Mobile Ad hoc Networking (MANET)
Internet-Draft
Intended status: Standards Track
Expires: November 30, 2012

U. Herberg
Fujitsu Laboratories of America
T. Clausen
LIX, Ecole Polytechnique

May 29, 2012

Using Integrity Check Values and Timestamps For Router Admittance in NHDP
draft-ietf-manet-nhdp-sec-02

Abstract

This document specifies a security extension to the MANET Neighborhood Discovery Protocol (NHDP). The extension introduces the use of Integrity Check Values (ICVs) and Timestamps in HELLO messages in order to provide a router admittance mechanism, and therefore to counter a selection of security threats to NHDP.

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 November 30, 2012.

Table of Contents

1. Introduction

This document specifies the use of Integrity Check Values (ICVs) for router admittance in the MANET Neighborhood Discovery Protocol (NHDP) [RFC6130]. It specifies the use of such ICVs for validating the identity of the originator of a HELLO message, for validating of the content (i.e., the links being advertised) of a HELLO message, and for validating the message integrity.

This document uses the TLVs defined in [RFC6622] within NHDP HELLO messages, and specifies extensions (as enabled by Section 16 in [RFC6130]) to the HELLO message processing.

Schematically, the mechanism specified in this document inserts itself between [RFC6130] processing/generation of HELLO messages and [RFC5444] encoding/decoding as illustrated in Figure 1.

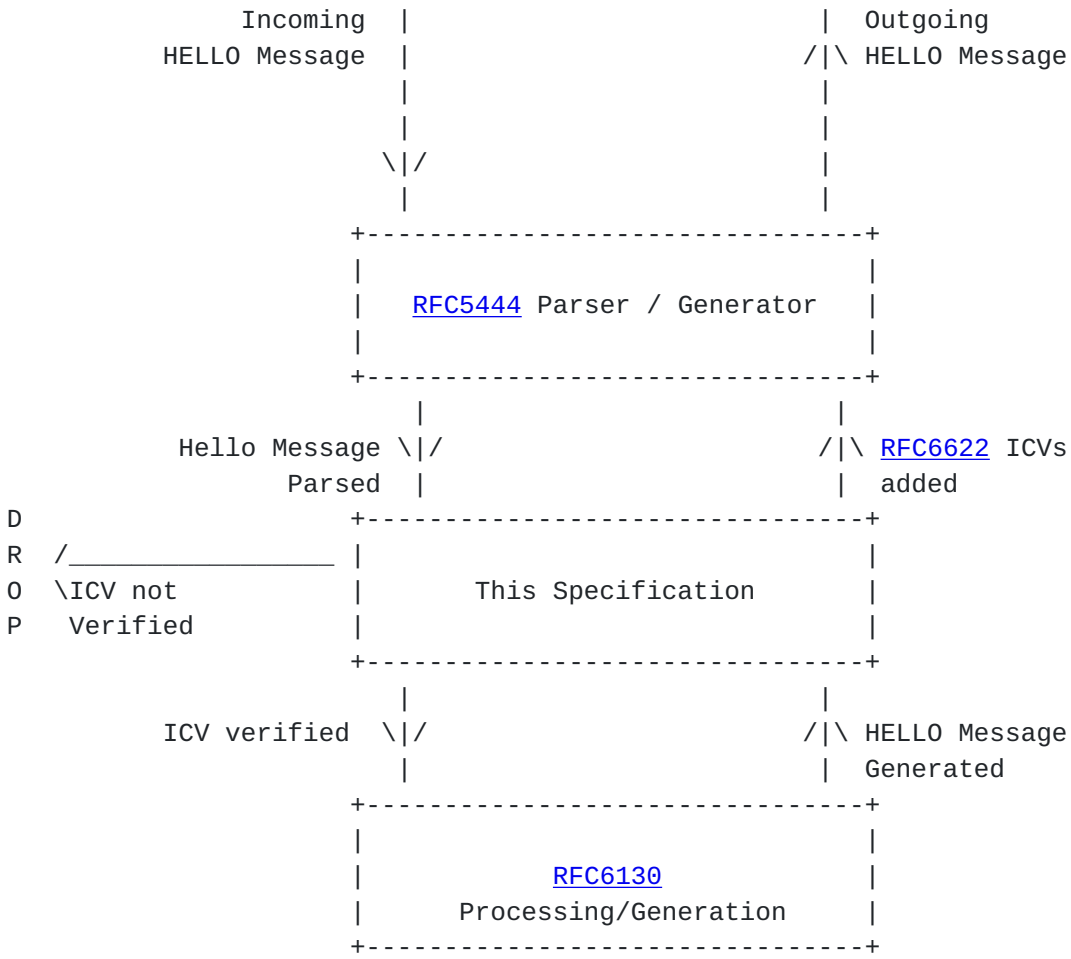

Figure 1: Relationship with RFC5444 and RFC6130.

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 RFC 2119 [RFC2119].

Additionally, this document uses the terminology of [RFC5444], [RFC6130], and [RFC6622].

Additionally, this document introduces the following terminology:

NHDP Router:
A MANET router, running NHDP as specified in [RFC6130].

3. Applicability Statement

[RFC6130] enables extensions to recognize additional reasons for rejecting a message as "badly formed and therefore invalid for processing", and mentions security as an explicit example.

This document:

- Specifies an extension to [RFC6130] by providing a framework for associating ICVs to messages and for using such invalid ICVs as one such "additional reason" for rejecting a message as "badly formed and therefore invalid for processing".

- Uses the containers for carrying ICVs and timestamps, as well as the registries for cryptographic code-points, specified in [RFC6622].

- Is applicable where ICVs are an appropriate security solution. Note that the choice of the cryptographic function are to be made for each given deployment, and that the choice of such is out of scope for this document.

- Assumes that a router which is able to generate correct ICVs (e.g., has valid cryptographic keys), is considered trusted.

- Assumes that the TLV type extension of the ICV Message TLV, as defined in [RFC6622] is 1, i.e., that an ICV is composed of a cryptographic function over a hash value of the message as defined in Section 12 of [RFC6622].

This document does NOT:

- Specify how to distribute cryptographic keys, shared secrets, parameters for cryptographic functions, etc.
- Specify how to detect compromised routers with valid keys.
- Specify how to handle compromised routers with valid keys, i.e., key-revocation etc.

4. Protocol Overview and Functioning

The framework presented in this document provides two functionalities:

- Generation of an ICV for an outgoing HELLO message.
- Verification of an ICV in order to determine if an incoming HELLO message MUST be rejected as "badly formed and therefore invalid for processing" [RFC6130].

When an NHDP Router generates a HELLO message on an interface, this extension:

- Specifies how to calculate an ICV for the message.
- Specifies how to include that ICV by way of a TLV.

The framework allows for adding several ICVs with different hash and cryptographic functions.

[RFC6130] allows for rejecting incoming HELLO messages prior to processing by NHDP. This extension specifies that for each ICV TLV in the Message TLV Block of an incoming message, the message MUST be rejected if the ICV can not be verified.

5. HELLO Message Content

HELLO messages MUST have the content as specified in [RFC6130]. In addition, in order to conform to this specification, each HELLO message MUST contain:

- A <msg-orig-addr> element (as specified in [RFC5444]).
- A <msg-seq-num> element (as specified in [RFC5444]).
- One or more ICV TLVs (as specified in [RFC6622]), generated according to Section 6.

If protection against replay attacks is desired, then a HELLO message MUST also contain:

o A TIMESTAMP TLV (as specified in [RFC6622]).

6. HELLO Message Generation

After HELLO message generation ([RFC6130] Section 11.1) and before HELLO message transmission ([RFC6130] Section 11.2), as permitted by [RFC6130] Section 12.1, the additional elements specified in Section 5 MUST (unless already present) be added to an outgoing HELLO message.

The following processing steps MUST be taken for each cryptographic algorithm that is used for generating ICVs for a HELLO message:

1. All existing TLVs (if any) of type ICV are temporarily removed from the message. Any temporarily removed TLVs MUST be stored, for being reinserted into the message in step 5.

2. The message size is recalculated to the size of the message without the temporarily removed ICV TLVs.

3. The ICV value is calculated over the whole message (as resulting after step 2) according to the chosen hash and cryptographic function and according to Section 12.1 of [RFC6622].

4. A TLV of type ICV and with type extension 1 is added in the Message TLV block, with the content according to Section 12.1 of [RFC6622].

5. All other ICV TLVs that have been temporary removed, are restored.

6. The message size is recalculated, including the new ICV TLV as well as any restored temporarily removed ICV TLVs.

7. HELLO Message Processing

[RFC6130] specifies that:

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

[RFC6130] proceeds to give a number of conditions that, each, will lead to a rejection of the HELLO message as "badly formed and

therefore invalid for processing". This document adds the following conditions to that list which, if true, MUST cause NHDP to consider the HELLO message as invalid for processing:

- The HELLO message does not include a <msg-orig-addr> element.
- The HELLO message does not include a <msg-seq-num> element.
- The Message TLV block of the HELLO message contains more than one TIMESTAMP TLV with the same type extension.
- Validation of ICVs in the Message TLV block of the HELLO message fails, according to Section 7.1.
- If protection against replay attacks is desired, validation of the TIMESTAMP TLV of the message fails, according to Section 7.2.

7.1. Invalidating a Message Based on ICVs

1. For each ICV Message TLV in the HELLO message, the ICV TLV is temporarily removed if:
   * The ICV Message TLV type extension is not equal to 1; OR
   * The ICV Message TLV type extension is equal to 1, AND the hash function and the cryptographic function indicated in that ICV Messsage TLV are unknown to the NHDP Router.
2. If no ICV Message TLVs remain after step 1, then validation fails:
   * The HELLO message MUST be considered "badly formed and therefore invalid for processing", and MUST be discarded.
3. Otherwise, the HELLO message with the remaining ICV Message TLVs (henceforth: "Known ICV Message TLVs") is processed as follows:
   1. All Known ICV Message TLVs are temporarily removed from the message, and the message size is recalculated.
   2. Each of the temporarily removed Known ICV Message TLVs from the step above is, then, processed as follows:
      + Calculate the message-hash-value over the HELLO message, using the hash function indicated by <hash-function> in the Known ICV Message TLV.

+ Calculate the message-ICV-Value over the resulting message-hash-value, using the cryptographic function, and the key ID, indicated by <cryptographic-function> and <key-id> in the Known ICV Message TLV.

+ If message-ICV-Value differs from the value of <ICV-data> in the Known ICV Message TLV, then validation fails:

  - The HELLO message MUST be considered "badly formed and therefore invalid for processing", and MUST be discarded.

4. Otherwise, the message is considered (with respect to this specification) "valid for processing", and:

   A. All temporarily removed ICV Message TLVs (i.e., all ICV TLVs temporarily removed in both step 1 and step 3) are restored.

   B. The message size is restored.

7.2. Invalidating a Message Based on Timestamps

An NHDP Router which requires protection against replay attacks MUST:

- Be configured with a list of TIMESTAMP type extensions, which it supports.

- For each of these TIMESTAMP type extensions, define MAX_TIMESTAMP_DIFF as the maximum allowed difference between the "expected timestamp value" and the "timestamp value" encoded in the TIMESTAMP TLV of an incoming HELLO message (e.g., to accommodate for propagation delays across a network).

A HELLO message MUST be considered "badly formed and therefore invalid for processing", and MUST be discarded if either of the two following conditions are true:

- The Message TLV Block of the HELLO message does not contain a TIMESTAMP TLV with a type extension matching (one of) the timestamp types, known by the receiving NHDP Router.

- The Message TLV Block of the HELLO message does contain a TIMESTAMP TLV with a type extension matching (one of) the timestamp types, known by the receiving NHDP Router, but where the value of that TIMESTAMP TLV differs from the expected value by more than MAX_TIMESTAMP_DIFF.

8. Provisioning of NHDP Routers

Before an NHDP Router is able to generate ICVs or validate messages, it MUST acquire the cryptographic key(s) and any parameters of the cryptographic function from all other routers that are to participate in the network. This document does not specify how a router acquires the cryptographic keys and parameters used in the MANET.

9. Summary of NHDP Interaction

When using the NHDP security extension, specified in this document, the following MUST be observed:

- HELLO messages MUST be generated according to [RFC6130].
- Outgoing HELLO messages, generated by [RFC6130], MUST be processed according to Section 6 after their generation and prior to their transmission by [RFC6130], in order that (an) ICV TLV(s) can be generated and inserted, as allowed by Section 16 in [RFC6130].
- Any other extension to [RFC6130] which adds information to a HELLO message MUST do so prior to the HELLO message being handed off for ICV generation according to this specification.
- An incoming HELLO message MUST be processed according to Section 7 prior to processing by [RFC6130] as allowed in Section 16 in [RFC6130].
- Any other NHDP extension, which has added information to a HELLO message and which wishes that the HELLO message is rejected if an ICV is not valid, MUST likewise process the HELLO message only after its processing according to this specification.

10. IANA Considerations

This document has no actions for IANA.

11. Security Considerations

This document specifies a protocol extension to NHDP which allows for alleviating some of the security threats of NHDP analyzed in [NHDP-sec-threats].

11.1. Alleviated Attacks

This section briefly summarizes which of the security threats, from among those detailed in [NHDP-sec-threats], that are alleviated by the framework presented in this document.

11.1.1. Identity Spoofing

As only NHDP Routers possessing valid cryptographic keys are able to add ICV TLVs HELLO messages, in a way which permits that these be validated successfully, identity spoofing is counteracted.

11.1.2. Link Spoofing

Link spoofing is counteracted by the framework specified in this document, with the same argument as in Section 11.1.1. A router without access to valid cryptographic keys cannot generate valid ICVs for inclusion in a HELLO message.

11.1.3. Replay Attack

Replay attacks are only counteracted if TIMESTAMP TLVs are included in HELLO messages. This is optional, and depends on synchronized clocks of all routers in the MANET. An attacker which records messages to replay them later can only do so in the time interval between the timestamp that is contained in the TIMESTAMP TLV and MAX_TIMESTAMP_DIFF later. As an attacker cannot modify the content of the TIMESTAMP TLV (since it does not possess the valid cryptographic keys for generating valid ICV TLVs), it cannot replay messages after this time interval. Within this time interval, however, it is still possible to perform replay attacks.

11.2. Limitations

Since jamming is a physical layer issue, it cannot be alleviated by protocols on the routing layer. This framework does not counteract jamming attacks.

If no synchronized clocks are available in the MANET, replay attacks cannot be counteracted by the framework provided by this document.

The framework provided by this document does not avoid or detect security attacks by routers possessing the cryptographic keys that are used to generate ICVs for messages.

This document depends on the quality of the used cipher algorithm and hash function, and is as such subject the same security considerations as applies to these.

This document relies on an out-of-band protocol or mechanism for distributing keys and cryptographic parameters. The security considerations of such protocol or mechanism also apply.

This document does also not provide a key revocation mechanism.

12. Acknowledgments

The authors would like to thank Jiazi Yi (Ecole Polytechnique) for his review and comments to this document.

13. References

13.1. 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 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, March 2011.

[RFC6622] Herberg, U. and T. Clausen, "Integrity Check Value and Timestamp TLV Definitions for Mobile Ad Hoc Networks (MANETs)", RFC 6622, May 2012.

13.2. Informative References

[NHDP-sec-threats] Herberg, U., Clausen, T., and J. Yi, "Security Threats for NHDP", work in progress draft-ietf-manet-nhdp-sec-threats-00.txt, April 2012.

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/

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/