Jak działa telefon komórkowy

Tomasz Kawalec
Instytut Fizyki UJ

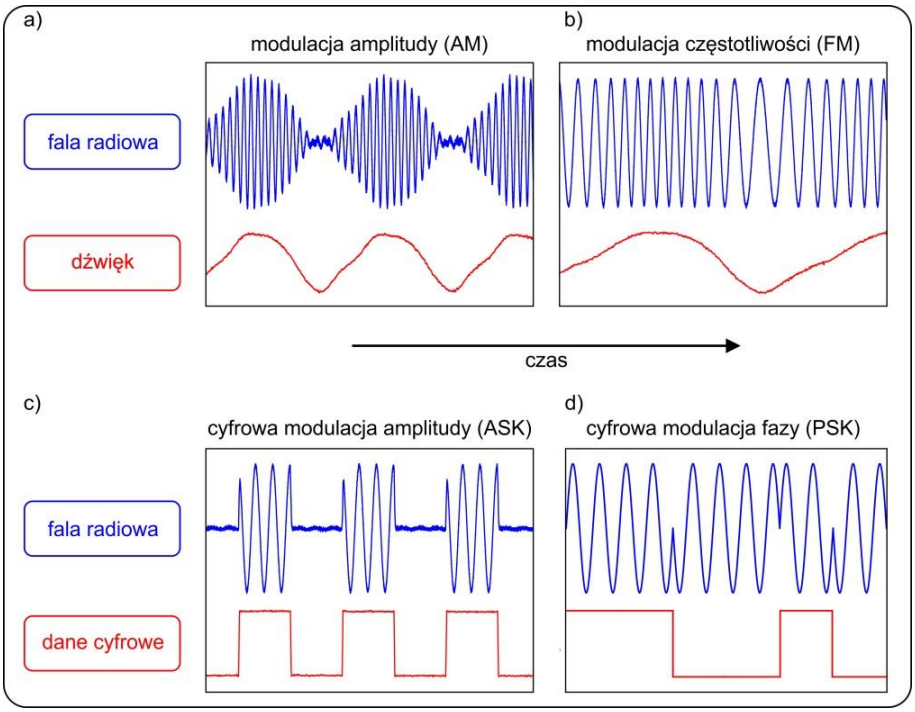
Codziennie korzysta z nich niemal każdy. Większość nie wie jednak, jak działają i jakie zjawiska fizyczne stanowią podstawę ich konstrukcji. Wszystko zaczyna się od naszego głosu.

Jak przesyłamy głos za pomocą fal radiowych?

Dźwięk, czyli drgania powietrza, są zamieniane na drgania prądu elektrycznego w mikrofonie. Dalsza droga sygnału zależy od tego, czy transmisja będzie analogowa, czy cyfrowa. W wersji analogowej sygnał trafia do modulatora – urządzenia, które zmienia (moduluje) parametry fali radiowej w takt drgań prądu. Najstarszy i najprostszy typ modulacji to modulacja amplitudy, czyli natężenia fali radiowej (rys. 1a). Jest jeszcze używana w komunikacji lotniczej oraz w radiofonii na falach długich, średnich i krótkich. Akronim AM od nazwy *amplitude modulation* znamy właśnie z oznaczeń na odbiornikach radiowych. Bardziej odpornym na zakłócenia typem modulacji jest modulacja częstotliwości (rys. 1b). W tym przypadku, w takt drgań prądu z mikrofonu, zmienia się nieco częstotliwość fali radiowej. Akronim FM (*frequency modulation*) również znamy z odbiorników radiowych. Ta modulacja jest szeroko stosowana w analogowej łączności profesjonalnej oraz radiofonii na falach ultrakrótkich (UKF). Była również wykorzystywana w telefonii komórkowej pierwszej generacji, w Polsce już zlikwidowanej.

W drugiej generacji telefonii komórkowej i nowszych oraz w wielu innych systemach profesjonalnych i domowych (system TETRA na przykład dla Policji czy system DECT dla telefonów domowych) korzysta się z transmisji cyfrowych. Takie transmisje pozwalają na przesyłanie nie tylko głosu, ale też danych i, ze względu na zastosowane szyfrowanie, są bez porównania trudniejsze do podsłuchania. Drgania prądu z mikrofonu są najpierw zamieniane na postać cyfrową, kompresowane, szyfrowane, a następnie kierowane do modulatora. Najprostszy typ modulacji cyfrowej to ASK (*amplitude shift keying* – patrz rys. 1c). W takt przesyłanych zer i jedynek fala radiowa jest wyłączana bądź włączana. Z tej modulacji korzystają na przykład niektóre typy pilotów do bram. Bardziej skomplikowaną modulacją jest FSK (*frequency shift keying*), w której zera i jedynki są przesyłane poprzez mniej lub bardziej skokowe zwiększenie lub zmniejszenie częstotliwości fali radiowej. Jeszcze innym typem jest PSK (*phase shift keying* – rys. 1d). Tutaj przy zmianie bitu następuje przeskok fazy fali radiowej – czyli jakby „przesunięcie" fali na osi czasu. W telefonii komórkowej, a także na przykład w WiFi, używane są skomplikowane kom-

binacje cyfrowych modulacji amplitudy i fazy lub zaawansowane odmiany cyfrowej modulacji częstotliwości. Oczywiście, zarówno przy transmisjach analogowych, jak i cyfrowych, w odbiorniku musi znajdować się demodulator, który zmiany parametrów fali radiowej zamienia z powrotem na drgania prądu (i ostatecznie dźwięk) lub ciągi danych.



Rys. 1

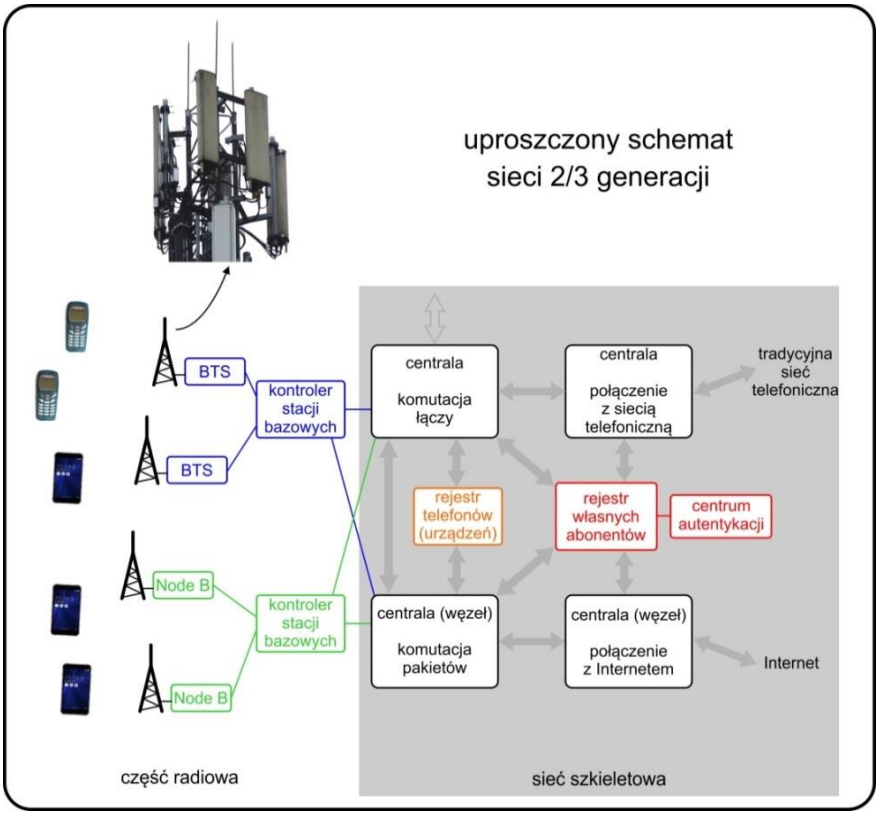
Jak zbudowana jest sieć telefonii komórkowej?

Sieć telefonii komórkowej została schematycznie przedstawiona na rys. 2. Tak, jak w każdej nowoczesnej łączności radiowej, telefony komunikują się tylko ze stacjami bazowymi – nigdy bezpośrednio między sobą, nawet gdy znajdują się tuż obok siebie. Zapewnia to dobrą jakość połączenia, ponieważ anteny stacji bazowych są umieszczane wysoko na budynkach, kominach i masztach. Sprawną komunikację zapewnia to, że nadawanie i odbieranie sygnału przez telefon odbywa się na dwóch różnych częstotliwościach. Stacje bazowe w telefonii drugiej generacji to BTS (*Base Transceiver Station*), a w technologii trzeciej generacji to Node B.

Część radiowa sieci komórkowej to przede wszystkim wiele stacji bazowych, zapewniających łączność radiową z naszymi telefonami na częstotliwościach około 1–2 GHz. Stacje te są sterowane przez odpowiednie kontrolery,

które przekazują sygnał cyfrowy dalej – do tak zwanej sieci szkieletowej. W tej sieci mamy szereg istotnych elementów:

- rejestr własnych abonentów wraz ze spisem używanych przez nich usług, współpracujący z centrum autentykacji. Centrum to przechowuje między innymi tajne klucze, dzięki którym sieć rozpoznaje nasz telefon – a właściwie naszą kartę SIM/USIM. Drugi z pary tajnych kluczy jest zapisany właśnie w karcie i w zasadzie nie jest w żaden sposób możliwy do ujawnienia.
- rejestr telefonów (ogólniej – urządzeń) to spis numerów IMEI telefonów, które zostały zgłoszone jako skradzione lub pracują nietypowo. Niestety, skuteczność takiego zabezpieczenia jest znikoma.
- centrale dla połączeń komutowanych – czyli takich, w których rozmowa jest przesyłana wzdłuż wyznaczonej trasy. Jest to metoda znana nam ze standardowej telefonii stacjonarnej.
- węzły dla połączeń pakietowych – czyli takich, w których dane są dzielone na mniejsze części (pakiety). Pakiety mogą wędrować do punktu docelowego różnymi drogami. Ta metoda to podstawa działania sieci Internet.



Rys. 2

Różnice między telefonią drugiej i trzeciej generacji – od kuchni

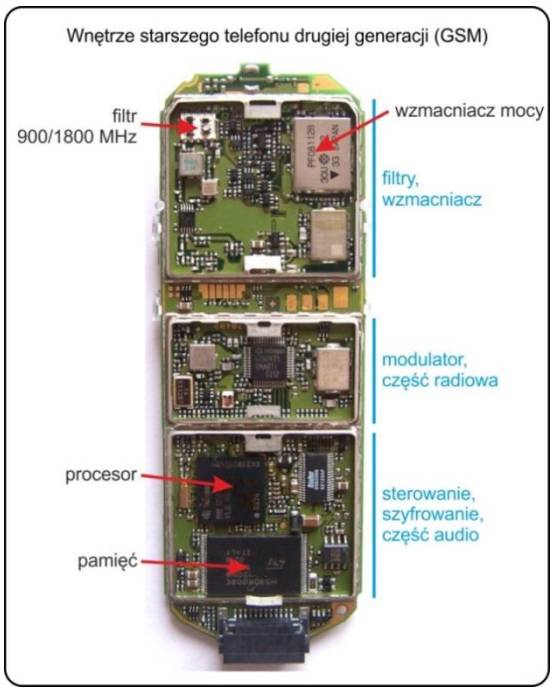
- Sieć drugiej generacji (w Polsce GSM) charakteryzuje się szyfrowaniem, które ze względu na rozwój komputerów może być w obecnych czasach relatywnie łatwo złamane. Ponadto, projektując sieć GSM zadbano, aby można było wymusić używanie specjalnie osłabionej wersji szyfrowania lub całkiem je wyłączyć. Miało to na celu zablokowanie wykorzystania telefonii komórkowej do tajnej komunikacji w krajach będących źródłem zagrożeń terrorystycznych. Dane cyfrowe z naszą rozmową są przesyłane radiowo w krótkich impulsach. W ten sposób, na jednej częstotliwości może pracować jednocześnie kilka telefonów – każdy z nich cyklicznie wysyłając dane tylko w swojej tak zwanej szczelinie czasowej. Charakterystyczne „burczenie" słyszane na przykład w radiu, gdy obok leży telefon komórkowy to właśnie wynik nadawania przez telefon tych impulsów – z częstotliwością około 216 Hz (czyli 216 razy na sekundę). Dostęp do Internetu w GSM jest jak na dzisiejsze standardy dość ograniczony, a sama usługa została do GSM dodana w ramach stopniowego rozwijania tego standardu.
- Sieć trzeciej generacji (w Polsce UMTS) – zapewnia silniejsze szyfrowanie oraz w pewnym zakresie kontrolę integralności transmisji. Oznacza to, że przesyłane do nas dane nie mogą być przez postronne osoby zmodyfikowane. Ta ważna cecha powoduje, że ewentualny atakujący nie może przykładowo tak podmienić komend, aby zmusić nasz telefon do włączenia słabszego szyfrowania lub w ogóle jego wyłączenia. Ponadto telefony sprawdzają czy sieć, z którą się łączą, jest autentyczna. Ten, wydawałoby się dziwny szczegół, jest niezwykle ważny. Eliminuje bowiem ataki typu „man in the middle" – w których atakujący używa własnej stacji bazowej do oszukania naszego telefonu. W przeciwieństwie do sieci drugiej generacji, szybki dostęp do Internetu był od początku planowany i wdrożony. Dzięki specjalnym technikom, wszystkie telefony zalogowane do jednej stacji bazowej, mogą pracować na jednej częstotliwości, w trybie tak zwanego rozpraszania widma. Technologia ta daje lepszą odporność na zakłócenia niż w GSM.

Ciekawostki

- Pierwsza sieć telefonii komórkowej NMT – Nordic Mobile Telephone – została uruchomiona w... Arabii Saudyjskiej.
- Akumulator pierwszego telefonu komórkowego starczał tylko na 20 minut rozmowy. Nie miało to jednak dużego znaczenia, ponieważ telefon ważył ponad kilogram i trudno byłoby dłużej utrzymać go przy uchu.
- W systemach z początku drugiej połowy XX wieku, będących prekursorami telefonii komórkowej, urządzenia telefoniczne były instalowane tylko w samochodach, ponieważ były ciężkie i zużywały bardzo dużo prądu.
- Nazwa „telefonia komórkowa" wzięła się z podziału terenu, na którym sieć komórkowa jest dostępna, na komórki – obszary obsługiwane przez jedną

stację bazową. Co ciekawe, maksymalny rozmiar takiej komórki w sieci GSM o promieniu około 35 kilometrów jest wyznaczony pośrednio przez prędkość światła, o czym można przeczytać więcej na stronie: http://www.neutrino.if.uj.edu.pl/archiwum/2015/28

- Mówimy, że komórki w sieci trzeciej generacji „oddychają" – oznacza to, że obszar obsługiwany przez jedną stację bazową może się dynamicznie powiększać lub zmniejszać, w zależności od chwilowej liczby abonentów na danym terenie.
- Sieć komórkowa sprawdza autentyczność naszego telefonu (naszej karty SIM lub USIM) metodą hasło-odzew (challenge-response). Polega to na tym, że sieć wysyła do telefonu odpowiednio przygotowaną przez centrum autentykacji liczbę losową. W karcie SIM na bazie tej liczby oraz jej tajnego klucza jest obliczany wynik pewnych operacji matematycznych. Wynik ten jest odsyłany do sieci. Jeśli jest zgodny z oczekiwanym przez sieć – telefon może się do niej zalogować.
- W telefonach starszego typu dość łatwo można rozpoznać poszczególne bloki funkcjonalne. Na rys. 3 jest widoczne wnętrze takiego telefonu, wraz z opisem głównych elementów.



Rys. 3