Dr Eric Murray

Principal Engineer

Vodafone Group

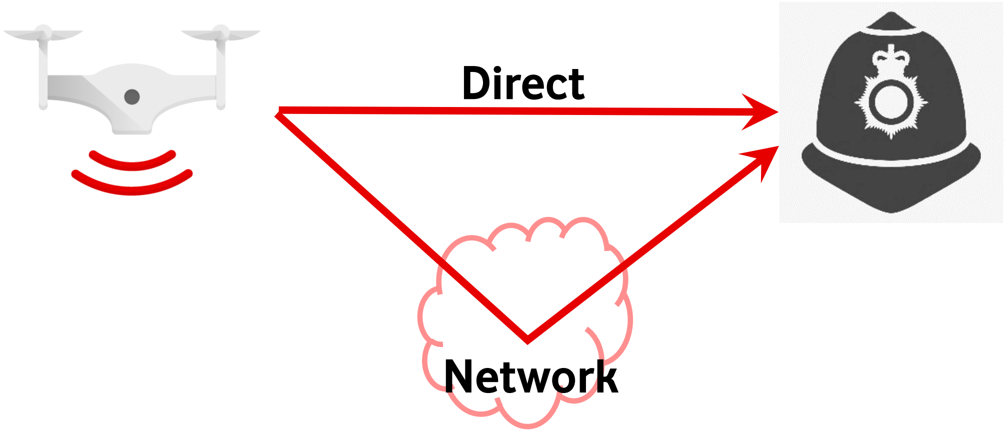
Technology Networks Architecture

Network-based Drone Authentication Through APIs

Dr. Eric Murray
Vodafone Group Technology
15 July 2020

EU Regulations on Drone Identification

- What does EU 2019/945 say?
  - Direct remote identification is mandatory (for most classes)
  - Network remote identification is optional
- Vodafone and the GSMA worked to ensure the requirement was **technology neutral**
- For **direct remote identification**
  - Original proposed regulation mandated short-range technologies, such as **WiFi** or **Bluetooth**
  - Now **Cellular D2D** (Device to Device) can also satisfy the published regulation
  - This technology is **maturing quickly** through its use in V2V (Vehicle to Vehicle) use cases
- For **network remote identification**
  - **Cellular** is the obvious "network", but the application data would be transparent to the network
  - It is expected that the requirements will evolve to include **U-space**, but still under development



Anticipating the evolution of requirements, Vodafone have been working on connecting and authenticating drones to U-space using cellular connectivity

How are Cellular Devices currently Authenticated?

- IMSI (International Mobile Subscriber Identity)
  - The **primary identifier** used for authentication by the cellular network, and very secure
  - Stored in the SIM, and **identifies the subscriber** (account owner) and not the device
  - **Used internally** by the network for uses such as:
    - billing and quota enforcement
    - associating the subscriber with other identities, such as the MSISDN (the "phone" number)
  - The **device itself can be identified by IMEI**, but this is not securely authenticated

- For voice and SMS, the **MSISDN** is forwarded to the destination to identify the call originator
- But for data services, **no unique identifier for the originator is provided**
  - The source IP address is **NATed using a shared pool**, so not unique to a specific user
  - The IP address, port and time of use can be used to identify the user **retrospectively**, but not in real-time
  - Authentication between client and server is separate from and transparent to the cellular network

Whilst client/server authentication could be used to authenticate drones to U-space, network-based authentication offers important security benefits

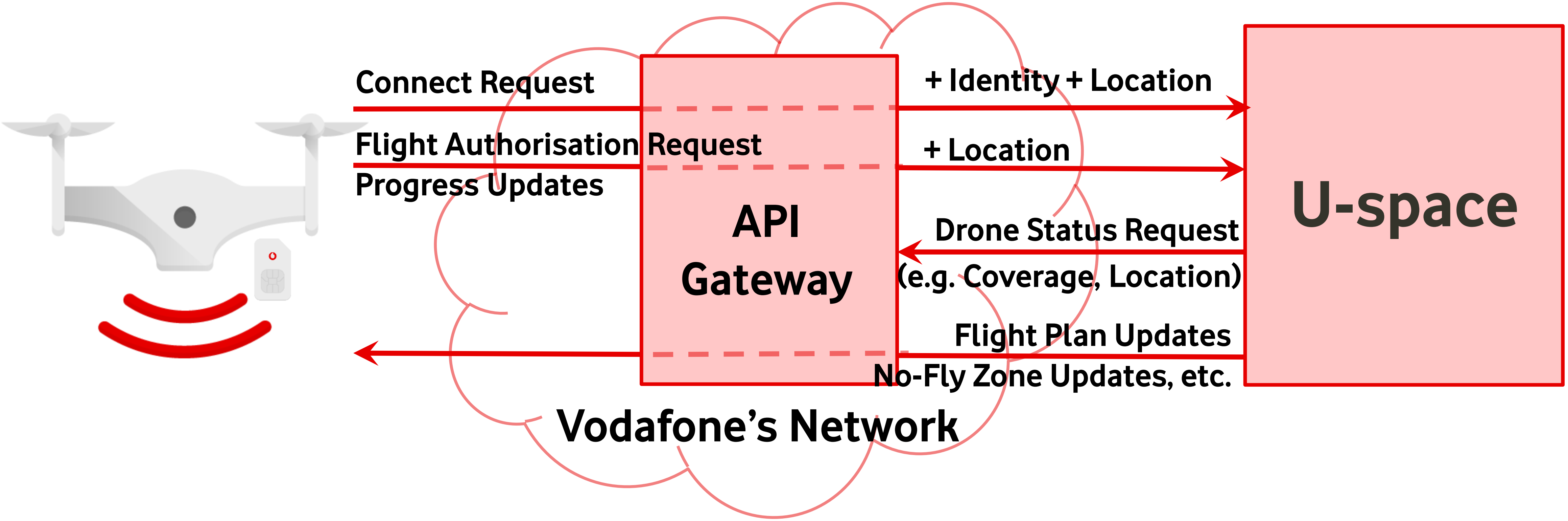
How Might the Requirements for Authenticating Drones Differ?

- Not all drone users will be “honest”, and may try to spoof the U-space
- Hence the U-space system would like to be sure that:
  - the connecting device really **is** a drone
  - it really is operated by **who** it says it is
  - it really is **where** it says it is
  - it is connected and **remains connected** via cellular for the duration of the flight
- All of this information is available to the cellular network **independently of the drone**
  - The SIM can be **registered as a drone SIM**
  - The drone IMSI can be used to **cross-reference the drone operator identity**
  - **Network-based geo-location techniques** (e.g. Vodafone’s Radio Positioning System) can be used to independently estimate the location of the drone
  - **Propagation prediction tools** can be used to confirm the proposed flight path has adequate cellular coverage

How can the cellular network provide these additional parameters to the U-space?

Communicating with U-Space via APIs

- The drone communicates with the U-space via an **API Gateway** within Vodafone's network
  – The API gateway **adds additional identifying information** to the connect request, independently of the drone



  – The U-space can get additional information using **additional APIs** (e.g. location updates or coverage predictions)
  – Drone and U-space can **exchange information during flight via API Gateway** (e.g. status updates, flight plan updates)
  – The API Gateway authenticates the U-space, and can support multiple U-spaces or changing U-space APIs transparently to the drone.

Summary

- **Cellular D2D** technology is one solution for EU "direct remote identification" requirements
  - This technology is rapidly maturing through its use for **Vehicle-to-Vehicle** uses cases
- But if the drone is also connected to the cellular network, Vodafone can provide **secure verification of the drone's identity** to U-space or other systems
  - The network can also verify parameters such as the **drone's location** or **predicted coverage quality**
- By interfacing through a **secure API Gateway**, this verification is independent of the drone application, and thus not easily spoofed
  - Equivalent to 2FA, with the second factor provided by Vodafone
- An API Gateway also allows **U-space systems to evolve** without the need to necessarily update the drone client

Vodafone have a large programme exposing network capabilities through APIs to support novel use cases