Workgroup: 6tisch Working Group
Internet-Draft:
draft-ietf-6tisch-enrollment-enhanced-
beacon-11
Published: 14 February 2020
Intended Status: Standards Track
Expires: 17 August 2020
Authors: D. Dujovne
Universidad Diego Portales
M. Richardson
Sandelman Software Works

IEEE 802.15.4 Information Element encapsulation of 6TiSCH Join and Enrollment Information

Abstract

In TSCH mode of IEEE STD 802.15.4, opportunities for broadcasts are limited to specific times and specific channels. Nodes in a TSCH network typically frequently transmit Enhanced Beacon (EB) frames to announce the presence of the network. This document provides a mechanism by which information critical for new nodes (pledges) and long sleeping nodes may be carried within the Enhanced Beacon.

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 August 2020.

Copyright Notice

Table of Contents

1. Introduction

[RFC7554] describes the use of the time-slotted channel hopping (TSCH) mode of [ieee802154]. As further detailed in [RFC8180], an Enhanced Beacon (EB) is transmitted during a slot designated as a broadcast slot.

1.1. Use of BCP 14 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.

Other terminology can be found in [I-D.ietf-6tisch-architecture] in section 2.1.

1.2. Layer-2 Synchronization

As explained in section 6 of [RFC8180], the Enhanced Beacon (EB) has a number of purposes: synchronization of ASN and Join Metric, carrying timeslot template identifier, carrying the channel hopping sequence identifier, and indicating the TSCH SlotFrame.

The EB is used by nodes already part of a TSCH network to announce their existence. Receiving an EB allows a Joining Node (pledge) to learn about the network and synchronize to it. The EB may also be used as a means for a node already part of the network to re-synchronize [RFC7554].

There are a limited number of timeslots designated as broadcast slots by each router in the network. Considering 10ms slots and a slot-frame length of 100, these slots are rare and could result in only 1 slot per second for broadcasts, which needs to be used for the beacon. Additional broadcasts for Router Advertisements, or Neighbor Discovery could even more scarce.

1.3. Layer-3 synchronization: IPv6 Router Solicitations and Advertisements

At layer 3, [RFC4861] defines a mechanism by which nodes learn about routers by receiving multicast Router Advertisements (RA). If no RA is received within a set time, then a Router Solicitation (RS) may be transmitted as a multicast, to which an RA will be received, usually unicast.

Although [RFC6775] reduces the amount of multicast necessary to do address resolution via Neighbor Solicitation (NS) messages, it still requires multicast of either RAs or RS. This is an expensive operation for two reasons: First, there are few multicast timeslots for unsolicited RAs; and second, if a pledge node does not receive an RA, and decides to transmit an RS, a broadcast aloha slot is consumed with unencrypted traffic. In this case, a unicast RS may be transmitted in response.

This is a particularly acute issue for the join process for the following reasons:

1. Use of a multicast slot by even a non-malicious unauthenticated node for a Router Solicitation (RS) may overwhelm that time slot.

2. It may require many seconds of on-time before a new pledge receives a Router Advertisement (RA) that it can use.

3. A new pledge may have to receive many Enhanced Beacons (EB) before it can pick an appropriate network and/or closest Join

Assistant to attach to. If it must remain in the receive state for an RA as well as find the Enhanced Beacon (EB), then the process may take a very long time.

This document defines a new IETF IE subtype to provide join and enrollment information to prospective pledges in a more efficient way.

2. Protocol Definition

[RFC8137] creates a registry for new IETF IE subtypes. This document allocates a new subtype.

The new IE subtype structure is as follows. As explained in [RFC8137] the length of the Sub-Type Content can be calculated from the container, so no length information is necessary.

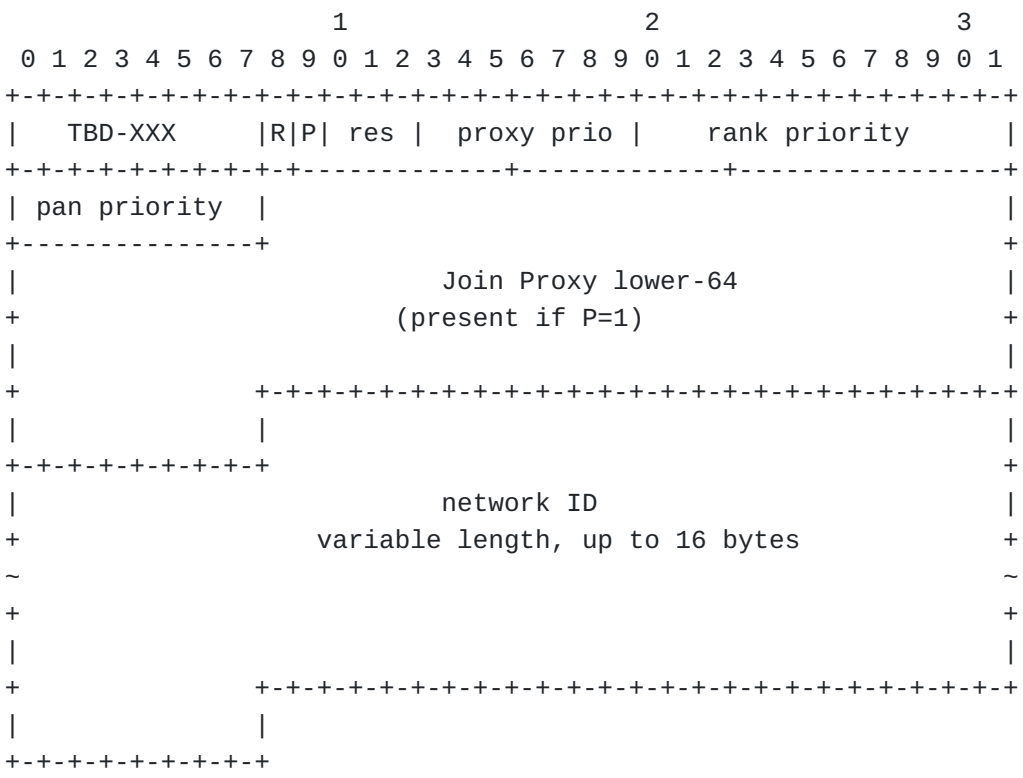

Figure 1: IE subtype structure

R: The Router Advertisement R-flag is set if the sending node will act as a Router for host-only nodes that need addressing via unicast Router Solicitation messages.

In most cases, every node sending a beacon will set this flag, and in a typical mesh, this will be every single node. When this bit is not set, it indicates that this node may be under

provisioned, or may have no additional slots for additional nodes. This could make this node more interesting to an attacker.

P: If the Proxy Address P-flag is set, then the Join Proxy lower-64 bit field is present. Otherwise, it is not provided.

This bit only indicates if another part of the structure is present, and has little security or privacy impact.

proxy priority (proxy prio): This field indicates the willingness of the sender to act as join proxy. Lower value indicates greater willingness to act as a Join Proxy as described in [I-D.ietf-6tisch-minimal-security]. Values range 0x00 (most willing) to 0x7e (least willing). A priority of 0x7f indicates that the announcer should never be considered as a viable enrollment proxy. Only unenrolled pledges look at this value.

Lower values in this field indicate that the transmitter may have more capacity to handle unencrypted traffic. A higher value may indicate that the transmitter is low on neighbor cache entries, or other resources.

rank priority: The rank "priority" is set by the 6LR which sent the beacon and is an indication of how willing this 6LR is to serve as an RPL parent within a particular network ID. This is a local value to be determined in other work. It might be calculated from RPL rank, and it may include some modifications based upon current number of children, or number of neighbor cache entries available. This value MUST be ignored by pledges, it is for enrolled devices only. Lower values are better.

An attacker can use this value to determine which nodes are potentially more interesting. Nodes which are less willing to be parents likely have more traffic, and an attacker could use this information to determine which nodes would be more interesting to attack or disrupt.

pan priority: The pan priority is a value set by the DODAG root to indicate the relative priority of this LLN compared to those with different PANIDs. This value may be used as part of the enrollment priority, but typically is used by devices which have already enrolled, and need to determine which PAN to pick. Unenrolled pledges MAY consider this value when selecting a PAN to join. Enrolled devices MAY consider this value when looking for an eligible parent device.

An attacker can use this value, along with the observed PANID in the Beacon to determine which PANIDs have more network resources, and may have more interesting traffic.

Join Proxy lower-64:

If the P bit is set, then 64 bits (8 bytes) of address are present. This field provides the suffix (IID) of the Link-Local address of the Join Proxy. The associated prefix is well-known as fe80::/64. If this field is not present, then IID is derived from the layer-2 address of the sender.

This field communicates a lower-64 bits that should be used for this nodes' layer-3 address, if it should not be derived from the layer-2 address. Communication with the Join Proxy occurs in the clear, this field avoids the need for an additional service discovery process for the case where the L3 address is not derived from the L2 address. An attacker will see both L2 and L3 addresses, so this field provides no new information.

network ID: This is a variable length field, up to 16-bytes in size that uniquely identifies this network, potentially among many networks that are operating in the same frequencies in overlapping physical space. The length of this field can be calculated as being whatever is left in the Information Element.

In a 6tisch network, where RPL [RFC6550] is used as the mesh routing protocol, the network ID can be constructed from a SHA256 hash of the prefix (/64) of the network. That is just a suggestion for a default value. In some LLNs where multiple PANIDs may lead to the same management device (the JRC), then a common value that is the same across all PANs MUST be configured.

If the the network ID is derived as suggested, then it will an opaque, seemingly random value, and will reveal nothing in of itself. An attacker can match this value across many transmissions to map the extent of a network beyond what the PANID might already provide.

3. Security Considerations

All of the contents of this Information Element are transmitted in the clear. The content of the Enhanced Beacon is not encrypted. This is a restriction in the cryptographic architecture of the 802.15.4 mechanism. In order to decrypt or do integrity checking of layer-2 frames in TSCH, the TSCH Absolute Slot Number (ASN) is needed. The Enhanced Beacon provides the ASN to new (and long-sleeping) nodes.

The Enhanced Beacon is authenticated at the layer-2 level using 802.15.4 mechanisms using the network-wide keying material. Nodes which are enrolled will have the network-wide keying material and can validate the beacon.

Pledges which have not yet enrolled are unable to authenticate the beacons, and will be forced to temporarily take the contents on

faith. After enrollment, a newly enrolled node will be able to return to the beacon and validate it.

In addition to the enrollment and join information described in this document, the Enhanced Beacon contains a description of the TSCH schedule to be used by the transmitter of this packet. The schedule can provide an attacker with a list of channels and frequencies on which communication will occur. Knowledge of this can help an attacker to more efficiently jam communications, although there is future work being considered to make some of the schedule less visible. Encrypting the schedule does not prevent an attacker from jamming, but rather increases the energy cost of doing that jamming.

4. Privacy Considerations

The use of a network ID may reveal information about the network. The use of a SHA256 hash of the DODAGID, rather than using the DODAGID (which is usually derived from the LLN prefix) directly provides some privacy for the the addresses used within the network. The DODAGID is usually the IPv6 address of the root of the RPL mesh.

An interloper with a radio sniffer would be able to use the network ID to map out the extent of the mesh network.

5. IANA Considerations

Allocate a new number TBD-XXX from Registry IETF Information Element (IE) Sub-type ID, as defined by [RFC8137]. This entry should be called 6tisch-Join-Info, and should refer to this document.

6. Acknowledgements

Thomas Watteyne provided extensive editorial comments on the document. Carles Gomez Montenegro generated a detailed review of the document at WGLC. Tim Evens provided a number of useful editorial suggestions.

7. References

7.1. Normative References

[BCP14] 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>.

[I-D.ietf-6tisch-minimal-security] Vucinic, M., Simon, J., Pister, K., and M. Richardson, "Constrained Join Protocol (CoJP) for 6TiSCH", Work in Progress, Internet-Draft, draft-ietf-6tisch-minimal-security-15, 10 December 2019, <http://www.ietf.org/

internet-drafts/draft-ietf-6tisch-minimal-security-15.txt>.

[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", 2015, <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>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/info/rfc6775>.

[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>.

[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", Work in Progress, Internet-Draft, draft-ietf-6tisch-architecture-28, 29 October 2019, <http://www.ietf.org/internet-drafts/draft-ietf-6tisch-architecture-28.txt>.

[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>.

[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>.

[RFC8180] Vilajosana, X., Ed., Pister, K., and T. Watteyne, "Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration", BCP 210, RFC 8180, DOI 10.17487/RFC8180, May 2017, <https://www.rfc-editor.org/info/rfc8180>.

Authors' Addresses

Diego Dujovne (editor)
Universidad Diego Portales
Escuela de Informatica y Telecomunicaciones, Av. Ejercito 441
Santiago, Region Metropolitana
Chile

Phone: +56 (2) 676-8121
Email: diego.dujovne@mail.udp.cl

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca