Workgroup: DRIP
Published: 12 March 2020
Intended Status: Standards Track
Expires: 13 September 2020
Authors: R. Moskowitz, HTT Consulting; S. Card, AX Enterprize; A. Wiethuechter, AX Enterprize

Crowd Sourced Remote ID

Abstract

This document describes using the ASTM Broadcast Remote ID (B-RID) specification in a "crowd sourced" smart phone environment to provide much of the FAA mandated Network Remote ID (N-RID) functionality. This crowd sourced B-RID data will use multi-lateration to add a level of reliability in the location data on the Unmanned Aircraft (UA). The crowd sourced environment will also provide a monitoring coverage map to authorized observers.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document defines a mechanism to capture the ASTM Broadcast Remote ID messages (B-RID) [F3411-19] on any Internet connected device that receives them and can forward them to the SPDP(s) responsible for the geographic area the UA and receivers are in. This will create a ecosystem that will meet most if not all data collection requrтments that CAAs are placing on Network Remote ID (N-RID).

These Internet connected devices 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 SPDP and which to drop. The SPDP will make any filtering decisions in what it forwards to the UTM(s).

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.

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

This document has minimal information about the actions of SPDPs. In general the SPDP is out of scope of this document. That said, the SPDPs 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 SPDPs 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 this is and there is not monitoring coverage. They may also use there information of where to place pro-active monitoring coverage.

An SPDP SHOULD only forward Authenticated B-RID messages like those defined in [tmrid-auth] to the UTM(s). Further, the SPDP SHOULD validate the Remote ID (RID) and the Authentication signature before forwarding anything from the UA.

When 3 or more Finders are reporting to an SPDP on a specific UA, the SPDP 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 SPDP feature is out of scope of this document.

1.1. 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.

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.

CAA
: Civil Aeronautics Administration. An example is the Federal Aviation Administration (FAA) in the United States of America.

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.

GCS
: Ground Control Station. The part of the UAS that the remote pilot uses to exercise C2 over the UA, whether by remotely exercising

UA flight controls to fly the UA, by setting GPS waypoints, or otherwise directing its flight.

Finder

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

Observer

Referred to in other UAS documents as a "user", but there are also other classes of RID users, so we prefer "observer" to denote an individual who has observed an UA and wishes to know something about it, starting with its RID.

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.

NETSP

Network RID Service Provider. USS receiving Network RID messages from UAS (UA or GCS), storing for a short specified time, making available to NETDP.

NETDP

Network RID Display Provider. Entity (might be USS) aggregating data from multiple NETSPs to answer query from observer (or other party) desiring Situational Awareness of UAS operating in a specific airspace volume.

N-RID

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

RID

Remote ID. A unique identifier found on all UA to be used in communication and in regulation of UA operation.

SDSP

Supplemental Data Service Provider. Entity providing information that is allowed, but not required to be present in the UTM system.

UA

Unmanned Aircraft. In this document UA's are typically though of as drones of commerical or military variety. This is a very strict definition which can be relaxed to include any and all aircraft that are unmanned.

UAS

Unmanned Aircraft System. Composed of Unmanned Aircraft and all required on-board subsystems, payload, control station, other required off-board subsystems, any required launch and recovery equipment, all required crew members, and C2 links between UA and the control station.

UTM

UAS Traffic Management. A "traffic management" ecosystem for uncontrolled operations that is separate from, but complementary to, the FAA's Air Traffic Management (ATM) system.

USS

UAS Service Supplier. Provide UTM services to support the UAS community, to connect Operators and other entities to enable information flow across the USS network, and to promote shared situational awareness among UTM participants. (From FAA UTM ConOps V1, May 2018).

3. Problem Space

3.1. Meeting the needs of Network ID

The Federal (US) Aviation Authority (FAA), in the December 31, 2019 Remote ID Notice of Proposed Rulemaking [FAA-NPRM], is requiring "Standard" and "Limited" Remote ID. Standard is when the UAS provides both Network and Broadcast RID. Limited is when the UAS provides only Network RID. The FAA has dropped their previous position on allowing for only Broadcast RID. We can guess as to their reasons; they are not spelled out in the NPRM. It may be that just B-RID does not meet the FAA's statutory UA tracking responsibility.

The UAS vendors have commented that N-RID places considerable demands on currently used UAS. For some UAS like RC planes, meaningful N-RID (via the Pilot's smartphone) are of limited value. A mechanism that can augment B-RID to provide N-RID would help all members of the UAS environment to provide safe operation and allow for new applications.

3.2. Trustworthiness of Proxied Data

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

3.3. Defense against fraudulent RID Messages

TBD

TBD

4. The Finder - SPDP Security Relationship

The SPDP(s) and Finders SHOULD use EDDSA keys as their trusted Identities. The public keys SHOULD be registered Hierarchical HITS, [hierarchical-hit] and [hhit-registries].

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

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

2. 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 SPDP sent during that period.

3. HIPv2 [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 SPDP.

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

4.1. The Finder Map

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

5. The CS-RID Messages

The CS-RID messages between the Finders and the SPDPs 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 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.

5.1. CS-RID MESSAGE TYPE

The CS-RID MESSAGE TYPE is:

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

5.2. The CS-RID B-RID Proxy Message

The Finders add their own information to the B-RID messages, permitting the SPDP(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 SPDP 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 SPDP. All this content is MACed using a key shared between the Finder and SPDP.

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)
```

5.2.1. CS-RID ID

The CS-RID ID is the ID recognized by the SPDP. This may be an HHIT Hierarchical HITs [hierarchical-hit], or any ID used by the SPDP.

5.3. CS-RID Finder Registration

The CS-RID Finder MAY use HIPv2 [RFC7401] with the SPDP to establish a Security Association and a shared secret to use for the CS-RID MAC generation. In this approach, the HIPv2 mobility functionality and ESP [RFC4303] support are not used.

When HIPv2 is used as above, the Finder Registration is a SPDP "wake up". It is sent prior to the Finder sending any proxied B-RID messages to ensure that the SPDP is able to receive and process the messages.

In this usage, the CS-RID is the Finder HIT. If the SPDP 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)
```

5.4. CS-RID SPDP Registration Response

The SPDP responds to the Finder Registration with a message that includes an update interval. This interval is the frequency that the Finder SHOULD notify the SPDP of its current location.

```
(   CS-RID MESSAGE TYPE,
    SPDP ID,
    CS-RID ID,
    CS-RID UPDATE INTERVAL,
    CS-RID MAC)
```

5.5. CS-RID Location Update

The Finder SHOULD provide regular location updates to the SPDP. The interval is based on the Update Interval from Section 5.4 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 SPDP 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. IANA Considerations

TBD

7. Security Considerations

TBD

7.1. Privacy Concerns

TBD

8. 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.

9. 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>.

[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>.

10. Informative References

[F3411-19] ASTM International, "Standard Specification for Remote ID and Tracking", February 2020, <http://www.astm.org/cgi-bin/resolver.cgi?F3411>.

[FAA-NPRM] Federal (US) Aviation Authority, "FAA Remote ID Notice of Proposed Rule Making", December 2019, <https://www.regulations.gov/docket?D=FAA-2019-1100>.

[hhit-registries]
Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HIT Registries", Work in Progress, Internet-Draft, draft-moskowitz-hip-hhit-registries-01, 17 October 2019, <https://tools.ietf.org/html/draft-moskowitz-hip-hhit-registries-01>.

[hierarchical-hit]
Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HITs for HIPv2", Work in Progress, Internet-Draft, draft-moskowitz-hip-hierarchical-hit-03, 16 December 2019, <https://tools.ietf.org/html/draft-moskowitz-hip-hierarchical-hit-03>.

[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>.

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

[tmrid-auth] Wiethuechter, A., Card, S., and R. Moskowitz, "TM-RID Authentication Formats", Work in Progress, Internet-Draft, draft-wiethuechter-tmrid-auth-05, 18 February 2020, <https://tools.ietf.org/html/draft-wiethuechter-tmrid-auth-05>.

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.

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

At this time, research on LIDAR and other detection technology is needed. Would more than UA location information be available? What information can be sent in a CS-RID message for such "unmarked" UAs?

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