Bern University of Applied Sciences
Engineering and Information Technology

InstaCircle

A Location-Bound Ad-Hoc Network for Android Devices

Jürg Ritter, 27.03.2013

Outline

- Introduction
- The Idea
- Communication Technologies
- Result
- Architecture & Design
- Conclusion
- Discussion

Introduction

- The E-Voting Group of the Bern University of Applied Sciences would like to gain some experience in dealing with decentralized E-Voting systems
- «Decentralized» → no central infrastructure
- In the E-Voting science community, a few approaches like HKRS12 have emerged
- 2 master theses in this area are planned in the next year
- Each thesis should implement a different approach

The Idea

- Implement E-Voting systems on mobile devices such as smartphones or tablets
- Many people possess such devices
- Spontaneous polls could be set up using these devices
- Today's mobile devices are powerful enough to combine strong cryptography and usability

The term «decentralized»

- Decentralized → no central infrastructure required
- Instead we need:
  - A broadcast system to keep all parties informed
  - Mechanisms to correct anomalies
  - A mechanism to join devices to an ad-hoc network easily

The goal

- Implement a communication platform which allows to
  - Easily join the mobile devices to an ad-hoc network
  - Send messages to all participants (broadcast)
  - Send messages to particular participants (unicast)
  - Correct anomalies such as message loss
  - Protect the communication and control the access to the conversation
- The communication has to work in a confined space (e.g a meeting room or a conference hall)
- Implementation for Android

Communication Technologies

- In the world of mobile devices, some standards for wireless communication have evolved
  - Bluetooth
  - Wi-Fi
  - Wi-Fi Direct
  - NFC
  - QR Codes

Bluetooth

- Bluetooth is a standard for wireless communication on mobile devices with the following properties:
  - Short range communication (ca. 5 meters indoors)
  - Peer-to-peer communication
  - Allows to build so called «Pico» networks with up to 3-4 nodes (depending on the device)
  - Low power consumption
  - Low bandwidth

Wi-Fi

- The Wi-Fi standard was intended to create a wireless version for ethernet
  - Mid range communication (ca. 30 meters indoors)
  - Hot spots are acting as data hubs
  - Scales very well
  - High bandwidth
  - Relatively high power consumption

Wi-Fi Direct

- Wi-Fi Direct is a Wi-Fi substandard
  - Intended as a peer-to-peer Wi-Fi
  - No hot spots needed (hot spots are set up ad-hoc)
  - Allows to build small group networks
  - Emerging standard, only new devices support it
  - Interacts with current Wi-Fi standard

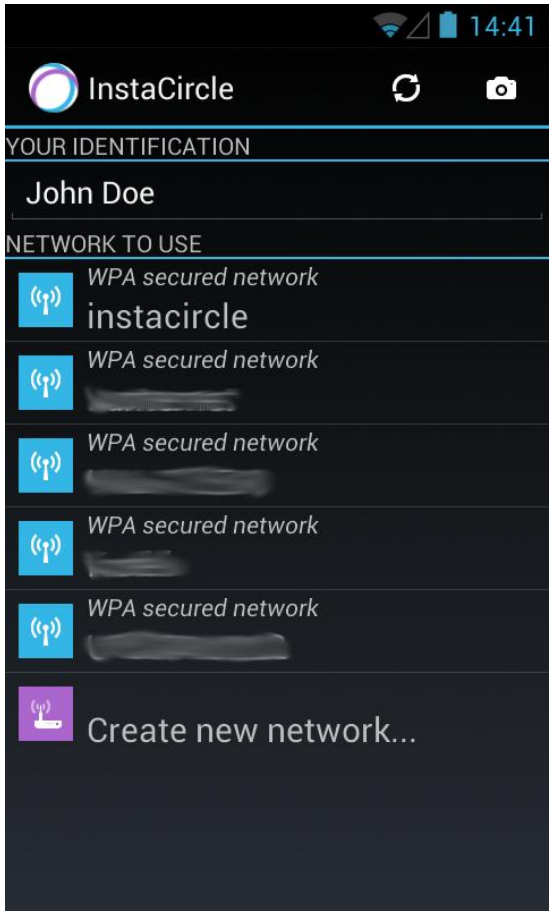
NFC

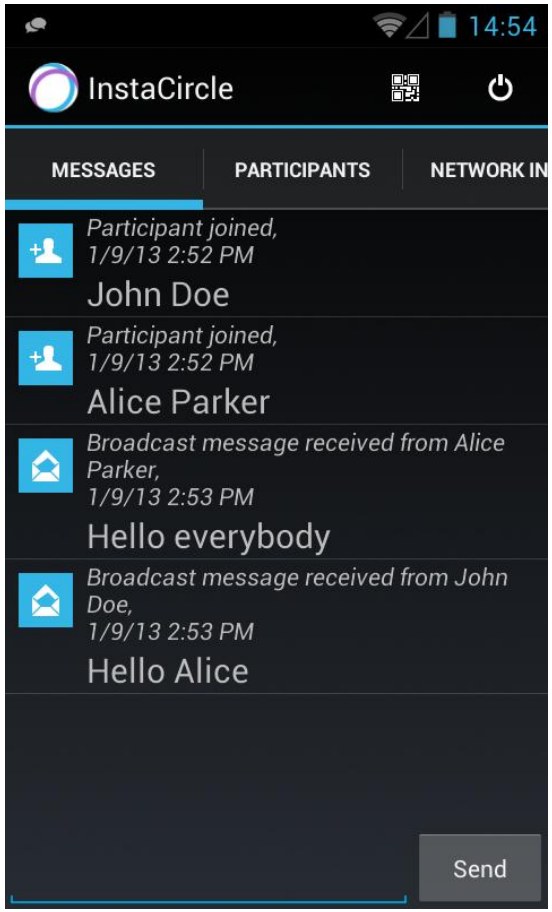
- Near Field Communication
  - Very shortrange communication (ca. 3 cm)
  - Similar to the RFID standard
  - Passive communication to NFC tags
  - Active communication to other devices
  - Low power consumption
  - Suitable for small amounts of data
  - Emerging standard → Available on new devices only

QR Codes

- Two-dimensional Barcode
- Encodes data in a bitmap which is readable by mobile devices
- Often used in marketing

Result: InstaCircle





Demo Video

SJbn.Co

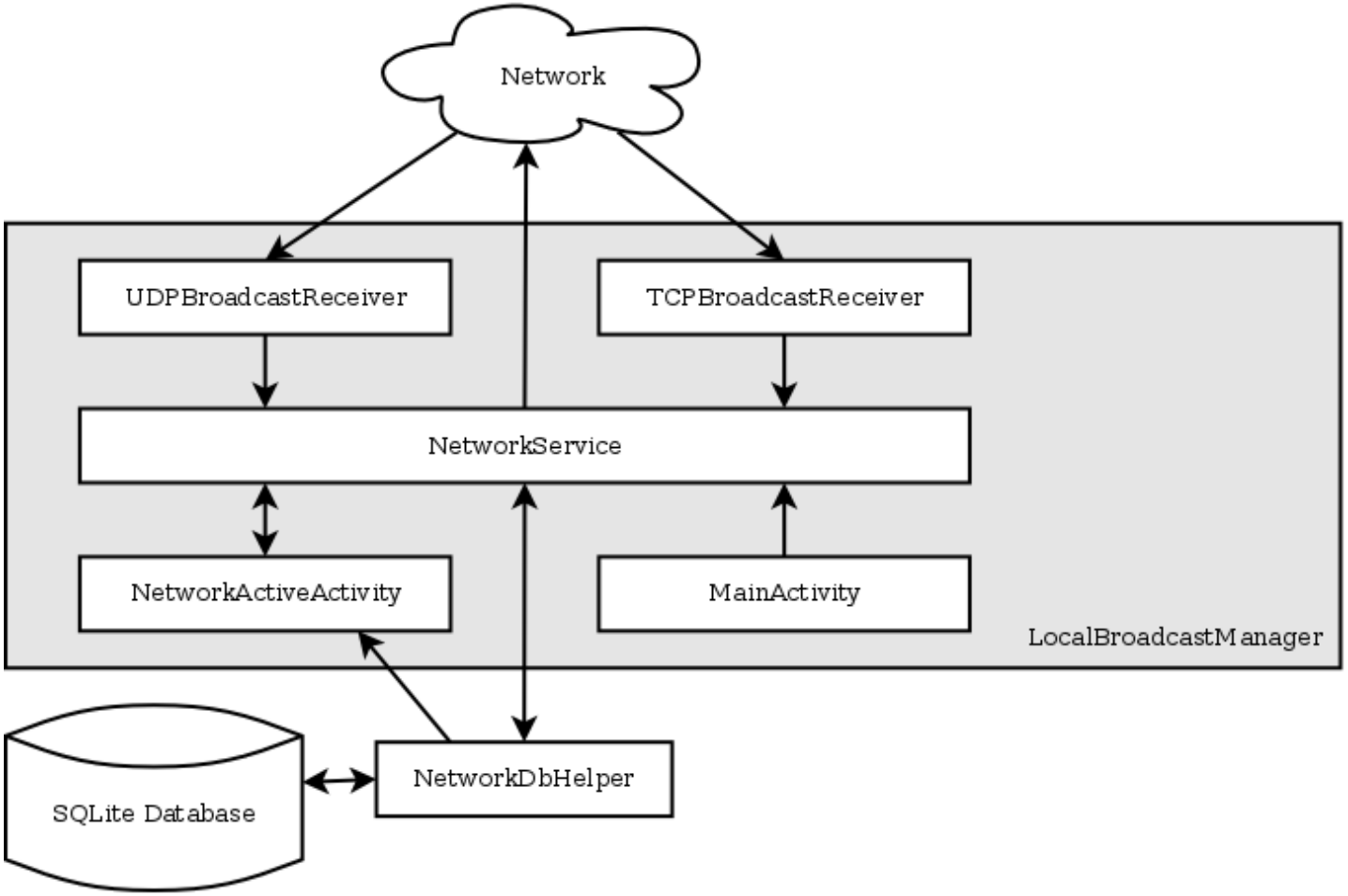
Features

- Create encrypted conversations on a new WLAN
- Create encrypted conversations on an existing WLAN
- Sharing mechanisms
  - Password
  - QR Code
  - NFC Tag
- Sending unicast messages to participants
- Resending mechanisms in case of message loss

Architecture (I)

- Application is based on Android components
  - Activities for the frontend
  - Service which is handling incoming and outgoing messages in the background
- Android broadcast mechanism for internal communication
- SQLite Database for message storage

Architecture (II)



Communication Technologies

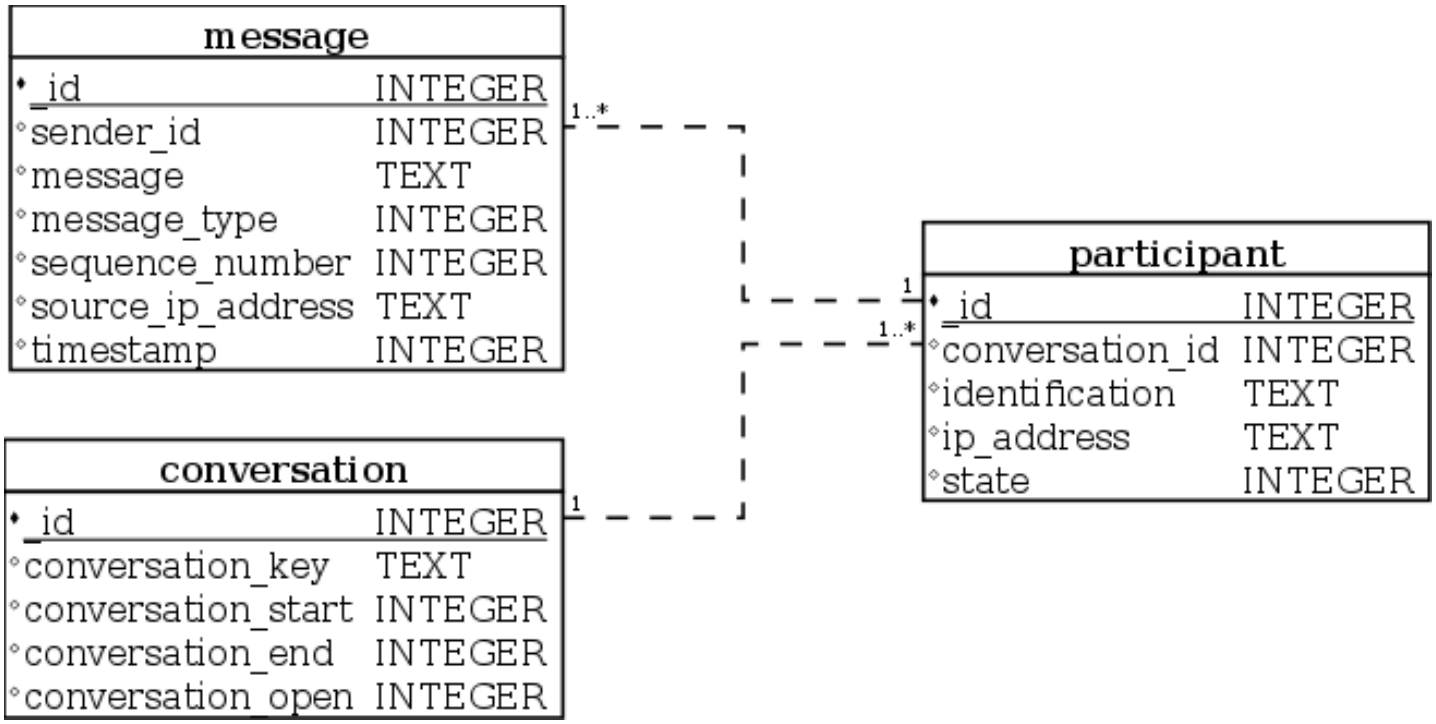
- Wi-Fi for data communication
- NFC for exchanging configurations
- QR Codes for exchanging configurations

Security

- Messages are encrypted using symmetric cryptography
- The symmetric key is derived from the password, the NFC tag or the QR code
- The access is restricted to people who
  - see or hear a password
  - see a QR code
  - have physical access to a NFC tag

  → Security based on physical location of the group

Data schema


message
_id INTEGER
sender_id INTEGER
message TEXT
message_type INTEGER
sequence_number INTEGER
source_ip_address TEXT
timestamp INTEGER
conversation
_id INTEGER
conversation_key TEXT
conversation_start INTEGER
conversation_end INTEGER
conversation_open INTEGER
participant
_id INTEGER
conversation_id INTEGER
identification TEXT
ip_address TEXT
state INTEGER
1..*
1
1..*
1

Problems and Challenges

- Reliable communication without a master
  - No centralized sequence number
  - No master time
- The Android Wi-Fi API
- The testing was restricted to 3 Samsung devices

Conclusion

- A decentralized communication platform for Android devices is available
- Decentralized broadcast communication is a challenge
- InstaCircle provides a platform for the two upcoming mastertheses

Discussion

- Are there…
  - any questions?
  - any remarks?

Bern University of Applied Sciences
Engineering and Information Technology

Thanks for your attention