ICN Research Group C. Gundogan
Internet-Draft TC. Schmidt
Intended status: Experimental HAW Hamburg
Expires: September 29, 2019 M. Waehlisch
link-lab & FU Berlin
M. Frey
F. Shzu-Juraschek
Safety IO
J. Pfender
VUW
March 28, 2019

Quality of Service for ICN in the IoT
draft-gundogan-icnrg-iotqos-00

Abstract

This document describes manageable resources in ICN IoT deployments and a lightweight traffic classification method for mapping priorities to resources. Management methods are further derived for controlling latency and reliability of traffic flows in constrained environments.

Table of Contents

1. Introduction

The performance of networked systems is largely determined by the resources available for forwarding messages between components. In addition to link capacities and buffer queues, Information-centric Networks rely on additional resources that shape its overall performance, namely Pending Interest Table space, and caching capacity.

Typical IoT deployments add tight resource constraints to this picture [RFC7228]: Nodes have processing and memory limitations, the underlying link layer technologies are lossy and restricted in bandwidth. Particularly in multi-hop networks, such constraints affect the overall performance, create bottlenecks, but may lead to cascading packet loss or energy depletion when PIT resources are independently evicted and forwarding states decorrelate [DECORRELATION]. Overprovisioning to counter performance flaws is infeasible for many IoT scenarios as it inflicts with use cases and increases deployment costs. Quality of Service (QoS) is a method to enhance overall performance by redistributing resources to a subset of messages, and - in the constrained IoT use case - to coordinate operations under resource scarcity.

IoT applications follow various use cases, of which different QoS requirements can be derived. While periodic sensor readings often comply with unmanaged performance, industrial control messaging or security alerts require (very) low latency, and safety-critical environmental recording or network management need (highly) reliable network services. Both quality levels can only be assured by appropriate resource reservations.

In order to achieve a QoS-aware information-centric IoT deployment, this document describes manageable resources in Section 3, defines a flow classification method in Section 4, and specifies priorities and their mappings in Section 5.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119]. The use of the term, "silently ignore" is not defined in RFC 2119. However, the term is used in this document and can be similarly construed.

This document uses the terminology of [RFC7476], [RFC7927], and [RFC7945] for ICN entities.

The following terms are used in the document and defined as follows:

Traffic Flow A traffic flow is a sequence of messages (Interest and data) that belong to one specific communication context. Due to in-network caching, ICN flows may be delocalized. A flow may also relate to several requesters in the presence of Interest aggregation.

3. Manageable Resources in the IoT

The following resources contribute to the overall network performance in Information-Centric IoT Networking and need management for QoS control.

3.1. Link Layer

The link layer manages access to the media and provides space to buffer packets. Low latency applications require that requests are prioritized compared to regular priority data. Based on the request response pattern of ICN, link layer resources can be preallocated for data packets.

3.2. Pending Interest Table

The Pending Interest Table (PIT) stores open requests at each hop. PIT resources are allocated when requests are forwarded, and they are released on returning responses.

Placement and replacement strategies of PIT entries directly influence the latency and reliability properties of traffic flows and thus should consider prioritization schemes. If the PIT is not saturated new PIT entries can be added. If the PIT is saturated, requests with higher priority should replace requests with lower priority to prevent higher latencies due to retransmissions.

3.3. Content Store

Content stores (CS) enable transparent in-network caching and thus improve the transport in wireless and lossy environments by reducing hop traversals for content requests [NDN-EXP].

Placement and replacement strategies of data in content stores can affect the latency and reliability properties of traffic flows. The latency can be reduced by placing data closer to the consumers. Reliability can be improved by replicating data in multiple content stores to be resilient to node failures.

4. Traffic Flow Classification

This document defines a traffic flow classification mechanism that aggregates names into equivalence classes in order to apply resource allocation decisions on messages of particular traffic flows.

A traffic class is a name prefix and each device maintains a list of valid classes. The actual distribution of traffic classes is out of scope of this document. The classes for request and response messages are derived by performing a longest prefix match (LPM) with the list of valid traffic classes and the Name TLV of the message. Examples are given in Figure 1.

```
list =
["/org", "/org /Hamburg", "/org /Berlin", "/org /Berlin /sensor" ]

LPM("/com"                     ,list) = ""
LPM("/org /Germany"            ,list) = "/org"
LPM("/org /Hamburg"            ,list) = "/org /Hamburg"
LPM("/org /Berlin /sensor /temp",list) = "/org /Berlin /sensor"
```

Figure 1: Example traffic flow class matches.

The empty traffic class "" is the default class for messages that do not match any valid traffic classes in the class list.

5. Priority Handling

We define two priority levels to set the priorities for traffic flows in regards to latency and reliability.

- Latency:
  - EXPEDITED
  - REGULAR
- Reliability:
  - RELIABLE
  - REGULAR

Each list entry of the traffic class list from Section 4 has an associated priority tuple which distinctly specifies priority levels for the resources in Section 3. The tuple is of the following form:

```
priority tuple = < LATENCY_PRIORITY, RELIABILITY_PRIORITY >
```

Figure 2: Schema of the priority tuple.

5.1. Link Layer

As described above, the link layer provides space to buffer outgoing packets. For the two latency priorities, this space can be allocated into the following two queues:

- EXPEDITED_FORWARDING_QUEUE
- REGULAR_FORWARDING_QUEUE

Packets will be appended to the queue corresponding to their priority level.

5.2. Pending Interest Table

In unsatured PITs, requests are added as new entries regardless of the priority level. In saturated PITs, EXPEDITED traffic replaces PIT entries of REGULAR traffic. If all entries in a saturated PIT are of a higher priority than the incoming request, then we RECOMMEND to drop the incoming request. If a saturated PIT contains entries of

the same priority as the incoming request, we RECOMMEND to drop the incoming request to avoid cancelling active but incomplete ICN operations.

5.3. Content Store

Nodes MAY implement a caching decision strategy instead of always caching all incoming content objects [ICN-CACHING]. If they do, the caching decision strategy MUST take the content object priority into account, such that lower priority content is not cached if the cache is saturated with higher priority content.

In unsaturated content stores, all content objects are passed to the cache decision strategy.

In saturated content stores, reliable traffic flows MUST be passed to the cache replacement strategy. Content objects with regular reliability requirements MUST be evicted first to make room for higher reliability content objects. Traffic flows with regular latency and regular reliability requirements MUST be passed to the cache replacement strategy. The cache replacement strategy MUST NOT evict content objects of higher reliability. Expedited traffic flows with regular reliability MUST be passed to the cache replacement strategy. Content objects with regular latency and regular reliability requirements MUST be evicted first, if an open PIT state is available. Otherwise, if no PIT state is available, then the cache replacement strategy MAY replace content objects of expedited or regular latency requirements and with regular reliability requirements.

6. Security Considerations

TODO

7. IANA Considerations

TODO

8. Informative References

[DECORRELATION]
Waehlisch, M., Schmidt, TC., and M. Vahlenkamp, "Backscatter from the Data Plane - Threats to Stability and Security in Information-Centric Network Infrastructure", Computer Networks Vol 57, No. 16, pp. 3192-3206, November 2013.

[I-D.moiseenko-icnrg-flowclass]
Moiseenko, I. and D. Oran, "Flow Classification in Information Centric Networking", draft-moiseenko-icnrg-flowclass-03 (work in progress), January 2019.

[ICN-CACHING]
Chai, W., He, D., Psaras, I., and G. Pavlou, "Cache 'Less for More' in Information-Centric Networks (Extended Version)", Computer Communications 36, 7 (2013) pp. 758-770, February 2013, <http://dx.doi.org/>.

[NDN-EXP] Gundogan, C., Kietzmann, P., Lenders, M., Petersen, H., Schmidt, TC., and M. Waehlisch, "NDN, CoAP, and MQTT: A Comparative Measurement Study in the IoT", Proc. of 5th ACM Conf. on Information-Centric Networking (ICN-2018) ACM DL, pp. , September 2018, <http://dx.doi.org/>.

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

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/info/rfc7228>.

[RFC7476] Pentikousis, K., Ed., Ohlman, B., Corujo, D., Boggia, G., Tyson, G., Davies, E., Molinaro, A., and S. Eum, "Information-Centric Networking: Baseline Scenarios", RFC 7476, DOI 10.17487/RFC7476, March 2015, <https://www.rfc-editor.org/info/rfc7476>.

[RFC7927] Kutscher, D., Ed., Eum, S., Pentikousis, K., Psaras, I., Corujo, D., Saucez, D., Schmidt, T., and M. Waehlisch, "Information-Centric Networking (ICN) Research Challenges", RFC 7927, DOI 10.17487/RFC7927, July 2016, <https://www.rfc-editor.org/info/rfc7927>.

[RFC7945] Pentikousis, K., Ed., Ohlman, B., Davies, E., Spirou, S., and G. Boggia, "Information-Centric Networking: Evaluation and Security Considerations", RFC 7945, DOI 10.17487/RFC7945, September 2016, <https://www.rfc-editor.org/info/rfc7945>.

Acknowledgments

This work was stimulated by fruitful discussions in the ICNRG research group. We would like to thank all active members for constructive thoughts and feedback. In particular, the authors would like to thank Ilya Moiseenko and Dave Oran for their work provided in [I-D.moiseenko-icnrg-flowclass]. This work was supported in part by the German Federal Ministry of Research and Education within the I3 project.

Authors' Addresses

Cenk Gundogan
HAW Hamburg
Berliner Tor 7
Hamburg D-20099
Germany

Phone: +4940428758067
EMail: cenk.guendogan@haw-hamburg.de
URI: http://inet.haw-hamburg.de/members/cenk-gundogan

Thomas C. Schmidt
HAW Hamburg
Berliner Tor 7
Hamburg D-20099
Germany

EMail: t.schmidt@haw-hamburg.de
URI: http://inet.haw-hamburg.de/members/schmidt

Matthias Waehlisch
link-lab & FU Berlin
Hoenower Str. 35
Berlin D-10318
Germany

EMail: mw@link-lab.net
URI: http://www.inf.fu-berlin.de/~waehl

Michael Frey
Safety IO
Franz-Ehrlich-Strasse 9
Berlin D-12489
Germany

EMail: michael.frey@safetyio.com

Felix Shzu-Juraschek
Safety IO
Franz-Ehrlich-Strasse 9
Berlin D-12489
Germany

EMail: felix.juraschek@safetyio.com

Jakob Pfender
Victoria University of Wellington
Kelburn Parade
Wellington NZ-6012
New Zealand

EMail: jpfender@ecs.vuw.ac.nz
URI: https://ecs.victoria.ac.nz/Main/GradJakobPfender