

# **Man-In-The-Middle**

Attenberger, Bollenmiller, Schuster, Wilhelm

-Team J3A-

Hochschule München

29. September 2017

# Inhalt

- **Projektziel**
- **Architektur**
  - OpenBTS
  - Osmocom
- **Umsetzung des Projektziels**
- **Probleme/ Lessons learned**
- **Live-Demo**



# Projektziel



# Projektziel

- Inbetriebnahme eines GSM Netzes
- Aufzeichnen und Abspeichern der Daten eines Telefongesprächs
- Lokales Abspielen des Gesprächs

## *Optionales Feature*

- Hinterlegung einer Rufnummer
- Abspielen des Telefongesprächs bei Anruf der festgelegten Nummer

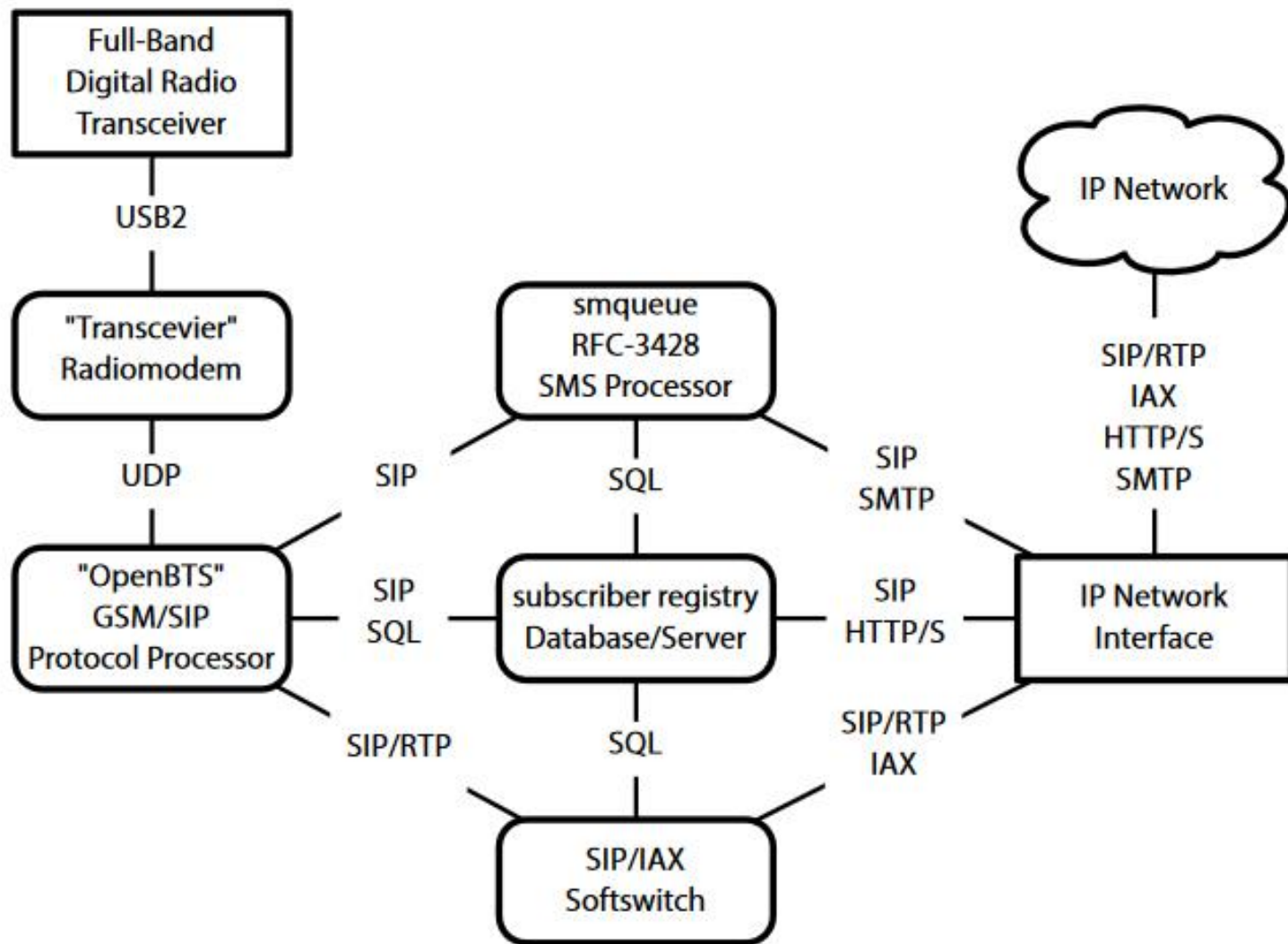




# Architektur OpenBTS





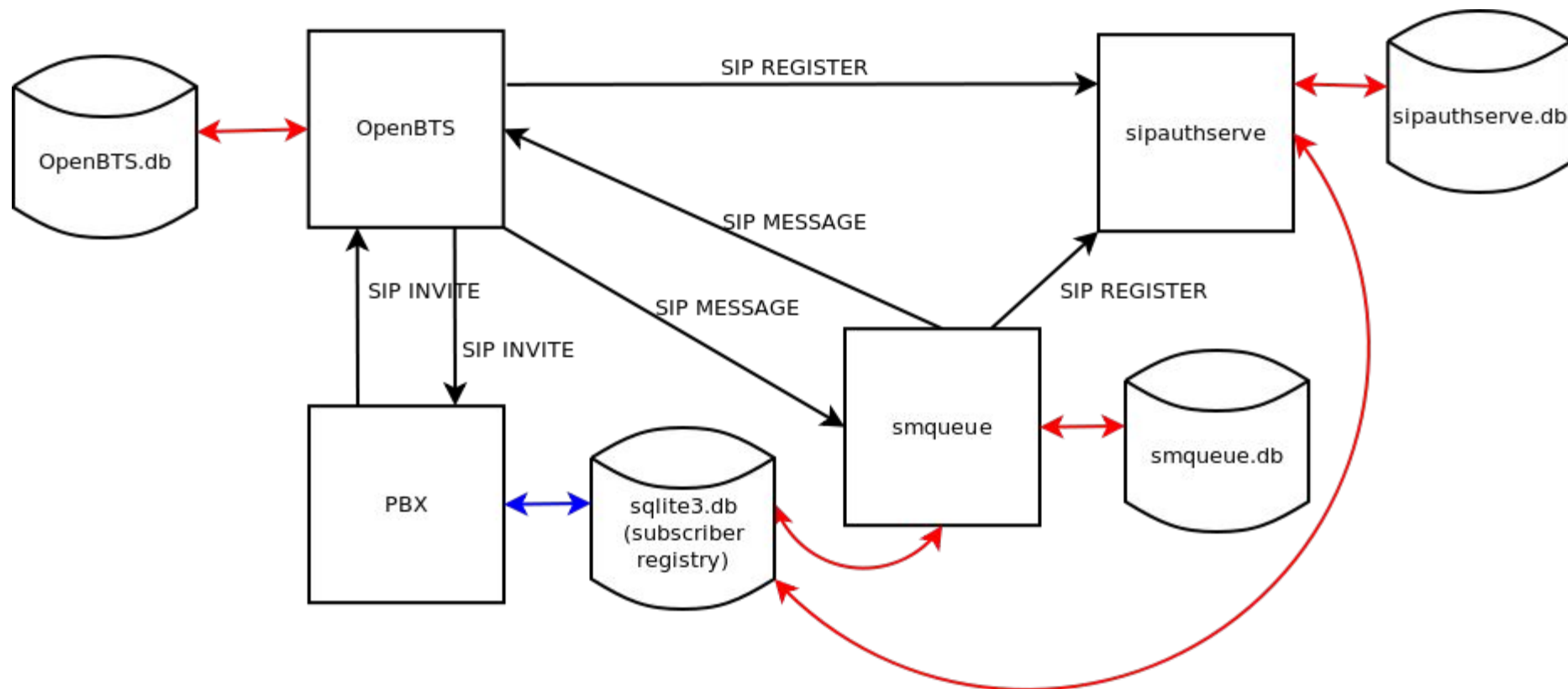


# Systemarchitektur eines GSM-Netzes mit OsmoBTS

Bestandteile von OpenBTS:

- OpenBTS: Die eigentliche OpenBTS-Anwendung, die den Großteil des GSM-Stacks oberhalb des Radiomodems realisiert
- Transceiver: Software-Radiomodem und Hardware-Kontrollsystem, welches für die Anbindung des USRP N210 SDR zuständig ist
- Asterisk: Private Branch Exchange (PBX), der Hauptfunktionen des Mobile Switching Center (MSC) übernimmt
- SIPAuthServe: Verwaltung einer Subscriber Registry Datenbank, die dem Home Location Register (HLR) ähnelt
- SMQueue: Store-and-Forward Message Service für die Übertragung und Speicherung von SMS-Nachrichten





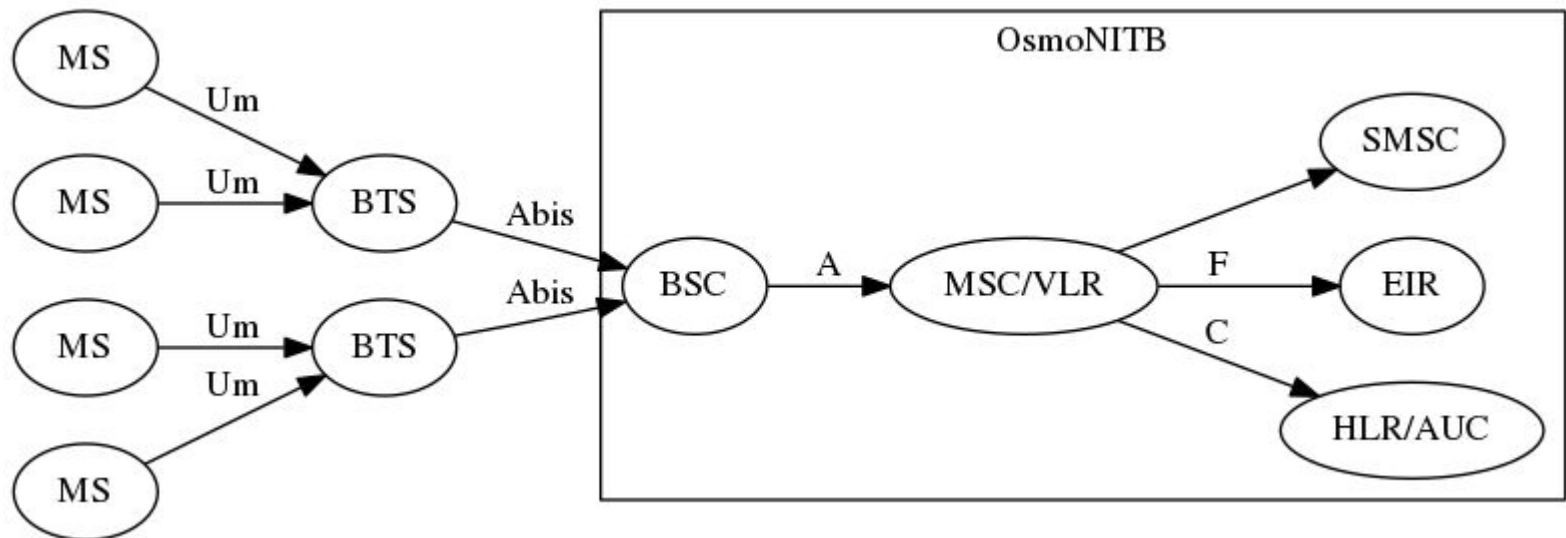
# Architektur Osmocom



# Systemarchitektur eines GSM-Netzes mit OsmoNITB

OsmoNITB ist ein Projekt aus dem OsmocomBB-Umfeld.

OsmoNITB implementiert das Network Switching Subsystem (NSS) im GSM-Netz, aber mit OpenBSC auch Teile des Base Station Subsystems (BSS).



# Systemarchitektur eines GSM-Netzes mit OsmoNITB

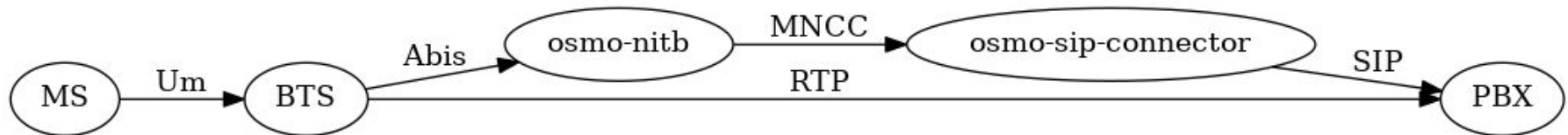
Bestandteile von OsmoNITB:

- BSC: Basisstation-Controller; Überwacht Mobilfunkverbindung und regelt die Leistung; Löst einen Zellenwechsel (Handover), falls erforderlich, aus
- MSC/ VLR: Mobile-service switching center ist Vermittlungsstelle im GSM/GPRS-Netz; Übernimmt die Anrufverwaltung/ Authentifizierung und Gebührenerfassung.  
Visitor Location Register (VLR) → Datenbank, die verwaltet, in welcher BTS ein MS zuletzt eingebucht war
- SMSC: Server für SMS-Dienste; Verarbeitung von Textmitteilungen
- EIR (Equipment Identity Register) → Optional; Datenbank für Seriennummern der Mobilgeräte (IMEI) gespeichert → Sperren verlorener oder gestohlener Endgeräte
- HLR/AUC: Home Location Register ist Datenbank in der die Rufnummer, IMSI & TMSI eines Mobiltelefons hinterlegt ist.  
Authentication Center (AUC): Authentifizierungszentrale; Ort, an dem Authentifizierungsschlüssel Ki abgelegt ist; Authentifizierung der SIM-Karte gegenüber Mobilfunknetz



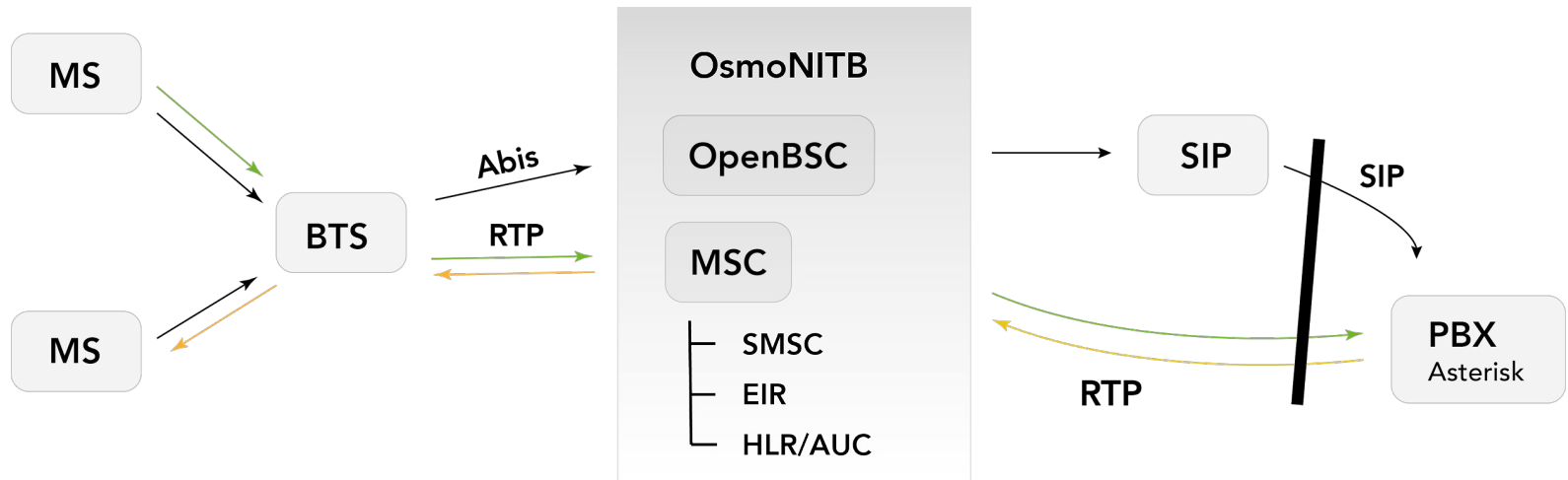
# VoIP im GSM-Netzes

- Osmocom-SipConnector wirkt als Vermittler der klassischen ISDN-Anrufsteuerungsprotokoll (MNCC) und dem SIP-Protokoll
- Connector ist notwendig um eine Verbindung mit Asterisk aufzunehmen
- Asterisk ist eine virtuelle Telefonanlage, die als Vermittlungsstelle genutzt werden kann



# Unser System

- Eine BTS, Osmocom-Abis-Interface, OsmoNITB, OsmocomSipConnector, Asterisk
- Abgriff der Gespräche am schwarzen Balken





# Umsetzung des Projektziels



# Umsetzung des Projektziel

- Aufzeichnen und Abspeichern der Daten
  - pcapsipdump

The screenshot displays the Wireshark interface with a packet capture file named '20170927-164237-30628-35366-f29af1b6-1e34-1236-b0a6-00265a686174.pcap'. The interface includes a menu bar (Datei, Bearbeiten, Ansicht, Navigation, Aufzeichnen, Analyse, Statistiken, Telefonie, Wireless, Tools, Hilfe) and a toolbar. The main display area shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The first packet is a SIP INVITE request from 127.0.0.1 to 127.0.0.1. Subsequent packets show SIP status responses (100 Trying, 180 Ringing, 200 OK) and an ACK. Following these are RTP and RTCP packets for a GSM audio stream. The bottom pane shows the details of the selected packet (Frame 1), indicating it is a Session Initiation Protocol (INVITE) packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	SIP/S...	684	Request: INVITE sip:35366@127.0.0.1:5060
2	0.000784	127.0.0.1	127.0.0.1	SIP	570	Status: 100 Trying
3	2.757274	127.0.0.1	127.0.0.1	SIP	586	Status: 180 Ringing
4	3.999479	127.0.0.1	127.0.0.1	SIP/S...	824	Status: 200 OK
5	3.999772	127.0.0.1	127.0.0.1	SIP	353	Request: ACK sip:35366@127.0.0.1:5060
6	4.016068	127.0.0.1	127.0.0.1	RTP	87	PT=GSM 06.10, SSRC=0x16E55A6E, Seq=26163, Time=1077569409, Mark
7	4.016848	127.0.0.1	127.0.0.1	RTP	87	PT=GSM 06.10, SSRC=0x2296DDD1, Seq=9545, Time=115475390
8	4.016862	127.0.0.1	127.0.0.1	RTCP	110	Sender Report Source description
9	4.034508	127.0.0.1	127.0.0.1	RTP	87	PT=GSM 06.10, SSRC=0x16E55A6E, Seq=26164, Time=1077569569
10	4.041646	127.0.0.1	127.0.0.1	RTP	87	PT=GSM 06.10, SSRC=0x2296DDD1, Seq=9546, Time=115475550
11	4.058700	127.0.0.1	127.0.0.1	RTP	87	PT=GSM 06.10, SSRC=0x16E55A6E, Seq=26165, Time=1077569720

Frame 1: 684 bytes on wire (5472 bits), 684 bytes captured (5472 bits)  
> Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
> User Datagram Protocol, Src Port: 5069, Dst Port: 5060  
> Session Initiation Protocol (INVITE)

20170927-164237-30628-35366-f29af1b6-1e34-1236-b0a6-00265a686174 | Pakete: 2874 · Angezeigt: 2874 (100.0%) · Ladezeit: 0:0.21 | Profil: Default

# Umsetzung des Projektziel

- Aufzeichnen und Abspeichern der Daten
  - pcapsipdump
- Extrahieren und konvertieren der Daten
  - pcap2wav
- vollständige Automatisierung
  - Incron
- Feature - Abhören der Nachricht
  - Bestimmte Rufnummer hinterlegen
  - Abspielen des Gesprächs bei Anruf der definierten Nummer



MitM

GSM-Netz erzeugen

Administratorpasswort:

.....

Transceiver:

Stoppen

OsmoBSC:

Stoppen

OsmoBTS:

Stoppen

Sip-Connector:

Stoppen

Wireshark:

Starten

SQLiteBrowser:

Starten

Gespräch ausspähen

PcapSipDump:

Stoppen

Slot 1

Slot 2

Slot 3

Slot 4

Slot 5

# Probleme/ Lessons learned



## Probleme/ Lessons learned

- Konfiguration von OpenBsc und Osmo-Bts ✓
- Installation sämtlicher Abhängigkeiten ✓
- Backup-System → parallele Inbetriebnahme zweier Systeme ✓
- Automatisierung des Abspeicherns und Abhörens ✓
- Aufzeichnen und Abspeichern des Telefongesprächs → Systemperformanz ✓
- Hinterlegen der Rufnummer ✓



# Live-Demo



**Vielen Dank für Ihre Aufmerksamkeit!**

**Fragen?**

