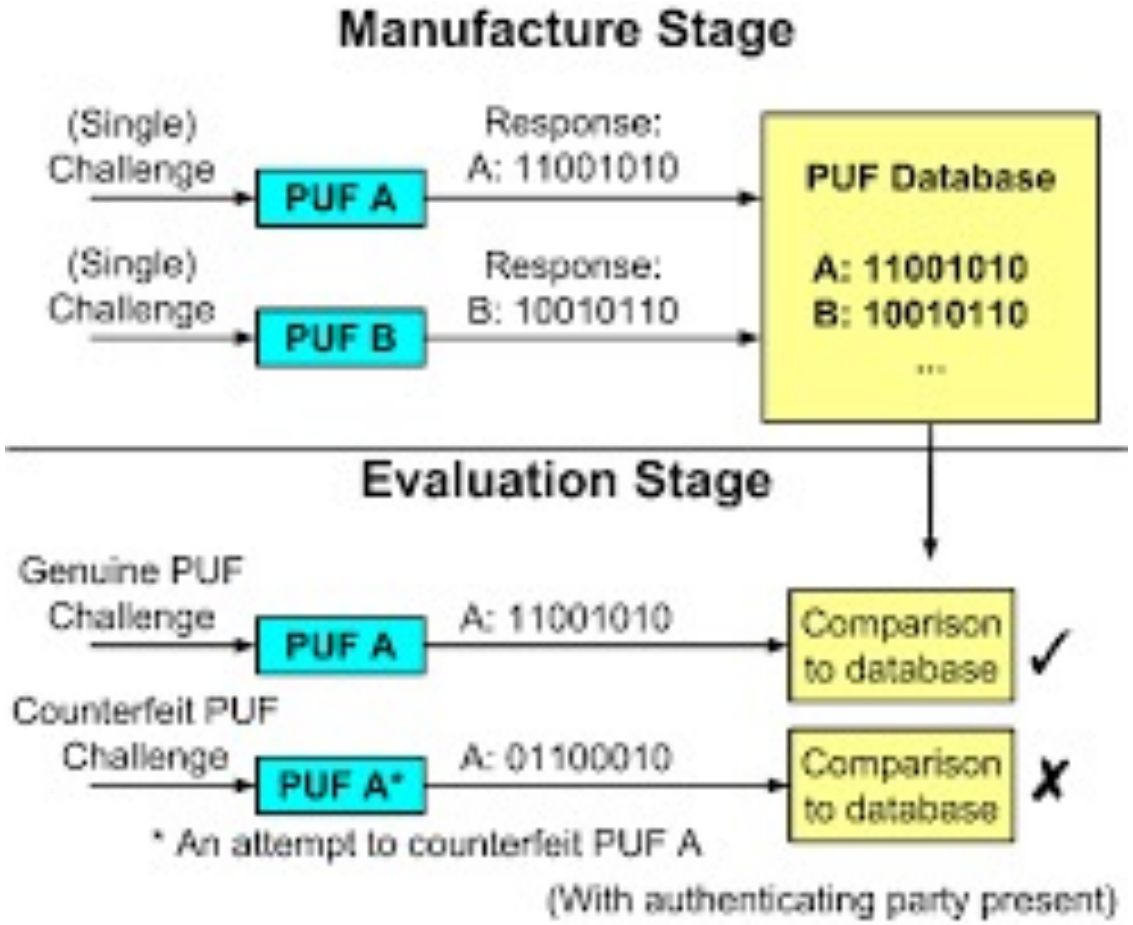


PUFs

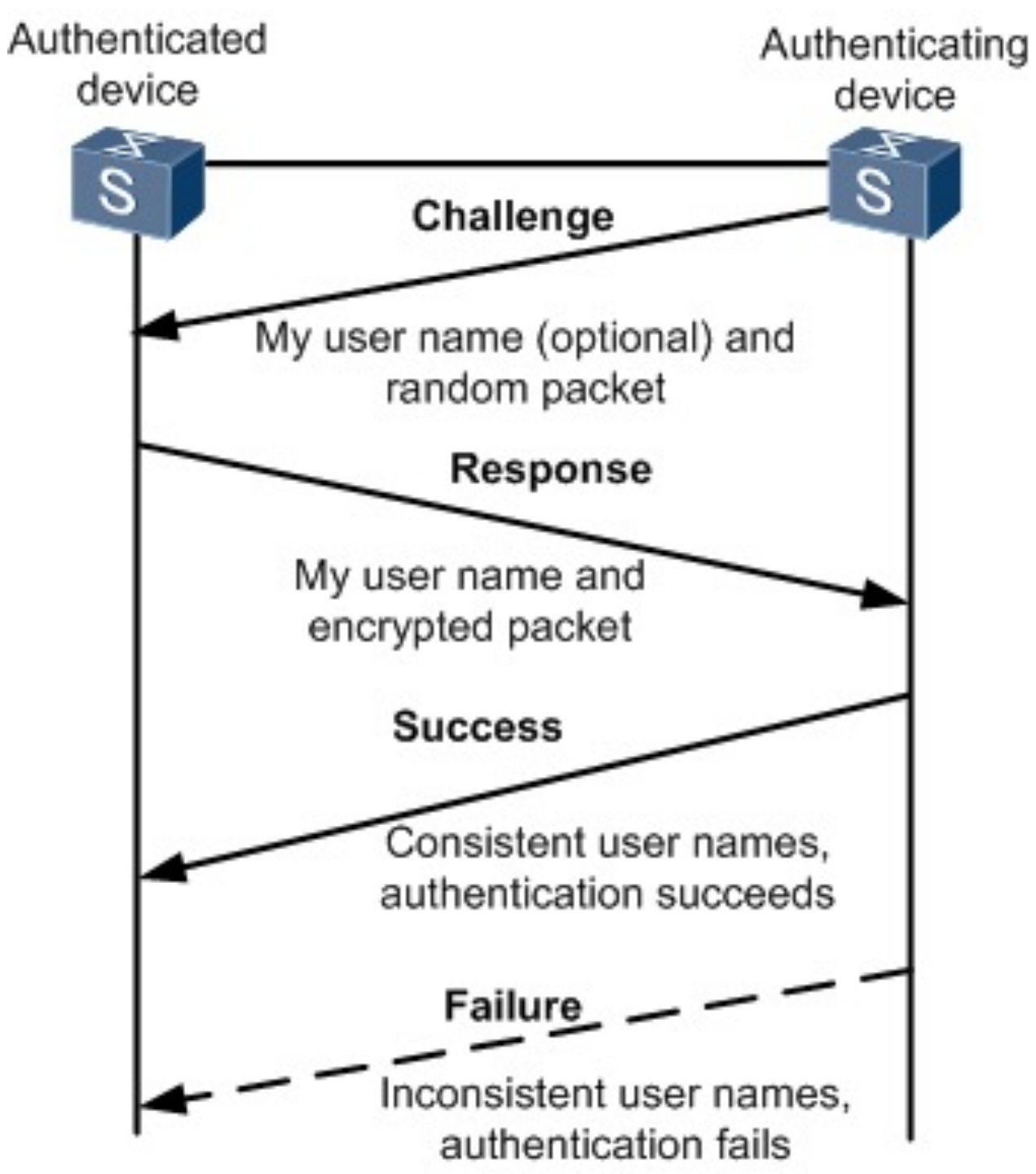


- Physical unclonable functions can be considered as digital fingerprints of integral circuits.
- PUFs exploits the inherent randomness that is unique to a device and cannot be cloned or forged.
- This intrinsic randomness is generated during the fabrication of the chip.
- A PUF can be modeled as R $=$ PUF(C), where the PUF uses its internal characteristics to map a challenge C to response R.

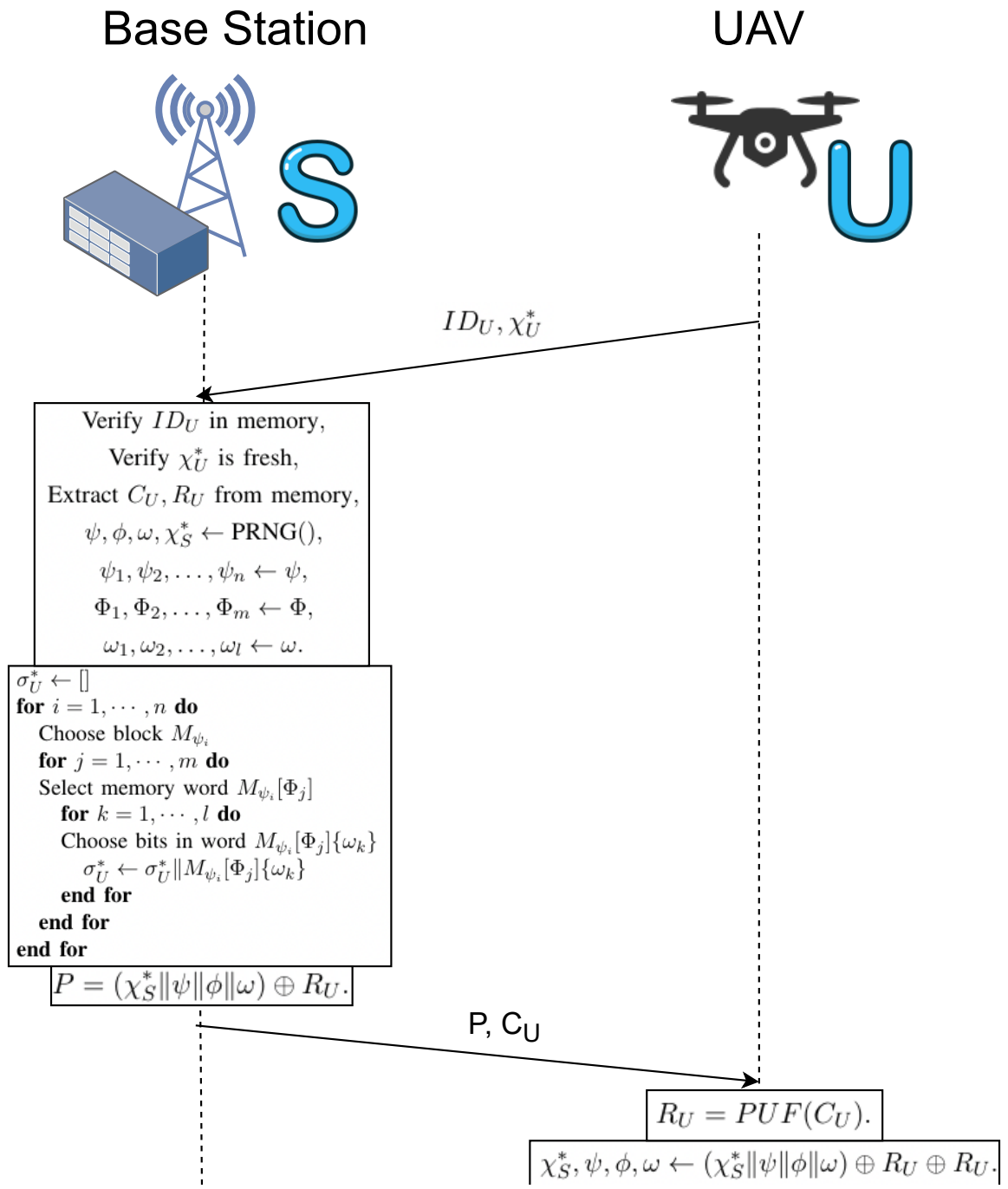
PUF Working


Manufacture Stage
(Single) Challenge
PUF A
Response: A: 11001010
(Single) Challenge
PUF B
Response: B: 10010110
PUF Database
A: 11001010
B: 10010110
...
Evaluation Stage
Genuine PUF Challenge
PUF A
A: 11001010
Comparison to database
✓
Counterfeit PUF Challenge
PUF A*
A: 01100010
Comparison to database
✗
* An attempt to counterfeit PUF A
(With authenticating party present)

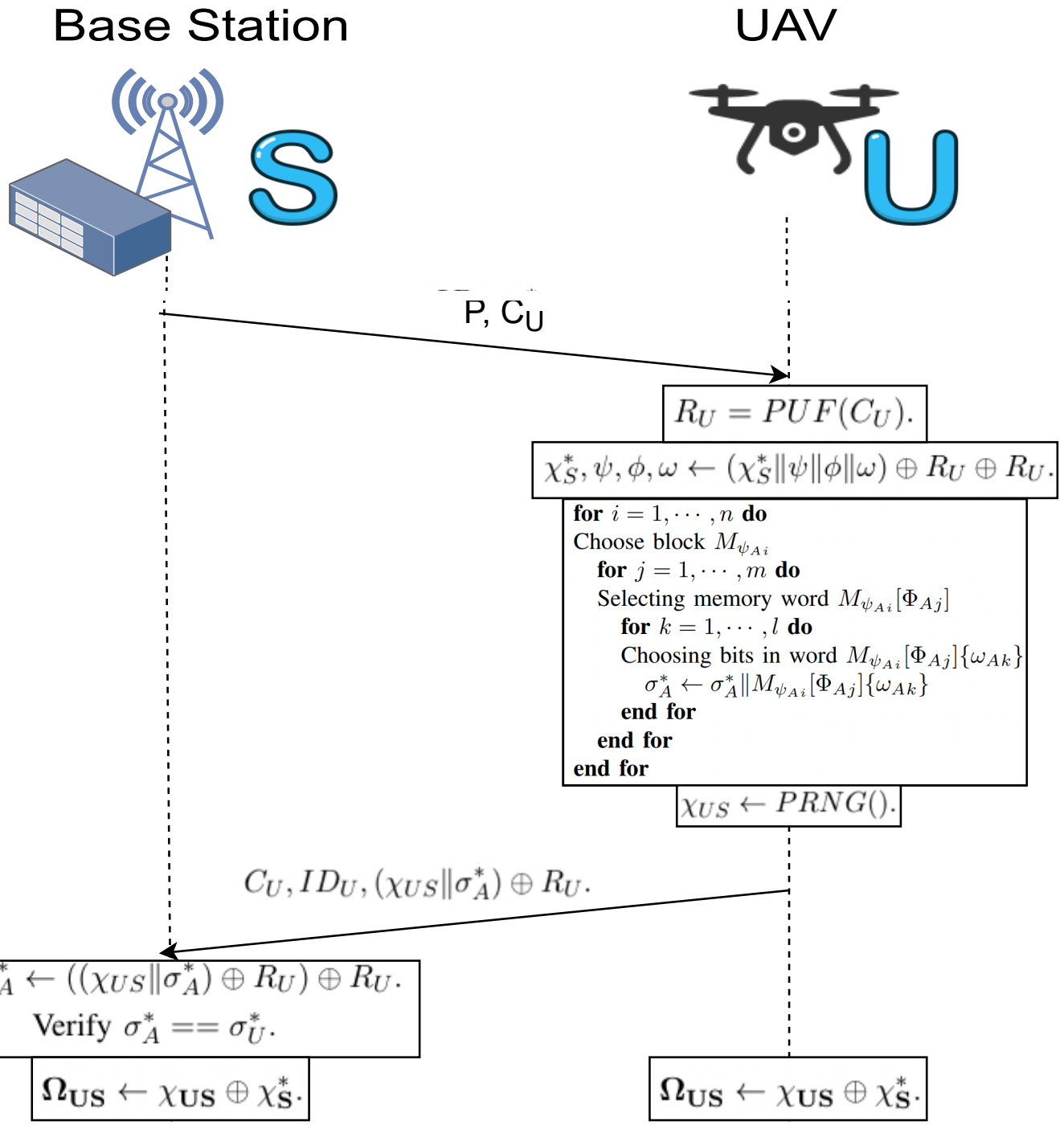
Overview of Protocol



Actual Protocol

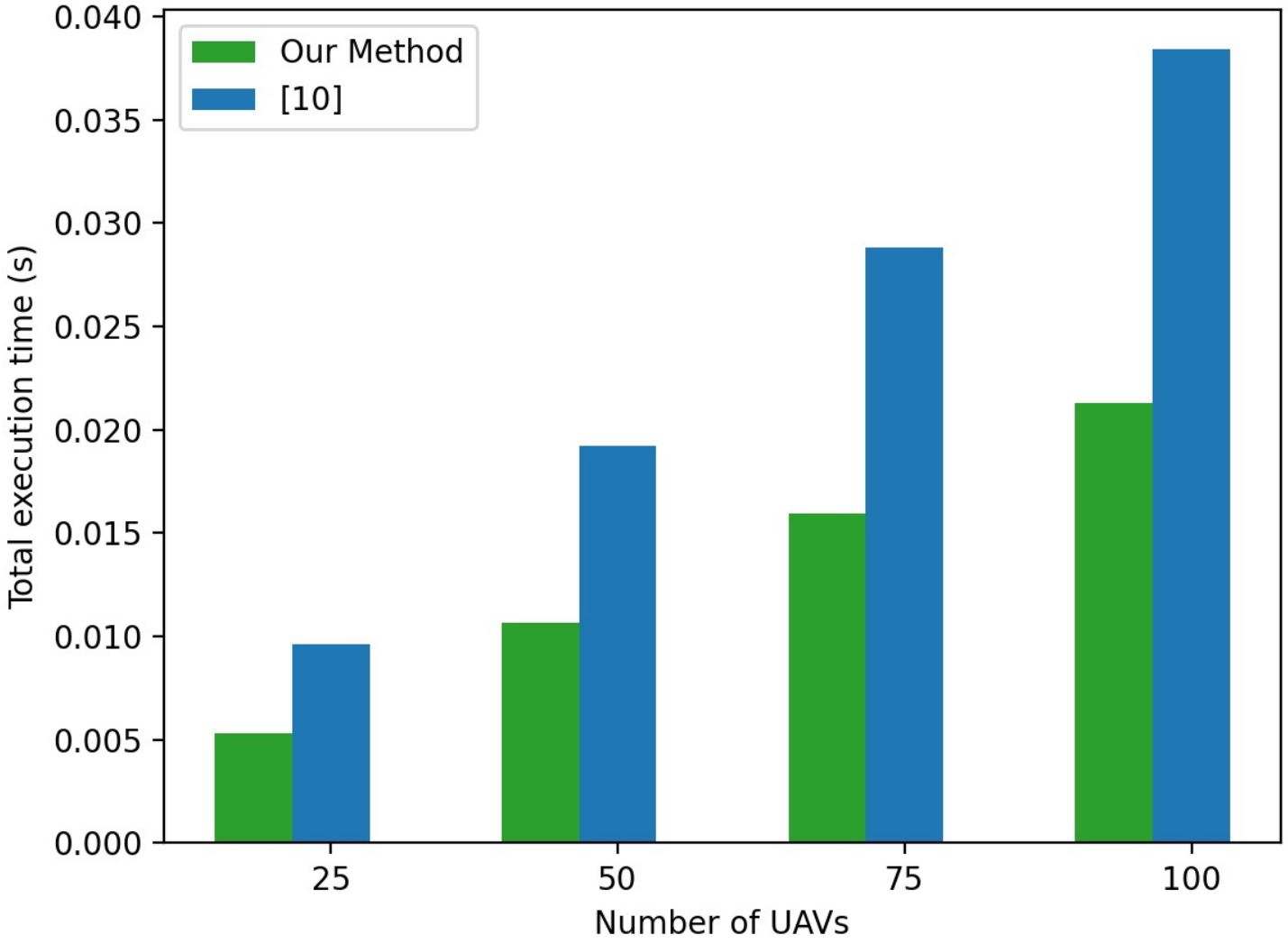


Actual Protocol



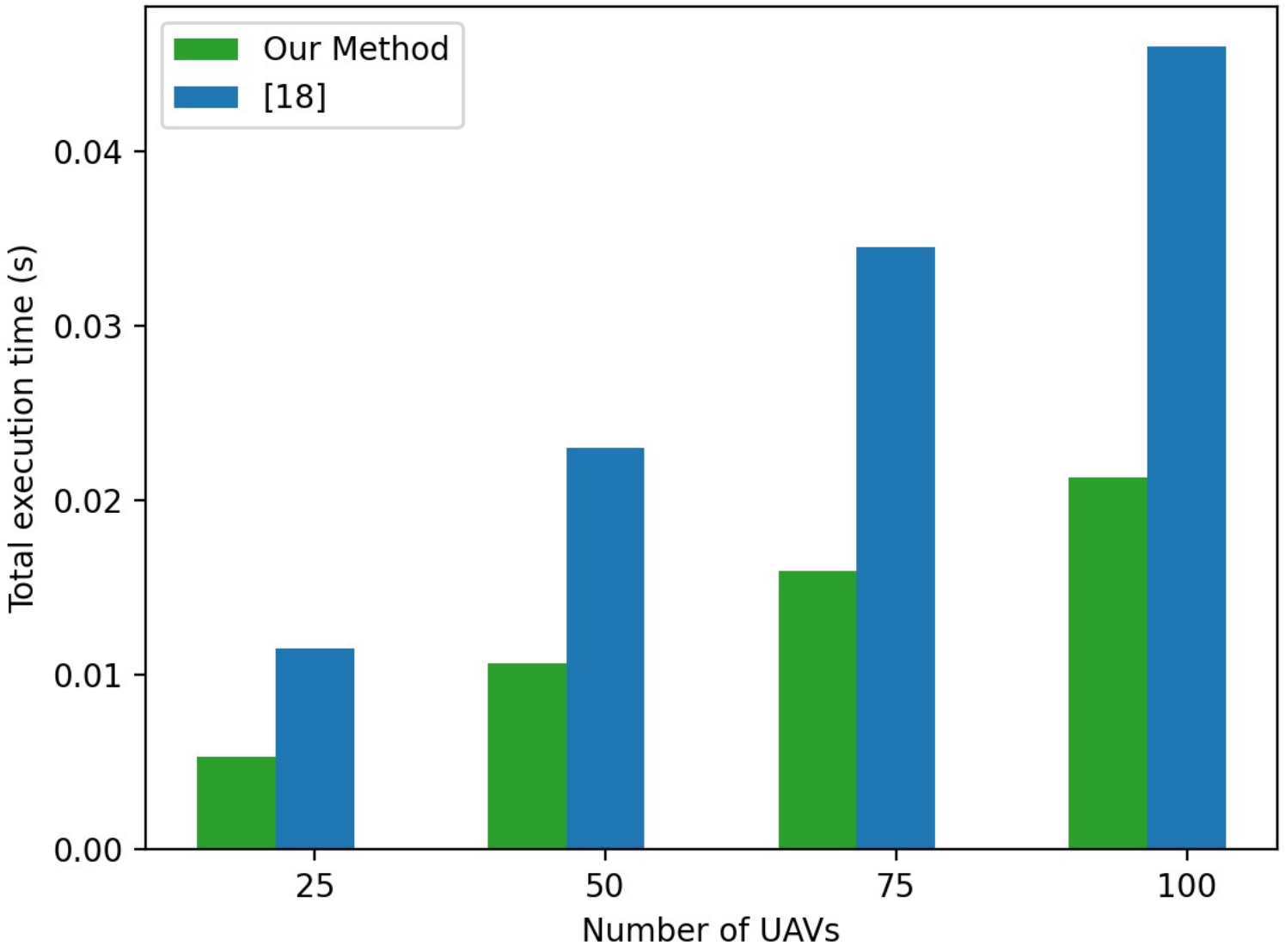
Results

Time taken (in sec) for 10 iterations of protocols.



Results

Time taken (in sec) for 10 iterations of protocols.




Questions!!!

Thank You..