Integrity Protection for the Neighborhood Discovery Protocol (NHDP) and
       Optimized Link State Routing Protocol Version 2 (OLSRv2)

Abstract

   This document specifies integrity and replay protection for the
   Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)
   and the Optimized Link State Routing Protocol version 2 (OLSRv2).
   This protection is achieved by using an HMAC-SHA-256 Integrity Check
   Value (ICV) TLV and a Timestamp TLV based on Portable Operating
   System Interface (POSIX) time.

   The mechanism in this specification can also be used for other
   protocols that use the generalized packet/message format described in
   RFC 5444.

   This document updates RFC 6130 and RFC 7181 by mandating the
   implementation of this integrity and replay protection in NHDP and
   OLSRv2.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc7183.

Copyright Notice

Table of Contents

1. Introduction

   This specification updates [RFC6130] and [RFC7181] by defining
   mandatory-to-implement security mechanisms (for integrity and replay
   protection). A deployment of these protocols may choose to employ an
   alternative(s) to these mechanisms; in particular, it may choose to
   protect packets rather than messages, it may choose to use an
   alternative Integrity Check Value (ICV) with preferred properties,
   and/or it may use an alternative timestamp. A deployment may choose
   to use no such security mechanisms, but this is not recommended.

   The mechanisms specified are the use of an ICV for protection of the
   protocols' control messages and the use of timestamps in those
   messages to prevent replay attacks. Both use the TLV mechanism
   specified in [RFC5444] to add this information to the messages.
   These ICV and TIMESTAMP TLVs are defined in [RFC7182]. Different ICV
   TLVs are used for HELLO messages in NHDP and TC (Topology Control)
   messages in OLSRv2, the former also protecting the source address of
   the IP datagram that contains the HELLO message. This is because the
   IP datagram source address is used by NHDP to determine the address
   of a neighbor interface, and it is not necessarily otherwise
   contained in the HELLO message, while OLSRv2's TC message is
   forwarded in a new packet; thus, it has no single IP datagram source
   address.

   The mechanism specified in this document is placed in the packet/
   message processing flow as indicated in Figure 1. It exists between
   the packet parsing/generation function of [RFC5444] and the message
   processing/generation function of NHDP and OLSRv2.

```
                       |                    |
        Incoming       |              /|\  Outgoing
         packet     \ | /              |   packet
                       |                    |
                 +-------------------------------+
                 |                               |
                 |         RFC 5444 packet        |
                 |        parsing/generation      |
                 |                               |
                 +-------------------------------+
                       |                    |
        Messages       |              /|\  Messages with
                    \ | /              |   added TLVs
                       |                    |
     D           +-------------------------------+
     R    /_____   |                 |
     O    \       Messages  |  Mechanism specified in  |
     P     (failed check)   |      this document      |
                            |                 |
                 +-------------------------------+
                       |                    |
        Messages       |              /|\  Messages
     (passed check) \ | /              |
                       |                    |
                 +-------------------------------+
                 |                               |
                 |       NHDP/OLSRv2 message     |
                 |      processing/generation     |
                 |                               |
                 +-------------------------------+
```
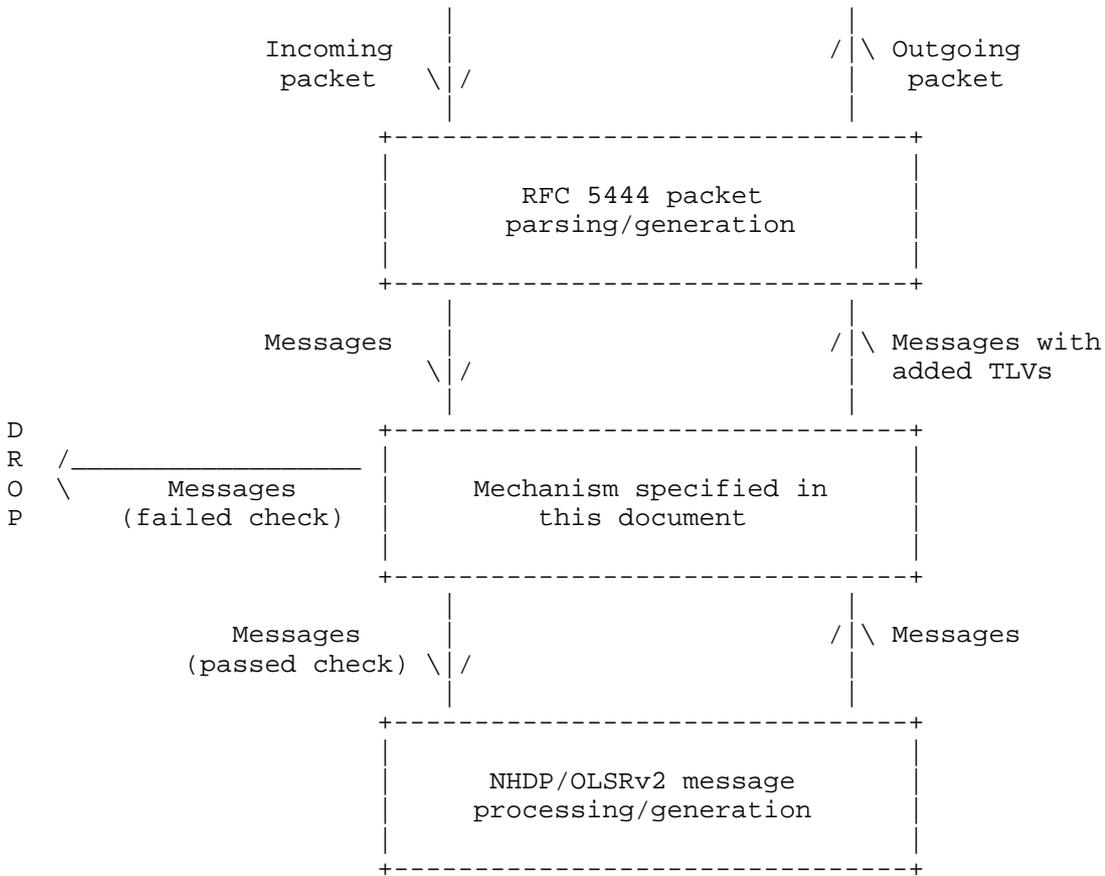
          Figure 1: Relationship with RFC 5444 and NHDP/OLSRv2

2. 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
   [RFC2119].

   Additionally, this document uses the terminology and notation of
   [RFC5444], [RFC6130], [RFC7181], and [RFC7182].

3. Applicability Statement

   [RFC6130] and [RFC7181] enable specifications of extensions to
   recognize additional reasons for rejecting a message as "badly formed
   and therefore invalid for processing", and mention security
   (integrity protection) as an explicit example. This document
   specifies a mechanism that provides this functionality.

   Implementations of [RFC6130] and [RFC7181] MUST include this
   mechanism, and deployments of [RFC6130] and [RFC7181] SHOULD use this
   mechanism, except when a different security mechanism is more
   appropriate.

   The applicability of this mechanism is determined by its
   characteristics, which are that it:

   o Specifies a security mechanism that is required to be included in
      conforming implementations of [RFC6130] and [RFC7181].

   o Specifies an association of ICVs with protocol messages, and
      specifies how to use a missing or invalid ICV as a reason to
      reject a message as "badly formed and therefore invalid for
      processing".

   o Specifies the implementation of an ICV Message TLV, defined in
      [RFC7182], using a SHA-256-based Hashed Message Authentication
      Code (HMAC) applied to the appropriate message contents (and for
      HELLO messages also including the IP datagram source address).
      Implementations of [RFC6130] and [RFC7181] MUST support an
      HMAC-SHA-256 ICV TLV, and deployments SHOULD use it except when
      use of a different algorithm is more appropriate. An
      implementation MAY use more than one ICV TLV in a message, as long
      as they each use a different algorithm or key to calculate the
      ICV.

   o Specifies the implementation of a TIMESTAMP Message TLV, defined
      in [RFC7182], to provide message replay protection.
      Implementations of [RFC6130] and [RFC7181] using this mechanism
      MUST support a timestamp based on POSIX time, and deployments
      SHOULD use it if the clocks in all routers in the network can be
      synchronized with sufficient precision.

   o Assumes that a router that is able to generate correct integrity
      check values is considered trusted.

This mechanism does not:

o Specify which key identifiers are to be used in a MANET in which
   the routers share more than one secret key. (Such keys will be
   differentiated using the <key-id> field defined in an ICV TLV in
   [RFC7182].)

o Specify how to distribute cryptographic material (shared secret
   key(s)).

o Specify how to detect compromised routers with valid keys.

o Specify how to handle (revoke) compromised routers with valid
   keys.

4. Protocol Overview and Functioning

   The mechanism specified in this document provides the following
   functionalities for use with messages specified by [RFC6130] and
   [RFC7181]:

o Generation of ICV Message TLVs (as defined in [RFC7182]) for
   inclusion in an outgoing message. An implementation of [RFC6130]
   and [RFC7181] MAY use more than one ICV TLV in a message, even
   with the same type extension, but these ICV TLVs MUST each use
   different keys or they MUST use a different algorithm to calculate
   the ICV, e.g., with different hash and/or cryptographic functions
   when using type extension 1 or 2. An implementation of [RFC6130]
   and [RFC7181] MUST at least be able to generate an ICV TLV using
   HMAC-SHA-256 and one or more secret keys shared by all routers.

o Generation of TIMESTAMP Message TLVs (as defined in [RFC7182]) for
   inclusion in an outgoing message. An implementation of [RFC6130]
   and [RFC7181] MAY use more than one ICV TLV in a message, but it
   MUST NOT use the same type extension. An implementation of
   [RFC6130] and [RFC7181] that is able to synchronize the clocks in
   all routers in the network with sufficient precision MUST at least
   be able to generate a TIMESTAMP TLV using POSIX time.

o Verification of ICV Message TLVs contained in a message, in order
   to determine if this message MUST be rejected as "badly formed and
   therefore invalid for processing" [RFC6130] [RFC7181]. An
   implementation of [RFC6130] and [RFC7181] MUST at least be able to
   verify an ICV TLV using HMAC/SHA-256 and one or more secret keys
   shared by all routers.

   o Verification of TIMESTAMP Message TLVs (as defined in [RFC7182])
      contained in a message, in order to determine if this message MUST
      be rejected as "badly formed and therefore invalid for processing"
      [RFC6130] [RFC7181]. An implementation of [RFC6130] and [RFC7181]
      that is able to synchronize the clocks in all routers in the
      network with sufficient precision MUST at least be able to verify
      a TIMESTAMP TLV using POSIX time.

   ICV Packet TLVs (as defined in [RFC7182]) MAY be used by a deployment
   of the multiplexing process defined in [RFC5444], either as well as
   or instead of the protection of the NHDP and OLSRv2 messages. (Note
   that in the case of NHDP, the packet protection is equally good, and
   also protects the packet header. In the case of OLSRv2, the packet
   protection has different properties than the message protection,
   especially for some forms of ICV. When packets contain more than one
   message, the packet protection has lower overheads in space and
   computation time.)

   When a router generates a message on a MANET interface, this
   mechanism:

   o Specifies how to calculate an ICV for the message.

   o Specifies how to include that ICV using an ICV Message TLV.

   [RFC6130] and [RFC7181] allow for the rejection of incoming messages
   prior to processing by NHDP or OLSRv2. This mechanism, when used,
   specifies that a message MUST be rejected if the ICV Message TLV is
   absent, or its value cannot be verified. Note that this means that
   routers whose implementation of NHDP and/or OLSRv2 does not include
   this specification will be ignored by routers using this mechanism,
   and these two sets of routers will, by design, form disjoint MANETs.
   (The unsecured MANET will retain some information about the secured
   MANET, but be unable to use it, not having any recognized symmetric
   links with the secured MANET.)

5. Parameters

   The following router parameters are specified for use by the two
   protocols; the first is required only by NHDP, but may be visible to
   OLSRv2, the second is required only by OLSRv2:

   o MAX_HELLO_TIMESTAMP_DIFF - The maximum age that a HELLO message to
      be validated may have. If the current POSIX time of the router
      validating the HELLO message, minus the timestamp indicated in the
      TIMESTAMP TLV of the HELLO message, is greater than
      MAX_HELLO_TIMESTAMP_DIFF, the HELLO message MUST be silently
      discarded.

o MAX_TC_TIMESTAMP_DIFF - The maximum age that a TC message to be
  validated may have. If the current POSIX time of the router
  validating the TC message, minus the timestamp indicated in the
  TIMESTAMP TLV of the TC message, is greater than
  MAX_TC_TIMESTAMP_DIFF, the TC message MUST be silently discarded.

The following constraints apply to these parameters:

o MAX_HELLO_TIMESTAMP_DIFF > 0

o MAX_TC_TIMESTAMP_DIFF > 0

However, these bounds are insufficient: MAX_HELLO_TIMESTAMP_DIFF and
MAX_TC_TIMESTAMP_DIFF MUST be least as great as the maximum expected
"age" of a message (i.e., the time difference between a message has
been sent by a router and received by all intended destinations).
For HELLO messages, this needs only cover a single hop, but TC
messages may have been forwarded a number of times. In particular,
for TC messages, if using jitter as specified in [RFC7181] and
[RFC5148], the largest contribution the age may be a delay of up to
F_MAXJITTER per hop (except the final hop) that the message has
traveled. Other factors in the delay of both message types, per hop,
may include the link-layer that is used in the MANET, and CPU and
memory resources of routers (e.g., queuing delays, and delays for
processing ICVs). An implementation MAY set lower and/or upper
bounds on these parameters, if so, then these MUST allow values
meeting these requirements. An implementation MAY make its value of
MAX_TC_TIMESTAMP_DIFF dependent on the number of hops that a TC
message has traveled.

The above constraints assume ideal time synchronization of the clock
in all routers in the network. The parameters
MAX_HELLO_TIMESTAMP_DIFF and MAX_TC_TIMESTAMP_DIFF (and any
constraints on them) MAY be increased to allow for expected timing
differences between routers (between neighboring routers for
MAX_HELLO_TIMESTAMP_DIFF, allowing for greater separation, but
usually not per hop, for MAX_TC_TIMESTAMP_DIFF).

Note that excessively large values of these parameters defeats their
objectives, so these parameters SHOULD be as large as is required,
but not significantly larger.

Using POSIX time allows a resolution of no more than one second. In
many MANET use cases, time synchronization much below one second is
not possible because of unreliable and high-delay channels, mobility,
interrupted communication, and possible resource limitations.

In addition, when using the default message intervals and validity
times as specified in [RFC6130] and [RFC7181], where the shortest
periodic message interval is 2 seconds, repeating the message within
a second is actually beneficial rather than harmful (at a small
bandwidth cost). Also, the use of [RFC5148] jitter can cause a
message to take that long or longer to traverse the MANET, thus even
in a perfectly synchronized network, the TC maximum delay would
usually be greater than 1 second.

A finer granularity than 1 second, and thus the use of an alternative
timestamp, is however RECOMMENDED in cases where, possibly due to
fast moving routers, message validity times are below 1 second.

6. Message Generation and Processing

   This section specifies how messages are generated and processed by
   [RFC6130] and [RFC7181] when using this mechanism.

6.1. Message Content

   Messages MUST have the content specified in [RFC6130] and [RFC7181],
   respectively. In addition, messages that conform to this mechanism
   MUST contain:

   o At least one ICV Message TLV (as specified in [RFC7182]),
      generated according to Section 6.2. Implementations of [RFC6130]
      and [RFC7181] MUST support the following version of the ICV TLV,
      but other versions MAY be used instead, or in addition, in a
      deployment, if more appropriate:

      * For TC messages:

         + type-extension := 1

      * For HELLO messages:

         + type-extension := 2

      * hash-function := 3 (SHA-256)

      * cryptographic-function := 3 (HMAC)

      The ICV Value MAY be truncated as specified in [RFC7182]; the
      selection of an appropriate length MAY be administratively
      configured. A message MAY contain several ICV Message TLVs.

   o At least one TIMESTAMP Message TLV (as specified in [RFC7182]),
      generated according to Section 6.2. Implementations of [RFC6130]
      and [RFC7181] using this mechanism MUST support the following
      version of the TIMESTAMP TLV, but other versions MAY be used
      instead, or in addition, in a deployment, if more appropriate:

      * type-extension := 1

6.2. Message Generation

   After message generation (Section 11.1 of [RFC6130] and Section 16.1.
   of [RFC7181]) and before message transmission (Section 11.2 of
   [RFC6130] and Section 16.2 of [RFC7181]), the additional TLVs
   specified in Section 6.1 MUST (unless already present) be added to an
   outgoing message when using this mechanism.

   The following processing steps (when using a single timestamp version
   and a single ICV algorithm) MUST be performed for a cryptographic
   algorithm that is used for generating an ICV for a message:

   1. All ICV TLVs (if any) are temporarily removed from the message.
       Any temporarily removed ICV TLVs MUST be stored, in order to be
       reinserted into the message in step 5. The message size and
       Message TLV Block size are updated accordingly.

   2. <msg-hop-count> and <msg-hop-limit>, if present, are temporarily
       set to 0.

   3. A TLV of type TIMESTAMP, as specified in Section 6.1, is added to
       the Message TLV Block. The message size and Message TLV Block
       size are updated accordingly.

   4. A TLV of type ICV, as specified in Section 6.1, is added to the
       Message TLV Block. The message size and Message TLV Block size
       are updated accordingly.

   5. All ICV TLVs that were temporary removed in step 1, are restored.
       The message size and Message TLV Block size are updated
       accordingly.

   6. <msg-hop-count> and <msg-hop-limit>, if present, are restored to
       their previous values.

   An implementation MAY add either alternative TIMESTAMP and/or ICV
   TLVs or more than one TIMESTAMP and/or ICV TLVs. All TIMESTAMP TLVs
   MUST be inserted before adding ICV TLVs.

6.3. Message Processing

   Both [RFC6130] and [RFC7181] specify that:

      On receiving a ... message, a router MUST first check if the
      message is invalid for processing by this router

   [RFC6130] and [RFC7181] proceed to give a number of conditions that,
   each, will lead to a rejection of the message as "badly formed and
   therefore invalid for processing". When using a single timestamp
   version, and a single ICV algorithm, add the following conditions to
   that list, each of which, if true, MUST cause NHDP or OLSRv2 (as
   appropriate) to consider the message as invalid for processing when
   using this mechanism:

   1. The Message TLV Block of the message does not contain exactly one
       TIMESTAMP TLV of the selected version. This version
       specification includes the type extension. (The Message TLV
       Block may also contain TIMESTAMP TLVs of other versions.)

   2. The Message TLV Block does not contain exactly one ICV TLV using
       the selected algorithm and key identifier. This algorithm
       specification includes the type extension, and for type
       extensions 1 and 2, the hash function and cryptographic function.
       (The Message TLV Block may also contain ICV TLVs using other
       algorithms and key identifiers.)

   3. Validation of the identified (in step 1) TIMESTAMP TLV in the
       Message TLV Block of the message fails, as according to
       Section 6.3.1.

   4. Validation of the identified (in step 2) ICV TLV in the Message
       TLV Block of the message fails, as according to Section 6.3.2.

   An implementation MAY check the existence of, and verify, either an
   alternative TIMESTAMP and/or ICV TLVs or more than one TIMESTAMP and/
   or ICV TLVs.

6.3.1. Validating a Message Based on Timestamp

   For a TIMESTAMP Message TLV with type extension 1 (POSIX time)
   identified as described in Section 6.2:

   1. If the current POSIX time minus the value of that TIMESTAMP TLV
       is greater than MAX_HELLO_TIMESTAMP_DIFF (for a HELLO message) or
       MAX_TC_TIMESTAMP_DIFF (for a TC message), then the message
       validation fails.

   2. Otherwise, the message validation succeeds.

   If a deployment chooses to use a different type extension from 1,
   appropriate measures MUST be taken to verify freshness of the
   message.

6.3.2. Validating a Message Based on Integrity Check

   For an ICV Message TLV identified as described in Section 6.2:

   1. All ICV Message TLVs (including the identified ICV Message TLV)
       are temporarily removed from the message, and the message size
       and Message TLV Block size are updated accordingly.

   2. The message's <msg-hop-count> and <msg-hop-limit> fields are
       temporarily set to 0.

   3. Calculate the ICV for the parameters specified in the identified
       ICV Message TLV, as specified in [RFC7182].

   4. If this ICV differs from the value of <ICV-data> in the ICV
       Message TLV, then the message validation fails. If the
       <ICV-data> has been truncated (as specified in [RFC7182], the ICV
       calculated in the previous step MUST be truncated to the TLV
       length of the ICV Message TLV before comparing it with the
       <ICV-data>.

   5. Otherwise, the message validation succeeds. The message's
       <msg-hop-count> and <msg-hop-limit> fields are restored to their
       previous value, and the ICV Message TLVs are returned to the
       message, whose size is updated accordingly.

7. Provisioning of Routers

   Before a router using this mechanism is able to generate ICVs or
   validate messages, it MUST acquire the shared secret key(s) to be
   used by all routers that are to participate in the network. This
   specification does not define how a router acquires secret keys.
   Once a router has acquired suitable key(s), it MAY be configured to
   use, or not use, this mechanism. Section 23.6 of [RFC7181] provides
   a rationale based on [BCP107] why no key management is specified for
   OLSRv2.

8. Security Considerations

   This document specifies a security mechanism for use with NHDP and
   OLSRv2 that allows for mitigating several security threats.

8.1. Mitigated Attacks

   This section briefly summarizes security threats that are mitigated
   by the mechanism presented in this document.

8.1.1. Identity Spoofing

   As only routers possessing the selected shared secret key are able to
   add a valid ICV TLV to a message, identity spoofing, where an
   attacker falsely claims an identity of a valid router, is countered.
   When using one or more shared keys for all routers in the MANET, it
   is only possible to determine that it is a valid router in the
   network, not to discern particular routers. Therefore, a malicious
   router in possession of valid keys (e.g., a compromised router) may
   still spoof the identity of another router using the same key.

8.1.2. Link Spoofing

   Link spoofing, where an attacker falsely represents the existence of
   a nonexistent link, or otherwise misrepresents a link's state, is
   countered by the mechanism specified in this document, using the same
   argument as in Section 8.1.1.

8.1.3. Replay Attack

   Replay attacks are partly countered by the mechanism specified in
   this document, but this depends on synchronized clocks of all routers
   in the MANET. An attacker that records messages to replay them later
   can only do so in the selected time interval after the timestamp that
   is contained in message. As an attacker cannot modify the content of
   this timestamp (as it is protected by the identity check value), an
   attacker cannot replay messages after this time. Within this time
   interval, it is still possible to perform replay attacks; however,
   the limits on the time interval are specified so that this will have
   a limited effect on the operation of the protocol.

8.2. Limitations

   If no synchronized clocks are available in the MANET, replay attacks
   cannot be countered by the mechanism provided by this document. An
   alternative version of the TIMESTAMP TLV defined in [RFC7182], with a
   monotonic sequence number, may have some partial value in this case,
   but will necessitate adding state to record observed message sequence
   number information.

   The mechanism provided by this document does not avoid or detect
   security attacks by routers possessing the shared secret key that is
   used to generate integrity check values for messages.

   This mechanism relies on an out-of-band protocol or mechanism for
   distributing the shared secret key(s) (and if an alternative
   integrity check value is used, any additional cryptographic
   parameters).

   This mechanism does not provide a key management mechanism. Refer to
   Section 23.6 of [RFC7181] for a detailed discussion why the automated
   key management requirements specified in [BCP107] do not apply for
   OLSRv2 and NHDP.

9. Acknowledgments

   The authors would like to gratefully acknowledge the following
   people: Justin Dean (NRL) and Henning Rogge (Frauenhofer FKIE).

10. References

10.1. Normative References

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC5444]   Clausen, T., Dearlove, C., Dean, J., and C. Adjih,
               "Generalized Mobile Ad Hoc Network (MANET) Packet/Message
               Format", RFC 5444, February 2009.

   [RFC6130]   Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc
               Network (MANET) Neighborhood Discovery Protocol (NHDP)",
               RFC 6130, April 2011.

   [RFC7181]   Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg,
               "The Optimized Link State Routing Protocol Version 2", RFC
               7181, April 2014.

   [RFC7182]   Herberg, U., Clausen, T., and C. Dearlove, "Integrity
               Check Value and Timestamp TLV Definitions for Mobile Ad
               Hoc Networks (MANETs)", RFC 7182, April 2014.

10.2. Informative References

   [BCP107]   Bellovin, S. and R. Housley, "Guidelines for Cryptographic
               Key Management", BCP 107, RFC 4107, June 2005.

   [RFC5148]   Clausen, T., Dearlove, C., and B. Adamson, "Jitter
               Considerations in Mobile Ad Hoc Networks (MANETs)", RFC
               5148, February 2008.

Authors' Addresses

    Ulrich Herberg
    Fujitsu Laboratories of America
    1240 E. Arques Ave.
    Sunnyvale, CA, 94085
    USA

    EMail: ulrich@herberg.name
    URI: http://www.herberg.name/

    Christopher Dearlove
    BAE Systems Advanced Technology Centre
    West Hanningfield Road
    Great Baddow, Chelmsford
    United Kingdom

    Phone: +44 1245 242194
    EMail: chris.dearlove@baesystems.com
    URI: http://www.baesystems.com/

    Thomas Heide Clausen
    LIX, Ecole Polytechnique
    91128 Palaiseau Cedex
    France

    Phone: +33 6 6058 9349
    EMail: T.Clausen@computer.org
    URI: http://www.thomasclausen.org/