**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | Text related to UWB MAC primitives | |
| Date Submitted | 15th September 2015 | |
| Source | Billy Verso (DecaWave),  Igor Dotlić (NICT) | billy.verso @ decawave.com  dotlic @ nict.go.jp |
| Re: | Draft text covering relative positioning and localization topics, and including two way ranging mechanisms | |
| Abstract | Text for inclusion in IEEE 802.15.8 | |
| Purpose | Provision of the text to facilitate its incorporation into the draft text of the IEEE 802.15.8 standard currently under development in the 802.15 TG8. | |
| Notice | This document does not represent the agreed views of the IEEE 802.15 Working Group or IEEE 802.15.8 Task Group. It represents only the views of the participants listed in the “Source(s)” field above. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. | |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. | |
| Patent Policy | The contributor is familiar with the IEEE-SA Patent Policy and Procedures:  <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and  <http://standards.ieee.org/guides/opman/sect6.html#6.3>.  Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and  <http://standards.ieee.org/board/pat>. | |

# Managing dynamic preamble selection (DPS)

It is anticipated that typical ranging traffic will take place using the normal preamble codes. Therefore, even if the messages are encrypted, a hostile device can monitor traffic, and turn on its transmitter to generally disrupt the ranging. To defeat this attack, this standard offers the DPS option, allowing the PDs participating in the ranging exchange to change preamble codes during the ranging exchange.

The coordination of DPS is beyond the beyond the scope of this standard, however it may be achieved by encrypted messages so that any hostile devices are denied knowledge of the preambles that will be used. To defeat a “jam and spoof the retry” attack the preambles used should be changed for each ranging attempt.

The *DPSIndexDuration* parameter ensures that the PD are returned to an interoperable data state in the event of not receiving an expected message. PD that do not implement DPS do not be give up any other ranging capabilities.

Figure *1* shows a suggested message sequence employing DPS for the three-message double-sided two-way ranging exchange. The messages represented in the dot boxes are simply suggestions showing how the DPS capability might be selected. The MLME.DPS.request primitive is described in 1.3.1.1, and the MLME-DPS.confirm, as described in 1.3.1.2.

Upon the generation of the MLME.DPS.confirm primitives, as illustrated in Figure 34, both of the PHYs have switched to use the TxDPSIndex and RxDPSIndex codes for their preamble symbols, and MAC sublayers on both sides have started timers of the *DPSIndexDuration* value. The changing of preamble code is intended to help protect against attack, but as a side effect neither PHYs can communicate with the rest of its peers. The *DPSIndexDuration* value serves to prevent this situation persisting any longer than is necessary. If this timer duration is exceeded before the MAC sublayer issues the MCPS.DATA.comfirm (for the originator) or the MCPS.DATA.indication primitive (for the recipient), then the MAC sublayer shall initiate the MLME.DPS.indication to the next higher layer as described in 1.3.1.3.



**Figure 1 – message sequence chart for the three message DS-TWR using DPS**