IEEE P802.15

Wireless Personal Area Networks

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | List of issues to be solved by the privacy group |
| Date Submitted | 14th May 2023 |
| Source | Tero Kivinen | E-mail: kivinen@iki.fi |
| Re: | May SG Privacy meeting |
| Abstract | Provide list of issues that SG privacy group needs to address |
| Purpose | Start working on the 802.15.4 privacy |
| Notice | This document has been prepared to assist the IEEE P802.15. 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. |

1. List of issues
	1. MAC addresses in the frames
		1. Generic

The frames cannot use stable extended address, they need to use extended addresses that are not permanent.

Use AAI-64 as defined in the 802c-2017, setting M/X/Y/Z bits as x/1/0/0 and leaving rest of 60 bits for private addressing. Do we need to reserve some bits to identify type of privacy address, i.e., temporary address of device, stable network identifier, stable device identifier.

* + 1. Do not use static addresses

This means devices should not use their static address in clear in any of the messages they are sending out, not even when they are joining a network, resuming from the sleep, or when they are restarted.

* + 1. Only one addresses

Lots of devices only have one configurable extended address recognized by the hardware, thus they can only receive broadcast frames and frames having their extended address as destination address. On the other hand they can turn radio to promiscuous mode to see all traffic if needed.

For privacy it would be better to have multiple address for each device. Perhaps we need a have capability information telling whether the device supports that.

For example the ranging might use temporary address for each ranging round.

We might also have location specific addresses for example for one shop to get discounts etc.

* + 1. Do not respond to static address

Devices needs to be able to not respond to messages sent to their stable extended address. Even if someone directly sends message using the stable extended address of the device (i.e., probing attack) device needs to have option not to respond to them.

* 1. Sending updates to the peers when address changes
		1. Generic

We need a method to send a message from on device to another telling that the first device is changing its mac address, and tell the new mac address the device is going to be using.

If we use method where we generate addresses using key hiearchy or something then everybody can generate address and find them out even if the node is sleeping or not in range. If we allow sender to generate addresses using their own methods, then we need to send them to recipient and if recipient hasn’t received notification of the addresses, he might not be able to recognize the sender.

Sender could send multiple next addresses, so that even if the device misses some updates it might still be able to sync up by sending request of getting next n addresses.

We also need a method of doing cold boot, i.e., when the crypto context is expired, and device needs to connect to each other without knowing each others private addresses, or crypto contextes. We do assume they still have some kind of long lived secret that they can use to authenticate each other.

* + 1. Identification of the address change message

We can use either the stable extended address of the device to identify the device doing the change, or we can use the some kind of authenticated identifier to identify the device. Using the previous temporary address will work in some cases, but if there is device who has missed previous update of the address then they do not know who is sending this message.

* + 1. Update security context

The security context of the 802.15.4 is tied to the extended address of the peer, the when the device receives a message saying one of its peers is changing addresses it needs to update the security context for that peer.

The secDeviceDescriptors are keyed by the extended address, if the extended address changes then all the peers connected to that device needs to know the new temporary address. The information stored in the security context includes the frame counters for replay protection (i.e., what was the last frame counter the other peer used when it sent message to us), thus there is security implications of this change. Using secFrameCounterPerKey feature of the 802.15.4 we will automatically reset the frame counters associated with that device to zero, as there will be new device using the same key, i.e. we will add new entry for the new device, and most likely mark the old entry as something that can be deleted after the address change is finished.

We do not need to reset the frame counter to zero, we could start it from the random value, and we could increment it with random value every time we use.

* + 1. Send update to peers before going to sleep

We need to send updates to peers before we go to sleep, so when we wake up we will be using new mac address, and there is no way of correlating the old mac address used before going to sleep with new one.

* + 1. Group keys

We need a mechanims that allows changing address tied to the group keys too, i.e., keys used for beacons or device discovery packets. As some devices might be sleeping when we change addresses, we have to have mechanism where the device needs to find the group key owner again even if the address is changed.

* + 1. KeySource

There is 8-octet KeySource field in the frames which can be tied to the extended address of the owner of the key. We need to use temporary KeySource not tied to the extended address of any device.

* + 1. Changing KeySources

We need a mechanism to update the KeySource too. This needs to be done at the same time when the MAC address of the owner of the key is changed. Note, that when MAC address and KeySource are both changed the attackers listening the traffic at that time, can quite easily correlate the old and new addresses and KeySources.

* 1. Beacons and network discovery

We need a method where new device can find the network to join, even if the device creating the network is using temporary address. Beacons used should not include information that can allow fingerprinting devices (if possible).

In this case we can take the random number + identification of the network we want to join, and send a joining message to broadcast (or multicast) address, and then the network owner, can recognize this and respond to it.

One issue is that 802.15.4 devices do not have hash functions built in to them, thus we most likely would need to use some encryption based systems for this like using the identification of the network as a key, and encrypt random number with it and sending it out along with the random number.

It would be better to allocate special multicast group address for these messages, so other devices in the network do not wake up when those messages are sent.

* 1. Network identification

The device joining network needs a method of identifying the network it is joining to even when the addresses used are random. We might need some form of encrypted network identification where the devices which do not know the network identification key can’t decode which network this.

This could be used to solve issue where there multiple gateways from same vendors and lots of clients are connecting to them and the clients need to know which of the gateways to connect to.

The format could be 64-bit extended address style identification, but we want to make sure nobody uses their actual extended address as network id as the extended addresses are guessable. We might want to make sure those network identifications have a format that does not collide with the actual extended addresses, or with the randomized changing addresses.

We could define use format simialr to AAI-64 as defined in the 802c-2017, and setting M/X/Y/Z bits as x/1/1/0 and leaving rest of 60 bits for actual network identification. This network id is never used as source or destination addresses, so it is not really an address, but we want to make sure it cannot be confused as actual address, so we want to use format that is different than any of the actual addresses.

* 1. Sequence numbers

Sequence numbers, i.e., DSN, BSN, and EBSN should not have that much privacy issues, but it could be good idea to reset them to random number after you change addresses.

* 1. Static identifiers in the KMP

The KMP selected should be something that does not use static identifiers sent in clear during the negotiation process (i.e., no static diffie-hellman keys).

1. Protocols
	1. Send list of address to peers

Replace the previous list, limited to max size of the frame. Can send multiple addresses, and recipient assumes all of them are something that you can use now or in the future as your address. Always sent encrypted.

* 1. Send multicast message trying to join network

Limit the amount of data we have here, so devices cannot be fingerprinted. Always sent in clear, as there is no crypto context. This can use network id as a key and encrypt random nonce using it and sending both the random nonce, and the encrypted nonce in multicast message, so recipient can verify whether it is intended recipient.

* 1. Reply to request to join network

Limit the amount of data we have here, so devices cannot be fingerprinted. We can use similar method than in the request to authenticate the network to the peer asking for it. Always sent in clear as there is no crypto context. After this the peer can start running IEEE Std 802.15.9 over the randomzied addresses to create crypto context.

* 1. Fast reconnect (optional)

When device has lost the address of the peer, but still has crypto context, he could send multicast message to the another group encrypted with keys it already has, and using its current random addresses. The remote peer could then try to decrypt this message with all the keys it has and if any of them work, it can then know who the peer is, update the address, and send message that updates the random addresses for him.

Note, this is most likely something that is only implemented in the more powerful device, like your mobile phone.

So when device is trying to reach some peer, but transaction expires, it could send this multicast message to try to see if the peer has changed its address, and this device has just missed that update.