IEEE P802.11
Wireless LANs

|  |
| --- |
| Protecting the Timestamp field in Beacon frames |
| Date: 2025-04-29 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Henry Ptasinski | Morse Micro |  |  | henry@e78com.com |
| David Halasz | Morse Micro |  |  | dave.halasz@ieee.org |

Abstract

The Timestamp field in 802.11 Beacon frames are currently unprotected, even when the frames are protected using BIP. This submission proposes changes to add protection for the Timestamp field in BIP-protected frames, in a manner that is transparent to legacy devices.

R0: Initial draft

R1: Additional discussion

R2: Add Timestamp check in clause 12.5.3.6

R3: Address comments

R4: Add restriction on usage when Beacon Period is <= 32

### Discussion:

In Beacon frames that are protected with BIP, the timestamp field remains unprotected. An attacker could modify the timestamp field in beacons to affect station behavior, such as causing a station with TWT enabled to wake at incorrect times which could result in excess power consumption by the station and degraded network performance.

When adding integrity protection to S1G Beacon frames, in order to minimize the amount of overhead added to the frames, they do not include an MME and instead use a MIC element (which does not include space for a BIPN). Instead of transmitting the BIPN with the frame, the BIPN is derived from the TSBTT/TBTT. This reduces the possibility of any modification of the Timestamp field to at most one beacon period.

Similar to the approach for deriving the BIPN based on the TSBTT/TBTT for S1G Beacon frames that are protected using BCE, the BIPN for Beacon frames that are protected using BIP can be derived from the TBTT as:

BIPN = CurrentTBTT / (1024 × dot11BeaconPeriod)

*CurrentTBTT* is the TBTT of the Beacon frame that is being protected.

At the transmitter this could be implemented as:

*Ceil(TSF/(1024 x dot11BeaconPeriod))*

The receiver could use:

*Floor(TSF/(1024 x dot11BeaconPeriod))*

Calculating the BIPN in this way still satisfies the requirement that “the transmitting STA shall insert a strictly increasing integer into the MME IPN/BIPN field.” Note that the BIPN will increment by 1 for each Beacon transmission, since the CurrentTBTT increases by 1024 × dot11BeaconPeriod for each TBTT, and is not affected by queueing or transmission delays as it is calculated based on the *target* beacon transmission time.

The BIP integrity value is computed over the entire frame, include the MME. Since the BIPN is derived from the CurrentTBTT, this provides protection for CurrentTBTT.

In order for devices to take advantage of this protection, they simply need to know that the AP is using this calculation when generating the BIPN. This can be accomplished simply by adding a flag in the RSNXE. No signaling is required from non-AP STAs.

For legacy devices, the frame structure and BIP algorithm is unchanged. To those devices, this new BIPN derivation will look like any other BIPN counter, so legacy devices do not require any changes to receive and validate the BIP protection on these Beacon frames, and the level of protection provided by BIP to legacy devices remains unchanged.

### 9.4.2.240 RSNXE

***Add a new entry in Table 9-373 and update the last entry as needed:***

***Table 9-373—Extended RSN Capabilities field***

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| <ANA> | Protected Timestamp | An AP sets the Protected Timestamp field to 1 when dot11ProtectedTimestamp is true, and sets it to 0 otherwise. For non-AP STAs, this field is reserved. See 12.5.3.4. |

### 12.5.3.4 BIP replay counters and packet numbers

Change the second paragraph as shown:

When beacon protection is enabled at ~~the~~a non-~~SP~~AP STA, the receiver shall maintain a 48-bit replay counter for each BIGTK. The receiver shall set the replay counter to the value of the BIPN in the BIGTK key data encapsulation (KDE) (see 12.7.2 (EAPOL-Key frames)) provided by the Authenticator in the 4-way handshake, FT 4-way handshake, FT handshake, group key handshake, or FILS authentication. The transmitter shall maintain a single BIPN for each BIGTK. When beacon protection is enabled at an S1G AP and BCE is enabled, the BIPN shall be implemented as a 48-bit representation of the number of TSBTTs or TBTTs since TSF time 0. If dot11ShortBeaconInterval is true, the BIPN shall be initialized using Equation (12-1):

Change the text starting at page 3041, line 18 as shown:

When beacon protection is enabled at an S1G AP and BCE is disabled, the BIPN shall be implemented as a 48-bit strictly increasing integer, initialized to 1 when the corresponding BIGTK is initialized. For non-S1G STAs, when dot11ProtectedTimestamp is false the BIPN shall be implemented as a 48-bit strictly increasing integer, initialized to 1 when the corresponding BIGTK is initialized. For non-S1G APs, when dot11ProtectedTimestamp is true, when adding protection to a Beacon frame the BIPN shall be calculated using Equation (12-5):

 BIPN = *CurrentTBTT* / (1024 × *dot11BeaconPeriod*) (12-5)

where

 *CurrentTBTT* is the TBTT of the Beacon frame that is being protected, in µs.

For non-S1G non-AP STAs, when dot11ProtectedTimestamp is true and the AP set the Protected Timestamp field in the RSNXE in the 4-way handshake to one, when checking protection on a Beacon frame the BIPN shall be calculated using Equation (12-5).

### 12.5.3.6 BIP reception

Modify setp (b)(3) as shown:

3) If the frame is a protected Beacon frame or a protected S1G Beacon frame, the receiver shall compare this MME IPN/BIPN to the value of the replay counter for the BIGTK identified by the MME Key ID field. If the integer value from the received MME IPN/BIPN field is less than or equal to the replay counter value for this BIGTK, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1. For non-S1G STAs, when dot11ProtectedTimestamp is true, the receiver shall calculate a BIPN for the frame using Equation (12-4), and compare this calculated BIPN to the integer value from the received MME IPN/BIPN field. If the two values are not equal, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.

### C.3 MIB detail

Add the following entry to the end of the Dot11StationConfigEntry{} list:

 dot11ProtectedTimestamp TruthValue

Add the following new entry to the dot11StationConfig TABLE:

dot11ProtectedTimestamp OBJECT-TYPE

 SYNTAX TruthValue

 MAX-ACCESS read-write

 STATUS current

 DESCRIPTION

"This is a control variable.

It is written by the SME or external management entity.

Changes take effect for the next MLME-START.request primitive or MLME-JOIN.request primitive.

This attribute, when true, indicates that the station implementation is capable of supporting Protected Timestamp fields in Beacon frames. The capability is disabled, otherwise. This attribute cannot be true at an AP when dot11BeaconPeriod is less than or equal to 32."

 DEFVAL { false }

::= { dot11StationConfigEntry <ANA> }

**References:**

[Draft P802.11REVme\_D7.0.pdf](https://grouper.ieee.org/groups/802/11/private/Draft_Standards/11me/Draft%20P802.11REVme_D7.0.pdf)