Workgroup: DRIP
Internet-Draft:
draft-moskowitz-drip-secure-nrid-c2-09
Published: 17 June 2022
Intended Status: Standards Track
Expires: 19 December 2022

Authors: R. Moskowitz, HTT Consulting
S. Card, AX Enterprize
A. Wiethuechter, AX Enterprize
A. Gurtov, Linköping University

Secure UAS Network RID and C2 Transport

Abstract

This document defines a transport mechanism for Unmanned Aircraft System (UAS) Network Remote ID (Net-RID). The Broadcast Remote ID (B-RID) messages can be sent directly over UDP or via a more functional protocol using CoAP/CBOR for the Net-RID messaging. This is secured via either HIP/ESP or DTLS. HIP/ESP or DTLS secure messaging Command-and-Control (C2) for is also described.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document defines a set of messages for Unmanned Aircraft System (UAS) Network Remote ID (Net-RID) derived from the ASTM Remote ID [F3411-19] broadcast messages and common data dictionary. These messages are transported from the UAS to its USS Network Service Provider (Net-RID SP) either directly over UDP or via CoAP/CBOR ([RFC7252]/[RFC8949]).

Direct UDP, referred here as Minimal Net-RID (MNet-RID), and CoAP/CBOR were selected for their low communication "cost". This may not be an issue if Net-RID originates from the Ground Control Station (GCS, Section 3.1.2), but it may be an important determinant when originating from the UA (Section 3.1.1). Particularly, very small messages may open Net-RID transmissions over a variety of wireless technologies.

This document also defines mechanisms to provide secure transport for these Net-RID messages and Command and Control (C2) messaging.

A secure end-to-end transport for Net-RID (UAS to Network RID Service Provider (Net-RID SP)) also should provide full Confidentiality, Integrity, and Authenticity (CIA). It may seem that confidentiality is optional, as most of the information in Net-RID is sent in the clear in Broadcast Remote ID (B-RID), but this is a potentially flawed analysis. Net-RID has evesdropping risks not in B-RID and may contain more sensitive information than B-RID. The secure transport for Net-RID should also manage IP address changes (IP mobility) for the UAS.

A secure end-to-end transport for C2 is critical for UAS especially for Beyond Line of Sight (BLOS) operations. It needs to provide data CIA. Depending on the underlying network technology, this secure transport may need to manage IP address changes (IP mobility) for both the UA and GCS.

Two options for secure transport are provided: HIP [RFC7401] with ESP [RFC7402] and DTLS 1.3 [RFC9147]. These options are generally defined and their applicability is compared and contrasted. It is up to Net-RID and C2 to select which is preferred for their situation.

MOBIKE [RFC5266] is an alternative to HIP for ESP key establishment. It functions enough like HIP that it was left out, but implied, for document simplicity. There may be some identity pieces needed to map HHITs and HIs to what MOBIKE uses.

To further reduce the communication cost, SCHC [RFC8724] is defined for both the direct UDP and CoAP layer [RFC8824]. For ESP "compression", ESP Implicit IV, [RFC8750] and Diet ESP [diet-esp] may be used together. DTLS 1.3 [RFC9147] as defined in Section 5.2 is fully compressed. DTLS for MNet-RID would only benefit from UDP compression. CoAP Net-RID and C2 could benefit from specific application header compression.

UDP SCHC compression is handled separately here from IP header as is currently defined by IP carrier (e.g. LoRaWAN, [RFC9011]). This is to allow for the endpoints to not need to know what constrained carrier is in-path and just design for worst case. and will be covered in any specific implementation.

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

See Section 2.2 of [RFC9153] for common DRIP terms. The following new terms are used in the document:

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

MNet-RID
A Minimal implementation of Network Remote ID, based on B-RID messages directly over UDP.

Net-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.

3. Network Remote ID

In UAS Traffic Management (UTM), the purpose of Net-RID is to provide situational awareness of UA (in the form of flight tracking) in a user specified 3D volume. The data needed for this is already defined in [F3411-19], but a standard message format, protocol, and secure communications methodology are missing. F3411, and other UTM based standards going through ASTM and other SDOs, provide JSON objects and some of the messages for passing information between various UTM entities (e.g., Net-RID SP to Net-RID SP and Net-RID SP to Net-RID DP) but does not specify how the data gets into UTM to begin with. This document will provide such an open standard.

A full-function CoAP-based Net-RID protocol is defined in Section 3.4. This provides for either transport of the appropriate B-RID messages and/or the [F3411-19] data elements encoded in CBOR.

A minimal messaging approach (MNet-RID, Section 3.3), only using the Broadcast Remote ID (B-RID) messages in [F3411-19], is sufficient to meet the needs of Net-RID. These messages can be sent to the Net-RID SP when their contents change. Further, a UAS supporting B-RID will have minimal development to add Net-RID support.

This approach has the added advantage of being very compact, minimizing the Net-RID communications cost.

Other messages may be needed in some Net-RID situations. Thus a simple message multiplexer is provided for MNet-RID and CoAP is defined for a richer messaging environment.

3.1. Network RID Endpoints

The US FAA defines the Network Remote ID endpoints as a USS Network Service Provider (Net-RID SP) and the UAS. Both of these are rather nebulous items and what they actually are will impact how communications flow between them.

The Net-RID SP may be provided by the same entity serving as the UAS Service Provider (USS). This simplifies a number of aspects of the Net-RID communication flow. The Net-RID SP is likely to be stable in the network, that is its IP address will not change during a mission. This simplifies maintaining the Net-RID communications.

The UAS component in Net-RID may be either the UA, GCS, or the Operator's Internet connected device (e.g. smartphone or tablet that is not the GCS). In all cases, mobility MUST be assumed. That is the IP address of this end of the Net-RID communication may change during an operation. The Net-RID mechanism MUST support this. The UAS Identity for the secure connection may vary based on the UAS endpoint.

3.1.1. Net-RID from the UA

Some UA will be equipped with direct Internet access. These UA will also tend to have multiple radios for their Internet access (e.g., Cellular and WiFi). Thus multi-homing with "make before break" behavior is needed. This is on top of any IP address changes on any of the interfaces while in use.

Multicast (GEN-10 in [RFC9153]) over multiple Internet connection technologies MAY be used improve QOS (GEN-7 in [RFC9153]) for Net-RID. (Author's question: Is this really qualify as multicast?)

3.1.2. Net-RID from the GCS

Many UA will lack direct Internet access, but their GCS are connected. As an Operator is expected to register an operation with its USS, this may be done via the Internet connected GCS. The GCS could then be the source of the secure connection for Net-RID (acting as a gateway).

There are two sources of the RID messages for the GCS, both from the UA. These are UA B-RID messages, or content from C2 messages that the GCS converts to RID message format. In either case, the GCS may be mobile with changing IP addresses. The GCS may be in a fast moving ground device (e.g. delivery van), so it can have as mobility demanding connection needs as the UA.

In a constrained wireless environment for the UA that is not functioning autonomously (i.e., at least C2 traffic to the GCS), this approach may be the most economical. It only uses the wireless to send the UA status once, to the GCS, that then provides the Net-RID functionality.

3.1.3. Net-RID from the Operator

Many UAS will have no Internet connectivity, but the UA is sending B-RID messages and the Operator, when within RF range, can receive these B-RID messages on an Internet Connected device that can act as the proxy for these messages, turning them into Net-RID messages.

3.2. Network RID Messaging

Net-RID messaging is tied to a UA operation (generally called a flight or mission). This consists of an initial secure link setup, followed by a set of mostly static information related to the operation. During the operation, continuous location information is sent by the UA with any needed updates to the mostly static operation information.

The Net-RID SP SHOULD send regular "heartbeats" to the UAS. If the UAS does not receive these heartbeats for some policy set time, the UA MUST take the policy set response to loss of Net-RID SP connectivity. For example, this could be a mandated immediate landing. There may be other messages from the Net-RID SP to the UAS (e.g., call the USS operator at this number NOW!). The UAS MUST follow acknowledge policy for these messages.

If the Net-RID SP stops receiving messages from the UAS (Section 3.2.3), it should notify the UTM of a non-communicating UA while still in operation.

3.2.1. Secure Link Setup

The secure link setup MUST be done before the operation begins, thus it can use a high capacity connection like WiFi. It MAY use the UA RID for this setup, including other data elements provided in the B-

RID Basic ID (Msg Type 0x0) Message. If the Basic ID information is NOT included via the secure setup (including the Net-RID SP querying the USS for this information), it MUST be sent as part of the Static Messages (Section 3.2.2)

3.2.1.1. UAS Identity

The UAS MAY use its RID if it is a HHIT (DET per [drip-uas-rid]). It may use some other Identity, based on the Net-RID SP policy.

The GCS or Operator smart device may have a copy of the UA credentials and use them in the connection to the Net-RID SP. In this case, they are indistinguishable from the UA as seen from the Net-RID SP. Alternatively, they may use their own credentials with the Net-RID SP which would need some internal mechanism to tie that to the UA.

3.2.1.2. HIP for ESP Secure Link

HIP [RFC7401] for ESP Secure Link is a natural choice for a DET RID. For this, the Net-RID SP would also need a HHIT, possibly following the process in [drip-registries].

3.2.1.3. DTLS Secure Link

For DTLS [RFC9147] secure link, DANCE [dane-clients] may be used with a DET's DNS lookup to retrieve a TLSA RR with the DET's HI encoded in PKIX SubjectPublicKeyInfo format (per [RFC7250]).

The Net-RID SP DTLS credential may follow DANE [RFC6698] or any other DTLS server credential method.

3.2.2. Static Messages

For simplicity, a class of UAS information is called here "Static", though in practice any of it can change during the operation, but will change infrequently. This information is the contents of the B-RID Self-ID (Msg Type 0x3), Operator ID (Msg Type 0x5), and System Messages (Msg Type 0x4). This information can simply be sent in the same format as the B-RID messages. Alternatively the individual data elements may be send as separate CBOR objects.

The Basic ID (Msg Type 0x0) Message may be included as a static message if this information was not used for the secure setup. There may be more than one Basic ID Message needed if as in the case where the Japan Civil Aviation Bureau (JCAB) has mandated that the Civil Aviation Authority (CAA) assigned ID (UA ID type 2) and Serial Number (UA ID type 1) be broadcasted.

The information in the System Message is most likely to change during an operation. Noteably the Operator Location data elements are subject to change if the GCS is physically moving (e.g. hand-held and the operator is walking or driving in a car). The whole System Message may be sent, or only the changing data elements as CBOR objects.

These static message elements may be sent before the operation begins, thus their transmission can use a high capacity connection like WiFi. Once the operation is underway, any updates will have to traverse the operational link which may be very constrained and this will impact data element formatting.

The Net-RID SP MUST acknowledge these messages. The UAS MUST receive these ACKs. If no ACK is received, the UAS MUST resend the message(s). This send/ACK sequence continues either until ACK is received, or some policy number of tries. If this fails, the UAS MUST act that the Net-RID SP connection is lost and MUST take the policy set response to loss of Net-RID SP connectivity. If the information changes during this cycle, the latest information MUST always be sent.

3.2.3. Vector/Location Message

Many CAAs mandate that the UA Vector/Location information be updated at least once per second. Without careful message design, this messaging volume would overwhelm many wireless technologies. Thus to enable the widest deployment choices, a highly compressed format is recommended.

The B-RID Vector/Location Message (Msg Type 0x1) is the simplest small object (24 bytes) for sending this information as a single CBOR object or via MNet-RID. It may be possible to send only those data elements that changed in the last time interval. This may result in smaller individual transmissions, but should not be used if the resulting message is larger than the Vector/Location Message.

3.3. The Minimal, UDP, Net-RID Protocol

The Minimal Network Remote ID protocol is a simple UDP messaging consisting of a 1-byte message type field and a message field of maximum 25-bytes length.

The Message Type Field is defined as follows:

Value	Type	
0	RESERVED	
1	B-RID Message	[F3411]
2	Net-RID SP ACK	
3	Net-RID SP Heartbeat	

The B-RID Message is 25 bytes:

Bytes	Description
1	B-RID Message Type/version
24	B-RID Message

The Net-RID SP ACK is 5 bytes:

Bytes	Description
4	Timestamp
1	B-RID Message Type/version from message ACKed

Should a 12byte hash of message be included as in Manifest?

The Net-RID SP Heartbeat is 4 bytes:

Bytes	Description
4	Timestamp

3.3.1. Compressing the MNet-RID message headers

The security envelope (ESP of DTLS) and UDP headers may be compressed to further minimize the communication cost of MNet-RID.

3.3.1.1. Compressing ESP/UDP headers

A normal ESP/AES-GCM-12/UDP wrapper for the NMet-RID messages is 10+28+8=46 bytes. By applying the SCHC compression via [diet-esp] and using [RFC8750] Implicit Cipher IVs, this is reduced to 4+12+0=16 bytes.

AES-CCM-12 has a smaller, but valuable, size reduction on compression, as CCM's IV is only 8 bytes compared to GCM's 16-byte

IV. Thus uncompressed, the wrapper is 10+20+8=38 bytes. Compressed it is 4+12+0=16 bytes. Or "over the wire", compressed CCM offers no improvements to GCM and its 2-pass process will tend to result in a poorer performace compared to GCM, even on these small messages. Thus GCM is the recommended mode-of-operation for AES.

Note that [RFC8750] does not provide implicit IV use for AES-GCM-12. At the time of writing the use case for the smaller ICV was not apparent. Here, the smaller hash is not a lower risk given the limited traffic within a single operation. If not provided elsewhere, this document will request ENCR_AES_GCM_12_IIV for IKE and both AES_GCM_12 and AES_GCM_12_IIV for HIP.

[diet-esp] may be completely statically configured, or may have HIP or IKE negotiated values. This will be determined by Net-RID SP policy.

TBD: diet-esp context and rules.

3.3.1.2. Compressing UDP/DTLS message headers

DTLS 1.3 [RFC9147] is designed for minimal hader overhead. Section 5.2 defines the DTLS header fields to use for minmal header size. The only practical compression gain with SCHC would be the UDP header, it could be compressed to zero bytes, but would require [lpwan-ipnumber].

The DTLS header defined in Section 5.2 with a 1-byte Sequence and no Length is 4 bytes. Only AES-GCM-16 is defined for DTLS, but has an implicit IV for 16 bytes. This along with the UDP header is 18 bytes. Using SCHC for UDP header compression to zero bytes (and an implicit SCHC rule) would require adding the DTLS 2-byte Length field. This results in a further 2 byte header size reduction. The resulting 16 bytes is the same as in ESP compression above. However the complexity of SCHC for only UDP compression may not be of value in some implementations.

TBD: udp context and rules.

3.4. CoAP Net-RID messages

The CoAP based Net-RID protocol is intended for a richer conversation between the UAS and USS. The USS, through the Net-RID SP, may compare actual UA progress against the filed flight plan and against other UA actual traffic. The USS may then send to the UAS recommended changes to the flight plan to de-conflict traffic or advise the UAS to avoid hazards (1st responder event, avoid space). The UAS may then negotiate changes to the plan, and act on them, as appropriate.

This sort of advanced UAS behavior is envisioned as part of total UTM activities. Discussions now ongoing in UTM will provide the data models and transactional UAS/USS interactions, that will drive UAS communications past the MNet-RID defined in Section 3.3 toward this more functional CoAP Net-RID protocol.

4. Command and Control

The Command and Control (C2) connection is between the UA and GCS. This is often over a direct link radio. Some times, particularly for BLOS, it is via Internet connections. In either case C2 SHOULD be secure from eavesdropping and tampering. For design and implementation consistency it is best to treat the direct link as a local link Internet connection and use constrained networking compression standards.

Both the UA and GCS need to be treated as fully mobile in the IP networking sense. Either one can have its IP address change and both could change at the same time (the double jump problem). It is preferable to use a peer-to-peer (P2P) secure technology like HIPv2 [RFC7401].

Finally UA may also tend to have multiple radios for their C2 communications. Thus multi-homing with "make before break" behavior is needed. This is on top of any IP address changes on any of the interfaces while in use.

4.1. Securing MAVLink

MAVLink [MAVLINK] is a commonly used protocol for C2 that uses UDP port 14550 for transport over IP. Message authenticity was added in MAVLink 2 in the form of a SHA-256 (secret | message) left-truncated to 6 byte. This does not follow HMAC [RFC2104] security recommendations, nor provides confidentiality.

The MAVlink authentication only provides 24-bit collision resistance but is not susceptible to a hash length attack. By following the security approach here, UAS C2 is superior to that currently provided within MAVlink. It provides 48-bit collision resistance and full confidentiality.

4.1.1. Compressed ESP for MAVlink

The approach in Section 3.3.1.1 can be used to fully secure MAVlink and include the UDP header for IP transport. Further, MAVlink itself can be compressed.

MAVlink messages contain a 1-byte Seq number and 2-byte CRC. Both of these can be generated from SCHC rules. These 3 bytes along with the

13-byte MAVlink signature provides the 16 bytes so that the over-the-wire cost is the same.

This secure MAVlink format may be sent directly over a local wireless link. The UDP port processing adds little cost. Sending this over IP provides the needed confidentiality at 8 bytes less than unencrypted messages.

TBD: MAVlink SCHC context and rules. These will be part of the MAVlink ESP setup.

4.2. Compressed UDP/DTLS for MAVlink

At this time, DTLS is NOT recommended for C2 security, as it is challenged with server mobility. It may be added at a later time.

DTLS may be viable when there is no possiblity for an IP address change for the GCS during an operation. An example of this is where the GCS is an Operations Center like might be used in a package delivery business.

5. Secure Transports

Secure UDP-based protocols are preferred for both Network Remote ID (Net-RID) and C2. Both HIPv2 and DTLS can be used. It will be shown below that HIPv2 is better suited in most cases.

For IPv6 and CoAP over both WiFi and Bluetooth (or any other radio link), SCHC [RFC8724] is defined to significantly reduce the per packet transmission cost. SCHC is used both within the secure envelope and before the secure envelope as shown in Section 5.2.10 of [lpwan-architecture]. For Bluetooth, there is also IPv6 over Bluetooth LE [RFC7668] for more guidance.

Local link (direct radio) C2 security is possible with the link's MAC layer security. SCHC SHOULD still be used as above. Both WiFi and Bluetooth link security can provide appropriate security, but this would not provide trustworthy multi-homed security.

5.1. HIP for Secure Transport

HIP has already been used for C2 mobility, managing the ongoing connectivity over WiFi at start of an operation, switching to LTE once out of WiFi range, and returning to WiFi connectivity at the end of the operation. This functionality is especially important for BLOS. HHITs are already defined for RID, and need only be added to the GCS via a GCS Registration as part of the UAS to USS registration to be usedfor C2 HIP.

When the UA is the UAS endpoint for Net-RID (Section 3.1.1), and particularly when HIP is used for C2, HIP for Net-RID simplifies protocol use on the UA. The Net-RID SP endpoint may already support HIP if it is also the HHIT Registrar. If the UA lacks any IP ability and the RID HHIT registration was done via the GCS or Operator device, then they may also be set for using HIP for Net-RID.

Further, double jump and multi-homing support is mandatory for C2 mobility. This is inherent in the HIP design. The HIP address update can be improved with [hip-fast-mobility].

5.2. DTLS for Secure Transport

DTLS is a good fit for Net-RID for any of the possible UAS endpoints. There are challenges in using it for C2. To use DTLS for C2, the GCS will need to be the DTLS server. How does it 'push' commands to the UA? How does it reestablish DTLS security if state is lost? And finally, how is the double jump scenario handled?

All the above DTLS for C2 probably have solutions. None of them are inherent in the DTLS design.

DTLS implementations SHOULD use a CID of 2 bytes. This is to support mobility and simplify SCHC rule handling. The Sequence Number size is a deployment choice. For MNet-RID rate of one Vector/Location update per second, a 1-byte value would result in a rollover in 4 minutes. This should not poise an operational challenge. The length field is recommended when SCHC is used as it can provided an authenticated length to use to regenerate the UDP header length field and any application length field like that in MAVlink.

5.3. Ciphers for Secure Transport

The cipher choice for either HIP or DTLS depends, in large measure, on the UAS endpoint. If the endpoint is computationally constrained, the cipher computations become important. If any of the links are constrained or expensive, then the over-the-wire cost needs to be minimized. AES-CCM and AES-GCM are the preferred, modern, AEAD ciphers. Section 3.3.1.1 shows that proper compression can provide the more efficient GCM at no over-the-wire cost. Thus AES-GCM is the recommended AES mode-of-operation.

NIST is working on selecting a new lightweight cipher that may be the best choice for use on a UA. The Keccak Xoodyak cipher in [new-hip-crypto] is a good "Green Cipher".

5.4. HIP and DTLS contrasted and compared

This document specifies the use of DTLS 1.3 for its 0-RTT mobility feature and improved (over 1.2) handshake. DTLS 1.3 is still an IETF draft, so there is little data available to properly contrast it with HIPv2. This section will be based on the current DTLS 1.2. The basic client-server model is unchanged.

The use of DTLS vs HIPv2 (both over UDP, HIP in IPsec ESP BEET mode) has pros and cons. DTLS is currently at version 1.2 and based on TLS 1.2. It is a more common protocol than HIP, with many different implementations available for various platforms and languages.

DTLS implements a client-server model, where the client initiates the communication. In HIP, two parties are equal and either can be an Initiator or Responder of the Base Exchange. HIP provides separation between key management (base exchange) and secure transport (for example IPsec ESP BEET) while both parts are tightly coupled in DTLS.

DTLS 1.2 still has quite chatty connection establishment taking 3-5 RTTs and 15 packets. HIP connection establishment requires 4 packets (I1,R1,I2,R2) over 2 RTTs. This is beneficial for constrained environments of UAs. HIPv2 supports cryptoagility with possibility to negotiate cryptography mechanisms during the Base Exchange.

Both DTLS and HIP support mobility with a change of IP address. However, in DTLS only client mobility is well supported, while in HIP either party can be mobile. The double-jump problem (simultaneous mobility) is supported in HIP with a help of Rendezvous Server (RVS) [RFC8004]. HIP can implement secure mobility with IP source address validation in 2 RTTs, and in 1 RTT with fast mobility extension.

One study comparing DTLS and IPsec-ESP performance concluded that DTLS is recommended for memory-constrained applications while IPSec-ESP for battery power-constrained [Vignesh].

6. IANA Considerations

TBD: May need ESP ciphers defined.

TBD: Add MNet-RID Message Type Field to DRIP registry.

7. Security Considerations

Designing secure transports is challenging. Where possible, existing technologies SHOULD be used. Both ESP and DTLS have stood "the test of time" against many attack scenarios. Their use here for Net-RID and C2 do not represent new uses, but rather variants on existing depoyments.

The same can be said for both key establishment, using HIPv2 and DTLS, and the actual cipher choice for per packet encryption and authentication. Net-RID and C2 do not present new challenges, rather new opportunities to provide communications security using well researched technologies.

8. Acknowledgments

Stuart Card and Adam Wiethuechter provivded information on their use of HIP for C2 at the Syracuse NY UAS test corridor. This, in large measure, was the impetus to develop this document.

9. References

9.1. 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>.

[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>.

[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>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/info/rfc8949>.

9.2. Informative References

[dane-clients] Huque, S., Dukhovni, V., and A. Wilson, "TLS Client Authentication via DANE TLSA records", Work in Progress, Internet-Draft, draft-ietf-dance-client-auth-00, 24 March 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-dance-client-auth-00>.

[diet-esp] Migault, D., Guggemos, T., Bormann, C., and D. Schinazi, "ESP Header Compression and Diet-ESP", Work in Progress, Internet-Draft, draft-mglt-ipsecme-diet-esp-08, 13 May 2022, <https://datatracker.ietf.org/doc/html/draft-mglt-ipsecme-diet-esp-08>.

[drip-registries] Wiethuechter, A., Card, S., Moskowitz, R., and J. Reid, "DRIP Entity Tag Registration & Lookup", Work in Progress, Internet-Draft, draft-ietf-drip-registries-03, 11 May 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-drip-registries-03>.

[drip-uas-rid] Moskowitz, R., Card, S. W., Wiethuechter, A., and A. Gurtov, "DRIP Entity Tag (DET) for Unmanned Aircraft System Remote ID (UAS RID)", Work in Progress, Internet-Draft, draft-ietf-drip-rid-28, 17 May 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-drip-rid-28>.

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

[hip-fast-mobility] Moskowitz, R., Card, S. W., and A. Wiethuechter, "Fast HIP Host Mobility", Work in Progress, Internet-Draft, draft-moskowitz-hip-fast-mobility-04, 17 June 2022, <https://datatracker.ietf.org/doc/html/draft-moskowitz-hip-fast-mobility-04>.

[lpwan-architecture] Pelov, A., Thubert, P., and A. Minaburo, "LPWAN Static Context Header Compression (SCHC) Architecture", Work in Progress, Internet-Draft, draft-ietf-lpwan-architecture-01, 26 November 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-lpwan-architecture-01>.

[lpwan-ipnumber] Moskowitz, R., "IP Number for SCHC", Work in Progress, Internet-Draft, draft-moskowitz-lpwan-ipnumber-00, 3 June 2022, <https://datatracker.ietf.org/doc/html/draft-moskowitz-lpwan-ipnumber-00>.

[MAVLINK] "Micro Air Vehicle Communication Protocol", 2021, <http://mavlink.io/>.

[new-hip-crypto] Moskowitz, R., Card, S. W., and A. Wiethuechter, "New Cryptographic Algorithms for HIP", Work in Progress, Internet-Draft, draft-moskowitz-hip-new-crypto-10, 2 August 2021, <https://datatracker.ietf.org/doc/html/draft-moskowitz-hip-new-crypto-10>.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/info/rfc2104>.

[RFC5266] Devarapalli, V. and P. Eronen, "Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE)", BCP 136, RFC 5266, DOI 10.17487/RFC5266, June 2008, <https://www.rfc-editor.org/info/rfc5266>.

[RFC6698]
Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/info/rfc6698>.

[RFC7250] Wouters, P., Ed., Tschofenig, H., Ed., Gilmore, J., Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7250, DOI 10.17487/RFC7250, June 2014, <https://www.rfc-editor.org/info/rfc7250>.

[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>.

[RFC7402] Jokela, P., Moskowitz, R., and J. Melen, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)", RFC 7402, DOI 10.17487/RFC7402, April 2015, <https://www.rfc-editor.org/info/rfc7402>.

[RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015, <https://www.rfc-editor.org/info/rfc7668>.

[RFC8004] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", RFC 8004, DOI 10.17487/RFC8004, October 2016, <https://www.rfc-editor.org/info/rfc8004>.

[RFC8724] Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zuniga, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation", RFC 8724, DOI 10.17487/RFC8724, April 2020, <https://www.rfc-editor.org/info/rfc8724>.

[RFC8750] Migault, D., Guggemos, T., and Y. Nir, "Implicit Initialization Vector (IV) for Counter-Based Ciphers in Encapsulating Security Payload (ESP)", RFC 8750, DOI 10.17487/RFC8750, March 2020, <https://www.rfc-editor.org/info/rfc8750>.

[RFC8824] Minaburo, A., Toutain, L., and R. Andreasen, "Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)", RFC 8824, DOI 10.17487/RFC8824, June 2021, <https://www.rfc-editor.org/info/rfc8824>.

[RFC9011]
Gimenez, O., Ed. and I. Petrov, Ed., "Static Context Header Compression and Fragmentation (SCHC) over LoRaWAN", RFC 9011, DOI 10.17487/RFC9011, April 2021, <https://www.rfc-editor.org/info/rfc9011>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/info/rfc9147>.

[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>.

[Vignesh] Vignesh, K., "Performance analysis of end-to-end DTLS and IPsec-based communication in IoT environments", Thesis no. MSEE-2017: 42, 2017, <http://www.diva-portal.org/smash/get/diva2:1157047/FULLTEXT02>.

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

Andrei Gurtov
Linköping University
IDA

SE-58183 Linköping
Sweden

Email: gurtov@acm.org