Information Distribution over GRASP

(draft-liu-anima-grasp-distribution-00)

Bing Liu (speaker), Sheng Jiang

@Anima WG, ietf94, Nov 2015

Background

- This new draft was inherited from draft-liu-anima-intent-distribution
  - Not limit the information to Intent only
  - Specifically proposed to use GRASP (A GeneRic Autonomic Signaling Protocol)
- This draft contains:
  - information distribution scenarios
  - requirements analysis of information distribution
  - gap analysis

Distribution Scenarios

- Whole domain distribution
  - E.g. flood network Intent to all the nodes in an autonomic domain
- Selective distribution
  - E.g. distribute some specific policies to the nodes that support a certain objective (possibly based on Discovery cache)
  - E.g. distribute some information to the nodes that belong to a certain role or hierarchy.
    - To reduce signaling storm
    - To gain some information isolation if the information is sensitive
- Incremental distribution
  - E.g. only distribute to the nodes newly get online

Basic Requirements for Node Behavior

- Flooding behavior
  - flood to all interfaces
    - includes both physical interfaces and virtual interfaces such as ACP tunnels
  - loop avoidance

- Selective Flooding
  - only flood the information to part of the interfaces
  - flood to a set of IP addresses (possibly by unicast)

- Point to Point exchange

Basic Requirements for Protocol Indication

- Indicate the distributed information

  - The autonomic nodes need to be able to distinguish the information that needs to be distributed from the other information.

- Indicate the selective flooding criteria

  - the node needs to be indicated which interfaces/addresses should be sent the distributed information.

Gap Analysis 1/2

- Node behavior
  - Flood within ACP
    - [Open Question] The nodes might need to distinguish the ACP tunnel interfaces from other physical/virtual interfaces
  - Loop avoidance
    - Current GRASP defines loop count, which could reduce possible loop messages but could not avoid them
- Indicate the distributed information
  - Current GRASP uses *Unsolicited Response* messages (encapsulate Synchronization objectives) to indicate information distribution. Nodes receive *Unsolicited Response* messages MUST flood them to all the other interfaces.
    - [Open Question] Unsolicited Response is an overloading of Response message. The overloading might easily cause protocol state machine bugs in implementations.
  - Alternatives
    - Define a new type of message dedicated for information distribution.
    - Define a new option dedicated for distribution. (could possibly encapsulated in *Request/Negotiation* messages)
    - Add flag(s) in current message(s)/option(s).
    - [Open Question] Which is the most proper method?

Gap Analysis 2/2

- Indicate the selective flooding criteria
  - Alternatives:
    - The criteria is carried in band of the message. (E.g. the message indicates a role or an objective)
    - Pub-sub mode: nodes to subscribe specific information to the distribution source. The source floods the information to subscribers only.
      - Problems:
        » pub-sub might need a central distribution source, which is in contrast to the architecture
        » distributed pub-sub between neighbors might too heavy for signaling?
  - [Open Question] Which do we want? Or other alternative(s)?

Other requirements for distribution

- **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.
- **Arbitrary Injecting Point (Optional?)**
  - The distributed object SHOULD be injected at any autonomic node within the domain (or within a specific group [TBD])
- **Confliction Handling (Optional?)**
  - there is possibility that two nodes advertise the same object but with conflict content.
- **Verification of Distributed Information**
  - Information integrity verification
    - The receiving node SHOULD be able to verify whether the information has been modified.
  - Source authorization verification
    - The receiving node SHOULD be able to verify whether the distribution source has the right to distribute such information (the source might just exceed its authority)

Next Steps

- Solicit opinions on the distribution requirements

- Discuss solutions for the gaps

- A question to the Chairs:
  - It is a work within the scope of current charter
  - Could possibly add it as a new milestone?

Comments?

Thank you!

IETF94, Yokohama