Sachverständigengutachten

Darstellung der Möglichkeiten, mithilfe von – ggf. auch personenbezogenen – Daten eine Lokalisierung bzw. Ortung von Personen durchzuführen

für den 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages

Prof. Dr. Hannes Federrath
Fachbereich Informatik
Universität Hamburg

19.09.2016

Kontaktdaten des Verfassers

Prof. Dr.-Ing. Hannes Federrath
Universität Hamburg
Fachbereich Informatik
Sicherheit in verteilten Systemen (SVS)
Vogt-Kölln-Str.39
22527 Hamburg

Telefon: 040-42883-2358
E-Mail: federrath@informatik.uni-hamburg.de
Web: https://svs.informatik.uni-hamburg.de

Ein herzlicher Dank für Diskussionen, Zuarbeiten und Hinweise zu diesem Gutachten geht an meine wissenschaftlichen Mitarbeiter Erik Sy und Ephraim Zimmer.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AOA Angle Of Arrival
CDMA2000 Second-Generation CDMA
CDMA Code Division Multiple Access
CI Cell Identity
COO Cell Of Origin
E-OTD Enhanced OTD
ESN Electronic Serial Number
GPS Global Positioning System
GSM Global System for Mobile Communications
HLR Home Location Register
HUMINT Human Intelligence
IMEI International Mobile Equipment Identity
IMSI International Mobile Subscriber Identity
LTE Long-Term Evolution
MEID Mobile Equipment Identifier
MFG Mobilfunkgerät
MNP Mobile Number Portability
MSISDN Mobile Subscriber Integrated Services Digital Network Number
RLF Radio Link Failure
RRLP Radio Resource Location Service Protocol
SIGINT Signals Intelligence
SIM Subscriber Identification Module
SS7 Signalling System No. 7
TOA Time of Arrival
U-TDOA Uplink-Time Difference Of Arrival
UMTS Universal Mobile Telecommunications System
VLR Visitor Location Register

1 Untersuchungsauftrag

1.1 Fragen des Untersuchungsausschusses

Es soll zu folgenden Fragen Stellung genommen werden:

1. Welche Daten sind dafür geeignet, unter den jeweils im Untersuchungszeitraum gegebenen technischen Möglichkeiten Personen in Regionen zu lokalisieren, in denen Tötungen mittels Drohnen stattfanden bzw. stattfinden. Wie unterscheiden sich diese technischen Gegebenheiten ggf. von den Bedingungen in Deutschland?
2. Welche technischen Methoden wurden bzw. werden für die Lokalisierung von Personen beim Einsatz militärischer Drohnen von US-Stellen benutzt?
3. Mit welcher Genauigkeit und unter welchen Voraussetzungen (unter besonderer Berücksichtigung der realen Bedingungen des Mobilfunkverkehrs in den Ländern Afghanistan, Pakistan, Jemen und Somalia im Untersuchungszeitraum) lässt sich ein Mobilfunkgerät so orten, dass von US-Stellen eine Fernlenkwaffe mit hinreichender Treffergenauigkeit für eine gezielte Tötung eingesetzt werden kann? Müssen ggf. noch weitere Informationen (Video, SIGINT, HUMINT etc.) für eine hinreichend genaue Zielbestimmung hinzutreten und wenn ja welche?
4. Ist unter Berücksichtigung der festgestellten Bedingungen eine Telefonnummer – beziehungsweise eine IMEI- oder IMSI-Identifizierung – als einziges technisches Datum mittelbar oder unmittelbar ausreichend, um eine Fernlenkwaffe mit hinreichender Treffergenauigkeit für eine gezielte Tötung einsetzen zu können?

1.2 Zusammenfassung der Antworten auf die Fragen

Der Fokus dieses Gutachtens liegt erstens auf der Beschreibung der technischen Möglichkeiten zur Ortung von Mobilfunkgeräten (MFG) unter den von den Mobilfunkstandards angenommenen Bedingungen (Signalausbreitung, Größe und Dichte der Funkzellen, Bebauung) und deren Methoden und zweitens auf den Möglichkeiten der autonomen Ortung ohne Nutzung der vor Ort vorhandenen Mobilfunkinfrastruktur, etwa mittels an Drohnen angebrachter IMSI-Catcher, d.h. unabhängig vom lokalen Mobilfunkbetreiber, ohne Unterstützung durch das MFG und ohne Verwendung von Lokalisierungsverfahren wie Global Positioning System (GPS).

Zu den Fragen des Untersuchungsausschusses wird zusammenfassend wie folgt Stellung genommen:

Zu 1. Die folgenden Daten in Mobilfunknetzen sind geeignet, MFG zu lokalisieren (siehe Abschnitt 2.2):

- öffentliche und netzinterne Rufnummern eines mobilen Teilnehmers:
  - Mobile Subscriber Integrated Services Digital Network Number (MSISDN),
  - International Mobile Subscriber Identity (IMSI),
- Gerätekennungen eines mobilen Teilnehmers:
  - International Mobile Equipment Identity (IMEI),
  - Electronic Serial Number (ESN),
  - Mobile Equipment Identifier (MEID) sowie
- ggf. weitere personenbezogene bzw. gerätespezifische Identifizierungsmerkmale wie beispielsweise die MAC-Adresse, welche eine Zuordnung von Datenverkehr zu einem Gerät bzw. einer Person ermöglichen.

Während des Untersuchungszeitraums konnten und können die beschriebenen Daten weltweit zur Ortung eingesetzt werden, soweit in der jeweiligen Region eine Funkabdeckung gegeben ist. In Deutschland ist die Funkzellendichte der Mobilfunknetze höher als in den im Untersuchungsauftrag genannten Regionen, so dass einige mobilfunkbasierte Lokalisierungsverfahren (siehe Abschnitt 3.1) in Deutschland genauere Ergebnisse liefern können.

Zu 2. Militärische Drohnen können zur autonomen Lokalisierung eines MFG die Ausbreitungsrichtung der Funkwellen messen. Hierzu wird die Methode Angle Of Arrival (AOA) verwendet (siehe Abschnitt 4). Falls das MFG eine Positionsbestimmung durch Global Positioning System (GPS) unterstützt, lassen sich je nach MFG zusätzlich GPS-Koordinaten durch einen an einer Drohne angebrachten IMSI-Catcher feststellen (siehe Abschnitt 3.1.4), sofern das MFG die GPS-Lokalisierung unterstützt.

Zu 3. Die auf Drohnen eingesetzten Methoden zur autonomen Lokalisierung erlauben je nach Einsatzbedingungen aus einer Höhe von 2 km die Lokalisierung mit einer Genauigkeit von 5 m bis 35 m (siehe Abschnitt 4). Durch die Wahl einer tieferen Flughöhe kann die Genauigkeit weiter gesteigert werden. GPS-fähige MFG ermöglichen die Lokalisierung mit einer Genauigkeit von unter 10 m [28]. Weitere Informationen wie beispielsweise Video, Signals Intelligence (SIGINT) oder Human Intelligence (HUMINT) sind zur Aufklärung des Zielgebiets ggf. hilfreich, aber für eine hinreichend genaue Ortung nicht notwendig.

Zu 4. Eine Telefonnummer (typischerweise die MSISDN) bzw. die netzinternen Rufnummern und Gerätekennungen (z.B. die IMEI und IMSI) sind unter günstigen atmosphärischen Bedingungen als einzige technische Daten ausreichend, um eine Fernlenkwaffe mit einem tödlichen Radius von 5 m mit hinreichender Treffergenauigkeit für eine gezielte Tötung einsetzen zu können. Die Zielführung mit Laser auf Basis einer ggf. zuvor durchgeführten Lokalisierung mit den nachfolgend beschriebenen Verfahren dürfte jedoch das übliche Verfahren der Fernlenkung sein.

2 Technische Grundlagen

Ausgangspunkt für die Ortung eines Mobilfunkgeräts (MFG) sind die vom Gerät ausgehenden Funkwellen sowie personenbezogene bzw. gerätespezifische Identifizierungsmerkmale (Rufnummern, Gerätekennungen).

Die von einem MFG ausgehenden Funkwellen können grundsätzlich geortet werden (siehe Abschnitt 2.1). Dabei ist es unerheblich, ob es sich um ein Mobiltelefon, Satellitentelefon, einen Tabletcomputer oder ein Funkgerät handelt.

In heutigen MFG des Massenmarktes können neben den Funkwellen auch Funktionen des jeweiligen Mobilfunknetzes (GSM, UMTS, LTE etc.), des Global Positioning Systems (GPS) und ggf. vorhandener Wireless LANs bei der Lokalisierung zum Einsatz kommen. Hier erfolgt die Ortung auf Basis personenbezogener bzw. gerätespezifischer Identifizierungsmerkmale (siehe Abschnitt 2.2). Entsprechendes gilt für Satellitentelefone.

2.1 Wellenausbreitung

Grundsätzlich lassen sich MFG aufgrund der Wellenausbreitungseigenschaften lokalisieren. Funkwellen breiten sich vom Ursprungsort in konzentrischen Kreisen aus und lassen sich durch Laufzeitpeilung und Richtungspeilung orten.

Bei der **Laufzeitpeilung** wird durch Zeitmessung bestimmt, welche Wegstrecke eine Funkwelle zurückgelegt hat. Daraus ergibt sich ein Radius, auf dem der Sender liegt. In einer Ebene sind zur Ortsbestimmung mindestens drei Messungen (an verschiedenen Orten) erforderlich, im Raum mindestens vier. Das satellitengestützte Global Positioning System (GPS) sowie die weit verbreiteten Mobilfunknetze nutzen die Laufzeitpeilung zur Ortsbestimmung von MFG. Die Methoden der Laufzeitpeilung werden gelegentlich als Time of Arrival (TOA) und Observed Time Difference (OTD) bezeichnet (siehe Abbildung 2.1). Konkrete Implementierungen der Laufzeitpeilung in Mobilfunknetzen sind z.B. Uplink-Time Difference of Arrival (U-TDOA) und Enhanced-OTD (E-OTD) (siehe auch Abschnitt 3.1.2).

Bei der **Richtungspeilung** wird mit einer Richtantenne ein Vektor bestimmt, auf dem der Ursprungsort der Welle liegt. In einer Ebene (z.B. auf der Erdoberfläche) sind bei der Richtungspeilung mindestens zwei Vektoren zur Ortung notwendig, im Raum (zusätzliche Bestimmung der Höhe) mindestens drei Vektoren. Die Richtungspeilung wird gelegentlich auch als Angle Of Arrival (AOA) bezeichnet (siehe auch Abbildung 4.2).

Ursachen für Ungenauigkeiten bei der Positionsbestimmung liegen in den physikalischen Eigenschaften der Funkwellen, welche durch Reflexion, Brechung, Streuung und Beugung oft nur auf indirektem Wege die Messpunkte erreichen.

Wir gehen vereinfachend davon aus, dass sich ein zu lokalisierendes MFG nicht bewegt. Bewegliche MFG lassen sich jedoch mit den hier beschriebenen Methoden gleichfalls

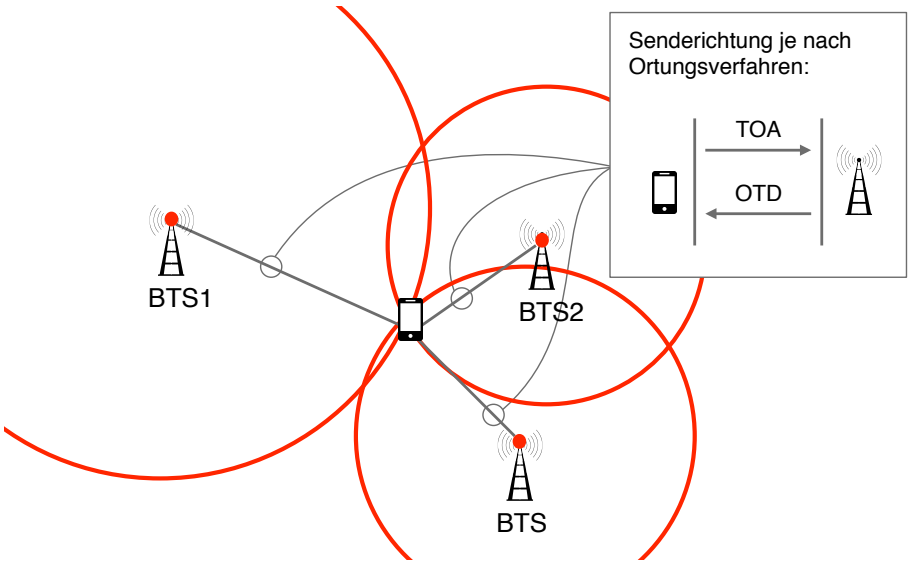

Abbildung 2.1: Lokalisierung mit Laufzeitpeilung (TOA und OTD)

orten, indem zusätzliche Annahmen über dessen Bewegungsrichtung getroffen und in die Berechnung des Ortes mit einbezogen werden.

Wird die Ortung von einem beweglichen Objekt durchgeführt, können die notwendigen Messungen (mindestens 2 bei Richtungspeilung, mindestens drei bei Laufzeitpeilung) von diesem einen Objekt an jeweils verschiedenen Orten erfolgen.

2.2 Identifizierungsmerkmale in Mobilfunknetzen

Mobilfunkgeräte (MFG) des Massenmarktes – dies können z.B. Handys, Tabletcomputer oder auch Laptops sein – nutzen heute üblicherweise einen der folgenden Mobilfunkstandards:

- Global System for Mobile Communications (GSM),
- Universal Mobile Telecommunications System (UMTS),
- Long-Term Evolution (LTE),
- Code Division Multiple Access (CDMA),
- Second-Generation CDMA (CDMA2000).

In CDMA- und CDMA2000-Netzen, die u.a. im Untersuchungszeitraums in Pakistan betrieben wurden [21], existieren nur gerätespezifische Kennungen. Dies sind die Electronic Serial Number (ESN) bzw. der Mobile Equipment Identifier (MEID). Die Kennungen ESN und MEID sind somit zugleich personenbezogene Merkmale, solange ein MFG nicht an eine andere Person weitergegeben wird.

In GSM-, UMTS und LTE-Netzen, die nahezu weltweit betrieben wurden und werden, kann eine Ortung eines MFG anhand der personenbezogenen Kennungen

- Mobile Subscriber Integrated Services Digital Network Number (MSISDN),
- International Mobile Subscriber Identity (IMSI)

und anhand der gerätespezifischen Kennung

- International Mobile Station Equipment Identity (IMEI)

erfolgen.

Die personenbezogene netzinterne Kennung IMSI ist üblicherweise in einem Subscriber Identity Module (SIM-Karte) gespeichert. Die SIM-Karte, die an eine bestimmte Person mit einer öffentlichen Rufnummer MSISDN ausgegeben wurde, personalisiert ein MFG.

Anhand der gerätespezifischen Kennung IMEI kann ein bestimmtes MFG unabhängig davon, ob bzw. welche SIM-Karte eingelegt ist, identifiziert werden.

Die Zuordnung der MSISDN zu einer bestimmten Person ist meist einem größeren Personenkreis bekannt.

Die Zuordnung der netzinternen Kennung IMSI zu einer bestimmten Person (bzw. zu seiner MSISDN) ist üblicherweise nur netzintern bekannt und wird in Datenbanken des Mobilfunkbetreibers gespeichert. Netzinterne Datenbanken der Mobilfunkanbieter, die Aufenthaltsorte der eingebuchten Teilnehmer speichern, sind das Home Location Register (HLR) und das Visitor Location Register (VLR).

Eine Zuordnung von MSISDN und IMSI bzw. der zugehörigen SIM-Karte lässt sich allerdings ggf. auch durch Dritte herstellen. So bieten etwa Online-Dienste [23, 22] die Möglichkeit zur Abfrage der Echtheit einer MSISDN kommerziell an. Mit solchen Online-Dienste kann auch die Zuordnung zu einem Mobilfunknetz, die sog. Mobile Number Portability (MNP), ermittelt werden.

Diese Online-Dienste greifen zurück auf standardisierte netzinterne Kommunikationsprotokolle der Mobilfunknetze. Ein solches Protokoll zur Abfrage und Übermittlung von mobilfunkinternen Daten ist das sog. Signalling System No. 7 (SS7) (siehe Abschnitt 3.1.4). SS7 erlaubt somit auch Dritten den Zugriff auf die netzinternen Datenbanken der Mobilfunkanbieter.

3 Lokalisierung

Alle folgenden Aussagen beziehen sich auf Lokalisierungsmethoden, die während des Untersuchungszeitraums generell möglich waren. Für den Untersuchungsgegenstand ist auch die konkrete Ausgestaltung des Mobilfunkverkehrs in den Ländern Afghanistan, Pakistan, Jemen und Somalia während des Untersuchungszeitraumes relevant. Wir besitzen keine spezifischen Kenntnisse über die dort zum Untersuchungszeitraum konkret vorhandene Mobilfunkinfrastruktur und den Verbreitungsgrad von GPS-fähigen Mobilfunkgeräten (MFG) in diesen Ländern.

3.1 Lokalisierung in zellularen Mobilfunknetzen

MFG können in den weit verbreiteten Mobilfunknetzen des Massenmarktes (GSM, UMTS etc.) ohne zusätzlichen technischen Aufwand geortet werden, d.h. das Mobilfunknetz implementiert bereits Funktionen zur Feststellung des Aufenthaltsorts eines Teilnehmers, die ggf. auch von Dritten genutzt werden können.

Neben der Abfrage der aktuellen Funkzelle, in die ein Teilnehmer eingebucht ist, lassen sich die Verfahren der Laufzeitpeilung mit Hilfe der ortsfesten Mobilfunkbasisstationen, sog. Base Transceiver Stations (BTS), einsetzen. MFG mit eingebautem GPS-Empfänger übermitteln zudem ggf. ihre GPS-Positiondaten an das Mobilfunknetz.

3.1.1 Abfragen der eingebuchten Funkzelle

Das Lokalisieren anhand der Funkzelle, in die ein Teilnehmer eingebucht ist, wird gelegentlich auch als Cell Of Origin (COO) bezeichnet. Jede Funkzelle hat in Mobilfunknetzen wie GSM, UMTS und LTE eine Nummer, die als Cell Identity (CI) bezeichnet wird (siehe Abbildung 3.1). Der Netzbetreiber speichert die CI aller eingebuchten Teilnehmer in seinen internen Datenbanken, um bei einem ankommenden Ruf die Verbindung in die Zelle weiterzuleiten, in der sich der Teilnehmer befindet.

Der Zugriff auf die in den internen Datenbanken gespeicherten Lokalisierungsinformationen durch Dritte ist mit den standardisierten Protokollen des Signalling System No. 7 (SS7) möglich (siehe Abschnitt 3.1.4).

Die Größe einer Funkzelle hängt von den örtlichen Gegebenheiten ab. In ländlichen Regionen kann eine Funkzelle einen Radius von ca. 30 km haben. In dicht bebauten städtischen Gebieten können Funkzellen einen Radius von 100 m haben bzw. werden teilweise auch durch Richtantennen gebildet, die einzelne Straßenzüge ausleuchten.

In Pakistan wurden im Untersuchungszeitraum auch die Mobilfunkstandards CDMA und CDMA2000 eingesetzt [21]. Diese Standards haben viele Gemeinsamkeiten mit GSM und UMTS, sodass die Ortung ähnlich erfolgen kann [4, 3]. MFG werden in CDMA- bzw.

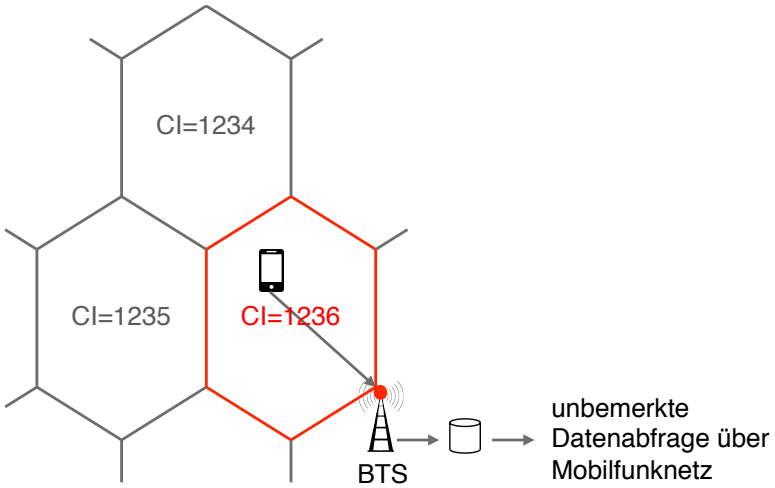

Abbildung 3.1: Netzbasierte Lokalisierung über Abfrage der Funkzelle

CDMA2000-Netzen ohne SIM-Karten betrieben, sodass anstelle der IMSI und der IMEI nur eine gerätespezifische Kennung existiert. Dies ist für CDMA die Electronic Serial Number (ESN) und für CDMA2000 die Mobile Equipment Identifier (MEID). Über einen SS7-Zugang können auch hier netzinterne Datenbanken von Dritten abgefragt und so die CI, d.h. die Kennung der aktuellen Funkzelle, ermittelt werden [3].

3.1.2 Laufzeitpeilung durch stationäre Mobilfunkbasisstationen

Zur Positionsbestimmung mit Hilfe der BTS, die in einem Versorgungsgebiet üblicherweise stationär sind, können eine Vielzahl von Verfahren verwendet werden [28, 19], welche auf der Laufzeitpeilung (TOA und OTD, siehe auch Abbildung 2.1) basieren.

Beim Verfahren Uplink-Time Difference Of Arrival (U-TDOA) wird die Ankunftszeit eines von einem MFG ausgesendeten Signals in der BTS gemessen und durch Differenzbildung der Ort des MFG bestimmt. Da das Mobilfunknetz anhand der Laufzeitunterschiede des Signals den Ort des MFG bestimmt, spricht man von einem netzbasierten Lokalisierungsverfahren.

Die Genauigkeit der Lokalisierung mit U-TDOA ist u.A. vom Abstand zwischen den Basisstationen abhängig. In einem Experiment mit einem Funkzellenradius von jeweils 5 km konnte die Position von 75 Prozent der MFG mit einer Genauigkeit von bis zu 100 m bestimmt werden [24].

Beim Verfahren Enhanced OTD (E-OTD) senden die Basisstationen Signale aus, das MFG empfängt die Signale und ermittelt seinen Ort selbständig, d.h. es handelt sich um ein sog. terminalbasiertes Lokalisierungsverfahren. E-OTD ist seit 1998 Bestandteil des GSM-Standards und ermöglicht Genauigkeiten von 50 m bis 125 m bei der Positionsbestimmung [28].

Da die E-OTD-Methode auf dem Empfang von Signalen aus mindestens zwei Nachbarfunkzellen angewiesen ist, kann sie nur in Gebieten mit entsprechend hoher Dichte an Mobilfunkbasisstationen genutzt werden. Diese Bedingung ist in den ländlichen

Regionen von Somalia, Jemen, Pakistan und Afghanistan überwiegend nicht erfüllt, sodass ausschließlich in den größeren Städten eine Ortung auf Basis von E-OTD erfolgen kann [11]. In ländlichen Regionen ist dennoch die genaue Positionsbestimmung durch das nachfolgend beschriebene GPS möglich, soweit das MFG einen GPS-Empfänger enthält.

3.1.3 Laufzeitpeilung durch GPS

Beim satellitengestützten Global Positioning System (GPS) berechnet das MFG anhand der Laufzeitunterschiede der von den GPS-Satelliten ausgesendeten Signale seine Position (siehe Abbildung 3.2), d.h. bei GPS handelt es sich um ein terminalbasiertes Lokalisierungsverfahren. Die Lokalisierung setzt einen GPS-Empfänger im MFG des Teilnehmers voraus und erreicht eine Genauigkeit von etwa 10 m [28].

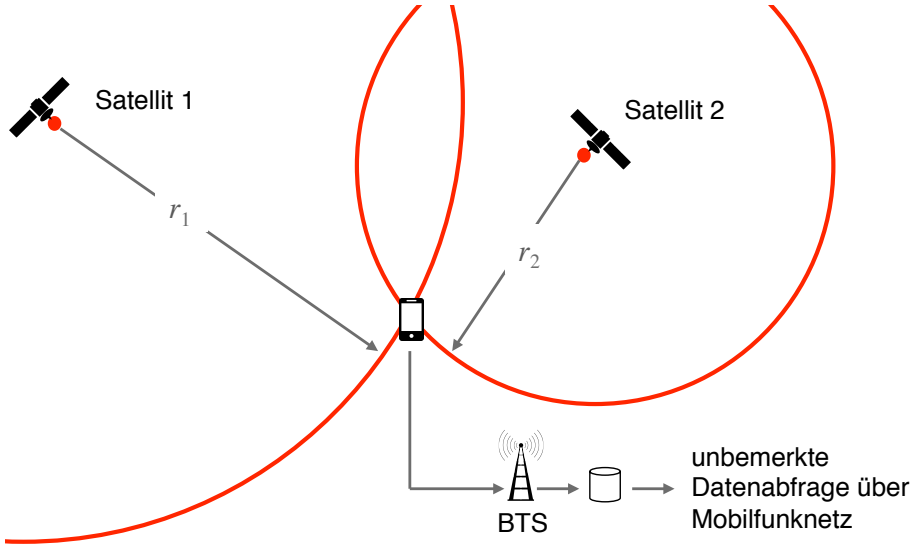

Abbildung 3.2: Terminalbasierte Lokalisierung mittels GPS (vereinfachte Darstellung)

3.1.4 Unberechtigte Abfrage von Lokalisierungsinformation

Da GPS und E-OTD terminalbasierte Lokalisierungsverfahren sind, erfährt das Mobilfunknetz zunächst nichts über den Aufenthaltsort eines MFG. Das Mobilfunknetz kann jedoch den aktuellen Ort eines MFG abfragen. In GSM- und UMTS-Netzen erfolgt die Abfrage der Standortdaten mit dem sog. Radio Resource Location Service Protocol (RRLP) [33]. Im LTE-Standard erfolgt die Abfrage durch einen sog. Radio Link Failure (RLF)-Bericht [30].

Zum Abfragen des Ortes mittels RRLP ist auch ein IMSI-Catcher (siehe Abschnitt 3.2) in der Lage.

Wie bereits angedeutet, ist der Zugriff auf die in den internen Datenbanken gespeicherten Lokalisierungsinformationen durch Dritte mit den standardisierten Protokollen des Signalling System No. 7 (SS7) möglich. Neben kommerziellen Anbietern [6, 15] gelang

es auch Privatpersonen [10], die SS7-Zugriffsmöglichkeit auf Ortungsinformation zu nutzen.

Die SS7-Abfrage ist nicht nur mit der aktuellen Nummer der Funkzelle (CI) möglich, sondern auch mit den durch U-TDOA, E-OTD und GPS ermittelten Koordinaten eines MFG.

3.2 Lokalisierung durch IMSI-Catcher

Ein IMSI-Catcher ist ein Gerät, welches die IMSI und die IMEI eines MFG auslesen kann. Hierfür tarnt sich der IMSI-Catcher als normale Basisstation eines Mobilfunknetzes und bringt erreichbare MFG im Einzugsbereich dazu, sich in die Funkzelle des IMSI-Catchers umzubuchen. Anschließend können die IMSI und die IMEI eines MFG abgefragt werden. Hierzu sendet der IMSI-Catcher einen sog. Identity Request an das MFG. Zumindest für GSM-Netze ist diese Angriffsmöglichkeit problemlos einsetzbar.

Für UMTS- und LTE-Netze existieren nach unserem Kenntnisstand keine universell einsetzbaren IMSI-Catcher, jedoch gibt es Forschungsansätze in diese Richtung [32, 30]. Praktische Relevanz haben in UMTS- und LTE-Netzen sog. **Downgrade-Angriffe**, welche UMTS- und LTE-fähige MFG zur Nutzung des GSM-Standards bewegen [5]. Auf diese Weise lassen sich in jedem Fall auch von Teilnehmern in UMTS- und LTE-Netzen die Standortdaten ermitteln.

Neben der Abfrage von IMSI und IMEI eines MFG durch einen Identity Request kann ein IMSI-Catcher auch dazu verwendet werden, lokal im MFG ermittelte Standortdaten (zumeist aus einer Ortung mittels GPS, E-OTD oder Wireless LAN) abzufragen: Zumindest im GSM lassen sich RRLP-Nachrichten (siehe Abschnitt 3.1.4) durch den IMSI-Catcher senden und empfangen. Die Standortübermittlung eines MFG an den IMSI-Catcher erfolgt dann ohne Kenntnis und Deaktivierungsmöglichkeit durch den Nutzer [33, 29].

3.3 Lokalisierung von Funkgeräten und Satellitentelefonen

Die Ortung von Funkgeräten unterscheidet sich von der im vorangegangenen Abschnitt beschriebenen Mobilfunkortung. Funkgeräte verwenden keine gerätespezifischen Merkmale, sodass eine personenbezogene Identifizierung erschwert wird. Anders als Mobiltelefone, die sich oft auch ohne eingelegte SIM-Karte mit einer Funkzelle verbinden und somit geortet werden können [34], lassen sich Funkgeräte nur während des aktiven Sendens von Signalen und damit während der aktiven Nutzung orten. Die Ortung eines Funkgeräts erfolgt durch Bestimmung der Empfangsrichtung wie sie in Abschnitt 2.1 beschrieben wurde.

Die Ortung von Satellitentelefonen kann beispielsweise durch Satellitenüberwachungssysteme wie ECHELON [26] umgesetzt werden. Üblicherweise sendet ein Satellitentelefon seine eigenen, selbständig gemessenen GPS-Koordinaten an den Satelliten des

Serviceproviders. Diese Daten können jedoch leicht durch andere Satelliten abgefangen werden und aufgrund der geringen Sicherheit der eingesetzten Verschlüsselung mitgelesen werden [7].

3.4 Lokalisierung durch Zugriff auf den Internet-Datenverkehr

Falls Zugriff auf den Internet-Datenverkehr eines MFG möglich ist, ergeben sich weitere Möglichkeiten zur Lokalisierung, die jedoch im Einzelnen hier nicht untersucht werden, da sie stark von den mobilen Software-Anwendungen (Apps) abhängen, die eine Person auf seinem MFG (hier: Smartphone) nutzt.

Beispielsweise heißt es für die Verwendung von Google Maps in den von Edward Snowden veröffentlichten Dokumenten für das Jahr 2008: „[i]t effectively means that anyone using Google Maps on a smartphone is working in support of a GCHQ system“ [2].

In Untersuchungen [8, 9] wurden im Internet-Datenverkehr von Smartphones unter anderem die IMSI, die IMEI sowie Standortdaten nachgewiesen. Eine andere Erhebung hat aus einem Mitschnitt von Internet-Datenverkehr durchschnittlich 50 Identifizierungsmerkmale pro Internetnutzer nachweisen können [17]. Teilweise können diese Identifizierungsmerkmale auch zur Zuordnung von Standortdaten im Internet-Datenverkehr genutzt werden.

Über die Namen der sichtbaren **Wireless LANs** eines MFG ist ebenfalls eine Positionsbestimmung möglich [18]. Das MFG scannt die in seiner Nähe empfangbaren Wireless LANs und sendet Daten über deren Empfangsstärke an eine Lokalisierungsdatenbank. Durch Auswertung des Internet-Datenverkehrs (zwischen den MFG und der Lokalisierungsdatenbank bzw. direkt auf der Lokalisierungsdatenbank) kann auch eine Lokalisierung von MFG durch Dritte erfolgen. Zudem lassen sich auch die über Wireless LAN ermittelten Standortdaten mittels RRLP (siehe Abschnitt 3.1.4) abrufen.

Weiterhin ist durch sog. **Remote Exploits** ein vollständiger Datenzugriff auf fremde MFG realisierbar [2, 31, 27]. Dabei wird auf dem MFG Schadsoftware installiert, mit der das Gerät vollständig kontrolliert werden kann. Für GPS-fähige Geräte ergibt sich hieraus ein unmittelbare Ortung.

Ob im Untersuchungszeitraum derartige Methoden zur Lokalisierung angewendet wurden, ist nicht bekannt.

4 Autonome Lokalisierung durch Drohnen

Im Folgenden wird zusammenfassend beschrieben, wie eine Drohne zur Ortung von Mobilfunkgeräten (MFG) des Massenmarktes (GSM, UMTS, CDMA etc.) eingesetzt werden könnte. Für diesen Zweck wird die Drohne mit einem speziellen IMSI-Catcher ausgestattet.

Grundlegende Informationen zur Lokalisierung von Funkwellen finden sich in Abschnitt 2.1. Allgemeine Erläuterungen zur Lokalisierung durch einen IMSI-Catcher finden sich in Abschnitt 3.2. Die Bedeutung des Radio Resource Location Service Protocol (RRLP) zur unberechtigten Abfrage von Lokalisierungsinformationen wird in Abschnitt 3.1.4 beschrieben.

Die Lokalisierung durch die Drohne erfolgt schrittweise:

1. Der IMSI-Catcher simuliert zunächst eine Funkzelle des Mobilfunknetzes.
2. Das MFG bucht sich in die simulierte Funkzelle ein. Dabei werden die IMSI und die IMEI des MFG an den IMSI-Catcher übertragen.
3. Mit Hilfe von RRLP werden ggf. auf dem MFG lokal mittels GPS oder anderer Lokalisierungsverfahren ermittelte Standortdaten abgefragt.
4. Während der Kommunikation zwischen MFG und IMSI-Catcher wird die Empfangsrichtung der Funkwellen bestimmt. Die Position des MFG ergibt sich aus dem Schnittpunkt der Erdoberfläche mit der Empfangsrichtung.

Ein von US-Stellen auf Drohnen eingesetzter IMSI-Catcher ist GILGAMESH, welcher laut Herstellerbeschreibung für das Frequenzspektrum des GSM-Mobilfunknetzes ausgelegt ist [1]. Die Sendeleistung dieses IMSI-Catchers ist vermutlich so groß, dass in Abhängigkeit von den geographischen und atmosphärischen Bedingungen eine Funkzelle mit einem Radius von max. 15 km aufgespannt werden kann.

Der IMSI-Catcher erfasst anschließend alle MFG durch einen Identity Request. Alle MFG senden ihre IMSI und ihre IMEI an den IMSI-Catcher. Dieser Vorgang kann auch mehrmals wiederholt werden, um zunächst den ungefähren Ort eines MFG einzugrenzen (siehe Abbildung 4.1).

Nach Auffinden einer bekannten IMSI bzw. IMEI könnte der IMSI-Catcher den aktuellen Ort des MFG mit dem Radio Resource Location Service Protocol (RRLP) abfragen (siehe Abschnitt 3.1.4), entweder um die Lokalisierungsgenauigkeit weiter zu erhöhen oder um den durch Peilung ermittelten Ort auf Plausibilität zu prüfen.

Zur Peilung der Funkwellen, d.h. Bestimmung der Empfangsrichtung der Funkwellen, wird Richtungspeilung (AOA, siehe Abbildung 4.2) und/oder Laufzeitpeilung (TOA, siehe Abbildung 4.3) angewendet.

Der Einsatz dieser Methoden durch militärische Drohnen ist nach unserem Kenntnisstand nicht belegt, erscheint jedoch technisch plausibel. Jedenfalls gelingt es technisch

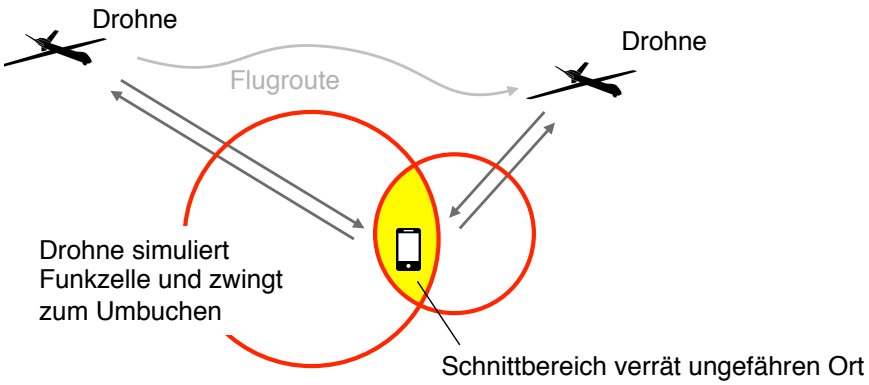

Abbildung 4.1: Ungefähre autonome Lokalisierung mittels Aufspannen einer Funkzelle durch einen an einer Drohne angebrachten IMSI-Catcher

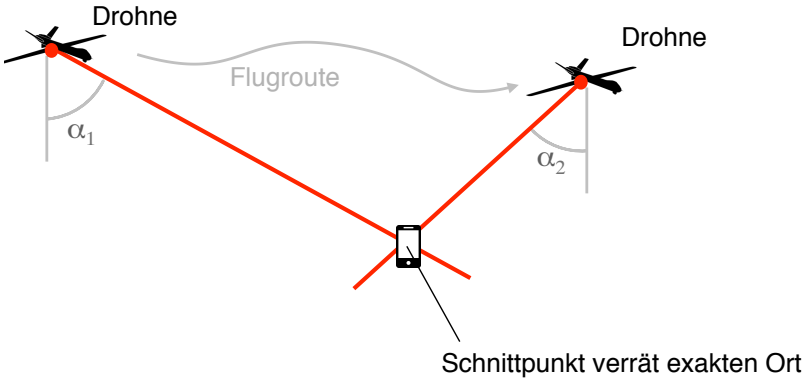

Abbildung 4.2: Autonome Lokalisierung durch eine Drohne mit Richtungspeilung (AOA)

interessierten Privatpersonen ohne Weiteres, eine entsprechende Peilung von MFG durchzuführen [25].

Für Drohnen sind entsprechende Antennen zur Bestimmung der Empfangsrichtung von Funkwellen kommerziell verfügbar und besitzen laut Herstellerangabe eine Messgenauigkeit von 2° bei einer Abdeckung von 360° im Azimutwinkel und 180° im Höhenwinkel [16].

Für die Ungenauigkeit der Positionsbestimmung des MFG ergibt sich somit ein Kreis mit einem Radius von 35 m bei einer angenommenen Flughöhe von 1 km.

Durch technische Optimierungen bei der Winkelmessung, beispielsweise die Fokussierung auf kleinere Azimut- und Höhenwinkel, sind Messgenauigkeiten im Bereich von $\pm$ 0,1° bis $\pm$ 1,0° realisierbar [14, 12, 35].

Unter der Annahme eines Messfehlers von maximal $\pm$ 1,0° kann der Aufenthaltsort des MFG aus einer Höhe von 2 km auf einen Kreis mit einem Radius von 35 m eingeschränkt werden.

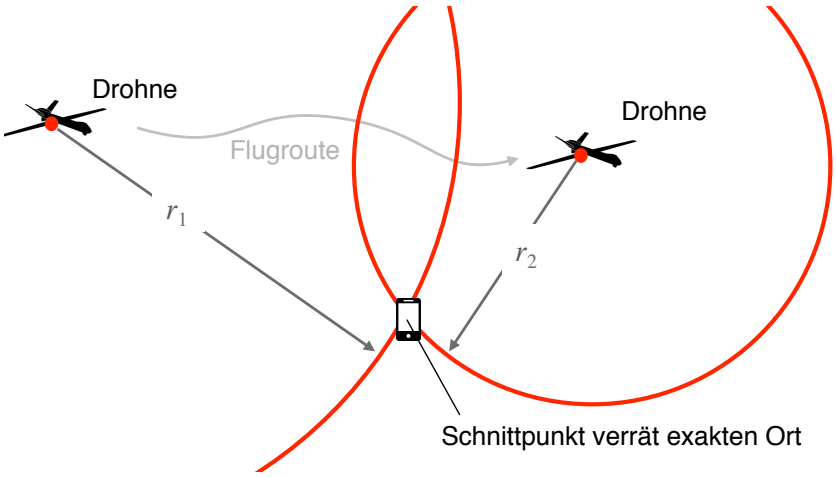

Abbildung 4.3: Autonome Lokalisierung durch eine Drohne mit Laufzeitpeilung (TOA)

Unter der Annahme eines Messfehlers von maximal $\pm$ 0,1° würde der Radius bei gleicher Höhe von 2 km unterhalb von 5 m liegen.

Zudem besteht die Möglichkeit, durch eine Reduzierung der Flughöhe die Positionsbestimmung weiter zu verbessern.

Somit ergibt sich unter günstigen atmosphärischen und geographischen Bedingungen die Möglichkeit, eine Fernlenkwaffe mit einem tödlichen Radius von 5 m mit hinreichender Treffergenauigkeit für eine gezielte Tötung einsetzen zu können.

Fernlenkwaffen wie die Hellfire-Raketen sollen mit einem 9 kg schweren Gefechtskopf einen bis zu 20 m großen tödlichen Radius haben [20]. Üblicherweise werden diese Systeme mit Laserunterstützung ferngelenkt.

Die konkrete Ausgestaltung des Mobilfunkverkehrs in den Ländern Afghanistan, Pakistan, Jemen und Somalia während des Untersuchungszeitraumes ist für die hier beschriebene Lokalisierung mittels IMSI-Catcher bedeutungslos, da das Lokalisierungsverfahren autonom arbeitet, d.h. nicht auf die Infrastruktur des Mobilfunknetzes angewiesen ist.

Abschließend ist festzustellen, dass die tatsächliche Arbeitsweise von auf Drohnen eingesetzten IMSI-Catchern leider nichts Näheres bekannt ist. Die Darstellung orientiert sich daher lediglich an den technischen Möglichkeiten, die während des Untersuchungszeitraumes bestanden.

Die Lokalisierung eines MFG bringt keine Gewissheit, welche konkrete Person das lokalisierte MFG bei sich hat, d.h. eine Personenidentifizierung ist mit den beschriebenen Verfahren nicht möglich. MFG können grundsätzlich auch falsche Identifizierungsmerkmale vortäuschen [13]. Somit ist eine zweifelsfreie Zuordnung von MFG zu Personen nicht möglich. Hier müssten ggf. weitere Aufklärungsmethoden hinzutreten.

Hamburg, 19.09.2016

Prof. Dr. Hannes Federrath

Literatur

[1] National Security Agency. *GILGAMESH (PREDATOR-based active geolocation)*. 2016. URL: https://theintercept.com/surveillance-catalogue/gilgamesh/ (besucht am 15. 09. 2016).

[2] James Ball. *Angry Birds and leaky phone apps targeted by NSA and GCHQ for user data*. 2014. URL: https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data (besucht am 02. 08. 2016).

[3] James J Caffery und Gordon L Stuber. *Overview of radiolocation in CDMA cellular systems*. In: *IEEE Communications Magazine* 36.4 (1998), S. 38–45.

[4] James Caffery und Gordon L Stuber. *Subscriber location in CDMA cellular networks*. In: *IEEE Transactions on Vehicular Technology* 47.2 (1998), S. 406–416.

[5] Giuseppe Cattaneo, Giancarlo De Maio und Umberto Ferraro Petrillo. *Security Issues and Attacks on the GSM Standard: A Review.* In: *J. UCS* 19.16 (2013), S. 2437–2452.

[6] Defencor Corporation. *Infiltrator Real-Time Tracking System*. URL: http://infiltrator.mobi/infiltrator.pdf (besucht am 02. 08. 2016).

[7] Benedikt Driessen. *Eavesdropping on Satellite Telecommunication Systems.* In: *IACR Cryptology ePrint Archive* 2012 (2012), S. 51.

[8] Manuel Egele u. a. *PiOS: Detecting Privacy Leaks in iOS Applications.* In: *NDSS*. 2011, S. 177–183.

[9] William Enck u. a. *TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones*. In: *ACM Transactions on Computer Systems (TOCS)* 32.2 (2014), S. 5.

[10] Tobias Engel. *SS7: Locate. Track. Manipulate.* 2014. URL: https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf (besucht am 02. 08. 2016).

[11] ENAiKOON GmbH. *OpenCellID Project*. 2016. URL: http://opencellid.org/ (besucht am 02. 08. 2016).

[12] Michael T Grabbe und Brandon M Hamschin. *Geo-Location Using Direction Finding Angles*. In: *Johns Hopkins APL Technical Digest* 31.3 (2013), S. 254–262.

[13] Sandro Grech und Pasi Eronen. *Implications of unlicensed mobile access (UMA) for GSM security*. In: *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*. IEEE. 2005, S. 3–12.

[14] D Guerin, S Jackson und J Kelly. *Passive Direction Finding - A Phase Interferometry Direction Finding System for an Airborne Platform*. 2012. URL: https://www.wpi.edu/Pubs/E-project/Available/E-project-101012-211424/unrestricted/DirectionFindingPaper.pdf (besucht am 02. 08. 2016).

[15] Verint Systems Inc. *Sky Lock - Product Descrition*. 2013. URL: https://assets.documentcloud.org/documents/2648148/Cellphone-Surveillance-Catalogue.txt (besucht am 02. 08. 2016).

[16] Southwest Research Institute. *Geolocation and COMINT Systems for UAV Platforms)*. URL: http://www.swri.org/3pubs/brochure/d16/GeoCom/GeoComBroch.pdf (besucht am 15. 09. 2016).

[17] Sakshi Jain, Mobin Javed und Vern Paxson. *Towards Mining Latent Client Identifiers from Network Traffic*. In: *Proceedings on Privacy Enhancing Technologies* 2016.2 (2015), S. 100–114.

[18] Jahyoung Koo und Hojung Cha. *Unsupervised locating of WiFi access points using smartphones*. In: *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 42.6 (2012), S. 1341–1353.

[19] Tomislav Kos, Mislav Grgic und Gordan Sisul. *Mobile user positioning in GSM/UMTS cellular networks*. In: *Proceedings ELMAR 2006*. IEEE. 2006, S. 185–188.

[20] Katrina Laygo u. a. *Drone Bombings in the federally administered Tribal areas: Public remote sensing applications for security monitoring*. In: *Journal of Geographic Information System* 4.2 (2012), S. 136.

[21] cellular-news Ltd. *Pakistan's PTCL Expands CDMA EVDO Rev A Coverage to 90% of the Population*. 2012. URL: http://www.cellular-news.com/story/Operators/53525.php (besucht am 02. 08. 2016).

[22] txtNation Ltd. *HLR Number Lookup*. 2016. URL: http://www.txtnation.com/mobile-messaging/hlr-number-lookup/ (besucht am 02. 08. 2016).

[23] Velocity Made Good Ltd. *A Brief Guide To HLR Lookups*. 2014. URL: https://www.hlr-lookups.com/open-downloads/a-brief-guide-to-hlr-lookups.pdf (besucht am 02. 08. 2016).

[24] R Mardeni u. a. *Efficient uplink time difference of arrival mobile device localization in cellular networks*. In: *2013 Asia-Pacific Microwave Conference Proceedings (APMC)*. IEEE. 2013, S. 1124–1126.

[25] Jorge Munoz-Castaner u. a. *Your Phone as a Personal Emergency Beacon: A Portable GSM Base Station to Locate Lost Persons*. In: *IEEE Industrial Electronics Magazine* 9.4 (2015), S. 49–57.

[26] Patrick S. Poole. *ECHELON: America's Secret Global Surveilance Network*. 2000. URL: http://www.bibliotecapleyades.net/ciencia/echelon04.htm (besucht am 02. 08. 2016).

[27] Marcel Rosenbach, Laura Poitras und Holger Stark. *iSpy: How the NSA Accesses Smartphone Data*. 2013. URL: http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html (besucht am 02. 08. 2016).

[28] Ana-Maria Roxin u. a. *Survey of wireless geolocation techniques*. In: *IEEE globecom workshops*. 2007, 9–Pages.

[29] Altaf Shaik u. a. *LTE and IMSI catcher myths*. Blackhat EU. 2015. URL: https://www.blackhat.com/docs/eu-15/materials/eu-15-Borgaonkar-LTE-And-IMSI-Catcher-Myths.pdf (besucht am 02. 08. 2016).

[30] Altaf Shaik u. a. *Practical attacks against privacy and availability in 4G/LTE mobile communication systems*. In: *arXiv preprint arXiv:1510.07563* (2015).

[31] Ashkan Soltani, Andrea Peterson und Barton Gellman. *NSA uses Google cookies to pinpoint targets for hacking*. 2013. URL: https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/ (besucht am 02. 08. 2016).

[32] Joe-Kai Tsay und Stig F Mjølsnes. *A vulnerability in the UMTS and lte authentication and key agreement protocols*. In: *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*. Springer. 2012, S. 65–76.

[33] Harald Welte. *Report of OpenBSC GSM field test*. 2009. URL: http://openbsc.osmocom.org/trac/raw-attachment/wiki/FieldTests/HAR2009/har2009-gsm-report.pdf (besucht am 02. 08. 2016).

[34] Svein Yngvar Willassen und Steinar Andresen. *A method for implementing mobile station location in GSM*. Norwegian University of Science an Technology. 1998.

[35] Pan Yujian u. a. *DOA estimation accuracy improvement for circular array interferometer with analog phase detector and its FPGA implementation*. In: *Wireless Symposium (IWS), 2014 IEEE International*. IEEE. 2014, S. 1–4.