Constrained Application Protocol (CoAP) over Bundle Protocol (BP)

draft-gomez-core-coap-bp-01

Carles Gomez

Anna Calveras

Universitat Politècnica de Catalunya

Introduction

- CoAP:
  - Application-layer protocol designed for IoT environments
  - Typical IoT environment constraints:
    - Low energy (often leading to intermittent connectivity), high delays, low bandwidth, high error rates…
  - Features:
    - Lightweight operation, asynchronous message exchanges, flexibility, based on REST

Draft: main goal and status

- Main goal:
  - Specify how CoAP is carried over BP
  - Intended Status: Standards Track

- Updated draft version (-01)
  - Aims to address feedback received from the CoRE and DTN WGs

- Acknowledgments:
  - Christian Amsüss, Edward J. Birrane, Marc Blanchet, Carsten Bormann, Scott Burleigh, Joshua Deaton, Jaime Jiménez, Achim Kraus, Brian Sipos, Rick Taylor, Marco Tiloca, Rodney Van Meter, and Magnus Westerlund

5. Encapsulating bundle

- For CoAP over BP, the CoAP message MUST be carried as the block-type-specific data field of the Bundle Payload Block (block type 1) of an encapsulating bundle
- Lifetime of the encapsulating bundle MUST be:
  - EXCHANGE_LIFETIME (for CoAP CON messages)
  - NON_LIFETIME (for CoAP NON messages)
- CoAP message response (to a CoAP message):
  - Destination EID SHALL be identical to the Source Node ID of the bundle encapsulating the received CoAP message
  - And vice versa
- CoAP messages MAY be aggregated as payload of one bundle
  - Discussion at CoRE WG

6. CoAP parameter settings and related times

- Most of the CoAP parameters and related times are relevant for CON messages
- The protocols below BP may support reliability and congestion control
  - In that case, using NON messages might suffice to achieve a reasonable degree of reliability and congestion control
  - Congestion control considerations for NON message transmission would still apply (4.7 and 4.8 of RFC 7252):
    - NSTART is 1 by default, changing it requires RTT measurements
    - In absence of advanced CoAP congestion control, a CoAP endpoint does not exceed PROBING_RATE (1 byte/s)
    - A sender MAY transmit multiple copies of a NON message

7. Observe

- Which notification was sent by the server later than another notification SHOULD be based on the creation timestamps of the encapsulating bundles

- If timestamp info not available at the application layer, the time between the reception times of the two notifications MAY be used instead
  - By default, if the difference between two notifications is 128 seconds, the last one received is the last one sent
  - If 128 seconds is insufficient in a scenario, the duration needs to > MAX_LATENCY of the scenario (see Appendix A)

9. URI scheme (I/II)

- The URI scheme for CoAP over BP is "coap"
  - Recommended in [draft-ietf-core-transport-indication]
  - The "coap" scheme is defined in Section 6 of [RFC7252]
- Authority component of the URI: creation of two new reserved domains in the .arpa name space:
  - .dtn.arpa
    - If endpoint ID based on the "dtn" scheme:
      - » reg-name of the endpoint ID, followed by .dtn.arpa
  - .ipn.arpa
    - If endpoint ID based on the "ipn" scheme:
      - » node-nbr, followed by the nbr-delim (".") and the service-nbr of the endpoint ID, followed by .ipn.arpa

9. URI scheme (II/II)

- Examples, URI of the discovery resource
  - endpoint ID dtn://JupiterSensor
    - coap://JupiterSensor.dtn.arpa/.well-known/core
  - endpoint ID ipn:81.2
    - coap://81.2.ipn.arpa/.well-known/core

- TO-DO:
  - Request a Well-known Service Number for CoAP
  - ipn URI Scheme Well-known Service Numbers for BPv7 registry [draft-ietf-dtn-ipn-update]

10. Securing CoAP over BP (I/II)

- CoAP base spec (RFC 7252) defines a binding to DTLS
  - DTLS security modes:
    - NoSec, PreSharedKey, RawPublicKey, and Certificate
    - Mandatory to implement: NoSec, RawPublicKey
- Also, RFC 8613:
  - Object Security for Constrained RESTful Environments (OSCORE)
  - Optional, end-to-end application-layer payload protection
  - Shared security context, may be based on pre-shared materials
    - Avoids initial handshake and related performance penalty, critical in BP environments
    - Use of DTLS for CoAP over BP is NOT RECOMMENDED
  - Group OSCORE protocol used to secure CoAP group communication [I-D.ietf-core-oscore-groupcomm]

10. Securing CoAP over BP (II/II)

- BPSec [RFC 9172] provides security services for BP
  - Integrity and/or confidentiality for one or more blocks of a bundle

- OSCORE protects, with confidentiality and integrity:
  - CoAP message payload
  - One CoAP message header field

- Protection against replay attacks:
  - OSCORE uses by default an anti-replay sliding window, window size of 32 [RFC 8613]
  - If greater window size needed (e.g., due to high latency), it needs to be known by both sender and receiver at security context establishment

11. IANA considerations (I/II)

- Creation of two new reserved domains in the .arpa name space (following RFC 6761):
  - .dtn.arpa
  - .ipn.arpa
- Expectation for application software:
  - No DNS resolution is attempted
  - Instead, the prefix is processed into an endpoint ID
- Domain Name Reservation Considerations (RFC 6761):
  - **Users**: not expected to recognize those names as special
  - **Application software**: expected to pass those names on to their CoAP over BP implementation.
    - CoAP over BP implementations are expected to recognize those names as BP endpoint IDs and MUST NOT pass them on to DNS-based resolvers

11. IANA considerations (II/II)

- Domain Name Reservation Considerations (cont'd):
  - **Name resolution APIs and libraries**: MAY indicate that .dtn.arpa and .ipn.arpa names resolve to the endpoint ID encoded inside them
    - Otherwise, they SHOULD report them as NXDOMAIN
  - **Caching DNS Servers**: MAY recognize the special domains and report them as NXDOMAIN
    - Otherwise, they will cache the .arpa DNS servers' responses.
  - **Authoritative DNS Servers**: MAY recognize the special domains and report them as NXDOMAIN
  - **DNS Server Operators**: No impact on DNS server operators is expected
  - **DNS Registries/Registrars**: Any changes to .dtn.arpa or .ipn.arpa require updates to this document and the corresponding process through IANA

Message ID discussion summary

- CoAP Message ID size: 16 bits
- Message ID size proposed for CoAP over BP: 24 bits
  - Pros:
    - Avoid a limitation of the message rate
  - Cons:
    - 1 additional byte of header overhead
    - Increased memory requirements for endpoints to keep track of Message IDs used
      - » Sender: to retire Message IDs
      - » Receiver: duplicate detection

Thanks!
Questions? Comments?

Carles Gomez

Anna Calveras

Universitat Politècnica de Catalunya