drip Working Group
Internet-Draft
Intended status: Standards Track
Expires: 4 September 2025

R. Moskowitz
HTT Consulting
A. Wiethuechter
AX Enterprize
3 March 2025

Crowd Sourced Remote ID
draft-wiethuechter-drip-csrid-03

Abstract

This document describes a way for an Internet connected device to forward/proxy received Broadcast Remote ID into UAS Traffic Management (UTM). This is done through a Supplemental Data Service Provider (SDSP) that takes Broadcast Remote ID in from Finder and provides an aggregated view using Network Remote ID data models and protocols. This enables more comprehensive situational awareness and reporting of Unmanned Aircraft (UA) in a "crowd sourced" manner.

Table of Contents

1. Introduction 3
1.1. Role of Finders 3
1.2. Role of Supplemental Data Service Providers 3
1.3. Relationship between Finders & SDSPs 4
2. Document Objectives 4
3. Terms and Definitions 4
3.1. Requirements Terminology 4
3.2. Definitions 4
4. Problem Space 5
4.1. Advantages of Broadcast Remote ID 5
4.2. Meeting the needs of Network Remote ID 5
4.3. Trustworthiness of Proxy Data 5
4.4. Defense against fraudulent RID Messages 6
5. Crowd Sourced RID Protocol 6
5.1. Detection & Report Models 6
5.2. Session Security 7
5.2.1. CBOR Web Token Method 8
5.2.2. ECEIS Method 8
6. Transports 8
6.1. CoAP 8
6.2. HIP 9
7. IANA Considerations 9
8. Security Considerations 9
9. Acknowledgments 9
10. References 9
10.1. Normative References 9
10.2. Informative References 10
Appendix A. Network RID Overview 11
Appendix B. Additional SDSP Functionality 12
B.1. Multilateration 12
B.2. Finder Map 12
B.3. Managing Finders 13
Appendix C. GPS Inaccuracy 13
Authors' Addresses 13

1. Introduction

> Note: This document is directly related and builds from [MOSKOWITZ-CSRID]. That draft is a "top, down" approach to understand the concept and high level design. This document is a "bottom, up" implementation of the CS-RID concept. The content of this draft is subject to change and adapt as further development continues.

This document defines a mechanism to capture [F3411] Broadcast Remote ID (RID) messages on any Internet connected device that receives them and can forward them to Supplemental Data Service Providers (SDSPs) responsible for the geographic area the UA and receivers are in. This data can be aggregated and further decimated to other entities in Unmanned Aircraft Systems (UAS) Traffic Management (UTM) similar to [F3411] Network RID. It builds upon the introduction of the concepts and terms found in [RFC9434]. We call this service Crowd Sourced RID (CS-RID).

1.1. Role of Finders

These Internet connected devices are herein called "Finders", as they find UAs by listening for Broadcast RID. The Finders are Broadcast 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 SHOULD send all received messages and the SDSP will make any filtering decisions in what it forwards into the UTM.

Finders can be smartphones, tablets, connected cars, special purpose devices 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 found in Broadcast RID.

1.2. Role of Supplemental Data Service Providers

The SDSP provides a gateway service for supplemental data into UTM. This document focuses on RID exclusively, other types of supplemental data is out of scope for this document.

The primary role of a CS-RID SDSP is to aggregate reports from Finders and forward them as a subscription based service to UTM clients. These clients MAY be a USS or another SDSP. An CS-RID SDSP SHOULD NOT proxy raw data/reports into UTM. An CS-RID SDSP MAY provide such a service, but it is out of scope for this document.

An SDSP MAY have its coverage constrained to a manageable area that has value to its subscribers. An CS-RID SDSP MAY not allow public reports of Broadcast RID due to policy. Policies of SDSPs is out of scope for this document.

[F3411] Network RID is the defined interface (protocol and model) for an SDSP to provide Broadcast RID as supplemental data to UTM.

1.3. Relationship between Finders & SDSPs

Finders MAY only need a loose association with SDSPs. The SDSP MAY require a stronger relationship to the Finders. The relationship MAY be completely open, but still authenticated to requiring encryption. The transport MAY be client-server based (using things like HIP or DTLS) to client push (using things like UDP or HTTPS).

2. Document Objectives

This document standardizes transports between the Finder and SDSP. It also gives an overview of Network RID. Specific details of Network RID is out scope for this document. All models are specified in CDDL [RFC8610].

3. Terms and Definitions

3.1. 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].

3.2. Definitions

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 Broadcast RID messages and forward them to an SDSP.

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.

4. Problem Space

Broadcast and Network RID formats are both defined in [F3411] using the same data dictionary. Network RID is specified in JSON sent over HTTPS while Broadcast RID is octet structures sent over wireless links.

4.1. Advantages of Broadcast Remote ID

Advantages over Network RID include:

* more readily be implemented directly in the UA. Network 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, Broadcast RID could be a straight-forward addition.
  - Small IoT devices can be mounted on UA to provide Broadcast RID.
* also be used by the UA to assist in Detect and Avoid (DAA).
* is available to observers even in situations with no Internet like natural disaster situations.

4.2. Meeting the needs of Network Remote ID

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

However, Network RID, or equivalent, is necessary for UTM knowing what soon may be in an airspace and is mandated as required in the EU. A method that proxies Broadcast RID into UTM can function as an interim approach to Network RID and continue adjacent to Network RID.

4.3. Trustworthiness of Proxy 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 Broadcast RID, SHOULD be authenticated to the SDSP (see Section 5.2). 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-AUTH].

The SPDP can manage the number of Finders in an area (see Appendix B.3) to limit DOS attacks from a group of clustered Finders.

4.4. Defense against fraudulent RID Messages

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

5. Crowd Sourced RID Protocol

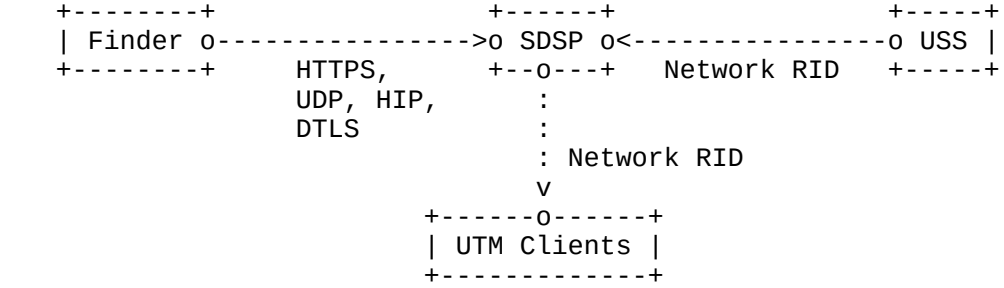

Figure 1: Protocol Overview

This document will focus on the general protocol specification between the Finder and the SDSP. Transport specification and use is provided in Section 6. A normative appendix (Appendix A) provides background to Network RID.

For all data models CBOR [RFC7049] MUST be used for encoding. JSON MAY be supported but its definition is out of scope for this document.

5.1. Detection & Report Models

The CS-RID model is for Finders to send "batch reports" to one or more SDSPs they have a relationship with. This relationship can be highly anonymous with little prior knowledge of the Finder to very well defined and pre-established.

Figure 2 is the report object, defined in CDDL, that is translated and adapted depending on the specific transport. It carries a batch of detections (up to a max of 10), the CDDL definition of which is shown in Figure 3.

```
report = [report_type: uint, report_time: time, finder_info: finder-info, ? report_data:
any]
finder-info: {
  finder_id: tstr / bstr / uuid / ip6,
  ? make: tstr,
  ? model: tstr,
  ? serial: tstr,
  ? ip_addr: ip4 / ip6,
  ? last_detect_time: time,
  ? position: #6.103
  ? status: any
}
```

Figure 2

```
detection = [timestamp: time, transport_type: &transport-types, mac_address: #6.48, data:
 bstr .size(26..255), ? rssi: uint, ? position: #6.103]
transport-types = (
  ble: 0, ble-lr: 1, beacon: 2, nan: 3
)
```

Figure 3

The position fields of both Figure 3 and Figure 2 are OPTIONAL. If multiple sets of these are present the deepest nested values take precedence. For example if position is used in both the Report and Detection structures then the value found in the individual Detections take precedence.

5.2. Session Security

Both Finder and SDSP SHOULD use EdDSA [RFC8032] keypairs as the base for their identities. These identities SHOULD be in the form of registered DRIP Entity Tags [RFC9374]. Registration is covered in [DIME-ARCH]. An SDSP MAY have its own DRIP Identity Management Entity (DIME) or share one with other entities in UTM.

An SDSP MUST NOT ignore Finders with DETs outside the DIME it is aware of, and SHOULD use [DIME-ARCH] to obtain public key information.

5.2.1. CBOR Web Token Method

A CWT is used to carry and apply a signature to the data. This is the primary method for sending data. A Claim ID of 170 is used for Report data.

5.2.2. ECEIS Method

ECIES is the preferred method to initialize a session between the Finder and SDSP. The following steps MUST be followed to setup ECIES for CS-RID:

1. Finder uses [DIME-ARCH] to obtain SDSP EdDSA key
2. EdDSA keys are converted to X25519 keys per Curve25519 [RFC7748] to use in ECIES
3. ECIES can be used with a unique nonce to authenticate each message sent from a Finder to the SDSP
4. 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
5. 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
6. 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

6. Transports

CS-RID transport from Finder to SDSP can vary from highly unidirectional with no acknowledgements to strong authenticated and encrypted sessions. Some transports, such as HIP and DTLS, MAY support bi-directional communication to enable control operations between the SDSP and Finder.

The section contains a variety of transports that MAY be supported by an SDSP. CoAP is the RECOMMENDED transport.

6.1. CoAP

When using CoAP [RFC7252] with UDP, a payload MUST be a CS-RID Report (Section 5.1). DTLS is the RECOMMENDED underlying transport for CoAP and uses a DET as the identity.

A Finder MUST ACK when accepting and RST when ignoring/rejecting a command from an SDSP.

As CoAP is designed with a stateless mapping to HTTP; such proxies are RECOMMENDED for CS-RID to allow as many Finders as possible to provide reports.

6.2. HIP

The use of HIP [RFC7401] imposes a strong authentication and Finder onboarding process. It is attractive for well defined deployments of CS-RID, such as being used for area security. A DET MUST be used as the primary identity when using this transport method.

The use of HIP as an underlying transport for CoAP is out of scope for this document.

7. IANA Considerations

TBD

8. Security Considerations

TBD

9. 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.

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/rfc/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/rfc/rfc8174>.

[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/rfc/rfc9153>.

10.2. Informative References

[DIME-ARCH] Wiethuechter, A. and J. Reid, "DRIP Entity Tags (DET) in the Domain Name System (DNS)", Work in Progress, Internet-Draft, draft-ietf-drip-registries-24, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-drip-registries-24>.

[DRIP-AUTH] 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>.

[F3411] ASTM International, "Standard Specification for Remote ID and Tracking", ASTM F3411-22A, DOI 10.1520/F3411-22A, July 2022, <https://www.astm.org/f3411-22a.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] Unknown, "Ionospheric response to the 2015 St. Patrick’s Day storm A global multi-instrumental overview", September 2015, <https://doi.org/10.1002/2015JA021629>.

[MOSKOWITZ-CSRID] Moskowitz, R., Card, S. W., Wiethuechter, A., Zhao, S., and H. Birkholz, "Crowd Sourced Remote ID", Work in Progress, Internet-Draft, draft-moskowitz-drip-crowd-sourced-rid-13, 9 October 2024, <https://datatracker.ietf.org/doc/html/draft-moskowitz-drip-crowd-sourced-rid-13>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/rfc8032>.

[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/rfc/rfc8610>.

[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/rfc/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/rfc/rfc9434>.

Appendix A. Network RID Overview

This appendix is normative and an overview of the Network RID portion of [F3411].

This appendix is intended a guide to the overall object of Network RID and generally how it functions in context with a CS-RID SDSP. Please refer to the actual standard of [F3411] for specifics in implementing said protocol.

For CS-RID the goal is for the SDSP to act as both a Network RID Service Provider (SP) and Network RID Display Provider (DP). The endpoints and models MUST follow the specifications for these roles so UTM clients do not need to implement specific endpoints for CS-RID and can instead leverage existing endpoints.

An SDSP SHOULD use Network RID, as it is able, to query a USS for UAS sending telemetry in a given area to integrate into the Broadcast RID it is receiving from Finders. How the SDSP discovers which USS to query is out of scope for this document.

An SDSP MUST provide the Network RID DP interface for clients that wish to subscribe for updates on aircraft in the SDSP aggregated coverage area.

Appendix B. Additional SDSP Functionality

This appendix is informative.

B.1. 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 Broadcast 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.

B.2. Finder Map

The Finders are regularly providing their SDSP with their location. With this information, the SDSP can maintain a monitoring map. That is a map of approximate coverage range of their registered and active Finders.

B.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 Broadcast 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.

Such operation SHOULD be using transports such as HIP or DTLS.

Appendix C. GPS Inaccuracy

This appendix is informative.

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 position 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 particularly 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.

Authors’ Addresses

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
United States of America
Email: rgm@labs.htt-consult.com

Adam Wiethuechter
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America
Email: adam.wiethuechter@axenterprize.com