



Anonymous Remote Identification of Unmanned Aerial Vehicles

**College of Science and Engineering (CSE), Hamad Bin Khalifa University (HBKU), Doha, Qatar*

+Eindhoven University of Technology, Eindhoven, Netherlands

Pietro Tedeschi*, Savio Sciancalepore⁺, Roberto Di Pietro*



ACSAC 2021, December 6-10, 2021, Online

Agenda



UAV Security and Privacy

Background on UAVs, Security and Privacy Issues



FAA Remote Identification Rule

Remote Identification *aka* RemoteID



Scenario and Adversarial Model

What we assumed for our scenario and for the adversary capabilities



Anonymous Remote IDentification

Our proposed framework: ARID



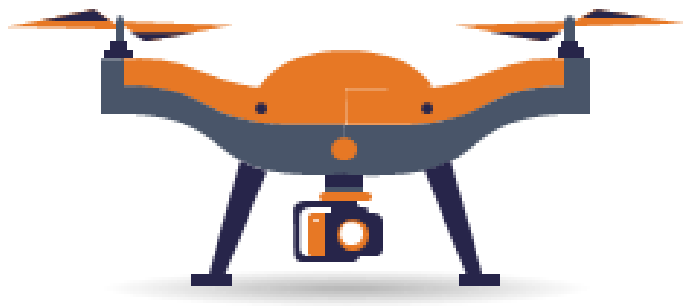
Security Analysis & Performance Evaluation

Security features offered by ARID and its performance assessment.



Conclusion and Future Work

What we offered and what are the future ARID extensions



THE NEW FLYING IOT

Background - UAVs and Drones

1

The new Market

UAVs are becoming enabling technology for several applications including monitoring, surveillance and shipping.

Market size is currently valued at \$5.80 billion

Compound annual growth rate (CAGR) of 56.5% up to the 2025

2

The Features

Exploit the Wi-Fi bands (2.4GHz - 5GHz) or 4G-LTE/5G

Navigation relies on GNSS technologies (GPS, Galileo, ...)

Limited battery lifetime

Capability to perform missions autonomously

3

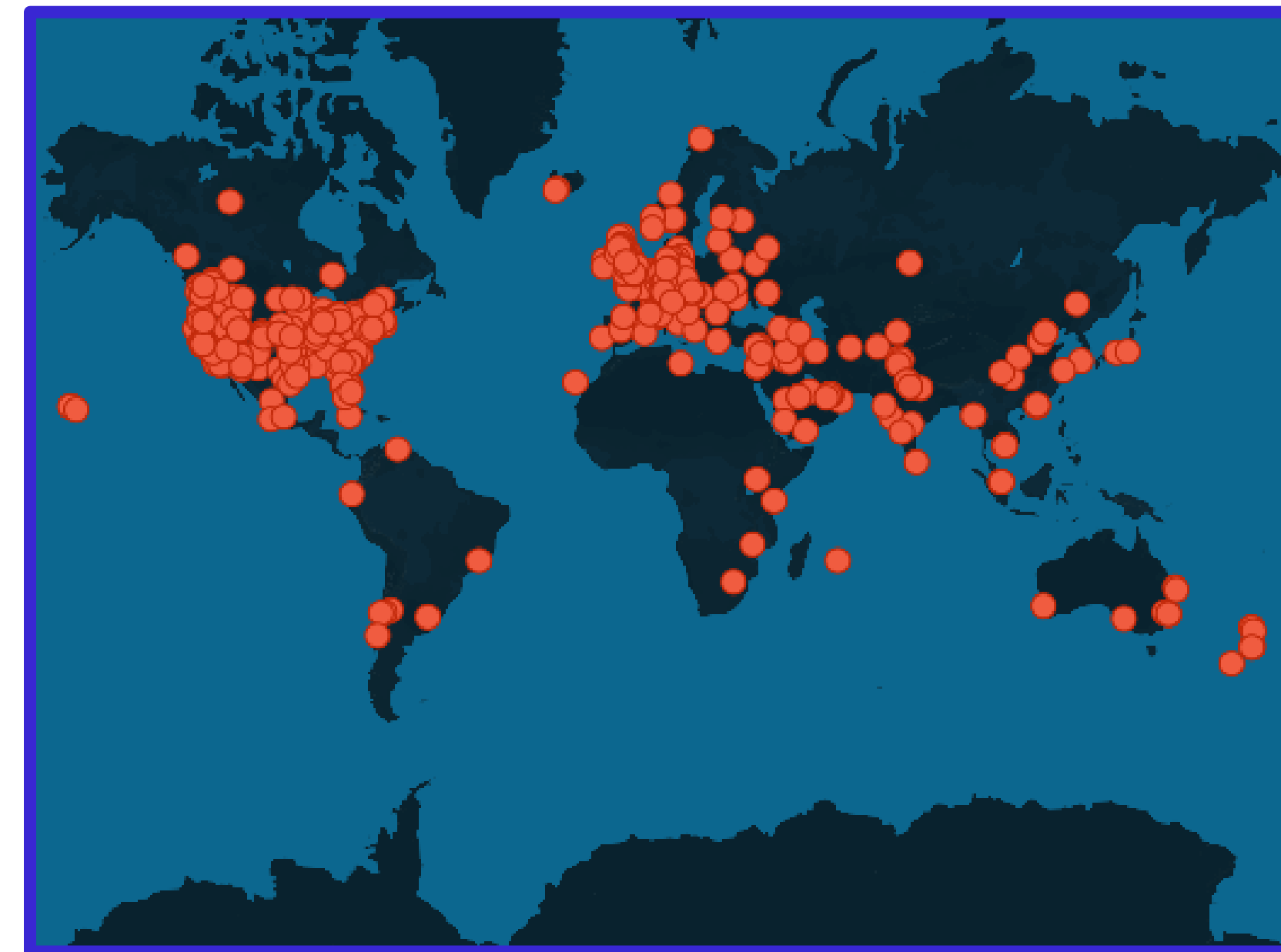
IoT can fly ...

Flying constrained devices (UAVs as the new "Flying IoT")



Worldwide Drone Incidents

- Police and air traffic control intervene after drone spotted at Newcastle – Stadiums - Newcastle, United Kingdom - October 8, 2021
- Criminals Use Drones to Drop 5 Liters of Flammable Liquid - Law Enforcement/First Responders - October 1, 2021
- Drone crashes into Leaning Tower of Pisa - Private/Non-Corporate - Pisa, Italy - September 28, 2021
- Drone spies on private home - Private/Non-Corporate - Albringhausen, Germany - July 11, 2021 ...



SOURCE: [HTTPS://WWW.DEDRONE.COM/](https://www.dedrone.com/)

FAA Remote Identification Rule

US-based **Federal Aviation Administration**(FAA) recently published a new dedicated regulation, namely *RemoteID*

- To enable enhanced accountability of Unmanned Aerial Vehicles(UAVs) operations
- It forces all UAVs operators to broadcast messages reporting their identity, location (GPS position), and information about ground station
- *RemoteID* does not specify how to generate such identifiers, nor provide guidelines to operators for their design
- *RemoteID* regulations became effective on the 21st of April 2021, and UAV operators need to comply with this rule from September 2022



**Federal Aviation
Administration**
REMOTE ID RULE

According to the Remote ID specification, UAV must periodically broadcast messages containing at least the following information

Unique ID	Drone Latitude, Longitude, Altitude, Speed	GCS Latitude, Longitude, Altitude	Timestamp	Emergency Status
-----------	--	--	-----------	---------------------

Motivations



drone life

News Products Industries Enthusiasts Regulations

When Will Remote ID Go Into Effect? FAA Announces Date

Posted By: Miriam McNabb on: March 13, 2021



Nextgov

TRENDING // THE FIRST 100 DAYS // THE HACK // 5G // SPONSORED: APPLIED INTELLIGENCE // SPONSORED: ARTIFICIAL INTELLIGENCE // IT MODERN

FAA Delays Drone Remote ID Tracking, 'Operations Over People' Rules



AINonline

BIZAV AIR TRANSPORT DEFENSE EVENTS SUBS

READ AIN'S 2021 NBAA-BAACE CO

BUSINESS AVIATION

NBAA: Remote ID Drone Rule Raises Privacy Concerns

by Kerry Lynch - January 22, 2021, 10:19 AM



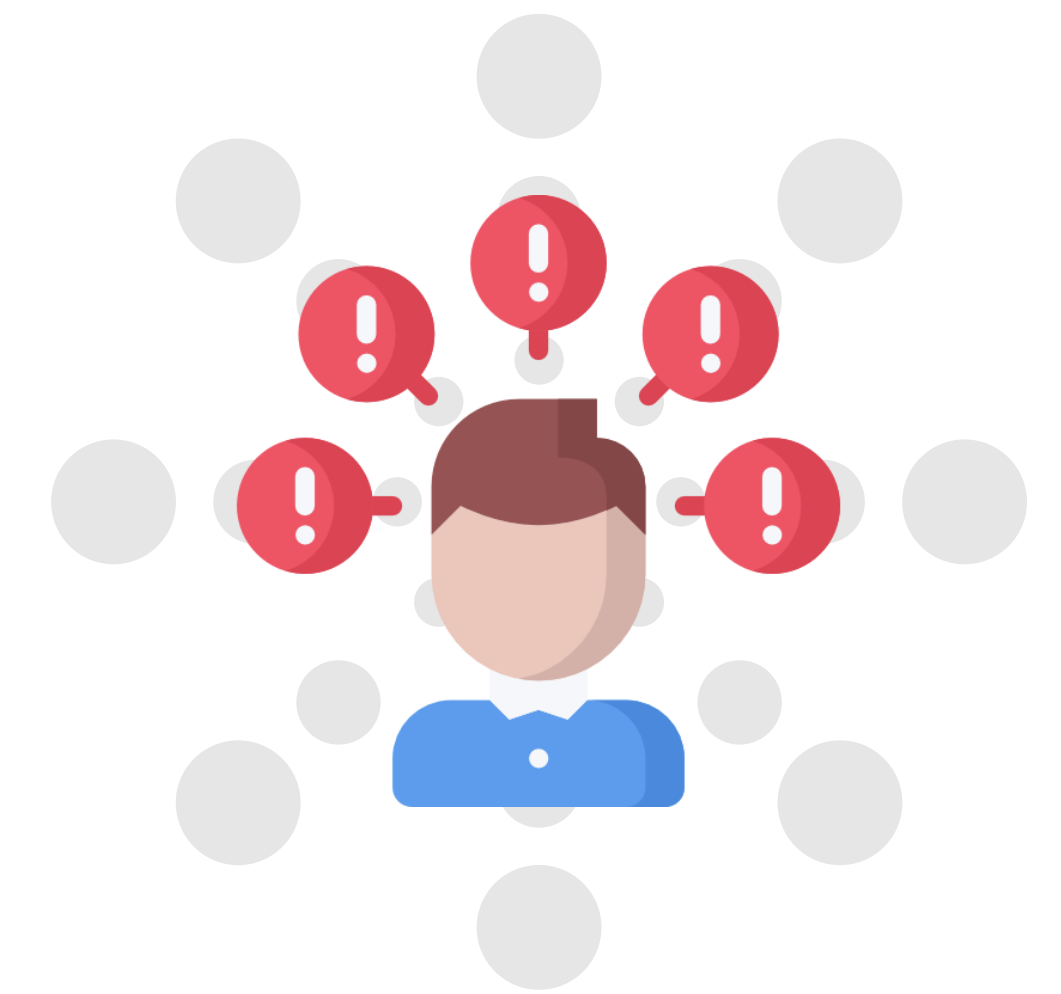
Privacy nightmare? FAA's drone tracking rules have big consequences

New rules require broadcast of information that could compromise delivery customers' privacy.

By Greg Nichols for Robotics | January 4, 2021 | Topic: Robotics

Cybersecurity Alert: FAA Releases New Rules Concerning Drone Use

Privacy Issue for Drone Operators



Drone Operators do not want to put privacy at risk

- Passive Tracking
- Privacy leakages for people (manufacturer, etc.)
- Operators want evidences for misbehaving drones

System and Security Requirements

Drones

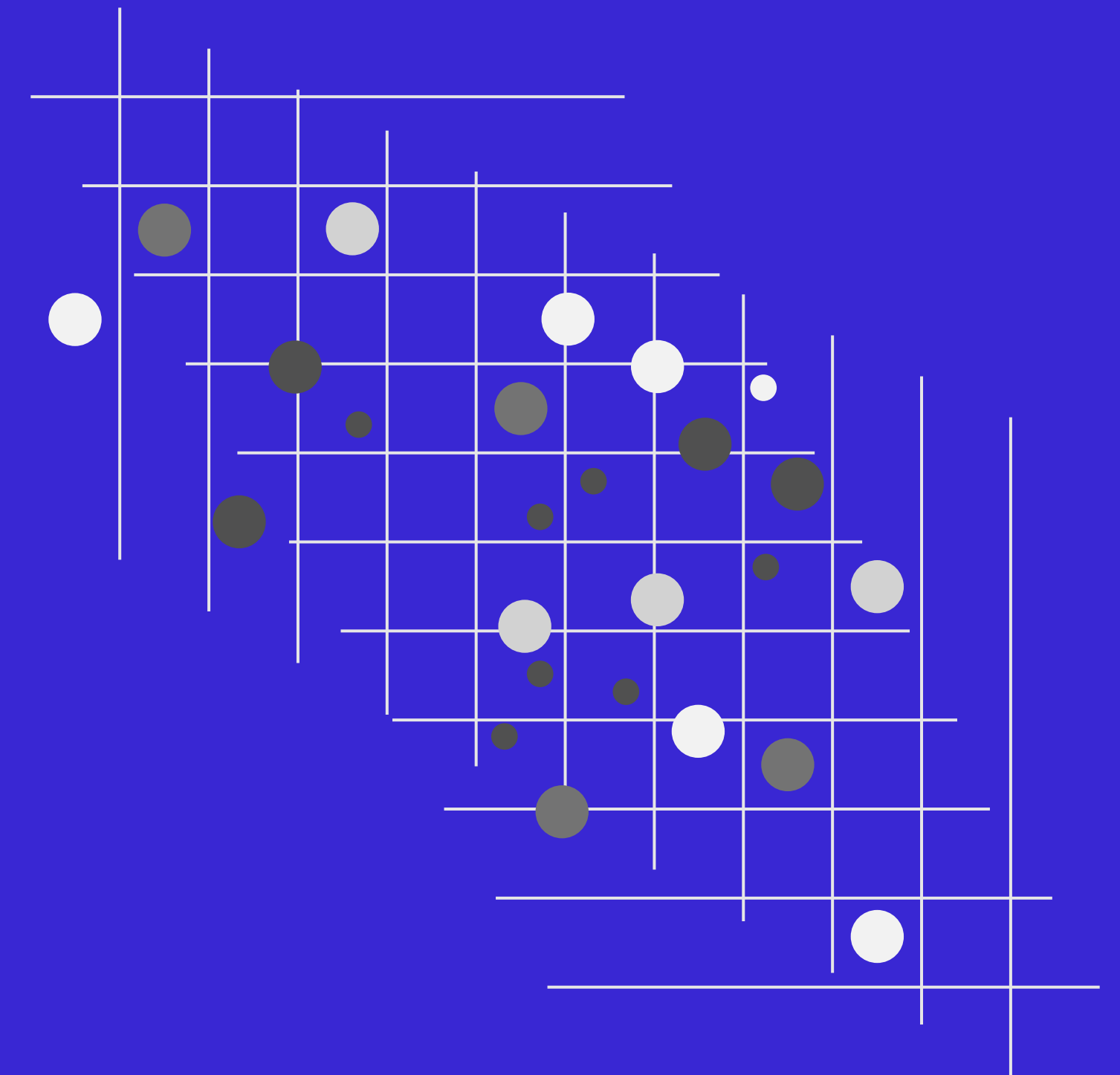
- No Long-Term Identity Broadcast
- Only Authority (based on a formal report) should identify long-term identity from messages
- Protection against External Cheating (False Reports)

Operators (e.g., Airport)

- Report misbehaving drones invading private areas

Authority (e.g., FAA)

- Verify private areas invasion claims by operators
- Identify misbehaving drones
- Be sure that operator is not cheating on drone position
- Zero interaction with drones' operators



Scenario and Adversary Model



Critical Infrastructure

generic receiver listening to the packets to detect any UAV invasion



Trusted Third Party

it releases the cryptographic materials, limited storage overhead--
-no storing of any sensitive data
(only TTP private key)



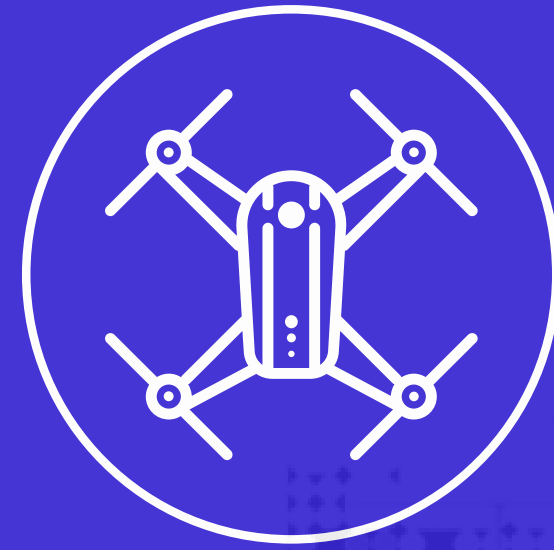
UAVs

broadcast connection-less interactions between any group of UAV (nullified MAC addr)



Adversary

passive and active capabilities---
drone tracking, eavesdropping long-term identity, UAV spoofing

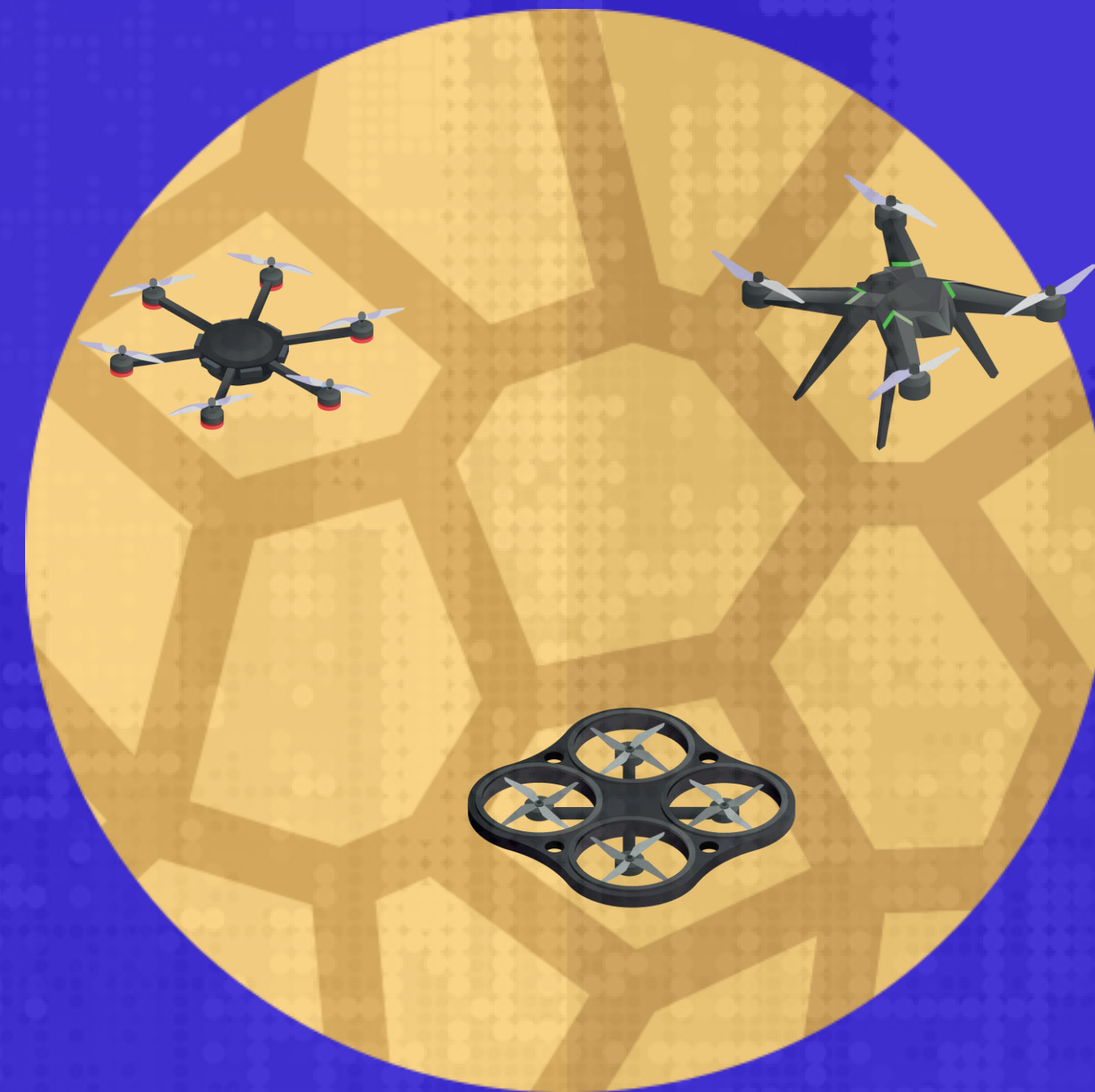


1) Registration Phase

2) On-Line Phase

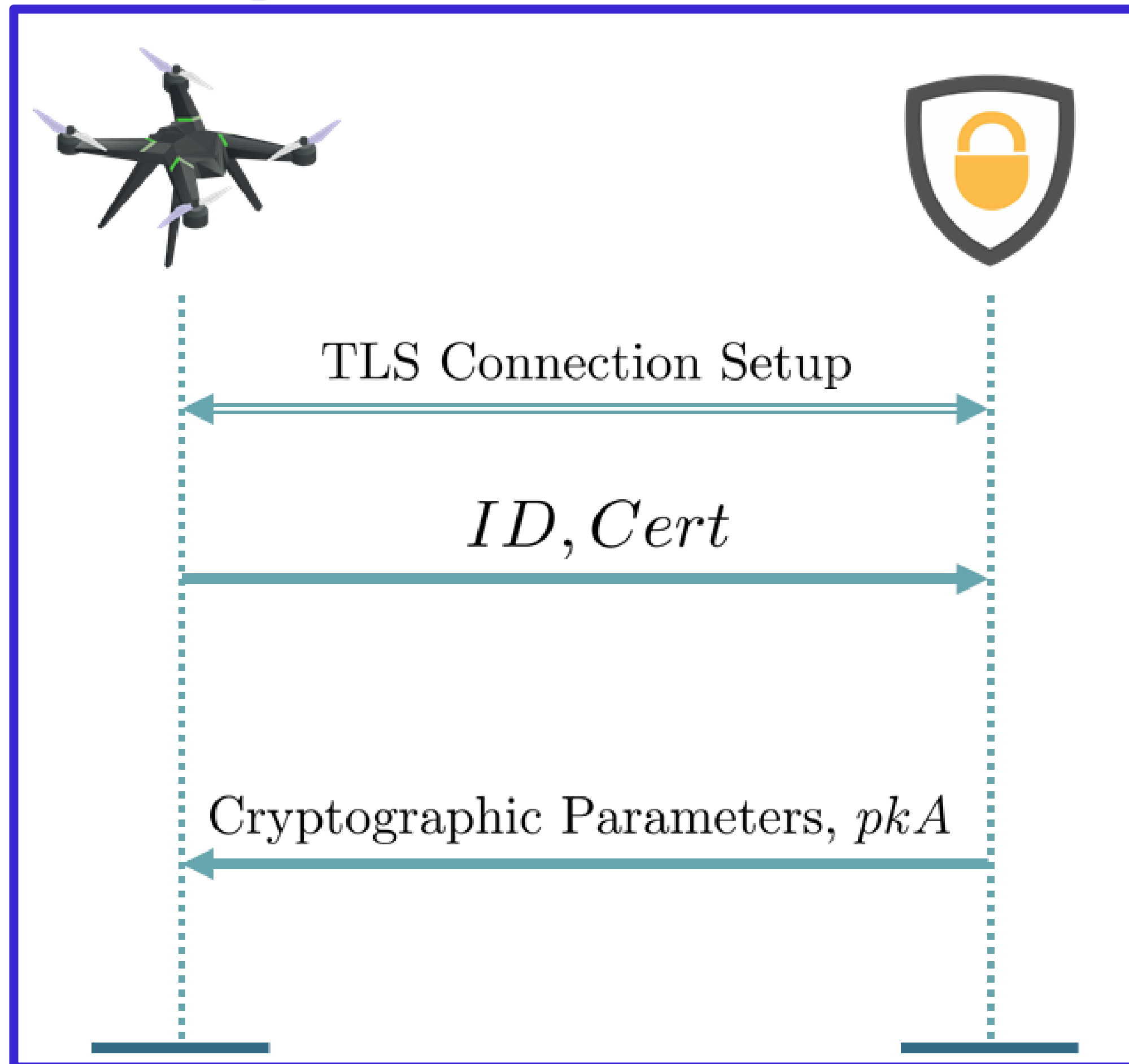
3) Reporting Phase

ARID - PHASES

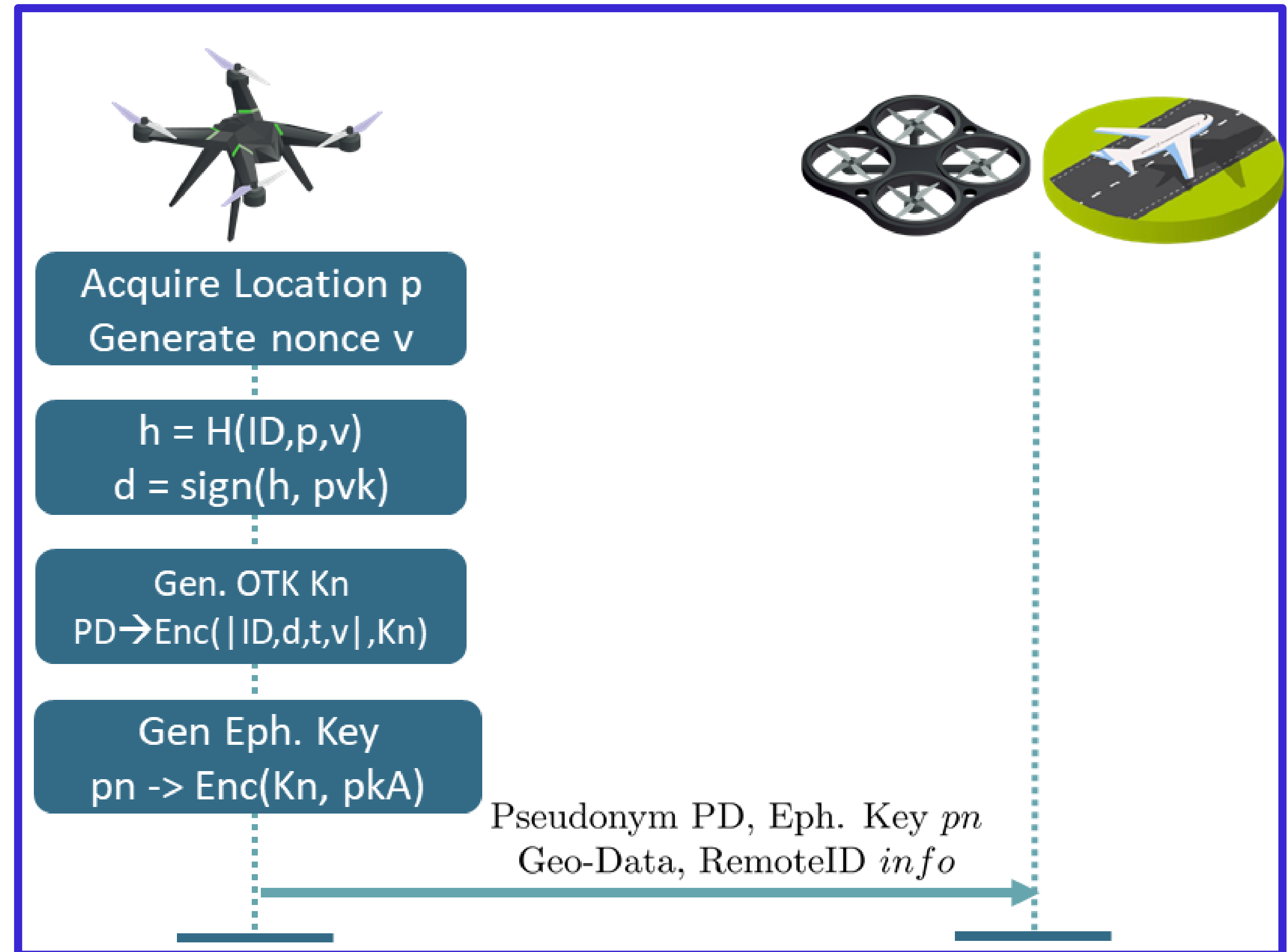


ARID: Anonymous Remote IDentification

1 Registration Phase

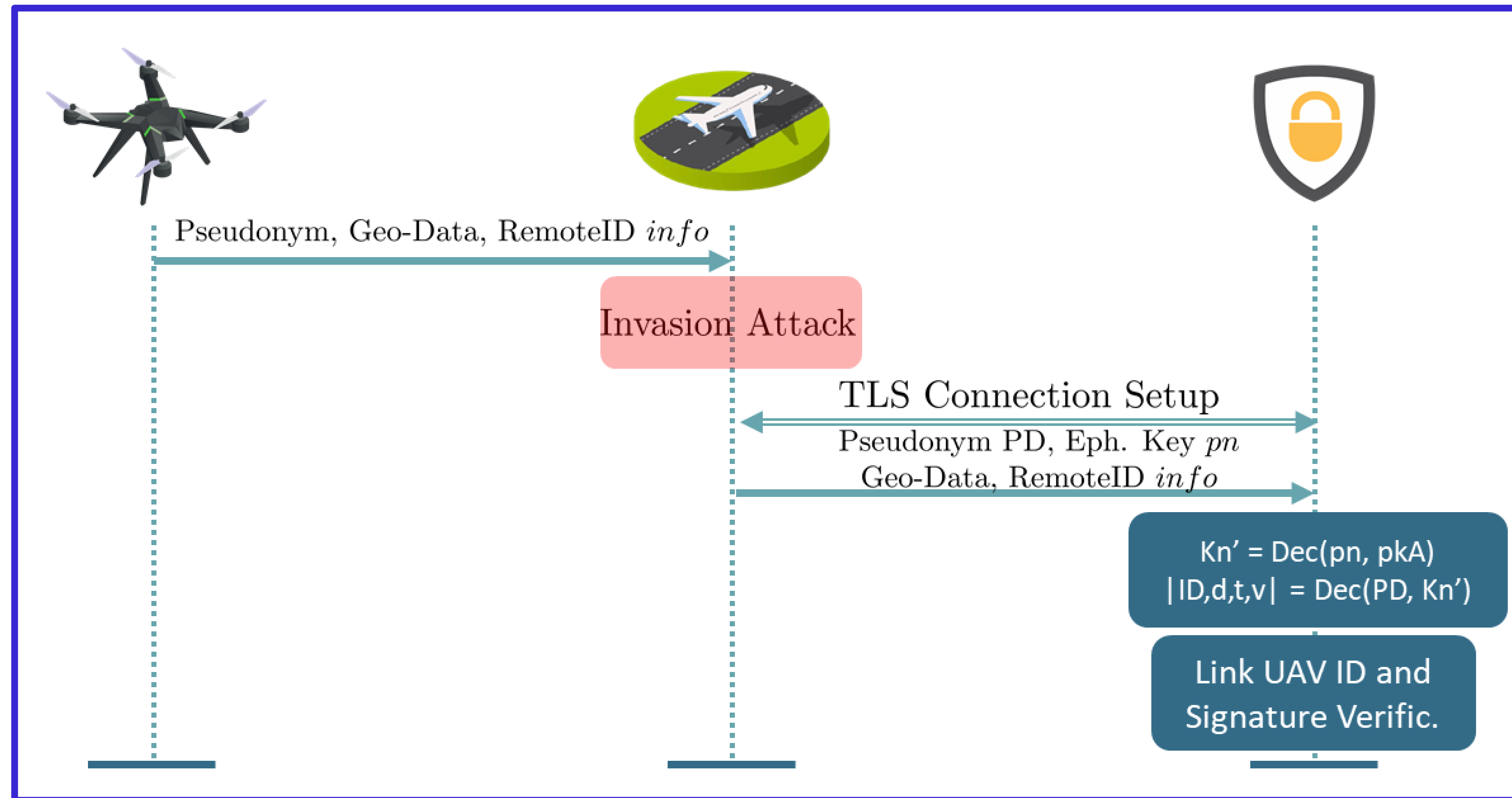


2 Online Phase



ARID: Anonymous Remote IDentification

3 Reporting Phase



Security Services



Security features offered by ARID

UAV Anonymity

UAV Message Authenticity

Protection against Replay Attacks

Partial Protection against UAV tracking

3DR Solo Details + ProVerif

- 3DR-Solo, CPU i.MX6 Solo - 1.00GHz ARM Cortex A9
- 7,948MB ROM, 512MB RAM
- Cryptographic Acceleration and Assurance Module
- 3DR Poky OS 1.5.1, OpenSSL 1.0.0, MAVLink 1.0

ARID at work

The image shows a Wireshark network capture of ARID packets. The top part is a packet list with columns for No., Time, Source, Destination, Protocol, and Length. The bottom part is a packet details pane for packet 845253, showing Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (UDP) details. The data field shows a 262-byte payload. Below the details pane, a terminal window displays the decryption process, including the AES key, the ciphertext length, and the decrypted data.

The terminal window shows the execution of ARID packets. The output consists of a series of log messages indicating the time taken to send each packet. The messages are as follows:

```
Time: 13.393997ms
[INFO] Sending ARID Packet
Time: 13.493685ms
[INFO] Sending ARID Packet
Time: 13.594755ms
[INFO] Sending ARID Packet
Time: 13.694151ms
[INFO] Sending ARID Packet
Time: 13.799184ms
[INFO] Sending ARID Packet
Time: 13.898701ms
[INFO] Sending ARID Packet
Time: 13.998803ms
[INFO] Sending ARID Packet
Time: 14.098784ms
[INFO] Sending ARID Packet
Time: 14.348343ms
[INFO] Sending ARID Packet
Time: 14.504507ms
[INFO] Sending ARID Packet
Time: 14.604584ms
[INFO] Sending ARID Packet
Time: 14.704643ms
```



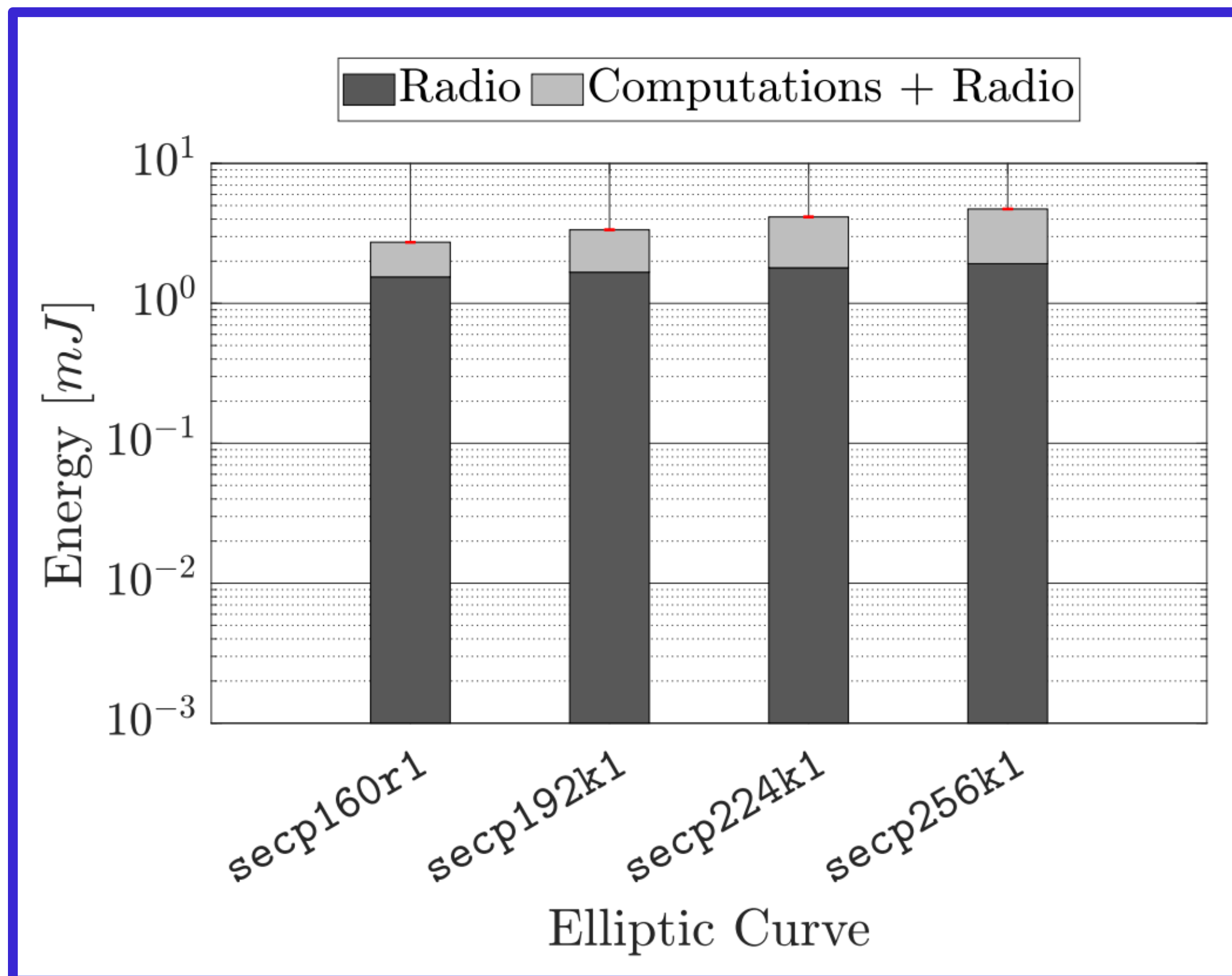
```
RESULT event(termAuth(id_1)) ==> event(acceptUAV(id_1)) is true.
RESULT not attacker(IDA[]) is true.
RESULT Non-interference IDA is true.
```



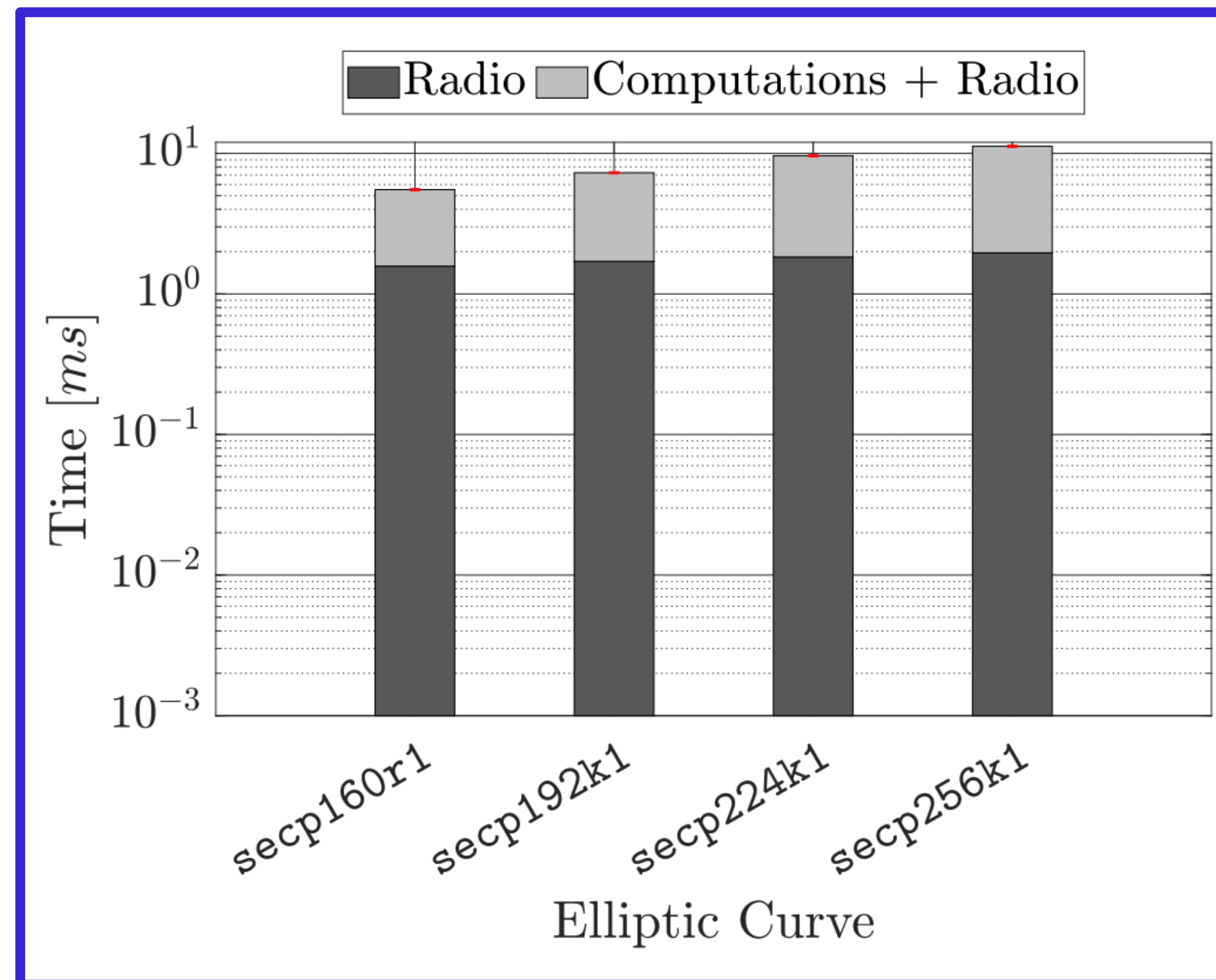
Performance Assessment

Impact of ARID on the battery lifetime. The most energy-consuming configuration of ARID (*secp256k1*) reduces the lifetime of the 3DR-Solo **by only 1.05%** compared to the default (non-anonymous) *RemoteID* configuration, further demonstrating its limited overhead.

Energy Consumption



Radio and Computation Time



Conclusion and Future Work

- Fully compliant with the latest *RemoteID* regulations by the FAA
- Complete anonymity and unlinkability of UAV broadcast messages + tunable level of security
- 11.23ms to create and transmit anonymous *RemoteID* messages & 4.72mJ of energy ($1.67 \cdot 10^{-6}$ % of the overall battery)
- Security properties have been discussed/formally proved via ProVerif
- Proof of Concept released as Open Source @ <https://github.com/pietrotedeschi/arid>





Any Questions?

THANK
YOU !



PIETRO TEDESCHI, PhD

Hamad Bin Khalifa University

e-mail: ptedeschi@hbku.edu.qa

linkedin: <https://www.linkedin.com/in/pietrotedeschi/>

