Lokalizator użytkowników sieci WiFi

15 czerwca 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

1 Wstęp

1.1 Opis apliakcji

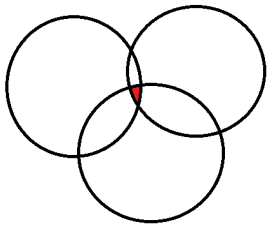
Celem projektu jest stworzenie aplikacji pozwalającej na określenie lokalizacji użytkownika sieci względem trzech urządzeń AP. System powinien przeskanować sieć w poszukiwaniu klientów podłączonych do punktów dostępowych. Użytkownik będzie mieć możliwość podejrzenia podstawowych informacji o każdym hoście w sieci, takicj 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 punkty dostępowe. Klienci powinni znaleść w swoim otoczeniu trzy punkty dostępowe, które mają wzlędem nich określoną siłę syganłu. Dane o tych sygnałach zostają przesyłane do serwera i interpretowane. W czasie rzeczywiśtym podawana jest lokalizacja danego klienta.

2 Działanie

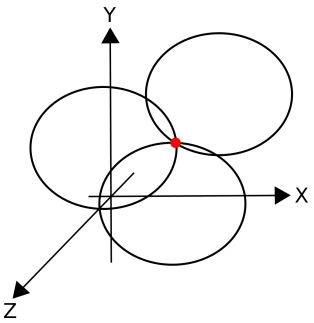
2.1 Trilateracja

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 sfere. Wyznaczenie współrzędnych klienta sprowadza się do znaleznienia miajsca przecięcia trzech sfer, każdej związanej z AP.



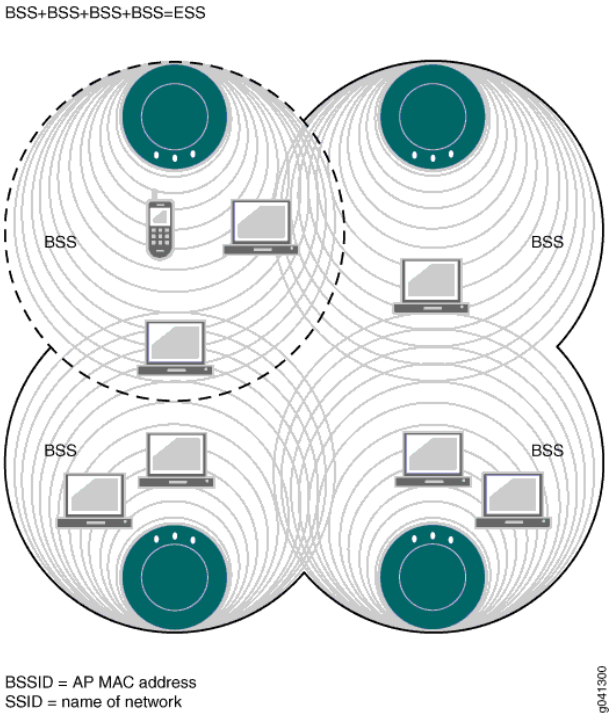
Rysunek 1: sfery wyznaczone przez siłe sygnału AP



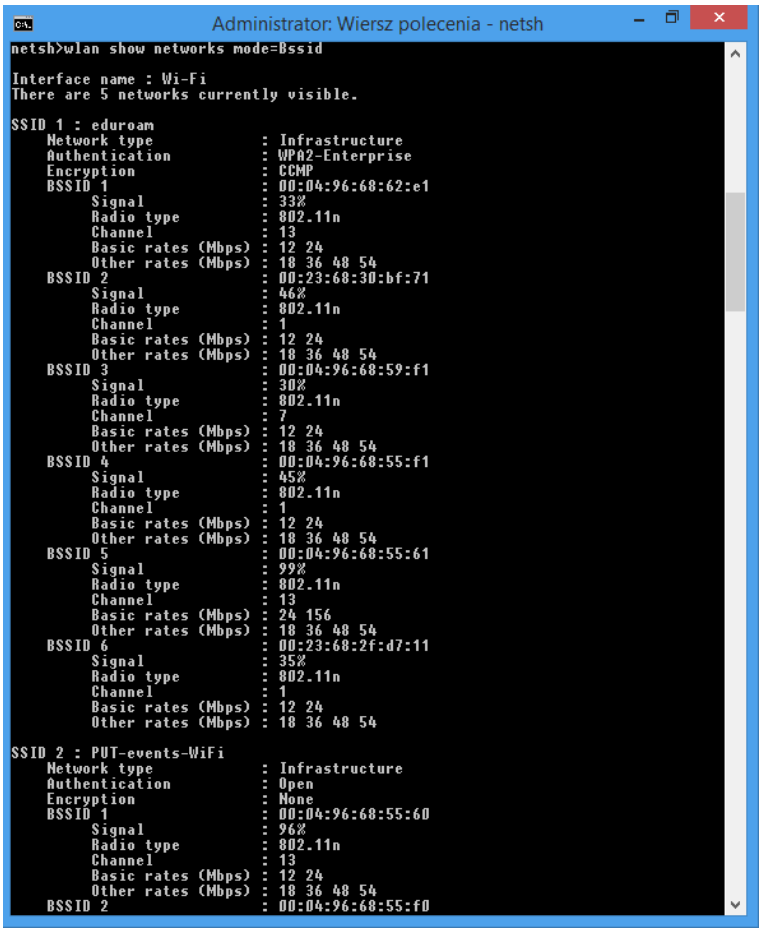
Rysunek 2: siła sygnału w przestrzeni

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.



Rysunek 3: BSSID i ESSID



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 Punkty dostępowe

Do przeprowadzenia testów aplikacji zostanie "zbudowana" prosta sieć utworzona na hotspotach z telefonów komórkowych. Do poprawnego działania będą potrzebne trzy lub więcej punkty dostępowe.

2.5 Beacony i ProbeRequest

Ramki Beacon służą punktom dostępowym do informowania potencjalnych klientów sieci o świadczeniu usługi połączenia bezprzewodowego. Zawierają informacje o adresie fizycznym AP.

Probe Request to pakiety wysyłane przez urządzenia sieciowe(np. smartfony) w celu wykrycia dostępnych punktów dostępowych. AP po otrzymaniu takiego pakietu może odczytać jaka jest siła sygnału urządzenia klienta względem niego.

2.6 Aplikacja serwera

Serwer otrzymuje dane od klienta i na podstawie poniższego wzoru wyznacza odległości do trzech punktów dostępowych. Następnie rysuje sfery i podaje lokalizacje użytkownika (część wspólna sfer).

$$d = 10^{((TxPower - RSSI)/(10*n))}$$

d - odległość w metrach
TxPower - maksymalna siła sygnału AP
RSSI - sygnał AP z punktu widzenia klienta
n - stała propagacji(2 dla wolnych przestrzeni)

```
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

2.7 Harmonogram prac

- przedtsawienie wstepnego projektu,
- zaprogramowanie modułu odpowiedzialnego za czytanie i interpretacje danych z urządzeń sieciowych,

- zaprogramowanie modułu odpowiedzialnego za rysowanie danych na układzie współrzędnych,
- testy aplikacji.

2.8 Funkcje-klient

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

2.9 Funkcje-serwer

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

3 Symulowanie działania aplikacji klienta

Z powodu problemów z odpowiednim odczytywaniem odległości punktów dostępowych, napisany został program symulujący wysyłanie "odpowiednich" dacnyh do serwera. Znaczy to w tym wypadku, że konkretna siła sygnału prezentuje zawsze tą samą odległości AP i wahania tych wartości nie są zbyt duże. Napisanie takiej aplikacji pozwoliło nam spreccyzować jaki efekt pracy chcemy uzyskać.

4 Napotkane problemy i potenjclane problemy przy dalszym rozwoju aplikacji

Mimo, że w teorii działanie aplikacji nie opiera się na żadnych skomplikowanych metodach czy obliczeniach, kilka rzeczy okazało się problematyczne. Projekty tego typu cieszą się raczaj wątpliwą popularnością i ciężko o udokumentowane przypadki naprawde dokładnego lokalizowania użytkownika sieci WiFi. Czymś co na pewno mogłoby uskutecznić działanie takiego systemu to możliwości finansowe. Pozwoliłoby to przygotować w pełni autorskie środowisko testowe.

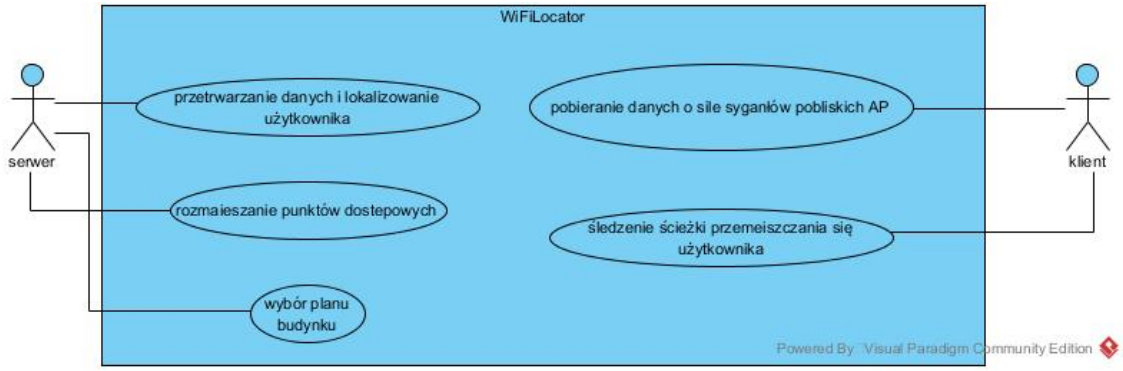
Kwestiami problematycznymi w projekcie okazały sie:

- **Sygnał RSSI nie jest dobrą miarą odległosci od AP** - siła sygnału punktu dostępowego może zależeć od wielu rzeczy. Mocy nadajnika, mocy odbirnika, poziomu naładowania baterii w takowych, modelu sprzętu, który służy w testowaniu. Podczas testów aplikacji okazało się, że w przypadku sprzętu róznych producentów, z różnymi kartami sieciowymi czy antenami, nie udało się uzyskać dokładnych wyników. Dwa urządzenia, znajdujące się w tej samej odległości od urządzenia z aplikacją kliencką, pokazywały na serwerze inne odległości. Znacząco inne.

- **Kalibracja** - aplikacja miała z założenia działać na zasadzie nakładania na plany budynków punktów dostepowych, rozmieszczania ich. Po rozmieszczeniu każdy z punktów, w czasie rzeczywistym, odbierał dane od aplikacji klienta i rysował okręgi zasięgów na planie. Należało w odpowiedni sposób skalibrować mapę z rzeczywistymi wymiarami np. pomieszczeń. Szukanie pewnego współczynnika skalującego metry na piksele okazało się dosyć problematyczne.

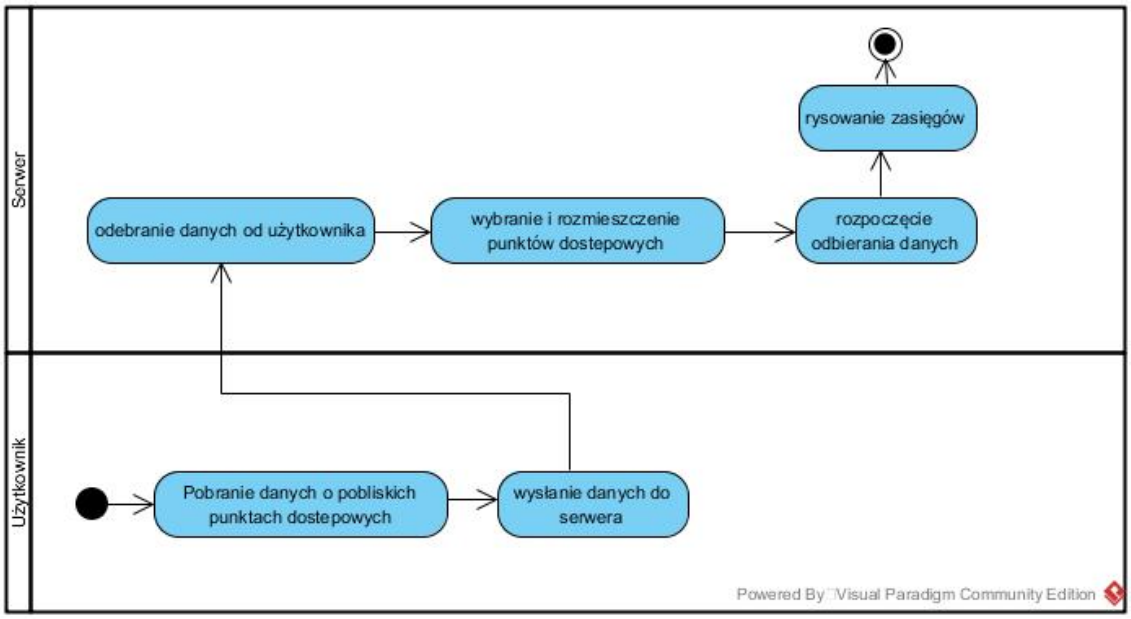
5 Diagramy apliakcji

Poniżej znajduje się podstawowy diagram przypadkóW użycia aplikacji. Widać na nim jak klient współpracuje z aplikacją serwera.



Rysunek 6: Diagram przypadkow uzycia

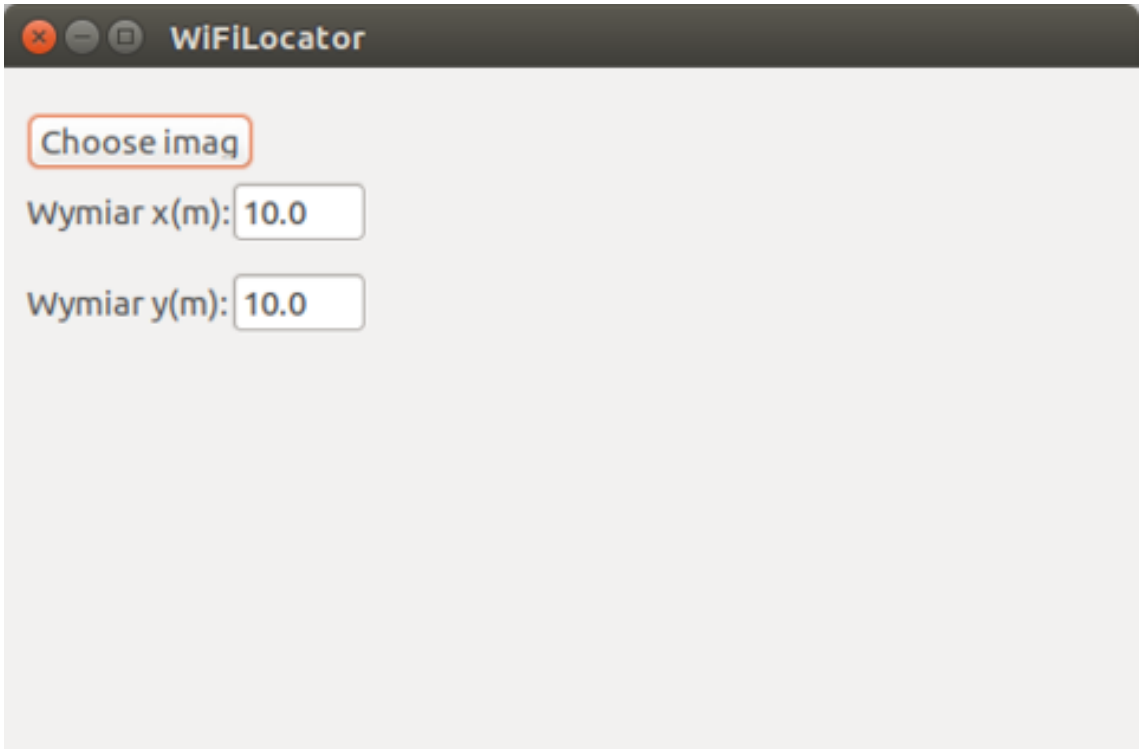
Diagram aktywności przedstawia jak przebiega proces przesyłania danych z aplikacji klienckiej do serwera i jak te dane są później analizowane.



Rysunek 7: Diagram aktywnosci - rysowanie

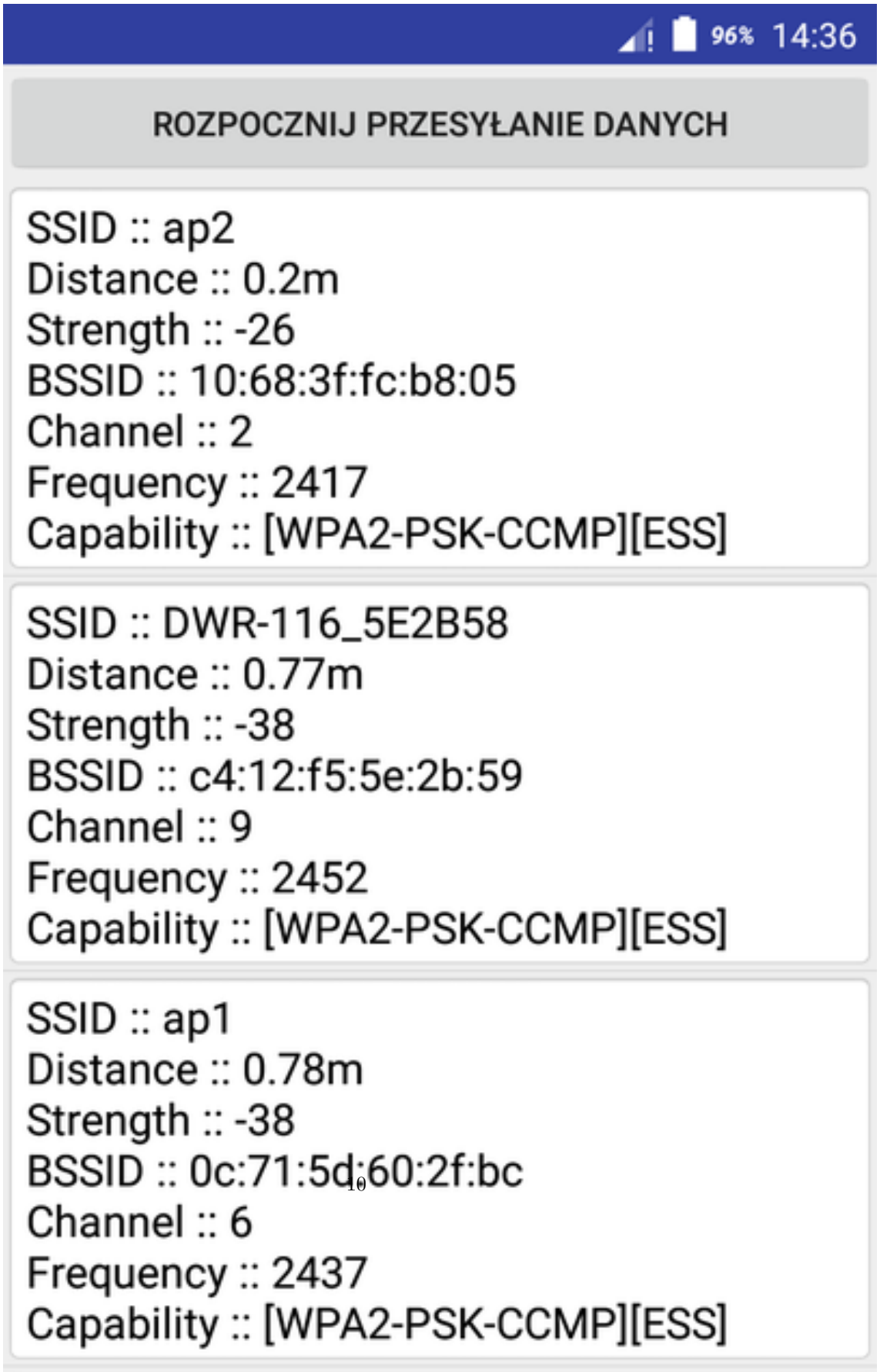
6 Podstawowe mockupy aplikacji

Możliwość wyznaczenia rozmiarów planszy(pomieszczenia)

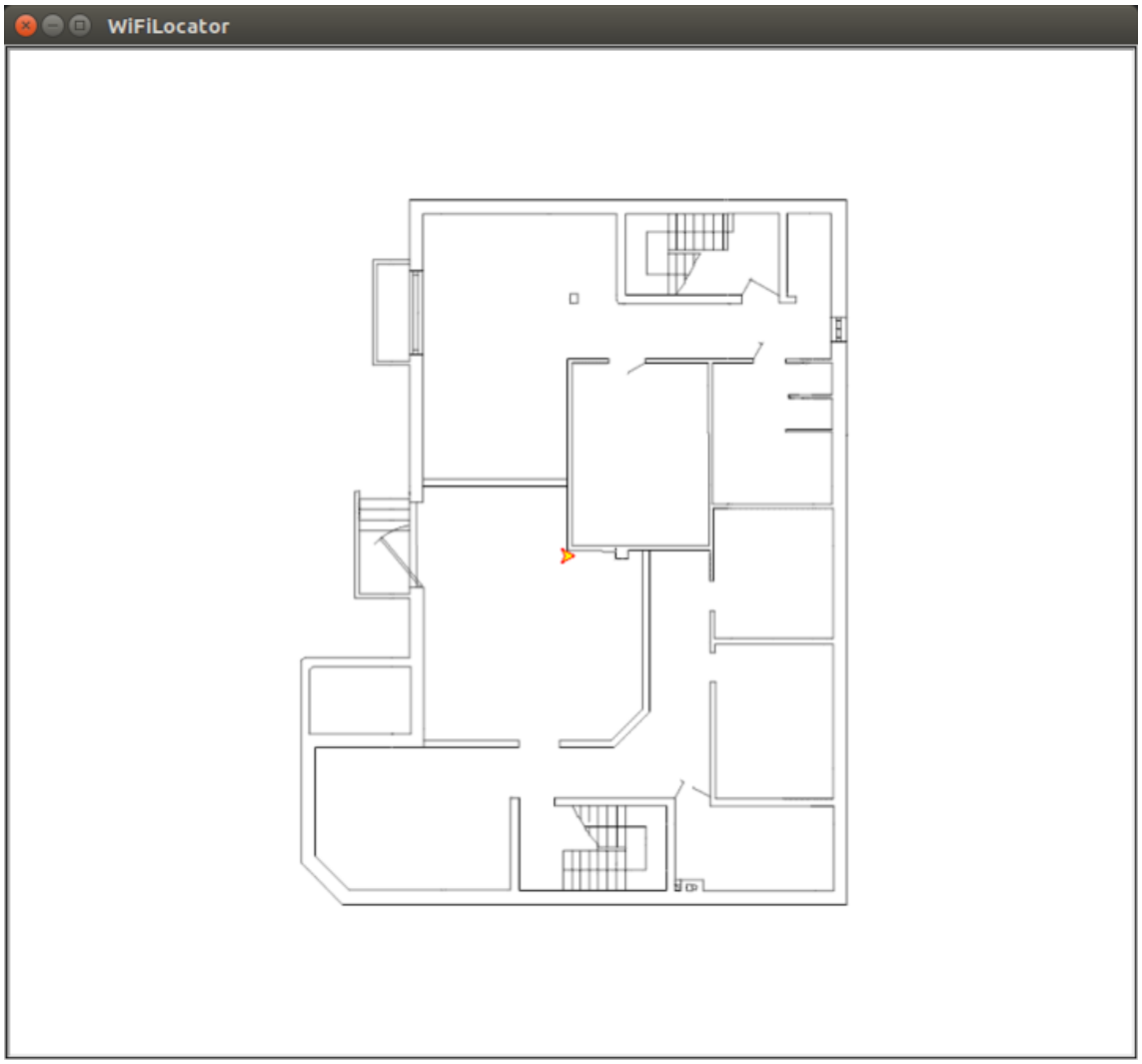


Rysunek 8: Wybór wymiarów

Widok aplikacji klienta. Lista wykrytych punktów dostępowych.


96% 14:36
ROZPOCZNIJ PRZESYŁANIE DANYCH
SSID :: ap2
Distance :: 0.2m
Strength :: -26
BSSID :: 10:68:3f:fc:b8:05
Channel :: 2
Frequency :: 2417
Capability :: [WPA2-PSK-CCMP][ESS]
SSID :: DWR-116_5E2B58
Distance :: 0.77m
Strength :: -38
BSSID :: c4:12:f5:5e:2b:59
Channel :: 9
Frequency :: 2452
Capability :: [WPA2-PSK-CCMP][ESS]
SSID :: ap1
Distance :: 0.78m
Strength :: -38
BSSID :: 0c:71:5d:60:2f:bc
Channel :: 6
Frequency :: 2437
Capability :: [WPA2-PSK-CCMP][ESS]

Aplikacja serwera po wyburze pliku graficznego.



Rysunek 10: Aplikacja serwera po wyburze pliku graficznego