

Mobile Ad hoc Networking (MANET)  
Internet-Draft  
Updates: [RFC6130](#) (if approved)  
Intended status: Standards Track  
Expires: September 23, 2013

U. Herberg  
Fujitsu Laboratories of America  
C. Dearlove  
BAE Systems ATC  
T. Clausen  
LIX, Ecole Polytechnique  
March 22, 2013

**Integrity Protection for Control Messages in NHDP and OLSRV2**  
**draft-ietf-manet-nhdp-olsrv2-sec-00**

Abstract

This document specifies integrity and replay protection for required implementation in the MANET Neighborhood Discovery Protocol (NHDP) and the Optimized Link State Routing Protocol version 2 (OLSRv2). This document specifies how an included integrity check value (ICV) and a timestamp TLV, defined in RFC6622bis, are used by NHDP and OLSRV2 for countering a number of security threats. The ICV TLV uses a SHA-256 based HMAC and a single shared secret key. The timestamp TLV is based on POSIX time, assuming router synchronization. The mechanism in this specification can also be used for other MANET protocols using [RFC5444](#).

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 <http://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 September 23, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal

Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- [1. Introduction . . . . .](#) [3](#)
- [2. Terminology . . . . .](#) [4](#)
- [3. Applicability Statement . . . . .](#) [4](#)
- [4. Protocol Overview and Functioning . . . . .](#) [6](#)
- [5. Parameters . . . . .](#) [7](#)
- [6. Message Generation and Processing . . . . .](#) [8](#)
  - [6.1. Message Content . . . . .](#) [8](#)
  - [6.2. Message Generation . . . . .](#) [8](#)
  - [6.3. Message Processing . . . . .](#) [9](#)
    - [6.3.1. Invalidating a Message Based on Timestamp . . . . .](#) [10](#)
    - [6.3.2. Invalidating a Message Based on Integrity Check . . . . .](#) [10](#)
- [7. Provisioning of Routers . . . . .](#) [11](#)
- [8. IANA Considerations . . . . .](#) [11](#)
- [9. Security Considerations . . . . .](#) [11](#)
  - [9.1. Alleviated Attacks . . . . .](#) [11](#)
    - [9.1.1. Identity Spoofing . . . . .](#) [11](#)
    - [9.1.2. Link Spoofing . . . . .](#) [11](#)
    - [9.1.3. Replay Attack . . . . .](#) [11](#)
  - [9.2. Limitations . . . . .](#) [12](#)
- [10. Normative References . . . . .](#) [12](#)
- [Authors' Addresses . . . . .](#) [12](#)



## **1. Introduction**

This specification defines a framework of security mechanisms that must be included in conforming implementations of the Neighborhood Discovery Protocol (NHDP) [[RFC6130](#)] and the Optimized Link State Routing Protocol version 2 (OLSRv2) [[OLSRv2](#)] for Mobile Ad hoc NETWORKS (MANETs). A deployment of these protocols may choose to employ 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, 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 [[RFC6622bis](#)]. Different ICV TLVs are used for HELLO messages in NHDP and TC messages in OLSRV2, the former also protecting the source address of the IP datagram that contains the HELLO message, because the IP datagram source address is used by NHDP to determine the address of a neighbor interface, and is not necessarily otherwise contained in the HELLO message.

The mechanism specified in this document must insert itself between NHDP's and OLSRV2's message processing/generation and the [[RFC5444](#)] packet parsing/generation, as illustrated in Figure 1.



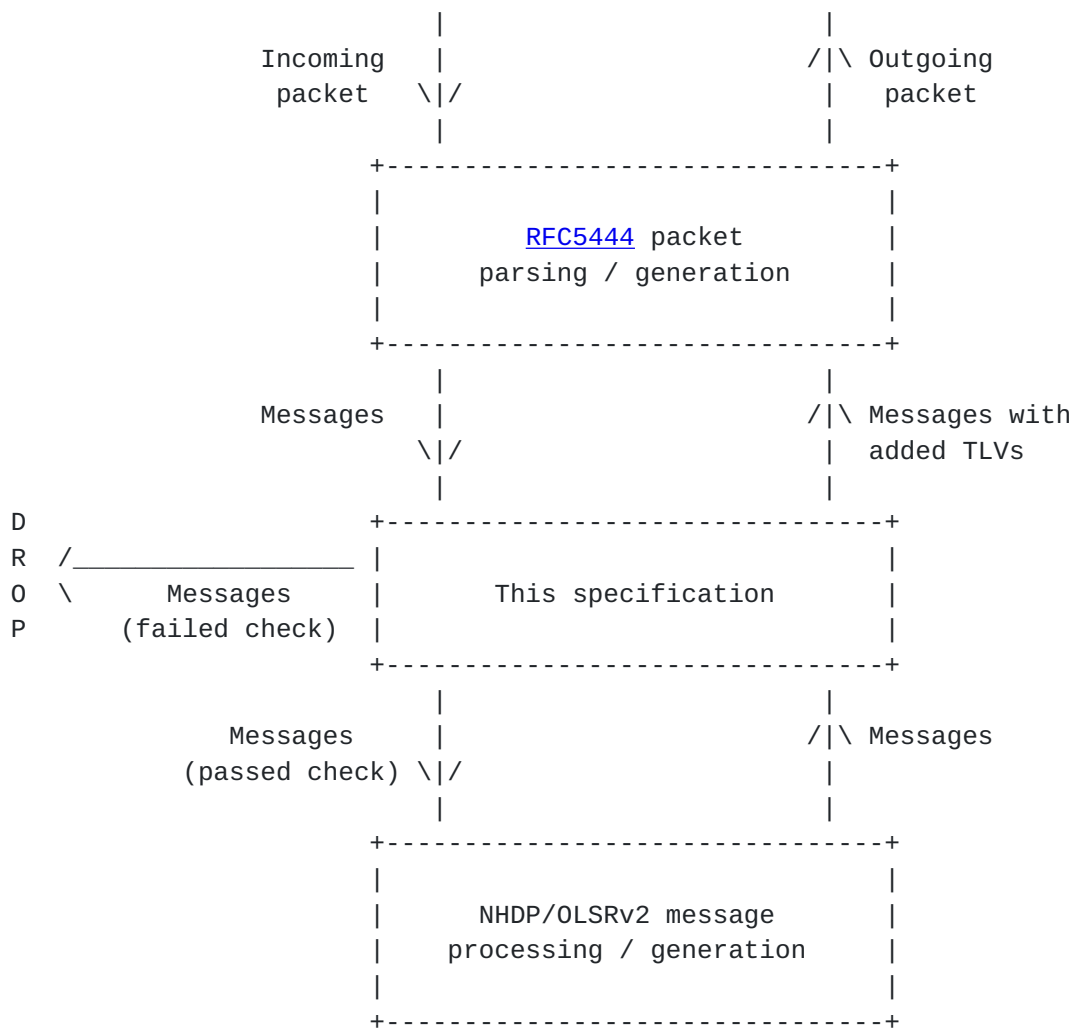


Figure 1: Relationship with [RFC5444](#) and NHDP/OLSRv2

**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 of [\[RFC5444\]](#), [\[RFC6130\]](#), [\[OLSRv2\]](#), and [\[RFC6622bis\]](#).

**3. Applicability Statement**

[\[RFC6130\]](#) and [\[OLSRv2\]](#) enable 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 framework that provides this functionality.

Implementations of [RFC6130] and [OLSRv2] MUST include this framework, and deployments of [RFC6130] and [OLSRv2] SHOULD use this framework, except for when a different security mechanism is more appropriate.

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

- o Specifies a security framework that is required to be included in conforming implementations of [RFC6130] and [OLSRv2].
- o Specifies an association of ICVs with messages, and for using missing or invalid ICVs as such an additional reason for rejecting a message as "badly formed and therefore invalid for processing".
- o Specifies the implementation of an ICV TLV, defined in [RFC6622bis], using a SHA-256 based HMAC applied to the appropriate message contents (and for HELLO messages also including the IP datagram source address). Deployments of [RFC6130] and [OLSRv2] using this framework should use the HMAC/SHA-256 ICV TLV, but may use different algorithms if more appropriate in a deployment. An implementation may also use more than one ICV TLV in a message as long as they each use a different algorithm to calculate the ICV.
- o Specifies the implementation of a TIMESTAMP TLV, defined in [RFC6622bis], to provide message replay protection. Deployments of [RFC6130] and [OLSRv2] using this framework SHOULD use a POSIX time based timestamp, if all routers can be sufficiently synchronized.
- o Assumes that a router that is able to generate correct integrity check values is considered trusted.

This framework does not:

- o Specify how to distribute cryptographic material (shared secret key).
- 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 framework specified in this document provides the following functionalities for use with messages owned by [\[RFC6130\]](#) and [\[OLSRv2\]](#):

- o Generation of ICV TLVs (as defined in [\[RFC6622bis\]](#)) for inclusion in an outgoing message. An implementation of [\[RFC6130\]](#) and [\[OLSRv2\]](#) may use more than one ICV TLV in a message, even with the same type extension, but these ICV TLVs MUST each 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 [\[OLSRv2\]](#) must at least be able to generate an ICV TLV using HMAC/SHA-256 and a single secret key shared by all routers.
- o Generation of TIMESTAMP TLVs (as defined in [\[RFC6622bis\]](#)) for inclusion in an outgoing message. An implementation of [\[RFC6130\]](#) and [\[OLSRv2\]](#) that is able to synchronize routers, must at least be able to generate a TIMESTAMP TLV using POSIX time.
- o Verification of ICV TLVs contained in a message, in order to determine if this message MUST be rejected as "badly formed and therefore invalid for processing" [\[RFC6130\]](#) [\[OLSRv2\]](#). An implementation of [\[RFC6130\]](#) and [\[OLSRv2\]](#) must at least be able to verify an ICV TLV using HMAC/SHA-256 and a single secret key shared by all routers.
- o Verification of a TIMESTAMP TLV (as defined in [\[RFC6622bis\]](#)) contained in a message, in order to determine if this message MUST be rejected as "badly formed and therefore invalid for processing" [\[RFC6130\]](#) [\[OLSRv2\]](#). An implementation of [\[RFC6130\]](#) and [\[OLSRv2\]](#) that is able to synchronize routers, must at least be able to verify a TIMESTAMP TLV using POSIX time.

ICV Packet TLVs (as defined in [\[RFC6622bis\]](#)) 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 framework:



- o Specifies how to calculate an integrity check value for the message.
- o Specifies how to include that integrity check value using an ICV Message TLV.

[RFC6130] and [[OLSRv2](#)] allow for rejecting incoming messages prior to processing by NHDP or OLSRV2. This framework specifies that a message must be rejected if the ICV Message TLV is absent, or its value cannot be verified.

## **5. Parameters**

This following router parameters is 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_HELLO_TIMESTAMP_DIFF < REFRESH_INTERVAL`
- o `MAX_TC_TIMESTAMP_DIFF > 0`
- o `MAX_TC_TIMESTAMP_DIFF < T_HOLD_TIME`

The second and fourth of those constraints assume ideal synchronization. These bounds MAY be relaxed to allow for expected timing differences between routers (between neighboring routers for `MAX_HELLO_TIMESTAMP_DIFF`). However it should also be noted that, in the ideal case, the parameters SHOULD be significantly less than those bounds.



## 6. Message Generation and Processing

This section specifies how messages are generated and processed by [RFC6130] and [OLSRv2] when using this framework.

### 6.1. Message Content

Messages MUST have the content specified in [RFC6130] and [OLSRv2] respectively. In addition, in order to conform to this framework, each message MUST contain:

- o At least one ICV Message TLV (as specified in [RFC6622bis]), generated according to [Section 6.2](#). Implementations of [RFC6130] and [OLSRv2] 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)

A message MAY contain several ICV Message TLVs.

- o At least one TIMESTAMP Message TLV (as specified in [RFC6622bis]), generated according to [Section 6.2](#). Implementations of [RFC6130] and [OLSRv2] using this framework 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 \[OLSRv2\]](#)) and before message transmission ([Section 11.2 of \[RFC6130\]](#) and [Section 16.2 of \[OLSRv2\]](#)), the additional TLVs specified in [Section 6.1](#) MUST (unless already present) be added to an outgoing message when using this framework.



The following processing steps 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 is 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 is updated accordingly.
4. A TLV of type `ICV`, as specified in [Section 6.1](#), is added to the Message TLV block. The message size is updated accordingly.
5. All ICV TLVs that were temporarily removed in step 1, are restored. The message size is updated accordingly.
6. <msg-hop-count> and <msg-hop-limit>, if present, are restored to their previous values.

### **6.3. Message Processing**

Both [[RFC6130](#)] and [[OLSRv2](#)] specify that:

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

[[RFC6130](#)] and [[OLSRv2](#)] 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, 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 framework:

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. 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.)





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 TLVs 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 alternative TIMESTAMP and/or ICV TLVs, or more than one TIMESTAMP and/or ICV TLVs.

#### **[6.3.1](#). Invalidating 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](#). Invalidating 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 is updated accordingly.
2. The message's <msg-hop-count> and <msg-hop-limit> fields are temporarily set to 0.
3. Calculate the integrity check value for the parameters specified in the identified ICV Message TLV, as specified in [[RFC6622bis](#)].
4. If this integrity check value differs from the value of <ICV-data> in the ICV Message TLV, then the message validation fails.
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 is able to generate ICVs or validate messages, it MUST acquire the single shared secret key that is to be used by all routers that are to participate in the network. This specification does not define how a router acquires this secret key.

## **8. IANA Considerations**

This document has no actions for IANA.

## **9. Security Considerations**

This document specifies a security framework for use with NHDP and OLSRV2 that allows for alleviating several security threats.

### **9.1. Alleviated Attacks**

This section briefly summarizes security threats that are alleviated by the framework presented in this document.

#### **9.1.1. Identity Spoofing**

As only routers possessing the shared secret key are able to add a valid ICV TLV to a message, identity spoofing is countered.

#### **9.1.2. Link Spoofing**

Link spoofing is countered by the framework specified in this document, using the same argument as in [Section 9.1.1](#).

#### **9.1.3. Replay Attack**

Replay attacks are partly counteracted by the framework 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.



## 9.2. Limitations

If no synchronized clocks are available in the MANET, replay attacks cannot be countered by the framework provided by this document. An alternative version of the TIMESTAMP TLV defined in [[RFC6622bis](#)], 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 framework 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 framework relies on an out-of-band protocol or mechanism for distributing the shared secret key (and if an alternative integrity check value is used, any additional cryptographic parameters).

This framework does not provide a key revocation mechanism.

## 10. Normative References

- [OLSRV2] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol version 2", [draft-ietf-manet-olsrv2-17](#) (work in progress), October 2012.
- [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 MANET Packet/Message Format", [RFC 5444](#), February 2009.
- [RFC6130] Clausen, T., Dean, J., and C. Dearlove, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", [RFC 6130](#), April 2011.
- [RFC6622bis] Herberg, U., Clausen, T., and C. Dearlove, "Integrity Check Value and Timestamp TLV Definitions for Mobile Ad Hoc Networks (MANETs)", Internet Draft [draft-herberg-manet-rfc6622-bis-00](#), February 2013.



Authors' Addresses

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

Email: [ulrich@herberg.name](mailto:ulrich@herberg.name)

URI: <http://www.herberg.name/>

Christopher Dearlove  
BAE Systems ATC

Phone: +44 1245 242194

Email: [chris.dearlove@baesystems.com](mailto: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](mailto:T.Clausen@computer.org)

URI: <http://www.thomasclausen.org/>



