Workgroup: DRIP
Internet-Draft:
draft-moskowitz-drip-crowd-sourced-rid-12
Published: 8 April 2024
Intended Status: Standards Track
Expires: 10 October 2024
Authors: R. Moskowitz, HTT Consulting
S. Card, AX Enterprize
A. Wiethuechter, AX Enterprize
S. Zhao, Intel
H. Birkholz, Fraunhofer SIT

Crowd Sourced Remote ID

Abstract

This document describes using the ASTM Broadcast Remote ID (B-RID) specification in a "crowd sourced" smart phone or fixed receiver asset environment to provide much of the ASTM and FAA envisioned Network Remote ID (Net-RID) functionality. This crowd sourced B-RID (CS-RID) data will use multilateration to add a level of reliability in the location data on the Uncrewed Aircraft (UA). The crowd sourced environment will also provide a monitoring coverage map to authorized observers.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 10 October 2024.

Table of Contents

1. Introduction

This document defines a mechanism to capture the ASTM Broadcast Remote ID messages (B-RID) [F3411-22a] on any Internet connected device that receives them and can forward them to the Supplemental Data Service Providers (SDSPs) responsible for the geographic area the UA and receivers are in. This crowd sourced B-RID (CS-RID) will create a ecosystem that will meet most if not all data collection requirements that Civil Aviation Authorities (CAA) are placing on Network Remote ID (Net-RID).

These Internet connected B-RID receivers are herein called "Finders", as they find UAs by listening for B-RID messages. The Finders are B-RID forwarding proxies. Their potentially limited spacial view of RID messages could result in bad decisions on what messages to send to the SDSP and which to drop. Thus they will send all received messages and the SDSP will make any filtering decisions in what it forwards into the UAS Traffic Management (UTM).

Finders can be smartphones, tablets, connected cars, or any computing platform with Internet connectivity that can meet the requirements defined in this document. It is not expected, nor necessary, that Finders have any information about a UAS beyond the content in the B-RID messages.

The SDSPs are similar to, but different from the Surveillance SDSPs in [F3623-23]. [F3623-23] defines sensors which are predominately radars, similar to Appendix A. The difference stems from [F3623-23] orientation with ICAO Aircraft numbers and aviation radar history of tracking objects in flight and trying to feed that data into UTM. It is likely that this document will act as guidance to [F3623-23] for future revisions to better align it with UTM over manned aviation Aircraft Traffic Control (ATC).

Finders MAY only need a loose association with the SDSP(s). They may only have the SDSP's Public Key and FQDN. It would use these, along with the Finder's Public Keypair to use Elliptic Curve Integrated Encryption Scheme (ECIES), or other security methods, to send the messages in a secure manner to the SDSP. The SDSP MAY require a stronger relationship to the Finders. This may range from the Finder's Public Key being registered to the SDSP with other information so that the SDSP has some level of trust in the Finders to requiring transmissions be sent over long-lived transport connections like ESP [RFC4303] or DTLS [RFC5238].

If a 1-way only secure packet forwarding method is used (e.g., not a TCP connection), the Finder SHOULD receive periodic "heartbeats" from the SDSP to inform it that its transmissions are being

received. The SDSP sets the rules on when to send these heartbeats as discuss below in Section 4.1.

1.1. Role of Supplemental Data Service Provider (SDSP)

The DRIP Architecture [RFC9434] introduces the basic CS-RID entities including CS-RID Finder and CS-RID SDSP. This document has minimal information about the actions of SDSPs. In general the SDSP is out of scope of this document. That said, the SDSPs should not simply proxy B-RID messages to the UTM(s). They should perform some minimal level of filtering and content checking before forwarding those messages that pass these tests in a secure manner to the UTM(s).

The SDSPs are also capable of maintaining a monitoring map, based on location of active Finders. UTMs may use this information to notify authorized observers of where there is and there is not monitoring coverage. They may also use this information of where to place pro-active monitoring coverage.

An SDSP should only forward Authenticated B-RID messages like those defined in [drip-authentication] to the UTM(s). Further, the SDSP SHOULD validate the Remote ID (RID) and the Authentication signature before forwarding anything from the UA, and flagging those RIDs that were not validated. The SDSP MAY forward all B-RID messages to the UTM, leaving all decision making on B-RID messages veracity to the UTM.

When 3 or more Finders are reporting to an SDSP on a specific UA, the SDSP is in a unique position to perform multilateration on these messages and compute the Finder's view of the UA location to compare with the UA Location/Vector messages. This check against the UA's location claims is both a validation on the UA's reliability as well as the trustworthiness of the Finders. Other than providing data to allow for multilateration, this SDSP feature is out of scope of this document. This function is limited by the location accuracy for both the Finders and UA.

1.2. Draft Status

This draft is still incomplete. New features are being added as capabilities are researched. The actual message formats also still need work.

2. Terms and Definitions

2.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in

BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses terms defined in [RFC9153] and [RFC9434].

2.2. Definitions

B-RID:
Broadcast Remote ID. A method of sending RID messages as 1-way transmissions from the UA to any Observers within radio range.

ECIES: Elliptic Curve Integrated Encryption Scheme. A hybrid encryption scheme which provides semantic security against an adversary who is allowed to use chosen-plaintext and chosen-ciphertext attacks.

Finder: In Internet connected device that can receive B-RID messages and forward them to a UTM.

Multilateration: Multilateration (more completely, pseudo range multilateration) is a navigation and surveillance technique based on measurement of the times of arrival (TOAs) of energy waves (radio, acoustic, seismic, etc.) having a known propagation speed.

Net-RID: Network Remote ID. A method of sending RID messages via the Internet connection of the UAS directly to the UTM.

3. Problem Space

3.1. Meeting the needs of Network Remote ID

The USA Federal Aviation Authority (FAA), in the January 2021 Remote ID Final rule [FAA-FR], postponed Network Remote ID (Net-RID) and focused on Broadcast Remote ID. This was in response to the UAS vendors comments that Net-RID places considerable demands on then currently used UAS.

However, Net-RID, or equivalent, is necessary for UTM and knowing what soon may be in an airspace. A method that proxies B-RID into UTM can function as an interim approach to Net-RID and continue as a adjunct to Net-RID.

3.2. Advantages of Broadcast Remote ID

B-RID has its advantages over Net-RID.

* B-RID can more readily be implemented directly in the UA. Net-RID will more frequently be provided by the GCS or a pilot's Internet connected device.

  - If Command and Control (C2) is bi-directional over a direct radio connection, B-RID could be a straight-forward addition.

  - Small IoT devices can be mounted on UA to provide B-RID.

* B-RID can also be used by the UA to assist in Detect and Avoid (DAA).

* B-RID is available to observers even in situations with no Internet like natural disaster situations.

3.3. Trustworthiness of Proxied Data

When a proxy is introduced in any communication protocol, there is a risk of corrupted data and DOS attacks.

The Finders, in their role as proxies for B-RID, are authenticated to the SDSP (see Section 4). The SDSP can compare the information from multiple Finders to isolate a Finder sending fraudulent information. SDSPs can additionally verify authenticated messages that follow [drip-authentication].

The SPDP can manage the number of Finders in an area (see Section 4.3) to limit DOS attacks from a group of clustered Finders.

3.4. Defense against fraudulent RID Messages

The strongest defense against fraudulent RID messages is to focus on [drip-authentication] conforming messages. Unless this behavior is mandated, SPDPs will have to use assorted algorithms to isolate messages of questionable content.

4. The Finder - SDSP Security Relationship

The SDSP(s) and Finders SHOULD use EdDSA [RFC8032] keys as their trusted Identities. The public keys SHOULD be registered DRIP UAS Remote ID [RFC9374] and [drip-registries]. Other similar methods may be used.

During this registration, the Finder gets the SDSP's EdDSA Public Key. These Public Keys allow for the following options for authenticated messaging from the Finder to the SDSP.

The SDSP uses some process (out of scope here) to register the Finders and their EdDSA Public Key. During this registration, the Finder gets the SDSP's EdDSA Public Key. These Public Keys allow for the following options for authenticated messaging from the Finder to the SDSP.

1. EdDSA keys are converted to X25519 keys per Curve25519 [RFC7748] to use in ECIES.

2. ECIES can be used with a unique nonce to authenticate each message sent from a Finder to the SDSP.

3. ECIES can be used at the start of some period (e.g. day) to establish a shared secret that is then used to authenticate each message sent from a Finder to the SDSP sent during that period.

4. HIP [RFC7401] can be used to establish a session secret that is then used with ESP [RFC4303] to authenticate each message sent from a Finder to the SDSP.

5. DTLS [RFC5238] can be used to establish a secure connection that is then used to authenticate each message sent from a Finder to the SDSP.

4.1. SDSP Heartbeats

If a 1-way messaging approach is used (e.g. not TCP-based), the SDSP SHOULD send a heartbeat at some periodicity to the Finders so that they get confirmation that there is a receiver of their transmissions.

A simple (see Section 6.6) message that identifies the SDSP is sent to the Finder per some published policy of the SDSP. For example, at the first reception by the SDSP for the day, then the 1st for the hour. It is NOT recommended for the SDSP to send a heartbeat for every message received, as this is a potential DOS attack against the SDSP.

4.2. The Finder Map

The Finders are regularly providing their SDSP with their location. This is through the B-RID Proxy Messages and Finder Location Update Messages. With this information, the SDSP can maintain a monitoring map. That is a map of where there Finder coverage.

4.3. Managing Finders

Finder density will vary over time and space. For example, sidewalks outside an urban train station can be packed with pedestrians at

rush hour, either coming or going to their commute trains. An SDSP may want to proactively limit the number of active Finders in such situations.

Using the Finder mapping feature, the SDSP can instruct Finders to NOT proxy B-RID messages. These Finders will continue to report their location and through that reporting, the SDSP can instruct them to again take on the proxying role. For example a Finder moving slowly along with dozens of other slow-moving Finders may be instructed to suspend proxying. Whereas a fast-moving Finder at the same location (perhaps a connected car or a pedestrian on a bus) would not be asked to suspend proxying as it will soon be out of the congested area.

5. UA location via multilateration

The SDSP can confirm/correct the UA location provided in the Location/Vector message by using multilateration on data provided by at least 3 Finders that reported a specific Location/Vector message (Note that 4 Finders are needed to get altitude sign correctly). In fact, the SDSP can calculate the UA location from 3 observations of any B-RID message. This is of particular value if the UA is only within reception range of the Finders for messages other than the Location/Vector message.

This feature is of particular value when the Finders are fixed assets with highly reliable GPS location, around a high value site like an airport or large public venue.

5.1. GPS Inaccuracy

Single-band, consumer grade, GPS on small platforms is not accurate, particularly for altitude. Longitude/latitude measurements can easily be off by 3M based on satellite postion and clock accuracy. Altitude accuracy is reported in product spec sheets and actual tests to be 3x less accurate. Altitude accuracy is hindered by ionosphere activity. In fact, there are studies of ionospheric events (e.g. 2015 St. Patrick's day [gps-ionosphere]) as measured by GPS devices at known locations. Thus where a UA reports it is rarely accurate, but may be accurate enough to map to visual sightings of single UA.

Smartphones and particulary smartwatches are plagued with the same challenge, though some of these can combine other information like cell tower data to improve location accuracy. FCC E911 accuracy, by FCC rules is NOT available to non-E911 applications due to privacy concerns, but general higher accuracy is found on some smart devices than reported for consumer UA. The SDSP MAY have information on the Finder location accuracy that it can use in calculating the accuracy

of a multilaterated location value. When the Finders are fixed assets, the SDSP may have very high trust in their location for trusting the multilateration calculation over the UA reported location.

6. The CS-RID Messages

The CS-RID messages between the Finders and the SDSPs primarily support the proxy role of the Finders in forwarding the B-RID messages. There are also Finder registration and status messages.

CS-RID information is represented in CBOR [RFC7049]. COSE [RFC8152] MAY be used for CS-RID MAC and COAP [RFC7252] for the CS-RID protocol. The CDDL [RFC8610] specification is used for CS-RID message description.

The following is a general representation of the content in the CS-RID messages.

```
(
  CS-RID MESSAGE TYPE,
  CS-RID MESSAGE CONTENT,
  CS-RID MAC
)
```

The CS-RID MESSAGE CONTENT varies by MESSAGE TYPE.

6.1. CS-RID MESSAGE TYPE

The CS-RID MESSAGE TYPE is defined in Figure 1:

Number	CS-RID Message Type
0	Reserved
1	B-RID Forwarding
2	Finder Registration
3	SDSP Response
4	Finder Location
5	SDSP Heartbeat

Figure 1

6.1.1. CDDL description for CS-RID message type

The overall CS-RID CDDL description is structured in Figure 2.

```
CSRID_Object = {
  application-context,
  info                => info_message,
  proxy_message       => broadcast_rid_proxy_message,
  finder_registration => finder_registration_message,
  sdsp_response       => sdsp_response_message,
  location_update     => location_update_message,
  sdsp_heartbeat      => sdsp_heartbeat_message,
}

info_message = {
  common_message_members,
  message_content => tstr,
}

common_message_members = (
  message_type  => message_types,
  mac_address   => #6.37(bstr),
)

message_types = &(
  Reserved            : 0,
  BRD                 : 1,
  Finder-Registration : 2,
  SDSP-Response       : 3,
  Finder-Location     : 4,
)
```

Figure 2

The application context rule is defined in Figure 3 for CS-RID application identification and version negotiation.

```
application-context = (
  application => "DRIP-CSRID",
  ? version => uint .size(1..2),
)
```

Figure 3

The predefined CDDL text string labels (author note: for JSON currently, will move to CBOR uint keys in upcoming versions) used in the specification is listed in Figure 4.

```
application           = "application"
version               = "version"
info                  = "message_info"
proxy_message         = "proxy_message-type"
finder_registration   = "finder_registration"
sdsp_response         = "sdsp_response"
location_update       = "location_update"
sdsp_heartbeat        = "sdsp_heartbeat"
rid                   = "id"
message_type          = "message_type"
mac_address           = "mac_address"
message_content       = "message_content"
timestamp             = "timestamp"
gps                   = "gps"
radio_type            = "radio_type"
broadcast_mac_address = "broadcast_mac_address"
broadcast_message     = "broadcast_message"
sdsp_id               = "sdsp_id"
proxy_status_type     = "proxy_status_type"
update_interval       = "update_interval"
```

Figure 4

6.2. The CS-RID B-RID Proxy Message

The Finders add their own information to the B-RID messages, permitting the SDSP(s) to gain additional knowledge about the UA(s). The RID information is the B-RID message content plus the MAC address. The MAC address is critical, as it is the only field that links a UA's B-RID messages together. Only the ASTM Basic ID Message and possibly the Authentication Message contain the UAS ID field.

The Finders add an SDSP assigned ID, a 64 bit timestamp, GPS information, and type of B-RID media to the B-RID message. Both the timestamp and GPS information are for when the B-RID message(s) were received, not forwarded to the SDSP. All this content is MACed using a key shared between the Finder and SDSP.

The following is a representation of the content in the CS-RID messages.

```
  (
    CS-RID MESSAGE TYPE,
    CS-RID ID,
    RECEIVE TIMESTAMP,
    RECEIVE GPS,
    RECEIVE RADIO TYPE,
    B-RID MAC ADDRESS,
    B-RID MESSAGE,
    CS-RID MAC
  )
```

6.2.1. CS-RID ID

The CS-RID ID is the ID recognized by the SDSP. This may be an HHIT [RFC9374], or any ID used by the SDSP.

6.2.2. CDDL description for CS-RID B-RID Proxy Message

The broadcast CS-RID proxy CDDL is defined in Figure 5

```
broadcast_rid_proxy_message = {
  common_message_members,
  rid                   => tstr,
  timestamp             => tdate,
  gps                   => gps-coordinates,
  radio_type            => radio_types,
  broadcast_mac_address => #6.37(bstr),
  broadcast_message     => #6.37(bstr),
}

radio_types = &(
  EFL : 0,
  VLF : 1,
  LF  : 2,
  MF  : 3,
  HF  : 4,
  HF  : 5,
  VHF : 6,
  UHF : 7,
  SHF : 8,
  EHF : 9,
)

gps-coordinates = [
  latitude : float,
  longitude: float,
  altitude : float,
]
```

Figure 5

6.3. CS-RID Finder Registration

The CS-RID Finder MAY use [RFC7401] with the SDSP to establish a Security Association and a shared secret to use for the CS-RID MAC generation. In this approach, the HIP mobility functionality and [RFC4303] support are not used.

When HIP is used as above, the Finder Registration is a SDSP "wake up". It is sent prior to the Finder sending any proxied B-RID messages to ensure that the SDSP is able to receive and process the messages.

In this usage, the CS-RID ID is the Finder HIT. If the SDSP has lost state with the Finder, it initiates the HIP exchange with the Finder to reestablish HIP state and a new shared secret for the CS-RID B-RID Proxy Messages. In this case the Finder Registration Message is:

```
(
  CS-RID MESSAGE TYPE,
  CS-RID ID,
  CS-RID TIMESTAMP,
  CS-RID GPS,
  CS-RID MAC
)
```

6.3.1. CDDL description for Finder Registration

The CDDL for CS-RID Finder Registration is defined in Figure 6

```
finder_registration_message = {
  common_message_members,
  rid       => tstr,
  timestamp => tdate,
  gps       => gps-coordinates,
}

gps-coordinates = [
  latitude : float,
  longitude: float,
  altitude : float,
]
```

Figure 6

6.4. CS-RID SDSP Response

The SDSP MAY respond to any Finder messages to instruct the Finder on its behavior.

```
  (
    CS-RID MESSAGE TYPE,
    SDSP ID,
    CS-RID ID,
    CS-RID PROXY STATUS,
    CS-RID UPDATE INTERVAL,
    CS-RID MAC
  )
```

The Proxy Status instructs the Finder if it should actively proxy B-RID messages, or suspend proxying and only report its location.

The Update Interval is the frequency that the Finder SHOULD notify the SDSP of its current location using the Location Update message.

6.4.1. CDDL description for SDSP Response

The CDDL for CS-RID SDSP response is defined in Figure 7

```
sdsp_response_message = {
  common_message_members,
  sdsp_id           => tstr,
  rid               => tstr,
  proxy_status_type => proxy_status_types,
  update_interval   => uint,
}

gps-coordinates = [
  latitude : float,
  longitude: float,
  altitude : float,
]

proxy_status_types = &(
  0: "forward",
  1: "reverse",
  2: "bi-directional",
)
```

Figure 7

6.5. CS-RID Location Update

The Finder SHOULD provide regular location updates to the SDSP. The interval is based on the Update Interval from Section 6.4 plus a random slew less than 1 second. The Location Update message is only sent when no other CS-RID messages, containing the Finder's GPS location, have been sent since the Update Interval.

If the Finder has not recieved a SDSP Registration Response, a default of 5 minutes is used for the Update Interval.

```
(
  CS-RID MESSAGE TYPE,
  CS-RID ID,
  CS-RID TIMESTAMP,
  CS-RID GPS,
  CS-RID MAC
)
```

6.5.1. CDDL description for Location Update

The CDDL for CS-RID Location update is defined in Figure 8.

```
location_update_message = {
  common_message_members,
  rid       => tstr,
  timestamp => tdate,
  gps       => gps-coordinates,
}

gps-coordinates = [
  latitude : float,
  longitude: float,
  altitude : float,
]
```

Figure 8

6.6. SDSP Heartbeat

The SDSP SHOULD send a heartbeat message at some periodicity to the Finders so that they get confirmation that their is a receiver of their transmissions.

```
(
  CS-RID MESSAGE TYPE,
  SDSP ID,
  CS-RID TIMESTAMP,
)
```

6.6.1. CDDL description for SDSP Heartbeat

The CDDL for CS-RID Heartbeat is defined in Figure 9.

```
sdsp_heartbeat_messagege = {
  common_message_members,
  sdsp_id   => tstr,
  timestamp => tdate,
}
```

Figure 9

7. The Full CS-RID CDDL specification

```
<CODE BEGINS>
; CDDL specification for Crowd source RID
; It specifies a collection of CS message types
;

;
; The CSRID overall data structure

CSRID_Object = {
    application-context,
    info =>  info_message,
    proxy_message => broadcast_rid_proxy_message,
    finder_registration => finder_registration_message,
    sdsp_response => sdsp_response_message,
    location_update => location_update_message,
}

;
; Application context: general information about CSRID message

application-context = (
    application => "DRIP-CSRID", ; TBD: consider CBOR tag
    ? version => uint .size(1..2),
)

; These members are include in every message
common_message_members = (
    message_type => message_types,
    mac_address => #6.37(bstr),
)

;
; CSRID message general information

info_message = {
    common_message_members,
    message_content => tstr,
}

broadcast_rid_proxy_message = {
    common_message_members,
    rid => tstr,
    timestamp => tdate,
    gps => gps-coordinates,
    radio_type => radio_types,
    broadcast_mac_address => #6.37(bstr)
    broadcast_message => #6.37(bstr)
}

finder_registration_message = {
```

```
    common_message_members,
    rid => tstr,
    timestamp => tdate,
    gps => gps-coordinates,
}

sdsp_response_message = {
    common_message_members,
    sdsp_id => tstr,
    rid => tstr,
    proxy_status_type => proxy_status_types,
    update_interval => uint,
}

location_update_message = {
    common_message_members,
    rid => tstr,
    timestamp => tdate,
    gps => gps-coordinates,
}

;
; Common rule definition

message_types = &(
    Reserved            : 0,
    BRD                 : 1,
    Finder-Registration : 2,
    SDSP-Response       : 3,
    Finder-Location     : 4,
)

gps-coordinates = [
    lat: float,
    long: float,
    alt : float,
]

; Radio types, choose from one of radio_types (required)
radio_types = &(
    EFL : 0,
    VLF : 1,
    LF  : 2,
    MF  : 3,
    HF  : 4,
    HF  : 5,
    VHF : 6,
    UHF : 7,
    SHF : 8,
```

```
    EHF : 9,
)

proxy_status_types = &(
    0: "forward",
    1: "reverse",
    2: "bi",
)

;
; JSON label names

application = "application"
version = "version"
info = "message_info"
proxy_message = "proxy_message-type"
finder_registration = "finder_registration"
sdsp_response = "sdsp_response"
location_update = "location_update"
rid = "id"
message_type = "message_type"
mac_address = "mac_address"
message_content = "message_content"
timestamp = "timestamp"
gps = "gps"
radio_type = "radio_type"
broadcast_mac_address = "broadcast_mac_address"
broadcast_message = "broadcast_message"
sdsp_id = "sdsp_id"
proxy_status_type = "proxy_status_type"
update_interval = "update_interval"

<CODE ENDS>
```

8. IANA Considerations

TBD

9. Security Considerations

TBD

9.1. Privacy Concerns

TBD

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/info/rfc8610>.

[RFC9153] Card, S., Ed., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements and Terminology", RFC 9153, DOI 10.17487/RFC9153, February 2022, <https://www.rfc-editor.org/info/rfc9153>.

10.2. Informative References

[drip-authentication] Wiethuechter, A., Card, S. W., and R. Moskowitz, "DRIP Entity Tag Authentication Formats & Protocols for Broadcast Remote ID", Work in Progress, Internet-Draft, draft-ietf-drip-auth-49, 21 February 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-drip-auth-49>.

[drip-registries] Wiethuechter, A. and J. Reid, "DRIP Entity Tag (DET) Identity Management Architecture", Work in Progress, Internet-Draft, draft-ietf-drip-registries-15, 1 April 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-drip-registries-15>.

[F3411-22a] ASTM International, "Standard Specification for Remote ID and Tracking", July 2022, <https://www.astm.org/f3411-22a.html>.

[F3623-23] ASTM International, "Standard Specification for Surveillance Supplementary Data Service Providers", December 2023, <https://www.astm.org/f3623-23.html>.

[FAA-FR] United States Federal Aviation Administration (FAA), "FAA Remote Identification of Unmanned Aircraft", January 2021, <https://www.govinfo.gov/content/pkg/FR-2021-01-15/pdf/2020-28948.pdf>.

[gps-ionosphere] "Ionospheric response to the 2015 St. Patrick's Day storm A global multi-instrumental overview", September 2015, <https://doi.org/10.1002/2015JA021629>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC5238] Phelan, T., "Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP)", RFC 5238, DOI 10.17487/RFC5238, May 2008, <https://www.rfc-editor.org/info/rfc5238>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[RFC9374] Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "DRIP Entity Tag (DET) for Unmanned Aircraft System Remote ID (UAS RID)", RFC 9374, DOI 10.17487/RFC9374, March 2023, <https://www.rfc-editor.org/info/rfc9374>.

[RFC9434] Card, S., Wiethuechter, A., Moskowitz, R., Zhao, S., Ed., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Architecture", RFC 9434, DOI 10.17487/RFC9434, July 2023, <https://www.rfc-editor.org/info/rfc9434>.

Appendix A. Using LIDAR for UA location

If the Finder has LIDAR or similar detection equipment (e.g. on a connected car) that has full sky coverage, the Finder can use this equipment to locate UAs in its airspace. The Finder would then be able to detect non-participating UAs. A non-participating UA is one that the Finder can "see" with the LIDAR, but not "hear" any B-RID messages.

These Finders would then take the LIDAR data, construct appropriate B-RID messages, and forward them to the SPDP as any real B-RID messages.

The MAC address for this messages SHOULD be a locally administered, random address. The Finder should make all effort to use the same address for a UA detected in this manner.

The UAS ID SHOULD be a UUIDv4 (Type=3). The Finder should make all effort to use the same UUID for a UA detected in this manner.

The SDSP would do the work of linking information on a non-participating UA that it has received from multiple Finders with LIDAR detection. In doing so, it would have to select a RemoteID to use.

A seemingly non-participating UA may actually be a UA that is beyond range for its B-RID but in the LIDAR range.

This would provide valuable information to SDSPs to forward to UTMs on potential at-risk situations.

At this time, research on LIDAR and other detection technology is needed. there are full-sky LIDAR for automotive use with ranges varying from 20M to 250M. Would more than UA location information be

available? What information can be sent in a CS-RID message for such "unmarked" UAs?

Acknowledgments

The Crowd Sourcing idea in this document came from the Apple "Find My Device" presentation at the International Association for Cryptographic Research's Real World Crypto 2020 conference.

Authors' Addresses

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
United States of America

Email: rgm@labs.htt-consult.com

Stuart W. Card
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: stu.card@axenterprize.com

Adam Wiethuechter
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: adam.wiethuechter@axenterprize.com

Shuai Zhao
Intel
2200 Mission College Blvd
Santa Clara, CA 95054
United States of America

Email: shuai.zhao@ieee.org

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
Germany

Email: henk.birkholz@sit.fraunhofer.de