Questionnaire on Remote ID

June 15, 2020

UTM Working Group

Website; Address feedback and comments to sayandeep@deepcyan.ai or abhiroop@algopixel.tech.

This handout lists the open decision items for our upcoming publication *"Remote Identification for Unmanned Aircraft Systems"*. The purpose is to gather feedback from (non-member) industry participants on key issues pertaining to hardware, architecture and adoption of Remote ID technology in the Indian UAS ecosystem.

Architecture

1. `ID` field of Remote ID data proposals
   (a) `UIN`, `DAN` with `ID Type` Field `0` for UIN, `1` for `DAN`
   (b) Unique ID decoupled from `UIN/DAN`
2. Non-NPNT Compliant drones
   (a) Are non-NPNT drones with DANs to be phased out, so pilots can be retrained on NPNT compliant UASs?
   (b) Is there a purpose to NPNT when we are allowing DAN-registered UASs to fly?
3. Network ID: UTM-SP Discovery and Data Submission[1]
   (a) Forwarding
   (b) DSS + P2P
4. Network ID: General availability of Telemtery data[2]
   (a) no
   (b) restrict to 50m radius around actor
   (c) no restrictions

Use cases

1. For each case[3]:
   (a) What should be the interaction flow?
   (b) Request-Response or PubSub?
   (c) What messaging protocol to use?
      i. Possible options: MQTT, XMPP, others
   (d) What network layer protocol to use?

[1] See Tech Report (draft) Section 2.1.6.1

[2] See Tech Report (draft) Section 2.1.6.2

[3] See Tech Report (draft) sections 2.1.5.1, 2.1.6.1

        i. Possible options: TCP/IP, UDP, others

    (e) What should be the data format?

        i. Possible options: JSON, XML, Thrift, Protobuf, others

    (f) What data or part thereof should be signed and how?

    (g) What data or part thereof should be encrypted and how?

    (h) Single/Multi UTM-SP in same operational volume

        i. Which uses cases have any ramifications

Privacy

1. Which Operational use cases[4] or Operational scenarios[5] require encryption beyond[6] channel encryption between UAS and UTM/DCSP already mandated by ASTM?

Security

1. Programmability: proposals

    (a) Auditable programming process

    (b) Cryptographically secure programming process[7]

2. Programmability: Who should/should not be able to program the remote ID into hardware

    (a) Remote ID Manufacturer

    (b) UAS Manufacturer

    (c) Operator

    (d) Pilot

Adoption

1. How would existing drones without any compliant RemoteID hardware become compliant?

    (a) Integrating with Remote ID hardware on market (to be imported, integrated and tested)

    (b) development of Remote ID chip/board in-house (open-sourced designs insert cfs. are available) & integration

2. What should the timeline by stakeholder be

    (a) UAS Manufacturers

        i. 6 months: product development/integration, testing

        ii. 3 months compliance testing & approval

[4] See Tech Report (draft) Appendix 3.2

[5] See Tech Report (draft) Appendix 3.1

[6] End-to-end encryption, etc.

[7] Similar to NPNT

    iii. Leeway: 3 months

  (b) UFII-UTM infrastructure for enablement

    i. development of interfaces/protocols (2 months)
    ii. implementation (6 months)

  (c) Operators & Pilots

    i. Training (?? months)

  (d) Law Enforcement

    i. Additional Hardware (?? months)
    ii. DSP integration (?? months)
    iii. Training (3 months - 2 years)

Supplementary issues

Comments