Abhören und Lokalisieren von Mobiltelefonen

Frank Rieger, frank@ccc.de

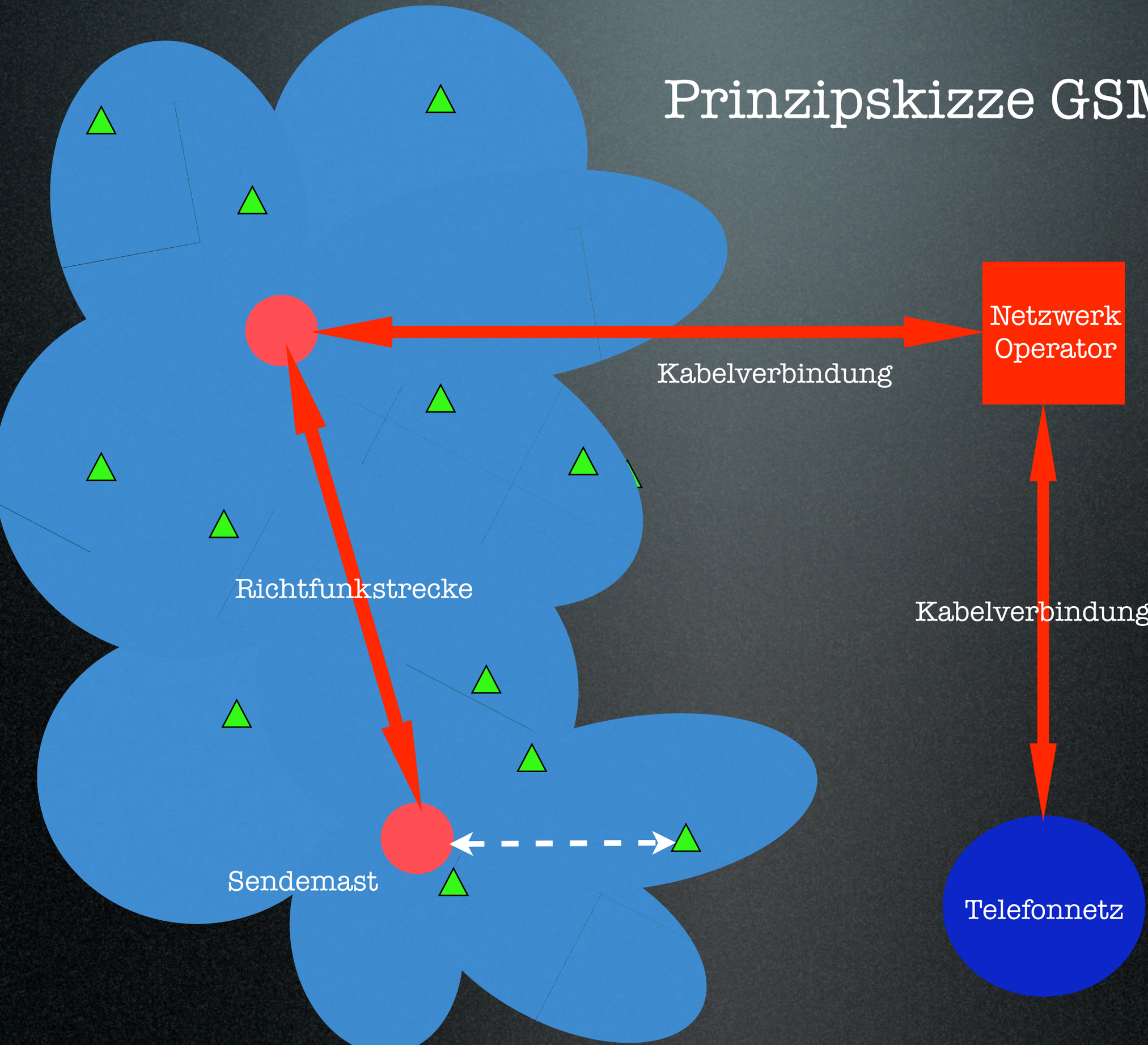
Das Abhör-Zeitalter

- Alle öffentlichen Kommunikationsnetze enthalten heute Abhör-Schnittstellen - legale, geduldete und illegale
- Keine Form elektronischer Kommunikation ist heute sicher gegen Abhören - es sei denn, sie ist stark verschlüsselt

Wer hört ab?

- Geheimdienste
- Strafverfolgungsbehörden
- Organisierte Kriminelle
- Grosskonzerne
- Privat”detektive”
- Interessierte Amateure

Prinzipskizze GSM-Netz



GSM Abhören - Legal

- “Bedarfsträger” mit entsprechender Legitimation (meist richterliche Anordnung) senden Anforderung an Provider für bestimmte Rufnummern
- Provider prüft i.d.R. formale Korrektheit der Anforderung
- Wenn Korrektheit gegeben und keine technischen Probleme im Weg, kommt Provider der Anforderung nach

Daten-Spuren

- “Bedarfsträger” erhält, wenn dazu legitimiert, auf Anforderung im Normalfall:
  - Gesprächsinhalte (ankommend und abgehend)
  - Anrufbeantworter-Nachrichten
  - Mitteilungen (SMS, MMS, e-mails)
  - Call Data Records (incl. Zell-Information)

Motivation für “Bedarfsträger”

- Telefonüberwachung erleichtert Ermittlungsalltag und spart Kosten
- Lokationsermittlung erspart lästige Observationen
- hohe Beweiskraft vor Gericht

Illegales Abhören

- Leitungsweg
- Luftschnittstelle
- Microwellen-Richtfunk-Verbindung
- Satelliten-Verbindungen

Abhören auf dem Leitungsweg

- Traditionelle Form der Überwachung
- Schnittstellen in Vermittlungsstellen, auch für technische Zwecke des Anbieters (bestochene Mitarbeiter...)
- Nicht zu bemerken, da digitale Kopie
- oft auch in privaten TK-Anlagen

Komplett-Aufzeichnung des Verkehrs

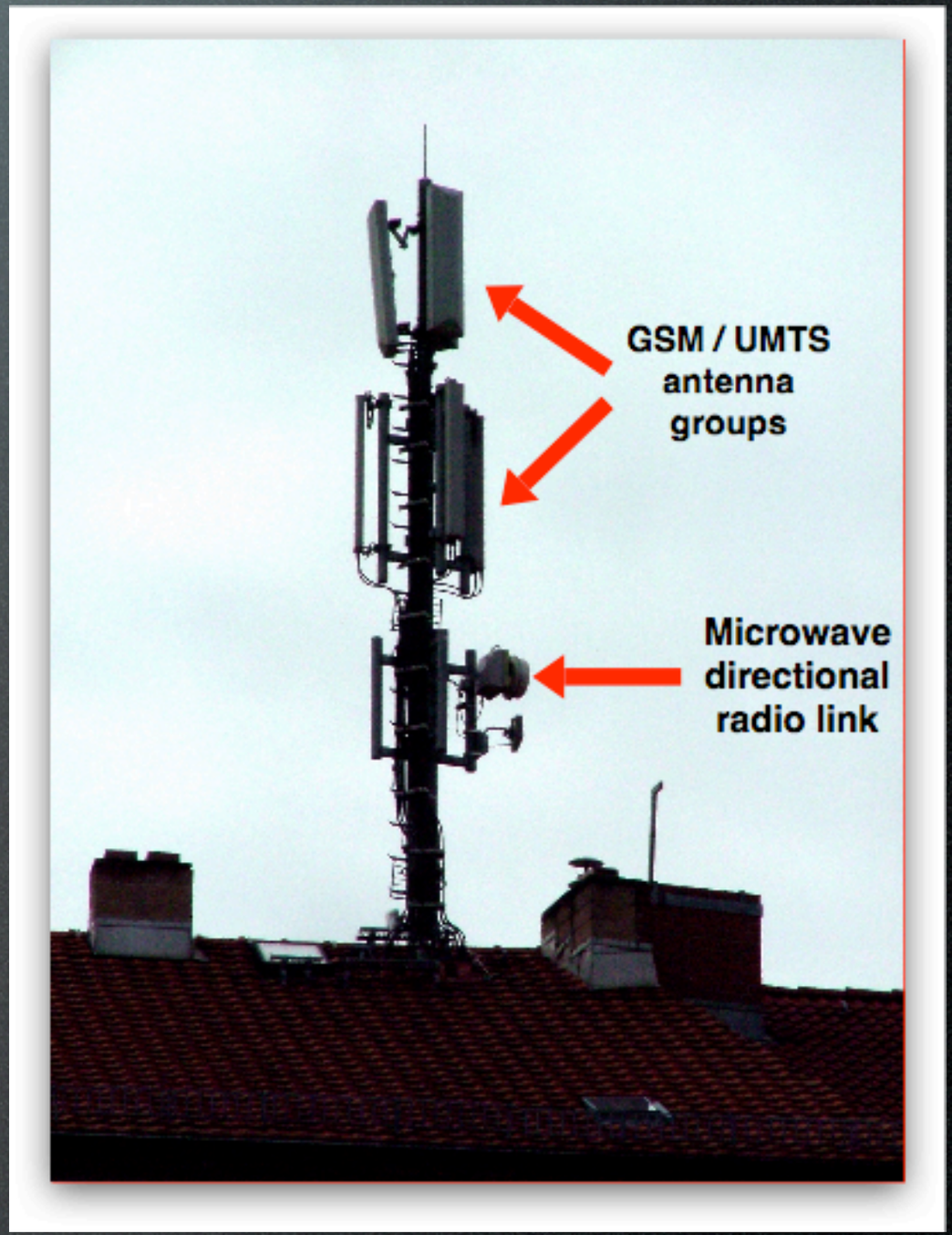
- Einige Staaten zeichnen den **kompletten** Telefonverkehr auf
- Beispielrechnung: Wieviel kostet es, alle Gespräche in Deutschland aufzuzeichnen? (Stand 2002, komprimiert auf 4,8Kbit/sec)
- Festnetz: 319.000.000.000 Minuten = ca. 10 Petabyte = ca. **30mil €**
- Mobilnetze: 32.000.000.000 Minuten = 1 Petabyte = **3mil €**

Abhören von Richtfunkverbindungen

- Mobilfunknetze sind oft mit unverschlüsselten Richtfunkverbin-dungen vermascht

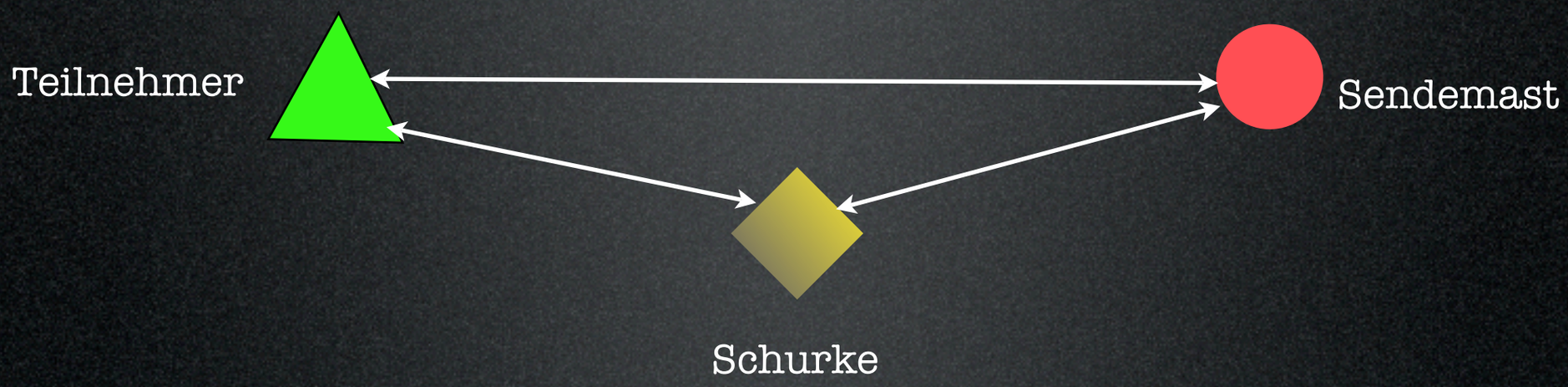
- Abhören ist mit kommerziellen oder Eigenbau-Geräten möglich

- Gespräche liegen als normale ISDN-Verbindung auf dem Link



Abhören durch die Luft

- Aktiv: Man-in-the-Middle Angriff aka. **IMSI-Catcher**
- Ursprüngliche Zielfunktion war Bestimmung der unbekannten IMSI eines Verdächtigen zur Rufnummern-ermittlung und darauffolgender Abhörkonfiguration im Netzwerk



Abhören durch die Luft

- Passiv: Empfang, Decodierung und Entschlüsselung des Funksignals
- GSM basiert auf schwacher, schlechter Verschlüsselung
- Fortschritte in Cryptoanalyse machen schnelle Entschlüsselung von GSM möglich

UMTS schafft keine Abhilfe

- UMTS enthält bessere Verschlüsselung und gegenseitige Authentifizierung Teilnehmer <> Netz
- Aber: alle UMTS Telefone sind auch GSM-Telefone
- Angreifer stört UMTS-Frequenzen, zwingt Telefon so zurück in GSM-Mode und verwendet die bekannten Angriffsmethoden

Die Abhör-Industrie

- Überwachungstechnologie ist zu signifikantem Industriezweig geworden
- Anlagen enthalten oft “Wartungsschnittstellen”, die den Diensten des Herstellerlandes Zugriffe erlauben
- konstanter, massiver Preisverfall

Was tun?

- Starke, vertrauenswürdige Verschlüsselung verwenden, zur Not verschlüsselte e-mail statt Telefon
- kritische Gespräche persönlich führen
- Telefonzellen sind nicht sicher!
- Codeworte u.ä. sind nicht sicher!

Lokalisierung von Mobiltelefonen

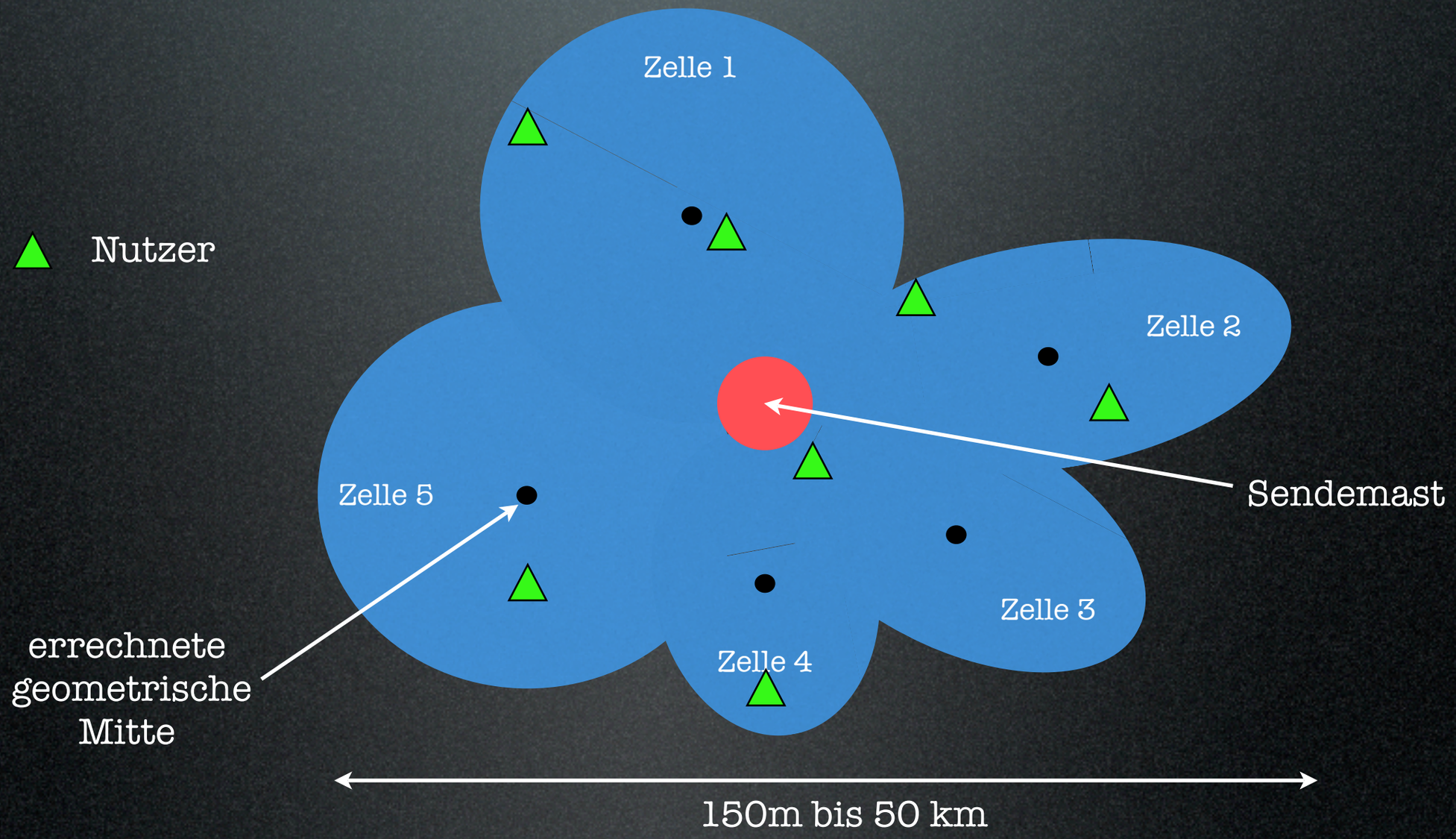
- fortlaufende Lokalisierung des Telefons ist technisches Merkmal des GSM-Netzes (Zustellung eingehender Anrufe, Abrechnung)
- Interessenten sind “Bedarfsträger” und kommerzielle, lokationsbasierte Dienste
- sehr unterschiedlicher Ausbau in den verschiedenen Ländern und Netzen

Lokations-Methoden

- Zell-ID
- Zell-ID plus Time of Arrival
- Triangulation
- Assisted GPS

Zell-ID

- Gibt die errechnete geometrische Mitte des Abdeckungsbereiches einer Zelle an

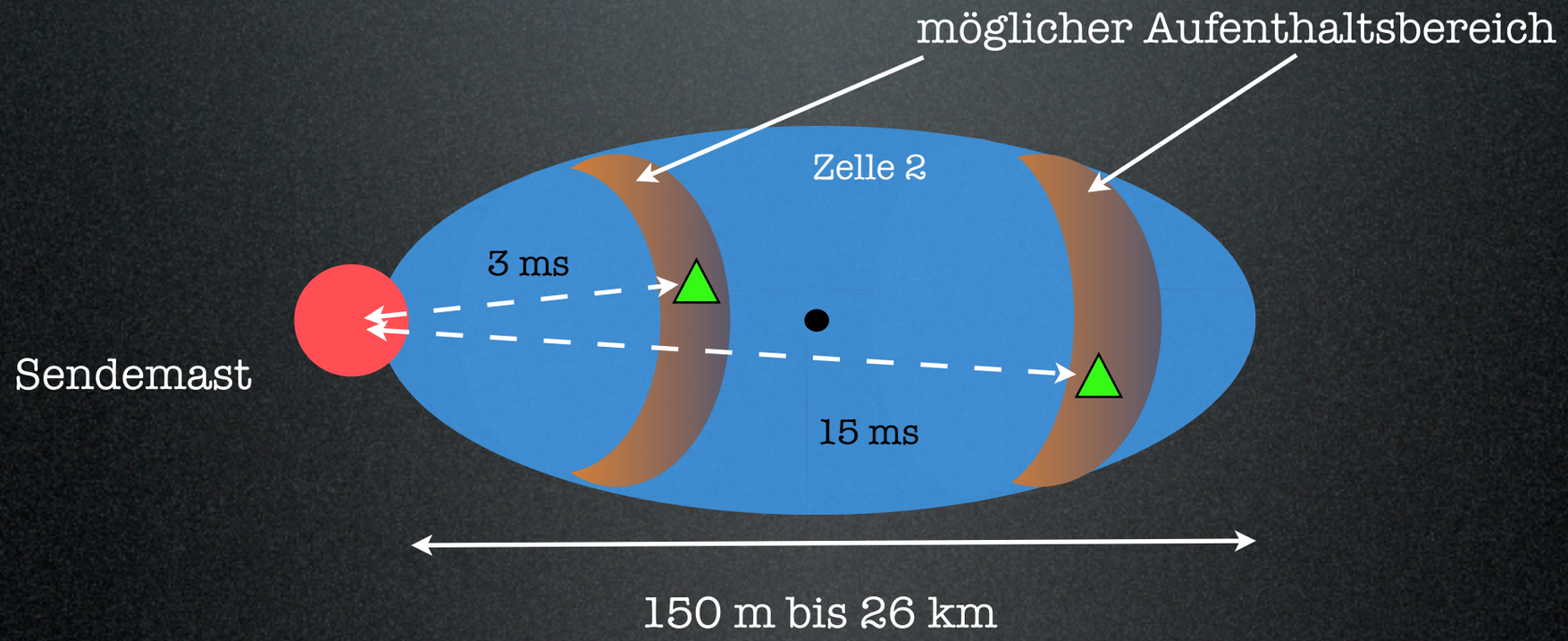


Grösse einer Zelle

- abhängig von Frequenzbereich (900 oder 1800 MHz) und Netzaufbau
- grundsätzlich 150 m bis 26 km
- kleinere Zellen in Städten, grössere auf dem Land
- kleinere Zellen in GSM1800 Netzen (früher nur E-Plus und O2), grössere in GSM900 Netzen (früher D1 und D2)
- Aber: alle Netzbetreiber haben nun GSM1800-Zellen zur Auffüllung

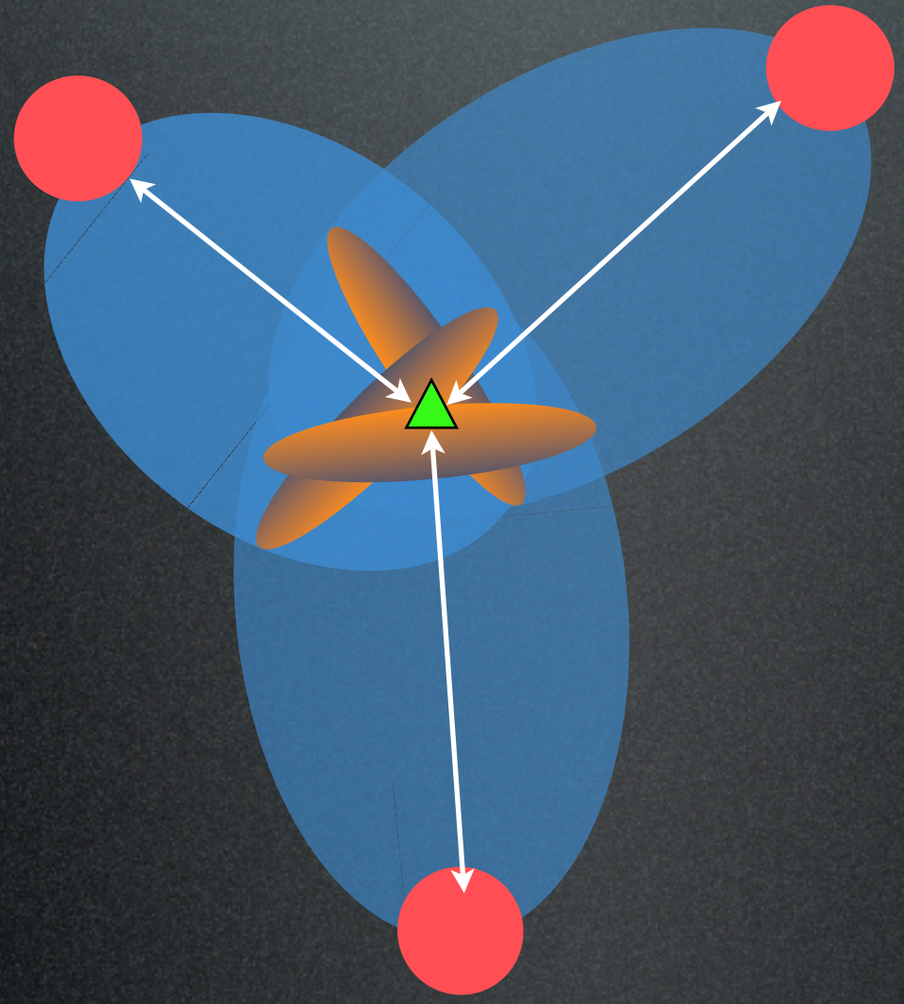
Zell-ID plus Time of Arrival

- Macht Lokationsbestimmung durch Analyse der Signal-Laufzeit genauer
- mittlere Positionsgenauigkeit (>250m)



Triangulation

- Kreuzpeilung durch Ermittlung der Signal-Laufzeiten und Richtung von drei oder mehr Sendemasten
- sehr hohe Positionsgenauigkeit (<50m)



Assisted GPS

- Erfordert Global Positioning System (GPS)-Empfänger im Mobiltelefon
- Kombination von Lokalisierung im Netz plus GPS führt zu hoher Genauigkeit (<10m) und schneller Positionserfassung
- Derzeit insbesondere in USA-Modellen wg. Verpflichtung zur Positionsbestimmung bei Notrufen

Was wird verwendet?

- Zell-ID wird zu jedem Call Data Record gespeichert und weitergegeben
- Zell-ID plus Time of Arrival wird bei einigen Anbietern gespeichert, Praxis der Weitergabe ist uneinheitlich
- Triangulation findet in Deutschland nur auf spezielle Anforderung statt und ist technisch relativ aufwendig

Nahe Zukunft

- Zell ID plus Time of Arrival wird Standardverfahren der Lokalisierung
- Triangulation wird einfacher
- Assisted GPS findet mehr Verbreitung
- direkte Behörden-Schnittstellen zu Lokationsdiensten
- geringe rechtliche Anforderungen an Lokationsüberwachung (siehe BVerfG-Urteil zu GPS-Wanze)

Ausschalten oder Akku ziehen?

- Akku ziehen belässt letzten Lokationseintrag in der Datenbank des Providers, weil Netz Verbindungsstörung annimmt
- Telefon ausschalten entfernt letzten Lokationseintrag in der Datenbank des Providers, da ordnungsgemäss abgemeldet

Kontakt

- e-mail: frank@ccc.de