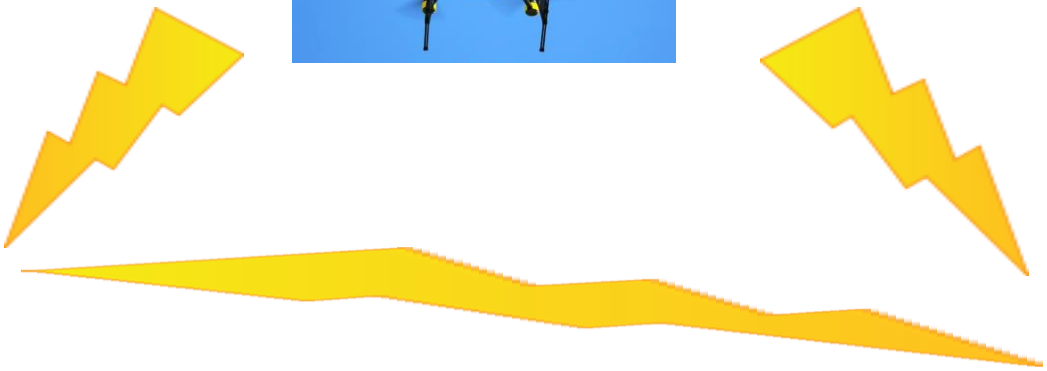


IETF 107

Drone Remote Identification Protocol (DRIP) WG

formerly Trustworthy Multipurpose Remote Identification (DRIP) BoF

draft-card-drip-reqs ⇒ draft-card-drip-arch

stu.card@axenterprize.com 315-725-7002
adam.wiethuechter@axenterprize.com
Robert Moskowitz rgm@labs.htt-consult.com

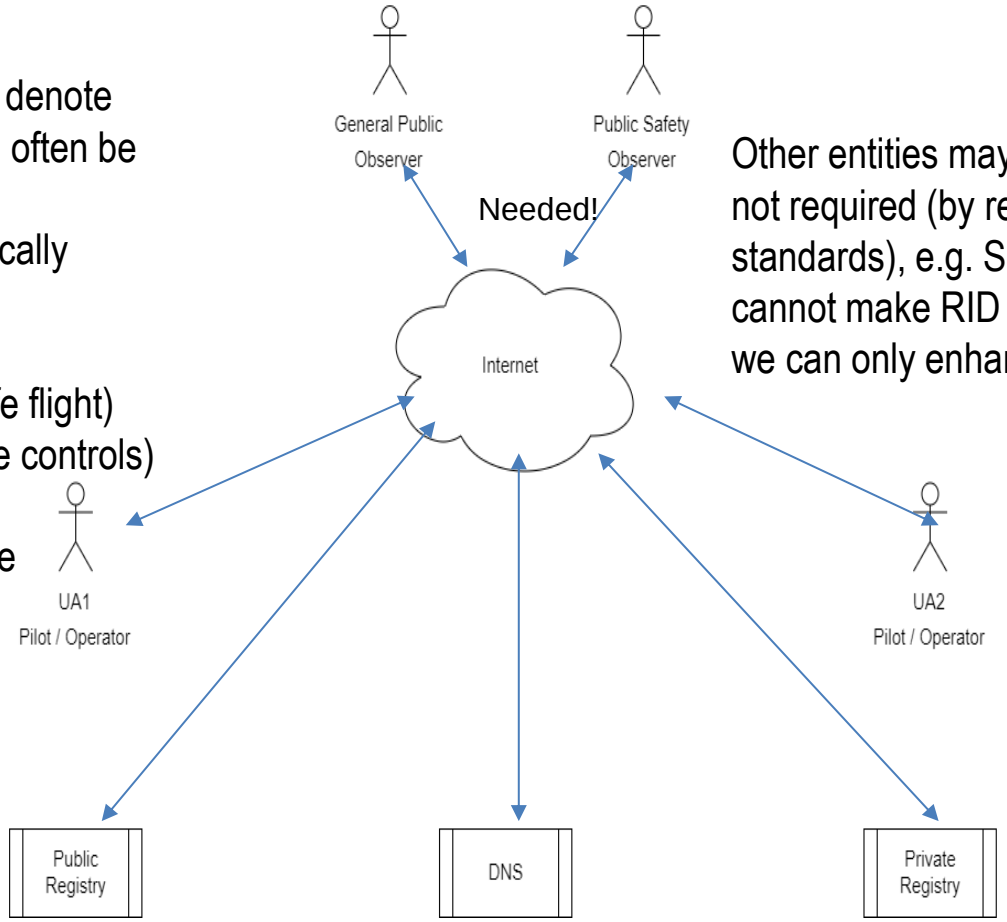
Warning: urgent need has justified solution space work in parallel w/requirements!

“Reference Architecture”:
really just the cast of characters

UA is Broadcast RID source

By “Pilot/Operator”, we denote several entities that will often be identical or colocated:

- UAS Operator (typically owner or lessee)
- Pilot In Command (responsible for safe flight)
- Remote Pilot (at the controls)
- GCS (the controls)
- Network RID source



Other entities may be in play but are not required (by regulations or external standards), e.g. SDSPs, but we cannot make RID depend on SDSPs, we can only enhance it w/such

By “registry”, we denote several functions that will almost certainly be offered by the same service bureaus:

- UAS Operator registry
- UA registry
- UTM USS
- Net-RID Service Provider
- Net-RID Display Provider

ASTM Broadcast RID w/o DRIP enhancements:

Unverifiable weakly correlated assertions of identity, position, velocity…

UA broadcasts Basic ID etc.

Observers:

- attempt to correlate Basic ID w/other (esp. track) data
- look up operator info in TBD registries via TBD query/response protocols protected by TBD access control mechanisms over the Internet.

Our Proposed DRIP Approach

- UAS RID should be **immediately actionable**:
  - Trustworthy *information*
  - Show whether *operator* is trusted, even w/o observer Internet connectivity
  - Enable instant Observer to Pilot & M2M secure comms, when IP connectivity is available between endpoints

  Privacy must be maintained if not forfeited by the UAS operator through clueless, careless or criminal actions

- Complement existing external standards
  - ASTM, CTA, International Civil Aviation Organization (ICAO), CAAs…
  - FAA cites ASTM F3411-19 as potential means of compliance… but security & threat model not addressed!
- Leverage existing Internet business models, services, infrastructure, protocols & IETF expertise
  - Complement ASTM F3411-19 to mitigate its shortfalls
  - Support a variety of applications related to UAS RID (e.g. C2, DAA, V2X)
- Stretch goal: integrate sources of track information other than operator direct self-reports
  - Gateway Broadcast RID to Network RID
  - Enable multilateration of relayed reports

Some network issues compounded by aero comms, constraining solutions

- Today's Internet has significant weaknesses in
  - Mobility, Multicast, Multihoming
  - Management, QoS, Security
- Aero wireless networking compounds these
  - 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
- ASTM F3411-19, per regulator guidance to support current smartphones as observer devices, imposes further constraints
  - One-way Bluetooth 4 advertisement (beacon) broadcast frames carry at most 24 bytes of payload
  - Even paged multi-frame messages carry at most 224 bytes (minus any ECC) to hold a signed message or certificate
- Security protocols requiring cryptographic processing are further challenged by
  - Limited on-board processing power
  - Brief contact time w/fast moving platforms
- Yet enormous safety implications (e.g. drone crashes into people or critical infrastructure) of insecure or unreliable protocols
- Aggregation of enough publicly broadcast RID transmissions enables inference of sensitive information about the physical world (e.g. air operations routes & schedules)

Updated ASTM F3411 + Updated Selected IETF Standards = DRIP

- Mapping an observed UA's **physical location -> UAS ID** similarity to the inverse problem of mapping an Internet **host ID -> logical location** (IP address) inspired leveraging Host Identity Protocol (HIP), bringing other benefits.
- We propose 2 minor tweaks to the ASTM F3411-19 UAS RID application standard.
  - Define a UAS ID Type (presumably 4) as a Hierarchical Host Identity Tag (HHIT)
  - Allow full 10 BT 4.x pages of Authentication Message to contain authentication data

  We participated in ASTM F38.02 UAS RID standard ratification because FAA needed to cite something now. ASTM F38.02 leadership agrees revision is needed & likes our ideas but will wait for FAA NPRM feedback.
- We propose several updates/enhancements to the IETF HIP standards.
  - New crypto must be integrated to fit signatures & certificates in the very small Bluetooth packets.
  - Host Identity Tags (HITs) must be extended to allow for a registry hierarchy (HHITs).
- We have both integrated baseline ASTM F3411-19 (OpenDroneID) & prototyped some of our extensions.
  - We have flown successfully test flown this at the NY UAS Test Site.
  - We have updated our prototypes to authenticate UAS RID claims & will soon fly again.

DRIP General Requirements *easily satisfied* if UAS ID is a HHIT in DNS & Whois (w/RDAP, EPP & XACML)

1. verify that messages originated from the claimed sender
2. verify that the UAS ID is in a registry & identify which one
3. *lookup, from the UAS ID, public information*
4. *lookup, w/AAA, per policy, private information*
5. *structure information for both human and machine readability*
6. *provision registries with*
    1. *static information on the UAS & its Operator / Pilot In Command / Remote Pilot*
    2. *dynamic information on its current operation within the UTM*
    3. *Internet direct contact information for services related to the foregoing*
7. *close the AAA-policy registry loop by*
    1. *governing AAA per registered policies*
    2. *administering policies only via AAA*
8. dynamically establish, w/AAA, per policy, E2E strongly encrypted communications w/the UAS RID sender & entities looked up from the UAS ID, inc. the GCS & USS

It is highly desirable that Broadcast RID receivers also be able to stamp messages with accurate date/time received and receiver location, then relay them to a network service (e.g. distributed ledger), *inter alia* for correlation to assess sender & receiver veracity.

DRIP General Requirements *easily satisfied* if UAS ID is a HHIT **w/proposed new crypto** in DNS & Whois

1. ***verify that messages originated from the claimed sender***
2. ***verify that the UAS ID is in a registry & identify which one***
3. *lookup, from the UAS ID, public information*
4. *lookup, w/AAA, per policy, private information*
5. *structure information for both human and machine readability*
6. *provision registries with*
    1. *static information on the UAS & its Operator / Pilot In Command / Remote Pilot*
    2. *dynamic information on its current operation within the UTM*
    3. *Internet direct contact information for services related to the foregoing*
7. *close the AAA-policy registry loop by*
    1. *governing AAA per registered policies*
    2. *administering policies only via AAA*
8. dynamically establish, w/AAA, per policy, E2E strongly encrypted communications w/the UAS RID sender & entities looked up from the UAS ID, inc. the GCS & USS

It is highly desirable that Broadcast RID receivers also be able to stamp messages with accurate date/time received and receiver location, then relay them to a network service (e.g. distributed ledger), *inter alia* for correlation to assess sender & receiver veracity.

DRIP: message authentication w/o Internet

UA Broadcasts ID certificate & other messages (e.g. position + velocity) *signed.*

General Public Observer

Public Safety Observer

Not Needed!

X

X

Internet

Observers verify signatures, ensuring received data (e.g. position track) all really came from UA w/claimed ID.

UA1
Pilot / Operator

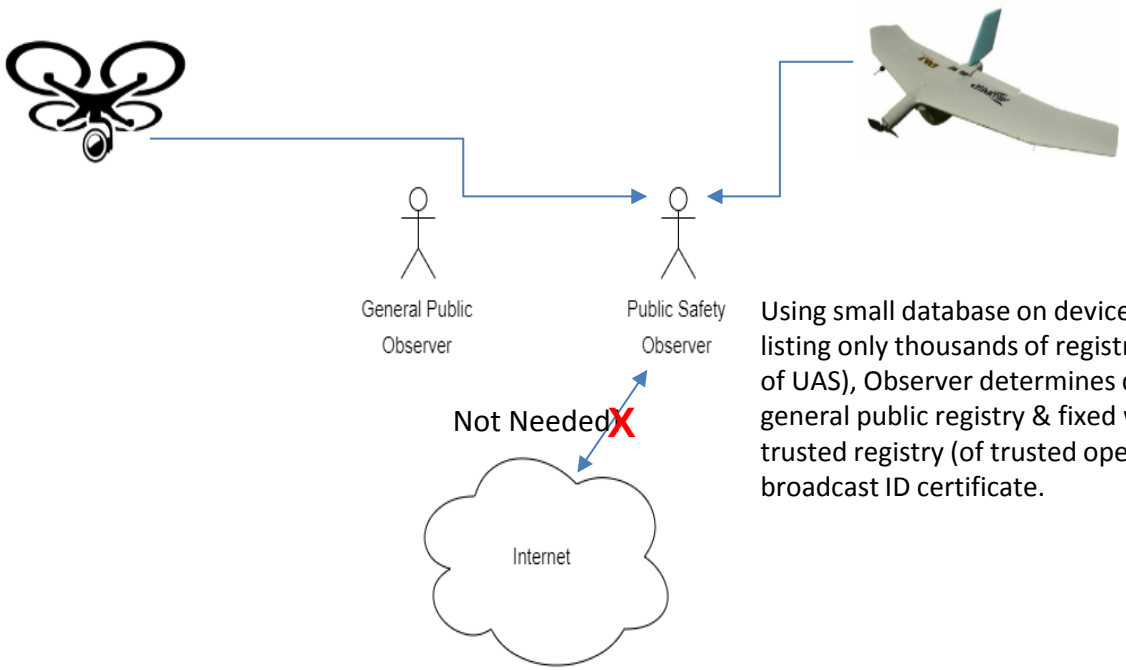
UA2
Pilot / Operator

Public Registry

DNS

Private Registry

DRIP: operator trust classification w/o Internet



Using small database on device (e.g., phone) listing only thousands of registries (not millions of UAS), Observer determines quadcopter is in general public registry & fixed wing in Observer trusted registry (of trusted operators) using UA broadcast ID certificate.

DRIP: operator registration

Operator generates HI keypair (**HIo** / **HIo(priv)**) along with cert **Coo**.
Operator sends **Coo** to Registry.

Registry validates **Coo** and makes decision to add Operator to Registry.
Registry (using its HI keypair) creates **Cro** and securely sends it back to Operator for confirmation.

DRIP: ua registration

General Public Observer

Public Safety Observer

(5) Operator securely embeds UA keypair and **Cra** into UA

Internet

(2) Operator sends, **Caa** and **Coa** to Registry

UA1
Pilot / Operator

UA2
Pilot / Operator

(1) Operator creates HI keypair for UA (**HIa** / **HIa(priv)**), generates cert **Caa** using them.
Operator using *his keypair* creates **Coa.**

(3.5) Registry adds HHIT and other info to DNS

(4) Croa and **Cra** are transmitted securely back to Operator/UA

(3) Registry validates **Caa**, plus inspects **Coa** and makes decision to add UA to Registry.
Registry (using its HI keypair) creates **Croa** as proof of registration of UA to Operator.
Registry also creates **Cra** to be used in DRIP Auth. Message.

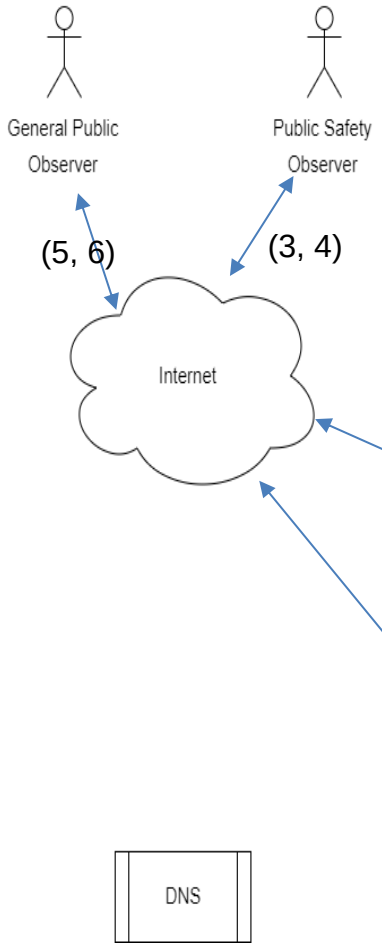
Public Registry

DNS

Private Registry

RDAP/XACML: access controlled registry lookup

(5, 6) Observer w/credentials not satisfying access control policy of this registration gets denied PII of Operator [XACML Request + Denial].



(3, 4) Observer w/credentials satisfying access control policy looks up PII of Operator [XACML Authorized RDAP Query + Response].

Leverage scalable protocols, infrastructure & business models of Internet domain name registration.

(1, 2) Operator privately registers HHIT based domain name.

DRIP General Requirements *easily satisfied* if UAS ID is a HHIT w/proposed new crypto in DNS & Whois, **plus HIP is deployed on participating UTM nodes**

1. *verify that messages originated from the claimed sender*
2. *verify that the UAS ID is in a registry & identify which one*
3. *lookup, from the UAS ID, public information*
4. *lookup, w/AAA, per policy, private information*
5. *structure information for both human and machine readability*
6. *provision registries with*
    1. *static information on the UAS & its Operator / Pilot In Command / Remote Pilot*
    2. *dynamic information on its current operation within the UTM*
    3. *Internet direct contact information for services related to the foregoing*
7. *close the AAA-policy registry loop by*
    1. *governing AAA per registered policies*
    2. *administering policies only via AAA*
8. ***dynamically establish, w/AAA, per policy, E2E strongly encrypted communications w/the UAS RID sender & entities looked up from the UAS ID, inc. the GCS & USS***

It is highly desirable that Broadcast RID receivers also be able to stamp messages with accurate date/time received and receiver location, then relay them to a network service (e.g. distributed ledger), *inter alia* for correlation to assess sender & receiver veracity.

DRIP: Observer to Pilot (O2P) comms

Steps:
(1) RID Bluetooth Broadcast
(2) DNS Query
(3) HIP Resource Record
(4) XACML Authorized RDAP Query
(5) Operator Personally Identifiable Information (PII)
(6,7) HIP sets up IPsec ESP Bound End-to-End Tunnel (BEET)

Observer w/credentials satisfying access control policy instantly establishes mutually authenticated, strongly encrypted comms w/pilot (e.g. to command exit from emergency UVR).

Pilot/Operator gets alert in web browser, accepts SIP VoIP call from Observer.

DRIP UAS Identifier Requirements *satisfied* by a HHIT in DNS & Whois (w/RDAP, EPP & XACML)

1. *20 bytes or smaller*
2. *sufficient to identify a registry in which the UAS is listed*
3. *sufficient to enable lookup of other data in that registry*
4. *unique within a to-be-defined scope*
5. *non-spoofable within the context of Remote ID broadcast messages (some collection of messages provides proof of UA ownership of ID)*

- A DRIP UAS ID MUST NOT facilitate adversarial correlation of UAS operational patterns; this may be accomplished e.g. by limiting each identifier to a single use, but if so, the UAS ID MUST support defined scalable timely registration methods.

- *Mechanisms standardized in DRIP MUST be capable of proving ownership of a claimed UAS ID, and SHOULD be capable of doing so immediately on an observer device lacking Internet connectivity at the time of observation.*

- *Mechanisms standardized in DRIP MUST be capable of verifying that messages claiming to have been sent from a UAS with a given UAS ID indeed came from the claimed sender.*

DRIP UAS Identifier Requirements Identifiers *satisfied* by a HHIT in DNS & Whois (w/RDAP, EPP & XACML) **used for only 1 UAS flight**

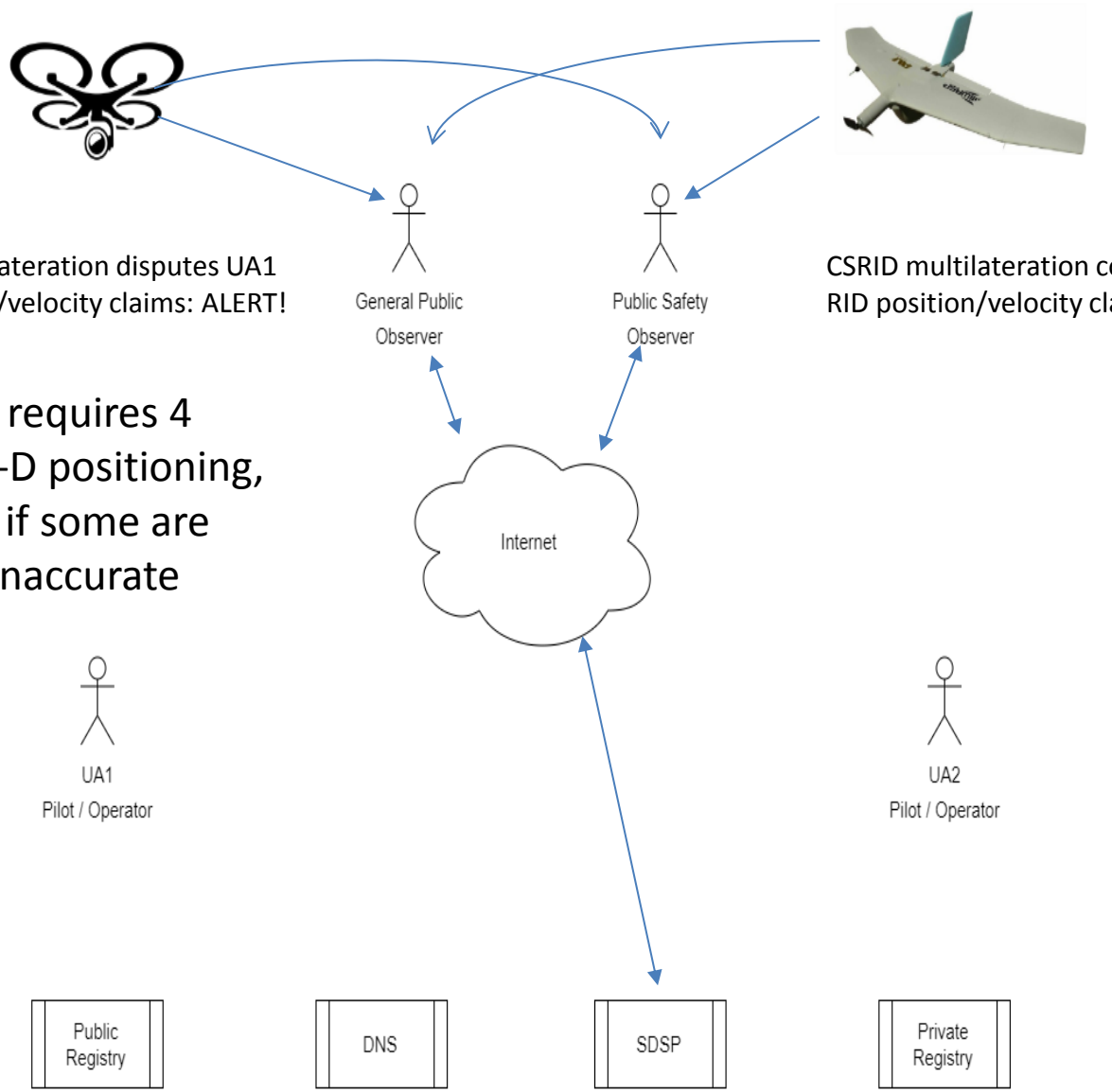
1. *20 bytes or smaller*
2. *sufficient to identify a registry in which the UAS is listed*
3. *sufficient to enable lookup of other data in that registry*
4. *unique within a to-be-defined scope*
5. *non-spoofable within the context of Remote ID broadcast messages (some collection of messages provides proof of UA ownership of ID)*

- ***A DRIP UAS ID MUST NOT facilitate adversarial correlation of UAS operational patterns; this may be accomplished e.g. by limiting each identifier to a single use, but if so, the UAS ID MUST support defined scalable timely registration methods.***

- *Mechanisms standardized in DRIP MUST be capable of proving ownership of a claimed UAS ID, and SHOULD be capable of doing so immediately on an observer device lacking Internet connectivity at the time of observation.*

- *Mechanisms standardized in DRIP MUST be capable of verifying that messages claiming to have been sent from a UAS with a given UAS ID indeed came from the claimed sender.*

Crowd Sourced RID (CS-RID): Broadcast RID → Network RID Gateway & Multilateration



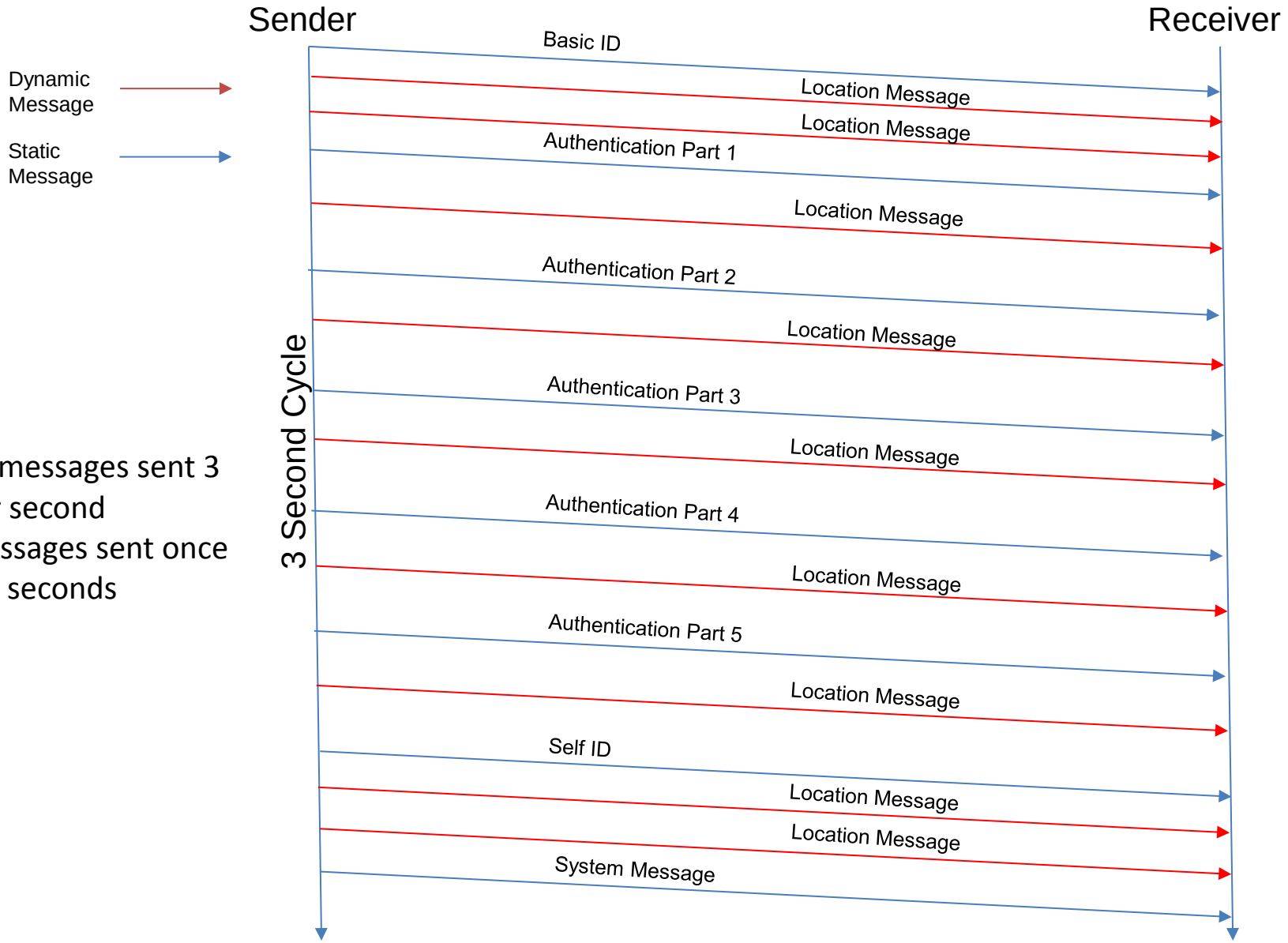
Multilateration requires 4 observers for 3-D positioning, more help esp. if some are [intentionally] inaccurate

Urgent Need

- Stakeholder needs recognized by regulators will influence standards that manufacturers will follow in producing aircraft & ground systems that will remain in use for many years.
- UTM & UAS RID will facilitate airspace useful Situational Awareness *only if* information is **immediately actionable.**
  - Trustworthy
    - Balance privacy of operators with legitimate authorities' Need To Know
    - Robust against cyber attack, poor wireless connectivity & clueless/careless operators
  - Enable observers to instantly determine UAS operator trust class (even w/o Internet)
  - Enable observers to instantly establish secure comms w/operator (w/IP connectivity)
  - Enable observers to confirm claimed position and velocity
- Much can be achieved by adopting/adapting existing Internet standards & infrastructure.
- We have gone a ways down the HIP road but are open to anything meeting the need.
- **We need your help!**

BACKUP SLIDES

UAS RID Authenticated Message Passing (AX prototype)



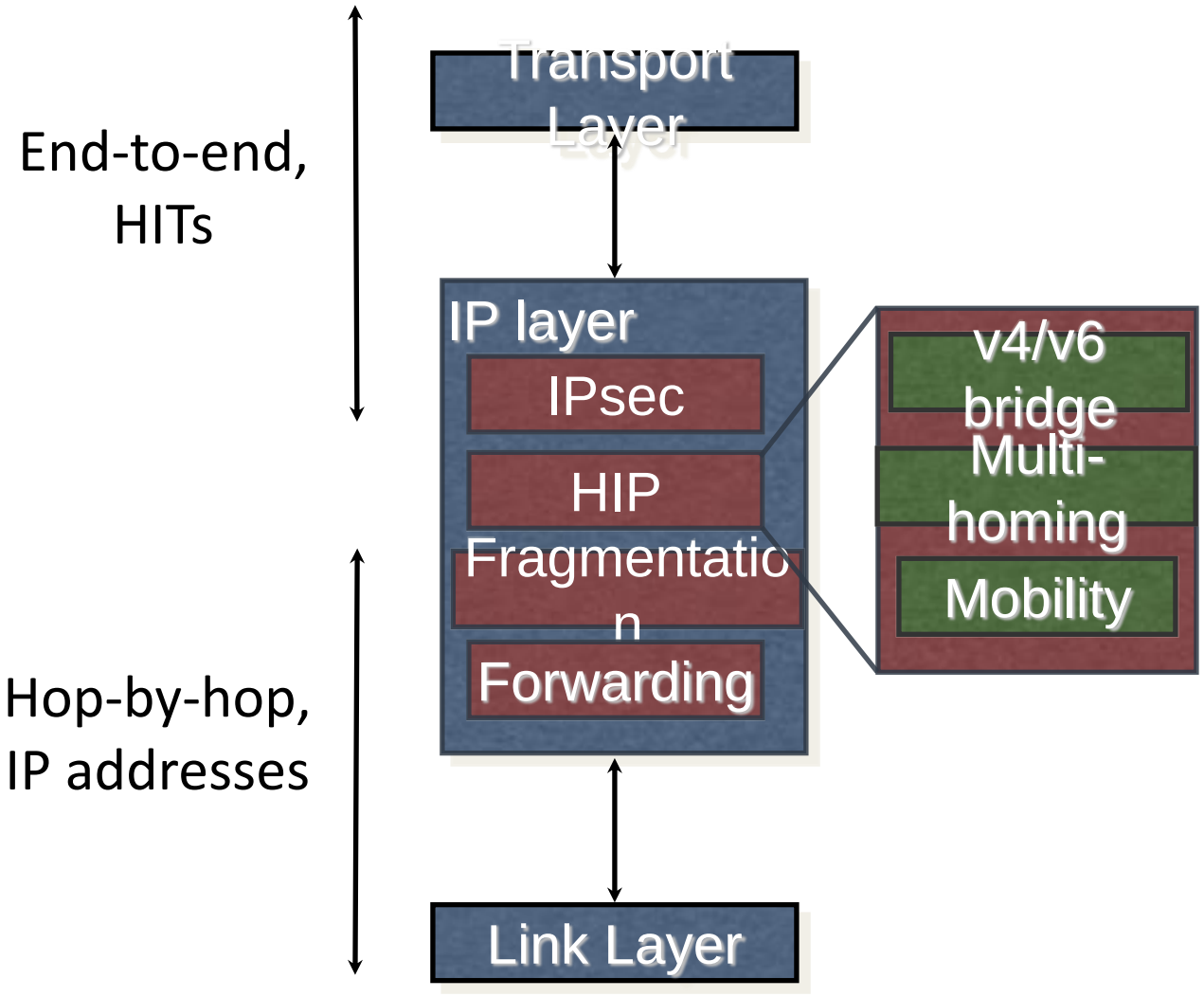
- Dynamic messages sent 3 times per second
- Static Messages sent once per three seconds

HIP Benefits

HIP is standardized in IETF Requests For Comment (RFCs) 4423[bis], 7343 (Overlay Routable Cryptographic Hash Identifier, ORCHID), 7401, 8002 - 8005

- HIP benefits for general network applications
  - Give each device a persistent identifier that remains the same across IP address changes, enabling persistent security associations & TCP connections
  - Give all packets a provenance, as in the "Secure Mobile Architecture" (Boeing, Lockheed-Martin, *et al*) described in, R. Paine's *Beyond HIP: The End to Hacking As We Know It*
  - Auto-configure IPsec VPNs (frustrating to do manually)
- HIP benefits for aero networking applications
  - Associate persistent identifier with aircraft tail #
  - Multihoming for make-before-break smooth handoff
- HIP benefits for the UAS RID application
  - With Internet connectivity (Network RID), also facilitates dynamic establishment of encrypted, mutually authenticated **secure comms** between Observer & UAS Pilot or Proxy (O2P2)
  - With standardized vetting by hierarchical registries, makes UAS ID & any other cryptographically signed claims **trustworthy** even w/o Internet connectivity (Broadcast RID)

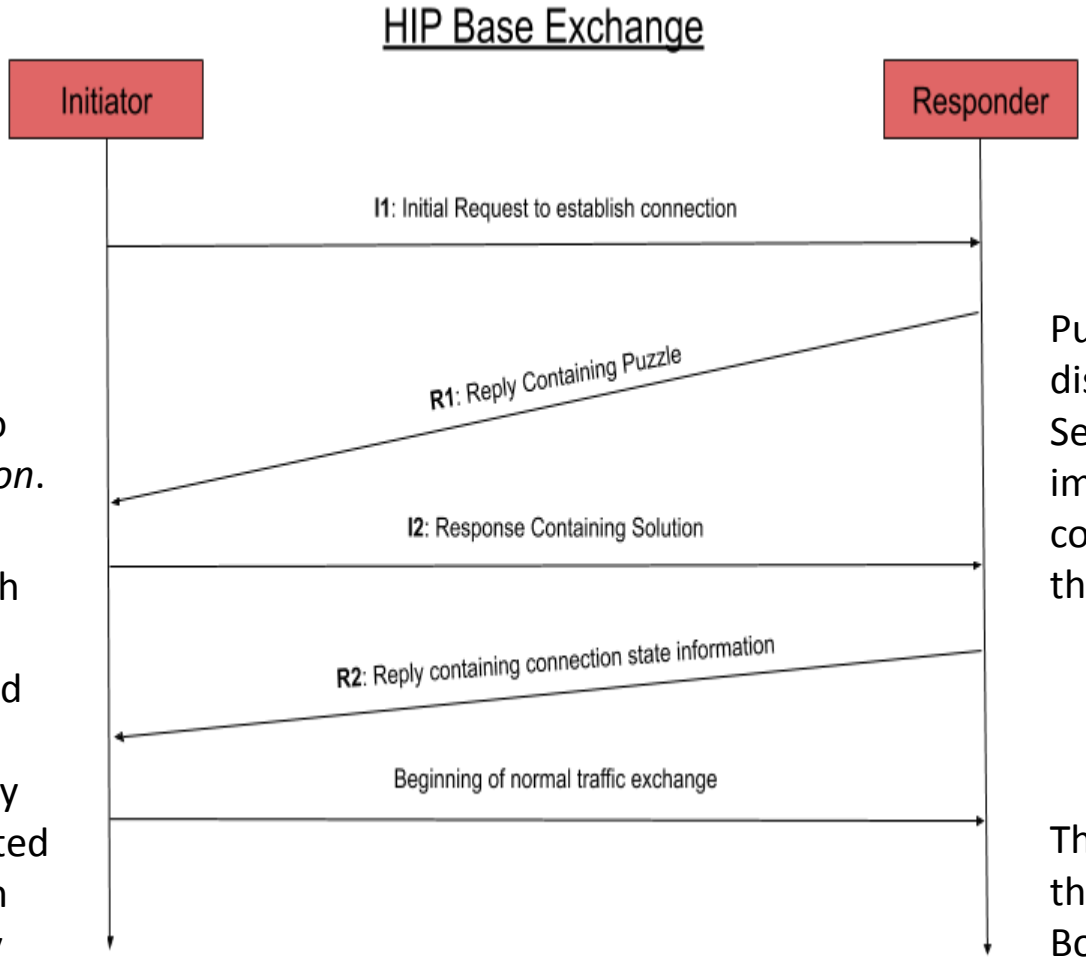
Where HIP Fits in the TCP/IP Stack



How HIP Mutually Authenticates Endpoint Identities

Initiator wants to contact a specific *identity*, has already looked it up in DNS to find its current *location*.

Now identities of both endpoints have been strongly authenticated & an IPsec Encapsulating Security Payload (ESP) encrypted tunnel between them has been dynamically established.



Puzzle defeats distributed Denial of Service attacks by imposing a computational cost on the initiator.

The normal traffic flows through the secure Bound End-to-End Tunnel (BEET).

Encode a HHIT as an ASTM F3411-19 UAS ID Type 1 or Type 3?

- Comply w/ANSI-CTA-2063-A.
- Set length field to “F” encoding value 15.
- In 15 character serial “number” field, encode:
  - last nibble of IANA HHIT prefix (1 char);
  - ORCHID Generating Algorithm ID (1 char);
  - 64 bit hash of HI (13 chars, 5 bits each).
- In DNS, map 4 character Manufacturer ID to a HHIT registry (RRA + HDA).
- Also map Type 3 (UUIDv4) values to HHITs in DNS?
  - UUIDv6 proposed Monday in ART looks interesting…

Encode a HHIT as an ASTM UAS ID Type 1 or Type 3?