TP Analyse de trames 802.11

Ce TP est adapté des Wireshark labs de Kurose et Ross proposés en suppléments à leur livre COMPUTER NETWORKING : A TOP DOWN APPROACH (© 2005-21012, J.F Kurose and K.W. Ross, All Rights Reserved).

Le standard ANSI/IEE 802.11, 1999 Edition (R2003) peut être récupéré à l'URL
`http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf`

1 Pour démarrer

1. Récupérer le fichier `Wireshark_802_11.pcap` de l'archive `http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip`. Cette trace a été collectée par AirPcap et wireshark dans un environnement comprenant un portable avec interface 802.11g, un point d'accès/routeur Linksys relié (en filaire) à deux PC. Les trames sont transmises sur le canal 6 (qui est aussi utilisé par d'autres équipements dans l'environnement, d'où la présence d'un grand nombre de trames qui ne nous intéressent pas). La trace peut être ouverte par Wireshark pour analyse des trames.

2 Trames Beacon

L'hôte est déjà associé à l'AP quand la trace commence.

1. Quels sont les SSID des deux points d'accès émetant la plupart des trames beacon ?
2. Quels est l'interval de temps entre deux trames beacon du point d'accès linksys_ses_24086 ? De l'AP "30 Munroe St" ?
3. Quelles sont (en hexa) les adresses MAC source et destination des trames beacon de l'AP "30 Munroe St" ?
4. Quels est (en hexa) le BSSID dans la trame beacon de l'AP "30 Munroe St" ?
5. Les trames beacon de l'AP "30 Munroe St" avertissent que l'AP supporte 4 débits de base et 8 débits étendus. Quels sont ces débits ?

3 Transfert de données

A $t = 24.82$, l'hôte fait une requête HTTP vers `http://gaia.cs.umass.edu/wireshark-labs/alice.txt`. L'adresse IP de gaia.cs.umass.edu est 128.119.245.12. Puis, à $t = 32.82$, l'hôte fait une requête HTTP vers `http://www.cs.umass.edu`.

1. Trouver la trame 802.11 contenant le segement TCP SYN d'établissement de connexion de la première requête. Quels sont les trois adresses MAC dans la trame 802.11 ? Laquelle de ces adresses est celle du terminal mobile ? Du point d'accès ? Du premier routeur ? Quel est l'adresse IP du terminal mobile ? Quelle est l'adresse IP destination et à quelle interface correspond-t-elle ?
2. Trouver la trame 802.11 contenant le segement TCP SYNACK de cette session TCP. Quels sont les trois adresses MAC dans la trame 802.11 ? Laquelle de ces adresses est celle de l'hôte ? Du point d'accès ? Du premier routeur ? Est-ce que l'adresse MAC de l'émetteur de la trame correspond à l'adresse IP de l'équipement qui à envoyé le segment TCP ?

4 Association/désassociation

L'association à un AP se fait par les trames ASSOCIATE REQUEST et ASSOCIATE RESPONSE (voir page 34 de la norme pour le détail des champs).

1. Quelles sont les deux trames émises par l'hôte juste après $t = 49$ pour clore l'association avec l'AP "30 Munroe St" ?

2. Examiner la trace pour trouver des trames AUTHENTICATION envoyées par un hôte vers un AP et vice-versa. Combien de messages AUTHENTICATION sont envoyés du terminal mobile vers l'AP linksys_ses_24086 aux environs du temps $t = 49$?
3. Est-ce que l'hôte demande que l'authentification utilise une clé ou soit ouverte ?
4. Voyez-vous une réponse AUTHENTICATION du linksys_ses_24086 ?
5. À quel temps a-t-on une trame AUTHENTICATION de l'hôte vers l'AP "30 Munroe St" et quant a lieu la réponse ?
6. À quel temps a-t-on une trame ASSOCIATE REQUEST de l'hôte vers l'AP "30 Munroe St" et quant est émise la trame ASSOCIATE RESPONSE correspondante ?
7. Quels débits l'hôte veut-il utiliser ? L'AP ?

5 Autres types de trames

La trace contient également des trames PROBE REQUEST ET PROBE RESPONSE.

1. Quels sont les adresses MAC d'émetteur, récepteur et BSSID de ces trames ? A quoi servent ces trames ?

6 Compte-rendu

Votre compte-rendu doit répondre brièvement aux questions posées dans ce TP et faire une synthèse sur 1/2 page d'un aspect récent en lien avec les réseaux sans-fil : 6LoWPAN, DASH7, ZigBee, WiMAX, ...

A rendre avant 15 jours en version pdf au chargé de TP (`Cyrille.Migniot@u-bourgogne.fr` ou `otogni@u-bourgogne.fr`).