Heartbeat Mechanism: Last Round

draft-ietf-dots-signal-channel-39

IETF#106 Singapore, November 2019

M. Boucadair, T. Reddy, J. Shallow

Draft Status

> De : Mirja Kuehlewind [mailto:ietf@kuehlewind.net]
> Envoyé : mardi 16 juillet 2019 17:41
> Objet : Re: [Dots] Behavior when keep-alives fail (RE: Mirja Kühlewind's
> Discuss on draft-ietf-dots-signal-channel-31: (with DISCUSS and COMMENT)

>
> Thanks for the updates. I think there is **one remaining issue on the use of**
> ping/heart-beats (see also my other message). However, I believe all other
> discuss points have been addressed now. Thanks for that!
>
> Mirja

The Issue

- The WG went for a design that leverages on base CoAP features:
  - CoAP Ping with a full control from the DOTS application
  - DOTS client behaves as CoAP client
  - DOTS server behaves as a CoAP server
- That design was challenged by Mirja (Transport AD)
  - We failed to progress since 05/2019 because of this pending issue.

The Alternative Approach

- The DOTS client behaves as CoAP ~~client~~ endpoint
- The DOTS server behaves as a CoAP ~~server~~ endpoint

```
NEW in -39:

   DOTS clients and servers behave as CoAP endpoints.  By default, a
   DOTS client (or server) behaves as a CoAP client (or server).
   Nevertheless, a DOTS client (or server) behaves as a CoAP server (or
   client) for specific operations such as DOTS heartbeat operations
   (Section 4.7).
```

The Alternative Approach

- ~~CoAP Ping with a full control from the DOTS application~~ Define DOTS-specific heartbeat messages

NEW in -39:

Operation	Operation Path	Details
Mitigation	/mitigate	Section 4.4
Session configuration	/config	Section 4.5
Heartbeat	**/hb**	**Section 4.7**

And

```
 +--rw dots-signal
        +--rw (message-type)?
            +--:(heartbeat)
               +--rw peer-hb-status                boolean
```

The Alternative Approach

- DOTS heartbeats are set as ~~Confirmable~~ Non-Confirmable

```
NEW in -39:
    The DOTS Heartbeat mechanism uses non-confirmable PUT requests
   (Figure 27) with an expected 2.04 (Changed) Response Code
   (Figure 28).  The PUT request used for DOTS heartbeat MUST NOT have a
   'cuid', 'cdid,' or 'mid' Uri-Path.  Such PUT requests MUST NOT be
   relayed by DOTS gateways.

        Header: PUT (Code=0.03)
        Uri-Path: ".well-known"
        Uri-Path: "dots"
        Uri-Path: "hb"
        Content-Format: "application/dots+cbor"

        {
          "ietf-dots-signal-channel:heartbeat": {
             "peer-hb-status": true;
           }
        }
```

The Alternative Approach

- CoAP uses PROBING_RATE to control the rate of sending when no response is received for a non-confirmable request
- DOTS controls this rate. It can be negotiated between the peer DOTS agents

```
NEW in -39:

 probing-rate:  The average data rate that must not be exceeded by
        a DOTS agent in sending to a peer DOTS agent that does not
        respond (referred to as PROBING_RATE parameter in CoAP).
```

The Alternative Approach

- ~~No interference between pacing of HBs and mitigation requests~~
- Add a guard to avoid interfering with mitigation requests
  - That would be blocked otherwise: delay signaling attacks to a DOTS server, which is undesirable.
  - Can be avoided by adequately tweaking the probing rate or the DOTS application dynamically adjusts the probing rate value (implementation-specific)

```
NEW in -39:

   Mitigation requests MUST NOT be delayed
   because of other congestion control checks.  Typically, mitigation
   requests must be sent without checks on probing rate (Section 4.7 of
   [RFC7252]).
```

The Alternative Approach

- CAUTION: probing-rate should be adequately set, otherwise side effects will be experienced (e.g., delay heartbeats)

```
NEW in -39:

      Given that the size of the heartbeat request can not exceed
      (heartbeat-interval * probing-rate) bytes, probing-rate should be
      set appropriately to avoid slowing down heartbeat exchanges.  For
      example, probing-rate may be set to 2 * ("size of encrypted DOTS
      heartbeat request"/heartbeat-interval) or (("size of encrypted
      DOTS heartbeat request" + "average size of an encrypted mitigation
      request")/heartbeat-interval).  Absent any explicit configuration
      or inability to dynamically adjust probing-rate values
      (Section 4.8.1 of [RFC7252]), DOTS agents use 5 bytes/second as a
      default probing-rate value.
```

The Alternative Approach

- No changes to how heartbeats are interpreted by peer DOTS agent

Summary

- We believe the new design addresses the pending “issue”