Use-Case Analysis regarding Trust Relations in Dynamic Networks

Benedikt Veith∗, Anthony Kiggundu∗, Dennis Krummacker∗, Christoph Fischer∗ and Hans D. Schotten∗†
∗Intelligent Networks Research Group, German Research Center for Artificial Intelligence (DFKI GmbH), D-Kaiserslautern.
Email: {benedikt.veith | anthony.kiggundu | dennis.krummacker | christoph.fischer | hans_dieter.schotten}@dfki.de
†Institute for Wireless Communication and Navigation, RPTU University of Kaiserslautern-Landau, D-67663 Kaiserslautern.
Email: {schotten}@rptu.de

Table of Contents

1. Introduction
2. Methodology
3. Use Case Analysis
4. Requirements for Trust as a Service

Motivation

- 5G to 6G:
  - more dynamic deployments
  - more stakeholders
  - more autonomous operation
- increasing set of trust issues

  → should be handled explicitly by network components
- Open6GHub design goal: **Trust as a Service**

  → technical measures for increasing/enabling trustworthy interaction between independent actors
- this work: analysis of trust relations in specific use cases

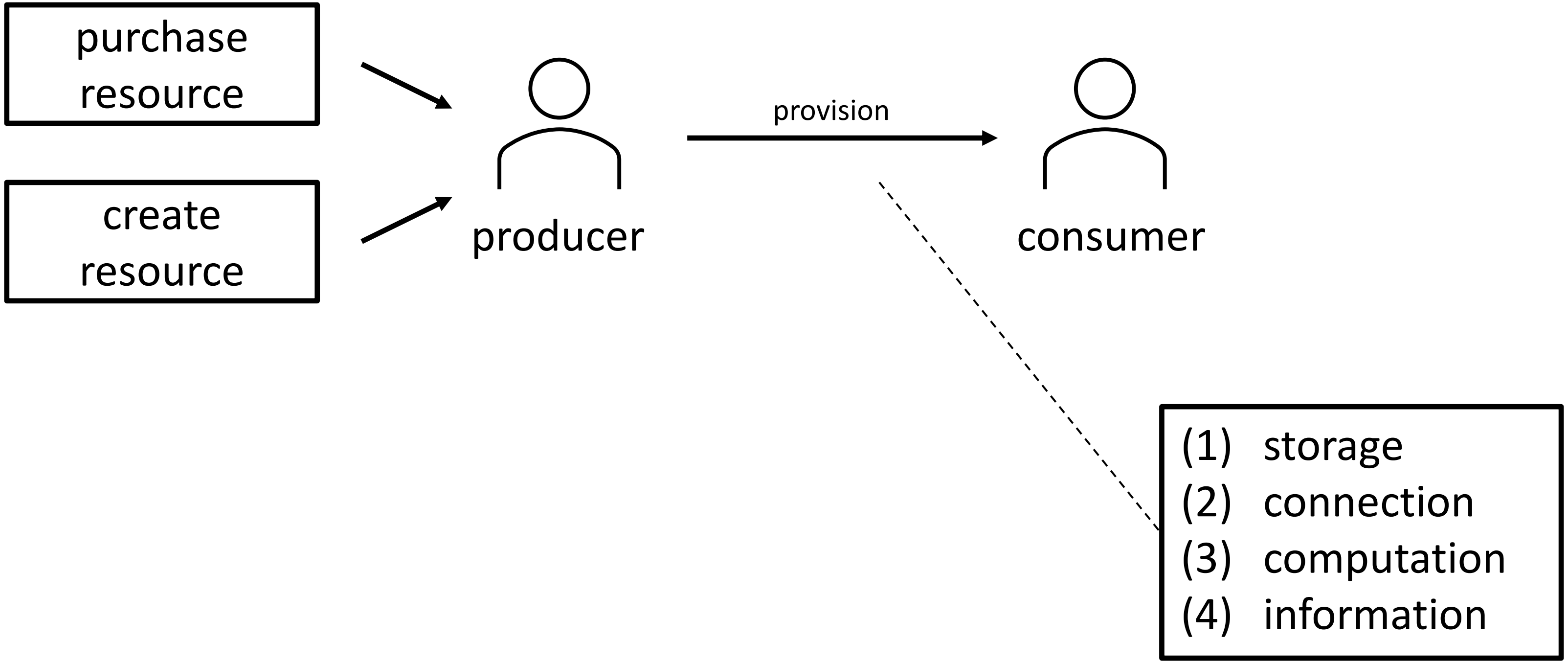
  → requirements for trust handling framework

Methodology: Roles vs. Actors

- some scenarios lead to dynamic role assignment in the network
- Actor:
  - an identity as it can be uniquely recognized by a specific technical system
  - tied to authentication framework and a secret source of truth (PUF, SIM, eSIM, asymmetrical keypair, etc.)
- Role:
  - scope of actions an Actor takes in a specific network and application context
- a device being compromised or a secret being stolen

  → the same Actor, possibly changing behavior

Methodology: Services



purchase resource

create resource

producer

provision

consumer

(1) storage
(2) connection
(3) computation
(4) information

Methodology: Trust Relations

- connection
  - single producer, multiple consumers
  - performance, integrity
  - protect from unauthorized access
- computation
  - privacy of input and output data
  - application of correct algorithm to input data
- storage
  - privacy, data access policy
  - integrity
- information
  - raw data, source code, etc.
  - privacy, restrictions on use of information, correctness

Use Cases

- Tactile Internet and Health Services
- Internet of Things and Digital Twins
- Omnipotent Terminals and Decentralized Control
- 3D Networks

Tactile Internet and Health Services

Scenarios:

- emergency, mobile medical facility
- Body Area Network (BAN) applications and handovers

Details:

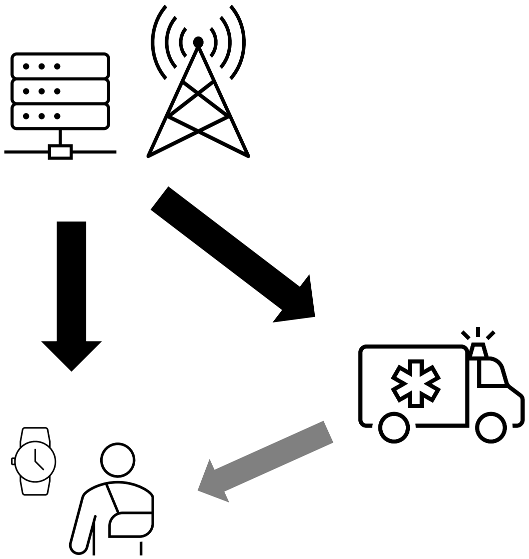
- sources of personal information:
  - medical devices in mobile facility
  - wearable devices in BAN
- privacy policy can not always be queried at patient (emergency cases)

Important Relations:

- storage: digital patient record to user
- computation: medical edge services to mobile facility (e.g. AI image recognition)

Specific Requirements:

- portable privacy policy configurations over different kinds of services
- traceability of information flows in emergency cases



Internet of Things and Digital Twins

Scenarios:

- task offloading between stationary IoT devices and UAVs
- interface from distribituted IoT devices to edge/fog infratructure
- DT: interaction between physical and digital assets

Details:

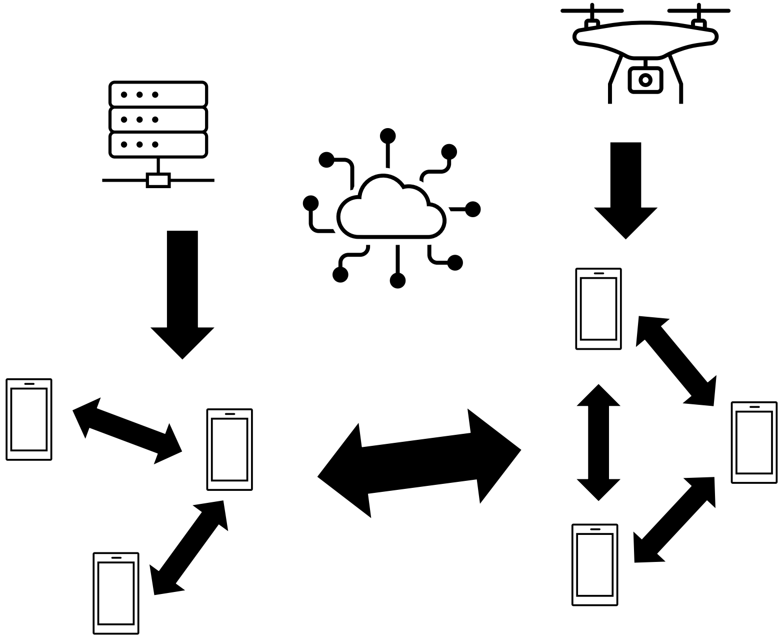
- autonomous interworking of many devices under separate control
- malicious injection of false data
- malfunctioning devices

Important Relations:

- communication: network to devices
- information: device to device across trust domains
- computation: edge to devices

Specific Requirements:

- Non-Repudiation of agents from different trust domains
- integrity of information, for traceability of behaviour



Omnipotent Terminals and Decentralized Control

Scenarios:

- D2D mesh, relay nodes, nomadic networks spawning out of static network

Details:

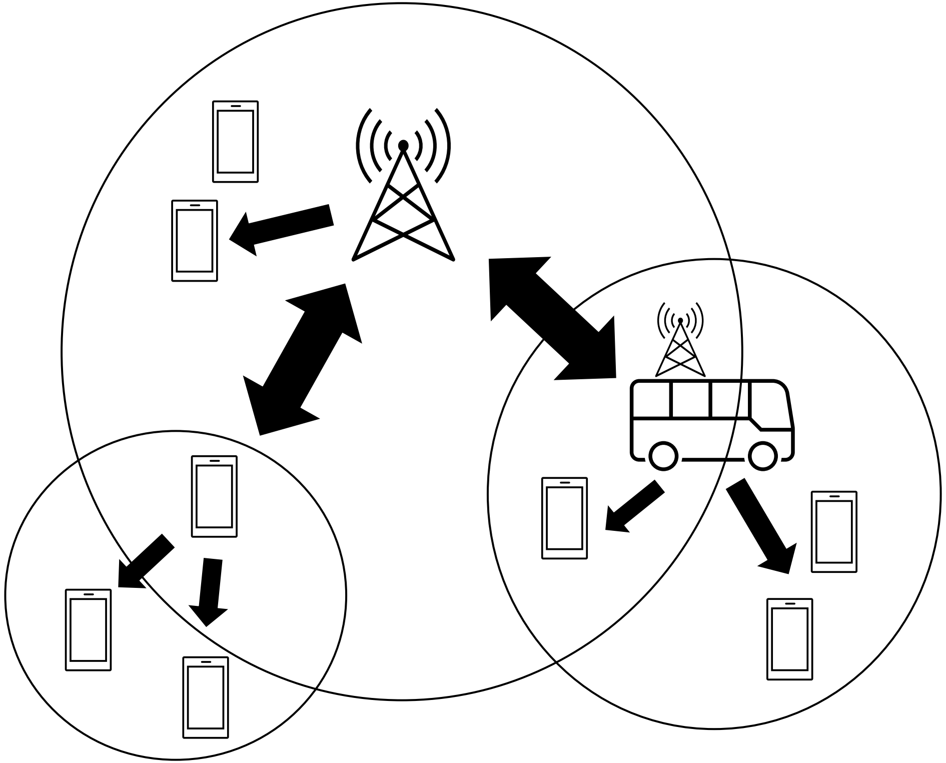
- negotiation for radio resources
- shift of operator responsibilities to distributed devices

Important Relations:

- provision of storage and connection among devices
- resource negotiation between nomadic networks

Specific Requirements:

- traceability of resource usage and channel conditions
- trusted negotiation platforms for radio resources
- reputation management for distributed nodes



3D Networks

Scenarios:

- High Altitude Platform Stations for broadband connectivity
- Underwater Internet of Things

Details:

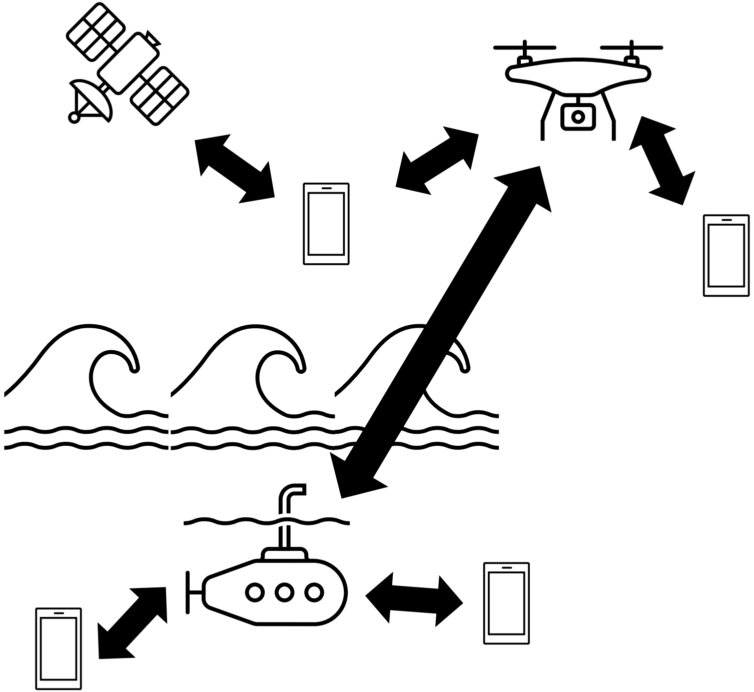
- dynamic network topology
- interaction with unknown mobile relay nodes

Important Relations:

- provision of connectivity

Specific Requirements:

- SLA Management
- compensation for missed performance objectives
- globally available authentication



Functional Requirements

Reputation Systems	trust relation management
Audit Logs	SLA logging, behavior traceability
Verifiable Databases	integrity proofs, verifiable consistency
Authenthication Mechanisms	identity management, non-repudiation

Thank you for your attention!

Questions to:

Benedikt Veith <benedikt.veith@dfki.de>