

Instrukcja

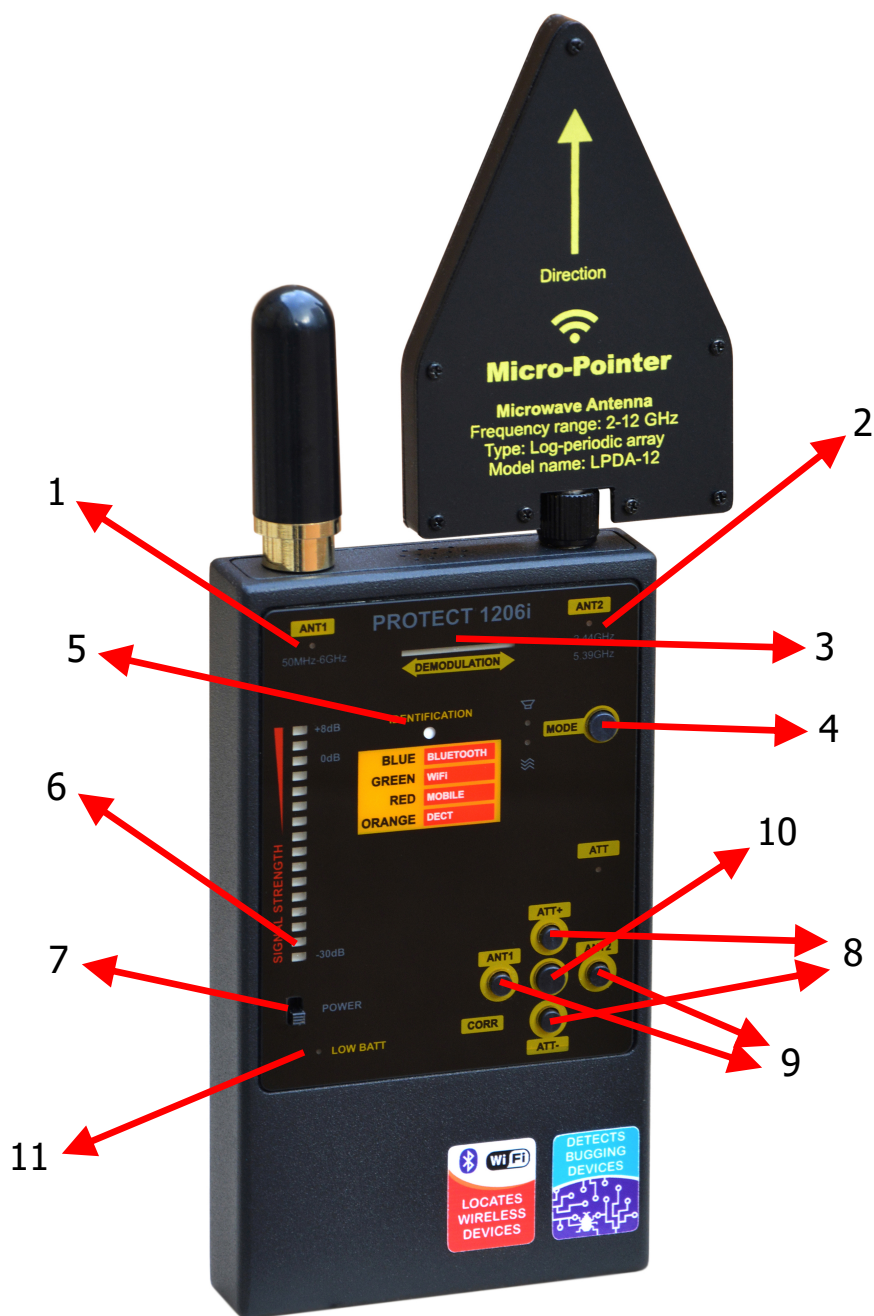
Detektor Protect 1206i



Spis treści:

1. Budowa	3
2. Działanie	4
3. Wykorzystanie.....	5
3.1. Wybór trybu pracy	5
3.2. Przeczesywanie obszaru.....	6
3.3. Sprawdzenie podejrzanego miejsca	6
3.4. Fizyczne szukanie.....	7
3.5. Sprawdzanie Bluetooth i WiFi	7
3.6. Sprawdzenie zakresu mikrofalowego.....	8
4. Sprawdzanie linii telefonicznych.....	9
5. Sprawdzanie osób	9
6. Odległość wykrywania	9

1. Budowa



1 – kanał 1 (50-6000 MHz)	6 – 16-segmentowy wskaźnik siły sygnału
2 – kanał 2 (Bluetooth i WiFi)	7 – przełącznik zasilania
3 – wyświetlacz demodulacji	8 – sterowanie czułością/tłumikiem
4 – zmiana trybu pracy	9 – przełączanie kanałów
5 – wskaźnik identyfikacyjny	10 – przycisk CORR
■ niebieski – Bluetooth	11 – wskaźnik niskiego stanu baterii
■ zielony – WiFi	
■ czerwony – GSM 900/1800	
■ pomarańczowy – DECT	

2. Działanie

Urządzenie posiada dwa oddzielne kanały radiowe, które współpracują z dwoma odpowiednimi antenami. Kanał **ANT1 (1)** jest używany do wykrywania w zakresie częstotliwości 50-6000 MHz, w celu poszukiwania wszystkich typów nadajników, z różnymi typami modulacji zarówno analogową jak i cyfrową, w tym VHF, UHF, GSM 900/1800/1900 MHz, 3G, Wi-Fi, Wi-Max, 4G (LTE) itp. Drugi kanał - **ANT2**, oznaczony jako "2,44 GHz 5,39 GHz" (**2**), jest używany do wykrywania Bluetooth i Wi-Fi (lub innych sygnałów z częstotliwością zbliżoną), ale z wyższą czułością.

Zwykła metoda wyszukiwania sugeruje użycie na początku anteny **ANT1 (1)**, tzn. 50-6000 Mhz, w celu pokrycia szerokiego zakresu częstotliwości. Później procedura przeszukiwania powinna być powtórzona na kanale drugim **ANT2 (2)**.

Użyj przycisków (**9**), aby przełączać się między kanałami **ANT1** i **ANT2**.

Protect 1206i ma aktywny tryb korelacji, który pomaga w czasie wyszukiwania. Ta funkcja pozwala operatorowi badać podejrzanego sygnały w określonych przypadkach. Kiedy przycisk "**CORR**" (**10**) zostanie wciśnięty w pobliżu podejrzanego miejsca, urządzenie wytwarza piszczące sygnały próbkujące. Dźwięk jest odbierany przez urządzenie podsłuchowe, a retransmitowany radiowo. Protect odbiera i demoduluje fale radiowe, a operator powinien obserwować wyświetlacz demodulacji (**3**). Wahania pojawiające się jednocześnie z sygnałem dźwiękowym ostrzegają o nadajniku radiowym lub innym rodzaju transmisji, która jest skorelowana z dźwiękiem.

Urządzenie Protect 1206i posiada 16-segmentowy wskaźnik siły sygnału (**6**) dający precyzyjne informacje operatorowi. Sygnały mogą być mierzone w zakresie od -30dB do + 8dB. Im bliżej urządzenie jest do źródła transmisji tym wyższy poziom wskazania.

Oprócz tego nowa wersja detektora ma zwiększony zakres dynamiki, co oznacza, że wskaźnik szybko wzrasta dla słabych sygnałów i powoli dla silnych sygnałów. Niektóre mocne źródła mogą powodować pełne wskazanie wyświetlacza (również gdy urządzenie znajduje się bardzo blisko nadajnika). W takich przypadkach należy używać przycisków tłumika **ATT+** i **ATT-** (**8**), aby zmienić czułość. Włącz tłumik blisko silnego źródła, gdy wskaźnik zapala się w pełni. Wtedy wskazanie zmniejszy się, a to umożliwi bardziej precyzyjne określenie lokalizacji źródła sygnału.

Należy zauważyć, że funkcja wibracji zostanie włączona, gdy wartość siły sygnału (**6**) zbliży się do szóstego segmentu.

Przycisk zmiany trybu pracy (**4**), zmienia metodę wskazania. Dostępne są cztery tryby:

- tryb dźwiękowy, gdy głośnik urządzenia wydaje demodulowany dźwięk
- tryb wibracji, gdy poziom sygnału na częstotliwości radiowej jest wysoki (osiągnie szósty segment na wskaźniku)
- tryb mieszany, gdy używane są oba powyższe typy wskazań
- cichy, gdy nie ma dźwięku, ani wibracji

Tryb dźwiękowy jest wygodny do szybkiego wyszukiwania, ponieważ doświadczony operator jest w stanie rozróżnić różne typy sygnałów.

Nadajnik radiowy może powodować efekt sprzężenia zwrotnego, gdy urządzenie jest blisko niego lub efekt zniknięcia dźwięków tła, które są zazwyczaj obecne z dala od nadajnika. W tym przypadku buczenie, które może być słyszalne w innych częściach pokoju może zniknąć, gdy Protect 1206i zbliży się do nadajnika. W głośniku będzie cisza.

W takim przypadku zaleca się użycie funkcji **CORR (10)** oglądając cały czas wskaźnik demodulacji (**3**). Wahania wskaźnika ostrzegają przed niebezpieczeństwem.

Tryby wibracji i mieszany są wygodne, gdy sprawdzamy obiekty i miejsca trudne do dotarcia. Operator może pracować bez konieczności oglądania wskaźników, wysoki poziom sygnału będzie sygnalizowany przez wibracje urządzenia.

Urządzenie Protect 1206i zasilane jest dwoma bateriami AAA (LR03). Zaleca się użyć baterii alkalicznych, aby osiągnąć optymalny czas pracy. Wskaźnik niskiego stanu baterii (**11**) włącza się, gdy baterie są bliskie wyczerpania.

3. Wykorzystanie

Przed rozpoczęciem przemiatania należy wykonać kilka czynności przygotowawczych. Po pierwsze należy wziąć pod uwagę czas i indywidualne okoliczności wyszukiwania. Istnieje wiele urządzeń, które są zdalnie sterowane. Zaleca się wykonanie całej operacji w godzinach pracy, w sytuacjach rzeczywistych, gdy osoba podsłuchująca najbardziej chciałaby słuchać. Może być konieczne zorganizowanie fikcyjnego spotkania. Nikt nie musi wiedzieć o oczekiwanym wyszukiwaniu.

Zasłoń wszystkie zasłony w pokoju. Włącz światło i wszystkie inne urządzenia, aby imitować normalne warunki pracy. Wskazane jest również włączenie jakiegoś źródła dźwięku, np. radia lub telewizora. To źródło dźwięku ma dwie bardzo ważne funkcje:

- aktywowane są nadajniki aktywowane głosem
- Twoje działania będą maskowane

3.1. *Wybór trybu pracy*

Podłącz antenę do **ANT1** i antenę mikrofalową Micro-Pointer do **ANT2**. Włącz urządzenie (**7**). Upewnij się, że wybrano **ANT1** (**9**). Wybierz tryb pracy za pomocą przycisku (**4**):

- W przypadku procedur tajnych używać trybu wibracji lub cichego.
- Tryb dźwiękowy jest wygodniejszy w celu zlokalizowania i sprawdzenia źródła sygnałów radiowych.
- Tryb wibracji lub mieszany pozwala operatorowi uniknąć ciągłego zerkania na zmiany wskazań wskaźników podczas sprawdzania trudno dostępnych miejsc.

Tryb dźwiękowy umożliwia operatorowi słuchanie sygnału tak, aby mógł on lepiej rozpoznać źródło. Nadajnik modulowany FM może wytwarzać sprzężenia zwrotne, gdy urządzenie znajduje się w jego pobliżu lub powodować efekt zniknięcia szumów tła, które zwykle występują dalej od nadajnika. W tym przypadku buczenie, które może być słyszalne w innych częściach pokoju może zniknąć, gdy Protect 1206i zbliży się do nadajnika. W głośniku będzie cisza.

W takim przypadku zaleca się użycie funkcji **CORR (10)** oglądając cały czas wskaźnik demodulacji (**3**). Wahania wskaźnika ostrzegają przed niebezpieczeństwem.

3.2. Przeczesywanie obszaru

Wejść do pomieszczenia z urządzeniem Protect 1206i, obserwując jego wskazania lub zwracając uwagę na wibracje. Włączaj i wyłączaj światła i inne urządzenia w pomieszczeniu. Chodź po pomieszczeniu stale zwracając uwagę na wskaźnik i/lub wibracje. Poziom wskaźnika wzrośnie lub zmaleje, gdy detektor znajdzie się bliżej lub dalej od urządzenia nadawczego. Przetestuj wszystkie przedmioty, które mogą zawierać ukryte urządzenie podsłuchowe. Zwróć szczególną uwagę poświęć miejscom, w których jest dostęp do sieci elektrycznej (gniazdka, przewody zasilające, urządzenia elektryczne itp.).

Odległość wykrycia może się różnić w zależności od sytuacji. Zwykle 1206i jest w stanie wykryć przeciętny podsłuch w odległości 30-100 cm, chociaż zaleca się sondowanie obiektów w odległości 10 cm.

Wskaźnik może wyświetlać 16 różnych poziomów.

W przypadku wykrycia zwiększonego poziomu sygnału, spróbuj znaleźć miejsce, gdzie jest on najsilniejszy.

Przesuń wykrywacz w różnych kierunkach i/lub obróć go. Włącz tłumik **ATT** blisko silnego źródła, gdy wskaźnik zapali się w pełni. Spadnie on, a następnie będzie wzrastał w miarę zbliżania do źródła umożliwiając precyzyjne określenie jego położenia. Nie zapomnij przywrócić normalnej czułości urządzenia przed kontynuowaniem wyszukiwania przez wyłączenie tłumika.

3.3. Sprawdzenie podejrzanego miejsca

Wskaźnik może często wykazywać zwiększony poziom sygnału w pobliżu przewodów lub metalowych przedmiotów, np. konstrukcji budynku. To może nie być podsłuch, ale raczej metal oddziałujący jak przedłużenie anteny. Podobna sytuacja może pojawić się w oknach od fal radiowych pochodzących z zewnątrz. To zjawisko zazwyczaj nie występuje na skoncentrowanym, małym obszarze i istnieje na dużych przestrzeniach, podczas gdy urządzenie podsłuchowe mają obszar silnego i skoncentrowanego pola na bardziej lokalnym obszarze.

Po znalezieniu dokładnej lokalizacji pola z wysokim sygnałem, wykonaj następujące czynności:

- Jeśli dyskrecja nie jest krytyczna, włącz tryb dźwiękowy i słuchaj dźwięku. Zwróć uwagę na obecność efektu pętli zwrotnej lub efektu zaniku w szumów w tle w pobliżu

podejrzanego miejsca. Można również rozpoznać typowe dźwięki protokołów komunikacyjnych, który wytwarzają:

- Bluetooth daje trzask/trzeszczenie
- Wi-Fi spowoduje skrzypienie/skrecz
- GSM daje brzęczenie
- DECT jest słyszalny jak transformator 50 Hz

Dioda identyfikacyjna (**5**) odpowiednio zmieni kolor. Proszę wziąć pod uwagę, że niektóre sygnały DECT mogą nie zostać rozpoznane.

- Naciśnij przycisk **CORR** podczas sprawdzania wskaźnika demodulacji, aby znaleźć synchroniczne wahania. To pokaże obecność korelacji, tzn. istnienie mikrofonu.
- Przełączaj urządzenie na **ANT2 (2)** raz na jakiś czas, aby sprawdzić, czy wykryty sygnał to sygnał Wi-Fi / Bluetooth, czy nie.

3.4. *Fizyczne szukanie*

Niezależnie od wyników, rozpocznij wyszukiwanie fizyczne. Wizualnie skontroluj i wysonduj każdy obiekt w danym obszarze. Zdemontuj, jeśli to konieczne, lampy, gniazdka telefoniczne i sieciowe oraz zdejmij przedmioty i telefony z mebli. Sprawdź ostrożnie wszystkie linie zasilania i linie telefoniczne. Otwórz książki, szafy itp. Pamiętaj, że szukanie fizyczne to podstawowa operacja podczas sprawdzania pomieszczenia. Nielegalne nadajniki często mają następujące cechy charakterystyczne:

- są małe, kompaktowe
- są ukryte
- są produkowane w małych ilościach, często ręcznie
- posiadają mikrofony lub kamery wideo
- często są umieszczane we wnętrzu innych urządzeń elektronicznych
- są połączone z linią telefoniczną
- mają własne źródło zasilania lub są podpięte do sieci elektrycznej
- posiadają antenę
- korzystają z sieci GSM (mają kartę SIM)

Jeśli znajdziesz podsłuch, nie przestawaj! Powinieneś kontynuować wyszukiwanie dokładniej, ponieważ osoby podkładające podsłuchy często instalują więcej niż jedno urządzenie. Mogą zainstalować jedno urządzenie, które można łatwo wykryć „na podpuchę”, a inne dobrze ukryte urządzenia mogą mieć zdalne sterowanie i niestandardową modulację.

3.5. *Sprawdzanie Bluetooth i WiFi*

Bluetooth i Wi-Fi mogą być łatwo wykorzystane do podsłuchiwania, a zatem potrzebują specjalnej uwagi. Konwencjonalne zestawy słuchawkowe Bluetooth, smartfony lub kamery mogą być

zainstalowane (lub celowo zostawione) w pomieszczeniach, w rzeczach osobistych lub na ciele, do przesyłania dźwięku lub obrazu. Ponadto, dobrze ukryte, dedykowane urządzenie podsłuchowe można stworzyć za pomocą dostępnych elektronicznych komponentów Bluetooth i Wi-Fi.

Dlatego zdecydowanie zalecamy powtórzenie skanowania obszaru za pomocą kanału drugiego ANT2 i anteny Micro-Pointer. W tym trybie Protect 1206i będzie wykrywał tylko urządzenia Bluetooth i Wi-Fi (i o zbliżonej częstotliwości działania) z większej odległości, dzięki czemu lokalizacja takich źródeł będzie znacznie łatwiejsza.

Nowa antena Micro-Pointer zapewnia doskonałe wzmocnienie, dobrą odległość detekcji i kierunkowość w celu szybszego namierzania. Powtórz procedurę skanowania wspomnianą w kroku 2, ale pamiętaj o tym, że kierunkowa antena Micro-Pointer widzi tylko sygnały w jej obszarze kierunkowym (naprzeciwko detektora). Dlatego skanuj wolniej, podczas obracania detektora w różnych kierunkach (w lewo, w prawo, w górę, w dół) w kilku punktach w pomieszczeniu.

Uwaga: przed rozpoczęciem rzeczywistego zmiatania można sprawdzić działanie wykrywacza na własnym routerze Wi-Fi.

Jeśli znalazłeś kierunek z wysokim poziomem sygnału, podchodź do źródła, wskazując je i obracając lekko detektor. Zbadaj uważnie źródło sygnału. Skonsultuj z pracownikami IT schemat bezprzewodowych punktów dostępowych oraz lokalizację bezprzewodowych telefonów używanych w sieci, aby upewnić się, że jest to punkt znany i legalny.

3.6. Sprawdzenie zakresu mikrofalowego

Kanał pierwszy **ANT1** detektora obejmuje częstotliwości w przedziale 50-6000 MHz. Trudno pokryć taki szeroki przedział jednorazowo, ale używana antena w nowej wersji urządzenia daje sobie radę z tym bardzo dobrze. Antena daje dobre wyniki podczas wykrywania sygnałów na częstotliwościach od 50 MHz i wyżej, do 3000 MHz, w tym wszystkich następujących pasm - VHF 140 MHz, UHF 450 MHz, 900 MHz, 1200 MHz i 2400 MHz.

Chociaż ta antena może być użyta do wykrywania sygnałów powyżej 3000 MHz, antena mikrofalowa Micro-Pointer może dać lepsze wyniki na tych pasmach. Dodatkowo antena mikrofalowa zapewnia łatwiejsze namierzanie dzięki kierunkowości. Dlatego w lewym gniazdku **ANT1** można używać anteny typu Micro-Pointer w czasie dodatkowego wyszukiwania zamiast **ANT2**, gdzie jest używana standardowo.

Podłącz antenę Micro-Pointer do **ANT1** zamiast anteny dookólnej i wybierz **ANT1 (9)**, aby uzyskać lepszą odległość detekcji na wyższych częstotliwościach; powyżej 2000 MHz. Sygnały na niższych częstotliwościach zostaną pominięte. Będziesz wykrywał Wi-Fi 2.4 GHz, niektóre pasma LTE (4G), Bluetooth, Wi-Max 2.3 GHz, 2.5 GHz, 3.5 GHz i 5.8 GHz, Wi-Fi 5 GHz i wszystkie inne sygnały, w tym audio oraz wideo powyżej 2 GHz. Przeskanuj ponownie pomieszczenie zwracając uwagę na kierunek anteny. Spróbuj skanować obiekty i powierzchnie możliwie blisko, ponieważ im większa jest częstotliwość, tym krótsza jest odległość wykrywania. Niektóre sygnały 5 GHz mogą być wykryte w odległości 20-50 cm.

Jest różnica między wykrywaniem anteną Micro-Pointer na kanale pierwszym **ANT1** i kanale drugim **ANT2**. Kanał **ANT2** został utworzony w celu wykrywania tylko Wi-Fi i Bluetooth. Jest bardziej czuły na powyższe sygnały i nie jest zdolny do wykrywania wszelkich innych sygnałów. Antena Micro-Pointer w **ANT2** będzie miała większą czułość, ale urządzenie nadal będzie mogło wykryć tylko Wi-Fi i Bluetooth.

ANT1 ma stałe pokrycie 50-6000MHz i antena Micro-Pointer podłączona do tego kanału będzie miała wyższą czułość na wszystkich częstotliwościach, nie tylko Wi-Fi i Bluetooth. Nie zapomnij podłączyć anten do ich pierwotnych kanałów po zakończeniu pracy: antena dookólna do **ANT1**, Micro-Pointer do **ANT2**.

4. Sprawdzanie linii telefonicznych

Podsłuchy mogą być instalowane w dowolnym miejscu przy linii telefonicznej. Może to być przy telefonie, gnieździe telefonicznym, skrzynce połączeniowej lub kablu. Większość aktywnych podsłuchów telefonicznych pracuje tylko wtedy, gdy słuchawka jest podniesiona. Tak więc sprawdzanie linii telefonicznych powinno być przeprowadzane tylko wtedy.

Powinieneś stosować antenę dookólną na **ANT1**, chociaż procedura może być powtórzona z anteną Micro-Pointer na **ANT1**.

Rozpocznij sprawdzanie od samego telefonu. Umieść urządzenie Protect 1206i w pobliżu zestawu i podnieś słuchawkę. Zwróć uwagę na podwyższenie poziomu sygnału (lub rozpoczęcie wibracji). Nie ma sensu testować telefonów bezprzewodowych (radiotelefonów), gdyż działają one dokładnie tak, jak urządzenia podsłuchowe ze względu na korzystanie z fal radiowych. Tylko fizyczna kontrola wystarczy, aby wiedzieć, czy są one na podsłuchu.

Przesuń detektor wzdłuż linii telefonicznej przy podniesionej słuchawce. Sprawdź wszystkie gniazda i skrzynki połączeniowe. Jeśli to możliwe, poproś drugą osobę o podnoszenie i odkładanie słuchawki. Jeśli zauważyłeś zmianę sygnału w tych momentach, tzn. że do linii jest podłączony podsłuch. Spróbuj zlokalizować miejsce, gdzie poziom sygnału jest najwyższy, a następnie wykonaj wyszukiwanie fizyczne.

5. Sprawdzanie osób

Istnieje wiele rodzajów nadajników przenośnych. Mogą transmitować rozmowy i (lub) sygnały wideo. Podłącz do urządzenia antenę dookólną do kanału pierwszego i wybierz **ANT1**. Zbliżaj się powoli do osoby. Jeśli poziom wskaźnika siły sygnału rośnie, to oznacza, że osoba nosi urządzenie podsłuchowe. Jeśli zmienisz lokalizację będziesz musiał wybrać inny tryb tłumienia zgodnie z szumem tła.

Innym sposobem testowania osób jest umieszczenie na biurku urządzenia Protect 1206i. W tym przypadku, trzeba uważnie obserwować wskaźnik siły sygnału, gdy zbliża się osoba podejrzana o posiadanie podsłuchu.

6. Odległość wykrywania

Odległość wykrywania zależy od dwóch głównych czynników:

- mocy wyjściowej nadajnika i jego częstotliwości
- sygnałów radiowych w otoczeniu (radio, TV, sieci WiFi itd. itp.)

Typowe odległości wykrywania:

Type of signal	Rod antenna in ANT1	Micro-Pointer in ANT2	Micro-Pointer in ANT1
VHF bug (140 MHz, 5 mW)	30-60 cm	–	–
UHF bug (450 MHz, 5 mW)	50-100 cm	–	–
GSM, LTE, CDMA 800-900MHz	30-200 cm	–	–
GSM 1900, 3G 2100 Mhz	30-100 cm	–	60-200 cm
2.4 GHz Wi-Fi accesspoint	30-80 cm	1-4 meters	0,5-2 meters
2.4 GHz Wi-Fi client	20-60 cm	60-120 cm	40-100 cm
Bluetooth	10-20 cm	20-80 cm	10-30 cm
LTE Higher ranges / Wi-Max	10-30 cm	–	30-100 cm
5 GHz Wi-Fi, 5 GHz video cameras, etc.	5-50 cm	30-100 cm	20-60 cm