Mobile Ad hoc Networking (MANET)
Internet-Draft
Updates: RFC6130 (if approved)
Intended status: Standards Track
Expires: August 22, 2013

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

February 18, 2013

Integrity Protection for Control Messages in NHDP and OLSRv2
draft-herberg-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 integrity check value (ICV) and a timestamp may be included as TLVs (defined in [RFC6622bis]) in NHDP's and OLSRv2's control messages, countering a number of security threats to NHDP and to OLSRv2. 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 August 22, 2013.

Table of Contents

1. Introduction

This specification defines a framework of security mechanisms that must be included in conforming implementations of the mobile ad hoc network (MANET) protocols Neighborhood Discovery Protocol (NHDP) [RFC6130] and the Optimized Link State Routing Protocol version 2 (OLSRv2) [OLSRv2]. A deployment of these protocols may however 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.

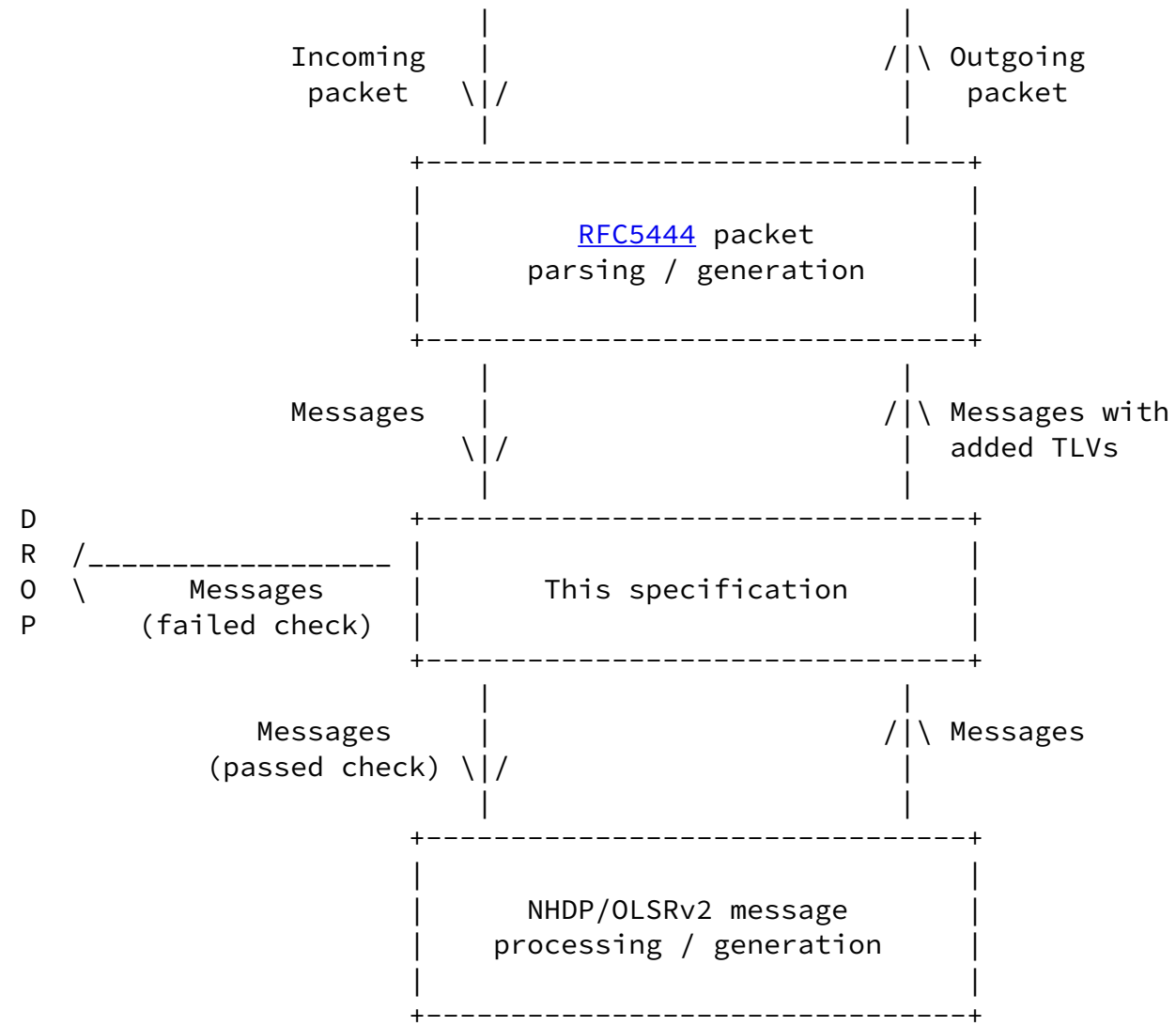
Incoming packet
Outgoing packet
RFC5444 packet parsing / generation
Messages
Messages with added TLVs
DROP
Messages (failed check)
This specification
Messages (passed check)
Messages
NHDP/OLSRv2 message processing / generation

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 as an explicit example.

This framework's applicability to provide that functionality is determined by its characteristics, which are that it:

- Specifies a security framework that is required to be included in conforming implementations of [RFC6130] and [OLSRv2].
- 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".
- Specifies ICV TLVs, 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) to implement the required association.
- Specifies a TIMESTAMP TLV, defined in [RFC6622bis], to provide message replay protection.
- Assumes that a router which is able to generate correct integrity

checks is considered trusted.

This framework does NOT:

- Specify how to distribute cryptographic material (shared secret key).
- Specify how to detect compromised routers with valid keys.
- 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 that may be used in the messages owned by [RFC6130] and [OLSRv2]:

- Generation of an ICV TLV (as defined in [RFC6622bis]) for inclusion in an outgoing message.
- Generation of a TIMESTAMP TLV (as defined in [RFC6622bis]) for inclusion in an outgoing message.

- Verification of an ICV TLV contained in a message, in order to determine if this message MUST be rejected as "badly formed and therefore invalid for processing" [RFC6130] [OLSRv2].
- 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].

Specific cases of the ICV and TIMESTAMP TLVs that MUST be implemented in conforming implementations of NHDP and OLSRv2 are specified in this document, referenced from [RFC6622bis].

ICV Packet TLVs 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 possible 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:

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

The ICV algorithm whose implementation is REQUIRED by this framework is an HMAC [RFC2104] using the SHA-256 hash function [RFC4634] and a single secret key shared by all routers.

[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:

- 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.
- 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:

- MAX_HELLO_TIMESTAMP_DIFF > 0
- MAX_HELLO_TIMESTAMP_DIFF < REFRESH_INTERVAL
- MAX_TC_TIMESTAMP_DIFF > 0
- 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 the modifications how messages are generated and processed in [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 specification, each message MUST contain:

- One ICV Message TLV (as specified in [RFC6622bis]), generated according to Section 6.2, with:
  - For TC messages:

    + type-extension := 1

    * For HELLO messages:

       + type-extension := 2

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

    * cryptographic-function := 3 (HMAC)

  o One TIMESTAMP TLV (as specified in [RFC6622bis]), with:

    * 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 in this case:

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

2. A TLV of type TIMESTAMP, as specified in Section 6.1, is added to the Message TLV block. The message size is updated accordingly.

3. A TLV of type ICV, as specified in [RFC6622bis], is added to the Message TLV block. The message size is updated accordingly.

4. <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". This document adds 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:

- The Message TLV block of the message does not contain exactly one TIMESTAMP TLV and exactly one ICV TLV, each with the type extension, and in the former case hash function and cryptographic function, specified in Section 6.1. (The message may contain additional ICV and/or TIMESTAMP TLVs, but with different parameters.)

- Validation of the ICV TLV in the Message TLV block of the message fails, according to Section 6.3.1.

- Validation of the TIMESTAMP TLV in the Message TLV block of the message fails, according to Section 6.3.2.

6.3.1. Invalidating a Message Based on Integrity Check

Consider the ICV Message TLV identified as described in Section 6.2:

1. The identified ICV Message TLV is 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 Section 6.1, as specified in [RFC6622bis].

4. If this message 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 if required (as it MUST be if the message is forwarded) the ICV Message TLV is returned to the message, whose size is updated accordingly. (Alternatively, the original received message may be used.)

6.3.2. Invalidating a Message Based on Timestamp

Consider the TIMESTAMP Message TLV 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.

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. References

10.1. 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.

10.2. Informative References

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104.

[RFC4634] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)", RFC 4634.

Authors' Addresses

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/

Christopher Dearlove
BAE Systems ATC

Phone: +44 1245 242194

Email: chris.dearlove@baesystems.com
URI: http://www.baesystems.com/

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

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