Network Working Group B. Liu
Internet-Draft S. Jiang
Intended status: Standards Track Huawei Technologies
Expires: May 4, 2017 October 31, 2016

Information Distribution over GRASP
draft-liu-anima-grasp-distribution-03

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 specifies additional node behavior.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

In an autonomic network, sometimes the nodes need to share a set of common information. One typical case is the Intent Distribution which is briefly discussed in Section 4.5 of [I-D.behringer-anima-reference-model]. However, the distribution should be a general function that one autonomic node should support, rather than a specific mechanism dedicated for Intent. This document firstly analyzes several basic information distribution scenarios

(Section 2), and then discusses the technical requirements (Section 3) that one autonomic node needs to fulfill.

This document proposes to achieve distribution function based on the GRASP (A Generic Autonomic Signaling Protocol) [I-D.ietf-anima-grasp]

. GRASP already provides some capability to support part of the distribution function. Along with that, this document also proposes some additional functionality. Detailed design is described in Section 4.

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 all the other nodes in the autonomic domain.

The distributed information might not relevant to every autonomic node, but it is flooded to all the devices.

2.2. Selective Distribution

When one node receive the information, it only replicates it to the neighbors that fit for a certain of conditions. This could reduce some unnecessary signaling amplification.

However, this scenario implies there needs to be corresponding mechanisms to represent the conditions and to judge which neighbors fit for the conditions. Please refer to Section 4.3.2 (selective flooding behavior).

2.3. Incremental Distribution

The distribution only goes to the nodes that newly get online. This might mostly happen between neighbors.

The incremental distribution could also be a sub scenario of the whole domain distribution. When one node is doing the whole domain distribution, it is possible that some of its neighbors are sleeping/off-line, so when the neighbors get online again, the node should do incremental distribution of the previous whole domain distributed information.

3. Distribution Requirements

3.1. Identifying 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.

3.2. Arbitrary Injecting Point

The distributed information SHOULD be injected at any autonomic node within the domain (or within a specific set of nodes [TBD]).

3.3. Avoiding Loops

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

3.4. Selective Flooding

When one node receive the information, it only floods it to the neighbors that fit for a certain of rules.

3.5. Point-to-Point Distribution

One node only distributes the information to another node. This is for the incremental distribution scenario.

3.6. Verification of Distributed Information

- o Information integrity verification

  The receiving 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 distributed information might still be invalid, since the distribution source might not have the right to distribute such information that it just exceeds its authority.

3.7. Conflict Handling

As long as it supports arbitrary point of injecting distribution, there is possibility that two nodes advertise the same information but with conflict attribute(s). Hence, there should be a mechanism to handle the conflict.

4. Distribution Function and Behavior Specification

This section specifies using certain GRASP messages for distribution, and also specifies the distribution behavior in an autonomic node.

4.1. Using GRASP Flood Synchronization Message

It is natural to use the GRASP Flood Synchronization message for distribution, since the Flood Synchronization behavior specified in GRASP is identical to the the whole domain distribution scenario described in Section 2.1. And the Flood Synchronization naturally fits for "Arbitrary Injection Point" and "Avoiding Loops" requirements.

4.2. Using GRASP Synchronization Message

It is natural to use the GRASP Synchronization message for Point-to-Point distribution. The two behavior is identical.

4.3. Selective Flooding

4.3.1. Selecting Cretiria

When doing selective flooding, the distributed information needs to contain the cretiria for nodes to judge which interfaces should be sent the distributed information and which are not. Specifically, the cretiria contains:

- o Matching condition: a set of matching rules.

- o Matching object: the object that the match condition would be applied to. For example, the matching object could be node itself or its neighbors.

- o Action: what behavior the node needs to do when the matching object matches or failed the matching condition. For example, the action could be forwarding or discarding the distributed message.

Example:

- o Matching condition: "Device role=IPRAN_RSG"

- o Matching objective: "Neighbors"

- o Action: "Forward"

This example means: only distributing the information to the neighbors who are IPRAN_RSG.

4.3.2. Node Behavior

1) The distribution initial node Includes the Selecting Cretiria information in the message that carries the distributed information.

2) The recieving node decides the action according to the Selecting Cretiria carried in the message.

2-1 When the Matching Object is "Neighbors", then the node matches the relevant information of its neighbors to the Matching Condition. If the node finds one neighbor matches the Matching Condition, then it forwards the distributed messge to the neighbor. If not, the node discards forwarding the message to the neighbor.

2-2 When the Matching Object is the node itself, then the node matches the relevant information of its own to the Matching Condition. If the node finds itself matches the Matching Condition, then it forwards the distributed messge to its neighbors; if not, the node discards forwarding the message to the neighbors.

4.4. Conflict Handling

The distribution information needs to include timestamps or version information. When conflict happens, the node only accepts the latest information.

4.5. Distribution Source Authentication

The distribution source authentication could be done at multiple layers:

- o Outer layer authentication: the GRASP communication is within ACP (Autonomic Control Plane, [I-D.behringer-anima-autonomic-control-plane]). This is the default GRASP behavior.

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

5. Security Considerations

TBD.

6. IANA Considerations

No IANA assignment is needed.

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-07 (work in progress), September 2016.

[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., Nobre, J., Ciavaglia, L., and M. Behringer, "ANIMA Intent Policy and Format", draft-du-anima-an-intent-04 (work in progress), July 2016.

[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