1. As a general comment, since the RR application messages themselves can be authenticated, there is a general preference with many applications to not have redundant L1/L2 security enabled. Therefore, when it comes to the DPP optimizations, it would be great if both AUTH = 0 and AUTH = 1 cases could be equally addressed and not assume security being in most cases enabled.
2. CRC and HMAC should be able to almost equally well verify data integrity. Therefore, I agree it is a good idea to eliminate the cases when both of these data fields would be simultaneously included in CTRL MSG.
3. I have some concerns about using HMAC verification as a means for a receiving radio to identify messages that are addressed to it.
   1. First and foremost, the concern is about computational requirements, especially with high message traffic volumes and with multiple co-existing DPP links/sessions. HMAC verification could be a somewhat computationally heavy operation to perform and with this approach it would need to be done continuously to every detected message in the CSMA channel. With multiple concurrent DPP links the verification would need to be done for each message multiple times, with each associated key separately.
   2. This approach also assumes the keys being used for HMAC validation to be unique to each radio. If these keys originate as TLS session keys this may not ever be an issue. But, it is not completely unheard of that someone wants to simplify their asset key management by installing the same key to multiple devices in the network. If there is any scenario where the HMAC validation keys somehow get derived from such non-unique provisioned keys, it could become a problem with this approach.
   3. One would need to be very careful with communication initiation and any key update scenarios, etc., since those could result in complete communication loss. Similarly, any operational factors that could result in HMAC verification failures such as time synchronization loss could impact expected communication if not designed carefully.
   4. It would become harder to debug the radio and radio network operation with data captures although this may only impact the development phase and not being able to monitor network activity is in fact one of the security objectives.