HIP
Internet-Draft
Intended status: Standards Track
Expires: April 26, 2009

F. Cao
Cisco Systems
H. Deng
China Mobile

October 23, 2008

Delivering Geographic Location in Host Identity Protocol (HIP) draft-cao-hip-geolocation-01

Status of this Memo

Abstract

This document defines a new parameter for delivering geographic location in Host Identity Protocol (HIP). For mobile users using HIP, one generic mechanism is proposed to share or update their geo-location information with either rendezvous servers or their peers. In addition, geo-location privacy is also protected with the help of the ENCRYPTED parameter.

Table of Contents

1. Introduction

This document defines a new extension for delivering geographic location in Host Identity Protocol (HIP) [RFC4423]. For some mobile users using HIP, their geo-location information can play an important role for some new location-based services.

For example, if a roaming user using HIP enters into a different location, his latest geo-location can be shared with his peers for various services, such as localized advertisements, social networking, and emergency services.

Another example is that rendezvous server may use geographic locations of its rendezvous clients for better services.

Additionally, location privacy has been a big concern for many mobile users, and must be addressed so that such geo-location information can be securely protected from end to end in HIP.

In this document, a new generic mechanism is proposed to share or update the geo-location information in HIP. Both the centralized approach based on rendezvous servers, or the distributed approach based on the peers, are discussed and demonstrated. Furthermore, geo-location privacy is also considered with the help of the ENCRPTED parameter.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Host Identity Tag (HIT): the hashed 128-bit value from host identifier in HIP

Rendezvous Server (RVS): A HIP registrar providing rendezvous service

Geo-location: Geographic location that may be presented in various formats, such as civil address, geodetic-2d, and geodetic-3d.

Peer connection: the relationship set up directly between initiator and responder in HIP.

Location-by-Reference (LbyR): the presentation of location information is the reference link where the actual value can be obtained.

Location-by-Value (LbyV): the presentation of location information is the actual value in one of the known formats describing the location.

3. Overview

This section gives an overview of the requirements and the mechanisms for delivering geographic location in HIP. In particular, some extensions are introduced to carry the geo-location information with the option of location privacy protection.

3.1. Requirements

Geo-location should be added by following the general HIP parameter definitions and satisfying the related location privacy guidelines.

The following requirements should be addressed:

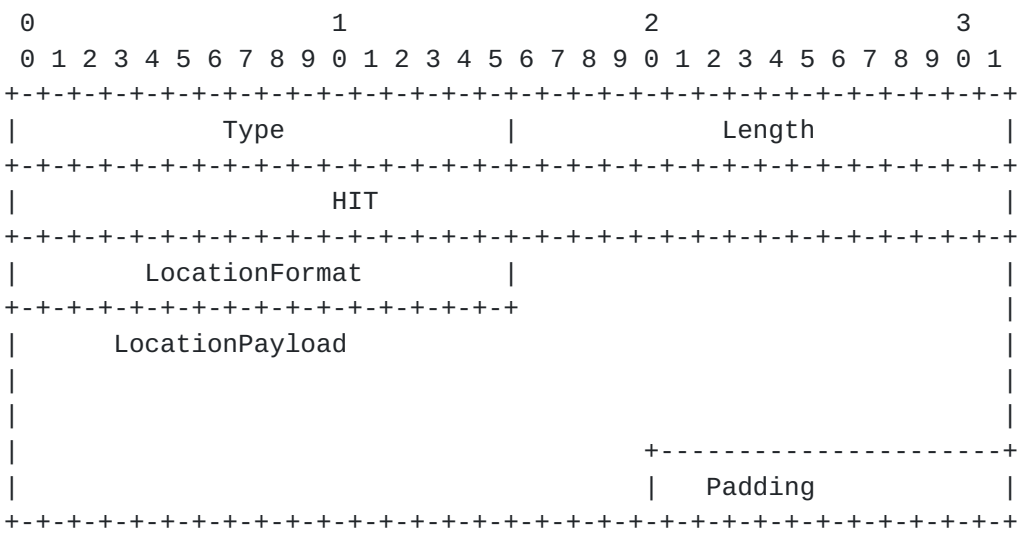
- The mechanism must be extensible for carrying current various geo-location formats and potential future formats
- The distributed model as peer connections must be outlined
- The centralized model as rendezvous services must be outlined
- The security mechanism for protecting geo-location privacy must be addressed

3.2. GEOLOC Parameter

When the initiator or the responder wants to share its geo-location with either rendezvous servers or its peers in HIP, the most efficient mechanism is to use a new geo-location parameter. Inside such a geo-location extension, the information about geo-location can be inserted and delivered along with HIP messages.

Similarly, in some centralized scenarios, the rendezvous servers may also distribute or update the geo-location information about some registered HIP clients by using this geo-location parameter.

The GEOLOC parameter are defined as follows:



Type 16 [TBD by IANA]
Length 16 [length in octets, excluding Type, length, padding]
HIT Host Identity Tag
LocationFormat 16 [type of geo-location formats]
LocationPayload the presentation of location in the indicated format

Figure 1: GEOLOC parameter format

"LocationFormat" specifies the exact format for presenting geo-location. Note that there are two categories in LocationFormat: one is LbyV, and the other LbyR.

In order to clarify the difference, the first bit, I, in LocationFormat is used as the indicator. If I is set to be 0, it means LbyV is presented. Otherwise, LbyR is presented when I is set to be 1.

All the current formats for geo-location can be included by assigning the numbers for them. For example, binay geodetic-3d format defined in [RFC3825] can be covered. Similarly, PIDF-LO defined in [RFC5139] can also be covered.

[TBD ... the enum for location formats ...]

"LocationPayload" will be inserted after "LocationFormat" and followed by the additional proper padding.

3.3. Privacy Protection

Location privacy is among the top concerns in Location-based services. Whenever mobile users like to share or receive the

location information, the secure mechanism must be available for addressing location privacy.

The secure mechanism can be fully built upon another exising HIP exention, by embedding geo-location GEOLOC into "Encrypted" parameter in HIP header (See Section 5.2.15 in RFC 5201).

The GEOLOC parameter can be embedded as follows:

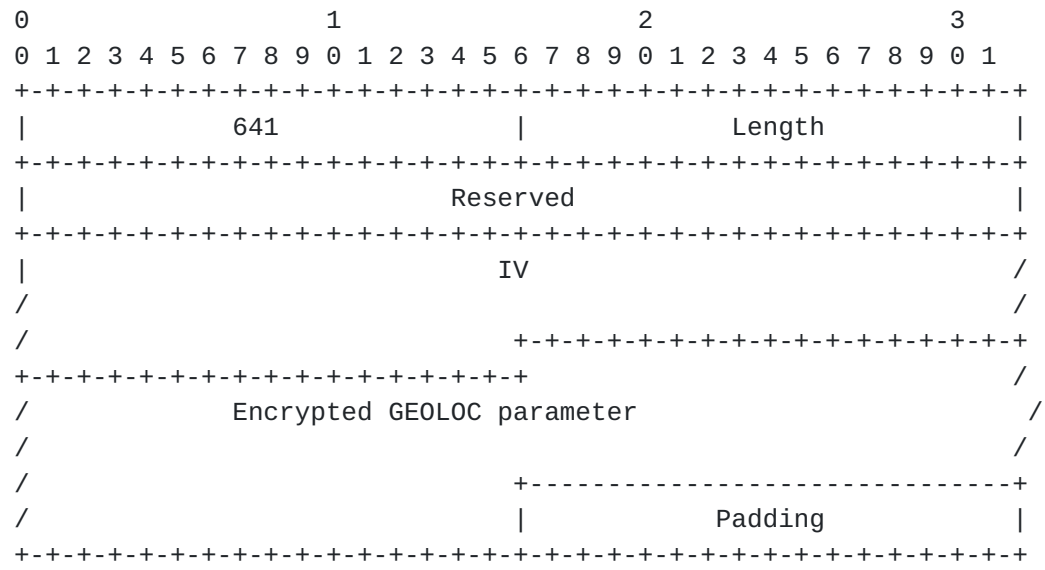


Figure 2: Encrypted GEOLOC parameter

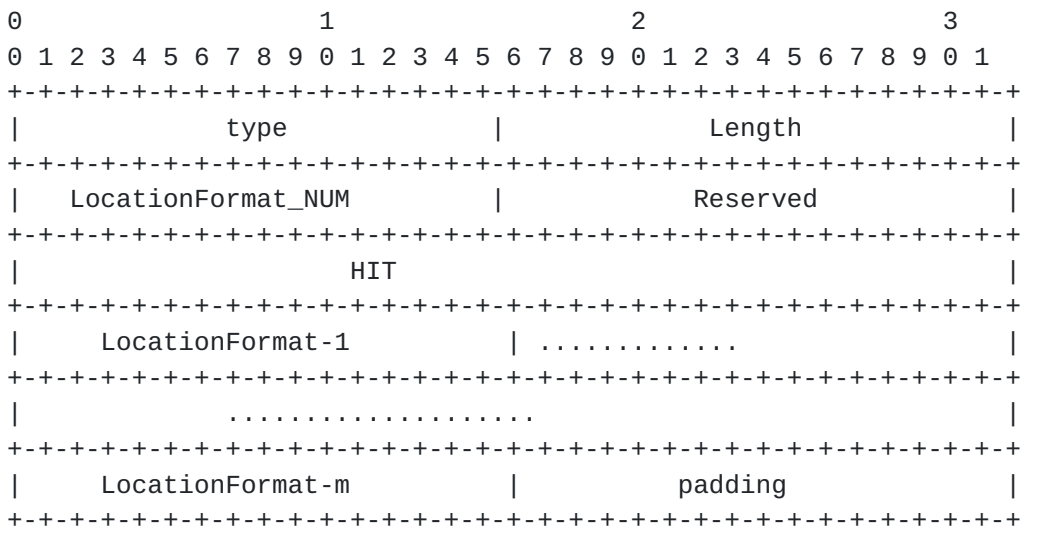
"Encrypted GEOLOC parameter" is created by following the procedures defined in "Encrypted" parameter.

With the help of "Encrypted" parameter, GEOLOC parameter can be fully protected without any disclosure to other parties that are not involved in this HIP connection.

3.4. Request for obtaining geo-location

This provides an option for allowing the HIP parties to ask for the geo-location information of others. Then it is up to location policies for granting or denying the permission to the requestor. requestor.

The GEOLOC_REQ parameter is defined as follows:



Type 16 [TBD by IANA]
Length 16 [length in octets, excluding Type, length, padding]
LocationFormat-NUM 16 [type of geo-location formats]

Figure 3: GEOLOC_REQ parameter format

LocationFormat_NUM lists the number of the preferred geo-location format(s) when GEOLOC parameters are returned back.

With the help of GEOLOC_REQ parameter, each HIP party can indicate its interest of acquiring the geo-location information of others.

But the receiver of such a GEOLOC_REQ parameter needs to check the location policy before granting such a request (To be discussed more in the following section).

[Open question: how RVS can provide the error codes for GEOLOC_REQ?]

4. Use cases with HIP flows

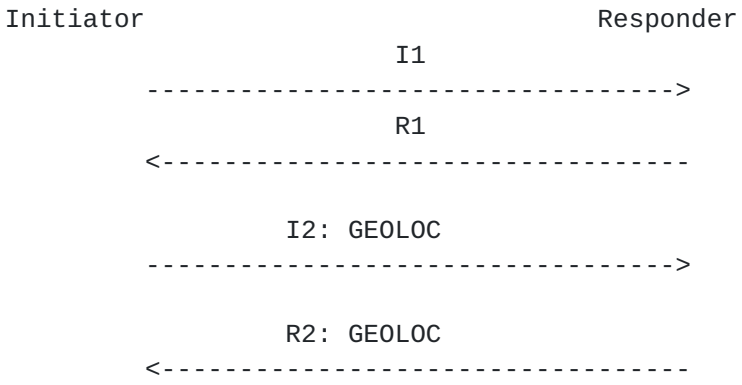
There are multiple ways to use this new Geo-location parameter in various scenarios. In this section, some major use cases are demonstrated, including

- sharing geo-location in setting up peer connections
- carrying geo-location in the registration with rendezvous servers
- distributing geo-location from rendezvous servers
- updating geo-location in peer connections
- updating geo-location to rendezvous servers

4.1. Setting up peer connection

The initiator or the responder can share his geo-location when the connection is set up.

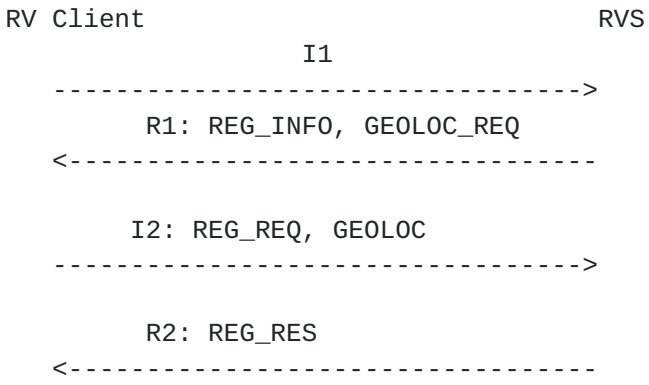
When location privacy is not needed, the initiator or the responder can begin sharing its geo-location information as the early as I2 or R2.



When location privacy is desired, the initiator or the responder must embed the GEOLOC parameter into Encrypted parameter and then send the finalized HIP packet in I2 or R2.

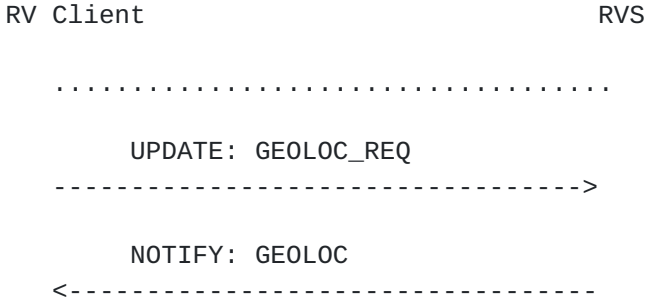
4.2. Registration in rendezvous services

Rendezvous clients can inform Rendezvous Server of their geo-locations during their registrations.



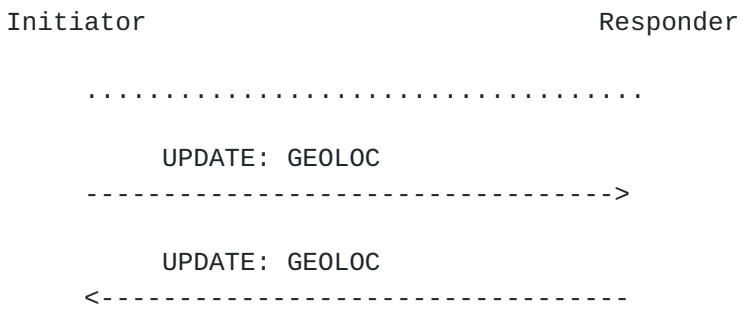
4.3. Distribution from rendezvous servers

RVS can serve as Location Server (LS) (See [RFC3693]) for sharing the location information with HIP clients, with the help of Rule Holder (RH) for location policies.



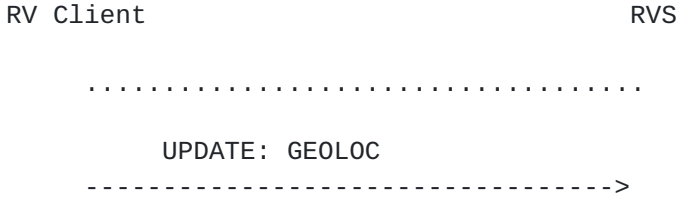
4.4. Updates in peer connections

For mobile users, they can update their geo-location when their positions have been changed.



4.5. Updates to rendezvous servers

For rendevous clients, they can update their rendevous servers with their latest geo-locations.



It is similar that GEOLOC can be embedded into ENCRYPTED parameter for location privacy protection.

5. Security Considerations

This document provides the HIP parameters for sharing geo-location information among HIP parties.

Some existing work on geo-location privacy (see [RFC3693, RFC3694]) should be carefully integrated so that the secure models can help to address the potential threats.

For example, RVS may include the functions of Location Information Server (LIS) and the Rule Holder (RH). The desired policies can be enforced when the geo-location information is exchanged through RVS among rendezvous clients.

On the other hand, RVS may become the target for disturbing the desired geo-location services.

The frequency of geo-location updates may also be used by the hackers as another way for generating DoS attacks.

[More to be added, such as rate limit on control packets with GEOLOC_REQ, frequency limit on geo-location update, ...]

6. IANA Considerations

This document updates the IANA registry for HIP parameters Types by assigning new values for the following new HIP parameter types:

- GEOLOC (defined in Overview Section)
- GEOLOC_REQ (defined in Overview Section)

7. Acknowledgments

The editor and the contributors would like to acknowledge the constructive feedback and input provided by David Ward, Varjonen Samu, and Suping Zhai.

8. References

8.1. Normative References

[1] Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, "Host Identity Protocol", RFC 5201, April 2008.

[2] Moskowitz, R. and P. Nikander, "Host Identity Protocol (HIP) Architecture", RFC 4423, May 2006.

[3] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", RFC 5204, April 2008.

[4] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", RFC 3693, February 2004.

[5] Danley, M., Mulligan, D., Morris, J., and J. Peterson, "Threat Analysis of the Geopriv Protocol", RFC 3694, February 2004.

[6] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", RFC 5139, February 2008.

[7] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004.

8.2. Informational References

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

[9] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

[10] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4776, November 2006.

Authors' Addresses

Feng Cao
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
USA

Email: fcao at cisco dot com

Hui Deng
China Mobile
53A Xibianmennei Ave.
Beijing 100053
China

Email: denghui at chinamobile dot com

Full Copyright Statement

Intellectual Property