



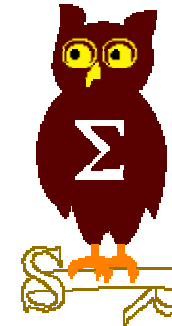
HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Groupe SUR de l'OSSIR

11 Février 2003



Présentation de WifiScanner

Jérôme Poggi

<Jerome.Poggi@hsc.fr>

Plan

- Présentation technique du 802.11b
 - Aperçu de la norme
 - Détail des trames
- Bases de WifiScanner
- Méthodes de détection
- Analyse et détection d'anomalies
 - Autres outils d'écoute
 - Fausses bornes / Piège à « renifleur »
 - Détection de SSID non diffusé
- Démonstration

Présentation technique du 802.11b

- Protocole radio de transport 11Mb/s
 - Normalisé à l'IEEE
 - CSMA/CA
 - Commercialement appelé Wi-Fi
- 3 type de trames radio
 - Administration
 - *Beacon, Probe, Association, Authentication*
 - Contrôle
 - *Acknowledge, Request/Clear to send*
 - Données



Mode de dialogue

- Exemple pour une association

- Équivalent à l'action de « brancher physiquement au réseau ».

```
      | client |      | -i- |  
      |-----|      |-----|  
                                     <--- beacons  
probe request --->  
                                     <--- probe response  
authentication request --->  
                                     <--- authentication response  
association request --->  
                                     <--- association response  
  
                                     <--- request to send  
clear to send --->  
                                     <--- data  
acknowledge --->
```

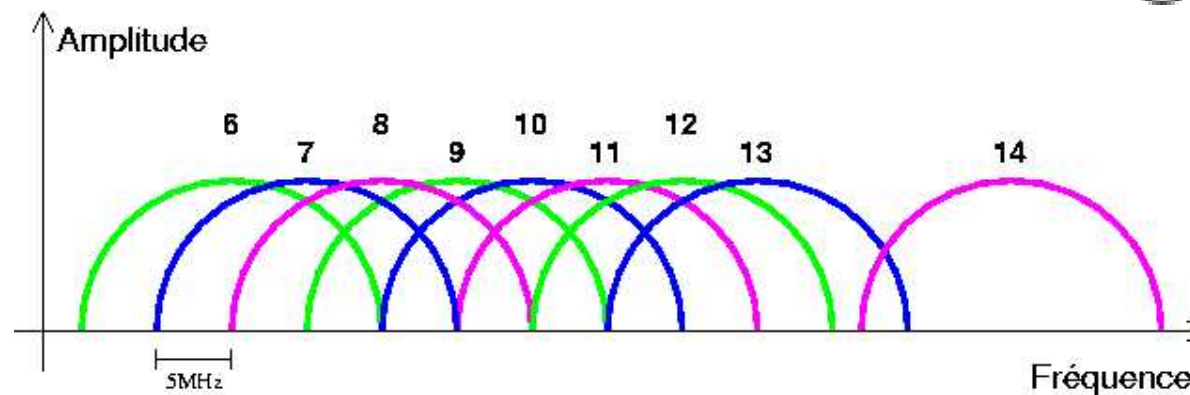
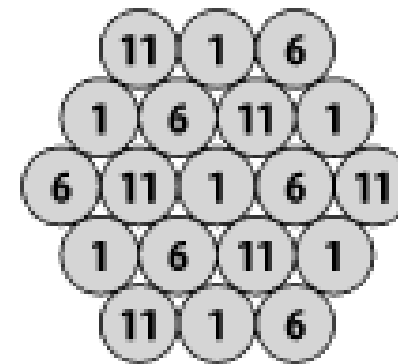
- Protocole verbeux

- Évitement des collisions CSMA/CA
- Gestion de la bande passante

Répartition du spectre

14 Canaux / 14 fréquences de porteuse

- Espacement de 5 Mhz entre les canaux
- Porteuse de 2412 Mhz à 2484 Mhz
 - Canal 14 et 13 espacé de 12 Mhz
 - Bande passante de 22Mhz
- Réglementation stricte en France



Détail de trames PrbReq

Frame 1 (36 bytes on wire, 36 bytes captured)
Arrival Time: Nov 8, 2002 09:39:28.343250000
Time delta from previous packet: 0.000000000 seconds
Time relative to first packet: 0.000000000 seconds
Frame Number: 1
Packet Length: 36 bytes
Capture Length: 36 bytes

IEEE 802.11

Type/Subtype: Probe Request (4)
Frame Control: 0x0040
Version: 0
Type: Management frame (0)
Subtype: 4
Flags: 0x0

Type de frame

DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 = PWR MGT: STA will stay up
..0. = More Data: No data buffered
.0.. = WEP flag: WEP is disabled
0... = Order flag: Not strictly ordered

Moyen de propagation

WEP activé ?

Duration: 0

Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

Source address: 00:40:96:33:90:f6 (00:40:96:33:90:f6)

BSS Id: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

Fragment number: 0

Sequence number: 288

MAC Adresses

IEEE 802.11 wireless LAN management frame

Tagged parameters (12 bytes)

Tag Number: 0 (SSID parameter set)

Tag length: 7

Tag interpretation: MonWlan

Tag Number: 1 (Supported Rates)

Tag length: 4

Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 [Mbit/sec]

SSID

Détail de trames *RTS/CTS*

Frame 60 (20 bytes on wire, 20 bytes captured)

IEEE 802.11

Type/Subtype: Request-to-send (27)

Frame Control: 0x00B4

Version: 0

Type: Control frame (1)

Subtype: 11

Flags: 0x0

DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)

.... .0.. = More Fragments: This is the last fragment

.... 0... = Retry: Frame is not being retransmitted

...0 = PWR MGT: STA will stay up

..0. = More Data: No data buffered

.0.. = WEP flag: WEP is disabled

0... = Order flag: Not strictly ordered

Duration: 698

Receiver address: 00:40:96:32:3f:f4 (00:40:96:32:3f:f4)

Transmitter address: 00:06:25:71:28:10 (00:06:25:71:28:10)

Frame 61 (14 bytes on wire, 14 bytes captured)

IEEE 802.11

Type/Subtype: Clear-to-send (28)

Frame Control: 0x00C4

Version: 0

Type: Control frame (1)

Subtype: 12

Flags: 0x0

DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)

.... .0.. = More Fragments: This is the last fragment

.... 0... = Retry: Frame is not being retransmitted

...0 = PWR MGT: STA will stay up

..0. = More Data: No data buffered

.0.. = WEP flag: WEP is disabled

0... = Order flag: Not strictly ordered

Duration: 485

Receiver address: 00:06:25:71:28:10 (00:06:25:71:28:10)

Détail de trame Beacon

Frame 1 (61 bytes on wire, 61 bytes captured)

IEEE 802.11

Type/Subtype: Beacon frame (8)

Frame Control: 0x0080

Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

Source address: 00:02:2d:02:05:b3 (00:02:2d:02:05:b3)

BSS Id: 00:02:2d:02:05:b3 (00:02:2d:02:05:b3)

Fragment number: 0

Sequence number: 496

Champ sur 12 bits

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Timestamp: 0x0000001D3F84B152

Beacon Interval: 0.102400 [Seconds]

Capability Information: 0x0001

Champ sur 64 bits

.... ..1 = ESS capabilities: Transmitter is an AP

.... ..0. = IBSS status: Transmitter belongs to a BSS

...0 = Privacy: AP/STA cannot support WEP

..0. = Short Preamble: Short preamble not allowed

.0.. = PBCC: PBCC modulation not allowed

0... = Channel Agility: Channel agility not in use

CFP participation capabilities: No point coordinator at AP (0x0000)

Tagged parameters (25 bytes)

Tag Number: 0 (SSID parameter set)

Tag length: 7

Tag interpretation: MonSSID

Tag Number: 1 (Supported Rates)

Tag length: 4

Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) [Mbit/sec]

Tag Number: 3 (DS Parameter set)

Tag length: 1

Tag interpretation: Current Channel: 3

Tag Number: 5 ((TIM) Traffic Indication Map)

Tag length: 4

Tag interpretation: DTIM count 0, DTIM period 1, Bitmap control 0x0, (Bitmap suppressed)

Bases de fonctionnement

- Environnement de compilation GCC 3.2 ou 2.97
- Entêtes du noyau Linux
- Linux Wlan-NG 0.1.15
 - Pilote Linux pour carte WLAN avec un chipset Prism/Intersil
 - <http://www.linux-wlan.org/>
 - Mozilla Public License
 - Évolution rapide, paramétrage très étendu (MIB complète)
 - Liste de diffusion dynamique
 - Intégré dans de multiples distributions
- libpcap 0.7.1
- Ethereal 0.8.x (libwiretap.a)
 - Sauvegarde du trafic en format pcap
- curses
 - Interface avec l'utilisateur
 - Bibliothèque optionnelle

Présentation de WifiScanner

- Outil d'audit et d'analyse de réseaux 802.11b
 - Chipset Prism avec pilote Wlan-NG sous Linux
 - <http://wifiscanner.sf.net/> ou <http://www.hsc.fr/outils/wifiscanner/>
- Licence GPL
- Affichage compact
- Interface curses temps réel
- Analyse d'anomalies
- Géolocalisation possible

```
WifiScanner v0.8.0 (Wlan driver version = 0.14) (c) 2002 Hervé Schauer Consultants (Jerome.Poggi@hsc-labs.com)
AP 00:06:2B:71:CB:11 (417,429)
STA 00:14:96:33:90:11 (0,243)

Summary
AP : 1
STA : 1
BEACON : 59
SSID : 0
Channel : 4
Invalid : 4
Dropped : 6
Weak : 0
Last IV: 20102122
Packets: 104

Scan
000000001111 1
1234567890123 4
IDS is OFF

Last Update 10:58:02
11/27/2002 10:58:00.821 *** 11_Mep_AP,114,000,FF:FF:FF:FF:FF:FF,00:06:2B:71:CB:11,2Mbps,AP Base (dedicated),Radio only,BEACON
11/27/2002 10:58:00.823 *** 00_Mep_AP,099,000,FF:FF:FF:FF:FF:FF,00:14:96:33:90:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:00.868 *** 00_Mep_AP,123,000,FF:FF:FF:FF:FF:FF,00:14:96:33:90:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:00.869 *** 00_Mep_STA,405,000,FF:FF:FF:FF:FF:FF,00:14:96:33:90:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:00.918 *** 00_Mep_STA,132,000,FF:FF:FF:FF:FF:FF,00:14:96:33:90:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:00.919 *** 00_Mep_STA,141,000,FF:FF:FF:FF:FF:FF,00:14:96:33:90:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:00.968 *** 00_Mep_STA,147,000,FF:FF:FF:FF:FF:FF,00:14:96:33:90:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:00.969 *** 00_Mep_STA,183,000,FF:FF:FF:FF:FF:FF,00:14:96:33:90:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:00.970 *** 00_Mep_STA,162,000,FF:FF:FF:FF:FF:FF,00:14:96:33:90:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:00.971 *** 00_Mep_AP,117,000,00:14:96:33:90:11,00:06:2B:71:CB:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:01.022 *** 00_Mep_STA,210,000,FF:FF:FF:FF:FF:FF,00:14:96:33:90:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:01.023 *** 00_Mep_AP,114,000,00:14:96:33:90:11,00:06:2B:71:CB:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:01.024 *** 00_STA,204,000,00:06:2B:71:CB:11,00:00:00:00:00:00,00:00:00:00:00:00,2Mbps,Client,Radio only,ACK
11/27/2002 10:58:01.068 *** 00_Mep_STA,240,000,FF:FF:FF:FF:FF:FF,00:14:96:33:90:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:01.069 *** 00_Mep_AP,117,000,00:14:96:33:90:11,00:06:2B:71:CB:11,2Mbps,Client,Radio only,PRBREQ
11/27/2002 10:58:01.070 *** 00_STA,240,000,00:06:2B:71:CB:11,00:00:00:00:00:00,00:00:00:00:00:00,2Mbps,Client,Radio only,ACK
11/27/2002 10:58:01.118 AUTHEN
11/27/2002 10:58:01.119 *** 00_STA,111,000,00:14:96:33:90:11,00:00:00:00:00:00,00:00:00:00:00:00,2Mbps,Client,Radio only,ACK
11/27/2002 10:58:01.120 *** 00_STA,240,000,00:06:2B:71:CB:11,00:00:00:00:00:00,00:00:00:00:00:00,2Mbps,Client,Radio only,ACK
11/27/2002 10:58:01.121 ASSREQ
11/27/2002 10:58:01.122 *** 00_STA,111,000,00:14:96:33:90:11,00:00:00:00:00:00,00:00:00:00:00:00,2Mbps,Client,Radio only,ACK
11/27/2002 10:58:01.122 ASSRES
11/27/2002 10:58:01.123 *** 00_STA,243,000,00:06:2B:71:CB:11,00:00:00:00:00:00,00:00:00:00:00:00,2Mbps,Client,Radio only,ACK
11/27/2002 10:58:01.668 *** 11_Mep_AP,117,000,FF:FF:FF:FF:FF:FF,00:06:2B:71:CB:11,2Mbps,AP Base (dedicated),Radio only,BEACON
11/27/2002 10:58:01.670 *** 00_Mep_STA,243,000,33:33:FF:33:90:11,00:14:96:33:90:11,2Mbps,STA Activity,Data To DS,DATA
11/27/2002 10:58:02.268 *** 11_Mep_AP,117,000,FF:FF:FF:FF:FF:FF,00:06:2B:71:CB:11,2Mbps,AP Base (dedicated),Radio only,BEACON
11/27/2002 10:58:02.269 *** 00_Mep_STA,114,000,33:33:FF:33:90:11,00:14:96:33:90:11,2Mbps,STA Activity,Data From DS,DATA
11/27/2002 10:58:02.571 *** 00_Mep_STA,240,000,00:06:2B:71:CB:11,00:00:00:00:00:00,00:00:00:00:00:00,2Mbps,Client,Radio only,ACK
11/27/2002 10:58:02.569 *** 00_STA,114,000,00:14:96:33:90:11,00:00:00:00:00:00,00:00:00:00:00:00,2Mbps,Client,Radio only,ACK
11/27/2002 10:58:02.570 *** 00_Mep_STA,114,000,00:14:96:33:90:11,00:06:2B:71:CB:11,2Mbps,STA Activity,Data From DS,DATA
11/27/2002 10:58:02.572 *** 00_Mep_STA,240,000,00:06:2B:71:CB:11,00:14:96:33:90:11,2Mbps,Client,Radio only,ACK
11/27/2002 10:58:02.573 *** 00_STA,114,000,00:14:96:33:90:11,00:00:00:00:00:00,00:00:00:00:00:00,2Mbps,Client,Radio only,ACK
11/27/2002 10:58:02.668 *** 00_Mep_STA,243,000,33:33:FF:33:90:11,00:14:96:33:90:11,2Mbps,STA Activity,Data To DS,DATA
11/27/2002 10:58:02.669 *** 00_STA,114,000,00:14:96:33:90:11,00:00:00:00:00:00,00:00:00:00:00:00,2Mbps,Client,Radio only,ACK
11/27/2002 10:58:02.768 *** 11_Mep_AP,117,000,FF:FF:FF:FF:FF:FF,00:06:2B:71:CB:11,2Mbps,AP Base (dedicated),Radio only,BEACON
```



Pourquoi WifiScanner ?

- Nécessité de pouvoir ajouter des options
- Besoins spécifiques
 - Données en temps réel
 - Signal de réception pour géolocalisation
 - Sauvegarde du trafic pour étude plus poussée
 - Affichage du type de client
 - Découverte de SSID
 - Détection d'anomalies et de pièges à *Wardriver*
- Découverte et étude du protocole

Méthodes de détection

- Détection d'équipements
 - Passif
 - Kismet, WifiScanner
 - Silencieuse, discrète, quasi indétectable
 - Actif
 - Netstumbler, Dstumbler
 - Bruyant, peu discret, détectable
 - Hybride ou Réactif
 - Outils commerciaux

Méthode d'analyse

- Écoute sur un canal unique ou sur les 14 canaux alternativement
- Étude de quasiment tous les champs 802.11b
- Corrélation / regroupement d'informations
- Récupération d'informations dans les champs non documentés des constructeurs
- Recherche des anomalies
- Rapport en fin d'exécution

Détection des autres renifleurs

- Détection de signature
- Netstumbler
 - Détection active (envoi de *ProbeRequest*)
 - Organisation fixe
 - Filtre Ethereal

```
((wlan.fc.type_subtype eq 32) and (llc.oui eq 0x00601d) and (llc.pid eq 0x0001)) and  
(data[4:4] eq 41:6c:6c:20 or data[4:4] eq 6c:46:72:75 or data[4:4] eq 20:20:20:20)
```

- Trames de données avec un contenu identifiable

Version	Contenu
3.2.0	<i>Flurble gronk bloopit, bnip Frundletrune</i>
3.2.3	<i>All your 802.11b are belong to us</i>
3.3.0	intentionnelement vide (suite d'espaces)

Détection des autres renifleurs

- DS tumbler (*BSD)
 - Détection active ou passive
 - Numéro de séquence faible (modulo 12)
 - Trames d'authentification
 - Numéro de séquence à 0x0B
 - Trames d'association
 - Numéro de séquence à 0x0C
 - Filtre Ethereal

```
(wlan.seq eq 11 and wlan.fc.subtype eq 11) or  
(wlan.seq eq 12 and wlan.fc.subtype eq 00)
```

Détection des autres renifleurs

- Wellenreiter
 - Renifleur en perl
 - Envoi de trames *ProbeRequest* avec un SSID identifiable

```
IEEE 802.11
  Type/Subtype: Probe Request (4) Frame Control: 0x0040
IEEE 802.11 wireless LAN management frame
  Tagged parameters (37 bytes)
    Tag Number: 0 (SSID parameter set)
    Tag length: 29
    Tag interpretation: this_is_used_for_wellenreiter
    Tag Number: 1 (Supported Rates)
    Tag length: 4
    Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 [Mbit/sec]

0000 40 00 00 00 ff ff ff ff ff ff 00 40 96 47 e2 7d @.....@.G.}
0010 ff ff ff ff ff ff 90 f0 00 1d 74 68 69 73 5f 69 .....this_i
0020 73 5f 75 73 65 64 5f 66 6f 72 5f 77 65 6c 6c 65 s_used_for_welle
0030 6e 72 65 69 74 65 72 01 04 02 04 0b 16 ff ff ff nreiter.....
0040 ff .
```

- Filtre Ethereal

```
(wlan.fc eq 0x0040) and (wlan_mgt.tag.number eq 0) and (wlan_mgt.tag.length eq 29) and
(wlan_mgt.tag.interpretation eq this_is_used_for Wellenreiter)
```

Détection de Windows XP

- Détection de réseaux sans fil
 - Pour s'y connecter et pour en faire la liste
- Détection active
 - Envoi de trames *ProbeRequest* avec un SSID identifiable

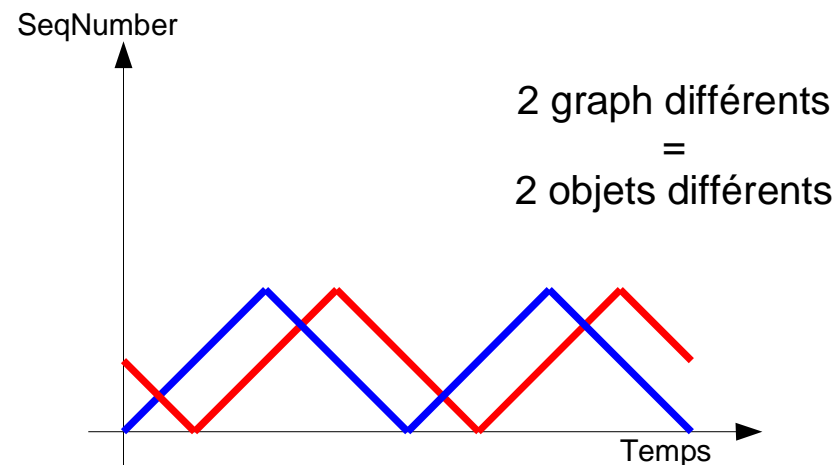
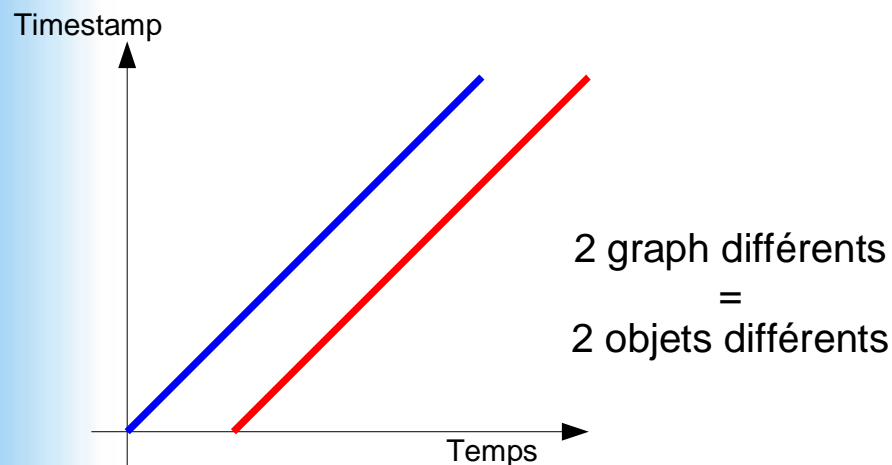
```
IEEE 802.11
Type/Subtype: Probe Request (4)
Frame Control: 0x0040 Version: 0
IEEE 802.11 wireless LAN management frame
Tagged parameters (40 bytes)
  Tag Number: 0 (SSID parameter set)
  Tag length: 32
  Tag interpretation: \024\t\003\021\004\021\t\016\r\n\016\031\002\027\031\002\024\037\a\004\005
\023\022\026\026\n\001\n\016\037\034\022
  Tag Number: 1 (Supported Rates)
  Tag length: 4
  Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 [Mbit/sec]
```

- Filtre Ethereal

```
(wlan.fc eq 0x0040) and (wlan_mgt.tag.number eq 0) and (wlan_mgt.tag.length eq 32) and
(wlan_mgt.tag.interpretation[0:4] eq 0c:15:0f:03)
```

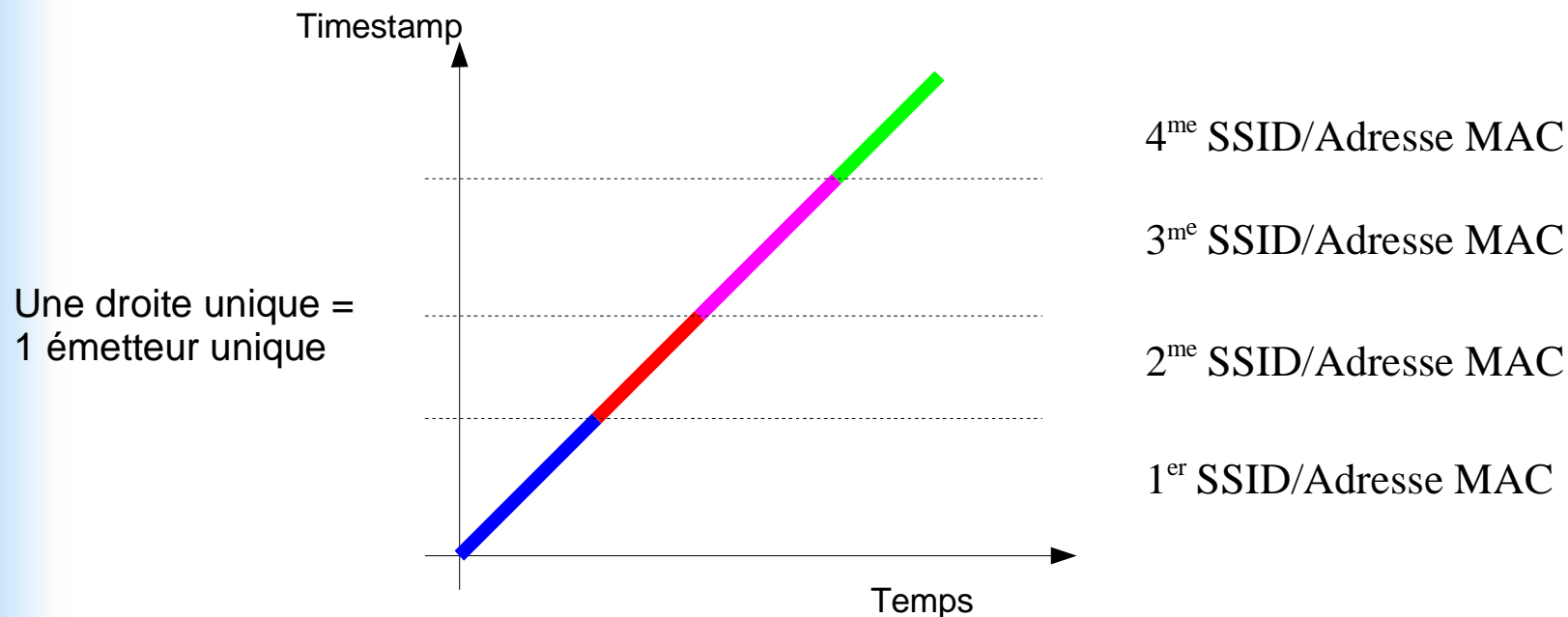
Détection des fausse bornes

- L'usurpation d'adresse MAC est possible
- La détection de cette usurpation est possible
 - Étude de la variation des champs
 - *Timestamp*
 - *Sequence number*



Détection des « pièges à *wardriver* »

- Inondation de *beacons* de fausses bornes
 - Adresse MAC changée périodiquement
 - SSID variable
 - Champ *timestamp* linéaire = *uptime* de la carte



Découverte du SSID caché

Frame 58 (46 bytes on wire, 46 bytes captured)

IEEE 802.11

Type/Subtype: Probe Request (4)

IEEE 802.11 wireless LAN management frame

Tagged parameters (22 bytes)

Tag Number: 0 (SSID parameter set)

Tag length: 12

Tag interpretation: MonSSIDcaché

Frame 59 (61 bytes on wire, 61 bytes captured)

IEEE 802.11

Type/Subtype: Probe Response (5)

Frame Control: 0x0050

Flags: 0x0

DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)

Destination address: 00:40:96:32:3f:f4 (00:40:96:32:3f:f4)

Source address: 00:06:25:71:28:10 (00:06:25:71:28:10)

BSS Id: 00:06:25:71:28:10 (00:06:25:71:28:10)

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Timestamp: 0x0000008EDD578883

Beacon Interval: 0.512000 [Seconds]

Capability Information: 0x0011

.... ...1 = ESS capabilities: Transmitter is an AP

...1 = Privacy: AP/STA can support WEP

Tagged parameters (25 bytes)

Tag Number: 0 (SSID parameter set)

Tag length: 12

Tag interpretation: MonSSIDCaché

Tag Number: 1 (Supported Rates)

Tag length: 4

Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) [Mbit/sec]

Tag Number: 3 (DS Parameter set)

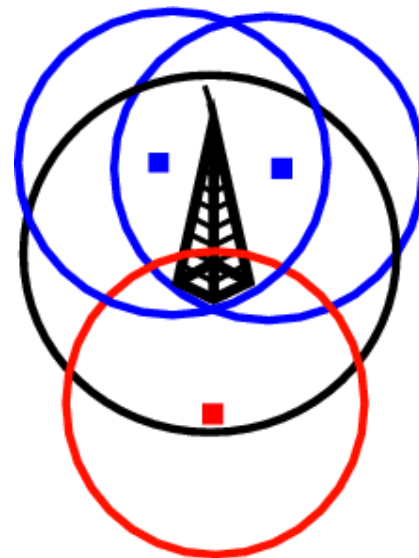
Tag length: 1

Tag interpretation: Current Channel: 11

Détection en aveugle

- Attention à la détection en aveugle
 - Équipements détectés hors de portée radio
 - Détectés par l'intermédiaire d'un équipement tiers
 - Analyse des trames 802.11b

client -> borne
borne -> client
-> attaquant



■ Attaquant
■ Client

Démonstration

Ce qu'il reste à faire

- Rendre le programme multi-thread
- Faire un niveau d'abstraction matériel, pour une meilleur portabilité
- Mettre en application les théories de détection de « piège à *wardriver* »
- Améliorer le module d'analyse d'anomalies
- Permettre de tout sauvegarder
 - *Keystream*, alertes, ...
- Pouvoir s'interfacer avec Snort et/ou Prelude
- Pouvoir filtrer avec des expressions BPF (*Berkeley Packet Filter*)
- Ajouter un horodatage aux détections
- Pouvoir changer la vitesse de parcours des canaux
- Donner le nom du constructeur de chaque équipement trouvé (base OUI de l'IEEE)
- Supprimer les bugs restants

Merci