

# Lokalizator użytkowników sieci WiFi

6 kwietnia 2017

Maciej Michalak	121992	maciej.k.michalak@student.put.poznan.pl
Patryk Masiakowski	116285	patryk.masiakowski@student.put.poznan.pl
Jakub Kostrzewski	122039	jakub.k.kostrzewski@student.put.poznan.pl

## Spis treści

<b>1</b>	<b>Wstęp</b>	<b>2</b>
1.1	Opis aplikacji . . . . .	2
<b>2</b>	<b>Działanie</b>	<b>2</b>
2.1	Trilateracja . . . . .	2
2.2	SSID i BSSID . . . . .	3
2.3	RSSI . . . . .	4
2.4	Aplikacja kliencka . . . . .	4
2.5	Harmonogram prac . . . . .	5
<b>3</b>	<b>Funkcje-klient</b>	<b>5</b>
<b>4</b>	<b>Funkcje-serwer</b>	<b>5</b>

# 1 Wstęp

## 1.1 Opis aplikacji

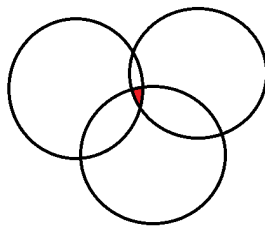
Celem projektu jest stworzenie aplikacji pozwalającej na określenie lokalizacji użytkownika sieci względem trzech urządzeń AP. System powinien przeskanować sieć w poszukiwaniu klientów podłączonych do punktów dostępowych. Użytkownik będzie mieć możliwość podejrzenia podstawowych informacji o każdym gościu w sieci, takiej jak nr. ip czy adres MAC. Do określenia względnej lokalizacji w sieci wykorzystana zostanie technika trilateracji. Aplikacja działa na zasadzie serwera interpretującego dane przesłane przez klientów. Klienci powinni znaleźć w swoim otoczeniu trzy punkty dostępowe, które mają względem nich określoną siłę sygnału. Dane o tych sygnałach zostają przesyłane do serwera i interpretowane. W czasie rzeczywistym podawana jest lokalizacja danego klienta. Wymogiem jest wcześniejsze zarejestrowanie danego urządzenia w systemie.

# 2 Działanie

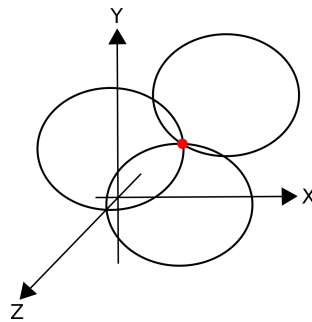
## 2.1 Trilateracja

Jest to metoda określania położenia obiektu w trójwymiarowej przestrzeni (w tym wypadku budynku). By metoda ta była skuteczna wymagana jest znajomość położenia trzech punktów dostępowych (AP). Znając odległości każdego punktu dostępowego od lokalizowanego urządzenia oraz współrzędne tych punktów można określić lokalizację urządzenia.

Każdą odległość AP od lokalizowanego urządzenia można przedstawić w przestrzeni jako sferę. Wyznaczenie współrzędnych klienta sprowadza się do znalezienia miejsca przecięcia trzech sfer, każdej związanej z AP.



Rysunek 1: sfery wyznaczone przez siłę sygnału AP

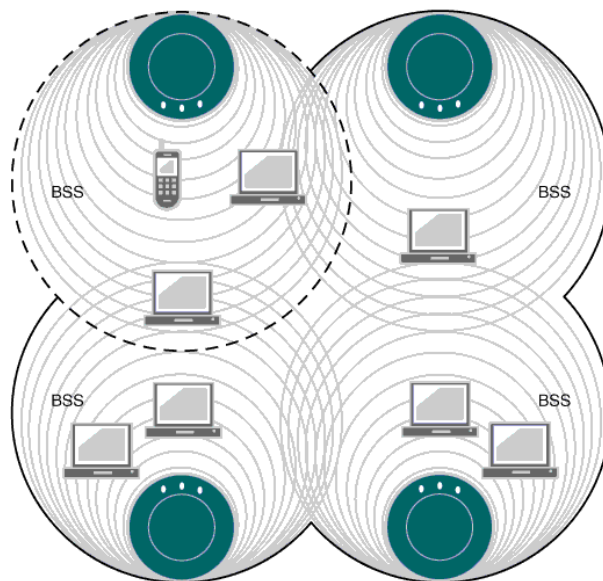


Rysunek 2: przykładowe działanie airodump-ng

## 2.2 SSID i BSSID

Początkowym etapem działania aplikacji będzie lokalizowanie pobliskich punktów dostępowych i ich identyfikacja na podstawie 48-bitowego numeru identyfikacyjnego BSSID czyli numeru MAC AP oraz identyfikatora SSID.

$$\text{BSS} + \text{BSS} + \text{BSS} + \text{BSS} = \text{ESS}$$



BSSID = AP MAC address  
SSID = name of network

g041300

Rysunek 3: BSSID i ESSID

```
Administrator: Wiersz polecenia - netsh
netsh>wlan show networks mode=Bssid

Interface name : Wi-Fi
There are 5 networks currently visible.

SSID 1 : eduroam
Network type      : Infrastructure
Authentication    : WPA2-Enterprise
Encryption        : CCMP
BSSID 1           : 00:04:96:68:62:e1
Signal           : 33%
Radio type       : 802.11n
Channel          : 13
Basic rates (Mbps) : 12 24
Other rates (Mbps) : 18 36 48 54
BSSID 2          : 00:23:68:30:bf:71
Signal           : 46%
Radio type       : 802.11n
Channel          : 1
Basic rates (Mbps) : 12 24
Other rates (Mbps) : 18 36 48 54
BSSID 3          : 00:04:96:68:59:f1
Signal           : 30%
Radio type       : 802.11n
Channel          : 7
Basic rates (Mbps) : 12 24
Other rates (Mbps) : 18 36 48 54
BSSID 4          : 00:04:96:68:55:f1
Signal           : 45%
Radio type       : 802.11n
Channel          : 1
Basic rates (Mbps) : 12 24
Other rates (Mbps) : 18 36 48 54
BSSID 5          : 00:04:96:68:55:61
Signal           : 99%
Radio type       : 802.11n
Channel          : 13
Basic rates (Mbps) : 24 156
Other rates (Mbps) : 18 36 48 54
BSSID 6          : 00:23:68:2f:d7:11
Signal           : 35%
Radio type       : 802.11n
Channel          : 1
Basic rates (Mbps) : 12 24
Other rates (Mbps) : 18 36 48 54

SSID 2 : PUT-events-WiFi
Network type      : Infrastructure
Authentication    : Open
Encryption        : None
BSSID 1           : 00:04:96:68:55:60
Signal           : 96%
Radio type       : 802.11n
Channel          : 13
Basic rates (Mbps) : 12 24
Other rates (Mbps) : 18 36 48 54
BSSID 2           : 00:04:96:68:55:f0
```

Rysunek 4: listowanie dostępnych essid

## 2.3 RSSI

RSSI jest wskaźnikiem mocy sygnału nadawanego przez dany punkt dostępowy. Wykorzystując wartości tego wskaźnika, możliwe jest określenie odległości lokalizowanego urządzenia od punktu dostępowego.

## 2.4 Aplikacja kliencka

Aplikacja kliencka będzie pisana pod urządzenia mobilne. Jej zadanie jest bardzo proste: Przesłać do serwera RSSI trzech dostępnych AP z jednej sieci o największych sygnałach. Gdy dostęp istnieje tylko do mniej niż trzech punktów dostępowych, lokalizacja określana jest na podstawie dostępnych dwóch punktów lub nawet tylko jednego(w tym wybadku jesteśmy w stanie określić tylko

promień w jakim znajdują się użytkownik). Na większych przestrzeniach w budynkach, nie ma jednak problemu ze znalezieniem przynajmniej trzech punktów dostępowych.

```
CH 9 ][ Elapsed: 16 s ][ 2013-10-04 12:12
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
54:78:1A:73:88:20	-50	29	0	0	11	54e.	WPA2	CCMP	MGT flashzone-seamless
54:78:1A:73:88:24	-50	23	0	0	11	54e.	OPN		Speedy Instan@wifi
54:78:1A:73:88:21	-50	19	0	0	11	54e.	OPN		FlexiZone
54:78:1A:73:88:22	-61	28	661	88	11	54e.	OPN		@wifi.id
54:78:1A:73:88:23	-50	18	0	0	11	54e.	OPN		Flash Zone
00:0C:42:FB:D2:C1	-65	27	0	0	1	54e.	WPA2	CCMP	PSK ENJOY CAFE 2
F4:EC:38:A4:1C:E2	-72	35	0	0	4	54e.	WPA2	CCMP	PSK ENJOY CAFE 1

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	50:B7:C3:3B:FC:0E	0	0 - 1	0	11	
54:78:1A:73:88:22	74:DE:2B:13:42:5E	-1	2e- 0	0	215	
54:78:1A:73:88:22	CC:52:AF:57:E5:88	-127	0e- 0e	362	448	

Rysunek 5: przykładowe działanie airodump-ng

## 2.5 Harmonogram prac

- przedstawięcie wstępnego projektu,
- stworzenie interfejsu graficznego,
- zaprogramowanie modułu odpowiedzialnego za czytanie i interpretację danych z urządzeń sieciowych,
- zaprogramowanie modułu odpowiedzialnego za rysowanie danych na układzie współrzędnych,
- testy aplikacji.

## 3 Funkcje-klient

- wyszukiwanie dostępnych AP po BSSID,
- pobieranie danych o sygnale względem każdego BSSID,
- wysyłanie danych do serwera.

## 4 Funkcje-serwer

- wyświetlanie dostępnych klientów w sieci,
- pobieranie danych o sygnałach RSSI od klientów,
- obliczanie lokalizacji w przestrzeni na podstawie trilateracji.