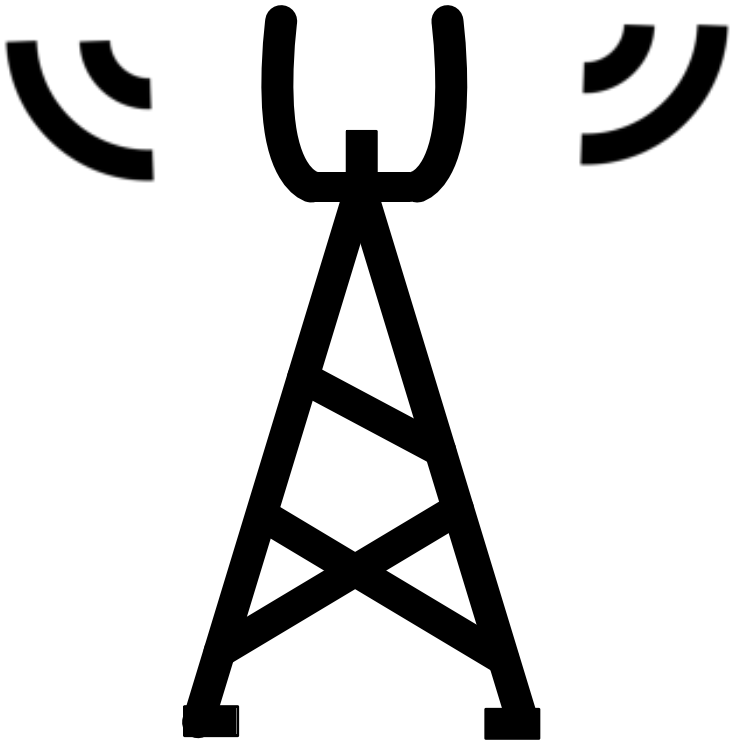
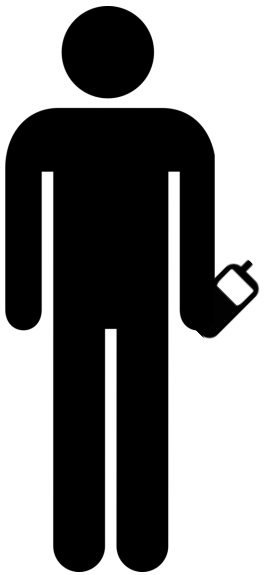
Location Privacy without Carrier Cooperation

Keen Sung Brian Neil Levine Marc Liberatore
School of Computer Science
University of Massachusetts Amherst

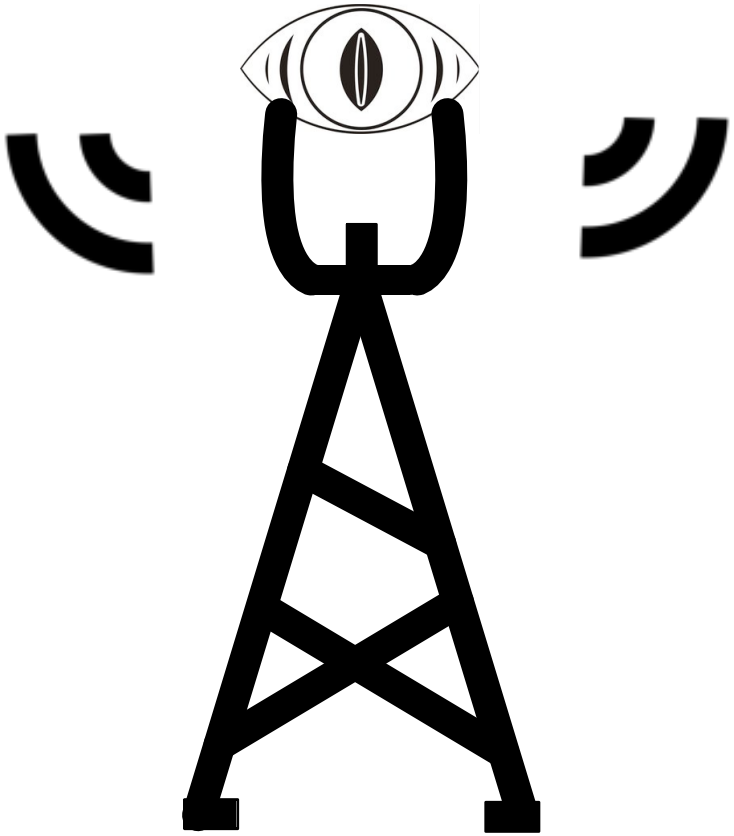
Supported in part by NSF award CNS-0905349

Mobile network operators can track location by associating SIM cards with cell towers

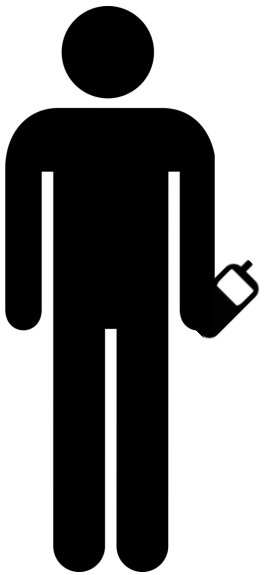




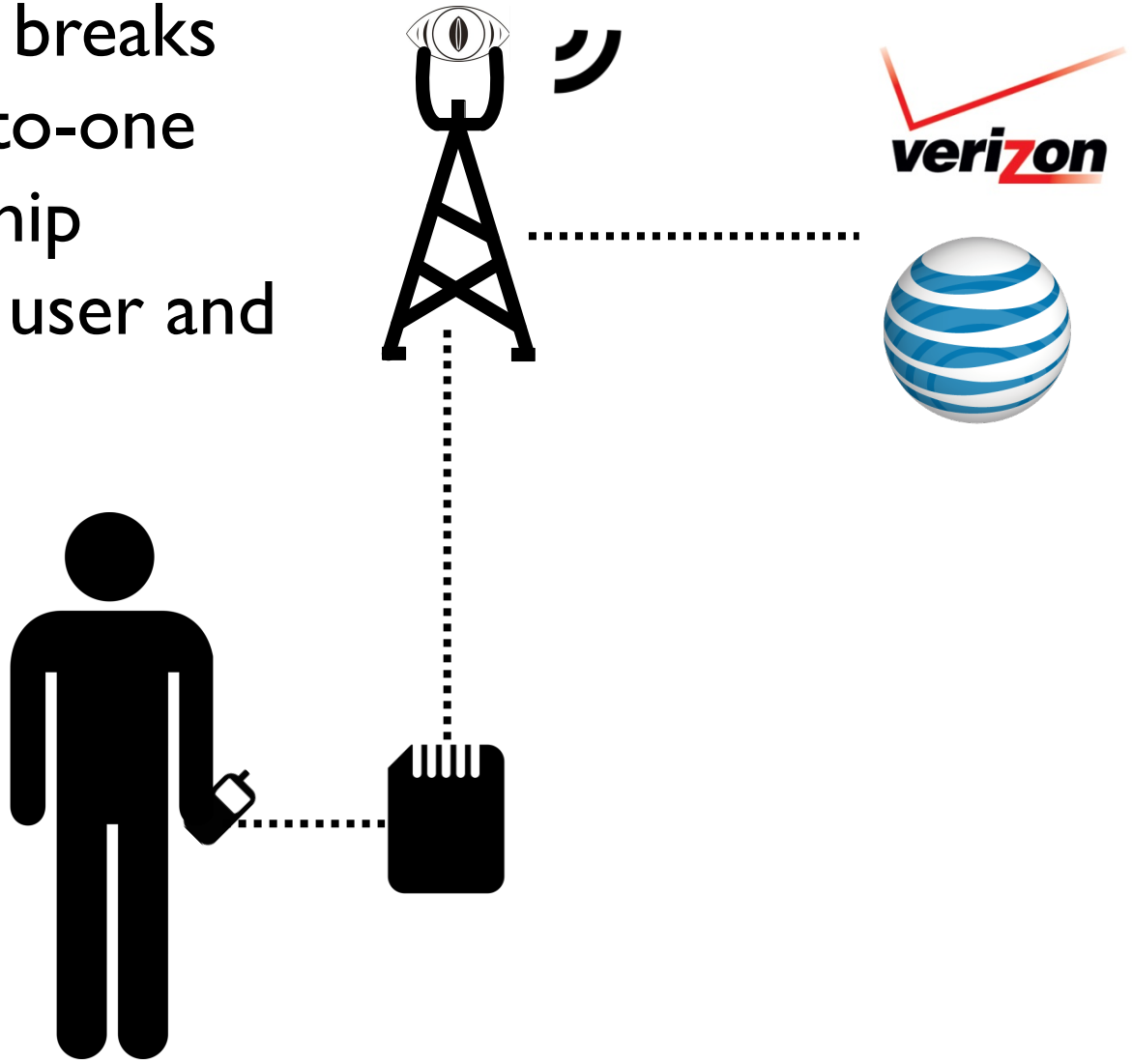
Mobile network operators can track location by associating SIM cards with cell towers



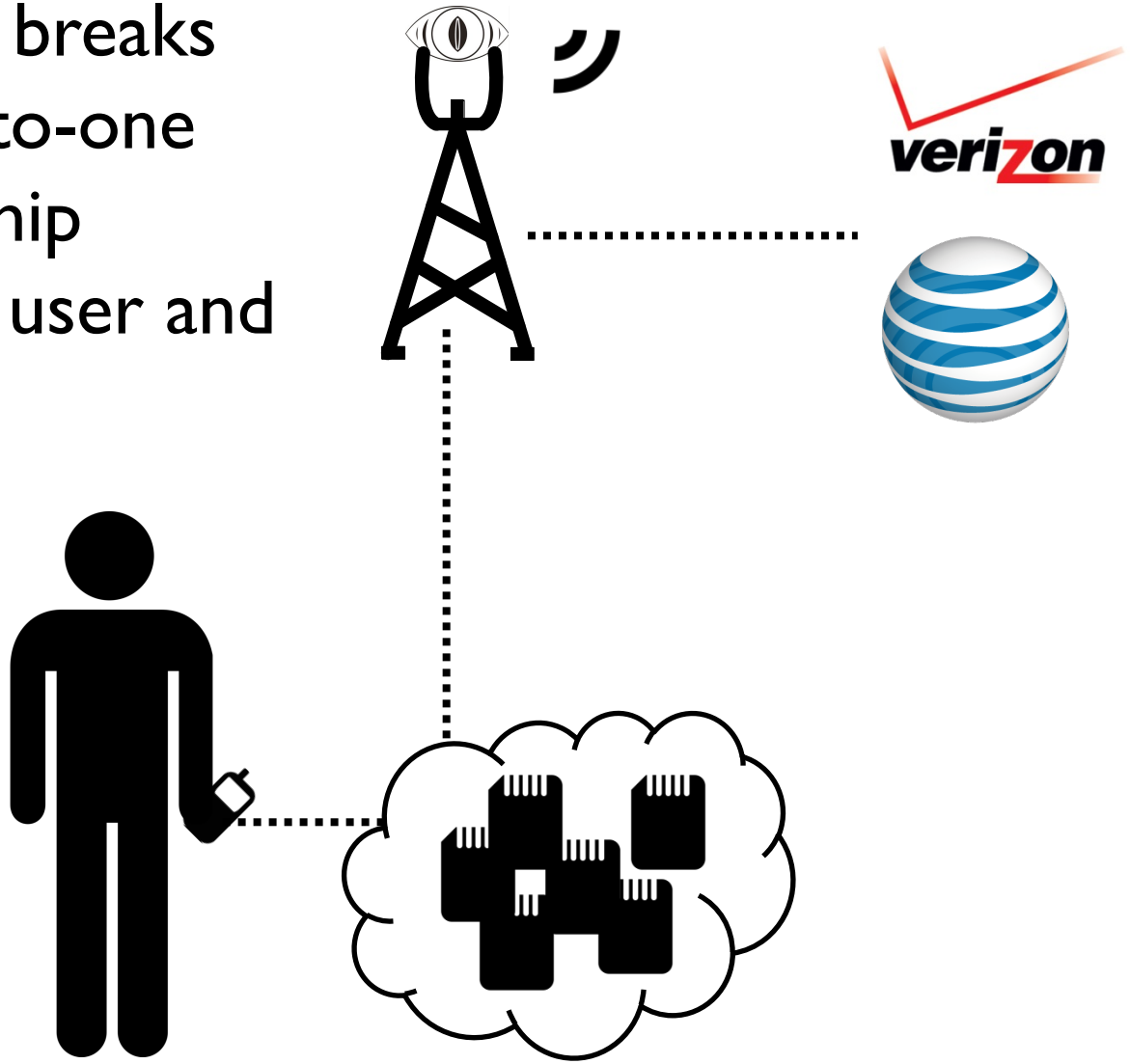
Mobile users want location privacy

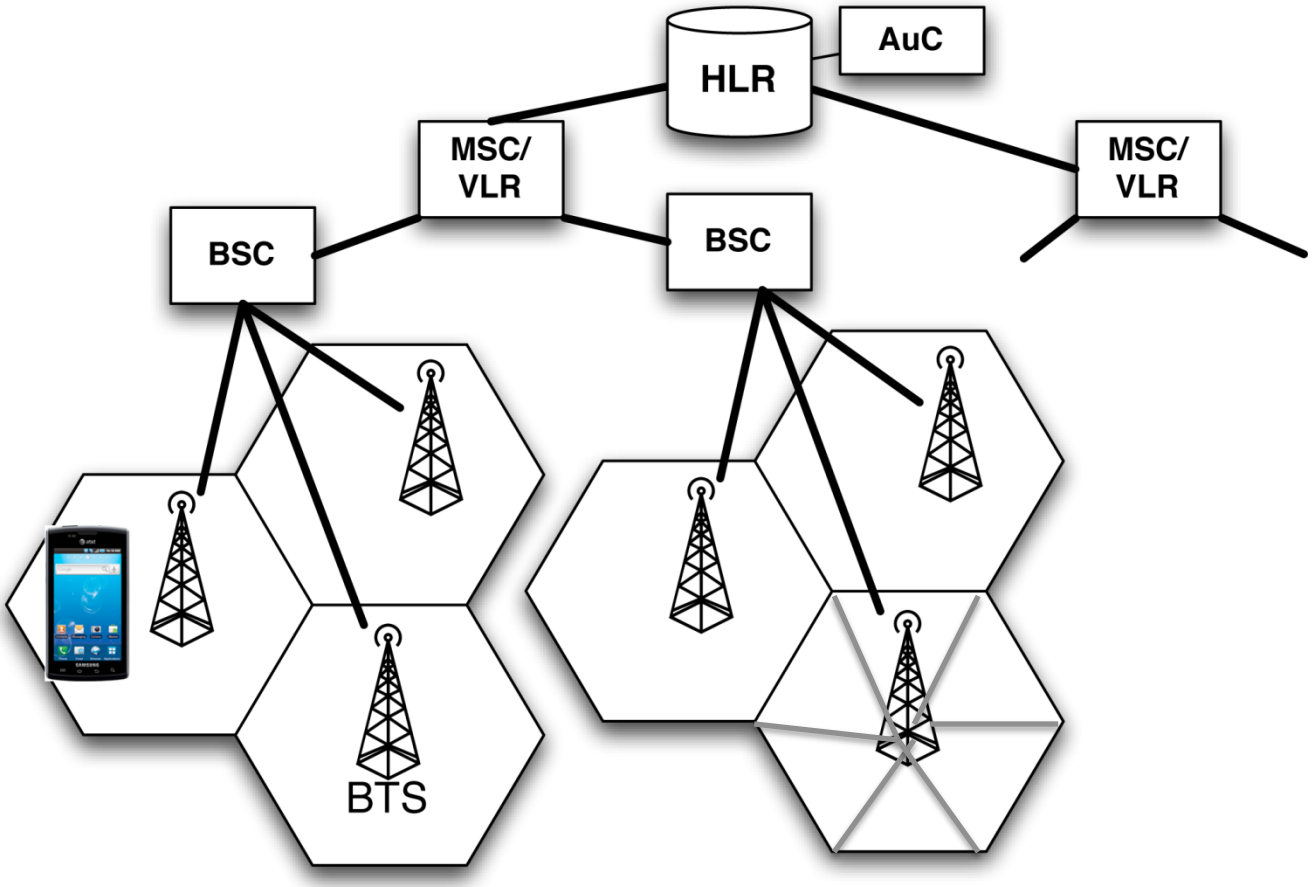


ZipPhone breaks the one-to-one relationship between user and SIM card

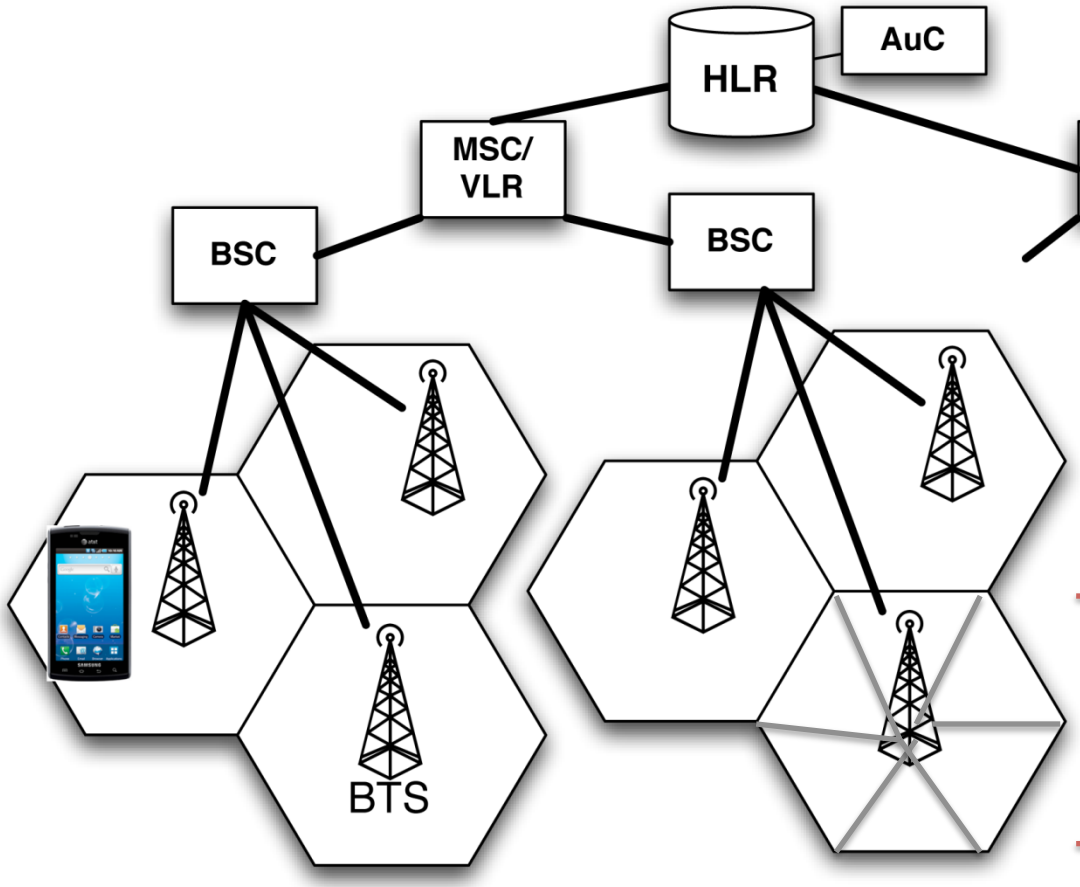


ZipPhone breaks the one-to-one relationship between user and SIM card





Cell: 1–100km^2



One HLR rule them

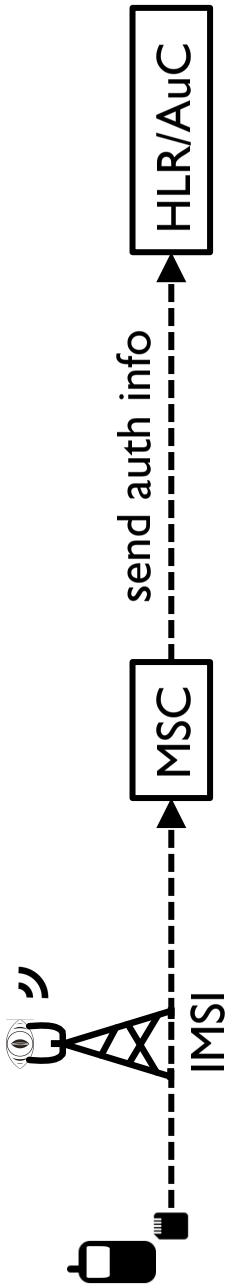
MSC manages several location areas

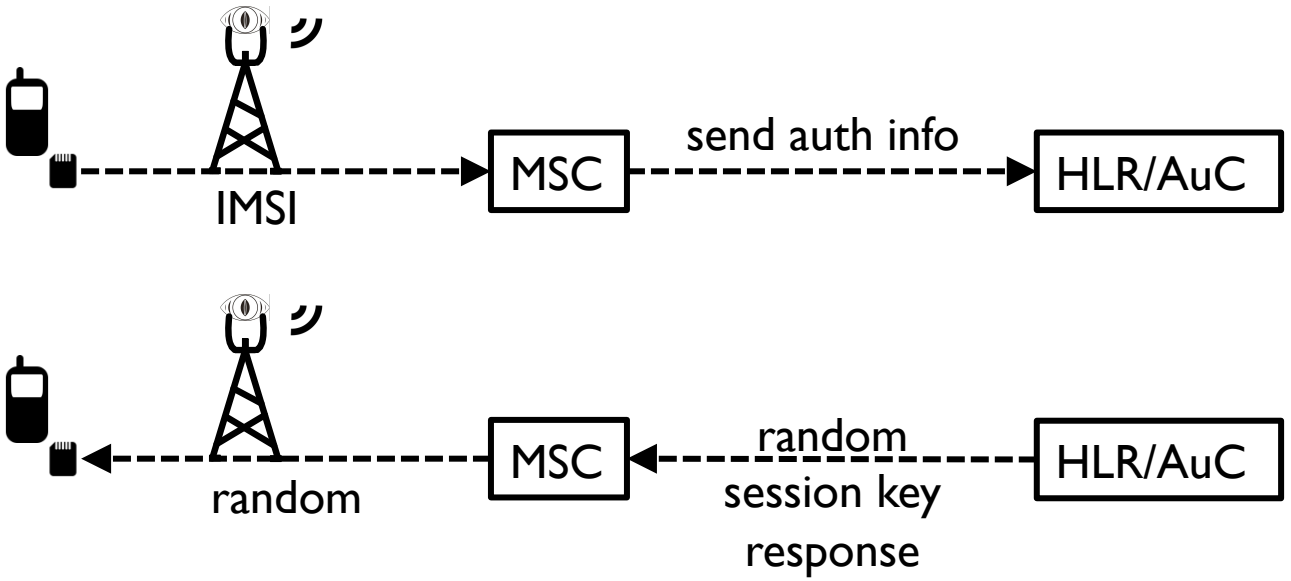
Location Area includes several BTSes

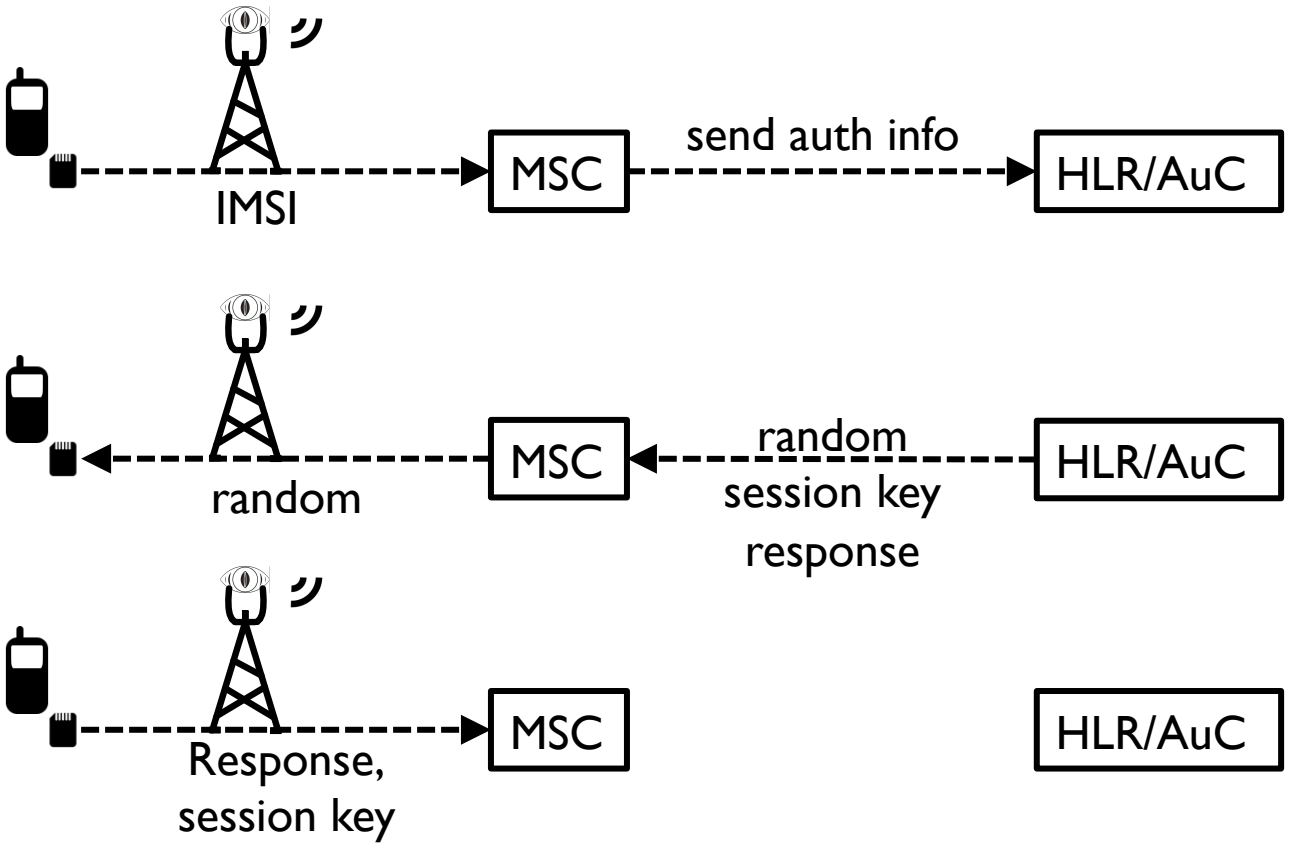
BTS manages Several cells

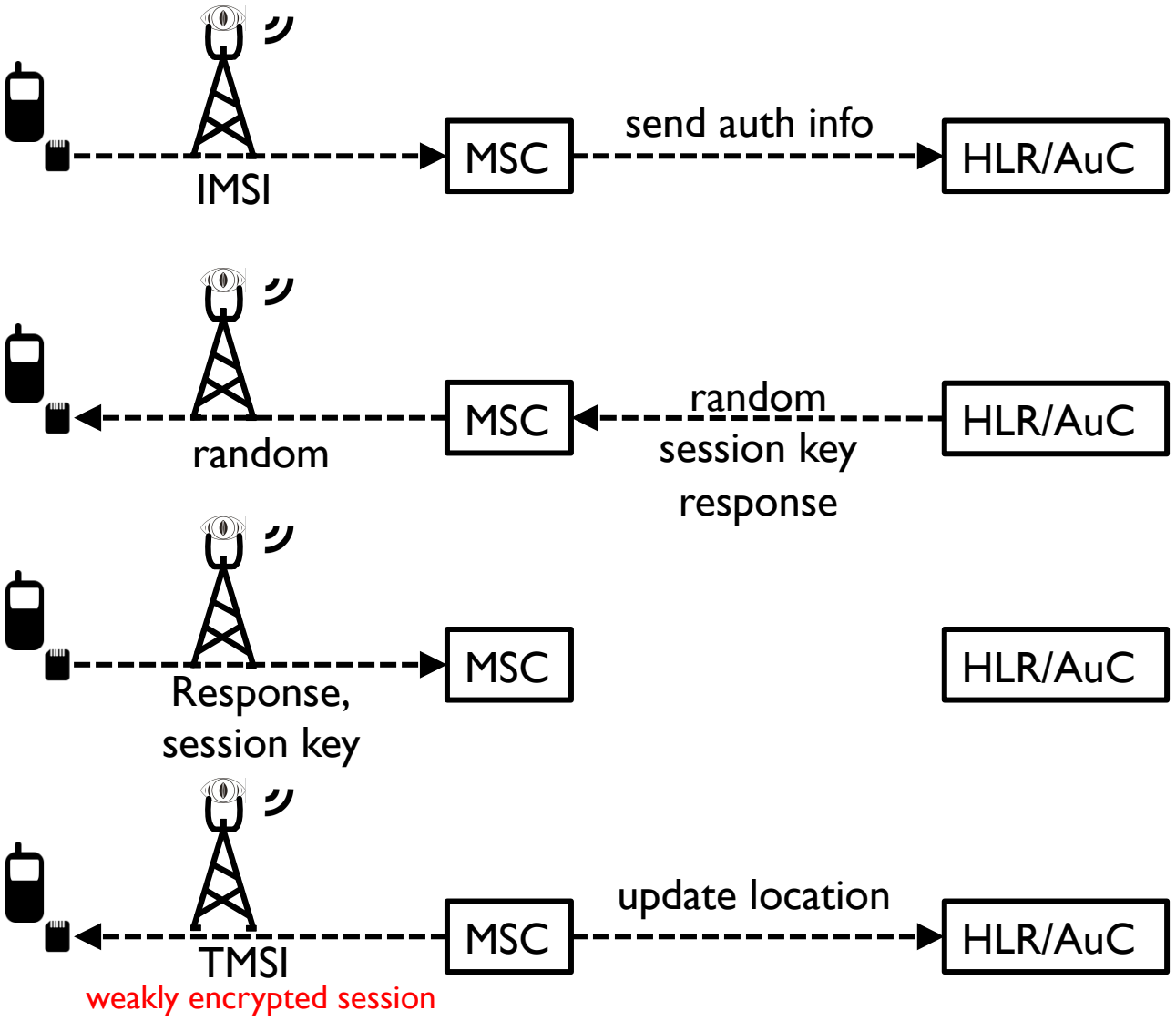
Cell: 1–100km^2

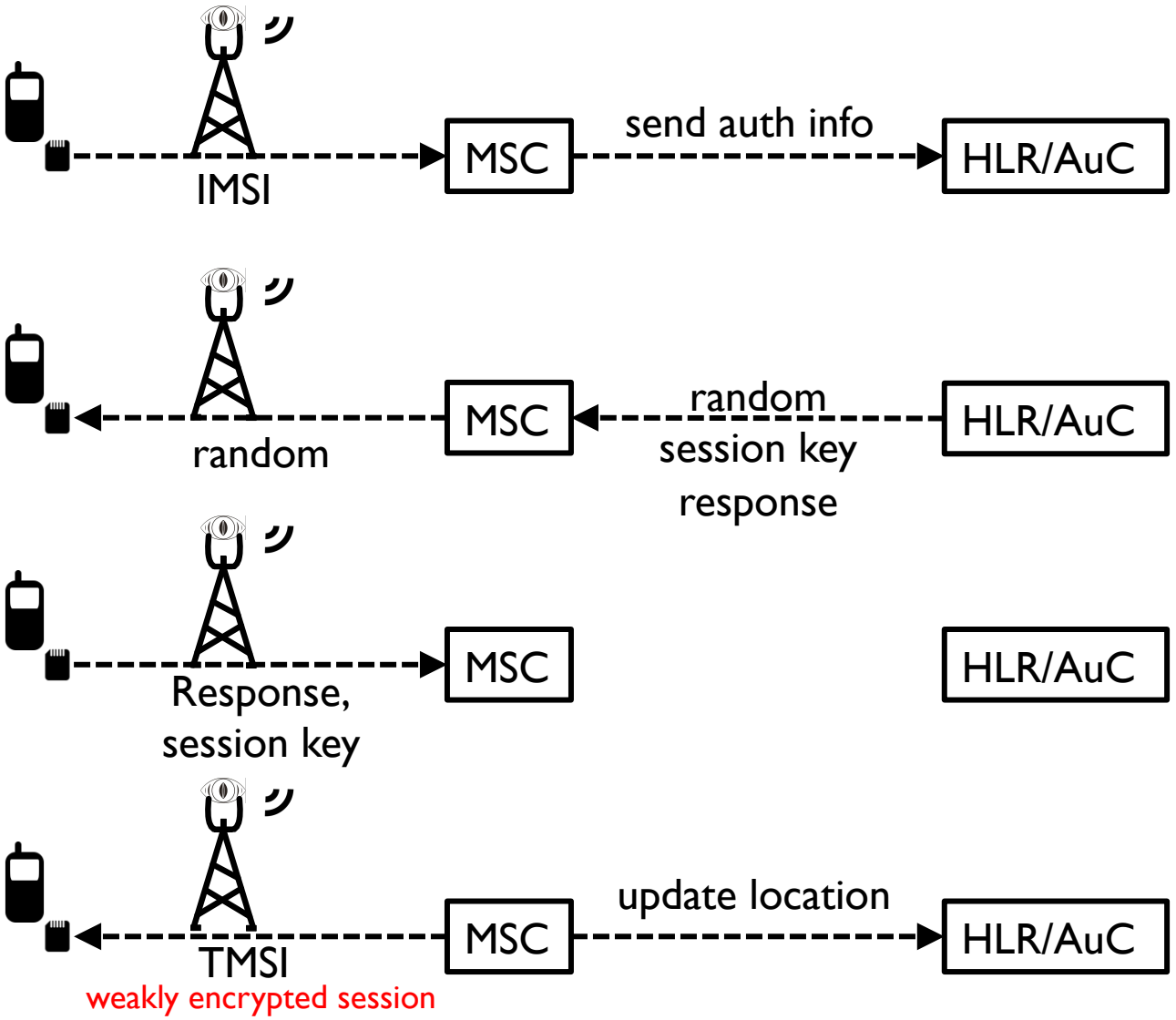
GSM




IMSI
MSC
send auth info
HLR/AuC
random
MSC
random
session key
response
HLR/AuC


MSC
send auth info
HLR/AuC
IMSI
MSC
random
session key
response
HLR/AuC
random
MSC
HLR/AuC
Response,
session key


IMSI
MSC
send auth info
HLR/AuC
random
MSC
random
session key
response
HLR/AuC
Response,
session key
MSC
HLR/AuC
TMSI
weakly encrypted session
MSC
update location
HLR/AuC



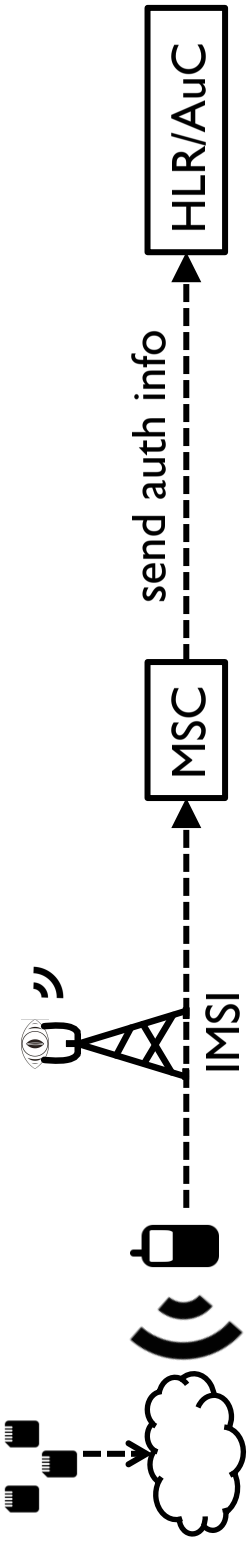
TMSI re-authenticates mobile to any location area within same MSC

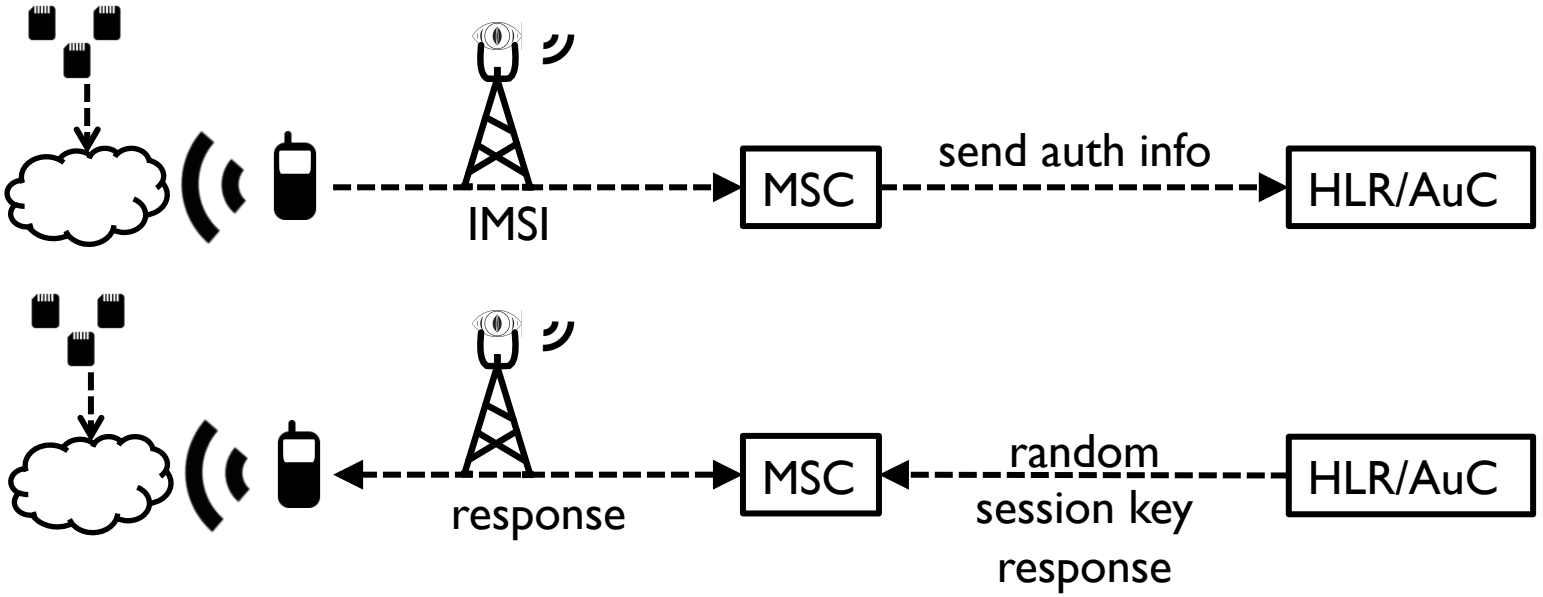
GSM authenticates *access* to an uncloneable SIM — not *possession*.

MSC

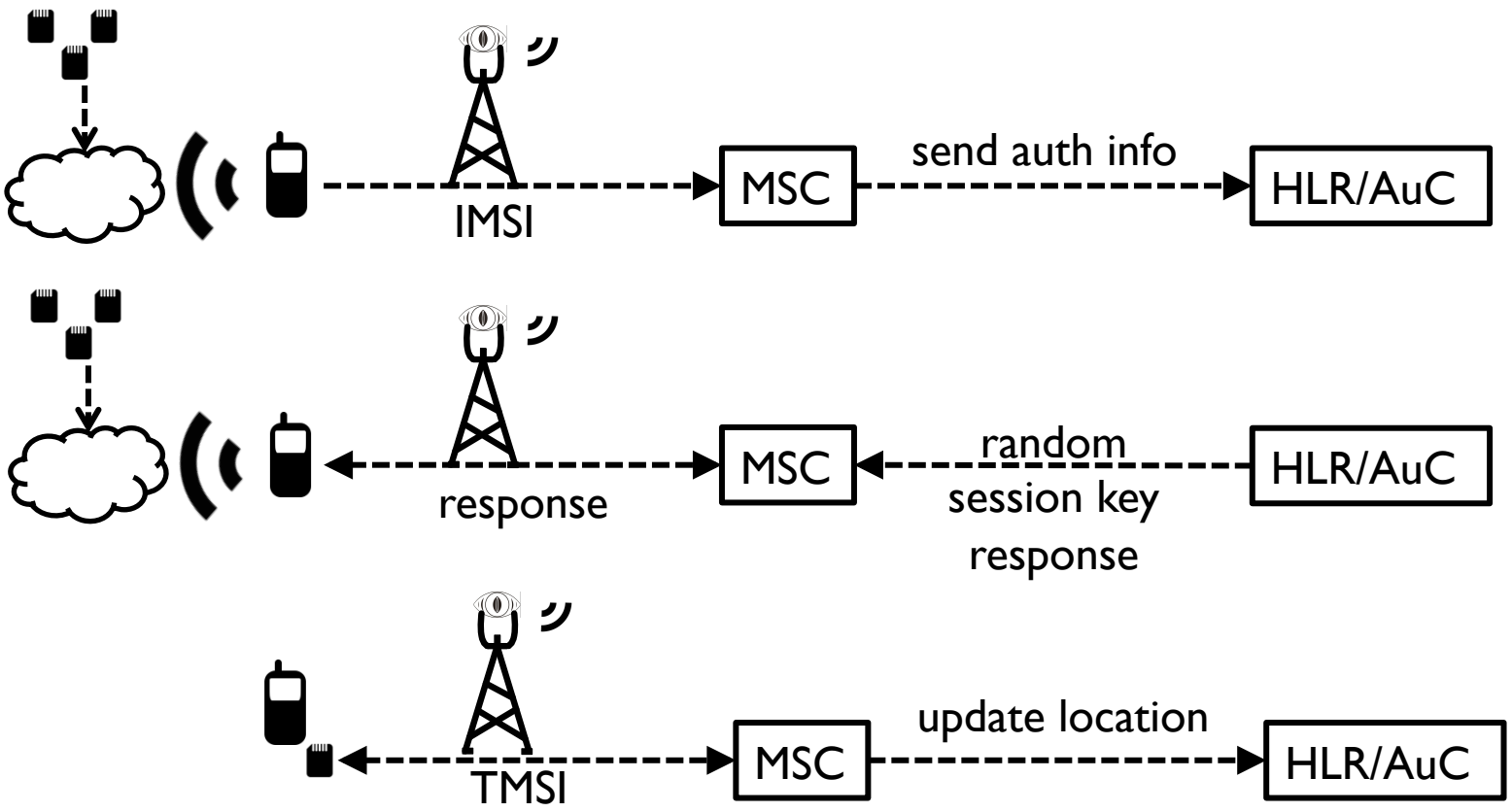
HLR/AuC

ZipPhone

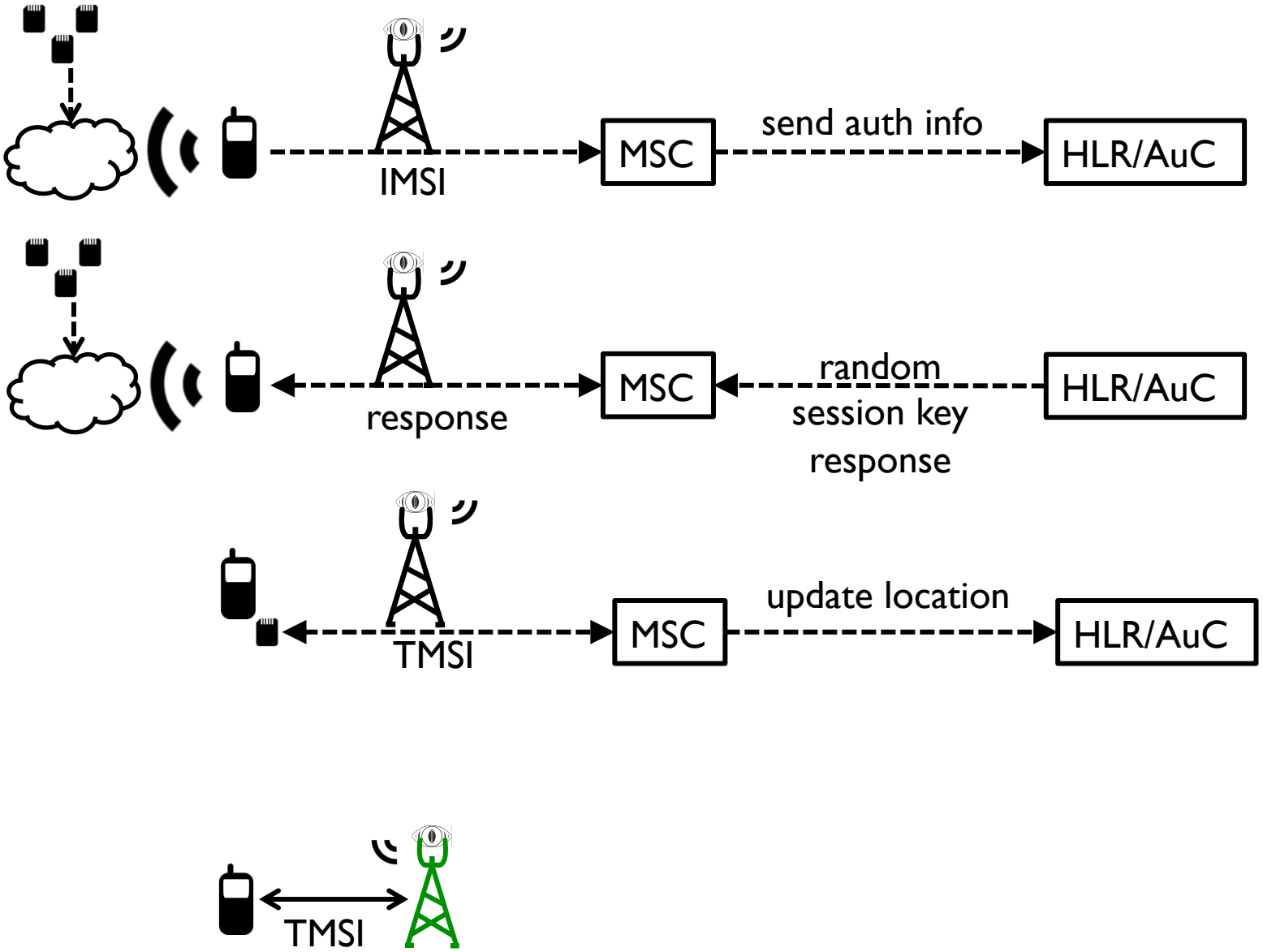



IMSI
MSC
send auth info
HLR/AuC
response
MSC
random
session key
response
HLR/AuC

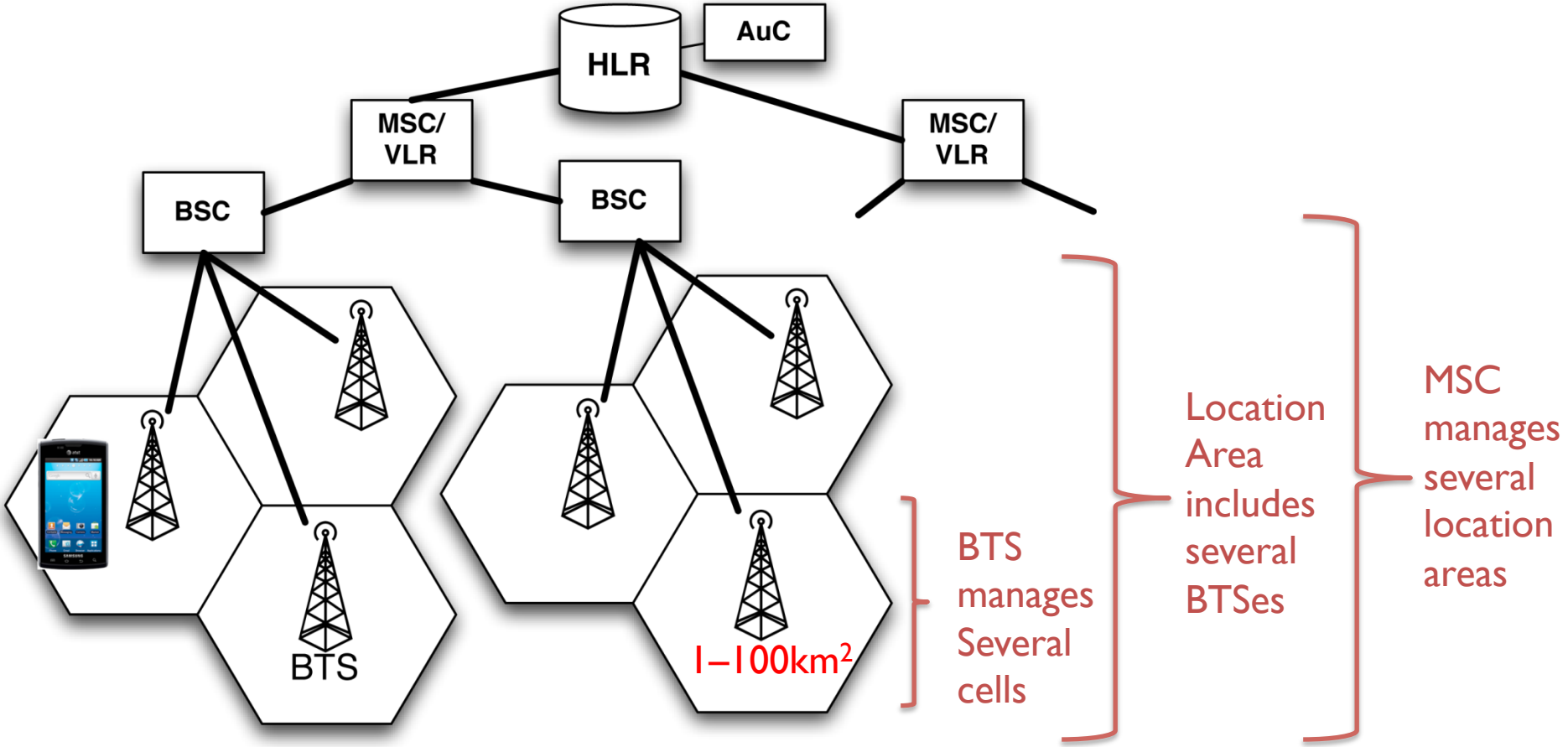
ZipPhone


IMSI
MSC
send auth info
HLR/AuC
response
MSC
random
session key
response
HLR/AuC
TMSI
MSC
update location
HLR/AuC

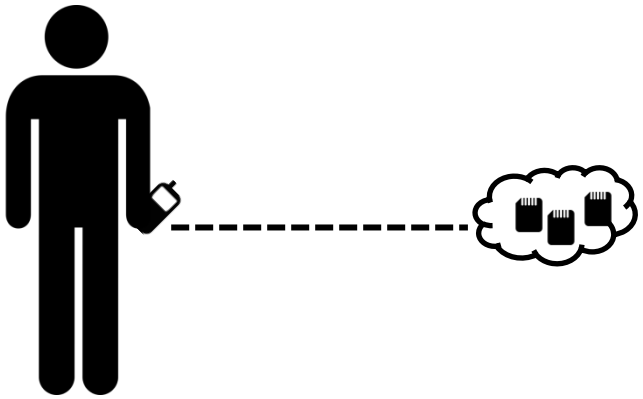
ZipPhone


IMSI
MSC
send auth info
HLR/AuC
response
MSC
random
session key
response
HLR/AuC
TMSI
MSC
update location
HLR/AuC
TMSI

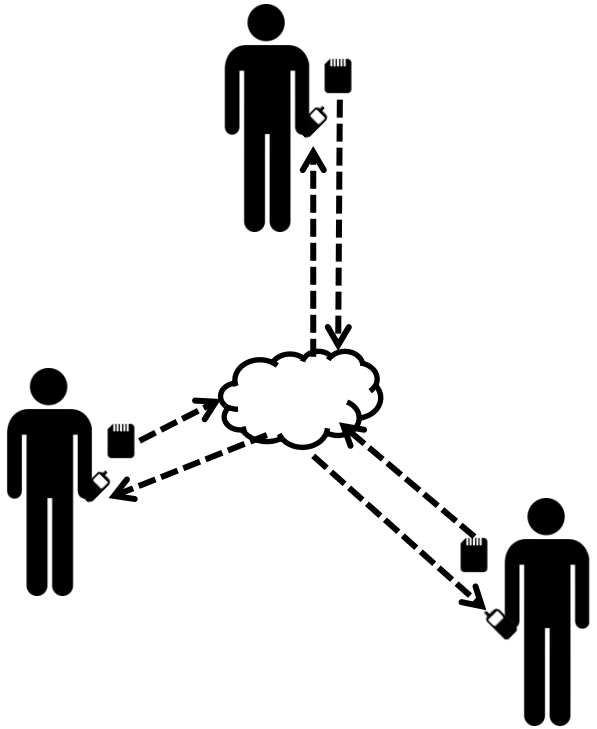
ZipPhone

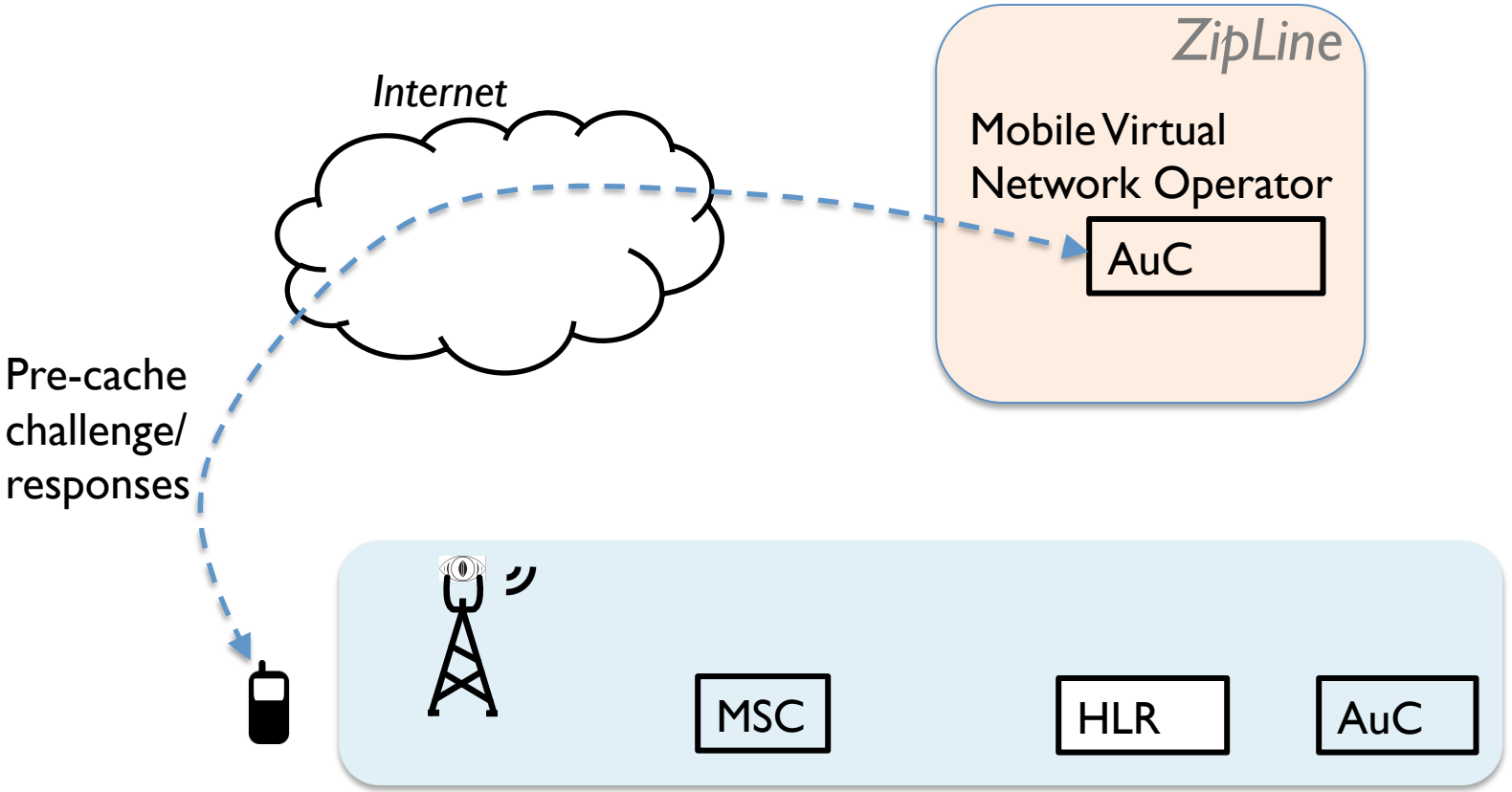

HLR
AuC
MSC/
VLR
MSC/
VLR
BSC
BSC
BTS
1–100km2
BTS
manages
Several
cells
Location
Area
includes
several
BTSes
MSC
manages
several
location
areas

ZipPhone



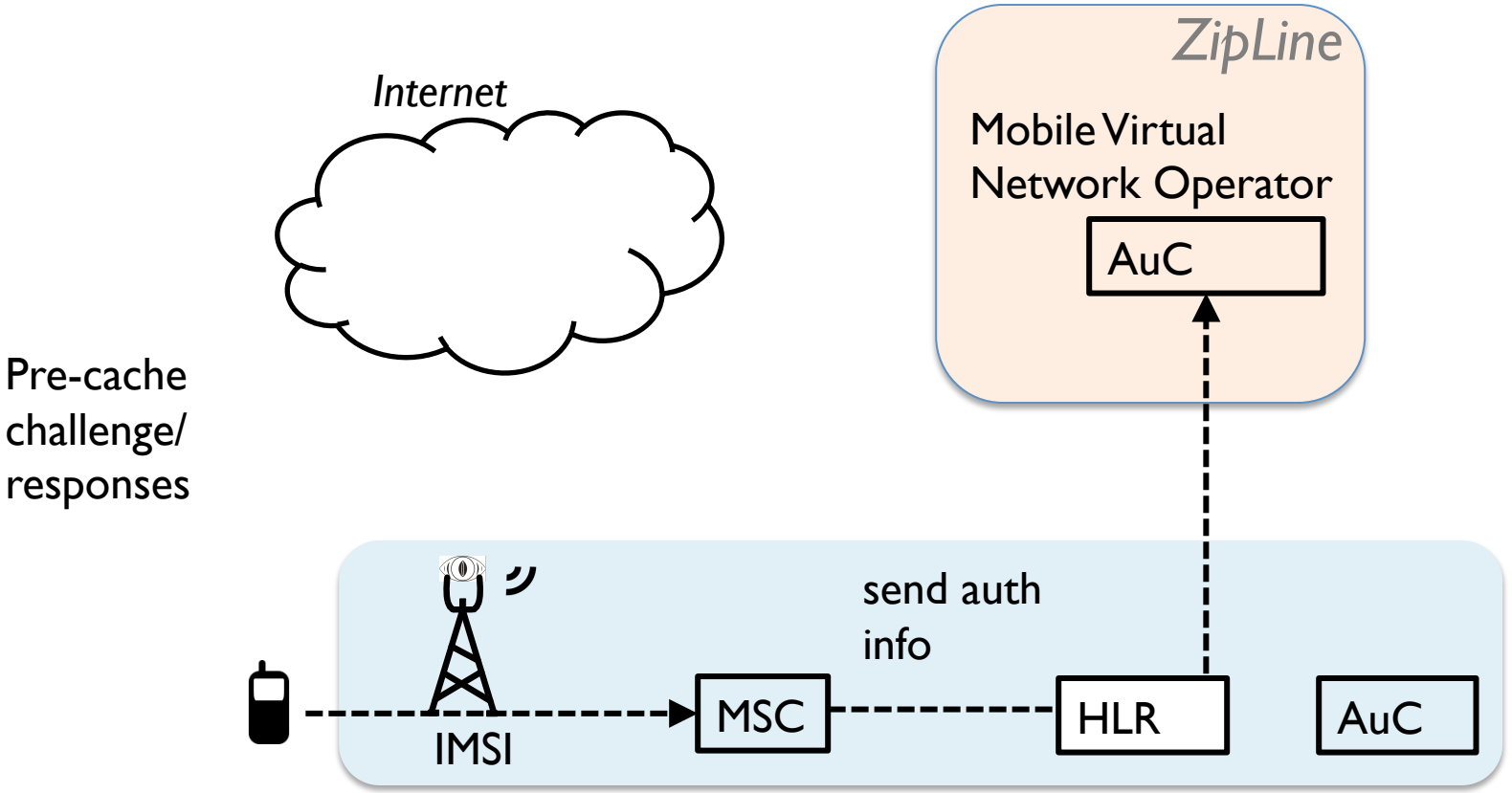
PeerPhone





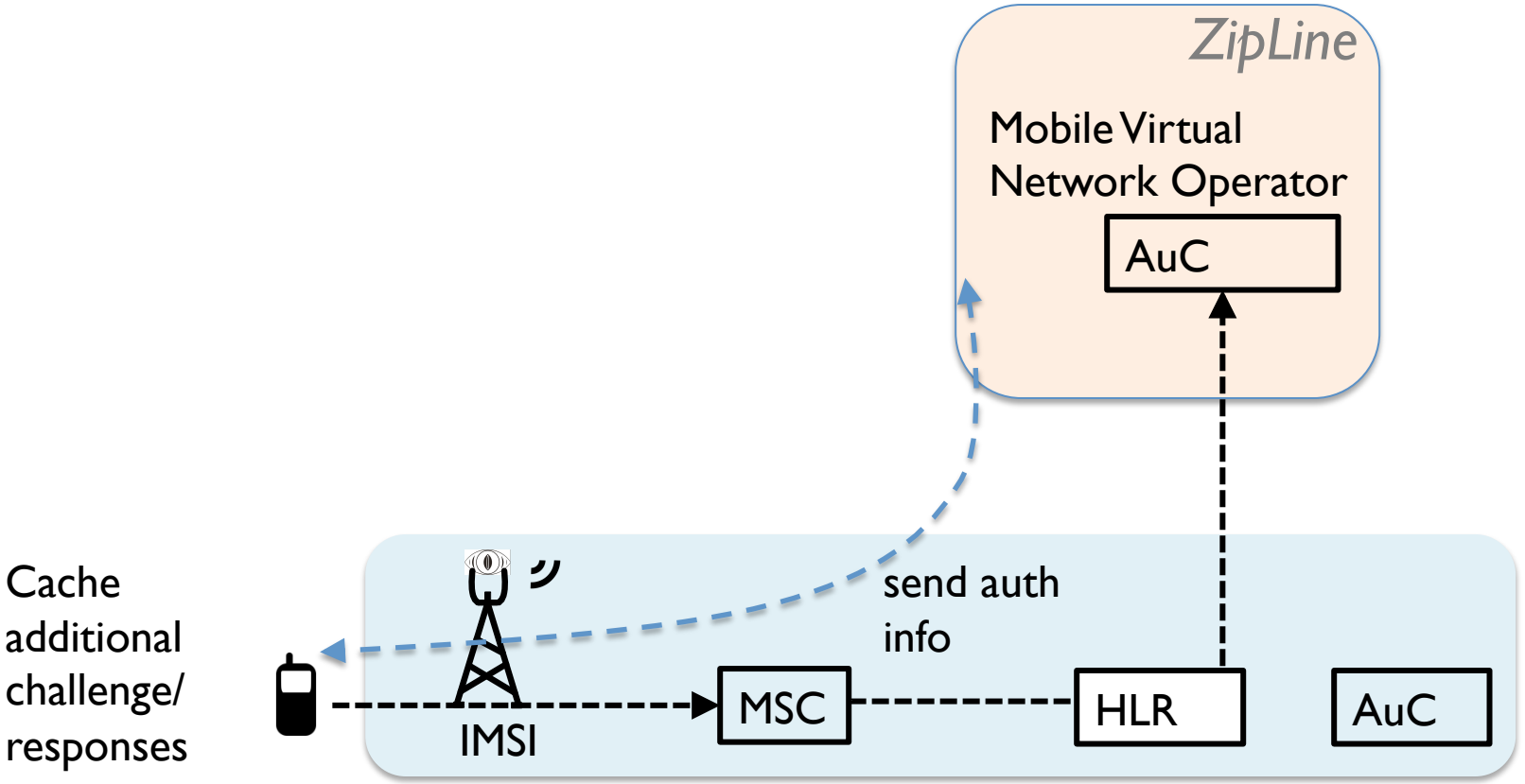
No problems performing location updating in the field.

Physical SIM cards aren't necessary.



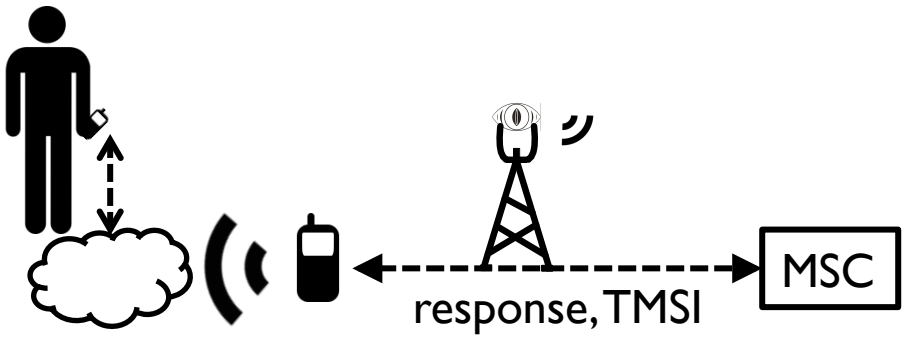
No problems performing location updating in the field.

Physical SIM cards aren't necessary.



No problems performing location updating in the field.

Physical SIM cards aren't necessary.



We can trade SIM functionality with others

Protocol signaling is relayed to willing peer.

By default, GSM use an 11-second timeout, retry as necessary

Cryptographic algorithms are public, all we need is the key.

PeerPhone

Retrieving Credentials from a SIM

- Almost all networks use A5/1 encryption
- A5/1 easily broken by known attacks
  - Since 2001
  - Bidding down on "upgraded" networks
  - ~~Master key is acquired in seconds~~

- *PeerPhone* use is more easily detected than *ZipPhone*.
- No prefetching, but good for all LAs within an MSC
- Correction to paper: **Session key** is acquired in seconds. Another partner is required outside of the original MSC for PeerPhone.

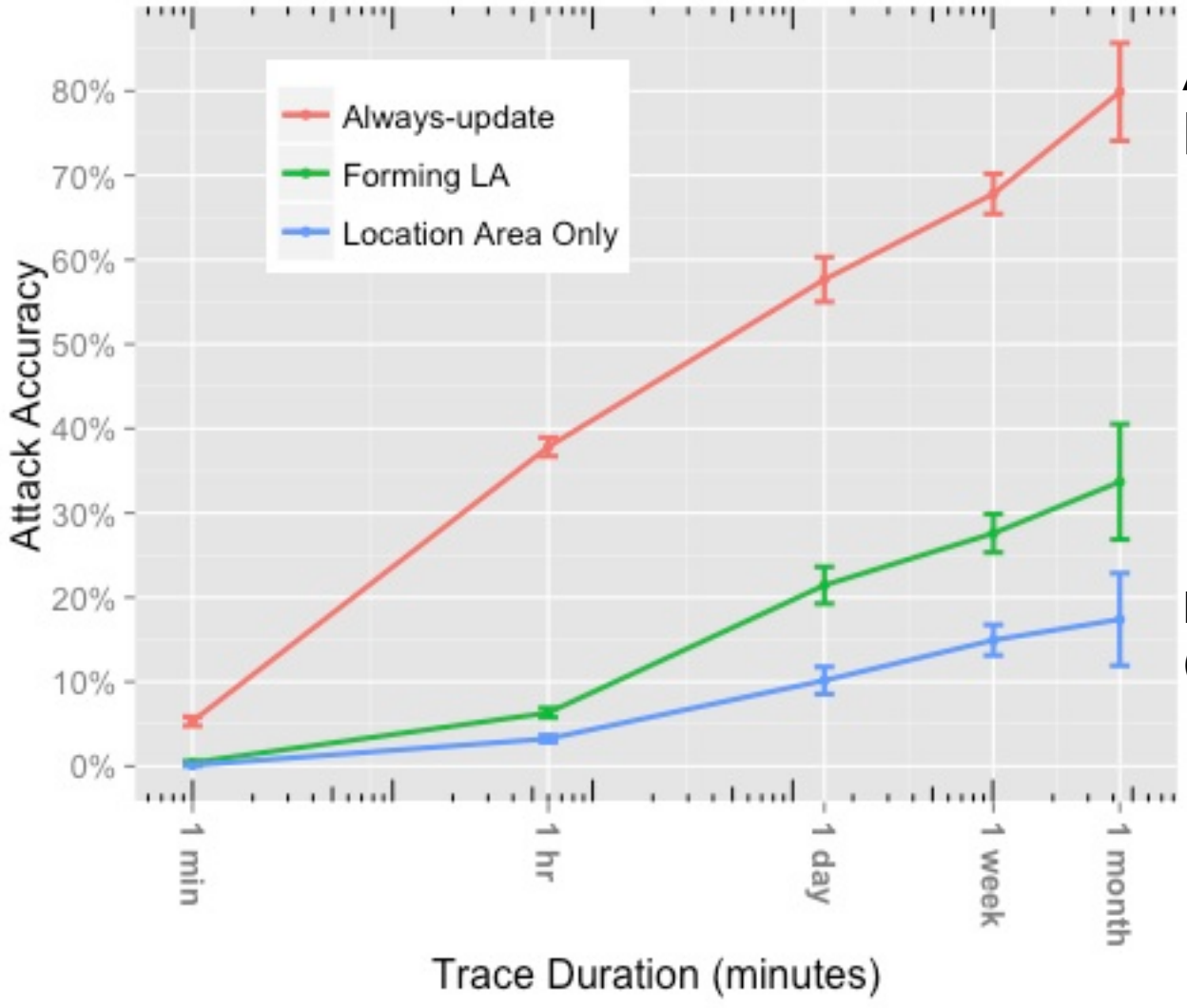
Location Profiling

- Is changing pseudonyms enough?

- *Always-update* policies are never used
- A "*forming* location area" policy is standard.

- Carriers always know your LA
  - Only know cell when receiving/sending voice/data.

Profile Attacks



As reported by [Mulder 2008]

Same data

Best case (this inference)

[Reality mining dataset]

Code at traces.cs.umass.edu

Passive Attacker

Preventing Fake Pages

- Active carriers can falsely *page* a phone
- *Pageknocking*: respond only when pages come within coded intervals of time

- Key *g*, parameter *n*, and time t
- Take first n bits of hmac(*g*, *t*).
  - Determines a sequence of transmits and pauses

- Requires Internet-based proxy

Active Attacks

- Localization based on only Cell ID
  - Off by 0.8 km in city
  - 0.5 km in suburbia
  - 2.9 km on highway
  - [Trevisani:2004],[Watzdorf:2010], [Ficek:2013]
- Localization based on multilateration, offset
  - Off by 0.11 m in tests
  - But tracking more than 20 users out of 410 exceeds network capacity [Ficek:2013]

Related Work

- "A home or work address can deanonymize" *given a consistent identifier.*
  - Pseudonyms can be changed often.
  - Bolot: anonymizing 25 million cellular users requires only day-long pseudonyms.
- See paper for comparison to past schemes for deploying GSM pseudonyms
  - e.g..,[Kesdogan:1996]
- Ficek's work on carrier limitations is excellent.

ZipPhone Summary

- Location privacy without the active cooperation of the carriers
  - Backwards- compatible and over the air.
  - Ideally deployed through a cooperative but untrusted MVNO
  - PeerPhone is more vulnerable to attacks, but immediately deployable

- Fake *pages* can be thwarted with portknocking.

- Previous study assumed always-update policy, too costly for carriers
- ZipPhone via realistic forming location area updates:
  - Deanonymized only 6% of the time (versus 41%)

- Future Work