PROBLÉM NELEGÁLNÍHO ODPOSLECHU A JEHO DETEKCE V SÍTI GSM A UMTS

Pavel Bezpalec, Michal Kašík

Katedra telekomunikační techniky
FEL, ČVUT v Praze

Shrnutí

- Protokoly standardu GSM jsou známy i dobře popsány
- GSM šifry A5/1 a A5/2 jsou již prolomeny

- Vývoj jde kupředu
  - komunikační- možnosti v telekomunikačních a datových sítí-ch
  - technologie a metody- odposlechů na komunikačních kanálech GSM
    - a se zpožděním i
  - technologie odhalování a lokalizace takovýchto odposlechů

? otázky ?

- Je nebezpečí nelegálního odposlechu reálné?
- Je nutné zařízení snadno dostupné ?
- Lze se proti jeho nasazení bránit?
- Jak?

Výskyt v ČR – vyjádření autorit

Tomáš Almer, ředitel útvaru zvláštních činností PČR

- „Při své činnosti narážíme náhodou na zařízení podobná Agátě“
  - ČT 14.5.2012
    - http://www.ceskatelevize.cz/ivysilani/10101491767-studio-ct24/212411058260514

- „Na Agátu narážejí policisté v terénu, když odposlouchávají podezřelé během vyšetřování. Naposledy v hlavním městě, ale míst, kde se zařízení používá, je po republice více. Myslím, že se nespletu, když řeknu, že četnost se zvyšuje.“
  - ČT 15.8.2012
    - http://www.ceskatelevize.cz/ct24/domaci/192240-odposlouchavat-mobil-je-s-agatou-snadne-jeji-porizeni-vyjde-na-miliony/

Dostupnost: www.alibaba.com

Dostupnost: www.alibaba.com

Alibaba.com
Global trade starts here.™

Products | What are you looking for...

Home > Products > Telecommunications > Communication Equipment > Other Telecommunications Products (132860)

See larger image

PGSM (Passive GSM Monitoring System)

FOB Price: Get Latest Price

Contact Supplier | Leave Messages

Add to Inquiry Cart | Add to My Favorites

Product Details | Company Profile

Report Suspicious Activity

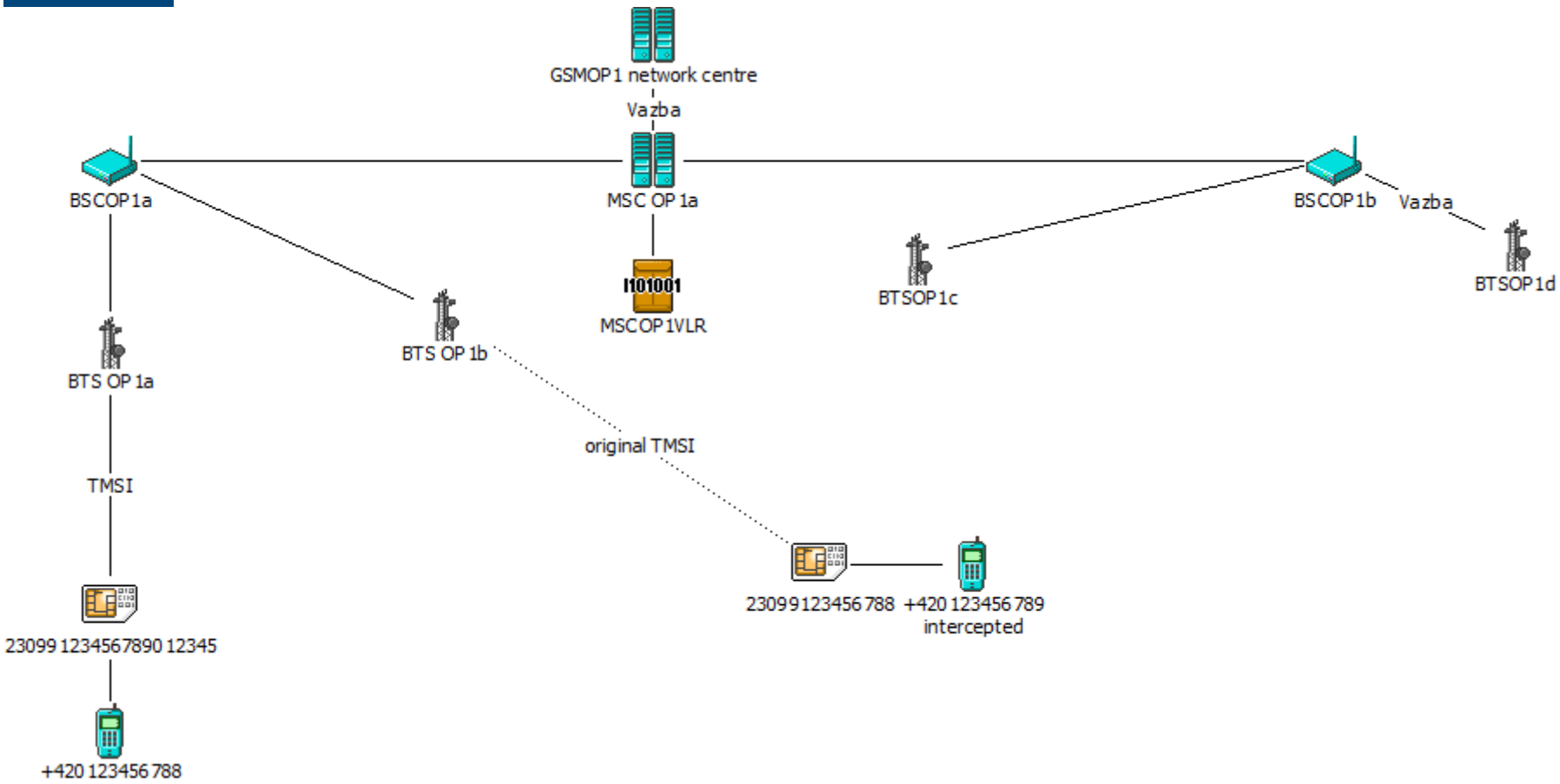
Obrana proti odposlechu

- **Šifrovací telefony**
  - Musí je používat i Vaši partneři a vyžadují kázeň a trpělivost
  - Peer-to-Peer zařízení jsou bezpečná
  - Zašifrované sítě jsou zranitelné DoS útokem na servery
- **Použití terestrických linek**
  - Ano, ale při dnešních zvyklostech jejich použití vyžaduje velkou kázeň od uživatelů
  - Nebývají všude dostupné
  - Jsou stejně zranitelné jako mobilní
- **Běžné prohlídky kanceláří – zcela neúčinné**
- **Detekce**
  - poskytne vodítko o nezákonné aktivitě protivníka
  - **důležitá výhoda !!!**

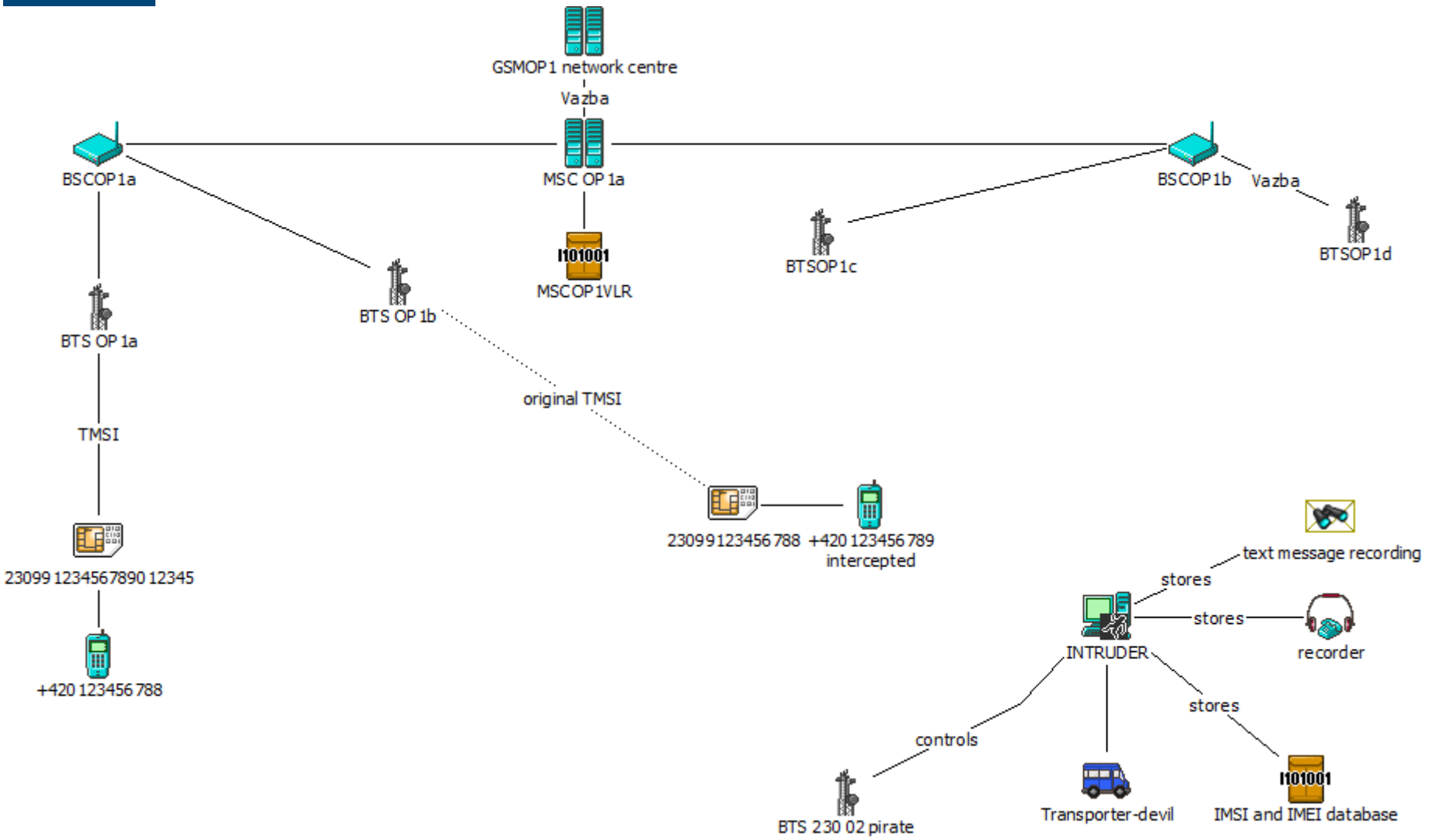
MAN IN THE MIDDLE

- Princip známý již více jak 200 let, poprvé použit s vynálezem telegrafu.
- Podstata
  - snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem
- Využívá zranitelnosti všech systémů, které ověřují identitu koncových uzlů pouze ve směru uživatel → síť
- MIM je obvykle detekovatelný pomocí pozice, která se neshoduje s předpokládanou pozicí.
  - v případě telegrafu i mobilní sítě

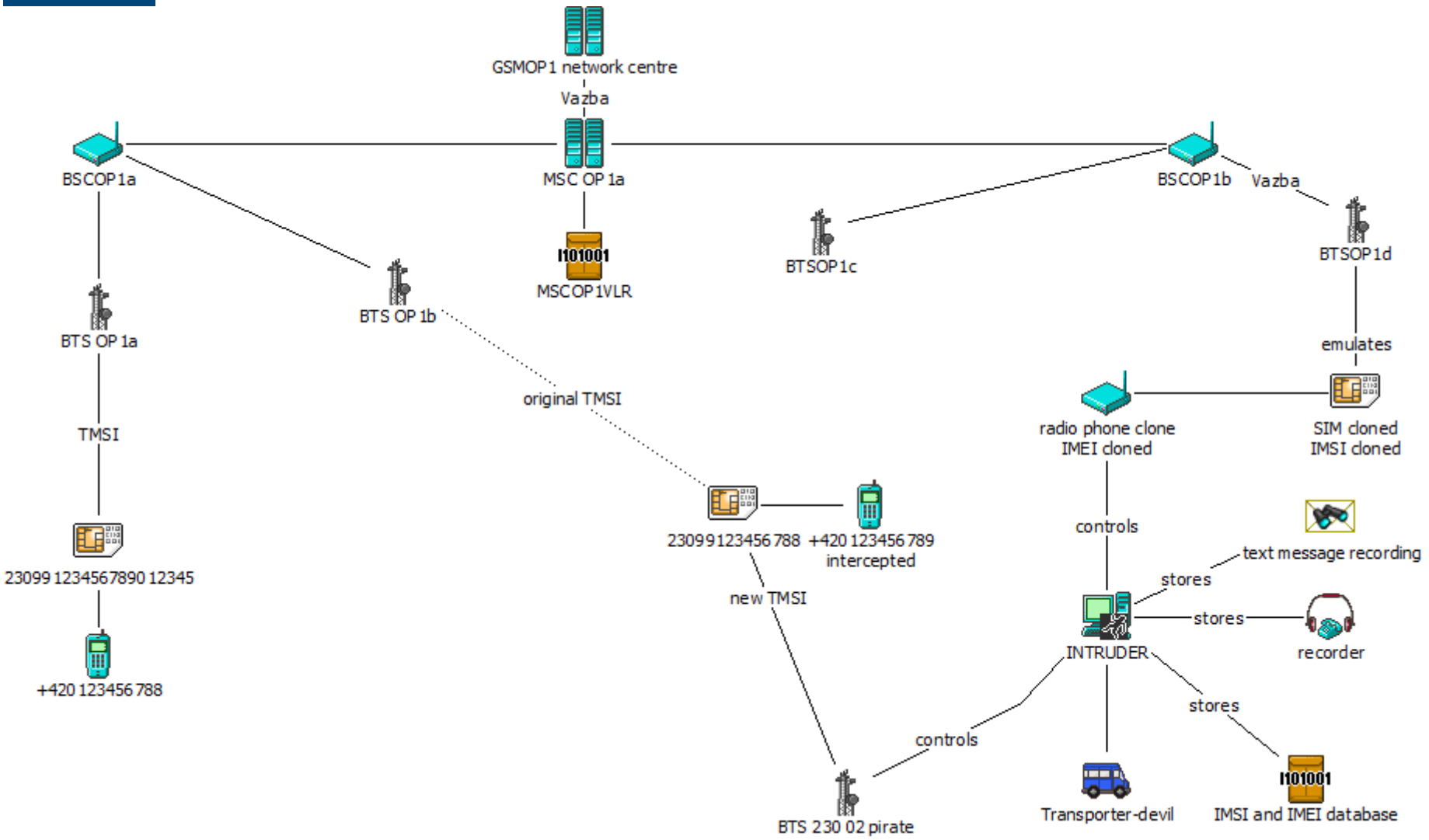
Stav bez odposlechu



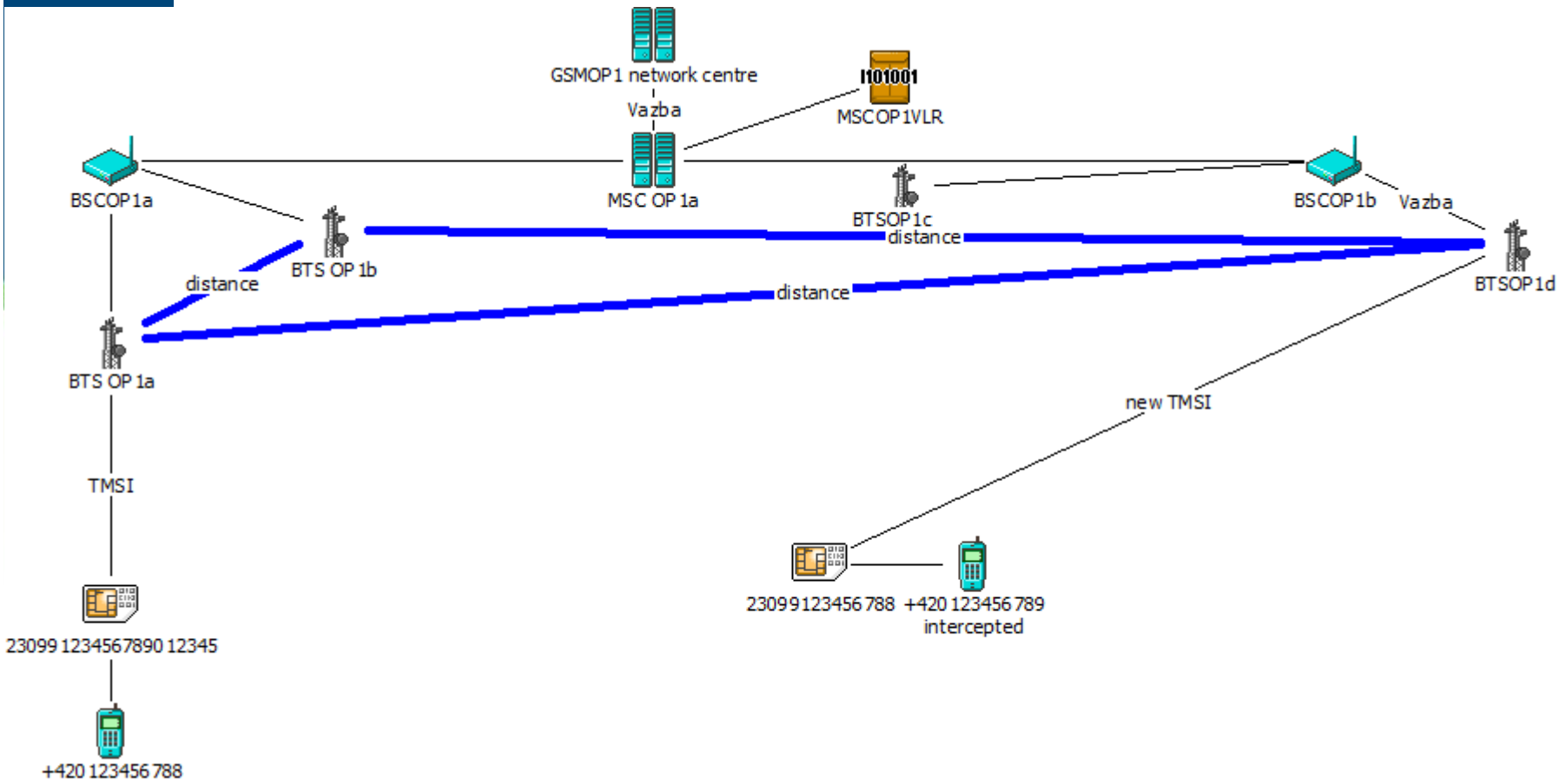
Příprava semiaktivního odposlechu



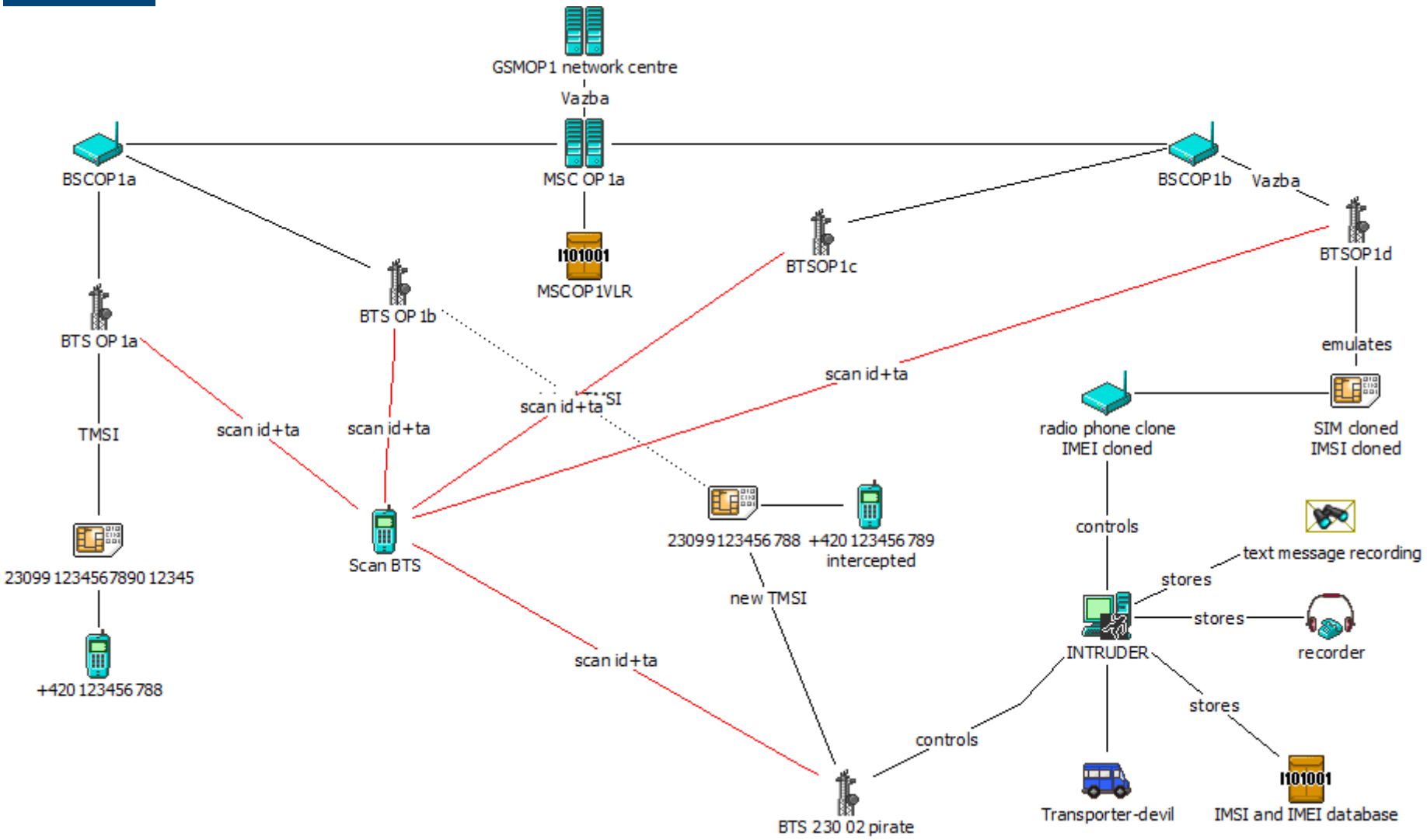
Stav při semiaktivním odposlechu



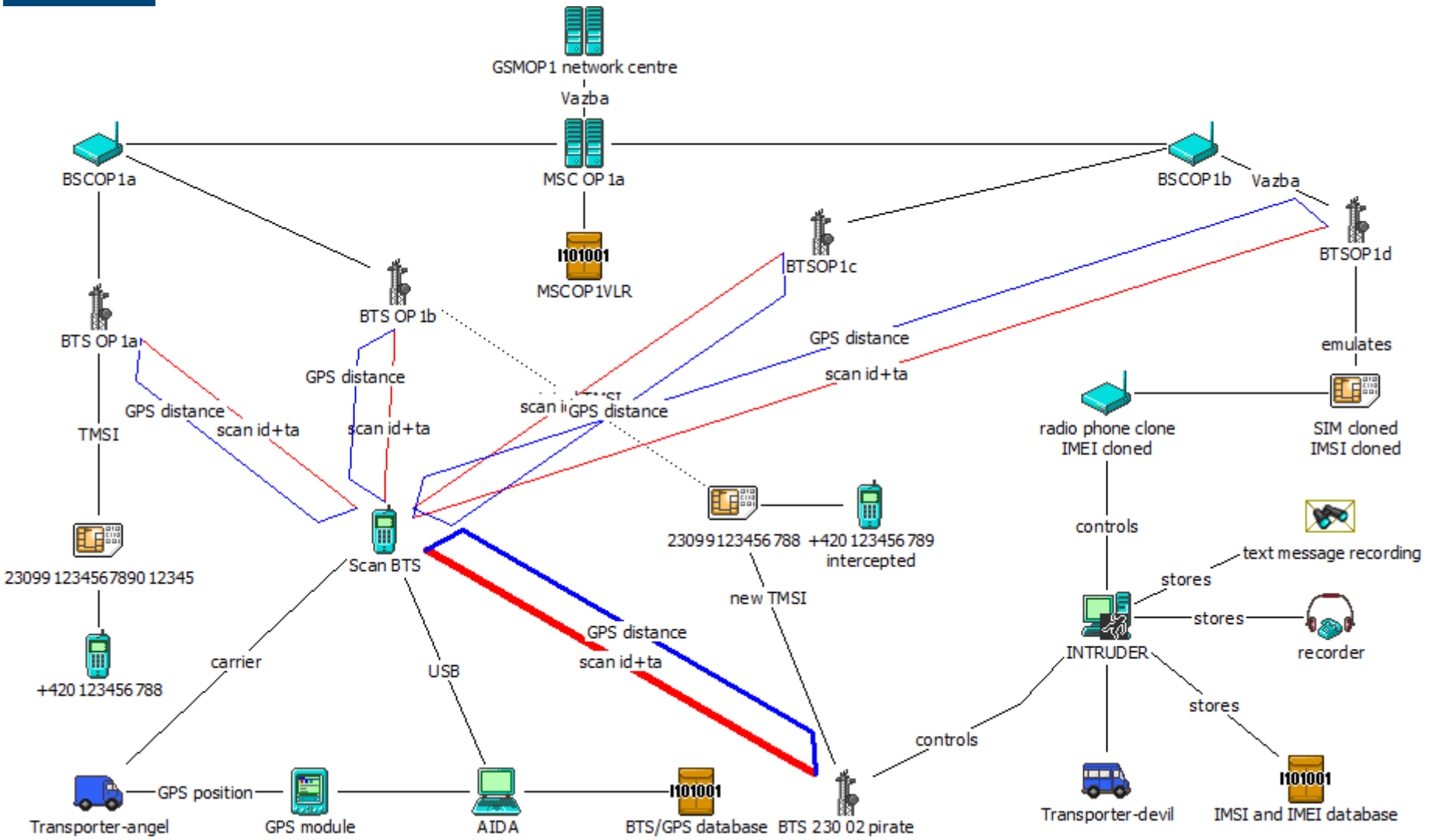
Náhled z dohledového centra GSM sítě



Detekce pomocí detektoru – měření



Detekce pomocí detektoru – vyhodnocení



Náhled z dohledového centra – klon je regulérním mobilním zařízením

- V oblasti pokryté signálem UMTS je nasazen jammer malého výkonu
  - Ten přinutí cílový telefon MS přejít od pásma GSM.
- Z pohledu dohledového centra nedojde k masovému výpadku na UMTS síti.
- Radiový klon telefonu se objeví ve VLR různých MSC.
  - Analýza tak obrovského množství dat je v reálném čase nemožná
  - Kritérium stanovení vzdálenosti mezi BTS na jejichž VLR je telefon registrován, je v praxi nepoužitelné.
- Hypoteticky je možno nasazení určit z výpisu telekomunikačního provozu MS, kde dojde k neočekávané změně buňky při nasazení odposlechu na MS, aniž by zařízení MS změnilo polohu.

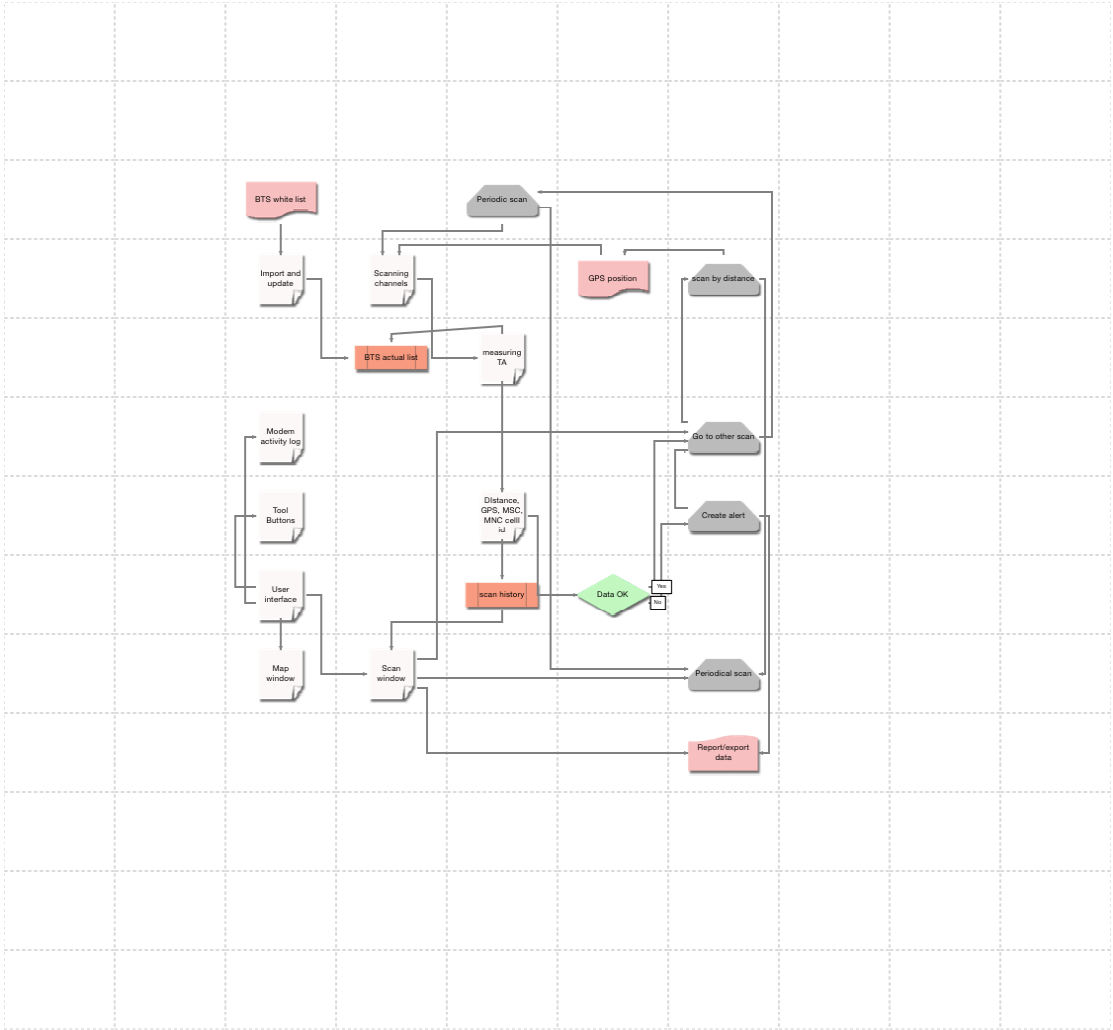
Aplikace a její funkce

- Hlavní funkce – schopnost detekce BTS na všech GSM kanálech

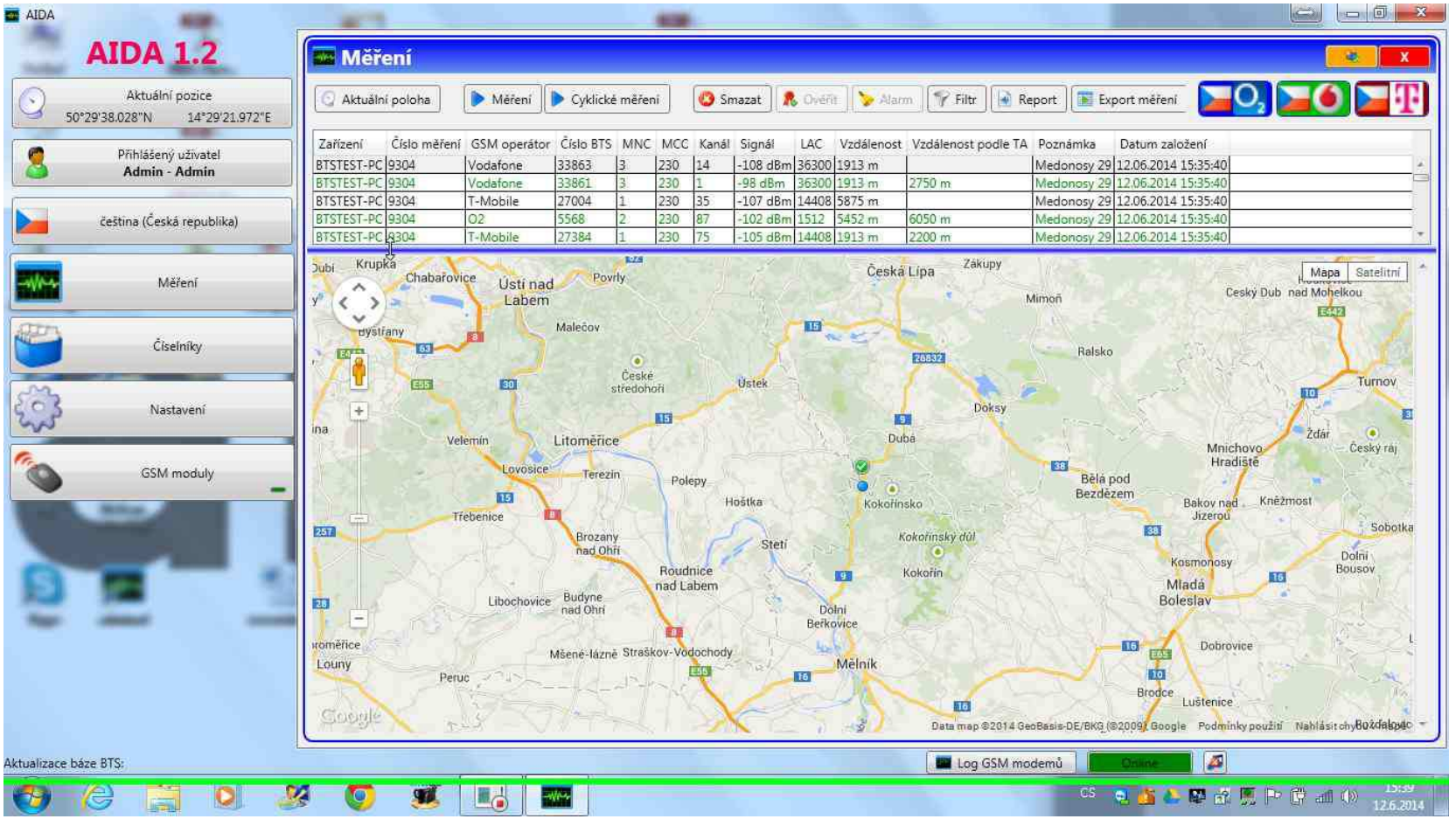
- Princip
  1. Mapování GSM prostředí
     - sken všech kanálů a hledání buněk příslušných BTS
  2. Zjištění TA na nalezených BTS
  3. Porovnání nalezeného stavu se skutečností a zjištění odchylek
     - mezi očekávanou pozicí buňky BTS, vypočtenou vzdáleností a změřeným TA
     - Dojde-li k rozporu ➔ systém rozešle upozornění
     - Je-li podezření na přítomnost účastníka, je možno mobilní jednotku instalovat do libovolného automobilu s 12 V napájením a provést triangulaci k zjištění přibližné polohy účastníka.

- Systém je na trhu pod komerčním názvem AIDA.

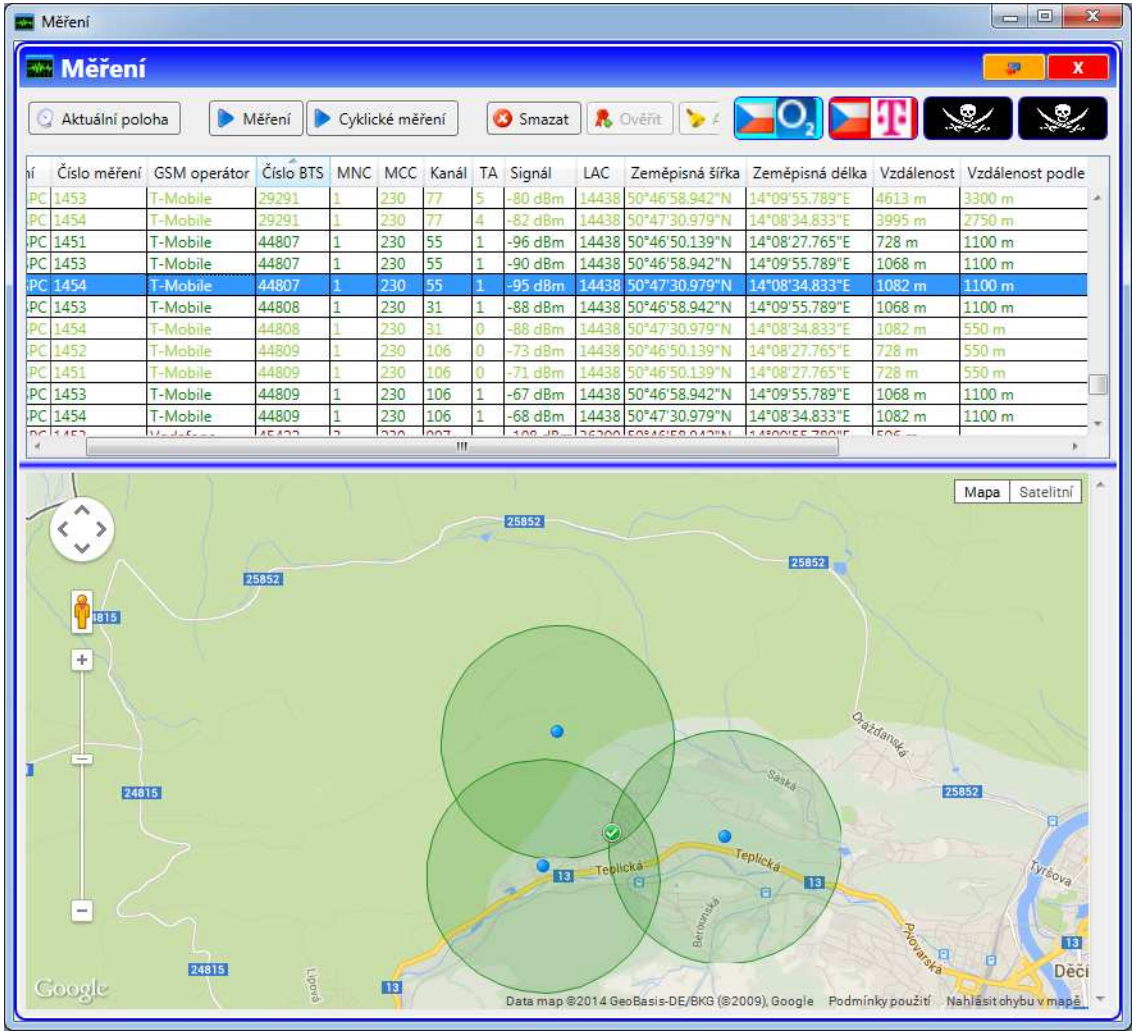
Aplikace – procesní schema



Aplikace – uživatelské rozhraní



TriAngulace od Time Advance parametru



Praktická ukázka

Department of Telecommunications Engineering
of Czech Technical University in Prague
is one of major players of the Czech telecommunications environment.