Projet XBT

Procédure de mesure et résultats

Historique des versions :

Version	Date	Commentaire
1.0	8/2/2022	Création
2.0	9/2/2022	Ajout des statistiques par personne

Table des matières

1 Principe et stratégie de mesure

1.1 Présentation de l'objectif

L'objectif est de reproduire les mesures effectuées avec des téléphones portables avec les applications de scanner bluetooth.
Il convient donc de bien comprendre ce que ces outils détectent.
Ces outils écoutent et affichent les messages d'advertising BLE.

1.2 Rappel sur les messages d'advertising BLE

Ces messages sont émis sur les canaux BLE suivant :

- le canal 37 à 2402 MHz
- le canal 38 à 2426 MHz
- le canal 39 à 2480 MHz

Le format général des paquets BLE est le suivant :

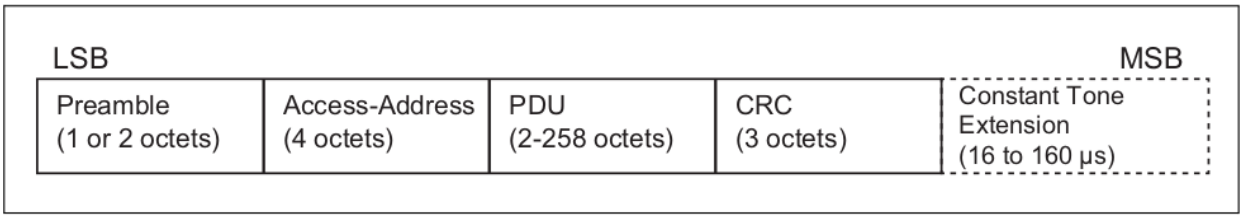

Figure 2.1: Link Layer packet format for the LE Uncoded PHYs

Le préambule est une suite de 0 et 1 afin de permettre au récepteur radio de se synchroniser et de détecter la fréquence d'horloge.
L'Access-Address est utilisée par le réception radio pour détecter le début d'un message. Les message d'advertising utilisent l'Access-Address: 0x8e89bed6
La PDU est le contenu du message proprement dit.
Le CRC est un moyen de vérification de l'intégrité du message, il est calculé sur la PDU.

La PDU est composé d'un header de 16 bits suivi de la payload.

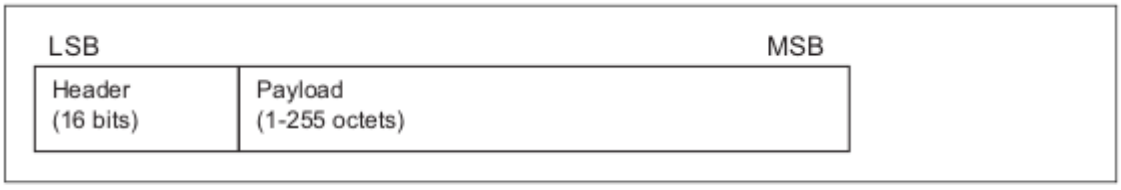

Figure 2.4: Advertising physical channel PDU

Voici la composition du header :

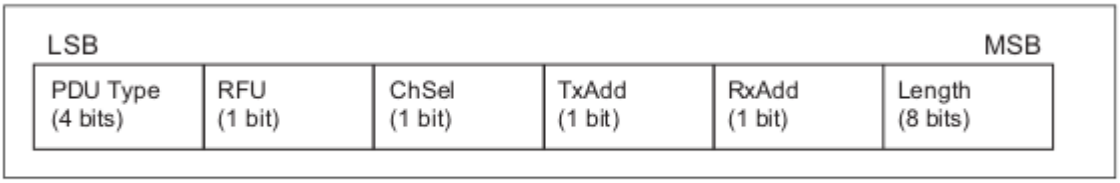

Figure 2.5: Advertising physical channel PDU header

Le champs PDU Type permet d'identifier le type de message. Les valeurs possibles évoluent de 0 à 8.
Le bit RFU n'est pas utilisé.
La signification des champs ChSel, TxAdd et RxAdd dépendent du type de PDU.
Le champs Lenght indique la longueur de la Payload en octets.

1.3 La méthode de mesure

La méthode de mesure est la suivante :

1. Capturer les messages d'advertising BLE
2. Traiter les messages afin d'identifier la nature de ces messages

L'objectif du traitement est de tenter de trouver une corrélation entre les messages reçu et les personnes testées.

1.4 Les moyens de capture des messages

1.4.1 Interfaces matérielles

Nous avons utilisé les interfaces matérielles suivantes :

- La carte Ubertooth One
- Le dongle TICC2540
- Le dongle nRF52840

Cependant nous avons principalement utilisé la carte Ubertooth One.
Cette carte est développé en OpenSource par Great Scott Gadget :
https://www.greatscottgadgets.com/ubertoothone

Cette carte est connectée sur un port USB et permet :

- d'écouter un canal BLE sur une fréquence donnée
- de détecter une Access-Address
- de capturer le message brut suivant l'Access-Address, la longueur dépend dont du champs Length capturé dans le Header de la PDU.

Cette carte produit des messages bruts, elle n'assurer pas l'intégrité du message, ceci est à la charge de l'application.

L'expérience montre que de très nombreux messages sont générés même en environnement en champ libre.

Il faut donc faire attention car la carte génère du bruit mais elle permet de « voir » les messages bruts à la différence des autres outils.

1.4.2 Les outils logiciels

Nous avons utilisé les logiciels suivant :

- Le logiciel Kismet
- Le logiciel Wireshark

Le tout en utilisant des PC sous Linux.

Cependant la grande majorité des mesures a été effectuée avec l'Ubertooth One.
Kismet produit un fichier .kismet dont on peut extraire les messages dans fichier .pcap avec l'outil : kismet_to_pcap.
Wireshark produit directement des fichiers .pcap ou .pcapng.

1.5 La méthode de traitement des messages

La source de donnée correspond aux fichiers .pcap et .pcapng produit lors des mesures. Ces fichiers sont exploités en utilisant la librairie python scapy : https://scapy.net

Parmi les messages capturés on commence par vérifier l'intégrité avec le CRC.
Les messages non intègres ne peuvent pas être traité par cette méthode et sont ignorés par les téléphones portables et les applications, donc il est légitime de les ignorer afin de reproduire ce comportement.

En suite pour chaque message on décode le message en suivant la spécification.
L'objectif dans ce décodage est d'écarter les messages dont on identifie clairement la provenance d'un équipement.

On commence par écarter les adresse MAC qui apparaissent lors de la mesure de plusieurs personnes. Ces adresses sont écartées par définition car on ne peut pas faire de lien entre la personne et l'adresse par définition.

Pour les autres on tente d'établir différents profiles de messages. Voici les profiles identifiés :

- Les messages qui contiennent une déclaration de nom

Certain messages contiennent un champs EIR_CompleteLocalName qui contient le nom de l'équipement. Ces paquets sont ignorés car les mesures effectués avec les téléphones portables ne doivent pas contenir de nom d'équipement.

- Les messages qui contiennent des données de fabricants

Certains messages contiennent un champs EIR_Manufacturer_Specific_Data qui identifie le nom du fabriquant de l'équipement. On vérifie que l'identifiant du fabriquant correspond à la liste déclarée sur le site suivant : https://www.bluetooth.com/specifications/assigned-numbers/company-identifiers
Nous n'avons pas trouvé de paquets contenant des identifiant hors de cette liste.
Voici la liste des fabricant que nous avons trouvé dans nos mesures :

- 0x6: Microsoft
- 0x4C : Apple
- 0x87 : Garmin
- 0x110 : Nippon Seiki Co., Ltd.
- 0x8AA : SZ DJI TECHNOLOGY CO.,LTD

Ces paquets sont ignorés car les mesures effectués avec les téléphones portables ne doivent pas contenir de nom de fabricants.

- Les messages qui déclarent des services connues

Certains messages contiennent des champs :

- EIR_CompleteList16BitServiceUUIDs
- EIR_CompleteList128BitServiceUUIDs
- EIR_IncompleteList128BitServiceUUIDs

Ces champs déclarent les services disponibles sur l'équipement qui émet le message.
Nous sommes parvenu dans tous les cas à identifier la source de ces services voici ce que nous avons trouvé :

- uuid_16 == 0xfd64: Application TousAntiCovid
- uuid_16 == 0xfd6f: Application TousAntiCovid
- uuid_128 == 0000fd64-0000-1000-8000-00805f9b34fb: Application TousAntiCovid
- uuid_128 == 291d567a-6d75-11e6-8b77-86f30ca893d3: Blackmagic Camera
- uuid_128 == adabfb00-6e7d-4601-bda2-bffaa68956ba: Fitbit Charge HR fitness trackers
- uuid_128 == abbaff00-e56a-484c-b832-8b17cf6cbfe8: Montre Vera Lite

Nous avons aussi des services génériques qui ne permettent pas d'identifier un équipement en particulier :

- uuid_16 == 0x1800: Generic access profile
- uuid_16 == 0x180a: Device information

- Les messages de type SCAN_REQ et SCAN_RSP

Ce messages ne permettent pas d'identifier un équipement avec certitude mais étant donné qu'ils rentrent dans un processus de communication, ils ne semblent pas correspondre à ce ce que l'on recherche.

- Il reste les messages qui ne contiennent pas de données permettant d'identifier la provenance

Dans la pratique ce sont des messages de type ADV_IND et ils ont un champs EIR Falgs.

L'outil d'analyse ressort les adresses MAC des messages dont on ne peut pas certifier la provenance.

2 La campagne au Pays-Basque

Nous avons effectué une campagne de deux jours dans un gîte.
Nous avions deux postes de mesures :

- un poste de mesure dans une petite cage de Faraday pour tenter d'atténuer les émissions environnementales
- un poste de mesure dans la pièce

Le premier jour a été très difficile car l'accueille des personnes était trop proche de la zone de mesure et donc les mesures ont été très perturbé par l'environnement.
Le second jour nous avons déporté la zone d'accueillie et l'environnement radio a été bien meilleur.

Pour le jour 1 :

- 45 personnes mesurées
- 55425 messages capturés
- 27458 messages avec CRC valide
- 129 adresses MAC identifiées
- 5 adresses MAC non identifiables
- 9 adresses MAC non identifiables mais avec des messages SCAN_RSP

Donc 14 adresses MAC a étudier :

MAC	**Numéro de la personne**	**Nombre de messages**
40:33:db:48:60:6c	34	2263
5e:9a:59:a4:19:71	34	2208
41:e7:8f:65:9e:27	34	2099
79:30:44:b6:9e:54	35	1936
53:5c:67:24:c4:de	35	1252
4d:f8:36:5b:21:09	34	882
69:05:b2:75:d8:92	18	41
71:00:62:75:ec:a7	18	36
40:c3:69:ae:11:fb	27	29
77:a5:0b:70:96:4f	27	26
77:59:17:5e:46:21	34	25
9c:9c:1d:21:cd:a8	33	19
6f:55:4d:1a:c4:8e	33	16
52:19:98:23:1c:ff	47	1

Voici les statistiques par personnes

Per.	début	fin	durée	Messages	Messages OK	MAC suspectes
2	10:34:44	10:46:57	12min 13s	67	13	
3	10:47:55	10:56:56	9min 1s	811	474	
4	10:57:25	11:00:49	3min 24s	1507	1036	
5	11:10:22	11:17:32	7min 9s	1974	1125	
7	11:21:01	11:25:35	4min 34s	1504	1000	
6	11:26:19	11:37:29	11min 9s	3661	2508	
8	11:42:06	11:42:23	0min 17s	3	0	
9	11:45:17	11:45:32	0min 15s	5	0	
10	11:49:27	11:49:51	0min 24s	5	0	
11	11:55:05	11:56:04	0min 58s	1216	0	
12	12:02:03	12:02:03	0min 0s	1	0	
13	12:05:22	12:07:45	2min 23s	6864	4667	
16	12:14:54	12:15:14	0min 20s	5	0	
17	12:18:21	12:18:32	0min 11s	2	0	
14	12:24:58	12:27:50	2min 51s	3799	0	
18	14:29:25	14:40:02	10min 36s	1064	500	69:05:b2:75:d8:92 71:00:62:75:ec:a7
19	14:41:31	14:46:19	4min 47s	177	31	
20	14:49:41	14:54:02	4min 21s	419	51	
21	14:55:48	15:00:04	4min 15s	297	18	
22	15:06:06	15:13:43	7min 36s	732	117	
23	15:16:17	15:20:00	3min 42s	228	29	
24	15:24:03	15:32:05	8min 1s	356	65	
25	15:35:10	15:42:39	7min 29s	656	148	
26	16:25:05	16:27:41	2min 35s	464	152	
29	16:51:47	17:04:53	13min 5s	922	256	
27	17:08:50	17:11:53	3min 2s	414	278	40:c3:69:ae:11:fb 77:a5:0b:70:96:4f
28	17:19:39	17:20:01	0min 21s	2	0	
30	17:25:16	17:28:46	3min 29s	12	0	
31	17:32:09	17:35:32	3min 22s	21	0	
32	17:36:55	17:41:41	4min 46s	47	20	
33	17:50:01	18:03:26	13min 25s	357	113	9c:9c:1d:21:cd:a8 6f:55:4d:1a:c4:8e
34	18:06:06	18:47:04	40min 58s	14915	9720	40:33:db:48:60:6c 5e:9a:59:a4:19:71 41:e7:8f:65:9e:27 4d:f8:36:5b:21:09 77:59:17:5e:46:21
35	18:50:15	19:07:40	17min 25s	7889	3789	79:30:44:b6:9e:54 53:5c:67:24:c4:de
36	19:18:44	19:21:05	2min 21s	252	7	
38	19:24:11	19:26:43	2min 31s	62	3	

Per.	début	fin	durée	Messages	Messages OK	MAC suspectes
37	19:28:54	19:32:06	3min 11s	192	3	
39	19:33:25	19:38:30	5min 4s	681	384	
40	19:39:21	19:42:29	3min 7s	551	154	
41	19:44:18	19:47:54	3min 35s	990	326	
42	19:48:59	19:53:13	4min 13s	1086	359	
43	19:53:32	20:00:11	6min 39s	417	59	
44	20:02:05	20:04:05	2min 0s	99	14	
46	20:07:13	20:13:23	6min 9s	486	26	
45	20:14:34	20:17:51	3min 16s	99	1	
47	20:19:00	20:21:18	2min 17s	114	12	52:19:98:23:1c:ff

Pour le jour 2 :

- 29 personnes mesurées
- 6833 messages capturés
- 1800 messages avec CRC valide
- 57 adresses MAC identifiées
- 1 adresses MAC non identifiables

MAC	Numéro de la personne	Nombre de messages
9c:9c:1d:21:cd:a8	52	17

Voici les statistiques par personnes

Per.	début	fin	durée	Messages	Messages OK	MAC suspectes
48	10:35:01	10:45:36	10min 35s	558	348	
49	10:47:22	11:01:23	14min 1s	514	77	
50	11:03:11	11:08:49	5min 38s	180	6	
51	11:11:22	11:18:02	6min 40s	197	4	
54	11:19:02	11:36:38	17min 35s	1185	490	
56	11:39:52	11:58:22	18min 29s	1121	76	
52	12:02:28	12:09:45	7min 16s	65	17	9c:9c:1d:21:cd:a8
53	12:11:19	12:27:46	16min 27s	65	4	
55	12:30:25	12:37:19	6min 54s	31	0	
57	12:51:12	15:04:38	133min 26s	667	214	
58	15:06:03	15:12:31	6min 28s	105	8	
59	15:14:52	15:46:33	31min 40s	197	43	
63 64	15:38:12	15:40:22	2min 9s	9	0	
60	15:48:55	15:57:02	8min 7s	65	0	
61	15:55:12	16:00:56	5min 44s	105	5	
62	16:02:02	16:04:55	2min 53s	50	0	

Per.	début	fin	durée	Messages	Messages OK	MAC suspectes
63	16:05:59	16:31:06	25min 6s	156	15	
64	16:16:11	16:29:24	13min 12s	584	177	
65	16:31:34	16:38:20	6min 45s	140	49	
66	16:39:05	16:42:47	3min 42s	138	52	
67	16:43:35	16:50:20	6min 44s	142	61	
68	17:05:30	17:17:36	12min 5s	106	7	
69	17:20:14	17:24:00	3min 46s	19	0	
70	17:25:03	17:26:04	1min 0s	8	0	
71	17:29:09	17:32:45	3min 35s	11	0	
72	17:34:10	17:40:00	5min 50s	24	0	
73	17:41:01	17:52:12	11min 11s	120	35	
74	17:53:47	17:58:34	4min 47s	150	98	
75	18:00:12	18:22:38	22min 26s	121	14	

Conclusion :

- La plupart des messages capturés ont un CRC invalide et ne répondent donc pas à une transmission d'informations basées sur le protocole IEEE BLE (« Bluetooth)

- La plupart des adresses MAC capturées par le protocole d'expérimentation lors de cette campagne correspondent à des devices (c'est à dire) de type Iphone, téléphone Androïde, montre connectée, tablette ou d'autre objets connecté avec un fabricant connu.

- Sur l'ensemble des personnes mesurées, seuls 7 au total présenteraient une émission d'information avec des adresses MAC dites « suspectes » (CRC valide et aucun device avec un fabricant connu). Sur ces 7 personnes, 4 sont vaccinées et 3 ne sont ni vaccinées et n'ont reçu aucun test RT-PCR ni antigénique

3 La campagne en Haute-Savoie

La campagne de teste c'est déroulée sur une après-midi dans un fond de vallée. L'environnement radio est très bon mais il y a quand même du passage de skieur et randonneurs.

Voici les résultats :

- 12 personnes mesurées
- 6766 messages capturés
- 3911 messages avec CRC valide
- 38 adresses MAC identifiées

Toutes les adresses sont identifiables.

Voici les statistiques par personnes

Personnes	début	fin	durée	Messages	Messages OK	MAC suspectes
01	12:41:40	12:56:11	14min 31s	124	0	
02	13:06:23	13:18:08	11min 44s	3065	2285	
03	13:31:58	13:33:53	1min 54s	411	224	
04	13:49:48	13:50:41	0min 53s	7	0	
05 06 07 08 09	14:18:28	14:31:11	12min 43s	883	457	
10	15:13:07	15:27:31	14min 23s	871	163	
11	15:39:20	15:45:58	6min 38s	1405	782	

Conclusion :

Lors de cette campagne, aucune adresse MAC suspectes n'a été détectée des participants.

4 La campagne de Limoges (filmée par Pierre Barnérias)

La campagne de Limoge ne fait pas strictement partie de cette procédure mais ayant eu accès aux fichier kismet nous avons appliqué le programme d'analyse sur ces données pour voir le résultat.

Voici les résultats :

- Nous n'avons pas le nombre de personnes testées, seulement de façon approximative (70)
- 43249 messages capturés
- 13678 messages avec CRC valide
- 209 adresses MAC identifiées

Conclusion :

Toutes les adresses sont identifiables et correspondent à un Device d'un fabricant connu.
Ici encore, de très nombreux messages présentent un CRC invalide et ne correspondent pas au protocole de communication BLE.
Aucune adresse MAC dite « suspecte » n'a été retrouvée sur l'ensemble des participants. Les résultats énoncés trop tôt dans le film correspondent à un biais d'interprétation de l'opérateur en charge de faire les mesures. L'analyse fine des trames d'information met en exergue que sur l'ensemble des participants, aucun d'eux ne présente une transmission d'information répondant au protocole BLE avec une adresse MAC de fabricant inconnu. Il y a donc une inexactitude des propos qui sont relatés dans le teaser du film et mis en avant par le réalisateur d'Hold-on que l'équipe du projet XB déplore.

5 Lexique :

Access-Address : Dans le protocole BLE les messages commencent pas une adresse permettant d'identifier le début d'un message.

Advertising : Fait référence aux messages d'advertising du protocole BLE.

BLE: Bluetooth Low Energy. Protocole de communication apparue dans le version 4.0 de la spécification bluetooth.

bluetooth : Protocole de communication. Voici le lien de la spécification dans sa dernière version 5.3 à date : https://www.bluetooth.com/specifications/specs/core-specification/

CRC : Contrôle de redondance cyclique. Technique de contrôle d'intégrité de données numériques.

Header : Les messages numériques sont généralement composés de deux parties, le Header l'entête qui sont fixes et permettent d'interpréter la suite des messages que l'on appel généralement Payalod, la charge utile.

Payalod: Les messages numériques sont généralement composés de deux parties, le Header l'entête qui sont fixes et permettent d'interpréter la suite des messages que l'on appel généralement Payalod, la charge utile.

PDU : Protocole Data Unit : Correspond on contenu utile d'un message.

RFU : Reserved For Futur Use. Réservé pour usage ultérieur.