IWICS, Inc - ODMA™

Opportunity Driven Multiple Access™

- *Beyond 3G™*

The Main Security Threats

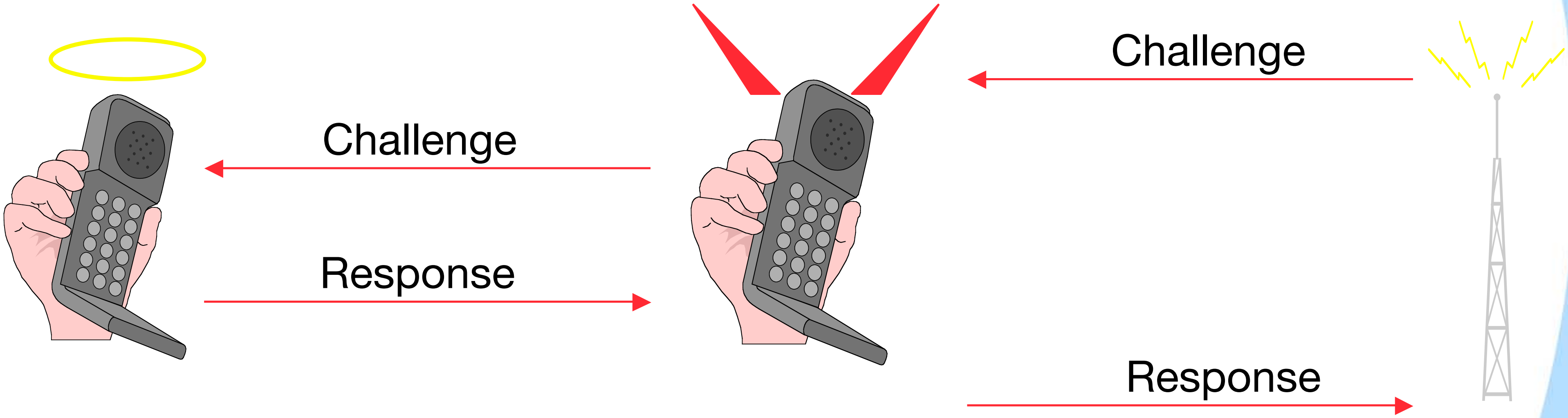
- Fraud
  - Making calls on someone else’s bill
- Eavesdropping
  - Overhearing someone else’s traffic
- Freeloading
  - Using some of the system resources for other purposes
- Tracking / Monitoring
  - Finding out where a particular subscriber is, or when they are making calls

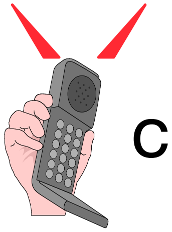
Fraud

- Impersonation
  - Attacker claims to be another subscriber
- Solution:
  - Subscriber has to authenticate self to network
  - Same principle as in GSM
  - Transparent to any relay nodes

Fraud

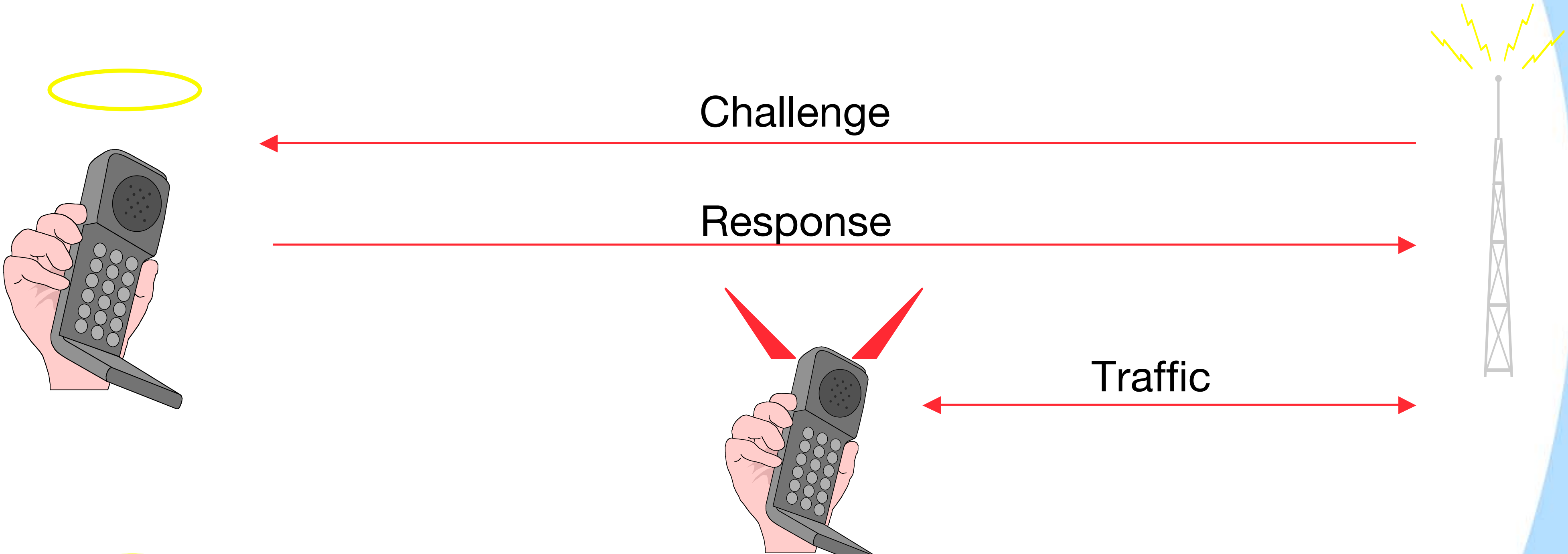
"Man in the middle":

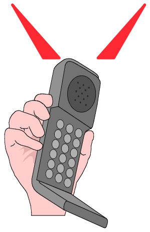


 convinces the base station that he is

Fraud

Seizure of a legitimate channel:



sets up the channel as usual, but then  takes it over

(perhaps by transmitting at higher power)

Fraud

- "Man in the middle" / channel seizure
    - In principle, possible against GSM
    - Possibly easier (more feasible) with ODMA
    - Encryption makes the attacks pointless; but encryption is not permitted in all countries

- Solution if encryption is not possible:
    - Individual packet payloads can be authenticated between the legitimate subscriber and the network
    - Transparent to any relay nodes

Eavesdropping

- Interception of traffic
  - Prevented by encryption, as in GSM, except in countries where encryption is not permitted
  - Packet payload encrypted between subscriber and network - transparent to any relay nodes

Eavesdropping

- Spoof base station
  - Subscriber sets up call, but to a fake base station
  - Fake base station forwards call on towards expected destination - subscriber thinks everything's OK
  - Base station turns off encryption, and can hear the call in clear
  - Theoretically possible against GSM
- Solution
  - Network authenticates itself to subscriber, as well as vice versa
  - Transparent to any relay nodes

Freeloading

- Transmitters and receivers using ODMA relay as a free communications medium
  - Specific to ODMA
  - Probably a very limited threat
- Solution, if necessary:
  - Each registered node has a “certificate” of authenticity from the network
  - Based on its certificate, one node authenticates packets passed to another node

Tracking/Monitoring

- Subscriber’s identity may appear in his (unencrypted) signaling communication or packet headers
  - An eavesdropper may be able to tell where the subscriber is
  - An eavesdropper may be able to tell when that subscriber is making calls
- Solution
  - As in GSM, aliases (e.g. TMSIs) can be used

Conclusions

- Most major threats can be solved in a way that is transparent to the ODMA relay mechanism
- Only minor new threats are introduced by ODMA, and they can be solved too if necessary

IWICS, Inc - ODMA™

Opportunity
Driven
Multiple
Access™

- *Beyond 3G™*