

6TiSCH
Internet-Draft
Intended status: Standards Track
Expires: December 21, 2018

X. Vilajosana, Ed.
P. Tuset
B. Martinez
Universitat Oberta de Catalunya
J. Munoz
Inria
June 19, 2018

Global Time Distribution in 6TiSCH Networks
draft-vilajosana-6tisch-globaltime-01

Abstract

This specification defines an optional extension to the Constrained Join Protocol (CoJP) defined by the Minimal Security Framework for 6TiSCH. The extension aims at providing global time distribution support so nodes in the 6TiSCH network can exploit global time information instead of relying only in relative network time based on the Absolute Sequence Number (ASN). The specification also defines a mechanism for resynchronization, to handle leap seconds or to enable periodic global time updates relying on a CoAP service.

Requirements Language

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 [RFC2119].

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 December 21, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Global Time Source	3
3. Global Time Extension to the Join Response	4
4. Resynchronization	7
5. Leap Second handling	8
6. Security Considerations	8
7. References	8
7.1. Normative References	8
7.2. Informative References	9
Authors' Addresses	9

1. Introduction

Time Synchronized Channel Hopping (TSCH) exploits node synchronization to build up deterministic access networks through scheduling [RFC7554]. 6TiSCH defines a control plane architecture to enable IEEE802.15.4 TSCH networks to securely bootstrap and in a distributed manner self-organize in order to meet application traffic needs [I-D.ietf-6tisch-architecture]. The synchronization accuracy between the nodes' clocks in a 6TiSCH network is dependent on the network maintenance traffic (Keep Alives), application traffic, and MAC layer guard time duration. It is well-known that, for a given traffic, the smaller the guard time, the smaller the tolerated drift between two nodes, and hence, the more precise their synchronization.

The concept of network synchronization is achieved through a virtual counter referred as Absolute Sequence Number (ASN). In a 6TiSCH network, each node updates its ASN at every slot, giving the nodes the same notion of time (with timeslot granularity). This time is relative to the moment the network started or reset and hence cannot be used to compare tagged events from different networks.

This document defines a data structure to map ASN and absolute time. The document then defines the procedure to transport the structure to the 6TiSCH nodes:

- o As an optional extension to the Constrained Join Protocol (CoJP) Join Response procedure within the Minimal Security Framework for 6TiSCH [I-D.ietf-6tisch-minimal-security].
- o As a CoAP Response [RFC7252] to a global time service exposed by the Join Registrar/Cordinator (JRC).

2. Global Time Source

In order to distribute global time information in a 6TiSCH network at least one component must be acting as a global time source and enabling nodes in the network to obtain the absolute time reference from it. The way global time is obtained and maintained in this network component is out of scope of this specification. As an example, this component can account for the global time in the network internally, can use an external source to obtain global time (e.g. GPS, NTP [RFC5905]) or, can be synchronized through a precision time protocol (PTP) such the IEEE-1588 [IEEE1588] to another network.

We use the example network in Figure 1 throughout this specification for illustration. The Join Registrar/Coordinator (JRC) acts as the global time information source for a node when it joins. How the JRC obtains such global time information is out of scope of this specification. The JRC can be a component outside of the 6TiSCH network. However it is required to be synchronize to it through the ASN. How the JRC obtains such synchronization to the 6TiSCH network is out of the scope of this specification. This specification defines how the JRC formats and distributes the absolute time reference to the 6TiSCH nodes in the network.

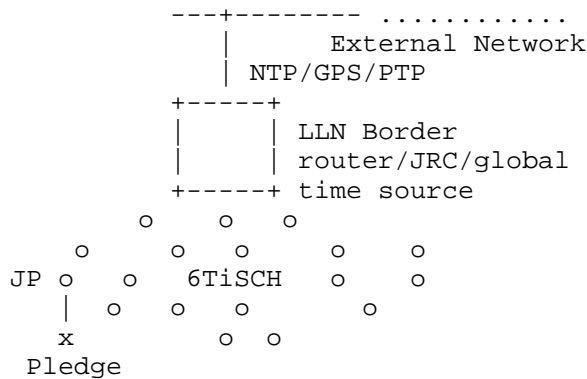


Figure 1: An example network

A Pledge node obtains its global time reference during the Secure Join Process with the JRC [I-D.ietf-6tisch-minimal-security]. This specification extends the Join Response message with an optional data structure which includes the global time reference and optionally the period for absolute time updates.

The global time reference is a mapping between the ASN of the network and the global time at the moment of processing the Join Response. After having obtained the global time reference, a 6TiSCH node maintains internally its timing until it updates it, resets or is disconnected from the network. Optionally, periodic refresh messages can be issued by the 6TiSCH node to the JRC using the JRC URI exposing the time service. These optional refresh messages MAY be used to cope with the clock drift caused by any possible imprecision between the configured timeslot length and the actual timeslot length. As an example, a timeslot can be configured to be 10ms long but because of the nature of the crystal in the device the timeslot becomes 10.1ms.

3. Global Time Extension to the Join Response

This document extends the Join Response message within the Constrained Join Protocol (CoJP) defined in [I-D.ietf-6tisch-minimal-security] with:

- o A byte string containing the ASN at which the CoAP Response (e.g, Join Response) is processed at the JRC. The 5-byte ASN is carried in network byte order.
- o An 8-bit unsigned integer containing an era counter. The era counter is used to account for wraps of the seconds counter. It starts at 0 and increments approximately every 136 years as per

definition of era in NTP [RFC5905]. Era 0 starts at 0h UTC 1st of January 1900.

- o A 32-bit unsigned integer containing a timestamp in seconds, captured at the beginning of the timeslot at which the CoAP Response (e.g. Join Response) is processed. Carried in network byte order. The seconds and fraction fields are based on the specification described in the NTP standard [RFC5905] for the Timestamp format. The seconds field accounts for seconds elapsed since the 0h on the 1 January 1900 UTC, as described by the NTP standard [RFC5905].
- o A 32-bit unsigned integer containing the number of picoseconds elapsed after the last entire second at the beginning of the timeslot at which the CoAP Response (e.g. Join Response) is processed. Carried in network byte order. Its granularity is described in the NTP standard [RFC5905].
- o Optionally, a byte string encoding a global time service URI in core-link format. The default value is 'gt'.
- o Optionally, an unsigned word lease value indicating the number of minutes of freshness of the assigned global time information. If this value is not provided the lease time is considered to be infinite. If this value is 0, a node does not refresh the global time information.

```
global_time_option = {  
    0 : bstr,           ; ASN  
    1 : uint8,          ; era counter  
    2 : uint32          ; seconds counter  
    3 : uint32          ; fraction  
    ? 4 : bstr          ; gt_service  
    ? 5 : uint16        ; gt_lease  
}
```

Name	Label	CBOR type	Reference
ASN	0	byte string	[[this document]]
era counter	1	unsigned integer (uint8)	[[this document]]
seconds counter	2	unsigned integer (uint32)	[[this document]]
fraction	3	unsigned integer (uint32)	[[this document]]
gt_service (optional)	4	byte string	[[this document]]
gt_lease (optional)	5	unsigned integer (uint16)	[[this document]]

To take into account possible leap seconds. An optional `leap_second_option` is defined by:

- o An 8-bit unsigned integer containing the action to be performed when the next leap second day is reached.
- o A 16-bit unsigned integer containing an offset in days to the beginning of the day (0 h UTC) when the next leap second must be applied. Carried in network byte order.

```
leap_second_option = {
    0 : uint8,           ; leap_indicator
    1 : uint16,          ; leap_offset
}
```

Name	Label	CBOR type	Reference
leap_indicator	0	unsigned integer (uint8)	[[this document]]
leap_offset	1	unsigned integer (uint16)	[[this document]]

The optional `leap_second_option` defines a leap second indicator, which identifies the type of correction that needs to be applied once the next leap second day is reached. The types are described in Figure 9 of the RFC5905 [RFC5905].

A `leap_offset` contains the offset in days to when the next leap second needs to be applied, following the action described in the leap second indicator.

The `global_time_option` and the `leap_second_option`, if present, SHOULD be appended following the Join Response Payload and MUST be encoded as a CBOR map objects [RFC7049].

4. Resynchronization

When a pledge receives the Join Response containing the `global_time_option`, it updates its internal absolute time clock/counter. If present, it also stores the `gt_service` link-format URI and the lease time.

After correcting a leap second or when the lease period is reached, a node MAY want to update the global time information values to keep track of the next leap second correction event or to renew its global time synchronization lease. This resynchronization is conducted through a CoAP GET Request to the JRC address and `gt_service` URI.

- o The request method is GET.
- o The type is Non-confirmable (NON).
- o The Proxy-Scheme option is set to "coap".
- o The Uri-Host option is defined by the JRC URI.
- o The Uri-Path option is set to `gt_service`.
- o The payload is empty.

The response is a CoAP Response Message with Response Code 2.05 (Content) containing the `global_time_option` as payload. The response

MAY contain a `leap_second_option` in case a leap second update is needed. Both options if present are encoded as CBOR dictionaries.

5. Leap Second handling

When a 6TiSCH node receives a global time synchronization message and this response contains a `leap_second_option`, the node MUST store the values until the leap second offset is reached.

When a leap second offset is reached, the leap second is corrected adding or subtracting a second to the last minute of the day as indicated by the `leap_indicator` field.

6. Security Considerations

The global time synchronization option is transported as part of the payload of the 6P Join Response message and secured by OSCORE (Object Security for Constrained RESTful Environments) as per [I-D.ietf-6tisch-minimal-security]. Since the JRC acts as the global time synchronization server, compromising the JRC will result in a compromise of the transported information.

A malicious 6N attacker may use a short lease time to generate high volumes of traffic in the network or even to try to deny the service to the JRC. Is up to the JRC to implement temporal blacklisting policies to avoid any DoS attack.

7. References

7.1. Normative References

- [I-D.ietf-6tisch-minimal-security]
Vucinic, M., Simon, J., Pister, K., and M. Richardson,
"Minimal Security Framework for 6TiSCH", draft-ietf-6tisch-minimal-security-06 (work in progress), May 2018.
- [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>>.
- [RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <<https://www.rfc-editor.org/info/rfc5905>>.

- [RFC6690] Shelby, Z., "Constrained RESTful Environments (CoRE) Link Format", RFC 6690, DOI 10.17487/RFC6690, August 2012, <<https://www.rfc-editor.org/info/rfc6690>>.
- [RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <<https://www.rfc-editor.org/info/rfc7049>>.
- [RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <<https://www.rfc-editor.org/info/rfc7252>>.
- [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>>.

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-14 (work in progress), April 2018.
- [IEEE1588]
IEEE standard for Information Technology, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," in IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002) , vol., no., pp.1-300", July 2008.

Authors' Addresses

Xavier Vilajosana (editor)
Universitat Oberta de Catalunya
156 Rambla Poblenou
Barcelona, Catalonia 08018
Spain

Email: xvilajosana@uoc.edu

Pere Tuset
Universitat Oberta de Catalunya
156 Rambla Poblenou
Barcelona, Catalonia 08018
Spain

Email: peretuset@uoc.edu

Borja Martinez
Universitat Oberta de Catalunya
156 Rambla Poblenou
Barcelona, Catalonia 08018
Spain

Email: bmartinezh@uoc.edu

Jonathan Munoz
Inria
2 rue Simone Iff
Paris 75012
France

Email: jonathan.munoz@inria.fr