



WARDRIVING ARTIKEL

Antwerpen in kaart

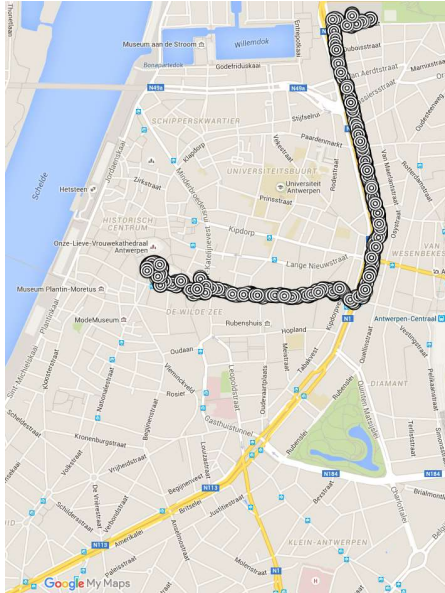
De zoektocht naar beveiligde en onbeveiligde wifi-netwerken in een grootstad

Peter Van de Putte, Daan Maes

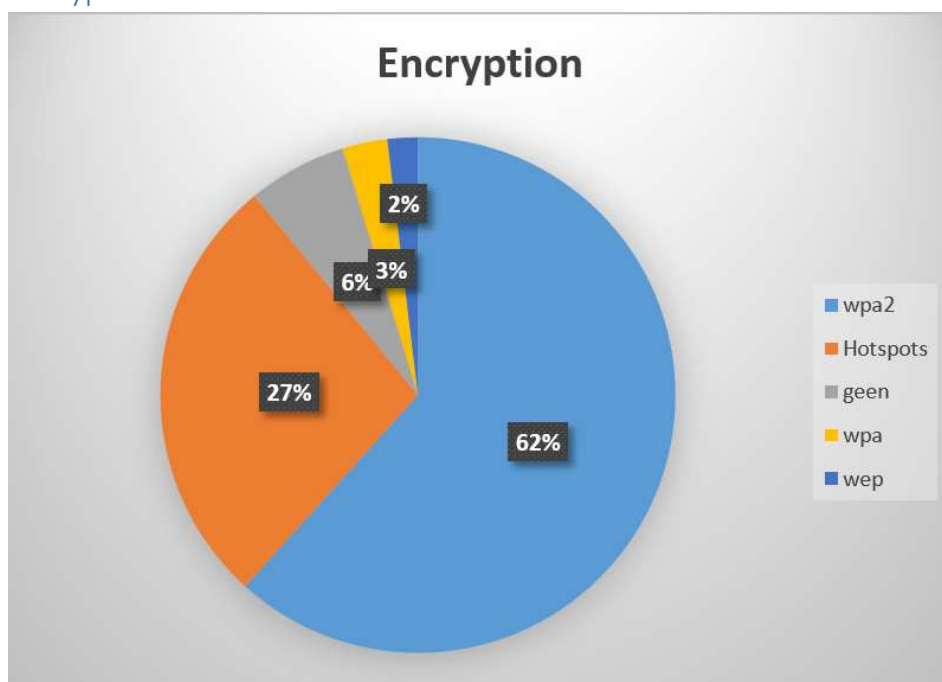
Gevonden netwerken

In totaal hebben we 3829 netwerken gevonden over een afstand van 2.7 kilometer.

Dat zijn bijna 1.5 netwerken per meter die er in Antwerpen kunnen worden gevonden.



Encryptiemethoden



De meest voorkomende encryptiemethode is WPA2(62%), wat ook de meest veilige methode is.

WPA1(3%) en WEP(2%) zijn minder veilig en representeren dus een kleiner deel van de encryptiemethoden.

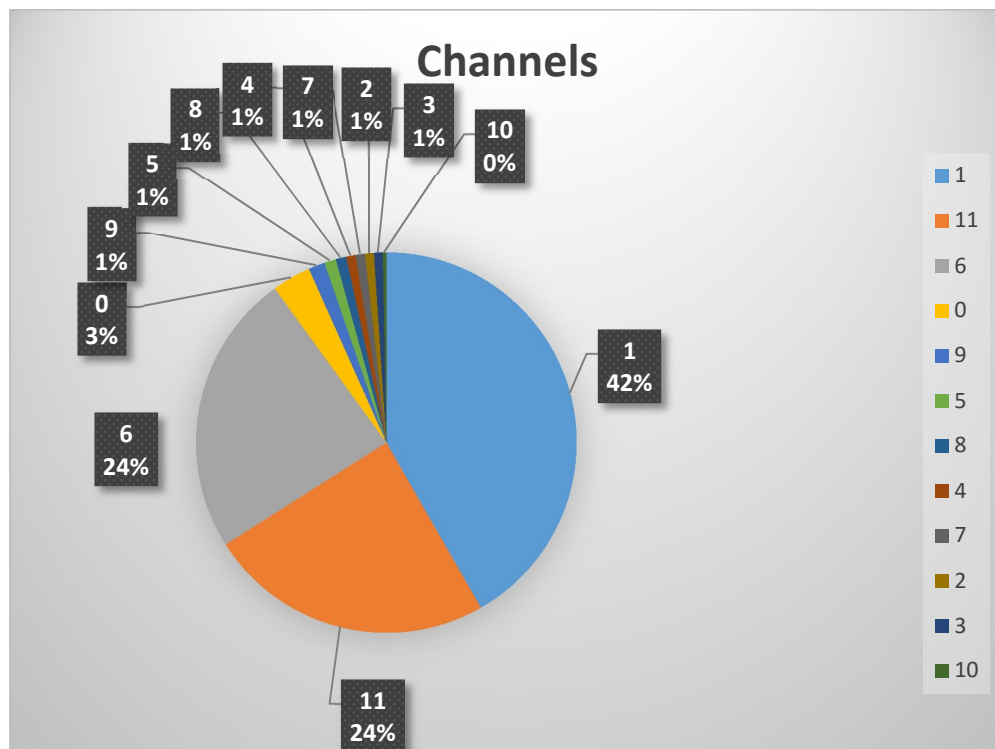
6% van alle netwerken heeft geen encryptiemethode en staat dus open voor alle mensen die toegang willen tot het netwerk en eventueel verkeerde dingen willen doen. Als we dit toetsen aan onze gevonden netwerken per meter, komen we uit op ongeveer 1 onbeveiligd netwerk per 20 meter in Antwerpen.

Hotspots(27%) maken tegenwoordig een groot deel uit van alle netwerken. Er wordt geen beveiligingssleutel toegepast maar gebruikers moeten zich meestal wel registreren alvorens het netwerk optimaal te kunnen gebruiken.

Onder deze hotspots vallen onder anderen:

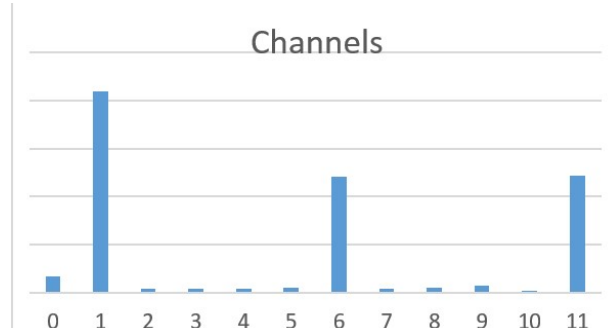
PROXIMUS_FON, Colombus-net, hhonors-public, TelenetHomespot, hhonors, Antwerpport en telentehotspot.

Channels



De minste netwerken werken op channel 10. Hier werken amper 0.3% van alle netwerken op.

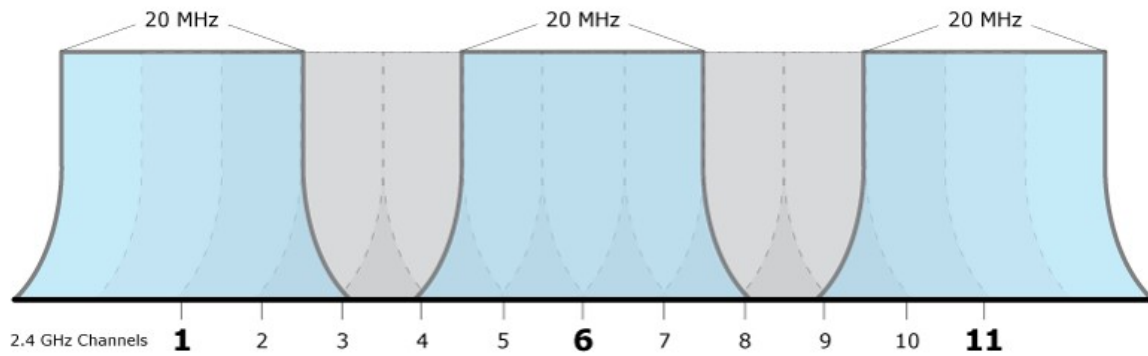
Bijna de helft van alle wifinetwerken werken op channel 1. Samen met channel 11(24%) en channel 6(24%) zijn ze verantwoordelijk voor 90 van de channels die gebruikt worden. Buiten deze drie worden er dus amper andere channels gebruikt.



Hoe komt dit ?

Slecht bereik of een langzame WiFi verbinding kan veroorzaakt worden door storing in je WiFi netwerk. De 3 meest voorkomende oorzaken van deze storing zijn: draadloze netwerken die op hetzelfde kanaal uitzenden, de router van de burens die op een overlappend kanaal uitzendt en storing op 2.4 GHz van iets dat geen WiFi signaal uitzendt.

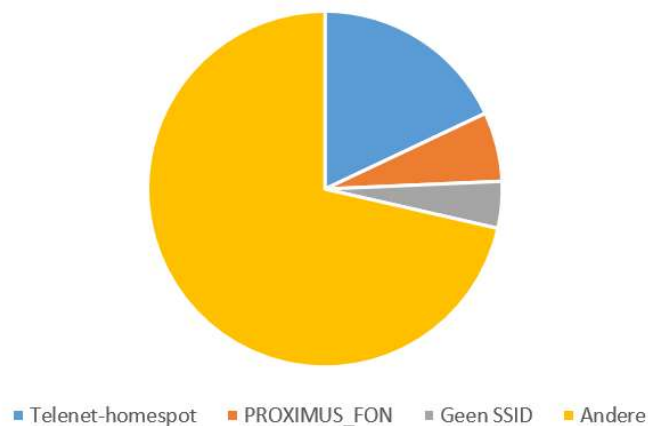
Kanaal 1, 6 of 11 zijn de beste WiFi kanalen omdat deze elkaar niet overlappen. Het is dan ook mogelijk om meerdere signalen naast elkaar op de 2.4 GHz band te versturen, omdat deze 100 MHz breed is en een kanaal een spectrum van 20 MHz gebruikt.



Indien er meerdere draadloze netwerken in de buurt zijn, is het vaak beter om hetzelfde kanaal (bij voorkeur 1, 6 of 11) te gebruiken, dan een overlappend kanaal. In dit geval is het het beste, het kanaal dat het minst gebruikt wordt bij de sterkste netwerken te gebruiken.

Met het gratis programma inSSIDer kun je bijvoorbeeld zien welke netwerken in de buurt zijn, hoe sterk het signaal is en op welk kanaal deze uitzendt en hier desnoods uit concluderen dat je beter van kanaal kan veranderen.

SSID



Als we kijken naar de SSIDs van de netwerken valt het op dat 18 procent van alle netwerken in Antwerpen een Telenethomspot is en 6 procent een PROXIMUS_FON netwerk.

Daarnaast zijn er ook een goede 4 procent van de netwerken die hun SSID niet tonen. Waarvan nog eens 22 procent van deze netwerken geen encryptie methode gebruikt. Toch even onderstrepen dat het verbergen van je SSID geen volwaardige maatregel is tegen indringers. Zo is het redelijk effectief tegen personen, die niet gericht zoeken naar het netwerk van een specifiek bedrijf. Maar een vastberaden hacker heeft dit zo gevonden.

Ook heeft het verbergen van een SSID vaak een omgekeerd effect. Zo zal een hacker die een netwerk vindt zonder SSID, dit netwerk eerder gaan aanvallen dan één met SSID. Dit omdat het verbergen van de SSID kan gelinkt worden aan het verbergen van gevoelige informatie. Laat dat nu eenmaal de hoofdreden zijn dan de hackers toeslagen.