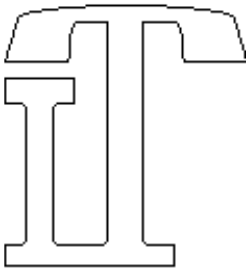


INSTYTUT TELEKOMUNIKACJI
POLITECHNIKI WARSZAWSKIEJ

SKR - L
Ćwiczenie 1

SYGNALIZACJA W SYSTEMIE GSM

Dariusz Mastalerz

Warszawa, październik 1997

Cel ćwiczenia

Celem ćwiczenia jest zapoznanie się z sygnalizacyją w sieci GSM podczas wykonywania standardowych procedur oraz z elementami sieci biorącymi udział w sygnalizacji, ze szczególnym uwzględneniem rejestrów VLR i HLR.

Wprowadzenie

Sygnalizacja w sieci GSM odbywa się na różnych płaszczyznach funkcjonalnych. Jest to np. sygnalizacja specyficzna dla systemu komórkowego (związana z mobilnością terminali) lub sygnalizacja związana z zestawianiem połączeń w sieci (komutacja). Oprócz tego sygnalizacja zachodzi również w różnych punktach sieci: w interfejsie radiowym lub wewnątrz sieci, pomiędzy komponentami "niewidocznymi" dla użytkownika (centrale, bazy danych). Poniżej omówione zostaną po kolei podstawowe elementy sieci GSM oraz interfejsy wykorzystywane przy sygnalizacji. Ze względu na specyfikę programu wykorzystywanego w ćwiczeniu w opisie skoncentrowano się na interfejsie radiowym i komunikacji między rejestrami HLR i VLR.

Architektura systemu GSM

W systemie GSM można wyróżnic kilka podstawowych elementów. Przede wszystkim należy wyróżnić dwa podsystemy funkcjonalne:

- podsystem komunikacji radiowej,
- podsystem sieciowy.

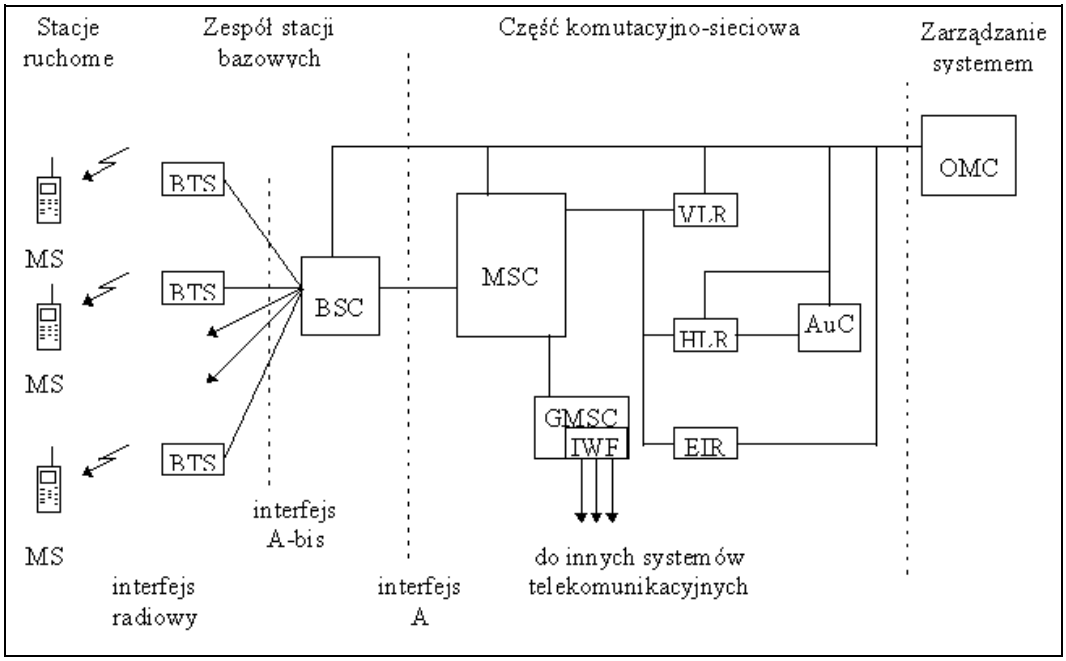
Na podsystem komunikacji radiowej składają się:

- terminale abonenckie (MS),
- stacje bazowe ze sterownikami i podstacjami nadawczo-odbiorczymi (BSS=BSC+BST).

Podsystem sieciowy składa się z:

- central obszarowych (MSC),
- centrum eksploatacyjnego (OSS),
- interfejsu z siecią publiczną PSTN.

Struktura sieci GSM przedstawiona jest na Rys. 1.



Rys. 1 *Struktura sieci GSM.*

Poszczególne elementy systemu

- **Zespół stacji bazowych** (*Base Station Subsystem BSS*)
  Każda komórka posiada jedną stację bazową. Zespół stacji bazowych umożliwia dostęp stacjom ruchomym do części stałej systemu GSM i dalej, w miarę potrzeby, do innych systemów telekomunikacyjnych.

  - **BTS - Stacje bazowe** (*Base Transceiver Station*) kontaktują się poprzez interfejs radiowy ze stacjami ruchomymi. BTS składa się z nadajnika i odbiornika sygnałów radiowych, anteny oraz układów przetwarzania sygnałów charakterystycznych dla interfejsu radiowego. Stacja bazowa stanowi interfejs pomiędzy połączeniem stałym do sterownika stacji bazowych, a łączem radiowym do stacji ruchomych.

  - **BSC - Sterowniki stacji bazowych** (*Base Station Controller*) połączone są z jednej strony z kilkoma lub kilkudziesięcioma stacjami bazowymi, pełnią względem nich funkcje sterujące. Sterownik stacji bazowych steruje takimi funkcjami jak przełączanie kanałów (handover) oraz sterowanie mocą stacji ruchomej (power control). Z drugiej strony BSC połączone są z centralą systemu ruchomego MSC.

- **Część komutacyjno-sieciowa** (*Network and Switching Subsystem NSS*)
  Realizuje ona funkcje komutacyjne systemu GSM.

  - **MSC - Centrala systemu ruchomego** (*Mobile Switching Centre*) wykonuje funkcje komutacyjne pomiędzy dwoma abonentami systemu GSM lub pomiędzy abonentem systemu GSM a abonentami innych systemów telekomunikacyjnych.
    Z jednej strony, centrala MSC komunikuje się ze stacjami ruchomymi,

z drugiej strony centrala MSC jest połączona z innymi centralami systemu GSM, w tym z centralą tranzytową **GSMC** umożliwiającą połączenie z innymi systemami. Wykorzystuje się przy tym tzw. moduł funkcji sprzęgających IWF (*InterWorking Functions*).
W odróżnieniu od central pracujących w stałej sieci telefonicznej, centrala MSC posiada dodatkowe funkcje wynikające z "ruchomego" charakteru abonentów, są to m.in.: rejestracja położenia abonenta, przywoływanie abonentów, przekazywanie parametrów kryptograficznych w celu szyfrowania transmisji itp.

- **HLR - Rejestr stacji własnych** (*Home Location Register*)
  W każdym rejonie obsługiwanym przez danego operatora systemu GSM znajduje się jeden lub kilka rejestrów HLR. W momencie rejestracji abonenta u operatora systemu, do rejestru wpisywane są dane nowego abonenta. Dotyczą one uprawnień, zawierają informacje pozwalające na identyfikację użytkownika oraz informację o aktualnym położeniu danej stacji ruchomej (adres centrali MSC odpowiadającej obszarowi, w którym aktualnie znajduje się stacja ruchoma). Informacja ta jest zmieniana na bieżąco wraz ze zmianami położenia stacji ruchomej.

- **VLR - Rejestr stacji obcych** (*Visitors Location Register*)
  Rejestr VLR zawiera informacje o abonentach aktualnie znajdujących się w obszarze obsługiwanym przez skojarzoną z nim centralę MSC. Gdy tylko stacja ruchoma przekracza granicę nowego obszaru, rejestr VLR skojarzony z obsługującą ten obszar centralą MSC żąda od rejestru HLR, w którym obca stacja zarejestrowana jest na stałe, danych o nowym dla siebie użytkowniku. Równocześnie rejestr HLR otrzymuje od rejestru VLR i zapamiętuje informacje o norym położeniu stacji ruchomej. Zawarte w rejestrze VLR dane o lokalizacji stacji ruchomej są bardziej szczegółowe niż dane rejestru HLR. W przypadku gdy omawiana stacja ruchoma żądać będzie połączenia, rejestr VLR zawierać będzie wszystkie informacje niezbędne do jego zestawienia, bez potrzeby odwoływania się w każdym przypadku do rejestru HLR.

- **AuC - Centrum identyfikacji** (*Authentication Centre*) jest modułem połączonym z rejestrem stacji własnych HLR, realizującym funkcje związane z zabezpieczaniem systemu przed niepowołanym dostępem. Chodzi tu zarówno o przeciwdziałanie próbom realizacji połączeń na koszt innych abonentów jak i o uniemożliwienie podsłuchiwania rozmów przesyłanych w kanale radiowym. Moduł AuC zawiera parametry konieczne do identyfikacji abonentów, tzw. klucze szyfrujące, a także same algorytmy szyfrowania i generator liczb losowych.

- **EIR - Rejestr identyfikacji wyposażenia** (*Equipment Identity Register*) jest bazą danych służącą do identyfikacji stacji ruchomych. W przeciwieństwie do analogowych systemów komórkowych, w systemie GSM uprawnienia abonenta nie są związane z terminalem używanym przez niego, a jedynie z inteligentnym modułem SIM będącym w jego posiadaniu. Tak więc identyfikacja abonenta dokonywana jest oddzielnie

od identyfikacji terminala. Rejestr EIR połączony jest z centralą MSC poprzez łącze sygnalizacyjne. Stacja ruchoma, która nie uzyskała akceptacji MSC (np. została zgłoszona do systemu jako skradziona) może zostać zablokowana.

- **Zespół eksploatacji i utrzymania** (*Operation and Maintenance Subsystem OMS*)
  Zespół eksploatacji i utrzymania w systemie GSM umożliwia operatorowi wgląd w pracę systemu oraz administrowanie nim - wydawanie abonamentów, wprowadzanie i uaktualnianie danych o abonentach, lokalizację i usuwanie uszkodzeń, pomiary ruchu telekomunikacyjnego i prowadzenie statystyk, naliczanie opłat itp. Z jednej strony zespół eksploatacji i utrzymania połączony jest, najczęściej za pomocą transmisji wykorzystującej protokół X.25, z częścią komutacyjno - sieciową systemu, a za jej pośrednictwem ze stacjami bazowymi i ruchomymi. Z drugiej strony, zespół OMS posiada interfejs człowiek - maszyna dla osób uczestniczących w obsłudze systemu. Zespół eksploatacji i utrzymania składa się najczęściej z pewnej liczby połączonych ze sobą tzw. centrów eksploatacji i utrzymania **OMC** (*Operation and Maintenance Centre*), które wspólnie, w strukturze rozproszonej, realizują jego funkcje.

- **Stacje ruchome** (*Mobile Stations MS*)
  Stacje ruchome spełniają rolę interfejsu abonenta z systemem GSM. Istnieją różne typy stacji ruchomych różniące się od siebie mocą nadajnika, a co za tym idzie także wielkością i pojemnością akumulatorów. Rozróżniamy najmniejsze kieszonkowe stacje ruchome (handheld), większe stacje przenośne (portable) i przewoźne oraz bezprzewodowe automaty wrzutowe i bezprzewodowe centrale abonenckie PBX (chodzi o typ łącza doprowadzającego sygnał z systemu GSM do centrali, a nie sposób przyłączenia terminali do centrali).

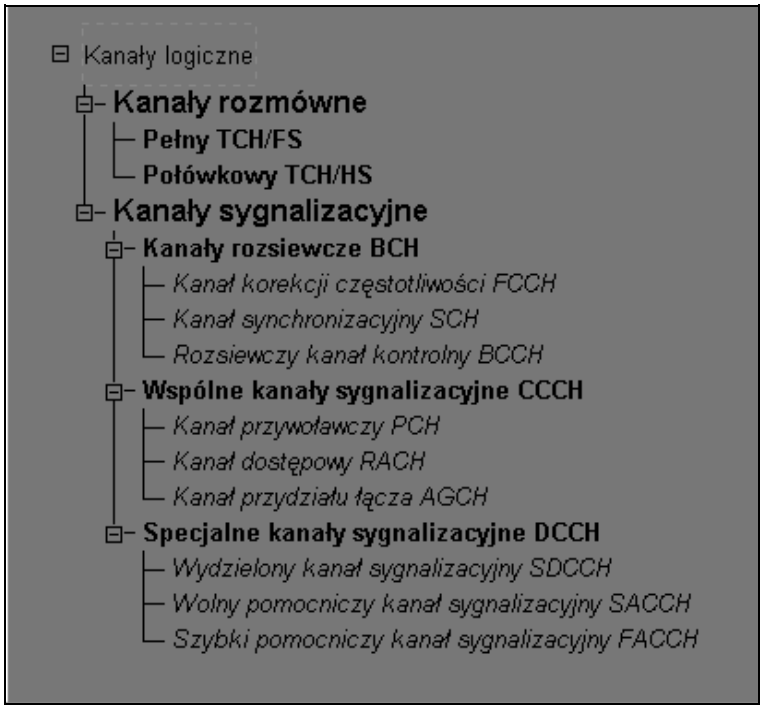
Interfejs radiowy

Komunikacja między siecią a stacją ruchomą odbywa się za pośrednictwem kanału radiowego. Jest to więc tak na prawdę komunikacja między BTS (BSC) a MS. Należy jednak pamiętać, że nadawcą i adresatem większości wiadomości sygnalizacyjnych nie jest podsystem stacji bazowej. Większość komunikatów obsługiwana jest przez dalsze elementy systemu: centralę MSC, czy rejestry HLR, VLR, AuC, EIR. Jedynie sygnalizacja dotycząca pomiarów parametrów kanału fizycznego, kodowania mowy i przełączania (handover) w obrębie tego samego BSC jest obsługiwana przez podsystem stacji bazowej.

Do transmisji w interfejsie radiowym służą kanały fizyczne, w których następnie umieszcza się określone kombinacje kanałów logicznych[1].

Struktura kanałów logicznych przedstawiona jest na Rys. 2.

[1)] Dokładny opis struktury kanału radiowego zostanie przedstawiony w następnycm ćwiczeniu.



Rys. 2 *Struktura kanałów logicznych.*

- **Kanały rozmówne** (*TCH - Traffic Channels*):
  dwukierunkowe, przeznaczone do transmisji mowy z przepływnością 13kbit/s i danych z przepływnością do 9.6kbit/s lub mowy z przepływnością 7 kbit/s i danych z przepływnością do 4.8 kbit/s (tzw. kanały połówkowe)

- **Kanały rozsiewcze** (*BCH - Broadcast Channels*):
  przeznaczone do transmisji informacji sygnalizacyjnych i synchronizacyjnych z BS do MS.
  - **kanał korekcji częstotliwości FCCH** (*Frequency Correction Channel*) - przenosi pakiet korekcyjny umożliwiający MS zsynchronizowanie się z częstotliwością BS,
  - **kanał synchronizacyjny SCH** (*Synchronization Channel*) - przenosi pakiet synchronizacyjny, umożliwiający MS synchronizację ramkową,
  - **kanał kontrolny rozsiewczy BCCH** (*Broadcast Control Channel*) - zawiera informacje identyfikujące stację bazową, operatora, numery kanałów w sąsiednich komórkach oraz inne parametry dostępu.

- **Wspólne kanały sygnalizacyjne** (*CCCH - Common Control Channels*):
  wykorzystywane do zestawiania połączeń między MS i BS.
  - **kanał przywoławczy PCH** (*Paging Channel*) - do przesyłania informacji przywoławczych z BS do MS,
  - **kanał wielodostępu (dostępowy) RACCH** (*Random Access Channel*) - do przesyłania żądania dostępu za stacji ruchomej do stacji bazowej,
  - **kanał przydziału łącza AGCH** (*Access Grant Channel*) - do przesyłania z BS do MS informacji o przydzieleniu wydzielonego kanału sygnalizacyjnego SDCCH (w odpowiedzi na żądanie dostępu).

- **Specjalne kanały sygnalizacyjne** (*DCCH - Dedicated Control Channels*):
  wykorzystywane do wymiany informacji sygnalizacyjnych między MS i BS w

trakcie obsługi żądania dostępu, identyfikacji abonenta i w czasie trwania połączenia (kanały są dwukierunkowe i łączą stację bazową z jedną, konkretną stacją ruchomą).

- **wydzielony kanał sygnalizacyjny SDCCH** (*Standalone Dedicated Channel*) - wykorzystywany w procedurach zgłoszenia i identyfikacji abonenta,
- **wolny pomocniczy kanał sygnalizacyjny SACCH** (*Slow Associated Control Channel*) - do przesyłania informacji systemowych w czasie trwania połączenia (sterowanie mocą stacji, wyprzedzeniem czasowym, przekazywanie wyników pomiarów poziomu sygnału własnej i sąsiednich stacji bazowych),
- **szybki pomocniczy kanał sygnalizacyjny FACCH** (*Fast Associated Control Channel*) - wykorzystywany do szybkiego przesyłania informacji sygnalizacyjnych (np. w czasie przenoszenia połączenia między komórkami).

Identyfikacja abonenta i stacji bazowych

Plan numeracyjny systemu GSM przewiduje istnienie wielu numerów identyfikujących abonenta, terminal ruchomy, sieć, stację bazową itd. Opisanie wszystkich używanych w systemie GSM numerów wykracza poza zakres niniejszego ćwiczenia. Poniżej przedstawione zostaną jedynie numery używane w programie. Zainteresowanych konstrukcją i zakresem użycia pozostałych numerów odsyłam do literatury.

Numery używane w programie można podzielić na następujące grupy:

- **numery identyfikujące abonenta**:
  - **MSISDN** (*Mobile Subscriber ISDN number*)
    Ten międzynarodowy numer katalogoey abonenta w sieci ISDN jest jedynym numerem widocznym "poza" siecią GSM. Pozwala na identyfikację abonenta (jest publikowany w książkach telefonicznych), nie odzwierciedla jednak drogi zestawiania połączenia wewnątrz siegi GSM. Służy jedynie do odnalezienia faktycznego numeru identyfikacyjnego IMSI wywoływanego abonenta.
  - **IMSI** (*International Mobile subscriber Identity*)
    Numer ten jest przydzielany każdemu abonentowi sieci GSM. Składa się maksymalnie z 15 cyfr i zawiera informację o macierzystym rejestrze HLR abonenta oraz jego unikatowy numer w macierzystej sieci PLMN (Public Land Mobile Network). Przechowywany jest w karcie SIM i w rejestrze HLR.
  - **TMSI** (*Temporary Mobile Subscriber Identity*)
    Numer nadawany abonentowi w celu zapewnienia dyskrecji położenia i anonimowości abonenta ruchomego. Pozwala on na identyfikację abonenta w danym obszarze przywołań. Z tego powodu używany jest tylko łącznie z numerem LAI. Numer jest zarządzany przez MSC/VLR. Jego przydział następuje podczas pierwszej rejestracji w danym obszarze przywołań, zaś unieważnienie po wykonaniu procedury aktualizacji położenia w nowym obszarze przywołań.

Uwaga: Numer nie jest kopiowany do HLR. Rejestr HLR używa do identyfikacji abonenta numeru IMSI.

- **MSRN** (*Mobile Station Roaming Number*)
  Tymczasowy numer abonenta wizytującego, generowany przez MSC/VLR na czas trwania jednego połączenia lub na czas między kolejnymi aktualizacjami położenia. W celu zachowania poufności zarówno lokalizacji abonenta, jak i jego faktycznego numeru IMSI, zestawienie połączenia przychodzącego do abonenta sieci komórkowej jest dokonywane na podstawie numeru MSRN. Numer MSRN ma taką samą strukturę jak numer ISDN w danym planie numeracji.

♦ **numery identyfikujące terminal**:

- **IMEI** (*International Mobile Equipment Identity*)[1]
  Każdy terminal ma przydzielony unikatowy w skali świata numer IMEI. Numer ten jest przechowywany w rejestrze EIR i służy do autoryzacji dostępu terminala do sieci. Sprawdzanie to nie jest jednak rutynowe, tj. nie wchodzi w skład standardowych procedur sygnalizacyjnych za względu na generowany ruch dodatkowy.

♦ **inne numery**:

- **LAI** (*Location Area Identity*)
  Numer identyfikacyjny obszaru przywoławczego identyfikujący rejestr VLR, w którego "zasięgu" znajduje się abonent. Jest używany razem z numerem TMSI do określenia lokalizacji abonenta w obrębie całej sieci.

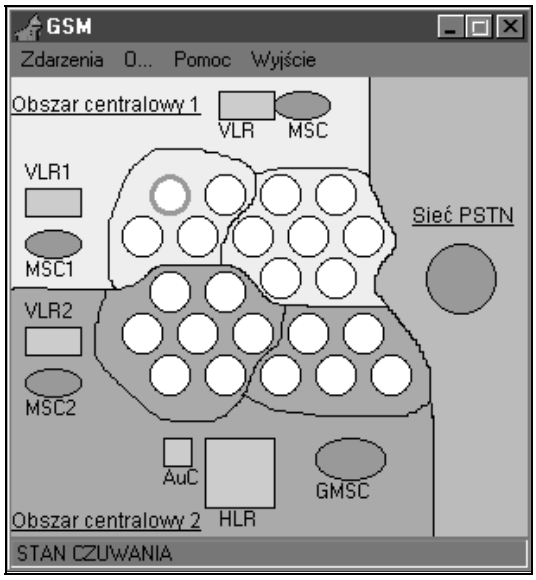
Opis programu

Zadaniem programu jest symulacja komunikacji pomiędzy bazami HLR, VLR, AuC oraz EIR.

Główne okno programu (Rys. 3) przedstawia sieć komórek, symbolicznie zaznaczonych kółkami. W jednej z komórek umiejscowiony jest abonent ruchomy, którego działania (przemieszczenie, rozmowa, włączenie / wyłączenie aparatu) wywołują potrzebę komunikacji pomiędzy rejestrami. Sygnalizacja pokazywana jest w programie na dwóch poziomach:

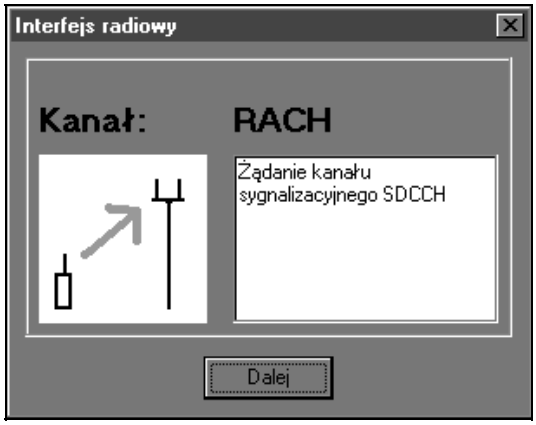
- na poziomie łącza radiowego,
- na poziomie sieci (poziom niewidoczny dla abonenta).

[1)] Numer ten nie jest wykorzystywany w programie. Został zamieszczony w opracowaniu dla kompletności opisu.



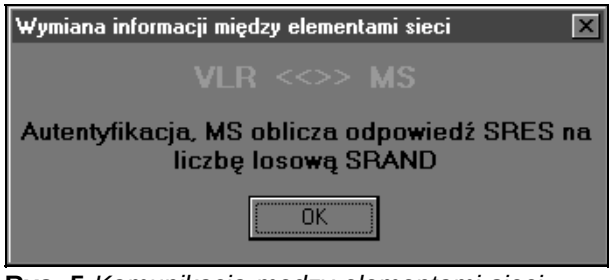
Rys. 3 *Główny formularz programu.*

Na Rys. 4 przedstawiony jest przykładowy ekran pokazujący przebieg komunikacji w kanale radiowym. Prezentowane są na nim informacje dotyczące kanału logicznego, kierunku transmisji oraz treści przesyłanego komunikatu.



Rys. 4 *Okno informacyjne kanału radiowego.*

Komunikacja pomiędzy elementami sieci prezentowana jest na osobnym formularzu programu (Rys. 5). Prezentowane są na nim treści wymienianych komunikatów oraz elementy sieci komunikujące się ze sobą (nadawca i odbiorca komunikatu). Równocześnie, na głównym formularzu ekranu (Rys. 3) aktywne elementy sieci są zaznaczane kolorem czerwonym.



Rys. 5 *Komunikacja mędzy elementami sieci.*

Przemieszczenie abonenta ruchomego może odbywać się jedynie w obrębie sąsiednich komórek, co jest zgodne z naturalnym sposobem przemieszczania w systemie GSM. Aby tego dokonać należy ustawić kursor myszy na komórce z ruchomym abonentem (oznaczona czerwoną obwódką), wcisnąć prawy przycisk myszy, ustawić kursor na innej, sąsiedniej komórce po czym kliknąć lewym przyciskiem[1].

Sieć komórek została podzielona na dwa **obszary centralowe**[2], z których każdy składa się z dwóch **obszarów przywoławczych**[3]. Dodatkowo po stronie sieci komórkowej znajduje się rejestr HLR, centrum autoryzacji AuC oraz centrala tranzytowa GMSC służąca do komunikacji z siecią PSTN (również zaznaczoną na ekranie). Dodatkowa centrala MSC (z rejestrem VLR)[4] jest wykorzystywana podczas zestawiania połączenia wychodzącego (przychodzącego) do (od) innego abonenta sieci komórkowej. W programie zakłada się, że ten "inny" abonent pozostaje zawsze pod kontrolą dodatkowej centrali MSC.

Użytkownik korzystając z opcji ***Zdarzenia*** w pasku menu ma możliwość wygenerowania następujących zdarzeń:

- **wyłączenie aparatu** - MS staje się niedostępny w sieci, możliwa jest zmiana jego lokalizacj, bez jakiegokolwiek komunikowania się ze stacjami bazowymi,

- **włączenia aparatu** - MS w ciągłej komunikacji ze stacjami bazowymi, rejestrowane są zmiany jego położenia względem obszarów przywołań,

Przy wybraniu tej opcji mamy do dyspozycji możliwość zrealizowania:

- **połączenia wychodzącego**,
- **połączenia przychodzego**

abonenta z innym abonentem GSM jak również sieci PSTN, a następnie:

- **rozłączenia tego połączenia**.

W przypadku gdy abonent ruchomy przemieszcza się pomiędzy dwoma komórkami będąc w stanie trwania połączenia występuje **handover**.

Łącznie zasymulowano w programie przebieg sygnalizacji dla 15 procedur:

- włączenie telefonu:
  - w starym obszarze przywołań
  - w nowym obszarze przywołań:
    - w starym obszarze centralowym

[1)] Można również stosować standardowy mechanizm systemu Windows: **drag-and-drop**.

[2)] pozostające pod kontrolą jednej centrali obszarowej MSC i zawierające jeden rejestr VLR.

[3)] posiadających ten sam identyfikator LAI.

[4)] umieszczona w górnej części ekranu i nie posiadająca numeru

- w nowym obszarze centralowym

- wyłączenie telefonu

- realizacja połączenia
  - wychodzącego:
    - do abonenta komórkowego
    - do abonenta sieci PSTN
  - przychodzącego:
    - od abonenta komórkowego
    - od abonenta sieci PSTN

- rozłączenie połączenia:
  - wychodzące (od abonenta komórkowego)
  - przychodzące (do abonenta komórkowego)

- handover:
  - między komórkami w obrębie jednego obszary przywoławczego
  - między obszarami przywoławczymi należącymi do jednego obszaru centralowego
  - między obszarami centralowymi

- aktualizacja położenia:
  - w nowym obszarze przywołań (w obrębie jednego obszaru centralowego)
  - w nowym obszarze centralowym

Przebieg ćwiczenia

1. Ćwiczenie rozpoczyna się krótkim sprawdzianem pisemnym (maks. 15 min), z zakresu niniejszej instrukcji i treści wykładowych.

2. Zapoznanie się z programem HLRVLR.

3. Zidentyfikować i wykonać wszystkie zaimplementowane w programie procedury. Uwaga! Znalezienie procedur niewymienionych w opisie ćwiczenia będzie osobno punktowane[1].

4. Wykonać 3 procedury wskazane przez prowadzącego i umieścić ich przebieg w sprawozdaniu, z uwzględnieniem wiadomości sygnalizacyjnych, kanałów logicznych oraz elementów sieci uczestniczących w sygnalizacji.

5. Dla wybranego przez prowadzącego ćwiczenie typu połączenia prześledzić i zapisać (jak w p.4) sygnalizację **od końca do końca**, tzn. z uwzględnieniem stron obu abonentów.

[1)] Nie należy przyjmować za pewnik, że takie procedury istnieją.

Bibliografia

- Hołubowicz W., Płóciennik P., Różański A., "Systemy łączności bezprzewodowej", rozdz. 3, Poznań 1997
- Dąbrowski M., "Systemy komórkowe", CITCOM-PW 1996
- Cichocki J., Kołakowski J., "Systemy telefonii komórkowej GSM", skrypt do wykładu prowadzonego w IR PW
- Hołubowicz W., Płóciennik P., "GSM - cyfrowy system telefonii komórkowej", Poznań 1995