IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for SBP Comments in LB272 - Part 2: SBP security/privacy | | | | |
| Date: 2023-05-11 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Cheng Chen | Intel |  |  | cheng.chen@intel.com |
| Ali Raissinia | Qualcomm |  |  | alirezar@qti.qualcomm.com |
| Claudio da Silva | Meta |  |  | [claudiodasilva@meta.com](mailto:claudiodasilva@meta.com) |
| Narengerile | Huawei |  |  | narengerile@huawei.com |

Abstract

This submission proposes resolutions to the following comments submitted in LB272 under Instance topic. The CIDs are referring to D1.0. The text used as reference is D1.0.

CIDs: 1427 1796 1932 2049 2050 2300 1674 1795 1933 2051

Revision history:

R0: Original version

R1: Added more coauthors.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **Page** | **Comment** | **Proposed change** | **Proposed resolution** |
| **Category 0** | | | | | | |
| 1427 | Wookbong Lee | 11.55.2 | 190.45 | There is a security concern in the SBP scheme. | Delete it | Rejected. The comment fails to identify a specific issue to be addressed. It fails to identify changes in sufficient detail so that the specific wording of the changes that will satisfy the commenter can be determined. |
| 1796 | Tianyu Wu | 11.55.2 | 190.50 | SBP is not complete in the draft. Security for SBP is missing. | Define security for SBP or remove SBP feature. | Rejected. The comment fails to identify a specific issue to be addressed. It fails to identify changes in sufficient detail so that the specific wording of the changes that will satisfy the commenter can be determined. |
| **Category 1** | | | | | | |
| 1932 | Mohamed Abouelseoud | 11.55.2.2 | 191.54 | The sensing responder cant distinguish between a WLAN sensing setup and SBP sensing setup. The responder should have the capability to accept or reject the setup based on this information | Include a bit in the sensing measurement parameter field to indicate if the setup is being done for a SBP session | Revised. See below for proposed changes. |
| 2049 | Debashis Dash | 11.55.2.2 | 191.54 | From a sensing responder's perspective there is no way to distinguish between a WLAN sensing setup and one being done for a SBP sensing setup. The parameters for the sensing setup currently are copied over from the SBP request frame and uses the same sensing measurement setup request frame as done during a WLAN sensing setup: "The SensingMeasurementParameter parameter within the MLME-SENSMSMTSETUP.request primitive 55 issued to initiate a WLAN sensing procedure used to satisfy an SBP request shall be identical to the Sensing- MeasurementParameter parameter within the corresponding MLME-SBP.request primitive." This doesn't include any indication of the measurement setup being a part of a SBP setup. | Include a bit in the sensing measurement parameter field to indicate if the setup is being done for a SBP session | Revised. See below for proposed changes. |
| **Category 2** | | | | | | |
| 2050 | Debashis Dash | 11.55.2.2 | 191.54 | When a sensing measurement setup is being done by a sensing initiator as a part of SBP measurement setup, the sensing responder has no way of identifying the SBP initiator. The parameters copied over from the SBP setup doesn't contain the identity of the SBP initiator: "The SensingMeasurementParameter parameter within the MLME-SENSMSMTSETUP.request primitive 55 issued to initiate a WLAN sensing procedure used to satisfy an SBP request shall be identical to the Sensing- MeasurementParameter parameter within the corresponding MLME-SBP.request primitive." | Include a new field in the setup request to indicate the SBP initiator's identity. The identity can be any existing identifiers like AID, USID or MAC address.  Include a parameter in the SBP setup to indicate to the SBP responder if it can include the SBP initiator's identity in the WLAN sensing setup with the sensing responder. | Revised. See below for proposed changes. |
| 2300 | Firouz Behnamfar | 11.55.2.2 | 191.54 | WLAN sensing responder is unable to identify the actual WLAN sensing initiator in the SBP procedure.  The sensing measurement setup in SBP does not contain any information on the identity of the sensing inititor. In fact, from the sensing responder perspective, the WLAN measurment setup request in SBP, which is initiated by a non-AP STA, and the WLAN sensing request, which originates from the AP, are identical. Due to various concerns, including privacy, the WLAN sensing measurement setup must contain information which enables the sensing responder to identify the true sensing initiator, so that the responder can decide whether or not to accept the setup request. | Add a new field to the setup request frame to enable the sensing responder to identify the true sensing initiator. | Revised. See below for proposed changes. |
| **Category 3** | | | | | | |
| 1674 | Chaoming Luo | 11.55.2.2 | 191.25 | It's not clear whether an existing MS (established before the SBP request) could be reused to satisfy the SBP request. | Add a paragraph to clarify: An existing MS which was established before the SBP request may be reused to satisfy the SBP request. | Revised. See below for proposed changes. |
| 1795 | Anuj Batra | 11.55.2.2 | 192.26 | No normative text to limit using existing measurement setup for any new SBP setup requests | Either add normative text to indicate that for each SBP request, SBP responder shall initiate a new measurement setup with WLAN sensing responders, or remove SBP | Revised. See below for proposed changes. |
| 1933 | Daniel Borges | 11.55.2.2 | 192.5 | I would like see some more normative text regarding privacy concerns and issues from the responder side for the SBP Setup procedure. | Please add normative text which does not re-use existing measurement setups without the explicit knowledge of the sensing responder. | Revised. See below for proposed changes. |
| 2051 | Debashis Dash | 11.55.2.2 | 192.26 | There is no normative text to limit the use of an existing measurement setups for any new SBP setup requests. The privacy requirement for a SBP setup cannot be assumed to be same as that of a WLAN sensing setup, since a SBP can be requested by any associated non-AP STA or un-associated non-AP STA. Current text doesn't dis-allow the use of any existing session to be used by a new SBP request that statisfies the sensing parameters. | Please add normative text to indicate that the SBP responder shall initiate a new measurement setup with WLAN sensing responders for each SBP request.  Include a bit during the session setup for the sensing responder to indicate if the sensing session(s) can be shared with any SBP initiator. If the sensing responder has indicated that their sessions can be shared with any SBP initiator, AP may skip a new measurement setup.  Please add a note that once the measurement setup is sucessfully completed, the sensing PPDUs can be shared if there are multiple measurement setups between the same sensing initiator and sensing responder with common parameters. | Revised. See below for proposed changes. |

**Discussion:**

All these CIDs are talking about SBP on one or more of the following categories.

1. Problem statement:

From the non-AP STA’s point of view, there is no differentiation between a sensing measurement setup used for a conventional sensing procedure and a sensing measurement setup triggered by an SBP procedure. In other words, if a non-AP STA receives a Sensing Measurement Setup Request frame from an AP, it cannot identify whether this request comes from the AP itself, or from another non-AP STA through the SBP procedure. As a result, this lack of information to identify the actual initiator of the sensing measurement setup may lead to some security concerns.

Discussion:

It is indeed true that currently we do not have a signaling to differentiate a sensing measurement setup used for a sensing procedure triggered by the AP itself between a sensing measurement setup used for satisfying an SBP request from a non-AP STA. The easiest way to differentiate it is to add some signaling in the Sensing Measurement Setup Request frame to identify whether the corresponding sensing measurement setup is used to satisfy an SBP procedure. In this case, when a non-AP STA receives a Sensing Measurement Setup Request frame from an AP, it will be able to know whether this is for the sensing procedure triggered by the AP itself, or for an SBP procedure triggered by another non-AP STA, which it can then determine whether to accept the request or not.

Proposed resolutions:

See below.

1. Problem statement:

If the sensing measurement setup is used to satisfy an SBP procedure, the non-AP STAs chosen as sensing responders cannot identify who is the SBP initiator that triggered the AP to initiate such a sensing measurement setup. Several commenters think we should enable these non-AP STAs to understand the identity of the SBP initiator so that they have more information to decide whether to accept the sensing measurement setup request.

Discussion:

In an SBP procedure, even if the SBP initiator does not know any of the sensing responders in the sensing procedure triggered by the SBP procedure, it is able to understand the AID/USID of each sensing responder in the SBP Report frame. In the meanwhile, it is true that currently a sensing responder does not know the identifier of the SBP initiator if it receives a sensing measurement setup request from an AP triggered by an SBP procedure.

Therefore, a reasonable method is to also include the AID/USID of the SBP initiator in the Senisng Measurement Setup Request frame if it is used to satisfy an SBP procedure.

Proposed resolutions:

1. Define a new subelement “SBP Specific subelement” for Sensing Parameters in Table 9-401r. If the SBP Procedure field in the Sensing Measurement Parameters field within the Sensing Measurement Parameters element is set to 1, this subelement is also included in the Sensing subelements field within the Sensing Measurement Parameters element. We then define one field “SBP Initiator AID12/USID12” in the SBP Specific subelement to include the AID12/USID12 of the SBP initiator.
2. The presence of the SBP Specific subelement also serves as the differentiation signaling for the previous problem. That is, if the SBP Specific subelement is present in the Sensing Measurement Parameters element, the corresponding sensing measurement setup is used for satisfying an SBP procedure.

Table 9-401r: Sensing subelement IDs for Sensing Parameters

|  |  |  |
| --- | --- | --- |
| Subelement ID | Name | Extensible |
| 0 | Non-TB Sensing Specific subelement | Yes |
| 1 | TB Sensing Specific subelement | Yes |
| 2 | SBP Specific subelement | Yes |
| ~~2~~3-255 | Reserved |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Subelement ID | Length | SBP Initiator AID12/USID12 | Reserved |
| Bits | 8 | 8 | 12 | 4 |

SBP Specific subelement format

1. Problem statement:

Whether existing sensing measurement setups, which may be established for other applications, can be reused for an SBP procedure.

Discussion:

The contributor thinks that we should not reuse existing sensing measurement setup(s) to satisfy an SBP procedure due to the following reasons:

1. It it not necessarily true that the existing measurement setup will have exactly the same parameters with the one triggerd by the SBP request.
2. The sensing measurement setup triggered by the SBP request will typically have a different Measurement Setup ID with the existing one, which will be used in the SBP reporting procedure to identify the SBP report.
3. The existing sensing measurement setup is triggered by a sensing application running on the SBP responder AP’s end, while the sensing measurement setup is triggered by a sensing application running on the SBP initiator’s end. We are not supposed to mix the two applications.
4. Even if the existing sensing measurement setup has exactly the same set of parameters with the one triggered by an SBP request, the sensing responders do not necessarily want to accept being involved in the SBP procedure. We should give them the option to choose whether to be involved in the SBP procedure or not, instead of directly assuming they agree to do it.

Proposed resolution:

Add some normative text to specify that after accepting an SBP request from an SBP initiator, the SBP responder AP shall initiate a new sensing procedure and shall initiate new sensing measurement setups with the sensing responders.

**Proposed changes to TGbf D1.0**

***TGbf editor, make the following changes in TGbf D1.0***

Modify Table 9-401r as follows and add the following paragraphs at the end of 9.4.2.319

Table 9-401r: Sensing subelement IDs for Sensing Parameters

|  |  |  |
| --- | --- | --- |
| Subelement ID | Name | Extensible |
| 0 | Non-TB Sensing Specific subelement | Yes |
| 1 | TB Sensing Specific subelement | Yes |
| 2 | SBP Specific subelement | Yes |

If the sensing initiator is an AP, and if the Sensing Measurement Request frame is transmitted to satisfy an SBP request, it also includes an SBP Specific subelement in the Sensing Measurement Request frame to describe the set of parameters associated with the SBP request. The format of the SBP Specific subelement is as shown in Figure 9-xxx (SBP Specific subelement format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Subelement ID | Length | SBP Initiator AID12/USID12 | Reserved |
| Bits | 8 | 8 | 12 | 4 |

Figure 9-xxx: SBP Specific subelement format

The SBP Initiator AID12/USID12 field indicates the 12LSBs of either the AID or the USID for the SBP initiator that triggers the AP to transmit the associated Sensing Measurement Request frame to satisfy the SBP request from the SBP initiator.

Add the following paragraph in 11.55.2.2

An SBP responder that sends an SBP Response frame with status code SUCCESS shall include an RSTA Availability Window element in the SBP response frame. The RSTA Availability Information field in the RSTA Availability Window element shall contain exactly one Availability Window Information subfield. The Availability Window Information subfield represents the availability window assigned by the SBP responder to the SBP initiator. The SBP responder shall set the Availability Window Broadcast Format subfield of the Header subfield in the RSTA Availability Information field of the RSTA Availability Window element to 0.

To satisfy an SBP request, the SBP responder shall initiate a new sensing procedure. The Sensing Measurement Request frame transmitted to a sensing responder used to satisfy an SBP request shall include an SBP Specific subelement containing the AID12/USID12 of the SBP initiator. The Measurement Session ID field in the Sensing Measurement Request frame(s) shall be the same as the Measurement Session ID sent in the SBP Response frame and shall be different than all the exiting Measurement Session IDs used with corresponding sensing responder(s).

## SP

Do you support the proposed resolutions to the CIDs and incorporate the text changes into the latest TGbf draft?

Y/N/A