Technische
Hochschule
Wildau [FH]
Technical University
of Applied Sciences

Secure Mobile Voice Communication on an Open Platform

Phase 1 of a Master Students' Project

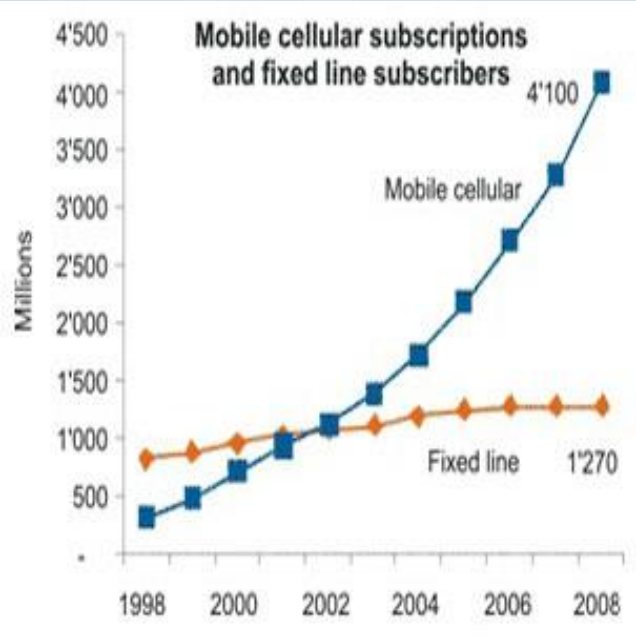
Authors: *Alexander Höftmann, Christine Mummert, Christian Paschke, Mario Stemmler, and Günter-Ulrich Tolkiehn*

Conference contribution at the RCM in Bhubaneswar, 25th Sept., 2010

Project idea and basic conditions

- Aim: Free, secure telephony for standard mobile phones
- Restrictions:
  - Solution achievable by a team of four in two terms, 6 CP (i.e 4 persons x 180 work-hours) per term
  - No encryption-related code development
- First phase: SIP telephony over WLAN, LAN
- Second phase: SIP telephony over Internet, use of GPRS, UMTS…

Motivation



- New, still growing global ubiquitousness
- Used for all purposes, incl. confidential ones
- Privacy is protected by law
- Security is commonly presumed

Chart source: http://www.mocom2020.com/2009/03/41-billion-mobile-phone-subscribers-worldwide/

photo source: http://www.zeit.de/digital/internet/2010-06/bundespraesident-twitter

Motivation

- Air interface renders special vulnerability
- While many older mobile communication systems were already hacked, GSM was for some time presumed secure
- Several brute force attacks on GSM were performed and published since 2007[1]
- In 12/2009 an attack within three months with a cluster of 40 commercial computers using CUDA graphic processors, with public software was reported at the 263C in Berlin

[1] see e.g. http://en.wikipedia.org/wiki/A5/1#Attacks_on_A5.2F1_as_used_in_GSM

[2] Chris Paget and Karsten Nohl 2009, see e.g. http://www.h-online.com/open/news/item/26C3-GSM-hacking-made-easy-893245.html

Motivation

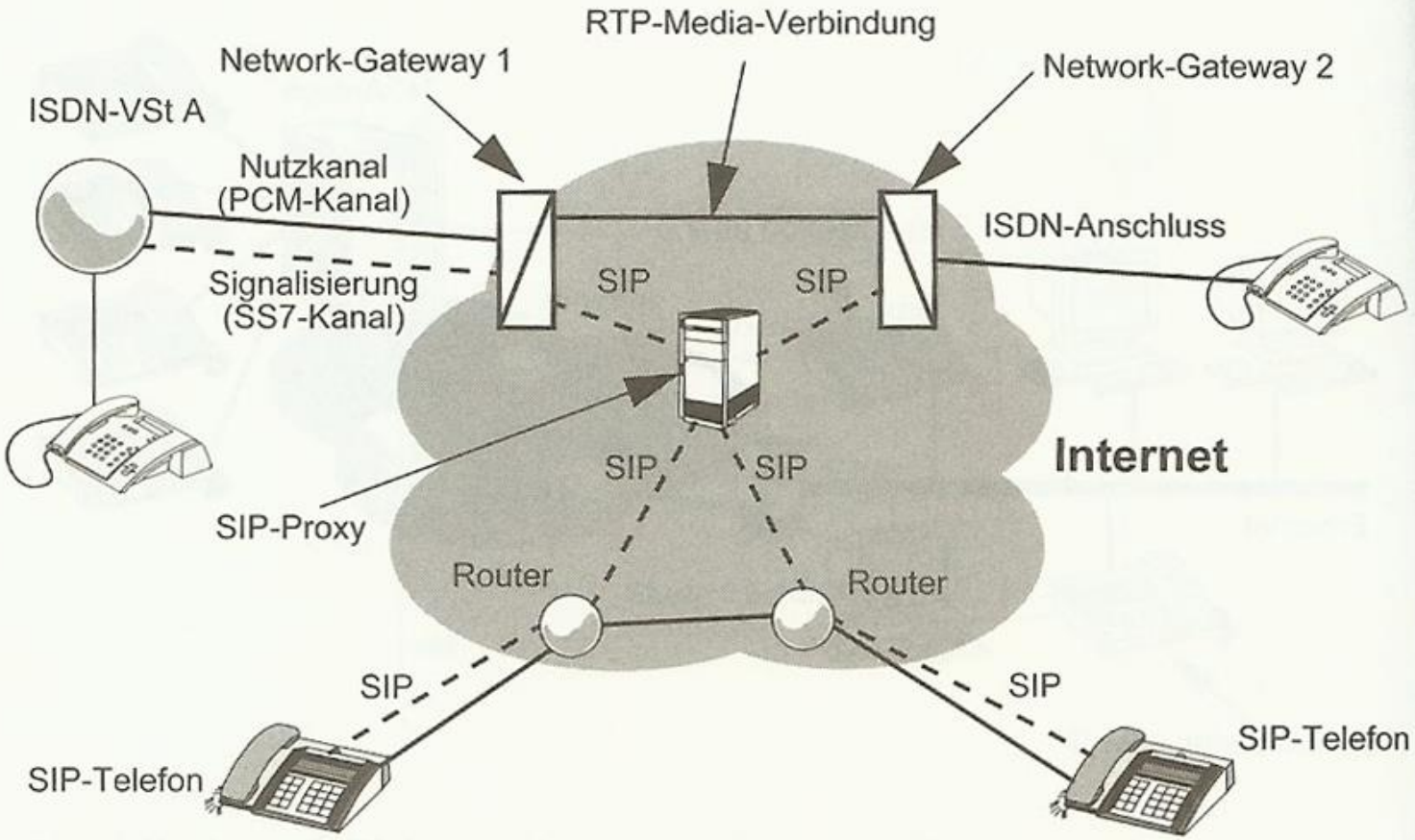
- Discussion with German encryption specialist ATMedia
- Other projects for secure mobile communication during the last 2 years, e.g.:
  - In 2/2008: DH Ryu and SG Nam reported about their project “Implementation of Wireless VoIP System based on VPN” using standard PC‘s with Linux and open source software
  - in 12/2009: rollout of 5250 secure mobile phones for members of the German federal government and administration (using secure voice over CSD)
  - German Telekom’s announcement of a secure VoIP-system *SiMKo2* on the CeBIT fair in 2010
  - TAS GmbH’s presentation of *Mobikrypt* for secure mobile conferencing on the same event

Our approach

- Use IP, not GSM telephony nor CSD
- Use open standard mobile platforms
  - Openmoko
  - Android
- Phase 1:
  - Use voice over WLAN on Android
  - Use Asterisk as switch
  - Use OpenVPN/OpenSSL in TUN (L3) mode
  - Stay on the LAN/WLAN first
- Phase 2: Everything else ☺
  - Out into the internet
  - Use GPRS, UMTS…

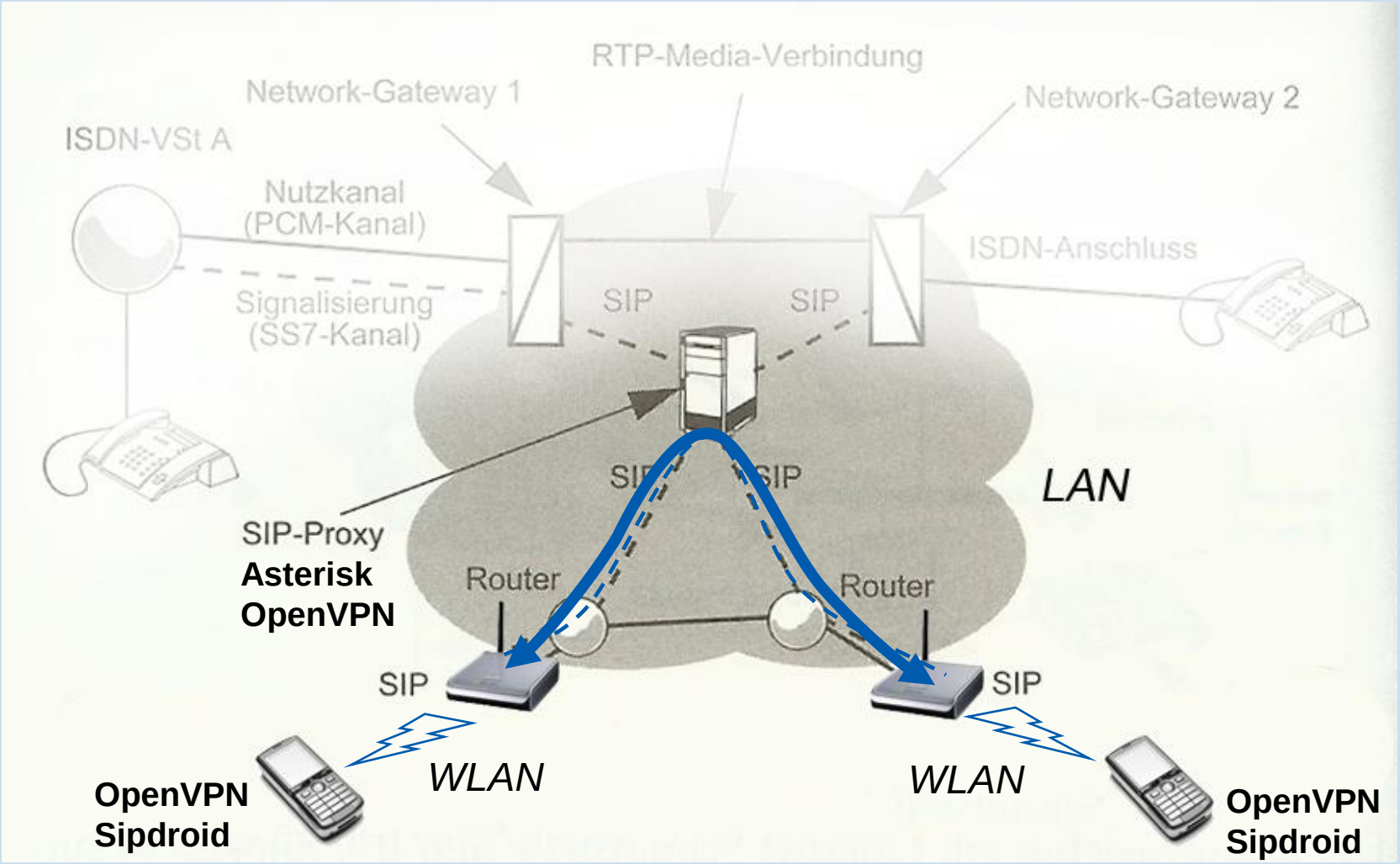
IP-telephony with SIP in the textbook

Abb. 6.26: *SIP-Telefone brauchen keinen Gateway*



Source: Siegmund, Next Generation Networks

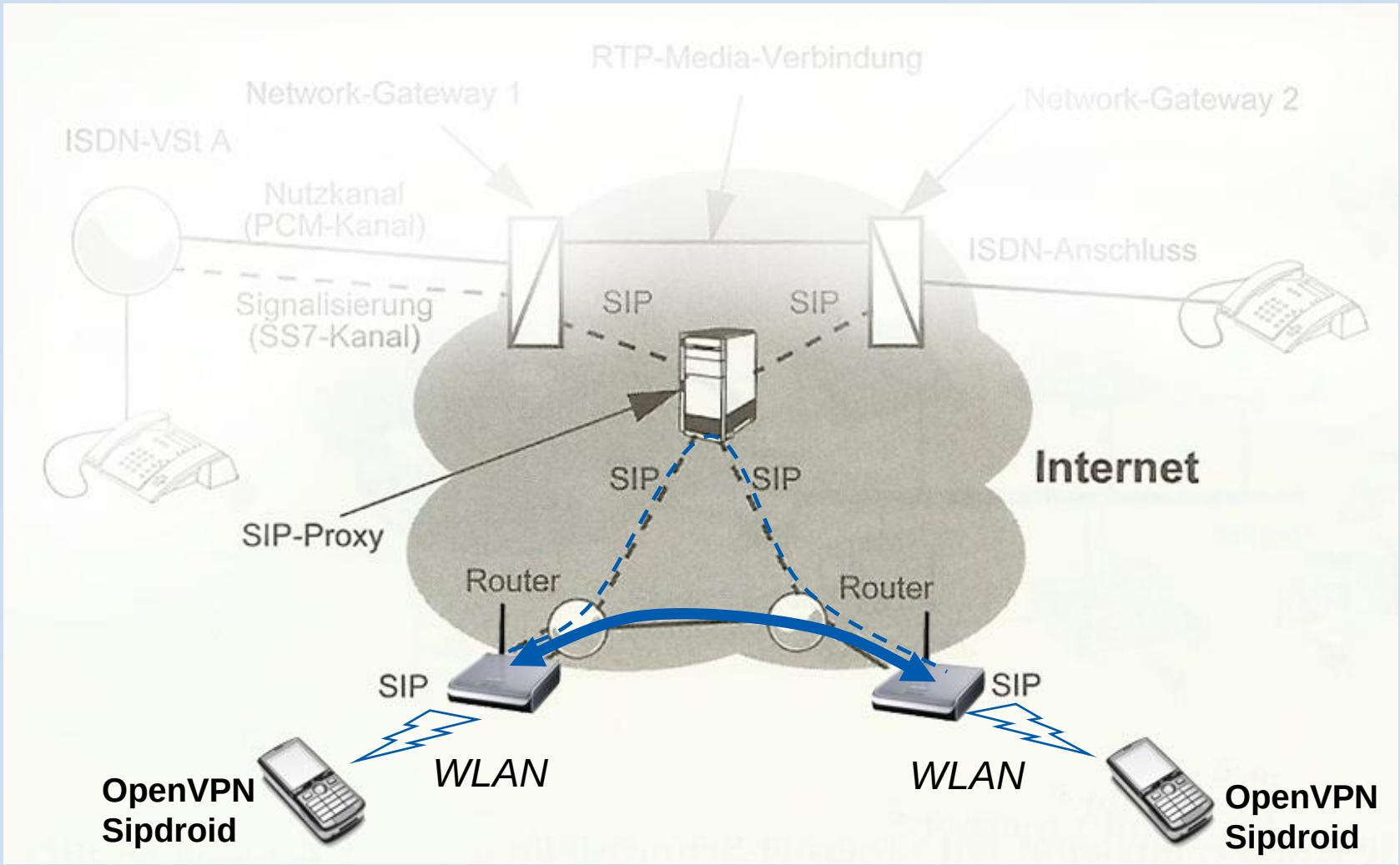
Phase 1:



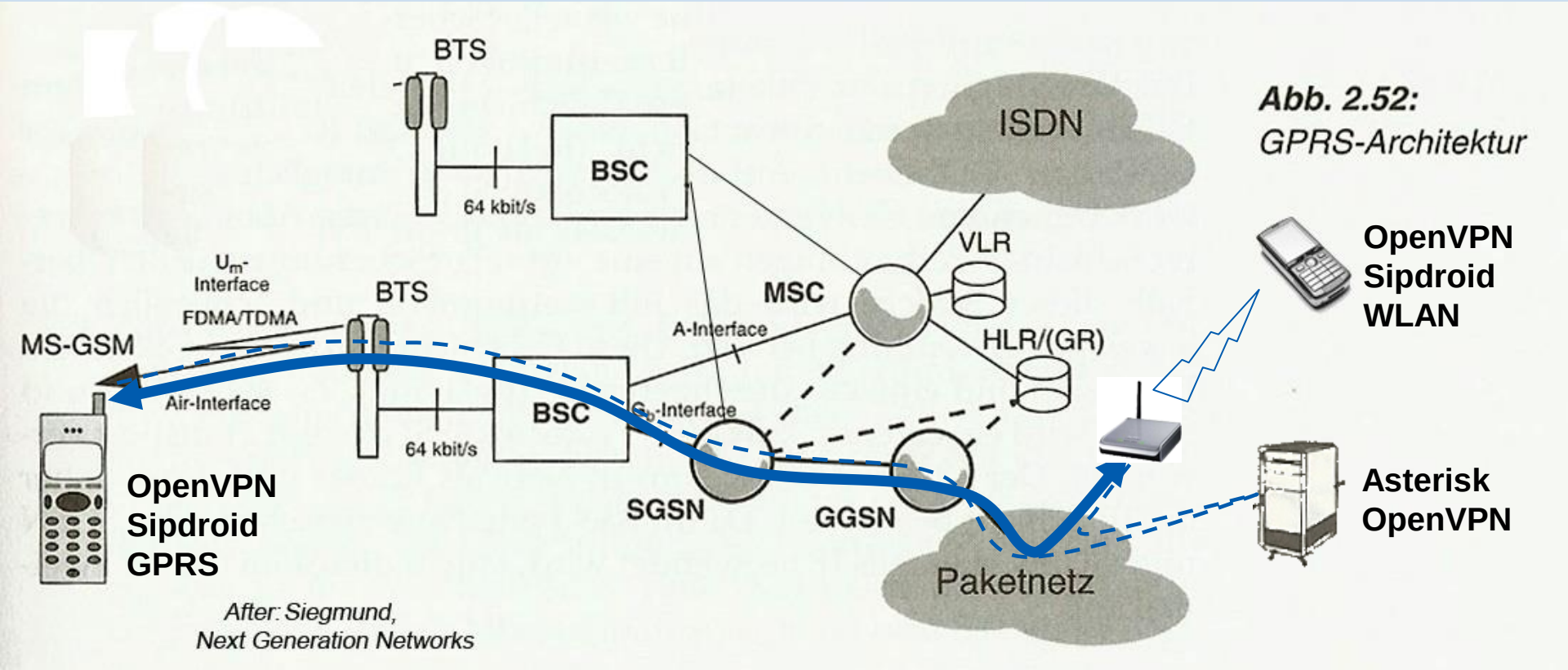
Items of interest and first results

- Voice quality: like GSM on first glance – quantitative measurements to follow
- Delay (<500ms), dependence on codec (G.711 and GSM) and encryption method, preliminary results not yet completely understood
- Consumption of system resources: VPN client: <10% CPU, SIP: 80–90% CPU

Phase 2, a: Via WLAN over the Internet

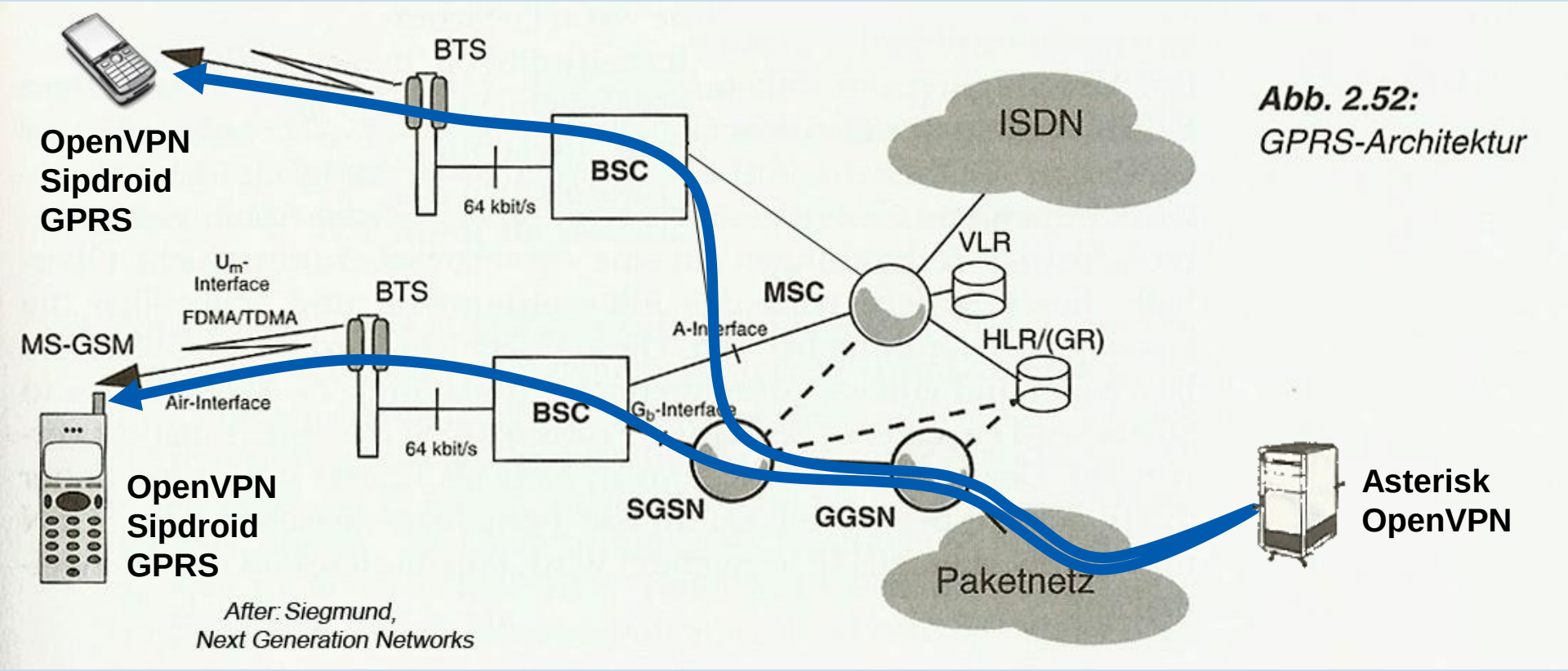


Phase 2, b: VoIP via GPRS

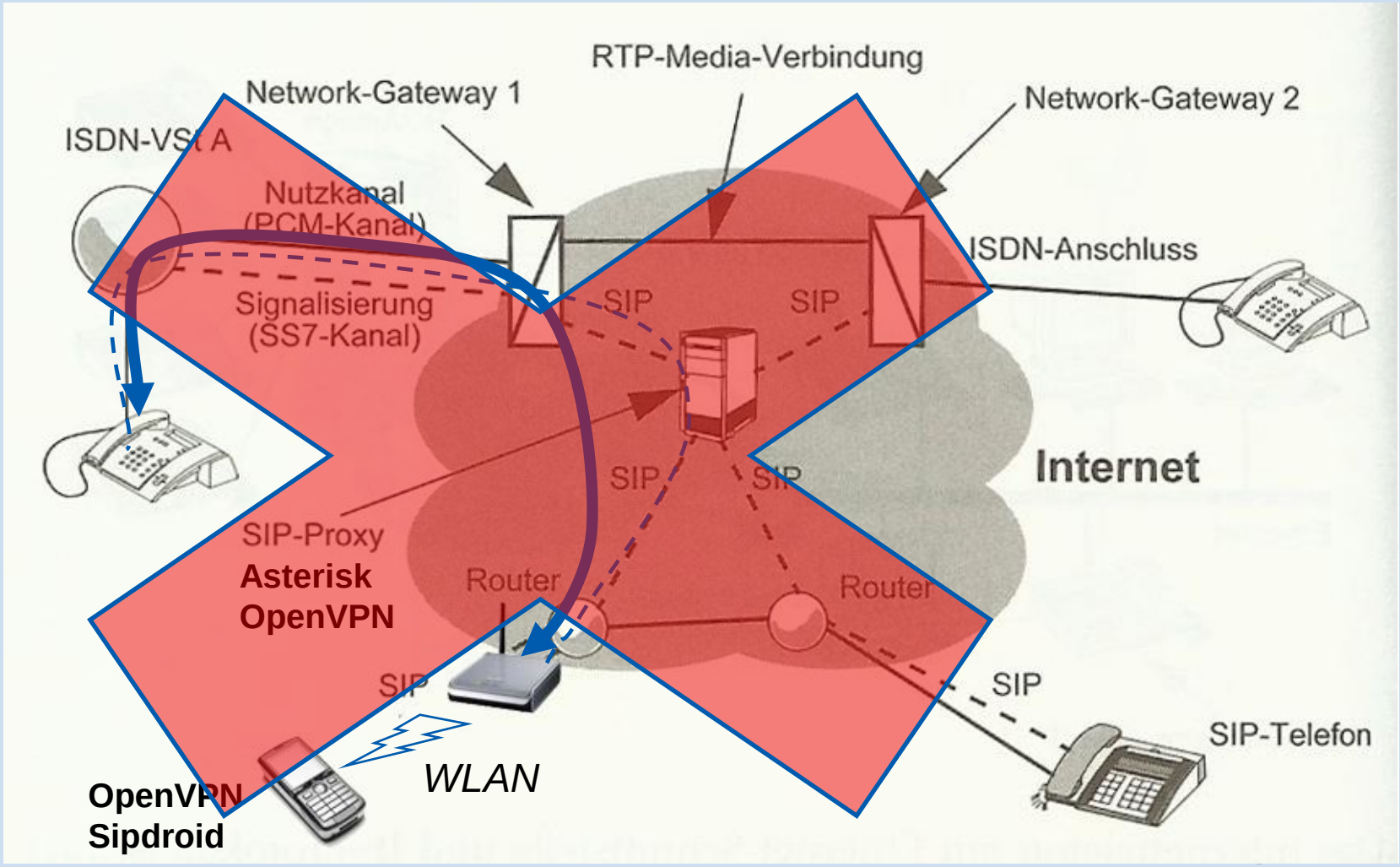


SGSN: Serving GPRS Support Node
GGSN: Gateway GPRS Support Node

Phase 2, b: VoIP via GPRS both ends



Phase 2, c: Via Internet, GW to PSTN?



Items of interest

- Voice quality (quantitative measurements)
- Delay, dependence on codec and encryption method
- Jitter
- Packet loss rates
- Prioritization
- Handover capability
- Consumption of system resources
- Battery life
- Connectivity
- Usability for end-users

Our successful team,

from left:
Christian Paschke
Christine Mummert
Alexander Höftmann
Mario Stemmler

Thanks for your attention!

- Questions and comments welcome!

Günter-Ulrich Tolkiehn
tolkiehn@th-wildau.de
Sip: 1627128@sipgate.de
Our own SIP server addresses on request