Geolocation methods in mobile networks

Erik Sy

Our technical analysis for the Parliamentary Investigative Committee

- Investigation about German involvement in US drone strikes

- German government officials claimed not to know about any possibility to use a phone number for targeting drone strikes

- Parliamentary Investigative Committee requested our research group for a analysis

- Our report contains information on:
  - Technical methods and their accuracy to localize mobile phones with drones
  - Required technical identifier for such a geolocation

NETZPOLITIK.ORG

START DATENSCHUTZ DIGITALKULTUR NETZNEUTRALITÄT ÜBERWACHUNG URHEBERRECHT

Informatik-Gutachten: Eine Telefonnummer ist ausreichend, um eine Person mit einer Drohnen-Rakete zu treffen

von Gastbeitrag am 20. September 2016, 18:41 in Überwachung / 4 Kommentare

Zur Lokalisierung einer Person reicht eine Telefonnummer, damit eine Drohne per Fernlenkwaffe gezielt töten kann. Zu diesem Fazit kommt ein Gutachten für den NSA-Untersuchungsausschuss. Geheimdienste und Regierungsparteien haben diese technische Möglichkeit bestritten – und Telefonnummern an die USA gegeben.

Kann Mobilfunkgeräte orten und Raketen darauf abfeuern: Drohne der U.S. Air Force.
Bild: Southwest Research Institute/U.S. Air Force.

Agenda

1. Purpose of geolocation data

2. General approaches for geolocation

3. Geolocation methods on drones

4. Technical identifier in mobile networks

5. Summary

Purpose of geolocation data

- Rescue missions and emergency evacuation

- Monitoring traffic conditions

- Identify people with mobile phones in surveillance footage

- Location tracking

- Targeted drone strikes

However: location data cannot proof the identify of a person!
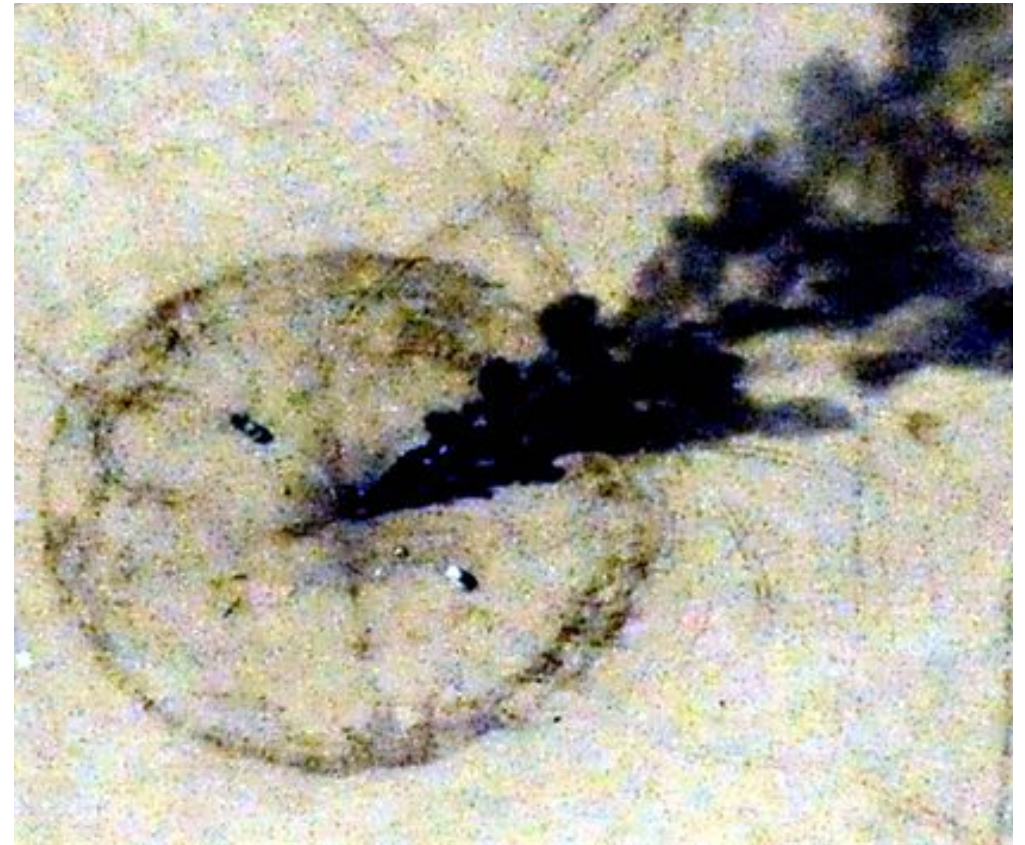

Drone strike with a Hellfire missile

General approaches for geolocation: time measurements

- **Trilateration used to determine location**
  - Position of base stations (BS) is known

- **Time of Arrival (TOA)**
  - Accuracy: 50 – 200 m

- **Time Difference of Arrival (TDOA)**

- **Enhanced Observed Time Difference (E-OTD)**
 - Accuracy: 50 - 125 m
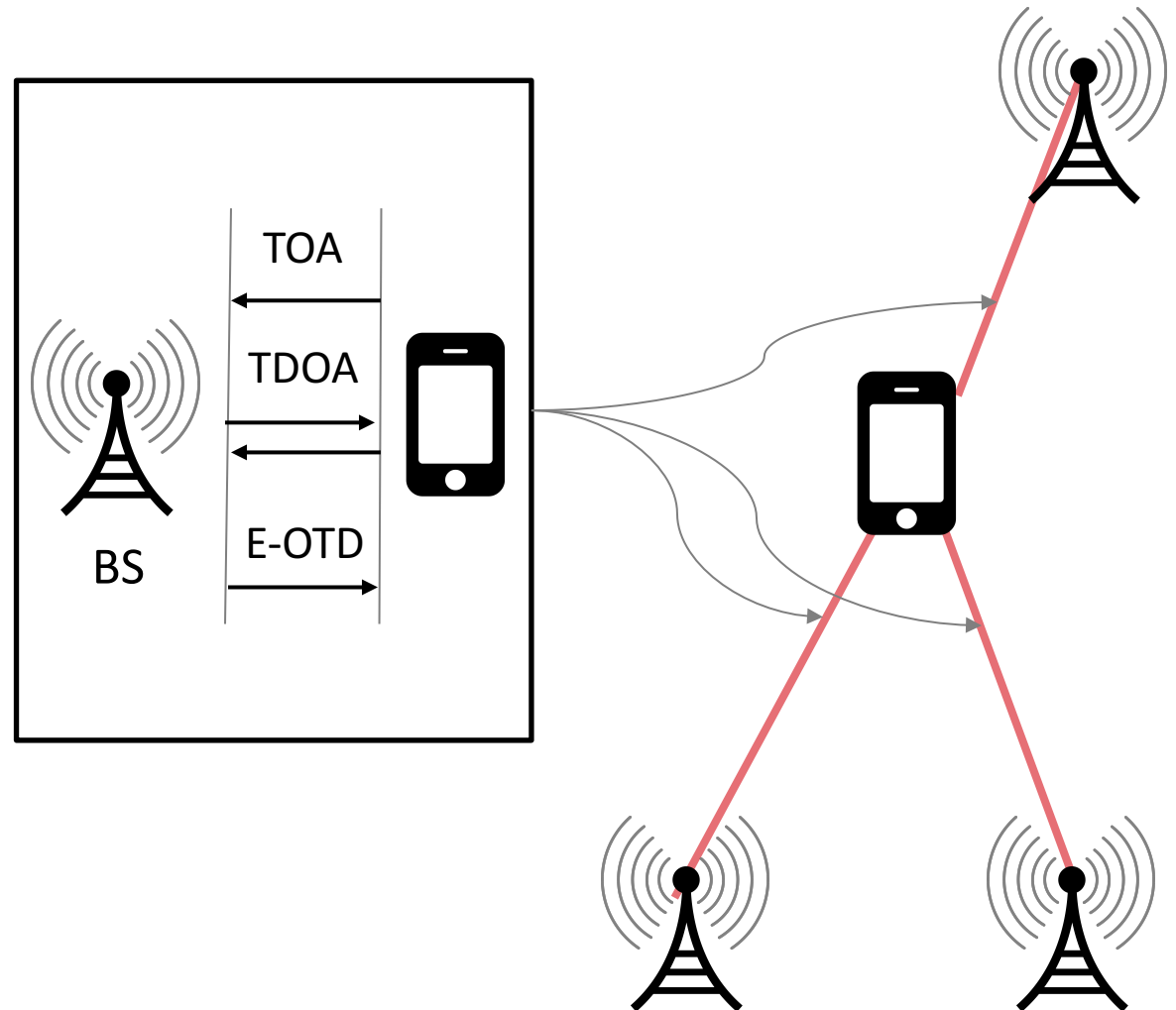
General approaches for geolocation: angular measurements

- BS measures direction of arrival

- Triangulation used to determine location
  - Position and alignment of antennas is known

- Accuracy:
  - 100 – 200 m

- Challenge:
  - non-line-of-sight

α_1

α_2
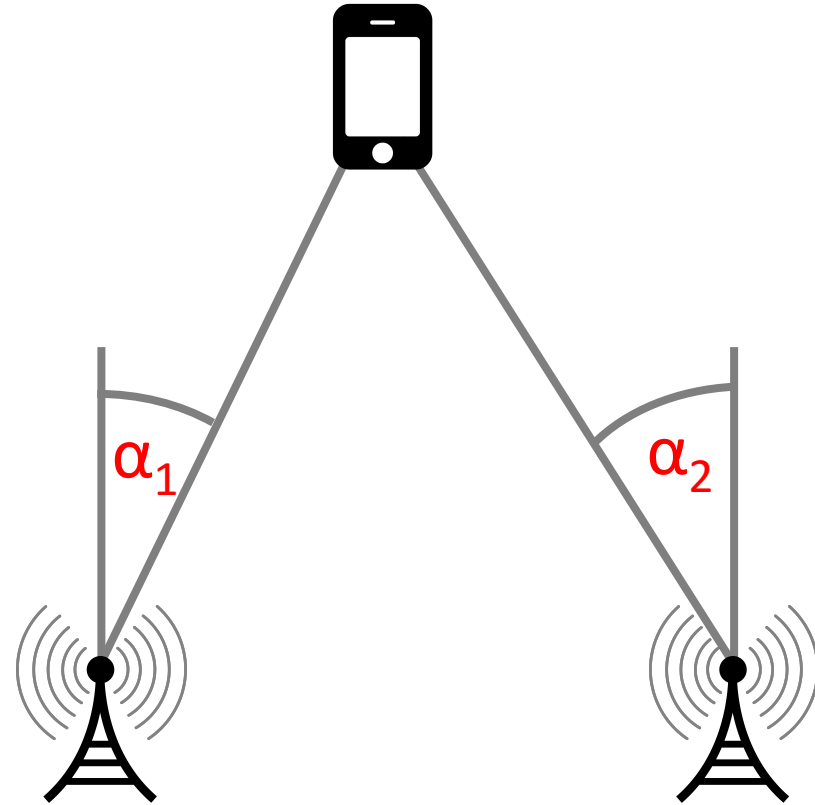
General approaches for geolocation: request for GPS coordinates

- Satellites broadcast their time and position

- Mobile phone uses trilateration to calculate it's position
  - Accuracy: below 10 m

- BS requests location from phone
  - Radio Resource Location Service Protocol (RRLP)

Multiple GPS satellites
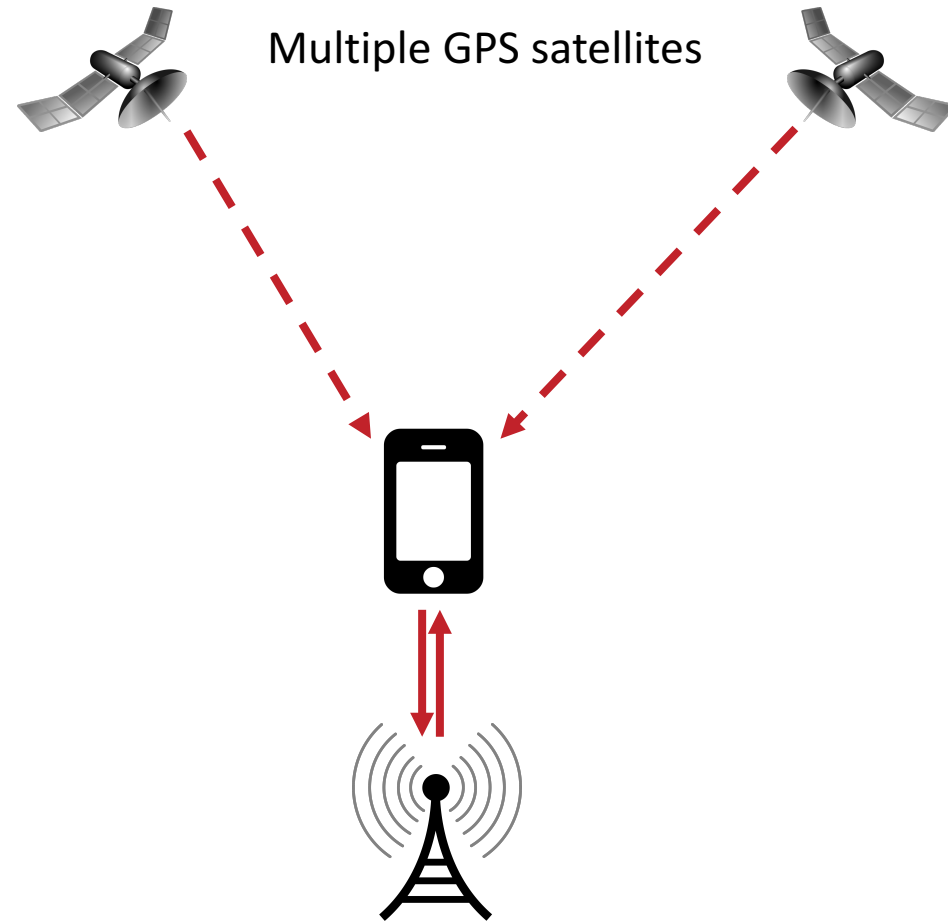
- Mobile phones send their GPS coordinates or names of nearby Wi-Fi Networks (SSID) to an online service
  - Accuracy: below 10 m

- Possible interception and evaluation of this Internet traffic

"It effectively means that anyone using Google Maps on a smartphone is working in support of a GCHQ system" (Snowden Archive, 2008)

"Our mission (VICTORYDANCE) mapped the Wi-Fi fingerprint of nearly every major town in Yemen." (Snowden Archive, 2012)

General approaches for geolocation: request for Cell IDs over SS7

- Signalling System No. 7 (SS7) used for communication between network provider

- Position of mobile phone is saved in location registers

- Third party can request these location information

- Commercial services available to access these data

CI=13

CI=12

CI=14

CI=15

Location register
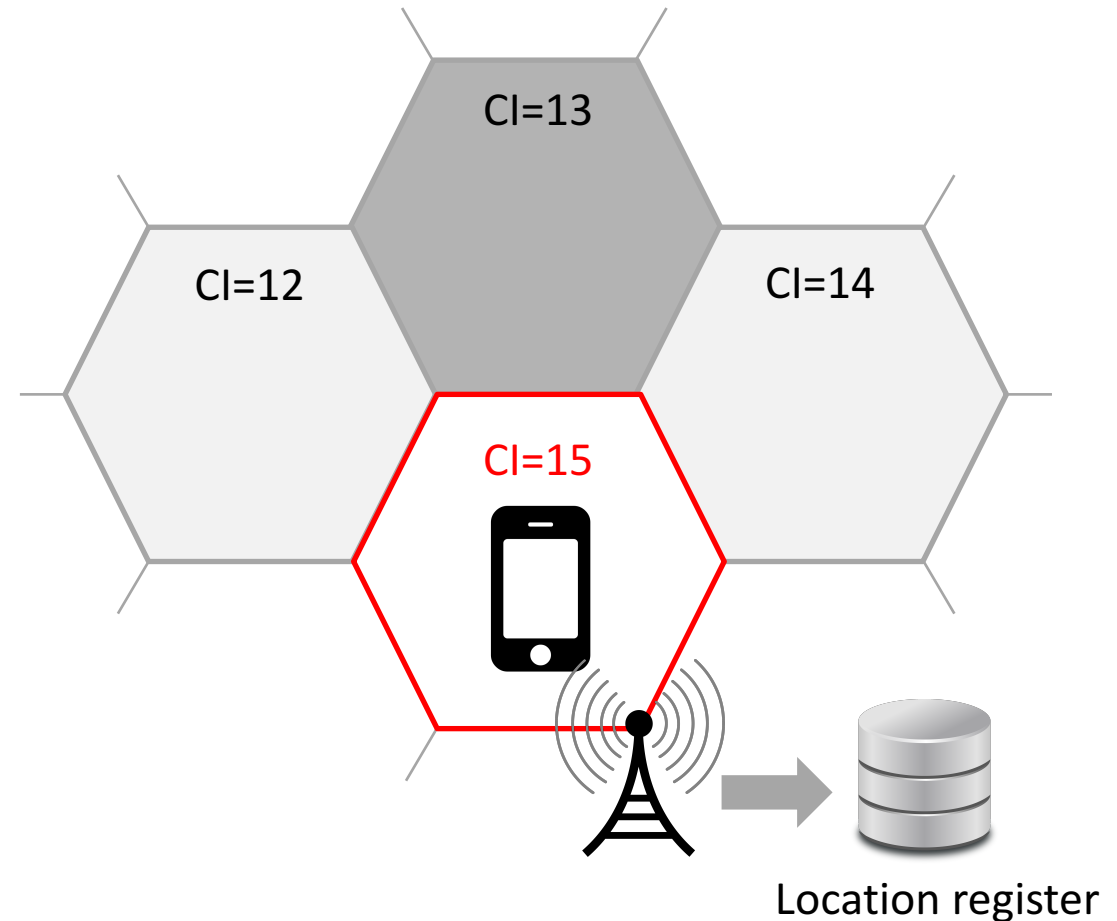
High-precision geolocation on drones

"As part of the GILGAMESH (PREDATOR-based active geolocation) effort (…) for operational use on unmanned aerial vehicle (UAV) flights." (Snowden Archive)

Leak more documents!

- Satellites broadcast their time and position

- Mobile phone uses trilateration to calculate it's position
  - Accuracy: below 10 m

- Drone requests location from phone
  - Radio Resource Location Service Protocol (RRLP)

Multiple GPS satellites
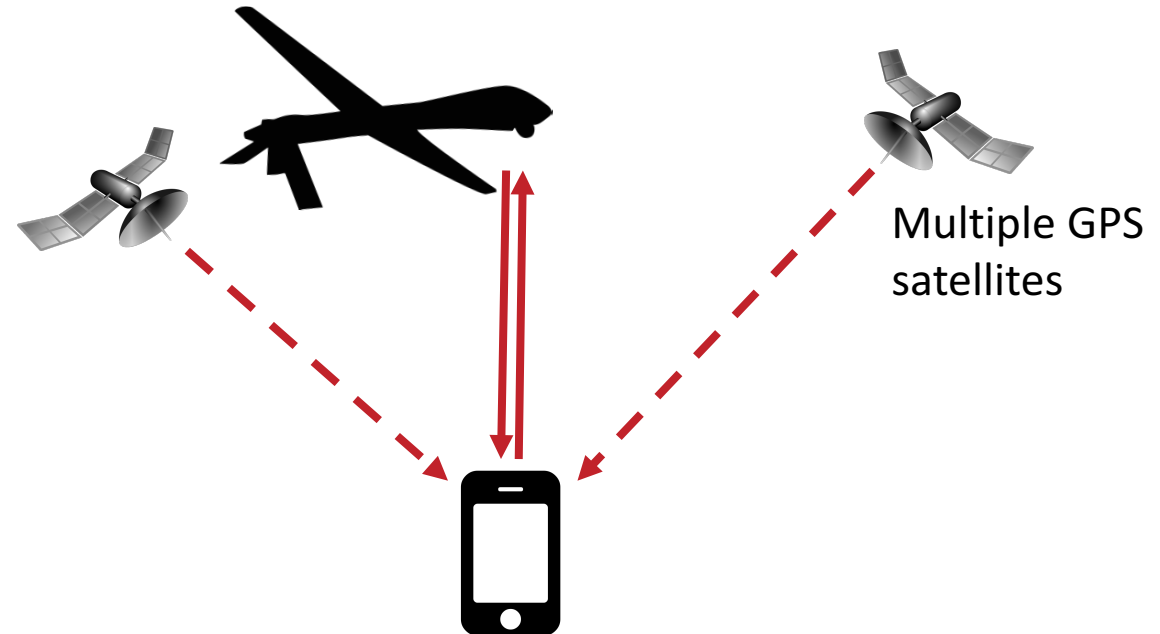
High-precision geolocation on drones: angular measurements

- Angular measurements
  - Estimated accuracy: between 5 m and 35 m radius from 2 km altitude
  - Other work: accuracy of 1 m from 3 km altitude for small airplanes

- Single measurement is sufficient, if the target is on the ground

- Small influence of environmental parameters
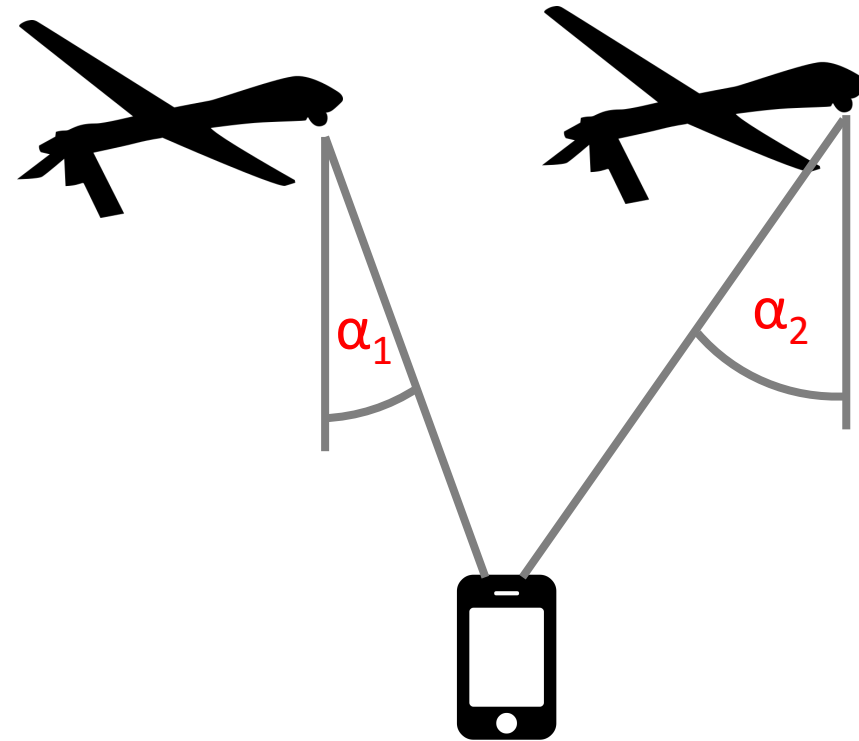
Which identifier are useful for geolocation?

- **Mobile networks**
  - Phone number
  - International Mobile Subscriber Identity (IMSI)
  - International Mobile Equipment Identity (IMEI)

- **Including Internet Traffic**
  - Traffic containing GPS coordinates or SSIDs
  - Client and device identifier

Further reading: www.icir.org/vern/papers/trackers-pets16.pdf

Summary

- Mobile phones can be localized by a variety of different methods

- A single drone can localize mobile phones with an accuracy to perform a drone strike

- Phone number, IMSI and IMEI can each be used for the geolocation of a mobile phone

- Geolocation methods cannot proof the identity of a person

Thank you!

References

- Nnenna, E. J., & Onyekachi, O. H. (2012). Mobile Positioning Techniques in GSM Cellular Networks: A Comparative Performance Analysis. *International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume*, *2*, 21-29.

- Kumar, V. (2014). Effect of Environmental Parameters on GSM and GPS. *Indian Journal of Science and Technology*, *7*(8), 1183-1188.

- Mir, H. S., & Sahr, J. D. (2007). Passive direction finding using airborne vector sensors in the presence of manifold perturbations. *IEEE Transactions on Signal Processing*, *55*(1), 156-164.