Drones and UAS: Standards

IETF activity on
Drone Remote ID Protocol
(DRIP!)
April 2, 2020

Robert Moskowitz
HTT Consulting

Agenda

- Remote ID in Unmanned Aircraft (UA)
- Hierarchical Host Identity Tags (HHIT) for RID
  - Just enough about HIP to use HHITs as IDs
- Using HHIT in UAS
  - And a bit more HIP background
- UA Operator Privacy Issues
- Enhanced UA Tracking through Crowd Sourcing

Remote ID in Unmanned Aircraft

- Civil Aeronautics Administrations mandates
  - Network UA tracking
    - Over Internet from UA or Ground Control Station (GCS)
      - To UAS Service Supplier (USS) and on to UA Traffic Management (UTM)
  - Broadcast UA tracking
    - To any observer over reasonable radio broadcasts
  - Cybersecurity for it all
  - A UA ID is needed for effective tracking

Remote ID in Unmanned Aircraft

- Lowest common denominator for broadcasting
  - Bluetooth 4 broadcast frame
    - Only 25 bytes for ID and other information
    - 20 byte RID size and no room to authenticate RID
  - No messaging enforcement of RID trust
- Proposed RID formats totally spoofable
  - Manufacturer Serial #, CAA #, UUID

Remote ID in Unmanned Aircraft

- Can a UA provide certificate for RID?
- Authentication Message can be 10 BT4 frames
  - What can be done in ~250 bytes?
  - Custom certificates
    - Fraud still possible as signers can assert any RID
    - How to build Infrastructure for implied trust?
    - How this works with no Infrastructure access – Disasters!
- Cryptographic RIDs...

HHITs for RID

- Just a quick side trip into HIP...
  - Born out need of device, not interface Identity
  - Host Identity (HI)
    - Cryptographic Identity of a Device, RFC 7401
      - THE IMPORTANT piece for RemoteID!
    - Interface independent and thus mobility independent
      - Identity, not Location for beyond RID use
  - And a simple Protocol for peer exchange
    - And session key agreement also for later

HHITs for RID

- But Host Identities cannot effectively be directly used in datagrams
  - Different algorithms, different lengths, etc.
- Thus Host Identity Tags (HITs)
  - Cryptographic hash of a Host Identity
  - Valid, non-routeable, IPv6 address
  - See RFC 7401 for more details

HHITs for RID

- Host can directly prove ownership of HI and HIT
  - Using HI private key to sign something containing HI public key or HIT
  - Signed object can be quite small
    - With EdDSA HI, HIT + Sig about 84 bytes
- With HITs, device can prove it is itself
  - But why trust it?
  - By adding a trust hierarchy into HITs

HHITs for RID

- Hierarchical HIT adds
  - Ownership/Registration
    - Entity backing host proof of HHIT ownership
  - Lightweight ‘proofs’, especially when using EdDSA
    - ~84 bytes of “This is my RID”
    - ~200 bytes of “Certificate of Registration”
    - Small offline cache for Certificate validation
  - Internet drafts available for HHIT, Registries, and Authentication message formats

Using HHIT in UAS

- Straight-forward and deployable trust in UA tracking
  - Can use DNS to identify Hierarchy owners
    - Avoid complexities of PKIs
  - Privacy can be achieved in HHIT per mission
    - Limits traffic analysis of prior uses of HHIT
  - Easy ownership transfer (compared to Serial #)

Using HHIT in UAS

- Use HIP in Command-and-Control (C2)
  - Privacy and mobility for C2
- A bit more of a dive into HIP
  - Applications isolated from interface IP addresses
    - Use HITs instead, ID/Loc separation theory
  - Mobility and multihoming (multiple interfaces)
    - Handles ‘double jump’ where both ends move
    - Make before break

UA Operator Privacy Issues

- UA System message broadcasts Operator location!
  - UA has no right to privacy in National Airspace
    - ~1” above ground to ~60,000 feet
  - Operator has right to privacy
    - Angry crowds with baseball bats and chainsaws!
  - How to protect, yet provide information to authorized observers?

UA Operator Privacy Issues

- Just encrypt the Operator location information…
  - Operator registers mission with USS
    - CAA requirement
    - Operator provides USS with short-lived PK
      - And gets USS PK
  - ECIES used to encrypt location information
    - Only USS can decrypt
      - And provide to authorized entities
- Internet Draft in the works (EoW goal)

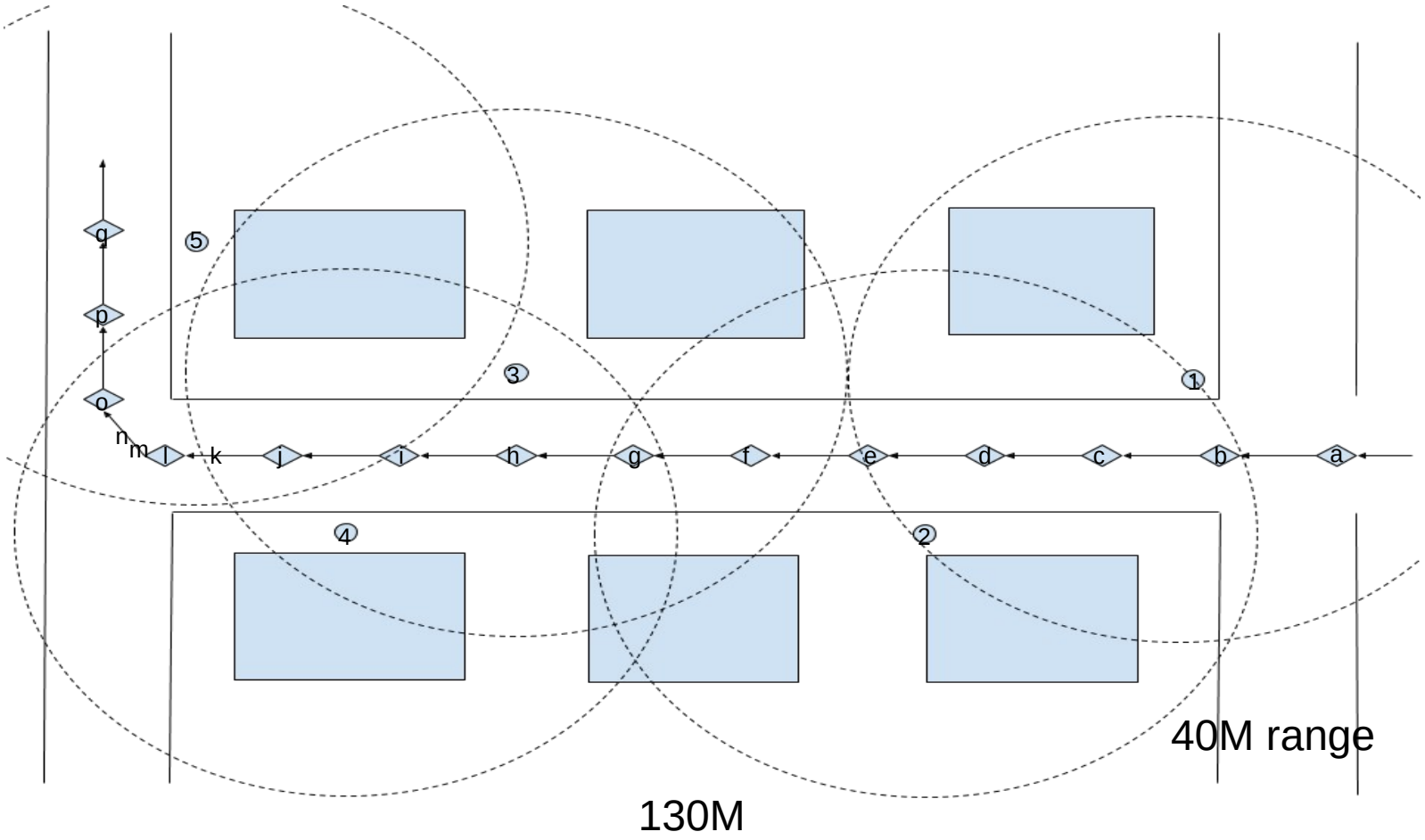
Crowd Sourced UA Tracking

- Inspired by Apple’s Find My app
- All Internet connected devices with appropriate radios can “Find” Broadcast RID messages
- With proper security can forward messages into UA tracking ecosystem
- “Finders” can be any smart device or purpose placed monitoring
  - At places of interest

Crowd Sourced UA Tracking

- Provide UTM with
  - Information on UAs that do not support N-RID
  - Multilateration to validate location claims by UA
    - At least 3, preferably 4 Finders
  - Provide map of coverage
  - Finders may use passive observation to report on non-participating UAs via LIDAR or cameras
- Internet Draft available

Crowd Sourced RemoteID



Where to find Information

- DRIP workgroup
  - https://datatracker.ietf.org/wg/drip/about/
- Related HIP documents
  - https://datatracker.ietf.org/wg/hip/documents/
    - See bottom of page for new drafts

QUESTIONS?