

Universidade do Minho  
Mestrado em Engenharia Informática  
Tecnologias e Protocolos de Infraestrutura



Universidade do Minho

## **Redes de Comunicações sem Fios e Móveis**

Ano Lectivo de 2008/2009

# **WifiSig Utilitário de Recolha de Assinaturas Wireless**

José Pedro Vilaça Novais  
Miguel Craveiro Martins de Almeida

22 de Janeiro de 2009

# Conteúdo

<b>Conteúdo</b>	<b>i</b>
<b>1 Resumo do WifiSig</b>	<b>1</b>
<b>2 Desenvolvimento e Funcionamento</b>	<b>2</b>
2.1 Cliente . . . . .	2
2.1.1 Utilização das ferramentas de <b>scanning</b> . . . . .	2
2.1.2 Envio dos dados para o servidor . . . . .	2
2.2 Servidor . . . . .	3
2.2.1 Tecnologia . . . . .	3
2.2.2 Recepção da informação . . . . .	3
2.2.3 Registo dos dados . . . . .	4
2.2.4 Criação do grafo . . . . .	4
Adjacências . . . . .	4
Pontos de acesso . . . . .	5
Descrições dos pontos de acesso . . . . .	5
Coloração do grafo . . . . .	6
2.2.5 Adjacência das redes . . . . .	6
2.2.6 Análise de interferência . . . . .	6
Cor das adjacências . . . . .	7
Cor dos pontos de acesso . . . . .	7
Eleição do melhor canal . . . . .	8
<b>Bibliografia</b>	<b>9</b>

# Capítulo 1

## Resumo do WifiSig

No âmbito do módulo de **Redes de Comunicações sem Fios e Móveis** da UCE de **Tecnologias e Protocolos de Infraestrutura**, foi desenvolvido um pequeno sistema de recolha cooperativa de assinaturas wireless, com o objectivo de dar a conhecer eventuais interferências de sinais rádio dos pontos de acesso Wi-Fi 802.11. A análise do ambiente rádio deverá ser feita automaticamente por vários computadores portáteis, que enviarão periodicamente a informação recolhida para um servidor central. Perante tal informação, é ainda elegido qual o melhor canal para um ponto de acesso operar.

## Capítulo 2

# Desenvolvimento e Funcionamento

O WifiSig conta com o apoio de vários computadores equipados com placas de rede sem fios (IEEE 802.11), que deverão recolher o máximo de informação possível sobre o ambiente rádio Wi-Fi que o rodeia. Deste modo, e havendo ligação à *Internet* em cada um deles, será então possível centralizar todos esses dados para posterior análise. De modo a que o cliente WifiSig instalado nos computadores consiga comunicar com o servidor central em qualquer lugar, a comunicação é feita através ligações HTTP.

Será então disponibilizada uma página *web* onde será possível identificar as adjacências das redes encontradas, tal como a eventual existência de interferência das redes vizinhas, assinalada com vários níveis de cor desde o verde (sem qualquer interferência) ao vermelho (eventualmente muita interferência).

### 2.1 Cliente

Esta aplicação é escrita em C e será responsável pelo trabalho de análise do ambiente rádio que rodeia os computadores cliente. Periodicamente<sup>1</sup> é feito um *scan* que recolherá o máximo de informação possível sobre os pontos de acesso ao seu alcance: BSSID, SSID, canal, sinal e ruído.

#### 2.1.1 Utilização das ferramentas de scanning

Os *scans* são feitos com o apoio de ferramentas que o sistema operativo disponibiliza (*airport*, *iwlist*, etc). No entanto é preciso que o WifiSig saiba "comunicar" com elas de forma correcta. Tendo a noção de que estas ferramentas podem sofrer alterações com o tempo e de que variam de sistema para sistema, o *parser* foi feito em *flex*, tornando-se muito acessível a sua adaptação.

#### 2.1.2 Envio dos dados para o servidor

A informação é enviada para o servidor via HTTP, tal como descrito em pormenor na secção 2.2.2. Para que o cliente WifiSig não tenha qualquer tipo de configurações, a utilização do *proxy* é feita de forma automática, recorrendo-se à variável de *environment* `http_proxy` do sistema.

---

<sup>1</sup>Por omissão este tempo está definido para 10 minutos, apesar de ser possível utilizar outro tempo escolhido pelo utilizador, bastando para isso executar o programa com o parâmetro do tempo, sem segundos. Ex: Fazer *scan* de minuto a minuto: `$ ./wifisig 60`

## 2.2 Servidor

A componente "servidor" deste sistema é na verdade um conjunto de aplicações em sintonia, capazes de reunir a informação recolhida pelos clientes e processá-la de forma útil e sempre disponível num site disponível na *web* - através do endereço <http://wifisig.guecks.com/>.

### 2.2.1 Tecnologia

São utilizadas as seguintes aplicações e servidores:

- Apache 2.0 com interpretador PHP 5.0 e CGI,
- CGI interpretadora de ficheiros GraphViz (.dot) - módulo Webdot,
- Servidor MySQL 5.0.

### 2.2.2 Recepção da informação

Por forma a ser possível utilizar o cliente WifiSig em qualquer lugar com ligação à Internet, a troca de informação entre o cliente e servidor é também feita via HTTP, através de um ficheiro `newscan.php` (publicamente disponível em <http://wifisig.guecks.com/newscan.php>). Este ficheiro espera receber a informação sobre as várias estações (identificadas por um número a começar em 0) através de variáveis HTTP do tipo GET.

Assumindo, a título de exemplo, um *scan* feito pelo cliente com o endereço MAC `00:1e:c2:b8:f0:31`, onde foram encontradas duas estações: uma sem SSID e outra com **eduroam**. Então, os dados recolhidos:

```
macUser: 00:1e:c2:b8:f0:31
ssid0:   eduroam
bssid0:  00:11:22:33:44:55
rssi0:   -64
noise0:  -98
channel0: 6
ssid1:   n/a
bssid1:  00:11:22:33:44:55
rssi1:   -47
noise1:  -97
channel1: 1
```

serão convertidos no seguinte endereço:

```
http://msc.guecks.com/wifisig/newscan.php?macUser=00:1e:c2:b8:f0:31&
&ssid0=eduroam\&bssid0=00:11:22:33:44:55&rssi0=-64&noise0=-98&channel0=6&
&ssid1=&bssid1=00:11:22:33:44:55&rssi1=-47&noise1=-97&channel1=1
```

Então, o *script* PHP no servidor deverá registar nas tabelas MySQL todos esses dados, para que possam mais tarde ser utilizados na geração do grafo.

### 2.2.3 Registo dos dados

A informação recolhida dos clientes é armazenada num base de dados MySQL. A sua estrutura é simples, feita de modo a facilitar o trabalho de geração do grafo, de acordo com a figura 2.1.

- **scans:** Nesta tabela cada *scan* periódico feito pelos clientes é identificado por um *idScan*. É também armazenado o endereço MAC do utilizador que o efectuou, para fins de *debugging*.
- **bssidScans:** Aqui são armazenados os dados relativos a cada uma das estações encontradas: BSSID, SSID, sinal, ruído e canal, sempre associados a um determinado *scan*.
- **bssids:** Esta tabela permite associar um nome a uma determinada estação através da sua BSSID. Isto facilita a identificação de pontos de acesso com o mesmo nome.

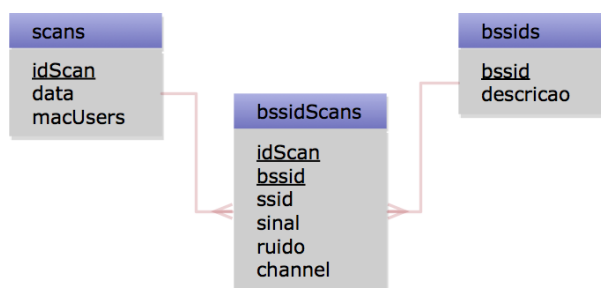


Figura 2.1: Diagrama E-R da base de dados que armazena os pontos de acesso encontrados.

### 2.2.4 Criação do grafo

Periodicamente<sup>2</sup>, é executado o script `gendot` (escrito em PHP) que gera o ficheiro `wifisig.dot` que será posteriormente fornecido ao `Webdot` sempre que um cliente o solicitar. Desta forma, o grafo encontra-se sempre disponível para visualização em qualquer formato (no site, é usado o PNG). Excepcionalmente, de cada vez que um utilizador atribuiu ou modifica a descrição de um ponto de acesso (secção 2.2.4), o grafo é também recalculado, para que se torne imediatamente visível a alteração feita.

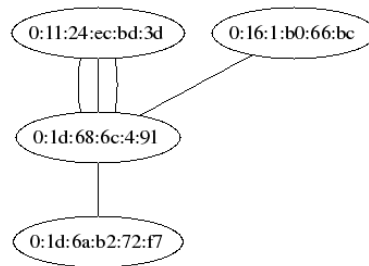
#### Adjacências

Com a ajuda do `Webdot/GraphViz` torna-se mais fácil a geração do grafo, pois este utilitário consegue uma distribuição equilibrada dos nodos no espaço, em função das suas adjacências. O formato `Webdot` espera receber as ligações entre os nodos no formato `nodoA - nodoB`.

Um excerto do `.dot` gerado poderá então ser o seguinte, que irá gerar o grafo da Fig. 2.2:

```
graph G {
  "0:11:24:ec:bd:3d" -- "0:1d:68:6c:4:91";
  "0:11:24:ec:bd:3d" -- "0:1d:68:6c:4:91";
  "0:11:24:ec:bd:3d" -- "0:1d:68:6c:4:91";
  "0:16:1:b0:66:bc" -- "0:1d:68:6c:4:91";
  "0:1d:68:6c:4:91" -- "0:1d:6a:b2:72:f7";
}
```

<sup>2</sup>Este trabalho é feito pela `crontab` do `Linux`, de 3 em 3 minutos



**Figura 2.2:** Exemplo de um grafo simples, sem qualquer otimização.

Tal como acontece neste exemplo, poderá haver um excesso de informação relativamente a algumas estações, quando um cliente efectua muitos *scans* num determinado local. Torna-se então necessário prever estes casos, evitando que sejam desenhadas várias arejas repetidas no grafo. Para evitar esta situação, em cada adjacência as **ssid** são ordenadas da menor para a maior (tornado, por exemplo **bb--aa** em **aa--bb**) e então marcadas com uma flag, para que não sejam repetidas mais tarde.

### Pontos de acesso

A identificação das adjacências é suficiente para a geração do grafo. No entanto, tal como se pode verificar na Fig. 2.2, não se torna intuitivo identificar os pontos de acesso pela sua **BSSID**. Atribui-se então uma etiqueta com a sua **SSID**, quando existe essa informação. Apesar desta melhoria, por vezes ainda se torna difícil identificar os pontos de acesso quando existem vários com a mesma **SSID**, como é o caso da nossa universidade. Para resolver este problema, permite-se que os utilizadores do WifiSig possam associar uma pequena descrição a cada estação - processo descrito na subsecção abaixo - mostrando-a entre parêntesis como no exemplo seguinte:

```
graph G {
  ...
  "0:11:24:ec:bd:3d" [label="eduroam\n(labcom)"]
}
```

### Descrições dos pontos de acesso

O módulo **Webdot** permite identificar a zona *clickable* de uma imagem num site, através de *maps* HTML. Assim, permite-se que o utilizador defina uma descrição com facilidade, simplesmente carregando no ponto de acesso na imagem que vê. É então apresentado um pequeno formulário para este propósito, como se vê na Fig. 2.3.

**Figura 2.3:** Formulário de atribuição de descrição a um ponto de acesso.

## Coloração do grafo

É possível ainda definir a cor dos nodos e das adjacências, simplesmente precedendo com `[color="#<código-hex-da-cor>"]`. A referência hexadecimal permite os canais RGB e ainda um canal `alpha`, útil para tornar mais agradável a visualização do grafo. A coloração dos pontos de acesso e das adjacências é feita de acordo com critérios descritos na secção 2.2.6.

O resultado da atribuição de cores aos exemplos acima, gera o grafo da Fig. 2.4 a partir do seguinte ficheiro `.dot`:

```
graph TD
  node [style=filled, truecolor]
  edge [truecolor]
  edge [color="#dedede"] "0:11:24:ec:bd:3d" -- "0:1d:68:6c:4:91";
  edge [color="#ff0000"] "0:16:1:b0:66:bc" -- "0:1d:68:6c:4:91";
  edge [color="#00ff00"] "0:1d:68:6c:4:91" -- "0:1d:6a:b2:72:f7";
  "0:11:24:ec:bd:3d" [fillcolor="#ffb501f", label="eduroam\n(labcom)"];
  "0:1d:6a:b2:72:f7" [fillcolor="#00ff01f"];
}
```

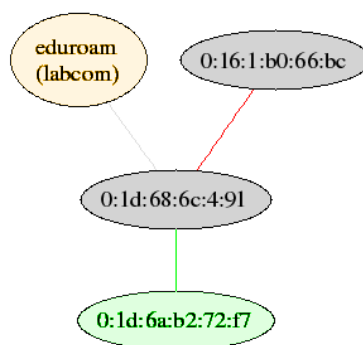


Figura 2.4: Exemplo de um grafo colorido.

### 2.2.5 Adjacência das redes

Quando um cliente efectua um *scan* e encontra mais do que uma rede, assume-se que essas redes se encontram fisicamente próximas uma da outra e por isso são consideradas adjacentes<sup>3</sup>.

### 2.2.6 Análise de interferência

A norma 802.11 divide os 2401-2483 MHz que tem disponíveis em vários canais de 22 MHz cada [1], para que seja possível a co-existência de vários pontos de acesso num mesmo local. No entanto, essa faixa é demasiado estreita para tantos canais e torna-se por isso impossível que nenhum se sobreponha. São então espaços de 5 em 5 MHz, de acordo com a figura 2.5, permitindo que pelo menos os canais 1, 6 e 11 sejam completamente separados.

<sup>3</sup>É importante ter-se em conta que os clientes WifiSig que analisam o ambiente rádio não deverão ser utilizados em computadores com interfaces de rádio com mais de 100mW nem utilizados amplificadores ou antenas externas, pois seriam assumidas adjacências que na realidade não existiam.

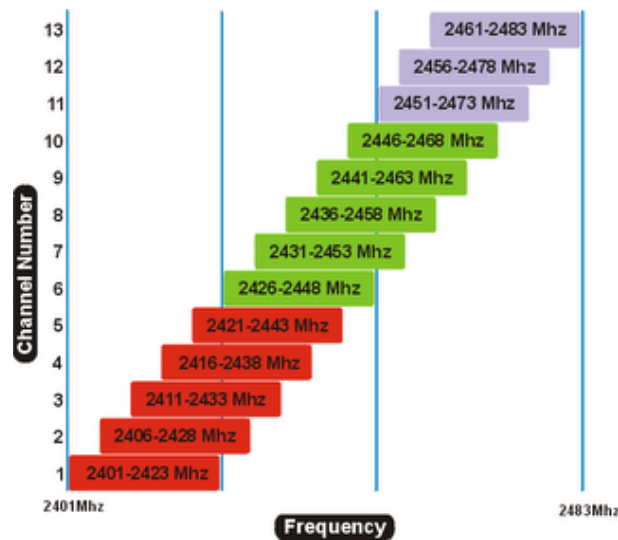


Figura 2.5: Gráfico ilustrativo da provável existência de interferências. [2]

### Cor das adjacências

Quando dois pontos de acesso se encontram num mesmo canal, é assumida interferência máxima nessa adjacência. Conforme os canais vão sendo mais afastados, menor será a probabilidade de interferência, até não haver nenhuma (quando existe uma diferença de 5 canais entre os dois). É este o critério que é tido em conta ao atribuir os 6 níveis de cor possíveis (ver Fig. 2.6):

- sobreposição dos canais: #ff0000 (vermelho)
- diferença de 1 canal: #fa6c2b (laranja escuro)
- diferença de 2 canais: #ff9500 (laranja claro)
- diferença de 3 canais: #ffb500 (amarelo escuro)
- diferença de 4 canais: #ffd300 (amarelo claro)
- não há sobreposição de canais: #00ff00 (verde)

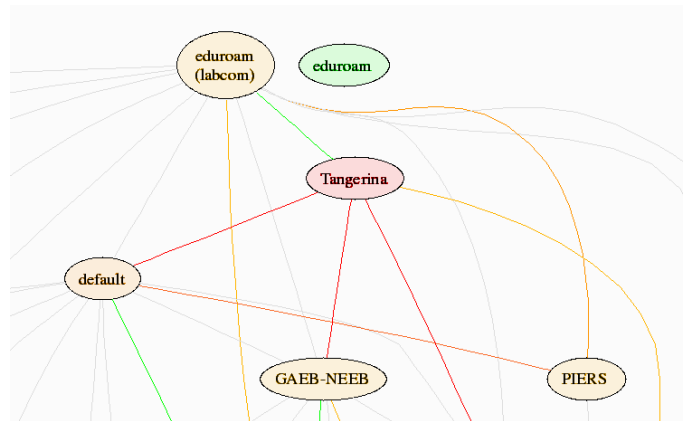
Foi reservada ainda a cor cinzenta (#dedede) para casos em que haja, por algum motivo, falta de informação sobre os canais.

### Cor dos pontos de acesso

Também é útil identificar os pontos de acesso com probabilidade de interferência, se forem identificados por uma cor. É então feito um cálculo análogo ao anterior (e com os mesmos níveis de cor) a fim de escolher a cor mais adequada para o ponto de acesso.

A cada ponto de acesso é **atribuído um peso** da eventual interferência, em função da diferença do seu canal e de cada um dos seus adjacentes<sup>4</sup>. O factor de sensibilidade desta escolha é configurável, mas é aconselhável utilizá-lo com o valor 3, ou seja, desde o verde ao vermelho, o salto entre cada cor é de 3 níveis de interferência: 0 (verde), 1, 4, 7, 10 e 13 (vermelho), como se pode verificar na Fig. 2.6.

<sup>4</sup>Note-se que neste cálculo apenas é tido em conta o último *scan* que encontrou um determinado ponto de acesso, pois o canal é um valor que pode mudar com muita frequência, especialmente quando é utilizado hardware que se adapta automaticamente ao meio



**Figura 2.6:** Exemplo de coloração dos pontos de acesso em função da presença de interferência.

### Eleição do melhor canal



**Figura 2.7:** Eleição do melhor canal de um ponto de acesso.

Para cada ponto de acesso é calculado qual o melhor canal, em função das redes adjacentes. A cada um dos 11 canais é atribuído um peso (de 0 a 5, de acordo com a Fig. 2.5), segundo os seguintes critérios:

- a cada canal onde se encontre um vizinho ( $i$ ) é atribuído o peso 5;
- aos canais imediatamente acima ( $i+1$ ) e abaixo ( $i-1$ ) é atribuído o peso 4;
- aos canais imediatamente acima ( $i+2$ ) e abaixo ( $i-2$ ) do anterior é atribuído o peso 3;
- aos canais imediatamente acima ( $i+3$ ) e abaixo ( $i-3$ ) do anterior é atribuído o peso 3;
- aos canais imediatamente acima ( $i+4$ ) e abaixo ( $i-4$ ) do anterior é atribuído o peso 2;
- aos canais imediatamente acima ( $i+5$ ) e abaixo ( $i-5$ ) do anterior é atribuído o peso 1;
- todos estes pesos são somados, atribuindo-se um peso final ao canal em questão;
- qualquer canal com peso 0 pode ser elegido como melhor canal e por isso é escolhido o que tiver valor absoluto mais baixo;
- caso o canal onde o ponto de acesso opera esteja completamente livre, o canal elegido é o próprio canal.

No final, simplesmente é elegido o canal mais leve: O número do melhor canal é indicado no ponto de acesso, tal como se vê na Fig. 2.7.

# Bibliografia

- [1] <http://en.wikipedia.org/wiki/802.11>.
- [2] [http://www.dd-wrt.com/wiki/index.php/lafonera\\_software\\_chilispot](http://www.dd-wrt.com/wiki/index.php/lafonera_software_chilispot).