



# 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 sítích
  - technologie a metody- odposlechů na komunikačních kanálech GSM
    - a se zpoždění-m 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](http://www.alibaba.com)

Welcome Ziy, Sign In (Not you?) | Chat online free with [TradeManager](#) Buy Sell Community My Alibaba My Favorites Help

**Alibaba.com** Global trade starts here.™

Products Suppliers Buyers Buy on [Alibaba.com](#) or [AliExpress.com](#)

passive dual gsm interception [Search Products](#)

About 1 results: Other Police & Military Supplies (1) [Advanced Search](#)

Home > Products > Security & Protection > Police & Military Supplies > **Other Police & Military Supplies (35571)** [Language Options](#)



**Passive GSM (Dual Band) / CDMA Monitoring System**

FOB Price: [Get Latest Price](#)

**Mr. Md. Astraf Uz Zaman**  
 Offline

[Contact Supplier](#)  
Send a Message to this Supplier

**Supplier Details**

**Ezzy Enterprise**  
[ Bangladesh ]  
Business Type:  
Trading Company, Agent,  
Distributor/Wholesaler  
[Contact Details](#)

Online Showroom: 39 Products  
[View this Supplier's Website](#)

[See larger image: Passive GSM \(Dual Band\) / CDMA Monitoring System](#)

[Add to My Favorites](#)

[Product Details](#) [Company Profile](#) [Report Item](#)





# Dostupnost: [www.alibaba.com](http://www.alibaba.com)



Products ▾

What are you looking for...



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



ZOOM

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 !!!**



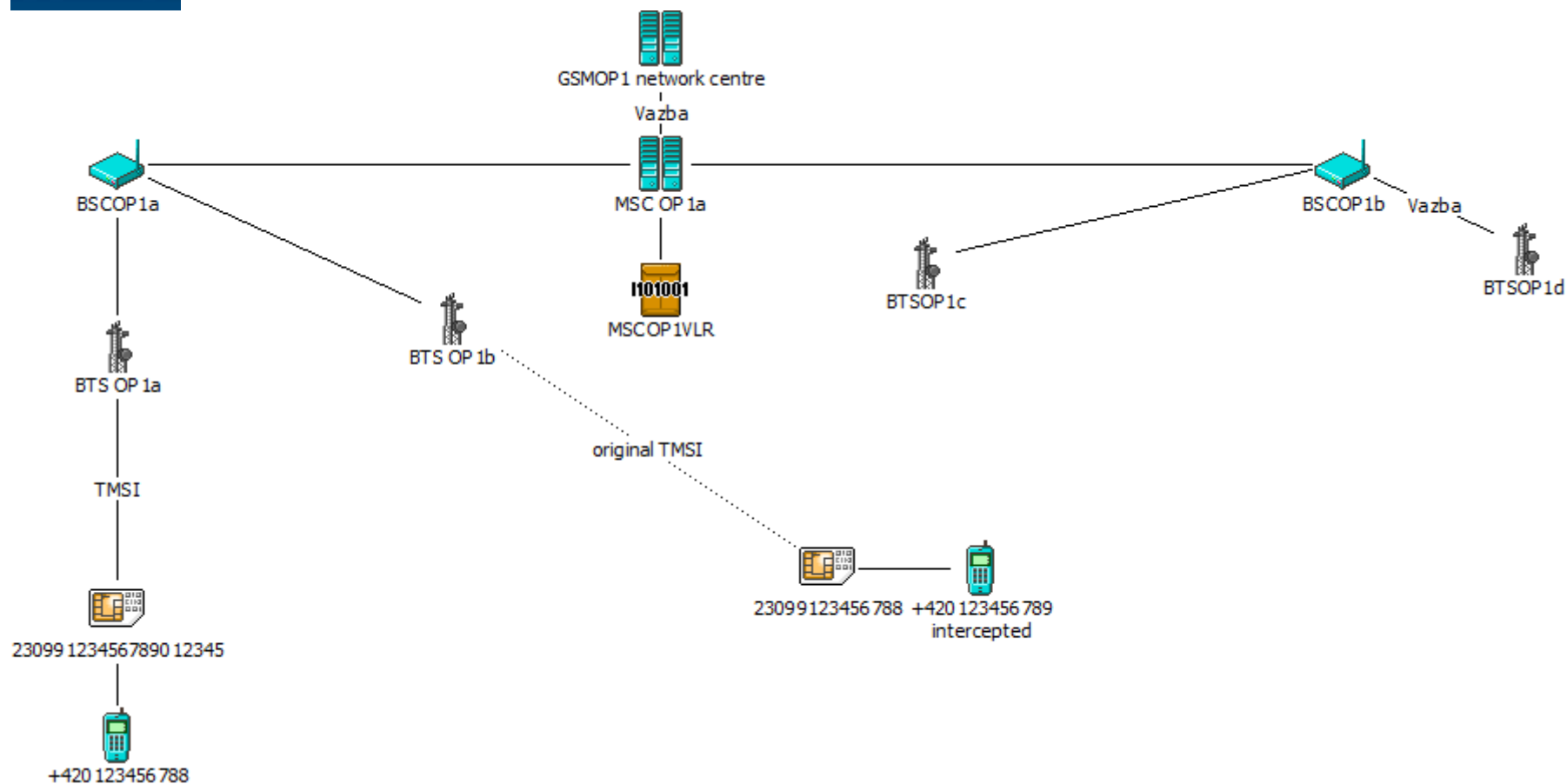
## MAN IN THE MIDDLE

- 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



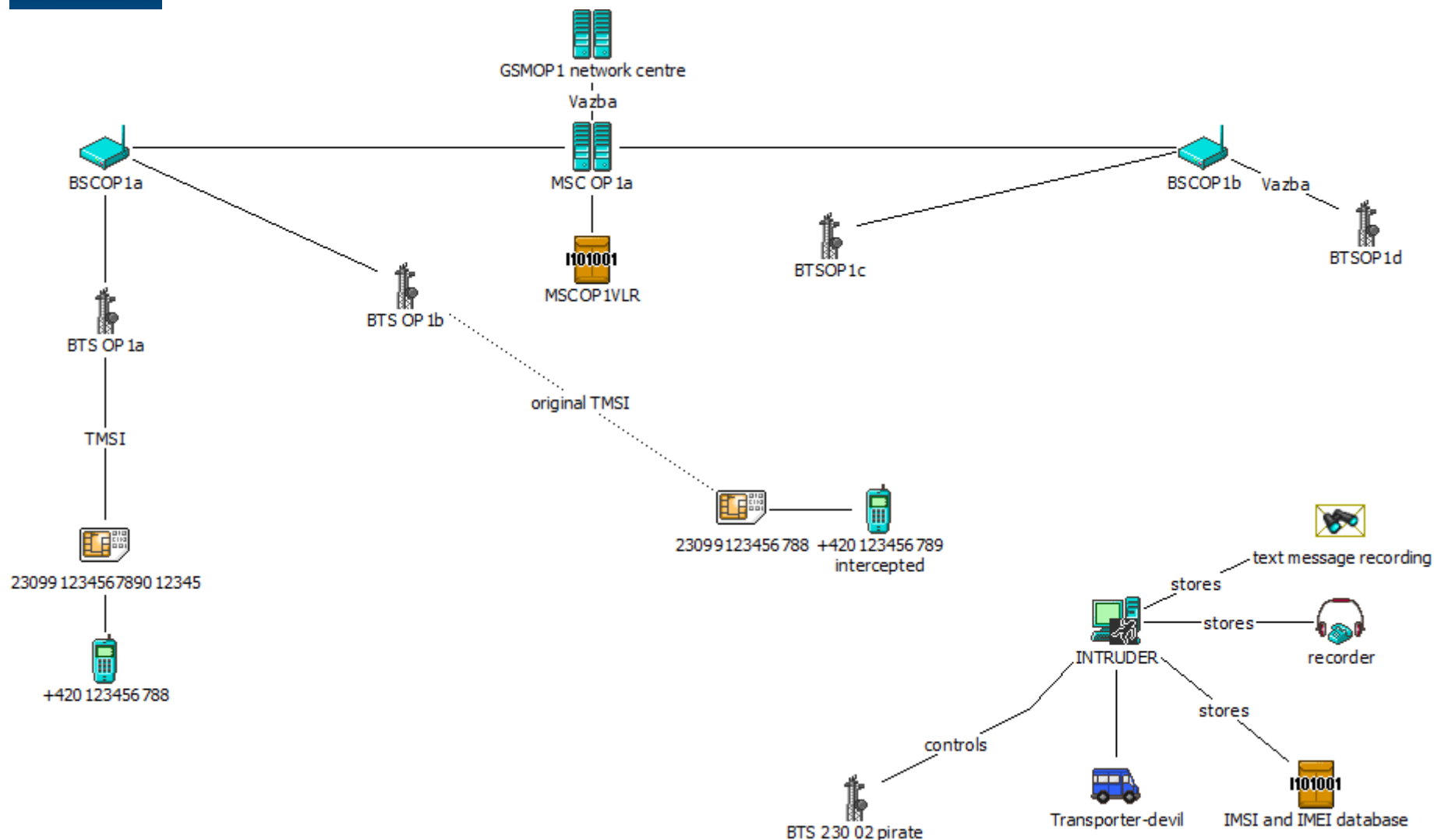


# Stav bez odposlechu



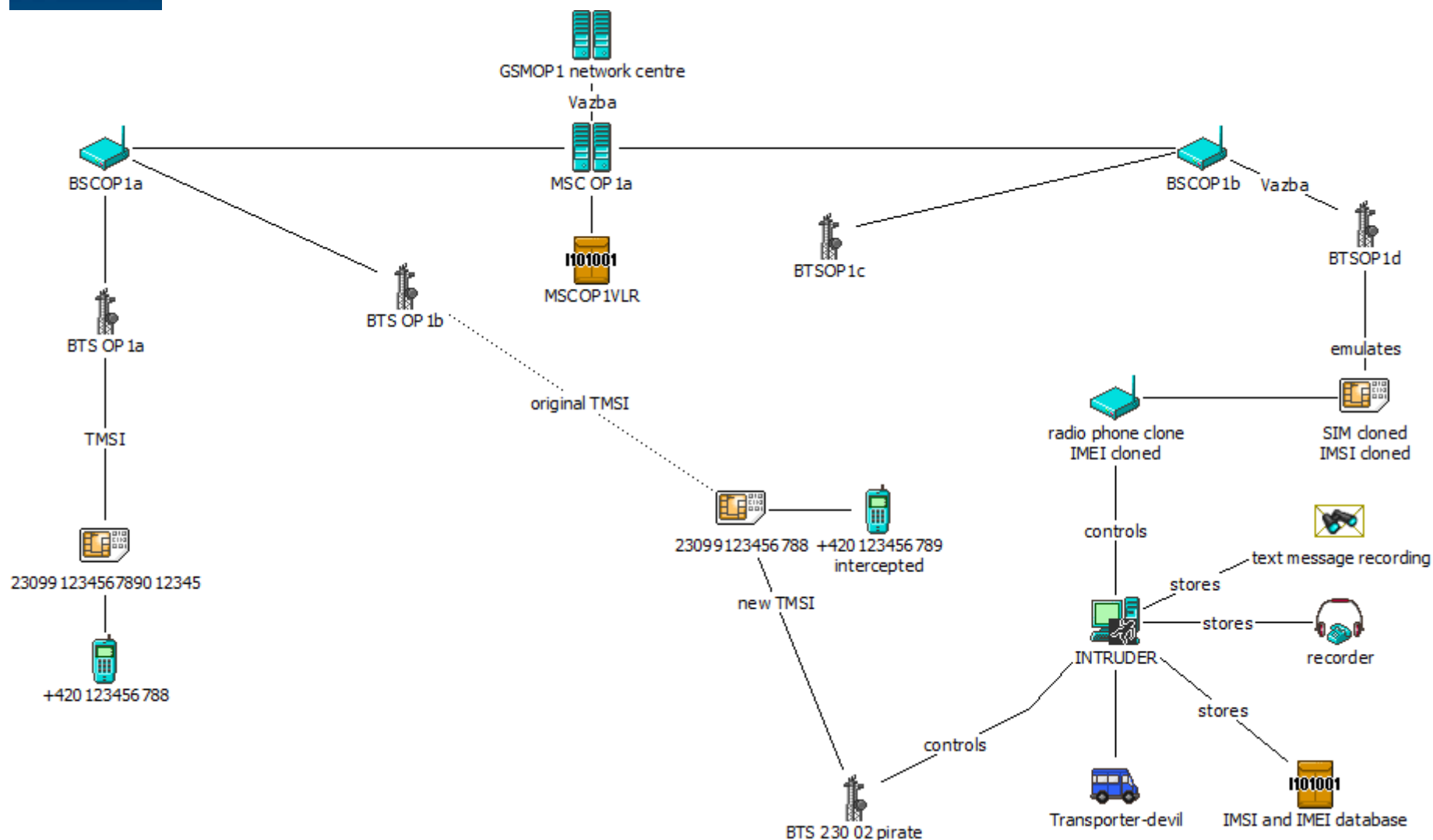


# Příprava semiaktivního odposlechu



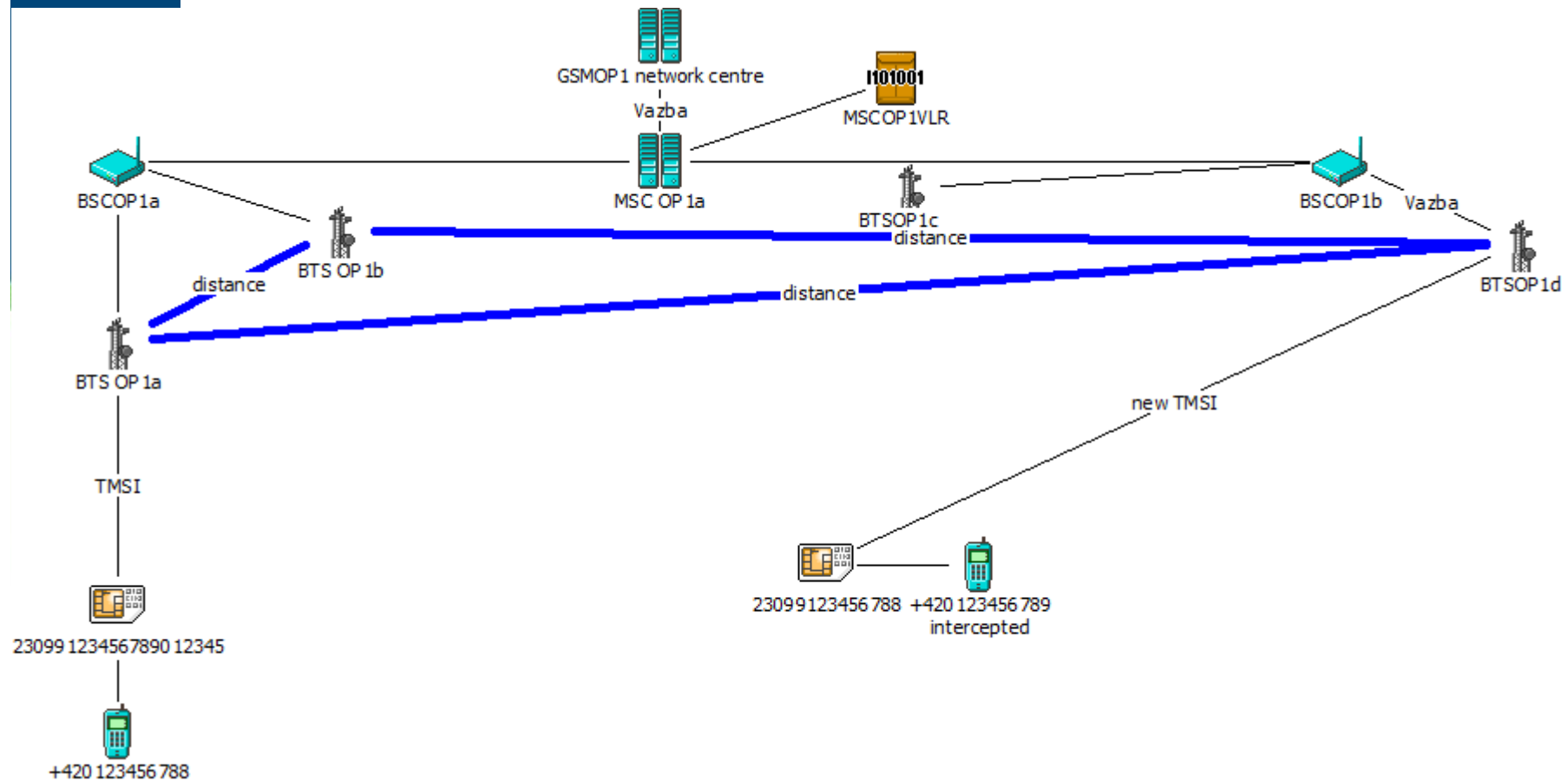


# Stav při semiaktivním odposlechu



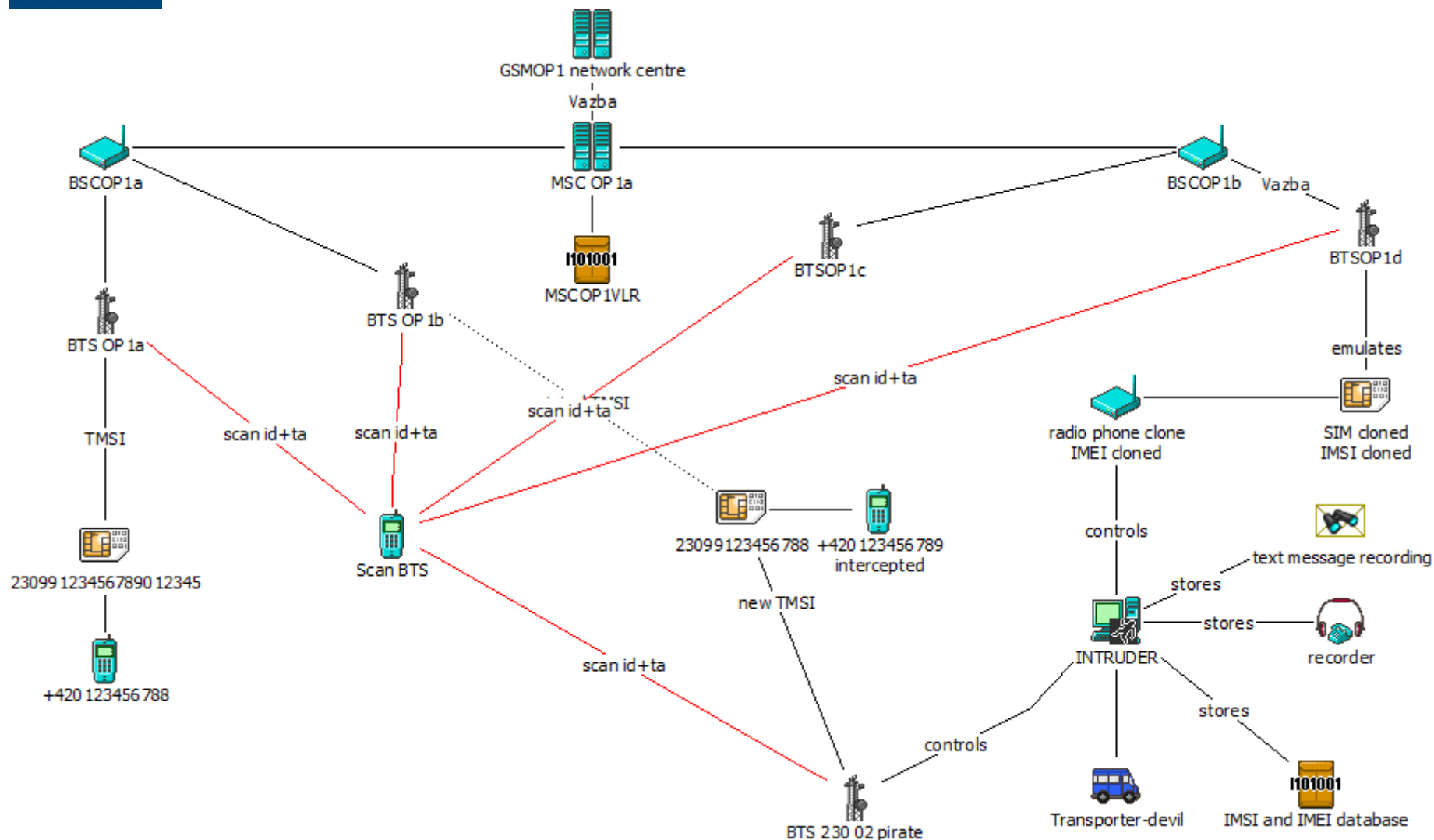


# Náhled z dohledového centra GSM sítě





# Detekce pomocí detektoru – měření







## 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.



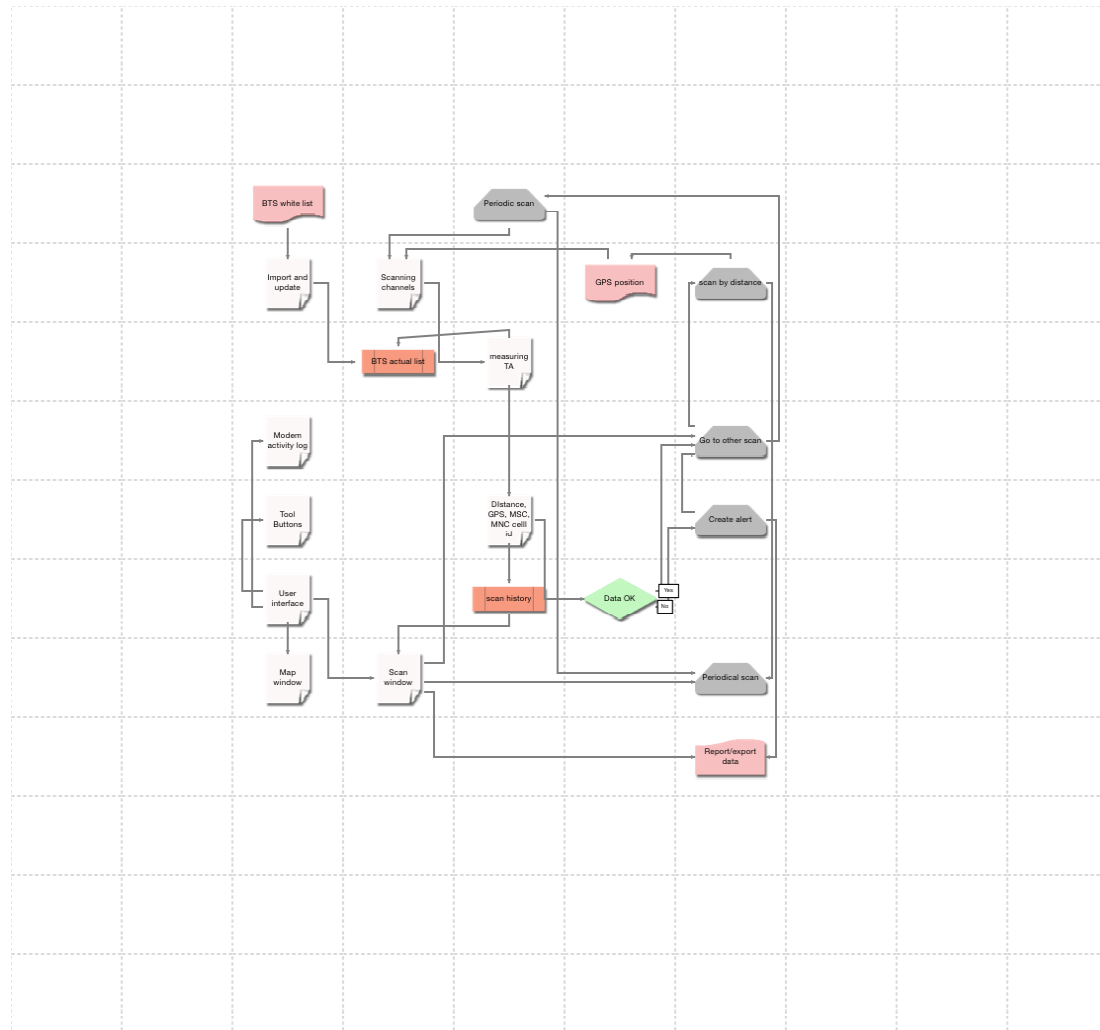
# Aplikace a její funkce

- 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 schéma





# Aplikace – uživatelské rozhraní

**AIDA 1.2**

Aktuální pozice  
50°29'38.028"N 14°29'21.972"E

Přihlášený uživatel  
**Admin - Admin**

čeština (Česká republika)

Měření

Číselníky

Nastavení

GSM moduly

**Měření**

Aktuální poloha Měření Cyklické měření Šmazat Ověřit Alarm Filtr Report Export měření

Zařízení	Číslo měření	GSM operátor	Číslo BTS	MNC	MCC	Kanál	Signál	LAC	Vzdálenost	Vzdálenost podle TA	Poznámka	Datum založení
BTSTEST-PC	9304	Vodafone	33863	3	230	14	-108 dBm	36300	1913 m		Medonosy 29	12.06.2014 15:35:40
BTSTEST-PC	9304	Vodafone	33861	3	230	1	-98 dBm	36300	1913 m	2750 m	Medonosy 29	12.06.2014 15:35:40
BTSTEST-PC	9304	T-Mobile	27004	1	230	35	-107 dBm	14408	5875 m		Medonosy 29	12.06.2014 15:35:40
BTSTEST-PC	9304	O2	5568	2	230	87	-102 dBm	1512	5452 m	6050 m	Medonosy 29	12.06.2014 15:35:40
BTSTEST-PC	9304	T-Mobile	27384	1	230	75	-105 dBm	14408	1913 m	2200 m	Medonosy 29	12.06.2014 15:35:40

Mapa Satelitní

Google

Data map ©2014 GeoBasis-DE/6K3 ©2009 Google Podmínky použití Nahlasit chybu

Aktualizace báze BTS: Log GSM modemů Online

CS 13:39 12.6.2014



# TriAngulace od Time Advance parametru

Měření

**Měření**

Aktuální poloha Měření Cyklické měření Smazat Ověřit

Ní	Číslo měření	GSM operátor	Číslo BTS	MNC	MCC	Kaná	TA	Signál	LAC	Zeměpisná šířka	Zeměpisná délka	Vzdálenost	Vzdálenost podle
PC	1453	T-Mobile	29291	1	230	77	5	-80 dBm	14438	50°46'58.942"N	14°09'55.789"E	4613 m	3300 m
PC	1454	T-Mobile	29291	1	230	77	4	-82 dBm	14438	50°47'30.979"N	14°08'34.833"E	3995 m	2750 m
PC	1451	T-Mobile	44807	1	230	55	1	-96 dBm	14438	50°46'50.139"N	14°08'27.765"E	728 m	1100 m
PC	1453	T-Mobile	44807	1	230	55	1	-90 dBm	14438	50°46'58.942"N	14°09'55.789"E	1068 m	1100 m
PC	1454	T-Mobile	44807	1	230	55	1	-95 dBm	14438	50°47'30.979"N	14°08'34.833"E	1082 m	1100 m
PC	1453	T-Mobile	44808	1	230	31	1	-88 dBm	14438	50°46'58.942"N	14°09'55.789"E	1068 m	1100 m
PC	1454	T-Mobile	44808	1	230	31	0	-88 dBm	14438	50°47'30.979"N	14°08'34.833"E	1082 m	550 m
PC	1452	T-Mobile	44809	1	230	106	0	-73 dBm	14438	50°46'50.139"N	14°08'27.765"E	728 m	550 m
PC	1451	T-Mobile	44809	1	230	106	0	-71 dBm	14438	50°46'50.139"N	14°08'27.765"E	728 m	550 m
PC	1453	T-Mobile	44809	1	230	106	1	-67 dBm	14438	50°46'58.942"N	14°09'55.789"E	1068 m	1100 m
PC	1454	T-Mobile	44809	1	230	106	1	-68 dBm	14438	50°47'30.979"N	14°08'34.833"E	1082 m	1100 m

Mapa Satelitní

Data map ©2014 GeoBasis-DE/BKG (©2009), Google Podmínky použití Nahlásit chybu v mapě



# Praktická ukázka





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