Enabling secure network enrollment in RPL networks
draft-ietf-roll-enrollment-priority-01

Abstract

   [I-D.ietf-6tisch-enrollment-enhanced-beacon] defines a method by
   which a potential [I-D.ietf-6tisch-minimal-security] join proxy can
   announce itself as a available for new Pledges to Join a network.
   The announcement includes a priority for join. This document
   provides a mechanism by which a RPL DODAG root can disable join
   announcements, or adjust the base priority for join operation.

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 September 20, 2020.

Table of Contents

1. Introduction

[RFC7554] describes the use of the time-slotted channel hopping
(TSCH) mode of [ieee802154]. [I-D.ietf-6tisch-minimal-security] and
[I-D.ietf-6tisch-dtsecurity-secure-join] describe mechanisms by which
a new node (the "pledge") can use a friendly router as a Join Proxy.
[I-D.ietf-6tisch-enrollment-enhanced-beacon] 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.

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 also total available memory available for Join
proxy neighbor cache slots.

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

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

A network operator might also be able to recognize when certain parts
of the network are overloaded and can not accomodate additional join
traffic, and it would like to adjust the join priority among all
nodes in the subtree of a congested link.

This document describes an RPL DIO option that can be used to
announce a minimum join priority. Each potential Join Proxy would
this value as a base on which to add (decreasing likely hood of
attracting traffic) values relating to local conditions.

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

1.1. 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.

2. Protocol Definition

The following option is defined to transmission in the DIO issued by
the DODAG root. It may also be added by a router on part of the sub-
tree as a result of some (out of scope for this document) management
function.

6LRs that see this DIO Option SHOULD increment the minimum priority
if they observe congestion on the channel used for join traffic.
(TODO: how much? Do we need to standardize this?)

A 6LR which would otherwise be willing to act as a Join Proxy, will
examine the minimum priority field, and to that number, add any
additional local consideration (such as upstream congestion). The
resulting priority, if less than 0x7f should enable the Join Proxy
function.

```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type = TBD01|Opt Length = 1|R| min. priority  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

R a reserved bit that SHOULD be set to 0 by senders, and MUST be
   ignored by receivers. The reserved bit SHOULD be copied to
   options created.

3. 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 join
   priority signal a confederate that it was a good time to send
   malicious join traffic.

   A malicious node (that was part of the RPL control plane) could also
   send DIOs with a different minimal join priority which would cause
   downstream mesh routers to change their Join Proxy behaviour. Lower
   minimal priorities would cause downstream nodes to accept more
   pledges than the network was expecting, and higher minimal priorities
   cause the join process to stall.

   The use of layer-2 or layer-3 security for RPL control messages
   prevents the above two attacks.

4. Privacy Considerations

   There are no new privacy issues caused by this extension.

5. IANA Considerations

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

6. Acknowledgements

   This has been reviewed by Pascal Thubert and Thomas Wattenye.

7. References

7.1. Normative References

   [I-D.ietf-6tisch-enrollment-enhanced-beacon]
             Dujovne, D. and M. Richardson, "IEEE 802.15.4 Information
             Element encapsulation of 6TiSCH Join and Enrollment
             Information", draft-ietf-6tisch-enrollment-enhanced-
             beacon-14 (work in progress), February 2020.

[I-D.ietf-6tisch-minimal-security]
          Vucinic, M., Simon, J., Pister, K., and M. Richardson,
          "Constrained Join Protocol (CoJP) for 6TiSCH", draft-ietf-
          6tisch-minimal-security-15 (work in progress), December
          2019.

[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>.

7.2. Informative References

[I-D.ietf-6tisch-architecture]
          Thubert, P., "An Architecture for IPv6 over the TSCH mode
          of IEEE 802.15.4", draft-ietf-6tisch-architecture-28 (work
          in progress), October 2019.

[I-D.ietf-6tisch-dtsecurity-secure-join]
          Richardson, M., "6tisch Secure Join protocol", draft-ietf-
          6tisch-dtsecurity-secure-join-01 (work in progress),
          February 2017.

[I-D.ietf-6tisch-terminology]
          Palattella, M., Thubert, P., Watteyne, T., and Q. Wang,
          "Terms Used in IPv6 over the TSCH mode of IEEE 802.15.4e",
          draft-ietf-6tisch-terminology-10 (work in progress), March
          2018.

[RFC8137] Kivinen, T. and P. Kinney, "IEEE 802.15.4 Information
          Element for the IETF", RFC 8137, DOI 10.17487/RFC8137, May
          2017, <https://www.rfc-editor.org/info/rfc8137>.

[RFC8366] Watsen, K., Richardson, M., Pritikin, M., and T. Eckert,
          "A Voucher Artifact for Bootstrapping Protocols",
          RFC 8366, DOI 10.17487/RFC8366, May 2018,
          <https://www.rfc-editor.org/info/rfc8366>.

Appendix A. Change history

version 00.

Author's Address

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca