Authors: R. Moskowitz   S. Card   A. Wiethuechter
         HTT Consulting   AX Enterprize   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 (N-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 N-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

   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 6 November 2022.

Table of Contents

1. Introduction

   This document defines a set of messages for Unmanned Aircraft System
   (UAS) Network Remote ID (N-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 (N-RID SP) either directly over UDP or via CoAP/CBOR
   ([RFC7252]/[RFC8949]).

   Direct UDP, referred here as Minimal N-RID (MN-RID), and CoAP/CBOR
   were selected for their low communication "cost". This may not be an
   issue if N-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 N-RID transmissions over a variety of wireless
technologies.

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

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

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] and
DTLS 1.3 [DTLS-1.3-draft]. These options are generally defined and
their applicability is compared and contrasted. It is up to N-RID
and C2 to select which is preferred for their situation.

To further reduce the communication cost, SCHC [RFC8724] is defined
for both the direct UDP and CoAP layer [RFC8824]. For ESP
"compression", either ESP Implicit IV, [RFC8750] and/or Diet ESP
[diet-esp] amy be used. SCHC for the IP/UDP layer is currently
defined by IP carrier (e.g. LoRaWAN, [RFC9011]) 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.

MN-RID

   A Minimal implementation of Network Remote ID.

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.

3. Network Remote ID

In UAS Traffic Management (UTM), the purpose of N-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, provide JSON objects and some of
the messages for passing information between various UTM entities
(e.g., N-RID SP to N-RID SP and N-RID SP to N-RID DP) but does not
specify how the data gets into UTM to begin with. This document will
provide such an open standard.

The Broadcast Remote ID (B-RID) messages in [F3411-19] are
sufficient to meet the needs of N-RID. These messages can be sent to
the N-RID SP when their contents change. Further, a UAS supporting
B-RID will have minimal development to add N-RID support.

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

Other messages may be needed in some N-RID situations. Thus a simple
message multiplexer is provided for MN-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 (N-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 N-RID SP may be provided by the same entity serving as the UAS
Service Provider (USS). This simplifies a number of aspects of the
N-RID communication flow. The N-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 N-RID communications.

The UAS component in N-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 N-RID communication may change during
an operation. The N-RID mechanism MUST support this. The UAS
Identity for the secure connection may vary based on the UAS
endpoint.

3.1.1. N-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.

3.1.2. N-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 N-RID (acting
as a gateway).

There are two sources for the GCS for the RID messages, 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.

3.1.3. N-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 N-RID messages.

3.2. Network RID Messaging

N-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 N-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 N-RID SP connectivity. For example, this could be a mandated immediate landing. There may be other messages from the N-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 N-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 N-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 N-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 N-RID SP. In this case, they are indistinguishable from the UA as seen from the N-RID SP. Alternatively, they may use their own credentials with the N-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 N-RID SP would also need a HHIT, possibly following the process in [drip-registries].

3.2.1.3. DTLS Secure Link

For DTLS [DTLS-1.3-draft] 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 N-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 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 N-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 N-RID SP connection is lost and MUST take the policy set response to loss of N-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 viva MN-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, N-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              N-RID SP ACK
  3              N-RID SP Heartbeat
```

The B-RID Message is 25 bytes:

```
  Bytes          Description

  1              B-RID Message Type/version
  24             B-RID Message
```

The N-RID SP ACK is 5 bytes:

```
  Bytes          Description

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

The N-RID SP Heartbeat is 4 bytes:

```
  Bytes          Description

  4              Timestamp
```

3.4. CoAP N-RID messages

TBD

4. **SCHC Message Compression**

    TBD

5. **Command and Control**

    The Command and Control (C2) connection is between the UA and GCS.
    This is often this 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.

5.1. **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 hash) left-
    truncated to 6 byte. This does not follow HMAC [RFC2104] security
    recommendations, nor provides confidentiality.

    By following the security approach here, UAS C2 is superior to that
    currently provided within MAVlink.

6. **Secure Transports**

    Secure UDP-based protocols are preferred for both Network Remote ID
    (N-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.

6.1. 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 N-RID (Section 3.1.1), and
particularly when HIP is used for C2, HIP for N-RID simplifies
protocol use on the UA. The N-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 N-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].

6.2. DTLS for Secure Transport

DTLS is a good fit for N-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.

6.3. 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.

For ESP with HIP [RFC7402], an additional 4 - 8 bytes can be trimmed
by using the Implicit IV for ESP option [RFC8750].

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".

6.4. 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].

7. IANA Considerations

TBD

8. 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 N-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. N-RID and C2 do not present new challenges, rather new opportunities to provide communications security using well researched technologies.

9. 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.

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>.

[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>.

10.2. 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-07, 11 March

2019, <https://datatracker.ietf.org/doc/html/draft-mglt-ipsecme-diet-esp-07>.

[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-02, 30 April 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-drip-registries-02>.

[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-24, 24 April 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-drip-rid-24>.

[DTLS-1.3-draft] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-dtls13-43, 30 April 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-dtls13-43>.

[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-03, 3 April 2020, <https://datatracker.ietf.org/doc/html/draft-moskowitz-hip-fast-mobility-03>.

[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>.

[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>.

[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>.

[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