Workgroup: ROLL Working Group
Internet-Draft:
draft-ietf-roll-enrollment-priority-09
Published: 16 May 2023
Intended Status: Standards Track
Expires: 17 November 2023
Authors: M. Richardson
Sandelman Software Works
R. A. Jadhav
Huawei Tech
P. Thubert
Cisco Systems
H. She
Cisco Systems
K. Iwanicki

Controlling Secure Network Enrollment in RPL networks

Abstract

[RFC9032] defines a method by which a potential [RFC9031] enrollment proxy can announce itself as a available for new Pledges to enroll on a network. The announcement includes a priority for enrollment. This document provides a mechanism by which a RPL DODAG root can disable enrollment announcements, or adjust the base priority for enrollment operations.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 17 November 2023.

Table of Contents

1. Introduction

[RFC7554] describes the use of the time-slotted channel hopping (TSCH) mode of [ieee802154]. [RFC9031] and [RFC9032] describe mechanisms by which a new node (the "pledge") can use a friendly router as a Join Proxy. [RFC9032] describes an extension to the 802.15.4 Enhanced Beacon that is used by a Join Proxy to announce its existence such that Pledges can find them.

1.1. Motivation and Overview

It has become clear that not every routing member of the mesh ought to announce itself as a *Join Proxy*. There are a variety of local reasons by which a 6LR might not want to provide the *Join Proxy* function. They include available battery power, already committed network bandwidth, and total available memory available for Neighbor Cache Entry (NCE) slots. An NCE entry is needed in order to maintain communication with the pledge.

There are other situations where the operator of the network would like to selectively enable or disable the enrollment process in a particular DODAG.

As the enrollment process involves permitting unencrypted traffic into the best effort part of a network, it would be better to have the enrollment process off when no new nodes are expected.

This document describes a RPL DIO option that can be used to set a minimum enrollment priority. The minimum priority expresses the (lack of) willingness by the RPL DODAG globally to accept new joins.

It may derive from multiple constraining factors, e.g., the size of the DODAG, the occupancy of the bandwidth at the Root, the memory capacity at the DODAG Root, or an administrative decision.

Each potential *Join Proxy* would utilize this value as a base on which to add values relating to local conditions such as its Rank and number of pending joins, which would degrade even further the willingness to take more joins.

When a RPL domain is composed of multiple DODAGs, nodes at the edge of 2 DODAGs may not only join either DODAG but also move from one to the other in order to keep their relative sizes balanced. For this, the approximate knowledge of size of the DODAG is an essential metric. Depending on the network policy, the size of the DODAG may or may not affect the minimum enrollment priority. It would be limiting its value to enforce that one is proportional to the other. The current size of the DODAG is therefore also advertised in the new option.

As explained in [RFC9032], higher values decrease the likelihood of an unenrolled node sending enrollment traffic via this path.

A network operator can set this value to the maximum value allowed, effectively disabling all new enrollment traffic.

Updates to the option propagate through the network according to the trickle algorithm. The contents of the option are generated at the DODAG Root and do not change at any hop. If the contents represent an update that is considered important (e.g., quickly disabling any enrollments), the option can trigger trickle timer resets at the nodes to speed up its propagation.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The term (1)"Join" has been used in documents like [RFC9031] to denote the activity of a new node authenticating itself to the network in order to obtain authorization to become a member of the network.

In the context of the [RFC6550] RPL protocol, the term (2)"Join" has an alternative meaning: that of a node (already authenticating to the network, and already authorized to be a member of the network), deciding which part of the RPL DODAG to attach to. This term "Join" has to do with preferred parent selection processes.

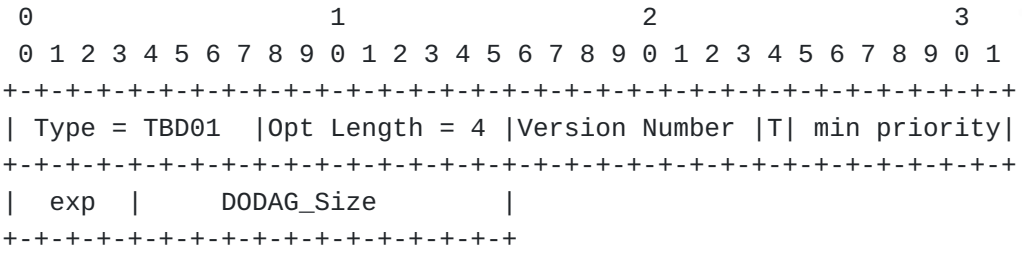
In order to avoid the ambiguity of this term, this document refers to the process (1)"Join" as enrollment, leaving the term "Join" to mean (2)"Join". The term "onboarding" (or IoT Onboarding) is increasingly used to describe what was called enrollment in other documents. However, the term *Join Proxy* is retained with its meaning from [RFC9031].

3. Protocol Definition

This document uses the extensions mechanism designed into [RFC6550]. No mechanism is needed to enable it.

3.1. Option Format

The following option is defined for transmission in DIOs issued by the DODAG root to be propagated within the DODAG.



Type to be assigned by IANA.

Version Number an 8-bit unsigned integer set by the DODAG root and denoting the version number of the contents of the option. The

version number is interpreted as a lollipop counter (see Section 7.2 of [RFC6550]).

T a bit indicating whether the particular version of the option is important in that adopting its contents should trigger a trickle timer reset at the node.

min priority a 7-bit field providing a base value for the Enhanced Beacon Join priority. A value of 0x7f (127) disables the *Join Proxy* function entirely.

exp a 4-bit unsigned integer indicating the power of 2 that defines the unit of the DODAG Size, such that (unit=2^exp).

DODAG_Size a 12-bit unsigned integer expressing the size of the DODAG in units that depend on the exp field. The size of the DODAG is computed as (DAG_Size*2^exp).

The size of the DODAG is measured by the Root based one the DAO activity. It represents a number of routes not a number of nodes, and can only be used to infer a load in a homogeneous network where each node advertises the same number of addresses and generates roughly the same amount of traffic. The size may slightly change between a DIO and the next, so the value transmitted MUST be considered as an approximation.

Future work like [I-D.ietf-roll-capabilities] will enable collection of capabilities such as this one in reports to the DODAG root.

3.2. Option Processing

The contents of the option MUST be generated by the DODAG Root. A 6LR MUST NOT change them when propagating the option.

Whenever the DODAG root changes the values of min priority or DODAG_Size in the option, it MUST also increment the value of Version Number. Moreover, if the change is considered important (i.e., it is expected to propagate in the DODAG quickly), the DODAG Root SHOULD also set the T bit to 1; otherwise, it MUST set the bit to 0.

Upon receiving the option, a 6LR first checks the value of the Version Number field in the option, *vr*, versus the value of the Version Number it has last adopted locally, *vl*.

*If *vl* is greater than *vr* (in the lollipop counter order), then the 6LR MUST ignore the received option.

*Otherwise, the 6LR MUST adopt the contents of the option (i.e., the values of Version Number, min priority, DODAG_Size, and the T

bit) as its local ones. Moreover, if *vl* was smaller than *vr* (in the lollipop counter order) and the T bit in the received option was set, then the 6LR MUST reset its DIO trickle timer.

A 6LR which would otherwise be willing to act as a *Join Proxy*, will examine the locally adopted value of min priority, and to that number, add any additional local consideration (such as upstream congestion, number of NCE slots available, etc.).

The maximum resulting value any 6LR can obtain this way is 0x7f.

The resulting priority, if less than 0x7f, should enable the *Join Proxy* function.

3.3. Upwards Compatibility

A 6LR which did not support this option would not act on it or propagate it in its DIO messages. In effect, the 6LR's children and grandchildren nodes could not receive any telemetry via that path. Therefore, 6LRs that support this option but do not receive it via any path SHOULD assume a default value of 0x40 as their base value for the Enhanced Beacon Join Priority.

A 6LR downstream of a 6LR where there was an interruption in the telemetry could err in two directions:

* if the value implied by the base value of 0x40 was too low, then a 6LR might continue to attract enrollment traffic when none should have been collected. This is a stressor for the network, but this would also be what would occur without this option at all.

* if the value implied by the base value of 0x40 was too high, then a 6LR might deflect enrollment traffic to other parts of the DODAG tree, possibly refusing any enrollment traffic at all. In order for this to happen, some significant congestion must be seen in the sub-tree where the implied 0x40 was introduced.

The 0x40 is only the half-way point, so if such an amount of congestion was present, then this sub-tree of the DODAG simply winds up being more cautious than it needed to be.

It is possible that the temporal alternation of the above two situations might introduce cycles of accepting and then rejecting enrollment traffic. This is something an operator should consider if when they incrementally deploy this option to an existing LLN. In addition, an operator would be unable to turn off enrollment traffic by sending a maximum value enrollment priority to the sub-tree. This situation is unfortunate, but without this option, the the situation

would occur all over the DODAG, rather than just in the sub-tree where the option was omitted.

4. Security Considerations

As per [RFC7416], RPL control frames either run over a secured layer 2, or use the [RFC6550] Secure DIO methods. This option can be placed into either a "clear" (layer-2 secured) DIO, or a layer-3 Secure DIO. As such this option will have both integrity and confidentiality mechanisms applied to it.

A malicious node (that was part of the RPL control plane) could see these options and could, based upon the observed minimal enrollment priority signal a confederate that it was a good time to send malicious join traffic.

Such as a malicious node, being already part of the RPL control plane, could also send DIOs with a different minimal enrollment priority which would cause downstream mesh routers to change their *Join Proxy* behavior.

Lower minimal priorities would cause downstream nodes to accept more pledges than the network was expecting, and higher minimal priorities cause the enrollment process to stall.

The use of layer-2 or layer-3 security for RPL control messages prevents the above two attacks, by preventing malicious nodes from becoming part of the control plane. A node that is attacked and has malware placed on it creates vulnerabilities in the same way such an attack on any node involved in Internet routing protocol does. The rekeying provisions of [RFC9031] exist to permit an operator to remove such nodes from the network easily.

5. Privacy Considerations

There are no new privacy issues caused by this extension.

6. IANA Considerations

Allocate a new number TBD01 from Registry RPL Control Message Options. This entry should be called Minimum Enrollment Priority.

7. Acknowledgements

This has been reviewed by Konrad Iwanicki and Thomas Watteyne.

8. References

8.1. Normative References

[ieee802154] IEEE standard for Information Technology, "IEEE Std. 802.15.4, Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks", n.d., <http://standards.ieee.org/findstds/standard/802.15.4-2015.html>.

[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>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <https://www.rfc-editor.org/info/rfc6550>.

[RFC7416] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and M. Richardson, Ed., "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)", RFC 7416, DOI 10.17487/RFC7416, January 2015, <https://www.rfc-editor.org/info/rfc7416>.

[RFC7554] Watteyne, T., Ed., Palattella, M., and L. Grieco, "Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement", RFC 7554, DOI 10.17487/RFC7554, May 2015, <https://www.rfc-editor.org/info/rfc7554>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9031] Vučinić, M., Ed., Simon, J., Pister, K., and M. Richardson, "Constrained Join Protocol (CoJP) for 6TiSCH", RFC 9031, DOI 10.17487/RFC9031, May 2021, <https://www.rfc-editor.org/info/rfc9031>.

[RFC9032] Dujovne, D., Ed. and M. Richardson, "Encapsulation of 6TiSCH Join and Enrollment Information Elements", RFC 9032, DOI 10.17487/RFC9032, May 2021, <https://www.rfc-editor.org/info/rfc9032>.

8.2. Informative References

[I-D.ietf-roll-capabilities] Jadhav, R., Thubert, P., Richardson, M., and R. N. Sahoo, "RPL Capabilities", Work in

Progress, Internet-Draft, draft-ietf-roll-capabilities-09, 9 November 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-roll-capabilities-09>.

Appendix A. Change history

version 00.

Authors' Addresses

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

Rahul Arvind Jadhav
Huawei Tech

Email: rahul.ietf@gmail.com

Pascal Thubert
Cisco Systems

Email: pthubert@cisco.com

Huimin She
Cisco Systems

Email: hushe@cisco.com

Konrad Iwanicki

Email: iwanicki@mimuw.edu.pl