# IETF 106
# Birds of a Feather 2019 NOV 19
# Trustworthy Multipurpose Remote Identification:
# draft-card-tmrid-uas-00

Stu Card, Bob Moskowitz, Adam Wiethuechter

Extending locator/identifier split & strong authentication techniques to identify physically nearby objects

# Unmanned Aircraft System (UAS) Remote Identification (RID)

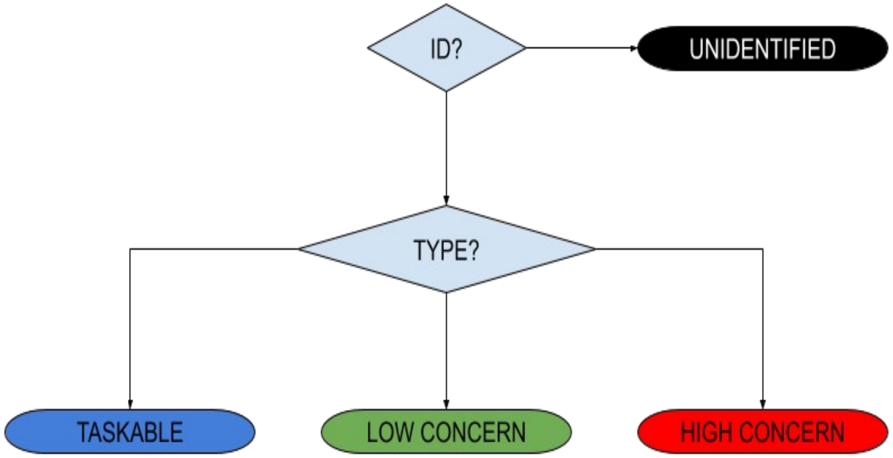
- Need means to identify nearby observed Unmanned Aircraft (UA)

  complicated by small size, hi speed (relative to size), remote operation, autonomy…
- Urgent: US FAA Notice of Proposed Rule Making (NPRM) this December
- ASTM F38.02 WK65041 new standard: OpenDroneID messages / multi transports
  - Network: from UAS (e.g. via LTE) or proxy (e.g. operator phone) via Internet to local observer phone
  - Broadcast: Bluetooth 4 / 5 & WiFi beacons (short packets!) direct to observer phone [w/o Internet]
- Initial ASTM standard falls short in making UAS RID information *immediately actionable*:
  - trustworthy
  - show whether operator is trusted, even if observer lacks Internet
  - enable instant O2P & M2M secure comms, if endpoints have Internet
- Aviators familiar w/radio comms, not networking; IETF could help
  - leverage existing Internet services/infrastructure/protocols (e.g. WHOIS/RDAP, DNS, HIP)
  - strengthen authentication, balance operator privacy w/genuine Need To Know
  - generalize to support V2X, self-separation, collision avoidance
- (UA physical location : UA ID) ~ (host logical location (IP) : host ID)

  we have prototyped & flown a HIP based extension to OpenDroneID @NY UAS Test Site

# UAS Remote ID is CRITICAL for UAS Traffic Management (UTM)

- Observing UA at a particular location, want to learn WHO
  - from which we can look up WHAT, WHY, “friendly”, etc.
- Relevant for many entities for various reasons
  - ATC, Public Safety Officials, Homeland Security, General Public, Private Security Personnel, Drone Operators…
  - V2X, C2, coordinated separation / collision avoidance, mission…



# ASTM F38.02 UAS Network Remote ID

- Uses various Internet media
  - Typically LTE
- Net-RID Service Provider (SP)
  - Gather data from connected UAS & other sources
- Net-RID Display Provider (DP)
  - Connection point for RID app
  - Aggregate data that user requests for a given area
- SP & DP can be co-located or not, same corp. or not
- UAS Service Supplier is expected to be SP only or both

# ASTM F.38.02 UAS Broadcast Remote ID

- One-way transmissions
  - UA to Observer devices w/RID app
- Short range media
  - Bluetooth 4.X beacon & 5 extended advertisement
  - Wifi w/Neighbor Awareness Networking (NAN)

# V2X Applications

- Remote ID itself as an app (vs enabling technology)
- Platform
  - Command & Control
  - Detect And Avoid (DAA) “self separation”
  - Collision Avoidance
- Payload
  - Mission apps, e.g. remote sensing

# Aerial Internet Weaknesses

- Today’s Internet has significant weaknesses in
  - Mobility
  - Multicast
  - Multihoming
  - Management
  - Quality of Service
  - Security
- Aero wireless networking compounds these…

# Some network issues compounded by aero comms

- Each non-trivial aircraft has multiple radios of different types
- Many types of radios hand off between base stations frequently
- Most open standard protocols are challenged by
    - Low data rates
    - High error (or loss) rates
    - Long latencies
    - Link asymmetry
    - Rapid wide variation in channel characteristics
- Security protocols requiring cryptographic handshakes are further challenged by
    - Limited on-board processing power
    - Brief contact time w/fast moving platforms
- Enormous safety implications (e.g. remotely crash my drone)
- Aggregation of enough public information enables inference of sensitive information about the physical world (e.g. air operations routes & schedules)

# 1st Mitigation for C2: Multiple Wireless Links

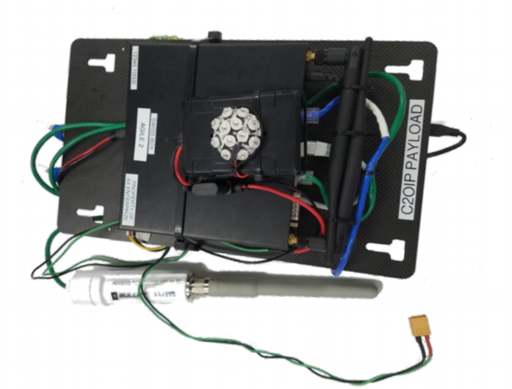
- Aviation authorities will require at least 2 largely independent radio systems for reliability
- Multiple links also greatly benefit security
  - jammer must jam all your links to deny you service
  - info can be spread over N links so an eavesdropper must listen on at least M of them to learn anything
- 3 links are obvious in many cases today
  - WiFi or other RF LOS coverage built to suit
  - LTE, w/extensive coverage already built out
  - Iridium or other global coverage systems
- End systems & users
  - Should know what network Quality of Service they currently can expect
  - But should *not* need to know which link[s] reach a given UA at a given time

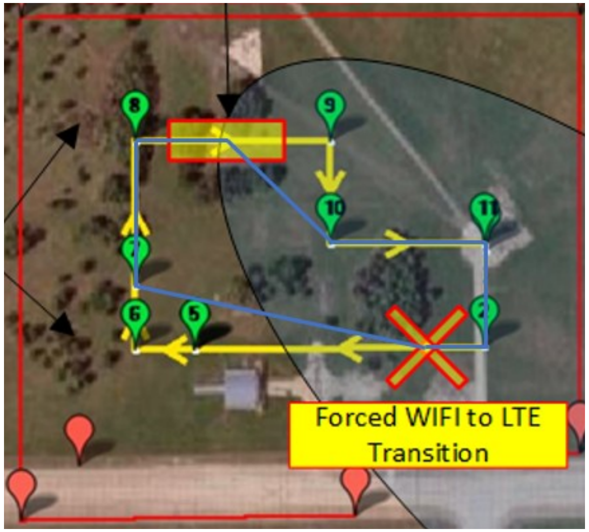
# $2^{nd}$ Mitigation for C2: Strong ID Based Security

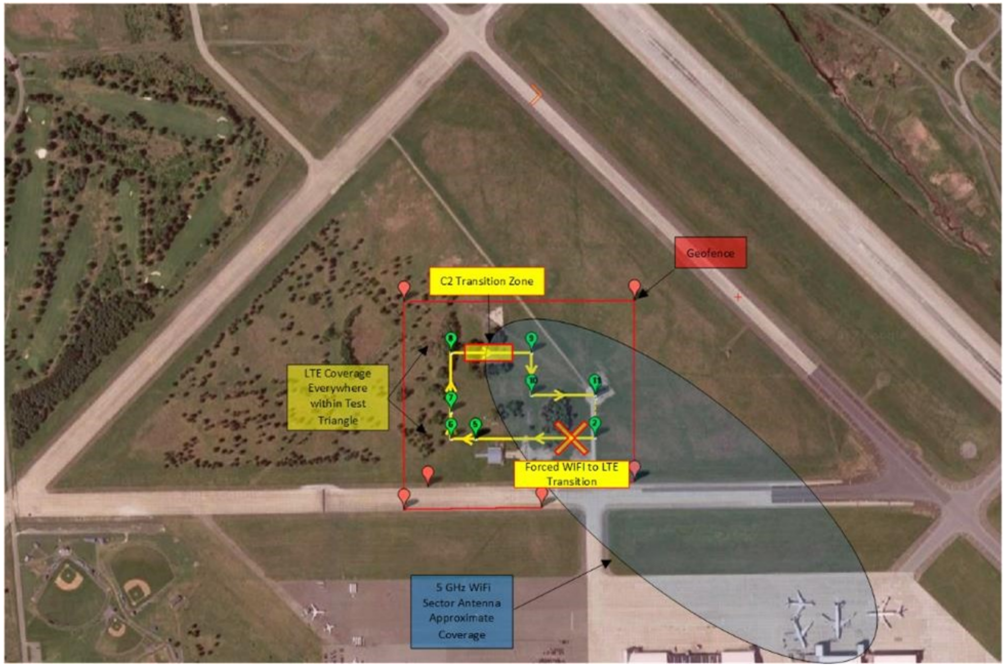
- Aircraft *identity* is distinct from its physical (spatial) & logical (network) *locations*
  - Aircraft identifiers should be distinct from locators (e.g. current IP addresses)
  - Security associations should belong to identity, not location, thus remain unaffected by handoff between radio base stations
- IETF Host Identity Protocol (HIP) offers
  - identifier / locator de-conflation as justified above
  - identifiers corresponding to crypto public keys
  - IPSEC interoperability w/automatic dynamic setup
  - multi-homing (multiple concurrent network connections)
  - smooth make-before-break handoff between base stations

# Cyber Resilient UAS Comms

- Demonstrated maintaining control of UAS w/HIP-based robust/secure C2.
- Assured C2 over multiple links (WiFi & LTE) w/automatic failover/fallback.
- Strongly encrypted communications between authenticated endpoints w/persistent IDs.



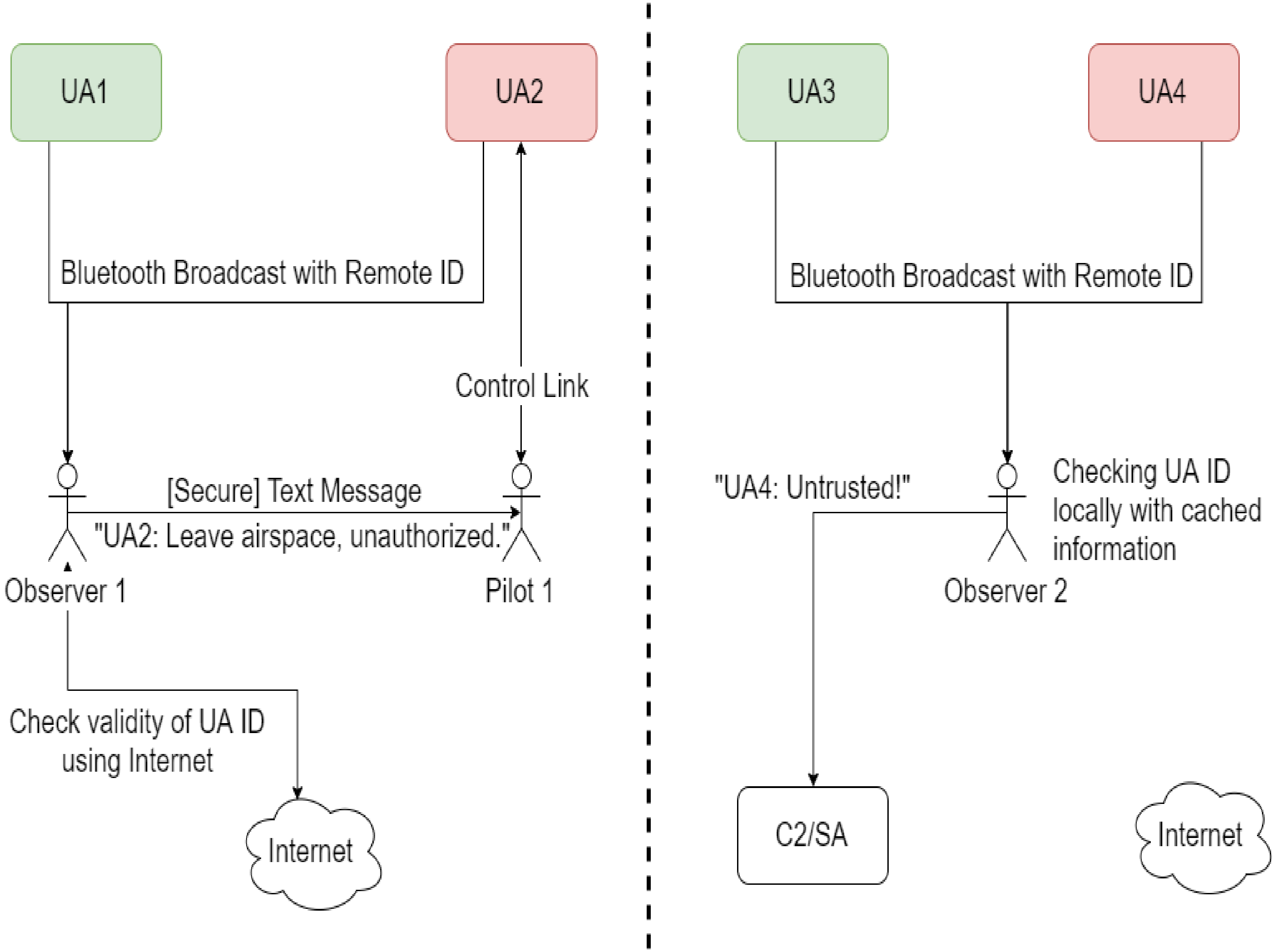



Geofence
C2 Transition Zone
LTE Coverage Everywhere within Test Triangle
Forced WIFI to LTE Transition
5 GHz WiFi Sector Antenna Approximate Coverage

# Our UAS RID approach

- Adopt & extend existing standards
  - ICAO, RTCA, CAAs inc. FAA, USAF…
  - FAA expected to adopt ASTM draft… but security & threat model not addressed in draft!
- Bring in the Internet Engineering Task Force (IETF)
  - large diverse base of relevant expertise, esp. network security
  - mapping **host ID -> logical location** (IP address) is similar to inverse mapping **physical location -> UAS ID,** so extending IETF standard Host Identity Protocol (HIP) & proposing it via ASTM
  - w/Internet connectivity (Network RID), also facilitates dynamic establishment of encrypted, mutually authenticated **secure comms** between observer & UAS (or its operator)
  - w/standardized vetting by hierarchical registries, makes UAS ID & any other cryptographically signed claims **trustworthy** even w/o Internet connectivity (Broadcast RID)

# We need it to be immediately actionable!


UA1
UA2
Bluetooth Broadcast with Remote ID
Control Link
[Secure] Text Message
"UA2: Leave airspace, unauthorized."
Observer 1
Pilot 1
Check validity of UA ID using Internet
Internet
UA3
UA4
Bluetooth Broadcast with Remote ID
"UA4: Untrusted!"
Checking UA ID locally with cached information
Observer 2
C2/SA
Internet

# Trustworthy Multipurpose Remote Identification (tmrid)

- UAS RID information must be immediately actionable:
  - Trustworthy
  - Enable instant O2P & M2M secure comms, if endpoints have Internet
  - Show whether operator is trusted, even if observer lacks Internet
  - Yet privacy must be maintained when it has not been forfeited by the UAS operator through clueless, careless or criminal actions

- IETF protocols can complement ASTM F38.02 to achieve the above plus:
  - support a variety of apps related to UAS RID (e.g. C2, DAA, V2X)
  - leverage existing Internet services/infrastructure (e.g. DNS, RDAP/WHOIS) to support UAS RID
  - we have prototyped & flown initial tmrid @NY UAS Test Site

- ASTM & IETF standards both need minor tweaks
  - we met w/ASTM 2 weeks ago

# HIP benefits for Remote ID

RFCs 4423[bis], 7343 (ORCHID), 7401, 8002 - 8005

- General
    - Give each device a persistent identifier that remains the same across IP address changes
        - enable persistent TCP connections, security associations, etc.
    - Give all packets a provenance
        - “Secure Mobile Architecture” (Boeing, Lockheed-Martin, et al)
        - see R. Paine’s *Beyond HIP*: *The End to Hacking As We Know It*
    - Auto-configure IPsec VPNs (frustrating to do manually)
- Aero networking
    - Associate persistent identifier with aircraft tail #
    - Multihoming for make-before-break smooth handoff

# Using HIP for RID

Network RID can leverage all of HIP advantages

- Persistent ID of all interconnected devices (UAS, USS)
- Automagic IPSec ESP tunnels from Observer to Pilot etc.

Broadcast RID

- Trustworthy (verifiable) persistent ID using HIT
- Observer can classify operator as trusted or not based on which HHIT registry cert is provided, even w/o current Internet connectivity

Beyond HIP: DNS, RDAP/WHOIS (registry providers, registrars)...