Information Distribution over GRASP
draft-liu-anima-grasp-distribution-00

Abstract

   This document discusses the requirement of information distribution
   capability in autonomic networks. Ideally, the autonomic network
   should support distributing some information which is generated/
   injected at an arbitrary autonomic node and be distributed among the
   whole autonomic domain. This docuemnt specifically proposes to
   achive this goal based on the GRASP (A Generic Autonomic Signaling
   Protocol), and proposes relevant protocol extension to GRASP.

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 April 21, 2016.

Copyright Notice

Table of Contents

1. Introduction

The GRASP is mostly for negotiation between two nodes. Besides
negotiation function, there is also requirement of simply delivering
information among nodes. GRASP synchronirozation is defined for this
requirement. However, the synchronization is a very simple mechanism
that might not fulfil all the information delivery requirements in a

autonomic network. So this document proposes a comprehensive
function called "Distribution Capability" to fulfil the goals.
Multicast/flooding behaviors are involved in distribution capability,
but distribution capability itself doesn't simply equal to these
behaviors.

This document describes the requirements of distributing information/
signal (e.g. Autonomic Network Intent, which is discussed in
[I-D.du-anima-an-intent]) in an autonomic network. Although the
most obvious distributed information might be Intent, this document
considers distribution capablility as a general function that the
autonomic networks should support,rather than a specific mechanism
dedicated for Intent. Ideally, the information/signal may be
generated/injected at an arbitrary autonomic node and be distributed
among the whole autonomic domain. This docuemnt specifically
proposes to achive this goal based on the GRASP (A Generic Autonomic
Signaling Protocol) [I-D.ietf-anima-grasp] , and proposes relevant
protocol extension to GRASP.

2. Information Distribution Scenarios

2.1. Whole Domain Distribution

Once the information is input to the autonomic network, the node that
firstly handle the information MUST be able to distribute it to the
all the other nodes in the autonomic domain.

2.2. Selective Distribution

The distribution only works on a specific group nodes to control
unnecessary flooding.

2.3. Incremental Distribution

The distribution only goes to the nodes that newly get online.

3. Distribution Capability Requirements

3.1. Generic requirements

3.1.1. Autonomic Domain Boundary

The domain boundary devices are supposed to know themselves as
boundary.When the distribution messages come to the devices, they do
not distribute them outside the domain.

[Editor's Notes] It is a practical issue that how an autonomic node
recognizes itself as a domain boundary device. It is not in the
scope of this document.

[3.1.2](#). Avoiding Signaling Storm

There should be a mechanism to prevent the distributed object to
travel around the domain again and again, so that there would not be
a large amout of redundant packets troubling the network.

[3.1.3](#). Arbitrary Injecting Point (Optional)

The distributed object SHOULD be injected at any autonomic node
within the domain (or within a specific group [TBD]).

[3.1.4](#). Confliction Handling (Optional)

As long as it supports arbitrary point of injecting an object, there
is possibility that two nodes advertise the same object but with
conflict content. Hence, there should be a mechanism to handle the
confliction.

[3.1.5](#). Verification of Distributed Information

o Information integrity verification

     The recieving node SHOULD be able to verify whether the
     distributed information is from the certain node. In other
     words, it needs to make sure the information hasn't been
     modified.

o Source authorization verification

     Even the information integrity was verified, the distibuted
     information might still be invalid, since the distribution
     source might doesn't have the right to distribute such
     information that it just exceeds its authority.

[3.2](#). Node Behavior

[3.2.1](#). Flooding

The flooding behavior is mostly for the whole domain distribution
scenario.

o Flooding to all interfaces

   a) Flooding to all the interfaces attached to the node. This is
      the basic requirement. The interfaces include both phisical
      interfaces and the virtual interfaces for example the ACP
      tunnels.

   b) Besides replicating the message to all interfaces, the node
      might also replicate the message to all recorded IP addresses
      of all the other nodes. The addresses might be got through
      some mechanisms such as routing protocol. This L3
      communication behavior could also be seen as a flooding. [Open
      Question] Do we need this L3 distribution feature?

   o Loop Avoidance

      When messages are flooded off link, it is highly possible that
      the message would be flooded back to the initiator again, thus
      there would be a large amount of duplicated messages circling
      around the network. So, there needs to be relevant mechanism
      to avoid/limit the packets loop.

3.2.2. Selective Flooding

   In contrast to flooding, there should be selective fooding of the
   node to achieve selective distribution.

   Selective flooding means the receiving node would only replica the
   informaion to part of the interfaces.

   [Editor's Note] Details TBD.

3.2.3. Point to Point

   To fulfil the incremental distribution, the nodes also need to
   support point to point mode. This behavior is already included in
   current GRASP in the form of Synchronization.

3.3. Distribution indication

   The autonomic nodes need to be able to distinguish the information
   that needs to be distributed from the other information. Hence,
   there should be an indication signal within the messgage that carries
   the information. This could be achieved through various ways:

   o A new message dedicated for distribution. The message itself
      means it needs to be distributed, the receiving nodes will
      distribute the whole messge.

o A new option dedicated for distribution. the receiving nodes might
   not need to distribute the whole messge, they could distribute the
   option in other messages they slected.

o An indicator such as flag in message or option. In this case,
   every existing message or option could be extended to indicate
   distribution.

[Open discussion] Which one is the best approach?

3.4. Selective distribution indication

When doing selective flooding, the node needs to be aware of which
interfaces should be sent the distributed information and which are
not.

One possible way is that the chosen interfaces match a certain
policy/rule which carried along with the distributed information.
The nodes would parse the policy/rule and decide which interfaces to
be flooded accordingly.

4. Information Distribution over GRASP

This section makes some extension to the signalling protocol to
fulfil the distribution requirement.

4.1. Distribution indication

4.1.1. Candidated solution 1: Overloading current messages

o Initiating Node

   a) Assuming there is a distribution module running apon GRASP in
      charge of the information distribution.

   b) The distribution module calls the GRASP module to encapsulate
      the distributed information into an Option (either dedicated
      distribution option or other options that extended by a
      Distribution flag) in an Unsolicited Response Message (as
      discussed in Section 3.3.5 of [I-D.ietf-anima-grasp]), and
      send the message to all the interfaces.

o Receiving Node

   a) Assuming there is an distribution module running upon GRASP in
      charge of the information distribution.

b) After recieving the distributed information, The GRASP module
   relay the message to other interfaces.

c) However, if the node is the distribution boundary, it MUST NOT
   relay the message again.

In this case, the Response Message is overloaded for distribution
indication, when it is an Unsolicited Response Message. This
solution is already covered by current [I-D.ietf-anima-grasp] .

4.1.2. Candidated solution 2: Information Distribution Message

Although the distribution behavior might be achieved by using current
GRASP messages, the message overloading might add unnecessary
complexity to the GRASP stack.

So, a new message dedicated for information distribution might be
better.

4.2. Selective Distribution indication

There needs to be new added mechanism to achieve this goal,
regardless of which distribution indication candidate solution is
chosen.

Specific desigh is TBD.

4.3. Node behavior

4.3.1. Flooding behavior

o Basic behavior

   When the node receives a distributed information message/
   option, it replicates the information to all the other
   interfaces.

o Loop Avoidance

   There might be multiple ways to achieve this goal. This
   document proposes two of them for discussion.

   One is as the following:

   a) The node maintains a flooding state table which stores each
      interface's record that whether a specific distributed
      message (or option) had been received or sent from it. The

identification could be the combination of the Sequence
Number and Node ID.

b) The node MUST NOT send a flooding message/option to the
   interfaces that had received or sent the same distributed
   information.

The other is:

flooding with sequence numbers for loop/duplicate avoidance

o Flooding TTL

In case an message/option is occasionally looped around, the
Flooding TTL is to guarantee the packet would not travel in a
infinite loop in the network.

4.3.2. Selective Flooding behavior

TBD.

4.3.3. Point to Point behavior

The point to point distribution has been covered by the GRASP
Synchronization function.

5. Security Considerations

The distribution source authentication could be done at multiple
layers:

o Outer layer authentication: the GRASP communication is within a
   protected channel such as ACP (Autonomic Control Plane,
   [I-D.behringer-anima-autonomic-control-plane]).

o Inner layer authentication: the GRASP communication might not be
   within a protected channel, then there should be embedded
   protection in distribution itself. Public key infrastructure
   might be involved in this case.

6. IANA Considerations

TBD.

7. Acknowledgements

This document is inherited from [I-D.ietf-anima-grasp] and
[I-D.behringer-anima-reference-model]. So thanks all the
contributors of the two work items.

This document was produced using the xml2rfc tool [RFC2629].

8. References

8.1. Normative References

[I-D.ietf-anima-grasp]
          Bormann, C., Carpenter, B., and B. Liu, "A Generic
          Autonomic Signaling Protocol (GRASP)", draft-ietf-anima-
          grasp-01 (work in progress), October 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
          Requirement Levels", BCP 14, RFC 2119,
          DOI 10.17487/RFC2119, March 1997,
          <http://www.rfc-editor.org/info/rfc2119>.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629,
          DOI 10.17487/RFC2629, June 1999,
          <http://www.rfc-editor.org/info/rfc2629>.

8.2. Informative References

[I-D.behringer-anima-autonomic-control-plane]
          Behringer, M., Bjarnason, S., BL, B., and T. Eckert, "An
          Autonomic Control Plane", draft-behringer-anima-autonomic-
          control-plane-03 (work in progress), June 2015.

[I-D.behringer-anima-reference-model]
          Behringer, M., Carpenter, B., Eckert, T., Ciavaglia, L.,
          Liu, B., Jeff, J., and J. Strassner, "A Reference Model
          for Autonomic Networking", draft-behringer-anima-
          reference-model-04 (work in progress), October 2015.

[I-D.du-anima-an-intent]
          Du, Z., Jiang, S., Jeff, J., and L. Ciavaglia, "Autonomic
          Network Intent and Format", draft-du-anima-an-intent-01
          (work in progress), July 2015.

[I-D.irtf-nmrg-autonomic-network-definitions]
          Behringer, M., Pritikin, M., Bjarnason, S., Clemm, A.,
          Carpenter, B., Jiang, S., and L. Ciavaglia, "Autonomic
          Networking - Definitions and Design Goals", draft-irtf-
          nmrg-autonomic-network-definitions-07 (work in progress),
          March 2015.

[I-D.pritikin-anima-bootstrapping-keyinfra]
          Pritikin, M., Richardson, M., Behringer, M., and S.
          Bjarnason, "Bootstrapping Key Infrastructures", draft-
          pritikin-anima-bootstrapping-keyinfra-02 (work in
          progress), July 2015.

Authors' Addresses

   Bing Liu
   Huawei Technologies
   Q14, Huawei Campus
   No.156 Beiqing Road
   Hai-Dian District, Beijing 100095
   P.R. China

   Email: leo.liubing@huawei.com

   Sheng Jiang
   Huawei Technologies
   Q14, Huawei Campus
   No.156 Beiqing Road
   Hai-Dian District, Beijing 100095
   P.R. China

   Email: jiangsheng@huawei.com